Secretos de los números primos

Dr. Félix García Merayo
Profesor Titular de Unversisdad-UPM.
Vicepresidente de ACTA

INTRODUCCIÓN

Si queremos contar la historia de un hecho, de un concepto, si queremos exponer sus propiedades, sus características, es obligado comenzar con unas definiciones, no sólo las que afecten directamente al concepto, número primo en este caso, sino también otras asociadas al mismo y que va a constituir el hilo conductor de este trabajo.

Supongamos $p > 1$ un entero perteneciente al conjunto $\mathbf{N}=\{0, 1, 2, 3, ...\}$ de los números naturales. Se dice que p es un número **primo absoluto** o, simplemente, **primo**, cuando los únicos divisores que admite en ese campo de los naturales es el 1 y el propio p. Según este criterio de la definición, son primos los números 2, 3, 5, 7, 11, ... No lo son, 4, 6, 8, 9, 10,....

Cualquier número natural que no sea primo, decimos que es **compuesto**. En este último caso, tal número equivale al producto de varios primos. Por ejemplo, el número compuesto 20, puede escribirse como

$$20 = 2 \cdot 2 \cdot 5 = 2^2.5$$

Por ello, se establece el teorema en el que se demuestra que todo número compuesto $m \in \mathbf{N}$, puede siempre expresarse mediante un producto formado por sólo factores primos. Es lo que conocemos como *des-*

LOS CINCUENTA PRIMEROS NÚMEROS PRIMOS

$p_1 = 2$	$p_2 = 3$	$p_3 = 5$	$p_4 = 7$	$p_5 = 11$	$p_6 = 13$	$p_7 = 17$
$p_8 = 19$	$p_9 = 23$	$p_{10} = 29$	$p_{11} = 31$	$p_{12} = 37$	$p_{13} = 41$	$p_{14} = 43$
$p_{15} = 47$	$p_{16} = 53$	$p_{17} = 59$	$p_{18} = 61$	$p_{19} = 67$	$p_{20} = 71$	$p_{21} = 73$
$p_{22} = 79$	$p_{23} = 83$	$p_{24} = 89$	$p_{25} = 97$	$p_{26} = 101$	$p_{27} = 103$	$p_{28} = 107$
$p_{29} = 109$	$p_{30} = 113$	$p_{31} = 127$	$p_{32} = 131$	$p_{33} = 137$	$p_{34} = 139$	$p_{35} = 149$
$p_{36} = 151$	$p_{37} = 157$	$p_{38} = 163$	$p_{39} = 167$	$p_{40} = 173$	$p_{41} = 179$	$p_{42} = 181$
$p_{43} = 191$	$p_{44} = 193$	$p_{45} = 197$	$p_{46} = 199$	$p_{47} = 211$	$p_{48} = 223$	$p_{49} = 227$
$p_{50} = 229$						

composición factorial de un número compuesto. Descomposición que, por otra parte, es única.

Es una convención considerar que los números 0 y 1, no son primos ni compuestos.

Puede darse una interpretación geométrica de las nociones de número primo y compuesto. En efecto; si un entero *m* es compuesto, entonces puede disponerse de forma regular en un rectángulo completo, pero no reducido a una sola línea. Si *m* es primo, esa disposición no puede conseguirse. Por ejemplo, 6 y 12, que son compuestos, pueden colocarse en forma rectangular como se indica en la Figura 1. Mientras que 5, no conseguiremos distribuirlo en un auténtico rectángulo: es un número primo.

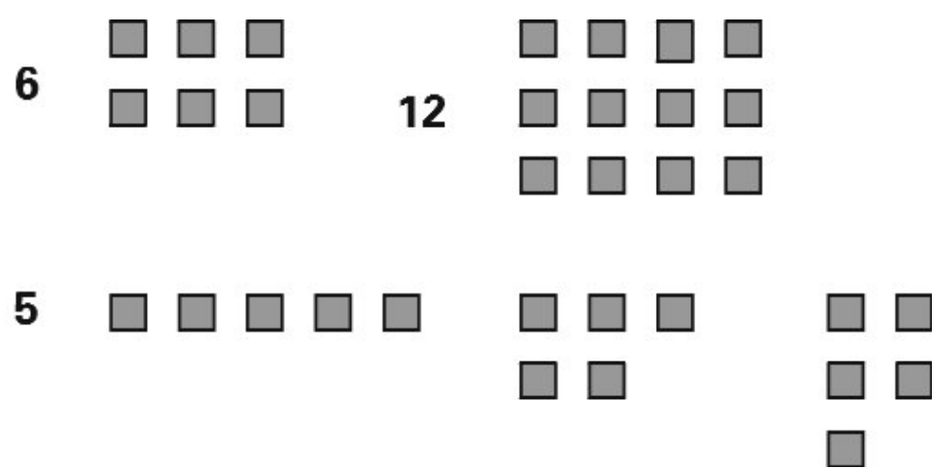

Figura 1. Representación geométrica de compuestos y primos.

Tendremos necesariamente también que definir múltiplos y divisores. Los productos de un número entero *a* por los enteros 1, 2, 3, ... reciben el nombre de **múltiplos** de *a*. También se dice que *a* es un **divisor** o submúltiplo de *b*, si podemos encontrar un entero *r* que al multiplicarlo por *a* nos da *b*. En teoría de números, eso se expresa como $b=a.r$. Así, entre los múltiplos de 7 estarían, 7x1=7, 7x2=14, 7x3=21, ...Y entre los divisores de 40, se encuentran 2, 4, 5, 10, ...

Introducida la noción de múltiplo, sabemos intuitivamente que los números enteros se distribuyen en dos grupos: los que son múltiplos de 2, que se denominan **números pares**; los restantes, son los **números impares**.

Una de las primeras nociones de la aritmética, aprendida de pequeños, es el concepto de **cociente exacto** de dos números naturales *p*, dividendo, y $q\neq0$, divisor. Se trata de realizar una operación para encontrar otro número natural *r*, tal que al multiplicarlo por el divisor obtengamos el dividendo, es decir, que sea, $p=q.r$. Tal división, que no siempre es posible, recibe el nombre de **división exacta**. Por ejemplo, 10/5=2 y 2 es el cociente exacto de la división también exacta, 10/5. No es posible, sin embargo, encontrar un cociente exacto para la división 10/3.

Por ello, también se definen los cocientes enteros de las divisiones no exactas. Sean *D* y *d*, $D \geq d$, dos números naturales no nulos y *q* otro natural tal que cumpla

$$qd \leq D < (q+1)\, d$$

Entonces, *q* y *q+1* son, respectivamente, los **cocientes enteros por defecto** y **por exceso** de la **división entera** *D*/*d*. Por ejemplo, la división 13/3 no es exacta desde el punto de vista de buscar un cociente entero único. Pero su cociente entero por defecto es 4 y el correspondiente por exceso será 4+1=5. Los enteros 4 y 5 cumplen la desigualdad propuesta anteriormente: $4.3 < 13 < (4+1).3$.

En otros lugares de este artículo nos veremos obligados a introducir otros conceptos nuevos.

