Sucesiones alicuatorias *

Manuel Benito y Juan Luis Varona

A todos los que de alguna manera estamos vinculados a la investigación en matemáticas nos han preguntado alguna vez qué se puede investigar aún en matemáticas. La mayoría de la gente con conocimientos matemáticos medios no piensa que en matemáticas quedan cosas por descubrir. La manera más fácil de responder a esa pregunta es mostrar un problema con solución desconocida. Pero, claro, tiene que ser un problema con un planteamiento lo suficientemente sencillo para que pueda ser entendido por un profano. Hasta hace años, el ejemplo más típico era el último teorema de Fermat. Como ya está demostrado, ha dejado de sernos útil en este sentido.

Afortunadamente, la teoría de números tiene muchísimos otros problemas abiertos de enunciado sencillo. Dos de los más conocidos son la conjetura de Goldbach (cada número par se puede expresar como suma de dos primos) y la existencia de infinitos primos gemelos (primos que se diferencian en dos). Realmente, los hay a cientos; tres libros dedicados a mostrar problemas de este tipo son [12, 9, 7]. Es de destacar, además, que muchos de ellos están bien adaptados a la realización de experimentos con ordenadores. Si una conjetura dice que no existen números con ciertas propiedades y logramos encontrar uno, esto, obviamente, echa por tierra la conjetura. En cambio, si la suposición es que existen infinitos números que cumplen algo, con un ordenador se puede intentar encontrar muchos de ellos, estudiando su distribución, o buscando cada vez el mayor número que satisface la propiedad. Estos récords, aunque no suelen aparecer en los medios de comunicación, tienen exactamente la misma utilidad que los récords deportivos, a los que tanto dinero se destina.

Aquí vamos a dedicarnos a hablar de uno de estos problemas abiertos, el de las sucesiones alicuatorias. En el camino, nos aparecerán unos cuantos más.

Para un entero positivo n denotamos por $\sigma(n)$ la suma de todos sus divisores (incluido 1 y n). Si la descomposición de n en factores primos es $n = p_1^{a_1} \cdots p_k^{a_k}$, entonces

$$\sigma(p_1^{a_1} \cdots p_k^{a_k}) = (1 + p_1 + \cdots + p_1^{a_1}) \cdots (1 + p_k + \cdots + p_k^{a_k}). \qquad (1)$$

*ESTO ES UNA AMPLIACIÓN DETALLADA DEL ARTÍCULO QUE APARECIÓ PUBLICADO EN: La Gaceta de la Real Sociedad Matemática Española, Vol. 2, n.º 2 (1999), 357–365.

Esto es así porque, si desarrollamos la expresión de la derecha, aparecen como sumandos todos los divisores de $p_1^{a_1} \cdots p_k^{a_k}$. Además, $1 + p + \cdots + p^a = \frac{p^{a+1}-1}{p-1}$ luego tenemos la siguiente fórmula directa para calcular $\sigma(n)$ en función de la descomposición en factores de n:

$$\sigma(n) = \frac{p_1^{a_1+1} - 1}{p_1 - 1} \cdots \frac{p_k^{a_k+1} - 1}{p_k - 1}. \tag{2}$$

A partir de σ construimos la función $s(n) = \sigma(n) - n$. Obviamente, $s(n)$ es la suma de los divisores propios de n (esto es, excluyendo el mismo n). Con otras palabras, $s(n)$ es la suma de las partes alícuotas de n.

Relacionados con s (o con σ) se pueden definir varios tipos de números (un libro con resultados recientes sobre el tema, y que incide en su aspecto computacional, es [13]):

Números perfectos: Un número se dice perfecto si es igual a la suma de sus divisores propios, es decir, si $s(n) = n$ (o $\sigma(n) = 2 \cdot n$). Si $s(n) > n$, el número n se llama abundante; si $s(n) < n$, defectuoso. Los primeros números perfectos son 6, 28 y 496. Es bien conocido que n es un número perfecto par si y sólo si es de la forma $n = 2^{p-1}(2^p - 1)$ con $2^p - 1$ primo (lo cual, a su vez, requiere que p sea primo). Pero se desconoce si existen o no números perfectos impares. En cuanto a los pares, encontrarlos se reduce a la búsqueda de números $M_p = 2^p - 1$ (que se denominan números de Mersenne) primos. No se sabe si hay o no infinitos de ellos; ni tampoco si hay infinitos compuestos. Actualmente, se conocen 37; el mayor es $2^{3021377} - 1$, que tiene más de 900,000 cifras (existe un premio de 50,000 dólares para la primera persona que encuentre un primo de un millón de cifras). La búsqueda de números de Mersenne primos está coordinada por G. Woltmann con el proyecto *Great Internet Mersenne Prime Search* en `http://www.mersenne.org/prime.htm`. Allí se pueden conocer los últimos avances e, incluso, descargar los programas necesarios para contribuir en la búsqueda con nuestro ordenador personal. Los tres últimos primos de Mersenne conocidos han sido encontrados por colaboradores de este proyecto en ordenadores personales (el anterior había sido encontrado en un superordenador CRAY).

