Números con nombre propio... e incluso apellido

Vicente Trigo Aranda

La teoría de números es una de las ramas clásicas de las Matemáticas y, seguramente, la más conocida, ya que muchos de sus resultados pueden comprenderse con sólo unos conocimientos rudimentarios de aritmética. De hecho, algunos de los grandes nombres, como Fermat, ni siquiera eran matemáticos profesionales.

En este artículo presentaré una sencilla introducción a este apasionante tema y le hablaré de una serie de números que resultan bastante curiosos para el público en general: primos, perfectos, amigos, etc. Su estudio fue considerado durante muchos siglos una especie de entretenimiento para matemáticos un tanto chalados... pero, como verá más adelante, su importancia actual no es desdeñable, ni mucho menos.

Además, para hacer más atractivo este asunto, hay una serie de cuestiones que aún permanecen abiertas a lo largo de miles de años; conjeturas que todavía no se ha podido demostrar ni que sean ciertas ni que sean falsas. ¿Qué especialidad científica puede ofrecer una serie de problemas tan sencillos que hasta son comprensibles por estudiantes de Primaria y que han resistido los ataques de los mejores cerebros de la humanidad? ¿No le gustaría pasar a la pequeña historia de las Matemáticas encontrando alguna solución? ¡Quién sabe! ... De todas formas, mi objetivo es mucho más modesto y me conformaré con que pase un rato entretenido leyendo este artículo.

TODO COMENZÓ EN GRECIA

El estudio científico y riguroso de las propiedades de los números se desarrolló durante la llamada Grecia Clásica y para comprender el por qué de ese enorme interés es preciso hacer un par de consideraciones previas.

La primera es de índole sociocultural. El concepto de ciudadano libre surgió en el siglo V aC en Atenas, dando lugar a su vez al nacimiento de la democracia. No obstante, no es oro todo lo que reluce... Según diversos estudios, en aquél entonces más de la mitad de la población eran esclavos (cuyo número aumentó con las posteriores conquistas de Alejandro) y los extranjeros rondaban la tercera parte; es decir, sólo alrededor de un 20% de los habitantes eran ciudadanos libres.

Había por tanto una parte de la sociedad que disponía de mucho tiempo libre (¿quién ha dicho que la cultura del ocio es un concepto actual?)... y tenga presente que no existía la tele ni Internet y el equivalente a los libros era artículo de superlujo. En resumen, el aburrimiento era tal que se inventaron las olimpíadas, el teatro, la poesía, etc., pero a pesar de todo seguían teniendo mucho tiempo para rellenar. El estudio de los números, que no exige grandes conocimientos matemáticos, podía ser un aceptable sustituto de los actuales crucigramas y pasatiempos.

Además, los números para los griegos cumplían una condición imprescindible para ser tomados en consideración: su utilidad práctica era completamente nula para ellos. La clase dirigente de una sociedad basada en la esclavitud no sólo no necesita resolver cuestiones técnicas, ya que otras personas son quienes trabajan, sino que además mira con malos ojos cualquier intento de avance en ese terreno.

Tan es así, que sólo un griego ha pasado a la historia de la matemática aplicada (en cambio, los surgidos en filosofía son incontables): Arquímedes. Este gran científico es considerado uno de los mayores cerebros de la humanidad, a la altura de Newton o Einstein, y nació el 287 aC en Siracusa... una colonia griega ubicada en Sicilia[1].

La segunda cuestión tiene que ver con el poco sofisticado sistema de numeración griego. Empleaban las letras de su alfabeto como signos de signos de numeración, de acuerdo con la siguiente tabla[2]:

Unidades			Decenas			Centenas		
Α α	Alfa	1	Ι ι	Iota	10	Ρ ρ	Rho	100
Β β	Beta	2	Κ κ	Kappa	20	Σ σ	Sigma	200
Γ γ	Gamma	3	Λ λ	Lambda	30	Τ τ	Tau	300
Δ δ	Delta	4	Μ μ	My	40	Υ υ	Ypsilon	400
Ε ε	Épsilon	5	Ν ν	Ny	50	Φ φ	Fi	500
			Ξ ξ	Xi	60	Χ χ	Ji	600
Ζ ζ	Dseta	7	Ο ο	Ómicron	70	Ψ ψ	Psi	700
Η η	Eta	8	Π π	Pi	80	Ω ω	Omega	800
Θ θ	Zeta	9						

