¿PARA QUÉ SIRVEN HOY LOS NÚMEROS?

PILAR BAYER ISANT
Real Academia de Ciencias

INTRODUCCIÓN

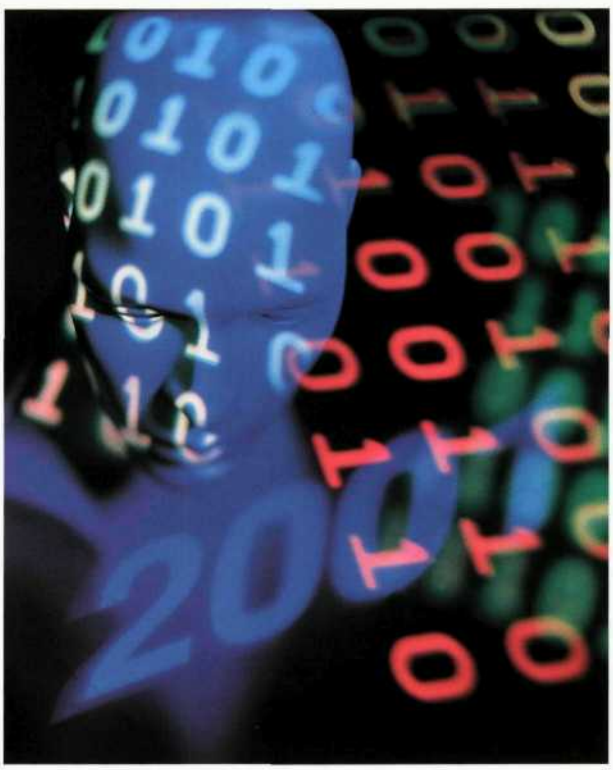
El saber matemático y el potencial de cálculo de las civilizaciones forman parte de su historia. Los conocimientos matemáticos forjados a través de siglos repercuten en avances científicos y tecnológicos de apreciable impacto. Sin embargo, y a pesar del carácter universal inherente a las matemáticas, no es extraño que se soslaye el papel de esta ciencia en la historia del pensamiento humano. Carentes inexplicablemente de todo eco social, los logros matemáticos persisten veladamente y no suelen contabilizarse en el haber de los pueblos. A lo sumo, se adscriben a ciertas minorías que tomaron gusto a lo difícil. Pero, bien pensado, conocer con precisión el movimiento de los astros, lanzar proyectiles, diseñar sistemas de votación ponderados, elaborar modelos de virus son actividades humanas que requieren el ineludible concurso de las matemáticas.

La llamada sociedad de la información conlleva asimismo el uso de herramientas matemáticas específicas. En las últimas décadas, las nuevas tecnologías se han afianzado en todos los ámbitos: comercio, administración, ciencias, medicina, ciencias sociales. Continuamente, los medios de comunicación ponen a nuestro alcance noticias relativas a telefonía digital, televisión digital, radio digital. Para bien o para mal, las tecnologías digitales inciden apreciablemente en los mercados financieros, por lo que pocos escapan a su influencia.

Dado que *digital* es un adjetivo derivado del sustantivo latino *digitus* (dedo) y que la primera calculadora usada por el *Homo sapiens* han sido los dedos de la mano, la mera presencia de este término transluce un componente matemático.

EL SISTEMA DE NUMERACIÓN BINARIO

Por regla general, elaboramos los cálculos de la vida cotidiana de acuerdo con el denominado *sistema de numeración decimal.* Nuestro sistema de numeración consta de diez dígitos: 1, 2, 3, 4, 5, 6, 7, 8, 9, 0, uno de los cuales



es el 0. Es de posición, puesto que el valor de cada cifra depende del lugar que ocupa. Y, en él, diez unidades forman una decena, diez decenas forman una centena, etc. La ausencia de unidades de un orden determinado se indica por medio del 0, con lo cual números como 37, 370, 703 indican cantidades distintas. Aunque hoy nadie cuestiona la naturalidad de esta manera de denotar los números, lo cierto es que su derivación y evolución han sido lentas.

Con el sistema de numeración decimal representamos no sólo los números *naturales,* sino también los números *enteros,* los números *racionales,* los números *reales* y los números *complejos.* Recordemos las notaciones habituales para estos conjuntos de números, así como su descripción:

$$\mathbb{N} = \{1, 2, 3, ...\},\ \mathbb{Z} = \{0, \pm 1, \pm 2, \pm 3, ...\},$$

$$\mathbb{Q} = \{\, a / b\colon a, b \text{ enteros}, b \neq o\},$$

$$\mathbb{R} = \{n + 0.d_1d_2d_3...\colon n \text{ entero}, 0 \leq d_i \leq 9\},$$

$$\mathbb{C} = \{\, a + bi\colon a, b \text{ reales}, i = \sqrt{-1}\,\}.$$

A pesar de la operatividad del sistema de numeración decimal, las tecnologías digitales suelen basarse en el denominado *sistema de numeración binario*. El sistema de numeración binario consta únicamente de dos dígitos: 0, 1. Es de posición. Y, en él, cada dos unidades de un mismo orden constituyen una unidad del orden superior. Los dígitos binarios permiten representar *todos* los números. Los siguientes ejemplos muestran la expresión binaria del número natural 41, del número racional 1/7, así como de los números reales raíz cuadrada de 2 y «pi»:

$$41 = 1 + 2^3 + 2^5 = 101001_2,$$
$$1/7 = 0.001001_2,$$
$$\sqrt{2} = 1.0110101000001001\ldots_2,$$
$$\pi = 11.0010010000111111\ldots_2.$$

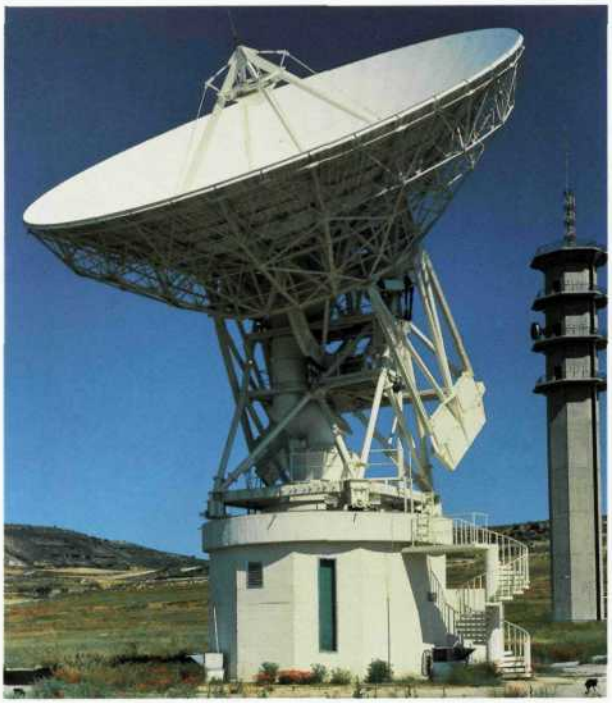
Atendiendo a tonalidades de grises, colores, o a frecuencias de sonidos, toda información de tipo gráfico o acústico es susceptible de ser digitalizada. Es decir, convertida en una sucesión de números representables a su vez por medio de ceros y de unos.

La implantación del sistema binario como instrumento idóneo para codificar la información se debe a su simplicidad. La simulación física del sistema binario es particularmente sencilla, bastando un soporte material susceptible de dos estados. Así, el 1 puede asimilarse a la presencia de un impulso electromagnético y el 0, a su ausencia. De esta forma, los dígitos binarios se convierten en la unidad de información básica o *bit*–acrónimo de *binary digit*–. Las tecnologías digitales codifican una conversación, una sinfonía, una película o un partido de fútbol en una sucesión de ceros y unos, idónea para ser transmitida a la velocidad de la luz y a largas distancias.

ORÍGENES DE LA BASE DOS

El origen de las cifras 0, 1 es muy desigual. En cierta forma, el 1 es la primera cifra utilizada en todos los sistemas de numeración y el 0, la más tardía.

El hombre prehistórico se valía ya de trazos verticales para contar, como han puesto de manifiesto astas de reno marcadas con muescas procedentes del Paleolítico superior. A su vez, unía varios trazos verticales para facilitar su recuento. Notemos que ningún motivo obliga a unir tales trazos de diez en diez. Podemos, con igual fortuna, utilizar cualquier cantidad de ellos: cinco, diez, doce, dos. La cantidad acordada con este fin constituye la *base* del sistema de numeración.



El sistema de numeración egipcio usado en la escritura jeroglífica (hacia 3000 a. C.) era un sistema de base 10, de siete cifras y carecía de 0. Para designar las primeras potencias de diez, *uno* era representado por un palo vertical; *diez*, por un asa; *cien*, por un caracol; *mil*, por una flor de loto; *diez mil*, por un dedo doblado; *cien mil*, por un renacuajo; y un *millón*, por un hombre con los brazos en alto. Mediante la repetición conveniente de estos símbolos, los egipcios escribían todos los números naturales. El sistema de numeración egipcio no era de posición pues el orden de las cifras de un número escrito resultaba irrelevante.

Para sumar dos cantidades, los egipcios reunían los guarismos correspondientes, sustituyendo diez unidades de un determinado orden por la unidad del orden superior. Así, diez asas equivalían a un caracol, diez renacuajos equivalían a un hombre con los brazos en alto. El doblar una cantidad era igualmente sencillo: cinco asas y un palo vertical multiplicados por dos equivalían a un caracol y dos palos verticales. Pero, ¿cómo proceder en la multiplicación y división de cantidades mayores?

Los egipcios resolvieron el problema de la multiplicación de una forma espléndida. Puesto que la única multiplicación sencilla era la multiplicación por 2, redujeron cualquier multiplicación de números naturales a una sucesión de sucesivas multiplicaciones por 2. Para ello, escribían el multiplicando como suma de potencias de 2 y doblaban el multiplicador tantas veces como fuera necesario, de acuerdo con la descomposición del multiplicando. Veamos un ejemplo, escrito en nuestra notación:

$$41 \times 59 = (2^0 + 2^3 + 2^5) \times 59 = 59 + (0 \times 118) +$$
$$+ (0 \times 236) + 472 + (0 \times 944) + 1888 = 2419.$$

A pesar de que carecían del 0, en la constatación de los egipcios de que todo número natural es expresable como suma de potencias de dos se aprecia un precedente del sistema de numeración binario.

La escritura jeroglífica egipcia evolucionó en las escrituras hierática y demótica. A la hora de representar gráficamente los números, estas escrituras evitaban la repetición de los símbolos a base de incrementar el número de sus guarismos y, por tanto, a costa de incrementar la dificultad nemotécnica de su escritura.

La fuente más valiosa para el conocimiento de la matemática egipcia la constituyen las inscripciones de sus monumentos y unos pocos papiros, algunos de los cuales poseen más de 3000 años de antigüedad.

En 1858, el egiptólogo Henry Rhind adquirió en un mercado de Luxor un papiro en escritura demótica, de 6 metros de largo por 30 centímetros de ancho, todo él de contenido matemático. Además de abundantes reglas de cálculo, el Papiro Rhind contiene una colección de 84 problemas. En ellos, los egipcios se muestran familiarizados con el cálculo de áreas, volúmenes y con el manejo de fracciones de numerador uno –las denominadas fracciones egipcias–. Según consta en el documento, el escriba Ahmes lo copió (hacia 1650 a. C.) de material más antiguo, procedente del Imperio Medio (entre el 2000 y el 1800 a. C.). Se ha especulado que la fuente intelectual del Papiro Rhind podría muy bien ser Imhotep, legendario médico y arquitecto del faraón Zoser que dirigió la construcción de la pirámide que lleva su nombre. En la actualidad, el Papiro Rhind se conserva en el Museo Británico.

ORÍGENES DE LOS SISTEMAS DE NUMERACIÓN DE POSICIÓN

Alrededor del año 2400 a. C., Mesopotamia contaba ya con sistemas de numeración de posición. El sistema de numeración sumerio era mucho más elaborado que el egipcio. Se trataba de un sistema de numeración de posición, de base 60, que, en un principio, careció del 0.

Los sistemas de numeración de posición permiten escribir los números con una gran economía de guarismos. El sistema de numeración sumerio poseía únicamente dos cifras: un clavo vertical denotaba el 1; una cuña horizontal denotaba el 10. La ausencia de unidades de un determinado orden se representaba mediante un espacio vacío, lo cual era frecuente fuente de errores. De este modo, dos clavos verticales seguidos de un espacio en blanco y de dos cuñas horizontales podían denotar tanto el número $(2 \times 60) + (2 \times 10) = 140$ como el número $(2 \times 60^2) + (2 \times 10) = 7220$. Para evitar estos inconvenientes, alrededor del 200 a. C. empezaron a usarse dos clavos inclinados para indicar que faltaban las unidades de un determinado orden intermedio. Este «0» mesopotámico constituye un precedente remoto de nuestro 0.