Números amigos: Son parejas de números (n, m) tales que $s(n) = m$ y $s(m) = n$ (o, lo que es equivalente, $\sigma(n) = \sigma(m) = n + m$). Ejemplos de amigos son $(220, 284)$, $(2620, 2924)$ y $(5020, 5564)$. Hasta ahora, se conocen varios miles. Se han desarrollado diversos métodos que, a partir de una pareja de amigos, generan otras parejas de números que son amigos con bastante probabilidad. Cuando se han aplicado, mediante el uso de ordenador, a tablas de amigos ya conocidos, se han obtenido más nuevos que los ya conocidos (véase, por ejemplo [11]). Esto es un argumento heurístico en favor de la existencia de infinitos pares de amigos. Pero tampoco se tiene una demostración.

Ciclos o números pandilla: Son tuplas $(a_1, \ldots, a_l)$ tales que $s(a_1) = a_2$, $s(a_2) = a_3$, $\ldots$, $s(a_l) = a_1$. Hasta ahora, se han encontrado 41 ciclos de longitud l mayor que 2 (obviamente, los de longitud uno son los números perfectos y los de longitud dos son los amigos). Sólo se conocen ciclos de longitudes 4, 5, 6, 8, 9 y 28. La mayoría de ellos han sido hallados con ordenador. Curiosamente no sucedió así con el que, a priori, podría parecer más raro, el de longitud 28: fue encontrado por Poulet en 1918; su componente más pequeño es 14316. Se desconoce, por ejemplo, si existen ciclos de longitud 3. O si existen infinitos.

Intocables de Erdős: Se llaman así a los n tales que $n \neq s(m)$ para todo m. Por ejemplo, 2 y 5. De nuevo, no se sabe si hay o no infinitos de ellos.[1]

1. Sucesiones alicuatorias

Ya estamos en condiciones de poder definir las *sucesiones de sumas de partes alícuotas* o, para abreviar, *sucesiones alicuatorias*: Dado un entero positivo n construimos la sucesión $\{s^k(n)\}_{k\in\mathbb{N}}$ definida recursivamente mediante $s^1(n) = s(n)$, $s^2(n) = s(s^1(n))$, $\ldots$, $s^k(n) = s(s^{k-1}(n))$.

Para una de tales sucesiones, existen cuatro posibilidades: (a) Que la sucesión termine en 1 (siendo el número anterior un primo). (b) Que la sucesión llegue a un número perfecto (y a partir de entonces permanezca constante). (c) Que llegue a un par de amigos o un ciclo. (d) Que no esté acotada.

E. Catalan [2] en 1887 y L. E. Dickson [5] en 1913 conjeturaron que la posibilidad (d) nunca ocurría. La conjetura de Catalan-Dickson continúa sin ser demostrada o refutada.

Una manera de ver que es falsa sería encontrar un n tal que $s^k(n) > s^{k-1}(n)$ para todo k. Aunque parece difícil que tal n exista. Sí que existen sucesiones con tantos términos crecientes como se desee, tal como probó H. W. Lenstra (véase [6]): para cada k, existe n tal que $n < s(n) < \cdots < s^k(n)$. El método es constructivo y fácil de entender, aunque los números que van saliendo son enormes. Argumentos heurísticos de Guy-Selfridge (basados en la persistencia de ciertos patrones que se repiten en las sucesiones, y que analizaremos más adelante) hacen suponer que, para infinitos valores de n, esto se puede conseguir con $k < (\log n)^{1-\varepsilon}$. Es más, ellos se atreven a conjeturar en el sentido contrario al de Catalan-Dickson: las sucesiones $\{s^k(n)\}_{k\in\mathbb{N}}$ son

[1] Nota posterior: En [12, problema 91, p. 119], la existencia o no de infinitos números intocables aparece como problema abierto. Pero, en 1973, el mismo Erdős probó no sólo que existen infinitos de ellos, sino algo más potente; concretamente, que su densidad inferior es positiva. Véase P. Erdős, *Über die Zhalen der Form* $\sigma(n) - n$ *und* $n - \varphi(n)$, Elem. Math. **28** (1973), 83–86; MR **49** #2502.

no acotadas para casi todo n par; es decir, la proporción de los enteros pares para los cuales $\{s^k(n)\}_{k\in\mathbb{N}}$ está acotada, tiende a cero.

El primer número que ofreció serias dudas fue $n = 138$ (Poulet, 1918). Fue resuelto por D. H. Lehmer, que encontró $s^{177}(138) = 1$, pasando por un máximo $s^{117}(138)$ de 12 cifras (en notación decimal). Desde entonces, el menor n cuya sucesión tiene comportamiento incierto es 276. Del estudio experimental de tal sucesión, computando cada vez más términos, se han ocupado G. A. Paxson, H. Cohen, D. H. Lehmer, H. J. Godwin, J. L. Selfridge, M. C. Wunderlich, T. Struppeck, R. K. Guy, A. Guy, M. Dickerman, P. Zimmermann y los autores. Actualmente, se ha llegado hasta $s^{1119}(276)$, un número de 107 cifras (P. Zimmermann, con la colaboración de S. Wagstaff y A. Lenstra).