Su sistema de numeración era aditivo; es decir, cada número era la suma de los valores correspondientes a sus cifras literales. Por ejemplo[3]:

$$\overline{\Sigma\Lambda\Theta} = 239$$

Resulta evidente que, con esta notación tan simple, es fácil establecer una relación entre cualquier palabra y el número resultante de sumar los valores de sus letras. Así, se tiene[4]:

Aceite = Ελαιόλαδο = 5 + 30 + 1 + 10 + 70 + 30 + 1 + 4 + 70 = 221

Pero, ¿por qué quedarse en los objetos? ¿Acaso las personas no tienen nombre y, por tanto, un número asociado?

Sócrates = Σωκρατησ = 200 + 800 + 20 + 100 + 1 + 300 + 8 + 200 = 1629
Arquímedes = Αρχιμηδησ = 1 + 100 + 600 + 10 + 40 + 8 + 4 + 8 + 200 = 971

El siguiente paso era de una lógica aplastante: buscar relaciones entre los números correspondientes a cada persona y atribuirles unas ciertas connotaciones cabalistas. De esta forma, surgieron los números primos, amigos, perfectos, etc. La numerología no sólo era un pasatiempo sino también una suerte de superstición y los augurios que se deducían de ella algo muy a tener en cuenta. ¡Cómo no fiarse de una persona si nuestros números son amigos! ¡Qué general tan magnífico que hasta su número es perfecto!

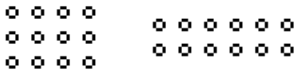
Es difícil contener la sonrisa ante tal simpleza, ¿no cree? Sin embargo, tampoco conviene mirar hacia atrás con demasiada suficiencia. Estamos en el tercer milenio y en nuestra civilización occidental, presuntamente la más formada científicamente de la historia, hay todavía demasiada gente que cree en cosas tan estrambóticas como el horóscopo, el tarot, etc... Así que mejor corramos un tupido velo.

LOS NÚMEROS PRIMOS

En la antigüedad los artículos de escritura (papiros, pergaminos, etc.) eran productos asequibles sólo para

[1] Murió el año 212 aC durante el saqueo de Siracusa por los romanos.
[2] "La numeración empleaba las veinticuatro letras del alfabeto griego clásico, a las cuales añadía los tres signos alfabéticos digamma (6), koppa (90) y sampí (900), que poco a poco cayeron en desuso" *Historia Universal de las cifras*, Georges Ifrah.
[3] Para diferenciar las letras numéricas de las alfabéticas escribían las primeras con una pequeña línea encima.
[4] He sacado las traducciones de un diccionario pero, como mis conocimientos de griego son nulos, no me extrañaría que hubiese algún término incorrecto. Me disculpo de antemano por los posibles errores, que no afectan a la finalidad ilustrativa de los ejemplos.

gente adinerada, motivo por el cual los dibujos y cálculos se solían hacer en el suelo o en la arena de la playa. Los números[5] se representaban mediante pequeños guijarros que podían agruparse generalmente en forma rectangular. Por ejemplo, el número 12 admite las dos distribuciones siguientes:



Sin embargo, resulta evidente que algunos números, como 7 u 11, sólo admiten una disposición lineal:

Si traducimos este hecho geométrico a un lenguaje aritmético, resulta que en el primer caso el número tiene varios divisores (es un número compuesto); en cambio, en el segundo sólo tiene los divisores triviales: él mismo y la unidad. Ésta es precisamente la propiedad que define a los números primos: no admiten divisiones (enteras, se sobreentiende). Así, por ejemplo, los números primos más pequeños son:

1, 2, 3, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97, 101,...

La primera pregunta que surge es evidente: ¿cuántos números primos hay? Euclides probó en sus *Elementos* que existen infinitos primos, una demostración modelo de sencillez, ingenio y elegancia, pero antes de mostrársela no me resisto a dedicar unas breves líneas a ese genial matemático que iluminó las Matemáticas durante más de dos milenios[6].

