Rev.R.Acad.Cienc.Exact.Fís.Nat. (Esp)
Vol. 104, Nº. 1, pp 49-60, 2010
XI Programa de Promoción de la Cultura Científica y Tecnológica

LOS NÚMEROS BASE DE LA CIENCIA Y DE LA TRANSMISIÓN ACTUAL DE LA INFORMACIÓN

MANUEL LÓPEZ PELLICER *

* Real Academia de Ciencias Exactas, Físicas y Naturales. Valverde 22, 28004 Madrid.

LOS NÚMEROS EN LA ANTIGÜEDAD

La Matemática sólo es familiar a minorías apasionadas por el razonamiento abstracto o por sus aplicaciones. Su escasa popularidad contrasta con que *la Matemática sea el lenguaje de la Naturaleza*, como decía Galileo.

En las últimas décadas ha aumentado su popularidad debido a la influencia de lo *digital* en la forma de calcular y de comunicarnos. Hace cincuenta años los empleados de banca eran expertos calculistas, obligados por la ausencia del ordenador. No hace mucho tiempo la mayoría de declaraciones de renta se hacían manualmente y exigían desplazamiento físico para su entrega; ahora se suelen hacer por Internet.

El calificativo *digital* recuerda la palabra latina *digitus* (dedo). Los dedos fueron uno de nuestros primeros instrumentos de cálculo. Desde hace más de cinco siglos se utiliza el *sistema de numeración decimal* que sólo tiene diez símbolos diferentes, que son los dígitos 0, 1, 2, 3, 4, 5, 6, 7, 8 y 9. Este sistema es posicional, pues el valor de cada cifra depende del lugar que ocupa y nos facilita una sencilla representación del conjunto $\mathbb{N}:=\{0,1,2,3,...\}$ de los números naturales, donde se puede hacer sin ninguna limitación las operaciones elementales suma y producto. La necesidad de realizar las operaciones inversas llevó a la construcción del conjunto $\mathbb{Z}:=\{0,\pm1,\pm2,\pm3,...\}$ de los números enteros y del conjunto $\mathbb{Q}:=\left\{\frac{a}{b}, a\in Z, b\in Z^*\right\}$ de los números racionales, donde Z^* es el conjunto de números enteros diferentes de 0. Los números racionales se pueden representar por una parte entera seguida de una parte decimal, que puede tener un número finito o infinito de cifras, que en el caso infinito se repiten periódicamente.

El cálculo de límites, necesario para la definición de radicales y funciones logarítmicas y trigonométricas, obligó a la ampliación del conjunto $\mathbb{Q}$ de los números racionales. Así se obtuvo el conjunto $\mathbb{R}$ de los números reales, que se pueden representar por una parte entera y otra decimal, cuyo número de cifras puede ser finito o infinito, con o sin periodo. Se llaman irracionales a los números reales con representación decimal infinita y no periódica, donde hemos sido redundantes por claridad. Finalmente, la necesidad de encontrar entes cuyo cuadrado fuese un número negativo llevó al conjunto $\mathbb{C}$ de los números complejos, formado por números de la forma $a+bi$, donde a y b son números reales e $i=\sqrt{-1}$.

Las tecnologías digitales utilizan el *sistema de numeración binario*, pues como sólo utiliza los dígitos 0, 1 es suficiente un soporte físico susceptible de presentarse en dos estados, que cada uno representará a uno de los dos dígitos de este sistema. El sistema de numeración binario es posicional y cada dos unidades de un mismo orden constituyen una unidad del orden superior. Por tanto:

$$101001_{(2} = 1\times2^5+1\times2^3+1 = 41$$

$$0,001001_{(2} = 1\times2^{-3}+1\times2^{-6} = \frac{1}{8}+\frac{1}{64} = \frac{9}{64}$$

Cualquier número puede representarse en el sistema binario. Las sucesivas cifras de

$$\sqrt{2} = 1,0110101000001001....{}_{(2}$$

o de

$$\pi = 11,001001000011111....{}_{(2}$$

se obtienen por aproximaciones sucesivas.

Transformando tonos de grises, colores o frecuencias de sonidos en secuencias de ceros y unos se consigue grabar una conversación o un espectáculo en una sucesión de ceros y unos que puede transmitirse a velocidad de la luz. A esta tecnología le acompaña el adjetivo digital.

El sistema de numeración binario fue utilizado por los egipcios para resolver el problema de la multiplicación. Desde unos 3000 años antes de Cristo compartieron la escritura jeroglífica con un sistema de numeración no posicional de siete cifras, sin cero, que representaba las sucesivas potencias de 10 por figuras (un palo vertical, un asa, un caracol, una flor de loto, un dedo doblado, ...; un hombre con los brazos en alto representaba un millón). La repetición de cifras permitió a los egipcios representar todos los números naturales y resolver el problema de sumar. El problema de la multiplicación lo redujeron a duplicaciones sucesivas mediante la descomposición uno de los factores en suma de potencias de 2. Por ejemplo, la descomposición

$$41 = 1\times 2^5 + 1\times 2^3 + 1$$

la obtenían observando que

$$2^5 < 41 < 2^6$$
$$41 - 2^5 = 9$$
$$2^3 < 9 < 2^4$$

y, finalmente, de

$$9 - 2^3 = 1$$

deducían que

$$41 - 2^5 = 2^3 + 1$$

que nos da la igualdad antes indicada:

$$41 = 2^5 + 2^3 + 1$$

Entonces la multiplicación 37×41 se puede hacer por duplicaciones sucesivas así:

$$37\times 41 = 37\times\left(2^5 + 2^3 + 1\right) =$$
$$= 37\times 2\times 2\times 2\times 2\times 2 +$$
$$+37\times 2\times 2\times 2 +$$
$$+37.$$

Figura 1. Fragmento del Papiro Rhind copiado por Ahmes≅ 1650 a.C.