Las sucesiones alicuatorias $\{s^k(n)\}_{k\in\mathbb{N}}$ y $\{s^k(m)\}_{k\in\mathbb{N}}$ correspondientes a dos enteros positivos n y m, con $n < m$, se dice que son laterales si existen índices i y j tales que $s^i(n) = s^j(m)$ (lógicamente, a partir de entonces ambas sucesiones coinciden); y se llama sucesión principal a la correspondiente a n. Es claro que, en el estudio de las sucesiones alicuatorias, basta con analizar las sucesiones principales.

En principio, el tratamiento computacional de una sucesión $\{s^k(n)\}_{k\in\mathbb{N}}$ para un n concreto parece fácil: basta aplicar reiteradamente la fórmula (2). Pero la dificultad radica en que la sucesión puede alcanzar términos muy grandes. Para poder seguir, (2) requiere factorizar enteros enormes. Y, con cualquiera de los algoritmos de factorización conocidos, esto supone un tiempo de cálculo que crece exponencialmente con el número de dígitos del número a factorizar.

Además de a la correspondiente a 276, se ha dedicado un gran esfuerzo computacional a muchas otras sucesiones. Comentemos a continuación en qué se ha centrado fundamentalmente este trabajo computacional. En [7, Cap. B6], se pueden encontrar más datos históricos (hasta 1994), y una amplia bibliografía sobre el tema.

Las cinco de Lehmer: Son las sucesiones principales que empiezan por un n menor que 1000. Concretamente, 276, 552, 564, 660 y 966.

Las catorce de Godwin: Son las que comienzan con n entre 1000 y 2000. Actualmente, sólo 12 de ellas permanecen en duda. Godwin, en 1980, encontró el final de la sucesión correspondiente a 1984; resultó ser una sucesión con un máximo de 29 cifras y una longitud de 672. Y Dickermann, en 1994, el final de la que comienza en 1248; esta vez, se obtuvo un máximo de 58 cifras y una longitud de 1075.

Asimismo, los autores han estudiado todas las sucesiones que comienzan en un número n menor de 10000. En todas ellas, se ha avanzado hasta términos mayores de 10^{90} y se ha encontrado el final de algunas que anteriormente estaban en duda. Más adelante en este mismo artículo comentamos con mayor

detalle nuestro trabajo con estas sucesiones.

Por último, W. Creyaufmüller [4] está intentando clasificar todas las sucesiones que comienzan en un $n < 10^6$. El estudio de las sucesiones que ofrecen dudas se prosigue hasta alcanzar términos de 60 cifras. Éste es un proyecto que está aún en desarrollo. Puede encontrarse información actualizada en `http://www.loria.fr/~zimmerma/records/aliquot.html` (página mantenida por P. Zimmermann).

Además de esta página web, existen otras dos dedicadas a los progresos en sucesiones alicuatorias: La mantenida por uno de los autores, `http://www.unirioja.es/dptos/dmc/jvarona/aliquot.html`, y la de W. Bosma, `http://www-math.sci.kun.nl/math/~bosma/nuth/ali.html`.

Todo el esfuerzo computacional para ir calculando términos de una sucesión alicuatoria se hace aplicando las fórmulas (1) o (2). Esto, cuando la sucesión alcanza términos enormes, requiere un gran tiempo de factorización. Las mejoras en los algoritmos de factorización (y la velocidad de los ordenadores) permiten avanzar en el estudio de las sucesiones.

Pero nadie puede garantizar que no exista algún método rápido que permita calcular $s(n)$ (o $\sigma(n)$) a partir de n sin necesidad de factorizar n. Realmente, ya Euler encontró un algoritmo recursivo para el cálculo de $\sigma(n)$. Lamentablemente, la recursión, cuando n es grande, requiere una gran cantidad de pasos previos. El método puede ser descrito mediante

$$\begin{aligned}\sigma(n) = {} & \sigma(n-1) + \sigma(n-2) - \sigma(n-5) - \sigma(n-7) \\ & + \sigma(n-12) + \sigma(n-15) - \sigma(n-22) - \sigma(n-26) \\ & + \sigma(n-35) + \sigma(n-40) - \sigma(n-51) - \sigma(n-57) \\ & + \sigma(n-70) + \sigma(n-77) - \sigma(n-92) - \sigma(n-100) \\ & + \cdots .\end{aligned}$$

Sobre esta fórmula debemos hacer las siguientes observaciones: (a) En los sumandos, se van alternando siempre dos signos + y dos −. (b) La ley que rige los números 1, 2, 5, 7, 12, 15, ... que se restan de n, se observa más fácilmente a partir de sus diferencias:

Números:	1	2	5	7	12	15	22	26	35	40	51	57	70	77	92	100	...
Diferencias:	1	**3**	2	**5**	3	**7**	4	**9**	5	**11**	6	**13**	7	**15**	8	**17**	....

Efectivamente, aquí tenemos, alternadamente, todos los enteros positivos 1, 2, 3, 4, 5, ... y (en negrita) los números impares 3, 5, 7, 9, 11, ... (c) En la fórmula recurrente, tomamos únicamente una cantidad finita de términos, descartando aquéllos en los que los números a los que hay que aplicar σ son negativos (es decir, como si $\sigma(a) = 0$ para $a < 0$). (d) Si en la fórmula recurrente aparece $\sigma(0)$, ponemos n en su lugar. No haremos más hincapié en este método. Para conocer más detalles, consultar [10, Cap. 6].

