

NÚMEROS INCREÍBLES



«Ian Stewart explica las ideas más complicadas de forma amena y brillante.»

New Scientist

Ian Stewart

CRÍTICA

Reseña

Imagina un número tan largo que, si lo escribieras, ocuparía todo el universo. Aquí lo vas a encontrar, junto a todo tipo de números –reales, imaginarios, racionales, irracionales, positivos, negativos, simples y complejos–. Ian Stewart explora las asombrosas propiedades de números que van del cero al infinito y nos enseña cómo han cambiado a lo largo de la historia. El Profesor Stewart nos guía en el descubrimiento de los códigos matemáticos, los sudoku, el cubo de Rubik, la escala musical y cómo un tipo de infinito puede ser mayor que otro. Asimismo, descubre que vivimos en un espacio en once dimensiones. *Números increíbles* maravillará a los fanáticos de los números y convertirá a aquellos que creen no serlo.

Índice

Prefacio

Números

Números pequeños

Números complejos

Números racionales

Números irracionales

Números pequeños especiales

Números grandes especiales

Números infinitos

El sentido de la vida, el universo y...

Lecturas adicionales

Agradecimientos por las imágenes

Prefacio

Siempre me han fascinado los números. Mi madre me enseñó a leer y a contar mucho antes de que empezase a ir al colegio. Aparentemente, cuando lo hice, volví al final del día quejándome de no haber aprendido nada. Sospecho que mis padres me habían estado preparando para afrontar ese día difícil diciéndome que aprendería todo tipo de cosas interesantes, y yo me lo tomé al pie de la letra. Pero pronto comencé a aprender sobre planetas y dinosaurios y cómo hacer animales de yeso. Y más cosas sobre números.

Sigo encantado con los números y aprendiendo más sobre ellos. En la actualidad, enseguida puntuizo que las matemáticas versan sobre muchas ideas diferentes, no solo números, por ejemplo, sobre formas, patrones y probabilidades, aunque los números soportan toda la asignatura. Y todo número es único e individual. Hay unos cuantos números que son especiales y destacan sobre el resto porque parecen tener un papel central en muchas áreas diferentes de las matemáticas. El más conocido de ellos es π (pi), que lo encontramos relacionado con las circunferencias, pero tiene una tendencia extraordinaria a aparecer en problemas que nada tienen que ver con circunferencias.

La mayoría de los números no pueden aspirar a tales niveles de importancia, pero es posible encontrar alguna característica inusual de uniformidad en el más modesto de los números. En *Guía del*

autoestopista galáctico, el número 42 era «la respuesta a la gran pregunta sobre el sentido de la vida, el universo y todo lo demás». Douglas Adams dijo que escogió el número porque un sondeo rápido entre sus amigos reveló que era totalmente aburrido. En realidad no lo es, como demuestra el capítulo final.

El libro está organizado en términos de los propios números, aunque no siempre en orden numérico. Además de los capítulos 1, 2, 3, etcétera, haya también un capítulo 0, un capítulo 42, un capítulo -1, un capítulo $22/7$, un capítulo π , un capítulo $43.252.003.274.489.856.000$ y un capítulo $\sqrt{2}$. Claramente muchos capítulos potenciales nunca consiguieron salir de la recta numérica. Cada capítulo comienza con un pequeño resumen de los principales temas que en él se tratan. No te preocunes si el resumen a veces parece críptico o si hace afirmaciones rotundas sin ninguna evidencia: todo se desvelará a medida que avances en la lectura.

La estructura es clara: cada capítulo se centra en un número interesante y explica *por qué* lo es. Por ejemplo, 2 es interesante porque la distinción impar/par aparece en todas partes en matemáticas y ciencia; $43.252.003.274.489.856.000$ es interesante porque es el número de maneras de reorganizar un cubo de Rubik.

Ya que el 42 está incluido debe de ser interesante. Bueno, *un poco*.

En este punto debo mencionar *Alice's Restaurant Massacree*, de Arlo Guthrie, una comedia musical absurda que relata con gran y repetitivo

detalle los sucesos involucrados en el vertido de basuras. Pasados diez minutos de canción, Guthrie se para y dice: «Pero no es de eso de lo que he venido a hablarte aquí». Finalmente, averiguas de qué ha querido hablar en realidad, pues esa basura es solo una parte de una historia más amplia. Es hora de mi momento Arlo Guthrie: lo cierto es que este *no es* un libro sobre números.

Los números son el punto de partida, una ruta a través de la cual podemos zambullirnos en las asombrosas matemáticas asociadas a ellos. Cualquier número es especial. Llegas a apreciarlos uno a uno, son como viejos amigos. Cada uno tiene su propia historia para contar. Con frecuencia esa historia nos lleva a muchos de los otros números, pero lo que realmente importa son las matemáticas que los vinculan. Los números son los personajes de una obra, y lo más importante es la obra en sí. Pero no puede haber una obra sin personajes.

Para evitar acabar con demasiado desorden, he dividido el libro en apartados según el tipo de número: números naturales pequeños, fracciones, números reales, números complejos, infinito... Con unas cuantas inevitables excepciones, el material se desarrolla en un orden lógico, de modo que en los primeros capítulos recae el trabajo preparatorio para los siguientes, incluso cuando el tema cambia por completo. Este requisito influye en cómo están ordenados los números y requiere algunos compromisos. El más significativo tiene que ver con los números complejos. Aparecen muy pronto, porque los necesito para

discutir algunas características de números más familiares. De manera similar, un tema avanzado en ocasiones surge de la nada porque ese es el único lugar razonable para mencionarlo. Si te encuentras con uno de esos pasajes y te resulta difícil seguirlo, sáltatelo y sigue adelante. Podrás volver a él más tarde.

Este libro es un volumen de acompañamiento para mi aplicación para iPad *Incredible Numbers*. No necesitas la aplicación para leer el libro, y no necesitas el libro para usar la aplicación. De hecho, libro y aplicación apenas se solapan. Se complementan, porque cada uno puede hacer cosas que el otro no puede.

Los números son increíbles de verdad, no en el sentido de que no crees nada de lo que oyes sobre ellos, sino en el sentido positivo: tienen un insuperable componente de sorpresa y puedes experimentarlos sin hacer ninguna operación. Puedes ver cómo los números evolucionaron históricamente, apreciar la belleza de sus patrones, averiguar cómo se usan, maravillarte ante las sorpresas: «No tenía ni idea de que el 56 fuese tan fascinante». Pero lo es. Realmente lo es.

Así como lo son los demás. Incluido el 42.

Números

Contenido:

§. *El origen de los números*

§. *El sistema numérico creciente*

§. *¿Qué es un número?*

1, 2, 3, 4, 5, 6, 7,... ¿Hay algo más sencillo? Y no obstante son los números, quizá más que ninguna otra cosa, los que han permitido a la humanidad enfangarse y tocar las estrellas.

Cada número particular tiene sus propias características y nos lleva a una variedad de áreas de matemáticas. Sin embargo, antes de examinarlos uno por uno, merece la pena echar un vistazo a tres grandes cuestiones: ¿cómo se originaron los números?, ¿cómo se desarrolló el concepto de número? y ¿qué *son* los números?

§. **El origen de los números**

Hace alrededor de 35.000 años, en el Paleolítico Superior, un humano desconocido talló 29 marcas en el peroné de un babuino. Se encontró en una cueva en la cordillera Lebombo, en Suazilandia, y se conoce como el «hueso de Lebombo». Se cree que es un palo de conteo, algo que registra números como una serie de muescas: |, ||, |||, etcétera. Hay 29,5 días en el mes lunar, de modo que podría ser un primitivo calendario lunar, o el

registro del ciclo de menstruación de una mujer. O, es más, una colección aleatoria de cortes. Un hueso garabateado.

El hueso de lobo, otro palo de conteo con 55 muescas, lo encontró en Checoslovaquia, en 1937, Karl Absolon. Tiene alrededor de 30.000 años. En 1960, el geólogo belga Jean de Heinzelin de Braucourt descubrió un peroné de babuino con muescas entre los restos de una pequeña comunidad de pescadores que había sido sepultada por un volcán en erupción. La ubicación es lo que ahora se conoce como Ishango, en la frontera entre Uganda y el Congo. Se atribuye al hueso una antigüedad de 20.000 años.

La interpretación más sencilla del hueso de Ishango es la de que se trata de un palo de conteo. Algunos antropólogos van más allá y detectan elementos de estructura aritmética, como multiplicación, división y números primos; otros creen que es un calendario lunar de seis meses; y hay quienes están convencidos de que las marcas se hicieron para proporcionar un buen agarre a una herramienta hecha de hueso y que no tienen significado matemático.

Es muy enigmático. Hay tres series de muescas. La serie central usa los números 3, 6, 4, 8, 10, 5, 7. Dos veces 3 es 6, dos veces 4 es 8 y dos veces 5 es 10; sin embargo, el orden para el par final es el inverso y 7 no encaja en el patrón en absoluto. La serie de la izquierda es 11, 13, 17, 19: los números primos del 10 al 20. La serie de la derecha proporciona los

números impares 11, 21, 19, 9. Las series de derecha e izquierda suman cada una 60.



Figura 1. Parte frontal y trasera del hueso de Ishango. Museo de Ciencias Naturales de Bruselas.

Un problema con la interpretación de patrones como este es que es difícil no encontrar un patrón en cualquier serie de números más bien pequeños. Por ejemplo, en la Tabla 1 se muestra una lista de áreas de diez islas en las Bahamas, en concreto los números 11-20 en términos de área total. Para mezclar los números en la lista he puesto las islas en orden alfabético. Te aseguro que esto es lo primero que intenté. Ciento es que la habría cambiado por otra cosa si no me hubiese valido para explicar mi propósito, pero funcionó, así que no la cambié.

¿Qué notamos en este «patrón» de números? Hay muchas secuencias cortas con características comunes:

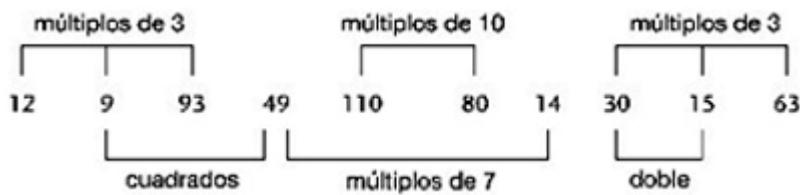


Figura 2. Algunos patrones aparentes en el área de las islas Bahamas.

Para empezar, hay una hermosa simetría en la lista. En cada extremo hay una terna de múltiplos de 3. En el medio, hay un par de múltiplos de 10, separando a dos múltiplos de 7. Además, dos cuadrados: $9 = 3^2$ y $49 = 7^2$, ambos cuadrados de números primos. Otro par adyacente está formado por 15 y 30, uno el doble del otro. En la secuencia 9-93-49, todos los dígitos tienen un 9. Los números crecen y decrecen de modo alterno, excepto por 110-80-14. ¡Oh! ¿Y te has dado cuenta de que *ninguno* de estos diez números es primo?

No hay más que decir. Otro problema con el hueso de Ishango es la imposibilidad virtual de encontrar evidencias extras que apoyen alguna interpretación concreta. Pero las marcas en él son realmente enigmáticas. Los rompecabezas de números siempre lo son. Así que vamos con algo menos polémico.

Hace diez mil años, en Oriente Medio la gente usaba piezas de barro para llevar un registro numérico. Quizá tenía que ver con los impuestos o como prueba de una propiedad. Los ejemplos más antiguos son Tepe Asiab y Ganj-iDareh Tepe, dos yacimientos en la cadena montañosa de

Zagros, en Irán. Las piezas eran pequeños trozos de barro de varias formas, algunas con marcas simbólicas.

Tabla 1

<i>Nombre</i>	<i>Área en millas cuadradas</i>
Berry	12
Bimini	9
Isla de Crooked	93
Pequeña Inagua	49
Mayaguana	110
Nueva Providencia	80
Isla Ragged	14
Cayo Rum	30
Cayo Sámana	15
Isla de San Salvador	63

Una bola marcada con + representaba una oveja, siete de esas bolas indicaban siete ovejas. Para evitar estar marcando un gran número de piezas, había una de un tipo diferente para diez ovejas. Y otra que representaba diez cabras, y así sucesivamente. La arqueóloga Denise Schmandt-Besserat dedujo que las piezas representaban elementos básicos de la época, como cereales, animales y jarras de aceite.

Alrededor de 4000 a. C., las piezas se unían con una cuerda a modo de collar. Como era fácil cambiar los números añadiendo o eliminando piezas, se introdujo una medida de seguridad: se envolvían las piezas con barro, que luego se cocía. Una discusión sobre los números podía resolverse rompiendo el sobre de barro para abrirlo. A partir de 3500 a. C., para evitar roturas innecesarias, los burócratas de la antigua Mesopotamia inscribían símbolos en el sobre, listando las piezas que había en él.

Fue entonces cuando una mente brillante se dio cuenta de que los símbolos convertían las piezas en redundantes. El resultado fue un sistema de símbolos numéricos escritos, lo cual estableció las bases de todos los sistemas subsiguientes de notación numérica y, posiblemente, de la propia escritura.

Como este libro no es de historia, daré la visión de sistemas notacionales posteriores como si surgiesen en conexión con números específicos. Por ejemplo, la notación decimal moderna y antigua se aborda en el capítulo [10]. Sin embargo, como el gran matemático Carl Friedrich Gauss señaló una vez, lo importante no son las notaciones, sino las nociones. Los temas que siguen tendrán más sentido si se ven en un contexto de concepción de los números cambiante por parte de la humanidad. De modo que empezaremos repasando los sistemas numéricos principales y alguna terminología importante.



Figura 3. Sobre de arcilla y piezas para la contabilidad, período de Uruk, de Susa.

§. El sistema numérico creciente

Tendemos a pensar en los números como algo fijo e inmutable: una característica del mundo natural. En realidad son una invención humana, pero una muy útil, porque representa aspectos importantes de la naturaleza, como cuántas ovejas posees o la edad del universo. La naturaleza nos sorprende reiteradamente destapando nuevas preguntas, cuyas respuestas a veces requieren nuevos conceptos matemáticos. Otras veces, la exigencia interna de indicios matemáticos en estructuras nuevas y potencialmente útiles. De vez en cuando estos indicios y problemas han llevado a los matemáticos a extender el sistema numérico inventando nuevos tipos de números.

Hemos visto cómo los números surgen primero como un método para contar cosas. En la temprana Grecia clásica, la lista de números empezaba 2, 3, 4, etcétera. El 1 era especial, no era «realmente» un número. Más tarde, cuando esta convención comenzó a parecer absurda, el 1 pasó a considerarse también un número.

El siguiente gran avance en la ampliación del sistema numérico fue la introducción de las fracciones. Estas son útiles para dividir algún producto entre varios. Si tres personas obtienen partes iguales de dos búsheles¹ de cereales, cada una recibe $\frac{2}{3}$ de un bushel.

Los antiguos egipcios representaban las fracciones de tres modos diferentes. Tenían jeroglíficos especiales para $\frac{2}{3}$ y $\frac{3}{4}$. Usaban varias porciones del ojo de Horus para representar 1 dividido por las primeras seis potencias de 2. Finalmente, ideaban símbolos para fracciones unitarias, las que son de la forma «uno sobre algo»: $\frac{1}{2}$, $\frac{1}{3}$, $\frac{1}{4}$, $\frac{1}{5}$, etcétera. Expresaban todas las otras fracciones como sumas de distintas fracciones unitarias. Por ejemplo:

$$\frac{2}{3} = \frac{1}{2} + \frac{1}{6}$$

No está claro por qué no escribían $\frac{2}{3}$, como $\frac{1}{3} + \frac{1}{3}$, pero no lo hacían.

El número cero llegó mucho después, probablemente porque no se necesitaba demasiado. Si no tienes ovejas, no hay necesidad de contarlas

¹ Unidad de medida de capacidad anglosajona. (*N. de la t.*)

o listarlas. Cero se introdujo primero como un símbolo y no se pensó en él como un número. Pero cuando los matemáticos chinos e hindúes introdujeron los números negativos [véase -1], el 0 tuvo que ser considerado un número también. Por ejemplo, $1 + (-1) = 0$, la suma de dos números debe sin duda contar como un número.



Figura 4. A la izquierda, jeroglíficos egipcios para $2/3$ y $3/4$. En el centro, ojo de Horus. A la derecha, jeroglífico de la fracción derivado de ellos.

Los matemáticos llaman al sistema de los números:

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

números naturales, y cuando se incluyen los números negativos, son los *enteros*.

..., $-3, -2, -1, 0, 1, 2, 3, \dots$

Las fracciones, el cero y las fracciones negativas forman los *números racionales*.

Un número es *positivo* si es mayor que cero, y *negativo* si es más pequeño que cero. De modo que cada número (ya sea un entero o un racional) está exactamente en una de las tres categorías: positivo, negativo o cero. Los números que usamos para contar:

$$1, 2, 3, 4, 5, 6, 7, \dots$$

son enteros positivos. Esta convención nos lleva a una terminología un poco burda: a menudo nos referimos a los números naturales:

$$0, 1, 2, 3, 4, 5, 6, 7, \dots$$

como los enteros *no negativos*. Siento esto.

Durante mucho tiempo, las fracciones fueron lo máximo que alcanzó el concepto de número. Pero en la antigua Grecia probaron que el cuadrado de una fracción nunca puede ser exactamente igual a 2. Más tarde esto se expresó como «el número $\sqrt{2}$ es irracional», esto es, no racional. Los griegos tenían un modo más engorroso de decir esto mismo, pero sabían que $\sqrt{2}$ debía existir: por el teorema de Pitágoras, es la longitud de la diagonal de un cuadrado de lado 1. Así que se necesitaban más números, los racionales solos no pueden hacerlo todo. Los griegos encontraron un

complicado método geométrico para lidiar con los números irracionales, pero no era completamente satisfactorio.

El siguiente paso hacia el concepto moderno de número fue hacer posible la invención de la coma decimal (,) y la notación decimal. Esto hizo posible representar los números irracionales con un grado alto de precisión. Por ejemplo:

$$\sqrt{2} \sim 1,4142135623$$

aproximado a 10 cifras decimales (el símbolo \sim significa «es aproximadamente igual a»). Esta expresión no es exacta: su cuadrado es realmente

$$1,9999999979325598129$$

Una aproximación mejor, que sería con 20 cifras decimales, es esta:

$$\sqrt{2} \sim 1,41421356237309504880$$

pero de nuevo no es exacta. Sin embargo, hay un sentido lógico riguroso en el cual una expansión decimal infinita es exacta. Por supuesto, esa expresión no puede escribirse completa, pero es posible establecer las ideas para que tenga sentido.

Los decimales con parte decimal infinita (incluyendo aquellos que la tienen finita, pues pueden pensarse como decimales que terminan en una cantidad infinita de ceros) se llaman *números reales*, en parte porque corresponden directamente a medidas del mundo natural como longitudes o pesos. Cuanto más precisa sea la medición, más cifras decimales necesitas; para obtener un valor exacto, necesitas infinitas. Tal vez resulte irónico que «real» esté definido por un símbolo infinito que no puede escribirse completamente. Los números reales negativos también están permitidos.

Hasta el siglo XVIII ningún otro concepto matemático se consideró como números genuinos. Pero ya en el siglo XV, unos cuantos matemáticos se preguntaron si habría un tipo de número nuevo: la raíz cuadrada de menos uno. Esto es, un número que da -1 cuando lo multiplicas por sí mismo. A primera vista se trata de una idea disparatada, porque el cuadrado de cualquier número real es positivo o cero. Sin embargo, resultó ser una buena idea seguir adelante y equipar a -1 con una raíz cuadrada, para lo cual Leonhard Euler introdujo el símbolo i . Esta es la letra inicial de «imaginario» (en inglés, latín, francés, alemán y español) y se llamaron así para distinguirlos de los viejos números reales. Por desgracia, esto llevó a mucho misticismo innecesario —Gottfried Leibniz una vez se refirió a i como «un anfibio entre ser y no ser»—, lo cual complicó una verdad clave. En concreto, tanto números reales como imaginarios tiene exactamente la misma

condición lógica. Son conceptos humanos que modelan la realidad, pero no son reales por sí mismos.

La existencia de i hace necesario introducir muchos otros números nuevos para poder hacer cálculos aritméticos, números como $2 + 3i$. Estos se llaman *números complejos*, y han sido indispensables en matemáticas y ciencias durante los últimos siglos. Es curioso, porque lo cierto es que son nuevos para la mayoría de la raza humana, pues no sueles encontrarte con números complejos en las matemáticas del colegio; no porque carezcan de importancia, sino porque las ideas son demasiado sofisticadas y las aplicaciones demasiado avanzadas.

Los matemáticos utilizan símbolos con florituras para los principales sistemas numéricos. No los usaré de nuevo, pero deberías verlos al menos una vez:

N = el conjunto de todos los números naturales $0, 1, 2, 3, \dots$

Z = el conjunto de todos los números enteros $-3, -2, -1, 0, 1, 2, 3, \dots$

Q = el conjunto de todos los números racionales

R = el conjunto de todos los números reales

C = el conjunto de todos los números complejos

Estos sistemas encajan unos dentro de otros como unas matrioskas:

$$N \subset Z \subset Q \subset R \subset C$$

El símbolo de la teoría de conjuntos \subset significa «está contenido en». Observa que, por ejemplo, todo entero es racional; un ejemplo sería el entero 3, que es también la fracción. Normalmente no lo escribimos de este modo, pero ambas notaciones representan el mismo número. De manera similar, todo número racional es también real, y todo real es también complejo. Los sistemas más antiguos se incorporan a los nuevos, no se reemplazan.

Incluso los números complejos no son el final de las extensiones del sistema numérico que los matemáticos han hecho a lo largo de los siglos. Están los cuaterniones H y los octoniones O [véase 4], por ejemplo. Sin embargo, estos son más provechosos desde un punto de vista algebraico que aritmético. Y acabaré mencionando un número más paradójico: infinito. Desde un punto de vista filosófico, infinito difiere de los números convencionales y no pertenece a ninguno de los sistemas numéricos estándar, desde los números naturales a los números complejos. Sin embargo, merodea por los márgenes, con un aspecto numérico pero sin ser un número como tal. Hasta que Georg Cantor revisó nuestro punto de partida, contar, y mostró que no solo infinito es un número en el sentido de contar, sino también que hay diferentes tamaños de infinito. Entre ellos están \aleph_0 , el número de números naturales, y C , el número de números reales, el cual es mayor. Cuanto

mayor es discutible: depende del sistema de axiomas que uses para formalizar las matemáticas.

Pero dejemos estos números hasta que hayamos desarrollado la suficiente intuición sobre números más ordinarios. Lo que me lleva a la tercera cuestión.

§. ¿Qué es un número?

Parece una pregunta sencilla, y lo es. Pero no así la respuesta.

Todos sabemos cómo usar los números. Todos sabemos qué aspecto tienen siete vacas, siete ovejas o siete sillas. Todos podemos contar hasta siete. Pero *¿qué es* siete?

No es el símbolo 7. Esa es una elección arbitraria y es diferente en muchas culturas. En árabe es , en chino es  o más formalmente .

No es la palabra «siete». En francés es *sept*, en alemán es *sieben*.

Hacia mediados del siglo XIX, algunos matemáticos con mentalidad lógica se dieron cuenta de que, aunque todo el mundo había estado usando los números durante miles de años, nadie sabía realmente qué eran. Así que hicieron la pregunta que nunca debería haberse formulado: *¿qué es* un número?

Es una pregunta más complicada de lo que parece. Un número no es algo que puedas mostrar a alguien en el mundo físico. Es una abstracción, un concepto mental humano, uno derivado de la realidad, pero no exactamente *real*.

Puede sonar preocupante, pero los números no son solo eso. Un ejemplo común es el «dinero». Todos sabemos cómo pagar algo y cuál es su cambio, y lo hacemos —ingenuamente imaginamos— intercambiando dinero. Tendemos a pensar en dinero como las monedas y billetes en nuestros bolsillos o carteras. Sin embargo, no es tan simple. Si usamos la tarjeta de crédito, no hay intercambio de monedas o billetes. En su lugar, hay señales que pasan a través de un sistema telefónico a la compañía de la tarjeta y finalmente a nuestro banco, y las cifras en las cuentas bancarias —la nuestra, la de la tienda, la de la compañía de la tarjeta— cambian. Un billete británico de 5 libras usado para llevar el mensaje «Prometo pagar bajo demanda al portador la suma de cinco libras», no es dinero en absoluto, sino la promesa de pagar dinero. Hubo un tiempo en el que podías llevarlo al banco y cambiarlo por oro, lo que era considerado como el dinero *real*. Ahora, todo lo que el banco haría sería cambiártelo por otro billete de 5 libras. Pero el oro tampoco era realmente dinero, era solo una manifestación física de este. Como prueba, el valor del oro no es fijo.

¿Es entonces el dinero un número? Sí, pero solo con un contexto legal específico. Escribir 1.000.000 de dólares en un trozo de papel no te convierte en millonario. Lo que hace que el dinero sea *dinero* es un cuerpo de convenciones humanas sobre cómo representamos los números del dinero y cómo lo cambiamos por bienes u otros números.

Lo que importa es lo que haces con él, no lo que es. El *dinero* es una abstracción.

Lo mismo pasa con los números. Aunque esta respuesta no resuelve mucho, porque *todo* en matemáticas es una abstracción. De modo que unos cuantos matemáticos siguieron preguntándose qué *tipo* de abstracción podía definir «número». En 1884, un matemático alemán llamado Gottlob Frege escribió *Los fundamentos de la aritmética*, estableciendo los principios fundamentales sobre los que se basan los números. Una década después, fue más allá, e intentó derivar esos principios de las leyes más básicas de la lógica. Su *Leyes básicas de la aritmética* se publicó en dos volúmenes, el primero en 1893 y el segundo en 1903.

Frege empezó a partir del proceso de contar y no se centró en los números que usamos, sino en las cosas que contamos. Si pones siete tazas en una mesa y las cuentas: «1, 2, 3, 4, 5, 6, 7», los objetos importantes parecen ser los números, pero para Frege lo importante eran las tazas. Contar tiene sentido porque tenemos una colección de tazas que queremos contar. Con una colección diferente, tendríamos un número diferente. Frege llamó a estas colecciones *clases* (en alemán). Cuando contamos cuántas tazas contiene esta clase en particular, establecemos una *correspondencia* entre la clase de las tazas y los símbolos numéricos 1, 2, 3, 4, 5, 6, 7.

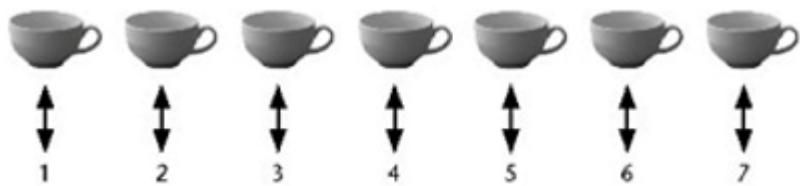


Figura 5. Correspondencia entre tazas y números.

De modo similar, dada una clase de platos, quizá seamos capaces de establecer también esta correspondencia:

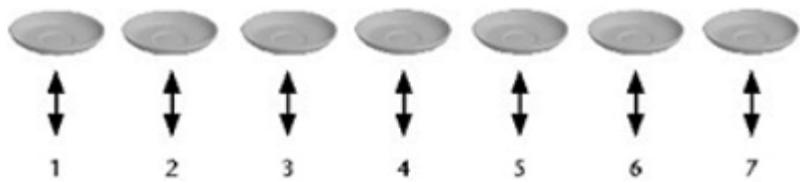


Figura 6. Correspondencia entre platos y números.

En tal caso, podemos concluir que la clase de platos contiene el mismo número de platos que la clase de tazas contiene de tazas. Incluso sabemos cuántos: siete.

Esto podría parecer obvio hasta el punto de la banalidad, pero Frege se dio cuenta de que nos estaba diciendo algo bastante profundo. En concreto, que podemos probar que la clase de platos contiene el mismo número de platos que la clase de tazas contiene de tazas, *sin* usar los símbolos 1, 2, 3, 4, 5, 6, 7 y sin saber cuántas tazas o platos hay. Es suficiente con establecer una correspondencia entre la clase de tazas y la clase de platos:



Figura 7. Correspondencia entre tazas y platos sin necesidad de números.

Técnicamente, este tipo de correspondencia es conocido como una correspondencia *uno a uno*: cada taza se empareja exactamente con un plato, y cada plato se empareja exactamente con una taza. El contar no funciona si te olvidas de alguna taza o cuentas la misma taza varias veces. Lo llamaremos correspondencia, mientras recordemos esta condición técnica.

Por cierto, si alguna vez te has preguntado por qué los niños en la escuela pasan cierto tiempo «emparejando» conjuntos de vacas con conjuntos de pollos, o cualquier otra cosa, dibujando líneas entre las imágenes, es culpa de Frege. Algunos educadores esperaban (y puede que todavía esperen) que su planteamiento podría mejorar la intuición para los números. Yo me inclino a verlo como promover la lógica e ignorar la psicología y acabar confundido en lo que se refiere al significado de «fundamental», pero no reiniciemos una guerra matemática aquí.

Frege concluyó que emparejar clases usando una correspondencia se encuentra en el fondo de lo que entendemos por «número». Contar cuántas cosas contiene una clase tan solo empareja esa clase con una clase estándar, cuyos miembros se denotan con los símbolos

convencionales 1, 2, 3, 4, 5, 6, 7, etcétera, dependiendo de la cultura de uno. Pero Frege no creía que el concepto de número debiese depender de la cultura, de modo que encontró un modo de evitar de una vez símbolos arbitrarios. Más exactamente, inventó un super símbolo universal, el mismo para cualquier cultura. Pero no puedes escribirlo, pues era algo puramente conceptual.

Empezó señalando que los miembros de una clase pueden ser clases ellos mismos. No tienen que serlo, pero no hay nada que lo impida. Una caja de latas de alubias es un ejemplo del día a día: los miembros de la caja son latas y los miembros de las latas son alubias. De modo que es correcto usar clases como miembros de otras clases.

El número «siete» está asociado, por correspondencia, a cualquier clase que se pueda emparejar con nuestra clase de tazas o la correspondiente clase de platos o la clase que consiste en los símbolos 1, 2, 3, 4, 5, 6, 7. Escoger una clase en concreto de estas y llamar *a eso* un número es una decisión arbitraria que carece de elegancia y resulta insatisfactoria. Así que ¿por qué no jugarse el todo por el todo y usar todas estas clases? Entonces «siete» puede definirse como la *clase de todas las clases* que están en correspondencia con cualquiera (por tanto todas) de las clases que acabamos de mencionar. Haciendo esto, podemos decir si cualquier clase dada tiene siete miembros comprobando si es miembro de esta clase de clases. Por comodidad etiquetamos esta clase de clases como «siete», pero la propia clase tiene sentido incluso si no lo hacemos. De

modo que Frege distinguió un número de un nombre arbitrario (o símbolo) para ese número.

Podría entonces definir qué es un número: es la clase de las clases que está en correspondencia con una clase dada (por tanto, también con las otras). Este tipo de clase es a lo que me refería como «super símbolo». Si estás en esta línea de pensamiento, esta es una idea brillante. De hecho, en lugar de escoger un nombre para el número, conceptualmente agrupamos *todos los posibles nombres* juntos en un único objeto y usamos ese objeto en su lugar.

¿Funcionó? Lo podrás ver más adelante, en el capítulo [\aleph_0].

Números pequeños

Contenido:

1. *La unidad indivisible*
2. *Pares e impares*
3. *Ecuación cúbica*
4. *Cuadrado*
5. *Hipotenusa pitagórica*
6. *Número de osculación*
7. *Cuarto primo*
8. *Cubo de Fibonacci*
9. *Cuadrado mágico*
10. *Sistema decimal*

1. La unidad indivisible

El número entero positivo más pequeño es el 1. Es la unidad indivisible en aritmética: el único número entero positivo que no puede obtenerse sumando dos números enteros positivos más pequeños.

§. Bases del concepto de número

El número 1 es por el que empezamos a contar. Dado cualquier número, creamos el número siguiente añadiendo 1:

$$2 = 1 + 1$$

$$3 = (1 + 1) + 1$$

$$4 = ((1 + 1) + 1) + 1$$

y así sucesivamente. Los paréntesis nos indican qué operaciones realizamos primero. Normalmente se omiten porque resulta que en este caso el orden no importa, pero es mejor ser cuidadoso al principio.

A partir de estas definiciones y las leyes básicas del álgebra, las cuales en un desarrollo lógico formal deben enunciarse explícitamente, podemos incluso probar el famoso teorema « $2 + 2 = 4$ ». La prueba cabe en una línea:

$$2 + 2 = (1 + 1) + (1 + 1) = ((1 + 1) + 1) + 1 = 4$$

En el siglo XX, cuando algunos matemáticos estaban intentando establecer los fundamentos de las matemáticas sobre unas bases lógicas firmes, usaron la misma idea, pero por razones técnicas empezaron desde 0 [véase 0].

El número 1 expresa una idea matemática importante: la de *unicidad*. Un objeto matemático con una propiedad particular es único si solo *un* objeto tiene esa propiedad. Por ejemplo, 2 es el único número primo par.

La unicidad es importante porque nos permite probar que algunos objetos matemáticos ligeramente misteriosos en realidad son objetos que ya conocemos. Por ejemplo, si podemos probar que algún número positivo n desconocido es a la vez par y primo, entonces n debe ser igual a 2. Para un ejemplo más complicado, el dodecaedro es el único sólido regular con caras pentagonales [véase 5]. De modo que si en alguna obra de matemáticas nos encontramos con un sólido regular con caras pentagonales, sabemos de inmediato, sin tener que hacer nada más, que tiene que ser un dodecaedro. Todas las demás propiedades de un dodecaedro vienen entonces a continuación.

§. Tabla del uno

Nunca nadie se ha quejado por tener que aprender la tabla del uno. «Uno por uno es uno, uno por dos es dos, uno por tres es tres...» Si multiplicamos cualquier número por 1, o lo dividimos por 1, sigue siendo el mismo número.

$$n \times 1 = n \quad n : 1 = n$$

Es el único número que se comporta de este modo.

En consecuencia, 1 es igual a su cuadrado, su cubo y todas las potencias mayores:

$$1^2 = 1 \times 1 = 1$$

$$1^3 = 1 \times 1 \times 1 = 1$$

$$1^4 = 1 \times 1 \times 1 \times 1 = 1$$

y así sucesivamente. Hay solo otro número con esta propiedad, el 0.

Por esta razón, generalmente el número 1 se omite en álgebra cuando aparece como coeficiente en una fórmula. Por ejemplo, en lugar de $1x^2 + 3x + 4$, escribimos $x^2 + 3x + 4$. Solo hay otro número tratado de esta manera, el 0, con el cual sucede algo todavía más drástico: en lugar de $0x^2 + 3x + 4$, escribimos $3x + 4$, y dejamos fuera el término $0x^2$ por completo.

§. ¿Es 1 primo?

Solía serlo, pero ya no lo es. El número no ha cambiado, pero la definición de «primo» sí.

Algunos números pueden obtenerse multiplicando otros dos números. Por ejemplo, $6 = 2 \times 3$ y $25 = 5 \times 5$. Este tipo de número decimos que es *compuesto*. Otros números no se pueden obtener de este modo: son los que llamamos *primos*.

Según esta definición, 1 es primo, y hasta hace 150 años esa era la convención estándar. Pero entonces resultó que era más conveniente

considerar 1 como un caso excepcional. En la actualidad se considera que ni es primo ni es compuesto, sino que es la *unidad*. Lo explicaré enseguida, pero antes necesitamos introducir otras ideas.

La secuencia de primos empieza

2 3 5 7 11 13 17 19 23 29 31 37 41 47

y aparentemente es muy irregular, excepto por unos cuantos patrones sencillos. Todos los primos excepto el 2 son impares, porque cualquier número par es divisible entre 2. Solo 5 puede acabar en 5 y ninguno puede acabar en 0, porque esos números son divisibles por 5.

Todo número entero mayor que 1 puede expresarse como un producto de números primos. Este proceso se llama *factorización* y los primos involucrados en él se llaman los *factores primos* del número. Además, la factorización es única, dejando al margen el cambiar de orden en el cual aparecen los factores. Por ejemplo:

$$60 = 2 \times 2 \times 3 \times 5 = 2 \times 3 \times 2 \times 5 = 5 \times 3 \times 2 \times 2$$

etcétera, pero el único modo de obtener 60 es reordenar la primera lista de primos. Por ejemplo, no hay una factorización en números primos que sea $60 = 7 \times$ algo.

Esta propiedad se llama «unicidad de la factorización en números primos». Probablemente parece obvio, pero a menos que hayas hecho una carrera de matemáticas, me sorprendería que alguien te hubiese indicado cómo probarlo. Euclides expuso una demostración en sus *Elementos* y se debió de dar cuenta de que no es obvio ni fácil, porque se toma su tiempo preparando el terreno. Para algunos sistemas más generales parecidos a los numéricos, ni siquiera es cierto. Pero sí lo es para la aritmética ordinaria, y es un arma muy efectiva en la armería matemática.

Las factorizaciones de los números del 2 al 31 son:

2 (primo)	3 (primo)	$4 = 2^2$
5 (primo)	$6 = 2 \times 3$	7 (primo)
$8 = 2^3$	$9 = 3^2$	$10 = 2 \times 5$
11 (primo)	$12 = 2^2 \times 3$	13 (primo)
$14 = 2 \times 7$	$15 = 3 \times 5$	$16 = 2^4$
17 (primo)	$18 = 2 \times 3^2$	19 (primo)
$20 = 2^2 \times 5$	$21 = 3 \times 7$	$22 = 2 \times 11$
23 (primo)	$24 = 2^3 \times 3$	$25 = 5^2$
$26 = 2 \times 13$	$27 = 3^3$	$28 = 2^2 \times 7$
29 (primo)	$30 = 2 \times 3 \times 5$	31 (primo)

La principal razón para tratar al 1 como un caso excepcional es que si contamos 1 como primo, entonces la factorización no es única. Por ejemplo $6 = 2 \times 3 = 1 \times 2 \times 3 = 1 \times 1 \times 2 \times 3$, etcétera. Una consecuencia aparentemente extraña de esta convención es que 1 no tiene factores primos. Sin embargo, aun así es un producto de primos de un modo bastante extraño: 1 es el producto de un «conjunto vacío» de primos. Esto es, *sino multiplicas ningún número primo*, obtienes 1. Probablemente parezca una locura, pero hay razones sensatas para esta convención. De modo similar, si «multiplicas» *un* único número primo, obtienes ese primo.

2. Pares e impares

Los números pares son divisibles por 2; los números impares no lo son. Por lo tanto, 2 es el único número primo par. Es una suma de dos cuadrados: $2 = 1^2 + 1^2$. Los otros primos con esta propiedad son precisamente aquellos cuyo resto es 1 al dividirlos por 4. Los números que son una suma de dos cuadrados pueden caracterizarse en términos de sus factores primos.

La aritmética binaria, usada en los ordenadores, está basada en potencias de 2 en lugar de en potencias de 10. Las ecuaciones cuadráticas, en las que está involucrada una potencia de dos de un número desconocido, pueden resolverse usando raíces cuadradas.

La distinción entre pares e impares se extiende a las permutaciones, que son modos de ordenar un conjunto de objetos. La mitad de las permutaciones son pares y la otra mitad impares. Te mostraré una aplicación clara: una prueba sencilla de que un famoso rompecabezas no puede resolverse.

§. Paridad (pares/impares)

Una de las distinciones más importante en todas las matemáticas es la que hay entre números pares e impares.

Empecemos con los números naturales 0, 1, 2, 3,... Entre ellos, los números pares son:

0 2 4 6 8 10 12 14 16 18 20...

y los impares son:

1 3 5 7 9 11 13 15 17 19 21...

En general, cualquier número natural que es múltiplo de 2 es par y cualquier número natural que no es múltiplo de 2 es impar. En contra de lo que algunos profesores parecen creer, 0 es par, porque es múltiplo de 2, en concreto, 0×2 .

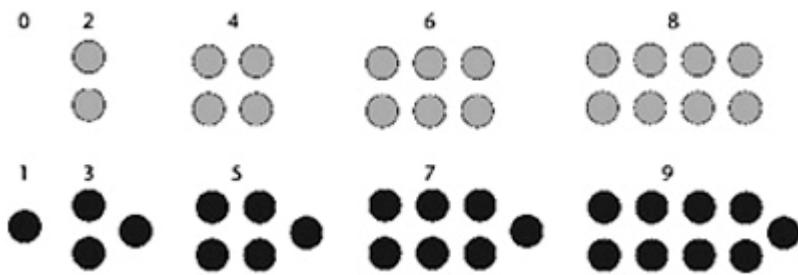


Figura 8. Números pares e impares.

Los números impares tienen resto igual a 1 cuando se dividen entre 2 (el resto es distinto de 0 y menor que 2, lo cual solo deja 1 como posibilidad). De modo que, algebraicamente, los números pares son de la forma $2n$, donde n es un número natural, y los números impares son de la forma $2n + 1$. (De nuevo, si tomamos $n = 0$, tenemos que 0 es par.) Para extender el concepto «par» e «impar» a los números negativos, permitimos que n sea negativo. Entonces $-2, -4, -6$, etcétera, son pares y $-1, -3, -5$, etcétera, son impares. Los números pares e impares se alternan a lo largo de la recta numérica.

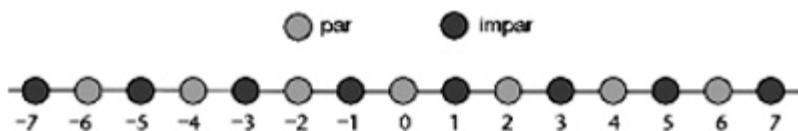


Figura 9. Los números pares e impares se alternan a lo largo de la recta numérica.

Una característica agradable de los números pares e impares es que obedecen a reglas aritméticas sencillas:

par + par = par

impar + impar = par

par + impar = impar

impar + par = impar

par × par = par

impar × impar = impar

par × impar = par

impar × par = par

no importa el número en concreto de que se trate. De modo que si alguien afirma que $13 \times 17 = 222$, sabes que está equivocado *sin* hacer los cálculos: impar × impar = impar y 222 es par.

§. El primo más pequeño y el único par

La lista de números primos empieza con 2, de modo que 2 es el número primo más pequeño. También es el único número primo par, porque por definición todos los números pares son divisibles por 2. Si el número que nos ocupa es 4 o mayor, se expresa como el producto de dos números más pequeños, de modo que es compuesto. Estas propiedades, aunque sean sencillas y obvias, dan a 2 un estatus de unicidad entre todos los números.

§. Teorema de los dos cuadrados

En el día de Navidad de 1640, el brillante matemático aficionado Pierre de Fermat escribió al monje Marín Mersenne y le hizo una pregunta intrigante: ¿qué números pueden escribirse como una suma de dos cuadrados perfectos?

El cuadrado de un número es lo que obtienes cuando lo multiplicas por sí mismo. Así, el cuadrado de 1 es $1 \times 1 = 1$, el cuadrado de 2 es $2 \times 2 = 4$, el cuadrado de 3 es $3 \times 3 = 9$, etcétera. El símbolo para el cuadrado de un número n es n^2 . De modo que $0^2 = 0$, $1^2 = 1$, $2^2 = 4$, $3^2 = 9$, etcétera.

Los cuadrados de los números del 0 al 10 son:

0 1 4 9 16 25 36 49 64 81 100

Por lo tanto, 4 es el primer cuadrado perfecto después de los menos interesantes 0 y 1.

La palabra «cuadrado» se usa porque estos números surgen al colocar puntos juntos en cuadrados.

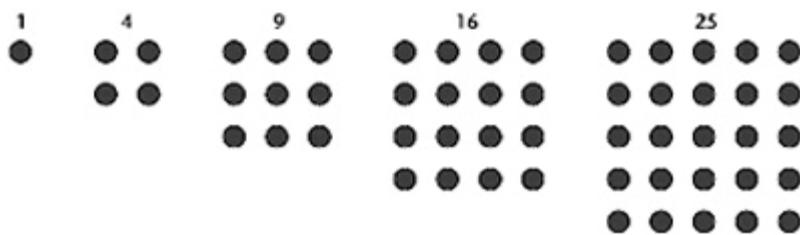


Figura 10. Cuadrados.

Cuando sumamos los cuadrados de dos en dos, obviamente podemos obtener los propios cuadrados; basta sumar 0 al cuadrado. Pero también obtenemos números como

$$1 + 1 = 2$$

$$4 + 1 = 5$$

$$4 + 4 = 8$$

$$9 + 1 = 10$$

$$9 + 4 = 13$$

$$16 + 1 = 17$$

que no son cuadrados. Aun así, muchos números no aparecen, por ejemplo, 3, 6, 7, 11.

Tabla 2

0	1	4	9	16	25	36	49	64	81	100	
0	0	1	4	9	16	25	36	49	64	81	100
1	1	2	5	10	17	26	37	50	65	82	
4	4	5	8	13	20	29	40	53	68	85	
9	9	10	13	18	25	34	45	58	73	90	
16	16	17	20	25	32	41	52	65	80	97	
25	25	26	29	34	41	50	61	74	89		
36	36	37	40	45	52	61	72	83			

49 49 50 53 58 65 74 98
64 64 65 68 73 80 89
81 81 82 85 90 97
100 100

A continuación hay una tabla que muestra todos los números del 0 al 100 que son suma de dos cuadrados. (Para obtener el número de las celdas que no están en negrita, suma el número en negrita en la parte superior de su columna con el número en negrita a la izquierda de su misma fila. Por ejemplo, $25 + 4 = 29$. Se han omitido las sumas mayores que 100.) A primera vista, es difícil encontrar un patrón, pero hay uno, que Fermat descubrió. El truco es escribir los *factores primos* de los números en la tabla. Dejando fuera el 0 y el 1, que son excepciones, tenemos:

$$\begin{array}{ccc}
 \underline{2=2} & 4=2^2 & \underline{5=5} \\
 8=2^3 & 9=3^2 & 10=2 \times 5 \\
 \underline{13=13} & 16=2^4 & \underline{17=17} \\
 18=2 \times 3^2 & 20=2^2 \times 5 & 25=5^2 \\
 26=2 \times 13 & \underline{29=29} & 34=2 \times 17 \\
 36=2^2 \times 3^2 & \underline{37=37} & 40=2^3 \times 5 \\
 \underline{41=41} & 45=3^2 \times 5 & 49=7^2 \\
 50=2 \times 5^2 & \underline{53=53} & 58=2 \times 29
 \end{array}$$

$$\begin{array}{lll}
 \underline{61 = 61} & 64 = 2^6 & 65 = 5 \times 13 \\
 68 = 2^2 \times 17 & 72 = 2^3 \times 3^2 & \underline{73 = 73} \\
 74 = 2 \times 37 & 80 = 2^4 \times 5 & 81 = 3^2 \\
 82 = 2 \times 41 & 85 = 5 \times 17 & \underline{89 = 89} \\
 90 = 2 \times 3^2 \times 5 & \underline{97 = 97} & 100 = 2^2 \times 5^2
 \end{array}$$

He subrayado los números que son primos, porque son la clave para el problema.

Faltan algunos primos, en concreto: 3, 7, 11, 19, 23, 31, 43, 47, 59, 67, 71, 79 y 83. ¿Puedes emular a Fermat y descubrir su característica común?

Cada uno de estos primos es un múltiplo de 4 menos 1. Por ejemplo, $23 = 24 - 1$ y $24 = 6 \times 4$. El primo 2 aparece en mi lista, de nuevo, lo cual es excepcional en algunos aspectos. *Todos* los primos impares en mi tabla son un múltiplo de 4 más 1. Por ejemplo, $29 = 28 + 1$ y $28 = 7 \times 4$. Los primeros primos de esta forma aparecen todos en mi lista y, es más, si la ampliase, parece que no faltaría ninguno.

Todo número impar es o bien un múltiplo de 4 menos 1 o bien un múltiplo de 4 más 1, esto es, es de la forma $4k - 1$ o $4k + 1$, para todo número natural k . El único primo par es 2. De modo que todo primo debe cumplir una de las siguientes condiciones:

- ser igual a 2
- ser de la forma $4k + 1$

- ser de la forma $4k - 1$

Los primos que faltan en mi lista de la suma de dos cuadrados son precisamente los primos de la forma $4k - 1$.

Estos primos pueden aparecer como *factores* de los números en la lista. Observa al 3, por ejemplo, que es factor de 9, 18, 36, 45, 72, 81 y 90. No obstante, todos estos números son en realidad múltiplos de 9, esto es, de 3^2 .

Si observas listas más largas desde el mismo punto de vista, aparece un patrón sencillo. En su carta, Fermat afirmaba haber probado que los números distintos de cero que son suma de dos cuadrados son *precisamente* aquellos para los que todo factor primo de la forma $4k - 1$ aparece con una potencia par. La parte más difícil era probar que todo primo de la forma $4k + 1$ es la suma de dos cuadrados. Albert Girard solo había llegado a hacer conjeturas en 1632, pero no había probado nada.

La tabla incluye algunos ejemplos, pero comprobemos el argumento de Fermat con algo un poco más ambicioso. El número 4.001 es claramente de la forma $4k + 1$; basta tomar k igual a 1.000. Es también primo. Por el teorema de Fermat, debería ser una suma de dos cuadrados. ¿Cuáles?

En ausencia de un método más inteligente, podemos intentar sustraer 1^2 , 2^2 , 3^2 , etcétera por turnos, y ver si obtenemos un cuadrado. Los cálculos empiezan así:

$$4.001 - 1^2 = 4.000: \text{no es un cuadrado}$$

$$4.001 - 2^2 = 3.997: \text{no es un cuadrado}$$

$$4.001 - 3^2 = 3.992: \text{no es un cuadrado}$$

Y finalmente llegamos a

$$4.001 - 40^2 = 2.401: \text{es el cuadrado de } 49$$

De modo que

$$4.001 = 40^2 + 49^2$$

y Fermat lo explica usando un ejemplo.

Esta es esencialmente la única solución, además de $49^2 + 40^2$. Obtener un cuadrado restando un cuadrado de 4.001 es un resultado raro, casi parece que fortuito. Fermat explicó por qué no lo es. También sabía que cuando $4k + 1$ es primo, hay solo un modo de dividirlo en dos cuadrados.

En general, no hay un camino sencillo y práctico de encontrar los números correctos. Gauss proporcionó una fórmula, pero no es muy práctica. La prueba tiene que demostrar que el cuadrado requerido existe, aunque sin proporcionar una manera rápida de encontrarlo, lo cual es algo técnico y requiere mucha preparación, por lo que no intentaré explicar la demostración aquí. Uno de los encantos de las matemáticas es

que afirmaciones verdaderas y sencillas no siempre se demuestran fácilmente.

§. Sistema binario

Nuestro sistema numérico tradicional se llama «decimal», porque usa 10 como su número base y en latín 10 es *decem*. Hay diez dígitos 0-9 y el valor de los dígitos se multiplica por 10 en cada posición que se avanza de derecha a izquierda. Así, 10 significa diez; 100, un centenar, 1.000, un millar; etcétera [véase 10].

Pueden establecerse sistemas de notación similares para números usando cualquier número como base. El más importante de estos sistemas de notación alternativos, llamado binario, usa base 2. Tiene solo dos dígitos, 0 y 1, y el valor de un dígito se dobla en cada posición que avanza de derecha a izquierda. En binario, 10 quiere decir 2 (usando nuestra notación decimal), 100 quiere decir 4, 1.000 quiere decir 8, 10.000 quiere decir 16, etcétera.

Para obtener números que no son potencias de 2, sumamos distintas potencias de 2. Por ejemplo, 23 en decimal es igual a

$$16 + 4 + 2 + 1$$

que usa un 16, ningún 8, un 4, un 2 y un 1. De modo que en notación binaria pasa a ser

10111

Los primeros números binarios y sus equivalentes decimales son:

<i>decimal</i>	<i>binario</i>	<i>decimal</i>	<i>binario</i>
----------------	----------------	----------------	----------------

0	0	11	1011
1	1	12	1100
2	10	13	1101
3	11	14	1110
4	100	15	1111
5	101	16	10000
6	110	17	10001
7	111	18	10010
8	1000	19	10011
9	1001	20	10100
10	1010	21	10101

Para «decodificar» los símbolos, por ejemplo, para el número 20, los escribimos como potencias de 2:

1 0 1 0 0

16 8 4 2 1

Las potencias de 2 que se dan con el símbolo 1 son 16 y 4. Súmalas: el resultado es 20.

§. Historia

En algún momento entre 500 a. C. y 100 a. C., el académico hindú Pingala escribió un libro llamado Chandahśāstra sobre rimas en poesía y listó diferentes combinaciones para sílabas largas y breves. Clasificó esas combinaciones usando una tabla, la cual en su forma moderna usa 0 para una sílaba breve y 1 para una larga. Por ejemplo,

00 = breve-breve

01 = breve-larga

10 = larga-breve

11 = larga-larga

Los patrones aquí son los mismos que en la notación binaria, pero Pingala no hacía cálculos aritméticos con sus símbolos.

El antiguo libro chino de adivinación, el *I Ching* (*Yì Jīng*), usaba 64 conjuntos de seis líneas horizontales, bien completas (*yang*) o partidas en dos (*yin*), como un oráculo. Estos conjuntos se conocen como *hexagramas*. Cada hexagrama consiste en dos *trigramas* puestos uno sobre otro. Originariamente el hexagrama era usado para predecir el futuro, arrojando tallos de milenrama al suelo y aplicando unas reglas para determinar qué hexagrama deberías observar. Más tarde pasaron a usarse tres monedas.

Si usamos 1 para representar una línea completa (*yang*) y 0 para una partida (*yin*), cada hexagrama se corresponde a un número binario de

seis dígitos. Por ejemplo, el hexagrama en la Figura es 010011. Según el método de adivinación, este es el hexagrama 60 (節 = jié), e indica «articulación», «limitación» o «moderación». Una interpretación típica (no me pidas que la explique porque no tengo ni idea) comienza:

Limitación Sobre: k'an lo catastrófico, agua. Bajo: *tui* la alegría, lago.
Juicio Limitación, éxito. Limitación irritante no debe ser perseverada.

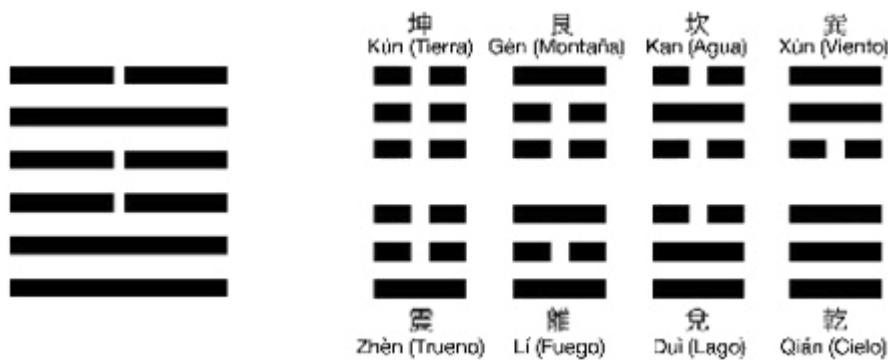


Figura 11. A la izquierda, un hexagrama. A la derecha, los ocho trigramas.

Image Agua sobre lago: la imagen de la limitación. Así el hombre superior crea números y medida, y examina la naturaleza de la virtud y la conducta correcta.

De nuevo, aunque los patrones binarios están presentes en el *I Ching*, la aritmética no lo está. En los escritos de Thomas Harriot (1560-1621) aparece más sobre la estructura matemática de los símbolos binarios, que dejó miles de páginas de manuscritos no publicados. Uno de ellos contiene una lista que empieza

1 1

2 2

3 2 + 1

4 4

5 4 + 1

6 4 + 2

7 4 + 2 + 1

y continúa hasta

$$30 = 16 + 8 + 4 + 2$$

$$31 = 16 + 8 + 4 + 2 + 1$$

Está claro que Harriot entendió el principio básico de la notación binaria. Sin embargo, el contexto de esta lista es una larga serie de tablas enumerando cómo varios objetos pueden combinarse de maneras diferentes, no aritmética.

En 1605, Francis Bacon explicó cómo codificar letras del alfabeto como secuencias de dígitos binarios, y se acercó mucho a usarlas como números. Los binarios finalmente llegaron como una notación aritmética en 1697, cuando Leibniz escribió al duque Rudolph de Brunswick proponiendo un «medallón o moneda conmemorativo».



Figura 12. Medallón binario de Leibniz.

El diseño muestra una tabla de las representaciones binarias de los números del 0 al 15, con la inscripción *Omnibus ex nihilo ducendis sufficit unum* («Para todo lo que surge de la nada, uno basta»). Matemáticamente, Leibniz está indicando que si tienes el símbolo 0 (nada) y añades el 1 (uno), entonces puedes obtener cualquier número (todo). Pero también estaba haciendo una afirmación religiosa simbólica: un único Dios puede crear todo de la nada.

La medalla nunca se acuñó, pero su solo diseño fue un paso significativo. En 1703, Leibniz estaba desarrollando las matemáticas binarias y publicó

un artículo «*Explication de l'arithmétique binaire*» en *Mémoires de l'Académie Royale des Sciences*. Escribió:

«En lugar de esta progresión por las decenas [notación decimal], durante muchos años he usado la más sencilla de todas, la que va de dos en dos». Indica que las reglas para la aritmética binaria son tan sencillas que nadie se puede olvidar de ellas, pero también dice que, debido a que la forma binaria de un número es alrededor de cuatro veces más larga que su forma decimal, el método no es práctico. En cierto modo profético, también dijo que «el cálculo de dos en dos es más fundamental para la ciencia y proporciona nuevos descubrimientos» y «estas expresiones de números facilitan mucho todo tipo de operaciones».

Esto es lo que tenía en mente. Para realizar cálculos aritméticos con números binarios, todo lo que necesitas saber es:

$$0 + 0 = 0$$

$$0 + 1 = 1$$

$$1 + 0 = 1$$

$$1 + 1 = 0 \text{ llevando } 1$$

$$0 \times 0 = 0$$

$$0 \times 1 = 0$$

$$1 \times 0 = 0$$

$$1 \times 1 = 1$$

Una vez que conoces esta información sencilla, puedes sumar y multiplicar dos números binarios cualesquiera, usando métodos similares a los que usas en aritmética ordinaria. También puedes hacer restas y divisiones.

§. Computación digital

Ahora sabemos que Leibniz dio en el clavo cuando sugirió que el sistema binario sería «fundamental para la ciencia». El sistema binario fue originariamente una rareza matemática, pero la invención de ordenadores digitales ha cambiado esto. La electrónica digital está basada en una distinción simple entre presencia, o ausencia, de una señal eléctrica. Si simbolizamos estos dos estados con 1 y 0, la razón para trabajar con un sistema binario se hace evidente. En principio, podemos construir ordenadores usando el sistema decimal, por ejemplo, permitiendo que los dígitos 0-9 se correspondan con señales a 0 voltios, 1 voltio, 2 voltios, etcétera. Sin embargo, en cálculos complicados se darían imprecisiones y no estaría claro si una señal de, por ejemplo, 6,5 voltios es el símbolo 6 en un voltaje elevado, o el símbolo 7, en uno reducido. Usando solo dos niveles de voltaje, muy separados, las ambigüedades de este tipo pueden eliminarse asegurándose que el error es siempre mucho más pequeño que la diferencia entre los dos niveles.

Con los métodos de fabricación actuales, sería posible construir ordenadores fiables usando base 3, o bases mayores, en lugar de 2. Pero ya se ha fabricado una cantidad enorme de tecnología usando el sistema binario, y es fácil pasar de binario a decimal como parte de la computación, de modo que otras bases no proporcionan una ventaja lo suficientemente grande comparadas con el sistema binario estándar.

§. Paridad de una permutación

La distinción entre números pares e impares es especialmente importante en la teoría de permutaciones, la cuales son modos de reordenar un lista ordenada de números o letras u otros objetos matemáticos. Si la lista contiene n objetos, entonces el número total de permutaciones posibles es el factorial

$$n! = n \times (n - 1) \times (n - 2) \times \dots \times 3 \times 2 \times 1$$

porque podemos escoger el primer número de n maneras, el segundo de $n - 1$, el tercero de $n - 2$, etcétera [véase 26!].

Hay dos tipos de permutaciones: *pares* e *impares*. Las permutaciones pares intercambian el orden de un número de pares de objetos par; las permutaciones impares intercambian el orden de un número de pares de objetos impar. Enseguida hablaré de esto con más detalle. A este «par» o «impar» se le conoce como la *paridad* de la permutación.

De las $n!$ posibles permutaciones, exactamente la mitad son pares y la otra mitad impares (excepto $n = 1$, caso en el que hay una permutación par y ninguna impar). De modo que cuando $n \geq 2$, hay $n!/2$ permutaciones pares y $n!/2$ impares.

Podemos comprender la diferencia entre permutaciones pares e impares usando diagramas. Por ejemplo, piensa en la permutación (que llamaremos A) que empieza con la lista

$$1, 2, 3, 4, 5$$

y la reordena del siguiente modo:

$$2, 3, 4, 5, 1$$

Los números en la lista se mueven como ves en la Figura:

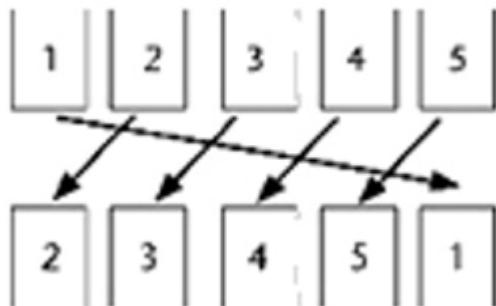


Figura 13. Diagrama para la permutación A.

De manera similar, si empezamos con la lista

2, 3, 4, 5, 1

y la reordenamos así:

4, 2, 3, 1, 5

entonces los símbolos se mueven como se indica en el siguiente diagrama:

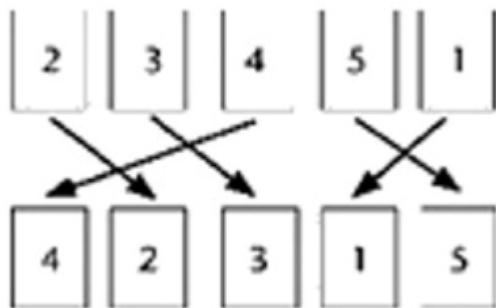


Figura 14. Diagrama para la permutación B.

Llama a esta permutación *B*. Observa que la lista en la que empezamos no necesita estar en un orden numérico habitual. Lo que cuenta no es el orden como tal, sino *cómo este cambia*.

§. Composición de permutaciones

Podemos *componer* (o combinar) dos permutaciones para crear otra. Al hacer esto, reordenamos la lista según la primera permutación y luego la

reordenamos según la segunda. El proceso es más fácil de entender al poner los dos diagramas juntos.

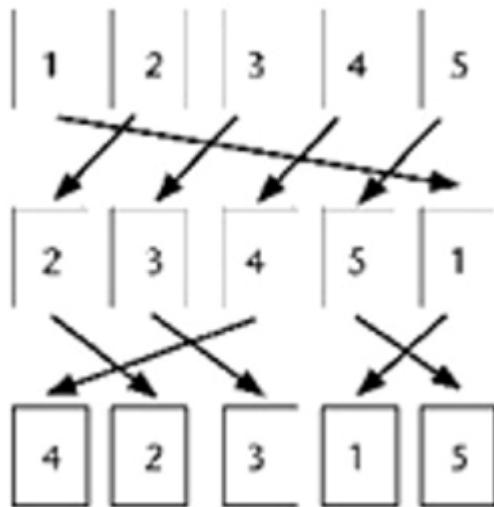


Figura 15. Diagrama de la permutación A seguida de la B.

Las dos permutaciones A y B se muestran con la fila superior de flechas y la fila inferior de flechas. Para componerlas (con lo que obtendremos una permutación que llamaré AB), seguimos pares de flechas que se correspondan y eliminamos la fila de números de en medio. Obtenemos esto:

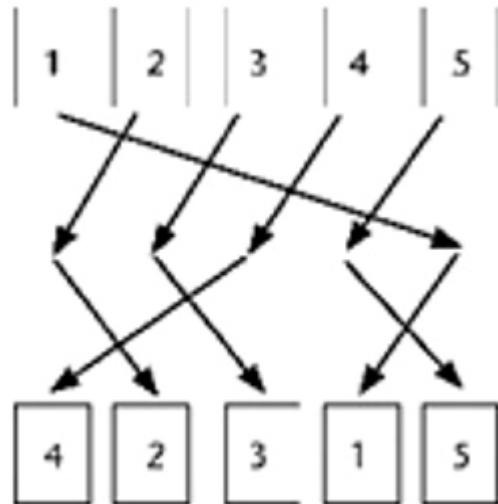


Figura 16. Diagrama para la permutación AB, antes de unificar las flechas.

Finalmente, unificamos las flechas para obtener:

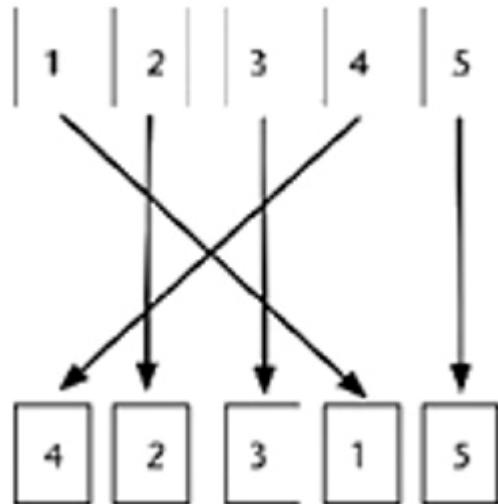


Figura 17. Diagrama para la permutación AB, después de unificar las flechas.

Esta es la permutación que convierte a la lista

1, 2, 3, 4, 5

en la lista

4, 2, 3, 1, 5.

§. Número de intersecciones y paridad

En la permutación A , la flecha más larga cruza las otras cuatro flechas. Decimos que esta permutación tiene un *total* de 4 *intersecciones* y lo escribimos como $c(A) = 4$. La permutación B tiene 3 intersecciones, $c(B) = 3$. Su composición AB tiene 5 intersecciones, $c(AB) = 5$.

Antes de que unificásemos las flechas, AB tenía 7 intersecciones. Es la suma del número de intersecciones de A y B : $4 + 3 = 7$. Cuando unificamos las flechas, dos intersecciones desaparecieron, las dos en la parte de la derecha. Estas dos flechas se cruzaban la una con la otra, y luego se volvían a cruzar. De modo que la segunda intersección «anula» a la primera.

Esta observación es cierta en general. Si componemos dos permutaciones cualesquiera A y B para obtener AB , entonces, antes de que se unifiquen y enderecen las flechas, el número de intersecciones de AB es el número de A más el número de B . Cuando enderezamos las flechas, el número de intersecciones puede permanecer igual o se sustraer un número par. De modo que aunque $c(AB)$ no necesariamente es igual a $c(A) + c(B)$, su

diferencia es siempre par. Y eso significa que la paridad de $c(AB)$ es la suma de las paridades de $c(A)$ y $c(B)$.

Decimos que una permutación A es par si $c(A)$ es par, e impar si $c(A)$ es impar. Por consiguiente, la *paridad* de la permutación A es «par» o «impar».

Una permutación par intercambia el orden de un número de pares de símbolos par.

Una permutación impar intercambia el orden de un número de pares de símbolos impar.

Esto implica que cuando componemos permutaciones:

par compuesto con par da par

impar compuesto con impar da par

par compuesto con impar da impar

impar compuesto con par da impar

igual que cuando se suman números pares e impares. Estas propiedades se usan en todas partes en matemáticas.

§. Juego del 15

Las paridades de las permutaciones podrían parecer un tema bastante técnico, pero tienen muchas aplicaciones. Una de las más entretenidas es un juego inventado por un norteamericano llamado Noyes Chapman. Se

hizo muy popular y se extendió a lo largo de Estados Unidos, Canadá y Europa. El empresario Mathias Rice lo fabricó como el Gen Puzzle y un dentista llamado Charles Leve ofreció un premio a quien fuese capaz de resolverlo. Se le conoce también con otros nombres como Cuadrado místico o Puzzle del 15.

El juego está formado por 15 piezas cuadradas corredizas, numeradas del 1 al 15; se empieza con los números ordenados excepto por el 14 y el 15 y una casilla vacía en la parte inferior a la derecha (véase la Figura de la izquierda). El objetivo del juego es deslizar piezas sucesivas en la casilla vacía (que se mueve a medida que las piezas se deslizan) y poner los cuadrados en el orden correcto (Figura de la derecha).

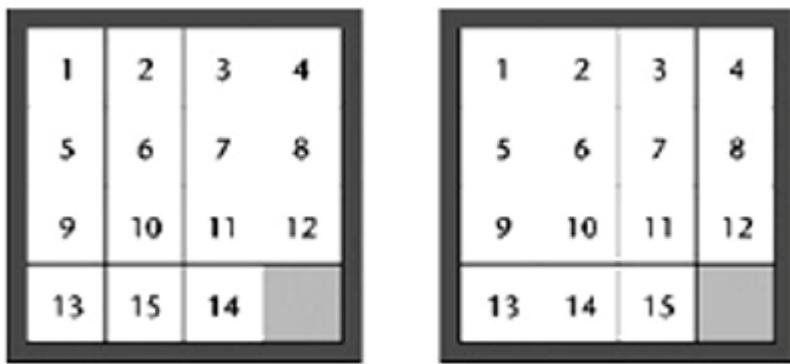


Figura 18. Se empieza esto... ... y se acaba con esto.

Este juego suele atribuirse al famoso autor de rompecabezas Sam Lloyd, que reavivó el interés en él en 1886 ofreciendo un premio de mil libras. Sin embargo, Lloyd estaba seguro de que el dinero no corría riesgo,

porque en 1879, William Johnson y William Storey habían probado que el Juego del 15 no tenía solución.

El punto fundamental es que cualquier posición en el juego puede pensarse como una permutación de la posición original, contando la casilla vacía como una «virtual» decimosexta pieza. La posición original, junto un par de piezas (14 y 15) intercambiadas, es una permutación impar de la posición final que se desea. Pero el requisito de que la casilla vacía acabe en el mismo sitio que empezó, implica que los movimientos permitidos solo llevan a permutaciones pares.

Por lo tanto, los movimientos permitidos, empezando por cualquier estado inicial, pueden llegar exactamente a la *mitad* de $16!$ reordenamientos posibles, que son $10.461.394.944.000$ reordenamientos. Por ensayo y error es imposible explorar más de una fracción de estas posibles disposiciones, lo cual fácilmente puede convencer a la gente de que si lo siguen intentando, podrían dar con una solución.

§. Ecuaciones cuadráticas

Los matemáticos distinguen las ecuaciones algebraicas por su grado, que es la mayor potencia de la incógnita que aparece. El grado de la ecuación

$$5x - 10 = 0$$

es uno, porque solo aparece la potencia de uno de x . El grado de

$$x^2 - 3x + 2 = 0$$

es dos, porque aparece el cuadrado (la potencia de 2) de x , pero no aparecen potencias mayores. El grado de

$$x^3 - 6x^2 + 11x - 6 = 0$$

es tres. Y así sucesivamente.

Hay nombres especiales para las ecuaciones de grados pequeños:

grado 1 = lineal

grado 2 = cuadrática

grado 3 = cúbica

grado 4 = cuártica

La principal tarea cuando aparece una ecuación es resolverla. Esto es, encontrar el valor (o valores) de la incógnita x que la verifiquen. La ecuación lineal $5x - 10 = 0$ tiene la solución $x = 2$, porque $5 \times 2 - 10 = 0$.

La ecuación cuadrática $x^2 - 3x + 2 = 0$ tiene la solución $x = 1$, porque $1^2 - 3 \times 1 + 2 = 0$, pero también tiene una segunda solución $x = 2$, porque $2^2 - 3 \times 2 + 2 = 0$. La ecuación cúbica $x^3 - 6x^2 + 11x - 6 = 0$ tiene tres

soluciones, $x = 1, 2$ ó 3 . El número de soluciones (reales) es siempre menor o igual que el grado.

Las ecuaciones lineales son fáciles de resolver y se han conocido métodos generales durante miles de años, que se remontan a mucho antes de que se inventara el álgebra simbólica. No sabemos exactamente cuándo, porque no existen los registros adecuados.

Las ecuaciones cuadráticas, de grado dos, son más complicadas. Pero el modo de resolverlas era conocido en la antigua Babilonia, hace 4.000 años, y es lo que veremos a continuación. Me ocuparé de las ecuaciones cúbicas, cuárticas y de grado cinco en los capítulos 3, 4 y 5.

§. La solución babilónica



Figura 19. Dos tablas matemáticas babilónicas.

En 1930, el historiador matemático Otto Neugebauer identificó tablas de barro de la antigua Babilonia que explicaban cómo resolver ecuaciones cuadráticas.

Primero necesitamos saber un poco sobre la notación numérica de Babilonia. No usaban base 10, sino base 60. De modo que 2.015 en notación babilónica (usaban marcas con forma de cuña en el barro, en lugar de nuestros dígitos) significaba:

$$2 \times 60^3 + 0 \times 60^2 + 1 \times 60^1 + 5 \times 60^0$$

que es:

$$2 \times 216.000 + 0 \times 3.600 + 1 \times 60 + 5 \times 1 = 432.065$$

en base decimal. Tenían también una versión de nuestra coma decimal, sumando múltiplos de 1/60, 1/600, etcétera.

Los historiadores reescriben los dígitos babilónicos así:

2, 0, 1, 5

y usan un punto y coma en lugar de la coma decimal. Por ejemplo:

$$14,30;15 = 14 \times 60 + 30 + 15/60 = 870 \frac{1}{4}$$

Veamos ahora la ecuación cuadrática. Una tabla babilónica, que se remonta alrededor de 4.000 años, plantea: «Encuentra el lado de un cuadrado si el área menos el lado es 14,30».

1 ፩	11 ፲፩	21 ፳፲፩	31 ፴፳፩	41 ፵፴፩	51 ፶៥፩
2 ፪	12 ፳፪	22 ፴፳፪	32 ፵፴፳፪	42 ፶៥፳፪	52 ፷៥፳፪
3 ፫	13 ፴፫	23 ፵፴፫	33 ፶៥፴፫	43 ፷៥፴፫	53 ፸៥፴፫
4 ፬	14 ፵፬	24 ፶៥፬	34 ፷៥፵፬	44 ፸៥፵፬	54 ፹៥፵፬
5 ፭	15 ፶៥፭	25 ፷៥፶៥	35 ፸៥፶៥	45 ፹៥፶៥	55 ፻៥፶៥
6 ፮	16 ፷៥፮	26 ፸៥፷៥	36 ፹៥፷៥	46 ፻៥፷៥	56 ፻៥፷៥
7 ፯	17 ፸៥፯	27 ፹៥፸៥	37 ፻៥፸៥	47 ፻៥፸៥	57 ፻៥፸៥
8 ፰	18 ፹៥፰	28 ፻៥፹៥	38 ፻៥፹៥	48 ፻៥፹៥	58 ፻៥፹៥
9 ፱	19 ፻៥፱	29 ፻៥፻៥	39 ፻៥፻៥	49 ፻៥፻៥	59 ፻៥፻៥
10 ፲	20 ፻៥፲	30 ፻៥፻៥	40 ፻៥፻៥	50 ፻៥፻៥	59 ፻៥፻៥

Figura 20. Símbolos cuneiformes babilónicos para los números 1-59.

Este problema involucra al cuadrado de una incógnita (el área del cuadrado), así como a la propia incógnita, de modo que se reduce a una ecuación cuadrática. En la tabla siguiente se explica cómo obtener la respuesta:

Tabla 4

Instrucciones babilónicas

Toma la mitad de 1, la cual es 0;30

Multiplica 0;30 por 0;30, que da 0;15

Nuestra notación

$\frac{1}{2}$

$\frac{1}{4}$

Suma esto a 14,30 para obtener 14,30;15 $(14 \times 60 + 30) + \frac{1}{4} = 870\frac{1}{4}$

Esto es el cuadrado de 29;30 $870\frac{1}{4} = (29\frac{1}{2}) \times (29\frac{1}{2})$

Ahora suma 0;30 a 29;30 $29\frac{1}{2} + \frac{1}{2}$

El resultado es 30, el lado del cuadrado 30

El paso más complicado es el cuarto, que haya un número (es 29) cuyo cuadrado es 870. El número 29 es la *raíz cuadrada* de 870. Las raíces cuadradas son la principal herramienta para resolver ecuaciones cuadráticas.

Esta presentación es típica de las matemáticas babilónicas. La descripción involucra a números específicos, pero el método es más general. Si cambias los números sistemáticamente y sigues el mismo procedimiento, puedes resolver otras ecuaciones cuadráticas. Si usas notación algebraica moderna, reemplazando los números con símbolos, y empiezas con una ecuación cuadrática general:

$$ax^2 + bx + c = 0$$

entonces el método babilónico produce la respuesta

$$\frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$$

Puede que la reconozcas: en efecto, es la fórmula que nos enseñaron en la escuela.

3. Ecuación cúbica

El número primo impar más pequeño es 3. La ecuación cúbica, la que implica una potencia de tres de la incógnita, puede resolverse usando raíces cúbicas y cuadradas. El espacio tiene 3 dimensiones. La trisección de un ángulo usando regla y compás es imposible. Hay exactamente 3 polígonos regulares que recubren el plano. Los siete octavos de todos los números son una suma de 3 cuadrados.

§. El primo impar más pequeño

El número primo más pequeño es 2, que es par. El siguiente es 3, y este es el número primo impar más pequeño. Cualquier otro número primo es, o bien de la forma $3k + 1$, o bien $3k + 2$, siendo k un número natural, porque $3k$ es divisible por 3. Pero hay muchas otras cosas interesantes que decir sobre el 3, de modo que dejaré los primos para el capítulo [7].

§. Ecuación cúbica

Uno de los grandes triunfos de las matemáticas en la Italia del Renacimiento fue el descubrimiento de que una ecuación cúbica puede resolverse usando una fórmula algebraica en la que hay involucradas raíces cúbicas y raíces cuadradas.

El Renacimiento fue un período de agitación e innovación intelectual. Los matemáticos de la época, que no fueron una excepción a esa tendencia, estaban decididos a superar las limitaciones de las matemáticas clásicas. El primer gran avance fue un método para resolver ecuaciones cúbicas. Diferentes matemáticos, que mantenían sus métodos en secreto, encontraron varias versiones de este método. Finalmente, Girolamo Cardano, apodado «Jerome Cardan», los publicó en uno de los más grandes libros de álgebra del mundo, el *Ars Magna*. Cuando lo hizo, otro matemático lo acusó de apropiarse de su secreto. No era poco probable. Alrededor de 1520, Cardano estaba en la bancarrota. Convirtió el juego en su fuente de financiación, explotando sus habilidades matemáticas para mejorar sus oportunidades de ganar. Cardano era un genio, pero también un sinvergüenza. Sin embargo, tenía una excusa verosímil, como veremos.

Esto es lo que sucedió. En 1535, Antonio Fior y Niccolò Fontana (apodado «Tartaglia», «el Tartamudo») se enfrentaron en un concurso público. Cada uno planteó al otro ecuaciones cúbicas que debían resolver y Tartaglia se impuso a Fior de forma aplastante. En esa época, las ecuaciones cúbicas se clasificaban en tres tipos distintos, porque los números negativos se desconocían. Fior sabía cómo resolver solo un tipo, y en principio Tartaglia sabía cómo resolver un tipo diferente, pero poco antes del concurso averiguó cómo resolver todos los demás. Por esa

razón planteó a Fior solo los tipos que este no podría resolver, y de este modo venció a su oponente.

Cardano, que trabajaba en su libro de álgebra, se enteró del concurso y se dio cuenta de que Fior y Tartaglia sabían cómo resolver ecuaciones cúbicas. Como este descubrimiento sin precedentes mejoraría mucho su libro, pidió a Tartaglia que le revelase su método. Finalmente, Tartaglia se lo mostró, y más tarde sostuvo que tenía la promesa de Cardano de que nunca lo haría público. Sin embargo, el método aparecía en *Ars Magna*, de modo que Tartaglia acusó a Cardano de plagio.

Pero Cardano tenía una excusa, pues también tenía una buena razón para darle la vuelta a su promesa, si es que en algún momento llegó a hacerla. Su discípulo Lodovico Ferrari había descubierto cómo resolver ecuaciones de grado cuatro [véase 4] y Cardano también las quería en su libro. Sin embargo, el método de Ferrari dependía de la resolución de una ecuación cúbica asociada, por lo que Cardano no podía publicar el trabajo de Ferrari sin publicar también el trabajo de Tartaglia. Tenía que ser frustrante.

Luego supo que Fior había sido estudiante de Scipio del Ferro, de quien se rumoreaba que había resuelto los tres tipos de ecuaciones cúbicas y había comunicado el secreto de solo una de ellas a Fior. Los documentos no publicados de Del Ferro estaban en posesión de Annibale del Nave, de modo que Cardano y Ferrari fueron a Bolonia en 1543 a consultar a Del Nave, y en los papeles encontraron las soluciones a los tres tipos de

ecuaciones cúbicas, tal como se rumoreaba. Esto permitió a Cardano argumentar, adecuadamente, que estaba publicando el método de Del Ferro y no el de Tartaglia.

Pero Tartaglia todavía se sentía engañado, y publicó una larga y mordaz diatriba contra Cardano. Ferrari le retó a un debate público, que ganó sin problema. Tartaglia nunca llegó a recuperar totalmente su reputación tras estos hechos.

Usando símbolos modernos, podemos escribir la solución de Cardano para la ecuación cónica en un caso especial, cuando $x^3 + ax + b = 0$, para a y b números dados. Si aparece x^2 , con un ingenioso truco nos deshacemos de él, de modo que este caso realmente vale para todos. La respuesta es:

$$x = \sqrt[3]{-\frac{b}{2} + \sqrt{\frac{b^2}{4} + \frac{a^3}{4}}} + \sqrt[3]{-\frac{b}{2} - \sqrt{\frac{b^2}{4} + \frac{a^3}{27}}}$$

en la que aparecen raíces cúbicas y raíces cuadradas. Te libraré de darte todos los detalles. Son ingeniosos y elegantes, pero este tipo de álgebra requiere tiempo para llegar a apreciarla, y puedes encontrarlos fácilmente en libros de texto o en Internet.

§. Dimensión del espacio

La geometría euclídea considera dos espacios diferentes: la geometría del plano, donde prácticamente todo está contenido en una hoja de papel lisa, y la geometría de sólidos del espacio. El plano es bidimensional: la posición de un punto puede especificarse usando dos coordenadas (x, y) . El espacio en el que vivimos es tridimensional: la posición de un punto puede especificarse usando tres coordenadas (x, y, z) .

Otro modo de decir esto es que en el plano (ahora posicionado verticalmente como una página de un libro o la pantalla de un ordenador), hay dos direcciones independientes: izquierda-derecha y arriba abajo. En el espacio hay tres direcciones independientes: norte-sur, este-oeste y arriba-abajo.

Durante más de dos mil años, los matemáticos (y todos los demás) asumieron que tres era el máximo. Pensaban que no podía haber un espacio cuatridimensional [véase 4], porque no había espacio para una cuarta dirección independiente. Si crees que lo hay, por favor, muévete en ese sentido. Sin embargo, esta creencia se basaba en una confusión entre el espacio físico real y las posibilidades abstractas matemáticas.

En términos de la percepción humana normal, el espacio parece comportarse de modo bastante parecido a la geometría sólida tridimensional de Euclides. Pero nuestra percepción está limitada a regiones cercanas, y según Albert Einstein, la imagen euclídea no se corresponde exactamente con la geometría de espacios físicos en escalas mayores. En cuanto nos movemos más allá de lo físico, hacia el mundo

abstracto de los conceptos matemáticos, es fácil definir «espacios» con tantas dimensiones como queramos. Tan solo permitimos más coordenadas en nuestra lista. En el espacio de cuatro dimensiones, por ejemplo, los puntos se especifican usando una lista de cuatro coordenadas (w, x, y, z). Ya no es posible dibujar imágenes, al menos al modo habitual, pero esa es una limitación del espacio físico y de la percepción humana, no de las matemáticas.

