Zubía 37-38 149-176 Logroño 2020-2021

LA CONJETURA DE ERDŐS-STRAUS*

MANUEL BELLO HERNÁNDEZ[1]
MANUEL BENITO MUÑOZ[2]
EMILIO FERNÁNDEZ MORAL[3]

RESUMEN

A finales de la década de 1940, Paul Erdős y Ernst G. Straus establecieron la siguiente conjetura (CES): *Dado un número natural* $n \geq 2$*, siempre existen números naturales x, y, z que cumplen*

$$\frac{4}{n} = \frac{1}{x} + \frac{1}{y} + \frac{1}{z}.$$

La conjetura hoy día sigue estando abierta. En este artículo presentamos un algoritmo sencillo que en caso de parada descompone la fracción $4/n$ ($n \geq 2$ entero) como suma de tres fracciones de numerador 1 (egipcias o unitarias), llegamos a formular varias conjeturas que ofrecen condiciones suficientes para la validez de la CES y demostramos, por ejemplo, que CES se cumple en particular para todos los valores n que están en la imagen del polinomio

$$p(a, b, c) = (a + 1)(4b + 3)(4c + 3) - (a + 1) - (4b + 3)$$

cuando las variables a, b y c toman valores enteros no negativos. Según comprobaciones asistidas por ordenador (nosotros lo hemos hecho para $n \leq 12 \times 10^{15}$),

* Registrado el 14 de abril de 2020. Aprobado el 19 de enero de 2021.

1. Dpto. de Matemáticas y Computación, Universidad de La Rioja, C/ Madre de Dios, 53, Edificio CCT, 26006 Logroño.
Correo electrónico: mbello@unirioja.es
2. Catedrático de Matemáticas jubilado. Instituto Práxedes Mateo Sagasta, Logroño.
Correo electrónico: mbenit8@palmera.pntic.mec.es
3. Profesor jubilado. Dpto. de Matemáticas y Computación, Universidad de La Rioja, C/ Madre de Dios, 53, Edificio CCT, 26006 Logroño.
Correo electrónico: emilio.fernandez@unirioja.es
La investigación del primer autor ha sido subvencionada parcialmente por el 'Ministerio de Economía y Competitividad', Proyecto MTM2014-54043-P.

Zubía | núm. 37-38 (2019-2020), pp. 149-176
ISSN 0213-4306

dichos valores n podrían incluir todos los números primos de la forma $4q + 1$ ($q \geq 1$). Y aunque, por un lado, probamos que los cuadrados no están en el conjunto imagen de $(\mathbb{N} \cup \{0\})^3$ por la función polinómica $p(a, b, c)$, por otro lado y con ayuda de esa función, hemos podido dar una demostración constructiva de que hay un conjunto tan grande como se quiera de números consecutivos para los que CES es cierta.

Palabras clave: Conjetura de Erdős-Straus; ecuaciones diofánticas; fracciones egipcias.

Paul Erdős and Ernst G. Straus conjectured in the late 1940s: Given a natural number $n \geq 2$ there are natural numbers x, y, z such that

$$\frac{4}{n} = \frac{1}{x} + \frac{1}{y} + \frac{1}{z}.$$

This conjecture (ESC) is open today. Among other results, in this paper we study ESC, we establish some conjectures that offer sufficient conditions for the validity of ESC, we give an algorithm which, if it stops, breaks down the fraction 4/n as a sum of three Egyptian fractions, and, for example, we show that ESC holds for all the values of n in the range of the polynomial

$$p(a, b, c) = (a + 1)(4b + 3)(4c + 3) - (a + 1) - (4b + 3),$$

when the variables a, b, c take nonnegative integer values. We conjecture that the values n of this polynomial include all the prime numbers of the form $4q+1$ ($q \geq 1$), and we have done a computer-assisted verification of this fact for $n \leq 12 \times 10^{15}$. On the one hand we prove that the perfect squares do not belong to the image set of $(\mathbb{N} \cup \{0\})^3$ by the mapping p but, on the other, with the help of that polynomial we have been able to give a constructive demonstration that there are arbitrarily long sequences of consecutive numbers for which ESC is true.

Key words: *Erdős-Straus' conjecture; Diophantine equations; Egyptian fractions.*

1. INTRODUCCIÓN

Las ecuaciones diofánticas plantean problemas de teoría de números que conectan esta rama de la matemática con el álgebra, la geometría, la topología y el análisis. Se trata a veces de problemas de enunciado muy sencillo, cuya formulación puede ser comprendida por un público bastante amplio, pero que en cambio

son muy difíciles de resolver. El ejemplo más señalado podría darlo el denominado «último teorema de Fermat», famosísimo resultado acerca de la imposibilidad de resolver la ecuación $x^n + y^n = z^n$ para $n > 2$ y x, y, z enteros no nulos, problema que quedó planteado en el siglo XVII y cuya solución definitiva, debida a Andrew Wiles en colaboración con Richard Taylor, no se obtuvo hasta mediada la década de 1990. Las técnicas empleadas o desarrolladas para la solución de este problema son hoy parte fundamental de la teoría algebraica de números.

Puede ser también el caso de la conjetura que estudiamos aquí. A finales de la década de 1940, Paul Erdős y Ernst Straus[1] conjeturaron (Bernstein 1962, p.1; Erdős 1950, p. 210; Guy 1994, p. 158–166): *Dado un número natural $n \geq 2$, siempre existen números naturales x, y, z para los que se cumple la ecuación*

$$\frac{4}{n} = \frac{1}{x} + \frac{1}{y} + \frac{1}{z}. \tag{1}$$

Dicho de otra manera, toda fracción racional $4/n$ con $n \geq 2$ se puede escribir, o descomponer, como suma de tres *fracciones unitarias* (fracciones de numerador 1, denominadas también *fracciones egipcias*). Erdős hizo pública esta conjetura, que Straus había comprobado ya hasta $n = 5000$, el año 1961 en una conferencia en la Universidad de Århus. La conjetura de Erdős-Straus, que abreviaremos como CES, combina propiedades aditivas y multiplicativas de los números naturales, y a fecha de hoy está comprobada para $n \leq 10^{17}$ pero su veracidad es aún un problema abierto.

Existen muchos artículos y resultados sobre esta conjetura. Para conocer la evolución en el tiempo de CES y su estado actual se pueden mirar, por ejemplo, las referencias (Elsholtz y Tao 2013), (Guy 1994) y (Mordell 1969). En este último libro, L. Mordell califica CES como «extremadamente interesante» y prueba que se cumple para todos los números naturales n excepto posiblemente para los que pertenecen a alguna de las clases de restos

$$1, 121, 169, 289, 361 \text{ o } 529 \pmod{840}.$$

Es inmediato ver que, si (1) tiene soluciones para un $n \geq 2$ dado, entonces también las tiene para todos los enteros positivos divisibles por n; por otra parte, $\frac{4}{4q+3} = \frac{1}{q+1} + \frac{1}{(q+1)(4q+3)}$, así que CES necesita ser comprobada, en realidad, sólo

1. Paul Erdős (1913-1996) es un matemático muy reconocido (Babai 1996), (Nešetřil 2000), con más de 1400 artículos publicados con más de 500 colaboradores científicos. Ernst Gabor Straus (1922-1983) fue el asistente de Albert Einstein en Princeton entre los años 1944 y 1948 (Cantor *et al.* 1985).

Zubía | núm. 37-38 (2019-2020), pp. 149-176
ISSN 0213-4306

para los números n que sean primos de la forma $4q + 1$ ($q \geq 1$). En nuestro artículo damos condiciones suficientes para la validez de CES y proponemos una conjetura (que llamamos *Conjetura q*) más fuerte. Otro de nuestros resultados originales es (Teorema 3.4) que no es posible generar de cierta manera natural un sistema finito de clases de congruencia para cuyos elementos se cumpla la conjetura de Erdős-Straus y cuya unión contenga a todos los números primos de la forma $4q + 1$. Por otra parte, hemos encontrado un polinomio en tres variables

$$p(a, b, c) := (a + 1)(4b + 3)(4c + 3) - (a + 1) - (4b + 3) \qquad (2)$$

tal que, si se denota

$$\mathcal{N}_1 := \{n \in \mathbb{Z} : (a, b, c) \in (\mathbb{N} \cup \{0\})^3 \text{ y } p(a, b, c) = n\},$$

se cumple que para todo $n \in \mathcal{N}_1$ la ecuación (1) tiene solución. Como se verá en la sección 3, el polinomio (2) proporciona una parametrización representativa de los números n tales que la descomposición de la fracción $4/n$ como suma de tres fracciones egipcias es *de tipo I*, es decir, una descomposición en la que solamente uno de los tres denominadores es múltiplo de n. Con ayuda del polinomio (2) hemos podido dar una demostración constructiva de que hay secuencias arbitrariamente largas de números naturales consecutivos n para los cuales la conjetura CES es cierta.

Por otra parte, hemos diseñado un algoritmo para hallar soluciones de (1) dado $n \geq 2$, que llamamos *greedy*, o de tipo *greedy*[2], porque en uno de sus pasos encuentra la fracción unitaria más próxima a cierta fracción intermedia obtenida. Según los experimentos numéricos que hemos realizado, nuestro algoritmo de tipo *greedy* se detiene para todos los primos $n < 12 \times 10^{15}$ y para clases generales de números cuya unión podría contener a todos los números primos de la forma $4q + 1$, aunque esto no lo hemos podido probar.