2. Patrones de comportamiento de las sucesiones

En una sucesión alicuatoria, existen patrones que se van repitiendo a lo largo de los términos de la sucesión; al menos, se repiten con bastante probabilidad. En primer lugar, veamos un ejemplo:

Supongamos $n = 2^3 \cdot 3 \cdot 5 \cdot p \cdot q$, con p y q primos distintos mayores que 5; lo mismo ocurre si hay más factores primos pero, por simplicidad, veámoslo de esa manera. Por (1), $s(n) = (1+2+4+8) \cdot 4 \cdot 6 \cdot (p+1) \cdot (q+1) - 2^3 \cdot 3 \cdot 5 \cdot p \cdot q = 15 \cdot 2^2 \cdot 2 \cdot 3 \cdot (p+1) \cdot (q+1) - 2^3 \cdot 3 \cdot 5 \cdot p \cdot q = 2^3 \cdot 3 \cdot 5 \cdot [3 \cdot (p+1) \cdot (q+1) - p \cdot q] = 2^3 \cdot 3 \cdot 5 \cdot m$, con m impar y no múltiplo de 3. Es decir, de nuevo obtenemos el patrón $2^3 \cdot 3 \cdot 5$, con 2 y 3 elevados exactamente a la misma potencia. Sin embargo, no se garantiza que 5 vuelva a aparecer como factor de $s(n)$ elevado únicamente a la potencia 1. El comportamiento es similar si los primos mayores que 5 están elevados a potencias impares, ya que $1 + p + \cdots + p^a$ es par cuando a es impar. En cambio, un factor p^a con a par no contribuye con un factor 2 en el primer sumando de la expresión entre corchetes que da m, puesto que $1 + p + \cdots + p^a$ es impar; es como si n no tuviese el factor p^a.

Antes de continuar, indicar que con p y q denotaremos siempre números primos impares distintos. En el estudio de la estructura de $s(n)$ a partir de la de n, cuando describimos un comportamiento en el que aparece $p \cdot q$, el comportamiento será similar si hay más de dos factores primos distintos. Lo ilustramos con dos por simplicidad en la escritura. Tampoco importa si los primos están elevados a potencias impares. Los factores primos de n elevados a potencias pares no tienen influencia; se comportan prácticamente como si no estuvieran.

Las estructuras estables no son raras. Ocurren siempre que aparece como factor un número perfecto (por ejemplo, $n = 2 \cdot 3 \cdot p \cdot q$ o $n = 2^2 \cdot 7 \cdot p \cdot q$) y con algunas otras combinaciones de primos, como $2^3 \cdot 3$ o $2^3 \cdot 3 \cdot 5$. Las comprobaciones son similares.

Por otra parte, es fácil demostrar que, si m es un número perfecto (o abundante) y m divide propiamente a n, entonces $s(n) > n$. Comprobémoslo: Por hipótesis, $\sigma(m) \geq 2 \cdot m$; además, $n = l \cdot m$ con $l > 1$. Así, debemos probar $\sigma(l \cdot m) > 2 \cdot l \cdot m$. Sean $\{1, d_1, d_2, \ldots, d_r\}$ los divisores de m. Entonces, $1, l, l \cdot d_1, l \cdot d_2, \ldots, l \cdot d_r$ son, todos ellos, divisores de $l \cdot m$. Por tanto, $\sigma(l \cdot m) \geq 1 + l + l \cdot d_1 + l \cdot d_2 + \cdots + l \cdot d_r > l \cdot (1 + d_1 + d_2 + \cdots + d_r) = l \cdot \sigma(m) \geq 2 \cdot l \cdot m$.

En todos los ejemplos de estructuras estables que hemos comentado se puede aplicar el resultado anterior, luego $s(n) > n$. Así, como la estructura se mantiene, parecería que conseguimos una sucesión que crece indefinidamente. Pero esto no es así, ya que las estructuras estables no lo son del todo, sino que a veces pueden desaparecer. Veámoslo de nuevo con unos ejemplos, esta vez aplicadas a $2^3 \cdot 3$.

Cuando tenemos un número de la forma $n = 2^3 \cdot 3 \cdot p$ (un sólo primo p mayor que 3), se sigue $s(n) = (1+2+4+8) \cdot 4 \cdot (p+1) - 2^3 \cdot 3 \cdot p = 2^2 \cdot 3 \cdot [5 \cdot (p+1) - 2 \cdot p]$. Ahora, si p es de la forma $p = 4 \cdot r + 1$, entonces $s(n) = 2^3 \cdot 3 \cdot [5 \cdot (2 \cdot r + 1) - p]$, y lo que aparece entre corchetes es par, luego aumenta la potencia de 2 en $s(n)$. Sin embargo, si $p = 4 \cdot r + 3$, obtenemos $s(n) = 2^3 \cdot 3 \cdot [5 \cdot (2 \cdot r + 2) - p]$ y esta vez lo que aparece entre corchetes es impar, luego la potencia de 2 se mantiene.