En el papiro Rhind (**Figura 1**), que se conserva en el *British Museum* y fue copiado por el escriba Ahmes alrededor del 1650 antes de Cristo, se encuentran muchas reglas de cálculo y una colección de 84 problemas, que demuestran la familiarización de los egipcios con las fracciones y con el cálculo de áreas y volúmenes.

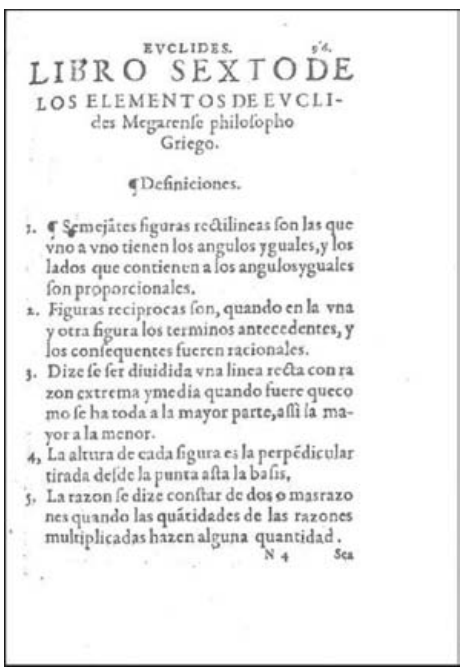
En Mesopotamia, y alrededor del año 2400 antes de Cristo, los sumerios tenían un sistema de numeración posicional mucho más elaborado que el egipcio, cuya base era 60 y sin 0. Grabaron su cultura matemática en tablillas de arcilla utilizando escritura cuneiforme. La tablilla Plimpton 322 (**Figura 2**) es una de las más

Figura 2. Tablilla Plimpton 322 con ternas pitagóricas≅ 1800 a. C.

célebres, pertenece a la época de Hammurabi (~1800 a.C.), se conserva en la Universidad de Columbia y contiene quince ternas pitagóricas, es decir quince soluciones de la ecuación $x^2 + y^2 = z^2$, lo que demuestra la familiaridad se los sumerios con el teorema llamado de Pitágoras (582 a. C. - 507 a. C.), más de un milenio antes de su nacimiento.

Los sistemas de numeración de griegos y romanos fueron alfabéticos e inoperantes para calcular, lo que obligó a los astrónomos griegos a seguir utilizando el sistema de numeración posicional mesopotámico de base sesenta y a desarrollar instrumentos primitivos de cálculo, palabra que parece provenir del vocablo latino *calculi*, que significa piedras. El instrumento de cálculo que más perduró fue el ábaco.

El inoperante sistema de numeración griego contrasta con que la cultura helénica produjera grandes obras matemáticas de las que sólo mencionaremos tres. *Los Elementos* (**Figura 3**), que se escribió alrededor del año 300 a.C. por Euclides (~365 - ~275 a.C.), profesor del Museo de Alejandría. Consta de trece libros dedicados al aprendizaje de la geometría, si bien en los libros VII, VIII y IX Euclides expuso cuestiones de divisibilidad. La *Sintaxis matemática*, escrita por Tolomeo de Alejandría (~85 - ~165 d.C.), fue libro de



EVCLIDES. 5ª.

LIBRO SEXTO DE LOS ELEMENTOS DE EVCLIdes Megarense philosopho Griego.

¶ Definiciones.

1. ¶ Semejãtes figuras rectilineas son las que vno a vno tienen los angulos yguales, y los lados que contienen a los angulos yguales son proporcionales.
2. Figuras reciprocas son, quando en la vna y otra figura los terminos antecedentes, y los consequentes fueren racionales.
3. Dize se ser diuidida vna linea recta con razon extrema y media quando fuere quecomo se ha toda a la mayor parte, assi la mayor a la menor.
4. La altura de cada figura es la perpẽdicular tirada desde la punta asta la basis.
5. La razon se dize consistir de dos o mas razones quando las quãtidades de las razones multiplicadas hazen alguna quantidad.

N 4 Sea

Figura 3. Página 1 del libro sexto de los Elementos de Euclides (≈300 a. C.)

referencia para los astrónomos durante más de mil años. Contiene una tabla de cuerdas de arco de medio en medio grado, antecedente de la tabla de senos. Esta obra se la conoce más por su nombre áraba, *Almagesto*, que significa *el más grande*. La *Arithmetica* de Diofanto (~200 - ~284) que consta de una colección de 150 problemas sobre propiedades de los números, que son tratados sin referencia a medidas concretas. El problema más célebre es el II-8 relativo a las ternas pitagóricas. Consiste en descomponer un cuadrado de un número natural en suma de dos cuadrados de números naturales. Su lectura suscitó a Fermat la conjetura sobre la imposibilidad de efectuar dicha descomposición con potencias n-ésimas, con exponente n mayor o igual a 3.

