Rev.R.Acad.Cienc.Exact.Fís.Nat. (Esp)
Vol. 109, Nº. 1–2, pp 59–72, 2017
XIX Programa de Promoción de la Cultura Científica y Tecnológica

Matemáticas, Lógica y Ordenadores: La Gran Alianza.

Fernando Bombal

1. INTRODUCCIÓN

Desde muy antiguo el Hombre ha desarrollado métodos y artilugios para ayudarle a realizar operaciones matemáticas. Pero es a partir de la Revolución Industrial cuando se empezó a disponer de la tecnología necesaria para desarrollar mecanismos eficaces para el cálculo rápido de operaciones matemáticas sencillas.

La necesidad de disponer de una gran capacidad de cálculo para resolver modelos matemáticos más y más complejos se fue incrementando a lo largo del siglo XX y especialmente durante la II Guerra Mundial, lo que impulsó decisivamente la aparición de los primeros “ordenadores” o “computadores” en sentido moderno. Si en su implementación real fueron importantes los avances de la mecánica, la electricidad y la electrónica, no fue menos decisivo para su creación la aportación de la matemática y la lógica para su desarrollo conceptual.

Por otro lado, la ventaja de disponer de una elevada potencia de cálculo a gran velocidad ha tenido un gran impacto en la investigación matemática. Y no sólo en áreas la simulación y creación de modelos, el análisis numérico de las soluciones de ecuaciones funcionales y las aplicaciones a la técnica y la ingeniería, sino en los dominios mismos de la matemática pura.

A continuación, tras realizar un breve recorrido por la historia del desarrollo de las máquinas de cálculo, trataremos de describir algunos de los hitos conceptuales que influyeron decisivamente en la creación de los ordenadores modernos, así como algunas de sus aplicaciones a la resolución de distintos problemas matemáticos.

2. BREVE HISTORIA DE LAS MÁQUINAS DE CÁLCULO

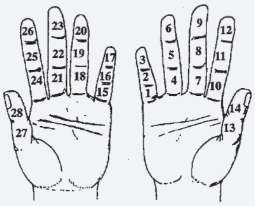
2.1. Los orígenes

Desde el comienzo de las primeras comunidades humanas aparece la necesidad de *contar* (enemigos, presas, productos para intercambio, etc.), *registrar* distintas clases de datos y *operar* con ellos.

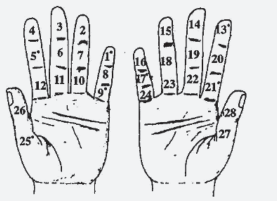
El instrumento más antiguo para contar y realizar algunas operaciones con números pequeños (y que se sigue utilizando hoy en día) es la *mano.* Además de la forma obvia de utilizar los dedos para contar hasta 10, a lo largo de los siglos se han desarrollado ingeniosos métodos para contar muchos más elementos y realizar cálculos con números pequeños (véase, p. ej., el Cap. 3 de [If]):

---

[1] Una parte importante de este trabajo se encuentra incluido, con pequeñas variaciones, en el trabajo [Bo].



Técnica de cuenta manual usada en la India, China e Indochina. Hace intervenir las catorce falanges de los dedos de ambas manos.

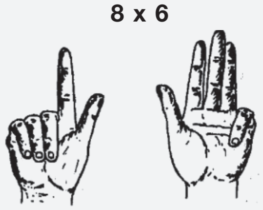


Cómputo manual usado en Irlanda en el siglo VII por Beda el Venerable: método que permite considerar los veintiocho años consecutivos del ciclo solar del calendario juliano con sus períodos bisiestos (señalados por un asterisco).

7 x 8

PRODUCTO DE 7 POR 8
Plegar: (7 - 5) dedos de una mano y (8 - 5) de la otra.
Resultado: 5 dedos plegados en total, 3 dedos levantados en una mano y 2 en la otra.
Por tanto:
7x8 = 5x10 + 3x2 = 56

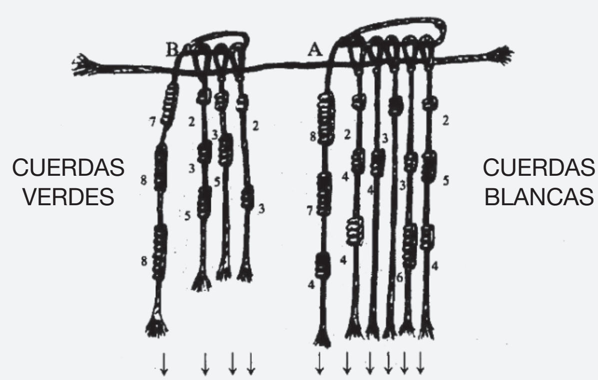
8 x 6



PRODUCTO DE 8 POR 6
Plegar: (8 - 5) dedos de una mano y (6 - 5) de la otra.
Resultado: 4 dedos plegados en total, 2 levantados en una mano y 4 en la otra.
Por tanto:
8x6 = 4x10 + 2x4 = 48

(Tomado de [Ifl])

En cuanto a los métodos de registro de datos, han sido muchos y variados, desde muescas en paredes rocosas, huesos tallados, palos y maderas talladas o los *quipus*, nudos de cuerdas utilizados por los incas para conservar datos numéricos (tributos, evaluación de cosechas, facturas de entrega, censo de poblaciones, etc.)



Uso del quipu por los pastores de las altiplanicies peruanas del siglo pasado para efectuar el recuento de su ganado:
1. Haz A (cuerdas blancas): recuento del ganado menor.
A_1 = 254 ovejas; A_2 = 36 corderos; A_3 = 300 cabras; A_4 = 40 cabritos; A_5 = 244 carneros; A_6 = total = 874 ovino y caprino.
2. Haz B (cuerdas verdes): recuento de los bóvidos.
B_1 = 203 toros; B_2 = 350 vacas lecheras; B_3 = 235 vacas estériles; B_4 = total = 788.

Al aumentar la complejidad de las sociedades humanas, aparece la necesidad de realizar *cálculos*, bien sea para llevar a cabo operaciones comerciales, como para recaudar tributos o repartir herencias. Al principio, para operaciones con cantidades pequeñas, bastaría utilizar una pequeña piedra[2] por cada elemento, representar cada número por un montón de guijarros del mismo cardinal, y efectuar manipulaciones obvias para realizar las operaciones sencillas. Obviamente, este método no es práctico para realizar operaciones con números grandes. Las primeras sociedades altamente organizadas en Elam y Mesopotamia emplearon fichas de arcilla de distinta forma para representar diferentes unidades en la base de numeración utilizada (60 en el caso de los sumerios), lo que permitió realizar operaciones (sumas, restas, multiplicaciones y divisiones) mucho más rápidamente con técnicas análogas:

[2] La palabra *cálculo* proviene del latín *calculus*, que significa "guijarro". Los griegos y romanos enseñaban a sus niños a contar y realizar cálculos elementales por medio de guijarros o fichas de distinta naturaleza. Pero es obvio que el método de enumeración cardinal por medio de un montón de piedras o guijarros es mucho más antiguo.