El patrón $2^3 \cdot 3$ también puede desaparecer con números de la forma $n = 2^3 \cdot 3^2 \cdot p \cdot q$. Aquí, $s(n) = 15 \cdot 13 \cdot (p+1) \cdot (q+1) - 8 \cdot 9 \cdot p \cdot q$. Si $p, q \equiv 1$ mód 4, entonces desaparece el 2^3 y surge, en su lugar, 2^2. Si $p, q \equiv 3$ mód 4, se mantiene el 2^3. Si $p \equiv 1$ y $q \equiv 3$ mód 4, entonces al menos aparece el factor 2^3; pero la potencia de 2 aumenta si 8 no divide a $q + 1$, es decir, si $q \equiv 3$ mód 8.

La existencia de estructuras estables ha sido analizada rigurosamente y plasmada en forma de definiciones generales. Así, Guy y Selfridge [8] dan los conceptos de guía y conductor (en inglés, *guide* y *driver*).

Un guía es un número de la forma 2^a, con $a > 0$, multiplicado por un subconjunto de factores primos de $\sigma(2^a)$ $(= 2^{a+1} - 1)$. Obsérvese que la potencia de los otros factores no es importante. La única que es esencial es la potencia de 2. Por ejemplo, $n = 2^3 \cdot 3 \cdot 5 \cdot m$ con m impar tiene a $2^3 \cdot 3 \cdot 5$ como guía (en efecto, $\sigma(2^3) = 15$), incluso aunque $\text{mcd}(m, 15) \neq 1$.

Ser conductor es algo más exigente que ser guía. Un conductor es $2^a \cdot v$, con $a > 0$, v impar y tal que v divide a $\sigma(2^a)$ y 2^{a-1} divide a $\sigma(v)$. La última condición se impone para que la potencia del primo 2 tienda a persistir al menos tanto como si el conductor fuera únicamente 2, para el cual la condición es trivial.

Por ejemplo, son guías, aunque no conductores, los siguientes números: 2^2, 2^3, 2^4, $2^5 \cdot 3$, $2^5 \cdot 3^2$, $2^5 \cdot 3^2 \cdot 7$ (sin embargo, $2^5 \cdot 3 \cdot 7$ sí es conductor), $2^3 \cdot 5$, $2^7 \cdot 3 \cdot 5$.

Los conductores están perfectamente clasificados (véase [8]): Los únicos conductores son 2, $2^3 \cdot 3$, $2^3 \cdot 3 \cdot 5$, $2^5 \cdot 3 \cdot 7$, $2^9 \cdot 3 \cdot 11 \cdot 31$ y los números perfectos pares.

No todos los patrones que se repiten entran en la definición de guía. Por ejemplo, no lo son $2^3 \cdot 3^2 \cdot 5 \cdot 13$, $2^5 \cdot 3^2 \cdot 7 \cdot 13$, $2^5 \cdot 3^3 \cdot 5$ y $2^5 \cdot 3^3 \cdot 5 \cdot 7$. Comprobemos la estabilidad de $2^5 \cdot 3^3 \cdot 5$. Si $n = 2^5 \cdot 3^3 \cdot 5 \cdot p \cdot q$, entonces $s(n) = 63 \cdot 40 \cdot 6 \cdot (p+1) \cdot (q+1) - 2^5 \cdot 3^3 \cdot 5 \cdot p \cdot q = 2^4 \cdot 3^3 \cdot 5 \cdot [7 \cdot (p+1) \cdot (q+1) - 2 \cdot p \cdot q]$ y el corchete contribuye con un 2^1 que hace que se mantenga el factor 2^5; sin embargo, es más fácil que cambie la potencia de 3, que resulta esencial en la estabilidad. La definición de guía se hace de tal forma que excluye los patrones cuya persistencia depende de consideraciones secundarias de la factorización de $\sigma(2^a)$ (en concreto, la estabilidad de $2^5 \cdot 3^3 \cdot 5$ depende de la potencia de 3,

y ésta es más fácil que cambie que la potencia de 2).

Cuando un término de una sucesión alicuatoria contiene un conductor, la sucesión se encuentra en una situación bastante estable, puesto que el conductor se va repitiendo, al menos con bastante probabilidad (lo mismo ocurre con muchos guías, aunque la estabilidad es menor). La disposición de factores necesaria para que pueda desaparecer es bastante exigente, luego es habitual que permanezca durante bastantes iteraciones.

Todos los conductores, salvo el 2, hacen la sucesión creciente (pues contienen un factor perfecto). Lo mismo sucede con muchos guías (no con los de la forma 2^a). Cuando la sucesión tiene a 2 como conductor, va decreciendo, al menos con bastante probabilidad. Por ejemplo, si $n = 2 \cdot p \cdot q$, entonces $s(n) = 3 \cdot (p+1) \cdot (q+1) - 2 \cdot p \cdot q = p \cdot q + 3 \cdot (p+q+1)$. Normalmente, al menos si los factores de n son grandes, $3 \cdot (p+q+1)$ es mucho menor que $p \cdot q$, luego $s(n) < n$.

Como le ocurre al resto de los guías, el 2 se puede ir. En efecto, sea $n = 2 \cdot p$, de donde $s(n) = 3 \cdot (p+1) - 2 \cdot p = p + 3$. Si $p = 4 \cdot r + 3$, entonces $s(n) = 2 \cdot (2 \cdot r + 3)$. Por el contrario, si $p = 4 \cdot r + 1$, entonces $s(n) = 2^2 \cdot (r+1)$ luego aparece, al menos, un factor 2^2. Como siempre, el comportamiento es similar si $n = 2 \cdot p^2 \cdot q$ o hay más factores primos elevados a potencias pares.