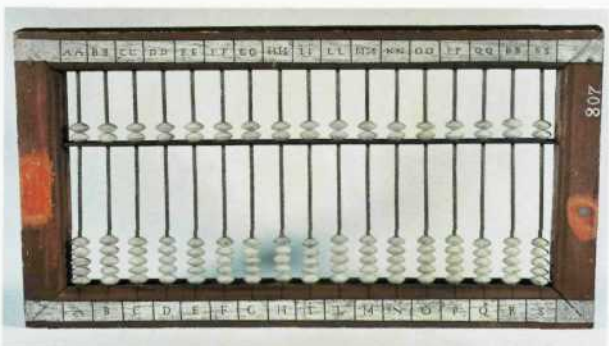
La matemática mesopotámica nos ha llegado a través de una gran cantidad de tablillas de arcilla grabadas en escritura cuneiforme. Una de las más célebres es la conocida con el nombre Plimpton 322, que se conserva en la Universidad de Columbia. Su contenido equivale a quince ternas pitagóricas o soluciones de la ecuación $X^2 + Y^2 = Z^2$. Si denotamos por *a, b* los catetos de un triángulo rectángulo y por *c* su hipotenusa, las entradas de las tres primeras columnas de la tablilla corresponden a las cantidades c^2/a^2, *a, b*, respectivamente. En una columna cuarta de la tablilla se aprecia la numeración de sus quince filas. La tablilla Plimpton 322 data de la época de Hammurabi (hacia 1800 a. C.) y, aunque se ignora su finalidad, pone de manifiesto la temprana familiarización de un matemático sumerio con el teorema de Pitágoras (h. 540 a. C.), mucho antes del establecimiento de las comunidades pitagóricas.

BREVE HISTORIA DEL CERO

El sistema de numeración griego era alfabético. En un contexto matemático, los griegos asignaban a cada letra del alfabeto un valor numérico. El sistema de numeración romano se basaba en principios parecidos. Tanto el sistema de numeración griego como el romano eran muy inoperantes a la hora de calcular. Su persistencia a lo largo de los siglos se debe a que los cálculos se efectuaban de forma mecánica, empleándose los números únicamente para anotar los resultados. De todos los instrumentos de cálculo utilizados –piedras *(calculi)*, cuentas, cuerdas–, el principal fue el *ábaco*.

Los ábacos constan de un marco en el que se insertan alambres con bolas engarzadas, o de cualquier otro mecanismo equivalente, apto para la visualización de las operaciones aritméticas. Los abaquistas, o personas especialmente entrenadas en su uso, no necesitan conocer el porqué de los movimientos de las bolas para efectuar una operación, basta con que sean hábiles en su manejo. En nuestros días, los ábacos todavía son usados en Oriente.

Los astrónomos griegos siguieron utilizando los sistemas de numeración de posición mesopotámicos de base 60. Tolomeo de Alejandría (h. 90 - h. 160) empleó un sím-



Ábaco chino.

bolo parecido a la letra griega ómicron para dar a entender que faltaban las unidades de un determinado orden. En el libro primero de su *Sintaxis matemática,* obra más conocida por el nombre árabe de *Almagesto* (que significa «el más grande»), Tolomeo construye una tabla de cuerdas de arcos desde $^1/_2°$ hasta 180°, de medio en medio grado, equivalente a una tabla actual de senos de ángulos de $^1/_4°$ hasta 90°, de cuarto en cuarto grado. El *Almagesto* se convirtió en el libro de referencia básico para los astrónomos durante más de mil años.

Tolomeo introdujo en su *Geografía* el sistema de longitudes y latitudes que todavía usamos hoy para fijar las coordenadas geográficas; sin embargo, en su época no se conocía ningún sistema para determinar longitudes geográficas. Según Carl C. Boyer, un cálculo de Tolomeo basado en una estimación errónea del radio de la Tierra efectuada por Posidonio (h. 135 - h. 50 a. C.) habría inducido a Cristóbal Colón a subestimar la distancia de Europa a la India navegando hacia el Oeste.

Tolomeo de Alejandría (h. 90 - h. 160 d. C.) consultando el astrolabio.

Euclides de Alejandría (s. III a. C.) demostró que existen infinitos números primos.

PROTOHISTORIA DE LA TEORÍA DE NÚMEROS

Los tratados más antiguos de la matemática griega que han llegado a nuestros días son las obras de Euclides (h. 315 - h. 225 a. C.). Euclides, formado probablemente en Atenas, no hacía especial hincapié en los aspectos prácticos de las matemáticas. Durante la dinastía de los Lágidas ocupó el cargo de profesor del Museo de Alejandría, donde escribió su obra más famosa, los *Elementos,* concebida como un libro para el aprendizaje de la geometría. La obra consta de trece libros. El material de los dos primeros se supone que procede en parte de los pitagóricos. Los Libros III y IV podrían estar tomados de Hipócrates (h. 430 a. C.), autor de unos *Elementos de geometría* que se han perdido. De Hipócrates sabemos por Aristóteles que, siendo mercader, perdió todo su dinero en Bizancio debido a un fraude; sin embargo, nunca consideró este hecho como una desgracia, pues a consecuencia de él pudo dedicarse al cultivo de la geometría. Hipócrates se habría dedicado al problema de cuadraturas de lúnulas, con la esperanza de poder un día cuadrar el círculo.

Tres de los trece libros de los *Elementos* están dedicados al estudio de los números naturales. En los Libros VII, VIII y IX, Euclides trata cuestiones básicas sobre divisibilidad, máximo común divisor y mínimo común múltiplo; describe el algoritmo para la determinación del máximo común divisor que aún usamos en nuestros días y define los conceptos de número primo, número perfecto, números amigos, etc., ya conocidos por los pitagóricos. Recordemos que un número natural se denomina *primo* si ca-

rece de divisores distintos de 1 y él mismo. Los primeros números primos son 2, 3, 5, 7, 11, 13, 17, 19. Euclides demuestra que existen infinitos números primos: «existen más números primos que en cualquier cantidad de números primos fijada de antemano». El lenguaje de los *Elementos* es preferentemente geométrico; así, ante una igualdad $n = mk$, Euclides nos dice que «n está medido por m».

Eratóstenes de Cirene (h. 284 - h. 202 a. C.), astrónomo, matemático y bibliotecario del museo, es recordado por haber ideado un procedimiento que permite obtener todos los números primos por debajo de una cantidad dada: la denominada criba de Eratóstenes. También realizó una medida del radio de la Tierra mucho más aproximada que la de Posidonio.

En relación con el estudio de los números, la Escuela de Alejandría produjo en el llamado segundo periodo (hacia el siglo III) una obra singular: la *Aritmética* de Diofanto. La *Aritmética* consta de una colección de 150 problemas relativos a propiedades de los números. Los números son tratados por sus propiedades intrínsecas, sin referencia alguna a medidas de grano, dimensiones de campos o unidades monetarias (salvo en un problema de mezclas, relativo al precio de unos vinos). En general, Diofanto se limitaba a ofrecer soluciones particulares exactas de los problemas, sin pretender ningún método general. Puesto que el contenido de la obra es eminentemente aritmético y en ella no se emplean métodos geométricos, Diofanto está más próximo a la matemática mesopotámica y a la matemática de los pitagóricos que a la matemática griega del primer periodo de la Escuela de Alejandría. Por ejemplo, en el célebre problema II-8, se ocupa de las ternas pitagóricas: «descomponer un cuadrado dado en suma de dos cuadrados».

Otros problemas de la *Aritmética* conducen a la resolución de ecuaciones de la forma:

$$X^2 = 1 + 30\,Y^2, \text{ o bien } X^2 = 1 + 26\,Y^2.$$

En honor de Diofanto de Alejandría, las ecuaciones polinómicas de coeficientes enteros (o racionales) de las que se buscan sus soluciones enteras (o racionales) reciben el nombre de ecuaciones *diofánticas*.

Orígenes del sistema de numeración decimal

La cuna del sistema de numeración decimal y de las cifras que empleamos en la actualidad se halla en la civilización india. Los matemáticos indios lograron reunir en un único sistema de numeración las ventajas que hemos apreciado en distintos sistemas de numeración de la Antigüedad. Su sistema de numeración es de posición, de base decimal y posee una cifra para cada uno de los diez numerales básicos, incluido el 0.

El matemático y astrónomo indio Aryabhata (n. 476) escribió alrededor del año 499 el *Aryabhatiya*, una obra descriptiva, versificada en 123 estrofas, en las que se suministran abundantes reglas de cálculo. El autor procede al cálculo de raíces cuadradas, raíces cúbicas, maneja progresiones aritméticas y proporciona fórmulas para el cálculo de áreas y volúmenes, aunque no todas correctas. En el *Aryabhatiya* se encuentra una tabla de senos de ángulos menores de 90° para 24 intervalos angulares de $3\,{}^{3}/_{4}{}^{\circ}$ cada uno. De su afirmación «de un lugar a otro, cada uno es diez veces el que le precede» se desprende que Aryabhata estaba familiarizado con el uso del sistema de numeración decimal de posición.

En cuanto a la procedencia de los guarismos que empleamos para la representación de los números, se han formulado hipótesis diversas. Al parecer, nuestras cifras derivan de las nueve primeras cifras *brahmi*, de los siglos III-II a. C., tras haber experimentado múltiples transformaciones. En la India se origina asimismo el guarismo del cual deriva nuestro 0: un huevo de oca. El primer testimonio epigráfico indio del 0 es una inscripción del año 876. La forma actual de las cifras no quedaría fijada en Occidente hasta el siglo XV, tras la invención de la imprenta.

Un siglo posterior a Aryabhata encontramos al matemático Brahmagupta (598 - 665), en cuya obra aparecen sistematizadas no sólo las reglas de cálculo del sistema decimal con el 0, sino también el cálculo con números negativos. Brahmagupta presenta muchas semejanzas con Diofanto de Alejandría. El álgebra de ambos es sincopada; es decir, las operaciones y las incógnitas se representan abreviando las palabras correspondientes.

El sistema de numeración decimal de posición y con el 0 fue usado por el matemático y astrónomo Bhaskara (1114 - 1185), autor del *Lilavati*, obra que contiene una recopilación de problemas cuya resolución conlleva el manejo de ecuaciones lineales, cuadráticas, cálculo de áreas, progresiones aritméticas, progresiones geométricas, cálculo de raíces y ternas pitagóricas. El nombre del tratado corresponde al de la hija de Bhaskara.

La transmisión a Occidente de los numerales indios

Cuenta una leyenda que el califa de Bagdad Al-Mamun (809 - 833), tras haber dialogado en sueños con Aristóteles, decidió traducir al árabe todas las obras griegas a su

Las cifras *nagari* del siglo XI.

Leonardo de Pisa, Fibonacci (1180-1250).

alcance. De esta forma, el *Almagesto* de Tolomeo y los *Elementos* de Euclides fueron traducidos al árabe en el siglo IX.

La *Casa de la Sabiduría,* fundada por los califas Harun al-Rasid y Al-Mamun se convirtió en el siglo IX en la heredera del Museo de Alejandría. Muhammad bin Musa al-Khwarizmi (m. hacia 845) fue el matemático más destacado de aquella institución. Su texto *De numero indorum,* escrito alrededor del 820, sirvió para consolidar las cifras indo-arábigas, el 0, el sistema de numeración de posición de base 10, así como sus reglas de cálculo. El original árabe de dicho texto se ha perdido; tampoco queda clara la autoría de la traducción latina, habiéndose atribuido ésta a Adelardo de Bath y a Juan de Sevilla. En cualquier caso, parece indudable que la traducción latina se realizó en nuestra Península, por lo que España tuvo un papel relevante en la transmisión del cálculo a Occidente. La versión más antigua conservada del texto mencionado de Al-Khwarizmi es del siglo XII y procede de la Escuela de Traductores de Toledo.

Citemos asimismo que Abu-l-Welfa (940 - 998) tradujo del griego la *Aritmética* de Diofanto, adelantándose a las traducciones latinas de la obra, que no verían la luz hasta el siglo XVI.

El hecho de poseer un sistema de numeración operativo permitió incrementar la precisión de los cálculos, así como conservar los resultados parciales, lo cual facilitaba enormemente la comprobación de los resultados. La aproximación del número $\pi = 3{,}14159265358979$ calculada por Al-Kasi (1380 - 1429) da cuenta de las posibilidades que el nuevo sistema de numeración ofrecía. Al-Kasi trabajó en el observatorio de Samarcanda. Su récord en el cálculo de π no sería emulado hasta finales del siglo XVI. (La frase «How I want a drink alcoholic, of course, after the heavy lectures involving quantum mechanics» sirve de recurso nemotécnico, puesto que el número de letras de cada palabra corresponde a los sucesivos dígitos de π calculados por Al-Kasi.)