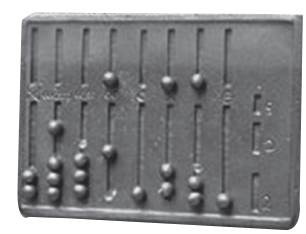
	NUMERACIÓN HABLADA	NUMERACIÓN CONCRETA (*cálculos*)	NUMERACIÓN ESCRITA		
	Nombres de número		Cifras arcaicas	Cifras cuneiformes	Estructura matemática
1	*geš*	cono pequeño			1
10	*u*	bola			10
60	*geš*	cono grande			10.6 (= 60)
600	*geš-u*	cono grande perforado			10.6.10 (= 60.10)
3.600	*šàr*	esfera			10.6.10.6 ($= 60^2$)
36.000	*šàr-u*	esfera perforada			10.6.10.6.10 ($= 60^2.10$)
216.000	*šàrgal*	?	?		10.6.10.6.10.6 ($= 60^3$)
DATACIONES ARQUEOLÓGICAS (a. C.)		Hacia mediados del IV milenio	Hacia 3200	Hacia 2650	

Nombres de número, cifras y «cálculos» de la civilización sumeria. Estos cálculos han sido hallados en un buen número de lugares mesopotámicos (Uruk, Nínive, Jemdet Nasr, Kish, Ur, Tello, Suruppak, etc). (Tomado de [If])

A mediados del tercer milenio a. de C. los calculadores sumerios van sustituyendo el uso de los *cálculos* por lo que puede considerarse el primer *instrumento* de cálculo: el *ábaco*[3]. Se trata de un tablero dividido en columnas, que delimitan los órdenes de magnitud de unidades sucesivas del sistema de numeración utilizado (sexagesimal en este caso) y sobre el que se depositan pequeñas canicas o astillas con las que se pueden realizar toda clase de cálculos aritméticos. El principio fue redescubierto por distintas civilizaciones, con diversas variaciones (véase, por ejemplo, [If]). Algunas, reemplazaron las columnas del tablero o mesa por varillas paralelas y cada ficha por un botón móvil que podía deslizarse a lo largo de la varilla, permitiendo agilizar los cálculos.

Madame Arithmatica, Gregor

Esta idea culminó en el famoso "contador de bolas" chino[4], de origen relativamente reciente (alrededor del siglo XIV de nuestra era), pero que sigue siendo utilizado ampliamente en todo el Extremo Oriente y Rusia. La estructura es similar, aunque con ligeras variaciones, con un precedente claro en el considerado "calculador romano de bolsillo" (Siglo I):



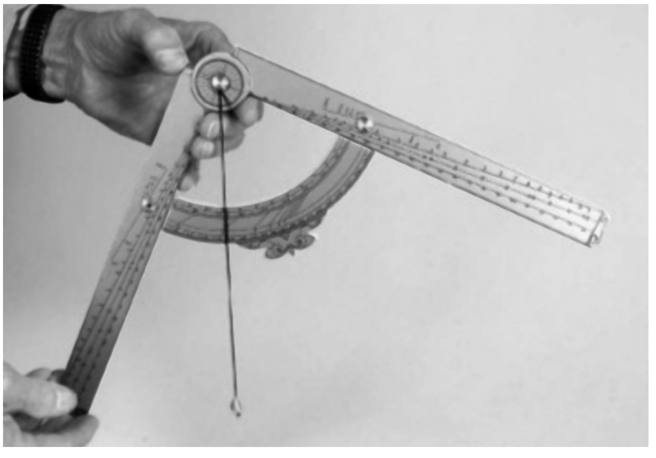
Ábaco Romano. Copia del original (Biblioteca Nacional de Francia) hecha en el Museo de Mainz, Maguncia, en 1977.

Suapan, ábaco chino actual.

[3] El nombre deriva de la palabra latina *abacus*, proveniente a su vez del griego *abakion* que significa "bandeja, mesa o tablilla"*,* aunque su principio fue descubierto mucho antes por diversas civilizaciones.

4 *Sua pan* en chino: literalmente "tablilla de cálculo". El nombre japonés es *soroban.*

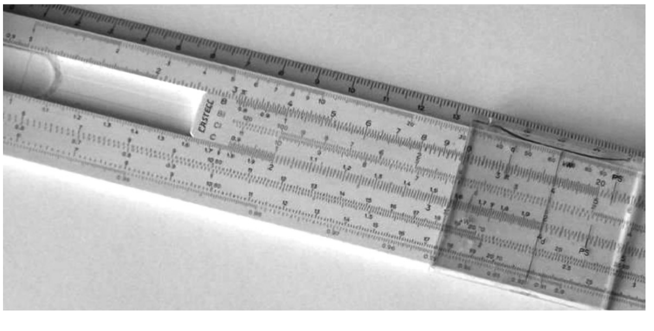
Otros dispositivos con escalas, algunos derivados de diversos instrumentos empleados en navegación o astronomía, fueron empleados para el cálculo. Entre ellos, podemos citar el *compás geométrico militar* inventado por **Galileo** (1564-1642) alrededor de 1600 y que permitía, incluso sin tener conocimientos matemáticos, calcular ángulos, obtener raíces cuadradas y cúbicas, calcular el interés compuesto o determinar la carga adecuada para un cañón.



Compás Geométrico-militar

El descubrimiento de los logaritmos por **John Napier** (1550-1617) estimuló la creación de *reglas de cálculo*, mediante la utilización de varias escalas movibles sobre un armazón rectangular fijo. El mismo **Isaac Newton** (1642-1727) empleó 3 escalas logarítmicas paralelas para resolver ecuaciones cúbicas en 1675.

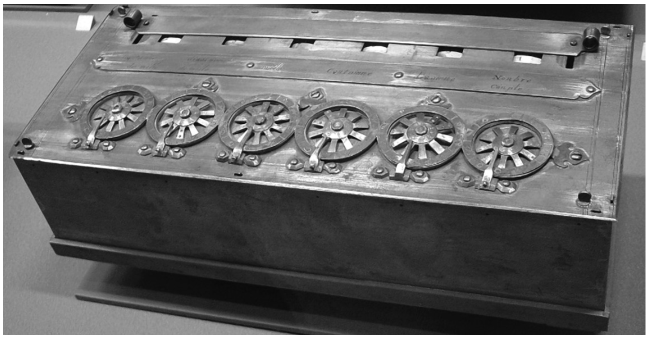
A partir del siglo XIX, especialmente con la Revolución Industrial y el aumento de la demanda de cálculo por parte de los ingenieros, las reglas de cálculo se generalizaron, unificando los sistemas de escalas empleados. Llegaron a ser la herramienta de cálculo más usado en la Ciencia y la Ingeniería hasta mediados del siglo XX.



Regla de cálculo

2.2. Las primeras máquinas de cálculo

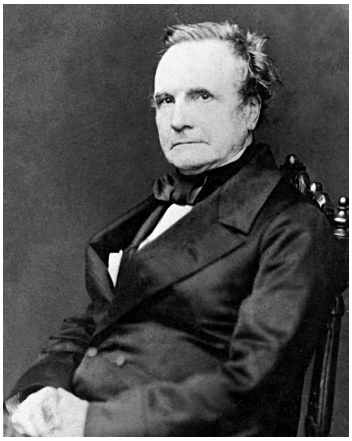
La primera máquina de calcular que funcionaba a base de ruedas y engranajes es la llamada *pascalina*, en honor a su inventor, **Blaise Pascal** (1623-1662), quien la desarrolló en 1642 para ayudar a su padre, a la sazón Jefe de la recaudación de impuestos de la región de Normandía, en sus cuentas. Pascal llegó a construir 50 de estas máquinas, de las que se conservan 9. La máquina permitía sumar y restar dos números de manera directa, y realizar multiplicaciones y divisiones por repetición.