TRANSMISIÓN A OCCIDENTE DEL SISTEMA DE NUMERACIÓN DECIMAL

El sistema de numeración decimal que utilizamos tienen su origen en la civilización india, cuyos matemáticos elaboraron un sistema de numeración de base decimal con un signo distinto para cada uno de los diez números básicos, incluido el cero, derivado de un guarismo que era un huevo de oca. Las otras nueve cifras derivan de las cifras brahmi, con origen entre los siglos tercero y segundo antes de Cristo. Aryabhata, matemático y astrónomo indio, escribió alrededor del año 499 la obra *Aryabhatiya,* que suministra abundantes reglas de cálculo, fórmulas para progresiones aritméticas, áreas y volúmenes y una tabla de senos, mostrando su familiarización con el sistema decimal. El cálculo con números negativos aparece un siglo después en la obra de Brahmagupta (598-665).

Al califa de Bagdad Abdullāh al-Mā'mūn (786-833) debemos la traducción al árabe de las obras griegas a su alcance. Según la leyenda, tomó esta decisión después de dialogar en sueños con Aristóteles. Fue cofundador con su padre, el califa Harun al-Rasid, de la *Casa de la Sabiduría*, heredera cultural del Museo de Alejandría que hizo posible las traducciones al árabe de los *Elementos* de Euclides y del *Almagesto*, que es la denominación árabe de la *Sintaxis Matemática* de Tolomeo, como se indicó en el apartado anterior. Años más tarde, Abu-l-Welfa (940-998) tradujo del griego la *Arithmetica* de Diofanto.

Figura 4. Página del libro Al-Jabr de Al-Khwarizmi (~790-~850).

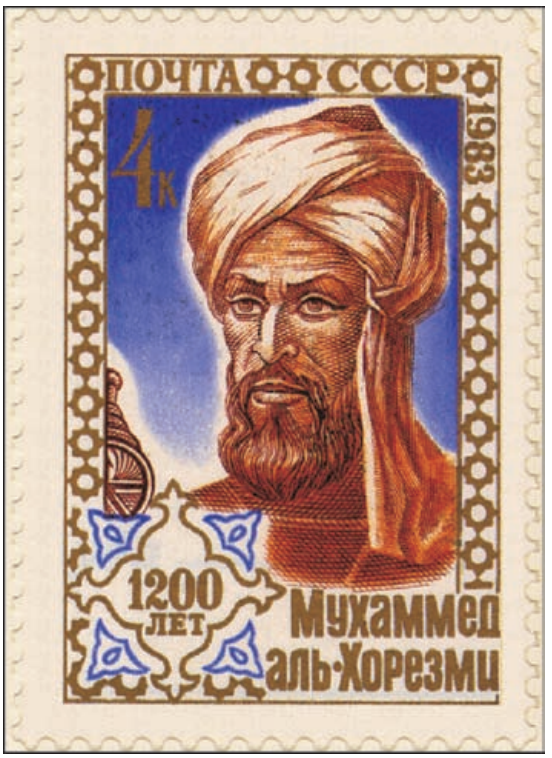


Figura 5. Muhammad ibn Musa Al-Khwarizmi (~790-~850).

En la *Casa de la Sabiduría* trabajó Abu Ja'far Muhammad ibn Musa Al-Khwarizmi (~ 790 - ~ 850) (**Figura 5**). Su libro *De numero indorum* (~ 820) consolidó las cifras indo-arábigas, el cero, el sistema de numeración de posición de base diez y sus reglas de cálculo. El texto original se perdió; la traducción más antigua que se conserva es del siglo XII y procede de la *Escuela de Traductores* de Toledo. La operatividad del sistema de numeración decimal permitió incrementar la precisión de los cálculos, siendo un ejemplo la aproximación del número $\pi = 3.1415926535358979$ obtenida Al-Kasi (1380-1429), que era astrónomo del observatorio de Samarcanda. Otra obra de Al-Khwarizmi es Al-Jabr (~ 830), de cuyo título deriva la palabra Álgebra (**Figura 4**).

El *Liber abaci* (1202) de Leonardo de Pisa (1180-1250) (**Figura 6**) ayudó a implantar el sistema decimal indo-árabe en Occidente. Leonardo de Pisa fue más conocido como Fibonacci por ser hijo de Bonaccio, un mercader con negocios en el norte de África. Su juventud en el mundo árabe le familiarizó con las cifras indo-arábigas y le permitió estudiar los *Elementos* de Euclides. Su *Liber abaci* no está dedicado al aprendizaje del ábaco, sino al del cálculo con las cifras indias, explicando el funcionamiento de las operaciones, incluyendo las pruebas del 7, 9, 11, 13, la divisibilidad, las proporciones y la resolución de las ecuaciones de primer y segundo grados. Contiene reglas sobre compraventas y cambios de monedas.

Figura 6. Leonardo de Pisa (1180-1250).

Leonardo de Pisa no usó la numeración decimal en las fracciones, que llegó con el matemático francés François Viète (1540-1603), facilitando el progreso de la trigonometría y del cálculo con logaritmos. Viète dedicó últimos años de vida al estudio de las ecuaciones algebraicas, realizando importantes contribuciones.