Leonardo de Pisa (1180 - 1250), más conocido por Fibonacci (hijo de Bonaccio), era hijo de un mercader que poseía negocios en el norte de África. Su juventud transcurrió en gran parte en el mundo árabe, en donde Fibonacci aprendió el cálculo con las cifras indo-arábigas y estudió los *Elementos* de Euclides. En 1202, Fibonacci dio a conocer su *Liber abaci,* verdadero compendio de las matemáticas medievales. En contra de lo que su título sugiere, el *Liber abaci* no estaba dedicado al aprendizaje del ábaco, sino al del cálculo con las cifras indias. Fibonacci explica el funcionamiento de las operaciones, así como las pruebas del 7, 9, 11, 13. Estudia propiedades de divisibilidad, reglas sobre compraventas, cambios con las monedas entonces en curso, proporciones, y resuelve ecuaciones de primer y segundo grados. Con todo, en el cálculo con fracciones, Fibonacci sigue haciendo uso de las fracciones egipcias. Se necesitaría más de un siglo para que las ventajas del sistema de numeración de posición se hicieran extensivas al cálculo con números racionales. El *Liber abaci,* anterior a la invención de la imprenta, sirvió de base para la formación de maestros y alumnos de la escuela toscana durante más de tres siglos, aunque no fue impreso hasta el siglo XIX. En la edición de Boncompagni, el *Liber abaci* poseía más de cuatrocientas páginas.

El texto de Luca Pacioli (1445 - 1514) *Summa de arithmetica, geometrica, proportioni et proportionalita* sería el sucesor del *Liber abaci.* La *Summa* contenía una recopilación de material perteneciente a aritmética, álgebra, geometría euclídea elemental y contabilidad. A partir de la segunda mitad del siglo XV, se imprimió un gran número de textos de aritmética, dirigidos principalmente a usos comerciales y escritos ya en lenguas vernáculas.

El matemático francés François Viète (1540 - 1603) hizo una encarecida defensa del uso de las fracciones decimales en lugar de las sexagesimales. Su implantación definitiva contribuyó enormemente al progreso de la trigonometría e hizo posible el cálculo con logaritmos. Durante los reinados de Enrique III y de Enrique IV, Viète tuvo un destacado papel como criptoanalista. Tras caer políticamente en desgracia, dedicó los últimos años de su vida al cultivo de la matemática, y realizó importantes contribuciones al estudio de las ecuaciones algebraicas.

LA INVENCIÓN DE LOS LOGARITMOS

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. Las operaciones de multiplicar y dividir realizadas con números altos, costosas en

tiempo, se verían en gran parte aliviadas mediante la invención de los logaritmos.

En sus reflexiones acerca de los términos de una progresión geométrica formada por las potencias enteras de un número dado, el matemático escocés John Napier (1550 - 1617), barón de Merchiston, observó que si este número era muy próximo a uno, entonces los términos de la progresión estaban muy próximos los unos de los otros. Tomando $1 - 10^{-7} = 0.9999999$ y escribiendo $n = 10^7 (1 - 10^{-7})^k$, Napier asignó a n el índice k, denominándole el *logaritmo* de n. La palabra logaritmo –compuesta de las palabras griegas *logos* (razón) y *arithmos* (número)– fue acuñada por el propio Napier. Los logaritmos aplicados a los términos de una progresión geométrica la convertían en una progresión aritmética.

Tras un trabajo de más de veinte años, en 1614 Napier publicó el tratado *Mirifici logarithmorum canonis descriptio,* con sus consiguientes tablas. Esta obra popularizó asimismo el uso de un punto para separar la parte entera de la parte decimal de los números. Posteriormente, otros autores utilizarían las comas, con idéntica finalidad.

Henry Briggs, el primer *Savilian Professor* de geometría de la Universidad de Oxford, modificó ligeramente la definición de Napier de los logaritmos, dando lugar a los logaritmos vulgares o de base 10: $y = \log x$ expresa que $x = 10^y$. Briggs publicó sus tablas de logaritmos con catorce cifras decimales en 1624; los nombres *característica* y *mantisa* para designar la parte entera y la parte fraccionaria del logaritmo de un número proceden, asimismo, del libro de Briggs.

Las tablas de logaritmos permitieron reemplazar las complicadas operaciones de multiplicación y división por las sencillas operaciones de suma y resta, respectivamente. El astrónomo Johannes Kepler (1571 - 1630) opinaba que la invención de los logaritmos multiplicaba por dos la vida de los astrónomos, puesto que les permitía doblar el número de cálculos que eran capaces de hacer. El deseo de disponer de tablas de logaritmos extensas y fiables hizo necesario el trabajo de muchos calculadores a lo largo de todo el siglo XVII.

Evangelista Torricelli (1608 - 1647), matemático y físico nacido en Florencia que ha pasado a la historia por la invención del barómetro, era discípulo de Galileo Galilei (1564 - 1642). Bajo la influencia de su maestro, Torricelli estudió las trayectorias parabólicas que siguen los proyectiles disparados desde un punto fijo con velocidad inicial constante pero con ángulo de tiro variable. Sus investigaciones prepararon el advenimiento del cálculo diferencial.

Uno de los problemas estudiados por Torricelli consistía en determinar el área encerrada por la curva $y = \log x$, su asíntota y una ordenada, así como el volumen obtenido al girar esta superficie alrededor del eje Ox. Ésta es la primera representación gráfica que se tiene de la *función logaritmo.* Hasta entonces los logaritmos no habían sido considerados como una función, sino solamente como un recurso de cálculo. La función logaritmo posee por función inversa la *función exponencial.* Ambas funciones son crecientes, pero la función exponencial crece mucho más aprisa que la función logaritmo. (Un crecimiento de los beneficios de *tipo exponencial* es altamente preferible a un crecimiento de *tipo logarítmico).* Las funciones polinómicas presentan un orden de crecimiento intermedio entre el logarítmico y el exponencial –unas cuantas pruebas en una calculadora científica no dejarán lugar a dudas.

Las tablas de logaritmos y de funciones trigonométricas *(senos, cosenos, tangentes)* resultaron de gran valor para mejorar la seguridad de los viajes de ultramar al permitir una aproximación mejor del cálculo de las coordenadas. Cartas de navegar con indicaciones de longitudes y latitudes se popularizaron en el mundo occidental a partir del siglo XVI y, a partir del XVII, los cálculos relativos a la resolución de triángulos se beneficiaron enormemente de la invención de los logaritmos.

DE LAS TERNAS PITAGÓRICAS AL «TEOREMA» DE FERMAT

Pierre de Fermat (1601 - 1665), abogado y miembro del consejo local del Parlamento de Toulouse, cultivaba las matemáticas por afición. Estudió con ahínco la *Aritmética* de Diofanto, gracias a la edición grecolatina que de ella hiciera Claude Gaspard de Bachet (1591 - 1639), en el año 1621. Las reflexiones de Fermat sobre distintos problemas de Diofanto, enviadas a sus coetáneos en forma de problemas, promovieron el interés por la teoría de números en Occidente. Se trataba de investigaciones relativas a las propiedades de los números enteros, desprovistas de toda utilidad aparente, y que se practicaban como entretenimiento intelectual.

Por medio de su método del «descenso infinito», Fermat probó que ningún cubo descompone en suma de dos cubos; es decir, que la ecuación $X^3 + Y^3 = Z^3$ carece de soluciones no triviales en los enteros –en contraposición al caso de las ternas pitagóricas, o sea del exponente 2.

Fermat se sintió asimismo fascinado por los números primos. Los matemáticos chinos sabían que si p es un número primo, $2^p - 2$ es múltiplo de p. Observando muchas expresiones de la forma $a^p - a$, para distintos valores de a y de p, Fermat dedujo que dicha cantidad sería siempre un múltiplo de p. Tal afirmación, conocida como el «pequeño teorema de Fermat», sería probada por Gottfried Wilhelm Leibniz (1646 - 1716). Fermat dedujo asimismo que todo primo de la forma $p = 4k + 1$ sería expresable como suma de dos cuadrados como, por ejemplo, $5 = 1^2 + 2^2$, $41 = 4^2 + 5^2$.

Muchas de las afirmaciones de Fermat acerca del comportamiento de los números fueron probadas (y algunas, desmentidas) por Leonhard Euler (1707 - 1783), Adrien Marie Legendre (1752 - 1833) y Carl Friedrich Gauss (1777 - 1855). Pero probar su afirmación de que la ecuación $X^n + Y^n = Z^n$ carece de soluciones enteras x, y, z, tales que $xyz \neq 0$, para todo $n > 2$, conocida como el «último teorema de Fermat», se convertiría en un acicate constante para el avance de la teoría de números.

GAUSS, «PRINCEPS MATHEMATICORUM»

La obra de Carl Friedrich Gauss (1777 - 1855) es una de las más impresionantes de la historia de las matemáticas. Nacido en Brunswick en el seno de una familia muy humilde, Gauss fue llamado *Princeps mathematicorum* por su coetáneos. Gauss reunía en su persona todas las cualidades que son de desear para el cultivo de la matemática: intuición, profundidad de pensamiento, rigor, facilidad de cálculo y constancia en el tratamiento de los problemas. Su estilo era apto tanto para la matemática «fundamental» como para la matemática «aplicada». Puede decirse que Gauss cultivó todas las ramas de la matemática de su época, algunas de las cuales adquirieron una personalidad y apariencia «modernas» a partir de sus planteamientos y metodología.

A los catorce años de edad, Gauss fue presentado al príncipe Carl Wilhelm Ferdinand de Brunswick-Lüneberg, quien, impresionado por el talento del joven, le concedió una beca que le permitió realizar sus estudios con holgura. A los quince años, Gauss ingresó en el Collegium Carolinum, un centro estatal que contaba escasamente diez años de antigüedad, y que poseía una biblioteca excelente. En el Collegium, Gauss estudió latín y griego y se familiarizó con los *Principia* de Newton, el *Algebra* de Euler y la *Mécanique analytique* de Lagrange.

A los dieciocho años de edad, Gauss ingresó en la Universidad de Göttingen. Teniendo en cuenta que esta universidad se encontraba en el estado de Hannover, este hecho equivalía a estudiar en el extranjero. La Universidad de Göttingen, fundada por el rey Georg II de Inglaterra, seguía el modelo de las universidades inglesas de Oxford y Cambridge. En Göttingen, Gauss gozó de «libertad académica»: no estuvo guiado por ningún tutor, no tuvo que someterse a ningún examen y sobre él no se ejerció ningún tipo de control curricular. Gauss fue alumno de la Universidad de Göttingen hasta los veintiún años. Durante esta estancia tuvo lugar la eclosión de su talento matemático. En sus años universitarios, Gauss dejó prácticamente terminada la redacción de un libro memorable: *Disquisitiones arithmeticae.*

Las *Disquistiones arithmeticae* fueron editadas en 1801 en Leipzig, ciudad que poseía una excelente tradición en la edición de libros. El libro contiene 700 páginas, redactadas en un hermoso y culto latín, repletas de hallazgos matemáticos relativos al comportamiento de los números. En la obra, Gauss agradece a su protector, el príncipe, el haber sabido sortear todos los obstáculos que retardaban la edición, dedicándole las palabras siguientes:

> ... nadie ignora que no son excluidas de Vuestro patrocinio aquellas ciencias que son consideradas por la gente más abstrusas y más alejadas de la utilidad de la vida diaria, porque Vos mismo os dais cuenta perfectamente de la vinculación íntima y necesaria entre todas las ciencias, con una mentalidad muy sabia y muy conocedora de todas las cosas que interesan para el aumento de la prosperidad de la sociedad humana.

Las *Disquisitiones arithmeticae* de Gauss abandonaban el carácter utilitario de las aritméticas renacentistas y se convertían en el primer libro moderno de teoría de números. En las *Disquisitiones,* Gauss retoma la tradición de la aritmética griega (Euclides, Diofanto) y de los matemáticos indios (Brahmagupta, Bhaskara) para dar un paso de gigante con respecto a las investigaciones efectuadas por Fermat, Euler y Lagrange. Gauss decía de la matemática que era «la reina de las ciencias» y de la teoría de números, que era «la reina de las matemáticas».

Una de las preguntas más difíciles que cabe formular a un matemático creativo es «para qué sirve» lo que está haciendo. ¿Cuál hubiera sido la respuesta de Gauss a tal pregunta? Hoy, transcurridos más de 200 años, sabemos que

Carl Friedrich Gauss (1777-1855).

las *Disquisitiones* no sólo representan un hito en la historia del pensamiento humano, sino que contienen, además, el germen de ideas matemáticas presentes en las modernas tecnologías.