Posteriormente, Sir **Samuel Morland** (1625-1695) en Inglaterra inventó una máquina para multiplicar en 1666. Poco más tarde el matemático y filósofo alemán **Gottfried Wilhelm Leibniz** (1646-1716) presentó en 1673 la primera calculadora para realizar directamente las operaciones aritméticas básicas. Era similar a la pascalina, pero utilizaba un cilindro con dientes en lugar de ruedas. En su diseño se basó **Charles Thomas de Colmar** para producir en 1820 la primera calculadora de distribución comercial masiva, que llamó *aritmómetro.* Se vendieron más de mil ejemplares, sobre todo a casas de seguros.

En 1900 el americano **Frank S. Baldwin** (1838-1925) patentó la primera máquina de calcular que podía realizar las cuatro operaciones aritméticas fundamentales de manera rápida y segura, imprimiendo el resultado. Su máquina sirvió de modelo para la mayor parte de las calculadoras mecánicas de mesa para uso comercial que se emplearon posteriormente.

Las crecientes necesidades de la tecnología demandaban métodos para resolver y calcular distintos problemas numéricos: cálculo de valores de una función, tablas de funciones especiales, resolución de ecuaciones lineales y no lineales con muchas incógnitas, aproximación de soluciones de ecuaciones diferenciales, etc. Se desarrollaron ingeniosos métodos de análisis numérico para disminuir el volumen de cálculos y los errores cometidos, lo que a su vez demandaba nuevas máquinas de cálculo más rápidas y complejas. A estas demandas respondían los intentos del inglés **Charles Babbage** (1791-1871) al diseñar las primeras calculadoras para usos matemáticos: La *Máquina de Diferencias* (1822) y la *Máquina Analítica* (1837)[5]. El diseño de esta última contenía conceptos como una unidad aritmética lógica independiente, una memoria integrada, control de flujo de datos y el uso de tarjetas perforadas para codificar información. Por ello se considera a Babbage como uno de los "padres" de la computación moderna.



Charles Babbage (1791-1871)

Los diseños de Babbage implicaban la fabricación de piezas y mecanismos de gran complejidad, lo que explica en parte el fracaso de su proyecto. El considerado gran continuador de la obra de Babbage fue el español **Leonardo Torres Quevedo** (1852-1918), quien aportó las primeras soluciones. Tras presentar una serie de memorias científicas en las que estableció los fundamentos teóricos, construyó una serie de máquinas analógicas, en las cuales un proceso matemático se transforma en un proceso operativo de ciertas magnitudes físicas que conduce a un resultado físico que se corresponde con la solución matemática buscada. De este modo, un problema matemático se resuelve mediante un modelo físico del mismo.

Leonardo Torres Quevedo (1852-1918)

Tras estos intentos, pronto se convenció Torres Quevedo que las soluciones puramente mecánicas para construir una máquina de calcular como la propuesta por Babbage presentaban dificultades insuperables. Y ello le llevó a estudiar y diseñar una *Máquina Analítica* basada en tecnología electromecánica, combinando los procesos mecánicos con los eléctricos, en particular con el uso de electroimanes[6], abriendo una nueva y fructífera área de trabajo e investigación. En su trabajo se establecen las bases de la automática moderna y plantea el problema de lo que luego se conoció como *inteligencia artificial* . También describe en su trabajo, por primera vez en la historia, la aritmética en coma flotante para realizar cálculos con grandes números.

En 1920 presentó en el *Musée National des Techniques de París* su "aritmómetro electromecánico", que se considera la primera calculadora electromecánica totalmente automática de la historia. En fin, realmente Torres Quevedo se adelantó en varias décadas a los grandes teóricos de las Ciencias de la Computación del siglo XX.

Aritmómetro electro-mecánico (1920)

La necesidad de disponer de máquinas de cálculo mu-

[5] Babbage abandonó su puesto de Profesor en Cambridge para dedicarse totalmente a la construcción de su máquina. Invirtió (y perdió) su fortuna personal en el intento y, aunque obtuvo financiación del gobierno británico, la falta de resultados efectivos hizo abandonar el proyecto y las máquinas no se construyeron en vida de Babbage. En 1991 el *London Science Museum* completó una versión operativa de la *Máquina Analítica*, iniciada por el hijo de Babbage en 1910.

[6] *Ensayos sobre automática. Su definición. Extensión teórica de sus aplicaciones.* Rev. Acad. Ci. Exac. Fís. Nat., **12** (1913), 391-418.

cho más eficientes fue creciendo sin cesar en el periodo de entre guerras, y fueron muchos los investigadores que trataron de conseguir lo que Babbage se había propuesto un siglo antes: una auténtica "máquina analítica". Para conseguir este objetivo fue necesario tanto el desarrollo de la lógica simbólica y los lenguajes formales como los avances en la electricidad y la electrónica. A este respecto, conviene citar el descubrimiento por parte de los inventores británicos **W. H. Eccles y F. W. Jordan** en 1918 del primer circuito electrónico biestable (conocido como *flip-flop*), base de los métodos de registro y almacenamiento en el sistema binario universalmente utilizado en las computadoras actuales.

2.3. La aparición de los ordenadores

La utilización sistemática de la electricidad a lo largo del siglo XX dio origen en los años 1930 a la aparición de los primeros computadores electrónicos. Uno de los primeros fue construido por el ingeniero aeronáutico alemán **Konrad Zuse** (1910-1995) con el nombre de **Z1** en 1936. Se trataba de una calculadora mecánica que utilizaba relés eléctricos para automatizar los procesos. Los cálculos estaban realizados en el sistema binario y la entrada de datos y salida de resultados se realizaba a través de una cinta perforada. Admitía posibilidades de programación, pero el prototipo nunca funcionó del todo bien. Posteriormente, Zuse creó otros diseños para subsanar los problemas del original, y así surgieron la **Z2** y la **Z3**. Esta última, fabricada en 1941, se considera la primera máquina programable y completamente automática, con casi todas las características de los computadores modernos. De hecho, se podían construir bucles lógicos en ella, aunque no poseía ninguna instrucción de salto condicional. Era una máquina realmente avanzada para la época. Por ejemplo, el ENIAC (*Electronic Numerical Integrator and Calculator*), de mucha mayor potencia de cálculo y del que hablaremos después, fue completado cuatro años más tarde que el Z3 y usaba válvulas de vacío (que consumían mucha energía y se estropeaban con frecuencia), en lugar de relés como el Z3. Además, ENIAC era decimal y el Z3 binario. Hasta 1948, para programar el ENIAC había que volver a soldar una nueva configuración de los cables, mientras que el Z3 leía los programas en una cinta perforada. En fin, la arquitectura de los computadores modernos es más parecida a la del Z3 que a la del ENIAC. Ninguna de las máquinas de Zuse sobrevivió a la Guerra Mundial, aunque existen réplicas en los museos de Berlín y Munich[7].