Hay que señalar que tampoco es posible dibujar imágenes del espacio *tridimensional*, porque el papel y el ordenador son bidimensionales. Pero nuestro sistema visual está habituado a interpretar objetos tridimensionales a partir de proyecciones bidimensionales, porque los rayos de luz entrantes los detecta la retina, la cual es realmente bidimensional. De modo que nos contentamos con dibujar una proyección de la forma tridimensional en un plano, lo cual es bastante parecido a como los ojos ven el mundo. Puedes inventar métodos similares para «dibujar» formas de cuatro dimensiones en papel, pero necesitan muchas explicaciones y requiere cierta práctica acostumbrarse a ellas.

Los físicos finalmente se dieron cuenta de que localizar un suceso tanto en el espacio como en el tiempo requiere cuatro coordenadas, no tres: las tres habituales para su posición espacial y una cuarta para el momento en que sucede. La batalla de Hastings tuvo lugar en una localización que está ahora cercana a la unión de las carreteras A271 y A2100, al noroeste

de Hastings, en la costa sur de Sussex. La latitud y la longitud de este punto las dan dos coordenadas. Sin embargo también tuvo lugar en el suelo, esto es, a cierto número de metros sobre el nivel del mar. Esa es la tercera coordenada espacial, así hemos especificado el lugar exacto relativo a la Tierra. (Ignoraré el movimiento de la Tierra alrededor del Sol, las revoluciones del Sol junto con el resto de la galaxia, el movimiento de la galaxia hacia M31 en Andrómeda y cómo todo el grupo local de galaxias está siendo absorbido hacia el Gran Atractor.)

Sin embargo, si hoy fueras a ese lugar no verías a los ingleses bajo el rey Harold II luchando contra el ejército invasor del duque Guillermo II de Normandía, y la razón es que estarías en la coordenada de tiempo errónea. Necesitas un cuarto dato, el 14 de octubre de 1066, para localizar la batalla en el espacio y el tiempo.

Así que aunque el espacio físico tiene solo tres dimensiones, el espacio-tiempo tiene cuatro.

El espacio tampoco podría parecer lo que parece cuando vamos más allá de las percepciones humanas normales. Einstein mostró que, en escalas muy grandes, aplicables cuando estamos estudiando el sistema solar o las galaxias, el espacio puede curvarse por la gravedad. La geometría resultante no es la misma que la euclídea. En la actualidad, en escalas muy pequeñas, aplicables a las partículas subatómicas, los físicos sospechan que el espacio tiene seis o siete dimensiones extra, quizás enrolladas muy apretadas, de manera que no las notamos [véase 11].

§. Imposibilidad de trisecar un ángulo y duplicar el cubo

Aunque los Elementos de Euclides proporcionan soluciones para un rango de problemas geométricos, dejaron varias preguntas sin respuesta. El libro proporciona un método para biseccionar cualquier ángulo (dividirlo en dos partes iguales), usando solo los instrumentos tradicionales: una regla sin marcas y un compás [véase 1/2]. (En rigor, «par de compases», por la misma razón que cortamos papel con un par de tijeras, no con una tijera, y llevamos un par de pantalones, no un pantalón. Pero hoy en día es difícil encontrarse con alguien tan pedante.) Sin embargo, Euclides fracasó en la tarea de proporcionar un método para la trisección de cualquier ángulo (dividirlo en tres partes iguales) usando estos instrumentos. Considerando un cubo dado, sabía cómo encontrar uno cuyo volumen fuese ocho veces mayor. Bastaba con doblar todos sus lados. Pero no proporcionó un método para que, dado un cubo, se encontrase otro con un volumen que fuese el doble, problema conocido como «la duplicación del cubo». Quizá su mayor omisión fue cuadrar el círculo: un método para construir un cuadrado con la misma área que un círculo dado [véase π]. En términos modernos, equivale a encontrar una construcción geométrica para una línea de longitud π , dada una línea de longitud la unidad.

Estos son los tres «problemas geométricos de la Antigüedad». En el pasado los resolvieron mediante nuevos tipos de instrumentos, pero no

concluyeron si estos nuevos métodos eran realmente necesarios. ¿Pueden resolverse estos tres problemas usando solo regla y compás?

Finalmente se probó que los tres problemas eran irresolubles con regla y compás. La cuadratura del círculo fue especialmente difícil [véase π]. Los otros dos dependen de una propiedad especial del número 3, en concreto, que no es un entero potencia de 2.

La idea básica es más fácil de ver en el contexto de la duplicación del cubo. El volumen de un cubo de lado x es x^3 . De modo que estamos intentando resolver la ecuación $x^3 = 2$. Esto puede hacerse, y la respuesta es la raíz cúbica de 2:

$$\sqrt[3]{2} = 1,259921049894873164767\dots$$

Pero ¿puede hacerse usando solo regla y compás?

En su texto clásico de teoría de números, *Disquisitiones arithmeticæ*, Gauss indicó que cualquier longitud obtenida a partir de la longitud unidad mediante una construcción de regla y compás puede expresarse algebraicamente resolviendo una serie de ecuaciones cuadráticas. Por tanto, un poco de álgebra demuestra que la longitud debe ser la solución de una ecuación con coeficientes enteros cuyo grado es una potencia de 2. En líneas generales, cada cuadrática extra dobla el grado.

Y para dar el golpe de gracia. La ecuación para la raíz cúbica de 2 es $x^3 = 2$, que tiene grado 3. Como *no* es una potencia de 2, esta longitud no

puede construirse con regla y compás. Pierre Wantzel explicó la letra pequeña que Gauss consideró demasiado trivial mencionar y escribió una prueba completa en 1837. Hay un detalle técnico: la ecuación cúbica debe ser «irreducible», lo que en este caso significa que no tiene una solución racional. Como $\sqrt[3]{2}$ es irracional, es fácil lidiar con este detalle. Wantzel también probó la imposibilidad de trisecar el ángulo, por razones similares. Si consideramos trisecar el ángulo 60° , un poco de trigonometría y de álgebra nos llevará a la ecuación cúbica

$$x^3 - 3x - 1 = 0$$

De nuevo, es irreducible, por lo que ninguna construcción con regla y compás es posible.

§. El número de recubrimientos del plano usando polígonos regulares

Solo tres polígonos regulares recubren el plano: el triángulo equilátero, el cuadrado y el hexágono.

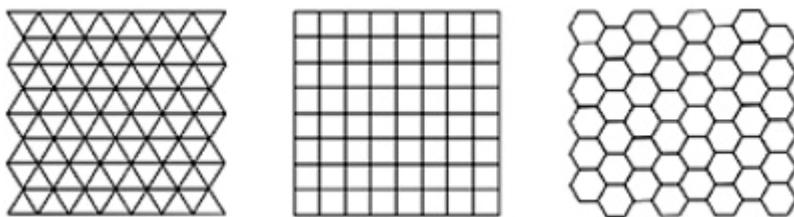


Figura 21. Tres modos de recubrir el plano: triángulos equiláteros, cuadrados y hexágonos.

La prueba es sencilla. El ángulo en la esquina de un polígono regular de n lados es:

$$180 - \frac{360}{\pi}$$

y los primeros valores son:

Tabla 5

<i>n</i>	<i>180 - 360/π</i>	<i>Polígono</i>
3	60	triángulo equilátero
4	90	cuadrado
5	108	pentágono
6	120	hexágono
7	128,57	heptágono
8	135	octógono

Ahora considera un recubrimiento con copias de uno de estos polígonos. En cualquier esquina se encuentran varios polígonos, de modo que el ángulo en la esquina del polígono debe ser 360° dividido entre un número entero. Los ángulos posibles son:

Tabla 6

<i>n</i>	<i>360/n</i>	Polígono
3	120	hexágono
4	90	cuadrado
5	72	no es el ángulo de un polígono regular
6	60	triángulo equilátero
7	51,43	no es el ángulo de un polígono regular

Observa que los ángulos en la primera tabla crecen a medida que el número de lados n crece, así como en la segunda tabla decrecen a medida que n crece. A partir de 7 lados, el ángulo en la segunda tabla es menor que 60° , pero el ángulo en la primera tabla es siempre mayor o igual que 60° . Por lo tanto, ampliar la tabla no nos proporcionará más soluciones.

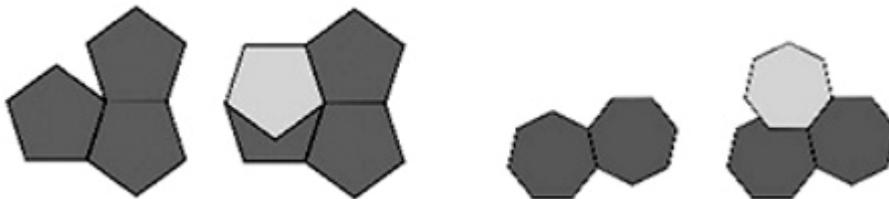


Figura 22. Izquierda: tres pentágonos dejan un hueco; cuatro se superponen. Derecha: dos heptágonos dejan un hueco; tres se superponen. Lo mismo ocurre con más de 7 lados.

Otro modo de decir esto es que los tres pentágonos dejan un hueco, pero cuatro se superponen unos con otros; dos heptágonos (o polígonos con más de 7 lados) dejan un hueco, pero tres se superponen unos con otros. Así, solo el triángulo equilátero, el cuadrado y el hexágono pueden encajarse unos con otros de modo exacto para hacer un recubrimiento.

§. Sumas de tres cuadrados

Como muchos números no son la suma de dos cuadrados [véase 2], ¿qué pasaría si los planteamos como suma de *tres* cuadrados? La mayoría de los números, pero no todos, pueden escribirse como la suma de tres cuadrados. La lista de los que no pueden empieza con los siguientes:

7 15 23 28 31 39 47 55 60 63 71 79 87 92 95 103

De nuevo, hay un patrón en estos números, y de nuevo cuesta verlo. Lo encontró en 1798 Adrien-Marie Legendre. Afirmó que la suma de tres cuadrados da como resultado exactamente números que *no* son de la forma $4^k(8n + 7)$. La lista de excepciones, que acabamos de ver, comprende todos los números que son de esta forma. Así, si $n = 0$ y $k = 0$, obtenemos 7, si $n = 1$ y $k = 0$, obtenemos 28, y así sucesivamente. Su resultado es correcto, pero su prueba tenía una laguna que solventó Gauss en 1801.

No es difícil probar que los números de la forma $4^k(8n + 7)$ no son la suma de tres cuadrados. Todo cuadrado deja un resto 0, 1 o 4 cuando se divide entre 8. De modo que la suma de tres cuadrados puede dejar cualquier resto obtenido sumando tres de estos números, lo cual da restos 0, 1, 2, 3, 4, 5 y 6, pero no 7. Esto nos dice que los números de la forma $8n + 7$ necesitan más de tres cuadrados. La parte relativa a 4^k es solo ligeramente más difícil. La parte más complicada es probar que todos los demás números son realmente sumas de tres cuadrados.

A medida que n se hace más grande, la proporción de números menores que n que son sumas de tres cuadrados tiende a $7/8$. El factor 4^k no afecta a esta proporción lo suficiente como para cambiar el límite para un n grande, y solo uno de los ocho restos de dividir entre 8 se excluye.

4. Cuadrado

El primer cuadrado perfecto (después de 0 y 1) es 4. Cualquier mapa en el plano puede colorearse con 4 colores de modo que las regiones adyacentes tengan colores diferentes. Todo número entero positivo es una suma de 4 cuadrados. Lo mismo ocurre con los cubos, permitiendo enteros negativos. Las ecuaciones de grado 4, en las que la incógnita aparece elevada a 4, pueden resolverse usando raíces cúbicas y raíces cuadradas (raíces cuartas son raíces cuadradas de raíces cuadradas). El sistema numérico de cuaterniones, basado en 4 cantidades

independientes, obedece *casi* todas las leyes estándar del álgebra. ¿Puede existir una cuarta dimensión?

§. Cuadrado perfecto

El número $4 = 2 \times 2$ es un cuadrado [véase 2]. Los cuadrados tienen una importancia fundamental en todas las matemáticas. El teorema de Pitágoras dice que el cuadrado del lado mayor de un triángulo rectángulo es la suma de los cuadrados de los otros dos lados, así que, en concreto, los cuadrados de los números son fundamentales en geometría.

Los cuadrados tienen muchos patrones ocultos. Observa las *diferencias* entre los cuadrados sucesivos:

$$1 - 0 = 1$$

$$4 - 1 = 3$$

$$9 - 4 = 5$$

$$16 - 9 = 7$$

$$25 - 16 = 9$$

¿Qué números son estos? Los números impares:

1 3 5 7 9

Otro patrón interesante es una consecuencia directa:

$$1 = 1$$

$$1 + 3 = 4$$

$$1 + 3 + 5 = 9$$

$$1 + 3 + 5 + 7 = 16$$

$$1 + 3 + 5 + 7 + 9 = 25$$

Si sumamos todos los números impares, hasta algún número en concreto, el resultado es un cuadrado.

Hay un modo de comprender por qué ambos hechos son ciertos y cómo se relaciona el uno con el otro, usando puntos (imagen de la izquierda).

Pueden también probarse usando álgebra, por supuesto.

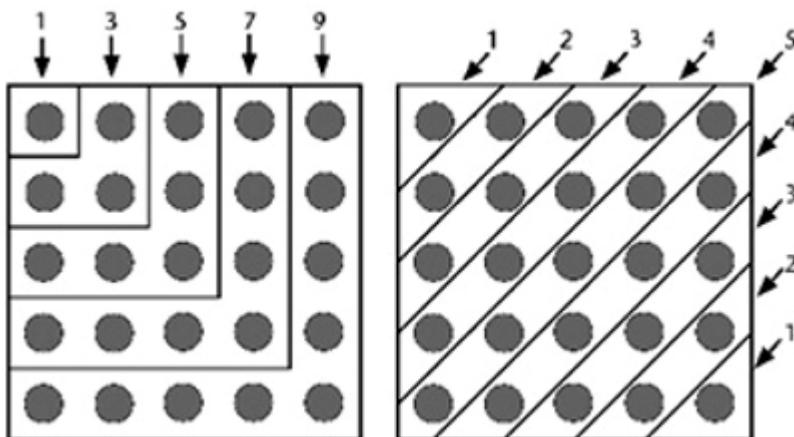


Figura 23. Izquierda: $1 + 3 + 5 + 7 + 9$. Derecha: $1 + 2 + 3 + 4 + 5 + 4 + 3 + 2 + 1$.

Aquí tienes otro bello patrón usando cuadrados:

$$1 = 1$$

$$1 + 2 + 1 = 4$$

$$1 + 2 + 3 + 2 + 1 = 9$$

$$1 + 2 + 3 + 4 + 3 + 2 + 1 = 16$$

$$1 + 2 + 3 + 4 + 5 + 4 + 3 + 2 + 1 = 25$$

También podemos verlo usando puntos (imagen de la derecha).

§. El teorema de los cuatro colores

Hace alrededor de 150 años, algunos matemáticos empezaron a hacerse preguntas sobre los mapas. No los problemas tradicionales asociados con hacer mapas precisos del mundo y representar un globo redondeado en una hoja de papel plana, sino cuestiones bastante más confusas sobre mapas en general. En concreto, cómo colorear las regiones de modo que aquellas que tuvieran una frontera común tuviesen diferentes colores.

Algunos mapas no necesitan muchos colores. Los cuadrados de un tablero de ajedrez forman un tipo de mapa muy regular, y solo se necesitan dos colores: blanco y negro, siguiendo el patrón habitual. Para los mapas hechos a partir de la superposición de círculos también son solo necesarios dos colores (véase *Professor Stewart's Casebook of Mathematical Mysteries*). Pero cuando las regiones se hacen menos regulares, los dos colores no bastan.

Por ejemplo, aquí tenemos un mapa de Estados Unidos con 50 regiones, sus 50 estados. Obviamente, 50 colores harían el trabajo, uno para cada estado, pero podemos hacerlo mejor. Intenta colorear las regiones y observa el menor número de colores que puedes usar. Ten en cuenta un asunto técnico: los estados que se encuentran en un único punto, como Colorado y Arizona, pueden compartir color, si quieras. No tienen un *borde* en común.

El mapa de Estados Unidos ejemplifica algunos principios generales sencillos. Alaska y Hawái no desempeñan realmente un papel, porque están aislados de todos los otros estados, así que podemos darles el color que queramos. Definitivamente, necesitamos al menos tres colores. De hecho, Utah, Wyoming y Colorado deben tener cada uno un color diferente, porque tomando dos de ellos tienen un borde común.



Figura 24. Los 50 estados de Estados Unidos.

Podemos escoger tres colores para estos estados. No importa cuáles, mientras sean diferentes. Coloreemos Utah de negro, Wyoming de gris oscuro y Colorado de gris, como se muestra:



Figura 25. Por qué se necesitan al menos tres colores.

Supongamos, solo como hipótesis, que queremos usar solo estos tres colores para el resto del mapa. Entonces Nebraska tendría que ser de color negro, ya que comparte borde con un estado gris oscuro y uno gris. Esto forzaría a que Dakota del Sur fuera gris. Podemos continuar de este modo un poco más, con solo una posibilidad para cada nuevo color, coloreando Montana, Idaho, Nevada, Oregón y California. En ese punto lo que tenemos es:



Figura 26. Si seguimos usando tres colores, nos quedamos atascados.

Arizona comparte borde con estados que hemos coloreado de gris, gris oscuro y negro. Como, hasta este punto, el color seleccionado para el estado era aquel que nos obligaban a usar los estados colindantes, los tres colores no valen para cubrir el mapa entero. Por lo tanto, necesitamos un cuarto, por ejemplo, gris claro, para poder seguir.

Faltan 38 estados para acabar. Excluyendo Alaska y Hawái, parece posible que en algún momento quizá necesitemos un quinto color, o un sexto..., quién sabe. Por otro lado, tener un cuarto color disponible cambia todo el juego. En concreto, algunos de los colores asignados previamente podrían cambiarse (coloreando Wyoming de gris claro, por ejemplo). Las elecciones de colores ya no deben ser forzosamente una única, así que se dificulta analizar el problema.



Figura 27. Un cuarto color viene al rescate.



Figura 28. Un quinto color no es necesario.

Sin embargo, podemos continuar, haciendo suposiciones cabales y cambiando los colores si algo va mal. Una de las posibilidades de coloreado resultantes tiene solo tres estados en gris claro: Arizona,

Virginia Occidental y Nueva York. Aunque hay 50 estados, hemos coloreado el mapa completo con tan solo *cuatro* colores.

(Otra consideración técnica: Michigan está partido en dos regiones que no están conectadas con el lago Michigan entre sí. Aquí hemos coloreado ambas de gris oscuro, pero en regiones desconectadas a veces se necesitan más colores. Esto tiene que tenerse en cuenta en una teoría matemática que sea completa, pero no es vital en este caso.)

El mapa de Estados Unidos no es especialmente complicado. Podemos concebir mapas con millones de regiones, todas ellas muy serpenteantes, con muchas protuberancias recorriendo toda la superficie. En esos casos quizá necesitemos muchos más colores. Sin embargo, los matemáticos que han trabajado sobre estas posibilidades han forjado la creencia de que nunca necesitarás más de cuatro colores, al margen de lo complejo que sea el mapa. Siempre que el mapa esté dibujado en un plano o en una esfera, con todas las regiones conectadas, cuatro colores bastarán.

Breve historia del problema de los cuatro colores

El problema de los cuatro colores se originó en 1852, cuando Francis Guthrie, un joven matemático y botánico surafricano, intentaba colorear los condados en un mapa de Inglaterra. Parecía que cuatro colores siempre eran suficientes, así que preguntó a su hermano Frederick si esto era un hecho sabido. Frederick le preguntó al distinguido y excéntrico matemático Augustus De Morgan; este, como no tenía ni idea, escribió a

un matemático todavía más distinguido, sir William Rowan Hamilton. Hamilton tampoco lo sabía y, para ser frances, tampoco pareció muy interesado en saberlo.

En 1879, el abogado Alfred Kempe publicó lo que creía ser una prueba de que bastaban cuatro colores, pero en 1889 Percy Heawood descubrió que Kempe había cometido un error. Indicó que el método de Kempe probaba que cinco colores eran siempre suficientes y ahí se quedó el asunto durante más de un siglo. La respuesta era cuatro o cinco, pero nadie sabía cuál era la correcta. Otros matemáticos intentaron estrategias como la de Kempe, pero pronto quedó claro que este método requería muchos cálculos tediosos. Finalmente, en 1976, Wolfgang Haken y Kenneth Appel resolvieron el problema usando un ordenador. Cuatro colores son siempre suficientes.

A partir de este trabajo pionero, los matemáticos se han acostumbrado a la ayuda del ordenador. Todavía prefieren pruebas que dependan únicamente del poder de la mente humana, pero la mayoría ya no exigen ese requisito. Aunque en la década de 1990, había todavía una cierta cantidad de inquietud justificada en torno a la prueba de Appel-Haken. De modo que en 1994, Neil Robertson, Daniel Sanders, Paul Seymour y Robin Thomas decidieron rehacer la prueba por completo, usando la misma estrategia básica pero simplificando la configuración. Los ordenadores de hoy en día son tan rápidos que toda la prueba puede verificarse en un ordenador doméstico en pocas horas.

§. Teorema de los cuatro cuadrados

En el capítulo [2], vimos cómo caracterizar sumas de dos cuadrados, y el capítulo [3] describe sumas de tres cuadrados. Pero cuando se trata de sumas de cuatro cuadrados, no necesitas determinar los números para los que funciona, pues todos lo hacen.

Cada cuadrado extra hace posible obtener más números, de modo que las sumas de cuatro cuadrados debería al menos cubrir algunos huecos. Los experimentos sugieren que todo número del 0 al 100 lo cumplen. Por ejemplo, aunque 7 no es una suma de tres cuadrados, es una suma de cuatro:

$$7 = 4 + 1 + 1 + 1$$

Este éxito temprano podría haber ocurrido porque estamos observando números bastante pequeños. ¿Quizás algunos números mayores necesiten cinco cuadrados, o seis, o más? No. Números mayores son también la suma de cuatro cuadrados. Los matemáticos buscaron una prueba que contuviese a todos los números positivos, y en 1770, Joseph-Louis Lagrange la encontró.

§. Conjetura de los cuatro cubos

Se han hecho conjeturas sobre que un teorema similar es cierto usando cuatro cubos, pero con un giro extra: están permitidos tanto cubos positivos como negativos. De modo que la conjetura es: todo entero es la suma de cuatro cubos de números enteros. Recuerda que un entero es un número que podría ser positivo, negativo o cero.

El primer intento de generalizar el teorema de los cuatro cuadrados a cubos apareció en *Meditationes Algebraicae*, de Edward Waring, en 1770. Este autor afirmaba sin prueba que todo número natural es la suma de cuatro cuadrados, nueve cubos, 19 cuartas potencias, etcétera. Asumió que todos los números implicados eran positivos o cero. Esta afirmación pasó a ser conocida como el «problema de Waring».

El cubo de un entero negativo es negativo, y esto permite nuevas posibilidades. Por ejemplo:

$$23 = 2^3 + 2^3 + 1^3 + 1^3 + 1^3 + 1^3 + 1^3 + 1^3 + 1^3$$

necesita nueve cubos positivos, pero podemos obtenerlo usando cinco cubos si algunos son negativos:

$$23 = 27 - 1 - 1 - 1 - 1 = 3^3 + (-1)^3 + (-1)^3 + (-1)^3 + (-1)^3$$

De hecho, 23 puede expresarse usando tan solo cuatro cubos:

$$23 = 512 + 512 - 1 - 1.000 = 8^3 + 8^3 + (-1)^3 + (-10)^3$$

Cuando permitimos números negativos, un número positivo grande puede casi anular a uno negativo grande. De modo que los cubos involucrados podrían, en principio, ser mucho más grandes que el número que nos ocupa. Por ejemplo, podemos escribir 30 como una suma de tres cubos si observamos que:

$$30 = 2.220.422.932^3 + (-283.059.965)^3 + (-2.218.888.517)^3$$

A diferencia del caso positivo, no podemos trabajar de modo sistemático a través de un número limitado de posibilidades.

Los experimentos llevaron a varios matemáticos a conjeturar que *todo* entero es la suma de cuatro cubos de enteros. Hasta ahora, no existe ninguna prueba, pero la evidencia es sustancial y se han hecho algunos progresos. Sería suficiente probar la afirmación para todos los enteros positivos (permitiendo cubos de positivos y negativos) porque $(-n)^3 = -n^3$. Cualquier representación de un número positivo m como una suma de cubos puede convertirse en la de una para $-m$ cambiando el signo de cada cubo. Los cálculos por ordenador verifican que todo entero positivo hasta 10 millones es una suma de cuatro cubos. Y en 1966, V. Demjanenko probó que cualquier número que no fuese de la forma $9k \pm 4$ es la suma de cuatro cubos.

Incluso es posible que, con un número finito de excepciones, todo entero positivo sea la suma de cuatro cubos de números *positivos o de cero*. En 2000, Jean-Marc Deshouillers, François Hennecart, Bernard Landreau e I Gusti Putu Purnaba hicieron una conjetura sobre que el mayor entero que no puede ser expresado así es 7.373.170.279.850.

§. Ecuación de grado cuatro (cuártica)

La historia de Cardano y la ecuación cúbica [véase 3] también involucra a la ecuación cuártica, que se da cuando la incógnita está elevada a cuatro:

$$ax^4 + bx^3 + cx^2 + dx + e = 0$$

El estudiante de Cardano resolvió esta ecuación. Se da una fórmula completa en *Quartic Function* y si la ves, comprenderás por qué no la incluyo aquí.

El método de Ferrari relaciona las soluciones de la ecuación cuártica con las de una ecuación cúbica asociada. Esto ahora se llama «resolvente de Lagrange», porque Lagrange fue el primer matemático en explicar por qué una cúbica hace el trabajo.

§. Cuaterniones

Vimos en la introducción que el sistema numérico se había extendido de manera repetitiva con la invención de nuevos tipos de números, y que culminaba con los números complejos, donde -1 tiene una raíz cuadrada [véase *i*]. Los números complejos tienen aplicaciones profundas en física. Pero hay una seria limitación. Los métodos están restringidos a las dos dimensiones del plano. El espacio, sin embargo, es tridimensional. En el siglo XIX, los matemáticos intentaron desarrollar un sistema numérico tridimensional, extendiendo los números complejos. Parecía una buena idea entonces, pero, al margen de lo que intentaran, no llegaron a ningún lugar útil.

William Rowan Hamilton, un matemático irlandés brillante, estaba particularmente interesado en inventar un sistema numérico tridimensional práctico, y en 1843 tuvo una idea genial: identificó dos obstáculos inevitables para crear ese sistema:

- Las tres dimensiones no funcionan.
- Hay que sacrificar una de las reglas estándar de la aritmética. En concreto, la propiedad commutativa para la multiplicación, que afirma que $ab = ba$.

En el momento en que se le ocurría la brillante idea, Hamilton se encaminaba a una reunión en la Royal Irish Academy por un paseo a lo largo de un canal. Había estado dándole vueltas en su cabeza al incomprensible rompecabezas de un sistema numérico tridimensional y,

de repente, se dio cuenta de que con tres dimensiones no tendrían sentido, pero con *cuatro* sí. Sin embargo, tenía que estar dispuesto a deshacerse de la propiedad conmutativa para la multiplicación.

Fue un verdadero momento de iluminación. Golpeado por esta increíble visión, Hamilton se detuvo, y grabó en la piedra de un puente una fórmula para esos números:

$$i^2 = j^2 = k^2 = ijk = -1$$

Llamó a este sistema «cuaterniones», porque los números tenían cuatro componentes. Tres son i , j , k y la cuarta es el número real 1. Un cuaternion típico tiene este aspecto:

$$3 - 2i + 5j + 4k$$

con cuatro números reales arbitrarios (en este caso 3, -2, 5, 4) como coeficientes. La suma de estos «números» es sencilla, y multiplicarlos también, si se usan las ecuaciones que Hamilton grabó en el puente. Todo lo que necesitas son unas cuantas consecuencias de esas ecuaciones, en concreto, estas:

$$i^2 = j^2 = k^2 = -1$$

$$ij = k$$

$$jk = i$$

$$ki = j$$

$$ji = -k$$

$$kj = -i$$

$$ik = -j$$

junto con la regla de que multiplicar cualquier número por 1 lo deja invariable.

Observa que, por ejemplo, ij y ji son diferentes. De modo que la propiedad conmutativa no se cumple.

Aunque esta deficiencia puede parecer incómoda al principio, no provoca serias dificultades. Tan solo tienes que tener cuidado con el orden en que escribes los símbolos cuando manejas el álgebra. Al mismo tiempo, estaban apareciendo varias áreas de matemáticas nuevas, en las cuales la propiedad conmutativa no se daba. Así que la idea tenía precedentes y no era disparatada.

Hamilton pensaba que los cuaterniones eran maravillosos, pero al principio la mayoría de los demás matemáticos los veían como algún tipo de rareza. No ayudaba que los cuaterniones no resultasen muy útiles para resolver problemas de física en el espacio tridimensional, o incluso cuatridimensional. No eran un fracaso absoluto, pero carecían de la versatilidad y generalidad de los números complejos en el espacio bidimensional. Tuvo cierto éxito usando i , j y k para crear un espacio tridimensional, pero esta idea fue suplantada por el álgebra de vectores,

la cual se convirtió en estándar en las ciencias matemáticas aplicadas. Sin embargo, los cuaterniones siguieron siendo de importancia vital en las matemáticas puras, y también tienen aplicaciones en los gráficos de los ordenadores, proporcionando un método sencillo para rotar objetos en el espacio. Asimismo tienen vínculos interesantes con el teorema de los cuatro cuadrados.

Hamilton no llamó a los cuaterniones «números», porque en esa época se estaban inventando muchos sistemas algebraicos parecidos a los numéricos. Los cuaterniones eran un ejemplo de lo que ahora llamamos un álgebra de división: un sistema algebraico en el cual es posible sumar, restar, multiplicar y dividir (excepto por cero), mientras se obedecen casi todas las propiedades estándar de la aritmética. El símbolo para este conjunto de cuaterniones es H (de Hamilton, ya que Q ya se usaba para los racionales).

Las dimensiones de los números reales, los números complejos y los cuaterniones son 1, 2 y 4. El siguiente número en la secuencia seguramente debería ser 8. ¿Hay algún álgebra de división de dimensión ocho? La respuesta es un limitado «sí». Los octoniones, también conocidos como los «números de Cayley», proporcionan dicho sistema. El símbolo es O . Aunque tiene que evitarse una propiedad más de la aritmética: la propiedad asociativa $a(bc) = (ab)c$. Además el patrón se detiene aquí, no hay un álgebra de división de dimensión 16.

Tanto a los cuaterniones como a los octoniones se les ha resucitado de la oscuridad porque tienen conexiones profundas con la mecánica cuántica y las partículas fundamentales de la física. La clave para esta área es la simetría de las leyes físicas y estos dos sistemas algebraicos tienen simetrías importantes e inusuales. Por ejemplo, las reglas para los cuaterniones permanecen sin cambios si reordenas i, j y k como j, k e i . Y una mirada más cercana muestra que puedes reemplazarlos por *combinaciones* apropiadas de *íes*, *jotas* y *kas*. Las simetrías resultantes están muy relacionadas con rotaciones en el espacio tridimensional y los juegos de ordenador con frecuencia usan cuaterniones para este propósito en su *software* de gráficos. Los octoniones tienen una interpretación similar en cuanto a rotaciones en el espacio 7-dimensional.

§. La cuarta dimensión

Desde tiempos inmemoriales, la gente ha reconocido que el espacio físico tiene tres dimensiones [véase 3]. Durante mucho tiempo, la posibilidad de un espacio con cuatro o más dimensiones parecía absurda. Sin embargo, en el siglo XIX esta sabiduría convencional se puso bajo un creciente escrutinio crítico y mucha gente empezó a interesarse mucho en la posibilidad de una cuarta dimensión. No solo los matemáticos, ni siquiera solo los científicos; filósofos, teólogos, espiritistas, gente que creía en fantasmas y algunos estafadores. Una cuarta dimensión proporciona una localización plausible para Dios, los

espíritus de los muertos o fantasmas. No en este universo, pero justo en la puerta de al lado y con un fácil acceso. Los charlatanes usaban trucos para «probar» que podían acceder a esta nueva dimensión.

La idea de «espacios» con más de tres dimensiones podría tener sentido lógico (estén o no emparejados con el espacio físico); primero se pusieron en marcha en matemáticas, gracias a nuevos descubrimientos como los cuaterniones de Hamilton. A principios del siglo XIX, ya no era obvio que tenías que detenerte en tres dimensiones. Piensa en las coordenadas. En el plano, la posición de cualquier punto puede describirse de un modo único por dos números reales x e y , combinados como un par de coordenadas (x, y) .

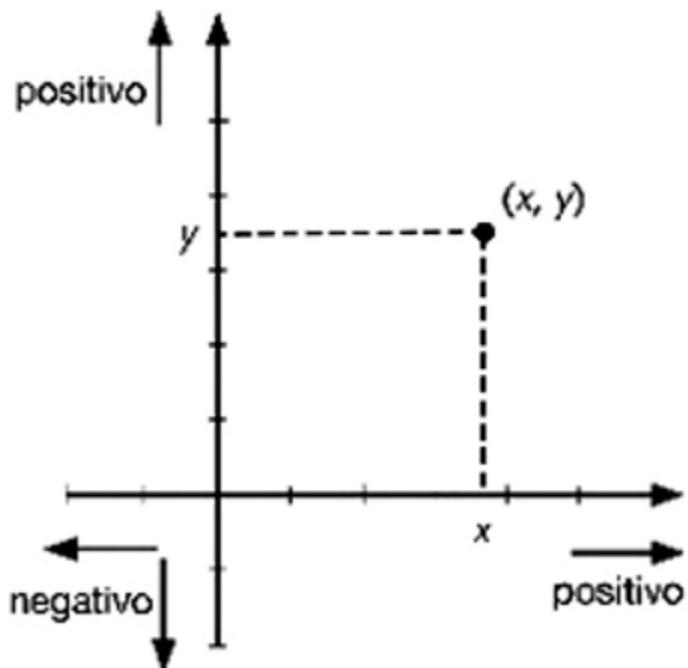


Figura 29. Coordenadas en el plano.

Para representar las tres dimensiones del espacio, todo lo que hacemos es añadir una tercera coordenada, z , en la dirección delante-detrás. Ahora tenemos una terna de números reales (x, y, z) .

Al dibujar figuras geométricas, parece que tuviéramos que parar ahí. Pero es fácil escribir cuádruplos de números (w, x, y, z) . O cinco. O seis. O, dame tiempo y mucho papel, un millón. Finalmente los matemáticos se dieron cuenta de que podían usar cuartetos para *definir* un «espacio» abstracto y, cuando lo hicieron, tuvieron cuatro dimensiones. Con cinco coordenadas, obtienes un espacio cinco-dimensional, y así sucesivamente. Había incluso una razonable noción de geometría en esos espacios, definida por analogía con el teorema de Pitágoras en dos y tres dimensiones. En dos dimensiones este teorema nos dice que la distancia entre puntos (x, y) y (X, Y) es:

$$\sqrt{(x - X)^2 + (y - Y)^2}$$

Su análogo en tres dimensiones nos dice que la distancia entre los puntos (x, y, z) y (X, Y, Z) es:

$$\sqrt{(x - X)^2 + (y - Y)^2 + (z - Z)^2}$$

Así que parece razonable definir la distancia entre dos cuartetos (w, x, y, z) y (W, X, Y, Z) como:

$$\sqrt{(w - W)^2 + (x - X)^2 + (y - Y)^2 + (z - Z)^2}$$

Resulta que la geometría que obtenemos es consistente y bastante análoga a la geometría de Euclides.

En este tema, los conceptos básicos están definidos algebraicamente usando cuádruplos, lo que garantiza que tengan un sentido lógico. Luego se *interpretan* por analogía con fórmulas algebraicas similares en dos y tres dimensiones, lo que le añade el «aspecto» de geometría.

Por ejemplo, las coordenadas de las esquinas de un cuadrado unidad en el plano son:

$$(0, 0)$$

$$(1, 0)$$

$$(0, 1)$$

$$(1, 1)$$

que son todas las combinaciones posibles de dos de ceros y unos. Las coordenadas de las esquinas de un cubo en el espacio son:

$$(0, 0, 0)$$

$$(1, 0, 0)$$

$$(0, 1, 0)$$

$$(1, 1, 0)$$

$$(0, 0, 1)$$

$$(1, 0, 1)$$

$$(0, 1, 1)$$

$$(1, 1, 1)$$

que son todas las combinaciones posibles de tres de ceros y unos. Por analogía, definimos un *hipercubo* en el espacio de dimensión cuatro usando los 16 posibles cuartetos de ceros y unos.

$$(0, 0, 0, 0)$$

$$(1, 0, 0, 0)$$

$$(0, 1, 0, 0)$$

$$(1, 1, 0, 0)$$

$$(0, 0, 1, 0)$$

$$(1, 0, 1, 0)$$

$$(0, 1, 1, 0)$$

$$(1, 1, 1, 0)$$

$$(0, 0, 0, 1)$$

$$(1, 0, 0, 1)$$

$$(0, 1, 0, 1)$$

$$(1, 1, 0, 1)$$

$$(0, 0, 1, 1)$$

$$(1, 0, 1, 1)$$

$$(0, 1, 1, 1)$$

$$(1, 1, 1, 1)$$

Otro nombre común para esta forma es *teseracto* [véase 6].

A partir de esta definición, podemos analizar el objeto resultante. Es muy parecido al cubo, solo que lo es más. Por ejemplo, un cubo se construye uniendo seis cuadrados, y, de manera similar, un hipercubo se construye uniendo ocho cubos.

Por desgracia, debido a que el espacio físico es tridimensional, no podemos hacer un modelo exacto de un hipercubo. Este problema es análogo en cierto modo al de que no podemos dibujar un cubo exacto en una hoja de papel. En su lugar, dibujamos una «proyección», como una fotografía o la pintura de un artista sobre una hoja plana de un papel o un lienzo. Como alternativa, podemos cortar un cubo por algunas de sus aristas y desdoblarlo para obtener en el plano una forma hecha de seis cuadrados con forma de cruz.

Podemos hacer algo análogo para un hipercubo. Podemos dibujar proyecciones en el espacio tridimensional, las cuales serían modelos sólidos, o en el plano, que serían líneas de dibujo. O podemos «desdoblarlo» para mostrar sus ocho «caras» cúbicas. Confieso que encuentro difícil interiorizar cómo se pliegan estos cubos en el espacio de dimensión cuatro, pero la lista de coordenadas del hipercubo dice que lo hacen.

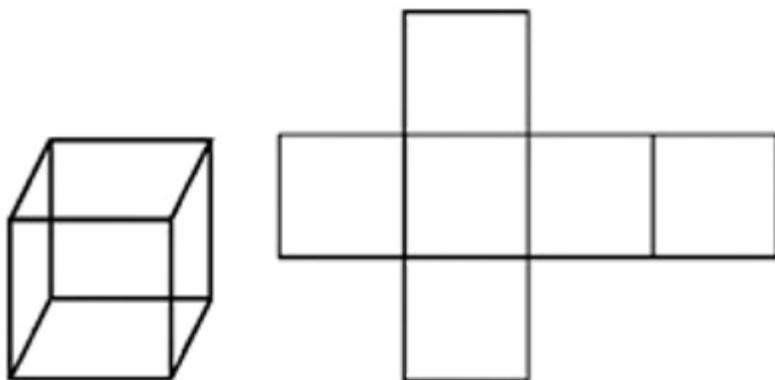


Figura 30. Cubo. Izquierda: proyectado en dos dimensiones. Derecha: desdoblado para mostrar sus seis caras cuadradas.

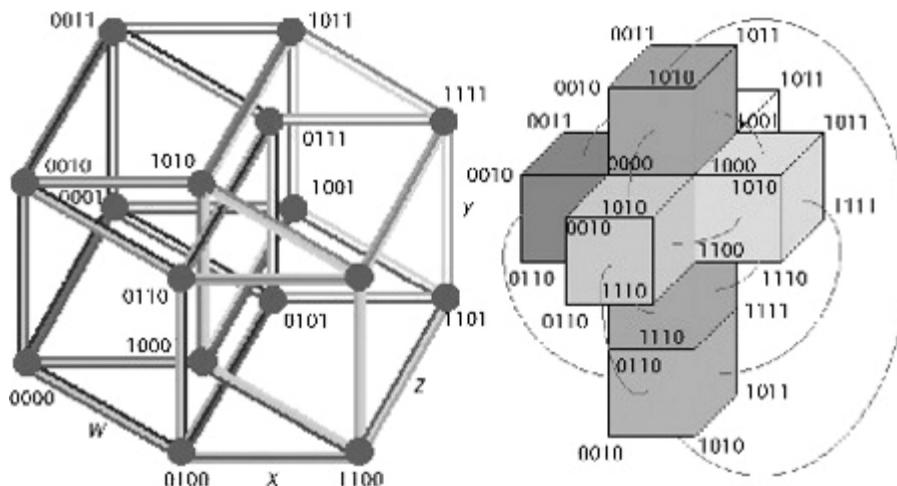


Figura 31. Hipercubo. Izquierda: proyectado en dos dimensiones. Derecha: desdoblado para mostrar sus ocho «caras» cúbicas. Los 0 y los 1 indican las coordenadas.

El artista surrealista Salvador Dalí usó un cubo desdoblado similar en varios trabajos, destacamos su *Crucifixión (Corpus hypercubus)* de 1954.



Figura 32. Crucifixión (*Corpus hypercubus*) de Dalí.

5. Hipotenusa pitagórica

Los triángulos pitagóricos tienen un ángulo recto y sus lados miden un número entero. El más sencillo tiene un lado mayor de 5 y los otros de 3 y 4. Hay 5 sólidos regulares. La ecuación de grado 5, en la que la incógnita está elevada a 5, *no puede* resolverse usando raíces quintas, o cualquier otra raíz. Las celosías en el plano y el espacio tridimensional no tienen simetrías de rotación de orden 5, por lo que esas simetrías no se dan en cristales. Sin embargo, pueden darse para celosías en cuatro dimensiones y en estructuras curiosas conocidas como «cuasicristales».

§. Hipotenusa de la menor terna pitagórica

El teorema de Pitágoras dice que el lado mayor de un triángulo rectángulo (la infame hipotenusa) está relacionado con los otros dos lados de un modo hermosamente sencillo: *el cuadrado de la hipotenusa es la suma de los cuadrados de los otros dos lados.*

Tradicionalmente lo llamamos «teorema de Pitágoras», pero su historia es turbia. Las tablas de barro sugieren que en la antigua Babilonia se conocía el teorema mucho antes de que Pitágoras lo enunciase; él se lleva la fama porque fundó un culto matemático, los pitagóricos, que creían que el universo se creó basado en patrones numéricos. Escritores de la Antigüedad atribuyeron varios teoremas matemáticos a los pitagóricos y, por extensión, a Pitágoras, pero no tenemos una idea real de las matemáticas que el propio Pitágoras desarrolló. Ni siquiera sabemos si los pitagóricos pudieron probar el teorema de Pitágoras o solo creían que era cierto. O, más probable, tenían evidencias convincentes que sin embargo no cumplen con lo que ahora consideraríamos una demostración.

Demostraciones de Pitágoras

La primera demostración conocida del teorema de Pitágoras aparece en los *Elementos* de Euclides. Es bastante complicada, e involucra un diagrama conocido por los estudiantes de la época victoriana como «los

calzoncillos de Pitágoras», porque parece ropa interior colgada en un tendedero. Se conocen, literalmente, cientos de demostraciones, la mayoría de las cuales hacen al teorema mucho más obvio.

Una de las más sencillas es una especie de rompecabezas matemático. Considera cualquier triángulo rectángulo, haz cuatro copias y colócalas dentro de un cuadrado.

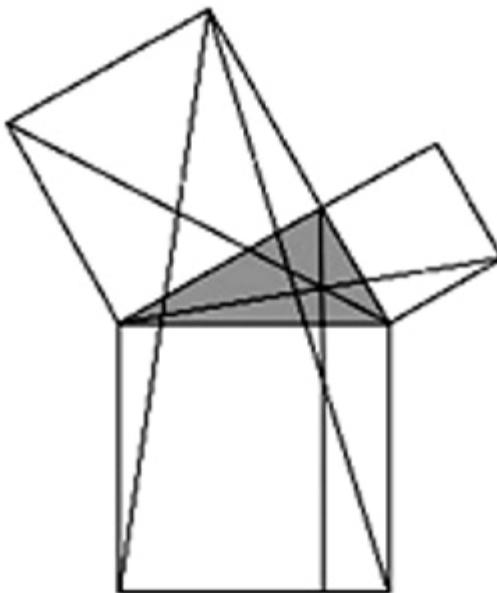


Figura 33. Los calzoncillos de Pitágoras.

En una de las ordenaciones vemos que los lados del cuadrado son las hipotenusas de los triángulos rectángulos; en la otra, son los catetos. Claramente, las áreas son iguales.

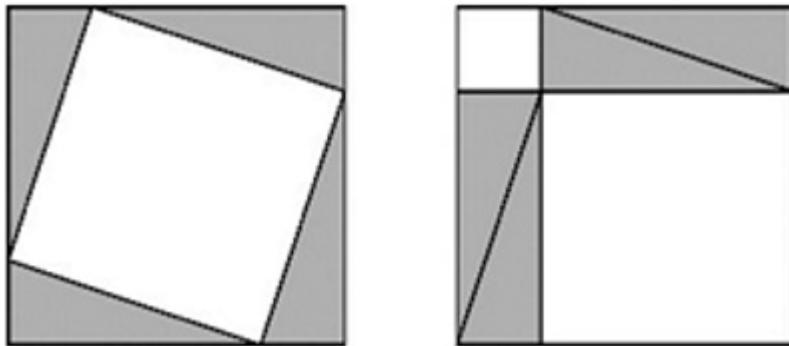


Figura 34. Izquierda: el cuadrado sobre la hipotenusa (más los cuatro triángulos). Derecha: la suma de los cuadrados de los otros dos lados (más los cuatro triángulos). Ahora, quita los triángulos

Otra demostración tipo rompecabezas es la disección de Perigal:

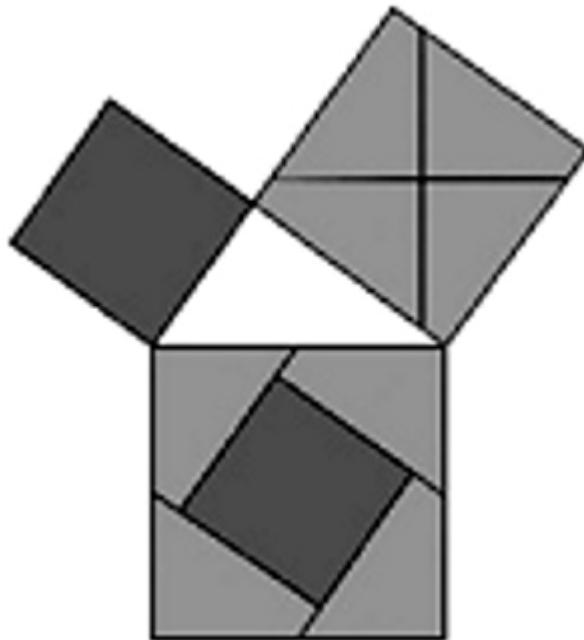


Figura 35. La disección de Perigal.

Hay también una demostración que usa un patrón de embaldosado. Bien podría ser como los pitagóricos, o algún predecesor desconocido, descubrieron el teorema por primera vez. Si observas cómo el cuadrado oblicuo se superpone a los otros dos, puedes ver que corta el cuadrado grande en piezas que se ensamblan para hacer los dos cuadrados pequeños. También puedes ver triángulos rectángulos, cuyos lados dan los tres tamaños del cuadrado.

Hay demostraciones impecables que se sirven de triángulos parecidos y trigonometría. Se conocen al menos cincuenta demostraciones diferentes.

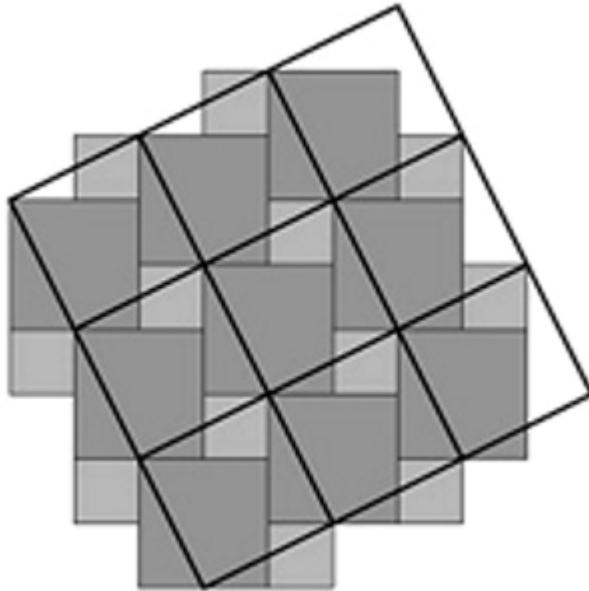


Figura 36. Demostración usando el embaldosado.

Ternas pitagóricas

El teorema de Pitágoras dio origen a una idea productiva en teoría de números: encontrar soluciones de ecuaciones algebraicas que sean

números naturales. Una terna pitagórica es una lista de tres números naturales a, b, c tales que

$$a^2 + b^2 = c^2$$

Geométricamente, la terna define un triángulo rectángulo cuyos lados miden lo que indican los números naturales.

La hipotenusa más pequeña en una terna pitagórica es 5. Los otros dos lados miden 3 y 4. Veamos:

$$3^2 + 4^2 = 9 + 16 = 25 = 5^2$$

La siguiente hipotenusa más pequeña es 10, porque:

$$6^2 + 8^2 = 36 + 64 = 100 = 10^2$$

Sin embargo, este es básicamente el mismo triángulo en el que cada uno de los lados vale el doble. La siguiente hipotenusa más pequeña de manera genuina es 13, porque

$$5^2 + 12^2 = 25 + 144 = 169 = 13^2$$

Euclides sabía que había infinidad de ternas pitagóricas genuinamente diferentes y dio lo que equivale a una fórmula para encontrarla todas. Más tarde, Diofanto de Alejandría enunció una receta sencilla que es básicamente la misma que la de Euclides.

Toma dos números naturales cualesquiera y considera:

- dos veces su producto
- la diferencia entre sus cuadrados
- la suma de sus cuadrados

Los tres números resultantes son los lados de un triángulo pitagórico.

Por ejemplo, toma los números 2 y 1. Entonces:

- dos veces su producto = $2 \times 2 \times 1 = 4$
- la diferencia entre sus cuadrados = $2^2 - 1^2 = 3$
- la suma de sus cuadrados = $2^2 + 1^2 = 5$

Y obtenemos el famoso triángulo 3 – 4 – 5. Si en su lugar tomamos los números 3 y 2, entonces:

- dos veces su producto = $2 \times 3 \times 2 = 12$
- la diferencia entre sus cuadrados = $3^2 - 2^2 = 5$
- la suma de sus cuadrados = $3^2 + 2^2 = 13$

y obtenemos el siguiente triángulo más famoso 5 – 12 – 13.

Por otro lado, tomando los números 42 y 23, nos lleva a:

- dos veces su producto = $2 \times 42 \times 23 = 1.932$
- la diferencia entre sus cuadrados = $42^2 - 23^2 = 1.235$
- la suma de sus cuadrados = $42^2 + 23^2 = 2.293$

y nadie ha oído jamás hablar del triángulo 1.235 – 1.932 – 2.293. Pero estos números funcionan:

$$1.235^2 + 1.932^2 = 1.525.225 + 3.732.624 = 5.257.849 = 2.293^2$$

Hay un giro final en la regla de Diofanto, que ya insinuamos: habiendo calculado tres números, podemos escoger cualquier otro número que queramos y multiplicarlos todos por él. Así, el triángulo 3 – 4 – 5 puede convertirse en el triángulo 6 – 8 – 10, multiplicando los tres números por 2, o en el triángulo 15 – 20 – 25 multiplicando los tres números por 5.

Usando el álgebra, la regla toma esta forma: sean u , v y k números naturales. Entonces el triángulo rectángulo de lados:

$$2kuv \text{ y } k(u^2 - v^2)$$

tiene hipotenusa

$$k(u^2 + v^2)$$

Hay modos alternativos de expresar la idea básica, pero todos se reducen a este, que da todas las ternas pitagóricas.

§. Sólidos regulares

Hay exactamente cinco sólidos regulares.

Un sólido (o poliedro) regular es una figura sólida con infinidad de caras planas. Las caras se cortan en rectas que se llaman «aristas»; las aristas se cortan en puntos que se llaman «vértices».

El clímax de los *Elementos* de Euclides es la demostración de que hay exactamente cinco poliedros *regulares*, poliedros en los que cada cara es un polígono regular (lados iguales y ángulos iguales), todas las caras son idénticas y en cada vértice se encuentra exactamente el mismo número de caras. Los cinco poliedros regulares (también llamados «sólidos regulares») son:

- El tetraedro, con 4 caras triangulares, 4 vértices y 6 aristas.
- El cubo o hexaedro, con 6 caras cuadradas, 8 vértices y 12 aristas.
- El octaedro, con 8 caras triangulares, 6 vértices y 12 aristas.
- El dodecaedro, con 12 caras pentagonales, 20 vértices y 30 aristas.
- El icosaedro, con 20 caras triangulares, 12 vértices y 30 aristas.



Figura 37. Los cinco sólidos regulares.

Los sólidos regulares aparecen en la naturaleza. En 1904, Ernst Haeckel publicó dibujos de organismos minúsculos conocidos como «radiolarios», que recordaban a los cinco sólidos regulares. Sin embargo, puede que hubiese arreglado algo la naturaleza, de modo que puede que no fuesen representaciones genuinas de criaturas vivas. Los tres primeros se dan también en cristales. El dodecaedro y el icosaedro no, aunque se han encontrado en ocasiones dodecaedros *irregulares*. Los dodecaedros genuinos pueden darse en cuasicristales, que son similares a los cristales excepto porque sus átomos no forman una estructura periódica.

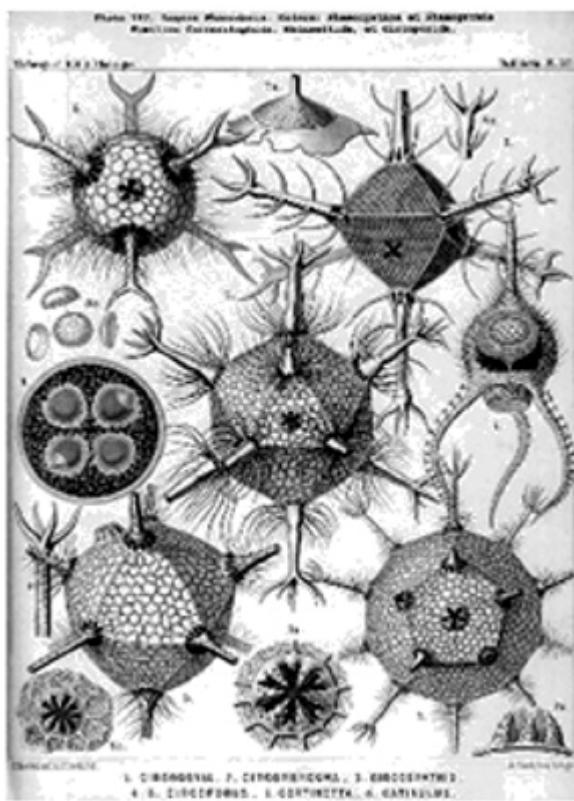


Figura 38. Dibujos de Haeckel de radiolarios con forma de sólidos regulares.

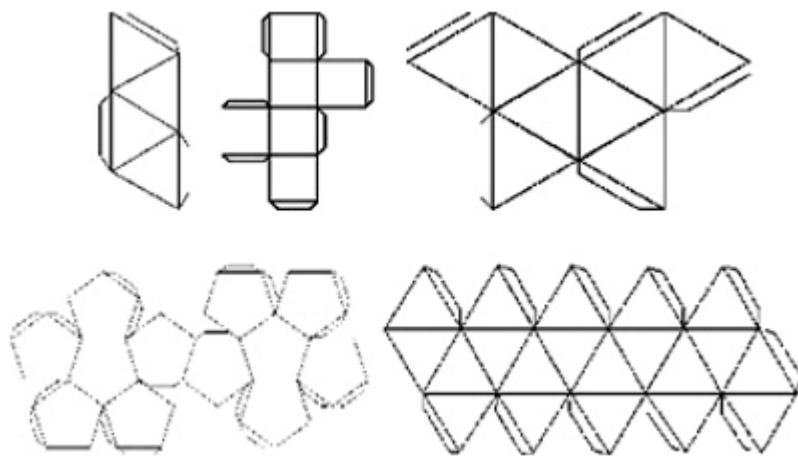


Figura 39. Desarrollos de los sólidos regulares.

Es divertido hacer modelos de los sólidos regulares con cartón cortando un conjunto de caras enlazadas, también llamado «desarrollo del sólido», y luego doblando por las aristas y pegando los pares de aristas apropiados. Ayuda añadir solapas en las aristas de cada uno de esos pares (como se muestra en la Figura) para el pegamento. Como alternativa, puedes usar cinta adhesiva.

§. Ecuación de grado 5

No hay fórmula algebraica para resolver las ecuaciones de grado 5.

Las ecuaciones de grado 5 tienen este aspecto:

$$ax^5 + bx^4 + cx^3 + dx^2 + ex + f = 0$$

El problema es encontrar una fórmula para las soluciones (puede haber hasta cinco). La experiencia con las cuadráticas, las cúbicas y las de

grado 4 sugiere que debería haber una fórmula para resolver las de grado 5, probablemente en la que se vean involucradas raíces quintas, raíces cúbicas y raíces cuadradas. Era una apuesta segura que esa fórmula no sería en realidad muy complicada.

Esta expectativa resultó ser errónea. Realmente no hay ninguna fórmula, al menos ninguna formada con los coeficientes a, b, c, d, e y f usando la suma, la resta, la multiplicación y la división, junto con la extracción de raíces. De modo que hay algo especial en relación con el número 5. Las razones para este comportamiento excepcional son bastante profundas y llevó bastante tiempo averiguarlas.

La primera señal del problema fue que cada vez que los matemáticos intentaban encontrar esa fórmula, no importa lo listos que fueran, fracasaban. Durante un tiempo, todo el mundo asumía que sucedía porque la fórmula era tan terriblemente complicada que nadie podía calcular el álgebra de modo correcto. Pero finalmente algunos matemáticos empezaron a preguntarse si esa fórmula existiría. Finalmente, en 1823, Niels Hendrik Abel se las arregló para probar que no existía. Poco tiempo después, Évariste Galois encontró un modo de decidir si una ecuación de cualquier grado, 5, 6, 7 o el que fuese, era resoluble usando ese tipo de fórmula.

La conclusión es que el número 5 es especial. Puedes resolver ecuaciones algebraicas (usando raíces enésimas para varios valores de n) para los grados 1, 2, 3 y 4, pero *no* 5. El aparente patrón se disipa.

No sorprende que ecuaciones de grado mayor que 5 sean todavía peores y, en particular, sufran del mismo problema: ninguna fórmula para la solución. Esto no significa que no exista solución, y no significa que no sea posible encontrar soluciones numéricas muy precisas. Expresa una limitación de las herramientas tradicionales del álgebra. Es como no ser capaz de hacer la trisección de un ángulo con regla y compás. La respuesta *existe*, pero los métodos especificados no son adecuados para averiguar cuál es.

§. Restricción cristalográfica

Los cristales en dos y tres dimensiones no tienen simetrías de rotación de orden 5.

Los átomos en un cristal forman una red, una estructura que se repite periódicamente en varias direcciones independientes. Por ejemplo, el patrón del papel de pared se repite a lo largo de la longitud del rollo de papel, pero normalmente también se repite en los laterales, quizá con un descenso de una pieza del papel de pared a la adyacente. Los papeles de pared son, de hecho, como un cristal bidimensional.

Hay 17 tipos diferentes de patrones de papel de pared en el plano [véase 17]. Estos se distinguen por sus simetrías, las cuales son modos de mover el patrón rígidamente y encajarlo exactamente en la cima de su posición original. Entre ellas están las simetrías de rotación, donde el patrón se rota un ángulo determinado respecto a un punto, el centro de rotación.

El orden de una simetría de rotación es el número de veces que se debe aplicar la rotación para volver todo a como estaba al principio. Por ejemplo, una rotación de 90° tiene orden 4. La lista de los posibles tipos de simetría para rotaciones de la estructura de un cristal revela una curiosidad para el número 5 en concreto: no hay. Hay patrones con simetrías de rotación de órdenes 2, 3, 4 y 6, pero ningún patrón del papel de pared tiene simetría de rotación de orden 5. No hay simetrías de rotación de orden mayor que 6 tampoco, pero el primer hueco es en 5. Lo mismo ocurre para patrones cristalográficos en el espacio tridimensional. En este caso la estructura se repite a lo largo de tres direcciones independientes. Hay 219 tipos de simetrías diferentes, o 230 si la imagen en el espejo de un patrón se considera distinta cuando el patrón no tiene simetría de reflexión. De nuevo los posibles órdenes de las simetrías de rotación son 2, 3, 4 y 6, pero no 5. Este hecho se llama «restricción cristalográfica».

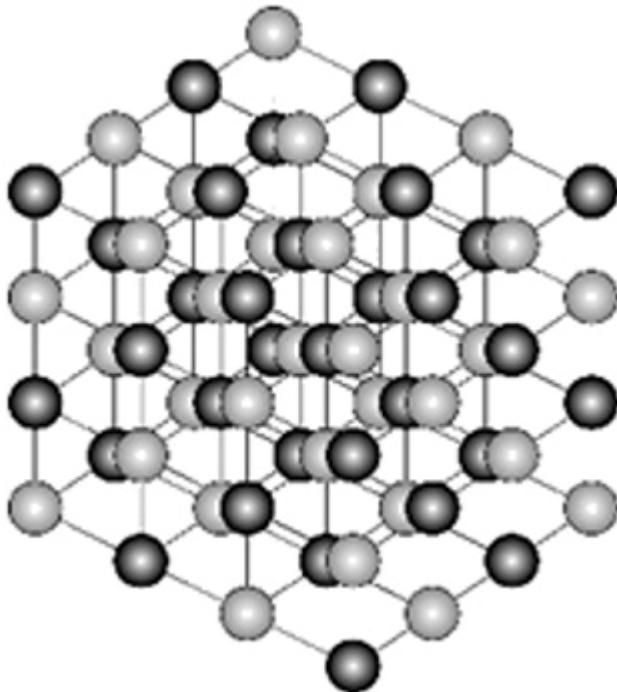


Figura 40. Estructura del cristal de la sal. Esferas negras: átomos de sodio. Esferas claras: átomos de cloro.

En cuatro dimensiones, existen estructuras con simetrías de orden 5 y cualquier orden dado es posible para estructuras de dimensión lo suficientemente alta.

§. Cuasicristales

Aunque las simetrías de rotación de orden 5 no son posibles en estructuras de dos o tres dimensiones, pueden darse en estructuras ligeramente menos regulares llamadas «cuasicristales». Siguiendo algunos bocetos hechos por Kepler, Roger Penrose descubrió patrones en el plano con un tipo más general de simetrías de orden 5: *cuasicristales*.

Los cuasicristales se dan en la naturaleza. En 1984, Daniel Shechtman descubrió que una aleación de aluminio y manganeso puede formar un cuasicristal, y después de cierto escepticismo inicial entre los cristalografos, ganó el premio Nobel de Química en 2011, cuando se probó que el descubrimiento era correcto. En 2009, un equipo dirigido por Luca Bindi encontró cuasicristales en un mineral de las montañas de Koryak, en Rusia, un compuesto de aluminio, cobre y hierro. Este mineral se conoce actualmente como «icosaedrita». Usando un espectrómetro de masas para medir las proporciones de los diferentes isótopos de oxígeno, mostraron que el mineral no se originó en la Tierra. Se formó hace unos 4.500 millones de años, la época cuando el sistema solar comenzaba a existir, y pasó mucho del tiempo intermedio orbitando en el cinturón de asteroides, antes de que alguna perturbación cambiase su órbita y finalmente cayera en la Tierra.

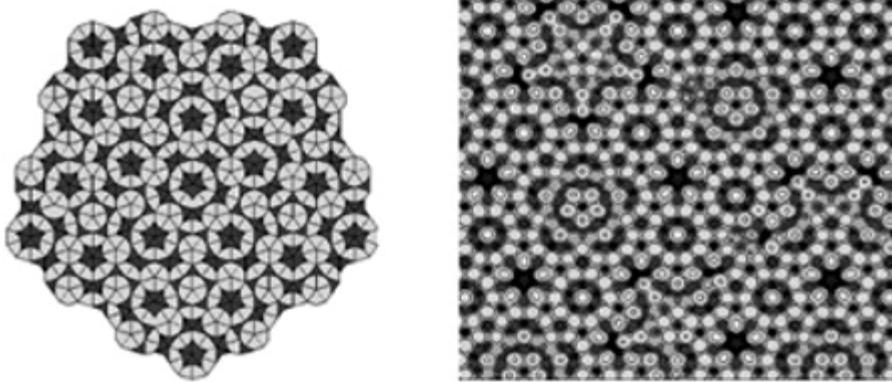


Figura 41. Izquierda: uno de los dos patrones de cuasicristales con simetrías de orden 5 exactas. Derecha: modelo atómico de un cuasicristal icosaédrico de aluminio-paladio-manganeso.

6. Número de osculación

El número más pequeño igual a la suma de sus divisores propios: $6 = 1 + 2 + 3$. El número de osculación en el plano es 6. Los panales están formados por polígonos regulares de 6 lados, hexágonos. Hay 6 politopos regulares de dimensión 4 (análogos a los sólidos regulares).

§. Número perfecto más pequeño

Los griegos en la Antigüedad distinguieron tres tipos de números naturales según sus divisores:

- Números *abundantes*, para los cuales la suma de los divisores «propios» (esto es, los divisores excluyendo el propio número) es mayor que el número.
- Números *deficientes*, para los cuales la suma de los divisores propios es más pequeña que el número.
- Números *perfectos*, para los cuales la suma de los divisores propios es igual al número.

Para los primeros números, tenemos la Tabla 7.

Esto muestra que se dan los tres tipos de números, pero también sugiere que los números deficientes son más comunes que los de los otros dos tipos. En 1998, Marc Deléglise probó una forma precisa de esta afirmación: a medida que n se hace arbitrariamente grande, la proporción de números deficientes entre 1 y n tiende a alguna constante entre 0,7526 y 0,7520, mientras la proporción de números abundantes está entre 0,2474 y 0,2480. En 1955, Hans-Joachim Kanold ya había probado que la proporción de los números perfectos tiende a 0. De modo que los tres cuartos de todos los números son deficientes y un cuarto son abundantes. Prácticamente ninguno es perfecto.

Tabla 7

Número	Suma de los divisores	Tipo
	<i>propios</i>	
1	0 (sin divisores propios)	deficiente
2	1	deficiente
3	1	deficiente
4	$1 + 2 = 3$	deficiente
5	1	deficiente
6	$1 + 2 + 3 = 6$	perfecto
7	1	deficiente
8	$1 + 2 + 4 = 7$	deficiente
9	$1 + 3 = 4$	deficiente

10	$1 + 2 + 5 = 8$	deficiente
11	1	deficiente
12	$1 + 2 + 3 + 4 + 6 = 16$	abundante
13	1	deficiente
14	$1 + 7 = 8$	deficiente
15	$1 + 3 + 5 = 9$	deficiente

Los dos primeros números perfectos son:

$$6 = 1 + 2 + 3$$

$$28 = 1 + 2 + 4 + 7 + 14$$

Así que el número perfecto más pequeño es 6. El número abundante más pequeño es 12.

En la Antigüedad encontraron los dos siguientes números perfectos: 28 y 496. Alrededor de 100 d. C., Nicómaco de Gerasa había encontrado el cuarto, que es 8.128. Alrededor de 1460, el quinto, 33.550.336, apareció en un manuscrito anónimo. En 1588, Pietro Cataldi encontró los números perfectos sexto y séptimo: 8.589.869.056 y 137.438.691.328.

Mucho antes de este trabajo Euclides dio una regla para formar números perfectos. En notación moderna dice que si $2^n - 1$ es primo, entonces $2^{n-1}(2^n - 1)$ es perfecto. Los números anteriores corresponde a $n = 2, 3, 5, 7,$

13, 17, 19. Los primos de la $2n - 1$ se llaman «primos de Mersenne» por el monje Marin Mersenne [véase $2^{57.885.161} - 1$].

Euler probó que todo número perfecto par es de esta forma. Sin embargo, durante al menos 2.500 años, los matemáticos no han sido capaces de encontrar un número perfecto impar, o probar que dicho número no existe. Si existe un número así, al menos debe tener 1.500 dígitos y 101 factores primos, de los cuales al menos 9 son distintos. Su factor primo más grande debe tener nueve o más dígitos.

§. Número de osculación

El número de osculación en el plano es el mayor número de círculos, de un tamaño dado, que pueden tocar a un círculo del mismo tamaño. Es igual a 6.

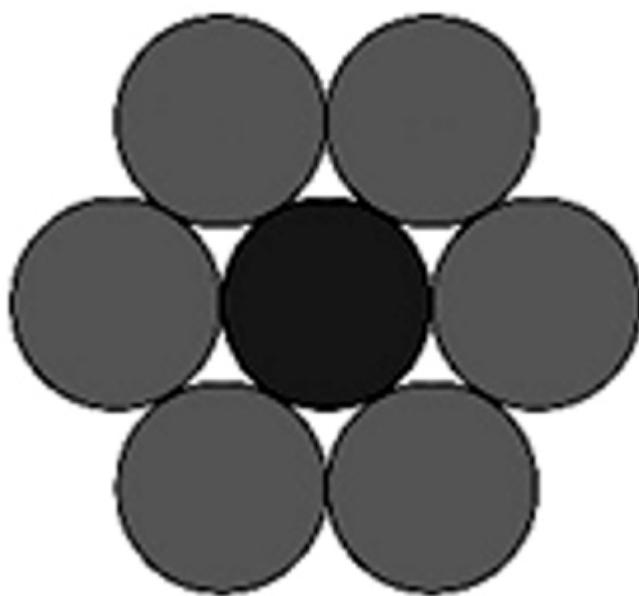


Figura 42. El número de osculación en el plano es 6.

Para la prueba basta con geometría elemental.

El número de osculación en el espacio tridimensional es el mayor número de esferas, de un tamaño dado, que pueden tocar a una esfera del mismo tamaño. Es igual a 12 [véase 12]. En este caso la prueba es mucho más complicada y durante mucho tiempo no se supo si 13 esferas podrían ser una posibilidad o no.

§. Panales

Los panales están formados por «baldosas» hexagonales, las cuales encajan unas con otras perfectamente para cubrir el plano [véase 3].

Según la *conjetura del panal* de abeja, el patrón del panal es el modo de dividir el plano en regiones cerradas que minimiza el perímetro total. Esta hipótesis fue planteada en la Antigüedad, por ejemplo, por el erudito romano Marcus Terentius Varro, en 36 a. C. Incluso podría remontarse al geómetra griego Pappus de Alejandría, alrededor de 325 a. C.

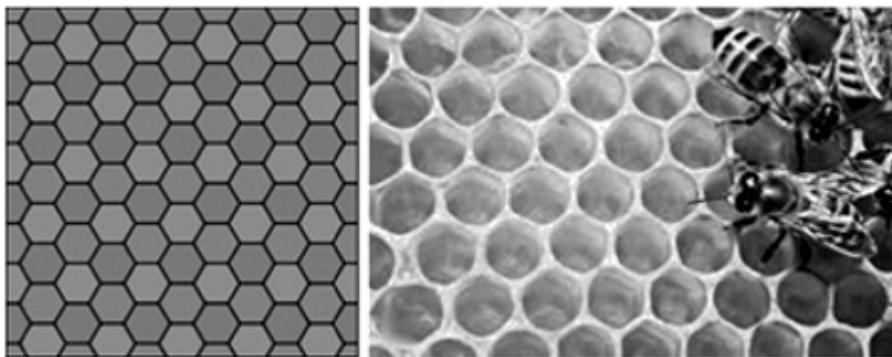


Figura 43. Izquierda: embaldosado de hexágonos regulares. Derecha: un panal de abejas.

La conjetura del panal de abeja es ahora un teorema; Thomas Hales lo probó en 1999.

§. Número de politopos cuatro-dimensionales

Los griegos probaron que eran exactamente cinco los sólidos regulares en tres dimensiones [véase 5]. ¿Qué pasa con los espacios de dimensiones diferentes de tres? Recuerda de [4] que podemos definir espacios matemáticos con cualquier número de dimensiones usando coordenadas. En concreto, el espacio cuatro-dimensional se compone de cuartetos (x, y, z, w) de números reales. Hay un concepto natural de distancia en estos espacios, basado en la analogía obvia del teorema de Pitágoras, de modo que, con buen juicio, podemos hablar de longitudes, ángulos, análogos de esferas, cilindros, conos, etcétera. Por lo tanto, tiene sentido cuáles son los análogos de los polígonos regulares en cuatro o más dimensiones. La respuesta contiene una sorpresa.

En dos dimensiones hay infinidad de polígonos regulares: uno por cada número entero positivo de lados a partir de tres. En cinco o más dimensiones, hay solo tres politopos, como se llaman, regulares. Son análogos al tetraedro, cubo y octaedro. Pero en el espacio de dimensión cuatro, hay *seis* politopos regulares.

Tabla 8

Nombre	Celdas	Caras	Aristas	Vértices
Pentácoron	5 tetraedros	10	10	5
Teseracto	8 cubos	24	32	16
Hexadecacoron o 16-cell	16 tetraedros	32	24	8
Icositetracoron o 24-cell	24 octaedros	96	96	24
120-cell	120 dodecaedros	720	1.200	600
600-cell	600 tetraedros	1.200	720	120

Los tres primeros politopos en la tabla son análogos al tetraedro, el cubo y el octaedro. El pentácoron también se llama 4-simplex, el teseracto es un 4-hipercubo. Los otros tres politopos son característicos del espacio 4-dimensional.

Al carecer del papel 4-dimensional, me quedo satisfecho mostrándote el aspecto de estos objetos cuando se proyectan en el plano.

Ludwig Schläfli clasificó los politopos regulares. Publicó algunos de sus resultados en 1855 y 1858 y el resto póstumamente, en 1901. Entre 1880 y 1900, otros nuevos matemáticos obtuvieron, independientemente, resultados similares. Entre ellos estaba Alicia Boole Stott, una de las

hijas del matemático y lógico George Boole, que fue la primera en usar la palabra «politopo». Demostró una comprensión de la geometría 4-dimensional desde una temprana edad, probablemente porque su hermana mayor, Mary, se casó con Charles Howard Hinton, un personaje extravagante (fue condenado por bigamia) con una pasión por el espacio cuatro-dimensional. Usó esta habilidad para calcular, por métodos puramente euclídeos, qué aspecto tenían los cortes transversales de los politopos: son sólidos simétricos muy complicados.

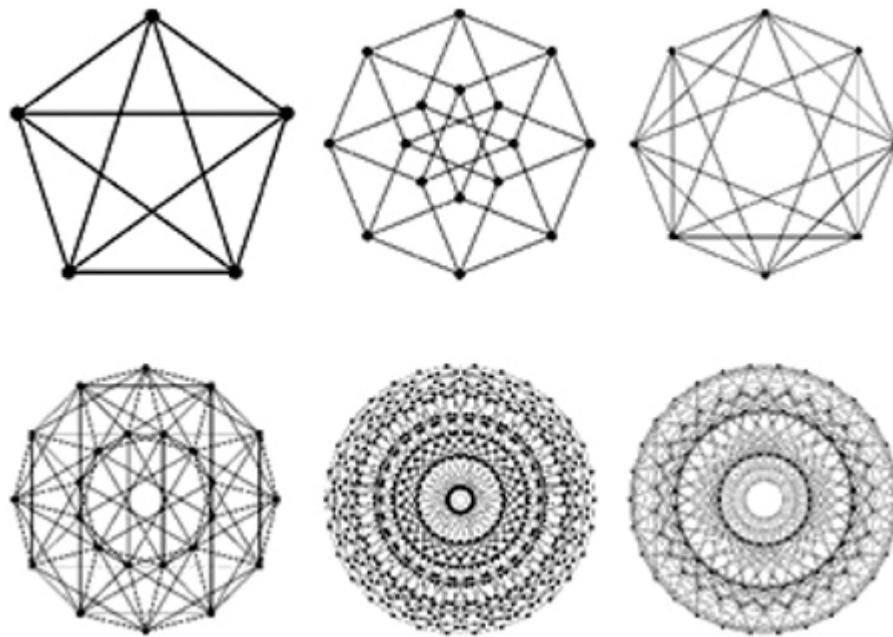


Figura 44. Los seis politopos regulares proyectados en el plano. De izquierda a derecha y de arriba abajo: pentácoron, teseracto, hexadecacoron, 24-cell, 120-cell y 600-cell.

7. Cuarto primo

El número 7 es el cuarto número primo y un lugar conveniente para explicar para qué son buenos los primos y por qué son interesantes. Los primos aparecen en la mayoría de los problemas en los cuales los números naturales se multiplican unos con otros. Son «ladrillos» para todos los números naturales. Vimos en [1] que todo número natural mayor que 1, o bien es primo, o bien puede obtenerse multiplicando dos o más primos.

El número 7 también tiene conexiones con un problema antiguo sin resolver sobre factoriales. Y es el número más pequeño de colores necesarios para colorear todos los mapas en un toro, de modo que las regiones adyacentes tengan diferentes colores.

§. Encontrar factores

En 1801, Gauss, el teórico de números destacado de su era y uno de los matemáticos más importantes de todos los tiempos, escribió un libro avanzado sobre teoría de números, *Disquisitiones arithmeticæ*. Entre todos los temas de alto nivel, indicó que dos temas muy básicos son vitales: «El problema de distinguir números primos de números compuestos y descomponer estos últimos en sus factores primos es conocido por ser uno de los más importantes y útiles en aritmética».

El modo más obvio de resolver ambos problemas es intentar todos los posibles factores uno a uno. Por ejemplo, para ver si 35 es primo y encontrar sus factores si no lo es, calculamos:

$$35: 2 = 17 \text{ con resto } 1$$

$$35: 3 = 11 \text{ con resto } 2$$

$$35: 4 = 8 \text{ con resto } 3$$

$$35: 5 = 7 \text{ exactamente}$$

Por lo tanto, $35 = 5 \times 7$, y como sabemos que 7 es un primo, tenemos completa la factorización.

Este procedimiento puede simplificarse un poco. Si tenemos ya una lista de primos, solo necesitamos intentarlo con los divisores primos. Por ejemplo, al establecer que 2 no divide de manera exacta a 35, sabemos que 4 no lo dividirá de manera exacta tampoco. La razón es que 2 divide a 4, de modo que 2 divide cualquier cosa que sea divisible por 4. (Lo mismo se aplica para 6, 8 o cualquier otro número par.)

También podemos dejar de seguir buscando una vez alcancemos la raíz cuadrada del número que nos ocupa. ¿Por qué? Un caso típico es el número 4.283, cuya raíz cuadrada es aproximadamente 65,44. Si multiplicamos dos números que son mayores que este, el resultado tiene que ser mayor que $65,44 \times 65,44$, que es 4.283. Así que, aunque dividamos 4.283 en dos o más factores, al menos uno de ellos es menor o igual que su raíz cuadrada. De hecho, debe ser menor o igual que 65, que es lo que obtenemos cuando ignoramos lo que hay detrás del punto decimal en la raíz cuadrada.

Por lo tanto, podemos encontrar todos los factores de 4.283 haciendo pruebas con los números primos entre 2 y 65. Si alguno de ellos dividiera 4.283 de manera exacta, continuaríamos factorizando el resultado después de hacer esta división, pero este sería un número más pequeño que 4.283. Resulta que ningún primo menor que 65 divide a 4.283. Por lo tanto, 4.283 es primo.

Si intentamos la misma idea para factorizar 4.183, cuya raíz cuadrada es 64,67, tenemos que intentarlo con todos los primos hasta 64. En este caso el primo 47 divide a 4.183 de manera exacta:

$$4.183 : 47 = 89$$

Resulta que 89 es primo. De hecho, esto ya lo sabemos, porque 4.183 no es divisible entre 2, 3, 5 y 7. De modo que 89 no es divisible por 2, 3, 5 y 7, pero estos son los únicos primos hasta su raíz cuadrada, que es 9,43. Con lo que tenemos que la factorización es $4.183 = 47 \times 89$.

Este procedimiento, aunque sencillo, no es muy útil para números grandes. Por ejemplo, para encontrar factores de

$$11.111.111.111.111.111$$

tendríamos que intentar todos los primos hasta su raíz cuadrada: 105.409.255,3.

Es una cantidad horrible de primos: 6.054.855 primos, para ser exactos. Finalmente, encontraríamos un factor primo, en concreto 2.071.723, y obtendríamos la factorización

$$11.111.111.111.111 = 2.071.723 \times 5.363.222.357$$

pero llevaría mucho tiempo hacer esto a mano.

Un ordenador puede resolverlo, por supuesto, pero una regla básica en esos cálculos es que si algo se hace muy difícil a mano para números moderadamente grandes, entonces se hace muy difícil para un ordenador para números suficientemente más grandes. Incluso un ordenador podría tener problemas llevando a cabo una búsqueda sistemática como esta si el número tiene 50 dígitos en lugar de 17.

Teorema de Fermat

Afortunadamente, hay métodos mejores y más eficientes de comprobar si un número es primo *sin* buscar los factores. Por lo general, estos métodos son prácticos para números con alrededor de un centenar de dígitos, aunque el grado de dificultad varía mucho dependiendo del número en concreto y la cantidad de dígitos que tiene es solo una guía aproximada. Por el contrario, los matemáticos actualmente no conocen métodos rápidos que garanticen encontrar los factores de *cualquier* número compuesto de ese tamaño. Sería suficiente encontrar tan solo un factor,

porque puede entonces dividirse y el proceso repetirse, pero, en el peor de los casos, este proceso supone demasiado tiempo para resultar práctico.

Las pruebas de primalidad prueban que un número es compuesto sin encontrar ninguno de sus factores. Tan solo muestran que la prueba de primalidad falla. Los números primos tienen propiedades especiales y podemos comprobar si un número dado las tiene. Si no, no puede ser primo. Es casi como encontrar un pinchazo en un globo soplando y viendo si se queda hinchado. Si no se queda hinchado, hay un pinchazo, pero esta prueba no nos dice exactamente dónde se localiza este. De modo que probar que hay un pinchazo es más fácil que encontrarlo. Lo mismo pasa con los factores.

La más simple de estas pruebas es el teorema de Fermat. Para enunciarlo, primero hablaremos de aritmética modular, a veces conocida como «aritmética de los relojes», porque los números dan vueltas alrededor como en un reloj. Escoge un número, para una analogía de reloj de 12 horas es el 12, y llámalo «módulo». En cualquier cálculo aritmético con números enteros, te permites reemplazar cualquier múltiplo de 12 por cero. Por ejemplo, $5 \times 5 = 25$, pero 24 es dos veces 12, así que restando 24 obtenemos $5 \times 5 = 1$ en módulo 12.

Gauss presentó la aritmética modular en *Disquisitiones arithmeticæ* y hoy en día se usa de manera general en la informática, la física y la ingeniería, así como en matemáticas. Es muy bella, porque casi todas las

reglas habituales de la aritmética funcionan. La principal diferencia es que no siempre puedes dividir un número entre otro, incluso cuando este no es cero. Es útil también porque proporciona un modo ordenado de tratar con cuestiones sobre divisibilidad: qué números son divisibles entre el módulo escogido y cuál es el resto cuando no son divisibles. El teorema de Fermat afirma que si escogemos cualquier módulo primo p , y tomamos cualquier número a que no es múltiplo de p , entonces la potencia $p - 1$ de a es siempre igual a 1 en aritmética de módulo p .

Supongamos, por ejemplo, que $p = 17$ y $a = 3$. Entonces el teorema predice que cuando dividimos 3^{16} entre 17, el resto es 1. Lo comprobamos:

$$3^{16} = 43.046.721 = 2.532.160 \times 17 + 1$$

Nadie en su sano juicio querría hacer los cálculos de ese modo para números muy grandes. Afortunadamente, hay un modo más inteligente y rápido de llevar a cabo este tipo de cálculos, elevando al cuadrado repetidamente el número y multiplicando los resultados oportunos.