El príncipe protector de Gauss murió en la batalla de Jena (1806), luchando contra las tropas de Napoleón. En 1807, Gauss obtuvo el cargo de director del Observatorio de Göttingen, que ocupó hasta el fin de sus días. A lo largo de su vida participaría en estudios sobre astronomía, análisis, mecánica celeste, cálculo de probabilidades, mecánica, electromagnetismo y geometría diferencial. Su intervención sería clave asimismo en el nacimiento de las geometrías no euclidianas.

«DISQUISITIONES ARITHMETICAE»

Las *Disquisitiones* constan de siete secciones. Las cuatro primeras se dedican al cálculo con *congruencias*. Si se fija un entero m y dados enteros a, b, Gauss dice que a y b son *congruentes* módulo m cuando su diferencia es un múltiplo de m

$$a \equiv b \pmod{m} \Leftrightarrow m \mid (a - b).$$

De este modo, $-16 \equiv 9 \pmod 5$, $-7 \equiv 15 \pmod{11}$. Fijado un módulo m, cada número entero es equivalente a un número entre 1 y m. A lo largo de 165 páginas, Gauss se dedica a investigar las propiedades de las clases de congruencia $\mathbb{Z}/m\mathbb{Z}$ cuando con ellas se efectúan las operaciones aritméticas habituales.

Un ejemplo de cálculo módulo 12 lo ofrecen las horas de los relojes. Por ejemplo, $8 + 7 \equiv 3 \pmod{12}$. Expresamos los años mediante números enteros, pero expresamos las horas por medio de clases de congruencia de $\mathbb{Z}/12\mathbb{Z}$. Si las horas se expresaran por medio de números enteros, nos sería muy costoso comunicar la hora que es.

El resultado fundamental de las primeras secciones del texto que comentamos lo constituye la «ley de reciprocidad cuadrática». Se trata de un resultado imprescindible en el estudio de las ecuaciones diofánticas de segundo grado, que expresa una sutil relación de dependencia entre los distintos números primos.

Las 375 páginas de que consta la sección quinta están dedicadas al estudio de las ecuaciones diofánticas de segundo grado $aX^2 + 2bXY + cY^2 = d$. Notemos que el caso $a = c = 1$, $b = 0$ corresponde a las sumas de dos cuadrados, ecuación que había sido estudiada por Fermat. Gauss clasifica las ecuaciones, así como sus soluciones. Agrupa las clases de ecuaciones en órdenes y en géneros, lo cual le facilita su tratamiento uniforme. En un *tour de force* impresionante, Gauss define una composición de clases de formas de discriminante $D = b^2 - ac$ y estudia las propiedades de esta composición, que corresponden a la estructura algebraica de «grupo abeliano». Esta estructura, así como su denominación, no sería formalmente estudiada en álgebra hasta la obra de Évariste Galois (1811 - 1832) y sus sucesores.

Gauss dedica las secciones sexta y séptima de las *Disquisitiones* a aplicaciones diversas de la teoría de las secciones precedentes. En la sección sexta, de 50 páginas, Gauss trata el problema de la descomposición de fracciones en fracciones simples y en fracciones decimales y estudia el problema de la factorización de los números naturales en producto de factores primos. Gauss expresa su convicción de que el problema de distinguir números primos de números compuestos y de descomponer éstos en sus factores primos le parece «uno de los más importantes y útiles de toda la aritmética».

La última sección de las *Disquisitiones* se dedica a la resolución de un problema heredado de la matemática griega. Los griegos sabían que los polígonos de $n = 3, 4, 5, 6$ lados se pueden trazar mediante el uso de la regla y el compás. A los diecinueve años, Gauss había descubierto que el polígono de 17 lados es asimismo trazable con regla y compás, siendo la constatación de este hecho la que le inclinaría definitivamente por el cultivo de las matemáticas. En las 75 páginas de la sección séptima, Gauss caracteriza todos los polígonos de n lados que son trazables con regla y compás. Un polígono de n lados es trazable con regla y compás si, y solamente si, $n = 2^t p_1 \dots p_r$, en donde los números primos p son de la forma $p = 2^m + 1$ y son dos a dos distintos. La metodología empleada constituye un precedente de la teoría de Galois y prepara, al mismo tiempo, las investigaciones de Ernst Eduard Kummer (1810 - 1893) sobre los cuerpos ciclotómicos, realizadas con vistas a la resolución del teorema de Fermat. Las *Disquisitiones* concluyen con varias tablas numéricas.

LAS PRIMERAS COMPUTADORAS MECÁNICAS

La complejidad creciente de los cálculos con que debían enfrentarse los matemáticos y los astrónomos provocó la paulatina incorporación de instrumentos adecuados para su elaboración mecánica.

A la edad de dieciocho años, Blaise Pascal (1623 - 1662) ideó una máquina de calcular mecánica con el fin de ayudar a su padre, que era recaudador de impuestos. La denominada *Pascalina* constaba de una serie de ruedas dentadas mediante las cuales se representaban los números en base 10, permitiendo su adición y su sustracción. La suma de una unidad se simulaba mediante un paso de la rueda y la sustracción, mediante un paso en el sentido contrario. En unos pocos años se vendieron cincuenta de estas máquinas.

La *Pascalina* (1642).

Poco después, Gottfried Wilhelm Leibniz (1646 - 1716) mejoraba la máquina de cálculo de Pascal, al diseñar una máquina que, basada igualmente en el sistema decimal y por medios enteramente mecánicos, era ya capaz de sumar, restar, multiplicar y dividir. Sin embargo, de construcción mucho más compleja que la *Pascalina,* la máquina de Leibniz no fue comercializada.

Leibniz se percató de que la representación binaria de los números era igualmente apta para la realización mecánica del cálculo. La idea de representar todos los números valiéndose únicamente de los guarismos 0, 1 resultó tan sorprendente y desconcertante para el filósofo que llegó a asimilar el 0 a la Nada y el 1 a Dios, por cuanto que «el uno basta para extraer el todo de la nada» *(«Omnibus ex nihil ducendis sufficit unum»).* En 1679, Leibniz redactó un manuscrito sobre el sistema binario titulado *De progressio dyadica* e ideó un instrumento que por medio de un sistema de bolas móviles permitía la simulación del cálculo binario. Pero, a pesar del interés mostrado por Leibniz y por otros matemáticos de la época –como el inglés Thomas Hariot, el francés Thomas Fantet y el propio Pascal–, el sistema binario quedó relegado durante más de 300 años a la categoría de simple curiosidad o rareza matemática.

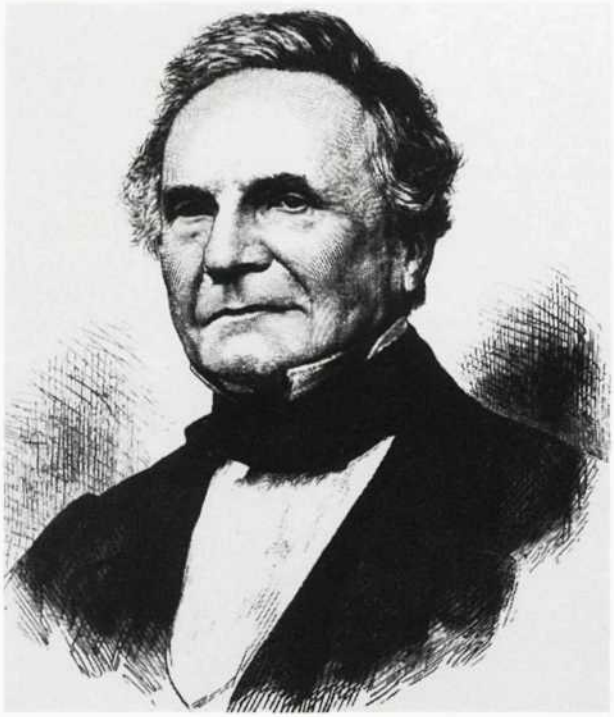
El *aritmómetro* de Thomas (1822).

A principios del siglo XIX, la complejidad de las relaciones comerciales y el desarrollo de la banca inherentes a la Revolución Industrial hicieron imprescindible la comercialización de diversas máquinas de calcular. La primera de ellas fue el *aritmómetro* de Thomas, construido en 1822. Se trataba de ingenios mecánicos dedicados a facilitar al máximo la labor de los computadores. Paulatinamente, las máquinas mejoraron sus prestaciones, siendo destacables la incorporación de teclados para la entrada de los datos (una idea tomada de las máquinas de escribir), así como dispositivos de impresión. En España destaca el *husillo sin fin,* una máquina ideada por el ingeniero Leopoldo Torres Quevedo (1852 - 1936) que permitía el cálculo con logaritmos y de la cual se conserva un ejemplar en la sede de la Real Academia de Ciencias Exactas, Físicas y Naturales.

LA AUTOMATIZACIÓN DEL CÁLCULO

Alrededor de 1820, el matemático británico Charles Babbage (1791 - 1871) pensó en la necesidad de una máquina para la confección de tablas que redujera al mínimo la intervención humana. Hijo de una acomodada familia de banqueros, Babbage estaba exasperado por la tremenda cantidad de errores de las tablas matemáticas impresas. En la mente de Babbage, estas máquinas debían ser capaces de efectuar automáticamente secuencias de operaciones, erradicar los errores de transcripción y evitar los errores de composición tipográfica. Los estudiantes de matemáticas de mi generación todavía sabemos por experiencia que calcular a mano con números de muchas cifras sin cometer errores es harto difícil y copiar números de muchos dígitos sin equivocarse es prácticamente imposible.

Durante once años, Charles Babbage ocupó la cátedra *Lucasian* de Matemáticas en la Universidad de Cambridge, la misma que desempeñara Newton en su día y que hoy ocupa el físico Stephen W. Hawking. Babbage dedicó gran parte de su energía y patrimonio al diseño de dos tipos de



Charles Babbage (1791-1871).

máquinas de calcular: la máquina de diferencias y la máquina analítica.

La base matemática de la máquina de diferencias estaba constituida por el denominado método de las diferencias finitas. El método permite determinar valores de funciones polinómicas utilizando únicamente la operación de adición. La máquina de diferencias hubiera calculado, e impreso, tablas de funciones trigonométricas, interés compuesto, logaritmos, etc. Sin embargo, en 1833, y tras diez años de apoyo financiero destinado a la manufacturación de sus componentes, el gobierno británico se retiró del proyecto. Únicamente llegó a ensamblarse una parte de la máquina, formada por 2000 de las piezas diseñadas por Babbage, que funcionó a la perfección. Según el proyecto de Babbage, la máquina hubiera constado de 25000 piezas metálicas y medido dos metros y medio de alto, por dos metros de ancho y por casi un metro de fondo.

En 1801, el mecánico Joseph-Marie Jacquard había llevado a la práctica la idea de utilizar unas tablillas de madera perforadas para la realización automática de complicados dibujos en telas. Jacquard diseñó un telar que tejía los dibujos automáticamente gracias a las órdenes guardadas en las tarjetas.

Babbage pensó en extrapolar la idea de Jacquard al diseño de una máquina de calcular, distinta de la máquina de diferencias, cuyas órdenes serían ejecutadas automáticamente gracias al uso de tarjetas perforadas. La denominó máquina analítica y solicitó el correspondiente apoyo financiero para su construcción, que le fue denegado.

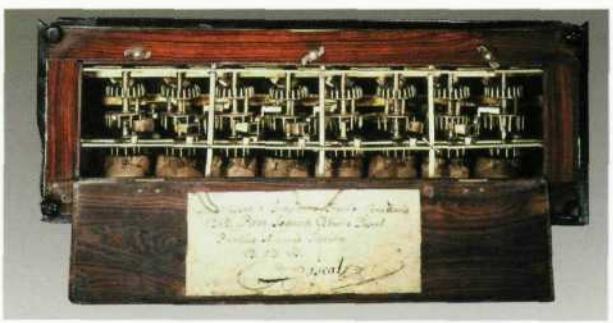
El proyecto de Babbage sobre la máquina analítica fue presentado a la Academia de Ciencias de París en 1884 por el ingeniero y general piamontés L. F. Menabrea, uno de los primeros en comprender su alcance. Un informe sobre la máquina analítica, publicado por Menabrea en el *Journal de Genève* en 1842, fue traducido al inglés y comentado con abundantes notas por Ada Augusta Byron, condesa de Lovelace (1815 - 1852), ayudante de investigación de Babbage. Se dice que Ada había heredado de su madre el talento por las matemáticas y de su padre, Lord Byron, la facilidad por los idiomas. En su comentario al texto de Menabrea, Lovelace dice que «la máquina analítica tejerá motivos algebraicos exactamente como los telares de Jacquard tejen flores y hojas».