Apenas se sabe nada de su vida salvo que vivió alrededor del 300 aC y que formó parte del núcleo de sabios de la Biblioteca de Alejandría, el mayor centro científico de la época. Su obra *Elementos* es un compendio de los conocimientos geométricos y numéricos de la antigüedad, pero Euclides le dio tal rigor a su exposición que sobresale con luz propia entre las creaciones científicas. Partiendo de una serie de axiomas y postulados[7] fue deduciendo toda una serie de resultados geométricos, con un método que sólo se superó en Matemáticas a comienzos del siglo XX. ¡Ahí es nada! ¡Se adelantó más de dos mil años a su tiempo!

Para demostrar que existen infinitos números primos, Euclides buscó un atajo que le permitiese un enfoque del problema más cómodo y simple. Tuvo la perspicacia de observar que su infinitud equivale a probar lo siguiente: dado cualquier número primo n, siempre es posible hallar otro mayor que él.

> Sea p el producto de todos los primos inferiores o iguales a n y considérese el número $p + 1$. Por ejemplo, si $n = 11$ se tendría $p + 1 = 2311$ (que es primo); si $n = 13$, $p + 1 = 30031$ (que es el producto de 59 y 509)

[5] Los griegos consideraban como tales los naturales, excluyendo el cero cuyo descubrimiento fue muy posterior. Es decir, cuando hable de números se sobreentenderá que me refiero a 1, 2, 3,...

[6] Hasta el siglo XIX sus *Elementos* eran libro de texto obligado en muchas universidades de todo el mundo.

[7] Como poca gente conoce sus famosos cinco postulados, aunque son ampliamente citados, se los indico a continuación. Observe la complejidad del quinto con respecto a los anteriores. Sólo cuando se puso en tela de juicio (siglo XIX) nacieron las geometrías no euclídeas, de la mano de Lobachevski y Riemann.

I) Por dos puntos distintos pasa una recta.

II) Un segmento rectilíneo puede ser siempre prolongado.

III) Hay una única circunferencia con un centro y un diámetro dados.

IV) Todos los ángulos rectos son iguales.

V) Si una secante corta a dos rectas formando a un lado ángulos interiores cuya suma es menor de dos rectos, las dos rectas suficientemente prolongadas se cortan en este mismo lado.

Si $p+1$ es primo, ya estaría probado el resultado.

Si $p+1$ es compuesto, sea q uno de sus factores primos. Resulta fácil ver que q no puede ser menor que n, puesto que si fuese así dividiría tanto a p como a $p+1$, lo que es imposible. Por tanto, ya está probado que existe un primo mayor que n.

En el momento de escribir este artículo, el mayor número conocido es $2^{6972593}$-1, que tiene la friolera de 2098960 cifras. Si desea conocer cuales son los cien mayores números primos encontrados, puede visitar la siguiente dirección:

http://www.utm.edu/cgi-bin/caldwell/primes.cgi/100/

Volviendo a Euclides, observe que su demostración sólo prueba la existencia de un primo mayor que n... encontrarlo ya es otra cosa. Eso nos lleva a la siguiente cuestión, ¿cómo saber si un número es primo o no?

La forma más directa de averiguarlo es ir dividiéndolo por todos los números primos no superiores a su raíz cuadrada: si en algún caso resulta divisible será compuesto; en caso contrario, es primo. Con números pequeños este método es válido pero si el número consta de muchas cifras la fuerza bruta no sirve, ni siquiera con los más potentes ordenadores[8].

Los griegos utilizaban la conocida como "criba de Eratóstenes", que es útil para hallar los números primos inferiores a un cierto límite: se escriben todos los números y se suprimen los múltiplos de 2, luego los de 3, los de 5 y así sucesivamente; al terminar el proceso los números no borrados de la lista serán primos. Como algoritmo didáctico puede tener validez pero su utilidad práctica es nula debido a su lentitud.

Otra cuestión que llama la atención es la frecuencia con la que aparecen los números primos: tan pronto se presentan separados por dos unidades (17 y 19 o 881 y 883, por ejemplo) como hay unos huecos enormes entre ellos[9]. ¿Cómo están distribuidos los números primos? ¿Cuántos hay en cada intervalo?

La respuesta no exacta, ni mucho menos. Un resultado nada trivial, atribuido a Hermite, afirma que el número de primos inferiores o iguales a n es, aproximadamente:

$$\frac{n}{\ln n}$$

Para acabar con los números primos (por el momento), no debemos olvidar los números primos entre sí, que son aquellos que no tienen ningún divisor común salvo la unidad. Por ejemplo, 9 y 14, 55 y 36, etc.