La organización del resto del artículo, que reexpone (Bello-Hernández *et al.* 2012) de forma abreviada, es como sigue. En la sección 2 estudiamos la descomposición de una fracción racional como suma de dos fracciones unitarias, y determinamos (Teorema 2.4) el número de descomposiciones de una fracción unitaria como suma de dos del mismo tipo. Completamos la sección proporcionando (Proposición 2.10) una condición necesaria sobre n para que la fracción $\frac{a}{n}$ admita alguna descomposición como suma de dos fracciones unitarias, cuando $a = p^\gamma$, $\gamma \geq 1$ y p es un número primo impar. En la sección 3 estudiamos la conjetura CES; mostramos cómo aparece, a través de distintas parametrizaciones, la expresión del polinomio (2) (subsección 3.1), y probamos que hay tantos números

2. En español está bastante extendido decir algoritmo *voraz*, o algoritmo *del avaro*, para denominar a este tipo de algoritmos. En nuestro artículo seguiremos usando la expresión inglesa.

Zubía | núm. 37-38 (2019-2020), pp. 149-176
ISSN 0213-4306

consecutivos como se quiera para los que CES es cierta. Con ayuda del mismo polinomio (2) planteamos nuestra *Conjetura q*, suficiente para la validez de CES, que está relacionada a su vez (Proposición 3.8) con la posible *universalidad* de cierto sistema de polinomios en tres variables. En la subsección 3.2 vemos que en la imagen de $(\mathbb{N} \cup \{0\})^3$ por el polinomio (2) no hay ningún cuadrado perfecto (Proposición 3.10). Dedicamos la última sección al estudio del algoritmo *greedy* que, en caso de parada, obtiene una descomposición de la fracción *4/n* como suma de tres fracciones unitarias; demostramos que acaba por detenerse para una amplia clase de números, y de hecho llegamos a caracterizar el conjunto de números para los que se detiene (Proposición 4.3). Terminamos el artículo probando (Proposición 4.4) la existencia de números que requieren de tantos pasos como se desee antes de la parada del algoritmo.

2. SOBRE SUMAS DE DOS FRACCIONES UNITARIAS

En esta sección estudiamos algunas cosas relacionadas con la descomposición de una fracción racional $\frac{m}{n}$ como suma de dos fracciones unitarias. Todos los resultados que vamos a presentar, salvo quizá el Teorema 2.4, son bien conocidos (ver Croot III *et al.* 2000), y los incluimos aquí solamente en favor de una lectura autocontenida. Destacamos especialmente la Proposición 2.10, referida al caso en que el numerador *m* es potencia de un número primo (ver Huang y Vaughan 2011).

En general, basta considerar una descomposición $n = abc$ del número n en tres factores (una *trifactorización*) para tener de forma inmediata una descomposición de la fracción $\frac{1}{n}$ como suma de otras dos fracciones unitarias, de la siguiente forma:

$$\frac{1}{n} = \frac{1}{a(a+b)c} + \frac{1}{b(a+b)c}. \tag{3}$$

Vamos a empezar probando que el número $R(n)$ de descomposiciones diferentes de la fracción $\frac{1}{n}$ como suma de otras dos fracciones unitarias es igual al número de trifactorizaciones de n de cierta forma especial. Anteponemos una definición sencilla.

Definición 2.1. *Sea* $n \in \mathbb{N}$. *Supongamos que* $n = abc$ *con* $a, b, c \in \mathbb{N}$. *Si*[3] $(a, b) = 1$, *entonces decimos que* $a \cdot b \cdot c$ *es una trifactorización admisible de n, y entendemos, en ese caso, que* $b \cdot a \cdot c$ *es la misma trifactorización admisible de n.*

Así, si $a \cdot b \cdot c$ es una trifactorización admisible de n, $b \neq c$ y $(a, c) = 1$, entonces $a \cdot c \cdot b$ es otra trifactorización admisible de n que es distinta de la primera. Por

3. Con la notación (a, b) se representa el *máximo común divisor* de los números a y b.

Zubía | núm. 37-38 (2019-2020), pp. 149-176
ISSN 0213-4306

ejemplo, si $n = p$ primo, caben dos trifactorizaciones admisibles de n, a saber, $n = 1 \cdot 1 \cdot p$ y $n = p \cdot 1 \cdot 1$. Si $n = pq$ con $p \neq q$ primos, caben estas cinco: $n = p \cdot q \cdot 1$, $n = p \cdot 1 \cdot q$, $n = q \cdot 1 \cdot p$, $n = (pq) \cdot 1 \cdot 1$ y $n = 1 \cdot 1 \cdot (pq)$.

Dado $n \in \mathbb{N}$, queda definida una aplicación $\Phi_n : a \cdot b \cdot c \mapsto \{x, y\}$ del conjunto de las trifactorizaciones admisibles de n en el conjunto de las descomposiciones de $\frac{1}{n}$ como suma de dos fracciones unitarias dada simplemente, de acuerdo con (3), por $x = a(a + b)c$, $y = b(a + b)c$. Vamos a probar, de hecho, que Φ_n es una biyección, de donde se deduce que los dos conjuntos anteriores tienen el mismo número de elementos. Comenzamos probando en el siguiente lema que Φ_n es sobreyectiva.

Lema 2.2. *Sea $n \in \mathbb{N}$ fijo. Si $\frac{1}{n} = \frac{1}{x} + \frac{1}{y}$ con $x, y \in \mathbb{N}$, existe una trifactorización admisible de n de la forma $n = a \cdot b \cdot c$, con $(a, b) = 1$, siendo $x = a(a + b)c$ e $y = b(a + b)c$.*

Demostración. Por hipótesis es $xy = (x + y)n$; sea $(x, y) = d$, de modo que $x = da$, $y = db$ con $(a, b) = 1$, y sustituyendo y dividiendo por d se obtiene $abd = (a + b)n$, de donde se deduce que $a|n$, $b|n$ y $(a + b)|d$. Por lo tanto, para $a = \frac{x}{d}$, $b = \frac{y}{d}$, $c = \frac{d}{a+b}$, se tiene $n = abc$, $x = a(a + b)c$, $y = b(a + b)c$, $(a, b) = 1$ y se verifica (3). □

Proposición 2.3. *Sea $n \in \mathbb{N}$. El número $R(n)$ de descomposiciones diferentes de la fracción unitaria $\frac{1}{n}$ como suma de dos fracciones unitarias es igual al número de trifactorizaciones admisibles de n.*

Demostración. Sólo queda ver que Φ_n es inyectiva. Supongamos que las trifactorizaciones $a_1 \cdot b_1 \cdot c_1$ y $a_2 \cdot b_2 \cdot c_2$ de n, siendo $(a_1, b_1) = 1$ y $(a_2, b_2) = 1$, generan la misma descomposición de $\frac{1}{n}$ como suma de dos fracciones unitarias según (3), es decir, que

$$\frac{1}{a_1(a_1 + b_1)c_1} + \frac{1}{b_1(a_1 + b_1)c_1} = \frac{1}{a_2(a_2 + b_2)c_2} + \frac{1}{b_2(a_2 + b_2)c_2}.$$

Entonces, o bien

$$a_1(a_1 + b_1)c_1 = a_2(a_2 + b_2)c_2 \quad \text{y} \quad b_1(a_1 + b_1)c_1 = b_2(a_2 + b_2)c_2$$

o bien

$$a_1(a_1 + b_1)c_1 = b_2(a_2 + b_2)c_2 \quad \text{y} \quad b_1(a_1 + b_1)c_1 = a_2(a_2 + b_2)c_2.$$

Si $a_1(a_1+b_1)c_1 = a_2(a_2+b_2)c_2$, entonces $a_1^2c_1 = a_2^2c_2$. Multiplicando esta igualdad por b_1b_2, nos queda $a_1b_2 = a_2b_1$. Como $(a_1, b_1) = 1$ y $(a_2, b_2) = 1$, la anterior

relación es equivalente a que $a_1 = a_2$ y $b_1 = b_2$. En el otro caso se procede de forma análoga y resulta que $a_1 = b_2$ y $a_2 = b_1$. □

Teorema 2.4. *Sea $n \in \mathbb{N}$ y $R(n)$ el número de descomposiciones diferentes de la fracción unitaria $\frac{1}{n}$ como suma de dos fracciones unitarias. Se cumple que $R(1) = 1$ y, si $n = \prod_{j=1}^{m} p_j^{\alpha_j}$ $(\alpha_j \geq 1)$ es la descomposición del número natural $n > 1$ en factores primos, se tiene*

$$R(n) = \frac{1}{2}\Big(\prod_{j=1}^{m}(2\alpha_j + 1) + 1\Big).$$

Demostración. Usaremos la Proposición 2.3. En primer lugar es obvio que $R(1) = 1$, pues la única descomposición de $\frac{1}{1}$ como suma de dos fracciones unitarias es $\frac{1}{2} + \frac{1}{2}$.