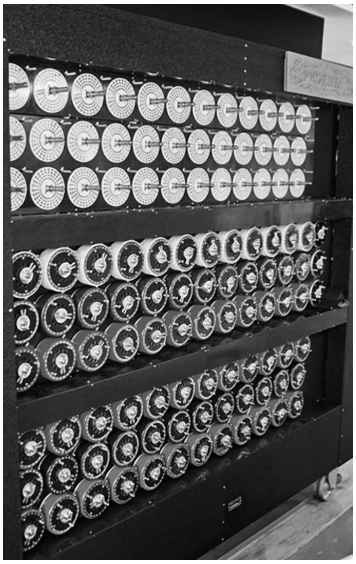
Por la misma época que Zuse creaba la Z1, al otro lado del Atlántico, el ingeniero estadounidense **John Atanasoff** (1903-1995) construyó algunas calculadoras para ayudarle en sus cálculos. La tolerancia mecánica requerida para conseguir una buena exactitud le llevó a considerar el uso de la electricidad y así, durante el invierno de 1937 diseñó un computador digital electrónico que utilizaba válvulas de vacío, cálculos en binario e implementaba una unidad que permitía cálculos lógicos booleanos. Para el desarrollo de la idea, contó con la ayuda de un alumno graduado, **Clifford Berry** (1918-1963), y así nació la *Atanasoff-Berry Company* (ABC). En noviembre de 1939 la ABC contaba con un prototipo operativo, que podía resolver sistemas de hasta 29 ecuaciones lineales.

Todas estas máquinas suponían un importante avance de conceptos, pero tenían una limitada capacidad de cálculo. Y fue precisamente la II Guerra Mundial la que propició la aparición de máquinas mucho más potentes, para resolver problemas originados por necesidades bélicas, tanto en Gran Bretaña como en Estados Unidos:

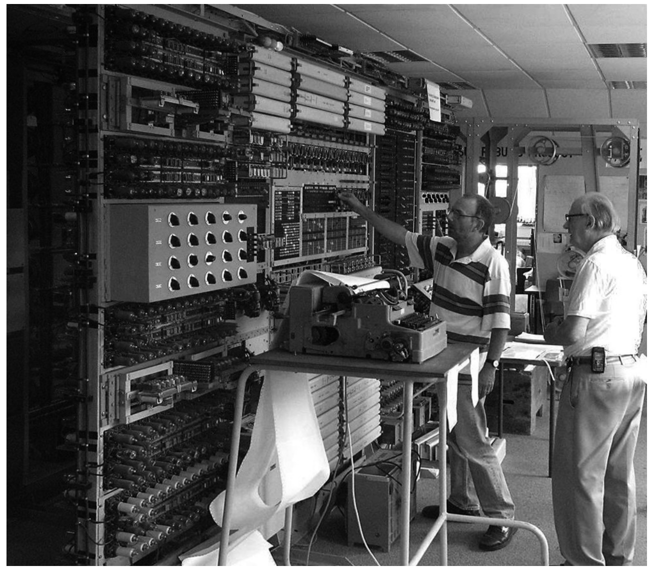
-A principios de 1939 el servicio secreto británico estableció en Bletchley Park, cerca de Londres, unas instalaciones para el descifrado de los mensajes enemigos, en caso de guerra. Matemáticos y criptógrafos, junto con jugadores de bridge y ajedrez, formaron un variopinto grupo, dirigido por el matemático **Alan Turing** (1912-1954)[8], del que hablaremos más adelante, para quebrar el cifrado de las distintas variaciones de la famosa máquina *Enigma* usada por los alemanes. Bajo sus directrices se construyó la primera "*bomba"*, versión muy evolucionada de una máquina diseñada por los servicios secretos polacos que habían estado trabajando desde 1929 en el descifrado de las primeras versiones de la *Enigma.* Tras

[7] En 1998 el matemático mejicano-alemán **Raúl Rojas** demostró que la Z3 era equivalente a una máquina universal de Turing (si tuviera almacenamiento infinito), y por tanto, podría emular *cualquier* cálculo que pueda hacer cualquier otra computadora.

[8] Remitimos al lector interesado a [Co].



Réplica de la *Bomba*



Réplica del *Colossus II* (2006)

la invasión alemana, gran parte de la sección de criptografía polaca huyó a Francia y Gran Bretaña, donde sus informaciones fueron extremadamente valiosas. La bomba emulaba el funcionamiento de 36 máquinas *Enigma* para tratar de descubrir la configuración de la misma en tiempo real (variaba cada día). En 1940 se consiguieron descifrar 178 mensajes alemanes. Llegaron a funcionar unas 70 “bombas” a la vez. La introducción en 1942 de un cuarto rotor en la máquina Enigma, obligó a aumentar el número de “bombas”[9]. Pero, además de Enigma, los alemanes empleaban una máquina aún más sofisticada para sus comunicaciones de alto nivel entre el Alto Mando y los oficiales superiores, llamada *Lorenz SZ40/42*. Para ello los británicos desarrollaron una nueva máquina, considerada el *primer computador electrónico digital y programable,* concebido para resolver problemas lógicos. El prototipo *“Colossus Mark 1”,* diseñado como sus sucesores por el ingeniero **Tommy Flowers** (1905-1998) (y en el que colaboró también Alan Turing), estuvo operativo en Bletchley Park en febrero de 1944. Una versión mejorada, la *Mark 2* entró en funcionamiento en junio de 1944. Se llegaron a construir 10 *“Colossus”*, pero como en el caso de las “bombas” de Turing, su existencia se mantuvo en secreto hasta los 1970.

Cuando terminó la guerra, Turing continuó colaborando para la construcción de máquinas cada vez más sofisticadas, como la ACE (*Automatic Computing Machine*). En 1948 fue contratado por la Universidad de Manchester, y allí construyó el primer ordenador del mundo que dispuso de un programa almacenado electrónicamente.

Al otro lado del Atlántico, la *Moore School of Engineering* era un centro dependiente de la Universidad de Pennsylvania que estaba especializado en el cálculo de tablas de tiro para las nuevas armas desarrolladas por la Armada. En 1941 se incorporó como Profesor el físico **John W. Mauchly** (1907-1980) y estableció una perdurable amistad con **John P. Eckert,** un recién egresado de la *School*, que le sugirió el uso de tubos de vacío para realizar cálculos. En 1942 Mauchly propuso a la Marina la construcción de un calculador electrónico de uso general, utilizando tecnología digital sin partes móviles, con una gran capacidad de cálculo. La Armada aceptó la propuesta; Mauchly se encargó del diseño y Eckert de su implementación, y así surgió el ENIAC[10], del que ya hemos hablado. Era una máquina 1.000 veces más potente que las existentes hasta entonces. Po-

[9] La mayoría fueron destruidas al finalizar la guerra. El descifrado de la máquina Enigma fue mantenido en secreto hasta los años 1960, así como los nombres de los principales artífices de la hazaña que probablemente acortó considerablemente la guerra. Recientemente se ha rodado una película, *The Imitation Game*, centrada en la figura de Alan Turing y sus actividades en Bletchley Park.