LOS PRIMEROS TIEMPOS

¿Desde cuándo conoce el hombre el concepto de número primo?. La investigación de las huellas más antiguas encontradas sobre este elemento de la aritmética, nos conduce a las riveras del lago Edwards en el Zaire, África Central, donde, entre los huesos encontrados, se ha exhumado uno, el hueso de Ishango, que contiene incisiones de hace 8 000 años, aproximadamente. Se conserva en el Instituto Real de Ciencias Naturales de Bélgica, en Bruselas. Debió de servir como mango de alguna herramienta. En uno de sus tres laterales se observan cuatro grupos de incisiones de distintos tamaños que corresponden a los números 11, 13, 17 y 19, es decir, a los números primos comprendidos entre el 10 y el 20. ¿Es azar o se trata de una primera tabla de números primos?, como propone Jean de Heinzelin. Otros historiadores prefieren ver días de un calendario, otros, cuentas primitivas, fases lunares e incluso marcas hechas por alguna mujer para señalar días de su ciclo menstrual. Al suponer esto último, en algunos círculos se ha planteado la profunda cuestión: el primer matemático podría haber sido una matemática.

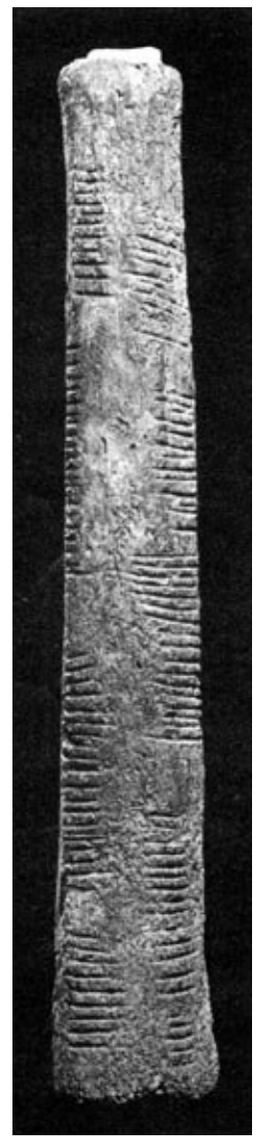

Figura 2. El hueso de Ishango.

Hasta la fecha no poseemos prueba alguna de que los egipcios o los babilonios hayan enunciado teoría, aunque sea sumaria, sobre los números primos, a pesar de que su actividad, en lo que al cálculo se refiere, estaba bien organizada y codificada. Por ejemplo, los babilonios sabían deducir *tripletas* de números *pitagóricos*, es decir, números que corresponden a las longitudes de los tres lados de un triángulo rectángulo, hipotenusa y dos catetos, y que obedecen a la relación, $a^2 = b^2 + c^2$, Figura 3. Y tal deducción exige una comprensión y precisión aritméticas que sobrepasa lo común. Por otra parte, los egipcios eran capaces de descomponer un número entero en producto de factores irreducibles y, sin embargo, no conocieron la descomposición de un entero en factores primos. Muchos investigadores afirman que los números primos debieron existir a los ojos de muchos hombres del tercer y segundo milenios, pero que el tiempo ha borrado las huellas, muescas, pinturas, dejadas sobre ellos.

Figura 3. Tabla babilónica 322 de Plimpton, Universidad de Columbia, con números pitagóricos distribuidos en cuatro columnas y quince filas.

LA ÉPOCA DE LOS GRIEGOS

Tanto el matemático griego **Pitágoras**, aproximadamente 569-500 a.C., que fue alumno de Thales, como sus discípulos, eran verdaderos apasionados de los números ya que, en su opinión, contenían las claves de la naturaleza. Durante dos siglos profundizaron en los conocimientos aritméticos. Pero sin embargo, no existe prueba alguna de que también conocieran los números primos. Pudiera deberse esto a la naturaleza secreta de su organización. Sí estudiaron sistemáticamente la noción de divisor que les condujo a la de *número perfecto*, número igual a la suma de sus divisores, contando el 1 pero excluyendo el propio número: 6 es perfecto ya que se cumple que 6=1+2+3. También les fueron familiares las nociones de *números triangulares*, cuyas unidades se pueden disponer en un triángulo o de *números cuadrados* en los que sus unidades pueden distribuirse en un cuadrado, Figura 4. Estos conceptos fueron extendidos por Boecio en el siglo V, introduciendo el concepto general de *números poligonales*.

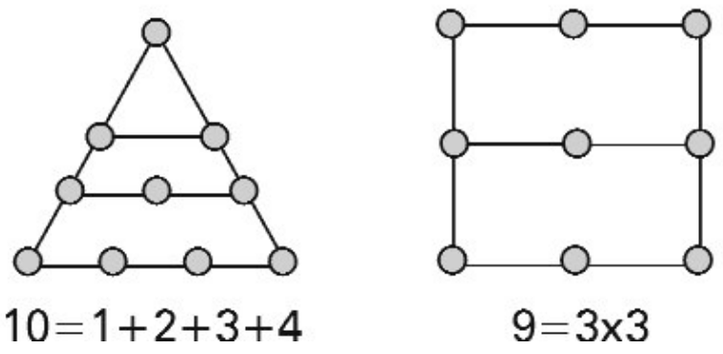

Figura 4. Ejemplos de números poligonales: triangulares y cuadrados.

El filósofo ateniense **Platón**, 428-348 a.C., fundó la escuela conocida con el nombre de Academia y, sin duda, mantuvo relación con los pitagóricos. En su *Parménide* menciona la teoría del *par* y del *impar*, pero en ningún momento se refiere a los números primos.

El vestigio más seguro y antiguo sobre el número primo aparece con la persona de **Aristóteles**, 384-322 a.C., alumno de Platón y preceptor de Alejandro Magno. Aristóteles evoca en varias ocasiones, no con teorías pero sí con ejemplos, los números primos y los compuestos.

Hacia finales del siglo IV a. C., la corriente del saber matemático pasó de Europa a África. El joven príncipe y soldado Alejandro Magno conquista el mundo griego y concibe la idea de formar un gran imperio si no hubiera sido porque su muerte a los treinta y tres años hace también que esa idea se olvide. Muere sólo dos años después de fundar la ciudad que llevaría su nombre, Alejandría. Esa población era el lugar adecuado para judíos, árabes y griegos. Allí se abrieron grandes bibliotecas y se perfeccionaron las matemáticas de los antiguos. La ciudad permaneció unos seiscientos años, pero su fin llegó en el 642 d. C., debido a las invasiones árabes surgidas por el Oeste.

La gran biblioteca de Alejandría con más de 700.000 volúmenes, fundada por Ptolomeo, sucesor de Alejandro, hacia el año 300 a.C., se pierde debido a la serie de desastres acontecidos. Pero un remanente de la ciencia y de la filosofía de esa biblioteca llegaría hasta días posteriores. En efecto, Ptolomeo creó una universidad y uno de sus primeros maestros fue **Euclides**, aproximadamente 330-275 a.C., cuyos primeros años de instrucción seguramente pasaron en Atenas, con Platón. Enseñó durante veinticinco o treinta años escribiendo, además,

sus conocidos *Elementos*. Éstos constituyen una descripción exhaustiva de las matemáticas de aquel tiempo. Los libros VII, VIII y IX enuncian la aritmética y contienen un estudio interesante de la teoría de números. Entre otras cosas, se introducen por primera vez, libro VII, definiciones y teorías sobre los números primos y compuestos, el máximo común divisor y el mínimo común múltiplo. No obstante, en otros libros como en el IX se tratan otros teoremas también sobre los números primos.