Por tanto, a principios del siglo XVII, el sistema de numeración indo-arábigo estaba totalmente introducido en Europa occidental y con él se sabían representar tanto los números enteros como los racionales. Resultaban costosas en tiempo las operaciones de multiplicar y dividir realizadas con números altos, que pronto se verían en gran parte aliviadas mediante la invención de los logaritmos.

John Napier (1550-1617) fue el introductor de los logaritmos en su obra *Mirifici logarithmorum canoni descriptio* (1614) que le llevó más de veinte años de trabajo. Los logaritmos aplicados a los términos de una progresión geométrica la convierten en una progresión aritmética, permitiendo así transformar productos en sumas y cocientes en diferencias. Napier popularizó asimismo el uso de un punto para separar las partes entera y decimal de los números. También acuñó la palabra logaritmo —compuesta de las palabras griegas *logos* (razón) y *arithmos* (número)

Henry Briggs fue el primer *Savilian Professor* de Geometría de la Universidad de Oxford y le debemos una modificación de la definición de Napier de los logaritmos, que dio origen a los logaritmos de base diez. Recordemos que $y = \log x$ significa que $x = 10^y$ En 1624 Briggs publicó sus tablas de logaritmos con catorce cifras decimales, popularizando los nombres de *característica* y *mantisa* para designar las partes entera y decimal del logaritmo de un número.

La opinión del astrónomo Johannes Kepler (1571-1630) de que la invención de los logaritmos multiplicaba por dos la vida de los astrónomos, al permitirles doblar el número de cálculos que eran capaces de hacer, era compartida en otras ramas de la ciencia, lo que motivó el trabajo de muchos calculadores del siglo XVII para obtener tablas de logaritmos fiables y de gran precisión, lo que dependía del número de decimales obtenidos.

Las tablas de logaritmos facilitaron la composición de tablas precisas de funciones trigonométricas (*senos*, *cosenos*, *tangentes*) así como la resolución de triángulos planos y esféricos, lo que permitió elaborar cartas de navegar precisas con indicación de longitudes y latitudes que mejoraron la seguridad de los viajes a América.

AUTOMATIZACIÓN DEL CÁLCULO

La operatividad del sistema decimal de numeración permitió nuevos desarrollos físico-matemáticos, que permitieron abordar problemas más complicados. La complejidad creciente de los cálculos matemáticos puso de manifiesto la insuficiencia del cálculo manual apoyado en tablas logarítmicas y trigonométricas, lo que llevó al desarrollo de máquinas que realizaban los cálculos automáticamente.

Blas Pascal (1623-1662) ideó a los 18 años una máquina que representaba los números por ruedas dentadas y permitía la adición y la sustracción. Se la llamó *Pascalina* y en pocos años se vendieron cincuenta de estas máquinas. Fue una gran ayuda para su padre que era recaudador de impuestos. Gottfried Wilhelm Leibniz (1646-1716) mejoró la Pascalina diseñando una máquina capaz de realizar las cuatro operaciones decimales, que no se comercializó por ser de construcción más compleja.

Cuando comenzaba la tercera década del siglo XIX, el matemático inglés Charles Babbage (1791-1871) pensó en la necesidad de una máquina para la confección automática de tablas, evitando la gran cantidad de errores de las tablas matemáticas impresas. Durante sus once años en la cátedra *Lucasiana* de Matemáticas en la Universidad de Cambridge diseñó dos tipos de máquinas de calcular: la máquina de diferencias y la máquina analítica.

La máquina de diferencias estaba basada en el método de las diferencias finitas. Sólo pudo ensamblar la décima parte de las piezas previstas por la retirada del apoyo del gobierno británico. La parte ensamblada funcionó perfectamente. Babbage (**Figura 7**) mejoró el proyecto de la máquina de diferencias (**Figura 8**) con un nuevo diseño encargado por el Museo de la Ciencia de Londres; se construyó entre 1985 y 1991,

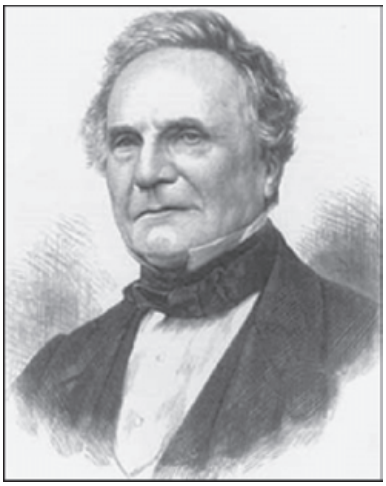


Figura 7. Charles Babbage (1971-1871).

su peso fue de tres toneladas y funcionó a la perfección, aunque la impresora no fue construida para abaratar los costes.

Babbage proyectó también una máquina de calcular que ejecutaría automáticamente órdenes contenidas en tarjetas perforadas. Se inspiró en ideas del mecánico Joseph-Marie Jacquard, quien en 1801 utilizó tablillas perforadas de madera para la realización automática de dibujos en telas, diseñando un telar que tejía los dibujos automáticamente mediante las órdenes almacenadas en las tarjetas. Babbage apellidó a su máquina analítica y no la pudo construir al negársele el apoyo financiero. La máquina analítica tenía un dispositivo