La clave es que *si la respuesta no es igual a 1, entonces el módulo con el que empezamos debe ser compuesto*. De modo que el teorema de Fermat forma las bases de una prueba eficiente que proporciona una condición necesaria para que un número sea primo. Y lo hace sin encontrar un factor. De hecho, esta podría ser la razón por la que es eficiente.

Sin embargo, la prueba de Fermat no es infalible: algunos números compuestos pasan la prueba. El más pequeño es 561. En 2003, Red Alford, Andrew Granville y Carl Pomerance probaron que hay infinidad de excepciones de este tipo: los números de Carmichael. La prueba de primos más eficiente hasta la fecha en cuanto a infalibilidad la idearon Leonard Adleman, Pomerance y Robert Rumely. Usa ideas de teoría de números que son más sofisticadas que el teorema de Fermat, pero con un espíritu similar.

En 2002, Manindra Agrawal y sus discípulos Neeraj Kayal y Nitin Saxena descubrieron una prueba de primalidad que en principio es más rápida que la prueba de Adleman-Pomerance-Rumely, porque se ejecuta en «tiempo polinómico». Si el número tiene n dígitos decimales, el algoritmo tiene un tiempo de ejecución proporcional a, como máximo, n^{12} . Ahora sabemos que esto puede reducirse a $n^{7,5}$. Sin embargo, las ventajas de su algoritmo no aparecen hasta que el número de dígitos en n es de alrededor de $10^{1.000}$. No hay hueco para encajar un número tan grande en el universo conocido.

§. Primos y códigos

Los números primos han adquirido importancia en criptografía, la ciencia de los códigos secretos. Los códigos son importantes para uso militar [véase 26], pero también compañías comerciales e individuos privados tienen secretos. No queremos que los delincuentes tengan

acceso a los números de cuentas del banco o tarjetas de crédito cuando usamos Internet, por ejemplo.

El modo habitual de reducir el riesgo es la encriptación: poner la información en código. El sistema RSA, un famoso código inventado por Ted Rivest, Adi Shamir y Leonard Adleman en 1978, usa números primos. De los grandes, de alrededor de 100 dígitos de longitud. Tiene la excepcional característica de que el modo de convertir un mensaje en código puede ser hecho público. Lo que no se revela es cómo ir en sentido contrario, cómo descifrar el mensaje. Eso necesita una pieza extra de información, que mantienes en secreto.

Cualquier mensaje puede fácilmente convertirse en un número, por ejemplo, asignándole un código de dos dígitos a cada letra y haciendo una cadena con todos esos códigos. Supongamos que decidimos usar los códigos $A = 01$, $B = 02$, etcétera, a los números del 27 en adelante le asignamos la puntuación y el espacio en blanco. Entonces:

<i>MENSAJE</i>	→	<i>M</i>	<i>E</i>	<i>N</i>	<i>S</i>	<i>A</i>	<i>J</i>	<i>E</i>
	→	13	05	14	20	01	10	05
	→							
	→	13051420011005						

Un código es un modo de convertir un mensaje dado en otro mensaje. Pero como cualquier mensaje es un número, un código puede pensarse como un modo de convertir un número dado en otro número. En este

momento, las matemáticas entran en juego y se pueden usar ideas de la teoría de números para crear códigos.

El sistema RSA empieza escogiendo dos primos p y q , cada uno de ellos de, por ejemplo, 100 dígitos. Los primos de este tamaño pueden encontrarse rápidamente con un ordenador usando una prueba de primalidad. Los multiplicamos para obtener pq . El método público para codificar los mensajes convierte el mensaje en un número y luego hace un cálculo basado en este número pq . Más abajo te facilito los detalles técnicos. Pero obtener el mensaje a partir del código requiere conocer p (así que q puede también calcularse fácilmente).

Sin embargo, si no dices públicamente qué es p , no pueden decodificar el mensaje, a menos que puedan *averiguar* el valor de p . Pero eso requiere factorizar pq , un número de 200 dígitos y a no ser que escojas p y q muy mal, parece imposible incluso con el superordenador más potente que exista. Si quien estableció el código pierde temporalmente p y q , estará en la misma posición que todos los demás. En concreto, fastidiado.

Detalles técnicos

Considera dos primos grandes p y q . Calcula $n = pq$ y $s = (p - 1)(q - 1)$. Escoge un número e entre 1 y s que no tenga ningún factor común con s . (Hay un modo muy eficiente de encontrar los factores comunes de dos números llamado «algoritmo de Euclides». Se remonta a la antigua Grecia y aparece en los *Elementos* de Euclides. Véase *Professor*

Stewart's Casebook of Mathematical Mysteries.) Haz n y e públicos. Designa e la «clave pública».

La aritmética modular nos dice que hay un único número d entre 1 y s para el cual el producto de deja un resto 1 en la división entre s . Esto es $de \equiv 1 \pmod{s}$. Calcula este número d . Mantén p , q , s y d en secreto. Designa ad la «clave privada».

Para poner un mensaje en código, represéntalo como un número m , como describí. Si es necesario, divide el mensaje largo en bloques y envía cada bloque de uno en uno. Luego calcula $c \equiv me \pmod{n}$. Este es el mensaje codificado y puede enviarse a su destinatario. Esta regla de encriptación puede hacerse pública de modo seguro. Hay un modo rápido de calcular c basado en la expansión binaria de e .

El destinatario, que conoce la clave privada d , puede decodificar el mensaje calculando $cd \pmod{n}$. Un teorema básico en teoría de números, una ligera extensión del teorema de Fermat, implica que el resultado es el mismo que en el mensaje original m .

Un espía intentando decodificar el mensaje tiene que averiguar d , sin saber s . Esto se reduce a conocer $p - 1$ y $q - 1$ o, de manera equivalente, p y q . Para encontrarlos, el espía tiene que factorizar n . Pero n es tan grande que esa operación no es factible.

Los códigos de este tipo se llaman «códigos de la trampilla», porque es fácil caer a través de la trampilla (poner un mensaje en código), pero difícil salir trepando de nuevo (decodificar el mensaje) a menos que se

tenga ayuda especial (la clave privada). Los matemáticos no saben con certeza si este código es totalmente seguro. Quizá hay un modo rápido de factorizar números grandes y todavía no hemos sido lo suficientemente inteligentes para encontrarlo. (Podría haber algún otro modo de calcular d , pero una vez que se sabe d , se puede averiguar p y q , lo que nos llevaría a un modo eficiente para encontrar factores.)

Incluso si el código es en teoría seguro, un espía podría ser capaz de hacerse con p y q con otros métodos, robando o sobornando o chantajeando a alguien que conoce el secreto. Este problema se da con cualquier código secreto. En la práctica, el sistema RSA se usa para un número limitado de mensajes importantes, por ejemplo, enviar a alguien la clave secreta para algún método más simple de poner mensajes en código.

§. El problema de Brocard

Si consideras todos los números desde 1 a n y los multiplicas, obtienes el «factorial de n », que se escribe como $n!$ Los factoriales cuentan el número de modos en los que n objetos pueden ordenarse [véase 26!].

Los primeros factoriales son:

$$1! = 1$$

$$2! = 2$$

$$3! = 6$$

$$4! = 24$$

$$5! = 120$$

$$6! = 720$$

$$7! = 5.040$$

$$8! = 40.320$$

$$9! = 362.880$$

$$10! = 3.628.800$$

Si sumamos 1 a estos números, obtenemos:

$$1! + 1 = 2$$

$$2! + 1 = 3$$

$$3! + 1 = 7$$

$$4! + 1 = 25$$

$$5! + 1 = 121$$

$$6! + 1 = 721$$

$$7! + 1 = 5.041$$

$$8! + 1 = 40.321$$

$$9! + 1 = 362.881$$

$$10! + 1 = 3.628.801$$

y reconocemos tres de estos como cuadrados perfectos, en concreto:

$$4! + 1 = 5^2$$

$$5! + 1 = 11^2$$

$$7! + 1 = 71^2$$

No se conoce ningún otro número así, pero no se ha probado que ningún número más grande, n , pueda dar como resultado que $n! + 1$ sea un cuadrado perfecto. Esta cuestión se conoce como «el problema de Brocard», porque en 1876 Henri Brocard preguntó si 7 era el mayor número con esta propiedad. Más tarde, Paul Erdős conjeturó que la respuesta era «no». En 2000, Bruce Berndt y William Galway probaron que no hay otras soluciones posibles para n menores que 1.000 millones. En 1993, Marius Overholt demostró que solo existe una cantidad finita, pero únicamente dando por hecho un problema no resuelto más importante en teoría de números llamado «conjetura ABC» (véase *Los grandes problemas matemáticos*).

§. Mapa de siete colores en un toro

Heawood trabajó en una generalización del problema de cuatro colores [véase 4] a mapas en superficies más complicadas.

La cuestión análoga en una esfera tiene la misma respuesta que en un plano. Imagina un mapa en una esfera y rótalo hasta que el polo norte esté en algún punto dentro de una región. Si borras el polo norte, puedes abrir la esfera perforada para obtener un espacio que es topológicamente

equivalente al plano infinito. La región que contiene el polo se convierte en una infinitamente grande que rodea el resto del mapa.

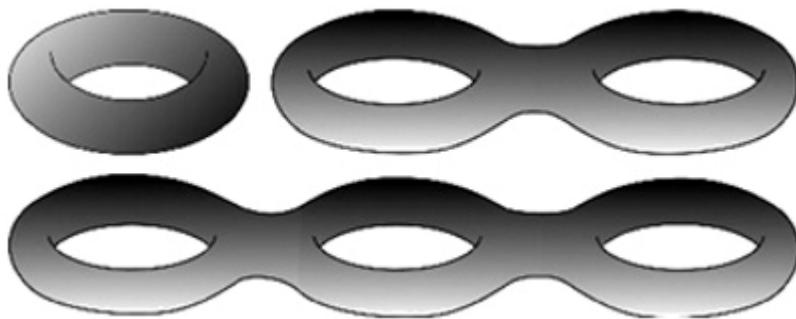


Figura 45. Toro, toro de 2 agujeros, toro de 3 agujeros.

Sin embargo, hay otras superficies más interesantes, como el toro, que tiene una forma similar a la de una rosquilla y superficies con varios de esos agujeros.

Hay un modo útil de visualizar el toro que suele facilitar la vida. Si cortamos el toro a lo largo de dos curvas cerradas, podemos abrirlo y que quede como un cuadrado.

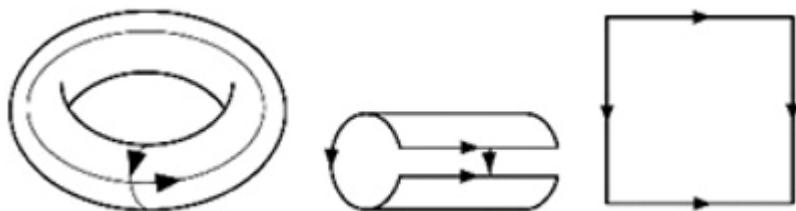


Figura 46. Haciendo un cuadrado plano a partir de un toro con cortes.

Esta transformación cambia la topología del toro, pero podemos salvar esto acordando tratar los puntos correspondientes en aristas opuestas

como si fueran idénticos (mostrados con flechas). Ahora viene la parte ingeniosa: realmente no necesitamos enrollar el cuadrado y unir las aristas correspondientes. Podemos trabajar con el cuadrado plano dado teniendo en mente la regla para identificar las aristas. Todo lo que hacemos en el toro, como dibujar curvas, tiene una construcción correspondiente y precisa en el cuadrado.

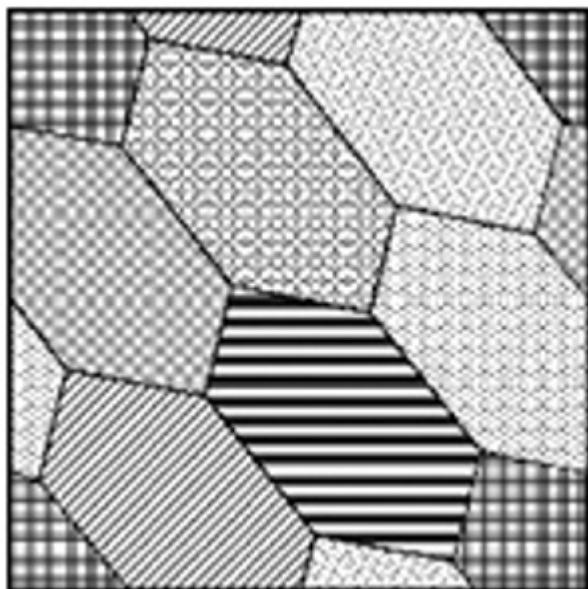


Figura 47. El mapa de un toro necesita siete colores.

Heawood probó que siete colores son necesarios y suficientes para colorear cualquier mapa en un toro. La imagen muestra que hacen falta siete, usando un cuadrado para representar el todo como se ha descrito. Observa que las regiones de aristas opuestas están emparejadas, como requiere esta representación.

Vimos que hay superficies como un toro pero con más agujeros. El número de agujeros se llama «género» y se representa con la letra g . Heawood hizo conjeturas de una fórmula para el número de colores necesario en un toro con g agujeros cuando $g \geq 1$: es el número entero menor o igual que

$$\frac{7 + \sqrt{48G + 1}}{2}$$

Cuando g va de 1 a 10, esta fórmula da los números

7 8 9 10 11 2 12 13 13 14

Heawood encontró su fórmula haciendo una generalización de su prueba para el teorema de los 5 colores en el plano. Pudo probar que, para cualquier superficie, el número de colores específico por su fórmula es siempre suficiente. Durante muchos años la gran pregunta fue si este número puede hacerse más pequeño. Ejemplos de los valores más pequeños del género sugieren que la estimación de Heawood es la mejor posible. En 1968, tras una larga investigación, Gerhard Ringel y John W. T. (Ted) Youngs completaron los detalles finales con una demostración que es correcta, basándose en su propio trabajo y en el de muchos otros. Sus métodos se sustentan en tipos especiales de redes y son lo suficientemente complicados para llenar un libro entero.

8. Cubo de Fibonacci

El primer cubo no trivial, también un número de Fibonacci. ¿Hay otros cubos de Fibonacci? Pensar sobre cubos llevó a Fermat a enunciar su famoso último teorema. Sophie Germain, una de las excelentes mujeres matemáticas, hizo una contribución importante a un caso especial. Andrew Wiles finalmente encontró una prueba completa 350 años más tarde de la conjetura original de Fermat.

§. Primer cubo (después de 1)

El cubo de un número se obtiene multiplicándolo por sí mismo y luego multiplicando el resultado por el número original. Por ejemplo, el cubo de 2 es $2 \times 2 \times 2 = 8$. El cubo de un número n se escribe como n^3 . Los primeros cubos son:

$n:$	0	1	2	3	4	5	6	7	8	9	10
$n^3:$	0	1	8	27	64	125	216	343	512	729	1.000

§. Último teorema de Fermat

Los cubos empezaron un hilo de pensamiento que duró más de 300 años. Alrededor de 1630, Fermat observó que sumando dos cubos distintos de cero el resultado parecía no ser un cubo. (Si se permite el cero, entonces $0^3 + n^3 = n^3$ para cualquier n .) Había empezado a leer una edición de

1621 de un famoso texto antiguo de álgebra, *Aritmética*, de Diofanto. En el margen de su copia del libro escribió «es imposible dividir un cubo en dos cubos, o una potencia de cuatro en dos potencias de cuatro o, en general, cualquier potencia mayor que dos en dos de esas potencias. He descubierto una demostración verdaderamente maravillosa de esto, pero este margen es demasiado pequeño para contenerla».

En lenguaje algebraico, Fermat estaba reclamando una demostración de que la ecuación:

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

no tiene soluciones enteras si n es cualquier entero mayor o igual que 3. Esta afirmación, ahora conocida como «último teorema de Fermat», vio la luz por primera vez en 1670, cuando el hijo de Fermat, Samuel, publicó una edición de la *Aritmética* que incluía las notas al margen de su padre.

Fermat probablemente comenzó a interesarse en esta pregunta porque conocía las ternas pitagóricas: dos cuadrados (de números enteros) que sumados dan un cuadrado. Un ejemplo común es $3^2 + 4^2 = 5^2$. Hay infinidad de estas ternas, y se conoce una fórmula general para ellas desde la Antigüedad [véase 5].

Si Fermat tenía una demostración, jamás nadie la ha encontrado. Sabemos que tenía una prueba válida para las cuartas potencias, basada en el hecho de que las cuartas potencias son un tipo especial de

cuadrados, en concreto, el cuadrado de un cuadrado, para relacionar esta versión del problema con las ternas pitagóricas. La misma idea muestra que, para probar el último teorema de Fermat, puede asumirse que la potencia n es o bien 4 o bien un número primo. A lo largo de los dos siglos siguientes, se probó el último teorema de Fermat para exactamente tres primos impares: 3, 5 y 7. Euler lidió con los cubos en 1770, Legendre y Peter Gustav Lejeune Dirichlet lo hicieron con potencias quintas alrededor de 1825; y Gabriel Lamé probó el teorema para las potencias séptimas en 1839.

QVÆSTIO VIII.

PROPOSITVM quadratum diuidere in duos quadratos. Imperatum sit ut diuidatur in duos quadratos. Ponatur primus i Q. Oportet igitur $16 - 1$ Q. æquales esse quadrato. Fingo quadratum à numeris quotquot libuerit, cum defectu tot vnitatum quod continet latus ipsius 16. esto à 2 N. — 4. ipse igitur quadratus erit $4 Q. + 16 - 16 N$. hæc æquabuntur vniitatibus $16 - 1$ Q. Communis adiiciatur vtrimeque defectus, & à similibus auferantur similia, sient 5 Q. æquales $16 N$. & fit 1 N. Erit igitur alter quadratorum $\frac{1}{2}$. alter verò $\frac{1}{2}$ & vtriusque summa est $\frac{1}{2}$ seu 16 . & vterque quadratus est.

TON δηταχθιστετράγωνοι μιλεῖται εἰς δύο τετραγώνους. ἐπιτετράχω δὴ η̄ ισ̄ διλέεται εἰς δύο τετραγώνους, καὶ τετράχω δὲ περίορος διωδίμως μαζ. δίλεται δέ τοι μικρός ισ̄ λείψει διωδίμως μαζ. Ιστοι δὲ τετραγώνοι πλάσαισθε τετράγωνοι λαὸς εἰς δύο δὴ πρώτοι λείψει ποιήσαντες δύον δέσποινται η̄ η̄ ισ̄ μηπλάσυσθαι. Εἰσι δὲ δέ λείψει η̄ οὐδὲν δέσποινται η̄ περίορος ισται διωδίμως δὲ μη̄ ισ̄ λείψει η̄ ισ̄. παῖς τοι μικρός ισ̄ λείψει διωδίμως μαζ. καὶ τοῦ περιστερίου η̄ λείψει, η̄ λαὸς δροὺς δρεισθαι. διωδίμως η̄ ισται ἀγριμοῦς ισ̄. καὶ γινεται δὲ αετοθύεις ισ̄. πάμεται. ισται δὲ μη̄ στοῦ εἰροσοπικῆλατον. οὐ δὲ μηδὲ εἰροσοπικῆλατον. Εἰ οὖ δύο σωποῦντες πάνται ν εἰροσοπικῆλατο, ισται μεράδεις ισ̄. καὶ ισται διάτρησης τετράγωνοι.

OBSERVATIO DOMINI PETRI DE FERMAT.

Cubum autem in duos cubes, aut quadratoquadratum in duos quadratoquadratos & generaliter nullam in infinitum ultra quadratum potestatem in duos eiusdem nominis fas est diuidere cuius rei demonstrationem mirabilem sanc detexti. Hanc marginis exiguitas non caperet.

Figura 48. Nota al margen de Fermat, publicada en la edición de su hijo de la Aritmética de Diofanto, encabezada con «Observación del maestro Pierre de Fermat

Sophie Germain hizo progresos significativos en lo que pasó a conocerse como el «primer caso» del último teorema de Fermat, en el cual n es primo y no se divide entre x , y o z . Como parte de un programa más ambicioso que nunca se completó, probó el teorema de Sophie Germain: si $xp + yp = zp$, donde p es un primo menor que 100, entonces xyz es divisible por p^2 . De hecho, probó bastante más que esto, pero la afirmación es más técnica. La prueba usa lo que ahora se llama «primos de Sophie Germain»: números primos p tales que $2p + 1$ son también primos. Los primeros primos de Sophie Germain son:

2 3 5 11 23 29 41 53 83 89 113 131 173 179 191

Y el mayor conocido es:

$$18.543.637.900.515 \times 2^{666.667} - 1$$

encontrado por Philipp Bledung en 2012. Hay conjeturas sobre que debería haber infinidad más, pero se trata de una cuestión abierta. Los primos de Sophie Germain tienen aplicaciones en criptografía y las pruebas de primalidad.

El último teorema de Fermat se probó que era cierto en 1995, más de tres siglos y medio después de ser enunciado, y lo hizo Andrew Wiles. Los métodos usados en la prueba están muy lejos de lo que había disponible en la época de Fermat o lo que él podía haber inventado.

Conjetura de Catalan

En 1844, el matemático belga Eugène Catalan hizo una pregunta fascinante sobre los números 8 y 9: «Le ruego, señor, que tenga el placer de anunciar en su periódico el siguiente teorema que creo cierto aunque todavía no haya tenido éxito en completar del todo la demostración, quizá otros sean más exitosos. Dos números naturales consecutivos, otros que no sean 8 y 9, no pueden ser potencias consecutivas, o dicho de otro modo, la ecuación $xm - yn = 1$ en la cual las incógnitas son enteros positivos (mayores que 1) solo admite una única solución».

Esta afirmación pasó a ser conocida como la conjetura de Catalan. Finalmente, Preda Mihăilescu la probó en 2002 usando métodos avanzados de la teoría algebraica de números.

§. Sexto número de Fibonacci y único cubo de Fibonacci no trivial

En 1202, Leonardo de Pisa escribió un texto de aritmética, *Liber Abbaci*(«Libro de cálculo») explicando los numerales hindú-arábigos 0-9 a la audiencia europea. Incluyó una cuestión curiosa sobre conejos. Empieza con un par de conejos jóvenes. Después de una estación, cada par joven se convierte en adulto, mientras que cada par adulto da lugar a un par joven. Los conejos son inmortales. ¿Cómo crece la población a medida que pasan las estaciones?

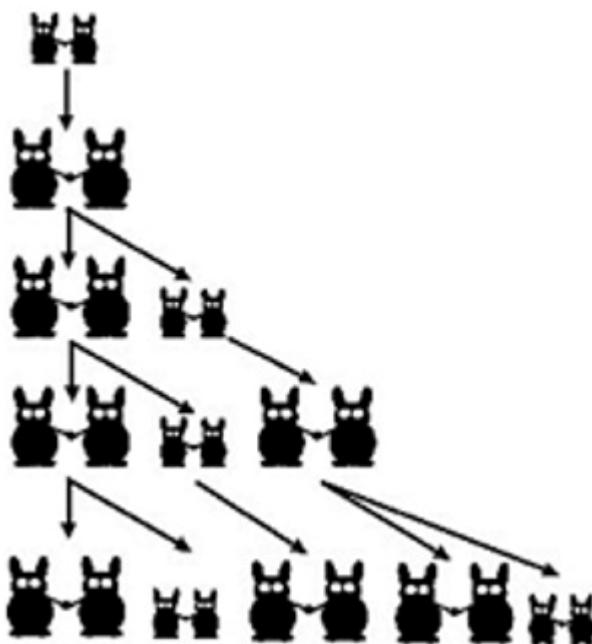


Figura 49. Las primeras generaciones en el modelo de conejos de Fibonacci.

Leonardo mostró que el número de pares sigue el patrón:

1 1 2 3 5 8 13 21 34 55 89 144

En ese patrón cada número después de los dos primeros es la suma de los dos que lo preceden. Así que, por ejemplo, $2 = 1 + 1$, $3 = 1 + 2$, $5 = 2 + 3$, $8 = 3 + 5$, $13 = 5 + 8$, etcétera. Leonardo más tarde adquirió el sobrenombre de «Fibonacci» (hijo de Bonaccio) y desde 1877, cuando Lucas escribió sobre esta secuencia, sus miembros han sido conocidos como los «números de Fibonacci». La secuencia suele darse con un 0

extra al principio, el número cero de Fibonacci. La regla de formación todavía funciona porque $0 + 1 = 1$.

Por supuesto, el modelo no es realista y no tenía intención de serlo. Era simplemente un problema numérico ingenioso en su libro de texto. Sin embargo, generalizaciones modernas, conocidas como «modelos de Leslie», son más realistas y tienen aplicaciones prácticas en poblaciones reales.

Propiedades de los números de Fibonacci

Los matemáticos han estado fascinados por los números de Fibonacci desde hace tiempo. Hay una conexión fundamental con el número de oro φ . Usando la propiedad básica de que $1/\varphi = \varphi - 1$, puede probarse que el n -ésimo número de Fibonacci F_n es *exactamente* igual a:

$$\frac{\varphi^n - (-\varphi)^{-n}}{\sqrt{5}}$$

Este es el número natural más próximo a $\varphi^n/\sqrt{5}$. De modo que los números de Fibonacci son aproximadamente proporcionales a φ^n , lo cual indica que crecen exponencialmente, como las potencias de un número fijo.

Hay muchos patrones en los números de Fibonacci. Por ejemplo, toma tres términos consecutivos, tales como 5, 8, 13. Luego calcula $5 \times 13 = 65$ y $8^2 = 64$, que difieren en 1. De modo más general,

$$F_{(n-1)} \times F_{(n+1)} = F_n^2 + (-1)^n$$

Las sumas de números consecutivos de Fibonacci satisfacen:

$$F_0 + F_1 + F_2 + \dots + F_n = F_{n+2} - 1$$

Por ejemplo:

$$0 + 1 + 1 + 2 + 3 + 5 + 8 = 20 = 21 - 1$$

No hay fórmula conocida para la suma de los inversos de los números de Fibonacci distintos de cero:

$$\frac{1}{1} + \frac{1}{1} + \frac{1}{2} + \frac{1}{3} + \frac{1}{5} + \frac{1}{8} + \frac{1}{13} + \dots$$

Numéricamente, esta «constante de Fibonacci inversa» es alrededor de 3,35988566243 y Richard André-Jeannin ha probado que es irracional, que no es una fracción exacta.

Muchos números de Fibonacci son primos. Los primeros de estos primos de Fibonacci son 2, 3, 5, 13, 89, 233, 1.597, 28.657 y 514.229. Los mayores primos de Fibonacci conocidos tienen miles de dígitos. No se sabe si hay infinitos primos de Fibonacci.

Una pregunta muy difícil, solucionada recientemente, es: ¿cuándo un número de Fibonacci es una potencia perfecta? En 1951, W. Ljunggren probó que el duodécimo número de Fibonacci $144 = 12^2$ es el único número de Fibonacci no trivial que es un cuadrado. Harvey Cohn dio otra prueba en 1964. (0 y 1 son potencias n -ésimas para todo n , pero no demasiado interesantes.) El sexto número de Fibonacci es $8 = 2^3$, y en 1969, H. London y R. Finkelstein probaron que es el único número de Fibonacci no trivial que es un cubo. En 2006, Y. Bugeaud, M. Mignotte y S. Siksek demostraron que los únicos números de Fibonacci que son potencias perfectas (mayores que la primera potencia) son 0, 1, 8 y 144.

9. Cuadrado mágico

El cuadrado mágico no trivial más pequeño tiene 9 celdas. Hay 9 recubrimientos del plano de polígonos regulares que están organizados del mismo modo en cada vértice. Un rectángulo de las dimensiones correctas puede dividirse en 9 cuadrados de diferentes tamaños.

§. El cuadrado mágico más pequeño

Los cuadrados mágicos son matrices cuadradas de números, normalmente los números 1, 2, 3,... hasta algún límite, en las que cada fila, cada columna y ambas diagonales suman la misma cantidad. No tienen un gran significado matemático, pero son divertidos. El cuadrado

mágico más pequeño (además del cuadrado trivial de 1×1 con solo el número 1 en él) es un cuadrado 3×3 , usando los dígitos 1 – 9.

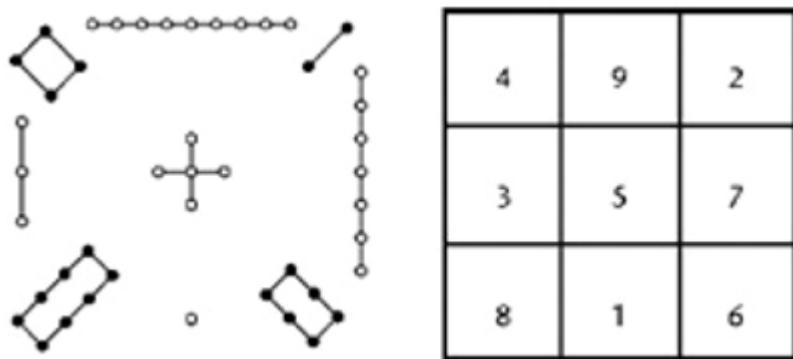


Figura 50. Izquierda: el Lo Shu. Derecha: versión moderna.

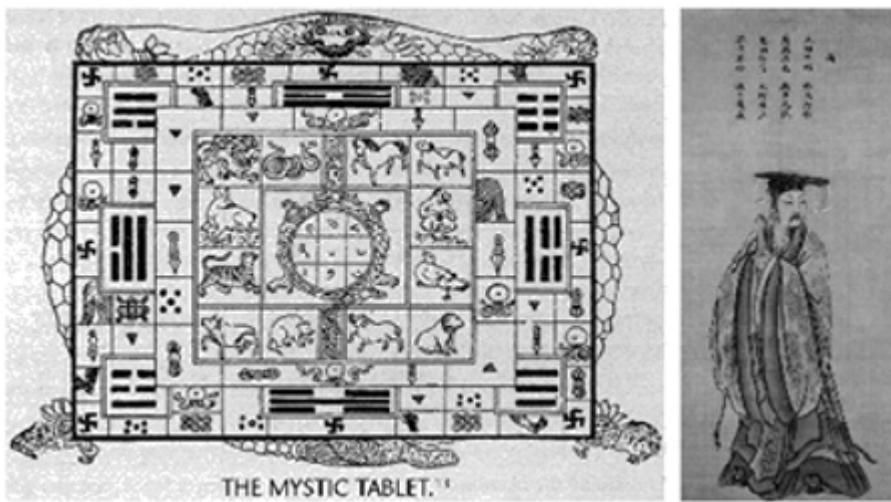


Figura 51. Izquierda: una imagen tibetana de Lo Shu. Derecha: emperador Yu.

El cuadrado mágico conocido más antiguo aparece en una vieja leyenda china sobre el emperador Yu ofreciendo sacrificios al dios del río Luo, debido a una gran inundación. Una tortuga mágica emerge del río,

portando un curioso diseño matemático en su caparazón. Era el Lo Shu, un cuadrado mágico dibujado en una rejilla de 3×3 que usaba puntos para los números.

Si el cuadrado mágico usa los nueve dígitos 1-9, una vez cada uno (es la suposición estándar que se usa a menos que haya buenas razones para considerar otra), el Lo Shu es la única solución mágica posible, excepto por rotaciones y reflexiones. Su *constante mágica* (la suma de los números en cualquier fila, columna o diagonal) es 15. El cuadrado muestra otros patrones también. Los números pares ocupan las cuatro esquinas. Los números diametralmente opuestos siempre suman 10.

El tamaño del cuadrado mágico es su orden. El Lo Shu tiene orden 3, y un cuadrado mágico de orden n tiene n^2 celdas, normalmente conteniendo los números del 1 al n^2 .

Otras culturas antiguas, como la persa y la hindú, también se interesaron en cuadrados mágicos. En el siglo X se grabó un cuadrado mágico de orden 4 en un templo en Khajurahu, en la India. Su constante mágica, como la de todos los cuadrados mágicos de orden 4 que usan los números del 1 al 16, es 34.

7	12	1	14
2	13	8	11
16	3	10	5
9	6	15	4

Figura 52. Cuadrado mágico de orden 4 del siglo X.

Hay muchos cuadrados mágicos diferentes de orden 4: 880 en total, sin contar las rotaciones o reflexiones como diferentes. El número de cuadrados mágicos de orden 5 es mucho mayor: 275.305.224. El número exacto de cuadrados mágicos de orden 6 no se conoce, pero está en torno a $1,7745 \times 10^{19}$.

El artista Durero representó un cuadrado mágico de orden 4 en su grabado *Melancolía I*, que también incluye otros objetos matemáticos. El cuadrado fue escogido de modo que la fecha, 1514, aparece en el medio de la fila inferior.

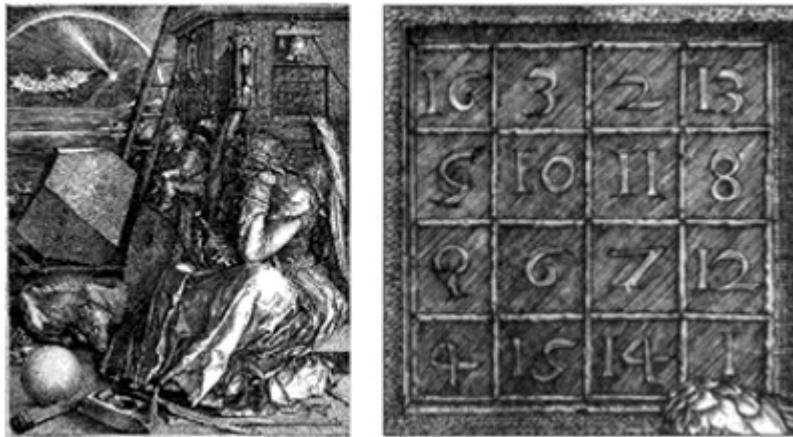


Figura 53. Izquierda: Melancolía I. Derecha: detalle del cuadrado mágico. Observa la fecha 1514, en la parte central inferior.

Los cuadrados mágicos existen para todos los órdenes mayores o iguales a 3, y de manera trivial para orden 1, pero no para orden 2. Hay métodos

generales para construir ejemplos, los cuales dependen de si n es impar, dos veces un número impar o un múltiplo de 4.

La constante mágica para un cuadrado mágico de orden n es $n(n^2 + 1)/2$

Para ver por qué, observa que el total de todas las celdas es $1 + 2 + 3 + \dots + n^2$, que es igual a $n(n^2 + 1)/2$. Como el cuadrado puede dividirse en n filas, cada una con la misma suma, la constante mágica se obtiene dividiendo esta suma entre n .

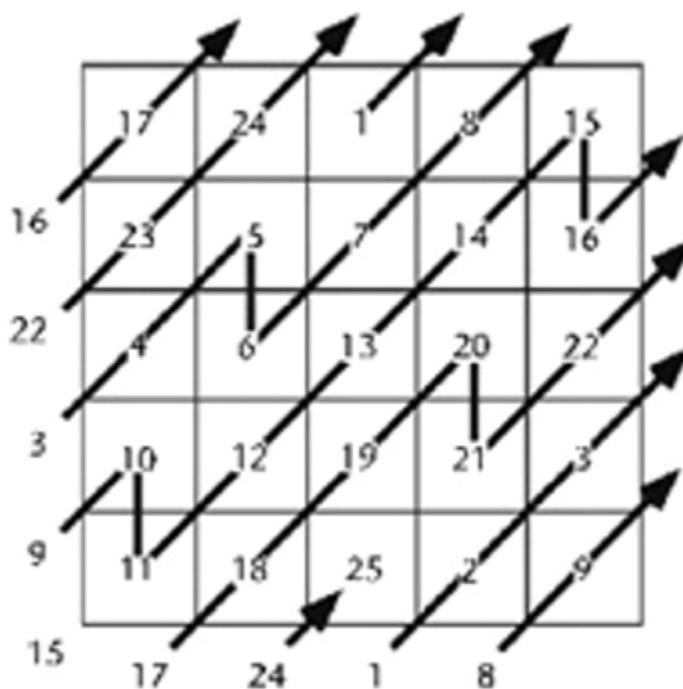


Figura 54. Método general para construir un ejemplo de un cuadrado mágico de tamaño impar. Coloca 1 en la parte superior en el centro, luego coloca sucesivamente los números 2, 3, 4,..., siguiendo las flechas en diagonal, «envolviendo» desde la parte superior a la inferior o de izquierda a derecha si es necesario. Cuando haya un número que tendría

que escribirse sobre uno existente, baja a la celda que está justo por debajo.

§.Tesselaciones arquimedianas

Nueve patrones de teselaciones (o embaldosados) usan más de un tipo de polígono regular, con exactamente la misma colocación de baldosas en cada esquina. Estas se conocen como arquimedianas, uniformes o teselaciones semirregulares.

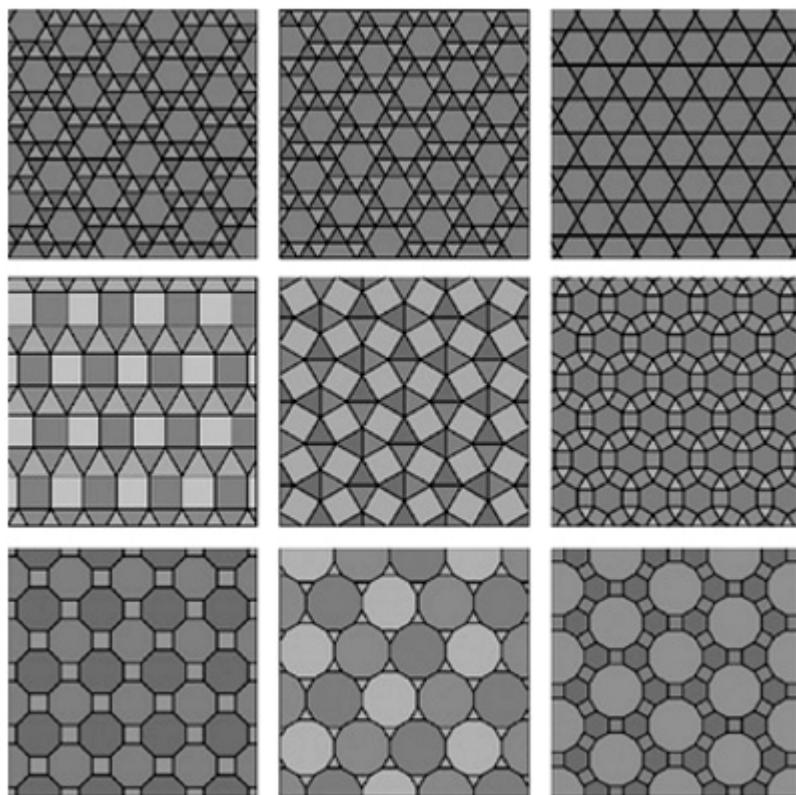


Figura 55. Las nueve teselaciones arquimedianas.

§. Cuadratura de un rectángulo

Un cuadrado puede dividirse fácilmente en nueve cuadrados más pequeños de igual tamaño dividiendo cada arista en tres. El número más pequeño de cuadrados *desiguales* en el cual un rectángulo con lados enteros puede dividirse es también nueve, pero la solución es mucho más difícil de encontrar.

Es sabido que un suelo rectangular puede recubrirse con baldosas cuadradas de igual tamaño, siempre y cuando sus aristas sean enteros múltiplos del tamaño de la baldosa. Pero ¿qué sucede si necesitamos usar baldosas cuadradas que son todas de *diferente* tamaño? La primera «cuadratura de un rectángulo» fue publicada en 1925 por Zbigniew Moron, usando diez baldosas cuadradas de tamaños: 3, 5, 6, 11, 17, 19, 22, 23, 24, 25. No mucho después, encontró una cuadratura de un rectángulo usando nueve baldosas cuadradas de tamaños: 1, 4, 7, 8, 9, 10, 14, 15, 18.

¿Qué ocurre en el caso de hacer un *cuadrado* a partir de baldosas cuadradas diferentes? Durante mucho tiempo, se pensó que esto era imposible, pero en 1939, Roland Sprague encontró 55 baldosas cuadradas distintas que encajaban unas con otras formando un cuadrado. En 1940, Leonard Brooks, Cedric Smith, Arthur Stone y William Tutte, por aquel entonces estudiantes del Trinity College, en Cambridge, publicaron un artículo relacionando el problema con redes eléctricas, la red cifra de qué tamaño son los cuadrados y cómo encajan unos con otros. Este método llevó a más soluciones.

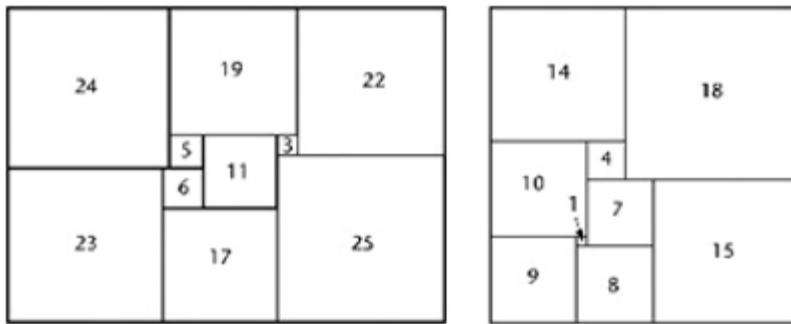


Figura 56. Izquierda: primera cuadratura del rectángulo de Moron.

Derecha: su mejora a nueve baldosas.

En 1948, Theophilus Willcocks encontró 24 cuadrados que encajaban unos con otros formando un cuadrado. Hasta hacía poco, se pensaba que no había un conjunto más pequeño que pudiese resolver el problema, pero en 1962, Adrianus Duijvestijn usó un ordenador para mostrar que solo se necesitaban 21 baldosas cuadradas, y que este es el número mínimo de ellas. Sus tamaños son: 2, 4, 6, 7, 8, 9, 11, 15, 16, 17, 18, 19, 24, 25, 27, 29, 33, 35, 37, 42 y 50.

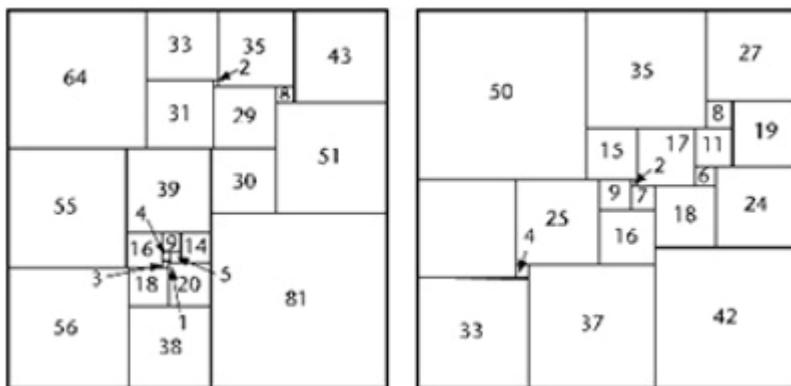


Figura 57. Izquierda: cuadratura del cuadrado de Willcocks con 24 baldosas. Derecha: cuadrado de 21 baldosas de Duijvestijn.

En 1975, Solomon Golomb preguntó: ¿puedes teselar el plano infinito sin dejar huecos usando exactamente una baldosa del tamaño de cada número entero: 1, 2, 3, 4, etcétera? Hasta hacía poco el problema estaba sin resolver, pero en 2008, James y Frederick Henle encontraron una demostración ingeniosa de que la respuesta es «sí».

10. Sistema decimal

El sistema decimal, que usamos para escribir números, está basado en 10, probablemente porque tenemos diez dedos. Son posibles otras bases, y algunas han sido usadas por culturas antiguas, destacando 20 y 60. Diez es tanto triangular como tetraédrico. Contrariamente a lo que Euler pensaba, existen dos cuadrados latinos ortogonales de 10×10 .

§. Contando de diez en diez

La notación actual para los números se llama «decimal» y usa el 10 como base numérica. *Decem* es la palabra latina para «diez». En este sistema, los mismos diez símbolos

0 1 2 3 4 5 6 7 8 9

se usan para denotar unidades, decenas, centenas, millares, etcétera. Se sabe cuál de ellas denota por la posición del símbolo en el número. Por ejemplo, en el número 2.015, los símbolos significan:

5 unidades

1 decenas

0 centenas

2 millares

El papel central aquí lo juegan las sucesivas potencias de 10:

$$10^0 = 1$$

$$10^1 = 10$$

$$10^2 = 100$$

$$10^3 = 1.000$$

Nos hemos acostumbrado tanto a esta notación que tendemos a pensar en ella como «números» simplemente y a asumir que hay algo especialmente matemático relacionado con el número 10. Sin embargo, métodos de notación muy similares pueden usar cualquier número como base. De modo que aunque el 10 sí que es especial, como veremos más adelante, no lo es en este aspecto.

Los ordenadores usan varias bases:

base 2 binaria [véase 2], símbolos: 0 1

base 8 octal, símbolos: 0 1 2 3 4 5 6 7

base 16 hexadecimal, símbolos: 0 1 2 3 4 5 6 7 8 9 A B C D E F

La duodecimal, base 12, con frecuencia ha sido propuesta como una mejora de la decimal, porque 12 es divisible por 2, 3, 4 y 6, mientras que 10 es divisible solo por 2 y 5. Los mayas usaban base 20 y en la antigua Babilonia usaban base 60 [véase 0 para ambas].

Podemos descomponer 2.015 en decimal como sigue:

$$2 \times 1.000 + 0 \times 100 + 1 \times 10 + 5 \times 1$$

o escribiendo las potencias de modo explícito:

$$2 \times 10^3 + 0 \times 10^2 + 1 \times 10^1 + 5 \times 10^0$$

Este sistema se llama «notación posicional», porque el significado del símbolo depende de su posición.

Los mismos símbolos en base 8 significarían:

$$2 \times 8^3 + 0 \times 8^2 + 1 \times 8^1 + 5 \times 8^0$$

En una notación decimal más familiar, esto es:

$$2 \times 512 + 0 \times 64 + 1 \times 8 + 5 \times 1 = 1.037$$

De modo que los mismos símbolos, interpretados usando diferentes bases, representan diferentes números.

Veámoslo con otra base menos común: 7. En Apellobetnees III, los habitantes alienígenas tienen todos siete colas y cuentan usándolas. Así, su sistema numérico tiene solo los dígitos del 0 al 6. Por lo que escribimos 10 cuando queremos decir 7, y así se continúa hasta 66, el cual escribiríamos como 48. Entonces para nuestro 49, usan 100, etcétera.

Esto es, un número como $abcd$ en apellobetneesiano se traduce al sistema decimal como:

$$a \times 7^3 + b \times 7^2 + c \times 7 + d = 343a + 49b + 7c + d$$

Con un poco de práctica, puedes hacer operaciones alienígenas usando este sistema, sin traducirlo al sistema decimal y volver a él de nuevo. Necesitas reglas como « $4 + 5 = 2$ llevando 1» (porque 9 decimal es 12 en base 7), pero aparte de esto todo resulta bastante familiar.

§. Historia de la notación numérica

Las primeras civilizaciones empleaban notaciones numéricas muy diferentes a la nuestra. Los babilonios usaban la notación de base 60, con símbolos cuneiformes para los sesenta dígitos [véase 0]. Los egipcios

tenían símbolos especiales para las potencias de 10 y los repetían para obtener otros números. En la Grecia antigua usaban su alfabeto para los números 1–9, 10–90, 100–900.

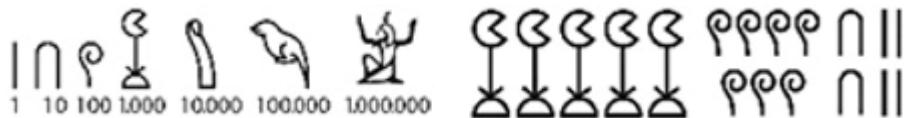


Figura 58. Izquierda: símbolos numéricos egipcios. Derecha: el número 5.724 en jeroglíficos egipcios.

La notación posicional actual y nuestros símbolos para los diez dígitos, 0–9, aparecieron en la India alrededor de 500 d. C., pero había predecesores. La historia es complicada, y las fechas, difíciles de determinar y controvertidas.

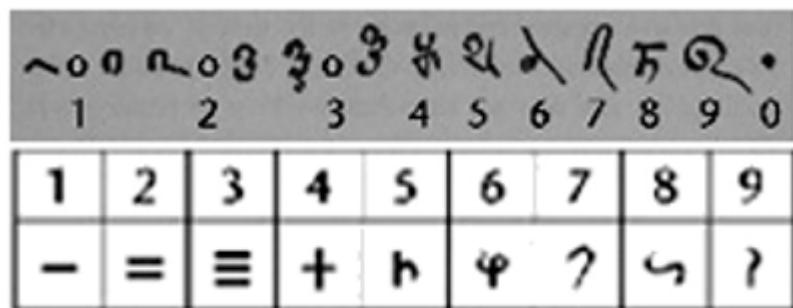


Figura 59. Arriba: símbolos del manuscrito de Bakhshali. Abajo: numeración brahmi.

El manuscrito de Bakhshali, encontrado en 1881, cerca de Bakhshali en Pakistán, escrito sobre madera de abedul, es el documento conocido más

antiguo de las matemáticas hindúes. Los académicos creen que está datado entre el siglo II a. C. y el siglo III d. C.; se cree que es una copia de una manuscrito anterior. Usa símbolos distintos para los dígitos 0 – 9. La numeración brahmi se remonta a 200-300 d. C., pero no usa notación posicional. En su lugar, había símbolos extra para los múltiplos de 10 y para 100 y 1.000, con reglas para combinar estos símbolos y obtener números como 3.000.

Más tarde, la numeración «hindú» se derivó de la brahmi. Esta fue usada por el matemático hindú Aryabhata en el siglo VI, en varias formas diferentes. Brahmagupta usó el 0 como un número por derecho propio en el siglo VII, y encontró reglas para realizar aritmética con cero.

Europea	0	1	2	3	4	5	6	7	8	9
Indoarábiga	٠	١	٢	٣	٤	٥	٦	٧	٨	٩
Indoarábiga oriental (persa y urdu)	۰	۱	۲	۳	۴	۵	۶	۷	۸	۹
Devanagari (Hindi)	०	१	२	३	४	५	६	७	८	९
Tamil	க	ஒ	ஒ	ஒ	ஒ	ஒ	ஒ	ஒ	ஒ	ஒ

Figura 60. Ejemplos de numeración arábiga e hindú.

La invención hindú se extendió a Oriente Medio, en concreto a través del matemático persa Al-Khwarizmi (*Sobre cálculo con numeración hindú*, 825) y el matemático árabe Al-Kindi (*Sobre el uso de los números de la India*, c. 830). Más tarde se extendió a Europa a través de las traducciones al latín del libro de Al-Khwarizmi.

El primer libro escrito expresamente para promocionar este sistema de notación en Europa fue *Liber Abbaci* de Fibonacci, en 1202. Llamó a la notación *modus Indorum* («método de los indios»), pero la asociación con Al-Khwarizmi era tan fuerte que la expresión «numeración árabe» fue la que se instauró, a pesar del título del libro de AlKhwarizmi. El nombre se vio reforzado porque muchos europeos tuvieron contacto con ellos a través de gente bereber árabe.

Los símbolos tardaron un tiempo en asentarse. En la Europa medieval, se empleaban docenas de variantes. Incluso hoy en día, diferentes culturas usan versiones diferentes de los símbolos.

Occidente	0	1	2	3	4	5	6	7	8	9
Arábiga oriental	٠	١	٢	٣	٤	٥	٦	٧	٨	٩
Persa	۰	۱	۲	۳	۴	۵	۶	۷	۸	۹
Chino simplificado*	〇	一	二	三	四	五	六	七	八	九
Chino complejo	零	壹	貳	叁	肆	伍	陆	柒	捌	玖
Mongol	0	0	2	3	0	4	5	0	6	0
Tibetano	୦	୧	୨	୩	୪	୫	୬	୭	୮	୯

*En Japón y en Corea se usan los caracteres chinos simplificados.

Figura 61. Algunos símbolos modernos para los números.

§. El separador decimal

El *Liber Abbaci* de Fibonacci contenía una notación que todavía usamos hoy en día: la barra horizontal en una fracción, como por ejemplo $\frac{3}{4}$ para

«tres cuartos». Los hindúes empleaban una notación similar, pero sin la barra, que al parecer introdujeron los árabes. Fibonacci la usó de manera generalizada, pero la misma barra podía formar parte de varias fracciones diferentes.

En la actualidad raramente usamos fracciones con un propósito práctico. En su lugar, usamos la coma decimal, así escribimos π como 3,14159, por ejemplo. Los decimales en este sentido datan de 1585, cuando Simon Stevin se convirtió en el tutor privado de Mauricio de Nassau, hijo de Guillermo «el Taciturno». Stevin se acabaría convirtiendo en ministro de Finanzas. Buscando métodos de contabilidad rigurosos, tuvo en cuenta la notación indoarábica, pero las fracciones le parecieron demasiado engorrosas.

Los babilonios, sin duda prácticos, representaban las fracciones en su sistema de base 60 permitiendo que dígitos apropiados representasen potencias de $1/60$, lo cual da lugar a nuestros modernos minutos y segundos, tanto para el tiempo como para los ángulos. En una forma modernizada de la notación babilónica, $6; 15$ significa $6 + 15 \times (1/60)$, lo cual escribiríamos como $6\frac{1}{4}$ o 6,25. A Stevin le gustó esta idea, excepto por su uso de la base 60, y buscó un sistema que combinase lo mejor de ambos: los decimales.

Su notación no incluía la coma decimal como tal, pero llevó rápidamente a la notación decimal actual. Donde nosotros escribiríamos 5,7731, por ejemplo, Stevin escribía 5@7①7②3③1④. Aquí el símbolo @ indica un

número entero, ① indica las décimas, ② las centésimas, etcétera. Los usuarios pronto prescindieron de ① y ②, y mantuvieron solo ③, que se redujo y simplificó hasta convertirse en los separadores decimales actuales; la coma decimal o el punto decimal.

Cuando publicó su nuevo sistema, enfatizaba en su funcionalidad y su uso en los negocios: «Todos los cálculos que se encuentran en los negocios podrían realizarse usando solo enteros sin la ayuda de las fracciones».

Números reales

Surge un problema si usas los decimales para las fracciones; a veces no son exactos. Por ejemplo, $1/3$ es muy próximo a 0,333, y todavía más próximo a 0,333333, pero ninguno es exacto. Para ver eso, multiplica por 3; deberías obtener 1, pero lo que realmente obtienes es 0,999 y 0,999999. Casi, pero no. Los matemáticos se dieron cuenta de que la expresión decimal «correcta» de $1/3$ debe ser infinitamente larga:

$$1/3 = 0,3333333333333333\dots$$

Sin acabar *nunca*... Y eso condujo a la idea de que un número como π tampoco se acabaría jamás, aunque no se repetían los mismos dígitos indefinidamente:

$$\pi = 3,141592653589793238...$$

Es importante darse cuenta de que $1/3$ es igual a $0,333\ 333\dots$ siempre y cuando los números no se acaben. Aquí hay una prueba. Sea

$$x = 0,333333\dots$$

Multiplica por 10. Con esto se pasa de x a $10x$ y se mueve la coma de $0,333333\dots$ un espacio a la derecha, de modo que:

$$10x = 3,333333\dots$$

Por lo tanto:

$$10x = 3 + x$$

$$9x = 3$$

$$x = 3/9 = 1/3$$

La afirmación de que $10x = 3 + x$ se basa en que los números no se acaban nunca. Si se detuviesen, incluso aunque considerásemos un trillón de repeticiones, la afirmación sería falsa.

Un razonamiento similar implica que $0,999999\dots$ sin acabarse nunca es exactamente igual a 1. Puedes o bien aplicar el mismo truco, que lleva a

$10x = 9 + x$, de modo que $x = 1$, o puedes simplemente multiplicar $1/3 = 0,333333\dots$ por 3.

Mucha gente está convencida de que $0,999999\dots$ sin acabarse nunca no es igual a 1. Creen que debe ser más pequeño. Eso es correcto si te detienes en algún punto, pero la cantidad por la que difiere de 1 se hace más pequeña también:

$$1 - 0,9 = 0,1$$

$$1 - 0,99 = 0,01$$

$$1 - 0,999 = 0,001$$

$$1 - 0,9999 = 0,0001$$

$$1 - 0,99999 = 0,00001$$

$$1 - 0,999999 = 0,000001$$

y así sucesivamente. Al hacer el límite esta diferencia tiende a cero. Se hace más pequeña que cualquier número positivo, por pequeño que este sea.

Los matemáticos definen el valor de un decimal infinito como el límite de los decimales finitos que tienes si te paras en algún punto, a medida que el número de cifras decimales incrementa indefinidamente. Para una secuencia infinita de nueves, el límite es exactamente 1. Nada menos que 1 valdría, porque un número de nueves suficientemente grande dará algo

mayor. No existe algo como «infinitos ceros seguidos por un 1», e incluso, aunque lo hubiera, no obtendrías 1 sumándolo a 0,999999...

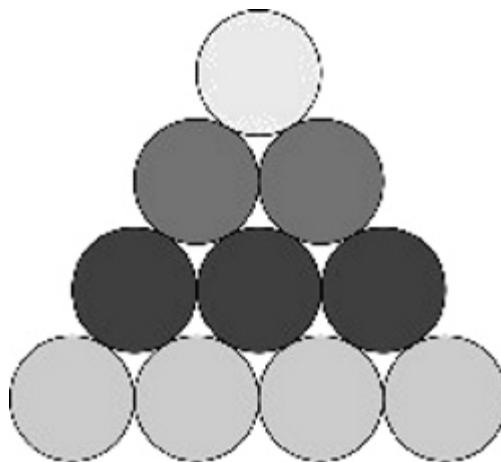


Figura 62. El cuarto número triangular.

Esta definición convierte a los decimales infinitos en un concepto matemático lógico. Los números resultantes se llaman «números reales», no porque se den en el mundo real, sino para distinguirlos de los problemáticos números «imaginarios» como i [véase i]. El precio que pagamos por usar el límite es que algunos números pueden tener dos expresiones decimales distintas, como 0,999999... y 1,000000..., algo a lo que enseguida te acostumbras.

§. El cuarto número triangular

El cuarto número triangular es:

$$1 + 2 + 3 + 4 = 10$$

El antiguo culto de los pitagóricos llamó a esta disposición *tetrakty*s y la consideraba sagrada. Los pitagóricos creían que el universo estaba basado en números y asignaban interpretaciones especiales a los primeros diez números. Hay mucho debate en torno a estas asignaciones. Ejemplos de varias fuentes incluyen:

- 1 Unidad, razón
- 2 Opinión, mujer
- 3 Armonía, hombre
- 4 Cosmos, justicia

Al ser la suma de los cuatro números principales, el 10 era especialmente importante. Simbolizaba los cuatro «elementos»: tierra, aire, fuego y agua; y los cuatro componentes del espacio: punto, línea, plano y sólido. Los diez bolos en una bolera están colocados de esta manera.



Figura 63. Los diez bolos.

§. Tercer número tetraédrico

Al igual que los números triangulares 1, 3, 6, 10, etcétera, son sumas de números enteros consecutivos, los números tetraédricos son sumas de números triangulares consecutivos.

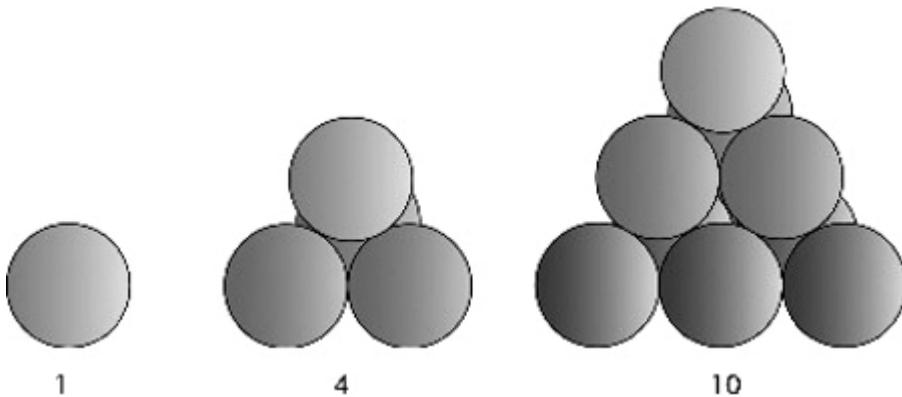
$$1 = 1$$

$$4 = 1 + 3$$

$$10 = 1 + 3 + 6$$

$$20 = 1 + 3 + 6 + 10$$

El n -ésimo número tetraédrico es igual a $n(n+1)(n+2)/6$

*Figura 64. Números tetraédricos.*

Geométricamente, un número tetraédrico de esferas puede apilarse como un tetraedro, una pila de triángulos decrecientes.

El número más pequeño, aparte de 1, que es tanto triangular como tetraédrico es el 10. Los únicos números que son tetraédricos y triangulares son: 1, 10, 120, 1.540 y 7.140.

§. Cuadrados latinos ortogonales de orden 10

En 1873, Euler estaba pensando en un juego matemático, los cuadrados mágicos, en el cual los números están ordenados en una rejilla cuadrada en la que todas las filas y columnas suman lo mismo [véase 9]. Pero la mente fértil de Euler apuntaba en una nueva dirección y publicó sus ideas en un artículo: «Un nuevo tipo de cuadrado mágico». Este es un ejemplo:

1 2 3

2 3 1

3 1 2

Las filas y las columnas suman todas lo mismo, en concreto, 6, de modo que excepto por una diagonal este es un cuadrado mágico, salvo que vulnera la condición estándar de usar números consecutivos, una vez cada uno. En su lugar, cada columna y cada fila están formadas por 1, 2 y 3 en algún orden. Esos cuadrados se conocen como «cuadrados latinos» porque los símbolos no necesitan ser un número, en concreto pueden ser las letras latinas A, B, C.

Esta es la descripción que hace Euler del rompecabezas: «Un problema muy curioso, el cual ha ejercitado durante algún tiempo el ingenio de mucha gente, me ha tenido involucrado en los siguientes estudios, que parecen abrir un nuevo campo de análisis, en concreto el estudio de las combinaciones. La pregunta gira en torno a la colocación de 36 oficiales, que deben ser colocados a partir de 6 rangos diferentes y también 6 regimientos diferentes, de modo que estén situados en un cuadrado en el que en cada línea (tanto horizontal como vertical) haya 6 oficiales de diferente rango y diferente regimiento».

Si usamos A, B, C, D, E y F para los rangos y 1, 2, 3, 4, 5 y 6 para los regimientos, el acertijo busca dos cuadrados latinos de 6×6 , uno para cada conjunto de símbolos. Además, tienen que ser *ortogonales*, lo que significa que ninguna combinación de los dos símbolos se da dos veces cuando los cuadrados se superponen. Es fácil encontrar colocaciones por separado para rangos y regimientos, pero encajar ambas, de modo que ninguna combinación de rango y regimiento se repita, es mucho más difícil. Por ejemplo, podemos intentarlo con:

A B C D E F

B C D E F A

C D E F A B

D E F A B C

E F A B C D

F A B C D E

y

1 2 3 4 5 6

2 1 4 3 6 5

4 3 5 6 1 2

6 4 1 5 2 3

5 6 2 1 3 4

3 5 6 2 4 1

Pero cuando las combinamos obtenemos:

A1 B2 C3 D4 E5 F6

B2 C1 D4 E3 F6 A5

C4 D3 E5 F6 A1 B2

D6 E4 F1 A5 B2 C3

E5 F6 A2 B1 C3 D4

F3 A5 B6 C2 D4 E1

y hay repeticiones. Por ejemplo, A1 aparece dos veces y B2 aparece cuatro veces, lo cual no es bueno.

Si intentamos el mismo problema para 16 oficiales de cuatro rangos (A, B, C, D) y cuatro regimientos (1, 2, 3, 4), no es difícil encontrar una solución:

A B C D

B A D C

C D A B

D C B A

1 2 3 4

3 4 1 2

4 3 2 1

2 1 4 3

Los cuadrados son ortogonales. Y de modo extraordinario, hay un tercer cuadrado latino ortogonal a ambos:

p q r s

s r q p

q p s r

r s p q

En la jerga, hemos descubierto un conjunto de *tres* cuadrados latinos de orden 4 mutuamente ortogonales.

Euler lo intentó lo mejor que pudo para encontrar un par adecuado de cuadrados latinos de orden 6 ortogonales, y fracasó. Lo que le convenció de que su acertijo de los 36 oficiales no tenía respuesta. Sin embargo, pudo construir pares de cuadrados latinos $n \times n$ ortogonales para todo n impar y todos los múltiplos de 4, y es fácil probar que no existen dichos cuadrados para orden 2. Quedan los tamaños 6, 10, 14, 18, etcétera (los dobles de los números impares) y Euler hizo la conjectura de que para esos tamaños no existían pares ortogonales.

Hay 812 millones de cuadrados latinos 6×6 diferentes e, incluso tomando atajos, no puedes hacer una lista de todas las posibles combinaciones. Aun así, en 1901, Gaston Tarry probó que Euler tenía razón para los cuadrados 6×6 . Pero resulta que estaba equivocado para los otros. En 1959, Ernest Tilden Parker construyó dos cuadrados latinos de 10×10 ortogonales. En 1960, Parker, Raj Chandra Bose y Sharadachandra Shankar Shrikhande habían probado que la conjectura de Euler es falsa para todos los tamaños excepto 6×6 .

46	57	68	70	81	02	13	24	35	99
71	94	37	65	12	40	29	06	88	53
93	26	54	01	38	19	85	77	60	42
15	43	80	27	09	74	66	58	92	31
32	78	16	89	63	55	47	91	04	20
67	05	79	52	44	36	90	83	21	18
84	69	41	33	25	98	72	10	56	07
59	30	22	14	97	61	08	45	73	86
28	11	03	96	50	87	34	62	49	75
00	82	95	48	76	23	51	39	17	64

Figura 65. Los dos cuadrados latinos 10×10 ortogonales de Parker.

Uno se muestra con el primer dígito y el otro con el segundo.

Cero y números negativos

Contenido:

§. 0 ¿Puede ser nada un número?

§. Bases de la notación numérica

§. -1 menos que nada

Tras exponer del 1 al 10, damos un paso atrás para presentar el 0.

Luego, otro paso atrás para llegar a -1 .

Esto descubre todo un nuevo mundo, el de los números negativos. También nos muestra nuevos usos de los números, que ya no son solo para contar.

§. 0 ¿Puede ser nada un número?

El cero surgió primero en sistemas para escribir los números. Era un recurso de notación. Solo más tarde fue reconocido como un número por derecho propio y se le permitió ocupar su lugar como una característica fundamental de los sistemas numéricos matemáticos. Sin embargo, tiene muchas características inusuales y, a veces, paradójicas. En particular, no resulta razonable dividir entre cero. En los cimientos de las matemáticas, todos los números pueden derivarse a partir de 0.

§. Bases de la notación numérica

En muchas culturas antiguas, los símbolos para 1, 10 y 100 no estaban relacionados. En la Grecia antigua, por ejemplo, usaban letras de su alfabeto para denotar los números 1-9, 10-90 y 100-900. Esto resulta potencialmente confuso, aunque normalmente es fácil decidir si el símbolo hace referencia a una letra o a un número a partir del contexto. Pero también complica la aritmética.

El modo en que escribimos números, con el mismo dígito representando números diferentes dependiendo de dónde está, se llama «notación posicional» [véase 10]. Este sistema tiene ventajas importantes para la aritmética de papel y lápiz, que hasta hace poco era como se hacían la mayoría de las operaciones del mundo. Con la notación posicional, lo principal que necesitas saber son reglas básicas para sumar y multiplicar los diez símbolos 0 – 9. Hay patrones comunes cuando los mismos símbolos aparecen en lugares diferentes. Por ejemplo:

$$23 + 5 = 28$$

$$230 + 50 = 280$$

$$2.300 + 500 = 2.800$$

1	α	alpha	10	ι	iota	100	ρ	rho
2	β	beta	20	κ	kappa	200	σ	sigma
3	γ	gamma	30	λ	lambda	300	τ	tau
4	δ	delta	40	μ	mu	400	ν	upsilon
5	ϵ	epsilon	50	ν	nu	500	ϕ	phi
6	ζ	vau*	60	ξ	xi	600	χ	chi
7	ζ	zeta	70	\o	omicron	700	ψ	psi
8	η	eta	80	π	pi	800	ω	omega
9	θ	theta	90	ς	koppa*	900	\beth	sampi*

* vau, koppa y sampi son caracteres obsoletos

Figura 66

No obstante, usando la antigua notación griega, las dos primeras tienen el siguiente aspecto

$$\kappa\gamma + \epsilon = \kappa\eta$$

$$\sigma\lambda + \nu = \sigma\pi$$

sin una estructura común obvia.

Sin embargo, hay una característica extra de la notación posicional, la cual aparece en 2.015: la necesidad de un símbolo cero. En este caso nos indica que no hay centenas involucradas. La notación griega no necesita hacer eso. En $\sigma\pi$, por ejemplo, σ significa 200 y π significa 80. Podemos decir que no hay unidades porque no aparece ninguno de los símbolos de las unidades: $\alpha - \theta$. En lugar de usar el símbolo cero, simplemente evitamos escribir cualquiera de los símbolos de las unidades.

Si intentamos hacer esto en el sistema decimal, 2.015 se convierte en 215, pero no podemos decir si significa 215, 2.150, 2.105, 2.015 o, es más, 2.000.150. Versiones iniciales de la notación posicional usaban un espacio 2 15, pero no es fácil darse cuenta de que hay un espacio, y dos espacios juntos son un espacio ligeramente más largo. De modo que es confuso y resulta fácil cometer un error.

Breve historia del cero

Babilonia

La primera cultura que introdujo un símbolo con el significado de «ningún número aquí» fue la babilónica. Recuerda [véase 10] que la notación numérica babilónica no usaba base 10, sino base 60. La primera aritmética de Babilonia indicaba la ausencia de un término 60^2 con un espacio, pero alrededor de 300 a. C. ya habían inventado un símbolo especial . Sin embargo, parece que en Babilonia no habían pensado en este símbolo como un número por derecho propio. Además, lo omitían si estaba al final del número, de modo que el significado tenía que sacarse a partir del contexto.

India

La idea de la notación posicional de base 10 aparece en *Lokavibhâga*, un texto sobre cosmología del jainismo que data de 458 d. C., el cual

también usa *shunya* (que significa «vacío»), donde nosotros usaríamos 0. En 498 d. C., el famoso matemático y astrónomo hindú Aryabhata describió la notación posicional como «posición a posición incrementa 10 veces su valor». El primer uso no controvertido de un símbolo específico para el dígito decimal 0 aparece en el año 876 d. C. en una inscripción en el templo Chaturbhuj, Gwalior, y adivina qué: es un círculo pequeño.

Los mayas

La civilización maya de América Central, la cual alcanzó su esplendor entre los años 250 y 900 d. C., empleó una notación de base 20 y tenía un símbolo explícito para cero.

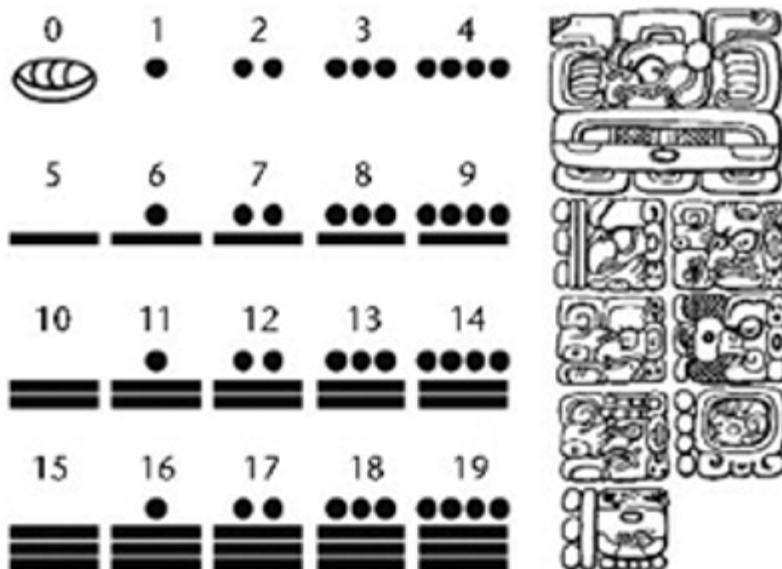


Figura 67. Izquierda: números mayas. Derecha: una estela en Quirigua en la que aparece la fecha de la creación maya: 13 baktun, 0 katun, 0

tun, 0 uinal, 0 kin, 4 Ahau 8 Cumku. Esto equivale a nuestro 11 de agosto de 3114 a.C.

Este método se remonta a mucho antes y se cree que fue inventado por los olmecas (1500-400 a. C.). Los mayas hicieron un uso considerable de los números en su sistema de calendario, un aspecto del cual se conoce como «la Cuenta Larga». Este asigna una fecha a cada día contando cuántos días han pasado desde una fecha de creación mítica, que sería el 11 de agosto de 3114 a. C. en el actual calendario occidental. En este sistema un símbolo para cero es esencial para evitar la ambigüedad.

¿Es el cero un número?

Antes del siglo IX d. C., el cero era visto como un *símbolo* práctico para los cálculos numéricos, pero no se le consideraba un *número* como tal. Probablemente, porque no contaba nada.

Si alguien te pregunta cuántas vacas tienes y las tienes, las señala de una en una y cuentas «una, dos, tres...». Pero si no tienes vacas, no señalias una y dices «cero», pues no hay ninguna vaca que señalar. Como no puedes obtener 0 contando, no resulta evidente que sea un número.

Si esta actitud parece extraña, merece la pena observar que, hace más tiempo todavía, no se pensaba en «uno» como un número. Si tienes vacas, seguramente tengas más de una. Una distinción parecida puede todavía encontrarse en el lenguaje moderno: la diferencia entre singular y

plural. En la Grecia antigua también tenían una forma «dual», con modificaciones específicas de palabras usadas cuando hablaban de dos objetos. De modo que en ese sentido «dos» no se consideraba un número como el resto. Otras cuantas lenguas clásicas hacían lo mismo, y algunas de las modernas, como el escocés, el galés y el esloveno todavía lo hacen. Quedan algunos rastros en el español como «ambos» para dos cosas, pero «todo» para más.

A medida que se extendió el uso del cero como un símbolo y los números se empleaban para otros propósitos distintos que contar, se hizo evidente que en la mayoría de los aspectos el cero se comporta como cualquier otro número. En el siglo IX, los matemáticos hindúes consideraban cero un número como cualquier otro, no solo un símbolo usado como separación de otros símbolos para que quedase más claro. Usaban el cero sin reservas en sus operaciones diarias.

En la imagen de la recta numérica, en la que los números 1, 2, 3,... están escritos en orden de izquierda a derecha, está claro dónde debe ir 0: inmediatamente a la izquierda de 1. La razón es sencilla: sumando 1 a cualquier número se mueve un paso hacia la derecha. Sumando 1 a 0 se mueve a 1, de modo que 0 tiene que ir en el lugar en el que un paso a la derecha dé como resultado 1. Y esto es un paso a la izquierda de 1.

La aceptación de números negativos determinó el lugar del cero como un número verdadero. Todo el mundo estaba contento con 3 siendo un número. Si aceptas que -3 también es un número y que siempre que

sumas dos números obtienes un número, entonces $3 + (-3)$ tiene que ser un número. Y este número es 0.

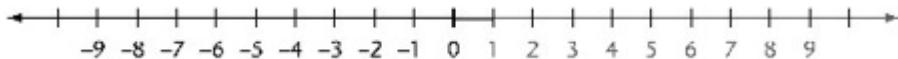


Figura 68. La recta numérica.

Características inusuales

Dije «en la mayoría de los aspectos, el cero se comporta como cualquier otro número» porque en circunstancias excepcionales no lo hace. Cero es especial. Tiene que serlo, porque es el único número que está claramente atrapado entre los números positivos y los negativos.

Está claro que sumando 0 a cualquier número no cambia. Si tenemos tres vacas y sumamos ninguna vaca, seguimos teniendo tres vacas. Ciertamente, hay cálculos extraños como este:

Un gato tiene una cola.

Ningún gato tiene ocho colas.

Por lo tanto, sumando:

Un gato tiene nueve colas.

Pero este pequeño lío es un juego de palabras que usa dos significados para «ningún».

Esta propiedad especial del 0 implica que $0 + 0 = 0$, lo cual nos dice que $-0 = 0$. Cero es su propio negativo. Es el único número así. Esto sucede precisamente porque 0 está atrapado en la recta numérica entre los números positivos y los negativos.

¿Qué ocurre con la multiplicación? Si tratamos la multiplicación como una suma que se repite, entonces:

$$2 \times 0 = 0 + 0 = 0$$

$$3 \times 0 = 0 + 0 + 0 = 0$$

$$4 \times 0 = 0 + 0 + 0 + 0 = 0$$

De modo que

$$n \times 0 = 0$$

para cualquier número n . Esto tiene sentido en las transacciones financieras: si pongo tres cantidades de cero dinero en mi cuenta, no he puesto ningún dinero en ella. De nuevo, cero es el único número con esta propiedad especial.

En aritmética, $m \times n$ y $n \times m$ son lo mismo para todos los números m y n . Esta convención implica que

$$0 \times n = 0$$

para cualquier n , a pesar de que no podemos sumar «ninguna copia» de n consigo misma.

¿Qué ocurre con la división? Dividir cero entre un número distinto de cero es sencillo: obtienes cero. La mitad de nada es nada. Pero cuando se trata de dividir un número por cero, sale a relucir la naturaleza inusual del cero. ¿Cuánto es, por ejemplo, $1: 0$? Definimos $m: n$ como cualquier número q que satisface que $q \times n = m$. De modo que $1: 0$ es cualquier número q que satisface que $q \times 0 = 1$. Sin embargo, *no existe tal número*. Para cualquier q que consideremos, tenemos que $q \times 0 = 0$. Nunca obtenemos 1.

El modo obvio de lidiar con esto es aceptarlo. La división entre cero está prohibida porque no tiene sentido. Por otro lado, la gente solía pensar que $1: 2$ tampoco tenía sentido, hasta que se introdujeron las fracciones, de modo que quizás no deberíamos rendirnos tan fácilmente. Podríamos intentar introducir un nuevo número que nos permita dividir por cero. El problema es que ese número transgrede las reglas básicas de la aritmética. Por ejemplo, sabemos que $1 \times 0 = 2 \times 0$ ya que ambas son cero. Dividiendo ambos lados entre cero, tendríamos $1 = 2$, lo cual es tonto. Así que parece sensato no permitir la división entre cero.

Número de la nada

El concepto más próximo a «nada» en matemáticas se da en teoría de conjuntos. Un conjunto es una colección de objetos matemáticos: números, formas, funciones, redes... Se define haciendo una lista o describiendo sus elementos. «El conjunto con los elementos 2, 4, 6, 8» y «el conjunto de los enteros pares entre 1 y 9» definen el mismo conjunto, el cual podemos formar enumerando sus elementos:

$$\{2, 4, 6, 8\}$$

donde las llaves indican el conjunto formado por lo que contienen.

Hacia 1880, el matemático alemán Cantor desarrolló una extensa teoría de conjuntos. Había estado intentando resolver algunos problemas técnicos en análisis relacionados con discontinuidades, lugares donde una función de repente da un salto. Su respuesta involucraba la estructura del conjunto de las discontinuidades. No eran las discontinuidades individuales lo que importaba; era todo el asunto. Lo que realmente interesaba a Cantor, debido a su conexión con el análisis, eran los conjuntos infinitamente grandes. Hizo el espectacular descubrimiento de que algunos infinitos son mayores que otros [véase \aleph_0].

Como mencioné en «¿Qué es un número?», otro matemático alemán, Frege, retomó las ideas de Cantor, pero estaba mucho más interesado en conjuntos finitos. Pensaba que podía resolver el gran problema filosófico de la naturaleza de los números. Reflexionó sobre cómo los conjuntos se

corresponden unos con otros; por ejemplo, emparejando tazas con platos. Los siete días de la semana, los siete enanitos y los números del 1 al 7, todos se emparejan perfectamente, de modo que todos definen el mismo número.

¿Cuál de estos conjuntos debería representar el número siete? La respuesta de Frege fue generalizada: *todos*. Definió un número como el conjunto de todos los conjuntos que se emparejan con un conjunto dado. De ese modo ningún conjunto es privilegiado y la elección es única en vez de ser una convención arbitraria. Nuestros nombres y símbolos para los números son solo etiquetas convencionales para estos gigantescos conjuntos. El número «siete» es el conjunto de *todos* los conjuntos que se emparejan con los enanitos y esto es lo mismo que el conjunto de todos los conjuntos que se emparejan con los días de la semana o la lista {1, 2, 3, 4, 5, 6, 7}.

Es quizá superfluo señalar que aunque esto es una solución elegante del problema *conceptual*, no constituye una notación razonable.

Cuando Frege presentó sus ideas en *Leyes fundamentales de la aritmética*, un trabajo de dos volúmenes que se publicó en 1893 y 1903, parecía como si hubiese resuelto el problema. Ahora todo el mundo sabía lo que era un número. Pero justo antes de que el volumen II fuese a imprenta, Bertrand Russell escribió una carta a Frege, la cual decía (y parafraseo): «Querido Gottlob: considera el conjunto de todos los conjuntos que no se contienen a sí mismos». Como el barbero del pueblo

que afeita a aquellos que no se afeitan solos, este conjunto es contradictorio en sí mismo. La paradoja de Russell, como se conoce ahora, reveló los peligros de asumir que conjuntos grandes de manera generalizada existen [véase \aleph_0].

Los lógicos matemáticos intentaron solucionar el problema. La respuesta resultó ser justamente lo opuesto de la regla «pensar a lo grande» de Frege agrupando todos los posibles conjuntos. En su lugar, el truco era seleccionar solo uno de ellos. Para definir el número 2, construye un conjunto estándar con dos elementos. Para definir 3, usa un conjunto estándar con tres elementos, y así sucesivamente. La lógica aquí no es circular siempre y cuando construyas los conjuntos primero, sin usar números de manera explícita, y asignes símbolos y nombres numéricos para ellos después.

El principal problema era decidir qué conjuntos estándar usar. Tenían que estar definidos de manera única y su estructura debía corresponderse con el proceso de contar. La respuesta vino de un conjunto muy especial, el llamado «conjunto vacío».

Cero es un número, la base de todo nuestro sistema numérico. Debería contar los elementos de un conjunto. ¿Qué conjunto? Bien, tiene que ser un conjunto sin elementos. No es difícil pensar en un conjunto así: «el conjunto de todos los ratones que pesan más de 20 toneladas». Matemáticamente, hay un conjunto sin elementos: el conjunto vacío. De nuevo no es difícil encontrar ejemplos: el conjunto de todos los primos

divisibles entre 4, o el conjunto de todos los triángulos con cuatro vértices. Estos parecen diferentes, uno está formado por números y el otro por triángulos, pero son el mismo conjunto, porque en realidad no hay números o triángulos en él, de modo que no puedes decir cuál es la diferencia. Todos los conjuntos vacíos tienen exactamente los mismos elementos, en concreto, ninguno. Por lo tanto, *el* conjunto vacío es único. Su símbolo, introducido por el grupo con el pseudónimo Bourbaki en 1939, es \emptyset . La teoría de conjuntos necesita el \emptyset , por la misma razón que la aritmética necesita el 0: todo es mucho más simple si se incluye.

De hecho, podemos definir el número 0 como el conjunto vacío.

¿Qué ocurre con el número 1? De modo intuitivo, necesitamos un conjunto con exactamente un elemento. Algo único. Bien... el conjunto vacío es único. De manera que definimos 1 como el conjunto cuyo único elemento es el conjunto vacío, en símbolos: $\{\emptyset\}$. Esto no es lo mismo que el conjunto vacío, porque tiene un elemento, mientras que el conjunto vacío no tiene ninguno. Se acuerda que ese elemento sea el conjunto vacío, pero hay un elemento en él. Piensa en un conjunto como una bolsa de papel que contiene a sus elementos. El conjunto vacío es una bolsa de papel vacía. El conjunto cuyo único elemento es el conjunto vacío es una bolsa de papel que contiene una bolsa de papel vacía. ¿Cuál es la diferencia? Tiene una bolsa en él.