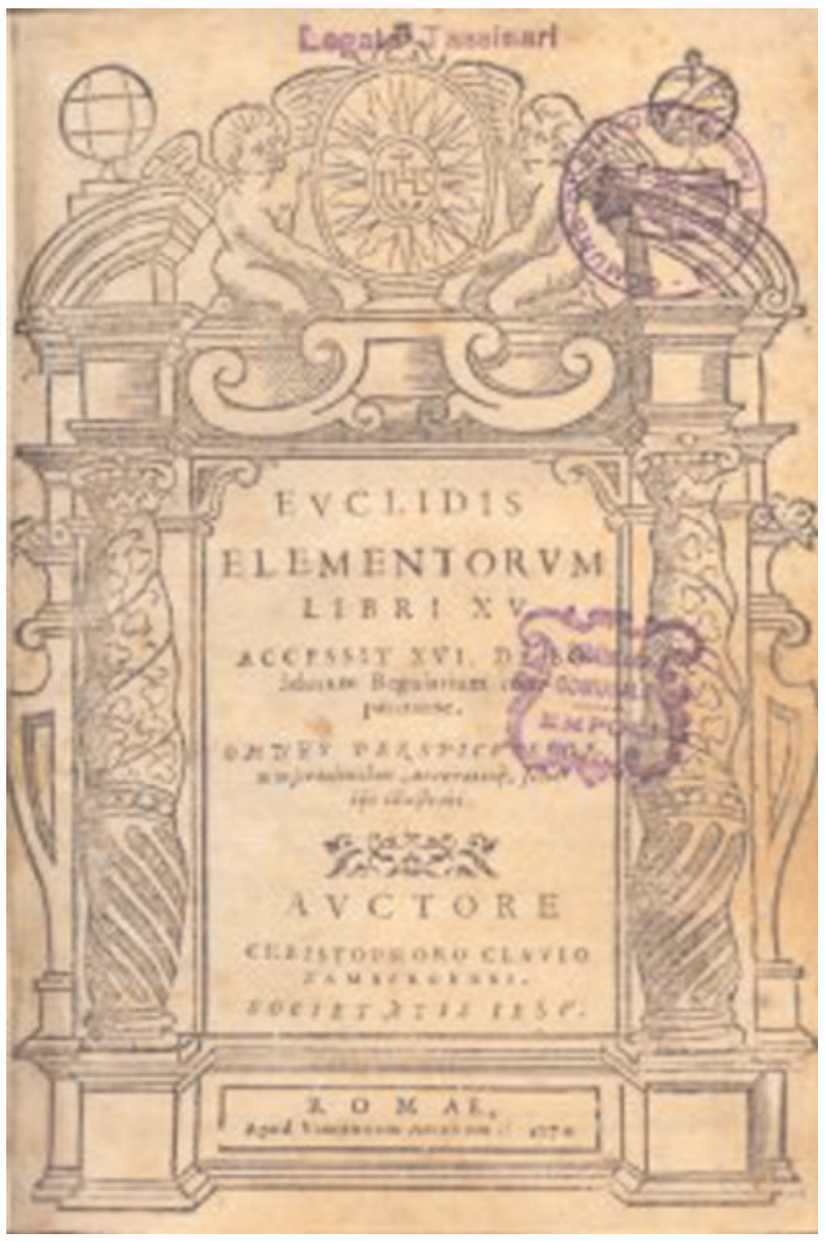

Figura 5. Portada de una edición latina del libro XV de los Elementos.

Euclides construye todo lo relativo a los números primos apoyándose en el concepto de máximo común divisor. Enuncia y demuestra resultados notables:

- El total de números primos es infinito.
- Un método para construir números perfectos pares: cuando 2^p-1 es primo, entonces el número par $2^{p-1}(2^p-1)$ es un número perfecto. Hoy día esos números primos de partida de la forma 2^p-1, se conocen con el nombre de *números primos de Mersenne*. Volveremos más adelante sobre ellos.
- Todo entero es divisible por un número primo.
- Todo número primo es primo con todo número que no le divida.
- Un producto de números primos no es divisible por ningún otro número primo.
- La potencia de un número primo sólo es divisible por ese primo y por sus potencias.

Euclides se encontró falto de una terminología y notación adecuadas para indicar tanto las potencias de un número entero como los productos. Por ello, aunque la descomposición, que ya hemos dicho que es única, de un número en factores primos era ya conocida por Euclides, es dos milenios después, en el año 1801, cuando se da, Gauss en *Disquisitiones arithmeticae*, una demostración completa y explícita. Hoy día se conoce como el *teorema fundamental de la aritmética*.

LIBRO SÉPTIMO
DE LOS *ELEMENTOS* DE EUCLIDES

.....

12. Número primo es aquél que sólo está medido por la unidad.

13. Números primos entre ellos son aquellos que tienen únicamente la unidad como medida común.

14. Número compuesto es el que es medido por cualquier número.

15. Números compuestos entre ellos son aquellos que tienen cualquier número como medida común.

.....

PROPOSICIÓN PRIMERA

Propuestos dos números distintos y restando sucesivamente el más pequeño del más grande, si el resto no mide al que está antes que él nada más que cuando se ha tomado la unidad, los números propuestos son primos entre ellos.

Para Euclides, la idea de número es totalmente geométrica. Por ello, acompañaba con frecuencia sus demostraciones aritméticas con gráficos formados por segmentos de recta. Entonces, un número ***A*** está medido con otro ***B***, si es posible hacer que ***B*** esté contenido en ***A*** un número entero de veces. Equivale a medir la longitud de un segmento con una regla patrón, Figura 6. El número ***A***=6 puede medirse con el ***B***=2. La expresión euclidiana, *2 mide a 6*, equivale a nuestra expresión actual, *2 divide a 6*, 2 es divisor de 6 ó 6 es un múltiplo de 2.

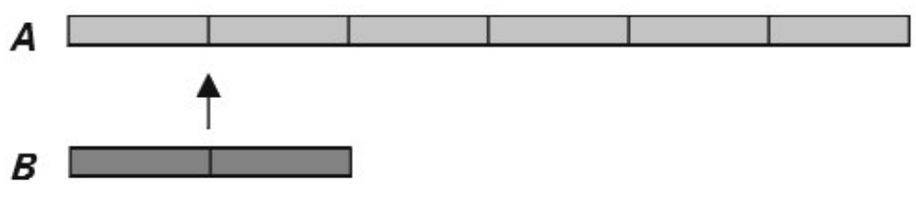

Figura 6. Concepto geométrico de número y divisor.

Haciendo uso de la proposición 12 de los *Elementos* de Euclides, estaríamos en condiciones de establecer un primer algoritmo para reconocer si un número es primo o no, comprobando si posee más divisores que el 1. Si *a* es ese número, bastará con dividirlo por todos los enteros *b* comprendidos entre 2 y *a*-1. Una división por *b* que sea exacta nos indicará que *a* no es primo, es compuesto, y el algoritmo podría detenerse a menos que deseemos encontrar todos los divisores de ese número compuesto *a*. Apliquemos este rudimentario algoritmo al entero *a*=10.

- División por 2: 10=5.2, división exacta; 10 no es primo; 2 y 5 divisores de 10.
- División por 3: 10=3.3+1, división inexacta.
- División por 4: 10=2.4+2, división inexacta.
- División por 5: 10=2.5, división exacta; 2 y 5 divisores de 10.
- División por 6: 10=1.6+4, división inexacta.
- División por 7: 10=1.7+3, división inexacta.
- División por 8: 10=1.8+2, división inexacta.
- División por 9: 10=1.9+1, división inexacta.
- Detener el algoritmo.

Conclusión: El número dado 10 no es primo y sus divisores son, 2 y 5.