Los guías de la forma 2^a con $a > 1$ hacen que la sucesión vaya oscilando, unas veces crece y otras decrece, dependiendo de los otros factores. Además, estos guías cambian bastante fácilmente.

Si nos fijamos, sólo hemos analizado el comportamiento de $s(n)$ cuando n es par. ¿Qué pasa cuando es impar?

Si $n = p$ primo, $s(n) = 1$ y la sucesión se acaba. Supongamos ahora que $n = p \cdot q$ impar. Entonces, $s(n) = (p+1) \cdot (q+1) - p \cdot q = p + q + 1$ es también impar (generalmente, además, $s(n) < n$). Análogamente ocurre, por ejemplo, con $n = p^2 \cdot q$. Pero también puede suceder que n sea impar y $s(n)$ par. Esto tiene lugar cuando $n = p^2$; en efecto, en este caso $s(n) = (p^2 + p + 1) - p^2$, que es par. Como siempre, lo mismo ocurriría con más factores primos, todos elevados a potencias pares.

Siempre existe la probabilidad de que una sucesión alicuatoria llegue a un par de amigos o a un ciclo, con lo cual la sucesión se repite cíclicamente, y podemos considerar que ha alcanzado su final. Además de esta posibilidad (que, realmente, no ocurre muchas veces), la única forma de que la sucesión acabe es que llegue a un primo (siempre impar, pues 2 es intocable). La mayoría de las veces, los sucesivos términos de una sucesión van siendo pares. Tenemos pues que analizar cómo una sucesión puede pasar de un término par a uno impar. Esto ocurre cuando tenemos un término $n = 2^a \cdot p^2$, con $a > 0$ (o casos similares con el primo p elevado a una potencia par e, incluso, más

primos, también elevados a potencias pares). En efecto, en este caso, $s(n) = (2^a - 1) \cdot (1 + p + p^2) - 2^a \cdot p^2$, que es impar. A falta de más información, sólo el azar puede determinar ahora si la sucesión alicuatoria continuará iterando por términos impares hasta alcanzar un primo (y, por tanto, acabar), o si en alguno de estos pasos se transformará de nuevo en un término par.

3. Nuestros progresos con sucesiones alicuatorias

Tal como comentábamos anteriormente, los autores se han preocupado en estudiar computacionalmente las sucesiones alicuatorias que comienzan en $n < 10000$. Este trabajo avanzaba no sólo en el estudio de las sucesiones de Lehmer y Godwin, sino también en estudios previos de otros autores, como A. Guy y R. K. Guy, que habían analizado las sucesiones que comenzaban en $n \leq 7044$. Fruto de este trabajo, hallamos el final de varias sucesiones. En particular, el de la sucesión que comienza en 4170. Ésta es, hasta ahora, la sucesión con final conocido que alcanza un término mayor; concretamente $s^{289}(4170)$ tiene 84 cifras y acaba en $s^{869}(4170) = 1$, siendo 79 el primo previo. (Obviamente, esta afirmación requiere descartar casos triviales: por ejemplo, cualquier sucesión que comience en un primo acaba inmediatamente por grande que sea el primo.) Este trabajo fue publicado en [1]. Allí, además, se muestra el estado de todas las sucesiones principales que comienzan en $n < 10000$ hasta alcanzar términos de, al menos, 75 dígitos.

No entraremos en detalles de los algoritmos de factorización empleados. Simplemente, comentar que, principalmente, se ha usado una combinación del método de las curvas elípticas y de la criba cuadrática multipolinomial (véase [3]). Así, para descomponer en factores un número de 60 cifras (sin factores pequeños) se emplea alrededor de tres cuartos de hora en un Pentium 100; de modo similar, hora y media si el número tiene 65 cifras, 5 horas para uno con 70 cifras, 18 horas con 75 cifras, un día y medio con 80 cifras, 4 días con 85 cifras, y dos semanas con 90 cifras. Aumentar el número de cifras del último término alcanzado en una sucesión alicuatoria puede requerir muchas iteraciones, y estamos tratando más de 80 sucesiones. Esto supone una gran cantidad de tiempo de cálculo.

Es de destacar que en ningún momento hemos utilizado ningún programa comercial para llevar a cabo los cómputos (la mayoría de los paquetes informáticos comerciales destinados al cálculo matemático, tanto numérico como simbólico, ni siquiera tienen los algoritmos necesarios implementados y, si los tienen y hemos conseguido probarlos, sus implementaciones han resultado ser bastante peores que los de diversos programas que se pueden encontrar gratis en internet). A lo largo de diversas etapas de nuestro trabajo, los paquetes