Figura 69. Construyendo los números a partir del conjunto vacío. Las bolsas representan conjuntos; sus elementos son su contenido. Las etiquetas muestran el nombre del conjunto. La bolsa en sí misma no es parte del contenido de ese conjunto, pero puede ser parte del contenido de otra bolsa.

El paso clave es definir el número 2. Necesitamos un conjunto definido de manera única con dos miembros. Así que por qué no usar los dos únicos conjuntos que hemos mencionado hasta ahora: \emptyset y $\{\emptyset\}$. De modo que definimos 2 como el conjunto $\{\emptyset, \{\emptyset\}\}$. Lo cual, debido a nuestras definiciones, es lo mismo que 0, 1.

Surge un patrón general. Definimos $3 = 0, 1, 2$, un conjunto con tres elementos, los cuales ya hemos definido. Luego $4 = 0, 1, 2, 3$ y $5 = 0, 1, 2, 3, 4$, y así sucesivamente. Todo se remonta al conjunto vacío, por ejemplo:

$$3 = \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\}$$

$$4 = \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}, \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\}\}$$

Probablemente no quieres ver el aspecto que tiene el número de los enanitos.

Los materiales de construcción aquí son abstracciones: el conjunto vacío y la acción de formar un conjunto haciendo una lista de sus elementos. Pero el modo en que estos conjuntos se relacionan unos con otros lleva a una construcción bien definida para el sistema numérico, en el cual cada número es un conjunto específico, que de manera intuitiva tiene ese número de elementos. Y la historia no se detiene aquí. Una vez has definido los números positivos enteros, una estratagema teórica para los conjuntos define los números negativos, las fracciones, los números reales (decimales infinitos), los números complejos, etcétera, hasta llegar al más reciente y sofisticado concepto matemático en teoría cuántica.

Así que ahora ya conoces el terrible secreto de las matemáticas: está todo basado en nada.

§. -1 menos que nada

¿Puede un número ser menos que cero? No si hablamos de vacas, a menos que se trate de «vacas virtuales» que debes a alguien. A continuación, obtienes una extensión natural del concepto de número que hace la vida más fácil a quienes se dedican al álgebra y a la contabilidad. Hay unas cuantas sorpresas: menos por menos es más. ¿Por qué?

Los números negativos

Después de aprender cómo sumar números, se nos enseña a realizar la operación inversa: la resta. Por ejemplo, $4 - 3$ es cualquier número que da 4 cuando se le suma 3. Por supuesto, es 1. La resta es útil porque, por ejemplo, nos dice cuánto dinero nos queda si tenemos 4 € y gastamos 3 €.

Restar un número más pequeño a uno más grande no da problemas. Si gastamos menos dinero del que tenemos en el bolsillo o el monedero, todavía nos queda dinero. Pero ¿qué sucede si restamos un número más grande a uno más pequeño? ¿Cuánto es $3 - 4$?

Si tienes tres monedas de 1 € en tu bolsillo, no puedes coger cuatro de ellas y entregarlas en la caja del supermercado. Pero en estos días de tarjetas de crédito, sí puedes gastar fácilmente más dinero del que tienes, no solo en el bolsillo, sino en el banco. Cuando eso sucede, contraes una *deuda*. En este caso, la deuda sería de 1 € sin contar los intereses. De modo que en cierto sentido $3 - 4$ es igual a 1, pero un tipo *diferente* de 1; una deuda, no dinero en efectivo real. Si 1 tuviese un opuesto, sería este. Para distinguir las deudas del dinero en efectivo, ponemos un signo menos delante del número. Con esta notación:

$$3 - 4 = -1$$

y hemos inventado un nuevo tipo de número: un número negativo.

Historia de los números negativos

Históricamente, la primera extensión importante del sistema numérico fueron las fracciones [véase $\frac{1}{2}$] Los números negativos fueron la segunda. Sin embargo, trataré estos tipos de números en el orden opuesto. La primera aparición conocida de los números negativos fue en un documento chino de la dinastía Han, 202 a. C.-220 d. C., llamado *Jiu Zhang Suan Shu* («Los nueve capítulos sobre el arte matemático»).

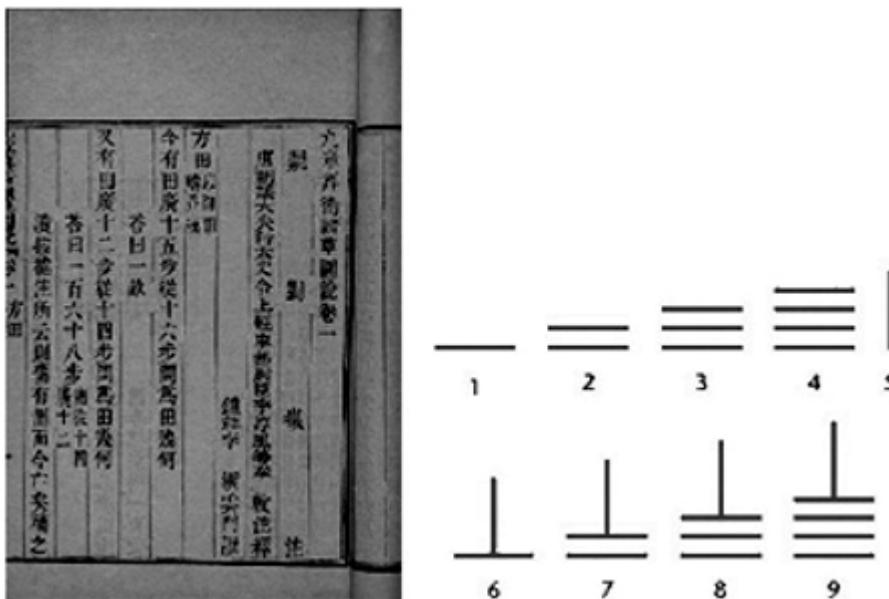


Figura 70. Izquierda: una página de *Los nueve capítulos sobre el arte matemático*. Derecha: palitos de contar chinos.

Este libro contaba con una ayuda física para hacer aritmética: palitos para contar. Se trata de pequeños palos, hechos de madera, hueso o un material similar que se disponían en patrones para representar números. En el lugar de las «unidades» de un número, un palito en horizontal

representa «uno» y un palito vertical representa «cinco». Se aplica lo mismo para el lugar de las «centenas». En los lugares de las «decenas» y «millares», las direcciones de los palitos se intercambian: un palito vertical representa «uno» y un palito horizontal representa «cinco». Los chinos dejaban un hueco donde nosotros pondríamos 0, pero no es fácil advertir ese hueco. La convención sobre intercambiar las direcciones ayuda a evitar la confusión si, por ejemplo, no hay nada en el lugar de las decenas. Es menos efectiva si hay varios ceros seguidos, pero eso es raro.



Figura 71. Cómo la dirección de los palitos de contar distingue 405 de 45.

Los nueve capítulos también se servía de palitos para representar los números negativos, usando una idea muy sencilla: colorearlos de negro en lugar de rojo. De modo que 4 palitos rojos menos 3 rojos da 1 palito rojo pero, 3 palitos rojos menos 4 rojos da 1 palito negro.

De esta manera, una disposición de palitos negros representa una deuda y la cantidad de la deuda es la correspondiente disposición de palitos rojos.

Los matemáticos hindúes también identificaron los números negativos y escribieron reglas para realizar cálculos aritméticos consistentes con ellos. El manuscrito Bakhshali, de alrededor de 300 d. C., incluye cálculos con números negativos, los cuales se distinguen por un símbolo + donde ahora usaríamos -. (Los símbolos matemáticos han cambiado reiteradamente a lo largo del tiempo, a veces de forma que ahora valoramos confusa.) La idea fue tomada por los matemáticos árabes y finalmente se extendió a Europa. Hasta el siglo XVII, los matemáticos europeos generalmente interpretaban una respuesta negativa como una prueba de que el problema que les ocupaba era imposible, pero Fibonacci se dio cuenta de que podrían representar deudas en cálculos financieros. En el siglo XIX, los números negativos ya no desconcertaban a los matemáticos.

Representación de los números negativos

Geométricamente, los números se pueden representar dispuestos a lo largo de una recta de izquierda a derecha empezando en 0. Ya hemos visto que esta recta numérica tiene una extensión natural que incluye los números negativos, los cuales van en la dirección opuesta.

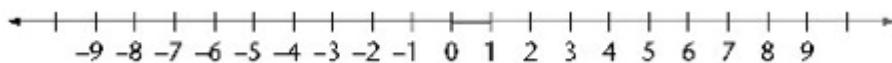


Figura 72. Recta numérica: los números positivos van hacia la derecha; los negativos, hacia la izquierda.

La suma y la resta tienen una representación sencilla en la recta numérica. Por ejemplo, para sumar 3 a cualquier número, mueve 3 espacios a la derecha. Para restar 3 a cualquier número, mueve 3 espacios a la izquierda. Esta descripción produce el resultado correcto tanto para los números positivos como para los negativos; por ejemplo, si empezamos con -7 y sumamos 3, movemos 3 espacios a la derecha y obtenemos -4 . Las reglas para la aritmética con números negativos también muestran que sumar o restar un número negativo tiene el mismo efecto que restar o sumar el positivo correspondiente. De modo que para sumar -3 a cualquier número, movemos 3 espacios a la izquierda. Para restar -3 a cualquier número, movemos 3 espacios a la derecha.

La multiplicación con números negativos es más interesante. Cuando nos encontramos por primera vez con la multiplicación, pensamos en ella como una suma repetida. Por ejemplo:

$$6 \times 5 = 5 + 5 + 5 + 5 + 5 + 5 = 30$$

La misma aproximación sugiere que deberíamos definir 6×-5 de un modo similar:

$$6 \times -5 = -5 + -5 + -5 + -5 + -5 + -5 = -30$$

Ahora, una de las reglas de la aritmética establece que multiplicar dos números positivos produce el mismo resultado, cualquiera que sea el orden de estos. Por ejemplo, 5×6 debería ser igual a 30. De hecho lo es, porque

$$5 \times 6 = 6 + 6 + 6 + 6 + 6 = 30$$

Así que parece razonable asumir la misma regla para los números negativos, en cuyo caso $-5 \times 6 = -30$ también.

¿Qué ocurre con -6×-5 ? Esto no está tan claro. No podemos escribir *menos seis cinco*s y sumarlos. De modo que tenemos que acercarnos con cuidado a la pregunta. Observemos lo que sabemos hasta ahora:

$$6 \times 5 = 30$$

$$6 \times -5 = -30$$

$$-6 \times 5 = -30$$

$$-6 \times -5 = ?$$

Parece razonable que el número que falta sea o bien 30 o bien -30. ¿Cuál es?

A primera vista, la gente suele decidir que debería ser -30 . Para la psicología parece ser que el cálculo está impregnado de un aire de «negatividad», por lo que la respuesta debería ser también negativa. Es el mismo tipo de suposición que subyace en la queja de «No lo has hecho, ¿no?». Sin embargo, es razonable señalar que si tú «no, no lo has hecho», entonces tú no has hecho un «no lo he hecho», que equivale a «hacerlo». Este comentario será justo dependiendo de las reglas gramaticales que estés asumiendo, ya que a veces el «no» extra también puede verse como añadirle énfasis.

Del mismo modo, el significado de -6×-5 es un asunto de convención humana. Cuando inventamos los nuevos números, no había garantías de que los viejos conceptos se pudiesen seguir aplicando a ellos. De modo que los matemáticos podían haber decidido que $-6 \times -5 = -30$. Es más, podían haber decidido que -6×-5 es un hipopótamo morado.

Sin embargo, hay varias razones diferentes por las que -30 no es una elección conveniente y todo apunta a la elección opuesta, 30 .

Una es que si $-6 \times -5 = -30$, es lo mismo que -6×5 . Dividiendo por -6 , tendríamos que $-5 = 5$, lo cual entra en conflicto con lo que ya hemos decidido sobre los números negativos.

Una segunda razón es que ya sabemos que $5 + -5 = 0$. Observa la recta numérica, ¿qué está a 5 pasos a la izquierda del 5? Cero. Ahora, multiplicando cualquier número positivo por 0 tenemos 0, y parece

razonable asumir lo mismo para los números negativos. De modo que tiene sentido asumir que $-6 \times 0 = 0$. Por lo tanto:

$$0 = -6 \times 0 = -6 \times (5 + -5).$$

Según la reglas habituales de la aritmética, esto es igual a:

$$-6 \times 5 + -6 \times -5$$

Con la elección de $-6 \times -5 = -30$, esto se convierte en $-30 + -30 = -60$.

De modo que $0 = -60$, lo cual no es muy razonable.

Por otro lado, si habíamos escogido $-6 \times -5 = 30$, tendríamos:

$$0 = -6 \times 0 = -6 \times (5 + -5) = -6 \times 5 + -6 \times -5 = -30 + 30 = 0$$

y todo cobraría sentido.

Una tercera razón es la estructura de la recta numérica. Cuando multiplicamos un número positivo por -1 , lo convertimos en el correspondiente número negativo; esto es, giramos por completo la mitad positiva de la recta numérica 180° , moviéndola de derecha a izquierda. ¿Dónde debería ir la mitad negativa? Si la dejamos donde estaba, tendríamos el mismo tipo de problema, porque -1×-1 sería -1 , lo que lo hace igual a -1×1 y concluiríamos que $-1 = 1$. La única alternativa

razonable es girar la mitad negativa de la recta numérica 180° también, moviéndola de izquierda a derecha. Esto está bien, porque ahora multiplicar por -1 gira en redondo la recta numérica, invirtiendo el orden. Lo que sigue, al igual que la noche sucede al día, es que multiplicar por -1 de nuevo gira la recta numérica otros 180° . Esto invierte el orden de nuevo y todo vuelva a estar como cuando se empezó. De hecho, el ángulo total es $180^\circ + 180^\circ = 360^\circ$, un giro completo, y lleva todo de nuevo a donde estaba al inicio. Así -1×-1 es donde -1 va cuando giras la recta, esto es, 1. Y una vez has decidido que $-1 \times -1 = 1$, se sigue que $-6 \times -5 = 30$.

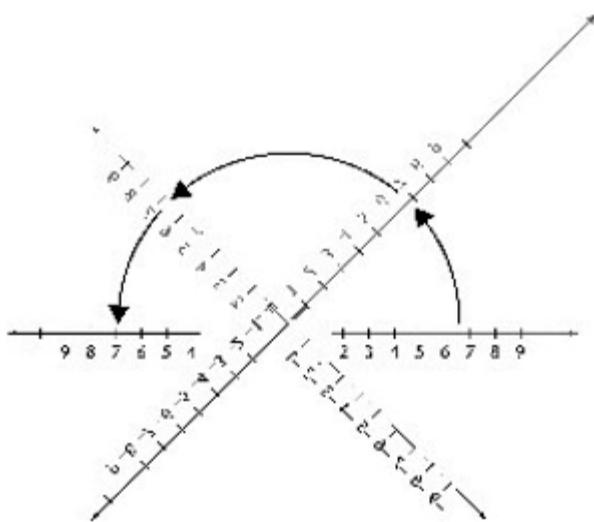


Figura 73. Girar la recta numérica 180° multiplica cada número por -1 .

Una cuarta razón es la interpretación de la cantidad negativa de dinero efectivo como deuda. En esta interpretación, multiplicar cierta cantidad de dinero en efectivo por un número negativo da el mismo resultado que

multiplicarla por el correspondiente número positivo, excepto que el dinero efectivo se convierte en deuda. Ahora, *restando* la deuda, «quitándola», tiene el mismo efecto que si el banco elimina la cantidad que le debes de su registro, lo que equivale a devolverte el dinero. Restar una deuda de 10 € de tu cuenta es como depositar 10 € de tu propio dinero: *incrementa* tu cuenta en 10 € El efecto neto de ambos, en estas circunstancias, es volver a poner tu balance a cero. Por lo tanto se concluye que -6×-5 tiene el mismo efecto en tu balance bancario que el quitar seis deudas de 5 €, y esto es incrementar tu balance en 30 €

El resultado de esos argumentos es que, aunque en principio quizá fuésemos libres de definir -6×-5 del modo en que quisiéramos, hay solo una única elección que hace que las reglas habituales de la aritmética se apliquen a los números negativos. Además, la misma elección tiene sentido cuando la aplicamos a la interpretación de un número negativo como una deuda. Y esa elección hace menos por menos igual a más.

Números complejos

Contenido:

§. i Número imaginario

Cuando los matemáticos querían dividir un número entre otro que no daba un resultado exacto, inventaron las fracciones.

Cuando querían restar un número mayor de uno más pequeño, inventaron los números negativos.

Cada vez que algo no puede hacerse, los matemáticos inventan algo nuevo que lo resuelva.

Así que cuando la imposibilidad de encontrar una raíz cuadrada de un número negativo empezó a ser un fastidio importante... adivina qué...

§. i Número imaginario

En el «Sistema numérico creciente» (Ver acápite **Números**, párrafo “El Sistema Numérico Creciente”), dije que tendíamos a pensar en los números como fijos e inmutables, pero realmente son invenciones humanas. Los números nacieron con la necesidad de contar, pero el concepto de número se extendió de manera reiterada: cero, los números

negativos, los números racionales (fracciones), los números reales (con infinitos decimales).

A pesar de las diferencias técnicas, todos estos sistemas tienen un aspecto parecido. Puedes hacer cálculos aritméticos con ellos y puedes comparar dos números para decidir cuál es mayor. Lo que quiere decir que hay una noción de orden. Sin embargo, a partir del siglo XV, algunos matemáticos se preguntaron si podría haber un nuevo tipo de número con propiedades menos comunes, para el cual la relación de orden habitual, «ser mayor que», ya no tuviese significado.

Como menos por menos es más, el cuadrado de cualquier número real es positivo. Por lo tanto, los números negativos no tienen raíces cuadradas dentro del sistema de los números reales. Esto es en cierto modo inapropiado, especialmente en álgebra. Sin embargo, algunos resultados curiosos en álgebra, al proporcionar fórmulas para resolver ecuaciones, sugerían que debería haber un modo de dar sentido a expresiones como $\sqrt{-1}$. De modo que los matemáticos decidieron, después de mucho desconcierto y de darle muchas vueltas, inventar un nuevo tipo de número, uno que produzca esas raíces cuadradas perdidas.

El paso clave es introducir una raíz cuadrada para -1 . Euler estableció el símbolo i para representar $\sqrt{-1}$ en un artículo escrito en Francia en 1777. Se llamó «número imaginario» porque no se comportaba como un número «real» tradicional. Al introducir i , hay que permitir números relacionados como $2 + 3i$, a los que se llama «complejos». Así que no

obtienes un solo número nuevo, sino un nuevo y ampliado sistema numérico.

Desde el punto de vista lógico, los números complejos dependen de los números reales. Sin embargo, la lógica se ve sobrepasada por lo que Terry Pratchett, Jack Cohen y yo mismo, en la serie de la ciencia de Mundodisco llamamos «narrativium»: el poder de una historia. Las historias matemáticas tras los números son lo que realmente importa y necesitamos los números complejos para contar algunas de esas historias, incluso para números que son más familiares.

Números complejos

La aritmética y el álgebra de los números complejos son sencillas. Usan las reglas normales de suma y multiplicación con un ingrediente extra: cada vez que escribas i^2 , debes reemplazarlo por -1 . Por ejemplo:

$$(2 + 3i) + (4 - i) = (2 + 4) + (3i - i) = 6 + 2i$$

$$(2 + 3i) \times (1 + i) = 2 + 2i + 3i + 3i \times i = 2 + 5i + 3 \times -1 =$$

$$(2 - 3) + 5i = -1 + 5i$$

Los primeros en explorar esta idea obtuvieron lo que parecía ser un tipo de número consistente desde un punto de vista lógico, que ampliaba el sistema de los números reales.

Había precedentes. El sistema numérico ya había sido ampliado muchas veces desde sus orígenes contando con los números naturales. Pero esta vez, la noción de «mayor que» tenía que sacrificarse; estaba bien para los números existentes, pero acababa dando problemas asumir que funcionaba para los nuevos números. ¡Números que no tienen un *tamaño*! Raro. Tan raro que en esta ocasión los matemáticos observaron que estaban ampliando el sistema numérico y se preguntaron si eso era legítimo. No se habían hecho esta pregunta antes, porque las fracciones y los números negativos tenían análogos sencillos en el mundo real. Pero i era tan solo un símbolo, y se comportaba de un modo que antes se consideró imposible.

Finalmente, el pragmatismo triunfó. La pregunta clave no era si nuevos tipos de número existían «realmente», sino si sería útil suponer que existían. Los números reales ya eran conocidos por ser útiles en ciencia, para describir medidas precisas de cantidades físicas. Pero no estaba claro que la raíz cuadrada de un número negativo tuviese sentido físico. No podías encontrarla en una regla.

Para sorpresa de los matemáticos, los físicos y los ingenieros del mundo, los números complejos resultan ser extraordinariamente útiles. Rellenaron un vacío curioso en matemáticas. Por ejemplo, las soluciones

de ecuaciones se comportan mucho mejor si se aceptan los números complejos. De hecho, ese fue el principal motivo para inventar los números complejos en primer lugar. Pero había más. Los números complejos hicieron posible resolver problemas en física matemática: magnetismo, electricidad, calor, sonido, gravedad y flujo de fluidos.

Lo que importa en esos problemas no es solo lo grande que es cierta cantidad física, la cual puede especificarse usando un número real, sino en qué dirección apunta. Como los números complejos viven en un plano (véase más abajo), definen una dirección: la recta desde 0 al número que nos ocupa. Por lo tanto, cualquier problema en el que estén involucradas direcciones en un plano es una aplicación potencial de los números complejos, y la física estaba llena de esas cuestiones. De hecho, interpretaciones menos literales de los números complejos también resultaron ser útiles. En particular, resultan ideales para describir ondas.

Durante mucho tiempo, los números complejos se usaban con ese propósito, incluso aunque nadie podía explicar qué eran esos números. Eran demasiado útiles para ignorarlos y parecía que funcionaban siempre, de modo que todo el mundo se acostumbró a ellos y casi todo el mundo dejó de preocuparse sobre qué significaban. Finalmente, algunos matemáticos se las arreglaron para establecer la idea de números complejos de modo que esta consistencia lógica pudiese probarse, interpretándolos usando coordenadas en el plano.

El plano complejo

Geométricamente, los números reales se pueden representar como puntos en una recta, la recta numérica, que es unidimensional. De manera análoga, los números complejos pueden representarse como puntos en un plano, que es bidimensional. Hay dos números básicos «independientes»: 1 e i , y todo número complejo es una combinación de estos.

El plano aparece en escena porque multiplicar números por -1 rota la recta numérica 180° [véase -1]. Signifique lo que signifique la raíz cuadrada de -1 , presumiblemente hace algo a la recta numérica y, sea lo que sea que hace, debe, *cuando se hace dos veces*, rotarla 180° . Así que ¿qué rota las cosas 180° cuando lo haces dos veces?

La rotación de 90° .

Esto nos lleva a intuir que la raíz cuadrada de -1 puede interpretarse en términos de una rotación de la recta numérica de 90° . Si hacemos un dibujo, nos damos cuenta de que esto no convierte la recta numérica en sí misma. En su lugar, crea una segunda recta numérica que forma un ángulo recto con la habitual. La primera recta se llama «la recta de los números reales». En la segunda recta residen los números imaginarios, como la raíz cuadrada de menos uno. Combinando ambas como ejes de coordenadas en el plano, obtenemos los números complejos.

«Real» e «imaginario» son nombres que se remontan a siglos atrás y reflejan una visión de las matemáticas en la que ya no creemos. En la actualidad, todos los conceptos matemáticos se consideran modelos

mentales de la realidad, no la realidad en sí misma. Por lo tanto, los números reales no son más o menos reales que los imaginarios. Aunque los números reales sí se corresponden bastante directamente con la idea de mundo real de medir la longitud de una recta, mientras que los números imaginarios no tienen una interpretación *directa* de ese tipo. Por eso han sobrevivido los nombres.

Si tomamos los números reales habituales y añadimos este número nuevo i , también debemos ser capaces de representar combinaciones como $3 + 2i$. Este número corresponde al punto en el plano con coordenadas $(3, 2)$. Esto quiere decir que se sitúa 3 unidades a lo largo del eje real seguido por 2 unidades paralelas al eje imaginario. En general, $z = x + iy$ se corresponde con el punto de coordenadas (x, y) .

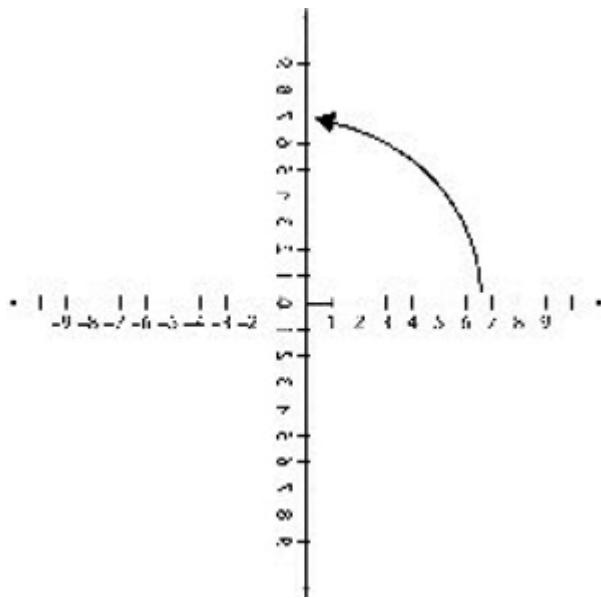


Figura 74. Rotar la recta numérica en un ángulo recto lleva a una segunda recta numérica.

A esta representación geométrica de los números complejos se la llama con frecuencia «diagrama de Argand», por el matemático francés Jean-Robert Argand, que los describió en 1806. Sin embargo, la idea se remonta al topógrafo noruego-danés Caspar Wessel, que lo publicó en 1797 como *Om Directionens analytiske Betegning* («Sobre la representación analítica de la dirección»). Dinamarca estuvo temporalmente unida a Noruega en esa fecha. Su artículo pasó desapercibido en ese momento porque pocos científicos podían leer danés.

Gauss reinventó la misma idea en su tesis doctoral de 1799 y se dio cuenta de que la descripción podía simplificarse usando coordenadas para considerar un número complejo como un par (x, y) de números reales. En la década de 1830, Hamilton *definió* los números complejos como «parejas de números reales», pareja lo usaba como nombre para un par ordenado. Así es como definimos los números complejos hoy en día. Un punto en el plano es un par ordenado (x, y) , y el símbolo $x + iy$ es solo otro nombre para ese punto o par. La misteriosa expresión i es entonces solo el par ordenado $(0, 1)$. El punto clave es que tenemos que definir la suma y la multiplicación para estos pares como:

$$(x, y) + (u, v) = (x + u, y + v)$$

$$(x, y)(u, v) = (xu - yv, xv + yu)$$

¿De dónde proceden estas ecuaciones? Surgen de sumar o multiplicar $x + iy$ y $u + iv$, asumiendo las leyes estándar del álgebra y reemplazando i^2 por -1 .

Estos cálculos motivan las definiciones, ya que asumimos las leyes de álgebra para ver cómo deberían ser las definiciones. La lógica deja de ser circular cuando verificamos las leyes del álgebra para estos pares, basado solo en las definiciones formales. No es una sorpresa que todo funcione, pero hay que comprobarlo. El razonamiento es largo pero sencillo.

Raíces de la unidad

La interacción entre álgebra y geometría en los números complejos es notable. Esto es especialmente obvio en las raíces de la unidad: soluciones para la ecuación $z^n = 1$ para z complejo y n número natural.

Por ejemplo, raíces quintas de la unidad satisfacen $z^5 = 1$.

Una solución obvia es $z = 1$, la única solución real. En los números complejos, sin embargo, hay otras cuatro. Son ζ, ζ^2, ζ^3 y ζ^4 , donde

$$\zeta = \cos 72^\circ + i \sin 72^\circ$$

Aquí $72^\circ = 360^\circ/5$. Hay fórmulas exactas:

$$\cos 72^\circ = \frac{\sqrt{5}-1}{4} \quad \sin 72^\circ = \sqrt{\frac{5+\sqrt{5}}{8}}$$

Estos cinco puntos forman los vértices de un pentágono regular, un hecho que puede probarse usando trigonometría. La idea básica es que, al igual que la multiplicación por i rota el plano complejo 90° , también la multiplicación por ζ rota el plano complejo 72° . Si haces esto cinco veces, obtienes 360° , lo cual es lo mismo que no rotar nada o multiplicar por 1. De modo que $\zeta^5 = 1$.

De forma más general, la ecuación $zn = 1$ tiene n soluciones: $1, \zeta, \zeta^2, \zeta^3, \dots, \zeta^{n-1}$, donde

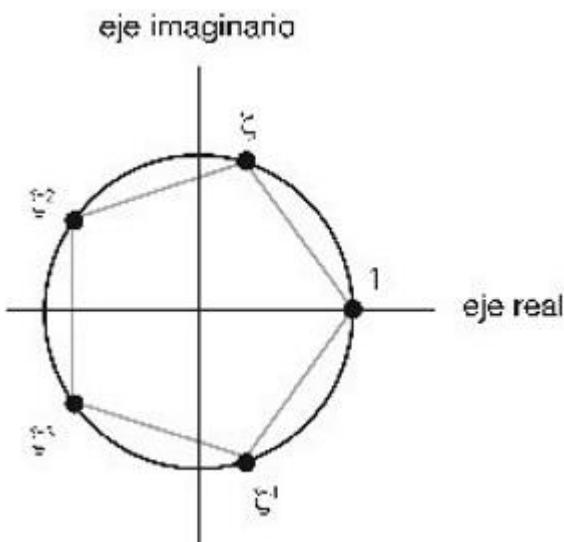


Figura 75. Las cinco raíces quintas de la unidad en el plano complejo.

$$\zeta = \cos \frac{360^\circ}{n} + i \sin \frac{360^\circ}{n}$$

Estas ideas proporcionan una interpretación algebraica de los polígonos regulares, que se usa para estudiar construcciones usando regla y compás en la geometría euclíadiana [véase 17].

Números racionales

Contenido:

- §. *Dividiendo lo indivisible*
- §. *Aproximación a pi*
- §. *Torres de Hanoi*

Vamos a observar las fracciones, a las que los matemáticos llaman «números racionales».

Históricamente, las fracciones aparecían cuando había que dividir entre varias personas los bienes o la propiedad, y cada una se quedaba con una porción.

Todo empezó con $\frac{1}{2}$, que surge cuando dos personas obtienen porciones iguales.

El resultado fue un sistema numérico en el cual la división siempre es posible, excepto entre cero.

§. $\frac{1}{2}$ *Dividiendo lo indivisible*

Ahora pasamos a las fracciones. Los matemáticos prefieren un término más elegante: *números racionales*. Estos son números como $\frac{1}{2}$, $\frac{3}{4}$ o,

$\frac{137}{42}$ formados al dividir un número entero entre otro. Imagínate a ti mismo tiempo atrás, cuando «número» significaba «número natural». En ese mundo, la división tiene sentido totalmente, cuando un número es exactamente un número de veces otro; por ejemplo $\frac{12}{3} = 4$. Pero de ese modo no obtienes nada nuevo. Las fracciones empiezan a ser interesantes precisamente cuando la división no da un resultado exacto. Más en concreto, cuando el resultado no es un número entero. Porque entonces necesitamos *un tipo nuevo de número*.

La fracción más sencilla, y la que aparece con más frecuencia en el día a día, es la mitad: $\frac{1}{2}$. El *Oxford English Dictionary* la define como: «cualquiera de las dos partes iguales o correspondiente en las que algo es dividido o puede dividirse». Las mitades abundan en la vida diaria: media pinta de cerveza o medio litro de leche, las dos mitades de un partido de fútbol o rugby, ofertas o tique a mitad de precio, media hora... ¿Medio lleno o medio vacío?

Además de ser la fracción más sencilla, $\frac{1}{2}$ se podría decir que es la más importante. Euclides sabía cómo hacer la bisección de segmentos y ángulos, es decir, dividirlos por la mitad. Una propiedad más avanzada aparece en la teoría analítica de números: se especula que los ceros no triviales de la función zeta de Riemann siempre tienen parte real $\frac{1}{2}$. Este es probablemente el problema sin resolver más importante de todas las matemáticas.

Haciendo la bisectriz de un ángulo

La naturaleza especial de $\frac{1}{2}$ aparece pronto en la geometría de Euclides. La proposición 9 del libro I de los *Elementos* proporciona una construcción «para hacer la bisectriz de un ángulo dado», es decir, para construir un ángulo de la mitad de tamaño. Se hace como sigue: dado un ángulo BAC , usa un compás para construir los puntos D y E equidistantes de A en las rectas AB y AC . Ahora traza un arco con centro en D y radio DE y un arco con centro en E y radio ED . Se cortan en el punto F , equidistante de D y E . La recta AF divide en dos partes iguales al ángulo BAC . Euclides describe el paso final de un modo ligeramente distinto: construye un triángulo equilátero DEF . Esta es una decisión táctica basada en lo que había probado previamente, y da exactamente el mismo resultado, porque el triángulo DEF es equilátero.

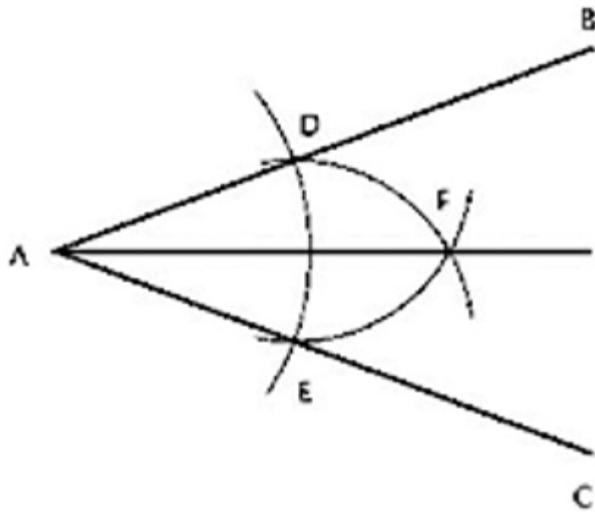


Figura 76. Cómo hacer la bisectriz de un ángulo.

La razón profunda de por qué esta construcción funciona es la simetría. El diagrama completo es simétrico, al considerar la reflexión en el eje AF. La reflexión es una simetría de orden 2: al realizarla dos veces, vuelves a donde empezaste. De modo que no es una sorpresa que dividamos el ángulo en *dos* partes iguales.

Euclides no nos muestra cómo hacer la trisección de un ángulo general (dividirlo en tres partes iguales) correspondiente a la fracción $\frac{1}{3}$. En el capítulo [3], vimos que alrededor de 2.000 años más tarde los matemáticos probaron que era imposible con los instrumentos tradicionales: la regla (sin marcas) y el compás. De hecho, las únicas fracciones de un ángulo general que pueden construirse de esta manera son de la forma $p/2^k$: dividir entre dos k veces y luego hacer p copias. Básicamente la única cosa que puedes hacer es repetir la bisección. Por lo tanto $p/2^k$ es especial en geometría.

La hipótesis de Riemann

En matemáticas avanzadas, $\frac{1}{2}$ aparece en lo que es probablemente el problema sin resolver más importante en toda la asignatura: la hipótesis de Riemann. Esta es una conjetura de aparente aspecto inocente propuesta por Georg Bernhard Riemann en 1859. Se trata de una propiedad profunda de un artilugio inteligente: la función zeta $\zeta(z)$, donde z es cualquier número complejo y ζ es la letra griega «zeta». La función zeta está muy relacionada con los números primos, de modo que

técnicas potentes usando los números complejos pueden usar esa función para probar la estructura de los primos.

Sin embargo, no podemos explotar estas técnicas hasta que hayamos resuelto algunas características básicas de la función zeta, y es ahí donde todo se complica. Las características clave son los *ceros* de la función zeta, los números complejos z para los cuales $\zeta(z) = 0$. Algunos ceros son fáciles de encontrar: todos los enteros negativos pares, $z = -2, -4, -6, -8, \dots$ Sin embargo, Riemann pudo probar que había infinidad de otros ceros y halló seis de ellos:

$$\frac{1}{2} \pm 14,135 i$$

$$\frac{1}{2} \pm 21,022 i$$

$$\frac{1}{2} \pm 25,011 i$$

(Los ceros siempre vienen en pares con partes imaginaria positiva y negativa.)

No necesitas tener mucha sensibilidad matemática para observar que estos seis números tienen algo interesante en común: son de la forma $\frac{1}{2} + iy$. Es decir, tienen parte real $\frac{1}{2}$. Riemann hizo la hipótesis de que la misma afirmación es válida para *todos* los ceros de la función zeta excepto para los enteros negativos pares. Esta conjetura pasó a ser

conocida como la «hipótesis de Riemann». Si fuese cierta (y todas las evidencias apuntan en esa dirección), tendría muchas consecuencias de gran alcance. Lo mismo resultaría para una variedad de generalizaciones, las cuales serían incluso más importantes.

A pesar de llevar más de 150 años de búsqueda extenuante, todavía no se ha encontrado ninguna prueba. La hipótesis de Riemann sigue siendo uno de los enigmas más desconcertantes e irritantes de todas las matemáticas. Su resolución sería una de los eventos más impresionantes en la historia de las matemáticas.

La ruta hacia la hipótesis de Riemann empezó con el descubrimiento de que los números primos, aunque de modo individual parecen incomprensiblemente irregulares, en conjunto siguen claros patrones estadísticos. En 1835, Adolphe Quetelet asombró a sus contemporáneos encontrando regularidades matemáticas en eventos sociales que dependían de elecciones humanas conscientes o de la intervención del destino: nacimientos, bodas, muertes, suicidios. Los patrones eran estadísticos: no se referían a individuos, sino al comportamiento medio de un gran número de personas. Casi al mismo tiempo, los matemáticos empezaron a darse cuenta de que el mismo truco funcionaba para los primos. Aunque cada uno es una individualidad irregular, colectivamente hay patrones escondidos.

Cuando Gauss tenía unos 15 años, escribió una nota en sus tablas de logaritmos: cuando x es grande, el número de primos menores o iguales a

x es aproximadamente $x/\log x$. Esto pasó a conocerse como el «teorema de los números primos» y al principio carecía de una prueba, de modo que en realidad era la conjetura de los números primos. En 1848 y 1850, el matemático ruso Pafnuty Chebyshev intentó probar el teorema de los números primos usando el análisis. A primera vista, no hay una conexión obvia, alguien podría intentarlo también usando la dinámica de fluidos o el cubo de Rubik. Pero Euler ya había señalado un vínculo curioso entre los dos temas, la fórmula donde p recorre todos los primos y s es cualquier número real mayor que 1. La condición de que $s > 1$ se necesita para hacer que la serie de la parte de la derecha tenga un valor significativo. La idea principal tras la fórmula es expresar la naturaleza única de la factorización de primos en lenguaje analítico. La función zeta $\zeta(z)$ es la serie en la parte derecha de esta ecuación; su valor depende de s .

$$\frac{1}{1 - 2^{-s}} \times \frac{1}{1 - 3^{-s}} \times \dots \times \frac{1}{1 - p^{-s}}$$

$$\frac{1}{1^s} + \frac{1}{2^s} + \frac{1}{3^s} + \frac{1}{4^s} + \frac{1}{5^s} + \frac{1}{6^s} + \frac{1}{7^s} + \dots$$

Chebyshev usó la fórmula de Euler para probar que, cuando x es grande, el número de primos menores o iguales que x es bastante próximo a $x/\log x$. De hecho, la razón está entre dos constantes, una ligeramente mayor que 1 y una ligeramente menor. Esto no era tan preciso como el teorema

de los números primos, pero llevaba a una prueba de otra conjetura pendiente, el postulado de Bertrand de 1845: si tomas cualquier entero y calculas su doble, existe un primo entre los dos.

Riemann se preguntaba si podía hacer más poderosa la idea de Euler exponiéndola a técnicas nuevas, y eso le llevó a una ambiciosa extensión de la función zeta: definirla no solo para una variable real, sino para una compleja. La serie de Euler es un buen comienzo. La serie tiene sentido totalmente para s *complejo*, siempre y cuando la parte real de s sea mayor que 1. (Este es un requerimiento técnico que implica que la serie converge, su suma a infinito es significativa.) La primera gran intuición que tuvo Riemann fue que él podía hacerlo mejor. Podía usar un procedimiento llamado «extensión analítica» para ampliar la definición de $\zeta(z)$ a *todos* los números complejos excepto 1. Ese valor está excluido porque la función zeta se hace infinita cuando $s = 1$.

Es la técnica de extensión la que implica que todos los enteros negativos pares son ceros, aunque no puedes verlo directamente a partir de la serie. También da pistas sobre nuevas propiedades de la función zeta, la cuales Riemann exploró. En 1859, juntó todas sus ideas en un artículo «Sobre el número de primos menores que una magnitud dada». En él, ofrecía una fórmula explícita y exacta para el número de primos menores que cualquier número real dado x . *Grosso modo* dice que la suma de los logaritmos de esos primos es aproximadamente:

$$-\sum_{\rho} \frac{x^{\rho}}{\rho} + x - \frac{1}{2} \log(1 - x^{-2}) - \log 2\pi$$

Donde Σ indica una suma de todos los números ρ para los cuales $\zeta(\rho)$ es cero, excluyendo los enteros negativos pares.

Si sabemos lo suficiente sobre los ceros de la función zeta, podemos deducir mucha información nueva sobre los primos a partir de la fórmula de Riemann. En concreto, información sobre las partes reales de los ceros nos permite deducir propiedades estadísticas de los primos: cuántos hay hasta algún tamaño dado, cómo están distribuidos entre los otros enteros, etcétera. Aquí es donde la hipótesis de Riemann reporta beneficios... *si* puedes probarla.

Riemann tenía la clarividencia para ver esta posibilidad, pero nunca forzó su programa hacia una conclusión sólida. Sin embargo, en 1896, Jacques Hadamard y Charles Jean de la Vallée Poussin independientemente usaron la visión de Riemann para deducir el teorema de los números primos. Lo hicieron probando una propiedad más débil de los ceros no triviales de la función zeta: la parte real está entre 0 y 1.

En 1903, Jorgen Gram mostró numéricamente que los primeros diez (pares #) ceros estaban en la recta crítica. En 1935, E. C. Titchmarsh había incrementado el número a 195. En 1936, Titchmarsh y Leslie Comrie probaron que los primeros 1.041 pares de ceros están en la recta crítica (la última vez que alguien hizo esos cálculos a mano). En 1953,

Turing descubrió un método más eficiente y usó un ordenador para deducir que los primeros 1.104 pares de ceros están en la recta crítica. El récord actual, de Yannick Saouter y Patrick Demichel, en 2004, es que los primeros 10^{13} (10 billones) ceros no triviales están en la recta crítica. Los matemáticos e informáticos han comprobado otros rangos de ceros. Hasta la fecha, todo cero no trivial que ha sido computado se encuentra en la recta crítica.

Por desgracia, en esta área de la teoría de números, evidencias experimentales de este tipo conllevan menos peso del que cabría esperar. Muchas otras conjeturas, aparentemente apoyadas por muchas evidencias, han fracasado. Se necesita solo *una* excepción para destrozar todo lo construido y, hasta donde sabemos, esa excepción podría ser tan grande que nuestros cálculos ni siquiera se aproximan. Esto es porque los matemáticos exigen pruebas y es lo que ha sustentado el progreso en esta área durante más de 150 años.

§. Aproximación a π 22/7

Muchas veces en las clases de matemáticas en las escuelas se dice «considerar $\pi = 22/7$ »². Pero ¿realmente podemos hacerlo si interpretamos el signo igual de forma literal? E incluso, si no nos preocupa un pequeño error, ¿de dónde viene esa fracción en concreto?

² En España, en la escuela se utiliza la aproximación 3,14.

Racionalizar π

El número π no puede ser exactamente igual a $22/7$ porque es irracional [véase $\sqrt{2}$ y π]; es decir, no es una fracción exacta $22/7$ donde p y q son números enteros. Este hecho, que desde hacía tiempo sospechaban los matemáticos, se probó por primera vez en 1768 por Johann Lambert. Desde entonces se han encontrado varias pruebas diferentes. En concreto, esto implica que la expresión decimal de π no se acaba nunca y no repite el mismo bloque de números una vez tras otra infinitamente; es decir, no es un decimal *periódico*. Esto no quiere decir que un bloque específico como 12345 no pueda darse muchas veces; de hecho, es muy probable que ocurra con frecuencia infinita. Pero no se puede obtener π repitiendo algún bloque fijo de dígitos infinitamente.

A veces, en matemáticas se evita esta dificultad usando una aproximación de π , en concreto $22/7$. No necesitas probar que es irracional para ver que no es exacta:

$$\pi = 3,141592\dots$$

$$22/7 = 3,142857$$

Además, $22/7$, que es número racional, es un decimal periódico, y sus dígitos decimales son:

$$22/7 = 3,142857142857142857\dots$$

Repite infinitamente el bloque 142857.

A lo largo de la historia, se han usado varios números racionales para aproximar π .

Hacia 1900 a. C., los matemáticos en Babilonia hacían cálculos equivalentes a la aproximación $\pi \sim 25/8 = 3 \frac{1}{8}$.

El matemático papiro de Rhind fue escrito por un escriba llamado Ahmes durante el Segundo Período Intermedio, alrededor de 1650-1550 a. C., aunque él afirma que lo copió de un papiro más antiguo del Imperio Medio, 2055-1650 a.C. Incluye un cálculo aproximado del área de un círculo; interpretado en términos modernos, el resultado es equivalente a aproximar π por $256/81$. Aunque no está claro si en el antiguo Egipto reconocían una constante específica análoga a π .

En torno al 900 a. C., en su *Shatapatha Brahmana*, el astrónomo Yajnavalkya approximó a todos los efectos π con $339/108$.

Alrededor de 250 a. C., el griego clásico Arquímedes, uno de los más grandes matemáticos que jamás ha vivido y también un excelente ingeniero, probó, con todo el rigor lógico, que π es menor que $22/7$ y mayor que $223/71$.

Hacia 150 a. C., Ptolomeo approximó π con $377/120$.

Alrededor de 250 d. C., el matemático chino Liu Hui mostró que $\pi \approx 2927/1250$.

Podemos comparar estas aproximaciones calculando hasta cinco decimales de cada una de ellas:

Tabla 9

Número Aproximación a 5 decimales Error relativo

3,14159		
22/7	3,14285	4 % más mayor
25/8	3,12500	5 % más pequeño
256/81	3,16049	6 % más mayor
339/108	3,13888	8 % más pequeño
223/71	3,14084	2 % más pequeño
377/120	3,14166	0,2 % más mayor
3927/1250	3,14160	0,02 % más mayor

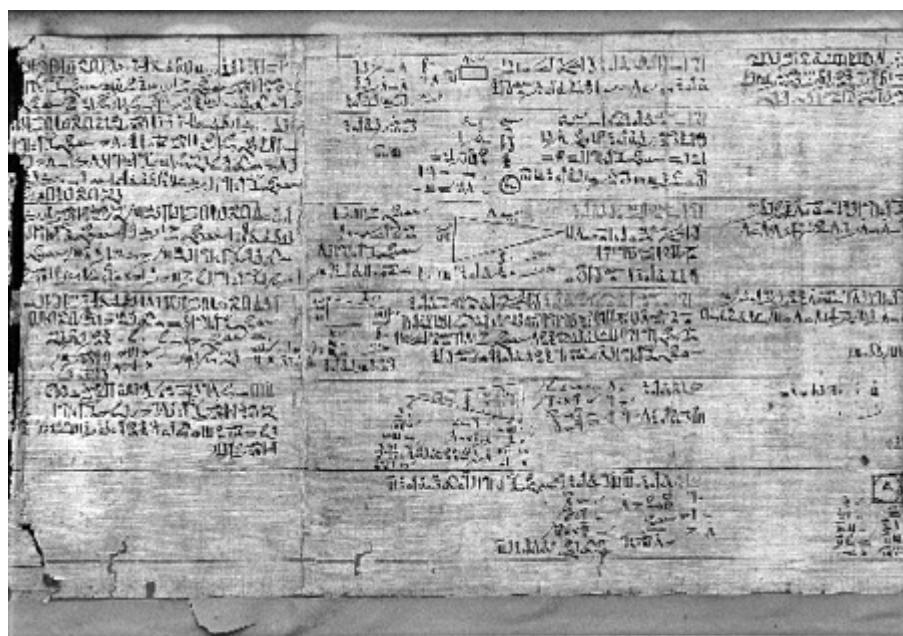


Figura 77. Parte del papiro de Rhind.

§. 466/885 Torres de Hanói

A primera vista, nadie diría que 466/885 es especial. Yo seguramente no lo diría, incluso después de haber hecho alguna investigación que conduce precisamente a ese número. Pero resulta estar íntimamente relacionado con un famoso rompecabezas, las Torres de Hanói, e incluso con una todavía más famosa forma, el triángulo de Sierpiński.

Mueve los discos

Las Torres de Hanói es un rompecabezas tradicional dado a conocer en 1883 por Lucas. Está formado por una serie de discos circulares de diferentes tamaños, colocados en tres estacas. Aquí consideraremos los tamaños como enteros positivos: $1, 2, 3, \dots, n$ y nos referiremos al juego como Hanói de n discos, aunque en los juegos que se comercializan suelen ser 5 ó 6.

Al principio los discos están todos en una única estaca, ordenados en modo decreciente de tamaño de abajo arriba. El objetivo del juego es mover todos los discos a una estaca diferente. Cada movimiento transfiere un disco de la cima de la pila a una nueva estaca. Sin embargo, un disco solo puede moverse de este modo si:

- disco sobre el cual se va a colocar es mayor, o
- la estaca no tenía ningún disco previamente.

La primera regla implica que cuando todos los discos se han transferido, de nuevo están colocados de modo que el tamaño es decreciente de abajo arriba.

Antes de seguir leyendo, deberías intentar resolver el rompecabezas. Empieza con dos discos y luego vete añadiendo hasta tener cinco o seis, dependiendo de lo ambicioso (y persistente) que seas.

Por ejemplo, puedes resolver Hanói de 2 discos tan solo en tres movimientos:

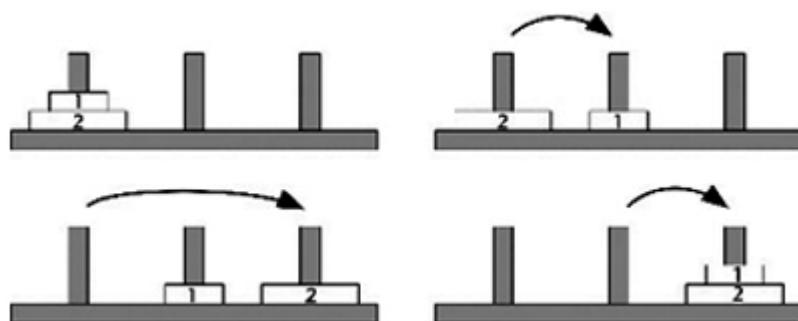


Figura 78. Resolviendo Hanói de 2 discos. Mueve el disco 1 al centro, luego mueve el disco 2 a la estaca de la derecha, después mueve el disco 1 a la estaca de la derecha.

¿Qué me dices de Hanói de 3 discos? Empieza así:

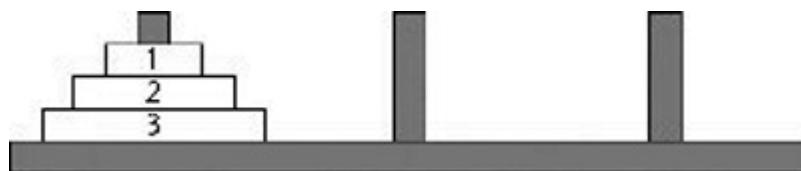


Figura 79. Posición inicial con 3 discos.

El primer movimiento básicamente se fuerza: el único disco que nos está permitido mover es el disco 1. Puede ir a cualquier de las otras dos estacas, no importa cuál escojamos, porque conceptualmente podemos intercambiar esas dos estacas sin que eso afecte al juego. De modo que, por ejemplo, movemos el disco 1 a la estaca central:

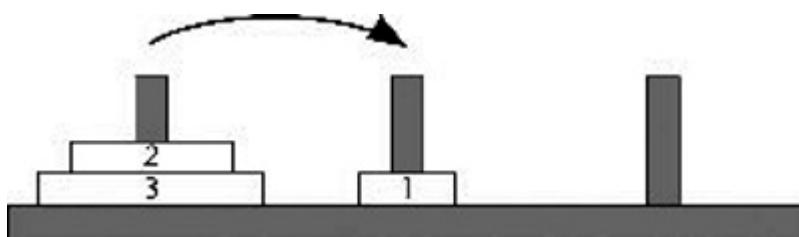


Figura 80. Primer movimiento.

En este punto, podemos mover el disco 1 de nuevo, pero con eso en realidad no avanzamos nada (o bien vuelve a donde empezó o se mueve a otra estaca vacía, a la cual podía haber ido directamente). De modo que tenemos que mover un disco diferente. No podemos mover el disco 3, ya que está bajo el disco 2, así que tenemos que mover el disco 2. Y no podemos poner el disco 2 sobre el disco 1. De modo que la única posibilidad es ponerlo en la estaca de la derecha:

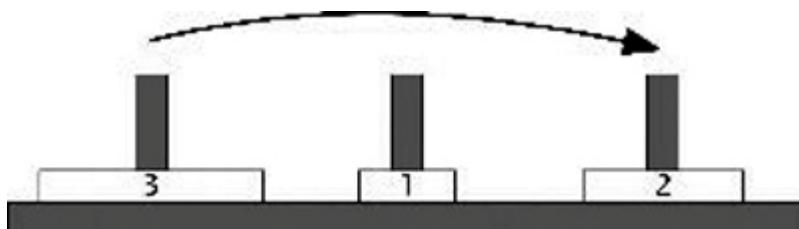


Figura 81. Segundo movimiento.

Ahora no podemos mover el disco 3, y sería tonto mover el disco 2 de nuevo. Así que movemos el disco 1. Si lo ponemos encima del disco 3, nos quedamos atascados y tenemos que deshacer el movimiento en el siguiente paso. De modo que solo hay una opción:

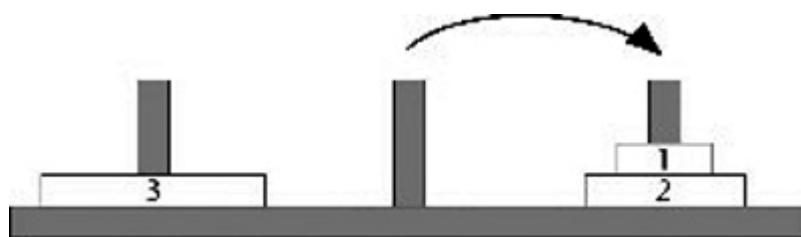


Figura 82. Tercer movimiento.

Ahora, ¿qué? O bien deshacemos ese movimiento o ponemos el disco 1 sobre el disco 3, lo que no parece que ayude mucho, o movemos el disco 3 a la estaca vacía:

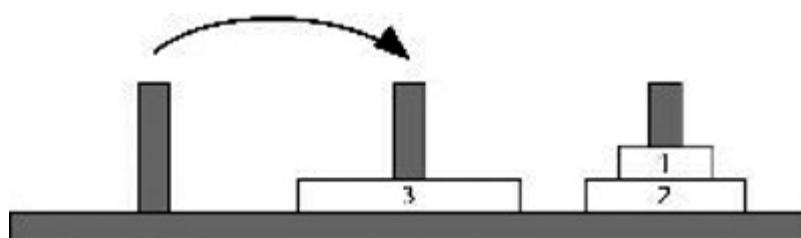


Figura 83. Cuarto movimiento.

En este punto, ya hemos recorrido un largo camino hacia la resolución del rompecabezas, porque hemos movido el disco más difícil, el disco 3,

a una nueva estaca. Obviamente, todo lo que tenemos que hacer ahora es poner los discos 1 y 2 sobre él. Además, *sabemos cómo hacerlo*. Ya hemos movido la pila formada por los discos 1 y 2 a una nueva estaca. Así que basta reproducir los movimientos, teniendo cuidado de escoger las estacas correctas:

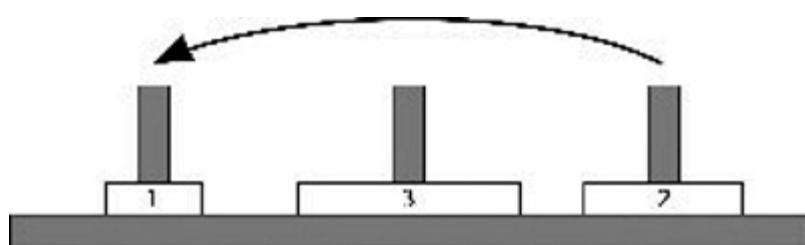


Figura 84. Quinto movimiento.

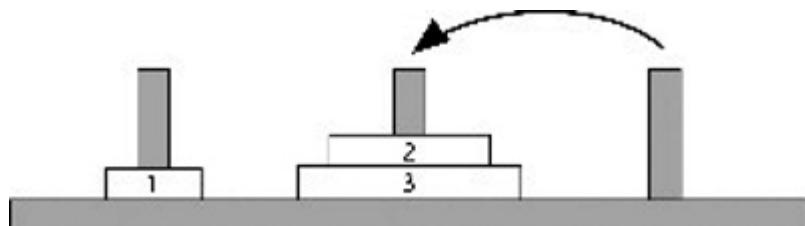


Figura 85. Sexto movimiento.

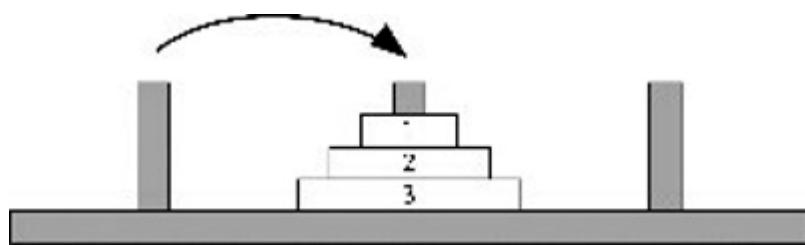


Figura 86. Séptimo movimiento.

¡Hecho!

Hemos resuelto Hanói mediante siete movimientos, que es $2^3 - 1$. Puede probarse que no es posible solucionarlo con menos movimientos. El método sugiere una solución ingeniosa para cualquier número de discos. Podemos resumirlo así:

- Primero mueve los dos discos que están encima a una estaca vacía.
- Luego mueve el disco mayor a la única estaca que queda vacía.
- Luego mueve los dos discos iniciales a la estaca que contiene el disco mayor.

El primer y el último paso de hecho son soluciones de Hanói de 2 discos. El paso intermedio es totalmente directo. La misma idea ahora resuelve el Hanói de 4 discos.

- Primero mueve los tres discos que están encima a una estaca vacía.
- Luego mueve el disco mayor a la única estaca que queda vacía.
- Luego mueve los tres discos iniciales a la estaca que contiene el disco mayor.

El primer y el último paso son la solución de Hanói de 3 discos, que acabamos de explicar. De nuevo, el paso intermedio es totalmente directo. La misma idea puede ahora aplicarse a Hanói de 5 discos, Hanói de 6 discos, etcétera. Podemos resolver el rompecabezas para *cualquier* número de discos, usando un procedimiento «recursivo» en el cual la solución para un número de discos dado se obtiene a partir de la solución de esa cantidad de discos eliminando uno. De modo que resolver Hanói

de 5 discos se reduce a resolver Hanói de 4 discos, el cual se reduce a resolver Hanói de 3 discos, el cual a su vez se reduce a resolver Hanói de 2 discos, el cual se reduce a resolver Hanói de 1 disco. Y este es fácil, basta coger el disco y colocarlo en una estaca diferente.

El método funciona del siguiente modo (para resolver Hanói de n discos):

- De momento ignora el disco más grande n .
- Usa la solución de Hanói de $(n - 1)$ discos para transferir los discos $1, 2, \dots, n - 1$ a una nueva estaca.
- Luego mueve el disco n a la estaca que queda vacía.
- Finalmente, usa la solución de Hanói de $(n - 1)$ discos *de nuevo* para transferir los discos $1, 2, \dots, n - 1$ a la estaca que contiene el disco n . (Observa que, por simetría, la estaca objetivo puede escogerse de cualquiera de las dos posibilidades cuando se invoca la solución de Hanói de $(n - 1)$ discos.)

El diagrama de estado

Los procedimientos recursivos pueden volverse muy complicados si se siguen paso a paso, y eso es lo que ocurre para las Torres de Hanói. Esta complejidad es inherente al rompecabezas, no solo en el método de la solución. Para ver por qué, representaré el rompecabezas geométricamente dibujando su *diagrama de estado*, que consiste en nodos que representan posibles posiciones de los discos, unidos por

líneas que representan movimientos permitidos. Para Hanói de 2 discos, el diagrama de estado tiene el aspecto que aparece en la Figura.

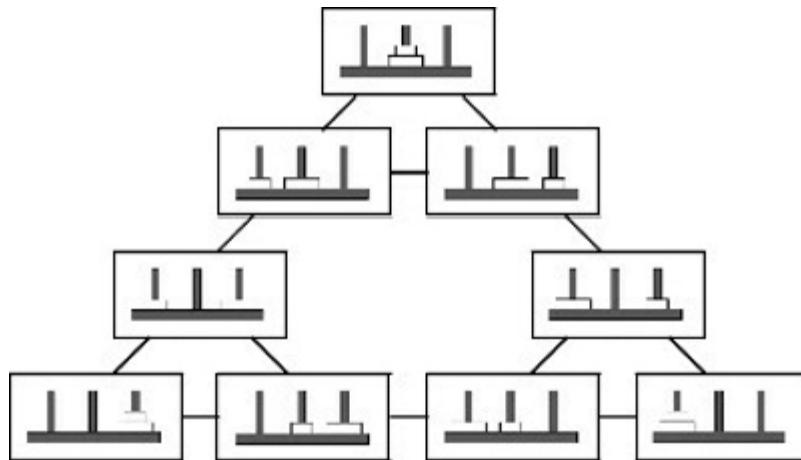


Figura 87. Diagrama de estado de Hanói de 2 discos.

Este diagrama puede verse como tres copias del diagrama correspondiente para el Hanói de 1 disco, unidas en tres lugares. En cada copia, el disco de abajo está en una posición fija, en una de las tres posibles estacas. Las uniones aparecen cuando una estaca vacía permite al disco de abajo moverse. Varios matemáticos observaron por separado que la solución recursiva del rompecabezas aparece en la estructura del diagrama de estado. Los primeros parecen haber sido R. S. Scorer, P. M. Grundy y Cedric A. B. Smith, que escribieron un artículo conjunto en 1944.

Podemos usar la solución recursiva para predecir el diagrama de estado cuando hay más discos. Para Hanói de 3 discos, haz tres copias del diagrama superior, cada una con un disco extra en la parte de abajo y

únelas formando un triángulo. Y así sucesivamente. La Figura 88 muestra el diagrama de estado para Hanói de 5 discos, omitiendo las posiciones de los discos:

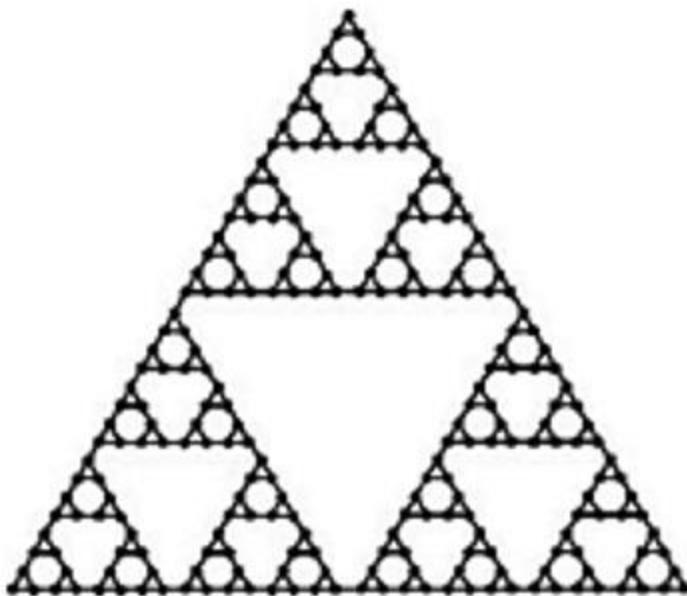


Figura 88. Diagrama de estado para Hanói de 5 discos.

H. T. Chan (1989) y Andreas Hinz (1992) usaron la estructura recursiva del diagrama de estado para obtener una fórmula para el número mínimo medio de movimientos entre los estados en Hanói de n discos. El número total de movimientos por las rutas más cortas, entre todos los pares posibles de posiciones, resulta ser:

$$\begin{aligned} & \frac{466}{885} 18^n - \frac{1}{3} 9^n - \frac{3}{5} 3^n + \left(\frac{12}{59} + \frac{18}{1.003} \sqrt{17} \right) \left(\frac{5 + \sqrt{17}}{2} \right)^n \\ & + \left(\frac{12}{59} - \frac{18}{1.003} \sqrt{17} \right) \left(\frac{5 - \sqrt{17}}{2} \right)^n \end{aligned}$$

Para n grande, esto es aproximadamente:

$$\left(\frac{466}{885}\right)18^n$$

porque todos los demás términos en la fórmula son mucho más pequeños que el primero. La longitud media de todas estas rutas es aproximadamente $\frac{466}{885}$ veces el número de movimientos a lo largo de un lado del diagrama de estado. Veamos ahora el significado de la extraña fracción $\frac{466}{885}$

Triángulo de Sierpiński

La misma fracción aparece en un problema muy relacionado. Hinz y Andreas Schief usaron la fórmula para el número medio de movimientos entre estados en la Torre de Hanói para calcular la distancia media entre dos puntos en una famosa figura conocida como el «triángulo de Sierpiński». Si los lados del triángulo tienen longitud 1, entonces la respuesta, por increíble que parezca, es exactamente $\frac{466}{885}$

El triángulo de Sierpiński se forma a partir de un triángulo equilátero, dividiéndolo en cuatro triángulos de la mitad de tamaño (el que se queda en el centro está invertido) y eliminando el triángulo del centro. Entonces se repite el mismo proceso en los tres triángulos equiláteros más pequeños que quedan y se continúa así indefinidamente. El resultado es

un ejemplo temprano de lo que ahora llamamos «fractal»: una forma que tiene una estructura intrincada, no importa cuánto se amplíe [véase $\log^3/\log 2$].



Figura 89. Las primeras seis etapas en la formación de un triángulo de Sierpiński.

El matemático polaco Wacław Sierpiński inventó este fascinante conjunto en 1915, aunque siglos antes ya se usaban formas parecidas con carácter decorativo. Lo describió como «simultáneamente cantoriana y jordaniana, en la que cada punto es un punto de ramificación». Con «cantoriana», Sierpiński quería decir que su conjunto estaba todo en una única pieza pero con una estructura intrincada. Con «jordaniana», quería decir que era una curva. Y con «cada punto es un punto de ramificación», quería decir que se cruzaba consigo misma en cada punto. Más tarde, Benoît Mandelbrot en broma le llamó la «junta» de Sierpiński por su parecido a la junta agujereada que une la culata al resto del motor.

Números irracionales

Contenido:

- §. Primer irracional conocido
- §. Medida de circunferencia
- §. Número de oro
- §. Logaritmos naturales
- §. Fractales
- §. Empaquetamiento de esferas
- §. Escala musical
- §. Constante de Apéry
- §. Constante de Euler

Las fracciones sirven para cualquier problema práctico de divisiones, y durante un tiempo, en la antigua Grecia, estuvieron convencidos de que las describían todo en el universo.

Entonces alguien investigó las consecuencias del teorema de Pitágoras y se preguntó cómo la diagonal de un cuadrado se relaciona con su lado.

La respuesta indicó que había algunos problemas que las fracciones no podían resolver.

Así nacieron los números irracionales. Juntos, los números racionales y los irracionales, forman el sistema de los números reales.

§. Primer irracional conocido $\sqrt{2} \approx 1,414213$

Los números racionales, las fracciones, resuelven la mayoría de los problemas prácticos, aunque algunos no tienen solución racional. Por ejemplo, los geómetras griegos descubrieron que la diagonal de un cuadrado de lado 1 no es un número racional. Si la diagonal tiene longitud x , entonces el teorema de Pitágoras afirma que:

$$x^2 = 1^2 + 1^2 = 2$$

de modo que $x = \sqrt{2}$. Para su disgusto, probaron que este resultado no es racional.

Esto llevó a los geómetras griegos a centrarse en longitudes geométricas e ignorar números. La mejor alternativa fue fortalecer el sistema numérico para que pueda hacer frente a este tipo de problemas.

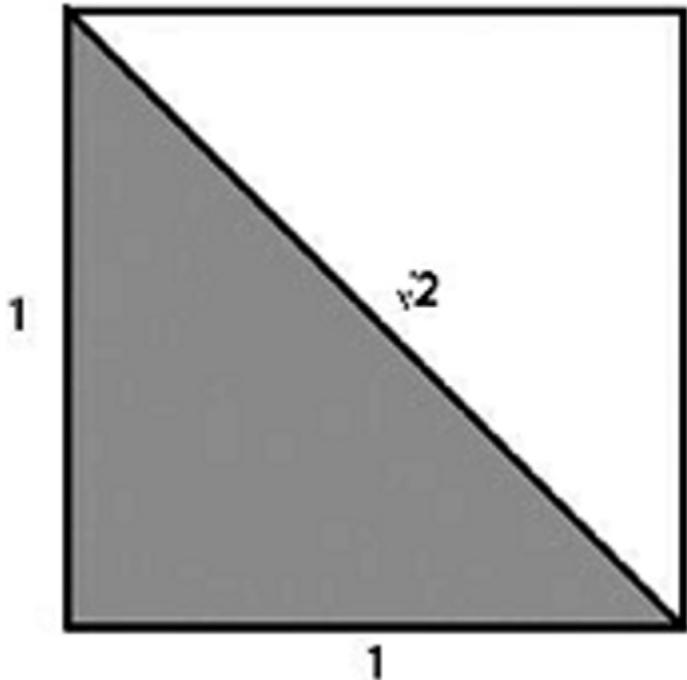


Figura 90. La diagonal de un cuadrado unidad.

Decimales, fracciones y números irracionales

En la actualidad, solemos escribir los números como decimales. Por razones prácticas, las calculadoras usan decimales finitos, los cuales tienen un número limitado de dígitos tras la coma decimal. En el capítulo inicial vimos que la diagonal del cuadrado unidad hasta diez dígitos decimales es:

$$\sqrt{2} = 1,4142135623$$

Sin embargo, un cálculo muestra que:

$$(1,4142135623)^2 = 1,99999999979325598129$$

exactamente. Aunque esto se aproxima a 2, no es igual a él.

Quizá dejamos de calcular demasiado pronto. Quizá un millón de dígitos darían un valor exacto de la raíz cuadrada de 2. En realidad, hay un modo muy sencillo de ver que esto no funcionará. La aproximación decimal de diez cifras acaba en 3. Cuando se eleva al cuadrado, obtenemos un decimal de 20 cifras acabado en 9, que es 3^2 . Esto no es una coincidencia: se debe al modo en que multiplicamos los decimales. La última cifra significativa de cualquier número decimal, diferente del 0, no es cero. De modo que su cuadrado acaba con una cifra distinta de cero. Como la expresión decimal de 2 es 2,000...con solo ceros, ningún cuadrado puede ser *exactamente* igual a 2.

Todos los números decimales en una calculadora son racionales. Por ejemplo, el valor de π con diez cifras decimales es 3,141592653 y esto es *exactamente* igual a la fracción:

$$3.141\overline{592.653}/1.000.000.000$$

Decimales de longitud fija representan un conjunto bastante limitado de fracciones, aquellas en las que el denominador (el número de la parte de abajo) es una potencia de 10. Otras fracciones son más complicadas en este sentido. Si tecleo $1/3$ en mi calculadora, aparece 0,333333333. En

realidad esto no es correcto del todo, pues si multiplicamos por 3, obtenemos $1 = 0,999999999$, que no es verdad, pues la diferencia es $0,0000000001$. Pero ¿quién se preocupa de una parte en 10.000 millones?

La respuesta depende de para qué lo quieras. Si estás haciendo una estantería y quieres cortar una placa de un metro de largo en tres partes iguales, entonces 0,333 metros (333 milímetros) es lo suficiente preciso. Pero si estás probando un teorema matemático y buscas que multiplicar 3 por $\frac{1}{3}$ sea 1, como tiene que ser, entonces incluso un pequeño error puede ser fatal. Si quieres expresar $\frac{1}{3}$ como un decimal con una precisión total, esos 3 tienen que continuar infinitamente.

Las cifras de $\sqrt{2}$ también continúan de manera infinita, pero no hay un patrón claro. Lo mismo se aplica para las cifras de π . Sin embargo, si quieres representar la longitud que aparece en geometría usando números, tienes que encontrar una representación numérica para cosas como $\sqrt{2}$ y π . El resultado fue el sistema que ahora llamamos «números reales». Pueden representarse mediante expresiones decimales infinitamente largas. En matemáticas avanzadas se usan métodos más abstractos.

El adjetivo «real» surge porque estos números encajan con nuestra idea intuitiva de medida. Cada posición decimal extra hace la medida más precisa. Sin embargo, el mundo real se vuelve un poco borroso si bajamos al nivel de las partículas fundamentales, de modo que los

decimales pierden contacto con la realidad alrededor de la decimoquinta posición decimal. Hemos abierto la caja de Pandora. Los objetos y estructuras matemáticas son (como mucho) *modelos* del mundo real, no la propia realidad. Si consideramos decimales que continúan infinitamente, el sistema numérico real es claro y ordenado; de modo que podemos hacer que las matemáticas los usen y luego comparar los resultados con la realidad, si es que ese es nuestro principal objetivo. Si queremos que los decimales se detengan después de cincuenta posiciones, o hacerlo todo algo confuso, obtenemos un complicado desorden. Hay siempre una compensación entre la conveniencia matemática y la precisión física.

Todo número racional es real. De hecho (no haré la prueba, pero no es demasiado difícil), las expresiones decimales de los números racionales son precisamente aquellas que se *repiten*. Esto es, repiten el mismo bloque finito de cifras infinitamente, quizá con algunas cifras diferentes al inicio. Por ejemplo:

$$137/42 = 3,2619047619047\dots$$

con un bloque inicial que es la excepción 3,2 y luego repeticiones indefinidas de 619047.

Sin embargo, muchos números reales no son racionales. Cualquier decimal que evite esas repeticiones sería un ejemplo. Así, puedo estar seguro de que

$$1,101001000100001000001\dots$$

con tramos que van incrementando su longitud de 0, no es racional. El término que se aplica a esos números es «irracional». Todo número real es o bien racional o bien irracional.

Prueba de que $\sqrt{2}$ es irracional

Todos los decimales finitos son fracciones, pero muchas fracciones no son decimales finitos. ¿Podría una de estas representar a $\sqrt{2}$ de modo exacto? Si la respuesta hubiese sido «sí», todo el cuerpo de trabajo griego sobre longitudes y áreas hubiese sido mucho más simple. Sin embargo, los griegos descubrieron que la respuesta es «no». No lo hicieron usando decimales, lo hicieron geométricamente.

Ahora vemos esto como una revelación importante, que abre un área vasta de nuevas y útiles matemáticas, pero en su momento fue algo vergonzoso. El descubrimiento se remonta a los pitagóricos, quienes creían que el universo estaba basado en los números. Al decir «números» pensaban en los números enteros y las fracciones. Por desgracia, uno de ellos, supuestamente Hipaso de Metaponto, descubrió que la diagonal de

un cuadrado unidad es irracional. Según se dice, anunció este hecho molesto mientras se celebrada una fiesta de pitagóricos en un bote en medio del mar, y los demás se pusieron tan furiosos que lo arrojaron por la borda y se ahogó. No hay evidencias históricas de este hecho, pero es muy probable que el descubrimiento no les gustara nada, ya que contradecía el núcleo de sus creencias.

La prueba griega emplea un proceso geométrico que ahora llamamos «algoritmo de Euclides». Es un modo sistemático de encontrar si dos longitudes dadas, a y b , son *commensurables* (ambas múltiplos enteros de alguna longitud común c). Si lo son, obtenemos el valor de c . Desde el punto de vista numérico actual, a y b son commensurables si y solo si a/b es racional, de modo que el algoritmo de Euclides es «realmente» una prueba para decidir si un número dado es racional.

El punto de vista geométrico griego los llevó a razonar de modo bastante diferente, según las siguientes pautas. Supongamos que a y b son múltiplos enteros de c . Por ejemplo, quizá $a = 17c$ y $b = 5c$. Dibuja una cuadrícula de 17×5 , con cada cuadrado de tamaño c . Observa que a lo largo de la parte de arriba, tendríamos a , que está compuesto por 17 copias de c ; y hacia abajo por un lado, b , que está compuesto de 5 copias de c . De modo que a y b son commensurables.

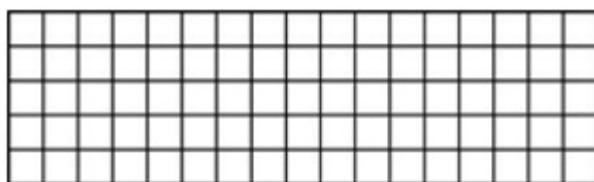
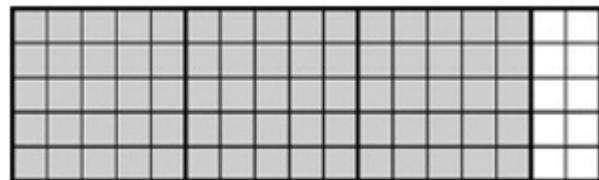
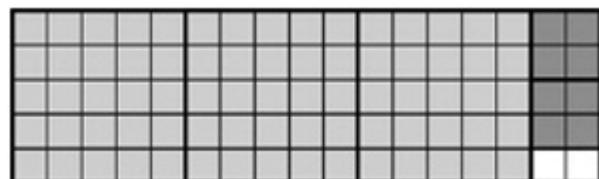


Figura 91. Cuadrícula 17×5 .

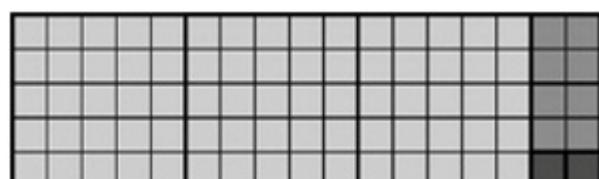
Luego corta tantos cuadrados de 5×5 como puedas.

*Figura 92. Corte de tres cuadrados de 5×5 .*

Esto deja un rectángulo de 2×5 . Repite el proceso en este rectángulo más pequeño, ahora con cuadrados de 2×2 .

*Figura 93. Luego corta dos cuadrados de 2×2 .*

lo que nos deja un rectángulo de 2×1 . Corta este en cuadrados de 1×1 , y no hay ningún rectángulo minúsculo restante, encaja perfectamente.

*Figura 94. Finalmente, corta dos rectángulos de 1×1 .*

Si las longitudes originales a y b son enteros múltiplos de una longitud común c , llega un momento en el que el proceso se acaba, porque todas las líneas están en la cuadrícula y los rectángulos se van haciendo más pequeños. A la inversa, si el proceso se detiene, entonces, trabajando hacia atrás, a y b son múltiplos enteros de c . En resumen: dos longitudes son commensurables si y solo si el algoritmo de Euclides, aplicado al rectángulo correspondiente, se detiene después de un número finito de pasos.

Si queremos probar que cierto par de longitudes es incommensurable, tan solo tenemos que confeccionar un rectángulo para el cual el proceso obviamente *no* se detenga. Para lidiar con $\sqrt{2}$, el truco es empezar con un rectángulo cuya forma se escoge para asegurar que, tras cortar *dos* cuadrados grandes, obtenemos una pieza restante que tiene exactamente las mismas proporciones que el original. Si es así, el algoritmo de Euclides estará cortando dos cuadrados infinitamente, de modo que nunca se detiene.

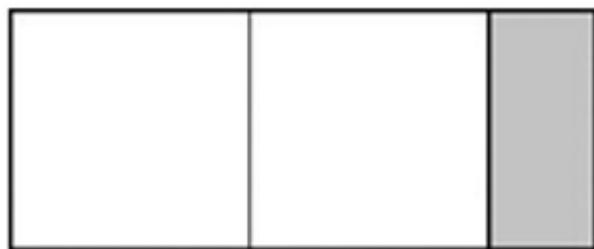


Figura 95. Haz el rectángulo sombreado con las mismas proporciones que el original.

Los griegos construyeron ese rectángulo geométricamente, pero nosotros podemos usar álgebra. Establece que los lados son a y 1. Entonces la condición necesaria es:

$$\frac{a}{1} = \frac{1}{a-2}$$

De modo que $a^2 - 2a = 1$, de donde $(a - 1)^2 = 2$, por lo tanto $a = 1 + \sqrt{2}$. Resumiendo, el algoritmo de Euclides implica que las longitudes $1 + \sqrt{2}$ y 1 son incommensurables, por lo que $1 + \sqrt{2}$ es irracional.

Luego $\sqrt{2}$ es también irracional. Para ver por qué, asume que $\sqrt{2}$ es un racional igual a p/q . Entonces $1 + \sqrt{2} = (p-q)/q$, el cual es racional. Pero no lo es, así que hemos llegado a una contradicción y nuestra suposición es falsa.

§. Medida de la circunferencia. $\Pi \approx 3,141592$

Los números que usamos para contar se convierten rápidamente en familiares, pero algunos números son mucho más extraños. El primer número ciertamente inusual con el cual nos encontramos cuando aprendemos matemáticas es. Este número surge en muchas otras áreas de matemáticas, no todas ellas relacionadas con las circunferencias. Los matemáticos han calculado más de 12 billones de cifras decimales de π . ¿Cómo lo han hecho? Comprender qué tipo de número es π resuelve la

antigua pregunta de si es posible hacer la cuadratura del círculo con regla y compás.

Razón de la circunferencia respecto a su diámetro

Nos encontramos con π por primera vez cuando calculamos la longitud de una circunferencia y el área de un círculo. Si el radio es r entonces la longitud de la circunferencia es $2\pi r$ y el área del círculo es πr^2 . Geométricamente, estas dos cantidades no están directamente relacionadas, de modo que es bastante destacable que el *mismo* número π aparezca en ambas. Hay una manera intuitiva de ver por qué sucede esto. Corta el círculo en un montón de secciones, como una *pizza*, y reordénalas para formar algo parecido a un rectángulo. El ancho de este rectángulo es aproximadamente la mitad de la circunferencia, es decir πr . Su altura es aproximadamente r . De modo que su área es aproximadamente $\pi r \times r = \pi r^2$.

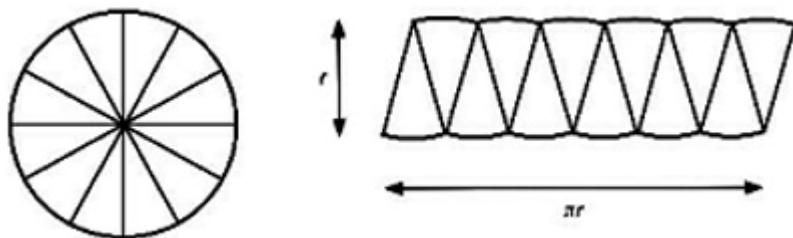


Figura 96. Aproximación del área del círculo.

Aunque esto es tan solo una aproximación. Tal vez los números que aparecen en conexión con la longitud de la circunferencia y con el área del círculo sean muy similares, pero no idénticos. Sin embargo, esto

parece poco probable, porque el razonamiento funciona, con independencia de lo finas que hagamos las secciones. Si usamos un número enorme de piezas muy finas, la aproximación se hace sumamente precisa. De hecho, al permitir que el número de piezas se haga tan grande como queramos, la diferencia entre la forma real y un verdadero rectángulo se hace tan pequeña como queramos. Usando los límites matemáticos, esta observación proporciona una prueba de que la fórmula para el área es correcta y exacta. Esto es por lo que el mismo número aparece tanto para la longitud de la circunferencia como para el área del círculo.