Sobre los planos, la máquina analítica contaba con un dispositivo de entrada y salida *(input- output)*, una serie de engranajes que formaban un «almacén» y un «molino», que actuaban de forma independiente. El almacén y el molino constituyen un precedente de la memoria y el procesador, respectivamente, de los ordenadores modernos. La máquina también estaba dotada de un mecanismo que permitía imprimir los resultados. Lovelace elaboró instrucciones codificadas en tarjetas perforadas con vistas a su introducción un día en la máquina analítica. En la Exposición Internacional de Londres de 1862 se exhibió una maqueta de la misma. Con toda justicia se conoce a Babbage como el «abuelo» de los ordenadores actuales y a Lovelace como la primera «programadora» de la historia.

A pesar de repetidos fracasos, Babbage mejoró el proyecto de la máquina de diferencias diseñando una segunda. Por encargo del Museo de la Ciencia de Londres, esta segunda máquina de diferencias fue construida entre 1985 y 1991, utilizando veinte planos del propio Babbage. La máquina, de tres toneladas de peso, funcionó a la perfección, aunque, con el fin de abaratar los costes la impresora no fue construida.

En la época de Babbage era prácticamente imposible encontrar la financiación necesaria para la construcción de instrumentos de cálculo, de interés puramente científico. Sin embargo, la situación cambió drásticamente en el siglo siguiente, en que los gobiernos emplearían ingentes sumas de dinero en la construcción de imponentes ingenios de cálculo.

El ingeniero y estadístico Hermann Hollerith retomó en 1888 la idea de la utilización de tarjetas perforadas, pero con una finalidad distinta. Hollerith creó un sistema de



Máquina de Hollerith (1890).

Máquina perforadora de tarjetas (1890).

codificación alfanumérico que permitía identificar las letras del alfabeto y las cifras del 0 al 9 con una sucesión de perforaciones en doce líneas de una tarjeta. La Hollerith's Tabulating Machine Company, fundada en 1896, se dedicó a la comercialización de máquinas tabuladoras que tenían como base las tarjetas perforadas. Las máquinas fueron empleadas en la elaboración del censo de los Estados Unidos en 1890 y en 1900. En 1911, la compañía se fusionó con otras dos y, a partir de 1924, la empresa pasó a denominarse IBM (International Business Machines).

EL CÁLCULO EN LA PRIMERA MITAD DEL SIGLO XX

Las necesidades de cálculo experimentaron un crecimiento vertiginoso en el periodo comprendido entre las dos guerras mundiales. Predecir la trayectoria de los torpedos lanzados por los submarinos o de las bombas lanzadas por los aviones, a fin de mejorar su puntería, son problemas cuya resolución conduce a la integración numérica de ecuaciones diferenciales y, en consecuencia, a procesos de cálculo numérico demasiado largos para ser realizados a mano. Descifrar las comunicaciones cifradas interceptadas al enemigo, mediante métodos eficaces y fiables, sin conocer la clave, conlleva la resolución de sistemas de ecuaciones algebraicas y de problemas de combinatoria demasiado largos asimismo para su resolución con los instrumentos al uso. La regla de cálculo y las calculadoras de sobremesa –primero mecánicas y más tarde eléctricas– resultaron muy pronto insuficientes para tales cometidos y cedieron el paso a los primeros ordenadores analógicos.

Antes de la Segunda Guerra Mundial, el ingeniero alemán Konrad Zuse (1910 -) había diseñado una familia de computadoras que utilizaron desde el primer momento el sistema de numeración binario. Sus modelos Z1 y Z2 (denominados de acuerdo con la inicial de su apellido) todavía eran mecánicos y tenían por finalidad la resolución de sistemas de ecuaciones algebraicas. Entre 1941 y 1944, Zuse construyó dos computadoras electromecánicas, los modelos Z3 y Z4, basadas en el uso de relés electromagnéticos. El Z3 era un ordenador ya controlado por un programa, que fue usado por el Instituto Alemán de Aeronáutica. Zuse fundó su propia compañía que llegó a construir veintiún ordenadores.

En 1937, G. Stibitz (1904 - 1995), ingeniero de los Bell Telephone Laboratories, utilizando algunos relés de desperdicio y un par de bombillas construyó una máquina capaz de sumar en binario. Los relés estaban cableados de manera que las bombillas se encendían cuando la suma era 1 y quedaban apagadas cuando la suma era 0. Posteriormente, Stibitz construyó los primeros circuitos binarios que permitían la realización de las operaciones aritméticas elementales y la conversión de números decimales a números binarios y viceversa.

Stibitz supo interesar a su compañía, que construyó, en 1939, el *Complex Calculator,* basado enteramente en el uso de la aritmética binaria. Los datos se introducían por medio de un teletipo, con lo cual la máquina no sólo era capaz de calcular, sino que los datos podían ser introducidos a distancia. En 1942, Stibitz ideó también la técnica de la *aritmética flotante,* que permite a la máquina trabajar con números muy grandes.

El *Complex Calculator,* fabricado en los Bell Telephone Laboratories, fue la primera calculadora binaria mundialmente conocida. En un congreso de la American Mathematical Society celebrado en 1940 en Hannover (New Hampshire), Stibitz conectó un teletipo a la máquina, que se encontraba en Nueva York, de manera que los asistentes podían encargarle una tarea y obtener la respuesta en menos de un minuto.

En 1943, IBM construyó la máquina ASCC *(Automatic Sequence Controlled Calculator),* más conocida como Harvard Mark I, una calculadora multifunción que realizaba en gran parte el sueño de Babbage. Su construcción pudo coronarse con éxito gracias a un proyecto pionero en I + D (como diríamos hoy) entre la Universidad de Harvard y la empresa IBM. El físico H. Aiken, que conocía los trabajos de Babbage, se puso en contacto con IBM, que financió el proyecto y aportó su experiencia. La máquina, aunque era esencialmente mecánica, utilizaba relés y embragues accionados por electroimanes. Pesaba cinco toneladas y medía 16 metros de largo, 2.60 metros de alto y 60 centímetros de fondo. Podía calcular tablas de funciones trigonométricas, de logaritmos, de funciones exponenciales, etc. Las órdenes eran introducidas mediante tarjetas perforadas. En un principio, la máquina estuvo destinada a cubrir las necesidades de cálculo de la marina de los Estados Unidos. Más adelante se crearon otras calculadoras de la misma serie: Mark II, Mark III y Mark IV. Es importante destacar que estas máquinas eran más fiables que el ENIAC (del que hablaremos a continuación) aunque más lentas. Las máquinas utilizaban el código BCD *(Binary Coded Decimal),* que codificaba cada cifra dígito decimal de forma binaria, a fin

Detalle del ENIAC.

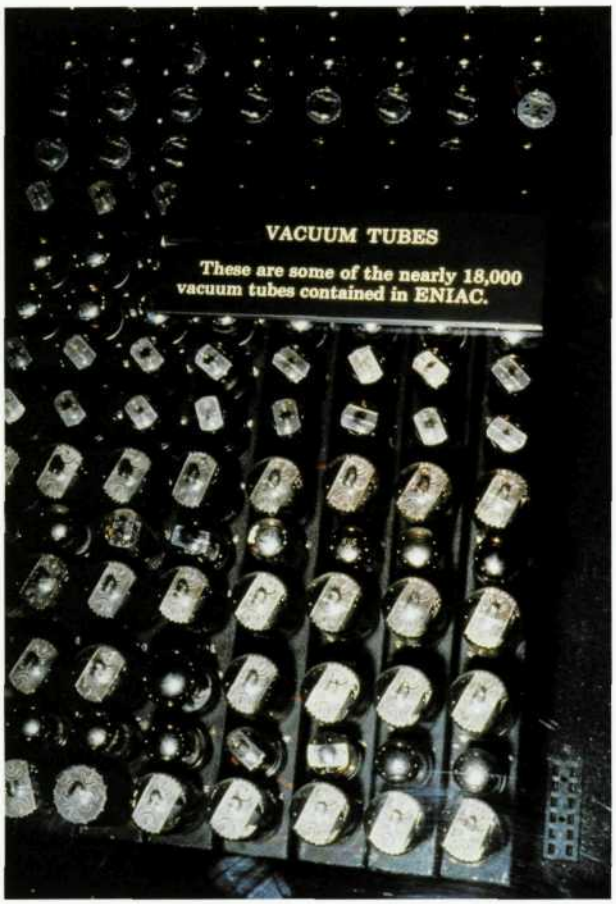
de introducir los datos en la calculadora. Al no codificarse los números, sino sólo cada una de sus cifras, la máquina efectuaba las operaciones como si trabajara en base 10.

A partir de 1940, el gobierno de los Estados Unidos inició una preparación de personal científico específicamente orientada a una posible entrada del país en la Segunda Guerra Mundial. Parte de la comunidad matemática fue entrenada en la resolución de problemas de balística, aeronáutica, criptografía, cálculo de probabilidades y estadística que surgían constantemente a raíz de la situación bélica. La dirección de estos programas fue confiada a los matemáticos John von Neumann (1903-1957), del Instituto de Estudios Avanzados de Princeton, y a Norbert Wiener (1894-1964), del Instituto de Tecnología de Massachusetts (MIT).

Para contrarrestar la superioridad de la artillería alemana puesta de manifiesta en el transcurso de la Primera Guerra Mundial, el ejército de los Estados Unidos fundó el Laboratorio de Investigación Balística (BRL). A fin de que la ingente cantidad de armas fabricada pudiera ser usada en los frentes de batalla se hizo necesaria la elaboración de tablas de balística. Cada cañón y cada tipo de proyectil susceptible de ser empleado requería una tabla con los datos numéricos de las posibles trayectorias. Cada una de estas tablas contenía entre 2000 y 4000 trayectorias. Al inicio de la Segunda Guerra Mundial, el cálculo de una trayectoria realizado con una calculadora de sobremesa requería unas veinte horas. Las personas calculadoras *(computers)* procedían de la Escuela Moore de Ingeniería Eléctrica, adscrita a la Universidad de Pensilvania. A medida que avanzaba la guerra, las calculadoras humanas no daban a basto.

En 1943 se firmó un contrato por el cual la Escuela Moore se comprometía a la realización del ENIAC *(Electronic Numerical Integrator and Computer),* una máquina electrónica, precursora de los primeros ordenadores. La máquina estuvo terminada en 1945 y al principio su principal usuario fue el personal del Laboratorio de Investigación Balística.

La técnica empleada en el ENIAC se basaba en el paso de electrones por tubos de vacío (las válvulas de las antiguas radios). La máquina incluía 18000 tubos de vacío, así como 1500 relés telefónicos. El tiempo que requería para hacer una operación elemental era de 24 milisegundos. Pesaba 30 toneladas y estaba constituido por cuarenta paneles de 3 metros de alto, 60 centímetros de ancho y 30 centímetros de fondo. Puesto que la vida media de cada válvula era de unas 3000 horas, era de esperar que cada diez minutos se fundiera una, por lo que debía ser reparado constantemente. La máquina utilizaba el sistema de numeración decimal. Poseía un lector de tarjetas perforadas capaz de leer 120 tarjetas por minuto. El ENIAC fue la primera calculadora analítica multifunción enteramente electrónica. Una vez finaliza la guerra, el ENIAC pudo emplearse para la computación científica y fue utilizado en muchos cálculos relativos a física nuclear y en los primeros cálculos de meteorología numérica. Como hecho curioso, citemos que el ENIAC fue capaz de calcular



Detalle del ENIAC.

más de 2000 dígitos de la expresión decimal de π. Se estima que en sus diez años de funcionamiento esta máquina realizó más cálculos que el resto de la humanidad hasta entonces.