Los números que son primos con respecto a 12 son: 5, 7 y 11... que casualmente también son números primos. Le propongo como pasatiempo que busque el mayor número que verifica esa misma condición: todos los primos con él son también primos... No se asuste, es relativamente pequeño.

NÚMEROS AMIGOS Y PERFECTOS

Dos números son amigos cuando cada uno de ellos es igual a la suma de los divisores del otro (sin contarlos a ellos, evidentemente). Por ejemplo, los griegos ya sabían que eran amigos los números 220 y 284:

284 = 1 + 2 + 4 + 5 + 10 + 11 + 20 + 22 + 44 + 55 + 110
220 = 1 + 2 + 4 + 71 + 142

Posteriormente se descubrieron las siguientes parejas: 1184 y 1210, 2620 y 2924, 5020 y 5564, 6232 y 6368, 10744 y 10856, 12285 y 14595, 17296 y 18416 (Fermat en 1636), etc[10]. Como curiosidad le diré que la segunda pareja más pequeña de números amigos (1184 y 1210) había pasado desapercibida para todo el mundo y la encontró en 1867 un joven italiano de 16 años: Nicolo Paganini.

Con la llegada de los ordenadores se fueron descubriendo muchas más parejas de números amigos y, en la actualidad, se conocen más de cinco mil. Si le apetece tener un listado de ellas, no dude en darse una vuelta por la siguiente dirección:

http://xraysgi.ims.uconn.edu:8080/amicable2.txt

[8] Para averiguar si un número es primo, los actuales programas informáticos se basan en métodos mucho más sofisticados, matemáticamente hablando: curvas elípticas, cribas cuadradas, algoritmos probabilísticos, etc.

[9] Es fácil obtener una sucesión de n números consecutivos de modo que ninguno sea primo. Si recuerda que el factorial de p, $p!$, es el producto de todos los enteros comprendidos entre 1 y p, puede comprobar que los siguientes números son todos ellos compuestos.

$$(n+1)!+2,\ (n+1)!+3,\ \ldots\ldots,\ (n+1)!+(n+1)$$

[10] Descartes probó que también eran amigos los números 9363584 y 9437056. ¡Vaya pasada!

Veamos ahora otros números cuya importancia matemática es bastante mayor. Un número se dice perfecto cuando es igual a la suma de todos sus divisores (salvo él mismo, claro está). Por ejemplo, son perfectos 6 y 28 puesto que se cumple:

$6 = 1 + 2 + 3$
$28 = 1 + 2 + 4 + 7 + 14$

Ya antes de nuestra era se conocían el tercer y cuarto número perfecto: 496 y 8128. Los dos siguientes (33550336 y 8589869056) costaron mucho más de localizar y aún hoy no llegan a cuarenta los números perfectos descubiertos.... Y es que, como indicaba Descartes, "*... et combien rares sont les nombres parfaits, aussi bien que les hommes parfaits*".

Euclides, que también estudió este tipo de números, probó que todos de la forma $2^n (2^{n+1} - 1)$ son perfectos siempre que $2^{n+1} - 1$ sea primo. Por tanto, el problema de hallar números perfectos es equivalente al de encontrar primos de esas características (reciben el calificativo de primos de Mersenne y a ellos me referiré más adelante)

Si le pica la curiosidad, puede ver todos los números perfectos conocidos hasta la fecha en la siguiente dirección:

http://forum.swarthmore.edu/dr.math/problems/perfect.html

ALGUNAS CUESTIONES TODAVÍA EN EL AIRE

Como he indicado al principio, la teoría de números es un filón todavía no agotado y aún ofrece oportunidades para labrarse un hueco en la pequeña historia de las Matemáticas. Seguidamente le comentaré algunas sencillas cuestiones que todavía permanecen sin resolver y en los siguientes apartados le hablaré de otras más que tienen nombre propio.

• Existen muchas parejas de números primos que se diferencian en dos unidades, los llamados primos gemelos: 5 y 7, 11 y 13, 17 y 19, etc. Los mayores primos gemelos conocidos hasta el momento son $4648619711505 \times 2^{60000} \pm 1$, cada uno de los cuales consta de 18075 cifras... pero, ¿existen infinitas de estas parejas?