n	276	552	564	660	966	1074	1134	1464	1476
k	1119	808	2970	439	472	1543	2234	1815	1055
dígitos	107	114	102	110	108	103	121	97	106
guía	$2\cdot3$	$2^5\cdot3\cdot7$	$2^2\cdot7$	2^2	$2\cdot3$	$2^2\cdot7$	$2^5\cdot3\cdot7$	$2^2\cdot7$	$2^3\cdot3\cdot5$
n	1488	1512	1560	1578	1632	1734	1920	1992	2232
k	748	1602	1336	1084	713	1367	1931	985	390
dígitos	97	94	101	100	102	99	97	102	102
guía	$2^3\cdot5$	$2^2\cdot7$	$2^5\cdot3\cdot7$	2^4	$2^3\cdot3\cdot5$	$2^2\cdot7$	$2^2\cdot7$	$2^3\cdot3\cdot5$	2^6
n	2340	2360	2484	2514	2664	2712	2982	3270	3366
k	471	974	796	2836	761	1347	810	417	1062
dígitos	99	95	97	95	100	95	97	98	100
guía	$2^3\cdot3\cdot5$	$2^2\cdot7$	$2^3\cdot3$	$2^3\cdot3\cdot5$	$2^2\cdot7$	$2^2\cdot7$	$2^4\cdot31$	$2^5\cdot3\cdot7$	2^3
n	3408	3432	3564	3630	3678	3774	3876	3906	4116
k	840	933	779	1193	1201	1193	830	679	897
dígitos	95	103	100	94	98	98	96	94	97
guía	$2^3\cdot3\cdot5$	$2^3\cdot3\cdot5$	$2^3\cdot3$	2^4	$2^2\cdot7$	$2^7\cdot3$	$2^2\cdot7$	$2^2\cdot7$	2^3
n	4224	4290	4350	4380	4788	4800	4842	5148	5208
k	519	913	1165	965	2152	1135	440	1545	1710
dígitos	98	92	97	100	105	101	91	95	96
guía	$2^3\cdot3\cdot5$	$2^2\cdot7$	$2^2\cdot7$	$2^2\cdot7$	$2^3\cdot3\cdot5$	$2^4\cdot31$	$2^2\cdot7$	$2\cdot3$	$2^3\cdot3\cdot5$
n	5250	5352	5400	5448	5736	5748	5778	6160	6396
k	1490	683	2696	1185	1093	958	742	1630	1234
dígitos	93	93	93	96	100	91	95	96	92
guía	2^5	$2^2\cdot7$	$2^2\cdot7$	$2^3\cdot3\cdot5$	$2^2\cdot7$	$2^2\cdot7$	$2^4\cdot31$	2^2	$2^3\cdot3\cdot5$
n	6552	6680	6822	6832	6984	7044	7392	7560	7890
k	893	1815	1177	885	1764	1113	498	846	891
dígitos	93	94	97	104	96	102	96	97	99
guía	$2^3\cdot3$	$2^4\cdot31$	$2^4\cdot31$	$2^3\cdot3$	$2^4\cdot31$	$2^4\cdot31$	$2^3\cdot3\cdot5$	$2^3\cdot5$	$2^2\cdot7$
n	7920	8040	8154	8184	8288	8352	8760	8844	8904
k	951	2205	647	1241	823	1246	2145	1184	963
dígitos	95	94	96	102	98	93	94	101	95
guía	$2^6\cdot127$	$2^3\cdot3\cdot5$	$2^2\cdot7$	$2^2\cdot7$	2^2	$2^2\cdot7$	$2^3\cdot3\cdot5$	$2^4\cdot31$	$2^2\cdot7$
n	9120	9282	9336	9378	9436	9462	9480	9588	9684
k	532	505	608	2111	545	447	924	1492	617
dígitos	92	95	97	92	94	97	91	93	92
guía	$2^3\cdot3$	$2^3\cdot3$	$2^6\cdot127$	$2^2\cdot7$	$2\cdot3$	$2^3\cdot3\cdot5$	$2\cdot3$	2^3	$2^5\cdot3\cdot7$
n	9708	9852							
k	671	591							
dígitos	95	92							
guía	$2^2\cdot7$	$2^2\cdot7$							

Cuadro 1: Sucesiones alicuatorias cuyo final está en duda.

que hemos empleado han sido PARI[2], KASH[3], MIRACL[4] y, fundamentalmente, UBASIC[5]. Los cálculos se han llevado a cabo en tiempos muertos, noches y fines de semana de numerosos ordenadores de las instituciones a las que pertenecemos, y en los personales de los autores o sus amigos.

Más tarde, tuvimos conocimiento de que P. Zimmermann y W. Bosma estaban haciendo, en parte, el mismo trabajo. Concretamente, P. Zimmermann estaba analizando las cinco sucesiones de Lehmer y las que comienzan por 1074 y 1134, y W. Bosma se estaba dedicando a las sucesiones que comienzan en $n \leq 50000$ (por ejemplo, el final de la sucesión 3556 fue encontrado por Bosma y los autores independientemente); lógicamente, cuantas más sucesiones se abarcan, menos tiempo computacional es posible dedicar a cada una. Entonces, nos repartimos el trabajo. Concretamente, en lo referente a las sucesiones que comienzan por $n < 10000$, en las que nos centraremos aquí, P. Zimmermann siguió con las suyas y nosotros nos dedicamos al resto. Realmente, desde la publicación de [1] no se ha encontrado el final de ninguna nueva de entre ellas. Pero se ha avanzado bastante en todas.