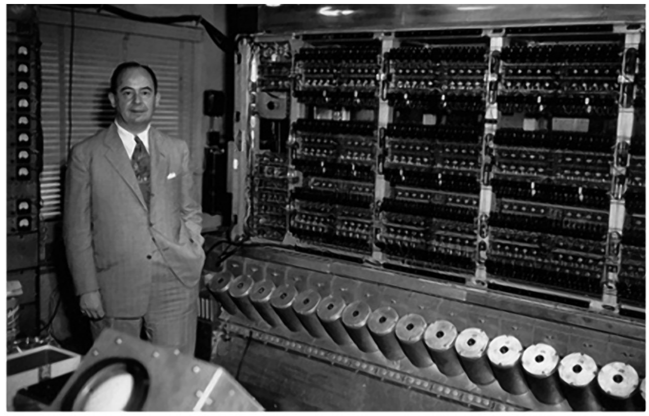
[10] La patente del ENIAC (*Electronic Numerical Integrator and Computer*), registrada por Mauchly y Eckert en 1946, fue invalidada por decisión del Juez **Larson** de la Corte Federal en 1973 al declarar que el ENIAC había “heredado” demasiadas ideas claves de la máquina ABC de Atanasoff. En efecto, Mauchly visitó a Atanasoff en junio de 1941 para ver el ABC y estudiar su diseño y tuvieron varias reuniones posteriores para hablar de temas de computación. Mauchly nunca dijo a Atanasoff que estaba trabajando en la construcción de un computador (adujo en el juicio que estaba bajo restricciones de seguridad militar). La decisión judicial provocó una gran controversia.

día realizar 5.000 sumas o realizar 14 multiplicaciones de 10 dígitos en un segundo. Ocupaba 167 m^2 y pesaba 27 toneladas. Requería la operación manual de unos 6.000 interruptores y, como hemos dicho, su programación se realizaba por *hardware*, realizando una nueva configuración del mismo y su fiabilidad no era muy grande. Pero su capacidad de cálculo era asombrosa. Posteriormente, **John von Neumann** (1903-1957) que a la sazón trabajaba en el *Proyecto Manhattan*, se unió al programa en 1944. Había llegado a la conclusión de que los métodos analíticos eran inadecuados para resolver las ecuaciones que surgían en el diseño de la bomba atómica (ondas de choque, difusión de neutrones, etc.) Así que optó por técnicas de discretización y resolución numérica. Pero para ello necesitaba mecanismos efectivos y rápidos de cálculo y una variedad de algoritmos para resolver rápidamente las ecuaciones discretizadas. Al tener conocimiento de la existencia del ENIAC, se dio cuenta de que era precisamente lo que necesitaba. De hecho, dedicó gran parte de sus esfuerzos posteriores a la teoría de la computación y al diseño de la estructura lógica de ordenadores.

En una conferencia que pronunció en Montreal en 1945 concluyó que

> *Los instrumentos realmente eficientes de alta velocidad de cálculo son los que nos proporcionarán en el campo de las ecuaciones no lineales en derivadas parciales y en muchos otros a los que ahora tenemos difícil o completamente imposible acceso, las herramientas necesarias para un progreso genuino.*

Von Neumann conoció a **Alan Turing** durante la estancia de éste en el Instituto de Estudios Avanzados de Princeton, el curso 1936-37 y probablemente tuvo noticia de la idea de máquina de Turing incluida en el artículo de 1936. Como hemos dicho, en 1944 se unió al grupo encargado de construir una nueva calculadora analítica



John Von Neumann con ENIAC

(la EDVAC: *Electronic Discrete Variable Automatic Computer*), que remediara los defectos conceptuales e imperfecciones del ENIAC. Después de muchas sesiones de trabajo, surgió poco a poco la idea de *programa grabado,* que evitaría tener que modificar la calculadora para cada problema, y dotaría al sistema de programación de la posibilidad de automodificarse. Estas ideas fueron expuestas en el famoso artículo *First draft of a report on the EDVAC,* publicado el 30 de junio de 1945 con la firma de Von Neumann[11]. En él se describe con precisión el diseño de lo que debería ser un computador digital electrónico, con una *unidad aritmético-lógica,* una *unidad de control,* y una *memoria* para almacenar tanto datos como instrucciones. Era el inicio de lo que se llamó la *arquitectura de Von Neumann* que ha inspirado el desarrollo físico de los ordenadores modernos[12].

Una vez establecida la arquitectura básica de lo que debe ser un computador, los avances en la electricidad y la electrónica[13] propiciaron un desarrollo vertiginoso en la creación de máquinas más potentes, más pequeñas y más baratas. Su impacto en la ingeniería y la tecnología ha sido impresionante y el mundo en que vivimos sería distinto sin estos dispositivos.

2.4 La contribución de Alan Turing

---

[11] En palabras del matemático y teórico de la computación **Herman H. Goldstine** (1913-2004), este informe es "*un análisis y una síntesis magistral de todas las reflexiones realizadas entre el otoño de 1944 y la primavera de 1945"* y constituye *"el más importante documento escrito hasta entonces sobre el cálculo y las calculadoras"*

[12] Es ciertamente difícil dar una definición de lo que es un ordenador en sentido moderno. En [If; págs.. 1646 y sigs.] se recogen hasta 10 definiciones distintas. Lo esencial es que un ordenador es una máquina analítica universal de programa grabado, capaz de manipular todo tipo de símbolos expresables mediante códigos *numéricos.* En cuanto a su plasmación física, no es necesario que utilicen cálculo binario ni que su construcción esté basada en circuitos electrónicos. Su estructura es independiente de la tecnología que se emplee en su construcción.

[13] El *Massachusetts Institute of Technology* (MIT) presentó en 1956 el primer computador transistorizado. El primer microprocesador fue desarrollado por *Intel* en 1971.

Además del desarrollo de la electrónica, una de las mayores contribuciones al diseño de ordenadores tuvo su origen en un importante y abstruso problema de lógica matemática, planteado por **Hilbert** en el Congreso Internacional de Matemáticos de Bolonia (1928): el llamado *Entscheidungsproblem* o "problema de decisión", que consiste en saber si existe un algoritmo que permita probar si una proposición bien formulada en el cálculo de predicados (lógica de primer orden) es o no un teorema, es decir, se puede deducir de los axiomas. La pregunta tiene un claro antecedente en los intentos de **G. Leibniz** (1646-1716) de construir una "máquina lógica universal", que permitiera determinar si una frase matemática era o no un teorema. Obviamente, para responder a la pregunta es preciso dar un sentido claro y preciso a lo que es un teorema (es decir, establecer claramente las leyes lógicas) y también a lo que es un *algoritmo*[14]. La idea general de lo que es un algoritmo, como conjunto finito de instrucciones que permite, a partir de unos datos iniciales, obtener una respuesta, es suficiente para dar una respuesta positiva a la pregunta de Hilbert (basta exhibir el algoritmo). Pero no lo es si la respuesta es negativa, ya que ello exige probar que *ningún* algoritmo resuelve el problema, y por tanto es preciso caracterizar completamente el concepto de algoritmo. Esto se consiguió en 1936, de manera independiente por el estadounidense **Alonzo Church**[15] (1903-1995) y su discípulo, el británico **Alan Turing**, del que ya hemos hablado.