El procedimiento del límite también *define* qué queremos decir por área en este contexto. Las áreas no son tan sencillas como imaginamos. Las áreas de los polígonos pueden definirse cortándolas en triángulos, pero las formas con aristas curvas no pueden dividirse de esa manera. Incluso el área de un rectángulo no es sencilla si sus lados son incommensurables. El problema no es establecer qué *es* el área, para lo cual basta multiplicar los dos lados. La parte difícil es probar que el resultado se comporta del modo en que debería hacerlo un área, por ejemplo, que cuando unes formas, se suman sus áreas. Las matemáticas escolares pasan de puntillas por estos problemas y esperan que nadie se dé cuenta.

¿Por qué los matemáticos usan un símbolo extraño para representar un número? ¿Por qué no escribir directamente el número? En la escuela podrían decir que $\pi = 22/7$, pero un profesor cuidadoso explicará que

esto es solo una aproximación [véase 22/7]. Así que, ¿por qué no usar una fracción exacta para π ?

No hay una. El número π es el ejemplo más conocido de número irracional.

Como $\sqrt{2}$, no puede representarse de manera exacta por ninguna fracción, por muy complicada que sea. Es muy difícil probar esto, pero los matemáticos saben cómo hacerlo y resulta cierto. Así que definitivamente necesitamos un símbolo nuevo, porque este número en concreto no puede escribirse exactamente usando los símbolos habituales de los números. Como π es uno de los números más importantes en todas las matemáticas, necesitamos una manera inequívoca para referirnos a él. Es la «p» griega, la primera letra de «perímetro».

La verdad es que el universo nos hace una jugarreta bastante cruel al no poder escribir un número de vital importancia, excepto usando fórmulas complicadas. Es un fastidio, quizá, pero fascinante, que se añade a la mística de π .

π y las circunferencias

Al principio encontramos π en conexión con las circunferencias. Las circunferencias son formas matemáticas muy básicas, de modo que cualquier cosa que nos diga sobre las circunferencias debe merecer la pena tenerla en cuenta. Las circunferencias tienen muchas aplicaciones útiles. En 2011, el número de circunferencias usadas en tan solo una

característica de la vida diaria era más de 5.000 millones, porque el número de coches que pasaban un punto de referencia era 1.000 millones, y en esa época un coche típico tenía cinco ruedas, cuatro en uso más una de repuesto (en la actualidad, con frecuencia la de repuesto es un kit de reparación de pinchazos, que ahorra gasolina y es más barato de hacer). Por supuesto hay muchas otras circunferencias en un coche, que van desde las arandelas al volante. Por no mencionar ruedas de bicicletas, camiones, autobuses, trenes, aviones...

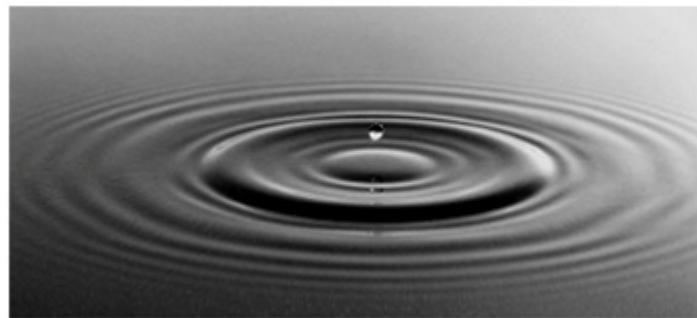


Figura 97. Ondas.



Figura 98. Arcoíris, arco de una circunferencia.

Las ruedas son solo una aplicación de la geometría de la circunferencia, que funcionan porque todo punto de la circunferencia se encuentra a la misma distancia del centro. Si giras una rueda circular alrededor de su centro, puede rodar con fluidez a lo largo de una carretera llana. Pero las circunferencias aparecen de muchos otros modos; las ondas en un lago son circulares y también los arcos de colores del arcoíris. Las órbitas de los planetas son, en una primera aproximación, circunferencias. De forma más precisa son elipses, una especie de circunferencias que han sido aplastadas en una dirección.

Sin embargo, los ingenieros pueden diseñar ruedas sin ningún conocimiento de π . Su verdadera importancia es teórica y es mucho más profunda. Los matemáticos se encontraron por primera vez con π en una ecuación básica sobre circunferencias. El tamaño de una circunferencia puede describirse usando tres números muy relacionados:

- su *radio*: la distancia del centro a cualquier punto en la circunferencia
- su *diámetro*: el ancho máximo de una circunferencia
- su *longitud*: la longitud de la propia circunferencia midiendo su perímetro.

El radio y el diámetro están relacionados de un modo muy sencillo: el diámetro es dos veces el radio y el radio es la mitad del diámetro.

La relación entre la longitud y el diámetro no es tan directa. Si dibujas un hexágono dentro de la circunferencia, puedes convencerte a ti mismo de que la longitud de la circunferencia es un poco mayor que tres veces el diámetro. La imagen muestra seis radios, que se usan por parejas para formar tres diámetros. El hexágono tiene el mismo perímetro que seis radios, es decir, tres diámetros. Y la circunferencia es claramente un poco más grande que el hexágono.

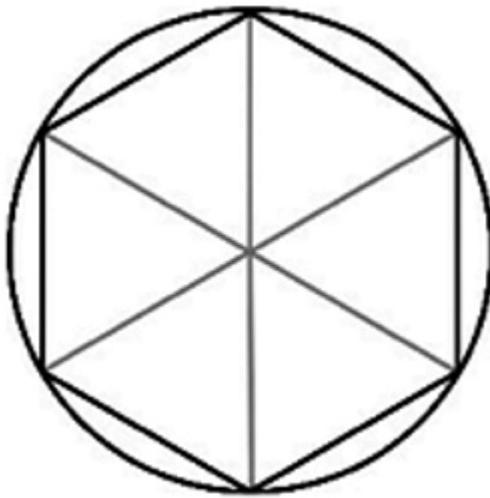


Figura 99. Por qué π es más grande que 3.

El número π se *define* como la longitud de cualquier circunferencia dividida entre su diámetro. Cualquiera que sea el tamaño de la circunferencia, esperamos que este número tenga el mismo valor, porque la longitud y el diámetro mantienen la misma proporción aunque

aumentes o disminuyas la circunferencia. Hace unos 2.200 años, Arquímedes elaboró una prueba completamente lógica de que el mismo número funciona para cualquier circunferencia.

Al pensar en los hexágonos dentro de la circunferencia, y doblar el número de lados de 6 a 12, luego 24, luego 48 y finalmente 96 lados, Arquímedes también obtuvo un valor bastante preciso para π . Probó que es mayor que $3\frac{10}{71}$ y menor que $3\frac{1}{7}$. En decimales, estos dos valores son 3,141 y 3,143. (Arquímedes trabajó con figuras geométricas, no con números reales y pensó en lo que ahora llamamos π en términos geométricos, de modo que esto es una moderna reinterpretación de lo que en realidad hizo. Los griegos no tenían notación decimal.)

El método de Arquímedes para calcular π puede hacerse tan preciso como queramos, para ello doblamos el número de lados del polígono usado y aproximamos la longitud de la circunferencia el número de veces que consideremos oportuno. Matemáticos posteriores encontraron métodos mejores (discutiremos algunos de ellos a continuación). El número π con 1.000 cifras decimales es:

3, 141 592 653 589 793 238 462 643 383 279 502 884 197 169 399 375
105 820 974 944 592 307 816 406 286 208 998 628 034 825 342 117
067 982 148 086 513 282 306 647 093 844 609 550 582 231 725 359
408 128 481 117 450 284 102 701 938 521 105 559 644 622 948 954
930 381 964 428 810 975 665 933 446 128 475 648 233 786 783 165
271 201 909 145 648 566 923 460 348 610 454 326 648 213 393 607

260 249 141 273 724 587 006 606 315 588 174 881 520 920 962 829
254 091 715 364 367 892 590 360 011 330 530 548 820 466 521 384
146 951 941 511 609 433 057 270 365 759 591 953 092 186 117 381
932 611 793 105 118 548 074 462 379 962 749 567 351 885 752 724
891 227 938 183 011 949 129 833 673 362 440 656 643 086 021 394
946 395 224 737 190 702 179 860 943 702 770 539 217 176 293 176
752 384 674 818 467 669 405 132 000 568 127 145 263 560 827 785
771 342 757 789 609 173 637 178 721 468 440 901 224 953 430 146
549 585 371 050 792 279 689 258 923 542 019 956 112 129 021 960
864 034 418 159 813 629 774 771 309 960 518 707 211 349 999 998
372 978 049 951 059 731 732 816 096 318 595 024 459 455 346 908
302 642 522 308 253 344 685 035 261 931 188 171 010 003 137 838
752 886 587 533 208 381 420 617 177 669 147 303 598 253 490 428
755 468 731 159 562 863 882 353 787 593 751 957 781 857 780 532
171 226 806 613 001 927 876 611 195 909 216 420 199.

Observando estos números, la característica más llamativa es la completa ausencia de cualquier patrón. Las cifras parecen aleatorias. Pero no pueden serlo, porque son las cifras de π y este es un número concreto. La carencia de patrón proporciona un fuerte indicio de que π es un número extraño. Los matemáticos sospechan con gran convicción que toda secuencia finita de cifras aparece en alguna parte (es más, con muchísima frecuencia) en la expresión decimal de π . De hecho, se cree

que π es un número *normal*, con lo cual se quiere decir que todas las secuencias de una longitud dada aparecen con la misma frecuencia. Estas conjeturas no han sido ni probadas ni refutadas.

Otros hechos sobre π

El número π se presenta en muchas otras áreas de matemáticas, a menudo sin tener una conexión obvia con las circunferencias. Hay siempre una conexión indirecta, porque de ahí es de donde proviene π y una de las maneras de definirlo. Cualquier otra definición tiene que dar el mismo número, de modo que en algún punto a lo largo del razonamiento tiene que probarse un vínculo con las circunferencias. Pero esto puede ser de manera *muy* indirecta.

Por ejemplo, en 1748, Euler observó una conexión entre los números π , e , i (la raíz cuadrada de menos 1 [véase e]). En concreto, la elegante fórmula:

$$e^{i\pi} = -1$$

Euler también observó que π aparece cuando sumamos ciertas series infinitas. En 1735, resolvió el problema de Basilea, una cuestión planteada por Pietro Mengoli en 1644: encontrar la suma de los inversos de todos los cuadrados; esto es una serie infinita, porque hay infinidad de cuadrados. Muchos de los grandes matemáticos de la época intentaron

resolverlo, sin conseguirlo. En 1735, Euler descubrió la maravillosamente sencilla respuesta.

$$\frac{\pi^2}{6} = \frac{1}{1^2} + \frac{1}{2^2} + \frac{1}{3^2} + \frac{1}{4^2} + \frac{1}{5^2} + \dots$$

Este descubrimiento inmediatamente le hizo famoso entre los matemáticos. ¿Puedes indicar el vínculo con las circunferencias? No, yo tampoco puedo. No puede ser increíblemente obvio porque muchos de los mejores matemáticos no pudieron resolver el problema de Basilea. Sorprendentemente pasa por usar la función seno, que a primera vista parece no tener conexión con el problema.

El método de Euler nos lleva a resultados parecidos para potencias cuartas, sextas y en general cualquier potencia par. Por ejemplo:

$$\frac{\pi^4}{90} = \frac{1}{1^4} + \frac{1}{2^4} + \frac{1}{3^4} + \frac{1}{4^4} + \frac{1}{5^4} + \dots$$

$$\frac{\pi^6}{945} = \frac{1}{1^6} + \frac{1}{2^6} + \frac{1}{3^6} + \frac{1}{4^6} + \frac{1}{5^6} + \dots$$

Es también posible usar solo denominadores pares o impares:

$$\frac{\pi^2}{24} = \frac{1}{2^2} + \frac{1}{4^2} + \frac{1}{6^2} + \frac{1}{8^2} + \frac{1}{10^2} + \dots$$

$$\frac{\pi^2}{8} = \frac{1}{1^2} + \frac{1}{3^2} + \frac{1}{5^2} + \frac{1}{7^2} + \frac{1}{9^2} + \dots$$

Sin embargo, no se han probado fórmulas parecidas para potencias impares, como cubos o potencias de cinco, y existe la conjetura de que no existen [véase $\zeta(3)$].

Sorprendentemente, esta serie y las relacionadas tienen profundas conexiones con los primos y la teoría de números. Por ejemplo, si escoges dos números naturales aleatoriamente, entonces la probabilidad de que no tengan un factor común (mayor que 1) es $6/\pi^2 \approx 0,6089$, el inverso de la suma de la serie de Euler.

Otra aparición inesperada de π se da en estadística. El área bajo la famosa «campana de Gauss», con ecuación $y = e^{-x^2}$, es exactamente $\sqrt{\pi}$.

En muchas fórmulas en física matemática aparece involucrado π . Algunas de ellas aparecen más abajo en la lista de fórmulas que contienen π . Los matemáticos han descubierto una variedad enorme de ecuaciones en las que π se presenta de forma destacada; algunas se tratan a continuación.

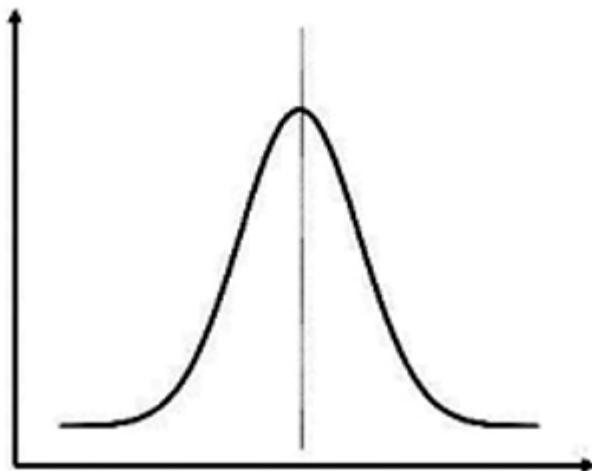


Figura 100. La campana de Gauss.

Cómo calcular π

En 2013, durante un período de 94 días, Shigeru Kondo usó un ordenador para calcular π con 12.100.000.000.050 cifras decimales, más de 12 billones. Los usos prácticos de π no necesitan este nivel de precisión y no se puede obtener midiendo circunferencias físicas. A lo largo de los años se han usado varios métodos diferentes, todos basados en fórmulas para π o procesos que ahora expresamos como fórmulas.

Dos buenas razones para llevar a cabo esos cálculos son ver cómo responden de bien estas fórmulas y probar ordenadores nuevos. Pero la principal razón, en realidad, es la tentación de batir récords. Unos cuantos matemáticos se sienten fascinados con calcular todavía más cifras de π porque, al igual que ocurre con las montañas y los alpinistas, «están ahí». Las actividades como esta para batir récords no son típicas de la mayoría de la investigación matemática y tienen poca importancia o valor práctico por sí mismas, pero han llevado a fórmulas totalmente

nuevas y fascinantes y han revelado conexiones inesperadas entre diferentes áreas de las matemáticas.

Las fórmulas para π generalmente suponen procesos infinitos, los cuales, cuando se han desarrollado lo suficiente, proporcionan buenas aproximaciones para ese número. Los primeros avances sobre el trabajo de Arquímedes se hicieron en el siglo XV, cuando los matemáticos hindúes representaron π como la suma de una serie infinita, una suma que no tiene fin. Si, como era el caso para estas fórmulas, el valor de la suma se hace muy próximo a un único número bien definido, su *límite*, entonces la serie puede usarse para calcular aproximaciones cada vez más precisas. Una vez alcanzado el nivel necesario de precisión, los cálculos se detienen.

Hacia 1400, Madhava de Sangamagrama usó una de esas series para calcular π con 11 cifras decimales. En 1424, el persa Jamshīd al Kāshī mejoró esto, usando aproximaciones por polígonos con un número de lados que iba incrementando, parecido a lo que había hecho Arquímedes. Obtuvo las 16 primeras cifras decimales considerando un polígono de 3×2^{28} lados. El método de Arquímedes para aproximar π inspiró a François Viète para escribir un tipo nuevo de fórmula para π en 1593, en concreto:

$$\frac{2}{\pi} = \frac{\sqrt{2}}{2} \frac{\sqrt{2 + \sqrt{2}}}{2} \frac{\sqrt{2 + \sqrt{2 + \sqrt{2}}}}{2} \dots$$

(Aquí, los puntos indican manipulación.) En 1630, Christoph Grienberger había llevado el método del polígono hasta las 38 cifras. En 1655, John Wallis encontró una fórmula diferente:

$$\frac{\pi}{2} = \frac{2}{1} \times \frac{2}{3} \times \frac{4}{3} \times \frac{4}{5} \times \frac{6}{5} \times \frac{6}{7} \times \frac{8}{7} \times \frac{8}{9} \dots$$

usando una aproximación bastante complicada para hallar el área de un semicírculo.

James Gregory redescubrió una de las series de Madhava para π en 1641. La idea era empezar con una función trigonométrica llamada «tangente» que escribimos como $\tan x$. Si medimos con radianes, un ángulo de 45° es $\pi/4$, y en este caso $a = b$, de modo que $\tan \pi/4 = 1$.

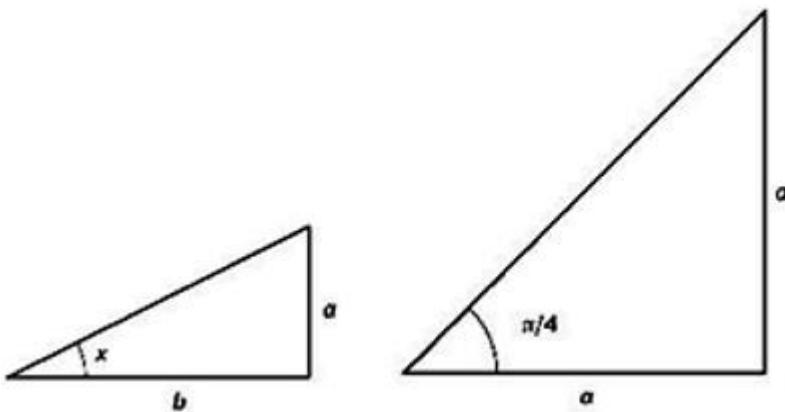


Figura 101. Izquierda: la tangente $\tan x$ es $\pi/4$. Derecha: cuando $x = 45^\circ$, la tangente es $a/b = 1$

Ahora consideramos la función inversa, la arcotangente, normalmente denotada por arctan. Esto «deshace» la función tangente; es decir, si $y = \tan x$, entonces $x = \arctan y$. En concreto, $\arctan 1 = \pi/4$. Madhava y Gregory descubrieron una serie infinita para la arcotangente:

$$\arctan y = y - \frac{y^3}{3} + \frac{y^5}{5} - \frac{y^7}{7} + \frac{y^9}{9} - \dots$$

Haciendo $y = 1$, tenemos:

$$\frac{\pi}{4} = 1 - \frac{1}{3} + \frac{1}{5} - \frac{1}{7} + \frac{1}{9} - \dots$$

En 1699, Abraham Sharp usó esta fórmula para obtener 71 cifras de π , pero la serie converge lentamente, es decir, hay que calcular muchos términos para obtener una aproximación buena. En 1706, John Machin usó una fórmula trigonométrica para $\tan(x + y)$ para mostrar que

$$\frac{\pi}{4} = 4 \arctan \frac{1}{5} - \arctan \frac{1}{239}$$

Y luego sustituyó $1/5$ y $1/239$ en la serie para arctan. Debido a que estos números son mucho más pequeños que 1, la serie converge más rápidamente, lo cual la hace más práctica. Machin calculó π con 100 cifras usando su fórmula. En 1946, Daniel Ferguson había llevado esta

idea general casi todo lo lejos que se podía, usando fórmulas parecidas pero diferentes, y alcanzó 620 cifras.

Hay muchas variantes complicadas de la fórmula de Machin, es más, hay una teoría completa de todas esas fórmulas. En 1896, F. Störmer sabía que

$$\frac{\pi}{4} = 44 \arctan \frac{1}{57} + 7 \arctan \frac{1}{239} - 12 \arctan \frac{1}{682} + 24 \arctan \frac{1}{12.943}$$

y hay muchas fórmulas incluso más impactantes a lo largo de estas líneas, las cuales convergen mucho más rápido gracias a los denominadores enormes que aparecen.

Nadie lo ha hecho mejor usando aritmética de lápiz y papel, pero calculadoras mecánicas y ordenadores electrónicos hicieron los cálculos más rápidos y eliminaron errores. La atención pasó a encontrar fórmulas que dieran aproximaciones muy buenas usando solo algunos términos.

La serie de Chudnovsky

$$\frac{1}{\pi} = 12 \sum_{k=0}^{\infty} \frac{(-1)^k (6k)! (545.140.134k + 13.591.409)}{(3k)! (k!)^3 640.320^{3k+\frac{3}{2}}}$$

encontrada por los hermanos David y Gregory Chudnovsky, genera 14 nuevas cifras decimales por término. Aquí el signo de la suma Σ quiere

decir sumar los valores de la expresión formulada a medida que k va recorriendo todos los naturales empezando en 0 y sin detenerse nunca.

Hay muchos otros métodos para calcular π , y siguen haciéndose nuevos descubrimientos. En 1997, Fabrice Bellard anunció que la cifra que ocupa la posición un billón en π , en notación binaria, es 1. Sorprendentemente no calculó los dígitos anteriores. En 1996, David Bailey, Peter Borein y Simon Plouffe habían descubierto una fórmula muy curiosa:

$$\pi = \sum_{n=0}^{\infty} \frac{1}{2^{4n}} \left(\frac{4}{8n+1} - \frac{2}{8n+4} + \frac{1}{8n+5} - \frac{1}{8n+6} \right)$$

Bellard usó una fórmula parecida, más eficiente para los cálculos:

$$\pi = \frac{1}{64} \sum_{n=0}^{\infty} \frac{(-1)^n}{2^{10n}} \left(-\frac{32}{4n+1} - \frac{1}{4n+3} + \frac{256}{10n+1} - \frac{64}{10n+3} - \frac{4}{10n+5} - \frac{4}{4n+7} + \frac{1}{10n+9} \right)$$

Con algo de análisis inteligente, el método da cifras binarias individuales.

La característica clave de la fórmula es que muchos de los números en ella, como 4, 32, 64, 256, $2^4 n$ y $2^{10} n$, son potencias de 2, las cuales son muy sencillas en el sistema binario usado para el trabajo interno de los

ordenadores. El récord de encontrar una única cifra binaria de π se bate regularmente; en 2010, Nicholas Sze de Yahoo calculó la cifra binaria en la posición dos mil billonésima de π , que resultó ser 0.

Se pueden usar las mismas fórmulas para encontrar cifras aisladas de π con aritméticas de base 4, 8 y 16. No se conoce nada de este tipo para cualquier otra base; no podemos calcular cifras decimales aisladas en particular. ¿Existen esas fórmulas? Hasta que se halló la fórmula de Bailey-Borwein-Plouffe, nadie imaginó que podría hacerse en base binaria.

Cuadrando el círculo

En la Grecia antigua buscaban una construcción geométrica para cuadrar el círculo: encontrar el lado de un cuadrado que tenga la misma área que un círculo dado. Finalmente se probó que, al igual que para la trisección del ángulo y la duplicación del cubo, no existía ninguna construcción con regla y compás [véase 3]. La prueba se basa en saber qué tipo de número es π .

Hemos visto que π no es un número racional. El siguiente paso más allá de los números racionales es a los números algebraicos, los cuales satisfacen una ecuación polinómica con coeficientes enteros. Por ejemplo, $\sqrt{2}$ es algebraico, ya que satisface la ecuación $x^2 - 2 = 0$. Un número que no es algebraico se llama «trascendental» y, en 1761,

Lambert, quien primero probó que π era irracional, lanzó la hipótesis de que en realidad es trascendental.

Se necesitaron 112 años hasta que Charles Hermite hizo el primer gran avance en 1873, probando que el *otro* número curioso y famoso en matemáticas, la base e de los logaritmos naturales [véase e] es trascendental. En 1882, Ferdinand von Lindemann mejoró el método de Hermite y probó que si un número distinto de cero es algebraico, entonces e elevado a la potencia de ese número es trascendental. Luego se aprovechó de la fórmula de Euler $e^{i\pi} = -1$, de este modo. Supongamos que π es algebraico, entonces también lo es $i\pi$. Por lo tanto, el teorema de Lindemann implica que -1 *no* satisface una ecuación algebraica. Sin embargo es obvio que lo hace, en concreto, $x + 1 = 0$. La única salida de esta contradicción en la lógica es que π no satisface una ecuación algebraica, es decir, es trascendental.

Una consecuencia importante de este teorema es la respuesta al antiguo problema geométrico de la cuadratura del círculo, es decir, a construir un cuadrado con la misma área que un círculo usando solo regla y compás. Esto es equivalente a construir un segmento de longitud π a partir de un segmento de longitud 1. La geometría de coordenadas muestra que cualquier número que pueda construirse de este modo tiene que ser algebraico. Y como π no es algebraico, esa construcción no puede existir. Esto no ha bastado para detener a alguna gente que sigue buscando una construcción con regla y compás incluso hoy en día. Parece que no

entienden lo que significa «imposible» en matemáticas. Es una confusión que viene de lejos. En 1872, De Morgan escribió *Un presupuesto de paradojas*, en el cual expone los errores de numerosas aspirantes a cuadraturas del círculo, comparándolas con miles de moscas revoloteando alrededor de un elefante, cada una de ella reclamando ser «mayores que el cuadrúpedo». En 1992, Underwood Dudley continuó la tarea en *Mathematical Cranks*. Por supuesto, puedes explorar aproximaciones geométricas a π y construcciones usando otros instrumentos. Pero, por favor, entiende que una construcción con regla y compás en el sentido clásico estricto no existe.

§. Número de oro

$$\varphi = \frac{1 + \sqrt{5}}{2} \approx 1,618034$$

Este número era conocido en la Grecia antigua, con relación a los pentágonos regulares y el dodecaedro en la geometría euclíadiana. Se asocia con la secuencia de los números de Fibonacci [véase 8] y explica algunos patrones curiosos en la estructura de plantas y flores. Comúnmente llamado «número de oro», parece haber recibido ese nombre entre 1826 y 1835. Se han promovido ampliamente sus propiedades místicas y estéticas, pero la mayoría de estos reclamos están sobrevalorados, algunos están basados en estadísticas sospechosas y

muchos de ellos no tienen ninguna base en absoluto. El número de oro, sin embargo, sí que tiene algunas características matemáticas notables, incluyendo vínculos con los números de Fibonacci y conexiones genuinas con el mundo natural, especialmente, así como con la numerología y la geometría de las plantas.

Geometría griega

El número φ («phi» griego, a veces escrito con una notación diferente: τ , «tau» griego) surge por primera vez en matemáticas en conexión con la geometría del pentágono regular en los *Elementos* de Euclides. Siguiendo la práctica estándar de la época, tuvo una interpretación geométrica, no numérica.

Hay una fórmula exacta para φ , que enseguida veremos. Con seis cifras decimales:

$$\varphi = 1,618034$$

Y con 100 es:

$$\begin{aligned} \varphi = & 1,618\,033\,988\,749\,894\,848\,204\,586\,834\,365\,638\,117\,720\,309\,179 \\ & 805\,762\,862\,135\,448\,622\,705\,260\,462\,818\,902\,449\,707\,207\,204\,189 \\ & 391\,137\,5 \end{aligned}$$

Una característica distintiva de φ aparece si calculamos su inverso $1/\varphi$.

De nuevo, con seis cifras decimales:

$$1/\varphi = 0,618034$$

Esto sugiere que $\varphi = 1 + 1/\varphi$. Esta relación puede escribirse como una ecuación cuadrática $\varphi^2 = \varphi + 1$, o en la forma estándar:

$$\varphi^2 - \varphi - 1 = 0$$

El álgebra de las ecuaciones cuadráticas muestra que esta ecuación tiene dos soluciones:

$$\frac{1 + \sqrt{5}}{2} \quad \frac{1 - \sqrt{5}}{2}$$

Numéricamente, estas son 1,618034 y -0,618034. Tomamos la solución positiva como la definición de φ . De modo que

$$\varphi = \frac{1 + \sqrt{5}}{2}$$

y de hecho, es el caso en que $\varphi = 1 + 1/\varphi$, exactamente.

Conexión con pentágonos

El número de oro aparece en la geometría del pentágono regular. Empieza con un pentágono regular cuyos lados tienen longitud 1.

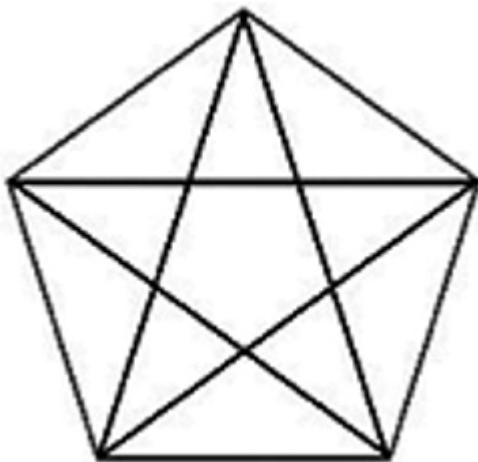


Figura 102. Un pentágono regular y sus diagonales.

Dibuja las cinco diagonales para hacer una estrella de cinco puntas. Euclides probó que cada diagonal tiene la longitud igual al número de oro.

Más concretamente, Euclides trabajó con «la división en media y extrema razón». Es una forma de cortar un segmento en dos partes de modo que la razón de la parte mayor respecto a la menor es igual a la razón de todo el segmento respecto a la parte mayor.

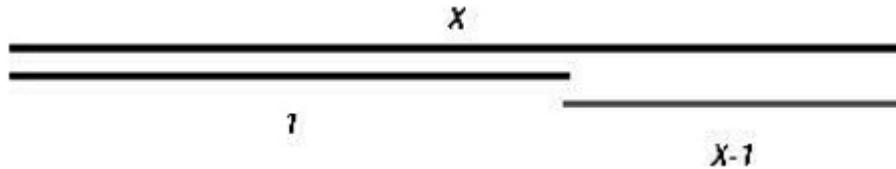


Figura 103. División en media y extrema razón: la razón de la longitud gris oscuro (1) respecto a la gris claro ($x - 1$) es igual a la razón entre la longitud negra (x) respecto a la gris oscura (1).

¿A qué número nos dirige este proceso? En símbolos, supongamos que el segmento negro tiene longitud x y el gris oscuro tiene longitud 1. Entonces, la longitud del segmento gris claro es $x - 1$. De modo que la condición de la división en media y extrema razón se reduce a la ecuación:

$$\frac{x}{1} = \frac{1}{(x - 1)}$$

Que operando queda:

$$x^2 - x - 1 = 0$$

Esta es la ecuación que define el número de oro, y queremos la solución que es mayor que 1, es decir, φ .

Euclides observó que en la imagen del pentágono, los lados dividen a la diagonal en media y extrema razón, lo cual le permitió construir un pentágono regular con los instrumentos tradicionales: regla y compás [véase 17]. Y el pentágono era importante para los griegos por formar las caras de uno de los cinco sólidos regulares, el dodecaedro. El clímax de

Elementos es una prueba de que existen exactamente cinco sólidos regulares [véase 5].

Números de Fibonacci

El número de oro está muy relacionado con los números de Fibonacci, introducidos en 1202 por Leonardo de Pisa [véase 8]. Recuerda que esta secuencia de números empieza:

1 1 2 3 5 8 13 21 34 55 89 144 233

Cada número, tras los dos primeros, se obtiene sumando los dos anteriores:

$$1 + 1 = 2$$

$$1 + 2 = 3$$

$$2 + 3 = 5$$

$$3 + 5 = 8\dots$$

y así sucesivamente. Las razones de números de Fibonacci consecutivos se van aproximando cada vez más al número de oro.

$$\begin{array}{ll}
 \frac{1}{1} = 1 & \frac{21}{13} = 1,6153 \\
 \frac{2}{1} = 2 & \frac{34}{21} = 1,6190 \\
 \frac{3}{2} = 1,5 & \frac{55}{34} = 1,6176 \\
 \frac{5}{3} = 1,6666 & \frac{89}{55} = 1,6181 \\
 \frac{8}{5} = 1,6 & \frac{144}{89} = 1,6179 \\
 \frac{13}{8} = 1,625 & \frac{233}{144} = 1,6181
 \end{array}$$

y esta propiedad puede probarse a partir de la regla para formar la secuencia y la ecuación cuadrática para φ .

A la inversa, podemos expresar los números de Fibonacci en términos del número de oro [véase 8]:

$$F_n = \frac{\varphi^n - (-\varphi)^{-n}}{\sqrt{5}}$$

Aparición en plantas

Durante más de dos mil años, la gente ha observado que los números de Fibonacci son muy comunes en el reino vegetal. Por ejemplo, muchas flores, especialmente de la familia de las margaritas, tienen un número de Fibonacci de pétalos. Las caléndulas suelen tener 13 pétalos. Las ásteres tienen 21. Muchas margaritas tienen 34 pétalos; si no, 55 o 89. Los girasoles tienen normalmente 55, 89 o 144 pétalos.

Otros números son más raros, aunque se dan; por ejemplo, las fuchsias tienen 4 pétalos. En estas excepciones a menudo están involucrados los números de Lucas: 4, 7, 11, 18 y 29, que se forman del mismo modo que los números de Fibonacci pero empezando con 1 y 3. Más adelante veremos algunos ejemplos.

Los mismos números aparecen en otras cuantas características de las plantas. Una piña tiene aproximadamente un patrón hexagonal en su superficie; los hexágonos son frutos individuales, que se fusionan cuando crecen. Encajan unos con otros en dos familias de espirales engranadas. Una familia va en sentido antihorario, vista desde arriba, y contiene 8 espirales; la otra va en sentido horario y contiene 13. También es posible ver una tercera familia de 5 espirales, girando en sentido horario con un ángulo menos pronunciado.

Las escamas de piñas de piñones forman un conjunto similar de espirales. También lo hacen las semillas en la cabeza de un girasol maduro, pero en este caso las espirales están en el plano.

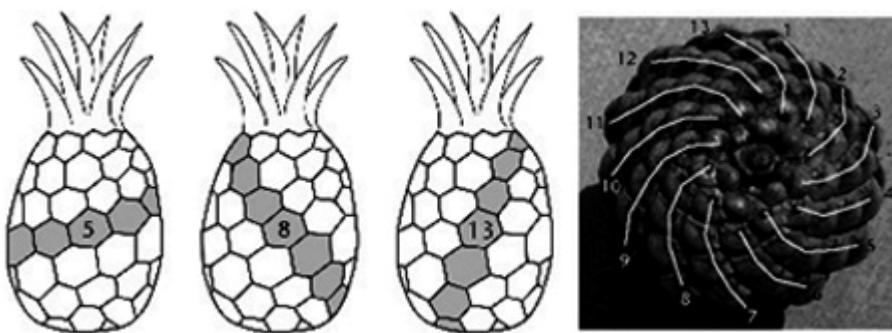


Figura 104. Izquierda: tres familias de espirales en una piña. Derecha: familia de 13 espirales en sentido antihorario en una piña de piñones.

La clave para la geometría de las espirales del girasol es el número de oro, el cual a su vez explica que aparezcan los números de Fibonacci. Divide una circunferencia completa (360°) en dos arcos que estén en proporción áurea, de modo que el ángulo determinado por el arco mayor es ϕ veces el ángulo determinado por el arco menor. Entonces el arco más pequeño es $1/(1+\phi)$ veces una circunferencia completa. Este ángulo, llamado «ángulo de oro», es aproximadamente $137,5^\circ$.

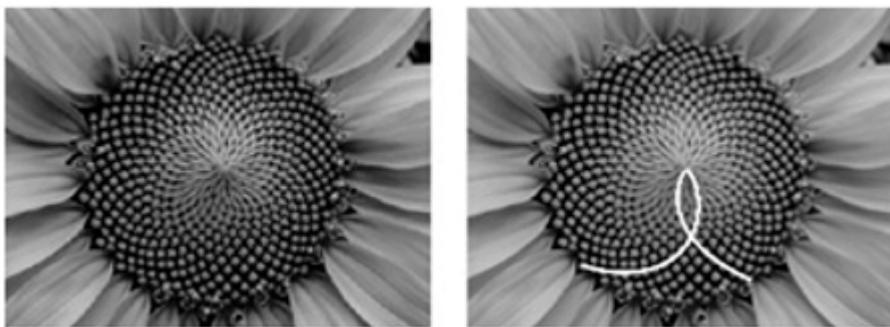


Figura 105. Las espirales de Fibonacci en la cabeza del girasol.
Izquierda: situación de las semillas. Derecha: miembros de dos familias de espirales; sentido horario (gris claro) y antihorario (gris oscuro).

En 1868, el botánico alemán Wilhelm Hofmeister observó cómo cambia el brote de una planta y estableció las bases para el trabajo sobre este problema que vino a continuación. El patrón básico del desarrollo está determinado por lo que sucede en el meristemo apical. Depende de pequeños grupos de células conocidas como «primordios», las cuales finalmente se convierten en semillas. Hofmeister descubrió que

primordios consecutivos están en espiral, cada uno está separado de su predecesor por el ángulo de oro A , de modo que la semilla enésima tiene un ángulo nA y la distancia desde el centro es proporcional a la raíz cuadrada de n .

Esta observación explica el patrón de semillas en la cabeza de un girasol. Puede obtenerse colocando semillas consecutivas en ángulos que son múltiplos enteros del ángulo de oro. La distancia desde el centro debería ser proporcional a la raíz cuadrada del número que nos ocupa. Si llamamos al ángulo de oro A , entonces las semillas van formando los ángulos:

$$A \ 2A \ 3A \ 4A \ 5A \ 6A\dots$$

y distancias proporcionales a:

$$1 \ \sqrt{2} \ \sqrt{3} \ \sqrt{4} \ \sqrt{5} \ \sqrt{6}\dots$$

En flores como las margaritas, los pétalos se forman en el extremo exterior de una familia de espirales. De modo que el número de Fibonacci de espirales implica un número de Fibonacci de pétalos. Pero ¿por qué tenemos números de Fibonacci para las espirales?

Debido al ángulo de oro.

En 1979, Helmut Vogel usó la geometría de las semillas de girasol para explicar por qué se da el ángulo de oro. Calculó qué sucedería a la inflorescencia si se empleaba la misma espiral, pero el ángulo de oro de $137,5^\circ$ se cambiaba un poco. El resultado fue que solo el ángulo de oro lleva a semillas que están puestas juntas, sin huecos o superposiciones. Incluso un cambio en el ángulo de una décima de grado provoca que el patrón se convierta en una única familia de espirales, con huecos entre las semillas. Esto explica por qué el ángulo de oro es especial y no es solo una coincidencia numérica.

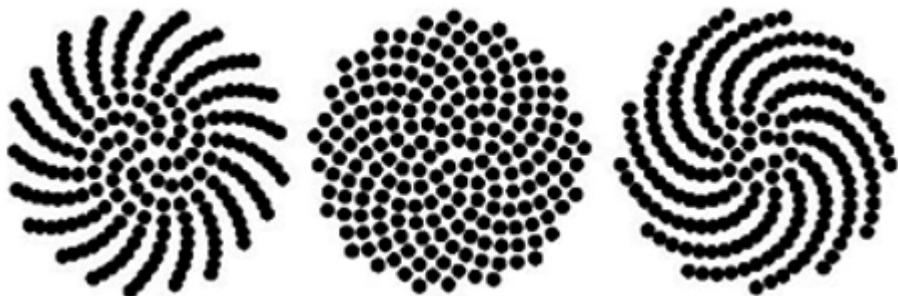


Figura 106. Colocación de semillas consecutivas usando los ángulos 137° , $137,5^\circ$ y 138° . Solo el ángulo de oro sitúa las semillas cuidadosamente.

Sin embargo, una explicación completa profundiza más en la cuestión. A medida que las células crecen y se mueven, crean fuerzas que afectan a las células vecinas. En 1992, Stéphane Douady e Yves Couder investigaron las mecánicas de esos sistemas usando tanto experimentos como simulaciones por ordenador. Encontraron que los ángulos entre las

semillas consecutivas son aproximaciones de fracciones de Fibonacci al ángulo de oro.

Su teoría también explica la confusa aparición de números que no son de Fibonacci, como los cuatro pétalos de la fucsia. Estas excepciones vienen de una sucesión muy parecida a la sucesión de Fibonacci y se llaman «números de Lucas»:

$$1 \ 3 \ 4 \ 7 \ 11 \ 18 \ 29 \ 47 \ 76 \ 123\dots$$

La fórmula para estos números es:

$$L_n = \varphi^n + (-\varphi)^{-n}$$

muy parecida a la fórmula para los números de Fibonacci que vimos anteriormente.

Los 4 pétalos de la fucsia son un ejemplo de un número de Lucas de pétalos. Algunos cactus exhiben un patrón de 4 espirales en una dirección y 7 en otra, u 11 en una dirección y 18 en la otra. Una especie de echinocactus tiene 29 nervios. Se han encontrado conjuntos de 47 y 76 espirales en girasoles.

Una de las áreas importantes de matemática aplicada es la teoría de la elasticidad, que estudia cómo los materiales se doblan o ceden cuando se les aplican fuerzas. Por ejemplo, esta teoría explica cómo vigas u hojas de metal se comportan en edificios y puentes. En 2004, Patrick Shipman

y Alan Newell aplicaron teoría de elasticidad para modelizar el brote de una planta creciendo, con particular énfasis en los cactus. Modelizaron la formación del primordio como abollándose en la superficie de la punta del brote y mostraron que esto llevaba a patrones superpuestos de ondas paralelas. Estos patrones están gobernados por dos factores: números de onda y dirección. Los patrones más importantes involucran la interacción de tres de esas ondas, y el número de onda para una onda debe ser la suma de los otros dos números de onda. Las espirales en la piña son un ejemplo, con números de onda 5, 8 y 13. Su teoría busca el origen de los números de Fibonacci directamente en la aritmética de los patrones de ondas.

¿Qué ocurre con la bioquímica subyacente? La formación del primordio está dirigida por una hormona llamada «auxina», en cuya distribución surgen patrones de ondas parecidos. De modo que la explicación completa de los números de Fibonacci y el ángulo de oro supone una interacción entre bioquímica, fuerzas mecánicas entre células y geometría. La auxina estimula el crecimiento del primordio. Los primordios ejercen fuerzas entre sí. Estas fuerzas crean la geometría. Significativamente, la geometría, a su vez, afecta a la bioquímica desencadenando la producción de auxina extra en lugares específicos. De modo que hay un conjunto complejo de trayectorias de retroalimentación entre la bioquímica, la mecánica y la geometría.

§. Logaritmos naturales $e \approx 2,718281$

Después de π , el siguiente número raro que nos encontramos, normalmente en cálculo, se llama « e », por «exponencial». Fue analizado por primera vez por Jacob Bernoulli en 1683. Aparece en problemas sobre interés compuesto, llevó a los logaritmos, y nos dice cómo variables como la temperatura, la radiactividad o la población humana crecen o disminuyen. Euler lo vinculó a π e i .

Tipo de interés

Cuando pedimos un préstamo o invertimos, quizá tengamos que pagar, o nos darán, un interés sobre la cantidad en cuestión. Por ejemplo, si invertimos 100 € con un tipo de interés del 10 % anual, entonces obtenemos 110 € de vuelta tras un año. Por supuesto, en esta época de crisis financiera el 10 % parece un interés sobre los depósitos tan alto que no es realista, pero a la vez tan bajo que tampoco es realista como interés sobre préstamos, especialmente con créditos personales a un TAE del 5.853 %. Sea lo que sea, es una cifra apropiada para propósitos ilustrativos.

A menudo, el interés es *compuesto*. Es decir, el interés se suma a la cantidad original y el interés se paga entonces sobre el total. A un tipo de interés compuesto de un 10 %, el interés sobre 110 € durante el siguiente año será 11 €, mientras que un segundo año de interés sobre la suma original sería solo de 10 €. Por lo tanto, tras dos años de un interés

compuesto del 10 %, tendríamos 121 € Un tercer año de interés compuesto sumaría 12,10 € a lo anterior, un total de 133,10 € y un cuarto año haría el total de 146,41 €

La constante matemática conocida como «e» aparece si imaginamos un tipo de interés de un 100 %, de modo que tras cierto período fijo de tiempo, por ejemplo un siglo, nuestro dinero se dobla. Para cada 1 € que invertimos, obtenemos de vuelta tras ese período 2 €

Supongamos que en lugar del 100 % de interés durante un siglo, aplicamos un tipo del 50 % (la mitad) durante medio siglo (el doble de frecuencia), y componemos eso. Después de medio siglo, tenemos en euros:

$$1 + 0,5 = 1,5$$

Después de la segunda mitad, tenemos:

$$1,5 + 0,75 = 2,25$$

La cantidad que obtenemos de vuelta es mayor.

Si dividimos el siglo en tres períodos iguales, y dividimos el tipo de interés por 3, nuestro 1 €crece como se indica a continuación, truncando a diez cifras decimales:

Incialmente: 1

Después de un período de $1/3$: 1,3333333333

Después de un período de $2/3$: 1,7777777777

Después de un período: 2,3703703704

que, de nuevo, es mayor.

Hay un patrón en los números anteriores:

$$1 = (1^{1/3})^0$$

$$1,3333333333 = (1^{1/3})^1$$

$$1,7777777777 = (1^{1/3})^2$$

$$2,3703703704 = (1^{1/3})^3$$

Los matemáticos se preguntaron qué sucedía al aplicar el tipo de interés continuamente, es decir, durante fracciones cada vez más pequeñas del período. En ese caso es cuando surge un patrón: si dividimos el período en n partes iguales, con un tipo de interés del $1/n$, entonces al final del período tendríamos:

$$(1 + \frac{1}{n})^n$$

El interés compuesto continuamente se corresponde a hacer que n pase a ser extremadamente grande. Probemos con algunos números (de nuevo calculamos hasta diez cifras decimales):

Tabla 10

n	$(1 + \frac{1}{n})^n$
2	2,2500000000
3	2,3703703704
4	2,4414062500
5	2,4883200000
10	2,5937424601
100	2,7048138294
1.000	2,7169239322
10.000	2,7181459268
100.000	2,7182682372
1.000.000	2,7182816925
10.000.000	2,7182816925

Tenemos que tomar valores muy grandes de n para ver el patrón, pero parece como si el límite, cuando n se hace muy grande, $\lim_{n \rightarrow \infty} (1 + \frac{1}{n})^n$, se acercase más y más a un número fijo, aproximadamente igual a 2,71828. Esto resulta ser cierto, y los matemáticos definen un número especial, llamado «e», que es el valor del límite:

$$e = \lim_{n \rightarrow \infty} \left(1 + \frac{1}{n}\right)^n$$

donde el símbolo *lim* significa «permitamos que *n* se haga infinitamente grande y veamos hacia qué valor tiende a establecerse la expresión».

Para 100 cifras decimales:

$e = 2, 718 281 828 459 045 235 360 287 471 352 662 497 757 247 093 699 959 574 966 967 627 724 076 630 353 575 945 713 821 785$

Es otro de esos números extraños que, como π , tiene una expresión decimal infinita pero nunca repite el mismo bloque de cifras una y otra vez. Es decir, e es irracional [véanse $\sqrt{2}$, π]. A diferencia de π , la prueba de que e es irracional es fácil, Euler la descubrió en 1737, pero no se publicó hasta siete años más tarde.

Euler calculó las primeras 23 cifras de e en 1748, y una serie de matemáticos posteriores mejoraron su resultado. En 2010 Shigeru Kondo y Alexander Yee habían calculado el primer billón de cifras decimales de e . Usaron un ordenador potente y un método mejorado.

Logaritmos naturales

En 1614, John Napier, octavo terrateniente de Merchiston (ahora Merchiston, parte de la ciudad escocesa de Edimburgo), escribió un libro

con el título *Mirifici Logarithmorum Canonis Descriptio* («Descripción del maravilloso canon de los logaritmos»). Parece que él mismo inventó la palabra *logaritmo*, del griego *logos*, «proporción», y *arithmos*, «número». Introdujo la idea de la siguiente manera:

Como no hay nada más tedioso, colegas matemáticos, en la práctica de las artes matemáticas, que el gran retraso sufrido en el hastío de largas multiplicaciones y divisiones, el hallazgo de razones y en la extracción de las raíces cuadradas y cúbicas, y los muchos errores resbaladizos que pueden surgir, he estado, por lo tanto, dando vueltas en mi mente a una técnica segura y diligente que podría ser capaz de mejorar y sobreponerse a estas dificultades. Al final, tras mucho pensamiento, he encontrado un modo increíble de acortar los procedimientos... Es una grata tarea establecer el método para el uso público de los matemáticos.

Napier sabía, debido a experiencias personales, que muchos problemas científicos, especialmente en astronomía, requerían multiplicar números complicados entre sí, o encontrar raíces cuadradas y raíces cúbicas. En una época en la que no había electricidad, no digamos ordenadores, los cálculos tenían que hacerse a mano. Sumar dos decimales era razonablemente sencillo, pero multiplicarlos era mucho más difícil. De

modo que Napier inventó un método para convertir la multiplicación en suma. El truco era trabajar con potencias de un número fijo.

En álgebra, las potencias de una incógnita x están indicadas por un número pequeño elevado. Es decir, $xx = x^2$, $xxx = x^3$, $xxxx = x^4$, y así sucesivamente, donde colocar dos letras juntas significa que habría que multiplicarlas. Por ejemplo, $10^3 = 10 \times 10 \times 10 = 1.000$ y $10^4 = 10 \times 10 \times 10 \times 10 = 10.000$.

Multiplicar dos de estas expresiones es fácil. Por ejemplo, supongamos que quieres calcular $10^4 \times 10^3$. Lo escribes:

$$\begin{aligned} 10.000 \times 1.000 &= (10 \times 10 \times 10 \times 10) \times (10 \times 10 \times 10) = \\ &= 10 \times 10 \times 10 \times 10 \times 10 \times 10 \times 10 = \\ &= 10.000.000 \end{aligned}$$

El número de ceros en la respuesta es 7, que es igual a $4 + 3$. El primer paso en los cálculos muestra *por qué* es $4 + 3$; ponemos cuatro 10 y tres 10 unos junto a los otros. De modo que:

$$10^4 \times 10^3 = 10^{4+3} = 10^7$$

Del mismo modo, cualquiera que sea el valor de x , si multiplicamos su potencia a -ésima por su potencia b -ésima, donde a y b son números enteros, entonces tenemos que la potencia $(a + b)$ -ésima:

$$x^a x^b = x^{a+b}$$

Es más interesante de lo que parece, porque a la izquierda multiplicamos una cantidad por otra, mientras que a la derecha el paso principal es sumar a y b , lo cual es más fácil.

Ser capaz de multiplicar potencias enteras de 10 no es un gran avance. Pero la misma idea puede extenderse para hacer cálculos más útiles.

Supongamos que quieres multiplicar 1,484 por 1,683. Haciendo toda la multiplicación obtienes 2,497572, que redondeado a tres cifras decimales es 2,498. En su lugar, podemos usar la fórmula $x^a x^b = x^{a+b}$ haciendo una elección apropiada de x . Si tomamos x igual a 1,001, entonces un poco de aritmética nos desvela que:

$$1,001^{395} = 1,484$$

$$1,001^{521} = 1,683$$

redondeando a tres cifras decimales. La fórmula nos dice entonces que $1,484 \times 1,683$ es:

$$1,001^{395+521} = 1,001^{916}$$

el cual redondeando a tres cifras decimales es 2,498. ¡No está mal!

El núcleo del cálculo es una suma fácil: $395 + 521 = 916$. Sin embargo, a primera vista este método hace el problema más difícil. Para calcular $1,001^{395}$, tienes que multiplicar 1,001 por sí mismo 395 veces y lo mismo se aplica para otras dos potencias. De modo que esto parece una idea bastante poco útil. El gran avance de Napier fue que esta objeción era errónea. Pero para vencerla, alguien tiene que hacer el trabajo pesado de calcular muchas potencias de 1,001, empezando con $1,001^2$ y seguir hasta algo como $1,001^{10.000}$. Cuando publicaron una tabla de estas potencias, todo el trabajo duro estaba hecho. Tan solo tienes que recorrer con tus dedos las sucesivas potencias hasta que veas 1,484 al lado de 395. De manera parecida localizas 1,683 al lado de 521. Luego sumas estos dos números para obtener 916. La fila correspondiente de la tabla te dice que esta potencia de 1,001 es 2,498. Trabajo acabado.

En el contexto de este ejemplo, decimos que la potencia de 395 es el *logaritmo* del número 1,484, y la de 521 es el logaritmo del número 1,683. De manera similar 916 es el logaritmo de su producto, 2,498. Escribimos log como una abreviatura, y lo que hemos hecho nos lleva a la ecuación:

$$\log ab = \log a + \log b$$

la cual es válida para cualquier número a y b . La elección bastante arbitraria de 1,001 se llama «base». Si usamos una base diferente, los logaritmos que calculamos son también diferentes, pero para cualquier base fija todo funciona del mismo modo.

Mejora de Briggs

Esto es lo que Napier debería haber hecho, pero por alguna razón hizo algo ligeramente distinto, y no tan conveniente. Un matemático llamado Henry Briggs estaba fascinado por el avance de Napier. Pero al ser el típico matemático, antes de que la tinta se secara en el papel ya empezó a preguntarse si había algún modo de simplificar todo. Y lo había. Primero, reescribió la idea de Napier para que funcionase en el modo que acabo de describir. Después, observó que usar potencias de un número como 1,001 se reduce a usar potencias de (una aproximación de) ese número especial e.

La potencia 1.000, $1,001^{1.000}$ es igual a $(1 + \frac{1}{1000})^{1000}$ y esto debe ser próximo a e, por la definición de e. Basta tomar $n = 1.000$ en la fórmula $(1 + \frac{1}{n})^n$. Así, en lugar de escribir:

$$1,001^{395} = 1,484$$

podemos escribir

$$(1,001 \cdot 1,000) \cdot 0,395 = 1,484$$

Ahora $1,001^{1,000}$ está muy próximo a e , de modo que una aproximación razonable es:

$$e^{0,395} = 1,484$$

Para obtener resultados más precisos, usamos potencias de algo mucho más cerca de 1, como $1,000001$. Ahora $1,000001^{1,000,000}$ es todavía más próximo a e . Esto hace la tabla mucho más grande, con aproximadamente un millón de potencias. Calcular esa tabla es una labor enorme, pero tiene que hacerse *solo una vez*. Si una persona lleva a cabo ese esfuerzo, las generaciones que le sucedan se habrán ahorrado una cantidad gigantesca de aritmética. Y no es tan duro multiplicar un número por $1,000001$. Tan solo tienes que ser muy cuidadoso para no cometer ningún fallo.

Esta versión de la mejora de Briggs redujo la definición del logaritmo natural de un número a ser la potencia a la cual hay que elevar e para obtener ese número. Es decir:

$$e^{\log x} = x$$

para cualquier x . Ahora:

$$\log xy = \log x + \log y$$

y una tabla de logaritmos naturales, una vez calculados, reduce cualquier problema de multiplicaciones a un problema de sumas.

Sin embargo, la idea se hace todavía más sencilla para cálculos prácticos si reemplazamos e por 10, de modo que $10 \log x = x$. Ahora tenemos *logaritmos en base 10*, que se escriben como $\log_{10} x$. La clave es que ahora $\log_{10} 10 = 1$, $\log_{10} 100 = 2$ y así sucesivamente. Una vez conoces los logaritmos de base 10 de los números entre 1 y 10, todos los otros logaritmos se pueden hallar fácilmente. Por ejemplo:

$$\log_{10} 2 = 0,3010$$

$$\log_{10} 20 = 1,3010$$

$$\log_{10} 200 = 2,3010$$

y así sucesivamente.

Los logaritmos de base 10 son más sencillos para aritmética en la práctica porque usamos el sistema decimal. Pero en matemáticas avanzadas no hay nada terriblemente especial en 10. Podríamos usar cualquier otro número como base para la notación. Resulta que los logaritmos naturales de Briggs, en base e , son más fundamentales en matemáticas avanzadas.

Entre las muchas propiedades de e , aquí mencionaré solo una. Aparece en la aproximación de Stirling al factorial, la cual es muy útil cuando n se hace grande:

$$n! \sim \sqrt{2\pi n} \left(\frac{n}{e}\right)^n$$

Crecimiento y decrecimiento exponencial

El número e aparece por todas partes en ciencia porque es básico en cualquier proceso natural en el cual, en cualquier momento dado, el ritmo de crecimiento (o decrecimiento) de cualquier cantidad es proporcional al valor de la cantidad en ese momento. Escribimos x' para el ritmo al cual la cantidad x cambia. Ese proceso es descrito por la ecuación diferencial:

$$x' = kx$$

para una constante k . Por cálculo, la solución es:

$$x = x_0 e^{kt}$$

en el momento t , donde x_0 es el valor inicial en el momento $t = 0$.

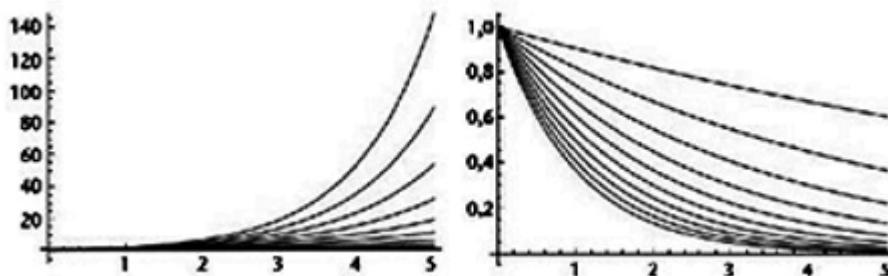


Figura 107. Izquierda: crecimiento exponencial e^{kt} para $k = 0,1, 0,2, \dots, 1$.

1. Derecha: decrecimiento exponencial e^{-kt} para $k = 0,1, 0,2, \dots, 1$.

Crecimiento exponencial

Cuando k es positivo, $x_0 e^{kt}$ crece cada vez más rápido a medida que lo hace t ; esto es *crecimiento exponencial*.

Por ejemplo, x podría ser el tamaño de una población de animales. Si no hay límites para sus recursos de alimento y hábitat, la población crece a un ritmo que es proporcional a su tamaño, de modo que se aplica el modelo exponencial. Finalmente, el tamaño de la población se hace tan grande que no es realista. En la práctica, el alimento o el hábitat o algún otro recurso empieza a escasear, limitando el tamaño, y se deben usar modelos más sofisticados. Pero este modelo sencillo tiene la virtud de mostrar que un crecimiento sin restricciones a un ritmo constante no es realista.

La población humana total sobre la Tierra ha crecido casi exponencialmente durante la mayor parte de la historia de la que se tiene registro, pero hay signos de que el ritmo de crecimiento podría haberse ralentizado hacia 1980. Si no, estamos ante un gran problema.

Proyecciones de la población futura asumen que esta tendencia continuará, pero incluso así hay una incertidumbre considerable. Naciones Unidas estima para 2100 un rango entre 6.000 millones (menos que la población actual, justo por debajo de los 7.000 millones) y 16.000 millones (más del doble que la población actual).

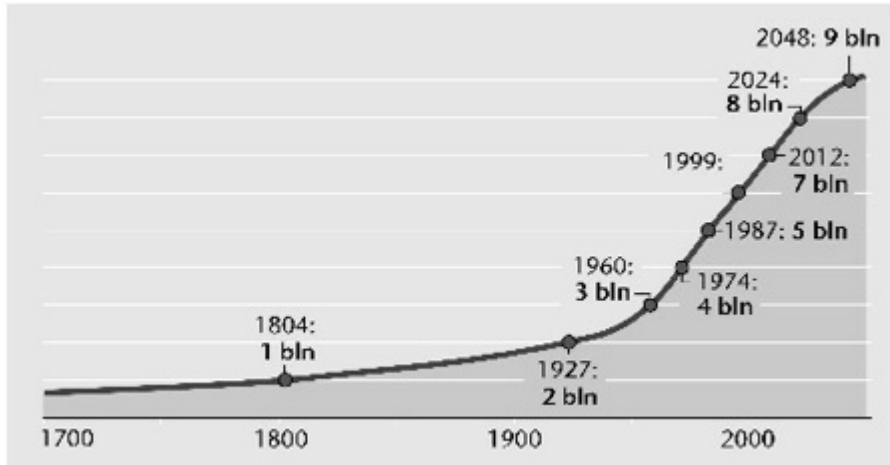


Figura 108. Crecimiento de la población mundial.

Decrecimiento exponencial

Cuando k es negativo, $x_0 e^{kt}$ decrece cada vez más rápido a medida que t aumenta; esto es *decrecimiento exponencial*.

Los ejemplos incluyen el enfriamiento de un cuerpo caliente y la radiactividad. Los elementos radiactivos se transforman en otros a través de procesos nucleares, y emiten partículas nucleares como radiación. El nivel de radiactividad decrece exponencialmente en el tiempo. De modo que el nivel de radiactividad $x(t)$ en el momento t sigue la ecuación:

$$x(t) = x_0 e^{-kt}$$

donde x_0 es el nivel inicial y k es una constante positiva, que depende del elemento en cuestión.

Se trata de una medida conveniente del tiempo para la cual la radiactividad persiste es el período de *semi desintegración*, un concepto introducido en 1907. Es el tiempo que necesita un nivel inicial x_0 para reducirse a la mitad de su tamaño. Supongamos que el período de semi desintegración es 1 semana, por ejemplo. Entonces el ritmo original al cual el material emite radiaciones es la mitad después de 1 semana, se reduce a un cuarto después de 2 semanas, un octavo después de 3 semanas, y así sucesivamente. Se necesitan 10 semanas para reducirlo a una milésima de su nivel original (realmente $1/1024$) y 20 semanas para reducirlo a una millonésima.

Para calcular el período de semi desintegración, solucionamos la ecuación:

$$\frac{x_0}{2} = x_0 e^{-kt}$$

Tomando logaritmos en ambas partes, el resultado es:

$$t = \frac{\log 2}{k} = \frac{0,6931}{k}$$

La constante k es conocida a partir de experimentos.

En accidentes con reactores nucleares actuales, los productos radiactivos más importantes son yodo-131 y cesio-137. El primero puede causar cáncer de tiroides, porque esa glándula concentra yodo. El período de semi desintegración del yodo-131 es solo 8 días, de modo que provoca poco daño si se dispone de la medicación apropiada (principalmente pastillas de yodo). El cesio-137 tiene un período de semi desintegración de 30 años, de modo que necesita alrededor de 200 años para que el nivel de radiactividad se reduzca a una centésima de su valor inicial. Por lo tanto, el peligro permanece durante un largo período de tiempo a menos que pueda limpiarse.

Conexión entre e y π (Fórmula de Euler)

En 1748, Euler descubrió una conexión notable entre e y π . Suele decirse que es la fórmula matemática más bella. Se necesita el número imaginario i también. La fórmula es esta:

$$e^{i\pi} = -1$$

Puede explicarse usando una conexión sorprendente entre el exponencial complejo y funciones trigonométricas, en concreto:

$$e^{i\theta} = \cos \theta + i \sin \theta$$

la cual se determina más fácilmente usando métodos del cálculo. En ella, el ángulo θ se mide en radianes, una unidad en la cual el círculo completo de 360° es igual a 2π radianes, considerando la circunferencia de radio 1. La medida del radián es un estándar en matemáticas avanzadas por hacer todas las fórmulas más sencillas. Para obtener la fórmula de Euler, sea $\theta = \pi$. Entonces $\cos \pi = -1$, $\sin \pi = 0$, de modo que $e^{i\pi} = \cos \pi + i \sin \pi = 1 + i \cdot 0 = -1$

Una prueba alternativa usando la teoría de ecuaciones diferenciales sigue la pista a la ecuación hasta la geometría del plano complejo, y tiene la virtud de explicar cómo π entra en juego. Intentaré hacer un boceto. La ecuación de Euler funciona porque multiplicar números complejos por i rota el plano complejo en un ángulo recto.

Si medimos con radianes, que es lo que usan los matemáticos para investigaciones teóricas, principalmente porque hace las fórmulas del cálculo más sencillas, un ángulo está definido por la longitud del arco correspondiente de la circunferencia unidad. Como la semicircunferencia unidad tiene longitud π , un ángulo recto es $\pi/2$ radianes. Usando ecuaciones diferenciales puede demostrarse que para cualquier número real x , multiplicando por el número complejo e^{ix} se rota el plano complejo en x radianes. En concreto, multiplicado por $e^{i(\pi/2)}$ lo rota un ángulo recto. Pero eso es lo que hace i . De modo que:

$$e^{i(\pi/2)} = i$$

Elevando al cuadrado ambos lados, obtenemos la fórmula de Euler.

$$\log 3/\log 2 \approx 1,584962$$

§. Fractales

Este curioso número, como $466/885$, es una propiedad básica del triángulo de Sierpiński, pero este caracteriza lo ondulada o rugosa que es la famosa curva patológica de Sierpiński. Las preguntas como esta surgen en geometría fractal, un nuevo modo de modelizar formas complejas en la naturaleza. Ahí generaliza el concepto de dimensión. Uno de los fractales más famosos, el conjunto de Mandelbrot, es una forma infinitamente compleja definida por un proceso muy simple.

Fractales

El triángulo de Sierpiński [véase $466/885$] es uno de un pequeño zoo de ejemplos que fueron creados a principios del siglo XX, a los cuales en ese momento se les dio un nombre bastante negativo de «curvas patológicas». Incluyen el copo de nieve de Helge von Koch y las curvas que recubren el plano de Giuseppe Peano y David Hilbert.

En la época, estas curvas necesitaban un tiempo para ser apreciadas: contraejemplos a afirmaciones matemáticas más o menos plausibles que eran en realidad falsas. La curva del copo de nieve es continua, pero no diferenciable en ningún punto, es decir, no se parte en ningún lado, pero está dentada en todas partes. Tiene longitud infinita, aunque encierra un área finita. Las curvas que recubren el espacio no son solo muy densas, sino que recubren el espacio. Cuando la construcción se lleva a cabo con frecuencia infinita, las curvas resultantes pasan a través de *todo punto* dentro del cuadrado sólido.

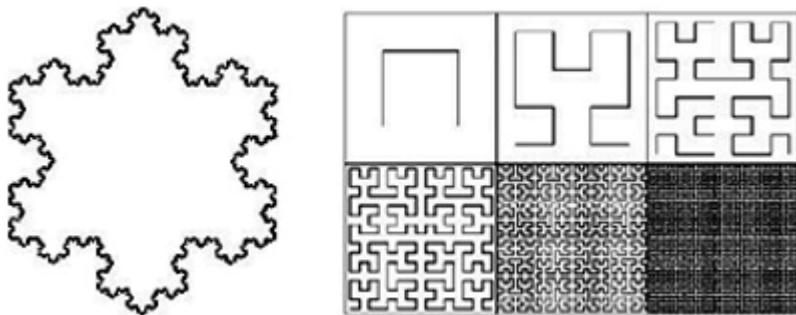


Figura 109. Izquierda: curva del copo de nieve. Derecha: etapas sucesivas en la construcción de la curva de Hilbert.

Algunos de los matemáticos más conservadores se burlaron de esas curvas, pues las consideraban intelectualmente estériles. Hilbert fue una de las pocas figuras que lideraban en la época que reconoció su importancia en ayudar a hacer las matemáticas rigurosas e iluminar sus bases lógicas y expresó un apoyo entusiasta para que sus extrañas propiedades se tomaran en serio.

En la actualidad vemos estas curvas con una perspectiva más positiva: fueron pasos tempranos hacia un área nueva de las matemáticas: la *geometría fractal*, de la cual Mandelbrot fue pionero en la década de los setenta del siglo XX. Las curvas patológicas fueron inventadas por razones puramente matemáticas, pero Mandelbrot se dio cuenta de que formas similares podían arrojar luz sobre irregularidades en el mundo natural. Indicó que triángulos, cuadrados, círculos, conos, esferas y otras formas tradicionales de la geometría euclíadiana no tenían una estructura refinada. Si aumentas una circunferencia, parece una recta uniforme. Sin embargo, muchas de las formas de la naturaleza tienen una estructura compleja en escalas muy pequeñas. Mandelbrot escribió: «Las nubes no son esferas, las montañas no son conos, las costas no son circunferencias y la corteza no es lisa, ni los rayos viajan en línea recta». Todo el mundo lo sabía, por supuesto, pero Mandelbrot comprendió su significado.

No estaba reclamando que las formas euclídeas no sean útiles. Tienen un papel notorio en ciencia. Por ejemplo, los planetas son aproximadamente esféricos, y para los primeros astrónomos esta fue una aproximación útil. Aparece una mejor aproximación si la esfera es aplastada para formar un elipsoide, el cual de nuevo es una forma euclíadiana sencilla. Pero para algunos fines, las formas sencillas no ayudan demasiado. Los árboles tienen ramas cada vez más pequeñas, las nubes son masas amorfas, las montañas están dentadas y las líneas de costa son serpenteantes.

Comprender estas formas matemáticamente y resolver problemas científicos sobre ellas requiere una nueva aproximación.

Piensa en las líneas de costa. Mandelbrot se dio cuenta de que se parecían bastante en un mapa, a cualquier escala. Un mapa con una escala grande muestra más detalle, con ondulaciones extra, pero el resultado se parece mucho a la línea de costa en un mapa a escala más pequeña. La forma exacta de la línea de costa cambia, pero la «textura» permanece bastante igual. De hecho, la mayoría de las características estadísticas de la línea de costa, como la proporción de bahías que tienen un tamaño relativo dado, son las mismas sin importar la escala del mapa empleada.

Mandelbrot introdujo la palabra «fractal» para describir cualquier forma que tuviese una estructura compleja sin importar cuánto la magnificases. Si la estructura en escalas pequeñas es la misma que en las grandes, el fractal se dice que es *auto similar*. Si solo las características estadísticas no varían con el cambio de escala, es *auto similar estadísticamente*. Los fractales más fáciles de entender son los auto similares. El triángulo de Sierpiński [véase ⁴⁶⁶/₈₈₅] es un ejemplo. Está hecho de tres copias de sí mismo, cada uno de la mitad de tamaño.

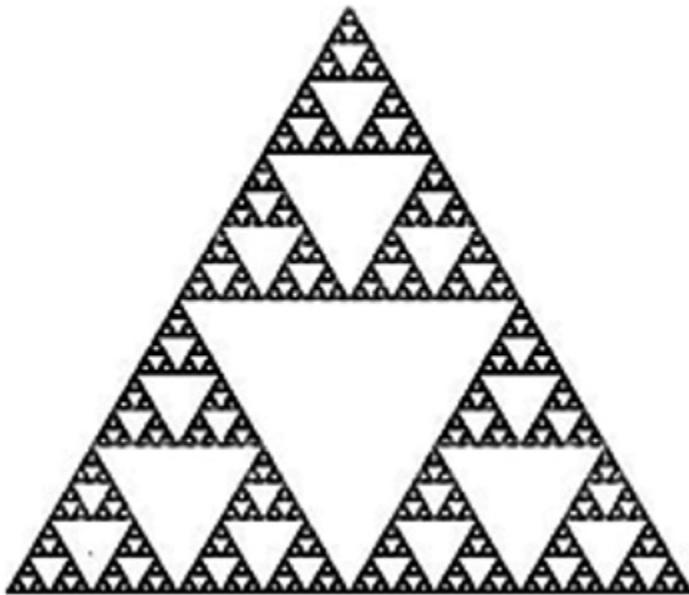


Figura 110. El triángulo de Sierpiński.

El copo de nieve es otro ejemplo. Puede formarse a partir de tres copias de la curva mostrada en la imagen de la derecha de la Figura 111. Este componente (aunque no todo el copo de nieve) es exactamente auto similar. Las etapas consecutivas en la construcción se forman con cuatro copias de la etapa anterior, cada una un tercio más grande. En el límite infinito, obtenemos una curva infinitamente compleja que se construye a partir de cuatro copias de sí misma, cada una de un tercio del tamaño. Esta forma es demasiado regular para representar una línea de costa real, pero tiene aproximadamente el grado de ondulación correcto, y curvas irregulares formadas de un modo similar pero con variaciones aleatorias se parecen a líneas de costa genuinas.

Los fractales están extendidos por todo el mundo natural. Siendo más precisos: formas que pueden ser *modeladas* por fractales de manera

rentable son comunes. No hay objetos matemáticos en el mundo real, son todos conceptos. Un tipo de coliflor llamada romanesco está hecha de minúsculos grumos, cada uno de los cuales tiene la misma forma que toda la coliflor. Las aplicaciones de los fractales van desde la estructura delicada de los minerales a la distribución de la materia en el universo. Los fractales se han usado como antenas para teléfonos móviles, para embutir grandes cantidades de datos en CD y DVD y para detectar células cancerígenas. Y de modo regular aparecen nuevas aplicaciones.

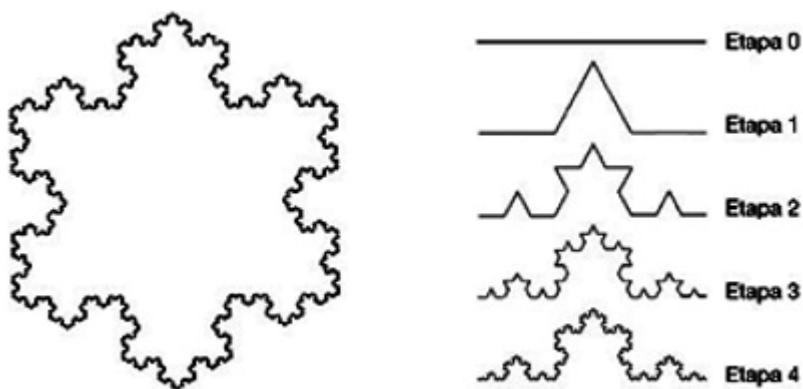


Figura 111. La curva del copo de nieve y las sucesivas etapas en su construcción.

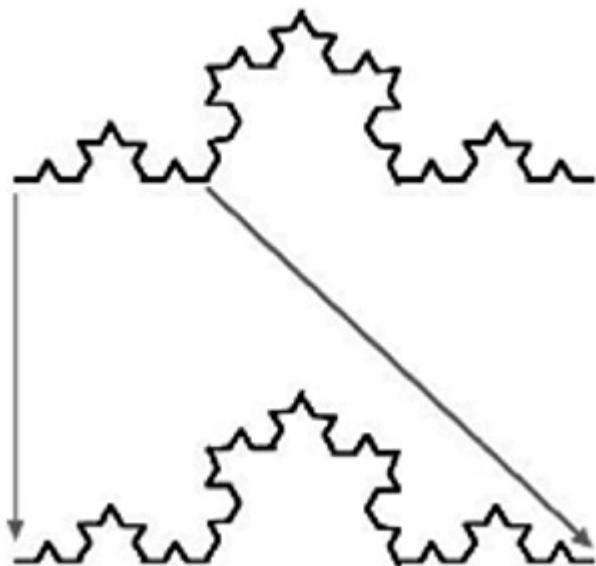


Figura 112. Cada cuarto de la curva, reducido en tres veces su tamaño, se parece a la curva original.



Figura 113. Romanesco

Dimensión fractal

La ondulación de un fractal o su efectividad rellenando el espacio pueden representarse por un número llamado «dimensión fractal». Para comprenderlo, primero consideramos formas no fractales más sencillas.

Si dividimos una recta en partes que sean $1/5$ del tamaño, necesitamos 5 de ellas para reconstruir la recta. Al hacer lo mismo con un cuadrado, necesitamos 25 partes, que es 5^2 . Con cubos necesitamos 125, que es 5^3 .

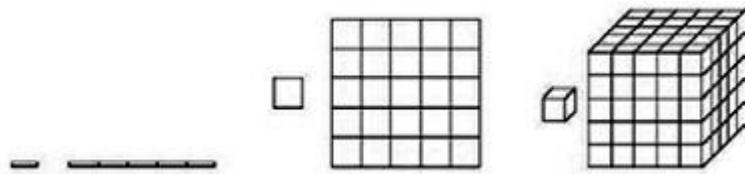


Figura 114. Efecto de escalar sobre «cubos» en dimensión 1, 2 y 3.

La potencia de 5 que aparece es igual a la dimensión de la forma: 1 para una recta, 2 para un cuadrado, 3 para un cubo. Si la dimensión es d y tenemos que encajar juntas k partes de tamaño $1/n$ para volver a montar la forma original, entonces $k = n^d$. Tomando logaritmos [véase e] y resolviendo para d , obtenemos la fórmula:

$$d = \frac{\log k}{\log n}$$

Probemos esta fórmula con el triángulo de Sierpiński. Para montar un triángulo a partir de copias más pequeñas, necesitamos $k = 3$ partes, cada que sea $1/2$ del tamaño. Por lo tanto, $n = 2$ y la fórmula obtenida es:

$$d = \frac{\log 3}{\log 2}$$

d es, aproximadamente, 1,5849. De modo que la dimensión del triángulo de Sierpiński, en este sentido en concreto, *no es un número entero*.

Cuando pensamos en dimensión en el sentido convencional, como el número de direcciones independientes disponibles, debe ser un número natural. Pero en lo que se refiere a fractales, estamos intentando medir lo irregulares o lo complejos que son, o lo bien que ocupan el espacio que les rodea, no en cuántas direcciones independientes pueden apuntar. El triángulo es visiblemente más denso que una línea, pero menos denso que un cuadrado sólido. De modo que la cantidad que queremos debería ser algo entre 1 (la dimensión de la recta) y 2 (la dimensión del cuadrado). Por lo tanto, *no puede ser* un número natural.

Podemos encontrar la dimensión fractal de la curva de un copo de nieve del mismo modo. Como antes, es más fácil trabajar con un tercio de la curva del copo de nieve, una de sus tres «aristas» idénticas, porque es auto similar. Para montar una arista de una curva del copo de nieve a partir de copias más pequeñas de la arista, necesitamos $k = 4$ partes, cada una $\frac{1}{3}$ del tamaño, de modo que $n = 3$. La fórmula obtenida es:

$$\textcolor{brown}{d} = \frac{\log 4}{\log 3}$$

que es aproximadamente 1,2618. De nuevo, la dimensión fractal no es un número entero y de nuevo tiene sentido. El copo de nieve es claramente

más ondulado que una recta, pero rellena el espacio peor que un cuadrado sólido. Otra vez, la cantidad que queremos debería ser algo entre 1 y 2, así que 1,2618 tiene mucho sentido. Una curva con dimensión 1,2618 es más ondulada que una curva de dimensión 1, como una línea recta, pero es menos ondulada que una curva de dimensión 1,5849, como es el triángulo de Sierpiński. La dimensión fractal de la mayoría de las líneas de costa está cerca de 1,25, más como el copo de nieve que como el triángulo de Sierpiński. Así que la dimensión es acorde con nuestra intuición sobre cuál de estos fractales es mejor llenando el espacio.

También da a los experimentalistas un modo cuantitativo de probar teorías basadas en fractales. Por ejemplo, como el hollín tiene una dimensión fractal alrededor de 1,8, los modelos fractales de la deposición del hollín, de la cual hay muchos, puede comprobarse viendo si da ese número.

Hay muchos modos diferentes de definir la dimensión de un fractal cuando no es auto similar. Los matemáticos usan la *dimensión de Hausdorff-Besicovitch*, bastante complicada de definir. Los físicos a menudo usan una definición más sencilla, la dimensión del *conteo de cajas*. En muchos casos, aunque no siempre, estas dos nociones de dimensión son la misma. Entonces usamos el término *dimensión fractal* para referirnos a cualquiera de ellas. Los primeros fractales eran curvas, pero pueden ser superficies, sólidos o formas de dimensiones mayores.

Ahora la dimensión fractal mide lo rugoso que es un fractal o lo efectivo que es llenando el espacio.

Las dos dimensiones fractales vistas son irracionales. Para el supuesto de que

$$\frac{\log 3}{\log 2} = \frac{p}{q}$$

con p y q enteros, entonces $q \log 3 = p \log 2$, de modo que $\log 3^q = \log 2^p$, así que $3^q = 2^p$. Pero esto contradice la unicidad de la factorización en primos. Un razonamiento parecido funciona para

$$\frac{\log 4}{\log 3}$$

Es extraordinario cómo hechos básicos como este aparecen en lugares inesperados, ¿no?

El conjunto de Mandelbrot

Quizá el fractal más famoso de todos es el conjunto de Mandelbrot. Representa qué ocurre a un número complejo si repetidamente lo elevas al cuadrado y sumas una constante. Es decir, escoges una constante compleja c , entonces formas $c^2 + c$, luego $(c^2 + c)^2 + c$, luego $((c^2 + c)^2 + c)^2 + c$, y así sucesivamente. (Hay otros modos de definir el conjunto pero este es el más sencillo.) Geométricamente, los números complejos

viven en el plano, extendiendo la recta habitual para los números reales. Hay dos posibilidades principales: o bien todos los números complejos en la secuencia anterior permanecen dentro de una región finita del plano complejo, o bien no lo hacen. Se colorea de negro esos c para los cuales la secuencia permanece dentro de cierta región finita, y aquellos que se escapan, de blanco. El conjunto de todos los puntos negros es el conjunto de Mandelbrot y tiene este aspecto:

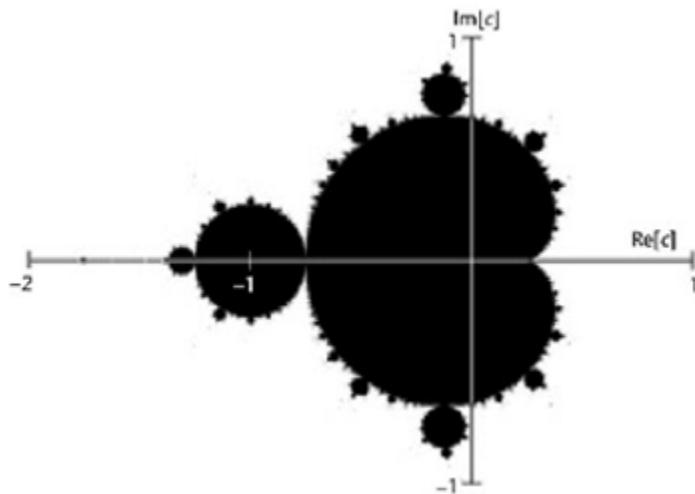


Figura 115. Conjunto de Mandelbrot.

La frontera del conjunto de Mandelbrot, los puntos en la arista, tan cerca como queramos tanto de los puntos negros como de los blancos, es un fractal. Su dimensión fractal resulta ser 2, de modo que es «casi recubrimiento del espacio». Para verlo con más detalle, podemos colorear los puntos blancos según lo rápido que la secuencia tiende a infinito. Ahora obtenemos un diseño extraordinariamente complejo, lleno de florituras y espirales y otras formas. Haciendo *zoom* para

ampliar la imagen nos lleva a niveles de detalle cada vez mayores. Puedes incluso encontrar conjuntos de Mandelbrot «hijos» completos si miras en los lugares correctos.

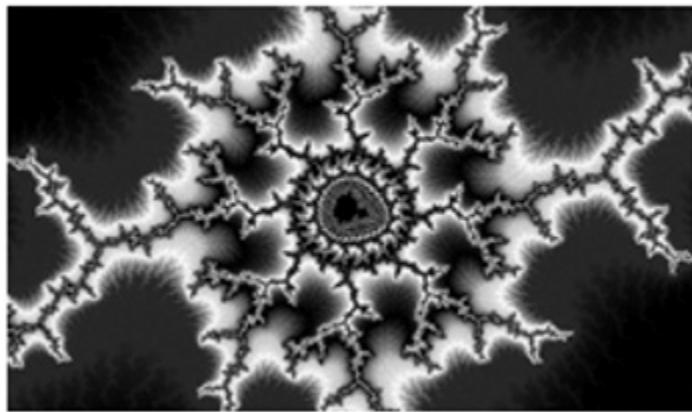


Figura 116. Un conjunto de Mandelbrot «hijo».

El conjunto de Mandelbrot como tal parece no tener ninguna aplicación importante, pero es uno de los sistemas dinámicos no lineales más sencillos basado en números complejos, de modo que ha atraído la atención de matemáticos en busca de principios generales que podrían tener una mayor aplicación. También demuestra un punto «filosófico» clave: reglas sencillas pueden llevar a resultados complicados, es decir, causas sencillas pueden tener efectos complicados. Es muy tentador, cuando se intenta comprender un sistema muy complicado, esperar que las reglas subyacentes sean igual de complicadas. El conjunto de Mandelbrot prueba que esta expectativa puede ser errónea. Esta percepción conforma el todo de la «ciencia de la complejidad», un área

nueva que intenta reconciliarse con sistemas aparentemente complicados, buscando reglas sencillas que conduzcan a ellos.