Cuando $n = p$, con p primo, se tiene $R(p) = 2$ como ya hemos indicado antes. Sea $n = p^\alpha$, $\alpha \geq 2$, y supongamos, por inducción en α, que $R(p^{\alpha-1}) = \alpha$. Las trifactorizaciones admisibles de n son $1 \cdot p^\alpha \cdot 1$ y las de la forma $a \cdot b \cdot (pc)$ obtenidas a partir de una trifactorización admisible $a \cdot b \cdot c$ de $p^{\alpha-1}$. Luego $R(p^\alpha) = 1 + R(p^{\alpha-1}) = \alpha + 1$.

El caso general lo probamos por inducción sobre el número de factores primos de n. Sea $n = \prod_{j=1}^{m} p_j^{\alpha_j}$ con $m \geq 2$ la descomposición en factores primos de un entero positivo n, y supongamos que $R(\prod_{j=2}^{m} p_j^{\alpha_j}) = \frac{1}{2}(\prod_{j=2}^{m}(2\alpha_j + 1) + 1)$. Observemos que si $a_1 \cdot b_1 \cdot c_1$ y $a_2 \cdot b_2 \cdot c_2$ son trifactorizaciones admisibles de $\prod_{j=2}^{m} p_j^{\alpha_j}$ y de $p_1^{\alpha_1}$ respectivamente, entonces $(a_1a_2)\cdot(b_1b_2)\cdot(c_1c_2)$ es una trifactorización admisible de $\prod_{j=1}^{m} p_j^{\alpha_j}$. Además, si $(a_1, b_1, c_1) \neq (1, 1, \prod_{j=2}^{m} p_j^{\alpha_j})$ y $(a_2, b_2, c_2) \neq (1, 1, p_1^{\alpha_1})$, se tiene que $(a_1b_2) \cdot (b_1a_2) \cdot (c_1c_2)$ es también una trifactorización admisible de $\prod_{j=1}^{m} p_j^{\alpha_j}$. De uno u otro modo resultan todas las posibles trifactorizaciones admisibles de n; por lo tanto

$$\begin{aligned} R\Big(\prod_{j=1}^{m} p_j^{\alpha_j}\Big) &= 2\big(R(p_1^{\alpha_1}) - 1\big)\Big(R\Big(\prod_{j=2}^{m} p_j^{\alpha_j}\Big) - 1\Big) + R\Big(\prod_{j=2}^{m} p_j^{\alpha_j}\Big) + R(p_1^{\alpha_1}) - 1 \\ &= \big(1 + 2(R(p_1^{\alpha_1}) - 1)\big)R\Big(\prod_{j=2}^{m} p_j^{\alpha_j}\Big) - \big(R(p_1^{\alpha_1}) - 1\big) \\ &= \frac{1}{2}\Big(\prod_{j=1}^{m}(2\alpha_j + 1) + 1 + 2\alpha_1\Big) - \alpha_1 = \frac{1}{2}\Big(\prod_{j=1}^{m}(2\alpha_j + 1) + 1\Big). \end{aligned}$$ □

El siguiente resultado ofrece una caracterización de las fracciones que se pueden descomponer como suma de dos fracciones unitarias.

Zubía | núm. 37-38 (2019-2020), pp. 149-176
ISSN 0213-4306

LEMA 2.5. *La fracción $\frac{m}{n}$ se puede descomponer como suma de dos fracciones unitarias si y sólo si existen $k_1, k_2 \in \mathbb{N}$ tales que*

$$k_1 k_2 = n^2, \tag{4}$$

$$m|(n + k_1) \text{ y } m|(n + k_2). \tag{5}$$

DEMOSTRACIÓN. Si se cumplen las condiciones (4) y (5), se tiene que los números naturales $a = (n + k_1)/m$ y $b = (n + k_2)/m$ satisfacen

$$\frac{1}{a} + \frac{1}{b} = m\Big(\frac{1}{n + k_1} + \frac{1}{n + k_2}\Big) = m\Big(\frac{2n + k_1 + k_2}{n^2 + (k_1 + k_2)n + k_1 k_2}\Big)$$
$$= m\Big(\frac{2n + k_1 + k_2}{n(2n + k_1 + k_2)}\Big) = \frac{m}{n}.$$

Recíprocamente, si $\frac{m}{n} = \frac{1}{a} + \frac{1}{b}$, con $a, b \in \mathbb{N}$, entonces para los números naturales $k_1 = am - n$ y $k_2 = bm - n$ se cumple que $m|(n + k_j)$ $(j = 1, 2)$, y

$$k_1 k_2 = (am - n)(bm - n) = abm^2 - (a + b)mn + n^2$$
$$= abmn\left(\frac{m}{n} - \left(\frac{1}{a} + \frac{1}{b}\right)\right) + n^2 = n^2,$$

como queríamos probar. □

LEMA 2.6. *Dados $a, n \in \mathbb{N}$ primos entre sí, es decir, tales que $(a, n) = 1$, la ecuación*

$$\frac{a}{n} = \frac{1}{x} + \frac{1}{y} \tag{6}$$

es resoluble en enteros positivos si y sólo si existen $u, v \in \mathbb{N}$ tales que $uv|n$ y $a|(u + v)$.

DEMOSTRACIÓN. Si $\frac{a}{n} = \frac{1}{x} + \frac{1}{y}$ y $(x, y) = d$, entonces $x = dx'$, $y = dy'$ con $(x', y') = 1$ y

$$adx'y' = n(x' + y').$$

Como $(x'y', x' + y') = 1$, se tiene que $x'y'|n$, y como $(a, n) = 1$, se tiene $a|(x' + y')$. Recíprocamente, si existen u, v tales que $uv|n$ y $a|(u + v)$, entonces $u + v = aa'$ y

$$\frac{a}{n} = \frac{aa'}{na'} = \frac{u + v}{na'} = \frac{1}{na'/u} + \frac{1}{na'/v},$$

con na'/u y na'/v enteros por hipótesis. □

Con mayor generalidad, denotaremos a continuación por $R_a(n)$, para a y n fijos, el número de soluciones $\{x, y\}$ de la ecuación (6), es decir, el número de representaciones distintas de la fracción $\frac{a}{n}$ como suma de dos fracciones unitarias. Vamos a completar esta sección proporcionando una condición necesaria sobre n para que sea $R_a(n) = 0$ cuando $a = p^\gamma, \gamma \geq 1$ y $p > 2$ primo.

Recordemos que, dado un número natural a, la relación de *congruencia módulo a* ($r \equiv s$ (mód a) si $r - s$ es múltiplo de a) divide el conjunto $\mathbb{Z}$ de los números enteros en a clases de equivalencia disjuntas, conteniendo cada una de ellas a los números que dan el mismo resto (de los a restos posibles $0, 1, \ldots, a-1$) al dividirlos por a. El conjunto de las a clases se denota por $\mathbb{Z}_a$. Los elementos de $\mathbb{Z}_a$ se pueden denotar ahora también por $0, 1, \ldots, a-1$, quedando inducidas en este conjunto operaciones de suma y producto[4] (*suma* y *multiplicación* de enteros *módulo a*; por ejemplo, $1 + 1 = 0$ en $\mathbb{Z}_2$; $2 + 3 = 1$ en $\mathbb{Z}_4$; $2 \cdot 2 = 0$ en $\mathbb{Z}_4$; $2 \cdot 3 = 1$ en $\mathbb{Z}_5$).

Sea $\mathbb{Z}_a^*$ el subconjunto de los elementos no nulos de $\mathbb{Z}_a$ que son primos con a; el conjunto $\mathbb{Z}_a^*$ tiene $\varphi(a)$ elementos[5]. Es bien conocido que $\mathbb{Z}_a^*$ es un grupo con la operación de multiplicación módulo a, de orden $\varphi(a)$. Cuando $a = p^\gamma$, $\gamma \geq 1$ y p primo impar, se sabe que $\mathbb{Z}_a^*$ es un grupo cíclico[6] y, por consiguiente, existe $g \in \mathbb{Z}_a^*$ tal que

$$\mathbb{Z}_a^* = \langle g \rangle = \{1, g, g^2, \ldots, g^{\varphi(a)-1}\}.$$

Este elemento g generador del grupo, que en general no es único, se llama una *raíz primitiva* módulo a. Por ejemplo, para $a = 9$ es $\mathbb{Z}_9^* = \{1, 2, 4, 5, 7, 8\} = \langle 2 \rangle$, un grupo cíclico de orden 6. Además de 2, también 5 es raíz primitiva módulo 9.

El siguiente lema (ver Fraleigh y Katz 2003, Thm. 6.14), que después vamos a utilizar, proporciona un resultado muy estándar sobre la estructura de los grupos cíclicos (usamos notación multiplicativa para la operación del grupo).

Lema 2.7. *Sea G el grupo cíclico de orden n engendrado por un elemento a, y sea s un entero no negativo. El orden del subgrupo $\langle a^s \rangle$ engendrado por el elemento a^s* (dicho de otra manera, el orden de a^s) *es n/d, donde $d = (n, s)$. Además, si s, t son enteros no negativos, $\langle a^s \rangle = \langle a^t \rangle$ si y sólo si $(n, s) = (n, t)$.*

4. Cuyas propiedades confieren a $\mathbb{Z}_a$, en general, una estructura algebraica de anillo con unidad. En particular, con la operación suma, $\mathbb{Z}_a$ es un grupo abeliano de *orden a* (es decir, de a elementos) cuya estructura es de *grupo cíclico*.