Alan Turing (1912-1954)

Los dos enfoques se probaron más adelante que son equivalentes, pero el argumento de Turing ha tenido más influencia que el de Church. La definición de Turing de algoritmo es hoy casi trivial: es cualquier procedimiento que pueda programarse en alguno de los lenguajes universales de programación para ser ejecutados en un ordenador actual. Esta definición tiene un grave problema, y es que en 1936 aún no existían los ordenadores como los conocemos hoy, ni los lenguajes de programación. Lo que hizo Turing en su trabajo [Tu] fue describir con precisión un instrumento ideal que pudiera ejecutar una función computable (≡algoritmo) ejecutando un *programa,* es decir, lo que hoy se conoce como *Máquina de Turing*[16], En su artículo, Turing probó que se podía describir una máquina de Turing que pudiera emular a cualquier otra máquina de Turing concreta, y por tanto ejecutar *toda* función computable (algoritmo). Es lo que hoy se conoce como *máquina universal de Turing*[17]. Muchos consideran esta descripción como el origen de los ordenadores con programa almacenado. Así en un artículo aparecido en la revista *Time* del 29 de marzo de 1999 se dice:

> *Todo el que teclea en un teclado de un ordenador actual está trabajando en una encarnación de una Máquina de Turing, que John von Neumann construyó a partir del trabajo de Alan Turing.*

---

[14] El Diccionario de la Real Academia Española define algoritmo como *"Conjunto ordenado y finito de operaciones que permite hallar la solución de un problema".* Hay muchos ejemplos en matemáticas de algoritmos: el algoritmo de multiplicación o división de enteros, el algoritmo de Euclides para el cálculo del m.c.d. de dos números, etc.

[15] Church utilizó en sus trabajos el llamado *cálculo lambda*, un sistema formal que permite definir claramente lo que es una "función computable" y que ha tenido gran influencia en el desarrollo de lenguajes de programación como el **Lisp** o el **Haskell.** Church probó que no existe un algoritmo (función computable) que decida si dos expresiones del cálculo lambda son lógicamente equivalentes o no.

[16] En una nota .sobre máquinas inteligentes publicada en 1948, Turing .escribió que una Máquina de Turing consistía en: "*.una ilimitada capacidad de memoria obtenida en la forma de una cinta infinita marcada con cuadrados, en cada uno de los cuales podría imprimirse un símbolo. En cualquier momento hay un símbolo en la máquina, llamado el símbolo leído. La máquina puede alterar el símbolo leído y su comportamiento está en parte determinado por ese símbolo, pero los símbolos en otros lugares de la cinta no afectan el comportamiento de la máquina. Sin embargo, la cinta se puede mover hacia adelante y hacia atrás a través de la máquina, siendo esto una de las operaciones elementales de la máquina. Por lo tanto cualquier símbolo en la cinta puede tener finalmente una oportunidad."*

[17] Hay una abundantísima literatura al respecto. Una buena descripción de las máquinas de Turing y del *problema de la parada* puede verse, por ejemplo, en [Ru].

Ya hemos visto que Turing contribuyó también decisivamente en la construcción de los ordenadores más avanzados del mundo hasta 1950, probablemente pensando en crear modelos cada vez más próximos a su imaginaria máquina de calcular esbozada en su trabajo de 1936.

Tras la guerra, Turing estuvo sometido a vigilancia por los servicios secretos británicos. Les preocupaba que el hombre que más sabía de códigos de seguridad fuera vulnerable al chantaje por su condición de homosexual. En 1952 Turing fue arrestado por "indecencia grave", como estaba considerada entonces la homosexualidad en Gran Bretaña, a raíz del juicio por un robo en su domicilio. Turing aceptó un tratamiento hormonal de castración química durante un año para librarse de la cárcel y ello, junto con la continua vigilancia por parte de la inteligencia británica, alteró profundamente su estado de ánimo. El 7 de junio de 1954, Turing fue encontrado muerto en su domicilio. El forense determinó que había muerto por envenenamiento por cianuro y la investigación judicial dictaminó que había sido un suicidio. En la casa había un frasco de cianuro potásico y junto a la cama hallaron media manzana con varios mordiscos.[18]

En su famoso artículo de 1936, Turing prueba primero que el llamado *problema de la parada* ("halting problema") es indecidible, es decir, que no existe un programa *P* que permita saber si *cualquier* programa concreto *q* va a terminar tras un número finito de pasos o no[19]. Después, Turing muestra que el *Entscheidungsproblem* se puede reformular como el problema de la parada, lo que da una respuesta negativa a la pregunta de Hilbert. Este argumento se ha mostrado de extraordinaria utilidad para proporcionar pruebas de indecibilidad en multitud de contextos.

Por ejemplo, una aplicación de este método proporcionó la solución (negativa) del décimo de los problemas propuestos por Hilbert en su famosa lista de 1900: *"encontrar un algoritmo que permita decidir si un polinomio en una o varias variables, con coeficientes enteros, tiene alguna raíz entera.* En 1960, **Martin Davis, Hilary Putman** y **Julia Robinson** mostraron cómo describir el comportamiento de un programa dado por medio una ecuación en términos de un polinomio con coeficientes enteros y una función exponencial, de forma que el programa se detiene si y sólo si la ecuación tiene alguna solución entera. En 1970, **Yuri Matyasevitch** logró eliminar la necesidad de la función exponencial, con lo cual ¡el décimo problema de Hilbert resultó ser equivalente al problema de la parada!

3. EL IMPACTO DEL ORDENADOR EN LA INVESTIGACIÓN MATEMÁTICA

La ventaja de disponer de una elevada potencia de cálculo a gran velocidad ha tenido un gran impacto en la investigación matemática. Y no sólo en áreas la simulación y creación de modelos, el análisis numérico de las soluciones de ecuaciones funcionales y las aplicaciones a la técnica y la ingeniería, sino en los dominios mismos de la matemática pura. A continuación vamos a ver alguno de los más destacados ejemplos:

3.1 El Teorema de los cuatro colores

En 1976 el anuncio de una demostración de un teorema de matemática pura apareció en las páginas del *New York Times*. Se trataba de la *conjetura de los cuatro colores,* propuesta en 1852 por **Francis Guthrie,** un abogado y matemático aficionado británico, quien propuso la siguiente afirmación: *"bastan cuatro colores para colorear cualquier mapa plano de regiones conexas, de modo que no haya regiones adyacentes con el mismo color"*.

Guthrie trasladó la pregunta a su hermano, estudian-

[18] Según el biógrafo de Turing, **Andrew Hodges**, la manzana no fue analizada y jamás se probó debidamente que hubiera sido bañada en cianuro, como todas la apariencias indicaban.

[19] Por supuesto, para muchos programas concretos pueden encontrarse pruebas de si paran o no. Por ejemplo, el programa *"encontrar un número impar suma de dos pares"* no se para nunca*; "encontrar un número natural que no sea la suma de tres cuadrados"* se para para $n=7$*; "encontrar un número que no sea la suma de cuatro cuadrados* (no se para: Teorema de Lagrange, 1770; ¡difícil!);*"encontrar un número par mayor que 2 que no sea suma de dos primos"* nadie sabe a día de hoy si se parará o no (Conjetura de Goldbach).

te del University College de Londres, quien a su vez se lo planteó a su profesor, el eminente **A. de Morgan** (1806-1871). La noticia sobre el problema se extendió rápidamente y muchos notables matemáticos intentaron resolverlo. En 1879 el matemático británico **Alfred Bray Kempe** (1849-1922) publicó un artículo en el *American Journal of Mathematics* en el que sostenía haber resuelto afirmativamente el problema de los cuatro colores. El artículo pasó el proceso de revisión, y poco después Kempe fue elegido miembro de la Royal Society y posteriormente nombrado *Sir* por sus contribuciones a las matemáticas.