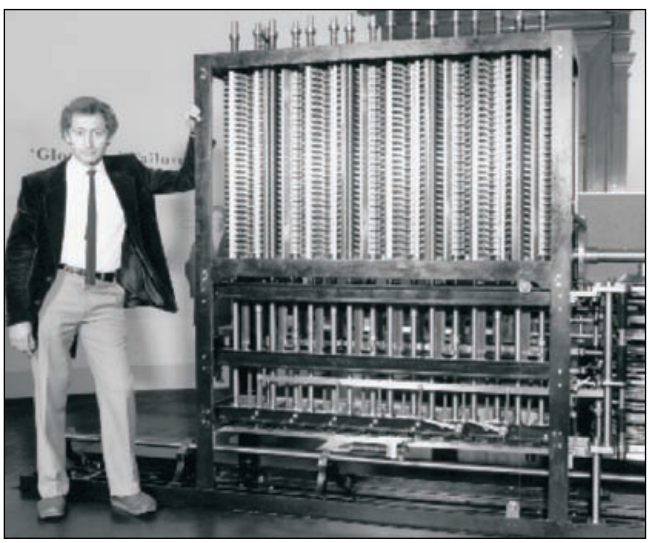


Figura 8. Reconstrucción de la máquina de diferencias de Babbage.

Figura 9. Ada Augusta Byron (1815-1852).

de entrada y salida (*input- output*), una serie de engranajes agrupados en dos partes, que actuaban independientemente y que fueron el precedente de la memoria y del procesador de los ordenadores modernos, y un mecanismo para imprimir los resultados. Babbage contó con la ayudante de investigación Ada Augusta Byron (1815-1852) (**Figura 9**), hija de Lord Byron, quien afirmaba que *la máquina analítica tejerá motivos algebraicos exactamente igual a como los telares de Jacquard tejen flores y hojas*. Además elaboró instrucciones codificadas en tarjetas perforadas para la introducción en la máquina analítica, cuando pasase del diseño a la realidad. En la Exposición Internacional de Londres de 1862 sólo se pudo exhibir su maqueta ante la imposibilidad de encontrar financiación, panorama que cambió en el siglo siguiente, cuando los gobiernos de los países desarrollados destinaron mucho dinero para la construcción de grandes máquinas de calcular.

La ideas contenidas en la máquina analítica de Babbage sugirieron al ingeniero y estadístico Hermann Hollerith utilizar tarjetas perforadas para codificar las letras del alfabeto y los dígitos por secuencias de perforaciones. En 1896 fundó la empresa *Hollerith's Tabulating Machine Company*, que se dedicó a la comercialización de máquinas de cálculo que tenían como base las tarjetas perforadas. Estas máquinas se utilizaron en la elaboración del censo de los Estados Unidos en 1890 y en 1900. Su compañía se fusionó con otras dos y desde 1924 se denominó IBM

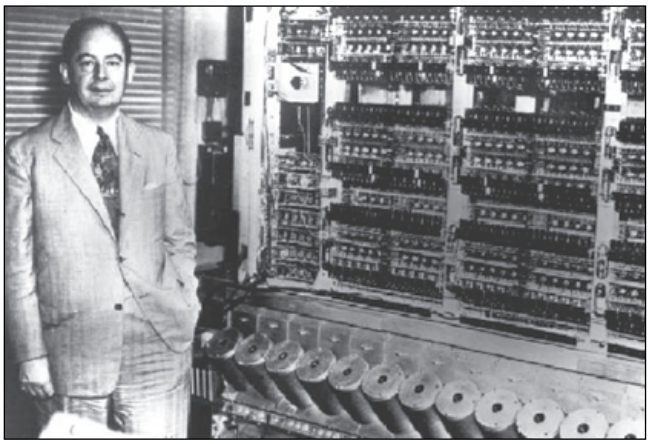


Figura 10. John von Neumann (1903-1957) junto a una parte del ENIAC.

(*International Business Machines*). En 1943, IBM construyó la máquina ASCC (*Automatic Sequence Controlled Calculator*), conocida como Harvard Mark I. Era una calculadora esencialmente mecánica, pero utilizaba relés y embragues accionados por electroimanes que, en gran parte, realizaba el sueño de Babbage. Pesaba cinco toneladas y podía calcular tablas de funciones trigonométricas, de logaritmos, de funciones exponenciales, etc. Las órdenes eran introducidas mediante tarjetas perforadas. Su construcción fue consecuencia de un proyecto entre la empresa IBM y la Universidad de Harvard, a través de su físico H. Aiken, que conocía bien los trabajos de Babbage.

A partir de 1940, el gobierno de los Estados Unidos inició la preparación de personal científico orientada a su posible intervención en la Segunda Guerra Mundial, confiando su dirección científica a los matemáticos John von Neumann (1903-1957) (**Figura 10**), del Instituto de Estudios Avanzados de Princeton, y a Norbert Wiener (1894-1964), del Instituto de Tecnología de Massa-chussets (MIT). Pero el aumento de las necesidades de cálculo a medida que avanzaba la guerra motivó contratar con la Escuela Moore para la construcción del ENIAC (*Electronic Numerical Integrator and Computer*) (**Figura 11**), máquina electrónica, precursora de los primeros ordenadores. Se terminó en 1945, siendo su principal usuario inicial el Laboratorio de Investigación Balística.