§. $\frac{\pi}{\sqrt{18}} \sim 0,740480$ Empaquetamiento de esferas

El número $\frac{\pi}{\sqrt{18}}$ es de importancia fundamental en matemáticas, física y química. Es la fracción del espacio que se llena cuando hacemos un paquete de esferas idénticas de la manera más eficiente, es decir, dejando el menor espacio posible vacío. En 1611 Kepler hizo conjeturas sobre este resultado, pero no se probó hasta que Thomas Hales completó una prueba asistida por ordenador en 1998. Todavía no se ha encontrado una prueba que un humano pueda comprobar directamente.

Paquetes de círculos

Empezamos con la pregunta más sencilla sobre el empaquetado de círculos idénticos en el plano. Si experimentas con unas docenas de monedas de la misma cantidad y las empujas unas contra otras para encajar tantas como sea posible, rápidamente encuentras que un ordenamiento aleatorio deja mucho espacio vacío. Si intentas librarte del espacio empujando las monedas más apretadas, parece que se empaquetan de modo más eficiente si las colocas siguiendo el patrón de un panal.

Sin embargo, se podría pensar que algún otro orden más ingenioso las apiñe de modo todavía más ajustado. No parece que esto sea probable,

pero no hay una prueba. Hay infinidad de modos de ordenar monedas idénticas, así que ningún experimento puede hacerse con todos.

El patrón del panal es muy regular y simétrico, a diferencia de ordenaciones aleatorias. Es también *rígido*: no puedes mover ninguna de las monedas, porque las otras la obligan a estar en una posición fija. A primera vista, una ordenación rígida debería llenar el espacio de modo más eficiente, porque no hay un modo de cambiarlo a una ordenación mejor moviendo monedas de una en una.



Figura 117. Izquierda: un ordenamiento aleatorio deja mucho espacio desaprovechado. Derecha: un patrón de panal se libra de la mayoría de los huecos.

Sin embargo, hay otros ordenamientos rígidos que son menos eficientes. Empecemos con los dos modos obvios de empaquetar círculos en un patrón regular:

- El entramado hexagonal o de panal, llamado así porque los centros de los círculos forman hexágonos.

- El entramado cuadrado, donde los círculos están ordenados como los cuadrados de un tablero de ajedrez.

El entramado cuadrado es también rígido, pero empaqueta los círculos de manera menos eficiente. Si haces patrones muy grandes, el entramado hexagonal cubre una mayor proporción del espacio en cuestión.



Figura 118. Izquierda: seis centros forman un hexágono regular.

Derecha: un empaquetado de entramado cuadrado.

Para hacer todo esto preciso, los matemáticos definieron la densidad de un empaquetado de círculos como el límite de la proporción de un área dada que es cubierta por los círculos, a medida que la región se va haciendo cada vez más grande. De modo informal, la idea es cubrir el *plano entero* con círculos y averiguar qué fracción del área está cubierta. Tomándolo literalmente, esta proporción es ${}^\circ/\infty$, que no tiene significado, de modo que cubrimos cuadrados cada vez más grandes y consideramos el límite.

Calculamos la densidad del empaquetado que usa el entramado de cuadrados. Si cada cuadrado tiene por área la unidad, los círculos tienen radio $\pi/2$, de modo que su área es $(\pi/2)^2 = \pi/4$. Para muchos cuadrados y muchos círculos, la proporción cubierta no cambia. De modo que, en el límite, obtenemos una densidad de $\pi/4$, que es aproximadamente 0,785.

Un cálculo más complicado para el entramado hexagonal nos lleva a una densidad de $\pi/\sqrt{12}$, aproximadamente 0,906, que es mayor que la densidad para el entramado de cuadrados.

En 1773, Lagrange probó que el entramado hexagonal da el empaquetado para círculos más denso en el plano. Pero esto dejó abierta la posibilidad de que una colocación menos regular pudiera hacerlo mejor. Se necesitaron 150 años para que los matemáticos eliminasesen esta posibilidad poco probable. En 1892, Axel Thue dio una conferencia bosquejando una prueba de que ningún empaquetado de círculos en el plano puede ser más denso que el entramado hexagonal, pero los detalles publicados son demasiados vagos para averiguar lo que la prueba propuesta era, menos aún para decidir si era correcta. Dio una nueva prueba en 1910, pero todavía tenía algunos vacíos en la lógica. La primera prueba completa la publicó Laszlo Fejes Tóth en 1940. Poco después, Beniamino Segre y Kurt Mahler encontraron pruebas alternativas. En 2010, Hai-Chau Chang y Lih-Chung Wang publicaron en la web una prueba más sencilla.

Conjetura de Kepler

La conjetura de Kepler trata sobre el problema análogo para empaquetar esferas idénticas en el espacio. A principios del siglo XVII, el gran matemático y astrónomo Kepler enunció su conjetura, en un libro sobre copos de nieve.

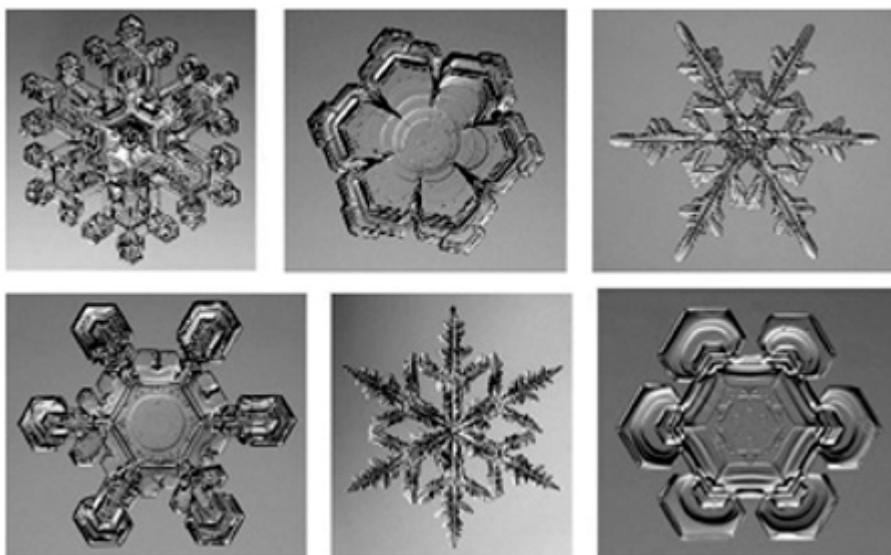


Figura 119. Estas imágenes muestran cristales de nieve reales que cayeron a tierra en Ontario, Alaska, Vermont, la península superior de Michigan y las montañas de Sierra Nevada de California. Fueron tomadas por Kenneth G. Libbrecht usando un fotomicroscopio especialmente diseñado para copos de nieve.

Kepler estaba interesado en copos de nieve porque con frecuencia tienen simetría séxtuple: repitiendo casi exactamente la misma forma seis veces, espaciada en ángulos iguales de 60° . Se preguntó por qué, y usó

lógica, imaginación y su conocimiento de patrones similares en la naturaleza para dar una explicación que está extraordinariamente próxima a la que conocemos hoy en día.

Kepler era el matemático de la corte del emperador Rodolfo II del Sacro Imperio Romano Germánico, y su trabajo fue financiado por John Wacker de Wackenfels, un rico diplomático y uno de los consejeros del emperador. En 1611, hizo a su mecenas un regalo de Año Nuevo: un libro expresamente escrito *De Nive Sexangula* («Sobre los copos de nieve de seis esquinas»). Empezó preguntando por qué los copos de nieve tenían seis lados. Para obtener una respuesta, analizó formas naturales que también tienen simetría séxtuple, como los panales en una colmena y las semillas dentro de una granada. Acabamos de ver que empaquetar círculos en el plano lleva de modo natural al patrón del panal. Kepler explicó la forma simétrica de los copos de nieve en términos de empaquetamientos de esferas en el espacio.

Sorprendentemente se acercó mucho a la explicación moderna: un copo de nieve es un cristal de hielo, cuya estructura atómica es muy similar a la de un panal. En concreto, tiene simetría hexagonal (en realidad, un poco más simétrico). La diversidad de las formas de los copos de nieve, todos con la misma simetría, resulta de las condiciones de cambio en las nubes de tormenta donde los copos se generan.

A lo largo del camino, Kepler hizo un comentario bastante casual, planteando un rompecabezas matemático que tardaría 387 años en

resolverse. ¿Cuál es el modo más eficiente de empaquetar esferas idénticas en el espacio? Sugirió que la respuesta debería ser lo que ahora llamamos «estructura cúbica centrada en las caras» (FCC por sus siglas en inglés, *face-centred cubic*).

Así es como normalmente los fruteros apilan las naranjas. Primero, haz una capa plana de esferas formando una rejilla cuadrada (Figura 120, izquierda). Luego haz una capa parecida encima, colocando cada esfera en las hendiduras entre cuatro esferas vecinas en la capa inferior (medio). Continúa de este modo (derecha) hasta que rellenes todo el espacio. Esto requiere extender cada capa hacia los lados para llenar un plano entero y colocar capas bajo la primera así como en la cima. La densidad de este empaquetado puede calcularse y es $\pi/\sqrt{18} \approx 0,740480$. Según Kepler, esta ordenación debería ser «el empaquetado más apretado», es decir, tiene la mayor densidad que es posible.

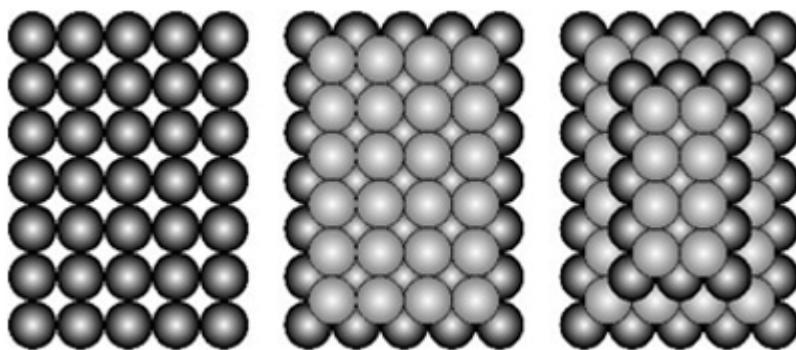


Figura 120. Estructura FCC. Izquierda: primera capa. Centro: primeras dos capas. Derecha: primeras cuatro capas.

Los fruteros empiezan con una caja o tablero y trabajan a partir de ahí hacia arriba capa a capa y esa es una manera de definir la estructura FCC. Pero el problema de Kepler pregunta sobre todos los empaquetamientos posibles, de modo que no podemos asumir que todo viene en capas planas. En realidad, el método del frutero soluciona un problema diferente. La pregunta es: ¿cambia eso la respuesta?

A primera vista el empaquetamiento del frutero parece la respuesta *equivocada*, porque usa capas de entramado de cuadrados y un entramado hexagonal es más denso. Los fruteros usan capas cuadradas porque colocan sus naranjas en cajas rectangulares, no porque quieran el empaquetado más apretado. ¿No sería mejor que la primera capa fuese un entramado hexagonal? De nuevo, capas sucesivas encajarían en las hendiduras de la capa inferior, cada una colocada siguiendo el mismo entramado hexagonal.

Kepler se dio cuenta de que no había diferencia alguna. El lado inclinado de la Figura de la derecha forma un entramado hexagonal. Capas paralelas a esa son también entramados hexagonales, encajando en las hendiduras de las capas vecinas. Por lo tanto, la ordenación alternativa usando capas hexagonales es solo una versión inclinada de la estructura FCC.

Sin embargo, sí nos dice algo significativo: empaquetado *infinitamente* diferentes, casi todos los que *no* son entramados, tienen la misma densidad que la estructura FCC. Hay dos modos diferentes de encajar un

entramado hexagonal en las hendiduras de otro y para cada capa sucesiva podemos escoger cualquier alternativa. Con dos capas, una ordenación es una rotación de la otra, pero a partir de tres capas en adelante eso ya no ocurre. Así que hay dos ordenaciones genuinamente diferentes para 3 capas, cuatro para 4 capas, ocho para 5 capas, y así sucesivamente. Con todas las capas en su lugar, el número de posibilidades es infinito. Sin embargo, cada capa tiene la misma densidad y las capas están igual de próximas para cualquier elección de hendiduras. De modo que la densidad es $\pi/\sqrt{18}$ para cualquier serie de elecciones. La existencia de infinidad de empaquetados con la misma densidad es un aviso de que el problema de Kepler esconde algunas sutilezas.

La conjetura de Kepler no se probó hasta 1998, cuando Thomas Hales y su discípulo Samuel Ferguson completaron una prueba asistida por ordenador. Hales envió la prueba a la prestigiosa publicación *Annals of Mathematics* en 1999. La comisión de expertos necesitó cuatro años para comprobarlo, pero los cálculos eran tan complicados y grandes que se sintieron incapaces de certificar su completa corrección. Finalmente, la prueba se publicó, pero con una nota que indicaba esta dificultad.

Irónicamente, la forma de evitar este problema probablemente sea reescribir la prueba de un modo cuya corrección pueda ser verificada... por un ordenador. El objetivo es que el programa de verificación sea probablemente más sencillo que la prueba de Hales, de modo que podría ser posible comprobar la lógica del *software* de verificación a mano.

Entonces podemos tener la seguridad de que hace lo que dice, lo cual es verificar la prueba mucho más compleja de la conjetura de Kepler.

Atento a esto.

§. $\sqrt[12]{2} \sim 1,059463$ Escala musical

La raíz duodécima de 2 es la razón de las frecuencias de notas sucesivas en la equitemperada escala musical. Es un acuerdo como aproximar π a $\frac{22}{7}$, excepto que esta vez los intervalos musicales naturales son números racionales sencillos y las potencias de $\sqrt[12]{2}$ proporcionan aproximaciones irracionales a estos. Aparece debido al modo en que el oído humano percibe el sonido.

Ondas de sonido

Físicamente, una nota musical es una onda de sonido, producida por un instrumento musical y detectada por el oído. Una onda es una perturbación en un sólido, líquido o gas que viaja sin cambiar su forma, o repite el mismo movimiento una y otra vez de manera regular. Las ondas son comunes en el mundo real; las ondas de luz, las ondas de sonido, las olas y las vibraciones son ejemplos. Las ondas en la Tierra provocan terremotos.

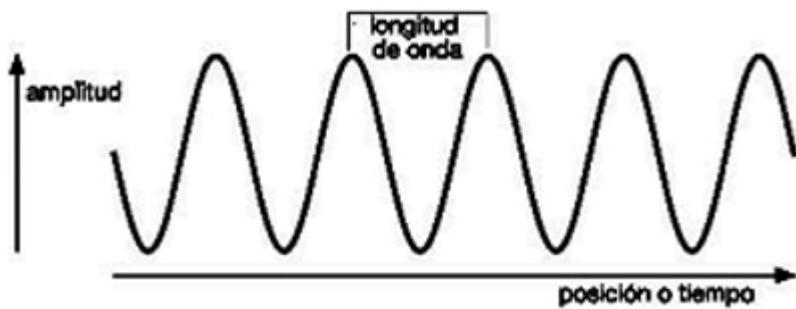


Figura 121. Curva sinusoidal.

La forma más básica y sencilla para una onda es una curva sinusoidal. La altura de la curva representa la *amplitud* de la onda, una medida de lo grande que es la perturbación correspondiente. Para las ondas de sonido esto se corresponde con lo alta que es la nota: una amplitud mayor perturba más el aire, lo que perturba más el oído y nos hace percibir un incremento en la sonoridad.

Otra característica importante de la curva sinusoidal es su *longitud* de onda: la distancia (o tiempo que transcurre) entre picos consecutivos de la amplitud. La longitud de onda determina la forma de la onda. Para las ondas de sonido, la longitud de onda determina el tono de la nota. Longitudes de onda más cortas hacen que la nota suene más alto, y longitudes de onda más largas hacen que la nota suene más baja.

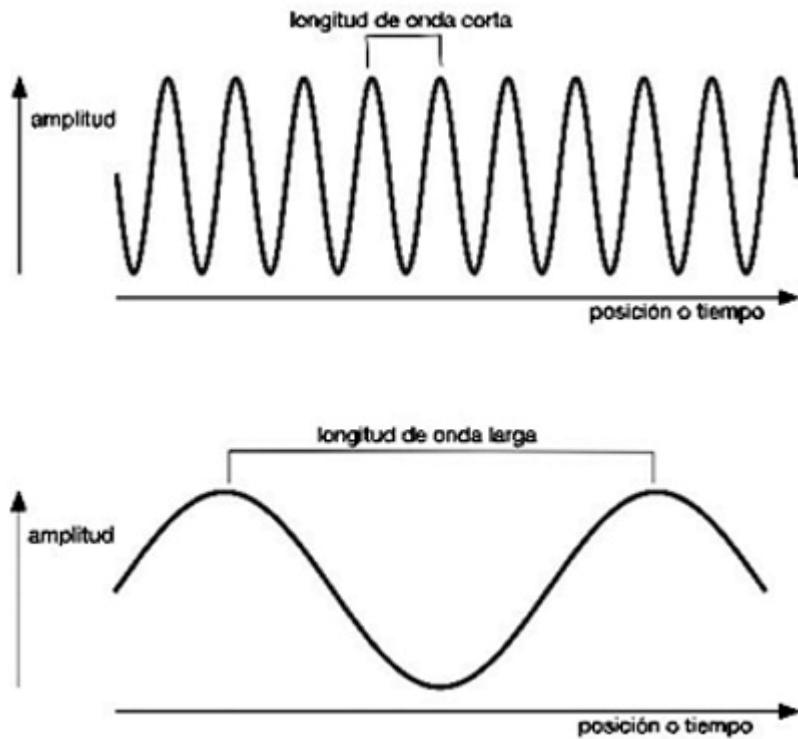


Figura 122. Longitud de onda.

Hay otro modo de medir la misma característica de la onda, lo que se conoce como su *frecuencia*, que es inversamente proporcional a la longitud de onda. Esto corresponde al número de picos de onda que aparecen en una distancia o tiempo dados. Las frecuencias son medidas en una unidad llamada «hercio» (Hz), que es una vibración por segundo. Por ejemplo, do central en un piano tiene una frecuencia de 261,62556 hercios, lo que quiere decir que cada segundo se dan algo más de 261 vibraciones.



Figura 123. Notación musical básica.

El do una octava más alta tiene una frecuencia de 523,25113 hercios: exactamente el doble de grande. El do una octava menor tiene una frecuencia de 130,81278 hercios: exactamente la mitad de grande. Estas relaciones son ejemplos básicos de cómo se vinculan con la música las matemáticas de ondas. Para profundizar más en el tema piensa en instrumentos de cuerda, como un violín o una guitarra, y por un momento considera solo una cuerda.

Supongamos que el instrumento está sobre uno de sus lados y estamos mirándolo de frente. Cuando el músico puntea la cuerda, vibra de lado a lado respecto al instrumento; para nosotros se mueve de arriba abajo. Esto lleva a un tipo de onda llamada «onda estacionaria», en la cual el final de la cuerda permanece fijo pero la forma cambia en un ciclo periódico.

La vibración más sencilla se da cuando la cuerda forma la mitad de la onda sinusoidal. La siguiente vibración más sencilla es una onda

sinusoidal completa. Después de eso viene una onda sinusoidal y media, luego 2 ondas sinusoidales, y así sucesivamente. Medias ondas aparecen porque una onda sinusoidal completa cruza la horizontal una vez en el medio, así como en cada extremo.

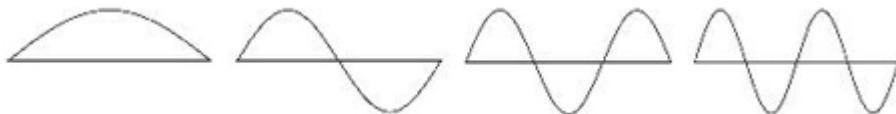


Figura 124. De izquierda a derecha: la mitad de una onda sinusoidal; una onda sinusoidal completa; una onda sinusoidal y media; dos ondas sinusoidales.

Aquí las longitudes de onda son $\frac{1}{2}$, 1, $\frac{3}{2}$, 2, y así sucesivamente. Las mitades están presentes porque estamos usando mitades de ondas. Si optamos por trabajar en unidades tales como que la longitud de la cuerda es $\frac{1}{2}$, entonces las longitudes de onda pasan a ser 1, 2, 3, 4, que resulta más sencillo.

Las frecuencias correspondientes, para la misma cuerda mantenida con la misma tensión están en razones de $1\frac{1}{2}$, $\frac{1}{3}$, $\frac{1}{4}$. Por ejemplo, si la vibración de media onda tiene frecuencia 261 hercios, cerca de do central, entonces estas frecuencias son:

$$261$$

$$261/2 = 130,5 \text{ Hz}$$

$$261/3 = 87 \text{ Hz}$$

$$261/4 = 65,25 \text{ Hz}$$

La media onda básica se llama la «fundamental» y las otras son «armónicos sucesivos».

Hace unos 2.500 años, los pitagóricos creían que todo en el mundo estaba gobernado por formas matemáticas y patrones numéricos. Descubrieron una relación extraordinaria entre números y armonía musical. Según la leyenda, Pitágoras estaba paseando por delante de la tienda de un herrero y observó que los martillos de diferentes tamaños emitían sonidos de diferente tono, y que martillos relacionados por números sencillos (uno el doble del tamaño que otro, por ejemplo) hacían ruidos que estaban en consonancia. Sin embargo, si intentas observar esto con martillos reales, descubrirás que la forma complicada de los martillos dificulta que vibren en armonía. Pero es cierto que, en conjunto, objetos pequeños hacen ruidos de tonos más altos que los grandes.

Un experimento pitagórico más plausible usaba una cuerda estirada, como Ptolomeo relata en su *Armónicas*, alrededor de 150 d. C. Los pitagóricos descubrieron que dos cuerdas con igual tensión y que tienen longitudes con una proporción sencilla, como $\frac{2}{1}$ o $\frac{3}{2}$, producen notas inusualmente armoniosas. Proporciones más complejas son discordantes y desagradables de escuchar.

Intervalos musicales

Los músicos describen pares de notas en términos de intervalos entre ellos, una medida de cuántos grados los separan en alguna escala musical. El intervalo más fundamental es la octava: avanza siete teclas blancas en un piano. Las notas que se separan una octava suenan muy parecidas, excepto que una nota es más alta que la otra, y son tremadamente armoniosas. Tanto es así que, de hecho, las armonías basadas en la octava pueden parecer un poco sosas. En un violín o una guitarra, el modo de tocar la nota una octava superior sobre una cuerda suelta es presionar la mitad de esa cuerda contra el diapasón. Una cuerda la mitad de larga toca una nota una octava mayor. Por lo tanto, la octava está asociada con una proporción numérica sencilla de $\frac{2}{1}$.

Otros intervalos armoniosos también se asocian con proporciones numéricas sencillas. Las más importantes para la música occidental son la cuarta, una proporción de $\frac{4}{3}$, la quinta, una proporción de $\frac{3}{2}$. (Los nombres tienen sentido si consideras una escala musical de todas las notas do-re-mi-fa-sol-la-si-do. Con do como base, la nota correspondiente a la cuarta es fa, a la quinta es sol y a la octava do. Si numeramos las notas consecutivamente con la base como 1, estas son respectivamente la 4^a, 5^a y 8^a notas de la escala.)

La geometría es especialmente clara en un instrumento como una guitarra, que tiene segmentos de metal llamados trastes insertados en

posiciones relevantes. El traste de la cuarta está a un cuarto del camino a lo largo de la cuerda, que para un quinto está a un tercio del camino y la octava es a mitad de camino. Puedes comprobarlo con una cinta métrica.

Escalas

Estas proporciones aportan una base teórica para una escala musical y llevaron a la escala que ahora usamos en la mayoría de la música occidental. Hay muchas escalas musicales diferentes, y describimos solo la más sencilla. Empieza con una nota base y asciende en quintos para obtener cuerda de longitudes:

$$1 \quad \frac{3}{2} \quad \left(\frac{3}{2}\right)^2 \quad \left(\frac{3}{2}\right)^3 \quad \left(\frac{3}{2}\right)^4 \quad \left(\frac{3}{2}\right)^5$$

Operando, estas fracciones pasan a ser:

$$1 \quad \frac{3}{2} \quad \frac{9}{4} \quad \frac{27}{8} \quad \frac{81}{16} \quad \frac{243}{32}$$

Todas estas notas, excepto las dos primeras, son demasiado agudas para permanecer en la octava, pero podemos bajarlas en una o más octavas, dividiendo repetidamente las fracciones entre 2 hasta que el resultado esté entre 1 y 2. Esto da lugar a las fracciones:

$$\begin{array}{cccccc} 1 & \frac{3}{2} & \frac{9}{4} & \frac{27}{16} & \frac{81}{64} & \frac{243}{128} \end{array}$$

Finalmente, las colocamos en orden ascendente y obtenemos:

$$\begin{array}{cccccc} 1 & \frac{9}{8} & \frac{81}{64} & \frac{3}{2} & \frac{27}{16} & \frac{243}{128} \end{array}$$

Esto se corresponde de modo bastante aproximado a las notas do, re, mi, sol, la, si en un piano.

Observa que falta fa. De hecho, al oído, el hueco entre $\frac{81}{64}$ y $\frac{3}{2}$ suena más amplio que los otros. Para llenar el hueco, insertamos $\frac{4}{3}$, la proporción para la cuarta, que es muy próxima a fa en el piano. También es útil completar la escala con un segundo do, una octava más alta, una razón de 2. Ahora obtenemos una escala musical basada completamente en cuartas, quintas, octavas, con tonos en las proporciones

$$\begin{array}{ccccccccc} 1 & \frac{9}{8} & \frac{81}{64} & \frac{4}{3} & \frac{3}{2} & \frac{27}{16} & \frac{243}{128} & 2 \\ Do & Re & Mi & Fa & Sol & La & Si & Do \end{array}$$

La longitud es inversamente proporcional al tono, así que tendríamos que invertir las fracciones para obtener las correspondientes longitudes.

Hemos representado todas las notas blancas en el piano, pero también hay notas negras. Estas aparecen porque números consecutivos en la

escala dan dos razones diferentes respecto a los otros: $\frac{9}{8}$ (llamado «tono») y $\frac{256}{243}$ («semitono»). Por ejemplo, la razón de $\frac{81}{64}$ respecto a $\frac{9}{8}$ es $\frac{9}{8}$, pero la de $\frac{4}{3}$ respecto a $\frac{81}{64}$ es $\frac{81}{64}$. Los nombres «tono» y «semitono» indican una comparación aproximada de los intervalos. Numéricamente son 1,125 y 1,05. El primero es mayor, así un tono se corresponde con un cambio más grande en el tono que un semitono. Dos semitonos dan una razón de $1,05^2$, que es aproximadamente 1,11, que no está lejos de 1,125. Por lo tanto, dos semitonos están cerca de un tono.

Continuando de esta manera, podemos dividir cada tono en dos intervalos, cada uno cercano al semitono, para obtener una escala de 12 notas. Esto puede hacerse de varias maneras diferentes, que producen resultados ligeramente distintos. Sin embargo, si se hace, puede haber problemas sutiles pero audibles cuando se cambia la clave de una pieza de música; los intervalos cambian ligeramente si, por ejemplo, movemos cada nota un tono más alto. En algunos instrumentos musicales, como el clarinete, esto puede provocar problemas técnicos serios, porque las notas se crean por aire pasando a través de agujeros en el instrumento, los cuales están en posiciones fijas. En otros, como el violín, se puede producir un rango continuo de notas, de manera que el músico puede ajustar la nota más sutilmente.

En otros, como la guitarra y el piano, se usa un sistema matemático diferente. Evita el problema de cambiar la clave, pero requiere algunos compromisos sutiles. La idea es hacer que el intervalo entre notas

consecutivas en la escala tenga exactamente el mismo valor. El intervalo entre dos notas depende de la proporción de sus frecuencias, de modo que para producir un intervalo dado tomamos la frecuencia de una nota y la *multiplicamos* por alguna cantidad fija para obtener la frecuencia de la otra.

¿Cuál debería ser la cantidad para un semitono?

Doce semitonos hacen una octava, una proporción de 2. Para obtener una octava, debemos tomar la frecuencia con la que empezamos y multiplicarla por alguna cantidad fija, correspondiente a un semitono, doce veces consecutivas. El resultado debe ser el doble de la frecuencia original. De modo que la razón para un semitono, elevado a la duodécima potencia, debe ser igual a 2. Es decir, la razón para un semitono debe ser la raíz duodécima de 2. Esto se escribe como $\sqrt[12]{2}$ y es aproximadamente 1,059463.

La gran ventaja de esta idea es que ahora muchas relaciones musicales funcionan *perfectamente*. Dos tonos hacen un semitono exacto y 12 semitonos hacen una octava. Mejor todavía, puedes cambiar la clave, donde la escala empieza, desplazando hacia arriba o hacia abajo todas las notas una cantidad fija.

Este número, la raíz duodécima de 2, lleva a la escala *equitemperada*. Es un acuerdo, por ejemplo, en la escala equitemperada la razón $4/3$ para un cuarto es $1,059^2 = 1,335$, en lugar de $4/3 = 1,333$. Un músico entrenado

puede detectar la diferencia, pero es fácil acostumbrarse a ella y la mayoría de nosotros nunca la notamos.

Es un número irracional. Supongamos que $\sqrt[12]{2} = p/q$ donde p y q son enteros. Entonces $p^{12} = 2q^{12}$. Factoriza ambos lados en factores primos. La parte de la izquierda tiene un número par (quizás 0) de 2. La parte de la derecha tiene un número impar. Esto contradice la factorización única en factores primos.

Cuerdas vibrantes y tambores

Para explicar por qué proporciones sencillas van de la mano con la armonía musical, tenemos que echar un vistazo a la física de las cuerdas vibrantes.

En 1727, John Bernoulli hizo el primer gran avance describiendo el movimiento de un sencillo modelo matemático de una cuerda de violín. Encontró que, en el caso más sencillo, la forma de la cuerda vibrante, en cualquier momento, es una curva sinusoidal. La amplitud de la vibración también forma una curva sinusoidal, en el tiempo más que en el espacio.

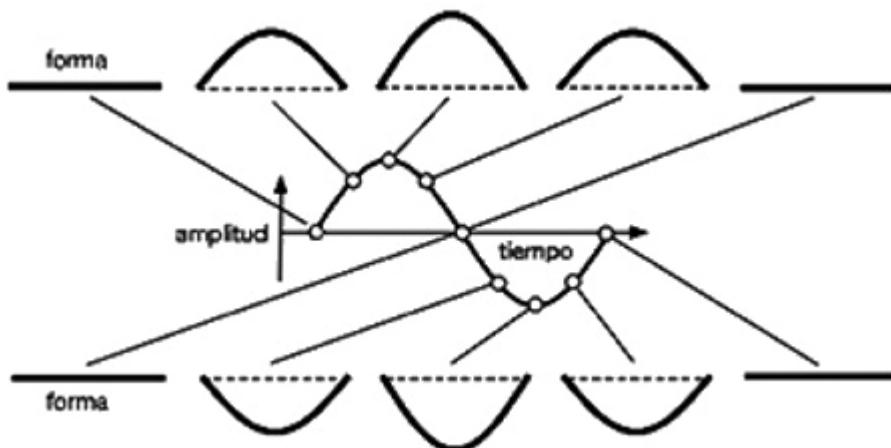


Figura 125. Instantáneas sucesivas de una cuerda vibrante. La forma es una curva sinusoidal en cada instante. La amplitud también varía sinusoidalmente con el tiempo.

Aunque había otras soluciones. Eran todas curvas sinusoidales, pero describían diferentes «modos» de vibración, con 1, 2, 3 o más ondas a lo largo de la longitud de la cuerda. De nuevo, la curva sinusoidal era una instantánea de la forma en cualquier instante, y su amplitud estaba multiplicada por un factor dependiente del tiempo, que también variaba sinusoidalmente.

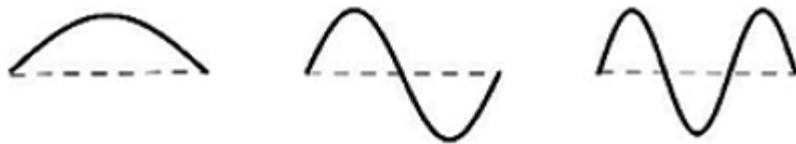


Figura 126. Instantáneas de los modos 1, 2, 3 de una cuerda vibrante. En cada caso, la cuerda vibra hacia arriba y hacia abajo, y su amplitud varía sinusoidalmente con el tiempo. Cuantas más ondas haya, más rápida es la vibración.

La cuerda está siempre en reposo en sus extremos. En todos los modos excepto el primero, hay puntos entre los extremos en los que la cuerda tampoco está vibrando, donde la curva se cruza con el eje horizontal. Estos «nodos» explican por qué se dan razones numéricas sencillas en los experimentos pitagóricos. Por ejemplo, como los modos

vibracionales 2 y 3 pueden darse en la misma cuerda, el hueco entre nodos sucesivos en la curva modo-2 es $\frac{3}{2}$ veces el hueco correspondiente en la curva modo 3. Esto explica por qué razones como $\frac{3}{2}$ surgen de modo natural a partir de las dinámicas de la cuerda vibrante.

El paso final es comprender por qué estas razones son armoniosas mientras que otras no lo son.

En 1746, Jean le Rond D'Alembert descubrió que las vibraciones de una cuerda obedecen a una ecuación matemática, llamada «ecuación de ondas». Describe cómo las fuerzas que actúan en la cuerda (su propia tensión y fuerzas como puntear la cuerda o usar un arco para moverla hacia los lados) afectan a su movimiento. D'Alembert se dio cuenta de que podía combinar las soluciones de curva sinusoidal de Bernoulli. Para simplificar la historia, considera solo un instante en un tiempo fijo, librándose de la dependencia del tiempo. La imagen muestra la forma de

$$5 \operatorname{sen} x + 4 \operatorname{sen} 2x - 2 \cos 6x$$

por ejemplo que es mucho más compleja que una simple curva del seno. Los instrumentos musicales reales normalmente producen ondas complejas en las que se ven involucrados diferentes términos de seno y coseno.

Para no complicar las cosas, echemos un vistazo a $\sin 2x$, que tiene una frecuencia del doble de $\sin x$. ¿Cómo suena? Es la nota *una octava mayor*, la que suena más armoniosa cuando se toca junto a la fundamental. Ahora, la forma de la cuerda para el segundo modo ($\sin 2x$) corta al eje en su punto medio. En ese nodo, permanece fijo. Si colocas tu dedo en ese punto, las dos mitades de la cuerda todavía serían capaces de vibrar según el patrón de $\sin 2x$, pero no en el de $\sin x$. Esto explica el descubrimiento pitagórico de que una cuerda la mitad de larga produce una nota una octava más alta. Una explicación similar funciona con las otras proporciones sencillas que descubrieron; todas están asociadas con curvas sinusoidales cuyas frecuencias tiene esa proporción, y esas curvas encajan perfectamente en una cuerda de longitud fija cuyos extremos no está permitido mover.

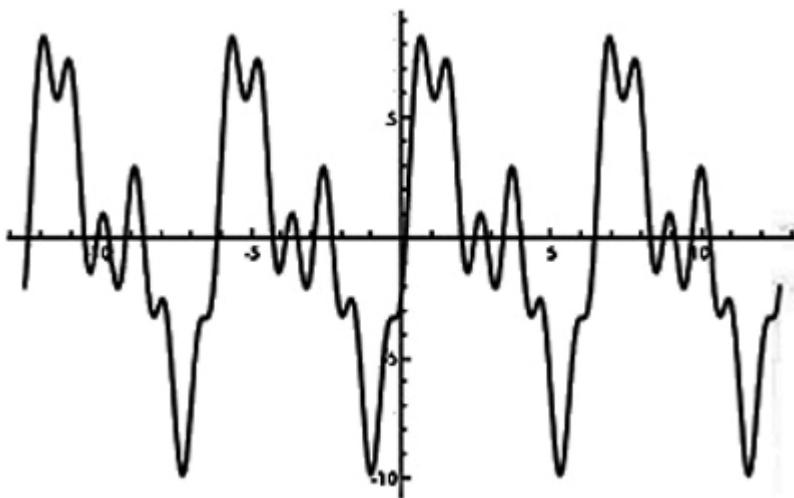


Figura 127. Combinación típica de senos y cosenos con varias amplitudes y frecuencias.

¿Por qué estas razones suenan armoniosas? En parte porque las ondas sinusoidales con frecuencias que no están en proporciones sencillas producen un efecto llamado «batimiento» cuando se superponen. Por ejemplo, a una razón como $\frac{8}{7}$ le corresponde $\sin 7x + \sin 8x$, que tiene esta forma de onda.

El sonido resultante es como un zumbido agudo que se va haciendo más alto y luego más suave. El oído responde a los sonidos entrantes aproximadamente del mismo modo que la cuerda del violín. Así, cuando dos notas chocan (se batan), el resultado no suena armonioso.

Aunque hay un factor extra. Los oídos de los bebés se adaptan a los sonidos que oyen con más frecuencia mientras su cerebro se desarrolla. De hecho, hay más conexiones nerviosas desde el cerebro al oído de las que hay en otra dirección y el cerebro puede usarlas para ajustar la respuesta del oído a los sonidos entrantes. De modo que lo que consideramos armonioso tiene una dimensión cultural. Pero las proporciones más sencillas son de manera natural más armoniosas y la mayoría de las culturas las usan.

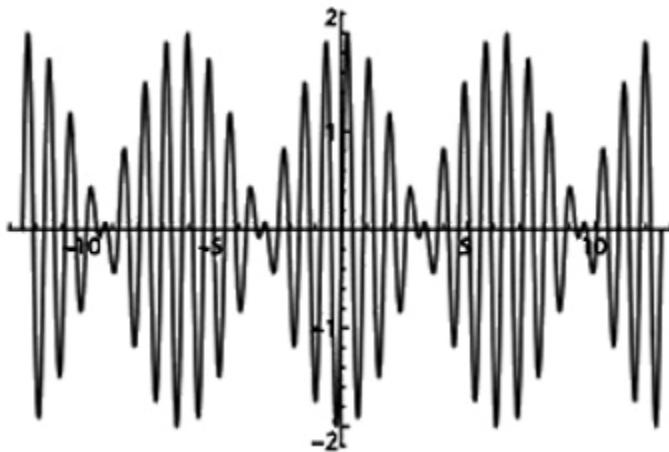


Figura 128. Batimientos.

Una cuerda es unidimensional, pero ideas muy parecidas se aplican en dimensiones mayores. Para calcular las vibraciones de un tambor, por ejemplo, consideramos una membrana vibrando (una superficie bidimensional) moldeada como la piel de un tambor. La mayoría de los tambores musicales son circulares, pero también podemos averiguar los sonidos hechos por un tambor cuadrado, un tambor rectangular o, es más, un tambor con la forma del dibujo de un gato.

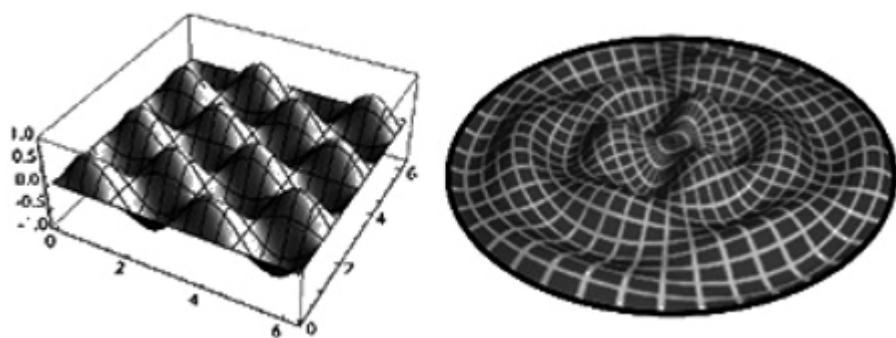


Figura 129. Izquierda: instante de modo uno de un tambor rectangular vibrante, con ondas números 2 y 3. Derecha: instante de modo uno de un tambor circular vibrante.

Para cualquier forma escogida del dominio, hay funciones análogas a los senos y cosenos de Bernoulli (los patrones más sencillos de vibración). Estos patrones se llaman «modos», o «modos normales», si quieres dejar totalmente claro de qué estás hablando. Todas las demás ondas pueden obtenerse superponiendo modos normales, de nuevo, usando una serie infinita si es necesario.

La forma también puede ser tridimensional: un sólido. Un buen ejemplo es una esfera sólida vibrante, un modelo sencillo de cómo la Tierra se mueve cuando hay un terremoto. Una forma más precisa sería un elipsoide ligeramente aplastado en los polos. Los sismólogos usan la ecuación de ondas y versiones más sofisticadas de ella que modelizan la física de la Tierra más fielmente, para comprender las señales producidas por terremotos.

Si estás diseñando un coche y quieres eliminar vibraciones no deseadas, estudia la ecuación de ondas para un objeto con la forma de un coche o cualquier parte de este que los ingenieros quieran entender. Diseñar edificios a prueba de terremotos es un proceso similar.

§. Constante de Apéry ($\zeta(3) \approx 1,202056$)

La constante de Apéry es un caso extraordinario de un patrón matemático que funciona para todos los números pares, aunque, hasta donde nosotros sabemos, parece no ser cierto para los números impares. La prueba de que este número es irracional apareció de modo totalmente inesperado.

Zeta de tres

¿Recuerdas la función zeta [véase $\frac{1}{2}$]? Está definida, sujeta a algunos tecnicismos sobre extensión analítica, por la serie

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

donde z es un número complejo [véase i]. Los matemáticos del siglo XVIII primero se encontraron con esta serie infinita en el caso especial $z = 2$, cuando Euler resolvió el problema de Basilea. En este lenguaje, esto requiere una fórmula para $\zeta(2)$, la cual es la suma de los inversos de los cuadrados perfectos. Hemos visto en $[\pi]$ que en 1735 Euler encontró la respuesta:

$$\zeta(2) = \frac{1}{1^2} + \frac{1}{2^2} + \frac{1}{3^2} + \frac{1}{4^2} + \frac{1}{5^2} + \dots = \frac{\pi^2}{6}$$

El mismo método funciona para potencias de cuatro, potencias de seis o cualquier potencia de un entero positivo par:

$$\zeta(4) = \frac{1}{1^4} + \frac{1}{2^4} + \frac{1}{3^4} + \frac{1}{4^4} + \frac{1}{5^4} + \dots = \frac{\pi^4}{90}$$

$$\zeta(6) = \frac{1}{1^6} + \frac{1}{2^6} + \frac{1}{3^6} + \frac{1}{4^6} + \frac{1}{5^6} + \dots = \frac{\pi^6}{945}$$

Y el patrón continúa con:

$$\zeta(8) = \frac{\pi^8}{9450} \qquad \zeta(10) = \frac{\pi^{10}}{93.555}$$

$$\zeta(12) = \frac{691\pi^{12}}{945.638.512.875} \qquad \zeta(14) = \frac{2\pi^{14}}{18.243.225}$$

Sobre la base de estos ejemplos, podríamos también esperar que la suma de los inversos de los cubos sea un racional múltiplo de π^3 , la suma de los inversos de las potencias de cinco sea un racional múltiplo de π^5 , etcétera. Sin embargo, cálculos numéricos sugieren claramente que esta suposición es errónea. De hecho, no se conoce ninguna fórmula para estas series, ya esté relacionada con π o no. Son muy misteriosas.

Como π es irracional, de hecho trascendental [véase π], las series anteriores tienen todas sumas irracionales. De modo que $\zeta(n)$ es irracional para $n = 2, 4, 6, 8, \dots$. Sin embargo, no sabemos si esto sigue siendo cierto para potencias impares. Parece probable, pero $\zeta(n)$ es

mucho más difícil de comprender para enteros impares porque los métodos de Euler dependen de que n sea par. Esta pregunta ha generado controversia entre muchos matemáticos, que en general llegaron exactamente a ninguna parte.

Cuando $n = 3$, inversos de los cubos, obtenemos un número que ahora conocemos como la «constante de Apéry».

$$\zeta(3) = \frac{1}{1^3} + \frac{1}{2^3} + \frac{1}{3^3} + \frac{1}{4^3} + \frac{1}{5^3} + \dots$$

Su valor numérico es este:

1,202 056 903 159 594 285 399 738 161 511 449 990 764 986 292...

Dividido entre π^3 , obtenemos:

0,038 768 179 602 916 798 941 119 890 318 721 149 806 234 568...

que no muestra signos de ser recurrente, por lo que no *parece* racional. Ciertamente no es un número racional con un numerador y un denominador pequeños. En 2013, Robert Setti calculó la constante de Apéry con 200.000 millones de cifras decimales. Parece todavía menos un racional múltiplo de π^3 y parece no estar relacionado con otras constantes matemáticas estándar.

Por tanto, supuso una gran sorpresa que en 1978 Raoul Apéry anunciara una prueba de que $\zeta(3)$ es irracional, y todavía una sorpresa mayor que la prueba resultara ser correcta. Sin intención de calumniar a Apéry, la prueba conlleva algunas afirmaciones increíbles, por ejemplo, que una secuencia de números que eran obviamente racionales pero parecía muy improbable que fuesen enteros en realidad *eran* enteros (todo entero es racional, pero no a la inversa). Esto empezó a hacerse plausible cuando los cálculos con ordenador seguían dando enteros, pero se tardó en encontrar una prueba de que esto continuaría de modo infinito. La prueba de Apéry es muy complicada, aunque no involucra técnicas desconocidas para Euler. Desde entonces, se han encontrado pruebas más sencillas.

Los métodos son especiales para $\zeta(3)$ y no parece que se extiendan a otros enteros impares. Sin embargo, en 2000, Wadim Zudilin y Tanguy Rivoal probaron que infinidad de $\zeta(2n + 1)$ deben ser irracionales. En 2001, demostraron que al menos uno de $\zeta(5), \zeta(7), \zeta(9)$ y $\zeta(11)$ es irracional, pero para tormento nuestro, su teorema no nos dice qué número de esos cuatro es irracional. A veces las matemáticas son así.

§. Constante de Euler ($\gamma \approx 0,577215$)

Este número aparece en muchas áreas del análisis y la teoría de números. Es definitivamente un número real y la apuesta inteligente es que es irracional, razón por la cual lo incluyo aquí. Surge a partir de la aproximación más sencilla de la suma de los inversos de todos los

números naturales hasta algún valor específico. A pesar de su ubicuidad y simplicidad, sabemos muy poco acerca de él. En concreto nadie puede probar que es irracional. Pero lo que sí sabemos es que si es racional, debe ser tremadamente complicado, cualquier fracción que lo represente involucraría números absolutamente gigantescos con más de 240.000 cifras.

Números armónicos

Los números armónicos son sumas finitas de inversos:

$$H_n = 1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \dots + \frac{1}{n}$$

No se conoce ninguna fórmula algebraica explícita para H_n , y parece probable que no exista ninguna. Sin embargo, usando el cálculo es bastante fácil mostrar que H_n es aproximadamente igual al logaritmo natural, $\log n$ [véase e]. De hecho, hay una aproximación mejor:

$$H_n \approx \log n + \gamma$$

donde γ es una constante. A medida que n se hace más grande, la diferencia entre los dos lados se hace tan pequeña como queramos.

La expresión decimal de γ comienza así:

$$\gamma = 0,577\,215\,664\,901\,532\,860\,606\,512\,090\,082\,402\,431\,042\,1\dots$$

y en 2013 Alexander Yee lo calculó con 19.377.958.182 cifras decimales. Se conoce como la «constante de Euler» porque la primera vez que apareció fue en un artículo que Euler escribió en 1734. Lo denotaba con C y con O , y más tarde lo calculó hasta con 16 cifras decimales. En 1790, Lorenzo Mascheroni también publicó resultados sobre el número, pero lo denotó con A y a . Intentó calcular 32 cifras decimales, pero se equivocó en las cifras de las posiciones 20 y 22. A veces se la conoce como «constante Euler-Mascheroni», pero teniendo todo en cuenta, Euler se merece la mayoría del crédito. En la década de 1830, los matemáticos habían cambiado la notación a γ , que ahora es la estándar.

La constante de Euler aparece en numerosas fórmulas matemáticas, especialmente en cálculo en conexión con series infinitas e integrales definidas. Su exponencial e^γ es común en teoría de números. Hay hipótesis acerca de que la constante de Euler es transcendental, pero ni siquiera se sabe si es irracional. Cálculos de su fracción continua prueban que si es racional, igual a $\frac{p}{q}$ para enteros p y q , entonces q es al menos $10^{242.080}$.

Una forma todavía más precisa para los números armónicos es:

$$H_n = \log n + \gamma + \frac{1}{2n} + \frac{1}{12n^2} + \frac{1}{120n^4}$$

con un error de casi $1/252n^4$

Números pequeños especiales

Contenido:

- 11. Teoría de cuerdas*
- 12. Pentominós*
- 17. Polígonos y patrones*
- 23. La paradoja del cumpleaños*
- 26. Códigos secretos*
- 56. La conjetura de la salchicha*
- 168. Geometría finita*

Volvemos a los números naturales, que tienen encanto por sí mismos. Cada uno es un individuo diferente con características especiales que lo hacen interesante.

De hecho, todos los números son interesantes. Prueba: si no, debería existir el número más pequeño carente de interés. Pero eso lo hace interesante: contradicción.

11. Teoría de cuerdas

Normalmente pensamos en el espacio que tiene tres dimensiones. El tiempo proporciona una cuarta dimensión para el espacio tiempo, el dominio de la relatividad. Sin embargo, una investigación actual en la frontera de la física, conocida como «teoría de cuerdas», concretamente

«teoría M», propone que el espacio-tiempo realmente tiene *once* dimensiones. Siete de ellas no se muestran a los sentidos humanos sin ayuda. De hecho, no han sido detectadas de manera definitiva en ningún experimento.

Esto podría parecer horrible y además podría no ser cierto, pero los físicos nos han demostrado repetidas veces que la imagen del mundo que percibimos por nuestros sentidos puede diferir significativamente de la realidad. Por ejemplo, materia aparentemente continua está hecha a partir de pequeñas partículas separadas, los átomos. Ahora algunos físicos creen que el espacio real es muy diferente del espacio en el que creemos que vivimos. La razón para escoger 11 dimensiones no es una observación del mundo real: es el número que hace que una estructura matemática crucial funcione consistentemente. La teoría de cuerdas es muy técnica, pero las ideas principales se pueden bosquejar en términos bastante sencillos.

Unificando la relatividad y la teoría cuántica

Los dos grandes triunfos de la física teórica son la relatividad y la mecánica cuántica. El primero, presentado por Einstein, explica la fuerza de la gravedad en términos de la curvatura del espacio-tiempo. Según la relatividad general (que Einstein desarrolló después de la relatividad especial, su teoría del espacio, el tiempo y la materia), una partícula moviéndose de una localización a otra sigue una geodésica: el camino

más corto que une esas dos localizaciones. Pero cerca de un gran cuerpo, como una estrella, el espacio-tiempo es distorsionado y esto hace que parezca que el camino está curvado. Por ejemplo, los planetas giran alrededor del Sol en órbitas elípticas.

La teoría original de la gravedad, descubierta por Newton, interpretó esta curvatura como el resultado de una fuerza y dio una fórmula matemática para la potencia de esa fuerza. Pero mediciones muy precisas mostraron que la teoría de Newton es ligeramente inexacta. Einstein reemplazó la fuerza de gravedad por la curvatura del espacio-tiempo y esta nueva teoría corrigió los errores. Desde entonces ha sido confirmada por una variedad de observaciones, principalmente de objetos astronómicos distantes.

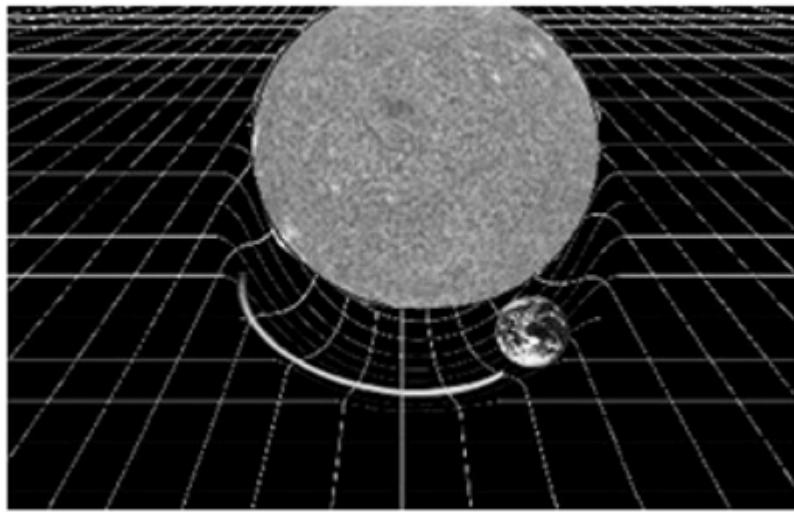


Figura 130. Cómo la curvatura del espacio-tiempo puede actuar como una fuerza. Una partícula pasando por un gran cuerpo, como una estrella, es desviada por la curvatura; el mismo efecto que una fuerza de atracción.

El segundo gran triunfo, la mecánica cuántica, la introdujeron varios grandes físicos, entre ellos Max Planck, Werner Heisenberg, Louis de Broglie, Erwin Schrödinger y Paul Dirac. Explica cómo se comporta la materia en las escalas más pequeñas, del tamaño de los átomos o más aún. En estas escalas, la materia se comporta como partículas minúsculas y como ondas. La mecánica cuántica predice muchos efectos extraños, muy diferentes de cómo el mundo se comporta a escala humana, pero miles de experimentos avalan estas predicciones. La electrónica moderna no funcionaría si la mecánica cuántica fuese muy diferente de la realidad. Para los físicos teóricos resulta poco satisfactorio tener dos teorías distintas, aplicadas en contextos diferentes, especialmente desde que discrepa la una de la otra cuando estos contextos se superponen, como sucede en cosmología, la teoría del universo como un todo. El propio Einstein empezó la búsqueda de una teoría del campo unificado que combine ambas de un modo acorde con la lógica. Esta búsqueda ha tenido un éxito parcial, pero hasta el momento solo con el dominio cuántico.

Estos éxitos unifican tres de las cuatro fuerzas físicas básicas. Los físicos distinguen cuatro tipos de fuerza en la naturaleza: gravitacional; electromagnética, la cual gobierna la electricidad y el magnetismo; nuclear débil, relacionada con la desintegración de partículas radiactivas; y nuclear fuerte, que une partículas como los protones y los neutrones.

Estrictamente hablando, todas estas fuerzas son «interacciones» entre partículas de materias. La relatividad describe la fuerza gravitacional y la mecánica cuántica se aplica a las otras tres fuerzas fundamentales.

En décadas recientes, los físicos han encontrado una teoría general única que unifica las tres fuerzas de la mecánica cuántica. Conocido como «modelo estándar», describe la estructura de la materia en escalas subatómicas. Según el modelo estándar, toda la materia está construida a partir de tan solo 17 partículas fundamentales.

Debido a varios problemas de observación —por ejemplo, las galaxias rotan de una manera que no coincide con las predicciones de la relatividad general si la única materia en ellas son las cosas que podemos ver—, los cosmólogos actualmente creen que la mayoría del universo está hecho a partir de «materia oscura», la cual probablemente requiere nuevas partículas más allá de estas 17. Si están en lo correcto, el modelo estándar necesitará ser modificado. Alternativamente, podríamos necesitar una nueva teoría de la gravedad o una teoría modificada de cómo los cuerpos se mueven cuando se aplica una fuerza.

Sin embargo, los físicos teóricos todavía no se las han arreglado para unificar la relatividad y la mecánica cuántica construyendo una única teoría que describa *las cuatro* fuerzas en una manera consistente, que además concuerde con ambas en sus propios dominios (el muy grande y el muy pequeño, respectivamente). La búsqueda por esta teoría del campo unificado, o *teoría del todo*, ha llevado a algunas ideas

matemáticas bellas, y ha culminado en la teoría de cuerdas. Hasta la fecha, no hay un apoyo experimental definitivo para esta teoría, y algunas otras proposiciones también son objeto de investigación activa. Un ejemplo típico es la gravedad cuántica de bucles, en la cual el espacio está representado como una red de bucles muy pequeños, un poco como una cota de malla. Técnicamente es una espuma de espín.

La teoría de cuerdas comenzó proponiendo que las partículas fundamentales no deberían pensarse como puntos. De hecho, existía la sensación de que la naturaleza realmente no hace puntos, de modo que el uso de un modelo con puntos bien podía ser la razón de que la teoría cuántica para partículas fuese inconsistente con la relatividad, que funciona con curvas y superficies lisas. En su lugar, las partículas deberían ser más como minúsculos bucles cerrados, llamados «cuerdas». Los bucles pueden doblarse, de modo que la noción de curvatura de Einstein aparece en escena de manera natural.

Además, los bucles pueden vibrar y sus vibraciones explican eficientemente la existencia de varias propiedades cuánticas como la carga eléctrica y el espín. Una de las características más desconcertantes de la mecánica cuántica es que esas características se suelen dar como un número entero multiplicado por alguna constante básica. Por ejemplo, el protón tiene carga +1 unidad, el electrón tiene carga -1 unidad y el neutrón tiene carga 0 unidades. Los *quarks*, partículas más elementales que se combinan para hacer protones y neutrones, tienen cargas $\frac{2}{3}$ y $-\frac{1}{3}$.

de una unidad. De modo que todo se da como múltiplos $-3, -1, 0, 2, 3$ de una unidad básica, la carga en algunos tipos de *quark*. ¿Por qué múltiplos enteros? Las matemáticas de las cuerdas vibrantes se comportan de una manera similar. Cada vibración es una onda, con una longitud de onda concreta [véase $\sqrt[12]{2}$]. Las ondas en un bucle cerrado deben encajar correctamente cuando el bucle se cierra, de modo que un número entero de ondas deben encajar alrededor del bucle. Si las ondas representan estados cuánticos, esto explica por qué todo aparece como múltiplos enteros.

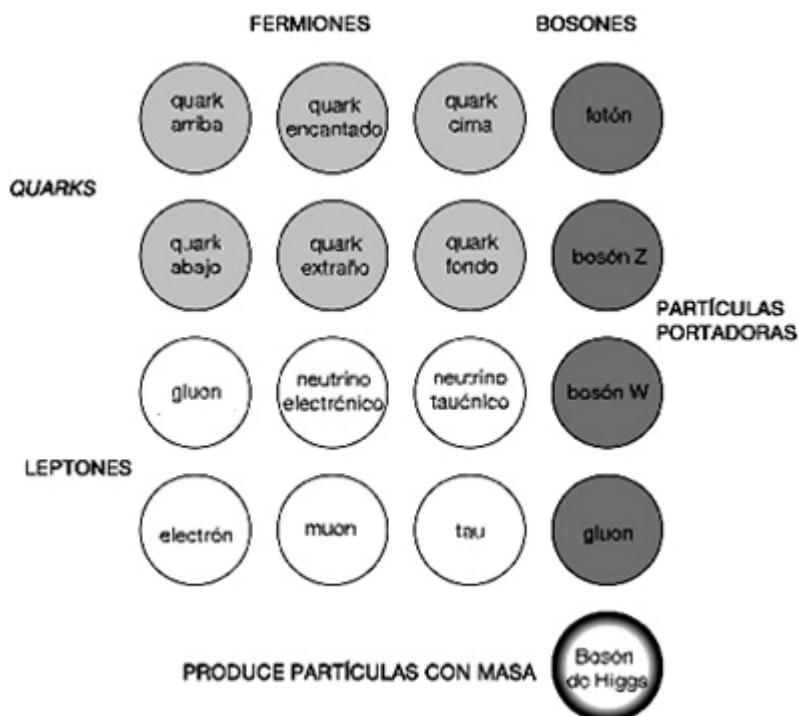


Figura 131. Las 17 partículas elementales.

La historia resultó no ser tan directa como eso, por supuesto. Pero perseguir la idea de partículas como bucles llevó a los físicos y matemáticos a algunas ideas extraordinarias y poderosas.

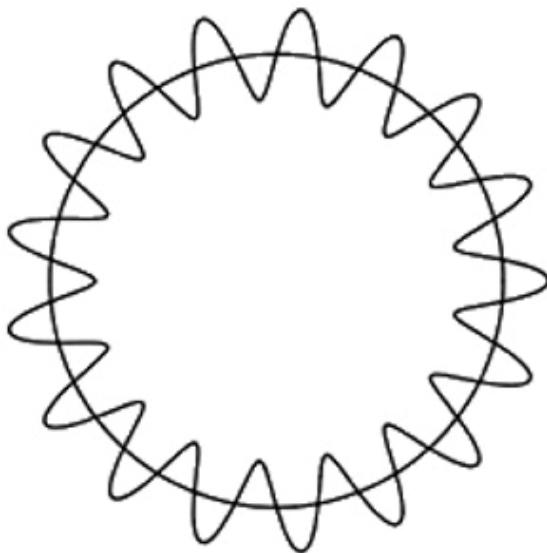


Figura 132. Un número entero de ondas encajan alrededor de un círculo.

Dimensiones extra

Una cuerda cuántica vibrante necesita algún tipo de espacio para vibrar. Para que las matemáticas tengan sentido, esto no puede ser un espacio ordinario. Tiene que haber una variable adicional, una *dimensión extra* del espacio, porque este tipo de vibración es una propiedad cuántica, no una espacial. A medida que la teoría de cuerdas se desarrollaba, los teóricos vieron claro que, para que todo funcionase, necesitaban varias dimensiones extra. Un nuevo principio llamado «supersimetría» sugería

que toda partícula debería tener una «compañera» con la que estuviese relacionada, una partícula más pesada. Las cuerdas deberían ser reemplazadas por las supercuerdas, permitiendo este tipo de simetría. Y las supercuerdas funcionaban solo si se asumía que el espacio tiene *seis dimensiones extra*.

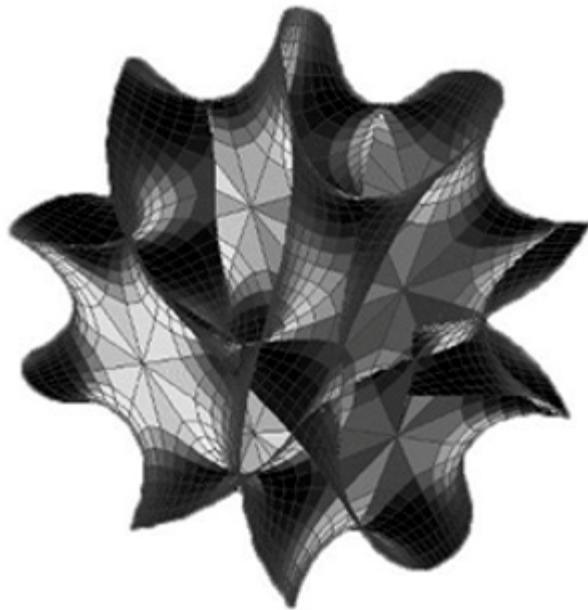


Figura 133. Proyección en el espacio ordinario de una variedad Calabi-Yau de seis dimensiones.

Esto también quiere decir que en lugar de una cuerda pensada como una curva del tipo de una circunferencia, esta debe tener una forma más complicada en seis dimensiones. Entre las formas que podrían aplicarse están las conocidas como «variedades Calabi-Yau».

Esta sugerencia no es tan rara como podría parecer, porque «dimensión» en matemáticas tan solo significa «variable independiente». El

electromagnetismo clásico describe la electricidad en términos de un campo eléctrico y un campo magnético, los cuales se extienden al espacio ordinario. Cada campo requiere tres variables nuevas: las tres componentes de la dirección en las cuales apunta el campo eléctrico e ídem para el magnetismo. Aunque estas componentes se alinean con las direcciones en el espacio, las fuerzas del campo a lo largo de estas direcciones son independientes de las propias direcciones. De modo que el electromagnetismo clásico requiere seis dimensiones extra: tres de la electricidad y tres del magnetismo. En cierto sentido, la teoría clásica de electromagnetismo requiere diez dimensiones: cuatro del espacio-tiempo más seis del electromagnetismo.

La teoría de cuerdas es parecida, pero no usa *estas* seis nuevas dimensiones. En cierto sentido, las nuevas dimensiones de la teoría de cuerdas (las nuevas variables) se comportan más como dimensiones espaciales ordinarias que las de la electricidad o el magnetismo. Uno de los grandes avances de Einstein fue combinar el espacio tridimensional y el tiempo unidimensional en un espacio-tiempo de cuatro dimensiones. De hecho, esto era necesario porque, según la relatividad, las variables del espacio y el tiempo se mezclan cuando los objetos se mueven muy rápido. La teoría de cuerdas es similar, pero ahora usa un espacio-tiempo de diez dimensiones con nueve dimensiones de espacio más una dimensión de tiempo.

Esta idea se impuso entre los teóricos por la necesidad de las matemáticas de ser consistentes de modo lógico. Si asumimos que el tiempo tiene una dimensión como es habitual, y el espacio-tiempo tiene d dimensiones, los cálculos llevan a términos en las ecuaciones llamada «anomalías», las cuales en general son infinitas. Esto conlleva un gran problema, porque no hay infinitos en el mundo real. Sin embargo, resulta que los términos en cuestión son múltiplos de $d - 10$. Esto es cero si y solo si $d = 10$ y las anomalías entonces desaparecen. De modo que para deshacerse de las anomalías se necesita que la dimensión del espacio-tiempo sea 10.

El factor $d - 10$ está inherente en la formulación de la teoría. Escoger $d = 10$ sortea el problema por completo, pero introduce lo que a primera vista es otro todavía peor. Restando una dimensión para el tiempo, nos encontramos que el espacio tiene nueve dimensiones, no tres. Pero si eso es cierto, seguramente lo habríamos percibido. *¿Dónde están las seis dimensiones extra?*

Una respuesta atractiva es que están presentes, pero enroscadas de modo tan apretado que no las notamos: de hecho, *no* podemos notarlas. Imagina una manguera larga. Vista desde cierta distancia, no notas su grosor, parece como una curva, la cual es unidimensional. Las otras dos dimensiones, la sección circular de la manguera, están enroscadas en un espacio tan pequeño que no pueden observarse. Una cuerda es como esto, pero enroscada de modo más apretado. La longitud de una

manguera es aproximadamente mil veces más larga que su grosor. La «longitud» de una cuerda (el movimiento espacial visible) es más de 10^{40} veces su «grosor» (las nuevas dimensiones en las cuales vibra).

Otra respuesta posible es que las nuevas dimensiones son realmente bastante grandes, pero la mayoría de los estados de las partículas están confinados a una localización fijada en estas dimensiones, como un bote flotando en la superficie del océano. El propio océano tiene tres dimensiones: latitud, longitud y profundidad. Pero el bote tiene que estar en la superficie, y explora solo dos de ellas: latitud y longitud. Algunas características, como por ejemplo la fuerza de la gravedad, sí exploran las dimensiones extra del espacio-tiempo, como un buzo saltando del bote. Pero la mayoría no lo hacen.

Alrededor de 1990, los teóricos habían ideado cinco tipos diferentes de teoría de cuerdas, principalmente difiriendo en las simetrías de sus dimensiones extra. Se les llamó tipos I, IIA, IIB, HO y HE. Edward Witten descubrió una unificación matemática elegante de las cinco, a la que llamó «teoría M». Esta teoría requiere que el espacio-tiempo tenga 11 dimensiones: diez del espacio y una del tiempo. Varios trucos matemáticos para pasar de uno de los cinco tipos de la teoría de cuerdas a otro se pueden ver como propiedades físicas del espacio-tiempo completo de 11 dimensiones. Al escoger «localizaciones» concretas en este espacio-tiempo de 11 dimensiones, podemos derivar los cinco tipos de teoría de cuerdas.

Incluso si la teoría de cuerdas resulta no ser la manera en la que funciona el universo, ha hecho contribuciones importantes a las matemáticas, por desgracia demasiado técnicas para tratarlas aquí. De modo que los matemáticos continuarán estudiándola y considerarán que tiene valor, incluso si los físicos deciden que no se aplica al mundo real.

§. 12 Pentominós

Un pentominó es una forma hecha al adecuar cinco cuadrados idénticos entre sí por sus aristas. Hay 12 posibilidades, sin contar las reflexiones como diferentes. Convencionalmente se nombran usando letras del alfabeto con formas parecidas. 12 es también el número de osculación en el espacio tridimensional.

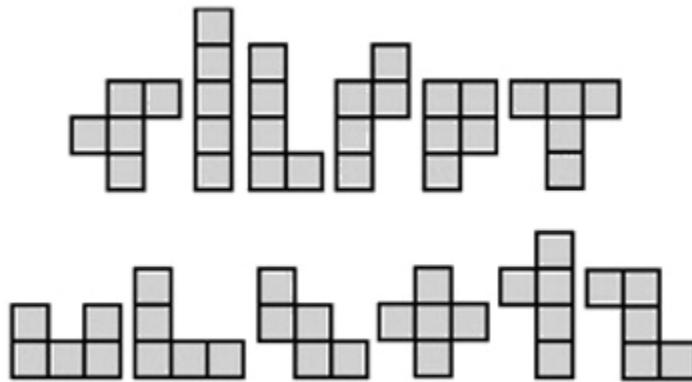


Figura 134. Los 12 pentominós.

Poliominós

De manera más general un n -ominó es una forma hecha usando cuadrados idénticos. El conjunto de estas formas se llama poliominós. Hay 35 hexominós ($n = 6$) y 108 heptominós ($n = 7$).

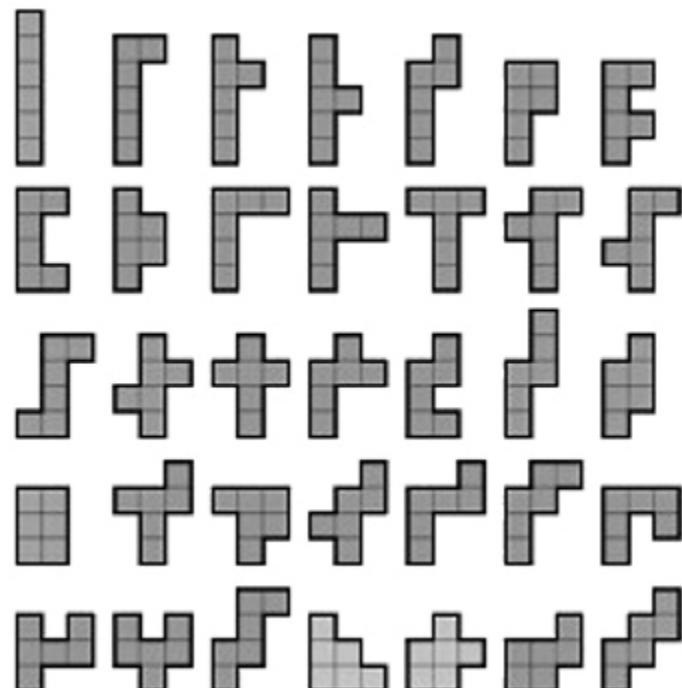


Figura 135. Los 35 hexominós.

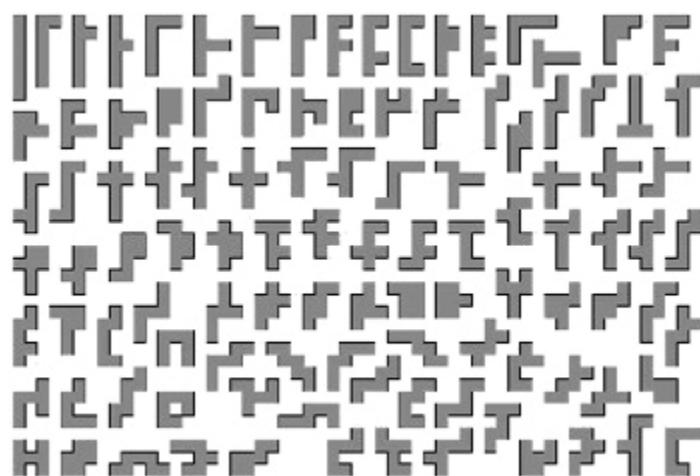


Figura 136. Los 108 heptomínós.

El concepto general y el nombre los inventó Solomon Golomb en 1953 y Martin Gardner los popularizó en *Scientific American*. El nombre es una derivación regresiva de la palabra «dominó», que son dos cuadrados unidos, en la cual se da a la letra «D» una ingeniosa interpretación como del latín *di* o del griego *do*, que significan «dos». (La palabra «dominó» realmente proviene del latín *dominus*, «señor»).

Los precursores abundan en la literatura. El creador de rompecabezas Henry Dudeney incluyó un rompecabezas de pentominó en su *Canterbury Puzzles* de 1907. Entre 1937 y 1957, la revista *Fairy Chess Review* incluyó muchas colocaciones dependiendo de hexominós, a los que llamó «problemas de disección».

Rompecabezas con poliominós

Los poliominós en general, y los pentominós en particular, forman las bases de un número enorme de rompecabezas y juegos de entretenimiento. Por ejemplo, pueden ensamblarse para hacer formas interesantes.

Los doce pentominós tienen un área total de 60, en unidades para las cuales cada componente cuadrada tiene área 1. Cualquier modo de escribir 60 como un producto de dos números naturales define un rectángulo, y es un rompecabezas ameno y bastante estimulante encajar

los pentominós unos con otros para formar un rectángulo así. Se pueden girar para obtener la imagen de reflejo en el espejo si es necesario. Los posibles rectángulos resultan ser: 6×10 , 5×12 , 4×15 y 3×20 . Es fácil comprobar que 2×30 y 1×60 son imposibles.

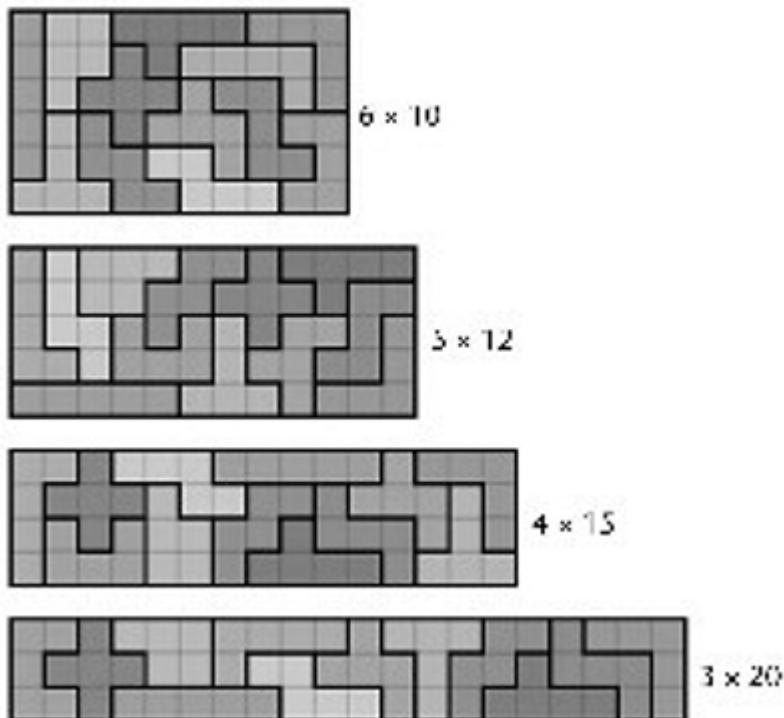


Figura 137. Posibles tamaños de los rectángulos de pentominós.

El número de maneras distintas de formar estos rectángulos (sin contar la rotación y la reflexión de todo el rectángulo como diferente pero permitiendo a rectángulos más pequeños rotarse y reflejarse mientras todo lo demás se queda fijo) es conocido:

6×10 : 2.339 maneras

5×12 : 1.010 maneras

4×15 : 368 maneras

3×20 : 2 maneras

Otro rompecabezas típico empieza con la ecuación $8 \times 8 - 2 \times 2 = 60$ y pregunta si un cuadrado de 8×8 con un agujero central de 2×2 puede embaldosarse con los doce pentominós. La respuesta es afirmativa:

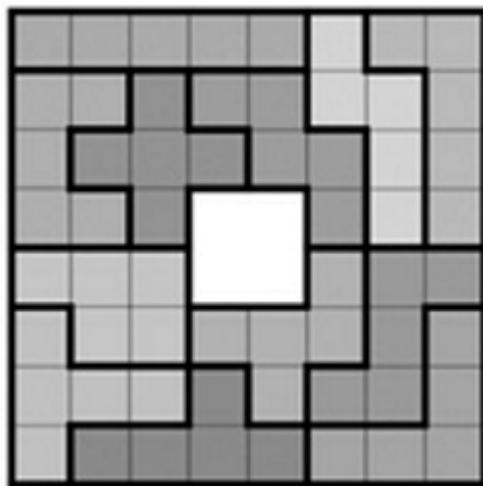


Figura 138. Cuadrado agujereado formado con pentominós.

Un modo atractivo de ensamblar unos hexominós con otros es un paralelogramo:

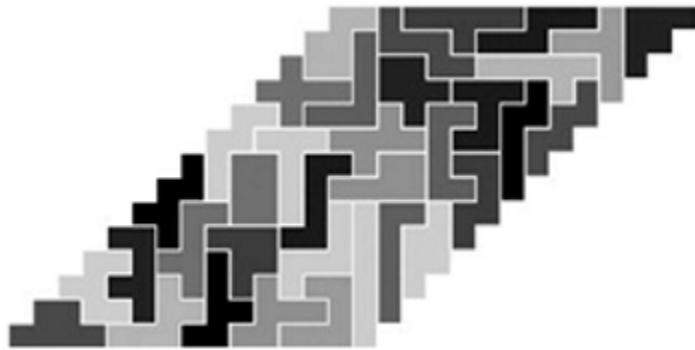


Figura 139. Paralelogramo formado con hexominós.

Número de poliominós

Los matemáticos e ingenieros informáticos han calculado cuántos n -ominós existen para muchos n . Si las rotaciones y las reflexiones no se consideran como diferentes, los números son:

Tabla 11

n número de n-ominós

1	1
2	1
3	2
4	5
5	12
6	35
7	108
8	369
9	1.285

10	4.655
11	17.073
12	63.600

Número de osculación para esferas

El número de osculación para los círculos —el mayor número de círculos que pueden tocar a uno dado, siendo todos del mismo tamaño— es seis [véase 6]. Hay también un número de osculación para las esferas —el mayor número de esferas que pueden tocar a una dada, siendo todas del mismo tamaño—. Ese número es 12.

Es bastante fácil demostrar que 12 esferas pueden tocar a una dada. De hecho, es posible hacer esto de modo que los puntos de contacto formen los 12 vértices de un icosaedro regular [véase 5]. Hay suficiente espacio entre estos puntos para encajar esferas sin que se toquen.

En el plano, los seis círculos en contacto con el central no dejan espacio libre y la disposición es rígida. Pero en tres dimensiones, hay mucho hueco libre y las esferas pueden moverse. Durante bastante tiempo, no se supo si podría haber hueco para una 13^a esfera si las otras 12 eran empujadas a los lugares correctos.

Dos famosos matemáticos, Newton y David Gregory, discutieron largamente sobre esta cuestión. Newton mantenía que el número correcto era 12, mientras que Gregory estaba convencido de que debería ser 13. A principios del siglo XIX, se intentó probar que Newton tenía razón, pero

esas explicaciones tenían vacíos. Una prueba completa de que 12 es la respuesta, apareció por primera vez en 1953.

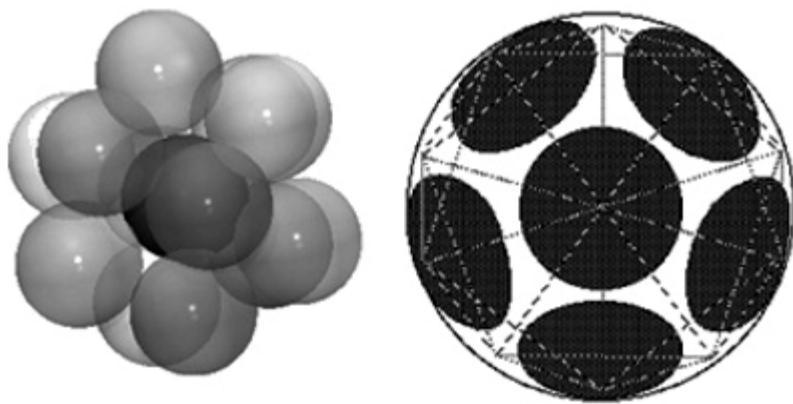


Figura 140. Izquierda: cómo 12 esferas pueden tocar a una esfera dada.

Derecha: «sombras» de 12 esferas tocando una esfera dada en una disposición icosaédrica.

Cuatro o más dimensiones

Una historia similar se da en el espacio de cuatro dimensiones, donde es relativamente fácil encontrar una disposición de 24 3-esferas, pero hay suficiente espacio, de modo que quizá podría encajar una 25.^a. Esta incógnita fue finalmente resuelta por Oleg Musin en 2003; como se esperaba, la respuesta es 24.

En la mayoría de las otras dimensiones, los matemáticos saben que algún número concreto de esferas que toquen una esfera dada es posible, porque pueden encontrar esa disposición, y que algún número mucho más grande generalmente es imposible, por varias razones indirectas. Estos números son el *límite inferior* y el *límite superior* para el número

de osculación. Debe de estar en algún punto entre ellos, y posiblemente sea igual a uno de ellos.

En tan solo dos casos más allá de cuatro dimensiones, el límite inferior y el superior coinciden, por lo que su valor común será el número de osculación. Sorprendentemente, estas dimensiones son 8 y 24, donde los números de osculación son, respectivamente, 240 y 196.650. En estas dimensiones, existen dos redes muy simétricas, análogas de dimensiones más altas de rejillas de cuadrados o de manera más general rejillas de paralelogramos. Estas celosías especiales se conocen como «E8» (o «estructura de Gosset») y «estructura de Leech», y las esferas pueden colocarse en puntos de la estructura adecuados. Por alguna milagrosa coincidencia, los límites superiores demostrables para el número de osculación en estas dimensiones son los mismos que los límites inferiores proporcionados por estas estructuras especiales.

El estado actual del tema se resume en la siguiente tabla, donde en negrita se muestran esas dimensiones para las cuales se conoce una respuesta exacta.

Tabla 12

Dimensi ón	Límite inferior	Límite superior	Dimensi ón	Límite inferior	Límite superior
1	2	2	13	1.130	2.233
2	6	6	14	1.582	3.492

3	12	12	15	2.564	5.431
4	24	24	16	4.320	8.313
5	40	45	17	5.346	12.215
6	72	78	18	7.398	17.877
7	126	135	19	10.688	25.901
8	240	240	20	17.400	37.974
9	306	366	21	27.720	56.852
10	500	567	22	49.896	86.537
11	582	915	23	93.150	128.096
12	840	1.416	24	196.560	196.560

§. 17 Polígonos y patrones

En su juventud, Gauss descubrió, para sorpresa de todo el mundo incluido él, que un polígono regular de 17 lados puede construirse usando regla y compás, algo que Euclides nunca sospechó. Ni tampoco nadie más durante unos dos mil años.

Hay 17 tipos de simetrías diferentes de patrón de papel pintado. Esto es realmente una versión bidimensional de la cristalografía: la estructura atómica de los cristales.

En el modelo estándar de la física de partículas, hay 17 tipos de partículas fundamentales [véase 11].

Polígonos regulares

Un polígono (griego para «muchos lados») es una forma cuyas aristas son líneas rectas. Es regular si cada arista tiene la misma longitud y todos los pares de aristas se unen formando el mismo ángulo.

Los polígonos regulares tienen un papel central en la geometría de Euclides y desde entonces se han convertido en fundamentales en muchas áreas de las matemáticas. Uno de los principales objetivos de los *Elementos* de Euclides era probar que existían exactamente cinco poliedros regulares, sólidos cuyas caras son polígonos regulares idénticos agrupados del mismo modo en cada vértice [véase 5]. Con este fin, tuvo que considerar caras que eran polígonos regulares con 3, 4 y 5 lados. Números de lados mayores no se dan en las caras de poliedros regulares.



Figura 141. Polígonos regulares con 3, 4, 5, 6, 7 y 8 lados. Nombres: triángulo equilátero, cuadrado, pentágono, hexágono, heptágono y octógono regular.

A lo largo del camino, Euclides necesitó construir estas figuras, usando las herramientas tradicionales de regla y compás, porque sus técnicas geométricas se basaban en esa suposición. Las construcciones más sencillas tienen como resultado el triángulo equilátero y el hexágono. Un

compás puede ubicar los vértices por sí solo. Para dibujar las aristas necesitamos una regla, pero ese es su único papel.