5. La *función indicatriz de Euler* $\varphi(m)$ se define precisamente como el número de elementos del conjunto $\{k \in \mathbb{N} : 1 \leq k < m, (k, m) = 1\}$.

6. Isomorfo, por consiguiente, al grupo cíclico aditivo $\mathbb{Z}_{\varphi(a)}$. Esto ocurre, como ya probó C. F. Gauss, sólo cuando $a = 1, 2, 4, p^\gamma$ o $2p^\gamma$, donde $\gamma \geq 1$ y p es un primo impar (*Disquisitiones Arithmeticæ*, artt. 52–56 y 82–89).

Zubía | núm. 37-38 (2019-2020), pp. 149-176
ISSN 0213-4306

Todo subgrupo de un grupo cíclico es cíclico, con lo que el siguiente resultado, igualmente estándar, es una sencilla consecuencia de este lema.

Corolario 2.8. *Si G es un grupo cíclico de orden finito n, y $\mathcal{H}_1$ y $\mathcal{H}_2$ son dos subgrupos de G del mismo orden, entonces $\mathcal{H}_1 = \mathcal{H}_2$, es decir, $\mathcal{H}_1$ y $\mathcal{H}_2$ están formados por los mismos elementos.*

El Lema 2.6 sugiere que la posibilidad de tener soluciones en la ecuación (6) depende solamente de los restos módulo a de los factores de n y, por lo tanto, de los restos módulo a de los factores primos de n, lo que conduce nuestro estudio a considerar la distribución de los factores primos de n en el grupo multiplicativo $\mathbb{Z}_a^*$. Nos ocuparemos sólo del caso en que $a = p^\gamma$ con $\gamma \geq 1$ y p es un número primo impar; el orden de $\mathbb{Z}_a^*$ es entonces $\varphi(p^\gamma) = p^{\gamma-1}(p-1) \equiv 0 \pmod 2$.

Lema 2.9. *Sean p un primo impar, $a = p^\gamma$ con $\gamma \in \mathbb{N}$ y $G = \mathbb{Z}_a^*$. Pongamos que sea $\varphi(a) = 2^m d$ con $m \geq 1$ y d impar. Si $g \in G$ es una raíz primitiva módulo a, consideremos el subgrupo de orden d, que denotaremos $\mathcal{H}_a$, engendrado por el elemento g^{2^m}, es decir,*

$$\mathcal{H}_a = \langle g^{2^m} \rangle = \{g^{2^m}, g^{2\cdot 2^m}, g^{3\cdot 2^m}, \ldots, g^{d\cdot 2^m}\}.$$

Entonces, las siguientes caracterizaciones de $\mathcal{H}_a$ son equivalentes:

(i) *$\mathcal{H}_a$ es el subgrupo maximal de G de orden impar.*

(ii) *$\mathcal{H}_a$ es el subgrupo maximal de G tal que $a - 1 \notin \mathcal{H}_a$.*

Demostración. Veamos primero que la propiedad (i) caracteriza al subgrupo $\mathcal{H}_a$. Se tiene $|G| = \varphi(a) = 2^m d$ con $m \geq 1$. Si g es una raíz primitiva módulo a, se tiene $\langle g \rangle = G$ y, aplicando el Lema 2.7, el orden del subgrupo $\mathcal{H}_a$ (lo mismo que el orden del elemento g^{2^m}) es d. Por consiguiente, $g^{2^m d} = g^{\varphi(a)} = 1$ y

$$g^{\varphi(a)/2} = g^{2^{m-1}d} = a - 1,$$

ya que $\left(g^{\varphi(a)/2}\right)^2 = 1$ y las potencias de g de exponentes $1, 2, \ldots, 2^m d$ cubren inyectivamente el conjunto $\mathbb{Z}_a^* = \{1, 2, \ldots, a-1\}$.

Según el teorema de Lagrange, el orden de cualquier subgrupo de G divide al orden de G; y según el Corolario 2.8, para un cierto orden dado el subgrupo de G con dicho orden es único. Por lo tanto, como d es el mayor número impar que divide a $\varphi(a)$ y $|\mathcal{H}_a| = d$, entonces $\mathcal{H}_a$ es el subgrupo maximal de G que tiene orden impar. Así que (i) caracteriza al subgrupo $\mathcal{H}_a$.

Para probar que (ii) equivale a (i) basta observar que $\{1, a-1\}$ es un subgrupo de G de orden 2 y que entonces, por el teorema de Lagrange, si un subgrupo de G contiene a $a - 1$, tiene que ser de orden par. □

Por ejemplo, cuando $a = 9$, $\mathcal{H}_9$ es el subgrupo $\langle 2^2 \rangle = \{1, 4, 7\} \subset \mathbb{Z}_9^*$, maximal de orden impar.

Proposición 2.10. *Siendo p un primo impar, sean $a = p^\gamma$ con $\gamma \geq 1$ y $\mathcal{H}_a$ el subgrupo de $\mathbb{Z}_a^*$ del Lema 2.9. Sea $n \in \mathbb{N}$ tal que $(n, a) = 1$ y supongamos además que todos los divisores primos de n pertenecen, módulo a, al subgrupo $\mathcal{H}_a$. Entonces, $R_a(n) = 0$.*

Demostración. Dado $n \in \mathbb{N}$ cumpliendo las hipótesis de la proposición, sean u y v dos enteros positivos primos entre sí y tales que $(uv)|n$. Todos los factores primos de u y los de v son también factores primos de n, luego pertenecen, módulo a, al subgrupo multiplicativo $\mathcal{H}_a$. Entonces u y v pertenecen, módulo a, a $\mathcal{H}_a$, es decir, $u \equiv u_0 \pmod{a}$ y $v \equiv v_0 \pmod{a}$, con $u_0 \in \mathcal{H}_a$ y $v_0 \in \mathcal{H}_a$.

Pero, según el Lema 2.9, $a - 1 \notin \mathcal{H}_a$, luego $a - v_0 \notin \mathcal{H}_a$, y entonces $u_0 \neq a - v_0$, es decir, $u_0 + v_0 \neq a$. Por otra parte, se tiene $1 < u_0 + v_0 < 2a$, luego $u + v \not\equiv 0 \pmod{a}$ y deducimos que $a \nmid u + v$, lo que según el Lema 2.6 permite asegurar que la fracción $\frac{a}{n}$ no se puede descomponer como suma de dos fracciones unitarias, es decir, que $R_a(n) = 0$. □

Observación 2.11. Para $a = 3$ tenemos $\mathbb{Z}_3^* = \{1, 2\} = \langle 2 \rangle$, de orden $\varphi(3) = 2 = 2 \cdot 1$, y el subgrupo $\mathcal{H}_3$ es $\langle 2^2 \rangle = \langle 1 \rangle = \{1\}$. De acuerdo con la proposición anterior, si todos los divisores primos de un número dado n son congruentes con $1 \pmod{3}$, se tendrá $R_3(n) = 0$. Equivalentemente, si la fracción $\frac{3}{n}$ admite alguna descomposición como suma de dos fracciones unitarias, entonces alguno de los divisores primos de n debe ser congruente con 0 o con 2 módulo 3. Por otro lado, si $n = 3k$ se tiene $\frac{3}{n} = \frac{1}{k} = \frac{1}{2k} + \frac{1}{2k}$ y, si $n = (3k + 2)(3h + 1)$, según el Lema 2.6 la fracción $\frac{3}{n}$ es descomponible como suma de dos fracciones unitarias, ya que $3|(3k + 2 + 3h + 1)$. Así concluímos que *la ecuación $\frac{3}{n} = \frac{1}{x} + \frac{1}{y}$ tiene solución si y sólo si n tiene un divisor que es múltiplo de 3 o congruente con 2 módulo 3*.

3. LA CONJETURA DE ERDŐS-STRAUS

Acabamos de ver que la ecuación $\frac{3}{n} = \frac{1}{x} + \frac{1}{y}$ tiene solución si y sólo si n tiene un divisor que es múltiplo de 3 o congruente con 2 módulo 3; dicho de otra manera, para descomponer la fracción $\frac{3}{n}$ como suma de fracciones unitarias harán falta al menos tres, en general. La conjetura de Erdős-Straus está asociada en primera instancia a la cantidad mínima de fracciones unitarias necesarias para descomponer la fracción $\frac{4}{n}$, pero en última instancia está vinculada con propiedades aritméticas de los números naturales como se verá en esta sección. El siguiente

Zubía | núm. 37-38 (2019-2020), pp. 149-176
ISSN 0213-4306

lema es bien conocido; consultar, por ejemplo (Bernstein 1962), (Mordell 1969, p. 287) o (Yamamoto 1965, Lemma 1).