El ENIAC tenía unos 18.000 válvulas de radio y unos 1.500 relés telefónicos. Pesaba 30 toneladas y debía ser reparado continuamente, pues, por término medio, cada diez minutos se fundía una válvula. Su lector de tarjetas perforadas leía 2 tarjetas cada segundo. Después de la Guerra, el ENIAC se empleó en computación científica. Funcionó diez años y, probablemente, realizó más cálculos que toda la humanidad hasta entonces. Dedicó 70 horas de su trabajo a facilitarnos 2000 dígitos del número π. Sus padres, los físicos J. Presper Eckert (1919-1995) y John William Mauchly (1907-1980), fundaron en 1947 la primera compañía informática de la historia: *Eckert-Mauchly Computer Corporation* (EMCC), que comercializó el UNIVAC (*Universal Automatic Computer*), que fue el primer ordenador comercializado y que, siguiendo una idea de von Neumann, incluía programas para almacenamiento de datos.

El diseño de los ordenadores estaba prácticamente terminado. Luego llegaron las mejoras técnicas que tienen nuestros ordenadores y superordenadores. En 1947, los *Bell Telephone Laboratories,* fabricaron los primeros transistores, que reemplazaron a las válvulas y supusieron menor tamaño y consumo de corriente con una vida media casi ilimitada. El Premio Nobel de Física de 1956 fue para sus inventores, W.B. Shockley, J. Bardeen y W.H. Brattain. A finales de los años cincuenta, J. Kilby y R.N. Noyce consiguieron integrar todos los constituyentes de un circuito electrónico en la superficie de un chip, naciendo los circuitos integrados. En 1970, *Intel* fabricó el primer microprocesador. En el año 2000, J. Kilby recibió el Premio Nobel de Física por su invención del chip, compartido con Z. Alferov y H. Kroemer, quienes fueron premiados por

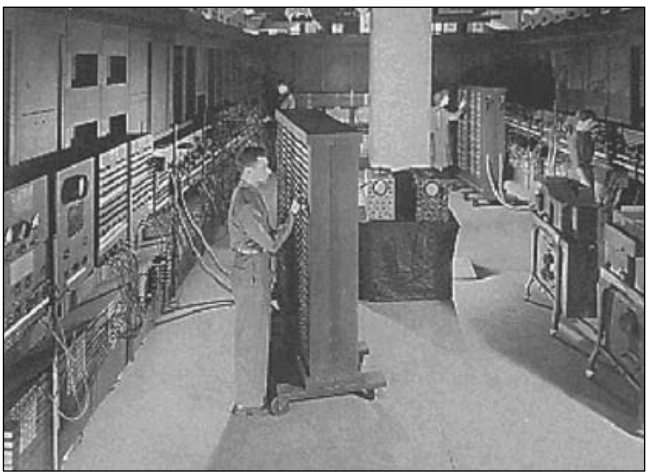


Figura 11. El ENIAC (Electronic Numerical Integrator and Computer).

sus trabajos en optoelectrónica, desarrollando la tecnología que hace posible la transmisión de señales por cable de fibra óptica.

CÓDIGOS CORRECTORES DE ERRORES

La información se almacena digitalmente, es decir en largas secuencias de ceros y unos, susceptible de enviarse a largas distancias a velocidad de la luz. Un pequeño error en el cambio de un 0 por un 1 durante la transmisión puede provocar la pérdida de una valiosa información.

En los años 1940, los *Bell Telephone Laboratories* crearon un centro de investigación matemática para la prevención y corrección de errores producidos en la transmisión de señales digitales. Entre los primeros matemáticos contratados por los laboratorios Bell se encontraban R.W. Hamming (1915-1998) y C. Shannon (1916-2001).

Hamming pensó completar bloques de bits antes de su transmisión con bits adicionales, de tal forma que los posible errores de transmisión pudieran ser detectados e incluso corregidos por la fuente receptora. Sugirió la utilización del *bit de paridad* para detectar errores, consistente en añadir a cada palabra un bit adicional igual a la suma módulo 2 de los siete bits anteriores. Si en la transmisión de la palabra completa a ocho bits se produce error entonces la máquina receptora detectará que hay un error al no cumplir esta condición de paridad, es decir que la suma módulo 2 de los siete primeros bits coincida con el octavo bit añadido. El bit de paridad no dice cual es el bit erróneo, lo que llevó a Hamming en 1950 a añadir cuatro bits adicionales que posibilitan la detección del bit erróneo cuando se produce un solo error en la transmisión. Vamos a explicarlo con un ejemplo. Imaginemos que se desea transmitir la palabra de 7 bits

$$d_1, d_2, d_3, d_4, d_5, d_6, d_7 = 0110101$$

Se trasladan los dígitos de esta palabra a las columnas que no sean potencia de 2 de la matriz 4×11 de la **tabla I**. La posición de una columna con dígito no nulo se escribe en columna en esa misma columna, previa la transformación de la posición a base dos, por ejemplo se puede observar que el dígito d_2 no es nulo y que está situado en la columna 5, siendo en el sistema binario $5=1\times2^0+0\times2^1+1\times2^2$. Pues bien, se indica que el dígito d_2 no es nulo escribiendo en la columna 5 los anteriores coeficientes de la representación binaria del número 5.

Las sumas módulo 2, de los elementos de cada fila nos da: $p_1, p_2, p_3, p_4 = 1,0,0,0$. Estos dígitos se escriben en las columnas que son potencia de dos, como se en en la **tabla II**.

En estas últimas columnas se repite el proceso hecho con las demás columnas, resultando, por ejemplo, que como $p_1=1$ es n nulo, está en la columna 1 y la expresión binaria de 1 es:

$$1=1\times2^0$$

se escriben los coeficientes de esta representación binaria en la primera columna. Nos quedará la matriz que se ve en la **tabla III**.