Construir un cuadrado es ligeramente más difícil, pero resulta directo una vez se sabe cómo construir un ángulo recto.

El pentágono regular es mucho más complicado. Aquí te explico como lo hace Euclides. Tres vértices distintos de un pentágono regular siempre forman un triángulo con ángulos 36° , 72° y 72° . Además puede invertir el proceso y obtener un pentágono regular dibujando una circunferencia que pase por los vértices de ese triángulo y haciendo la biseción de los dos ángulos de 72° , algo que Euclides había mostrado cómo hacer mucho antes en su libro [véase ½].

Ahora todo lo que necesitaba era un modo de construir un triángulo con su forma especial, lo que resultó ser la parte más difícil. De hecho, se necesita otra construcción complicada, que a su vez depende de una anterior. Por lo tanto, no es ninguna sorpresa averiguar que Euclides no obtiene el pentágono regular hasta el libro IV de su obra de trece tomos.

La figura muestra una construcción más sencilla y más moderna. Empieza con una circunferencia de centro O y diámetro CM. Dibuja OS en ángulo recto con CM y halla su punto medio, L. Dibuja una circunferencia centrada en L que pase por O y toque al círculo inicial en S. Traza ML, siendo los puntos de corte con la circunferencia N y P. Dibuja arcos de las circunferencias (gris) de centro M y que pasen por N

y por P, cortando a la circunferencia grande en B, D, A y E. ABCDE (marcado con línea discontinua) es un pentágono regular.

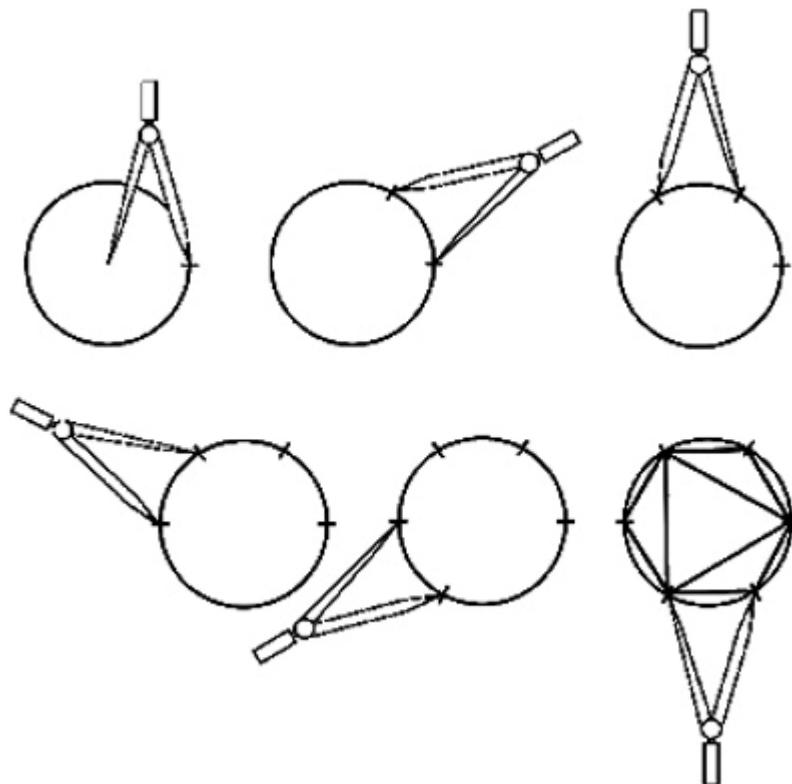


Figura 142. Dibuja una circunferencia y marca un punto en ella. Marca los puntos sucesivos alrededor de la circunferencia con el compás manteniendo la misma distancia. Esto nos lleva a las seis esquinas de un hexágono regular. Cogiendo uno de cada dos vértices se forma un triángulo equilátero.

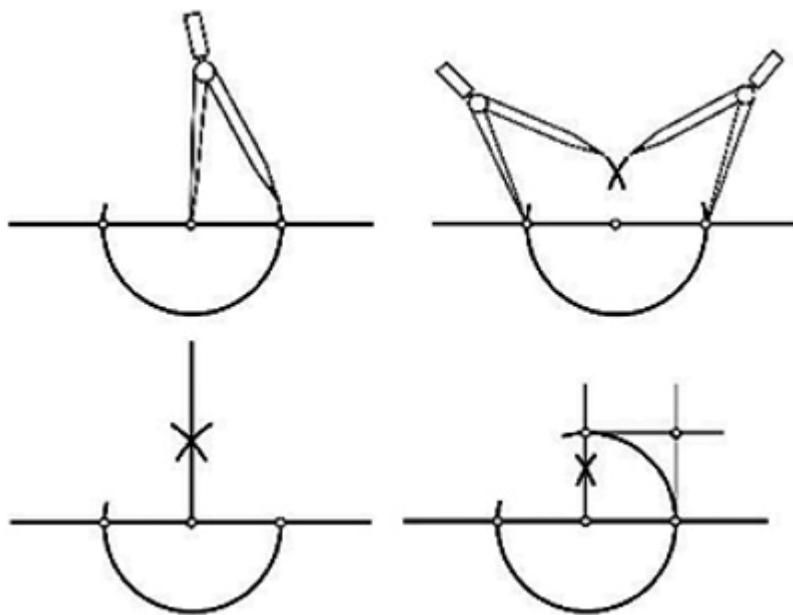


Figura 143. Dado un punto en una recta, fija el centro del compás en ese punto y dibuja una circunferencia cortando la línea dos veces. Abre el compás y dibuja dos arcos que se crucen. La línea en la tercera figura está en el ángulo recto con la línea original. Repite los pasos para obtener los otros lados del cuadrado.

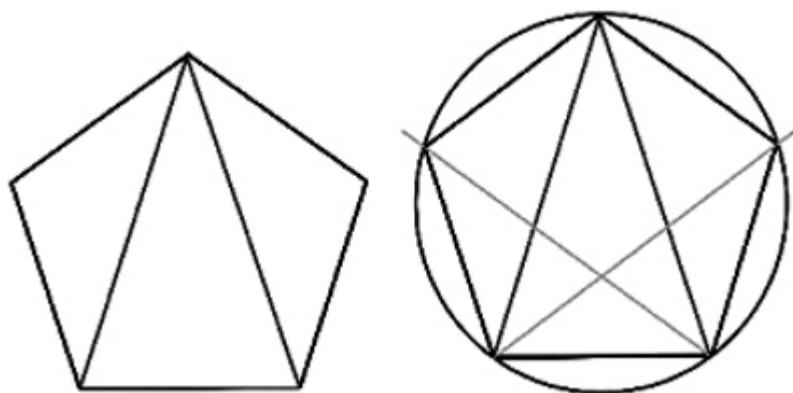


Figura 144. Izquierda: estos tres vértices de un pentágono regular forman un triángulo con ángulos 36° , 72° y 72° . Derecha: dado ese triángulo, dibuja una circunferencia que pase por sus vértices (gris)

oscuro) y haz la bisección de los ángulos de 72° (gris claro) para obtener los otros dos vértices del pentágono.

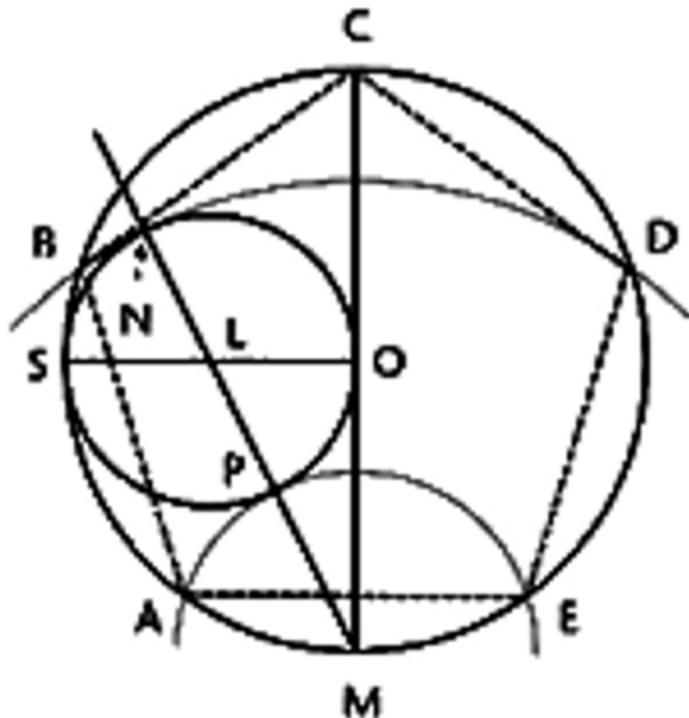


Figura 145. Construcción más sencilla de un pentágono regular.

Más de seis lados

Euclides también sabía cómo doblar el número de lados de cualquier polígono regular, haciendo la bisección de sus ángulos centrales. Por ejemplo, aquí se muestra cómo convertir un hexágono regular en un polígono de 12 lados regular.

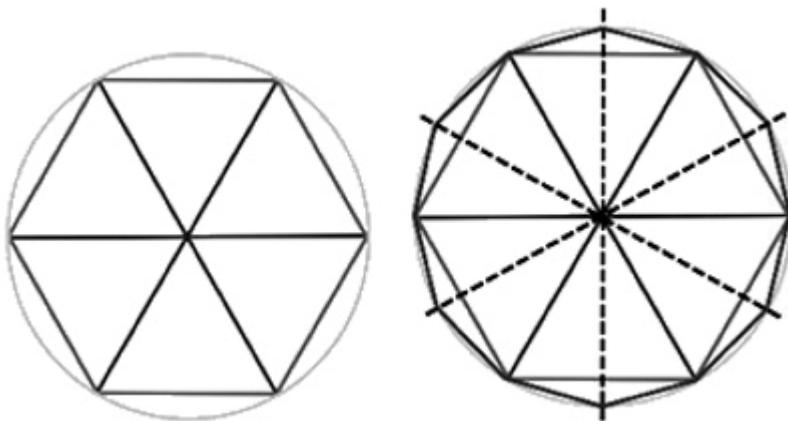


Figura 146. Izquierda: empieza con un hexágono dentro de una circunferencia. Dibuja sus diagonales. Derecha: haz la biseción de los ángulos centrales (aparece con línea discontinua). Estas cortan a la circunferencia en otros seis vértices de un dodecágono regular.

Combinando estas construcciones para un triángulo equilátero y un pentágono regular, obtenemos un polígono regular de 15 lados. Esto funciona porque $3 \times 5 = 15$ y 3 y 5 no tienen un factor común.

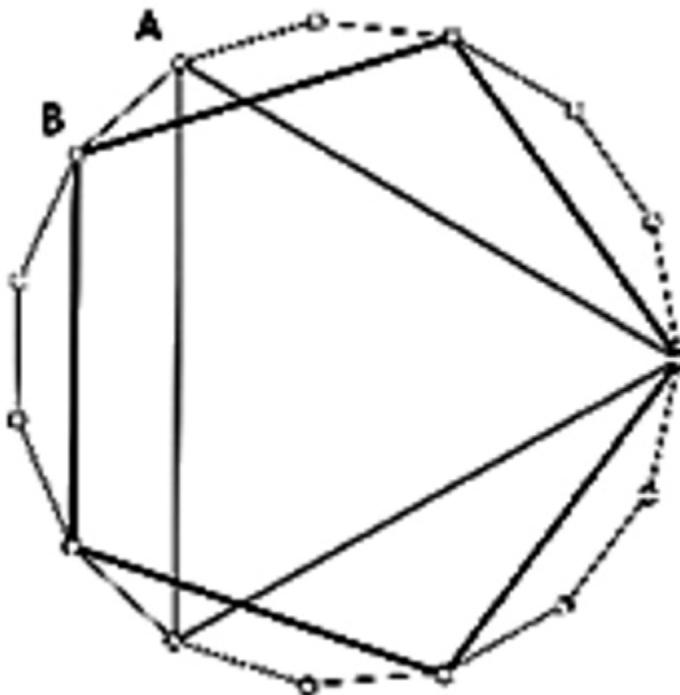


Figura 147. Cómo hacer un polígono de 15 lados. Los puntos A, en un triángulo equilátero, y B, en un pentágono regular, son vértices sucesivos de un polígono regular de 15 lados. Usa un compás para desplazarte por las posiciones de los otros vértices.

Combinando todos estos trucos, Euclides supo cómo construir polígonos regulares con este número de lados:

3 4 5 6 8 10 12 15 16 20 24 30 32 40 48

Y así sucesivamente con los números 3, 4, 5 y 15, junto con cualquier otro que puedas obtener a partir de ellos doblándolo repetidas veces. Pero faltan muchos números; el primero es el 7.

Los griegos fueron incapaces de encontrar una construcción con regla y compás para estos polígonos regulares que faltaban. Eso no significa que esos polígonos no existan, tan solo sugería que el método de la regla y el compás no era el adecuado para construirlos. Parece que nadie ha pensado que para alguno de estos números desaparecidos podría ser posible una construcción de regla y compás, o incluso haberse hecho la pregunta.

El polígono regular de 17 lados

Gauss, uno de los más grandes matemáticos que ha existido, a punto estuvo de convertirse en lingüista. Pero en 1796, cuando tenía 19 años, se dio cuenta de que el número 17 tiene dos propiedades especiales que, combinadas, implican que existe una construcción de regla y compás para un polígono regular de 17 lados (heptadecágono).

Descubrió este hecho sorprendente no pensando en geometría, sino en álgebra. En los números complejos hay precisamente 17 soluciones para la ecuación $x^{17} = 1$, y resulta que forman un polígono regular de 17 lados en el plano [véase «Raíces de la unidad» en i]. Esto se conocía bien por aquel entonces, pero Gauss señaló algo que a todo el mundo se le había escapado. Como él, sabían que el número 17 es primo, y también que es una unidad mayor que una potencia de 2, en concreto, $16 + 1$, donde $16 = 2^4$. Sin embargo, Gauss probó que la combinación de estas dos propiedades implica que la ecuación $x^{17} = 1$ puede resolverse usando las

operaciones habituales de álgebra: suma, resta, multiplicación y división, junto con la formación de raíces cuadradas. Y todas estas operaciones pueden realizarse geométricamente usando regla y compás. En resumen, debe de haber una construcción de regla y compás para un polígono regular de 17 lados. Y eso eran grandes noticias, porque nadie había soñado con algo así durante más de dos mil años. Fue completamente inesperado y carente de precedentes. Llevó a Gauss a decidirse por la carrera de matemáticas.

No escribió una construcción explícita, pero cinco años más tarde, en su obra maestra *Disquisitiones arithmeticæ*, escribió la fórmula:

$$\frac{1}{16} \left[-1 + \sqrt{17} + \sqrt{34 - 2\sqrt{17}} \right. \\ \left. + \sqrt{68 + 12\sqrt{17} - 16\sqrt{34 + 2\sqrt{17}} - 2(1 - \sqrt{17})(\sqrt{34 - 2\sqrt{17}})} \right]$$

Y probó que el polígono regular de 17 lados puede construirse siempre que se pueda construir un segmento de esa longitud dado un segmento de longitud la unidad. Como solo aparecen raíces cuadradas, es posible trasladar la fórmula a una construcción geométrica bastante complicada. Sin embargo, hay métodos más eficientes, que descubrieron diferentes personas cuando estaban analizando la prueba de Gauss.

Gauss era consciente de que el mismo argumento se aplica si se reemplaza 17 por cualquier otro número con las mismas dos

propiedades: un primo que es una potencia de 2 más 1. Estos números se llaman «primos de Fermat». Usando álgebra, puede probarse que si $2k + 1$ es primo, entonces el propio k debe ser 0 o una potencia de 2, de modo que $k = 0$ o $2n$. Un número de esta forma se llama «número de Fermat». Los primeros números de Fermat se muestran en la Tabla 13:

Tabla 13

$k = 2^n$	$2^k + 1$	<i>¿Primo?</i>	
	0	2	sí
0	1	3	sí
1	2	5	sí
2	4	17	sí
3	8	257	sí
4	16	65.537	sí
5	32	4.294.967.297	no

(es igual $641 \times 6.700.417$)

Los seis primeros números de Fermat son primos. Los tres primeros, 2, 3 y 5, corresponden a construcciones conocidas por los griegos. El siguiente, 17, es un descubrimiento de Gauss. Luego vienen dos números más asombrosos todavía: 257 y 65.537. La perspicacia de Gauss prueba que los polígonos regulares con este número de lados *también* se pueden construir con regla y compás. En 1832, F. J. Richelot publicó una

construcción para el polígono regular de 257 lados. J. Hermes, de la Universidad de Lingen, dedicó diez años de su vida al polígono regular de 65.537 lados. Su trabajo inédito puede encontrarse en la Universidad de Gotinga, pero se cree que contiene errores. No está claro que merezca la pena comprobarlo, porque se sabe que la construcción existe. Encontrar una es rutina, excepto por lo enorme de los cálculos. Supongo que podría ser un buen test de los sistemas de verificación de pruebas por ordenador.

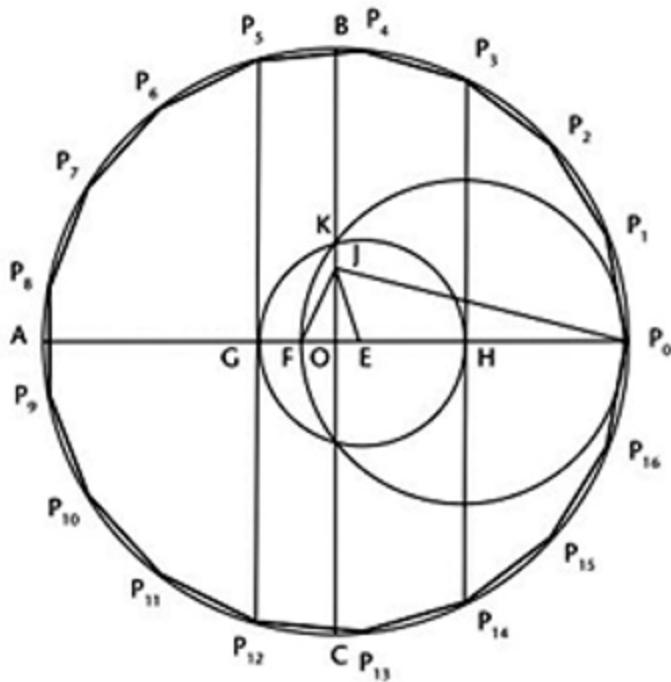


Figura 148. El método de Richmond para construir un polígono regular de 17 lados. Toma dos diámetros perpendiculares AOP_0 y BOC de una circunferencia. Dibuja $OJ = \frac{1}{4}OB$ y el ángulo $OJE = \frac{1}{4}OJP_0$. Encuentra F de modo que el ángulo EJF tenga 45° . Dibuja una circunferencia con FP_0 como diámetro, que cortará a OB en K . Dibuja

una circunferencia de centro E que pase por K, que corta AP₀ en G y H.

Dibuja HP3 y GP5, perpendicular a AP₀.

Durante un tiempo, se pensó que todos los números de Fermat eran primos, pero en 1732 Euler se dio cuenta de que el 7º número de Fermat, $4.294.967.297$ es compuesto, que es igual a $641 \times 6.700.417$. (Ten en cuenta que en aquella época los cálculos tenían que hacerse a mano. Hoy en día un ordenador revelaría esto en un instante.) Hasta la fecha, no se ha probado que más números de Fermat sean primos. Son compuestos para $5 \leq n \leq 11$ y en estos casos se conoce una factorización en números primos.

Los números de Fermat son compuestos para $12 \leq n \leq 32$, pero no se conocen todos los factores y cuando $n = 20$ y 24 no se conoce ningún factor explícito. Hay una prueba indirecta para saber si un número de Fermat es primo y estos dos casos no pasan la prueba. El número de Fermat más pequeño cuyo estatus no se conoce se da para $n = 33$ y tiene 2.585.827.973 cifras decimales. Ahora eleva 2 a esa potencia y súmrale 1... ¡Gigante! Sin embargo, la esperanza no está perdida del todo debido al tamaño: el mayor número de Fermat compuesto conocido es $F_{2.747.497}$, que es divisible entre:

$$57 \times 2^{2.747.499} + 1$$

(Marshall Bishop, 2013).

Parece plausible que los primos de Fermat conocidos son los únicos, pero nunca se ha probado. Si es falso, entonces habría un polígono regular construible con un número de lados primo absolutamente gigantesco.

Patrones de papel de pared

Un patrón de papel de pared repite la misma imagen en dos direcciones distintas: hacia abajo en la pared y a lo largo de la pared (posiblemente con cierta inclinación). La repetición que va bajando la pared se debe a que el papel se imprime en un rollo continuo, usando un cilindro giratorio para crear el patrón. La repetición a lo largo de la pared hace posible continuar con el patrón hacia los lados, para cubrir la pared por completo.

El número de posibles *diseños* para un patrón de pared es gigantesco. Pero muchos patrones diferentes están ordenados de manera idéntica, tan solo usando diferentes imágenes. Los matemáticos distinguen los patrones diferentes en su esencia por sus simetrías. ¿Cuáles son las diferentes maneras de deslizar el patrón o rotarlo o incluso voltearlo (como reflejándolo en un espejo), de modo que el resultado final sea el mismo que al principio?

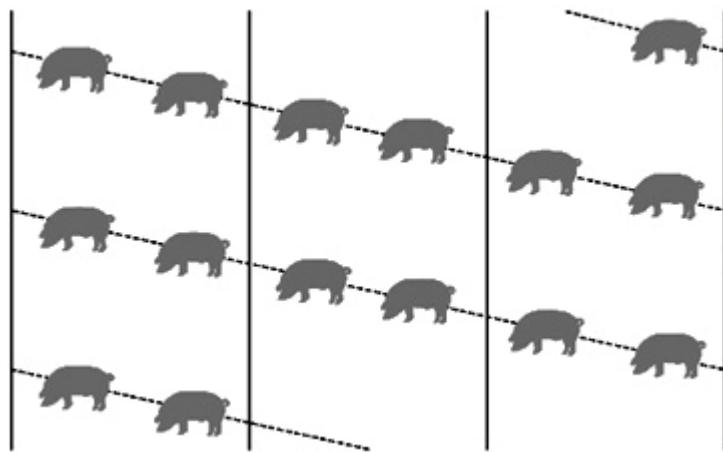


Figura 149. Patrón de papel de pared que se repite en dos direcciones.

Simetrías en el plano

El grupo de simetrías de un diseño en un plano comprende todos los movimientos rígidos del plano que no deforman el propio diseño. Hay cuatro tipos importantes de movimientos rígidos:

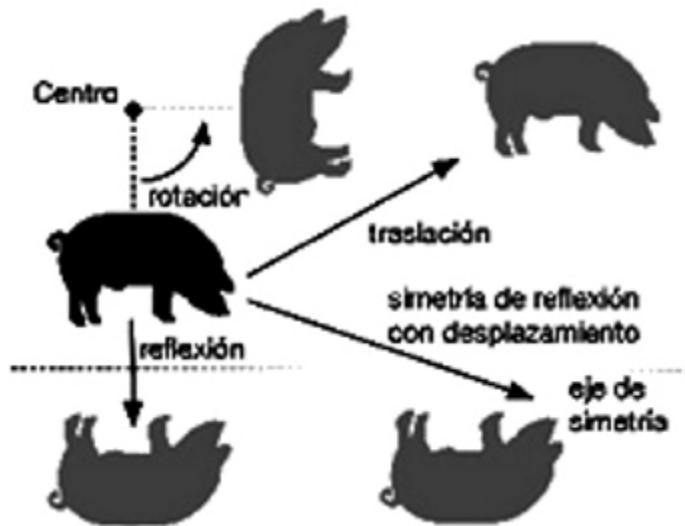


Figura 150. Cuatro tipos de movimiento rígido.

- translación (deslizar sin rotar)
- rotación (girar alrededor de algún punto fijo, el centro de rotación)
- reflexión (reflejar respecto a alguna recta, el eje de simetría)
- simetría de reflexión con desplazamiento (reflejar y mover a lo largo del eje de simetría)

Si el diseño es de extensión finita, solo la rotación y la simetría de reflexión son posibles. Las rotaciones solo llevan a simetrías cíclicas, mientras que las rotaciones más reflexiones dan simetrías diédricas.

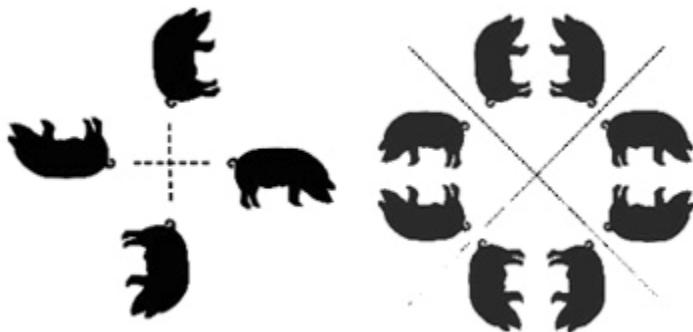


Figura 151. Izquierda: grupo cíclico de simetrías (en este caso son rotaciones de múltiplos del ángulo recto). Derecha: grupo diédrico de simetrías (las líneas de puntos son ejes de simetría).

Los patrones de la pared, que pueden continuar infinitamente, pueden tener translaciones y simetrías de reflexión con desplazamiento. Por ejemplo, podemos pintar el grupo diédrico del diseño del cerdo en un azulejo cuadrado y usarlo para embaldosar el plano. (El diagrama

muestra solo cuatro de la colección infinita de azulejos.) Ahora hay traslaciones (por ejemplo, las flechas continuas) y simetrías de reflexión con desplazamiento (por ejemplo, las flechas punteadas).

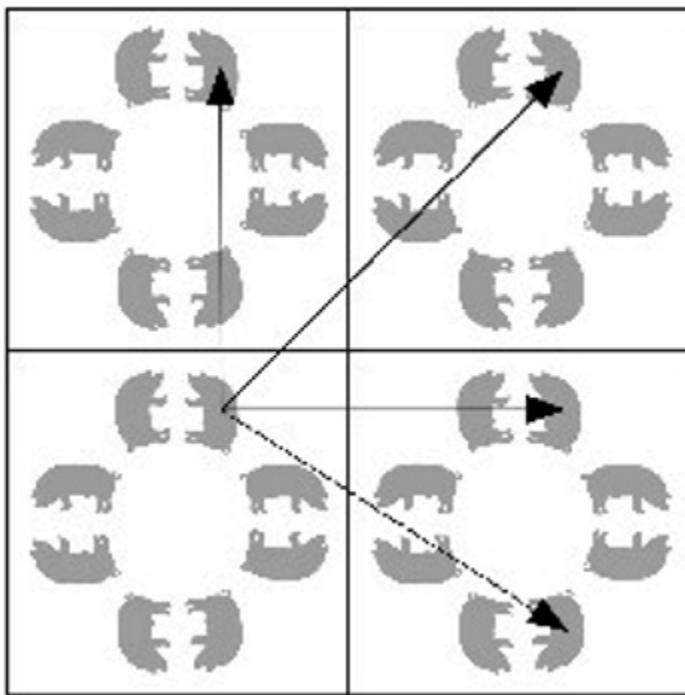


Figura 152. Colección de azulejos cuadrados mostrando la traslación (flechas continuas) y simetrías de reflexión con desplazamientos (las flechas punteadas).

Los 17 tipos de simetría de papel de pared

Para mi papel de pared con el patrón de unas flores, las únicas simetrías son desplazamientos a lo largo de dos direcciones en las cuales el patrón se repite, o varios de esos desplazamientos realizados por turnos. Este es el tipo más simple de simetría de papel de pared y todo diseño de papel de pared en sentido matemático tiene estas simetrías de red, por definición. No estoy reivindicando que no haya un papel de pared que

sea básicamente tan solo un mural, sin simetrías más allá de la trivial «deja esto sin cambios». Tan solo estoy excluyendo esos patrones de esta discusión.

Muchos tipos de papel de pared tienen simetrías extra como rotaciones y reflexiones. En 1924, George Pólya y P. Niggli probaron que había exactamente 17 tipos de simetrías diferentes de patrón de papel de pared. En tres dimensiones, el problema correspondiente es listar todos los posibles tipos de simetría de estructuras de cristales. En este caso hay 230 tipos. Curiosamente, esa respuesta fue descubierta antes de que nadie resolviese la versión bidimensional mucho más fácil para el papel de pared.

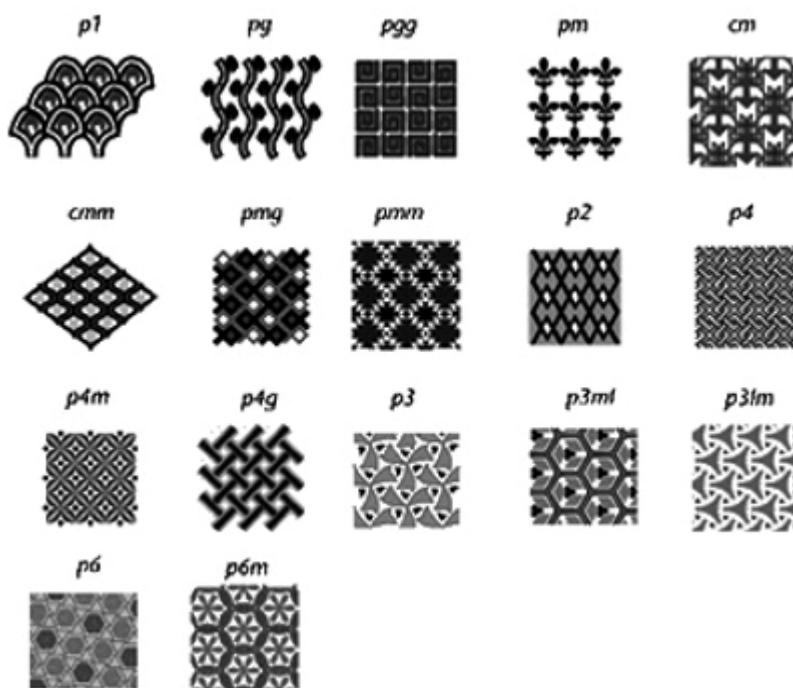


Figura 153. Los 17 tipos de patrón de papel de pared y su notación cristalográfica internacional (de MathWorld, un recurso web de Wolfram).

§. 23 La paradoja del cumpleaños

Durante un partido de fútbol, hay normalmente 23 personas en el campo: dos equipos de 11 jugadores cada uno más el árbitro. (Hay también dos árbitros asistentes justo en el límite del campo y otro más lejos, pero los ignoraremos junto con los camilleros, espontáneos que saltan al campo y entrenadores furiosos.) ¿Cuál es la probabilidad de que dos o más de esas 23 personas tengan la misma fecha de cumpleaños?

Con más probabilidad de sí que de no

La respuesta es sorprendente, a menos que la hayas visto antes. Para que los cálculos sean sencillos, asume que solo son posibles 365 fechas de cumpleaños diferentes (sin 29 de febrero para la gente que nació en año bisiesto), y que cada una de estas fechas tenga exactamente la misma probabilidad: $1/365$. Las cifras reales muestran pequeñas pero significativas diferencias, con algunas fechas o momentos del año más probables que otros; estas diferencias varían entre países. La probabilidad buscada no cambia demasiado si tienes en cuenta estos factores, y el resultado es igual de sorprendente.

También asumimos que las probabilidades para cada jugador son independientes de las de los demás, lo cual no sería cierto si, por ejemplo, los jugadores fueron deliberadamente escogidos para tener diferentes cumpleaños. O, digamos, si el partido tuviese lugar en el alienígena mundo de hielo de Gnx Prime. Allí cada nueva generación de monstruos alienígenas emerge simultáneamente de su tubo de hibernación bajo tierra y generaciones distintas no juegan en los mismos equipos, algo como un cruce entre cigarras magicicadas y los humanos en la Tierra. Tan pronto como dos gnxoides llegan al campo, la probabilidad de que comparten la misma fecha de cumpleaños inmediatamente se convierte en 1.

Es más fácil encontrar una probabilidad relacionada: la oportunidad de que los 23 cumpleaños sean *diferentes*. Las reglas para calcular probabilidades entonces nos dicen que hay que restar esto a 1 para obtener la respuesta. Es decir, la probabilidad de que no suceda un evento es uno menos la probabilidad de que el evento suceda. Para describir el cálculo nos ayuda asumir que la gente llega al campo de uno en uno.

- Cuando llega la primera persona, nadie más está presente. De modo que la probabilidad de que sus cumpleaños sean diferentes es distinta de cualquier otro que esté presente es 1 (seguro).

- Cuando llega la segunda persona, su cumpleaños tiene que ser diferente del de la primera persona, de modo que hay 364 opciones de 365. La probabilidad de que esto suceda es:

$$\frac{364}{365}$$

- Cuando entra la tercera persona, su cumpleaños tiene que ser diferente del de las dos primeras personas, de modo que hay 363 opciones de 365. Las reglas para calcular las probabilidades nos dicen que cuando queremos la probabilidad de que sucedan dos sucesos independientes, entonces *multiplicamos* sus probabilidades. De modo que la probabilidad de que no se duplique el cumpleaños en este punto es:

$$\left(\frac{364}{365}\right) \times \left(\frac{363}{365}\right)$$

- Cuando llega la cuarta persona, su cumpleaños tiene que ser diferente del de las primeras personas, de modo que hay 362 opciones de 365. La probabilidad de que no se repita en este momento es:

$$\left(\frac{364}{365}\right) \times \left(\frac{363}{365}\right) \times \left(\frac{362}{365}\right)$$

El patrón debería estar ahora claro. Después de que k personas hayan llegado, la probabilidad de que los k cumpleaños sean distintos es:

$$p(k) = \left(\frac{364}{365}\right) \times \left(\frac{363}{365}\right) \times \left(\frac{362}{365}\right) \times \dots \times \left(\frac{365-k+1}{365}\right)$$

Cuando $k = 23$, esto resulta ser 0,492703, ligeramente menor que $\frac{1}{2}$. De modo que la probabilidad de que al menos dos personas tengan el mismo cumpleaños es $1 - 0,492703$, que es:

$$0,507297$$

Esto es ligeramente mayor que $\frac{1}{2}$.

En otras palabras; con 23 personas en el campo, es más probable que al menos dos de ellas tengan la misma fecha de cumpleaños, que todas las fechas sean diferentes.

De hecho, 23 es el número más pequeño para el cual esta afirmación es cierta. Con 22 personas, $P(22) = 0,524305$, ligeramente mayor que $\frac{1}{2}$. Ahora la probabilidad de que al menos dos personas tengan el mismo cumpleaños es $1 - 0,524305$, que es:

$$0,475695$$

Esto es ligeramente menor que $\frac{1}{2}$.

La imagen muestra cómo $P(k)$ depende de k , para $k = 1$ hasta 50. La recta horizontal muestra el valor de equilibrio de $\frac{1}{2}$.

La sorpresa es lo pequeño que es el número 23. Con 365 fechas entre las que escoger, es fácil imaginar que necesitas mucha más gente antes de que una coincidencia sea más probable que no. Esta intuición es errónea porque, a medida que vamos introduciendo gente, se multiplica una secuencia cada vez más decreciente de opciones. De modo que el resultado decrece más rápido de lo esperado.

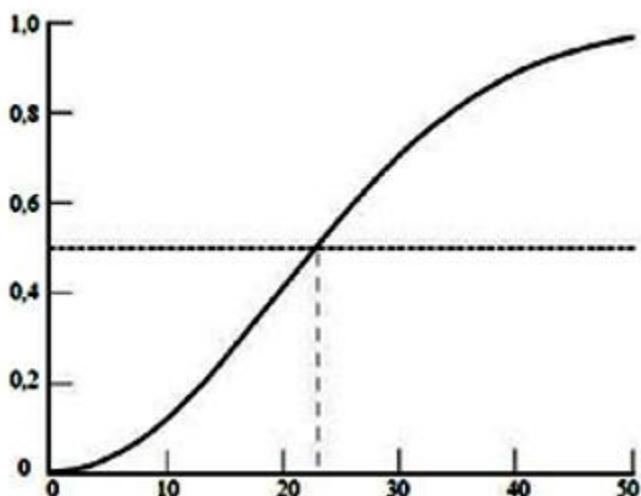


Figura 154. Cómo $P(k)$ depende de k .

Mismo cumpleaños que tú

Podría haber otra razón por la que nos sorprenda lo pequeño que es el número. Quizá confundamos el problema con uno diferente: ¿cuánta gente debería haber para hacer mayor que $\frac{1}{2}$ la probabilidad de que uno de ellos tenga el mismo cumpleaños *que tú*?

Esta cuestión es ligeramente más sencilla de analizar. De nuevo, le damos la vuelta y calculamos la probabilidad de que *nadie* tenga el mismo cumpleaños que tú. Para cada nueva persona que consideremos, la probabilidad de que su cumpleaños sea diferente del tuyo es siempre la misma, en concreto:

$$\frac{364}{365}$$

De modo que con k personas, la probabilidad de que todos sus cumpleaños sean diferentes del tuyo es:

$$\frac{364}{365} \times \dots \times \frac{364}{365} = \left(\frac{364}{365}\right)^k$$

Aquí los números que se multiplican no decrecen. Su producto decrece a medida que usamos más de ellos, porque $\frac{364}{365}$ es menor que 1, pero el ritmo de decrecimiento es más lento. De hecho, ahora necesitamos $k = 253$ antes de que este número caiga por debajo de $\frac{1}{2}$.

$$\left(\frac{364}{365}\right)^{253} = 0,499523$$

La sorpresa, si es que la hay, es lo grande que es este número.

Cumpleaños en Júpiter

Obtenemos 23 porque hay 365 días en un año. El número 365 no tiene especial significado matemático aquí; aparece por razones astronómicas. Desde un punto de vista matemático, deberíamos analizar un problema más general, donde el número de días en un año pueda ser cualquiera que deseemos.

Empezaremos con el problema del cumpleaños para globulinos, alienígenas de ficción que flotan en la atmósfera de helio-hidrógeno de Júpiter porque sus células están llenas con hidrógeno. Júpiter está más lejos del Sol que la Tierra, de modo que su «año» (el tiempo que tarda el planeta en recorrer la órbita alrededor del Sol) es más largo que el nuestro (4.332,59 de nuestros días). También gira mucho más rápido, de modo que su «día» (el tiempo que tarda el planeta en dar una vuelta alrededor de su eje) es más corto que el nuestro (9 h 55 min 30 s). Por lo tanto, el «año» de Júpiter contiene aproximadamente 10.477 «días» jovianos.

Cálculos similares muestran que siempre que 121 globulinos, tres equipos de 40 globulinos más un árbitro, están involucrados en un juego de flota-la-pelota, la probabilidad de que al menos dos de ellos compartan cumpleaños es ligeramente mayor que $\frac{1}{2}$. De hecho,

$$1 - \left(\frac{10.476}{10.477} \times \frac{10.475}{10.477} \times \dots \times \frac{10.356}{10.477} \right) = 0,501234$$

mientras que con 120 globulinos, la probabilidad es 0,495455.

Los matemáticos jovianos, insatisfechos con tener que calcular repetidamente esa probabilidad para diferentes números de días en el año, han desarrollado una fórmula general. No es muy precisa, pero es una aproximación muy buena. Lo que responde la pregunta general: si hay n fechas posibles entre las que escoger, ¿cuántos entes deben estar presentes para que la probabilidad de que al menos dos de ellos tengan el mismo cumpleaños exceda de $\frac{1}{2}$?

Lo que los jovianos no saben es que una flota invisible de alienígenas invasores del planeta Neeblebruct ha estado dando vueltas alrededor de Júpiter durante medio siglo joviano. A lo largo de los años han abducido muchos cuarenta y doses de los matemáticos jovianos con la esperanza de descubrir su secreto. La dificultad es que un año neebelbructiano contiene exactamente $42^4 = 3.111.696$ días neebelbructianos y nadie se las ha ingeniado para averiguar cuál es el sustituto correcto para 121.

Este problema puede resolverse usando el secreto joviano. Han probado que con n fechas entre las que escoger, y k entes presentes, la probabilidad de que al menos dos de ellos tenga el mismo cumpleaños supera por primera vez $\frac{1}{2}$ cuando k está cerca de

$$\sqrt{\log 4} \times \sqrt{n}$$

donde la constante $\sqrt{\log 4}$ es la raíz cuadrada del logaritmo de 4 con base e y su valor es aproximadamente 1,1774.

Probemos esta fórmula con otros tres ejemplos:

- Tierra: $n = 365$ y $k \approx 22,4944$.
- Marte: $n = 670$ y $k \approx 30,4765$.
- Júpiter: $n = 10.477$ y $k \approx 120,516$.

Redondeando hasta el próximo entero, los puntos de ruptura se dan para 23, 31 y 121 enteros. Estos son, de hecho, los números exactos. Sin embargo, la fórmula no es tan precisa para un n grande. Aplicada al año neebelbructiano, en el que $n = 3.111.696$, la fórmula da:

$$k = 2.076,95$$

Que al redondear da 2.077. Un cálculo con detalle muestra que

$$P(k) = 0,4999$$

que es ligeramente menor que $\frac{1}{2}$. El número correcto resulta ser 2.078 para el cual:

$$P(k) = 0,5002$$

La fórmula explica por qué el número de entes necesarios para que una coincidencia de cumpleaños sea más probable que no lo sea es tan pequeño. Es del mismo tamaño general que la *raíz cuadrada* del número de días en el año. Esto es mucho más pequeño que el número de días. Por ejemplo, para un año que dura un millón de días la raíz cuadrada es tan solo mil.

Número esperado

Una variante común de este problema es: con n cumpleaños posibles, ¿cuál es el número *esperado* de entes necesarios para que al menos dos de ellos compartan cumpleaños? Es decir, ¿cuántos entes necesitamos de media?

Cuando $n = 365$, la respuesta resulta ser 23,9. Esto es tan próximo a 23 que las dos preguntas a veces se confunden. De nuevo, hay una fórmula que es una buena aproximación:

$$k \approx \sqrt{\frac{\pi}{2}} \times \sqrt{n}$$

y la constante $(\sqrt{\pi})/2 = 1,2533$. Esto es un poco mayor que $\sqrt{\log 4} = 1,1774$.

Frank Mathis ha encontrado una fórmula más precisa para el número de entes necesarios para que una coincidencia de cumpleaños tenga más probabilidades de ocurrir que de no ocurrir:

$$\frac{1}{2} + \sqrt{\frac{1}{4} + 2\pi \log 2}$$

Srinivasa Ramanujan, un matemático hindú autodidacta con un don especial para las fórmulas, encontró una más precisa para el número de entes esperados:

$$\sqrt{\frac{\pi n}{2}} + \frac{2}{3} + \frac{1}{12} \sqrt{\frac{\pi}{2n}} - \frac{4}{135n}$$

§. 26 Códigos secretos

La palabra «código» nos lleva a pensar inmediatamente en James Bond o en *El espía que surgió del frío*. Pero casi todos nosotros usamos códigos secretos en nuestra vida diaria para actividades perfectamente normales y legales como, por ejemplo, la banca por Internet. Nuestras comunicaciones con nuestro banco están encriptadas, puestas en código, así los criminales no pueden leer los mensajes y tener acceso a nuestro dinero. Al menos no fácilmente.

Hay 26 letras en el alfabeto inglés, y códigos prácticos a menudo usan el número 26. En concreto, la máquina Enigma, usada por los alemanes en la segunda guerra mundial, empleaba rotores con 26 posiciones que se correspondían con las letras. Así ese número proporciona una ruta de entrada razonable a la criptografía. Sin embargo, no tiene propiedades

matemáticas especiales en este contexto, y principios similares funcionan con otros números.

El cifrado César

La historia de los códigos se remonta al menos al antiguo Egipto, y hacia 1900 a. C. Julio César usaba un código sencillo en la correspondencia privada y para secretos militares. Su biógrafo, Suetonio, escribió: «Si tenía cualquier cosa confidencial que decir, la escribía cifrada, es decir, cambiando el orden de las letras en el alfabeto, de modo que ni una palabra pudiese entenderse. Si alguien deseaba descifrarlo y conocer su significado, debía sustituir la cuarta letra del alfabeto, es decir D, por A, y continuar luego con las otras».

En la época de César el alfabeto no incluía las letras J, U y W, pero trabajaremos con el alfabeto actual porque es más familiar. Su idea era escribir el alfabeto en el orden habitual, y luego colocar una versión trasladada debajo, quizá algo así:

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

F G H I J K L M N O P Q R S T U V W X Y Z A B C D E

Puedes codificar un mensaje convirtiendo cada letra del alfabeto normal en una letra en la misma posición del alfabeto desplazado. Es decir, A se

convierte en F, B se convierte en G, y así sucesivamente. Como por ejemplo:

JULIUSCAESAR
OZQNZXHFJXFW

Para codificar el mensaje, basta leer la correspondencia entre los alfabetos en el otro sentido:

OZQNZXHFJXFW
JULIUSCAESAR

Para obtener un artilugio práctico que automáticamente desvele el alfabeto, colocamos las letras en una circunferencia o cilindro:



Figura 155. Artilugios prácticos para descifrar.

El cifrado de César es demasiado simple para ser seguro por razones que explico a continuación, pero incorpora algunas ideas básicas comunes a todos los cifrados, es decir, sistemas de codificación:

- *Texto plano*: mensaje original.
- *Texto cifrado*: versión encriptada.
- *Algoritmo de encriptación*: método usado para convertir texto plano en texto cifrado.
- *Algoritmo de desencriptación*: método usado para convertir el texto cifrado en texto plano.
- *Clave*: información secreta necesaria para encriptar y desencriptar el texto.



Figura 156. Características generales de un sistema de cifrado.

En el cifrado de César, la clave es el número de letras que se traslada el alfabeto. El algoritmo de encriptación es «desplazar el alfabeto la clave». El algoritmo de desencriptación es «desplazar el alfabeto la clave en sentido inverso», es decir, menos la clave en el mismo sentido.

En este sistema de cifrado, la clave de encriptación y la clave de desencriptación están muy relacionadas: una es menos la otra, es decir, el mismo desplazamiento pero en sentido opuesto. En esos casos, saber la clave de encriptación equivale exactamente a saber la clave de desencriptación. Un sistema de este tipo se llama «cifrado simétrico».

En apariencia César empleó códigos más sofisticados también, que eran mejores.

Formulación matemática

Podemos expresar el cifrado de César matemáticamente usando aritmética modular [véase 7]. En este caso, el módulo es 26, el número de letras del alfabeto. La aritmética se realiza del modo habitual, pero se suma un ingrediente: cualquier entero múltiplo de 26 puede reemplazarse por cero. Esto es precisamente lo que necesitamos para hacer que el alfabeto desplazado dé la vuelta hasta el principio de manera consistente. Ahora las letras A-Z están representadas por los números 0-25, con A = 0, B = 1, C = 2 y así sucesivamente hasta llegar a Z = 25. El cifrado de encriptación que desplaza A (en la posición 0) a F (en la posición 5) es la regla matemática:

$$n \rightarrow n + 5 \pmod{26}$$

Observa que U (en la posición 20) va a $20 + 5 = 25 \pmod{26}$, que representa Z, mientras que V (en la posición 21) va a $21 + 5 = 26 = 0 \pmod{26}$, que representa A. Esto muestra cómo la fórmula matemática asegura que el alfabeto da la vuelta correctamente.

El cifrado de desencriptación es una regla similar:

$$n \rightarrow n - 5 \pmod{26}$$

Como $n + 5 - 5 = n \pmod{26}$, desencriptación deshace encriptación.

En general, con la clave k , con el significado de «trasladar k pasos a la derecha», el cifrado de encriptación es la regla:

$$n \rightarrow n + k \pmod{26}$$

y el de desencriptación es la regla:

$$n \rightarrow n - k \pmod{26}$$

La ventaja de convertir el cifrado en un lenguaje matemático es poder describir códigos de manera precisa, y analizar sus propiedades, sin preocuparse del alfabeto utilizado. Así todo funciona con *números*. Esto también nos permitiría considerar símbolos adicionales: letras en minúscula (a, b, c,...), signos de puntuación, números...; bastaría cambiar

26 a algo más grande y decidir de una vez y para siempre cómo asignar los números.

Descifrando el cifrado César

El cifrado César es muy inseguro. Como se describió, hay solo 26 posibilidades, de modo que puedes probarlas todas hasta desencriptar un mensaje que parezca tener sentido. Eso no funcionaría para una variación, llamada «código por sustitución», en el cual el alfabeto está desordenado, no solo desplazado. Ahora hay $26!$ códigos [véase $26!$], que es una cantidad enorme. Aunque hay un modo sencillo de descifrar esos códigos, ya que en cualquier lenguaje dado, algunas letras son más comunes que otras.

En inglés, la letra más común es E, y aparece alrededor de un 13 % de las veces. Luego viene la T, en un 9 %, luego la A, un 8 %, etcétera. Si interceptas un texto cifrado largo y sospechas que ha sido generado desordenando el alfabeto, puedes calcular la frecuencia de cada letra; probablemente no encajarán exactamente con la imagen teórica, porque los textos varían.

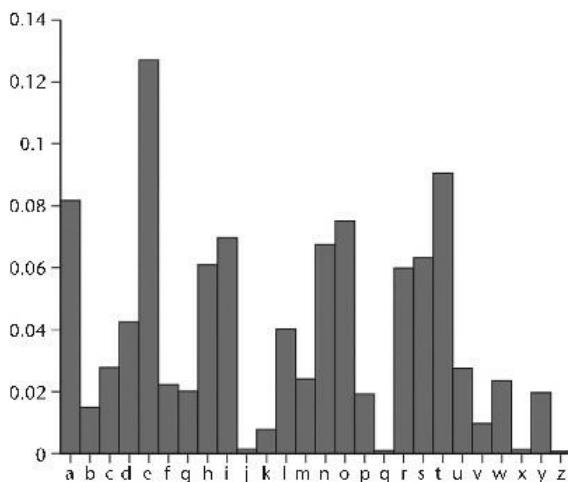


Figura 157. Frecuencia de una letra dada en un texto típico en inglés.

Pero si, por ejemplo, la letra Q aparece con más frecuencia en el texto cifrado que cualquier otra, puedes tratar de sustituir E por Q. Si la siguiente letra más común es M, ver qué sucede si sustituyes T por M, y así sucesivamente. Puedes alterar el orden un poco, incluso así tendrías muchas menos posibilidades que probar.

Supongamos, por ejemplo, que el texto cifrado es, en parte,

XJMNQXJMABW

y sabes que las tres letras más frecuentes en todo el texto cifrado son Q, M y J, en ese orden. Sustituye E por Q, T por M y A por J, dejando el resto en blanco.

- A T - E - A T - - -

No es difícil adivinar que el mensaje podría ser:

MATHEMATICS

Si tienes más texto cifrado, pronto verías si eso tiene sentido, porque ahora estás intuyendo que X se desencripta como M, N se desencripta como H, A se desencripta como I, B se desencripta como C y W se desencripta como S. Si en algún otro lugar el texto cifrado es:

WBAQRBQHABMALR

entonces tu desencriptación provisional sería:

SCIE-CE-ICTI—

lo cual sugiere que podría ser:

SCIENCEFICTION

La doble aparición de N suma una confirmación útil, y ahora falta saber cómo se desencriptan N, F y O. Este proceso es rápido, incluso a mano, y rápidamente se decodifica el código.

Hay miles de métodos de codificación diferentes. El proceso de descifrar un código, averiguar cómo desencriptar mensajes sin que se digan los algoritmos o la clave, depende del código. Hay algunos métodos prácticos que son casi imposibles de descifrar, porque la clave va cambiando antes de que los criptógrafos que intentan descifrar el código tengan suficiente información. Durante la segunda guerra mundial esto se lograba usando «libretas de un solo uso»; básicamente una libreta de claves complicadas, cada una de las cuales era usada una vez para un mensaje corto y luego se destruía. El principal problema con esos métodos es que el espía tenía que llevar la libreta a todas partes, o en la actualidad algún aparato electrónico que desempeñe el mismo papel, y este podría encontrarse en su posesión.

La máquina enigma

Uno de los sistemas de cifrado más famosos es la máquina alemana Enigma, usada en la segunda guerra mundial. El código fue descifrado por matemáticos e ingenieros electrónicos que trabajaban en Bletchley Park; el más famoso, pionero de los ingenieros informáticos, es Alan Turing. Les resultó de gran ayuda en esta tarea tener en su posesión una máquina Enigma en funcionamiento, que les fue proporcionada en 1939 por un equipo de criptógrafos polacos que ya habían hecho avances significativos en el descifrado del código Enigma.

Otros códigos alemanes también se descifraron, incluyendo el todavía más difícil código Lorenz, y en este caso ninguna máquina real estaba disponible. En su lugar, un equipo de criptoanalistas dirigidos por Ralph Tester dedujo la estructura probable de la máquina a partir de los mensajes que envió. Luego Tutte tuvo una idea genial que supuso un comienzo en el descifrado del código, la cual proporcionó información útil sobre el modo en que la máquina funcionaba. Después de eso, los avances fueron más rápidos. La tarea práctica de descifrar este código requirió un artilugio electrónico, Colossus, diseñado y construido por un equipo dirigido por Thomas Flowers. Colossus fue, de hecho, uno de los ordenadores electrónicos pioneros, diseñado para una tarea específica.



Figura 158. Una máquina Enigma.

La máquina Enigma constaba de un *teclado* para introducir el texto plano, y una serie de *rotores*, cada uno con 26 posiciones correspondiente a las letras del alfabeto. Las máquinas iniciales tenían tres rotores, más tarde esto fue incrementando a un conjunto de cinco (ocho para la armada alemana) de los cuales tan solo tres se seleccionaban en un día cualquiera. El objetivo de los rotores era desordenar las letras del texto plano *de modo que cambiase cada vez que se tecleaba una nueva letra*. El método preciso es complicado. Véase: [máquina enigma](#).

Más o menos, el proceso es el siguiente:

Cada rotor cifra el alfabeto como un cifrado César, con el desplazamiento determinado por su posición. Cuando se da una letra al primer rotor, el resultado desplazado se pasa al segundo rotor y se desplaza de nuevo; luego el resultado se pasa al tercer rotor y se desplaza una tercera vez. En este punto, la señal alcanza un *reflector*, un conjunto de 13 cables que conectan las letras en pares, el cual intercambia la letra resultante por aquella a la que está conectada. Entonces el resultado pasa de vuelta a través de los tres rotores, para producir la letra del código final correspondiente a la entrada dada.

Luego se lee el texto cifrado en un *panel de luces*: 26 bombillas, una tras cada letra del alfabeto, que se encienden para mostrar la letra en el texto cifrado que corresponde al texto plano que acabamos de teclear.

La característica más ingeniosa del artilugio es cómo la correspondencia entre la letra del texto plano y la letra que resulta en el texto cifrado *cambia* en cada pulsación sucesiva. A medida que cada nueva letra se pulsa en el teclado, los rotores se mueven a la siguiente posición, cifrando el alfabeto de una manera diferente. El que está a la derecha se mueve un paso hacia delante cada vez. El que está en el centro se mueve un paso cuando el rotor de la derecha pasa la Z y vuelve a la A. Y el que está a la izquierda hace lo mismo con respecto al rotor central.

Los rotores, por lo tanto, funcionan de forma similar al cuentakilómetros de un coche (antes de que fuesen electrónicos). Aquí la cifra de las «unidades» hace ciclos de 0 a 9 y luego vuelve a 0, un paso de cada vez. La cifra de las «decenas» hace lo mismo, pero se mueve solo cuando se «lleva una» de la posición de las unidades, cuando esta pasa de 9 y vuelve a 0. De modo similar, la cifra de las «centenas» incrementa 1 solo cuando se lleva una cifra de la posición de las decenas. La serie de tres cifras, por lo tanto, va de 000 a 999, sumando 1 en cada paso y luego volviendo a 000.



Figura 159. Una serie de tres rotores.

Aunque los rotores de Enigma tenían 26 «cifras» (las letras de la A a la Z) en lugar de 10. Además, podían colocarse en cualquier posición de arranque, un total de $26 \times 26 \times 26 = 17.576$ posiciones. En el uso real, esta posición de arranque se establecía al principio del día y se usaba durante 24 horas antes de volver a cambiarse.

He descrito los pasos del proceso en términos de rotores izquierdo, central y derecho, pero en realidad la máquina podía ajustarse para usar cualquiera de los seis modos posibles de colocar los rotores en orden. Esto multiplica inmediatamente los posibles ajustes iniciales por 6 y da 105.456 posibilidades.

Para uso militar, se proporcionaba un nivel añadido de seguridad con un panel con clavijas, el cual intercambia pares de letras dependiendo de qué letra se conectaba con qué letra por un cable conector. Se usaban hasta diez de esos cables, lo cual daba 150.738.274.937.250

posibilidades. De nuevo, los ajustes del panel con clavijas se renovaban cada día.

Este sistema tiene una ventaja práctica importante para los usuarios: es simétrico. La misma máquina puede usarse para desencriptar el mensaje. Los ajustes iniciales para un día concreto deben transmitirse a todos los usuarios; los alemanes usaban una versión de libretas de un solo uso para lograrlo.

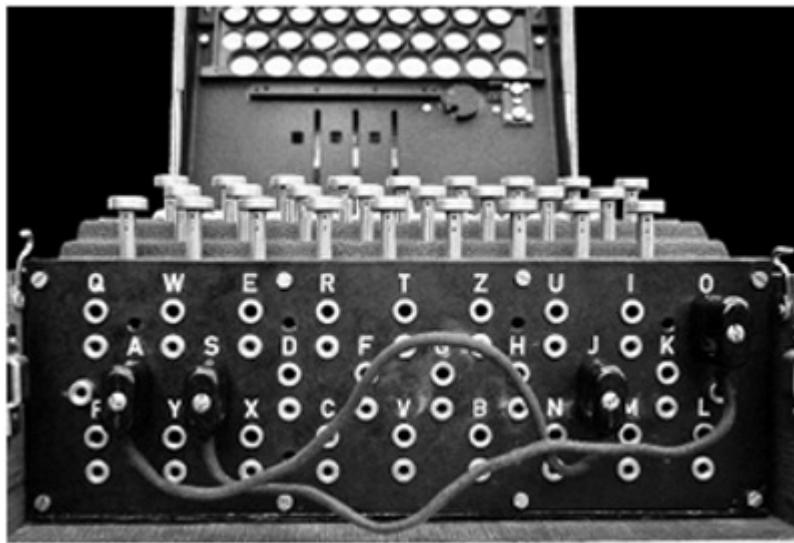


Figura 160. El panel de clavijas con dos cables de conexión colocados.

Descifrando el código enigma

Sin embargo, el procedimiento también introduce debilidades. La más notoria era que si el enemigo, en este caso los Aliados, podía averiguar los ajustes, entonces todo mensaje enviado ese día podía desencriptarse. Había otras. En concreto, el código era vulnerable si los mismos ajustes

se empleaban dos días consecutivos, como sucedía ocasionalmente por error.

Explotando estas debilidades, el equipo de Bletchley Park descifró el funcionamiento del código Enigma por primera vez en enero de 1940. Su trabajo se apoyó mucho en el conocimiento y las ideas obtenidas por un grupo polaco de criptoanalistas dirigido por el matemático Marian Rejewski, quien había estado intentando descifrar el código Enigma desde 1932. Los polacos identificaron un fallo, basado en la manera en que los ajustes del día se transmitían a los usuarios. Esto, de hecho, reducía el número de ajustes que había que considerar de 10.000 billones a 100.000. Catalogando estos patrones en los ajustes, los polacos pudieron calcular rápidamente qué ajustes se habían usado en un día concreto. Inventaron una máquina llamada «ciclómetro» para que les ayudase. Preparar el catálogo les costó alrededor de un año, pero una vez estuvo completo, solo se tardaba 15 minutos en deducir los ajustes del día y descifrar el código.

Los alemanes mejoraron su sistema en 1937 y los polacos tuvieron que empezar de nuevo. Desarrollaron varios métodos. El más potente fue un artilugio que llamaron «bomba kryptologiczna» («bomba criptológica»). Cada uno de ellos realizaba un análisis en bruto de los 17.576 ajustes posibles de los tres rotores, para cada uno de los seis órdenes posibles en los cuales podían colocarse.

En 1939, poco después de llegar a Bletchley Park, Turing introdujo una versión británica de la *bomba kryptologiczna*, conocida como «the bombe». De nuevo, su función era deducir los ajustes del rotor inicial y el orden de los rotores. En junio de 1941 había cinco bombas en uso, al final de la guerra en 1945, había 210. Cuando la armada alemana se pasó a máquinas de cuatro rotores, se fabricaron bombas modificadas.

A medida que el sistema alemán se modificaba para incrementar la seguridad, quienes se encargaban de descifrarlo encontraban modos de anular las mejoras. En 1945, los Aliados pudieron desencriptar casi todos los mensajes alemanes, pero el alto mando alemán continuaba creyendo que todas las comunicaciones eran totalmente seguras. Sus criptógrafos, por el contrario, no tenían tales delirios, pero dudaban que nadie fuese capaz de hacer el enorme esfuerzo necesario para descifrar el código. Todos los Aliados habían logrado una ventaja enorme, pero tenían que tener cuidado de cómo la usaban para evitar revelar su habilidad para desencriptar los mensajes.

Códigos asimétricos

Una de las mayores ideas en criptografía es la posibilidad de claves *asimétricas*. En este caso la clave de encriptación y la clave de desencriptación son diferentes, tanto es así que no es posible en la práctica averiguar la clave de desencriptación aunque sepas la de encriptación. Esto podría parecer extraño, ya que un proceso es el

inverso del otro, pero hay métodos para establecerlos de modo que «hacer el método de encriptado hacia atrás» no sea factible. Un ejemplo es el código RSA [véase 7], basado en propiedades de los números primos en aritmética modular. En este sistema, el algoritmo de encriptación, el algoritmo de desencriptación y la clave de encriptación pueden hacerse *públicas*, e incluso así no es posible deducir la clave de desencriptación. Sin embargo, receptores legítimos pueden hacerlo porque también tienen la *clave secreta*, lo que les dice cómo desencriptar mensajes.

§. 56 La conjetura de la salchicha

Se ha probado que la colocación de esferas cuya «envolvente convexa» tiene el volumen más pequeño es siempre una salchicha para 56 esferas o menos, pero no para 57.

Empaquetado de film transparente

Para comprender este resultado, empecemos con algo más sencillo: empaquetar círculos. Supongamos que estás empaquetando juntos en el plano muchos círculos idénticos, y los envuelves con film transparente, rodeándolos con la curva más pequeña que puedas. Técnicamente esta curva se llama «envolvente convexa» del conjunto de círculos. Con siete círculos, por ejemplo, podías intentar una «salchicha» larga.



Figura 161. Forma de salchicha con su envoltorio.

Sin embargo, supongamos que quieres hacer el área total dentro de la curva lo más pequeña posible. Si cada círculo tiene radio 1, entonces el área para la salchicha es:

$$24 + \pi = 27,141$$

Pero hay una colocación mejor de los círculos, un hexágono con un círculo central, y ahora el área es:

$$12 + \pi + 6\sqrt{-3} = 25,534$$

que es más pequeña.

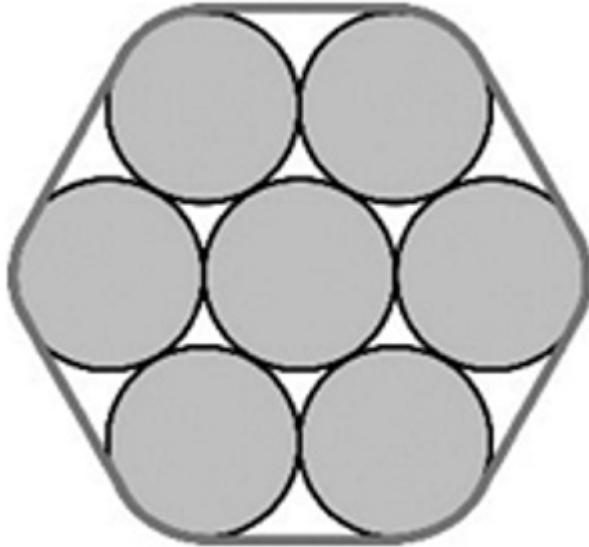


Figura 162. Forma hexagonal con su envoltorio. Esta da un área más pequeña que la salchicha.

De hecho, incluso con tres círculos, la forma de salchicha no es la mejor. El área dentro de la curva para la salchicha es:

$$8 + \pi = 11,14$$

Pero para el triángulo de círculos es:

$$6 + \pi + \sqrt{3} = 10,87$$

Sin embargo, si usas *esferas* idénticas en lugar de círculos y los envuelves con film transparente haciendo que la superficie tenga la menor *área* posible, entonces para siete esferas resulta que la salchicha alargada lleva a un *volumen* total más pequeño que la colocación

hexagonal. De hecho, este patrón de salchicha da el volumen más pequeño dentro del envoltorio para cualquier número de esferas hasta 56 (incluido). Pero con 57 esferas o más, las disposiciones que minimizan el volumen son más redondeadas.

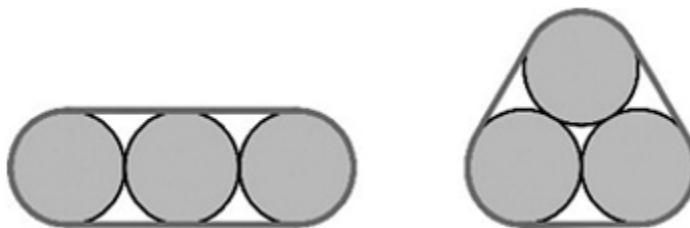


Figura 163. La forma de salchicha con su envoltorio para tres círculos.

El triángulo tiene un área más pequeña.

Menos intuitivo es lo que pasa en espacios de cuatro o más dimensiones. La colocación de esferas de cuatro dimensiones cuyas envolturas dan el «volumen» tetradimensional más pequeño es una salchicha para cualquier número de esferas hasta al menos 50.000. Aunque *no* es una salchicha para más de 100.000 esferas. De modo que el empaquetado del volumen menor usa salchichas de esferas muy largas y delgadas hasta obtener una cantidad ingente de ellas. Nadie sabe el valor preciso en el cual las salchichas de cuatro dimensiones dejan de ser la mejor opción.

El cambio más fascinante *probablemente* aparezca con cinco dimensiones. Podrías imaginar que en cinco dimensiones las salchichas son la mejor opción hasta, por ejemplo, 50.000 millones de esferas, y que luego algo más redondeado da un volumen pentadimensional más

pequeño; y para seis dimensiones se aplicaría lo mismo lo que nos llevaría a trececientos millones, y así sucesivamente. Pero en 1975, Laszlo Fejes Tóth formuló la

conjetura de la salchicha, la cual afirma que para cinco dimensiones o más, la disposición de las esferas cuya envolvente convexa tiene volumen mínimo es *siempre* una salchicha, por muy grande que el número de esferas pueda ser.

En 1998, Ulrich Betke, Martin Henk y Jörg Wills probaron que Tóth estaba en lo correcto para cualquier número de dimensiones mayor o igual a 42. Hasta la fecha, esto es lo mejor que se ha podido hacer.

§. 168 Geometría finita

Durante siglos, la geometría de Euclides fue la única geometría. Se pensaba que era geometría verdadera del espacio, lo cual significa que ninguna otra geometría sería posible. Ya no creemos en esa afirmación. Hay muchos tipos de geometrías no euclídeas, correspondientes a superficies curvas. La relatividad general ha mostrado que el espacio-tiempo real es curvo, no plano, cerca de cuerpos enormes como las estrellas [véase 11]. Otro tipo de geometría, la geometría proyectiva, proviene de la perspectiva en arte. Hay incluso geometrías con una cantidad finita de puntos. La más sencilla tiene siete puntos, siete rectas y 168 simetrías, y nos lleva a la increíble historia de los grupos simples

finitos, culminando en el extraño grupo conocido, con razón, como «el monstruo».

Geometría no euclídea

A medida que los humanos empezamos a navegar por el globo, la geometría esférica, la geometría natural en la superficie de una esfera, empezó a cobrar protagonismo, porque una esfera es un modelo bastante preciso de la forma de la Tierra, aunque no es exacto, ya que la Tierra está más cerca de un esferoide, achatado por los polos. Pero la navegación tampoco era exacta. Sin embargo, una esfera es una superficie en el espacio euclídeo, de modo que parecía que la geometría esférica no era un nuevo tipo de geometría, tan solo una especialización de la euclídea. Después de todo, nadie consideró la geometría de un triángulo como la desviación radical de Euclides, incluso si técnicamente un triángulo no es plano.

Todo esto cambió cuando los matemáticos empezaron a observar más de cerca una característica de la geometría de Euclides: la existencia de rectas paralelas. Estas son líneas rectas que nunca se encuentran, no importa cuánto se extiendan. Seguramente Euclides se dio cuenta de que las paralelas escondían sutilezas, porque fue lo suficiente astuto para hacer de su existencia uno de los axiomas básicos en su desarrollo de la geometría. Debió de haberse dado cuenta de que no era obvio.

La mayoría de sus axiomas son claros e intuitivos: «dos ángulos rectos cualesquiera son iguales», por ejemplo. Por el contrario, el axioma de las paralelas era un poco trabalenguas: «Si un segmento se corta con dos rectas formando dos ángulos interiores en el mismo lado esa suma es menor que dos ángulos rectos, entonces las dos rectas, si se extienden indefinidamente, se cortan en el lado en el cual los ángulos suman menos que los dos ángulos rectos». Los matemáticos empezaron a preguntarse si este tipo de complejidad era necesaria. ¿Podría ser posible probar la existencia de paralelas a partir del resto de los axiomas de Euclides?

Se las arreglaron para reemplazar la formulación engorrosa de Euclides por unos supuestos más intuitivos y sencillos. Quizá el más sencillo es el axioma de Playfair: dada una recta y un punto que no está en esa recta, hay una única paralela a la recta dada que pasa por ese punto. El nombre se debe a John Playfair, quien lo afirmó en su *Elements of Geometry* de 1795. Estrictamente hablando, presupone que hay al menos una paralela, porque otros axiomas se podían usar para probar que existía una paralela. Se hicieron muchos intentos de obtener el axioma de la paralela a partir del resto de axiomas de Euclides, pero todos fracasaron. Finalmente, la razón se hizo evidente: no podía hacerse. Existen modelos de geometría que satisfacen todos los axiomas de Euclides *excepto* el de las paralelas. Si existiese una prueba para el axioma de las paralelas, entonces ese axioma sería válido en ese modelo; sin embargo, no lo es. Por lo tanto, no hay prueba.

De hecho, la geometría esférica proporciona ese modelo. «Recta» se reinterpreta como «circunferencia máxima», la circunferencia que resulta en una esfera al cortarse esta por un plano que pasa por el centro. Dos circunferencias máximas cualesquiera se cortan; por lo tanto, no hay paralelas en toda esta geometría. Sin embargo, este contraejemplo pasó desapercibido, porque dos circunferencias máximas cualesquiera se cortan en dos puntos, diametralmente opuestos el uno al otro. Por el contrario, Euclides requería que dos rectas cualesquiera se cortasen solo en un punto, a menos que fuesen paralelas y no se cortasen en ninguno.

Desde un punto de vista actual, la respuesta era directa: reinterpretar «punto» como «par de puntos diametralmente opuestos». Esto da lo que ahora llamamos «geometría elíptica». Pero esto era demasiado abstracto para paladares más tempranos, y dejó un agujero que Playfair explotó cuando descartó esas geometrías. En su lugar, los matemáticos desarrollaron la geometría hiperbólica, en la cual infinidad de paralelas a una recta dada pasan a través de un punto dado. Un modelo estándar es el disco de Poincaré, que es el interior de un círculo. Una *recta* está definida como cualquier arco de un círculo que corta la frontera en un ángulo recto. Se necesitó casi un siglo para que estas ideas calasen y dejasesen de ser controvertidas.

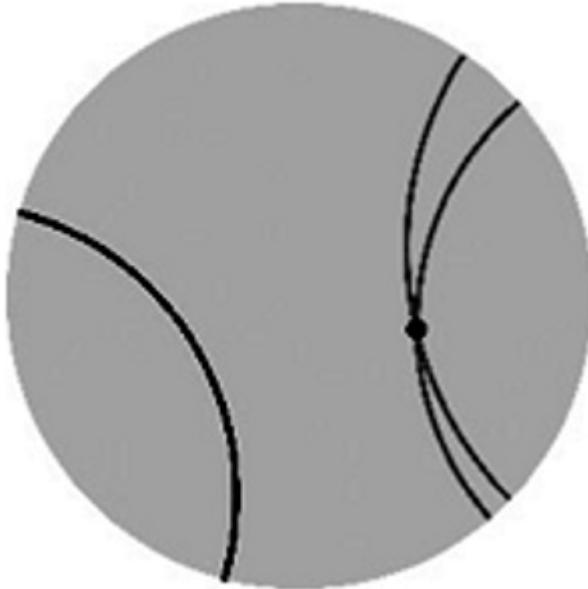


Figura 164. El modelo del disco de Poincaré del plano hiperbólico (la superficie gris). Las dos líneas grises son paralelas a la negra y pasan a través del mismo punto.

Geometría proyectiva

Mientras tanto, otra variante de la geometría de Euclides estaba emergiendo. Esta vino del lado del arte y la arquitectura, donde los artistas del Renacimiento italiano estaban desarrollando dibujos con perspectiva. Supongamos que estás frente a un plano de Euclides, entre dos paralelas, como alguien de pie en medio de una carretera totalmente recta que es infinitamente larga. ¿Qué ves?

Lo que *no* ves es dos rectas que nunca se cortan. En su lugar, ves dos rectas que se cortan en el horizonte.

¿Cómo puede ser esto? Euclides dijo que las paralelas no se cortaban, pero tus ojos te dicen que lo hacen. Realmente no hay una contradicción

lógica. Euclides dijo que las paralelas no se cortan *en un punto del plano*. El horizonte no es parte del plano; si lo fuera, sería la arista del plano, pero un plano no tiene arista. Lo que un artista necesita no es un plano euclídeo, sino un plano con un extra añadido: el horizonte. Y este puede pensarse como una «recta en el infinito», compuesta de «puntos en el infinito», los cuales están donde las paralelas se cortan.

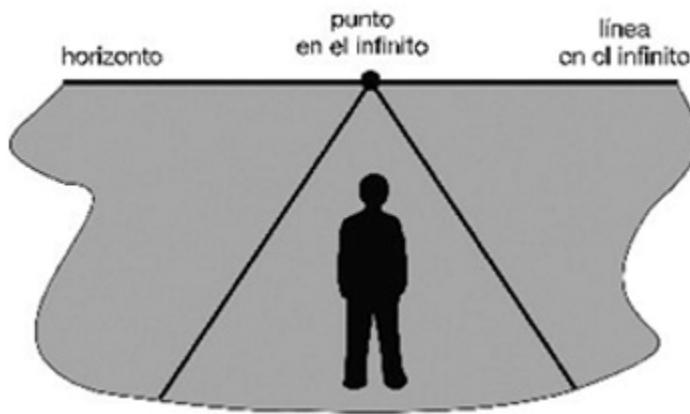


Figura 165. Las paralelas se cortan en el infinito.

Esta descripción tiene más sentido si pensamos en lo que hace un artista: coloca un caballete con un lienzo y transfiere la escena frente a él al lienzo *proyectándola*. Hace esto a ojo o usando artilugios mecánicos u ópticos. Matemáticamente, proyectas un punto en el lienzo dibujando una recta desde el punto al ojo del artista y dibujando un punto donde esa recta corta al lienzo. Así es básicamente como funciona una cámara: la lente proyecta el mundo exterior en un carrete o, para las cámaras

digitales, en un dispositivo de carga acoplada. De manera similar, tu ojo proyecta una escena en tu retina.

Para ver de dónde viene el horizonte, redibujamos la imagen de las paralelas desde el lateral (Figura de la derecha). Los puntos en el plano euclídeo (gris) proyectan puntos bajo el horizonte. Las rectas frente al artista proyectan rectas que *acaban* en el horizonte. El propio horizonte no es la proyección de un punto en el plano: supongamos que intentas encontrar ese punto proyectándolo de nuevo, como se muestra con la flecha; este es paralelo al plano, así que no se corta nunca con él, continúa «hasta infinito» sin chocarse con el plano. Por lo tanto, *nada* en el plano se corresponde con el horizonte.

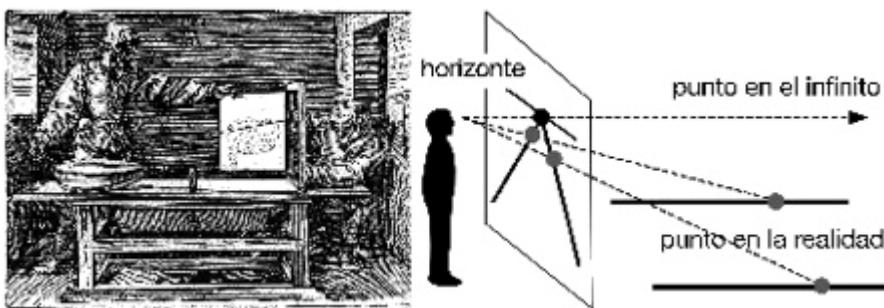


Figura 166. Izquierda: grabado de Durero de 1525 que ilustra la proyección. Derecha: proyección de rectas paralelas en el lienzo.

Una geometría consistente lógicamente puede definirse sobre la base de esta idea. El plano euclídeo se extiende añadiendo una «recta en el infinito», hecha de «puntos en el infinito». En esta configuración, llamada «geometría proyectiva», las paralelas no existen; dos rectas

distintas cualesquiera se cortan exactamente en un punto. Además, como en la geometría euclídea, dos puntos cualesquiera pueden unirse formando una recta, de modo que ahora hay una «dualidad» agradable: si intercambiamos puntos por rectas y rectas por puntos, todos los axiomas siguen siendo válidos.

El plano de Fano

Persiguiendo esta idea nueva, los matemáticos se preguntaron si podría haber análogos finitos de la geometría proyectiva, es decir, configuraciones hechas a partir de un número finito de puntos y rectas, en el cual:

- Dos puntos distintos cualesquiera estén exactamente en una recta.
- Dos rectas distintas cualesquiera se corten exactamente en un punto.

De hecho, esas configuraciones existen, no necesariamente como diagramas en el plano o en el espacio. Pueden definirse algebraicamente estableciendo un tipo de sistema de coordenadas para la geometría proyectiva. En lugar del par de números reales (x, y) que normalmente usamos para el plano euclídeo, usamos una terna (x, y, z) . Normalmente las ternas definen coordenadas en el espacio euclídeo tridimensional, pero imponemos una condición adicional: las únicas cosas que importan

son las proporciones entre las coordenadas. Por ejemplo, (1, 2, 3) representan el mismo punto que (2, 4, 6) o (3, 6, 9).

Ahora podemos *casi* reemplazar (x, y, z) por el par $\frac{x}{z}, \frac{y}{z}$, lo cual nos lleva de vuelta a dos coordenadas y al plano euclídeo. Sin embargo, z puede ser cero. Si eso ocurre, podemos pensar en $\frac{x}{z}$ e $\frac{y}{z}$ como «infinito», con la característica maravillosa de que la proporción x y todavía tiene sentido. De modo que puntos con coordenadas $(x, y, 0)$ están «en infinito» y el conjunto de todos ellos forma la recta en el infinito, el horizonte. Solo una terna tiene que excluirse para hacer que todo esto funcione: estamos de acuerdo en que $(0, 0, 0)$ no representa un punto. Si lo hiciese, representaría todos los puntos, ya que (x, y, z) y $(0x, 0y, 0z)$ serían lo mismo. Pero este último es $(0, 0, 0)$.

Una vez nos acostumbramos a estas «coordenadas homogéneas», como así se llaman, podemos desarrollar un juego similar en generalidades mayores. En concreto, podemos obtener configuraciones finitas con las propiedades requeridas cambiando las coordenadas de los números reales a enteros módulo p , para un p primo. Si consideramos $p = 2$, el caso más sencillo, las coordenadas posibles son 0 y 1. Hay ocho ternas, pero de nuevo $(0, 0, 0)$ no está permitido, lo que deja siete puntos:

$$(0, 0, 1) (0, 1, 0) (1, 0, 0) (0, 1, 1) (1, 0, 1) (1, 1, 0) (1, 1, 1)$$

La «geometría proyectiva finita» resultante se conoce como el «plano de Fano», llamado así por el matemático italiano Gino Fano, quien publicó la idea en 1892. De hecho, describió un espacio tridimensional proyectivo finito con 15 puntos, 35 rectas y 15 planos. Usa cuatro coordenadas, con los valores 0 y 1, excluyendo $(0, 0, 0, 0)$. Cada plano tiene la misma geometría que el plano de Fano.

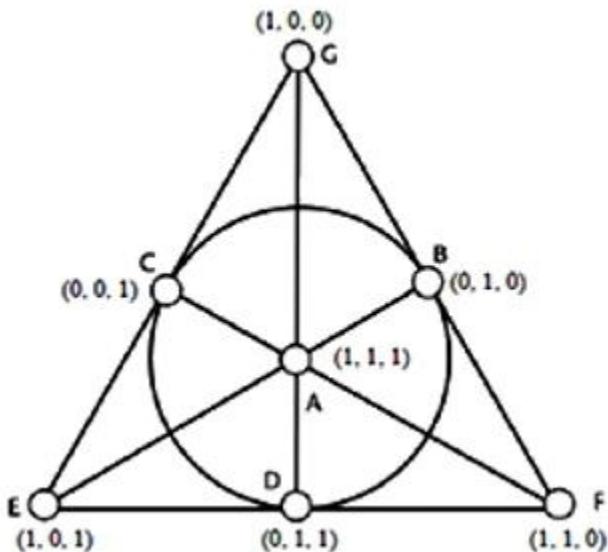


Figura 167. Los siete puntos y las siete rectas del plano de Fano.

El plano de Fano tiene siete rectas, cada una contiene tres puntos; y siete puntos, cada uno está en tres rectas. En el dibujo, todas las líneas son rectas, excepto BCD, que es circular, pero viene de intentar representar enteros de módulo 2 en un plano convencional. Realmente, los siete puntos se tratan simétricamente. Las coordenadas de cualquiera de los

tres puntos que forman una recta siempre suman cero; por ejemplo, la recta de abajo se corresponde con:

$$\begin{aligned}(1, 0, 1) + (0, 1, 1) + (1, 1, 0) &= \\ = (1 + 0 + 1, 0 + 1 + 1, 1 + 1 + 0) &= (0, 0, 0)\end{aligned}$$

ya que $1 + 1 = 0$ módulo 2.

Simetrías del plano de Fano

Aunque todavía no hay ninguna señal del número 168, estamos cerca. La clave es la simetría. Una *simetría* de un objeto matemático o sistema es un modo de transformarlo que conserve su estructura. Las simetrías naturales de la geometría euclídea son movimientos rígidos, los cuales no cambian ángulos o distancias. Algunos ejemplos son las traslaciones, que hacen deslizamientos en el plano hacia los lados; las rotaciones, que lo giran alrededor de un punto fijo; y las reflexiones, que lo reflejan respecto a alguna recta fija.

Las simetrías naturales de la geometría proyectiva no son movimientos rígidos, porque las proyecciones pueden distorsionar formas y comprimir o magnificar longitudes y ángulos. Son proyecciones: transformaciones que no cambian las relaciones de incidencia, es decir, cuando un punto está o no está en una recta. Las simetrías ahora se reconocen como

propiedades vitales de todos los objetos matemáticos. De modo que es natural preguntar cuáles son las simetrías del plano de Fano.

En este caso no quiero decir simetrías del diagrama de movimiento rígido, en el sentido de un triángulo equilátero que tiene seis simetrías de movimiento rígido. Quiero decir permutaciones de siete puntos, tales como que siempre que tres puntos formen una recta, los puntos permutados también formarán una recta. Por ejemplo, podría transformar la recta de abajo EDF en la circunferencia CDB. Denotemos esto así:

$$E' = CD' = DF' = B$$

en donde el apóstrofe indica cómo transformar estas tres letras. Tenemos que decidir qué serían A', B', C' y G', de manera que no acabemos con una permutación. Tienen que ser diferentes de C, D y B. Podríamos probar con:

$$A' = E$$

y ver qué implica. Como ADG es una recta, A'D'G' debe ser una recta. Pero hemos decidido ya que A' = E y D' = D. ¿Qué debería ser G'? Para encontrar la respuesta, observa que la única recta que contiene E y D es EDF. De modo que tenemos que hacer que sea G' = F. Completando rectas sucesivas de esta manera, averiguamos que B' = G y C' = A. Así

mi permutación asocia ABCDEFG con 'B'C'D'E'F'G', que es EGADCBF.