El estado actual de los cálculos para sucesiones alicuatorias que comienzan en $n < 10000$ es el que aparece resumido en la tabla 1, que amplía los resultados de [1]. En ella mostramos las 83 sucesiones principales cuyo final es aún desconocido. También incluimos el número de dígitos decimales del último $s^k(n)$ alcanzado para cada sucesión, y el guía en ese momento. Los datos de las 7 primeras sucesiones son de P. Zimmermann. Es de destacar que en todas las sucesiones se ha llegado a términos mayores que 10^{90}; en varias de ellas se han alcanzado las 100 cifras. El desarrollo completo de todas las sucesiones que parecen en la tabla puede conseguirse, mediante `ftp` anónimo, en `ftp://navalsaz.unirioja.es/pub/aliquot`.

Agradecimientos

Deseamos dar las gracias a Paul Zimmermann por brindarnos su colaboración durante varios años, y por permitirnos reproducir aquí los últimos términos alcanzados por él en las sucesiones que comienzan en $n \leq 1134$ (que también se pueden encontrar en su página web antes citada). Así mismo, debemos nuestro agradecimiento a las diversas personas que nos han cedido tiempo

[2]C. Batut, D. Bernardi, H. Cohen y M. Olivier, disponible en `ftp://megrez.ceremab.u-bordeaux.fr/pub/pari`.

[3]Desarrollado por M. E. Posh y *The KANT Group*; disponible en `ftp://ftp.math.tu-berlin.de/pub/algebra/Kant/Kash`. Para más información, véase `http://www.math.TU-Berlin.DE/~kant/kash.html`.

[4]M. Scott, disponible en `ftp://ftp.compapp.dcu.ie/pub/crypto`.

[5]Yuji Kida, disponible en `ftp://rkmath.rikkyo.ac.jp/ubibm`.

de cálculo en sus ordenadores personales o en los de sus instituciones; entre ellos Carlos José Pérez, Emilio Fernández, Jesús Murillo, M.ª Vico Pascual, Julio Rubio, Lourdes Benito y Esperanza Infante. También a numerosos becarios de salas informáticas de la Universidad de La Rioja. Si alguien se siente olvidado, le pedimos disculpas de antemano.

Del mismo modo, gracias a la Universidad de La Rioja y al Instituto Sagasta de Logroño por permitirnos usar sus ordenadores, en los que se llevaron a cabo la mayor parte de los cálculos. Por último, el segundo autor quiere agradecer a la Universidad de La Rioja los innumerables cortes de electricidad que hicieron el trabajo computacional mucho más entretenido.

Despedida

Hemos comenzado este artículo hablando de problemas abiertos en teoría de números. Acabemos con un acertijo relacionado con ellos.

Supongamos que, cada mes, los matemáticos plantean un nuevo problema de teoría de números. Y que, cada año, se resuelve uno de los aún abiertos, siempre el más antiguo. ¿Cuántos problemas quedarán sin resolver al final de los tiempos? ¿Y si, en vez de resolverse uno cada año, se resuelven dos, siempre los dos que ocupan las posiciones centrales (considerando los problemas ordenados temporalmente)?

Referencias

[1] M. Benito y J. L. Varona, Advances in aliquot sequences, *Math. Comp.* **68** (1999), 389–393.

[2] E. Catalan, Propositions et questions diverses, *Bull. Soc. Math. France* **18** (1887–88), 128–129.

[3] H. Cohen, *A course in computational algebraic number theory*, Springer-Verlag, 1993.

[4] W. Creyaufmüller, *Primzahlfamilien* (2.ª ed.), Wolfgang Creyaufmüller, Aachen, 1997.

[5] L. E. Dickson, Theorems and tables on the sum of the divisors of a number, *Quart. J. Math.* **44** (1913), 264–296.

[6] P. Erdős, On asymptotic properties of aliquot sequences, *Math. Comp.* **30** (1976), 641–645.

[7] R. K. Guy, *Unsolved Problems in Number Theory* (2.ª ed.), Springer-Verlag, 1994.

[8] R. K. Guy y J. L. Selfridge, What drives an aliquot sequence?, *Math. Comp.* **29** (1975), 101–107. Corrigendum, *ibid.* **34** (1980), 319–321.

[9] V. Klee y S. Wagon, *Old and new unsolved problems in plane geometry and number theory*, The Math. Assoc. of Amer., Washington, 1991.

[10] G. Pólya, *Matemáticas y razonamiento plausible*, Tecnos, Madrid, 1966.

[11] H. J. J. te Riele, On generating new amicable pairs from given amicable pairs, *Math. Comp.* **42** (1984), 219–223.

[12] W. Sierpiński, *A selection of problems in the theory of numbers*, Pergamon Press, 1964.

[13] S. Y. Yan, *Perfect, amicable and sociable numbers. A computacional approach*, World Scientific, Singapur, 1996.

Manuel Benito,
Instituto Sagasta,
C/ Doctor Zubía s/n, 26003 Logroño.
e-mail: mbenit8@palmera.pntic.mec.es

Juan Luis Varona,
Departamento de Matemáticas y Computación, Universidad de La Rioja,
C/ Luis de Ulloa s/n, 26004 Logroño.
e-mail: jvarona@dmc.unirioja.es
URL: http://www.unirioja.es/dptos/dmc/jvarona/welcome.html