Es evidente que la suma módulo 2 de los elementos de cada fila dará 0. El número que se transmite es

		$d_1=0$		$d_2=1$	$d_3=1$	$d_4=0$		$d_5=1$	$d_6=0$	$d_7=1$
				1				1		1
					1					1
				1	1					
								1		1

Tabla I

$p_1=1$	$p_2=0$	$d_1=0$	$p_3=0$	$d_2=1$	$d_3=1$	$d_4=0$	$p_4=0$	$d_5=1$	$d_6=0$	$d_7=1$
				1				1		1
					1					1
				1	1					
								1		1

Tabla II

$$p_1,p_2,d_1,p_3,d_2,d_3,d_4,p_4,d_5,d_6,d_7 = 10001100101$$

Veamos ahora su utilidad: si se comete un error en la transmisión de este número, y se cambia, por ejemplo, el último digito por 0, entonces el receptor al recibir el número erróneo formará la matriz y obtendrá la **tabla IV**.

La suma módulo 2 de sus filas da 1,1,0,1, que, como es obvio, son las componentes de la columna d_7 cuando era correcta. Por tanto, la transformación

$$1\times 2^0+1\times 2^1+0\times 2^2+1\times 2^2=11$$

nos indica la columna en la que se cometió un error en la transmisión. El cambio del dígito de esa columna resuelve el problema. Este código de corrección de errores es de tipo *lineal*, pues genera dos matrices, la *matriz generadora del código*, que en el ejemplo sería la matriz 4×11 y *matriz de control* que en el ejemplo es la matriz obtenida al sumar módulo 2 las filas de la matriz generadora del código. La matriz de control con una sencilla transformación nos indica el dígito erróneo.

Hay muchos otros códigos de corrección de errores. Los *códigos de repetición* consisten en repetir dígitos. Si se triplica cada bit antes de su transmisión y se recibe una secuencia de la forma 111, la máquina la interpretará como correcta. Pero si se recibe una secuencia de la forma 001, es seguro que se habrá producido algún error. Puesto que es más probable que la secuencia correcta sea 000 que 111, podremos programar la máquina para que corrija el bit que es más probable que esté equivocado; en este caso, la máquina cambiará la palabra 001 por la palabra 000. Cada bit de información se completa con dos bits de control; este código de repetición triple es capaz de corregir un error en cada bloque de tres bits, pero triplica el coste de la transmisión.

Los códigos correctores de errores han tenido un papel destacado en los viajes espaciales, donde un

$p_1=1$	$p_2=0$	$d_1=0$	$p_3=0$	$d_2=1$	$d_3=1$	$d_4=0$	$p_4=0$	$d_5=1$	$d_6=0$	$d_7=1$
1				1				1		1
					1					1
				1	1					
								1		1

Tabla III

$p_1=1$	$p_2=0$	$d_1=0$	$p_3=0$	$d_2=1$	$d_3=1$	$d_4=0$	$p_4=0$	$d_5=1$	$d_6=0$	$d_7=0$
1				1				1		
					1					
				1	1					
								1		

Tabla IV

error de transmisión puede ocasionar la pérdida de importantes datos científicos. Por ejemplo, códigos diseñados por I.S. Reed y D.E. Muller en 1954 se utilizaron en 1972 para la transmisión de fotografías en blanco y negro de Marte cuando llegó la nave espacial Mariner 9. Los códigos diseñados por M. Golay en 1948 estaban basados en teoría de grupos y fueron utilizados en 1979 y 1981 para la transmisión de fotografías en color de Júpiter y Saturno por el Voyager.

LA SEGURIDAD EN LA TRANSMISIÓN EN LA RED

El origen de la criptología, arte de transmitir un mensaje cifrado para que sólo pueda ser entendido por el destinatario, es tan antiguo como la humanidad, pues el hombre siempre ha sentido la necesidad de proteger mensajes de posibles espías. Por Internet, por ejemplo, se envían diariamente grandes cantidades de datos que necesitan tratamientos criptográficos seguros.

En los métodos de clave privada, el emisor y el receptor acuerdan la clave de cifrado. El emisor aplica la clave al mensaje digital que desea enviar, lo que supone que no envía la secuencia de unos y ceros que digitaliza su mensaje sino otra secuencia, llamada mensaje cifrado, que es la recibida por el receptor, quien no tiene más que aplicar la clave inversa para recuperar así el mensaje original, operación que se llama descifrado. El momento del intercambio de la clave es inseguro, pues el espionaje intentará siempre hacerse con la clave.

En 1976, W. Diffie y M.E. Hellman propusieron hacer pública la clave de cifrado. Su idea es hacer pública una o varias claves con las cuales cualquier emisor puede enviar información cifrada al receptor, que puede ser Hacienda, un banco o una entidad comercial. La seguridad estriba en que sólo ese receptor debe disponer de una clave adicional con la que poder descifrar con facilidad el mensaje. Veamos un ejemplo conocido como método RSA.