Lema 3.1. *Sea n un número primo. La ecuación* (1) *tiene solución si y sólo si existen números naturales a, b, c, d tales que se cumple alguna de las siguientes condiciones:*

$$(4abc - 1)d = (a + b)n, \tag{7}$$

$$(4abc - 1)d = an + b. \tag{8}$$

Demostración. Si se cumple (7), o bien (8), dividiendo estas ecuaciones por *abcdn* obtenemos respectivamente

$$\frac{4}{n} = \frac{1}{abcn} + \frac{1}{bcd} + \frac{1}{acd}, \tag{9}$$

$$\frac{4}{n} = \frac{1}{abcn} + \frac{1}{bcd} + \frac{1}{acdn}. \tag{10}$$

Recíprocamente, si (1) tiene la solución $\{x, y, z\}$, entonces se tiene $4xyz = n(xy + yz+zx)$. Ya que n es primo, dividirá a alguno[7] de los números x, y o z; supongamos, por ejemplo, que $x = an$. Entonces (1) es equivalente a

$$\frac{4a - 1}{na} = \frac{1}{y} + \frac{1}{z},$$

es decir, a la descomposición

$$\frac{1}{na} = \frac{1}{(4a - 1)y} + \frac{1}{(4a - 1)z}. \tag{11}$$

Como n es primo, tenemos que considerar dos casos: que sea $(4a - 1, n) = 1$ o que sea $(4a - 1, n) = n$.

Si $(4a - 1, n) = 1$, de acuerdo con el Lema 2.2 existen números naturales a_1, a_2, a_3 tales que $a = a_1a_2a_3$, $(na_1, a_2) = 1$ y

$$(4a - 1)y = na_1(na_1 + a_2)a_3, \quad (4a - 1)z = a_2(na_1 + a_2)a_3. \tag{12}$$

Como también es $(na, 4a - 1) = (na_1a_2a_3, 4a - 1) = 1$, existen α, β tales que $y = \alpha na_1a_3$, $z = \beta a_2a_3$. Sustituyendo en (12) obtenemos $(4a-1)\alpha = (na_1+a_2) = (4a - 1)\beta$, de donde resulta $\alpha = \beta$. Por lo tanto, los números $A = a_1$, $B = a_2$, $C = a_3$ y $D = \alpha$ satisfacen la condición

$$(4ABC - 1)D = nA + B.$$

7. Aunque no a los tres: si $x = nx_1$, $y = ny_1$, y $z = nz_1$, sería $4 = \frac{1}{x_1} + \frac{1}{y_1} + \frac{1}{z_1} < 3$, absurdo.

En el caso $(4a-1, n) = n$, existe j tal que

$$4a - 1 = jn. \tag{13}$$

Sustituyendo esta expresión en (11) obtenemos $\frac{1}{a} = \frac{1}{jy} + \frac{1}{jz}$. De donde se sigue que existen enteros positivos a_1, a_2, a_3 tales que $a = a_1a_2a_3$, $(a_1, a_2) = 1$ y

$$jy = a_1(a_1 + a_2)a_3, \quad jz = a_2(a_1 + a_2)a_3. \tag{14}$$

De (13) resulta que $(j, a) = (j, a_1a_2a_3) = 1$ luego, por (14), existen α, β tales que $y = \alpha a_1a_3$, $z = \beta a_2a_3$. Sustituyendo en (14) se obtiene $j\alpha = a_1 + a_2 = j\beta$ y $\alpha = \beta$. Multiplicando por α la ecuación(13) se concluye que los números $A = a_1$, $B = a_2$, $C = a_3$ y $D = \alpha$ satisfacen la condición

$$(4ABC - 1)D = (A + B)n. \qquad \square$$

Si n es primo, las relaciones (7) y (8) son equivalentes, respectivamente, a (9) y (10). El número n divide sólo a uno de los denominadores de la descomposición (9), mientras que en la (10) divide a dos. Nos referiremos a ellas denominándolas respectivamente *descomposición de tipo I*, o *de tipo II*, de la fracción $\frac{4}{n}$. Mediante cambios de variables en (7) y (8) se obtienen inmediatamente, para los valores de n, las parametrizaciones que aparecen y se prueban en el lema siguiente.

Lema 3.2. (i) *Sea n un número primo. La condición* (7) *se cumple si y sólo si existen números naturales* $\alpha, \beta, \gamma, \delta$ *tales que*

$$\delta n = (4\alpha\beta\gamma\delta - 1) - 4\alpha^2\gamma. \tag{15}$$

(ii) *Sea* $n \geq 2$ *un número entero. La condición* (8) *se cumple si y sólo si existen números naturales* $\alpha, \beta, \gamma, \delta$ *tales que*

$$n = (4\alpha\beta\gamma - 1)\delta - 4\beta^2\gamma. \tag{16}$$

Demostración. (i) Si n es primo y se cumple (7), se deduce que d divide a $a+b$, pues suponer $(d, n) = n$ conduce a la desigualdad $a + b + 1 \geq 4ab$ que no tiene soluciones enteras positivas. Sea entonces $e = \frac{a+b}{d}$; de aquí resulta $b = de - a$, y la condición (7) da: $en = (4acde - 1) - 4a^2c$. Haciendo $\delta = e, \alpha = a, \beta = d$, y $\gamma = c$, obtenemos (15). Recíprocamente, si se cumple (15), deshaciendo los cambios anteriores obtenemos (7).

(ii) Si consideramos que se cumple (8), deducimos que $b + d$ es divisible por a. Sea $s = \frac{b+d}{a}$; resulta $d = as - b$, y de (8) obtenemos la relación $n + s = 4bcd$. Tomando $\alpha = a, \beta = b, \gamma = c$ y $\delta = s$ resulta inmediatamente (16). Y recíprocamente, si se cumple (16), sin más que deshacer los cambios anteriores obtenemos (8). $\square$

Zubía | núm. 37-38 (2019-2020), pp. 149-176
ISSN 0213-4306

La simetría de las relaciones (15) y (16) y la comparación de ejemplos numéricos hacen pensar que una fracción $\frac{4}{p}$, con p primo, tiene una descomposición de tipo I si y sólo si tiene una descomposición de tipo II. Pero no se sabe aún si esto es cierto, este problema está también abierto.

Haciendo $\beta = \gamma = 1$ en (16), se sigue que si $n + 4$ tiene un divisor congruente con 3 (mód 4) entonces la fracción $\frac{4}{n}$ se puede expresar como suma de tres fracciones unitarias. Equivalentemente, si $\frac{4}{n}$ no se puede expresar como suma de tres fracciones unitarias, entonces $n + 4$ no tiene ningún divisor congruente con 3 (mód 4) y por consiguiente, como es bien conocido, es expresable como suma de dos cuadrados. Luego la cantidad de números $n \leq N$ para los que (1) no tiene solución es a lo sumo igual a la de números $m \leq N + 4$ que se pueden expresar como suma de dos cuadrados. Por otra parte, por un teorema debido a E. Landau (Landau 1908, p. 305–312; Hardy 1940, p. 9–10, 55, 60–64), la densidad[8] del conjunto de los números n para los que (1) no tiene solución es 0. Una estimación más precisa de la densidad del conjunto de números n para los que (1) tiene solución se puede ver en (Vaughan 1970).

Definición 3.3. *Decimos que* un sistema finito de congruencias $a_i \pmod{n_i}$, $(1 \leq i \leq N)$ cubre el conjunto $A \subseteq \mathbb{N}$ *cuando todo* $x \in A$ *verifica* $x \equiv a_i \pmod{n_i}$ *para al menos un valor de* i. *Cuando* $A = \mathbb{N}$, *el sistema de congruencias se llama un* sistema completo de restos[9].

Adelantando una situación que se va a plantear a continuación, supongamos que en la ecuación (8), en la que n representa un número primo, fijamos los valores de tres de los cuatro parámetros a, b, c, d, por ejemplo $a = b = 1$, $d = 2$, y dejamos libre (recorriendo $\mathbb{N}$) el valor del otro, c en este caso. La ecuación $(4c-1)2 = n+1$ nos proporciona en particular una congruencia que deberá ser satisfecha por n necesariamente: $n \equiv -3 \pmod{8}$. A veces no se concluirá una congruencia, sino sólo un conjunto finito de valores posibles de n; por ejemplo, si en la ecuación (7) se toman $b = 1$, $c = 2$, $d = 3$ dejando libre a, resulta $3(8a - 1) = (a + 1)n$. Considerando que $n \neq 3$ ha de ser primo y poniendo entonces $a + 1 = 3e$, resulta $en = 24e - 9$, de donde se sigue que $e|9$, lo que da los siguientes valores posibles para n: 15, 21, 23, de los que sólo este último es primo.

K. Yamamoto (Yamamoto 1965; ver también los resultados de A. Schinzel en Schinzel 2000) prueba que para un cuadrado perfecto n no se satisface ni (7) ni (8) con alguna restricción en los parámetros (ver más adelante el comienzo de la sección 3.2), de modo que fijando parámetros en esas dos ecuaciones no podemos

8. Si $A \subset \mathbb{N}$ y $\delta_n = |\{k \in A : k \leq n\}|$, la *densidad* de A es el valor $\lim_{n\to\infty} \frac{\delta_n}{n}$ cuando este límite existe.