• Muchos de los números primos son de la forma $n^2 + 1$. Por ejemplo, esto se cumple con 17 ($4^2 + 1$), 37 ($6^2 + 1$), etc. ¿Hay infinitos números primos de esa forma?

• Con respecto tanto a los números amigos como a los perfectos, la cuestión más importante por dilucidar corresponde a su infinitud: ¿Existen infinitos números perfectos? ¿Existen infinitas parejas de números amigos? En ambos casos se cree que la respuesta es positiva, pero todavía no se ha logrado demostrarlo.

• Como he indicado antes, Euclides probó que todo número perfecto par es de la forma $2^n (2^{n+1} - 1)$ siempre que $2^{n+1} - 1$ sea primo... pero, ¿hay algún número perfecto impar? Se supone que la respuesta es negativa pero de nuevo la demostración se torna huidiza. Eso sí, se ha comprobado que si existe algún número perfecto impar debe ser superior a 10^{300}.

FERMAT Y SU ÚLTIMO TEOREMA

Pierre Fermat (1601-1665) era un jurista que se dedicaba a las Matemáticas en sus ratos libres, a pesar de lo cual descubrió muchos resultados importantes en teoría de números y probabilidad. En opinión de Martin Gadner fue "el más grande matemático aficionado que haya existido nunca" (*Orden y sorpresa*) ... Sin embargo, también los genios meten la pata.

Durante mucho tiempo se buscaron expresiones que permitiesen obtener números primos, pensando que quizá existiera una fórmula general para todos ellos.

Como puede imaginar no se encontró tal fórmula aunque sí otras parciales que permitían generar algunos números primos rápidamente y en aquellos siglos, cuando las calculadoras aún no existían, resultaron bastante útiles para comprobar resultados, plantear problemas, etc. Por ejemplo, si se aburre puede entretenerse verificando la validez de las siguientes expresiones generadoras de primos:

$n^2 + 17n - 1$	con $n = 1, 2, ..., 15$
$2n^2 + 29$	con $n = 0, 1, ..., 28$
$n^2 - n + 41$	con $n = 0, 1, ..., 40$
$n^2 - 79n + 1601$	con $n = 0, 1, ..., 79$

Fermat también investigó esas fórmulas y pensaba que siempre eran primos los números de la forma:

$$2^{2^n} + 1$$

Observe que cuando n toma los valores 1, 2, 3 y 4, la expresión anterior resulta ser un número primo: 5, 17, 257 y 65537; sin embargo, cuando $n = 5$ se obtiene el valor 4294967297, que es un número compuesto[11]. Si quiere entretenerse le propongo que halle sus dos divisores primos (uno tiene tres cifras y el otro siete). Eso sí, le aconsejo que utilice una calculadora; si intenta hacerlo a mano comprobará que la tarea es un tanto ardua a pesar de la pista que le he dado, lo cual hace más comprensible el error de Fermat.

Esta pequeña anécdota es sólo eso, una anécdota, y no desmerece la gran capacidad matemática de Fermat ni sus extraordinarias intuiciones. Para que se haga una idea de su calidad matemática le comentaré uno de sus teoremas, del que no dio la demostración.

Es evidente que todo número primo impar es necesariamente de la forma $4n + 1$ o $4n - 1$. Fermat afirmó que los del primer tipo siempre se pueden poner como suma de dos cuadrados perfectos (por ejemplo, $41 = 4^2 + 5^2$); en cambio, los del segundo tipo no. En 1749, casi cien años después de dar a conocer este resultado Fermat, Euler logró demostrarlo... tras siete años de trabajo.