Procediendo de esta manera para comprobar si un número es o no primo, se observa que se realizan cálculos innecesarios. Podríamos habernos detenido en la división por 3. Esta es la razón: si *a* no es primo, entonces cada división exacta *a*=*b.c* es tal que uno de los dos números, el *b* o el *c*, es menor o igual que el valor entero por defecto de $\sqrt{a}$, valor que se indica por $\lfloor\sqrt{a}\rfloor$. De esta proposición resulta que, para descomponer un entero y comprobar si es o no primo, es suficiente con detenerse en el valor $\lfloor\sqrt{a}\rfloor$.

En el ejemplo anterior de *a*=10, tenemos que es $\lfloor\sqrt{10}\rfloor$= 3, lo que indica que no es necesario efectuar la tercera división por 4 para deducir que el entero propuesto no es primo. Nos ahorraremos seis divisiones.

Empleando el mismo procedimiento con 101, bastaría con detenernos en la división por $\lfloor\sqrt{101}\rfloor$= 10. Todas esas divisiones por 2, 3, 4,...,10, son inexactas, luego 101 es primo.

ALGORITMO 1 PARA COMPROBAR SI UN ENTERO *a* ES PRIMO

- Intentar todas las divisiones de *a* por los enteros comprendidos entre *a* y $\sqrt{a}$.
- Al encontrar una división exacta, detenerse y concluir que *a* no es primo.
- Si no se encuentra ninguna división exacta, *a* es primo.

ALGORITMO PARA ENCONTRAR TODOS LOS DIVISORES DE *a*

- Intentar todas las divisiones de *a* por los enteros comprendidos entre *a* y $\sqrt{a}$.
- Por cada división exacta, añadir a la lista de divisores de *a*, el divisor ensayado y el cociente obtenido.

En los *Elementos* se encuentra la proposición 32 que dice:

Todo número compuesto está medido por algún número primo.

No olvidemos que *medido por* significa *divisible por*. Entonces, lo que deberíamos entender en nuestro actual lenguaje matemático, sería:

Todo número entero superior a 1 es divisible por, al menos, un número primo.

Esta proposición, contenida en el libro VII, está también demostrada allí y siguiendo razonamientos semejantes a los empleados actualmente.

A partir de la citada proposición, se demuestra también que, *si un entero a es compuesto, entonces es posible encontrar uno o varios divisores de a entre los números enteros comprendidos entre 2 y* $\sqrt{a}$. Esta proposición sirve de base para crear otro algoritmo con el que comprobar si un número es o no primo más eficaz que el descrito anteriormente.

ALGORITMO 2 PARA COMPROBAR SI UN ENTERO *a* ES PRIMO

- Intentar todas las divisiones de *a* por los enteros **primos** comprendidos entre *a* y $\sqrt{a}$.
- Al encontrar una división exacta, detenerse y concluir que *a* no es primo.
- Si no se encuentra ninguna división exacta, *a* es primo.

Resumiendo: comprobar si un número es primo se consigue realizando, como mucho, $\lfloor\sqrt{a}\rfloor$ divisiones, aplicando el Algoritmo 1 e incluso menos con el Algoritmo 2.

No obstante, este último algoritmo, que se presenta como el más económico de los dos descritos en cuanto a número de operaciones a realizar, solo será aplicable si el entero *a* es lo suficientemente pequeño; de no darse esta condición, el problema con el que nos encontraríamos sería el tener que conocer los números primos hasta $\sqrt{a}$.

Para encontrar los números primos contenidos en un determinado intervalo, el matemático griego **Eratóstenes**, aproximadamente 276-194 a.C., inventa un procedimiento que desde hace años se conoce con el nombre de *criba de Eratóstenes*, criba que nos fue dada a conocer por Nicómaco de Estagira que vivió 300 años después que él. Eratóstenes nació en Cirene, hoy en Libia. Estudió en Alejandría y más tarde en Atenas antes de acceder a la dirección de la biblioteca de Alejandría. Fue el preceptor del hijo de Ptolomeo III. Y no sólo se dedicó a la aritmética, sino también a otros dominios de la matemática y de la geometría, a él se debe la medición del perímetro de la Tierra, además de ser un gran atleta.

La *criba* es un método muy popular para encontrar los números primos sucesivos dentro de un determinado intervalo. Advertir que, no obstante, este método no nos proporciona una regla para obtener ordenadamente una relación de todos los números primos. Hagamos una descripción del algoritmo con que formarla y supongamos que nos proponemos buscar los primos entre el 2 y el 100. El procedimiento es generalizable, aunque no efectivo, para límites cualquiera *m* , *n*.

- Escribir todos los enteros entre el 2 y el 100.
- Se conserva el primer primo, el 2, y se suprimen todos sus múltiplos, lo que equivale a ir suprimiendo los elementos de la tabla de dos en dos.
- Se conservará el siguiente entero no suprimido, el 3, también primo, y se suprimirán todos sus múltiplos.
- Se conservará el siguiente entero no suprimido, el 5, que también es primo, suprimiendo después todos sus múltiplos.

¿Y cuándo finalizaremos este proceso?. Se continuará con el proceso de supresión hasta alcanzar el mayor entero sin suprimir cuyo cuadrado no exceda, en nuestro caso, de 100, es decir, hasta el 10. En la Figura 7 podemos encontrar la lista de los números primos hasta el 100. Al llegar al 11, ya no se suprimirá ninguno más, ya que es $11^2>100$.

2	3	~~4~~	5	~~6~~	7	~~8~~	~~9~~	~~10~~	11	~~12~~	13
~~14~~	~~15~~	~~16~~	17	~~18~~	19	~~20~~	~~21~~	~~22~~	23	~~24~~	~~25~~
~~26~~	~~27~~	~~28~~	29	~~30~~	31	~~32~~	~~33~~	~~34~~	~~35~~	~~36~~	37
~~38~~	~~39~~	~~40~~	41	~~42~~	43	~~44~~	~~45~~	~~46~~	47	~~48~~	~~49~~
~~50~~	~~51~~	~~52~~	53	~~54~~	~~55~~	~~56~~	~~57~~	~~58~~	59	~~60~~	61
~~62~~	~~63~~	~~64~~	~~65~~	~~66~~	67	~~68~~	~~69~~	~~70~~	71	~~72~~	73
~~74~~	~~75~~	~~76~~	~~77~~	~~78~~	79	~~80~~	~~81~~	~~82~~	83	~~84~~	~~85~~
~~86~~	~~87~~	~~88~~	89	~~90~~	91	~~92~~	~~93~~	~~94~~	~~95~~	~~96~~	97
~~98~~	~~99~~	~~100~~									

Figura 7. Lista de los primos comprendidos entre 2 y 100.

Hemos advertido que para números altos el procedimiento es ineficaz. Resultará más útil aplicar el ALGORITMO 1, descrito anteriormente, para conocer si un entero es primo o compuesto.