AVANCES TECNOLÓGICOS

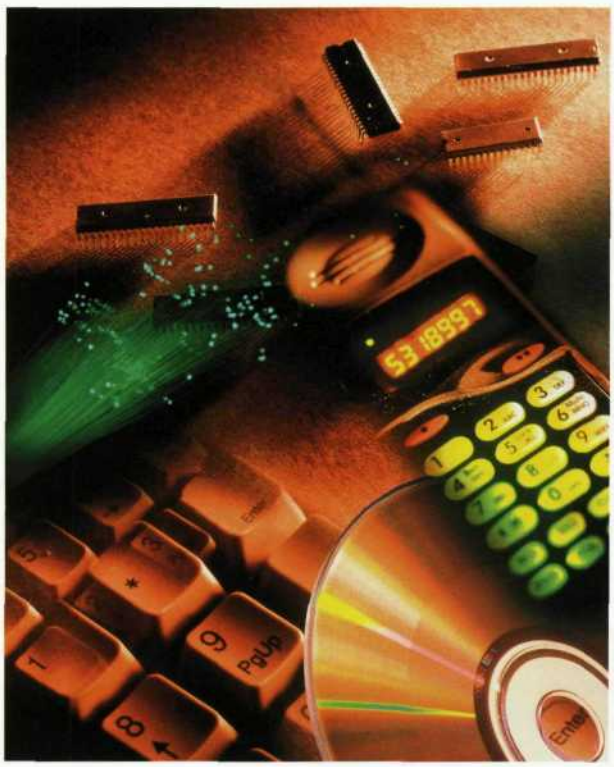
Al finalizar su proyecto con la Armada de los Estados Unidos, los principales artífices del ENIAC, los físicos J. Presper Eckert (1919 -) y John William Mauchly (1907 - 1980) fundaron en 1947 la primera compañía informática de la historia: Eckert-Mauchly Computer Corporation (EMCC), cuyo principal producto comercializado fue el UNIVAC *(Universal Automatic Computer)*. El UNIVAC incluía programas para almacenamiento de datos, siguiendo una idea de Von Neumann. Poseía una memoria principal de mil palabras, una memoria secundaria sobre una cinta magnética y dispositivos de *input-output:* máquinas de escribir, tarjetas, impresora. El UNIVAC fue el primer ordenador comercializado.

En el año 1948, la máquina IBM SSEC fue utilizada para calcular tablas de posición de la Luna, de importancia para los posteriores viajes espaciales. La calculadora SAGE 1950, diseñada en el MIT, sería utilizada en la «guerra fría».

Los elevados costes de las investigaciones encaminadas a la mejora de los ordenadores ocasionaron la fusión de diversas empresas en grandes compañías. El camino recorrido desde el aparatoso ENIAC hasta los rápidos ordenadores que pueblan nuestras mesas es realmente espectacular. Durante más de cincuenta años, la informática ha experimentado revoluciones casi ininterrumpidamente.

En 1947, los Bell Telephone Laboratories, adscritos en la época a la compañía AT&T, fabricaron los primeros transistores, con lo que tenía lugar el nacimiento de la microelectrónica. Los transistores reemplazaron con ventajas a los tubos de vacío, ya que ofrecían un menor consumo de corriente, una menor producción de calor, un tamaño mucho más reducido y una vida media casi ilimitada. Sus inventores, W. B. Shockley, J. Bardeen y W. H. Brattain, recibieron por tal motivo el premio Nobel de Física en 1956.

A finales de los años cincuenta, J. Kilby, de Texas Instruments, y R. N. Noyce, de Fairchild Semiconductors, encontraron la manera de integrar todos los constituyentes de un circuito electrónico (transistores, resistencias, condensadores, etc.) y sus correspondientes interconexiones en la superficie de un chip, lo que supuso la aparición de los primeros circuitos integrados. En 1970, Intel fabricaba el primer microprocesador. El constante perfeccionamiento experimentado en el proceso de fabricación de los chips ha determinado la extraordinaria evolución de la microelectrónica en los últimos años. Desde la finalización de la Segunda Guerra Mundial, las gentes de Silicon Valley han puesto de manifiesto que la paz también puede ser rentable.



En el año 2000, J. Kilby recibía el premio Nobel de Física por su invención del chip, compartido con Z. Alferov y H. Kroemer. Estos últimos lo recibían por sus trabajos en optoelectrónica –la tecnología que hace posible la transmisión de señales por cable de fibra óptica.

La teoría matemática de la información

Siguiendo un esquema bien conocido por los lingüistas, en toda transmisión de información cabe distinguir una *fuente emisora, un canal de transmisión* y *una fuente receptora*. El nacimiento de la teoría matemática de la información se sitúa en los años 1940 y, desde entonces, esta nueva rama de la matemática no ha dejado de progresar. La teoría de los códigos correctores de errores y la criptología numérica son partes integrantes de la misma. El objetivo de la teoría de los códigos correctores de errores es la fidelidad de las transmisiones y el objetivo de la criptología es su privacidad.

Capítulos clásicos de la matemática encuentran una aplicabilidad que hubiera sido impensable hace unos años. Tal es el caso de la teoría de números, que a su carácter de disciplina básica ha añadido en la actualidad importantes aplicaciones en teoría de códigos y en criptología.

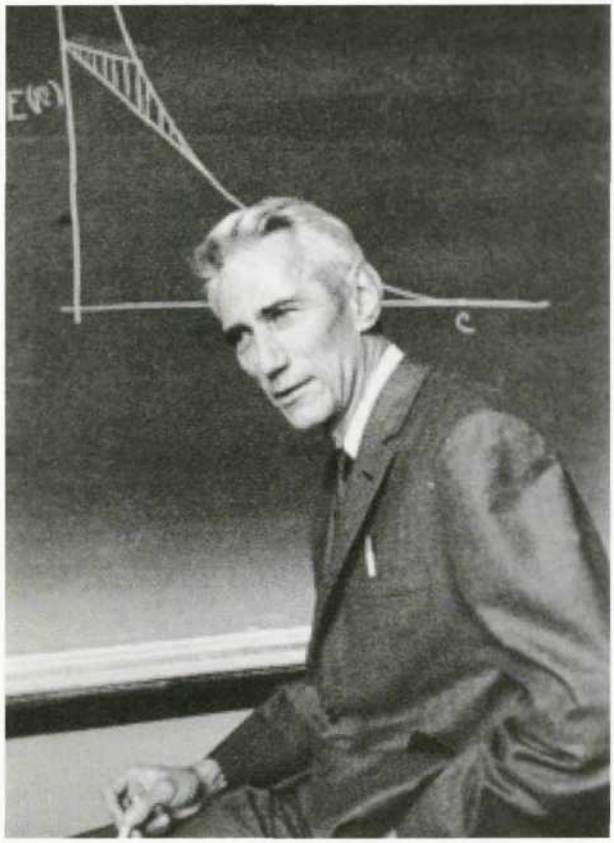
La teoría de los códigos correctores de errores

En los años cuarenta del siglo XX, los Bell Telephone Laboratories decidieron crear un centro de investigación matemática cuya finalidad principal era la 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).

Al digitalizar la información en forma de ceros y unos, los cambios en alguno de estos dígitos eran harto frecuentes, llegando incluso a producir una parada de las máquinas. Ello era especialmente lamentable durante los fines de semana, puesto que las máquinas podían quedar detenidas durante muchas horas. El propio Hamming relata la perplejidad de unos matemáticos colocados al frente de unas máquinas que no acababan de funcionar. Tenían la impresión, nos cuenta, de que «debían hacer algo no convencional en un medio no convencional».

La idea de Hamming consistió en completar bloques de bits, antes de proceder a su transmisión, con bits adicionales, de tal forma que los posibles errores de transmisión pudieran ser detectados y/o corregidos por la fuente receptora.

El *bit de paridad* proporciona un ejemplo de código *detector* de errores. Imaginemos que codificamos determinada información por medio de palabras de siete bits. A continuación, completamos cada palabra con un octavo bit, igual a 0 si la suma de los siete bits anteriores es par, e igual a 1, si es impar. Si en la transmisión de la palabra de ocho bits se produce un error, éste será detectado por la máquina, puesto que la palabra recibida no va a satisfacer el criterio de paridad. El denominado *bit de paridad* es un código detector de un error. No obstante, es incapaz de indicarnos cuál es el bit equivocado, por lo que no es un código corrector de errores. Si se hace uso de este código, cada siete bits de información se verán completados con un bit de control.



Claude Shannon (1916-2001).

Los *códigos de repetición* proporcionan ejemplos de códigos *correctores* de errores. Acordemos, por ejemplo, en triplicar cada bit antes de su transmisión. Si 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 equivocado; en este caso, la máquina cambiará la palabra 001 por la palabra 000. Si usamos este código, cada bit de información se completará con dos bits de control. El código de repetición triple es capaz de corregir un error en cada bloque de tres bits, pero, obviamente, triplica el coste de las transmisiones.

En general, tanto los códigos detectores de errores como los códigos correctores de errores obedecen al mismo principio: alargan palabras de longitud k en palabras de longitud n mediante la adición de bits de control. La razón k/n se denomina la *tasa de transmisión* del código.

Un concepto básico en teoría de códigos lo constituye la denominada *distancia de Hamming*. Dos palabras se dice que están a distancia r cuando difieren en r bits exactamente. Si la distancia mínima entre dos palabras de un código es $d = 2e + 1$, o bien $d = 2e + 2$, el código será capaz de corregir e errores. El cociente d/n se conoce como la *distancia mínima relativa* del código.

A igualdad de errores corregidos por bloque, los códigos más económicos serán aquellos cuya tasa de transmisión sea más alta; es decir, esté más cercana a la unidad.

En 1948, Shannon demostró que en todo canal de transmisión –expuesto a ruidos y sin memoria– existe un esquema de codificación cuya probabilidad de error es tan pequeña como se quiera, siempre que la información se transmita con tasa de rendimiento inferior a la capacidad del canal y los mensajes a transmitir sean suficientemente largos. (Todos los conceptos que aparecen en el teorema de Shannon se pueden modelizar matemáticamente.) A pesar de la influencia enorme del teorema de Shannon en teoría de códigos, debemos advertir que este teorema no es constructivo. Dado un caso particular, el teorema de Shannon nada nos dice acerca de cómo diseñar un código adecuado; únicamente garantiza su existencia. Con el tiempo se ha visto que el diseño de códigos cuyas constantes fueran próximas a las que predice la teoría de Shannon no es nada fácil.

Hamming diseñó en 1950 una familia de códigos correctores de errores que mejoraban los códigos de repetición. El código de Hamming más sencillo alarga palabras de cuatro bits en palabras de siete bits:

$$(x, y, z, t) \to (x, y, z, t, x + y + z, y + z + t, x + y + t).$$

Su tasa de transmisión es, por tanto, 0.57. El conjunto de palabras de longitud cuatro que podemos formar con dos bits posee 16 elementos; éste es asimismo el número de palabras codificadas, cuyo conjunto constituye el *código*. Por otra parte, el conjunto de palabras de longitud siete que podemos formar con dos bits posee 128 elementos. Cualquiera de estas palabras de siete bits difiere a lo sumo en un bit de una palabra del código. Con ello, el código de Hamming es capaz de corregir un error en cada bloque de siete bits. Por ejemplo, si se recibe la palabra 1011110, el código la dará por equivocada y la corregirá por la palabra 1001110.

Los ejemplos anteriores pertenecen a la amplia familia de los *códigos lineales*. En los códigos lineales, las palabras se interpretan como vectores de un espacio vectorial sobre un cuerpo finito y el alargamiento de las mismas con bits de control se realiza mediante el concurso de una aplicación lineal cuya matriz se denomina la *matriz generadora del código*. La detección de los errores se efectúa asimismo por otra matriz, denominada *matriz de control*. Otro aspecto muy importante a tener en cuenta en el diseño de los códigos es que el algoritmo de corrección de errores debe efectuarse sin que sea demasiado costoso en tiempo. En el diseño de buenos códigos correctores de errores interviene un gran número de recursos algebraicos.

El cuerpo finito más sencillo es el cuerpo de dos elementos $\mathbb{F}_2 = \{0,1\}$. Pero, para cada potencia $q = p^f$ de un número primo p, existe un cuerpo $\mathbb{F}_q$ que posee exactamente q elementos. El estudio de los cuerpos finitos se inicia en el siglo XIX, con E. Galois, y está ligado directamente al problema de la resolución por radicales de las ecuaciones algebraicas. Los cuerpos finitos más sencillos son los cuerpos $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$, formados por las clases de restos módulo un número primo. Muchas de sus propiedades se encuentran ya demostradas en las *Disquisitiones arithmeticae* de C. F. Gauss.