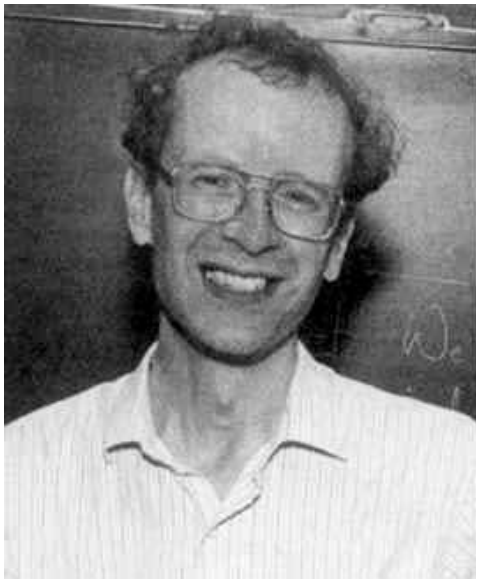
Teniendo en cuenta las contribuciones de Fermat a las Matemáticas era de esperar que se hiciese un hueco en su historia, de modo que su nombre sería conocido por especialistas en la materia y lo normal sería que no saliese del ámbito académico... Sin embargo, la casualidad hizo que todavía hoy sea recordado por mucha gente e incluso aparezca de vez en cuando en la prensa.

Cinco años después de su muerte, su hijo Samuel publicó las anotaciones que Fermat había escrito en los márgenes de un ejemplar de la *Arithmetica* de Diofanto. Una de ellas, escrita alrededor de 1630, decía que si a, b y c son números naturales, nunca se verifica la siguiente igualdad para valores de n mayores que 2.

$$a^n + b^n = c^n$$

Ese resultado, conocido como el último teorema de Fermat, ha tenido una importancia notable en el desarrollo de las Matemáticas ya que durante más de 350 años resistió los ataques de todos los grandes matemáticos, que fueron abriendo caminos nuevos en sus investigaciones en busca de una prueba que nunca encontraron. Encima, y para desesperación de todos ellos, Fermat dejó escrito: "He encontrado una demostración realmente admirable, pero el margen es muy pequeño para ponerla"

Lo más probable es que Fermat se confundiese, como le sucedió también a Euler que en 1973 creyó haber descubierto una demostración del teorema[12]. Sin embargo, ésta siguió escondida y no se encontró hasta 1993. Andrew Wiles, un matemático británico nacido en 1953 y profesor en Princeton, parece que finalmente ha dejado zanjada la cuestión.



[11] El primero que lo demostró fue Euler. Si no me equivoco, tampoco resulta primo para $n = 6, ..., 17$. ¿Existe algún primo de Fermat superior a 65537?... Por el momento se desconoce la respuesta. ¡Otra cuestión más en el aire!

[12] La ampliación del último teorema de Fermat al caso de tres o cuatro sumandos es falsa. Por ejemplo, $3^3 + 4^3 + 5^3 = 6^3$ y $30^4 + 120^4 + 315^4 + 272^4 = 353^4$

Wiles anunció su hallazgo en una serie de charlas que dio en Cambridge en junio de 1993. Para darle más suspense al asunto, resultó que al redactar su trabajo para su publicación halló un error. ¡Imagine su desesperación! ... Siguió dándole vueltas al tema hasta que, finalmente, el 19 de septiembre de 1994 tuvo una revelación[13] y dejó resuelto el último teorema de Fermat. Su demostración fue publicada en *Annals of Mathematics* en 1995 bajo el título *Modular elliptic curves and Fermat's Last Theorem*.

LA CONJETURA DE GOLDBACH

Christian Goldbach (1690-1764) fue profesor de Matemáticas y llegó a ser tutor del zar Pedro II. Estudioso de la teoría de números, mantenía una fluida correspondencia con Euler y en una carta que le envió, fechada el 7 de junio de 1742, le indicaba que, según él, todo número entero es suma de tres números primos, como máximo. Es sencillo ver que para ello basta con probar que todo número par es suma de dos números primos y esta es precisamente la expresión con la que se ha popularizado la conjetura de Goldbach.

[13] *... suddenly, totally unexpectedly, I had this incredible revelation. It was the most important moment of my working life. Nothing I ever do again ... it was so indescribably beautiful, it was so simple and so elegant, and I just stared in disbelief for twenty minutes, then during the day I walked round the department. I'd keep coming back to my desk to see it was still there - it was still there.*

Hasta el momento, y gracias a los modernos ordenadores, se ha comprobado que la conjetura Goldbach se verifica con todos los números pares inferiores a $4x10^{14}$, pero no se ha podido demostrar que siempre se cumpla. ¡Otra cuestión más en el aire!

Al hablar de este tema no puedo dejar de recomendarle una excelente novela, *El tío Petros y la conjetura de Goldbach* de Apostolos Doxiadis, con la que espero que disfrute tanto como yo.