9. O *covering system*, ver (Guy 1994, p. 251).

Zubía | núm. 37-38 (2019-2020), pp. 149-176
ISSN 0213-4306

obtener un sistema completo de restos. El siguiente teorema pone el énfasis en esto sin utilizar el resultado de Yamamoto. Probamos en él que no se puede cerrar CES argumentando con sistemas finitos de congruencias obtenidos a partir de las relaciones (7) u (8) fijando que tres de los cuatro parámetros *a, b, c, d* que aparecen en ellas tomen valores en correspondientes subconjuntos finitos de $\mathbb{N}^3$ y dejando el otro parámetro libre. De hecho, los números primos de la forma $n = 4q + 1$ no se van a poder cubrir.

Teorema 3.4. *Sean S_1, S_2, S_3 y S_4 subconjuntos finitos de $\mathbb{N}^3$. Cada uno de los conjuntos*

$$\begin{aligned}
\mathcal{F}_1 &:= \{n \text{ primo} : \ n \text{ verifica } (7) \text{ u } (8) \text{ con } a \in \mathbb{N}, (b, c, d) \in S_1\},\\
\mathcal{F}_2 &:= \{n \text{ primo} : \ n \text{ verifica } (7) \text{ u } (8) \text{ con } b \in \mathbb{N}, (a, c, d) \in S_2\},\\
\mathcal{F}_3 &:= \{n \text{ primo} : \ n \text{ verifica } (7) \text{ u } (8) \text{ con } c \in \mathbb{N}, (a, b, d) \in S_3\},\\
\mathcal{F}_4 &:= \{n \text{ primo} : \ n \text{ verifica } (7) \text{ u } (8) \text{ con } d \in \mathbb{N}, (a, b, c) \in S_4\}
\end{aligned}$$

es, en general, la unión de un conjunto finito y del conjunto cubierto por un cierto sistema finito de congruencias. Pero la unión $\bigcup_{i=1}^{4} \mathcal{F}_i$ no cubre el conjunto de los números primos de la forma $n = 4q + 1$.

Demostración. En primer lugar, los parámetros (a, b, c, d) asociados a un número n que satisface (8) son tales que a divide a $b + d$. De modo que cuando (b, c, d) recorre el conjunto finito S_1, el parámetro a queda restringido a poder tomar sólo un número finito de valores también, y eso deja sólo un número finito de valores posibles para n.

En segundo lugar, los números n generados por (8) cuando $(a, b, d) \in S_3$ están dados por

$$n = 4bcd - \frac{b + d}{a}. \tag{17}$$

Sea $T_3 := \text{mcm}\{bd : (a, b, d) \in S_3\}$; veamos que los números n del conjunto $\{4T_3t + 1 : t \in \mathbb{N}\}$ no se pueden obtener en la relación (17) cuando $(a, b, d) \in S_3$ y c queda libre. De lo contrario existirían $(a_0, b_0, d_0) \in S_3$ y $t_0, c_0 \in \mathbb{N}$ tales que

$$4T_3t_0 + 1 = 4b_0c_0d_0 - \frac{b_0 + d_0}{a_0}$$

o, equivalentemente,

$$1 = 4b_0d_0(c_0 - e_0) - \frac{b_0 + d_0}{a_0},$$

Zubía | núm. 37-38 (2019-2020), pp. 149-176
ISSN 0213-4306

donde $e_0 \in \mathbb{N}$; lo que es imposible, porque de aquí se sigue

$$4 = \frac{1}{b_0 d_0 (c_0 - e_0)} + \frac{1}{a_0 d_0 (c_0 - e_0)} + \frac{1}{a_0 b_0 (c_0 - e_0)}.$$

Por otra parte, si $T_4 := \operatorname{mcm}\{(4abc - 1) : (a, b, c) \in S_d\}$, los números del conjunto $\{4T_4 t + 1 : t \in \mathbb{N}\}$ no se pueden obtener como valores de n en la relación (8) cuando $(a, b, c) \in S_4$ y d queda libre. De lo contrario existirían $(a_0, b_0, c_0) \in S_4$ y $t_0, d_0 \in \mathbb{N}$ tales que

$$a_0(4T_4 d_0 t_0 + 1) + b_0 = (4a_0 b_0 c_0 - 1)d_0$$

y, según el Lema 3.2, existirían números naturales $\alpha_0, \beta_0, \gamma_0$ y δ_0 tales que

$$4T_4 t_0 + 1 = (4\alpha_0 \beta_0 \gamma_0 - 1)\delta_0 - 4\beta_0^2 \gamma_0$$

o, equivalentemente,

$$1 = (4a_0 b_0 c_0 - 1)(\delta_0 - 4e_0) - 4b_0^2 c_0,$$

con $e_0 \in \mathbb{N}$. Y de nuevo esto es imposible porque se sigue

$$4 = \frac{1}{b_0 c_0 (a_0(\delta_0 - 4e_0) - b_0)} + \frac{1}{a_0 b_0 c_0} + \frac{1}{a_0 c_0 (a_0(\delta_0 - 4e_0) - b_0)},$$

absurdo. Por la simetría de la ecuación (8) en los parámetros b y d, se concluye de la misma manera que, si $T_4 := \operatorname{mcm}\{(4abc - 1) : (a, b, c) \in S_4\}$, los números del conjunto $\{4T_4 t + 1 : t \in \mathbb{N}\}$ no se pueden obtener como valores de n en la relación (8) cuando $(a, b, c) \in S_4$ y d queda libre.

Con análogos argumentos tenemos, en primer lugar, que el conjunto de los números n que se pueden representar por (7) con $(b, c, d) \in S_1$ o con $(a, c, d) \in S_2$ (la ecuación es simétrica en a y b) es finito: siguiendo la demostración de (15) en el Lema 3.2, el número $e = \frac{a+b}{d}$ divide a $1 + 4a^2 c$, de modo que si (a, c, d) toma valores en un conjunto finito, también están en un conjunto finito los posibles divisores de los números $1 + 4a^2 c$.

Y en segundo lugar tenemos que si $T_3' := \operatorname{mcm}\{abd : (a, b, d) \in S_3\}$ y $T_4' := \operatorname{mcm}\{(4abc - 1) : (a, b, c) \in S_4\}$, entonces los números n en las progresiones $\{4T_3' t : t \in \mathbb{N}\}$ o $\{4T_4' t : t \in \mathbb{N}\}$ no se pueden obtener como valores de n en (7) para $(a, b, d) \in S_3$ o $(a, b, c) \in S_4$, respectivamente. Pues suponiendo, por reducción al absurdo, que para un $t_0 \in \mathbb{N}$ dado existen $(a_0, b_0, d_0) \in S_3$ y $c_0 \in \mathbb{N}$ tales que

$$(a_0 + b_0)(4T_3' t_0 + 1) = (4a_0 b_0 c_0 - 1)d_0,$$

resulta que equivalentemente se tiene

$$1 + \frac{a_0 + b_0}{d_0} = 4a_0b_0(c_0 - e_0),$$

donde $e_0 = \frac{(a_0+b_0)T_3't_0}{a_0b_0d_0}$, de donde se sigue nuevamente una imposibilidad.

En conclusión, los números n del conjunto

$$\{4T_2T_3T_4T_3'T_4't + 1 : t \in \mathbb{N}\},$$

para todo t suficientemente grande, no se pueden representar como (7) u (8) con tres de los cuatro parámetros en los correspondientes conjuntos S_1, S_2, S_3 y S_4. Según el teorema de Dirichlet de las progresiones aritméticas[10], tendríamos así infinitos números primos $n = 4q + 1$ para los que las ecuaciones (7) o (8) no tendrían solución bajo las condiciones enunciadas. □

3.1. Sobre descomposiciones de tipo I. Conjetura *q*

En muchos artículos sobre CES se estudia la posibilidad de descomposiciones como (10), *de tipo II*, porque en ese caso es más fácil obtener soluciones parametrizadas de (1). Por nuestra parte, el siguiente lema nos permite obtener una representación paramétrica de los números n para los cuales la fracción $\frac{4}{n}$ admite una descomposición *de tipo I*, como (9).

Lema 3.5. *Sea $n \in \mathbb{N}$. Existen $a, b, c, d \in \mathbb{N}$ tales que se cumple* (7) *si y sólo si se pueden encontrar $x, t, \lambda \in \mathbb{N}$ tales que*

$$\frac{x\,n + t}{\lambda} \in \mathbb{N} \quad \text{y} \quad \frac{n + \lambda}{4\,x\,t} \in \mathbb{N}. \tag{18}$$

Demostración. Supongamos que existen naturales x, t, λ, y, z tales que

$$\frac{x\,n + t}{\lambda} = y \quad \text{y} \quad \frac{n + \lambda}{4\,x\,t} = z.$$

Equivalentemente se cumplen

$$x\,n + t = y\,\lambda \quad \text{y} \quad \lambda = 4\,z\,x\,t - n,$$

o bien,

$$(x + y)n = (4\,x\,y\,z - 1)t.$$

Es decir, $(4abc - 1)d = (a + b)n$, si ponemos $x = a, y = b, z = c$ y $t = d$. □

10. P. G. Lejeune Dirichlet probó en 1837 el siguiente resultado: Si $(a, d) = 1$, entonces la progresión aritmética $a + nd$, $n = 1, 2, \ldots$, contiene infinitos primos.