No es trivial visualizar estas transformaciones, pero podemos encontrarlas algebraicamente de esta manera. Hay más de las que podrías esperar. De hecho, sorprendentemente, hay 168.

Para probarlo, usamos el método que hemos visto, que es típico. Empieza con un punto A. ¿Adónde puedes ir? En principio, a cualquiera de A, B, C, D, E, F y G, de modo que hay 7 opciones. Supongamos que se mueve a A'. Una vez hecho, observa el punto B. Luego podemos mover B a cualquiera de las 6 posiciones que quedan sin toparnos con problemas con las relaciones de incidencia. Esto da $7 \times 6 = 42$ potenciales simetrías hasta el momento. Una vez que se decide que A y B van a A' y B', no tenemos opción sobre adónde mover E, el tercer punto en la recta AB. Debemos moverlo al tercer punto en A'B', cualquiera que este sea, no hay ninguna otra posibilidad. Sin embargo, todavía hay cuatro puntos cuyo destino está sin decidir. Escoge uno de ellos: puede moverse a *cualquiera* de esos cuatro puntos. Pero una vez se escoge su destino, todo lo demás está determinado por la geometría.

Puede comprobarse que todas las combinaciones conservan las relaciones de incidencia: rectas correspondientes siempre se cortan en los puntos correspondientes. De modo que en total hay $7 \times 6 \times 4 = 168$ simetrías. Un modo civilizado de probar todo esto es usar álgebra lineal en el cuerpo de enteros de módulo 2. Las transformaciones concernientes

son entonces representadas como matrices invertibles 3×3 , con entradas 0 o 1.

La cuártica de Klein

El mismo grupo aparece en análisis complejo. En 1893, Adolf Hurwitz probó que una superficie compleja (técnicamente, una superficie de Riemann compacta) con g agujeros tiene como máximo $84(g - 1)$ simetrías. Cuando hay tres agujeros, este número es 168. Felix Klein construyó una superficie conocida como la «cuártica de Klein», con ecuación:

$$x^3y + y^3z + z^3x = 0$$

con *coordenadas homogéneas complejas* (x, y, z). El grupo de simetría de esta superficie resulta ser el mismo que el del plano de Fano, de modo que tiene el orden máximo posible que predice el teorema de Hurwitz, 168.



Figura 168. Tres secciones reales de la cuártica de Klein.

La superficie está relacionada con un teselado con triángulos del plano hiperbólico, en el cual en cada vértice se encuentran siete de ellos.

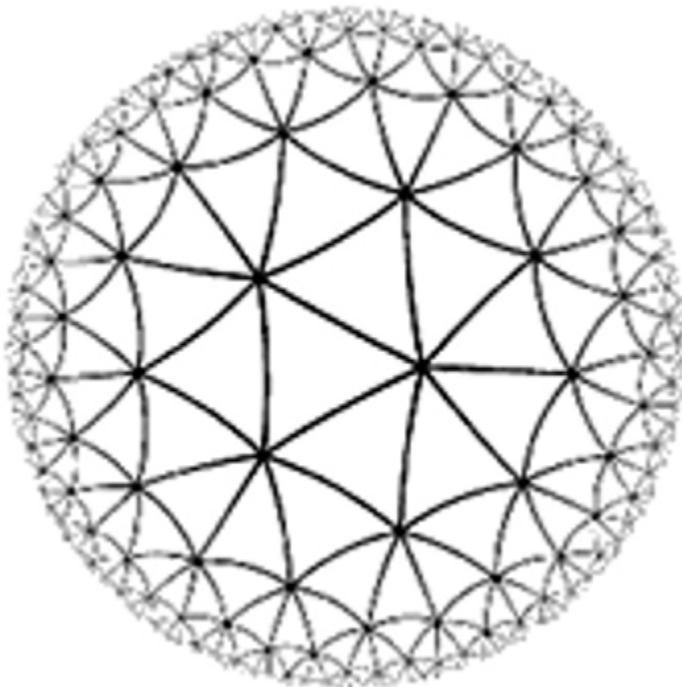


Figura 169. Teselado asociado del plano hiperbólico, representado en el modelo del disco de Poincaré.

Grupos simples y el monstruo

Las simetrías de cualquier sistema matemático u objeto forman un *grupo*. En el lenguaje ordinario esto tan solo quiere decir una colección, o conjunto, pero en matemáticas se refiere a una colección con una característica extra. Dos miembros cualesquiera de la colección pueden *combinarse* para dar otro en la colección. Es parecido a la multiplicación: dos miembros g, h , del grupo se combinan para dar el producto gh . Pero los miembros, y la operación que los combina, pueden

ser los que queramos; siempre y cuando tengan algunas propiedades sutiles, que están motivadas por las simetrías.

Las simetrías son transformaciones, y el modo de combinar dos transformaciones es realizar primero una de ellas y luego la otra. Esta noción particular de «multiplicación» obedece a varias leyes algebraicas sencillas. La multiplicación es asociativa: $(gh)k = g(hk)$. Hay una identidad 1 tal que $1g = g1 = g$. Todo g tiene un inverso g^{-1} tal que $g^{-1}g = 1$. (La propiedad commutativa $gh = hg$ no es un requerimiento, ya que no funciona para muchas simetrías.) Cualquier sistema matemático que cuente con una operación que obedezca a estas tres reglas se llama «grupo».

Para las simetrías, la propiedad asociativa es automáticamente cierta porque estamos combinando transformaciones, la identidad es la transformación «hacer nada», y la inversa de una transformación es «deshacerlo». De manera que las simetrías de cualquier sistema u objeto forman un grupo bajo la composición. En concreto, esto es cierto para el plano de Fano. El número de transformaciones en su grupo de simetría (llamado «orden del grupo») es 168. Resulta ser un grupo muy inusual.

Muchos grupos pueden dividirse en combinaciones de grupos más pequeños, un poco como factorizar números en primos, pero el proceso es más complicado. Los análogos de factores primos se llaman «grupos simples». Estos son grupos que no pueden dividirse de esta manera. «Simple» no quiere decir «fácil», significa «tener solo un componente».

Hay infinidad de grupos finitos, grupos de orden finito, es decir, con una cantidad finita de miembros. Si escoges uno al azar, raramente es simple, de la misma forma que los primos son extraños comparados con los números compuestos. Sin embargo, hay infinidad de grupos simples, de nuevo, igual que con los primos. De hecho, algunos están relacionados con los primos. Si n es cualquier número, entonces los enteros módulo n [véase 7] forman un grupo si componemos miembros mediante la adición. Esto se llama «grupo cíclico de orden n ». Es simple exactamente cuando n es primo. De hecho, todos los grupos simples de orden primo son cíclicos.

¿Hay otros? Galois, en su trabajo sobre la ecuación de grado 5, encontró un grupo simple de orden 60. No es primo, por lo tanto el grupo no es cíclico. Consiste en todas las permutaciones pares [véase 2] de cinco objetos. Para Galois, los objetos eran las cinco soluciones de la ecuación de grado 5 [véase 5] y el grupo de simetría de la ecuación consistía en las 120 permutaciones de estas soluciones. Dentro estaba su grupo de orden 60 y Galois lo sabía porque el grupo es simple, no hay fórmula algebraica para las soluciones; la ecuación tiene *el tipo erróneo de simetría* para resolverse mediante una fórmula algebraica.

El siguiente grupo simple no cíclico más grande tiene orden 168 y es el grupo de simetría del plano de Fano. Entre 1995 y 2004, aproximadamente un centenar de expertos en álgebra se las arreglaron para clasificar todos los grupos simples finitos, es decir, hacer una lista

de todo. El resultado de este trabajo monumental, al menos 10.000 páginas en revistas, es que todo grupo simple finito encaja en una familia infinita de grupos muy relacionados, y hay 18 familias diferentes. Una familia, la de los grupos lineales proyectivos especiales, empieza con el grupo simple de orden 168.

Bueno, no todos. Hay exactamente 26 excepciones, llamadas «grupos esporádicos». Estas criaturas son un revoltijo fascinante, individuos excepcionales que a veces se relacionan unos con otros si no se es muy estricto. La tabla lista los 26 con sus nombres y órdenes.

La mayoría de estos grupos reciben el nombre de la persona que los descubrió, pero el más grande se llama «el monstruo»; con razón, porque su orden es aproximadamente 8×10^{53} . Para ser precisos:

$$= 808\,017\,424\,794\,512\,875\,886\,459\,904\,961\,710\,757\,005\,754\,368\,000\\ 000\,000$$

Véase la tabla para la factorización en primos, que es más útil para los especialistas en teoría de grupos. Estuve tentado de hacer un capítulo sobre este número, pero me decidí por ponerlo en 168 para proporcionar una imagen más amplia.

El monstruo lo predijeron en 1973 Bernd Fischer y Robert Griess, y lo construyó en 1982 Griess. Es el grupo de simetrías de una curiosa estructura algebraica, el álgebra de Griess. El monstruo tiene conexiones

sorprendentes con un área totalmente diferente de las matemáticas: formas modulares en análisis complejo. Algunas coincidencias numéricas dieron pistas de esta relación, lo cual llevó a John Conway y Simon Norton a formular su conjetura *moonshine*, probada en 1992 por Richard Borcherds. Demasiado técnica para explicarla aquí, tiene conexiones con la teoría de cuerdas de la física cuántica [véase 11]. Si quieres detalles, echa un vistazo a: [*Monstrous moonshine*](#).

Tabla 14. Los 26 grupos simples finitos esporádicos.

Símbolo	Nombre	Orden
M_{11}	grupo de Mathieu	$2^4 \cdot 3^2 \cdot 5 \cdot 11$
M_{12}	grupo de Mathieu	$2^6 \cdot 3^3 \cdot 5 \cdot 11$
M_{22}	grupo de Mathieu	$2^7 \cdot 3^2 \cdot 5 \cdot 7 \cdot 11$
M_{23}	grupo de Mathieu	$2^7 \cdot 3^2 \cdot 5 \cdot 7 \cdot 11 \cdot 23$
M_{24}	grupo de Mathieu	$2^{10} \cdot 3^3 \cdot 5 \cdot 7 \cdot 11 \cdot 23$
J_1	grupo de Janko	$2^3 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 19$
J_2	grupo de	$2^7 \cdot 3^3 \cdot 5^2 \cdot 7$

	Janko	
J_3	grupo de Janko	$2^7 \cdot 3^5 \cdot 5 \cdot 17 \cdot 19$
J_4	grupo de Janko	$2^{21} \cdot 3^3 \cdot 5 \cdot 7 \cdot 11^3 \cdot 23 \cdot 29 \cdot 31 \cdot 37 \cdot 43$
Co_1	grupo de Conway	$2^{21} \cdot 3^9 \cdot 5^4 \cdot 7^2 \cdot 11 \cdot 13 \cdot 23$
Co_2	grupo de Conway	$2^{18} \cdot 3^6 \cdot 5^3 \cdot 7 \cdot 11 \cdot 23$
Co_3	grupo de Conway	$2^{10} \cdot 3^7 \cdot 5^3 \cdot 7 \cdot 11 \cdot 23$
Fi_{22}	grupo de Fisher	$2^{17} \cdot 3^9 \cdot 5^2 \cdot 7 \cdot 11 \cdot 13$
Fi_{23}	grupo de Fisher	$2^{18} \cdot 3^{13} \cdot 5^2 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 23$
Fi_{24}'	grupo de Fisher	$2^{21} \cdot 3^{16} \cdot 5^2 \cdot 7^3 \cdot 11 \cdot 13 \cdot 17 \cdot 23 \cdot 29$
HS	grupo de Higman-Sims	$2^9 \cdot 3^2 \cdot 5^3 \cdot 7 \cdot 11$
McL	grupo de McLaughlin	$2^7 \cdot 3^6 \cdot 5^3 \cdot 7 \cdot 11$
He	grupo de	$2^{10} \cdot 3^3 \cdot 5^2 \cdot 7^3 \cdot 17$

	Held	
Ru	grupo de Rudvalis	$2^{14} \cdot 3^3 \cdot 5^3 \cdot 7 \cdot 13 \cdot 29$
Suz	grupo de Suzuki	$2^{13} \cdot 3^7 \cdot 5^2 \cdot 7 \cdot 11 \cdot 13$
O'N	grupo de O'Nan	$2^9 \cdot 3^4 \cdot 5 \cdot 7^3 \cdot 11 \cdot 19 \cdot 31$
HN	grupo de Harada- Norton	$2^{14} \cdot 3^6 \cdot 5^6 \cdot 7 \cdot 11 \cdot 19$
Ly	grupo de Lyons	$2^8 \cdot 3^7 \cdot 5^6 \cdot 7 \cdot 11 \cdot 31 \cdot 37 \cdot 67$
Th	grupo de Thompson	$2^{15} \cdot 3^{10} \cdot 5^3 \cdot 7^2 \cdot 13 \cdot 19 \cdot 31$
B	Monstruo bebé	$2^{41} \cdot 3^{13} \cdot 5^6 \cdot 7^2 \cdot 11 \cdot 13 \cdot 17 \cdot 19 \cdot 23 \cdot 31 \cdot 47$
M	Monstruo	$2^{46} \cdot 3^{20} \cdot 5^9 \cdot 7^6 \cdot 11^2 \cdot 13^3 \cdot 17 \cdot 19 \cdot 23 \cdot 29 \cdot 31 \cdot 41 \cdot 47 \cdot 59 \cdot 71$

Números grandes especiales

Contenido:

Factoriales

Cubo de Rubik

Sudoku

El primo más grande conocido

Los números naturales no se terminan nunca. No existe el número más grande, porque siempre puedes hacerlo mayor sumándole 1.

Por lo tanto, la mayoría de los números naturales son demasiados grandes para escribirlos, sea cual sea el sistema de notación que se use.

Por supuesto, siempre se puede hacer el truco de definir el símbolo $\text{\textcircled{3}}$ para que sea el número grande en el que se esté pensando. Pero eso no es un sistema, solo un símbolo único.

Por suerte, raramente necesitamos números realmente grandes. Pero resultan fascinantes por sí solos. Y cada cierto tiempo, uno de ellos es importante en matemáticas.

$$26! = 403\,291\,461\,126\,605\,635\,584\,000\,000$$

§. Factoriales

El número de maneras de colocar las letras del alfabeto en orden.

Reorganizar cosas

¿De cuántas maneras diferentes puede reorganizarse una lista? Si la lista contiene dos símbolos, por ejemplo A y B, hay dos maneras:

AB BA

Si la lista contiene tres letras, A, B y C, hay seis maneras:

ABC ACB BAC BCA CAB CBA

¿Qué ocurre si contiene cuatro letras: A, B, C y D?

Puedes escribir todas las posibilidades, sistemáticamente, y la respuesta resulta ser 24. Hay un modo ingenioso de ver por qué esto es correcto. Piensa en dónde aparece D. Puede ser en la primera, en la segunda, en la tercera o en la cuarta posición. En cada caso, imagina eliminar la D. Entonces obtienes una lista con solo A, B y C en ella, la lista tiene que ser una de las seis posibilidades indicadas más arriba. Las seis pueden darse; tan solo introduce D en la lista en la posición correcta. De modo que podemos escribir todas las posibilidades como un conjunto de cuatro listas de seis disposiciones, así:

D en la primera posición:

DABC DACB DBAC DBCA DCAB DCBA

D en la segunda posición:

ADBC ADCB BDAC BDCA CDAB CDBA

D en la tercera posición:

ABDC ACDB BADC BCDA CADB CBDA

D en la cuarta posición:

ABCD ACBD BACD BCAD CABD CBAD

Todas estas disposiciones son diferentes, bien porque tienen la D en un lugar diferente, bien porque tienen la D en el mismo lugar por usar una colocación diferente de ABC. Además, cada colocación de ABCD se da en algún sitio: la posición de D nos dice a qué conjunto de seis hay que mirar y luego qué sucede cuando D es eliminada, nos dice qué colocación de ABC seleccionar.

Como tenemos cuatro conjuntos de colocaciones, cada uno que contiene seis de ellas, el número total de colocaciones es $4 \times 6 = 24$.

Podríamos haber averiguado las seis colocaciones de ABC de manera parecida, esta vez considerando donde aparece C, y luego eliminándola:

CAB CBA ACB BCA ABC BAC

De hecho, podemos incluso hacer lo mismo con solo las dos letras AB:

BA AB

Este modo de enumerar las colocaciones sugiere un patrón común. El número de maneras de organizar...

... 2 letras es $2 = 2 \times 1$.

... 3 letras es $6 = 3 \times 2 \times 1$.

... 4 letras es $24 = 4 \times 3 \times 2 \times 1$.

Entonces, ¿cuántas maneras hay de organizar las 5 letras ABCDE? El patrón sugiere que la respuesta debería ser:

$$5 \times 4 \times 3 \times 2 \times 1 = 120$$

y podemos demostrar que es correcto pensando en las cinco posiciones diferentes para E, cada una con 24 colocaciones posibles de ABCD si la eliminamos. Esto demuestra que el número que queremos es 5×24 , es decir, $5 \times 4 \times 3 \times 2 \times 1$.

Con el mismo razonamiento, el número de maneras diferentes de reordenar n letras es:

$$n \times (n - 1) \times (n - 2) \times \dots \times 3 \times 2 \times 1$$

que se llama «factorial de n » y se escribe como $n!$ Basta considerar todos los números de 1 a n y multiplicarlos.

Los primeros factoriales son:

$$1! = 1 \quad 6! = 720$$

$$2! = 2 \quad 7! = 5.040$$

$$3! = 6 \quad 8! = 40.320$$

$$4! = 24 \quad 9! = 362.880$$

$$5! = 120 \quad 10! = 3.628.800$$

Como puedes ver, los números se incrementan rápidamente, de hecho, cada vez más rápido.

El número de colocaciones de todo el alfabeto de 26 letras es, por lo tanto:

$$\begin{aligned} 26! &= 26 \times 25 \times 24 \times \dots \times 3 \times 2 \times 1 = \\ &= 403\,291\,461\,126\,605\,635\,584\,000\,000 \end{aligned}$$

El número de maneras diferentes de ordenar una baraja francesa de 52 cartas es:

$$\begin{aligned} 52! &= 80\,658\,175\,170\,943\,878\,571\,660\,636\,856\,403\,766\,975\,289\,505 \\ &\quad 440\,883\,277\,824\,000\,000\,000 \end{aligned}$$

La función gamma

En cierto sentido:

$$\left(-\frac{1}{2}\right)! = \sqrt{\pi}$$

Para que tenga sentido la afirmación introducimos la función gamma, que extiende la definición de factoriales a todos los números complejos mientras mantiene sus propiedades clave. La función gamma normalmente se define usando cálculo integral:

$$\Gamma(t) = \int_0^{\infty} x^{t-1} e^{-x} dx$$

La conexión con factoriales para un entero positivo n es:

$$\Gamma(n) = (n - 1)!$$

Usando una técnica conocida como «extensión analítica», podemos definir $\Gamma(z)$ para todos los números complejos z .

La función gamma $\Gamma(z)$ es infinita para valores enteros negativos de z y finita para todos los demás números complejos. Tiene aplicaciones

importantes en estadística y tiene la propiedad clave que define el factorial:

$$\Gamma(z + 1) = 2 \Gamma(z)$$

excepto que es para $(z - 1)!$, no para $z!$ Gauss sugirió remediar esto definiendo la función Pi: $\Pi(z) = \Gamma(z + 1)$, lo cual coincide con $n!$ cuando $z = n$, pero la notación de gamma es más común hoy en día.

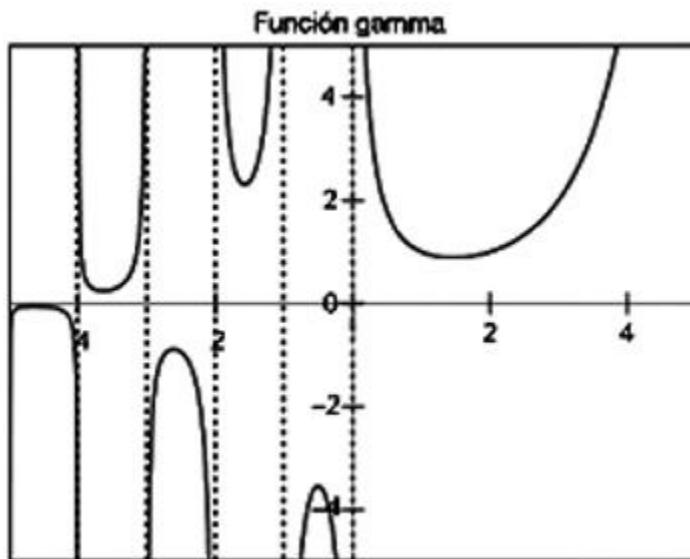


Figura 170. Gráfica de $\Gamma(x)$ para x real

La fórmula de duplicación para la función gamma afirma que:

$$\Gamma(z)\Gamma\left(z + \frac{1}{2}\right) = 2^{1-2z}\sqrt{\pi}\Gamma(2z)$$

Si hacemos $z = \frac{1}{2}$, obtenemos:

$$\Gamma\left(\frac{1}{2}\right) \Gamma(1) = 2^0 \sqrt{\pi} \Gamma(1)$$

De modo que:

$$\Gamma\left(\frac{1}{2}\right) = \sqrt{\pi}$$

Este es el sentido en que

$$\left(-\frac{1}{2}\right)! = \sqrt{\pi}$$

§. 43.252.003.274.489.856.000 Cubo de Rubik

En 1974, el profesor húngaro Ernő Rubik inventó un rompecabezas que consistía en cubos móviles. Se conoce como «cubo de Rubik» y en todo el mundo se han vendido alrededor de 350 millones de copias. Todavía recuerdo la Sociedad de Matemáticas de la Universidad de Warwick importando cajas de cubos desde Hungría, hasta que se hicieron tan populares que las compañías comerciales se ocuparon de fabricarlos. Este número enorme nos dice cuántas posiciones diferentes hay para un cubo de Rubik.

Geometría del cubo de Rubik

El rompecabezas consiste en un cubo, dividido en 27 cubos más pequeños, cada uno de un tercio del tamaño. Los *aficionados* los llaman «piezas». Cada cara del cubo es de un color determinado. Rubik tuvo una idea ingeniosa cuando diseñó un mecanismo que permitía que cada cara del cubo rotase. Rotaciones repetidas mezclan los colores de las piezas. El objetivo es obtener las piezas de vuelta a su posición original, de modo que de nuevo cada cara del cubo tenga el mismo color.

El cubito del centro no puede verse y de hecho es reemplazado por el ingenioso mecanismo de Rubik. Las piezas del centro de las caras giran, pero no se mueven a una cara nueva, así que sus colores no cambian. Por lo tanto, a partir de ahora, asumimos que estas seis *caras* no se mueven, excepto por girar en su misma posición. Es decir, si colocamos el cubo de Rubik entero con una orientación diferente, sin realmente girar ninguna cara, se considera que no tienen ningún efecto significativo.



Figura 171. Cubo de Rubik.

Las piezas que pueden moverse son de dos tipos: 8 *piezas de esquina* y 12 *piezas de arista*, que están en el medio de una arista del cubo. Si mezclas los colores de estas piezas de esquina y arista de todos los modos posibles, por ejemplo, quitando todas las pegatinas de colores y reemplazándolas con una colocación diferente, el número de posibles modos de organizar los colores es:

519 024 039 293 878 272 000

Sin embargo, eso no está permitido en el juego de Rubik; todo lo que puedes hacer es rotar las caras del cubo. Así que la pregunta que surge es: ¿cuántas de estas maneras de organizar pueden obtenerse usando una

serie de rotaciones? En principio, podría ser una fracción minúscula de ellas, pero los matemáticos han probado que exactamente un doceavo de las posiciones anteriores puede obtenerse por series de movimientos permitidos, como describo brevemente más adelante. Por lo tanto, el número de maneras de organizar colores permitidas en el cubo de Rubik es:

$$43\,252\,003\,274\,489\,856\,000$$

Si cada uno de los 7.000 millones de personas de toda la raza humana pudiesen conseguir una de estas colocaciones cada segundo, se tardaría alrededor de 200 años en recorrerlas todas.

Cómo calcular estos números

Las 8 piezas de esquina pueden colocarse de $8!$ maneras. Observa que:

$$8! = 8 \times 7 \times 6 \times 5 \times 4 \times 3 \times 2 \times 1$$

Este número aparece porque hay 8 opciones para el primer cubito, que pueden combinarse con cualquiera de las 7 opciones que quedan para el segundo, que puede combinarse con cualquiera de las 6 opciones que restan para el tercero y así sucesivamente [véase $26!$]. Cada cubito de esquina puede rotarse independientemente en 3 orientaciones diferentes.

Así que hay 3^8 maneras de escoger las orientaciones. En total, hay $3^8 \times 8!$ modos de ordenar las piezas de esquina.

De manera similar, las 12 piezas de arista pueden organizarse de 12! maneras, donde:

$$12! = 12 \times 11 \times 10 \times 9 \times 8 \times 7 \times 6 \times 5 \times 4 \times 3 \times 2 \times 1$$

Cada uno puede colocarse con 2 orientaciones, así que pueden escogerse en 2^{12} maneras. En total, hay $2^{12} \times 12!$ maneras de colocar las piezas de las aristas.

El número de formas posibles de combinar estas colocaciones se obtiene multiplicando los dos números, lo que da $3^8 \times 8! \times 2^{12} \times 12!$ Y al operar obtenemos 519.024.039.293.878.272.000.

Como he señalado, la mayoría de estas colocaciones no pueden obtenerse por una serie de rotaciones del cubo. Cada rotación afecta a varias piezas de una vez, y ciertas características de conjunto entero de piezas pueden cambiar. Estas características se llaman «invariantes» y en este caso hay tres:

Paridad en las piezas. Hay permutaciones de dos tipos: pares e impares [véase 2]. Una permutación par intercambia el orden de un número par de pares de objetos. Si se combinan dos permutaciones pares realizándolas por turnos, la permutación resultante es par. Ahora, cada

rotación del cubo de Rubik es una permutación par de las piezas. Por lo tanto, cualquier combinación de rotaciones es también una permutación par. Esta condición reduce a la mitad el número de posibles colocaciones.

Paridad en las caras. Cada rotación es una permutación par de las aristas, y lo mismo ocurre para series de rotaciones. Esta condición, de nuevo, reduce a la mitad el número de colocaciones posibles.}

Trialidad en las esquinas. Numera las 24 caras de las esquinas con los enteros 0, 1, 2, de modo que los números vayan en el sentido de las agujas del reloj en el orden 0, 1, 2 en cada esquina. Haz esto de forma que los números en dos caras opuestas estén etiquetados con 0, como en la imagen de la derecha en la Figura. La suma de todos estos números, considerada en módulo 3, es decir, considerando solo el resto de la división entre 3, no se ve alterada por ninguna rotación del cubo. Esta condición divide el número de posibles colocaciones entre 3.

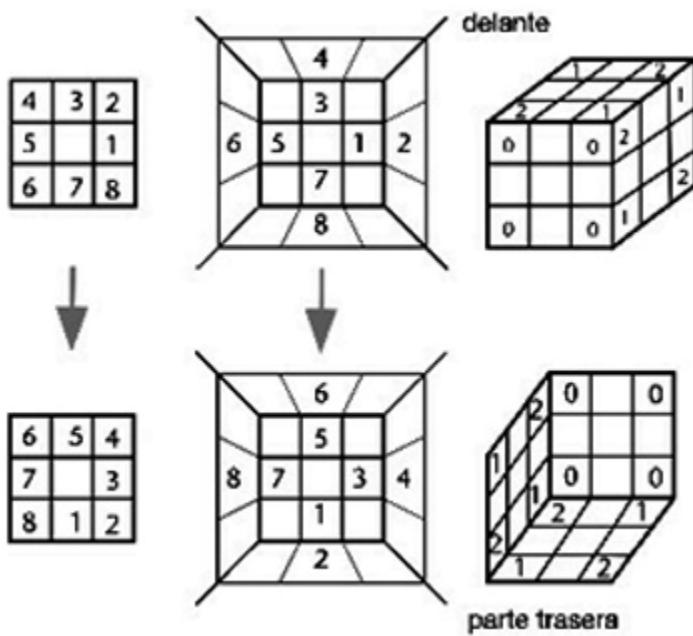


Figura 172. Invariantes del grupo de Rubik. Izquierda: efecto de un giro de un cuarto en sentido de las agujas del reloj en las piezas. Centro: etiquetas en las piezas que son arista. Derechas: etiquetas en las piezas que son esquina.

Teniendo en cuenta las tres condiciones, el número de posibles modos de organizar tiene que dividirse entre $2 \times 2 \times 3 = 12$. Es decir, el número de modos de organizar que puede producirse por una serie de rotaciones es:

$$3^8 \times 8! \times 2^{12} \times \frac{11!}{12} = 23\,252\,003\,274\,489\,856\,000$$

Las técnicas matemáticas usadas para analizar el cubo de Rubik también llevan a maneras sistemáticas de resolverlo. Sin embargo, estos métodos

son demasiado complicados para describirlos aquí, y comprender por qué funcionan es un proceso largo y a veces técnico.

Número de Dios

Definimos «movimiento» en el cubo de Rubik como un giro de un número cualquiera de ángulos rectos de una única cara. La cantidad más pequeña de movimientos que resolverán el rompecabezas, no importa cuál sea la posición inicial, se llama «número de Dios», probablemente porque daba la impresión de que la respuesta estaría más allá de las habilidades de resolución propias de meros mortales. Sin embargo, esa previsión resultó ser demasiado pesimista. En 2010, Tomas Rokicki, Herbert Kociemba, Morley Davidson y John Dethridge aplicaron un poco de ingenio matemático más la fuerza bruta de un ordenador para probar que el número de Dios es 20. El cálculo se ejecutó simultáneamente en un gran número de ordenadores y habría durado 350 años usando un único ordenador.

§. 6.670.903.752.021.072.936.960 Sudoku

Aunque el sudoku se propagó en el mundo en 2005, sus antecedentes se remontan mucho más atrás. Consiste en colocar las cifras del 1 al 9 en un cuadrado 9×9 que está dividido en nueve subcuadrados de 3×3 . Cada fila, columna o subcuadrado debe contener una de cada una de las cifras.

Hay algunas cifras que proporciona el autor del juego. Este es el número de las distintas cuadrículas de sudoku que hay. No se van a agotar.

5			7					
6		1	9	5				
9	8				6			
8			6					3
4		8	3					1
7			2					6
6				2	8			
	4	1	9					5
		8			7	9		

5	3	4	6	7	8	9	1	2
6	7	2	1	9	5	3	4	8
1	9	8	3	4	2	5	6	7
8	5	9	7	6	1	4	2	3
4	2	6	8	5	3	7	9	1
7	1	3	9	2	4	8	5	6
9	6	1	5	3	7	2	8	4
2	8	7	4	1	9	6	3	5
3	4	5	2	8	6	1	7	3

Figura 173. Izquierda: una cuadrícula de sudoku. Derecha: su solución.

De los cuadrados latinos al sudoku

A menudo se atribuye el origen de la historia del sudoku al trabajo de Euler sobre cuadrados latinos [véase 10]. Una cuadrícula completa de sudoku es un tipo especial de cuadrado latino: los subcuadrados 3×3 introducen limitaciones extra. Un rompecabezas similar apareció en 1892 cuando el periódico francés *Le Siècle* pidió a sus lectores completar un cuadrado mágico del que se habían eliminado algunos números. Poco después, *La France* usó cuadrados mágicos que contenían solo las cifras del 1 al 9. En las soluciones, bloques de 3×3 también contenían las nueve cifras, pero este requerimiento no se hizo explícito.

La forma moderna del sudoku probablemente debería atribuirse a Howard Garns, quien se cree que ha inventado una serie de

rompecabezas publicados en 1979 por Dell Magazines como «el lugar del número». En 1986, Nikoli, una compañía japonesa, publicó sudokus en Japón. Al principio, el nombre era *sūji wa dokushin ni kagiru* («las cifras están limitadas a una aparición»), pero rápidamente se convirtió en *sū doku*. *The Times* empezó a publicar sudokus en Reino Unido en 2004, y en 2005 se hicieron populares mundialmente.

El número enorme:

6 670 903 752 021 072 936 960

que ilustra este capítulo es el número de diferentes cuadrículas de sudoku. El número de cuadrados latinos de 9×9 es alrededor de un millón de veces más grande:

5 524 751 496 156 892 842 531 225 600

El número de cuadrículas de sudoku fue publicado en el grupo de noticias de USENET *rec.puzzle* sin prueba en 2003. En 2005, Bertram Felgenhauer y Frazer Jarvis explicaron los detalles con ayuda de un ordenador, basándose en algunas afirmaciones plausibles pero que están sin probar. El método supone comprender las simetrías del sudoku. Cada cuadrícula completa concreta tiene su propio grupo de simetría [véase 168], que consiste en transformaciones (intercambios de filas y

columnas, cambios de notación) que deja la cuadrícula sin cambios. Pero la estructura clave es el grupo de simetría del conjunto de todas las cuadrículas posibles: modos de transformar cualquier cuadrícula en otra (quizá la misma cuadrícula pero no necesariamente).

Las transformaciones de simetría a las que nos referimos son de varios tipos. Las más obvias son las $9!$ permutaciones de nueve cifras. Sistématicamente permutar las cifras de una cuadrícula de sudoku obviamente produce otra cuadrícula de sudoku. Pero también se puede intercambiar filas, siempre que se conserve la estructura de bloques de tres. Se puede hacer lo mismo con las columnas, así como reflejar una cuadrícula dada respecto de su diagonal principal. El grupo de simetría tiene orden $2 \times 6^4 \times 6^4 = 3.359.232$. Al contar las cuadrículas, hay que tener en cuenta estas simetrías. La prueba es complicada, de ahí el uso de ordenadores. Los vacíos en la prueba original ya se han cubierto. Para detalles y más información véase: [*Mathematics of Sudoku*](#).

Como las variaciones simétricas de una cuadrícula dada son esencialmente la misma cuadrícula disfrazada, también podemos preguntar: ¿cuántas cuadrículas *distintas* hay si las simétricamente relacionadas se consideran equivalentes? En 2006, Jarvis y Ed Russell calcularon este número: 5.472.730.538. No es el número inicial dividido entre 3.359.232 porque algunas cuadrículas tienen simetrías propias.

Como para el cubo de Rubik, las técnicas matemáticas usadas para analizar el sudoku también proporcionan modos sistemáticos de

resolverlo. Sin embargo, los métodos son demasiado complicados para describirlos aquí y pueden resumirse mejor como un ensayo y error sistemático.

§. $2^{57.885.161} - 1$ (un total de 17.425.170 dígitos) El primo más grande conocido

¿Cuál es el primo más grande? Ya desde 300 a. C. o en torno a esa fecha, Euclides probó que ese número no existe. «Los números primos son más que cualquier multitud asignada.» Es decir, existen infinidad de primos. Los ordenadores pueden extender la lista de primos considerablemente, la principal razón para detenerse es que se quedan sin memoria o la impresión se hace ridículamente grande. Este es el que posee el récord en la actualidad.

Los números de Mersenne

Ha surgido una industria menor en torno a la búsqueda del primo más grande conocido. Esta búsqueda es sobre todo interesante como un ejercicio para batir récords y para probar nuevos ordenadores. En abril de 2014 el número primo más grande conocido era $2^{57.885.161} - 1$, un número tan enorme que tiene 17.425.170 cifras.

Los números de la forma:

$$M_n = 2^n - 1$$

se llaman «números de Mersenne» por el monje francés Marin Mersenne. Si estás decidido a batir récords para primos grandes, los números de Mersenne son el modo de proceder, porque tienen características especiales que nos permiten decidir si son primos, incluso cuando se hacen demasiado grandes para los métodos más generales.

Con álgebra sencilla se prueba que si $2n - 1$ es primo, entonces n tiene que ser primo. Los primeros matemáticos debieron de pensar que el inverso también es cierto: M_n es primo si n es primo. Sin embargo, Hudalricus Regius, en 1536, se dio cuenta de que $M_{11} = 2.047$ no es primo, aunque 11 sí lo es.

De hecho,

$$2^{11} - 1 = 2.047 = 23 \times 89$$

Pietro Cataldi demostró que M_{17} y M_{19} son primos, una tarea fácil con los ordenadores actuales, pero no en su día, ya que todos los cálculos tenían que hacerse a mano. También afirmó que M_n es primo para $n = 23, 29, 31$ y 37 . Sin embargo:

$$M_{23} = 8.388.607 = 47 \times 178.481$$

$$M_{29} = 536.870.911 = 233 \times 1.103 \times 2.089$$

$$M_{37} = 137.438.953.471 = 223 \times 616.318.177$$

Por lo tanto, estos tres números de Mersenne son compuestos. Fermat descubrió los factores de M_{23} y M_{37} en 1640 y Euler encontró los factores de M_{29} en 1738. Más tarde, Euler probó que Cataldi tenía razón en lo referente a que M_{31} era primo.

En 1644, Mersenne, en el prefacio de su libro *Cogitata Physica-Mathematica*, afirmó que M_n es primo para $n = 2, 3, 5, 7, 13, 17, 19, 31, 67, 127$ y 257 . Esta lista tuvo intrigados a los matemáticos durante más de doscientos años. ¿Cómo obtuvo los resultados de números tan grandes? Finalmente quedó claro: había hecho solo una suposición fundamentada. Su lista contenía varios errores. En 1876, Lucas probó que Mersenne estaba en lo correcto en lo referente a:

$$M_{127} = 170\ 141\ 183\ 460\ 469\ 231\ 731\ 687\ 303\ 715\ 884\ 105\ 727$$

usando un ingenioso test para la primalidad de M_n que había inventado. Derrick Lehmer ideó una ligera mejora del test de Lucas en 1930. Define una secuencia de números S_n como $S_2 = 4, S_3 = 14, S_4 = 194 \dots$ con $S_{n+1} = S_n^2 - 2$. La prueba de Lucas-Lehmer afirma que M_p es primo si y solo si M_p se divide entre S_p . Es esta prueba la que arroja luz sobre la primalidad, o no, de los números de Mersenne.

Finalmente se reveló que Mersenne estaba equivocado en varios casos: dos en su lista son compuestos ($n = 67$ y 257), y omitió $n = 61, 89$ y 107 ,

que dan números primos. A pesar de eso, considerando la dificultad de los cálculos a mano, hizo un buen trabajo.

En 1883, Ivan Mikheevich Pervushin probó que M_{61} es primo, un caso que a Mersenne se le escapó. R. E. Powers luego demostró que a Mersenne también se le escaparon M_{89} y M_{107} , ambos son primos. En 1947, la condición de M_n había sido comprobada para n hasta 257. Los primos de Mersenne en ese rango se dan para $n = 2, 3, 5, 7, 13, 17, 19, 31, 61, 89, 107$ y 127. La lista actual de primos de Mersenne es:

Tabla 15

<i>n</i>	Año	Lo descubrió...
2	—	(en la Antigüedad)
3	—	(en la Antigüedad)
5	—	(en la Antigüedad)
7	—	(en la Antigüedad)
13	1456	anónimo
17	1588	Cataldi
19	1588	Cataldi
31	1772	Euler
61	1883	Pervushin
89	1911	Powers
107	1914	Powers
127	1876	Lucas

521	1952	Robinson
607	1952	Robinson
1.279	1952	Robinson
2.203	1952	Robinson
2.281	1952	Robinson
3.217	1957	Riesel
4.253	1961	Hurwitz
4.423	1961	Hurwitz
9.689	1963	Gillies
9.941	1963	Gillies
11.213	1963	Gillies
19.937	1971	Tuckerman
21.701	1978	Noll y Nickel
23.209	1979	Noll
44.497	1979	Nelson y Slowinski
86.243	1982	Slowinski
110.503	1988	Colquitt y Welsh
132.049	1983	Slowinski
216.091	1985	Slowinski
756.839	1992	Slowinski, Gage <i>et al.</i>
859.433	1994	Slowinski y Gage
1.257.787	1996	Slowinski y Gage
1.398.269	1996	Armengaud, Woltman <i>et al.</i>

2.976.221	1997	Spence, Woltman <i>et al.</i>
3.021.377	1998	Clarkson, Woltman, Kurowski <i>et al.</i>
6.972.593	1999	Hajratwala, Woltman, Kurowski <i>et al.</i>
13.466.917	2001	Cameron, Woltman, Kurowski <i>et al.</i>
20.996.011	2003	Shafer, Woltman, Kurowski <i>et al.</i>
24.036.583	2004	Findley, Woltman, Kurowski <i>et al.</i>
25.964.951	2005	Nowak, Woltman, Kurowski <i>et al.</i>
30.402.457	2005	Cooper, Boone, Woltman, Kurowski <i>et al.</i>
32.582.657	2006	Cooper, Boone, Woltman, Kurowski <i>et al.</i>
37.156.667	2008	Elvenich, Woltman, Kurowski <i>et al.</i>
42.643.801	2009	Strindmo, Woltman, Kurowski <i>et al.</i>
43.112.609	2008	Smith, Woltman, Kurowski <i>et al.</i>
57.885.161	2013	Cooper, Woltman, Kurowski <i>et al.</i>

La búsqueda para primos realmente grandes se ha centrado sobre todo en los números de Mersenne por varias razones. En la notación binaria

usada por los ordenadores, $2n$ es 1 seguido por una cadena de n ceros, y $2n - 1$ es una cadena de n unos. Esto acelera algo la aritmética. La prueba de Lucas-Lehmer es mucho más eficiente que los métodos generales para probar la primalidad, así que resulta práctica para números mucho más grandes. Esta prueba nos lleva a los 47 primos de Mersenne de la tabla. Se pueden encontrar actualizaciones o más información en: [mersenne](#).

Números infinitos

Contenido:

§. Alef cero: el infinito más pequeño

§. Cardinal del continuo

Como ya he señalado antes, los matemáticos nunca se han detenido ante algo solo porque sea imposible. Si es lo suficientemente interesante, encuentran maneras de *hacerlo* posible.

No existe el mayor número natural. Los números naturales no se acaban nunca. Todo el mundo lo sabe.

Pero cuando Georg Cantor decidió preguntar *lo grande* que era ese concepto de «no acabarse nunca», elaboró un método innovador para que tuviesen sentido números infinitamente grandes. Una consecuencia es que algunos infinitos son más grandes que otros.

Muchos de sus contemporáneos pensaron que estaba loco. Pero había un método en la locura de Cantor y sus nuevos números transfinitos resultaron ser apropiados e importantes.

Tan solo había que acostumbrarse a ellos. Lo cual no resultó fácil.

§. \aleph_0 Álef cero: el infinito más pequeño

Los matemáticos hacen uso libre y amplio de la palabra «infinito». De manera informal, algo es infinito si no puedes contar lo grande que es

usando los números naturales ordinarios, o medir su longitud usando números reales. En ausencia de un número convencional, usamos «infinito» como un parámetro de sustitución. Infinito no es un número en el sentido habitual. Es, por así decirlo, cuál sería el mayor número posible, si es que esa frase tiene sentido lógico. Pero a menos que seas muy, pero muy cuidadoso con lo que quieras decir, no lo es.

Cantor encontró un modo de convertir infinito en un número genuino contando conjuntos infinitos. Aplicando esta idea al conjunto de todos los números naturales definió un número infinito que llamó \aleph_0 (álef cero). Es mayor que cualquier número entero. De modo que es infinito, ¿verdad? Bien, en cierto modo. Es, sin duda, un infinito. El infinito más pequeño, de hecho. Hay otros, y son más grandes.

Infinito

Cuando los niños aprenden a contar y empiezan a sentirse cómodos con grandes números como mil o un millón, con frecuencia se preguntan cuál es el mayor número posible. Quizá crean que es algo como:

1.000.000.000.000.000

Pero entonces se dan cuenta de que pueden hacer un número mayor poniendo otro 0 al final, o sumando 1 para obtener:

1.000.000.000.000.001

Ningún número natural en concreto puede ser el mayor, porque sumando 1 se obtiene cualquier número mayor. Los números naturales no se acaban nunca. Si empiezas a contar y no te detienes, no alcanzas el mayor número posible y paras, porque no existe tal cosa. Hay infinidad de números.

Durante cientos de años, los matemáticos fueron muy cautelosos en lo que al infinito se refiere. Cuando Euclides probó que existen infinidad de números primos, no lo expresó así. Dijo que «los primos son más que cualquier multitud dada». Es decir, no hay un primo que sea el mayor.

Dejando aparte la prudencia, lo obvio es seguir los precedentes históricos e introducir un nuevo tipo de número, mayor que cualquier número entero. Llámalo «infinito» y dale un símbolo, el habitual es ∞ , como un 8 tumbado. Pero el infinito puede causar problemas, porque a veces su comportamiento es paradójico.

¿Es con toda seguridad ∞ el mayor número posible? Bien, por definición es mayor que cualquier número entero, pero las cosas no son tan claras cuando nos proponemos hacer aritmética con nuestro número nuevo. El problema obvio es: ¿cuánto es $\infty + 1$? Si es mayor que ∞ , entonces ∞ no es el mayor número posible. Pero si es lo mismo que ∞ , entonces $\infty = \infty + 1$. Restando ∞ , se obtiene $0 = 1$. ¿Y qué ocurre con $\infty + \infty$? Si es mayor

que infinito, tenemos el mismo problema. Pero si es lo mismo, entonces $\infty + \infty = \infty$. Restando ∞ , se obtiene $\infty = 0$.

La experiencia con extensiones del sistema numérico previas muestra que cada vez que introduces nuevos tipos de números, quizá tengas que sacrificar algunas de las reglas de aritmética y álgebra. En este caso, parece que tenemos que prohibir la resta si ∞ está involucrado. Por razones similares, no podemos asumir que dividir por ∞ funcione del modo que normalmente esperaríamos. Pero es un número bastante débil si no puede usarse para restar o para dividir.

Ese podría haber sido el final de la historia, pero los matemáticos lo encontraron extremadamente útil para trabajar con infinitos procesos. Podrían descubrirse resultados útiles dividiendo formas en piezas que se hacen cada vez más pequeñas sin que esto tenga un fin. La razón de por qué el mismo número π se da tanto en la longitud de la circunferencia como en el área de un círculo es un ejemplo [véase π]. Arquímedes hizo buen uso de esta idea alrededor del año 200 a. C. en su trabajo sobre círculos, esferas y cilindros. Encontró una prueba complicada, pero rigurosa desde el punto de vista lógico, de que el método da las respuestas correctas.

A partir del siglo XVII, la necesidad de una teoría apropiada de este tipo de proceso se hizo apremiante, especialmente para series infinitas, en las cuales números y funciones importantes podían aproximarse a cualquier precisión deseada sumando cada vez más números que van decreciendo.

Por ejemplo, en $[\pi]$ vimos que donde la suma de los inversos de los cuadrados es expresada en términos de π . Esta afirmación es cierta solo cuando la serie continúa infinitamente. Si nos detenemos, la serie da un número racional, que es una aproximación a π , pero no puede ser igual a él ya que π es irracional. En cualquier caso, donde sea que nos detengamos, sumar el siguiente término hace la suma más grande.

$$\frac{\pi^2}{6} = 1 + \frac{1}{4} + \frac{1}{9} + \frac{1}{16} + \frac{1}{25} + \frac{1}{36} + \dots$$

La dificultad con sumas infinitas como esta es que a veces no parecen tener sentido. El caso clásico es:

$$1 - 1 + 1 - 1 + 1 - 1 + 1 - 1 + \dots$$

Si esta suma se escribe como:

$$(1 - 1) + (1 - 1) + (1 - 1) + (1 - 1) + \dots$$

Se convierte en:

$$0 + 0 + 0 + 0 + \dots$$

que claramente es 0. Pero si está escrita de forma diferente, asumiendo que las leyes habituales del álgebra se aplican, se convierte en:

$$1 + (-1 + 1) + (-1 + 1) + (-1 + 1) + \dots$$

Esto es:

$$1 + 0 + 0 + 0 + \dots$$

lo cual, igual de claro, debería ser 1.

El problema es que esta serie no converge, es decir, no se estabiliza hacia un valor específico acercándose más y más a él a medida que se añaden más términos. En su lugar, el valor cambia repetidamente entre 1 y 0.

$$1 = 1$$

$$0 = 1 - 1$$

$$1 = 1 - 1 + 1$$

$$0 = 1 - 1 + 1 - 1$$

y así sucesivamente. Esta no es la única fuente de potenciales problemas, pero indica el camino hacia una teoría lógica de series infinitas. Las que tienen sentido son las que convergen, lo cual quiere decir que, a medida que se añaden más y más términos, la suma tiende hacia algún número

específico. La serie de los inversos de los cuadrados es convergente y converge exactamente a $\pi^2/6$.

Los filósofos distinguen entre *infinito potencial* e *infinito real*. Algo es potencialmente infinito si en principio puede continuarse indefinidamente, como sumar más y más términos a una serie. Cada individuo suma su finito, pero el proceso que genera estas sumas no tiene un punto fijo en el que se detiene. El infinito real se da cuando todo un proceso o sistema infinito se trata como un único objeto. Los matemáticos han encontrado un modo razonable de interpretar el infinito potencial de series infinitas. Usan varios procesos infinitos potencialmente diferentes, pero en todos ellos el símbolo se interpretaba como «continúa esto lo suficiente y te acercarás tanto como quieras a la respuesta correcta».

El infinito real era un tema diferente, del que intentaron mantenerse alejados.

¿Qué es un número infinito?

Ya hice esta pregunta para números naturales finitos ordinarios: 1, 2, 3,... Llegué hasta la idea de Frege, la clase de todas las clases en correspondencia con una clase dada, y me detuve, con una insinuación que quizá sea un problema.

Lo es.

La definición es muy elegante una vez te acostumbras a ese tipo de pensamiento y tiene la virtud de definir un objeto único. Pero la tinta de la obra maestra de Frege apenas se había secado cuando Russell presentó una objeción. No a la idea subyacente, sobre la cual había estado reflexionando él mismo, sino al tipo de clase que Frege tenía que usar. La clase de todas las clases en correspondencia con nuestra clase de tazas es *enorme*. Considera tres objetos, agrúpalos en una clase y el resultado debe ser un miembro de la clase de clases de Frege. Por ejemplo, la clase cuyos miembros son la Torre Eiffel, una margarita concreta de un prado del condado de Cambridge y el humor de Oscar Wilde tiene que incluirse.

Paradoja de Russell

¿Tienen sentido las clases de gran amplitud? Russell se dio cuenta de que, en general, no lo tienen. Su ejemplo era una versión de la famosa paradoja del barbero. En un pueblo hay un barbero que afeita precisamente a quienes no se afeitan a sí mismos. ¿Quién afeita al barbero? Con la condición de que todos en el pueblo son afeitados por alguien, no puede existir ese barbero. Si el barbero no se afeita a sí mismo, entonces por definición debe afeitarse a sí mismo. Si se afeita a sí mismo, viola la condición de que solo la gente a la que él afeita son quienes no se afeitan a sí mismos.

Aquí asumimos que el barbero es un caballero para evitar problemas con el género. Sin embargo, señoras, somos conscientes de que en la actualidad muchas de ustedes se afeitan, aunque normalmente no la barba. De modo que una mujer barbero no es una resolución de la paradoja tan satisfactoria como se pudiera pensar.

Russell encontró una clase, bastante parecida a las que Frege quería usar, que se comporta justo como el barbero: *la clase de todas las clases que no se contienen a sí mismas*. ¿Se contiene esta clase a sí misma o no? Ambas posibilidades se descartan. Si *se contiene* a sí misma, entonces hace lo que todos sus miembros hacen: *no se contiene* a sí misma. Pero si *no se contiene* a sí misma, satisface la condición para pertenecer a la clase, así que *sí se contiene* a sí misma.

Aunque esta paradoja de Russell no prueba que la definición de Frege de un número es contradictoria desde un punto de vista lógico, no significa que simplemente no puedas asumir, sin prueba, que cualquier condición verdadero/falso define una clase, en concreto, aquellos objetos para los que la condición es cierta. Y eso dejó la lógica de la aproximación de Frege para el arrastre. Más tarde, Russell y su colaborador, Alfred North Whitehead, intentaron cubrir el hueco desarrollando una teoría elaborada sobre clases que pueden definirse razonablemente en un marco matemático. El resultado fue un trabajo de tres volúmenes, *Principia Mathematica* («Principios matemáticos»), un homenaje deliberado a Isaac Newton), el cual expone todas las matemáticas desde las propiedades

lógicas de clases. Requirió varios cientos de páginas definir el número 1 y unas cuantas más definir + y probar que $1 + 1 = 2$. Después de eso, el progreso se hace mucho más rápido.

Álef-0: el número infinito más pequeño

Ya pocos matemáticos usan el enfoque de Russell-Whitehead para clases, porque enfoques más sencillos funcionan mejor. Una figura clave en la formulación actual de los fundamentos lógicos de las matemáticas es Cantor. Empezó como Frege, intentando entender los fundamentos lógicos de los números naturales. Pero su investigación le llevó en una nueva dirección: asignar números a conjuntos *infinitos*. Pasaron a ser conocidos como «cardinales transfinitos». Su característica más notable es que hay más de uno.

Cantor también trabajó con colecciones de objetos, lo que él llamó «conjuntos» (en alemán) en vez de clases, porque los objetos en ellos estaban más restringidos que aquellos que Frege había permitido (es decir, todo). Como Frege, empezó a partir de la idea intuitiva de que dos conjuntos tienen el mismo número de miembros si y solo si puede hacerse una correspondencia. A diferencia de Frege, hizo esto para conjuntos infinitos también. De hecho, quizás empezase con la idea de que esto era como definir infinito. ¿Estás seguro de que cualquier conjunto infinito puede ponerse en correspondencia con cualquier otro?

Si es así, habría exactamente un número infinito y sería mayor que cualquier número finito, fin de la historia.

Tal y como resultó, fue solo el principio.

El conjunto infinito básico es el conjunto de todos los números naturales.

Como estos se usan para contar cosas, Cantor definió un conjunto como contable si sus miembros podían ponerse en correspondencia con el conjunto de los números naturales. Observa que, considerando este conjunto completo, Cantor estaba hablando sobre un infinito real, no potencial. El conjunto de todos los números naturales obviamente es contable; basta hacer que cada número se corresponda consigo mismo.

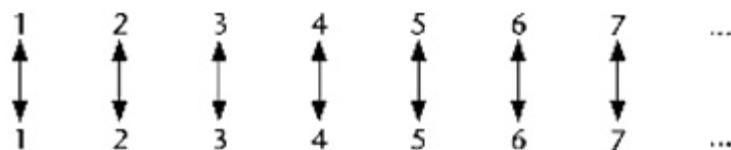


Figura 174

¿Hay otros? Sí, y son raros. ¿Qué os parece?

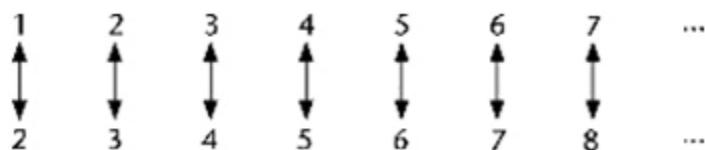


Figura 175

Elimina el número 1 del conjunto de los números naturales y el número de miembros en el conjunto no decrece en 1, se mantiene exactamente igual.

Convenimos, si paramos en algún número finito, acabar con un número suelto en el final de la parte derecha, pero cuando usamos *todos* los números enteros, no hay un último en la parte derecha. Cada número n se empareja con $n + 1$, y esto es una correspondencia entre el conjunto de todos los números naturales y el mismo conjunto eliminando 1. La parte es del mismo tamaño que el todo.

Cantor llamó a sus números infinitos «cardinales», porque ese es un nombre sofisticado para los números que usamos para contar en la aritmética ordinaria. Para enfatizar, los llamamos «cardinales transfinitos» o «cardinales infinitos» sin más. Para el cardinal de los números naturales, escogió un símbolo inusual, la primera letra del alfabeto hebreo, \aleph (álef), porque la idea completa era inusual. Agregó el subíndice 0, para obtener \aleph_0 , por razones que explicaré en el próximo capítulo.

Si todo conjunto infinito puede emparejarse con los números que usamos para contar, \aleph_0 sería tan solo un símbolo sofisticado para «infinito». Y de primera entrada, parecía como si este pudiese ser el caso. Por ejemplo, hay muchos números racionales que no son enteros, así que parece plausible que el cardinal para los racionales podría resultar ser mayor que \aleph_0 . Sin embargo, Cantor probó que se puede emparejar los

racionales a los números naturales. De modo que su cardinal es *también* \aleph_0 .

Para ver aproximadamente cómo funciona, consideremos solo los números racionales entre 0 y 1. El truco es listarlos en el orden correcto, que *no* es su orden numérico. En su lugar, los ordenamos por el tamaño de su denominador, el número en la parte inferior de la fracción. Para cada denominador específico, los ordenamos entonces según su numerador, el número de la parte superior. La lista queda así:

$$\frac{1}{2}, \frac{1}{3}, \frac{2}{3}, \frac{1}{4}, \frac{3}{4}, \frac{1}{5}, \frac{2}{5}, \frac{3}{5}, \frac{5}{5}, \frac{1}{6}, \frac{5}{6} \dots$$

donde, por ejemplo, falta $\frac{2}{4}$ porque es igual a $\frac{1}{2}$. Ahora podemos emparejar estos racionales con los números naturales considerándolos en este orden concreto. Todo racional entre 0 y 1 aparece en algún lugar de la lista, de manera que no dejamos fuera ninguno.

Hasta aquí, la teoría de Cantor nos ha llevado a un solo cardinal infinito, \aleph_0 . Pero no es tan sencillo, como se demuestra en el próximo capítulo.

§. **C** Cardinal del continuo

La idea más brillante de Cantor es que algunos infinitos son más grandes que otros. Descubrió algo notable sobre el «continuo», un nombre sofisticado para el sistema numérico real. Su cardinal, que denotamos con **C**, es mayor que \aleph_0 . No solo quiere decir que algunos números

reales no son números naturales, ya que algunos números racionales (la mayoría, de hecho) no son números naturales, pero los enteros y los racionales tienen el *mismo* cardinal \aleph_0 . Para los cardinales infinitos, el todo no necesita ser mayor que la parte, como advirtió Galileo. Quiere decir que no puedes emparejar todos los números reales uno a uno con todos los números naturales, no importa cómo los mezcles.

Como \mathfrak{c} es mayor que \aleph_0 , Cantor se preguntó si había algún cardinal infinito entre ellos. Su hipótesis del continuo afirma que no hay ninguno. No pudo probar ni refutar este argumento. Entre otros, Kurt Gödel en 1940 y Paul Cohen en 1963 probaron que la respuesta es «sí y no». Depende de cómo establezcas los fundamentos lógicos de las matemáticas.

Infinito no numerable

Recuerda que un número real puede escribirse como un decimal, el cual puede bien acabarse después de una cantidad finita de cifras, como 1,44, o bien seguir infinitamente, como π . Cantor se dio cuenta (aunque no en estos términos) de que el infinito de los números reales es definitivamente más grande que el de los números naturales, \aleph_0 .

La idea es aparentemente simple. Para demostrarlo, hace una prueba que concluye en contradicción. Supongamos, con la esperanza de llegar a una contradicción lógica, que los números reales pueden emparejarse con los

números naturales. Entonces hay una lista de decimales infinitos de la forma:

$$1 \leftrightarrow a_0, \mathbf{a}_1 a_2 a_3 a_4 a_5 \dots$$

$$2 \leftrightarrow b_0, b_1 \mathbf{b}_2 b_3 b_4 b_5 \dots$$

$$3 \leftrightarrow c_0, c_1 c_2 \mathbf{c}_3 c_4 c_5 \dots$$

$$4 \leftrightarrow d_0, d_1 d_2 d_3 d_4 d_5 \dots$$

$$5 \leftrightarrow e_0, e_1 e_2 e_3 e_4 \mathbf{e}_5 \dots$$

tal que todo decimal infinito posible aparece en algún lugar en la parte de la derecha. De momento, ignora las negritas, enseguida me referiré a eso. La idea genial de Cantor es construir un decimal infinito que posiblemente no pueda aparecer. Tiene la forma:

$$0, x_1 x_2 x_3 x_4 x_5 \dots$$

donde:

x_1 es diferente de a_1

x_2 es diferente de b_2

x_3 es diferente de c_3

x_4 es diferente de d_4

x_5 es diferente de e_5

y así sucesivamente. Estos son los dígitos que marqué en negrita.

La característica principal aquí es que si tomas un decimal infinito y cambias solo *una* de sus cifras, no importa lo atrás que esté en la cadena de decimales, cambias su valor. No por mucho, quizá, pero eso no importa. Lo importante es que se cambia. Obtenemos nuestro nuevo número «desaparecido» jugando esta carta con cada número en la lista presuntamente completa.

La condición de x_1 significa que este número nuevo no es el primero en la lista, porque tiene la cifra incorrecta en el primer lugar tras la coma decimal. La condición de x_2 significa que este número nuevo no es el segundo de la lista, porque tiene la cifra incorrecta en el segundo lugar después de la coma decimal. Y así sucesivamente. Como tanto los decimales como la lista continúan indefinidamente, la conclusión es que el número nuevo no está *en ningún lugar* en la lista.

Pero nuestra suposición era que *está* en la lista. Esto es una contradicción, de modo que nuestra suposición es incorrecta y esa lista no existe.

Un asunto técnico que necesita atención: evita usar 0 o 9 como cifras en el número que se construye, porque la notación decimal es ambigua. Por ejemplo 0,10000... es exactamente el mismo número que 0,09999... (hay dos modos distintos de escribir $\frac{1}{10}$ como un decimal infinito). Esta

ambigüedad se da solo cuando el decimal acaba en una secuencia infinita de ceros o una secuencia infinita de nueves.

Esta idea se llama «argumento de la diagonal de Cantor», porque las cifras a_1, b_2, c_3, d_4, e_5 , etcétera, van a lo largo de la diagonal de la parte derecha de la lista. (Fíjate en la posición de las cifras en negrita.) La prueba funciona precisamente porque tanto las cifras como la lista pueden emparejarse a los números naturales.

Es importante comprender la lógica de esta prueba. Ciento es que podemos enfrentarnos al número particular que construimos fijándolo en la parte superior de la lista y moviendo los otros un espacio hacia abajo. Pero la lógica de la prueba por reducción al absurdo es que ya hemos asumido que no será necesario. El número que construimos se supone que está ya en la lista, *sin* modificar esta. Pero no está. Por lo tanto, esa lista no existe.

Como todo número natural es un número real, esto implica que, en la configuración de Cantor, el infinito de todos los números reales es mayor que el infinito de todos los números naturales. Modificando la paradoja de Russell, fue mucho más lejos, al probar que no existe el número infinito más grande. Eso le llevó a concebir una serie infinita de números infinitos cada vez más grandes, conocidos como «cardinales infinitos» (o «transfinitos»).

Inexistencia del infinito más grande

Cantor pensó que su serie de números infinitos debería empezar así:

$$\aleph_0 \aleph_1 \aleph_2 \aleph_3 \aleph_4 \dots$$

con cada número infinito sucesivo siendo el «siguiente», en el sentido de que no hay nada entre ellos. Los números naturales se corresponden con \aleph_0 . También los números racionales. Pero los números reales no necesitan ser racionales. El argumento de la diagonal de Cantor prueba que $\textcolor{brown}{c}$ es mayor que \aleph_0 , de modo que, presumiblemente, los números reales se deberían corresponder con \aleph_1 . Pero ¿lo hacen?

La prueba no nos indica eso. Dice que $\textcolor{brown}{c}$ es mayor que \aleph_0 , pero no descarta la posibilidad de que haya algo entre ellos. Con lo que Cantor sabía, $\textcolor{brown}{c}$ podría ser, por ejemplo, \aleph_3 . O algo peor.

Algo pudo probar. Los cardinales infinitos sí pueden ordenarse de esa manera. Además, los subíndices 0, 1, 2, 3, 4, ... no se acaban con los números naturales finitos. Debe de haber también un número transfinito \aleph_{\aleph_0} , por ejemplo, el número transfinito más pequeño que es mayor que todos los \aleph_n siendo n cualquier número natural. Y si las cosas se detienen aquí, vulneraría su teorema de que no existe un número transfinito que sea el mayor, de modo que no se detienen. Nunca.

Lo que no pudo probar es que los números reales se corresponden con \aleph_1 . Quizá sean \aleph_2 y haya algún otro conjunto entre medias, de modo que ese conjunto sea \aleph_1 . Por mucho que lo intentó, no pudo encontrar ese

conjunto, y tampoco pudo probar que no existía. ¿Dónde están los números reales en esta lista de álefs? No tenía ni idea. Sospechaba que los números reales sí se correspondían con \aleph_1 , pero era pura conjectura. De modo que acabó usando un símbolo diferente, la gótica \mathfrak{c} , que viene de «continuo», el nombre que entonces se usaba para el conjunto de todos los números reales.

Un conjunto finito con n elementos tiene 2^n subconjuntos diferentes. De modo que Cantor definió 2^A , para cualquier cardinal A , considerando algún conjunto con cardinal A y definiendo 2^A como el cardinal del conjunto de todos los subconjuntos de ese conjunto. Entonces pudo probar que 2^A es mayor que A para cualquier cardinal infinito A . Lo cual, accidentalmente, implica que no hay un cardinal infinito que sea el mayor. También pudo probar que $\mathfrak{c} = 2^{\aleph_0}$. Parecía probable que $\aleph_{n+1} = 2^{\aleph_n}$. Es decir, considerar el conjunto de todos los conjuntos lleva al siguiente cardinal infinito más grande. Pero no pudo probarlo.

No pudo ni siquiera demostrar el caso más sencillo, cuando $n = 0$, lo cual es equivalente a afirmar que $\mathfrak{c} = \aleph_1$. En 1878, Cantor conjeturó que esta ecuación, que pasó a conocerse como la «hipótesis del continuo», es cierta. En 1940, Gödel probó que la respuesta «sí» es consistente desde el punto de vista lógico con la suposición habitual de la teoría de conjuntos, lo cual era alentador. Pero luego, en 1963, Cohen probó que la respuesta «no» también es consistente desde el punto de vista lógico.

Uy, vaya...

Esto no es una contradicción lógica en matemáticas. Su significado es mucho más extraño y, de algún modo, más perturbador: la respuesta depende de la versión de la teoría de conjuntos que se use. Hay más de un modo de establecer los fundamentos lógicos de las matemáticas y, mientras todos ellos están de acuerdo en el material básico, pueden no concordar en conceptos más avanzados.

Como solía decir Pogo, el personaje animado de Walt Kelly: «nos hemos encontrado con el enemigo, y somos nosotros». Nuestra insistencia en lógica axiomática se está convirtiendo en un quebradero de cabeza.

Hoy sabemos que muchas otras propiedades de los cardinales infinitos también dependen de qué versión de la teoría de conjuntos se use. Además, estas cuestiones tienen vínculos cercanos con otras propiedades de conjuntos que no involucran a los cardinales de manera explícita. El área es un paraíso para los lógicos matemáticos, pero, en conjunto, el resto de los matemáticos parecen trabajar bien sea cual sea la versión de la teoría de conjuntos que utilicen.

El sentido de la vida, el universo y...

Contenido:

§. 42. Nada aburrido

¿Es *realmente* 42 el número más aburrido que existe?

§. 42. Nada aburrido

Bueno, eso ciertamente desvela el misterio.

Como mencioné en el prefacio, este número aparece de manera destacada en *Guía del autoestopista galáctico*, de Douglas Adams, donde es la respuesta a «la gran pregunta sobre el sentido de la vida, el universo y todo lo demás». Este descubrimiento inmediatamente hizo surgir una nueva pregunta: ¿qué era realmente la gran pregunta sobre el sentido de la vida, el universo y todo lo demás? Adams dijo que escogió este número porque una encuesta rápida entre sus amigos sugirió que era totalmente aburrido.

Aquí quiero defender al 42 de esta calumnia. Ciento es que no está a la par de 4 o π o incluso 17, en términos de importancia matemática. Sin embargo, no carece completamente de interés. Es un número oblongo, un número de Catalan, y la constante mágica del cubo mágico más pequeño. Y algunas cosas más.

Número oblongo

Un número oblongo es el producto de dos números enteros consecutivos.

Por tanto, es de la forma $n(n + 1)$. Cuando $n = 6$, obtenemos $6 \times 7 = 42$.

Como el n -ésimo número triangular es $\frac{1}{2}n(n + 1)$, un número oblongo es dos veces un número triangular. Es, entonces, la suma de los n primeros números pares. Un número oblongo de puntos pueden colocarse en forma de rectángulo, con un lado una unidad mayor que el otro.

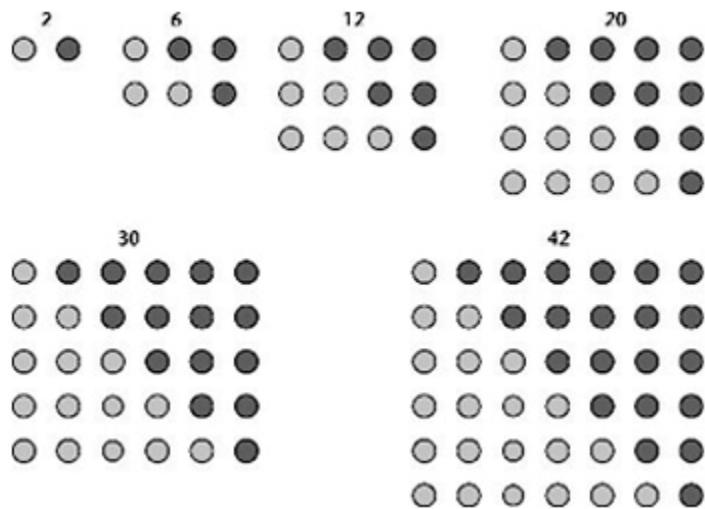


Figura 176. Los seis primeros números oblongos. Lo sombreado muestra por qué cada uno es dos veces un número triangular.

Se cuenta que a Gauss, cuando era muy joven, se le puso el problema del tipo general:

$$1 + 2 + 3 + 4 + \dots + 100$$

Inmediatamente se dio cuenta de que si la misma suma se escribe en orden descendente

$$100 + 99 + 98 + 97 + \dots + 1$$

entonces los pares correspondientes suman 101. Como hay 100 de esos pares, el resultado total es $100 \times 101 = 10.100$, que es un número oblongo. La respuesta al problema planteado por el profesor es la mitad de eso: 5.050. Sin embargo, en realidad no sabemos qué números planteó a la clase el profesor de Gauss y, probablemente, eran más difíciles que estos. De ser así, la perspicacia de Gauss fue todavía más aguda.

El sexto número de Catalan

Los números de Catalan surgen en muchos problemas de combinatoria diferentes; estos números cuentan el número de modos de llevar a cabo varias tareas matemáticas. Se remontan a Euler, quien contaba el número de modos en el cual un polígono puede dividirse en triángulos conectando sus vértices. Más tarde, Eugène Catalan descubrió un vínculo con el álgebra: de cuántas maneras se pueden insertar paréntesis en una suma o producto. Llegaré a eso enseguida, pero primero permítome presentar los números. Los primeros números de Catalan C_n para $n = 0, 1, 2, \dots$ son:

1 1 2 5 14 42 132 429 1.430 4.862

Hay una fórmula usando factoriales:

$$C_n = \frac{(2n)!}{(n+1)!n!}$$

Una buena aproximación para un n grande es:

$$C_n \approx \frac{4^n}{\frac{3}{n^2} \sqrt{\pi}}$$

que es otro ejemplo de π en un problema que aparentemente no tiene conexión con los círculos o las esferas.

C_n es el número de maneras diferentes de cortar un polígono regular de $n + 2$ lados en triángulos.

Es también el número de árboles binarios con enraizado con $n + 1$ hojas. Estas se obtienen empezando con un único punto, la raíz, y luego permitiendo que dos ramas germinen a partir de ese punto. Cada rama termina en un punto o en una hoja. A su vez, cada punto debe ser el germen de dos ramas.

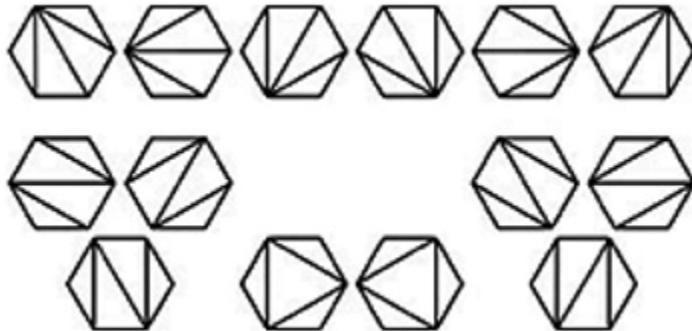


Figura 177. Las 14 triangulaciones de un hexágono.

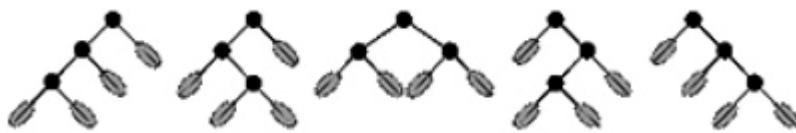


Figura 178. Los cinco árboles binarios con enraizamiento con cuatro hojas.

Si esta idea parece esotérica, tiene una conexión directa con el álgebra: es el número de maneras diferentes de insertar paréntesis en un producto como $abcd$, donde hay $C_3 = 5$ posibilidades:

$$((ab)c)d \ (a(bc))d \ (ab)(cd) \ a((bc)d) \ a(b(cd))$$

En general, con $n + 1$ símbolos, el número de paréntesis es C_n . Para ver la conexión, escribe los símbolos al lado de las hojas del árbol e inserta paréntesis según los pares que se unen en un punto. Más detalladamente (véase la Figura), etiquetamos las cuatro hojas a, b, c, d de izquierda a derecha. Trabajando de abajo arriba, escribe (bc) al lado del punto que

une b a c . Luego el punto sobre eso une a al punto marcado (bc), de modo que el nuevo punto se corresponde con $(a(bc))$. Finalmente el punto en la parte de arriba une eso a d , así se obtiene $((a(bc))d)$.

Muchos otros problemas de combinatoria llevan a los números de Catalan; estos que hemos visto son una pequeña muestra de los más fáciles de describir.

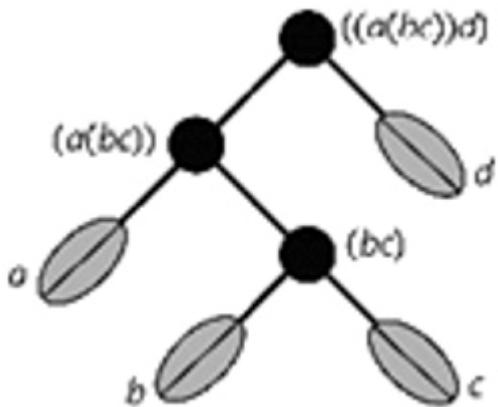


Figura 179. Pasando un árbol binario con enraizamiento a álgebra.

Cubos mágicos

La constante mágica de un cubo mágico de $3 \times 3 \times 3$ es 42. Ese cubo contiene cada uno de los números del 1 al 27 y la suma a lo largo de cualquier fila paralela a una arista o cualquier diagonal pasando por el centro es la misma, la constante mágica. La suma de las 27 entradas es $1 + 2 + \dots + 27 = 378$. Se divide en nueve ternas que no interseccionan que suman la constante mágica, de modo que esta debe ser $378/9 = 42$.

Esas disposiciones existen. En la Figura se muestra una de ellas.

1	17	24
15	19	8
26	6	10

23	3	16
7	14	21
12	25	5

18	22	2
20	9	13
4	11	27

Figura 180. Capas sucesivas de un cubo mágico de $3 \times 3 \times 3$.

Otras características especiales

- 42 es el número de particiones de 10 (modos de escribirlo como una suma de números positivos enteros en su orden natural) como por ejemplo:

$$1 + 2 + 2 + 5 \quad 3 + 3 + 4$$

- 42 es el segundo número esfénico (números que son producto de tres primos distintos). En este caso, $42 = 2 \times 3 \times 7$. Los primeros números esfénicos son:

$$30 \quad 42 \quad 66 \quad 70 \quad 78 \quad 102 \quad 105 \quad 110 \quad 114 \quad 130$$

- 42 es el tercer número pentadecagonal, análogo a los números triangulares, pero basado en un polígono regular de 15 lados.
- 42 es supermultiperfecto: la suma de los divisores de la suma de sus divisores (incluyendo 42) es seis veces el propio número.

- Durante un tiempo, 42 fue la medida de irracionalidad más conocida para π , un modo preciso de cuantificar «lo irracional que es» π . Específicamente, Kurt Mahler probó en 1953 que

$$\left| \pi - \frac{p}{q} \right| \geq \frac{1}{q^{42}}$$

para cualquier racional $\frac{p}{q}$. Sin embargo, en 2008, V. Kh. Salikov reemplazó 42 por 7,60630853, de modo que 42 volvió a ser aburrido en este contexto.

- 42 es el tercer número primario pseudoperfecto. Satisface la condición:

$$\frac{1}{p_1} + \frac{1}{p_2} + \dots + \frac{1}{p_K} + \frac{1}{N} = 1$$

donde los p_j son los distintos primos que dividen N . Los primeros números primarios pseudoperfectos son:

2

6

42

1.806

47.058

2.214.502.422

52.495.396.602

- 42 es el número de n de conjuntos para cuatro enteros positivos diferentes $a, b, c, d < n$ tales que $ab - cd, ac - bd$ y $ad - bc$ son todos divisibles entre n . Es el único número conocido con esta propiedad, pero no se sabe si existen otros.
- 42 es la dimensión más pequeña para la cual la conjetura de la salchicha *se ha probado* que es correcta [véase 56]. Sin embargo, existe la hipótesis de que es cierta para todas las dimensiones mayores o iguales que 5, de modo que la importancia de 42 aquí depende del estado actual de conocimiento.

¿Ves? ¡Nada aburrido!

Lecturas adicionales

- Carl B. Boyer. *A History of Mathematics*, Wiley, Nueva York, 1968 (hay trad. cast.: *Historia de la matemática*, Alianza, Madrid, 1999).
- John H. Conway y Richard K. Guy. *The Book of Numbers*, Springer, Nueva York, 1996.
- John H. Conway y Derek A. Smith. *On Quaternions and Octonions*, A. K. Peters, Natick MA, 2003.
- John H. Conway, Heidi Burgiel y Chaim Goodman-Strauss. *The Symmetries of Things*, A. K. Peters, Wellesley MA, 2008.
- Tobias Dantzig. *Number: The Language of Science*, PiPress, Nueva York, 2005 (hay trad. cast.: *El número. Lenguaje de la ciencia*, Hobbs-Sudamericana, Buenos Aires, 1971).
- Augustus De Morgan. *A Budget of Paradoxes* (2 vols., reimpr.), Booksfor Libraries Press, Nueva York, 1969.
- Underwood Dudley. *Mathematical Cranks*, Mathematical Association of America, Nueva York, 1992.
- Marcus Du Sautoy. *The Music of the Primes*, Harper-Perennial, Nueva York, 2004 (hay trad. cast.: *La música de los números primos*, El Acantilado, Barcelona, 2007).
- Richard J. Gillings. *Mathematics in the Time of the Pharaohs* (reimp.), Dover, Nueva York, 1982.

- Anton Glaser. *History of Binary and Other Nondecimal Numeration*, Tomash, Los Ángeles, 1981.
- Jan Gullberg. *Mathematics from the Birth of Numbers*, Norton, Nueva York, 1997.
- Richard K. Guy. *Unsolved Problems in Number Theory*, Springer, Nueva York, 1994.
- G. H. Hardy y E. M. Wright. *An Introduction to the Theory of Numbers*, Oxford University Press (4.ª ed.), Oxford, 1960.
- Andreas M. Hinz, Sandi Klavzar, Uros Milutinovic y Ciril Petr. *The Tower of Hanoi-Myths and Maths*, Birkhäuser, Basel, 2013.
- Gareth A. Jones y J. Mary Jones. *Elementary Number Theory*, Springer, Berlín, 1998.
- George Gheverghese Joseph. *The Crest of the Peacock: Non-European Roots of Mathematics*, Penguin, Londres, 1992 (hay trad. cast.: *La cresta del pavo real: las matemáticas y sus raíces no europeas*, Pirámide, Madrid, 1996).
- Viktor Klee y Stan Wagon. *Old and New Unsolved Problems in Plane Geometry and Number Theory*, Mathematical Association of America, Nueva York, 1991.
- Mario Livio. *The Golden Ratio*, Broadway, Nueva York, 2002 (hay trad. cast.: *La proporción áurea*, Ariel, Barcelona, 2006). —, *The Equation That Couldn't Be Solved*, Simon & Schuster, Nueva

York, 2005 (hay trad. cast.: *La ecuación jamás resuelta*, Ariel, Barcelona, 2007).

- John McLeish. *Number*, Bloomsbury, Londres, 1991.
- O. Neugebauer. *A History of Ancient Mathematical Astronomy* (3vols.), Springer, Berlín, 1975.
- Paulo Ribenboim. *The Book of Prime Number Records*, Springer, Nueva York, 1984.
- Ernő Rubik, Támás Varga, Gerszon Kéri, György Marx y Támás Vekerdy. *Rubik's Cubic Compendium*, Oxford University Press, Oxford, 1987.
- Karl Sabbagh. *Dr Riemann's Zeros*, Atlantic Books, Londres, 2003.
- W. Sierpiński. *Elementary Theory of Numbers*, North-Holland, Ámsterdam, 1998.
- Simon Singh. *Fermat's Last Theorem*, Fourth Estate, Londres, 1997 (hay trad. cast.: *El enigma de Fermat*, Planeta, Barcelona, 1998).
- Ian Stewart. *Professor Stewart's Cabinet of Mathematical Curiosities*, Profile, Londres, 2008 (hay trad. cast.: *La cuadratura del cuadrado y otras curiosidades matemáticas del gabinete del profesor Stewart*, Crítica, Barcelona, 2009). —, *Professor Stewart's Hoard of Mathematical Treasures*, Profile, Londres, 2009 (hay trad. cast.: *Baúl de tesoros matemáticos*, Crítica,

Barcelona, 2010). —, *Professor Stewart's Casebook of Mathematical Mysteries*, Profile, Londres, 2014.

- Frank J. Swetz. *Legacy of the Luoshu*, A. K. Peters, Wellesley MA, 2008.
- Jean-Pierre Tignol. *Galois's Theory of Algebraic Equations*, Longman, Londres, 1988.
- Matthew Watkins y Matt Tweed. *The Mystery of the Prime Numbers*, Inamorata Press, Dursley, 2010.
- Jeremy Webb (ed.). *Nothing*, Profile, Londres, 2013.
- Robin Wilson. *Four Colors Suffice* (2. ªed.), Princeton University Press, Princeton, 2014.

Recursos *online*

Se mencionan fuentes *online* concretas a lo largo del texto. Para el resto de información matemática, puedes empezar con Wikipedia y Wolfram MathWorld.

Agradecimientos por las imágenes

El autor y la editorial agradecen el permiso para usar lo siguiente:

- Figura 1 Wikimedia creative commons, Albert11s;
- Figura 3 Wikimedia creative commons, Marie-Lan Nguyen;
- Figura 31 Livio Zucca;
- Figura 32 Museo de Arte Metropolitano de Nueva York; obsequio de Chester Dale;
- Figura 63 Wikimedia creative commons, Fir0002Flagstaffotos;
- Figura 77 Archivo Lessing;
- Figura 108 Allianz SE; Figura 119 Kenneth Libbrecht;
- Figura 130 thoughtyoumayask.com;
- Figura 133 Jeff Bryant y Andrew Hanson;
- Figura 153 Wolfram MathWorld;
- Figura 159 Wikimedia creative commons;
- Figura 160 Wikimedia creative commons, Matt Crypto;
- Figura 168 Joe Christy.

A pesar de haber intentado contactar por todos los medios con los propietarios del *copyright* de las ilustraciones, el autor y la editorial agradecerían cualquier información sobre las ilustraciones que no hayan sido capaces de localizar, y se comprometen a hacer las enmiendas necesarias en futuras ediciones.