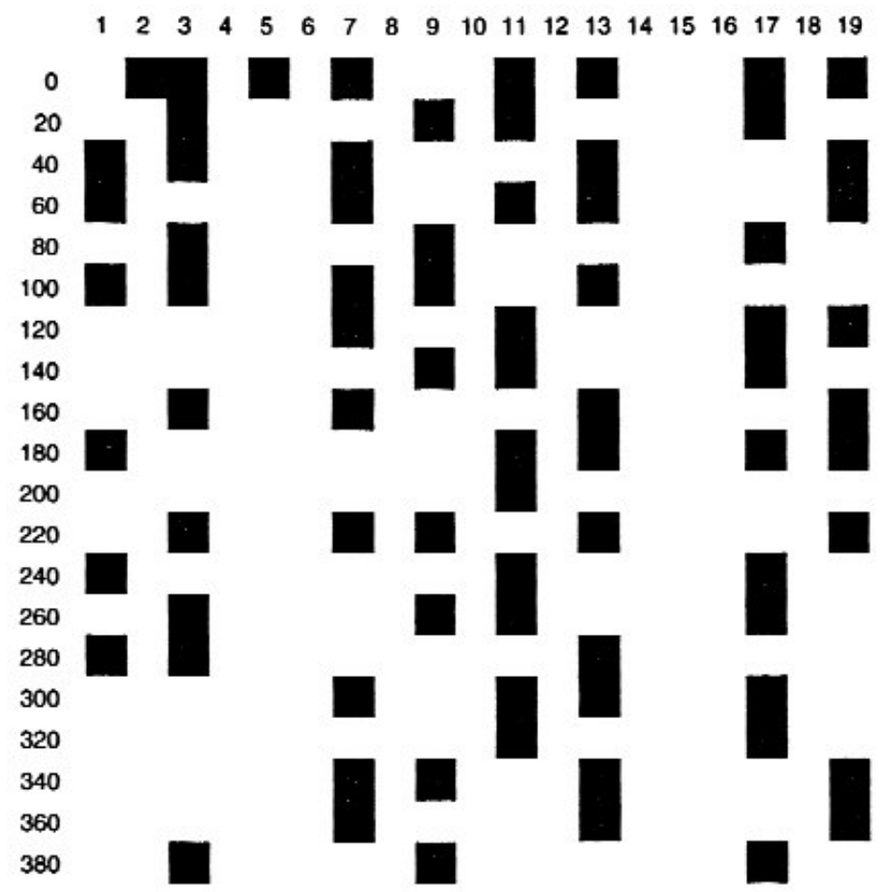

Figura 8. La criba aplicada a los 400 primeros enteros.

En la Figura 8 se representa, en forma de tablero enlosado de 20x20, el resultado de la criba de Eratóstenes aplicada a los 400 primeros números enteros. Las columnas correspondientes a los números pares y a los múltiplos de 5 están vacías, excepto las que corresponden al 2 y al 5.

GRANDES NÚMEROS

Hoy día, conocemos muy bien las propiedades aritméticas de los *números pequeños*; pero nos vemos enfrentados habitualmente al manejo de *grandes números* de los que comienza a escapársenos su manejo, sus propiedades. En

concreto, y en relación con los números primos, vamos a enunciar algunas consideraciones que dejan patente la dificultad de su manejo a medida que crece el número de sus cifras.

Números de 9 ó 10 cifras

No existe dificultad alguna para factorizar mediante números primos los enteros de este tamaño y es posible también construir la tabla de primos correspondiente.

Números de 100 cifras

No es posible, y lo será por mucho tiempo, construir una tabla de números primos que posean 100 cifras e, incluso, menos. No obstante, lo que sí es posible es comprobar si un número con esas cifras es o no primo.

Números con 1000 cifras

Existen tests probabilísticos con un alto grado de certidumbre para comprobar si un entero de ese tamaño de cifras es o no primo. Es común el uso en criptografía de números primos de mil cifras.

Números con un millón de cifras

Se sabe comprobar si un número de ese tamaño es o no primo sólo cuando posea una forma particular: 2^p-1, números de Mersenne. Para ellos se dispone de un algoritmo especial.

Números con mil millones de cifras

Es muy posible que nunca pueda conocerse un número primo de este tamaño.

LOS INDIOS, LOS MULSULMANES, LOS ITALIANOS

Los matemáticos de la época Antigua y de la Edad Media estuvieron preocupados más por la geometría que por los números y por razonar sobre ellos. Esta falta de interés quedó obviada cuando se adoptó el sistema decimal indio, es decir, la notación posicional que daba al número un valor según la localización que tuviera dentro de una cantidad. En concreto, en Europa la notación posicional se adoptó en el siglo XI.

En el mundo musulmán, hemos de citar a **Ibn al-Banna**, 1258-1339, que vivió en el Marruecos actual, que conoció y utilizó la *criba de Eratóstenes*, por tanto también los números primos, y que dejó anotado que para encontrar los primos hasta el número *n*, era suficiente con examinar los múltiplos de números inferiores hasta el $\sqrt{n}$.

En la Italia medieval, destacar a **Fibonacci**, Leonardo de Pisa, 1170-1250, gran conocedor de los matemáticos árabes, nos dejó una lista de los enteros primos inferiores al 100 con la misma anotación a la que ya hemos aludido anteriormente al referirnos a Ibn al-Banna.

En este recorrido por la historia de los números primos vamos ahora a dar el salto hasta el siglo XVI por encontrar en ese tiempo hechos relevantes sobre la aritmética y el conocimiento de tales números. Comenzaremos con dos matemáticos franceses.

BACHET DE MÉZIRIAC Y MARÍN MERSENNE

Claude Gaspard **Bachet de Méziriac**, 1581-1638, encontró un resultado aritmético relacionado con el máximo común divisor de dos números *a* y *b*. Dice así: *si es mcd(a,b)=c, entonces existen dos enteros x e y tales que ax+by=c*. Esta última identidad ha sido atribuida, erróneamente y durante años, a **Étienne Bezout** y se conoce por ello como *teorema* o *identidad de Bezout*.

Pero lo más notable de Méziriac es el siguiente enunciado sobre números primos, aparecido en su publicación, *Problèmes plaisants et délectables*, en 1624: *dados dos números primos, a y b, al encontrar el menor múltiplo de cada uno de ellos, ambos múltiplos se diferencian en una unidad el uno del otro.* Aritméticamente lo expresaríamos así: $ax - by=1$. En su misma publicación, él da el procedimiento a seguir para encontrar una solución general al problema enunciado, procedimiento muy próximo al algoritmo de Euclides utilizado para calcular el máximo común divisor de dos números.

Marin **Mersenne**, 1588-1648, estudió en el colegio de los jesuitas de La Flèche, donde también cursó estudios Descartes, antes de tomar los hábitos de la orden de *los mínimos*. También estudió teología en la Sorbona. Publicó obras de ciencias y filosofía, siendo un defensor de las teorías de Galileo. El padre Mersenne mantuvo correspondencia con sabios como Descartes, Pascal, Torricelli, Huygens y otros. Se interesó por analizar si los números de la forma 2^p-1, números que llevan su nombre, son o no primos. Ya dijimos que tales números eran conocidos por Euclides. Se designan por M_p precisamente en honor a Mersenne.

Mersenne trató de encontrar, como hemos advertido, una fórmula que representara a todos los primos. No la encontró; pero su trabajo sobre números de la forma 2^p-1, *p* primo, ha suscitado, a través del tiempo, un gran interés, sobre todo en la investigación de números pri-

mos grandes.

En 1644, Mersenne afirmaba que $M_p=2^p-1$ era un número primo para p=2, 3, 5, 7, 13, 17, 19, 31, 67, 127, 257 y compuesto para los otros exponentes hasta el 257. En 1732, Euler pretende ampliar la lista afirmando que M_{41} y M_{47} eran primos, pero se equivoca. En 1883, Pervushin y también Lucas encuentran un primer error en la lista de Mersenne: prueba que M_{61}, ausente de la lista citada, es primo. Se descubren otros cuatro errores: M_{67} y M_{257} no son primos, mientras que M_{89} y M_{107}, también ausentes de la relación de Mersenne, sí lo son.