Zubía | núm. 37-38 (2019-2020), pp. 149-176
ISSN 0213-4306

Observación 3.6. Si para un $n \in \mathbb{N}$ se cumple (18), entonces para el número $N = n + 4xt\lambda j$, donde $j \in \mathbb{N}$ es arbitrario, también se cumple (18). En efecto,

$$\frac{xN+t}{\lambda} = \frac{x(n+4xt\lambda j)+t}{\lambda} = \frac{xn+t}{\lambda} + 4x^2tj \in \mathbb{N},$$

y

$$\frac{N+\lambda}{4xt} = \frac{(n+4xt\lambda j)+\lambda}{4xt} = \frac{n+\lambda}{4xt} + \lambda j \in \mathbb{N}.$$

Y de esto se deduce, en particular, que el conjunto de los valores n para los que la ecuación (1) tiene solución es un abierto de la topología de Furstenberg de $\mathbb{Z}$ (ver Niven *et al.*, p. 34).

El lema anterior permite probar fácilmente el siguiente resultado.

Teorema 3.7. *Para los números $n = p(\alpha, \beta, \gamma)$ de la forma*

$$p(\alpha,\beta,\gamma) = (\alpha+1)(4\beta+3)(4\gamma+3) - (\alpha+1) - (4\beta+3), \tag{19}$$

donde $\alpha, \beta, \gamma \in \mathbb{N} \cup \{0\}$, la ecuación (1) *tiene solución.*

Demostración. Para los valores $n = p(\alpha, \beta, \gamma)$ se cumplen las condiciones (18) con $x = 1$, $t = \alpha + 1$ y $\lambda = 4\beta + 3$. □

De hecho, se puede usar la fórmula más general

$$\frac{4}{abc-a-b} = \frac{1}{a^{\frac{bc-1}{4}}} + \frac{1}{a(ac-1)^{\frac{bc-1}{4}}} + \frac{1}{(ac-1)^{\frac{bc-1}{4}}(abc-a-b)} \tag{20}$$

para tener una descomposición de tipo I de la fracción $\frac{4}{p(\alpha,\beta,\gamma)}$ como suma de tres fracciones unitarias.[11]

Vamos a denotar desde aquí por $\mathcal{N}_1$ el conjunto imagen de $(\mathbb{N} \cup \{0\})^3$ por el polinomio $p(x, y, z) = (x + 1)(4y + 3)(4z + 3) - (x + 1) - (4y + 3)$, es decir,

$$\mathcal{N}_1 = \{n \in \mathbb{Z} : \exists (a, b, c) \in (\mathbb{N} \cup \{0\})^3 \text{ tal que } p(a, b, c) = n\}. \tag{21}$$

Basándonos en una verificación asistida por ordenador para $4q + 5 < 12 \times 10^{15}$ hemos propuesto la siguiente conjetura que implicaría la validez de CES:

11. Por otra parte, si $bc \equiv 1$ (mód m), entonces las conjeturas de Sierpiński y Schinzel se cumplen para $n = abc - a - b$. A. Schinzel conjeturó que, dado $m \in \mathbb{N}$, la ecuación $\frac{m}{n} = \frac{1}{x} + \frac{1}{y} + \frac{1}{z}$ tiene soluciones $x, y, z \in \mathbb{N}$ para todo $n \in \mathbb{N}$, $n \geq n_m$; el caso $m = 5$ había sido considerado antes, y comprobado para $1 < n \leq 10^3$, por W. Sierpiński (Sierpiński 1956). Ver (Erdős 1956).

Conjetura q. *Todos los números primos de la forma* $4q + 5$ $(q \geq 0)$ *pertenecen al conjunto* $\mathcal{N}_1$.

A continuación veremos dos consecuencias del Teorema 3.7. La primera, en línea con la *Conjetura q*, proporciona una nueva condición suficiente para CES. En la segunda probamos que se pueden encontrar tantos números consecutivos como se desee para los que (1) tiene solución.

Proposición 3.8. *Si, para todo* $q \in \mathbb{N}$ *dado, existen x, y, z enteros no negativos tales que se cumple alguna de las siguientes igualdades:*

$$q = 1 + 3x + 3y + 4xy, \tag{22}$$

$$q = 5 + 5x + 5y + 4xy, \tag{23}$$

$$q = \tfrac{1}{4}\big(p(x, y, z) - 5\big) = 2x + 2y + 3z + 3xy + 3xz + 4yz + 4xyz \tag{24}$$

siendo $p(x, y, z)$ *el polinomio* (19)*, entonces CES es cierta.*

Demostración. Si todo $q \in \mathbb{N}$ satisface (22), (23) o (24), como se tiene

$$q = 1 + 3x + 3y + 4xy \iff 4q + 5 = (4x + 3)(4y + 3),$$

$$q = 5 + 5x + 5y + 4xy \iff 4q + 5 = (4(x + 1) + 1)(4(y + 1) + 1),$$

entonces para los números q que admiten una representación como (22) o como (23), los correspondientes números $4q + 5$ son compuestos. Por lo tanto, si q es un número para el cual $4q + 5$ es primo, entonces q se tendrá que representar por (24). De modo que en este caso se va a tener $4q(x, y, z) + 5 = p(x, y, z)$ para ciertos enteros no negativos x, y, z y, aplicando el Teorema 3.7, concluimos que la ecuación (1) tiene solución para $n = 4q + 5$. □

Proposición 3.9. *Hay secuencias arbitrariamente largas de números naturales consecutivos n para los que la ecuación* (1) *tiene solución en enteros positivos.*

Demostración. Bastará probarlo con secuencias de «números consecutivos» de la forma $n \equiv 1 \pmod 4$. Sea $N \in \mathbb{N}$ fijo y $B = \{0, 1, 2, \ldots, N - 1\}$. Si $b_1, b_2 \in B$ y $b_1 \neq b_2$, se tiene que el m.c.d. $(4b_1 + 3, 4b_2 + 3)$ es impar y que

$$(4b_1 + 3, 4b_2 + 3) \big| \big(4b_1 + 3 - (4b_2 + 3)\big) = 4(b_1 - b_2).$$

Por consiguiente,

$$(4b_1 + 3, 4b_2 + 3) \big| 3(b_1 - b_2) = 3b_1 + 2 - (3b_2 + 2).$$

Zubía | núm. 37-38 (2019-2020), pp. 149-176
ISSN 0213-4306

Entonces, se puede aplicar el teorema chino de los restos (Hua 1982, Ch. 2, Thms. 7.1, 7.2) para deducir que existe T tal que

$$T \equiv 3b_j + 2 \pmod{4b_j + 3}, \quad b_j \in B,$$

es decir, existen enteros positivos c_j tales que, para cada $b_j \in B$,

$$T = (4b_j + 3)c_j + 3b_j + 2 = q(0, b_j, c_j) + (b_j + 2),$$

considerando el polinomio $q(x, y, z)$ de (24). Según la Proposición 3.8, la ecuación (1) tiene solución, y además con descomposición de tipo I, para todo $n = 4q + 5$ donde

$$q \equiv -(b_j + 2) \pmod{T}, \quad b_j \in B.$$

En particular, (1) tiene solución para $n = 4Tk - 4(b_j + 2) + 5$, $b_j \in B$, $k \in \mathbb{N}$. Para concluir[12] basta observar que, para $k = 1$, el conjunto $\{4T - 4(b_j + 2) + 5 : b_j \in B\}$ está formado por «números consecutivos» de la forma $4q + 5$. □

3.2. El conjunto $\mathcal{N}_1$ no contiene cuadrados

El conjunto $\mathcal{N}_1$ se ha definido en (21). En la subsección anterior ha quedado probado que para todo $n \in \mathcal{N}_1$ la ecuación (1) tiene solución, y nuestra *Conjetura q* afirma que dicho conjunto contiene a todos los números primos de la forma $4q + 5$ ($q \geq 0$). En esta subsección vamos a probar, en dirección contraria, que el conjunto $\mathcal{N}_1$ no contiene ningún cuadrado perfecto.

Necesitaremos utilizar alguna herramienta especial de la teoría de números: los *símbolos de Jacobi* y *de Legendre*. Sea p un primo impar, y sea $n \in \mathbb{N}$ tal que $(n, p) = 1$; el *símbolo de Legendre de n sobre p* se define así:

$$\left(\frac{n}{p}\right) := \begin{cases} 1, & \text{si } n \text{ es resto cuadrático módulo } p, \\ -1, & \text{si } n \text{ no es resto cuadrático módulo } p. \end{cases}$$

El *símbolo de Jacobi* se define a partir del *símbolo de Legendre* (ver Hua 1982, 3.1, 3.6). Si m es un número impar cuya descomposición en factores primos es $p_1 \cdots p_k$, donde los $p_j > 2$ pueden repetirse, y $n \in \mathbb{N}$ es tal que $(n, m) = 1$, entonces el *símbolo de Jacobi de n sobre m* se define, en términos de símbolos de Legendre, por:

$$\left(\frac{n}{m}\right) := \prod_{j=1}^{k} \left(\frac{n}{p_j}\right).$$

12. De hecho se ha probado más que lo enunciado: existen un número T y N restos consecutivos módulo T, con N tan grande como se quiera, de modo que en el conjunto cubierto por el sistema finito de congruencias generado se cumple CES.