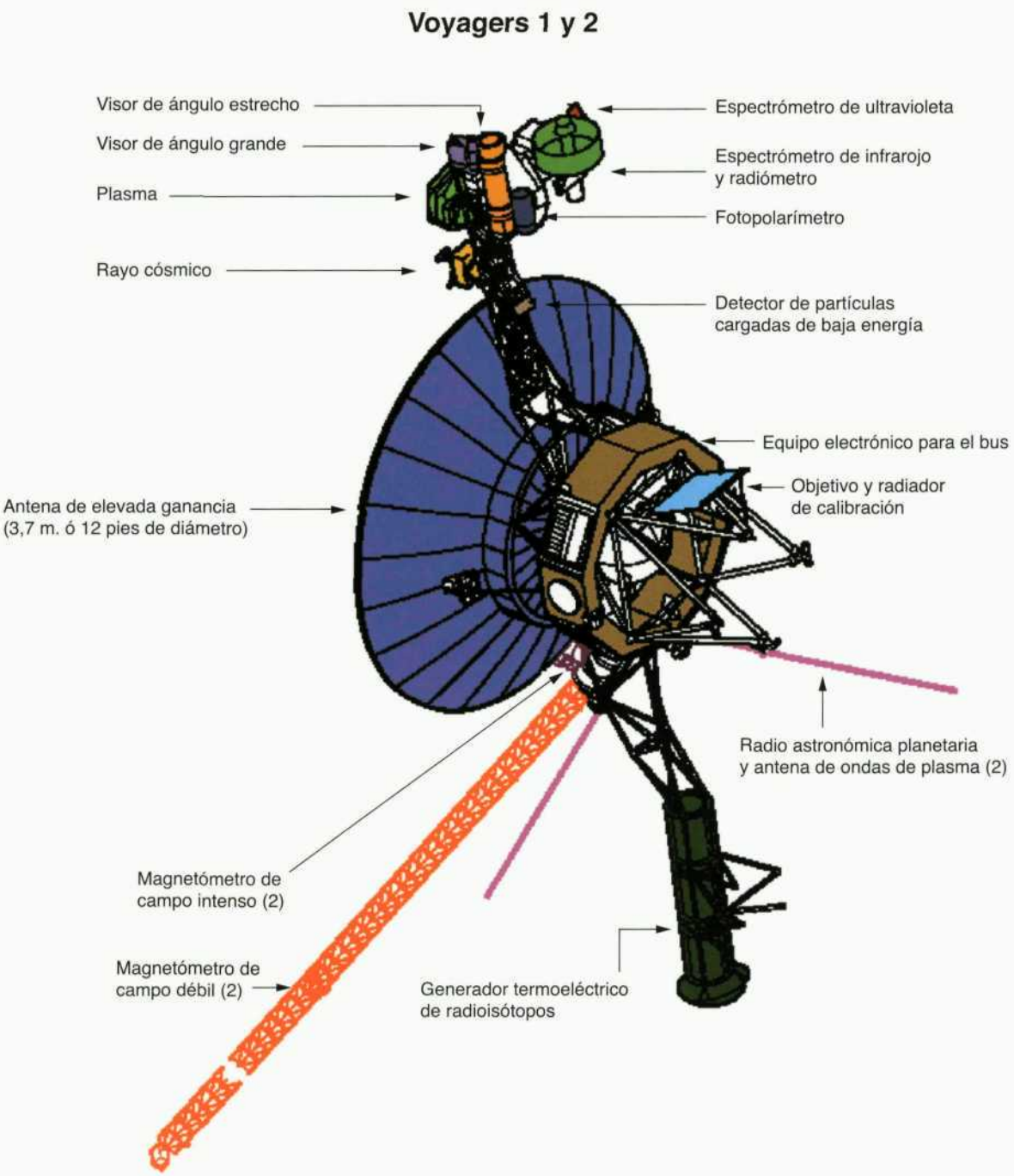
Los códigos correctores de errores diseñados por I. S. Reed y D. E. Muller, en 1954, fueron utilizados por la nave espacial *Mariner 9*, en 1972, para la transmisión de fotografías en blanco y negro de Marte. Los códigos diseñados por M. Golay, en 1948 (basados en teoría de grupos), fueron utilizados por el *Voyager*, en los años 1979-1981, para la transmisión de fotografías en color de Júpiter y Saturno. R. C. Bose, D. K. Ray-Chaudhuri y A. Hocquenghem diseñaron los códigos (BCH) usados por la NASA. Redd Solomon creó los códigos (RS) usados por Philips en los discos compactos (CD).

El diseño de los discos en formato DVD representa un gran avance con respecto al de los CD. El método de codificación de los discos compactos transforma ocho bits de usuario en 17 bits de código modulador. En el DVD, ocho bits de usuario se completan en tan sólo 16 bits de código modulador. Tal característica hace que su eficacia sea alrededor de un 6 % mayor.

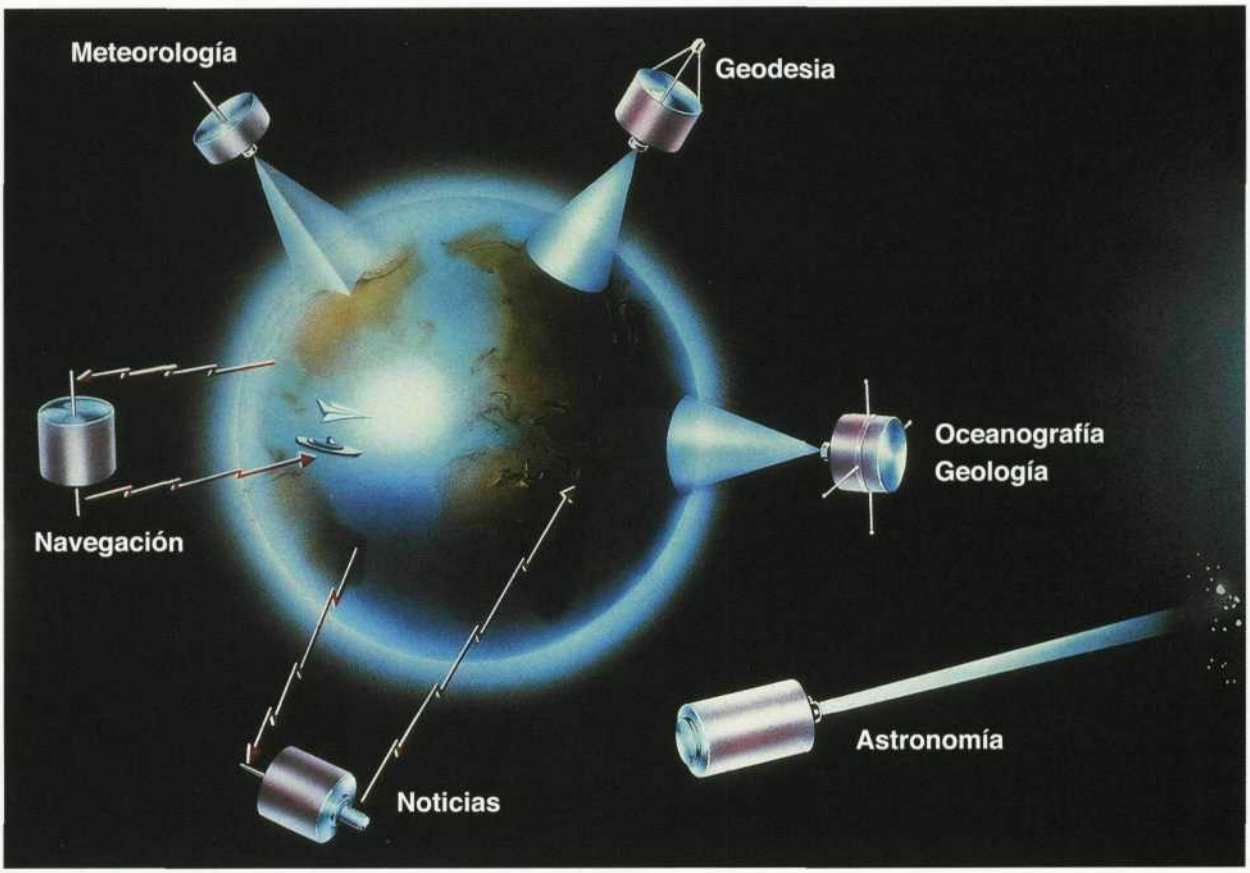
El matemático ruso V. D. Goppa puso de relieve en 1977 que la teoría subyacente a los códigos lineales quedaba mejor explicada a la luz de teoremas clásicos de geometría algebraica, siempre que éstos fueran trasladados al marco de la geometría algebraica sobre cuerpos finitos. La geometría algebraica sobre cuerpos finitos es una rama de la matemática desarrollada en los últimos cincuenta años y que ha proporcionado resultados teóricos muy profundos. La idea básica de Goppa consiste en la utilización del clásico teorema de Riemann-Roch para el cómputo de las principales constantes asociadas al código.

La construcción *efectiva* de códigos de Goppa requiere, a su vez, la construcción *efectiva* de curvas algebraicas sobre cuerpos finitos con un gran número de puntos sobre su cuerpo de definición, que deben asimismo conocerse *efectivamente*. Tal hecho ha conllevado un aumento del interés por la resolución *efectiva* de problemas diofánticos, constituyendo una de las ramas más activas y atractivas de la teoría de números computacional.

Se ha visto que las fibras de modelos enteros de las llamadas curvas de Shimura proporcionan curvas definidas sobre cuerpos finitos con buenas propiedades para su utilización en el diseño de códigos. Las curvas de Shimura, cuyo desarrollo teórico se inició en la década de 1950, son una de las herramientas básicas en la célebre demostración de A. Wiles del teorema de Fermat. En su tratamiento confluyen técnicas de geometría hiperbólica, análisis complejo, análisis p-ádico, álgebra no conmutativa y aritmética no conmutativa.



Los códigos de Golay fueron utilizados por el *Voyager*.



Quinientos satélites artificiales orbitan alrededor de la Tierra.

LA SEGURIDAD EN LA RED

En todas las épocas, los humanos han sentido la necesidad de enviar mensajes a determinados destinatarios que estuvieran protegidos del acecho de terceros. Los orígenes de la criptología, o arte que se encarga del cifrado y descifrado de mensajes, se pierden en el tiempo.

Las modernas tecnologías parece que no hacen sino incrementar las necesidades de cifrado en la transmisión de información. Multitud de datos circulan hoy por la red requiriendo tratamientos criptográficos seguros. Desde el punto de vista matemático, ello constituye un reto, puesto que se trata de lograr criptosistemas que sean a la vez económicos y fiables.

Los métodos de cifrado clásicos y los modernos difieren en un punto esencial. En los métodos clásicos, emisor y receptor acuerdan la clave de cifrado y la clave de descifrado, antes de la transmisión del mensaje. El conocimiento de la clave de cifrado es equivalente al de la clave de descifrado, pues basta invertir la primera. Estos sistemas de cifrado se denominan de *clave privada.*

Mediante procedimientos combinatorios, por ejemplo, pueden crearse claves privadas que ofrezcan un buen grado de seguridad. Sin embargo, todos los sistemas de clave privada adolecen de un defecto: el momento del intercambio de claves suele ser altamente inseguro. Ello es bien sabido por los criptoanalistas, o espías, que harán todo lo posible para hacerse con las claves, mediante procedimientos que suelen tener poco de científicos.

La criptología dio un giro espectacular en 1976, gracias a una idea de W. Diffie y M. E. Hellman, quienes propusieron hacer pública la clave de cifrado. En los denominados criptosistemas de *clave pública,* cualquier emisor puede mandar información cifrada a un receptor mediante el uso de la clave pública de éste. El receptor puede ser un banco, Hacienda, un hospital, un particular, o una entidad comercial cualquiera. Sin embargo, sólo el receptor debe estar en condiciones de leer la información cifrada que le mandan los emisores. La pregunta es: ¿cómo puede conseguirse esto?

Diffie y Hellman propusieron utilizar en la clave de cifrado *funciones de un solo sentido* –en el supuesto que tales funciones existan–. Se trata de utilizar una función en el cifrado del mensaje que sea poco costosa en tiempo de computación, pero cuya función inversa sea muy costosa en tiempo de computación mediante los ordenadores de que se dispone en la actualidad. Sin embargo, la función de descifrado ha de ser poco costosa de calcular si se dispone de información suplementaria. Esta información suplementaria está en manos del receptor de los mensajes, pues es quien ha elaborado la clave pública de cifrado.

La idea de Diffie y Hellman se ha implementado de maneras diversas. En 1977, Rivest-Shamir-Adleman creaban el criptosistema de clave pública RSA, uno de los más populares. En 1978, McEliece daba a conocer una familia de criptosistemas basados en la teoría de los códigos correctores de errores. En 1985, T. ElGamal ideaba el criptosistema del logaritmo discreto. Y, en 1993, A. J. Menezes y S. A. Vanstone implementaban criptosistemas basados en la aritmética de las curvas elípticas.

En el método RSA, la clave pública está constituida por un par de números (N, a), el primero de los cuales, N, es igual al producto de dos números primos p, q, $N = pq$. Una vez cortado el mensaje en unidades suficientemente pequeñas, su cifrado se lleva a cabo mediante la función potencial $y = x^a$, de exponente a, calculada en el grupo multiplicativo de $\mathbb{Z}/N\mathbb{Z}$. Este cálculo puede hacerse a gran velocidad, bastando para ello la expresión de a en base 2, que reducirá la potenciación a sucesivas elevaciones al cuadrado. El descifrado se lleva a cabo mediante la potenciación con otro exponente, que denotaremos por b. A fin de recuperar el mensaje inicial, la cantidad $ab - 1$ debe ser múltiplo de $(p-1)(q-1)$. Por tanto, el cálculo del exponente b requiere previamente el conocimiento de los factores primos p, q.