Desgraciadamente, en 1890 un profesor de la Universidad de Durham, **Percy John Heawood** (1861-1955), demostró que la prueba de Kempe estaba equivocada. El problema seguía abierto.

El hecho de que cinco colores eran suficientes, había sido probado en 1890 por Percy Heawood en el mismo artículo en el que mostraba que la prueba de Kempe era errónea, pero el paso a cuatro colores era considerablemente más difícil y resistió los esfuerzos de dos generaciones de matemáticos. Hay que decir que, sin embargo, los intentos de solución contribuyeron de forma importante al desarrollo de la topología.

Pero la razón de que un problema matemático despertara el interés de la prensa en 1976 residía, además de la fácil comprensión del enunciado, en el método de demostración, ya que en la misma era esencial el uso del ordenador.

Los matemáticos **Kenneth Appel** (1932-2013) y **Wolfgang Haken** (1928-) tras un esforzado trabajo teórico, lograron reducir el problema a la comprobación de unas 1500 configuraciones básicas. Desde luego, comprobar estas configuraciones básicas y todas las combinaciones de colores de cada una, era una tarea más allá de la capacidad de cualquier equipo de matemáticos, incluso con la ayuda de los ordenadores existentes. Appel y Haken se dedicaron a buscar atajos y estrategias que pudieran usarse en un ordenador para acelerar el proceso de comprobación de las configuraciones básicas. Y así, cinco años después de que empezaran a trabajar en el problema, con la ayuda de un complejo programa de ordenador y el uso de más de 1.200 horas de computación, pudieron anunciar al mundo que todas las configuraciones básicas habían sido analizadas y no precisaban más de cuatro colores. ¡El problema propuesto por Guthrie 124 años antes había sido resuelto!


K. Appel y W. Haken en 1970

La demostración presentada por Appel y Haken fue seguida de una amplia controversia, pues introduce una nueva concepción de lo que se entiende por *demostración matemática*, que no depende exclusivamente de un razonamiento humano, ya que contiene etapas en el programa que nunca podrán ser comprobadas por un matemático. Por otro lado, el proceso puede estar sometido a errores, tanto de *software* como de *hardware,* además de los errores de redondeo que aparecen cuando ser trabaja con números no enteros. Es, por tanto, un argumento que depende de la fiabilidad de una máquina y la convicción de que *siempre* se obtendrá el mismo resultado al correr el programa con todo tipo de ordenadores.

Hay que decir que con el paso del tiempo, la oposición hacia este tipo de argumentos (las llamadas *"demostraciones de silicio"*) se ha ido aminorando, tanto por los resultados obtenidos como por la aceptación de los argumentos esgrimidos por los propios Appel y Haken:

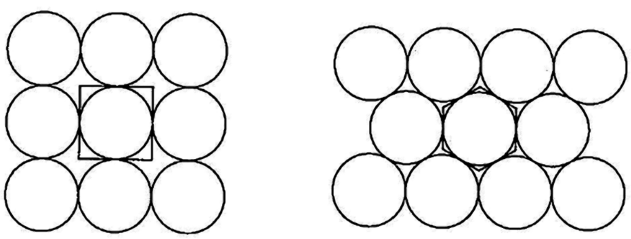
> *"Existe una tendencia a considerar que la verificación de resultados obtenidos por ordenador mediante programas independientes no proporciona una tan gran certeza de su corrección como la verificación manual de las demostraciones tradicionales de los teoremas. Este punto de vista es defendible para aquellos teoremas cuyas demostraciones son de longitud razonable y sumamente teóricas. Pero cuando las demostraciones son largas y de carácter muy computacional, puede aducirse que aunque sea posible la verificación manual, la probabilidad de*

error humano es considerablemente mayor que la de error de máquina” (el subrayado es mío)[20].

Es cierto que el razonamiento “tradicional” ha producido errores a lo largo de la historia, algunos de los cuales han pervivido durante años (sin ir más lejos, recuérdese la falsa “prueba” de Kempe). Además, las matemáticas han alcanzado tal de nivel de especialización y complejidad que incluso en los casos citados por Appel y Haken, la verificación de un resultado puede llevar años y depender de un número muy reducido de especialistas.

3.2 La Conjetura de Kepler

En 1600, Sir Walter Raleigh preguntó a su asistente, el matemático **Thomas Harriot** (1560-1621) cuál era la forma más eficiente de apilar balas de cañón en la bodega de un buque. El problema atrajo la atención del matemático y astrónomo **Johannes Kepler** (1571-1630), quien en 1611 lo reformuló como el siguiente problema matemático: *“Encontrar cuál es la configuración de esferas de un radio dado que tiene máxima densidad[21]”* Por supuesto, se puede plantear un problema similar en el plano (considerando disposiciones de círculos con la máxima densidad respecto al área) o, en general, en cualquier dimensión *n*.



Configuraciones de círculos (cuadrada y Hexagonal)

Para disposiciones *regulares*, es decir, tales que los centros de las esferas forman un retículo simétrico, **Gauss** probó en 1831 que la mejor configuración en el plano es la hexagonal (es decir, formada por círculos inscritos en hexágonos que teselan el plano), y en el espacio la formada por capas apiladas sobre una configuración cuadrada (o hexagonal, son equivalentes) de modo que las esferas de la capa superior estén colocadas en los huecos que quedan en la capa inferior (configuración de centros no alineados; exactamente la que suelen utilizar los fruteros para colocar las naranjas y otros frutos esféricos)[22].

El caso general es mucho más difícil y forma parte del problema 18 de Hilbert, y son muchos los matemáticos que han intentado resolverlo. El problema llegó a los titulares de prensa en 1990, cuando **Wu-Yi Hsiang**, reputado profesor de la Universidad de California en Berkeley, afirmó haber demostrado la conjetura. La historia tiene paralelismos con la de Andrew Wiles, ya que durante el proceso de revisión se encontraron una serie de errores importantes en la prueba. Pero no tuvo el mismo final feliz, pues aunque un año más tarde Hsiang presentó una demostración revisada en la que afirmaba haber corregido los errores, no convenció a la comunidad matemática. Y aunque Hsiang siguió defendiendo la validez de su prueba, los argumentos en su contra se fueron acumulando. Incluso uno de los antiguos colaboradores de Hsiang envió a la misma revista en la que apareció la supuesta prueba de Hsiang (*International Journal of Mathematics*) un contraejemplo a uno de sus lemas fundamentales.Finalmente, el problema parece haber sido resuelto.