Con ánimo de dar una amplia cobertura publicitaria a la novela y visto que la conjetura no se ha podido demostrar en más de 250 años, su editorial ofrece un premio de un millón de dólares a cualquier persona que pueda probar la conjetura de Goldbach en un plazo de dos años (acaba en marzo del 2002). Si se anima a intentarlo, puede informarse más sobre el tema en la página:

http://www.apostolosdoxiadis.com/million.htm

LOS PRIMOS DE MERSENNE

El monje francés Marin Mersenne (1588-1648) también buscó una fórmula que generase todos los primos e investigó los números de la forma $2^p - 1$ siendo p primo, que desde entonces se conocen por el nombre de números de Mersenne.

En su libro *Cogitata Physica-Mathematica* de 1644, Mersenne conjeturó que eran primos los números $2^p - 1$ sólo para los siguientes valores de $p \leq 257$:

p = 2, 3, 5, 7, 13, 17, 19, 31, 67, 127 y 257

Mersenne omitió tres valores de p (61, 89 y 107) para los cuales $2^p - 1$ es primo y se equivocó en dos (67 y 257) para los que resulta un número compuesto. Así, por ejemplo:

$$2^{67} - 1 = 147573952589676412927 = 193707721 \times 761838257287$$

Si quiere conocer los 38 primos de Mersenne conocidos hasta la fecha (incluso con todas sus cifras), puede hallarlos en la siguiente página:

http://www.isthe.com/chongo/tech/math/prime/mersenne.html

La ventaja de los números de Mersenne radica en que existe una manera relativamente cómoda de estudiar su primalidad: el llamado test de Lucas-Lehmer, que dice lo siguiente:

> Siendo p impar, $2^p - 1$ es primo si y sólo si $2^p - 1$ divide a $S(p - 1)$, cumpliéndose que $S(n + 1) = S(n)^2 - 2$ y $S(1) = 4$

Observe que la traducción de este test a pseudocódigo es, en principio, muy sencilla y por esta razón los mayores números primos encontrados en la actualidad son todos ellos también números de Mersenne:

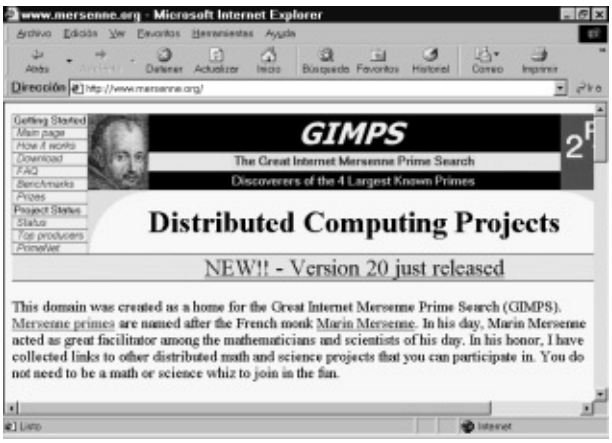
```
Test_Lucas_Lehmer (p):
  s := 4;
  for i from 3 to p do s:= s^2 – 2 mod 2^p – 1;
      if s = 0 then 2^p – 1 es primo
      else 2^p – 1 es compuesto;
```

Como no podía ser menos, los números de Mersenne también ofrecen una serie de conjeturas todavía sin

resolver: ¿Existen infinitos números de Mersenne primos? ¿Y compuestos?

EL PROYECTO GIMPS

La búsqueda de nuevos números primos de Mersenne exigiría enormes superordenadores con una gran potencia de cálculo... pero también cumplirían el mismo papel miles de pequeños ordenadores interconectados, ¿no? Esa fue la idea que dio lugar en 1996 al nacimiento del proyecto GIMPS (*Great Internet Mersenne Prime Search*).



Cualquier persona puede participar en la búsqueda de primos de Mersenne, sólo se precisa una conexión a Internet e instalar en el ordenador personal un sencillo programa que se activa cuando el ordenador está parado sin hacer nada. Todo ello coordinado mediante un servidor llamado Primenet.

Por ejemplo, el mayor primo conocido hasta la fecha lo obtuvo Nayan Hajratwala, una más de las miles que personas que participan en el proyecto GIMPS a lo largo del mundo. Curiosa forma de pasar al Guiness, ¿no cree? ... pero es que además, si se decide a tomar parte en él, también puede llevarse una buena cantidad de dinero.