Vemos, por tanto, que la seguridad del cifrado RSA está directamente relacionada con la dificultad de descomponer el entero N en factores primos. Notemos que esta dificultad no existe para el receptor de los mensajes, puesto que éste ha creado su clave pública a partir de dos números primos p, q, suficientemente altos.

El número de claves públicas que podemos crear en el sistema RSA dentro de un intervalo depende de la densidad de los números primos en el intervalo citado. Para la elección de estos primos son asimismo necesarios generadores de números aleatorios y tests probabilísticos de primalidad. A medida que los números crezcan, los cálculos serán más costosos.

El método de ElGamal se basa a su vez en la dificultad de resolver eficazmente el problema del logaritmo discreto en determinados grupos finitos. Los grupos en cuestión se construyen mediante grupos multiplicativos de clases de restos, de cuerpos finitos, o de puntos de torsión de curvas elípticas.

En general, el diseño de sistemas criptográficos de clave pública está directamente relacionado con problemas de complejidad computacional. Un problema se dice de *clase P* (o de tiempo polinómico) si existe un algoritmo que permite su resolución en un tiempo acotado por una función polinómica en el número de bits de los datos del problema (*input*). Se supone que el algoritmo se implementa en una *máquina de Turing*, idealización de los ordenadores actuales. Un problema se dice de *clase NP* (o de tiempo polinómico no determinista) si en un tiempo polinómico se puede comprobar que una pretendida solución es, de hecho, una solución. Uno de los problemas fundamentales que tiene planteada la teoría de la computación es saber si $P \neq NP$.

Si cogemos un entero N de unas 30 cifras y lo pretendemos factorizar por el método directo de las divisiones sucesivas hasta su raíz cuadrada, teniendo en cuenta que el número de primos inferiores a 10^{15} es 29844570422669, un ordenador capaz de realizar 10^9 divisiones por segundo tardará más de ocho horas. Aunque se conocen diversos algoritmos de factorización, como el de D. Shanks (1969), de Fermat-Pollard (1974), de Brilhard-Morrison (1975), de H. W. Lenstra (1985), o los métodos de criba, que reducen el cálculo anterior a segundos en uno de nuestros ordenadores de sobremesa, el mejor resultado que se ha podido demostrar es que tales algoritmos son de tiempo subexponencial.

Hoy por hoy no se sabe si el problema de la factorización o bien el problema del logaritmo discreto son de clase P, por medio de algoritmos implementados en una máquina de Turing. Puede decirse que la seguridad de los actuales métodos criptográficos se apoya en la ignorancia: por una parte, no se conocen en los medios académicos métodos de factorización suficientemente eficaces y, por la otra, no se saben construir ordenadores suficientemente rápidos, capaces de convertir tiempos de ejecución exponenciales o subexponenciales en tiempos polinómicos.

Desde el punto de vista teórico, tampoco se ha podido probar que existan funciones de *un solo sentido*, que son las que preconiza el método de Diffie y Hellman. La experiencia indica, sin embargo, que hay funciones que se comportan como tales.

El éxito de los sistemas criptográficos de clave pública no implica, ni mucho menos, que se hayan relegado al olvido los sistemas criptográficos de clave privada. De hecho, se utilizan ambos a la vez. Los sistemas criptográficos de clave pública son utilizados para transmitir de forma segura las claves de los sistemas criptográficos de clave privada. La razón de obrar así es que, en general, los cálculos en los sistemas criptográficos de clave pública son mucho más laboriosos.

DEL BIT AL QUBIT

En 1997, la criptología experimentó otro cambio digno de tenerse en cuenta. Peter Shor sorprendió a la comunidad científica con el diseño de 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*. El mismo Shor dio la solución al problema de logaritmo discreto, también en tiempo polinómico, haciendo uso asimismo de la computación cuántica.

Dicho brevemente: un criptoanalista que estuviera en posesión de un ordenador cuántico podría romper todas las claves públicas de cifrado empleadas en la actualidad. Para romper la clave en el método RSA, Shor «utiliza» el ordenador cuántico en el cálculo del orden de un entero x módulo N, elegido al azar. Después esta información es usada en la factorización de N, que puede in-

Un superordenador.

cluso llevarse a cabo en una máquina de Turing, en tiempo polinómico.

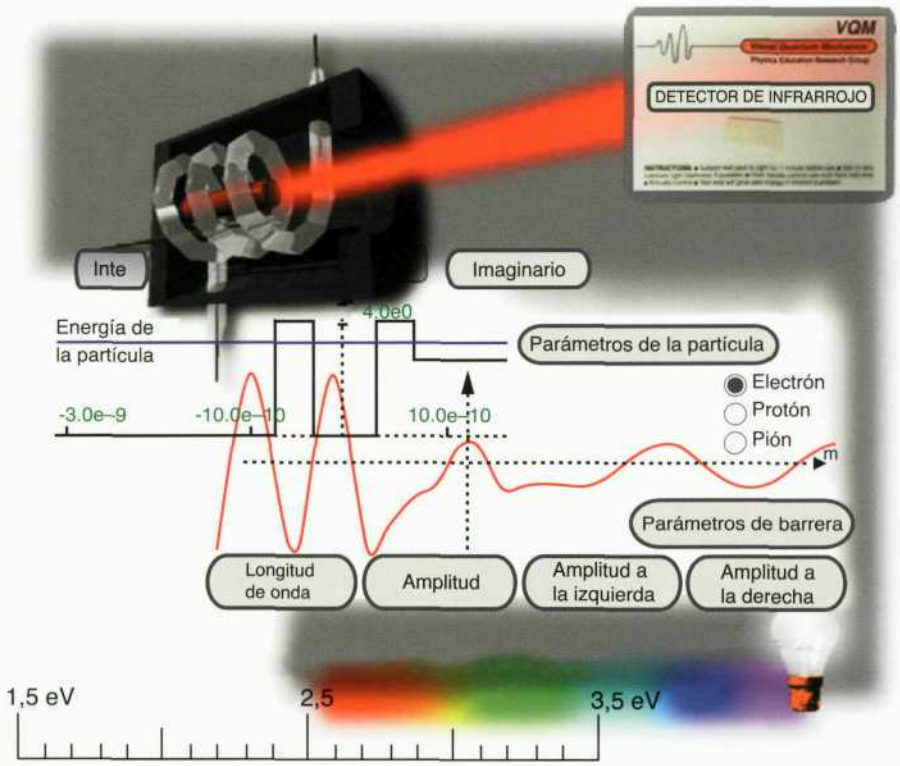
Siguiendo el paradigma de la mecánica cuántica, un ordenador cuántico no produciría una respuesta, sino una superposición de todas las respuestas posibles afectadas de distintas probabilidades. En la computación cuántica, el formalismo de la computación electromagnética es sustituido por el de la computación cuántica. El bit es reemplazado por el *qubit* (o bit cuántico). Un qubit es un estado cuántico

$$|\varphi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle,$$

en donde α, β denotan números complejos tales que $|\alpha|^2 + |\beta|^2 = 1$. Desde el punto de vista matemático, un qubit es un número cuaternio de Hamilton de norma 1, por lo que su manejo entra de lleno en el terreno de la aritmética no conmutativa. Desde el punto de vista físico, un qubit se interpreta como el bit $|0\rangle$, afectado de la probabilidad $|\alpha|^2$, y el bit $|1\rangle$, afectado de la probabilidad $|\beta|^2$.

La computación cuántica exige cambios sustanciales en el diseño de los algoritmos. Las puertas lógicas empleadas en las máquinas de Turing se ven sustituidas por puertas cuánticas. Las primeras tienen por base el álgebra de Boole; las segundas, los espacios de Hilbert y sus transformaciones unitarias.

En la actualidad, los ordenadores cuánticos existen únicamente sobre el papel y en la mente de algunas personas. ¿Pero acaso la historia no nos muestra que las visiones de los científicos, tarde o temprano, acaban por materializarse?



BIBLIOGRAFÍA

1. Bailey, Ronald H. (1997) *La Segunda Guerra Mundial. El frente civil: Los Estados Unidos I-II.* Ed.: Ediciones Folio, S. A.
2. Bauer, Friedrich L. (2000) *Decrypted Secrets.* Ed.: Springer.
3. Bell, Alan D. (1996) La próxima generación de discos compactos. *Investigación y Ciencia* **240**, 4-9.
4. Boyer, Carl B. (1999) *Historia de la Matemática.* Ed.: Alianza Editorial.
5. Cardwell, Donald (1994) *Historia de la tecnología.* Ed.: Alianza Editorial, Colección Alianza Universidad.
6. Cebrián, Juan Luis (2000) *La red.* Ed.: Punto de Lectura.
7. *Ciència, Tecnologia i Ambient, Anuari 1998.* (1999). Enciclopèdia Catalana.
8. *Diccionario Oxford de Informática* (1983). Ed.: Ediciones Díaz de Santos.
9. Flegg, Graham (1989) *Numbers Through the Ages.* Ed.: The Open University. MacMillan.
10. Gauss, Carl Friedrich (1996) *Disquisicions aritmètiques.* Traducción al catalán por G. Pascual (1801) *Disquisitiones Arithmeticae.* Ed.: Societat Catalana de Matemàtiques, Institut d'Estudis Catalans.
11. García Barreno, Pedro (dir.) (2000) *La Ciencia en tus manos.* Ed.: Espasa Calpe, Colección Espasa Fórum.
12. Guedj, Denis (1998) *El imperio de las cifras y los números.* Biblioteca de Bolsillo CLAVES. Ed.: Ediciones B, S. A.
13. Hilton, Peter (1996) Enigma, book review. *Notices AMS*, v. **43**, n. **6**, 681-682.
14. Ifrah, Georges (1997): *Historia Universal de las cifras.* Ed.: Espasa Calpe, Colección Espasa Fórum.
15. Jean, Georges (1998) *La escritura, memoria de la humanidad.* Biblioteca de Bolsillo CLAVES. Ed.: Ediciones B, S. A.
16. Kaku, Michio (1998) *Visiones.* Temas de debate. Ed.: Editorial Debate, S. A.
17. Lo, Hoy-Kwong; Popescu, Sandu; Spiller, Tim (eds.) (1998) *Introduction to Quantum Computation and Information.* Ed.: World Scientific.
18. MacWilliams, F. Jessie y Sloane, N. J. Alexander (1977) *The Theory of Error-Correcting Codes.* Ed.: North-Holland.
19. Mahon, T. (1986) *Las gentes de Silicon Valley.* Ed.: Planeta.
20. Martín Casalderrey, Francisco (2000) *Cardano y Tartaglia. Las matemáticas en el Renacimiento italiano.* La matemática en sus personajes, v. 4. Ed.: Nivola.
21. Morgan, Samuel, P. (1998) Richard Wesley Hamming (1915-1998). *Notices AMS*, v. **45**, n. **8**, 972-982.
22. National Council of Theachers of Mathematics (NCTM) (1969) *National Topics for the Mathematics Classroom.* Thirty-first Yearbook. Washington.
23. Peralta, Javier (1999) *La matemática española y la crisis de finales del siglo XIX.* Ciencia abierta, v. 1. Ed.: Nivola.
24. Perera Domínguez, Manuel (1999) ENIAC, matemáticas y computación científica. *La Gaceta de la Real Sociedad Matemática Española*, v. **2**, n. **3**, 495-518.
25. Pla, Josep (1966) *Calligraphia et tipographia. Arihtmetica et numerica. Chronologia.* Càtedra i Unitat de Paleografia i Diplomàtica. Ed.: Publicacions Universitat de Barcelona.
26. Rahman, A. (ed.) (1998) *History of Indian Science, Technology and Culture AD 1000-1800.* Ed.: Oxford University Press.
27. Santcliment, Francesc (1482): *Summa de l'art d'Aritmètica.* Introducció i notes a cura d'Antoni Malet. Ed.: Eumo Editorial, 1998.
28. Shor, Peter (1997) Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM Journal of Computing* **26**, 1484-1509.
29. Singh, Simon (2000) *Los códigos secretos.* Pequeña gran historia. Ed.: Debate.
30. Stein, Dorothy (1985) *Ada Byron. A life and a legacy.* Ed.: MIT Press.
31. Tahn, Malba (1998) *L'home que calculava.* Ed.: Editorial Empúries.
32. Vera, Francisco (1970) *Científicos Griegos I, II.* Ed.: Aguilar.
33. Vernet, Juan (1999) *Lo que Europa debe al Islam de España.* El Acantilado, 2. Ed.: Quaderns Crema.
34. Von Neumann, John (1958) *El ordenador y el cerebro.* Ed.: Bon Ton.
35. Yan, Song Y. (2000) *Number Theory for Computing.* Ed.: Springer.