Actualmente se conocen 38 números primos de Mersenne. El primero de ellos para p=2, es decir, M_2=3 y el último para p= 6972593, es decir, $Mp=2^{6972593}-1$, que contiene más de dos millones de cifras, exactamente 2 098 960. Fue descubierto por Hajratwala, Woltman, Kurowski y otros en 1999, empleando para ello varios ordenadores y bajo el proyecto *GIMPS*, *Great Internet Mersenne Prime Search*. No obstante, no puede afirmarse que la lista se componga de sólo 38 números: es posible que existan otros en el enorme intervalo comprendido entre $2^{3021377}-1$ y $2^{6972593}-1$, pero no se han encontrado aún. Quizá eso suceda cuando los computadores cuánticos sean una realidad y sirvan como instrumento real de computación.

NÚMERO	TOTAL CIFRAS	AÑO	ORDENADOR	EQUIPO
$180(M_{127})^2+1$	79	1951	EDSAC 1	Miller & Wheeler
M_{521}	157	1952	SWAC	Robinson
M_{607}	183	1952	SWAC	Robinson
M_{1279}	386	1952	SWAC	Robinson
M_{2203}	664	1952	SWAC	Robinson
M_{2281}	687	1952	SWAC	Robinson
M_{3217}	969	1957	BESK	Riesel
M_{4253}	1 281	1961	IBM 7090	Hurwitz
M_{4423}	1 332	1961	IBM 7090	Hurwitz
M_{9689}	2 917	1963	ILLIAC 2	Gillies
M_{9941}	2 993	1963	ILLIAC 2	Gillies
M_{11213}	3 376	1963	ILLIAC 2	Gillies
M_{19937}	6 002	1971	IBM 360/91	Tuckerman
M_{21701}	6 533	1978	Cyber 174	Noll , Nickel
M_{23209}	6 987	1979	Cyber 174	Noll
M_{44497}	13 395	1979	Cray 1	Nelson , Slowinski
M_{86243}	25 962	1982	Cray 1	Slowinski
M_{132049}	39 751	1983	Cray X-MP	Slowinski
M_{216091}	65 050	1985	Cray X-MP	Slowinski
$391\,581\times2^{216193}-1$	65 087	1989	Amdahl 1200	Brown
M_{756839}	227 832	1992	Cray 2	Slowinski , Gage
M_{859433}	258 716	1994	Cray C90	Slowinski , Gage
$M_{1257787}$	378 632	1996	Cray T94	Slowinski , Gage
$M_{1398269}$	420 921	1996	Pentium 90Mhz	GIMPS Woltman, Armengaud
$M_{2976221}$	895 932	1997	Pentium 100Mhz	GIMPS Woltman, Spence
$M_{3021377}$	909 526	1998	Pentium 200Mhz	GIMPS Wo., Kurowski, Clarkson
$M_{6972593}$	2 098 960	1999	Machines variées	GIMPS Hajratwala, Wo., Ku

Tabla 1. Números más grandes de Mersenne obtenidos por ordenador.

Otros muchos sabios y científicos han estado relacionados con los números primos y a la magia que encierran. La lista sería demasiado larga y hablar detalladamente de sus contribuciones al tema desbordaría los límites de este trabajo. No obstante daremos algunos nombres.

- El francés **Fermat**, 1601-1665, con sus teoremas demostrados y sus conjeturas, como la que afirma que *todo número de la forma* $F_n=2^{2^n}+1$ *es primo*.

- **Pascal**, 1623-1662, filósofo, matemático, inventor de la calculadora *Pascalina* y al que se le debe el establecimiento de criterios generales de divisibilidad.

- Christian **Goldbach**, nacido en Könisberg, 1690, y fallecido en Mocú, 1764, célebre por su conjetura, *todo número par superior a 2 puede escribirse como suma de dos números primos*, conjetura que aún no ha sido probada, aunque la mayoría de los matemáticos la hayan considerado siempre cierta.

- Nos referimos ahora al matemático más grande de todos los tiempos, el suizo Leonardo **Euler**, 1707-1783. Mantuvo correspondencia con Goldbach que le transmite la conjetura de Fermat, citada anteriormente, que le sirve para interesarse por los números primos. Prueba entre 1753 y 1772 que $M_{31}=2^{31}-1$ es primo, número que quedaría como el primo más grande encontrado hasta ese momento.

- Entre 1730 y 1866, **Bezout**, **Gauss**, **Legendre**, **Dirichlet**, **Tchebychev**, **Riemann**. Entre 1842 y 1962, **Lucas**, **Hadamar**, **La Vallée Poussin**.

CÓMO PROBAR SI UN NÚMERO GRANDE ES PRIMO

Test de Lucas-Lehmer

2^p-1 es primo si y sólo si 2^p-1 divide a $S(p-1)$, siendo $S(1)=4$ y $S(n+1)=S(n)^2-2$, $n>1$.

Teorema de Proth, 1878

Si N es de la forma $N=k.2^n+1$, con $k<2^n$, y existe un entero a tal que

$$a^{(N-1)/2}+1 = 0 \pmod N$$

entonces, N es un número primo. La relación última es una relación de congruencia.

Hemos citado a Edouard **Lucas**. Nación en Amiens en 1842 y murió en Paris en 1891. Lucas descubrió un método para comprobar si un número de Mersenne es o no primo. El método se conoce con el nombre de *test de Lucas*. Fue mejorado en 1930 por el americano Lehmer, proporcionando un algoritmo que más tarde se ha utilizado en computadores. El test de Lehmer sirve actualmente para comprobar la fiabilidad de los supercomputadores.

Lucas considera la sucesión r_n de enteros naturales definida por la ecuación de recurrencia, $r_{n+1}=r_n^2-3$, con la condición inicial, $r_1=3$. Entonces, el número de Mersenne con p de la forma $p=4k+3$, es primo, si y sólo si M_p divide a r_{p-1}.

DISTRIBUCIÓN DE LOS NÚMEROS PRIMOS

La separación entre dos números primos consecutivos es con una frecuencia infinita igual a 2 unidades. Esto es lo que ocurre, por ejemplo, con los pares 3-5, 5-7, 11-13, 17-19, 29-31, 37-41, 43-47, ..., que reciben el nombre de *primos gemelos*. Sin embargo, entre los números $n!+2$ y $n!+n$, por ejemplo, no existe ningún número primo, todos son compuestos. Tomando números lo suficientemente grandes, la separación entre dos primos consecutivos es también tan grande como se quiera. Resumiendo: la separación entre dos primos consecutivos oscila ampliamente y no sigue ninguna regla estable. Sobre este tema existen numerosas conjeturas pero ninguna de ellas está probada. Una es precisamente la relacionada con los primos gemelos: *existe un número infinito de números primos p tales que, p+2 también es primo.*

Si nos apoyáramos en la criba de Eratóstenes podríamos deducir los resultados que se recogen en la tabla que sigue, en la que se da una distribución, por intervalos de enteros, del total de números primos contenidos en cada intervalo.

INTERVALO	TOTAL	ACUMULADO
1 – 10	4	4
10 – 20	4	8
20 – 30	2	10
30 – 40	2	12
40 – 50	3	15
50 – 60	2	17
60 – 70	2	19
70 – 80	3	22
80 – 90	2	24
90 – 100	1	25

Tabla 2. Distribución de los números primos entre 2 y 100.