Si da la casualidad de que su ordenador es el primero en encontrar un primo de Mersenne de más de diez millones de cifras, ganará más de cincuenta mil dólares... y todo ello aprovechando los ratos libres en que su ordenador está encendido sin hacer nada.

Si le interesa este proyecto, ya sea por pasar a la pequeña historia de las Matemáticas o simplemente por el dinero a ganar, acuda a la siguiente dirección donde encontrará una amplia información sobre este proyecto en castellano, junto con el programa gratuito que le permitirá incorporarse al GIMPS.

http://www.ctv.es/USERS/gbv/GIMPS/prime.htm

También existe una página internacional dedicada a este problema donde además encontrará información sobre otros varios temas que se pretenden resolver mediante la cooperación de ordenadores personales conectados a la Red. Le recomiendo su visita:

http://www.mersenne.org/

PERO, ¿TIENEN ALGUNA UTILIDAD ESTAS COSAS?

Seguramente a estas alturas se estará preguntado cómo es que alguien paga dinero por encontrar un número primo... ¿Acaso no es una tontería típica de los matemáticos, un pasatiempo inútil para gente aburrida? Mucha gente lo cree así; por ejemplo, el gran Isaac Asimov, en su libro *Cien preguntas básicas sobre la ciencia*, afirmaba: "Los números primos presentan problemas aparentemente inocentes, pero que son muy difíciles de resolver, y los matemáticos no pueden resistir el desafío. ¿Qué utilidad tiene eso? Ninguna; pero eso precisamente parece aumentar el interés"

Sin embargo, Asimov se equivocaba. Es innegable que hay algo de reto en enfrentarse a un problema numérico simplemente porque está ahí, de la misma forma que un alpinista escala una montaña por el simple placer de hacerlo, sólo porque está ahí. No obstante, si todo quedara en un mero desafío personal nadie ofrecería dinero por encontrar un número primo, ¿verdad?

Lo cierto es que los números primos y demás mueven mucho dinero... y todo a causa de la Informática. Su primera aplicación tiene que ver con la puesta a punto de nuevos modelos de ordenadores; por ejemplo, para comprobar si presentan algún fallo de programación (como pasó en su día con el Pentium) se les puede hacer pasar varios tests donde deban resolver complejos problemas numéricos de solución conocida: cifras de un número, divisores de otro, etc.

Otra utilidad de los números, todavía más importante, tiene que ver que la seguridad de los datos que circulan por la Red o que están almacenados en los archivos

de diversas entidades y organismos. ¿Cómo protegerlos de visitas no autorizadas? ¿Cómo lograr que las transacciones vía Internet sean seguras? ¿Cómo evitar que las empresas competidoras accedan a nuestra información?...

Como ve, son cuestiones que pueden suponer mucho dinero. A lo largo de la historia se introdujeron diversos procedimientos para mantener el secreto de los mensajes, desde la clave del césar hasta la máquina Enigma alemana en la Segunda Guerra Mundial, pero actualmente casi todas las técnicas de encriptación se sustentan en los números primos.

Al tratarse de un tema bastante complejo, me voy a limitar a darle un somero comentario para que se haga una idea de por donde van los tiros. El método RSA, llamado así por los apellidos de sus creadores (Ronald Rivest, Adi Shamir y Leonard Adlermann), está basado en los números casi primos (¡otra definición más!). Se dice que un número es casi primo cuando tiene dos divisores y ambos son primos; por ejemplo, 91 es casi primo pues es el producto de 7 y 13, primos los dos.

El método RSA cifra la información en función de un número casi primo (clave pública) de centenares de cifras cuyos dos factores primos también son muy grandes y que, además, cumplen una serie de propiedades (motivo por el cual se les denomina primos fuertes). Mediante otro número primo (clave privada) la información puede ser descifrada.

Teóricamente conociendo la clave pública podrían hallarse sus factores pero, al tratarse de números que constan de centenares de cifras, el proceso exigiría tantos años de cálculo en un superordenador que en la práctica el cifrado resulta inviolable... salvo que miles de ordenadores personales interconectados por Internet se pusiesen de acuerdo.