En 1998 **Thomas C. Hales** (1954-) anunció haber probado la conjetura, mostrando que la configuración regular de centros no alineados es, efectivamente, la óptima. Como en el caso del Teorema de los Cuatro Colores, se trata de un proceso de reducción del número de configuraciones posibles. La demostración de Hales logra reducir el problema a minimizar una ecuación de 150 variables sobre unas 5.000 configuraciones de esferas. Se trata de un trabajo de más de 250 páginas de razonamientos matemáticos y 3 gigabytes de datos y programas de ordenador. La Revista *Annals of Mathematics*, una de las más prestigiosas, designó un panel de 12 expertos para revisar la demostración.

[20] citado en [DH; página 276]. También remitimos al lector interesado al artículo de **R. Thomas (**[Th]) que, además de una breve historia y la relación del problema con otros resultados, describe, sin entrar en detalles técnicos, una nueva prueba que, aunque sigue las mismas ideas de la de Appel y Haken, reduce sensiblemente en número de configuraciones a estudiar (de 1476 a 633) y utiliza un algoritmo más eficiente de cálculo que utiliza solamente aritmética entera, y por tanto no origina problemas de redondeo..

[21] Es decir, haga máximo el cociente entre el volumen total de las esferas y el del espacio que las contiene

[22] Kepler había ya calculado la densidad de la configuración cuadrada de círculos (~0,785) y la hexagonal (~0,907), y también la de las configuraciones regulares de esferas cuadrada con centros alineados (~0,524), hexagonal con centros alineados (0,605) y (cuadrada o hexagonal) con centros no alineados (~0,740). Véanse las figuras.

Thomas C. Hales

Tras 4 años de trabajo (2003), el presidente del comité de revisión declaró que el comité estaba 99% seguro de la exactitud de la prueba, pero que no iban a continuar. Finalmente, en 2005, apareció publicada la parte "humana" de la prueba en *Annals.*

En enero de 2003, Hales anunció la creación del *Proyecto Flyspeck* para transcribir su demostración a una prueba formal que pudiera ser comprobada por alguno de los verificadores formales de teoremas, como *Isabelle*. El 9 de agosto de 2014 se completó el Proyecto, anunciando que el programa creado había verificado la demostración de Hales y que no encontró errores.

El problema del empaquetamiento óptimo de hiperesferas en dimensión n tiene considerable importancia en la corrección de errores en la transmisión de mensajes. El conjunto de cadenas binarias de n símbolos forman los vértices de un hipercubo de n dimensiones. Para evitar la transmisión de errores hay que tratar que los vértices que codifican mensajes no sean adyacentes. Una configuración de hiperesferas con máxima densidad maximiza el número de posibles mensajes a enviar, minimizando la posibilidad de error.

Particularmente importantes es el caso $n = 24$. **John Leech** encontró en 1965 una configuración regular de hiperesferas especialmente densa, en el contexto de la teoría de códigos. Analizando el grupo de simetrías del retículo de esta distribución, el matemático británico **John H. Conway** (1937 -) descubrió 3 de los 26 *grupos esporádicos* que aparecen en el teorema de clasificación de grupos finitos simples.

3.3 La Conjetura "débil" de Goldbach

En una carta enviada al gran matemático suizo **Leonard Euler** (1707-1783) en 1742, su amigo, el prusiano **Christian Goldbach** (1690-1764), formuló la siguiente conjetura: *"Todo número par mayor que 2 se puede expresar como suma de dos números primos"* Aunque muchos matemáticos desde entonces han intentado resolverla, todavía no se sabe si es cierta o no y es uno de los problemas abiertos más importantes en la Teoría de Números (de hecho, forma parte del problema 8 de la lista de Hilbert). Se ha comprobado su veracidad para todos los números menores que 10^{18}.

Una modificación de la conjetura original es la siguiente: *"Todo número impar mayor que 5 puede escribirse como suma de tres números primos"*. Se conoce como "Conjetura *débil* de Goldbach", ya que una respuesta afirmativa a la conjetura original implica obviamente una respuesta afirmativa a la modificada.

El matemático ruso **I. M. Vinográdov** (1891-1983) probó en 1937 que la conjetura es cierta para todo número impar mayor que una constante C "suficientemente grande". Aunque Vinográdov no dio ninguna estimación para C, muchos trabajos posteriores se dedicaron a encontrar estimaciones cada vez menores. La mejor (hasta 2002) se debe a **Liu** y **Wang** que obtuvieron el valor $C = e^{3100} > 10^{1346}$, una cifra enorme, intratable por métodos computacionales (10^{100} es mayor que el producto del número estimado de partículas subatómicas del Universo por el número de segundos desde el Big Bang).

En 2013, el matemático peruano afincado en Francia **Harald Helfgott** (1977 -) anunció que había resuelto afirmativamente la conjetura débil de Goldbach, en un trabajo de más de 200 páginas, dividido en dos artículos y un apéndice. Su método consta de una parte analítica, con un uso intensivo del análisis de Fourier, para conseguir reducir la cota C a 10^{30} y de una parte computacional (en colaboración con el informático **David Platt)**, de verificación numérica por ordenador de la conjetura hasta $8{,}8 \times 10^{30}$. Remitimos al lector al magnífico artículo [He], en el que el autor describe con claridad y precisión las ideas fundamentales de su demostración.

REFERENCIAS

[Bo] F. Bombal, *Una mirada a las matemáticas del siglo XX.* Discurso inaugural del año académico 2015-2016 en la Real Academia de Ciencias Exactas. Físicas y Naturales. Rev. R. Acad. Cienc. vol **108**, Nos. 1-2 (2015), 147-176.

[By] C. Boyer, *Historia de la Matemática.* Alianza Universidad Textos, **94**. Alianza Editorial, 1986.

[CMD] S. Chicara, S. Mitsuo and J. W. Daubenb, Editors, *The intersectin of History and Mathematics.* Birkhäuser, 1994.

[Co] J. Copeland, *Alan Turing. El pionero de la era de la información.* Turner Publicaciones S. L., 2013

[CPW] T. Cubitt, D. Pérez-García, M. M. Wolf, *Undecidability of the Spectral Gap.* arXiv:1502.04573.

[DH] P. J. Davis, R. Hersh, *Experiencia matemática.* MEC y Labor, Barcelona, 1982.

[Ha] J. Hadamard, *Psicología de la invención en el campo matemático.* Espasa Calpe, 1947.

[He] H. Helfgott, *La conjetura débil de Goldbach* La Gaceta de la RSME, vol. **16,** Núm. **4,** (2013), 709-726.

[If] G. Ifrah, *Historia Universal de las Cifras.* Espasa Calpe, Madrid, 1997.

[LP] M. López Pellicer, *Alrededor de la Hipótesis de Riemann.* Lección inaugural del año académico 2012-2013. Publicaciones de la Real Academia de Ciencias Exactas, Físicas y Naturales. Madrid, 2012.

[Od] P. Odifredi, *The Mathematical Century. The 30 greatest problems of the last 100 years.* Princeton Univ. Press, 2000.

[Sm] S. Smale, *Mathematical problems for the next century*. En "Mathematics: Frontiers and Perspectives", American Math. Soc., 2000.

[Th] R. Thomas, *An update on the four-color theorem.* Notices of the A.M.S., vol. **47**, N. **7** (1998), 848-859.

[Tu] A. Turing, *On computable numbers, with an application to the Entscheidungsproblem.* Proc. London Math. Soc, vol. 42 (1937), 230-265