Como podemos observar, la distribución está lejos de ser uniforme o, como ya hemos dicho, de seguir una tendencia.

Si trabajásemos con una tabla mucho más amplia que la escrita, y contabilizásemos los números primos comprendidos entre 1 y 10^n, con n lo suficientemente grande, nos encontraríamos con resultados como los siguientes:

Entre 1 y 10 , 4
Entre 1 y 10^2 , 25
Entre 1 y 10^3 , 168
Entre 1 y 10^4 , 1229
Entre 1 y 10^5 , 9592
Entre 1 y 10^6 , 78498
.....

A este respecto, y en la teoría de números primos, se utiliza una función denominada **función de números primos π**, para indicar el total de primos menores o iguales a un cierto entero. Entonces, $\pi(m)$ significaría el total de primos menores o iguales a m. Por ejemplo, considerando la tabla anterior, tendríamos, $\pi(10)=4$, $\pi(20)=8$, $\pi(100)=25$.

Hemos dicho más arriba que la sucesión de los números primos es infinita. Haciendo uso de la función $\pi(m)$, podríamos expresar lo mismo escribiendo, $lim_{m\to\infty}\ \pi(m) = \infty$.

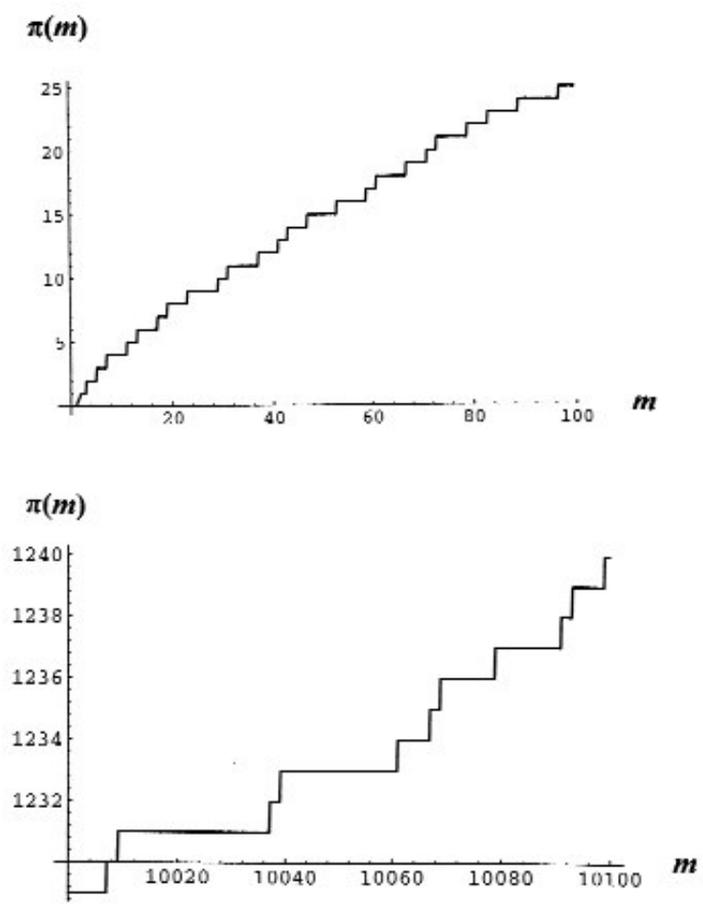

Figura 9. Gráficas de $\pi(m)$, $1 \le m \le 100$ y $10000 \le m \le 10100$.

Volviendo a los intervalos señalados en la tabla anterior, observamos y confirmamos que la distribución de los números primos no presenta tendencia alguna, Figura 9. Al final del siglo XVIII, tales observaciones condujeron, de forma independiente, a Gauss y Legendre a establecer la hipótesis o conjetura de que el número $\pi(m)$ tiene, para cada uno de ellos, respectivamente, los valores aproximados siguientes:

$$\pi(m) \approx \frac{m}{l_e m} \quad \text{o bien} \quad \pi(m) \approx \frac{m}{l_e m - 0{,}83}$$

Si aplicásemos la aproximación de Gauss al caso $m=100$, encontraríamos el valor 22, mientras que la tabla nos dice que exactamente existen 25 números primos iguales o menores que 100. Para el caso $m=1000$, al que corresponde exactamente 168 primos, el resultado que obtendríamos con la fórmula es de 144. Para $m=10^6$, se obtiene el valor aproximado de 72382 que se diferencia del exacto en 6116 unidades.

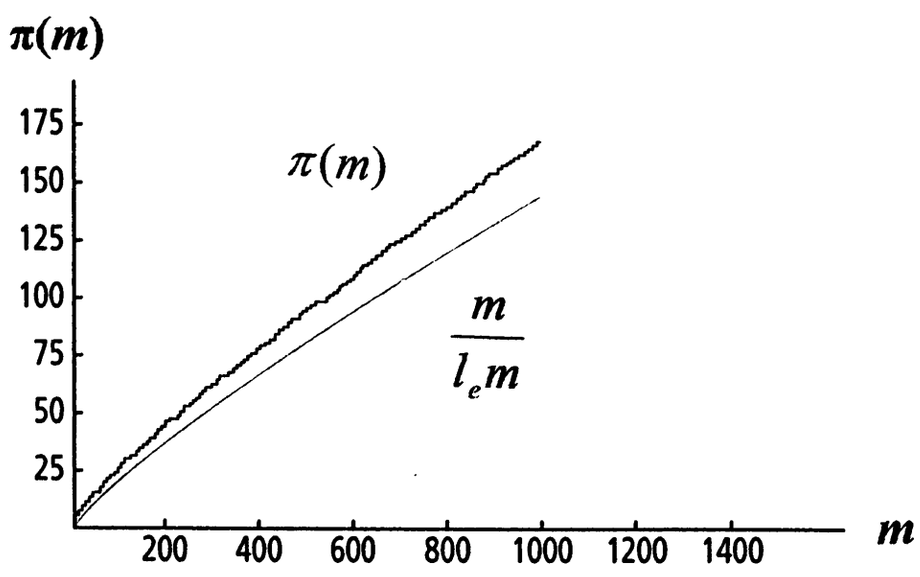

Figura 10. Curvas $\pi(m)$ y $m/l_e m$, para valores de m.

Las conjeturas de Gauss y Legendre se convierten en teorema demostrado, en 1895, por Hadamard y La Vallée Poussin, una vez más de forma independiente. El teorema se conoce como *Teorema de los números primos.*

Pero antes en el tiempo, concretamente en 1852, Chebyshev se convirtió en el primer matemático, después de Euclides, que demostró la siguiente relación sobre la función π:

$$0{,}929 \frac{m}{l_e m} < \pi(m) < 1{,}1 \frac{m}{l_e m}$$

Con la aparición de los grandes ordenadores, los métodos para el cálculo de π han mejorado mucho. Así, en 1994, Marc Deleglise y Rivat obtuvieron el valor de $\pi(10^{18})$, que es del orden de $24{,}7 \times 10^{15}$. Hoy día, se ha llegado a calcular $\pi(10^{20})$ que es del orden de $22{,}2 \times 10^{17}$.

UNA FÓRMULA PARA ENCONTRAR TODOS LOS NÚMEROS PRIMOS

Ya hemos dicho que la sucesión de números primos es infinita. Desde que se conoce este hecho, los matemáticos buscan una fórmula que suministre tales números. Al no ser esto posible, a la fecha, se han conformado con algo más modesto: fórmulas que proporcionen una cantidad muy amplia de números primos. Veamos algunas de ellas.