La clave pública está formada por dos números, *N* y *a*, determinados así:

- *N* es el producto de dos números primos *p* y *q*, es decir $N = p \times q$.
- *a* es un divisor de la suma de 1 más un múltiplo de $(p-1)\times(q-1)$ es decir:

$$a \times b = 1 + m(p-1)(q-1)$$

- El número *b* de la igualdad anterior es la clave adicional que sólo debe conocer el receptor y que le permite descifran el mensaje dado que si *H* es menor que *N*

$$H^{a\times b} (\mathrm{mod}\, N) = H$$

Por tanto, el cifrado y descifrado se hace así:

- El mensaje a trasmitir es digital, por lo que se trata de un número *H* escrito en base dos, que, para facilitar esta exposición, podemos pensar que está escrito en base decimal.
- El emisor envía el número *V* resultado de la siguiente operación:

$$H^a \pmod N = V$$

- El receptor descifra el mensaje recibido mediante la transformación:

$$V^b \pmod N = H$$

La seguridad del cifrado RSA depende de la dificultad de descomponer el entero *N* en factores primos. Por tanto se deben elegir dos números primos muy grandes cuyo producto será el número ***N*.** Vamos a indicar un ejemplo, que no se podría aplicar en la práctica por ser pequeños los números primos utilizados, renunciando a la seguridad por facilitar su comprensión y tratarse de un ejercicio didáctico.

Los números primos p y q son 61 y 53, por lo que

$$N = 61 \times 53 = 3233.$$

El múltiplo elegido de $(p-1)\times(q-1) = 60 \times 52 =$ 3120 es

$$3120 \times 15 = 46800$$

Finalmente, el número

$$1 + 46800 = 46801$$

se descompone en producto de dos factores

$$46801 = 17 \times 2753$$

que nos da los números $a = 17$ y $b = 2753$.

Para enviar el número $H = 123$, cifrado con el método RSA, se efectúa el cálculo

$$123^{17} \pmod{3233} = 855$$

y se envía el número 855, que lo recibirá el receptor y lo descifrará así:

$$855^{17} \pmod{3233} = 123$$

recuperando el número que el emisor deseaba comunicar.

Es pues claro que el cifrado RSA es más seguro en cuanto resulte más difícil descomponer *N* en un producto de números primos, por lo que interesa seleccionar dos números primos *p* y *q* muy grandes cuyo producto nos dará el número *N*, pues si *N* tuviese unas 30 cifras y se intentase factorizar por divisiones sucesivas hasta su raíz cuadrada se tardarían 8000 horas con un ordenador capaz de realizar un millón de divisiones por segundo. No obstante, este resultado no debe hacernos sentirnos totalmente tranquilos respecto al tema de la seguridad en la red, pues hay diversos algoritmos de factorización muchísimo mas rápidos, como los de Fermat-Pollard (1974), Brilhard-Morrison (1975), de H.W. Lenstra (1985), o los métodos de criba, que reducen mucho la duración de la factorización de un número en ordenadores de sobremesa, y que, afortudamente, son poco conocidos por los piratas informáticos. En 1997, Peter Shor (**Figura 12**) diseñó un algoritmo para la factorización de enteros en producto de números primos en tiempo polinómico, caso de que su implementación pudiera realizarse en un *ordenador cuántico*. Este resultado implica que el método de cifrar mensajes RSA dejará de ser seguro en cuanto los ordenadores cuánticos sean una realidad física, pues entonces la factorización de un número grande se podrá hacer en muy poco tiempo.

Figura 12. Peter Shor (1959-).

La idea fundamental del método RSA, utilizar una función que sea poco costosa en tiempo de computación para el cifrado del mensaje, pero que su función inversa sea muy costosa en tiempo de computación, a menos que se disponga de una información adicional, subyace en los criptosistemas de clave pública, como el de T. ElGamal (1985) basado en el

criptosistema del logaritmo discreto y el de A.J. Menezes y S.A. Vanstone (1993) basados en la aritmética de las curvas elípticas.

BIBLIOGRAFÍA

1. Bayer, Pilar: ¿*Para qué sirven hoy los números*? en Horizontes Culturales. Real Academia de Ciencias Exactas, Físicas y Naturales. Real Academia de Ciencias Exactas, Físicas y Naturales y Espasa Calpe (2002) . ISBN: 84-670-0132-2. Páginas 87–107.

2. Boyer, Carl B.: *Historia de la Matemática.* Alianza Editorial, 1999.

3. Cardwell, Donald: *Historia de la tecnología*. Alianza Universidad, 1994.

4. Flegg, Graham: *Numbers Through the Ages.* The Open University. MacMillan, 1989.

5. García Barreno, Pedro (editor): *La Ciencia en tus Manos*. Espasa Fórum. Espasa Calpe, 2000.

6. Ifrah, Georges: *Historia Universal de las Cifras*. Espasa Fórum. Espasa Calpe, 1997.

7. Morgan, Samuel, P.: Richard Wesley Hamming (1915-1998). *Notices AMS*, v. 45, n. 8, 972-982 (1998).

8. Perera Domínguez, Manuel: ENIAC, matemáticas y computación científica. *La Gaceta de la Real Sociedad Matemática Española*, v. 2, n. 3, (1999) 495-518.

9. Shor, Peter: Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM Journal of Computing* 26, 1484-1509 (1997).

10. Singh, Simon: *Los códigos secretos*. Pequeña gran historia. Editorial Debate, 2000.

11. von Neumann, John: *El ordenador y el cerebro.* Bon Ton, 1958.

12. Yan, Song Y.: *Number Theory for Computing*. Springer, 2000.