Nos hemos referido a la conjetura de Fermat de que los números de la forma $F_n = 2^{2^n}+1$, son primos. Para $n=0, 1, 2, 3$ y 4, se obtienen los valores 3, 5, 17, 257 y 65537, que efectivamente son primos. Pero aplicando la fórmula para F_5, el número obtenido ya no lo es. Este resultado nos lleva a afirmar que, a partir de $n=5$, algunos números de Fermat no son primos.

Una tentativa de buscar una fórmula algo más prometedora, pero sin duda poco eficiente, fue la debida al matemático inglés Hardy, 1877-1947. La fórmula expresa que, para todo entero m, el factor primo más grande $H(m)$ de m es,

$$H(m) = \lim_{r\to\infty} \lim_{p\to\infty} \lim_{q\to\infty} A(r, p, q)$$

siendo A una función de tipo trigonométrico. Como puede concluirse, el interés práctico de esta fórmula es nulo. Existen otros métodos más sencillos y más rápidos para calcular $H(m)$.

En toda la bibliografía sobre teoría de números y, en especial, sobre primos, se cita la espiral de Ulam de la que se deduce una nueva fórmula para encontrar números primos. El matemático Estanislao Marcin Ulam, 1909-1984, de origen polaco, asistía en 1963 a una conferencia más bien aburrida, en su opinión, por lo que se entretuvo escribiendo sobre una hoja de papel cuadriculado la sucesión de los números enteros en forma de espiral, Figura 11. La sorpresa fue que los números primos mostraban una tendencia evidente a alinearse en diagonales dentro del cuadro obtenido.

Debido a este descubrimiento, Ulam, David Wells y Myron decidieron trabajar con espirales que comenzaban en enteros distintos del 1. La que comienza en 41 presenta una perfecta diagonal de números primos.

Ulam, además, descubre una fórmula que ya había sido propuesta por Euler:

$$P(m) = m^2+m+41$$

fórmula con la que pueden encontrarse números primos para los cuarenta primeros valores de m, desde el cero

en adelante. Así, es P(0)=41, P(1)=43, P(2)=47, ..., P(24)=641, ..., P(39)=1601, valores primos situados sobre una diagonal de Ulam.

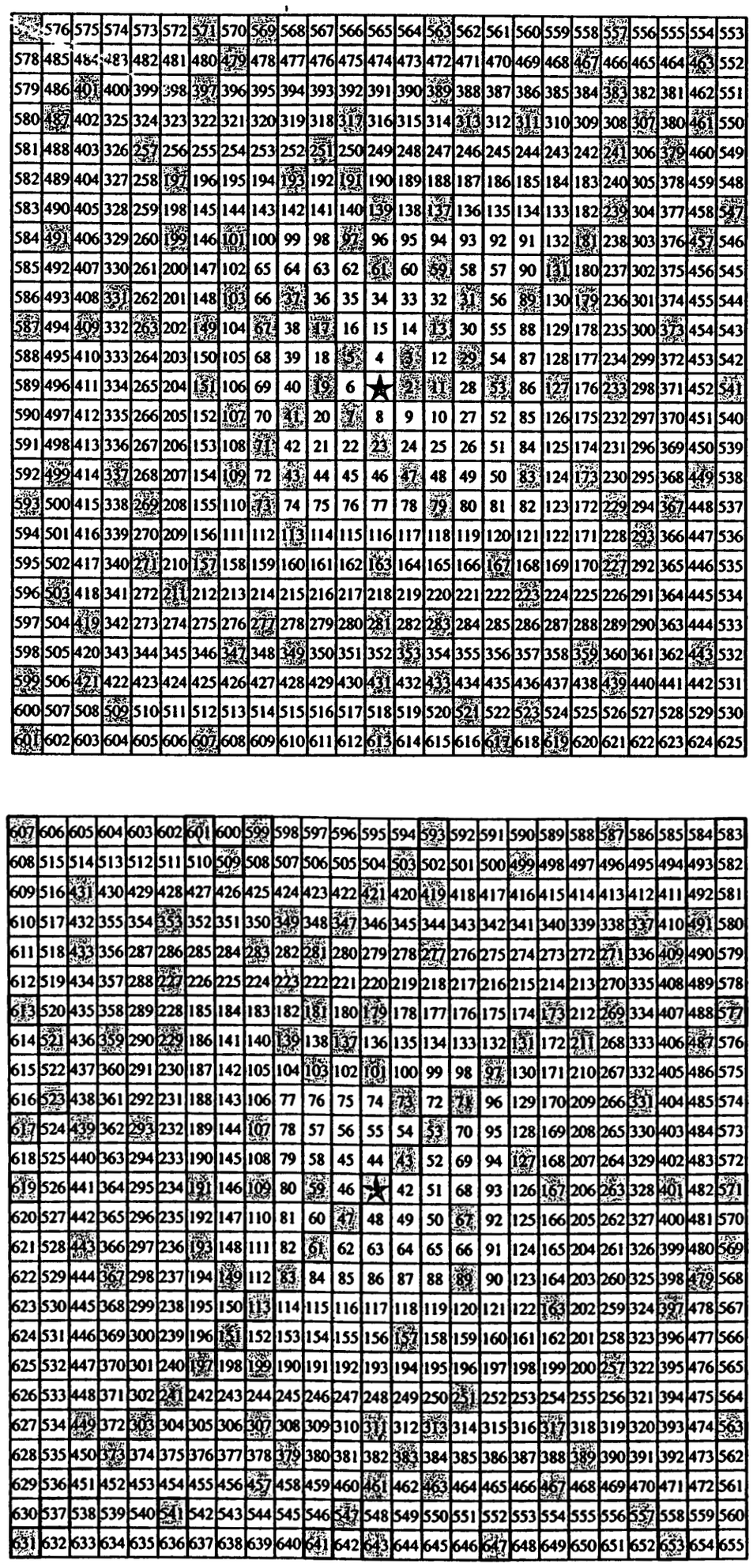

Figura 11. Espirales de Ulam desde el 1 al 625 y desde el 41 al 655.

La fórmula anterior, para $1 \leq m \leq 107$, proporciona un número primo prácticamente de cada dos, exactamente con un porcentaje de acierto del 47,5%.

Ulam descubrió otras fórmulas bastante eficientes:

- La expresión, $P(m)= 4m^2+170m+1847$ tiene un porcentaje de éxito de cerca del 47% y proporciona 760 primos no encontrados por la fórmula de Euler.
- La fórmula de Ulam, $P(m)=4m^2+4m+59$ tiene un porcentaje de éxito de casi el 44% y nos da 1500 primos no encontrados por ninguna de las dos fórmulas anteriores.

No obstante, y para terminar, no existe fórmula polinómica alguna que nos proporcione todos los números primos. Dicho de forma más precisa: no puede existir polinomio alguno que engendre sólo números primos cuando su variable recorra el conjunto de los números naturales.

Encontrar una fórmula para generar todos los números primos es una cuestión que acaba de comenzar, pero ni mucho menos resuelta.

Lo que se lee sin esfuerzo ninguno
se ha escrito siempre con un gran esfuerzo.

Jardiel Poncela

Algunos esquemas contenidos en este artículo han sido tomados y, en algún caso, modificados de Merveilleux nombres premiers, ediciones BELIN y de Secrets de nombres, ediciones ARCHIMÈDE