Zubía | núm. 37-38 (2019-2020), pp. 149-176
ISSN 0213-4306

Sean m y m' números naturales impares y n y n' naturales de modo que los símbolos de Jacobi que aparecen a continuación tengan sentido. Las siguientes propiedades del símbolo de Jacobi son bien conocidas:

(i) Si $n \equiv n' \pmod{m}$ y $(n, m) = 1$, entonces $\left(\frac{n}{m}\right) = \left(\frac{n'}{m}\right)$.

(ii) $\left(\frac{n}{m}\right)\left(\frac{n}{m'}\right) = \left(\frac{n}{mm'}\right)$.

(iii) $\left(\frac{n}{m}\right)\left(\frac{n'}{m}\right) = \left(\frac{nn'}{m}\right)$.

(iv) Si $n \equiv 3 \pmod{4}$, entonces $\left(\frac{-1}{n}\right) = -1$.

(v) *Ley de reciprocidad cuadrática para símbolos de Jacobi*. Sean m y n impares primos entre sí. Entonces $\left(\frac{n}{m}\right)\left(\frac{m}{n}\right) = (-1)^{\frac{n-1}{2}\frac{m-1}{2}}$.

(vi) Si $(n, d) = 1$ y m es tal que $n \equiv -m \pmod{d}$, entonces $\left(\frac{d}{n}\right) = \left(\frac{d}{m}\right)$ (Hua 1982, p. 305).

Proposición 3.10. *El conjunto $\mathcal{N}_1$ no contiene cuadrados perfectos.*

Demostración. Sea $n \in \mathcal{N}_1$: existen enteros no negativos x, y, z tales que

$$n + (4y + 3) = (x + 1)\big((4y + 3)(4z + 3) - 1\big) = (x + 1)t,$$

donde $t = (4y+3)(4z+3)-1$ (observar que $t \equiv 0 \pmod{4}$). Como $(t, 4y+3) = 1$, también es $(t, n) = 1$, así como $(n, n + t) = 1$.

Aplicando entonces (v) y dado que $n \equiv 1 \pmod{4}$, se tiene

$$\left(\frac{n}{n+t}\right)\left(\frac{n+t}{n}\right) = (-1)^{\frac{n-1}{2}\frac{n+t-1}{2}} = 1. \tag{25}$$

Por otra parte, $n + t \equiv t \pmod{n}$ implica por (i) que

$$\left(\frac{n+t}{n}\right) = \left(\frac{t}{n}\right). \tag{26}$$

Usando que $n \equiv -(4y + 3) \pmod{t}$ y (vi) se tiene

$$\left(\frac{t}{n}\right) = \left(\frac{t}{4y+3}\right). \tag{27}$$

Pero $t \equiv -1 \pmod{4y + 3}$, así que usando (i) y (iv) obtenemos

$$\left(\frac{t}{4y+3}\right) = \left(\frac{-1}{4y+3}\right) = -1. \tag{28}$$

De (26), (27) y (28) concluimos que $\left(\frac{n+t}{n}\right) = -1$, y entonces de (25) resulta

$$\left(\frac{n}{n+t}\right) = -1,$$

de modo que n no puede ser un cuadrado perfecto, ya que si $(a, b) = 1$, el símbolo de Jacobi (a^2/b) es igual a 1. □

Zubía | núm. 37-38 (2019-2020), pp. 149-176
ISSN 0213-4306

Observación 3.11. En (Yamamoto 1965), usando el símbolo de Kronecker[13], Yamamoto observa que los números naturales n que cumplen $(4abc-1)d = (a+b)n$ para a, b, c, d naturales y $(n, abd) = 1$, no son cuadrados perfectos. Pero el conjunto $\mathcal{N}_1$ contiene números n que no se incluyen en esta *clase de Yamamoto*. Es el caso, por ejemplo, del número $n = 2009$. Se tiene

$$2009 = 42 \cdot 7 \cdot 7 - 42 - 7 = p(41, 1, 1),$$

luego $2009 \in \mathcal{N}_1$, pero no pertenece a la clase de Yamamoto, ya que

$$2009(1 + 293) = (4 \cdot 1 \cdot 293 - 1)42 \quad \text{y} \quad (2009, 293 \cdot 42) = 7.$$

4. UN ALGORITMO DE TIPO *GREEDY* PARA CES

En esta sección describimos y analizamos el comportamiento de un algoritmo sencillo, que denominamos *algoritmo greedy para CES* que, tras recibir la entrada de un número natural n, en caso de parada devuelve una descomposición de la fracción $\frac{4}{n}$ como suma de dos o tres fracciones egipcias[14]. Utilizándolo, en sesiones de cálculo asistido por ordenador hemos llegado a verificar CES para todos los números primos $n \leq 10^{12}$.

En la Figura 1 mostramos un esquema de la secuencia de instrucciones de este algoritmo.

En el Paso 2 del algoritmo, para cada $j = 1, 2, \ldots$, después de fijar de una manera muy obvia x_j y hallar la diferencia $\delta_j = \frac{4}{n} - \frac{1}{x_j}$, se determina la fracción unitaria $\frac{1}{y_j}$ más próxima menor o igual que δ_j. Entra entonces el Paso 3: si la fracción δ_j es ya unitaria el algoritmo se detiene; si no, el algoritmo abre un bucle en el que busca, y de ahí el nombre que le damos, la descomposición *greedy* de δ_j como suma de dos fracciones unitarias. De hecho, si $r_j \equiv -nx_j \pmod{4j-1}$ con $r_j \in [1, 4j-2]$, entonces

$$\delta_j = \frac{4x_j - n}{nx_j} = \frac{4j-1}{nx_j} = \frac{1}{y_j} + \frac{r_j}{nx_jy_j}.$$

13. El símbolo de Kronecker se define en términos del símbolo de Jacobi. El símbolo de Kronecker (m/n) coincide con el correspondiente símbolo de Jacobi cuando n es un número impar positivo, cosa que ciertamente nosotros hemos usado para escribir la propiedad (vi) del símbolo de Jacobi. Remitimos al lector interesado a (Hua 1982, 12.3) o (Montgomery y Vaughan 2007, p. 296).

14. En los casos $n = 4k$ y $n = 4k + 2$ el algoritmo no proporciona las descomposiciones más inmediatas. Por ejemplo, para $n = 8$ nos devuelve $\frac{4}{8} = \frac{1}{3} + \frac{1}{6}$, y para $n = 10$ nos devolverá $\frac{4}{10} = \frac{1}{3} + \frac{1}{15}$.

Zubía | núm. 37-38 (2019-2020), pp. 149-176
ISSN 0213-4306

Entrada: Un número natural $n \geq 2$

Paso 1: Sean $j := 1$ y $q := \lfloor \frac{n}{4} \rfloor$ (la parte entera de $\frac{n}{4}$)

Paso 2: Sean $x_j := q + j$, $\delta_j := \frac{4}{n} - \frac{1}{x_j}$ e $y_j := \lceil \frac{1}{\delta_j} \rceil = 1 + \lfloor \frac{x_j n}{4j-1} \rfloor$

Paso 3:

si $\frac{4}{n} - \frac{1}{x_j} - \frac{1}{y_j} = 0$ **entonces**

  Resultado: $\boxed{\frac{4}{n} = \frac{1}{x_j} + \frac{1}{y_j}}$ y **Fin.**

en otro caso

  si $z_j = \frac{1}{\frac{4}{n} - \frac{1}{x_j} - \frac{1}{y_j}} \in \mathbb{Z}$ **entonces**

    Resultado: $\boxed{\frac{4}{n} = \frac{1}{x_j} + \frac{1}{y_j} + \frac{1}{z_j}}$ y **Fin.**

  en otro caso

    incrementar el índice $j \longleftarrow j + 1$ y volver al **Paso 2**

Figura 1. Algoritmo *greedy* para CES.

El algoritmo se detendrá si, para algún j, r_j divide a nx_jy_j, y entonces el denominador de la tercera fracción unitaria será $z_j = \frac{nx_jy_j}{r_j}$.

Por ejemplo, en el caso $n = 97$, el resultado final es

$$\frac{4}{97} = \frac{1}{28} + \frac{1}{182} + \frac{1}{35308},$$

y el algoritmo se detiene después de dejar el siguiente rastro de valores sucesivos de las variables internas:

j	q	x_j	δ_j	y_j	z_j
1	24	25	3/2425	809	1961825/2
2	24	26	7/2522	361	910442/5
3	24	27	11/2619	239	625941/10
4	24	**28**	15/2716	**182**	**35308**

En el caso $n = 7969$ el índice j llega a tomar el valor 10, y el algoritmo se

Zubía | núm. 37-38 (2019-2020), pp. 149-176
ISSN 0213-4306

detiene (diremos que *en* 10 *pasos*) mostrando la descomposición

$$\frac{4}{7969} = \frac{1}{2002} + \frac{1}{409076} + \frac{1}{251014351588}.$$

Vamos a ver a continuación que, cuando $n = p(x, y, z)$, donde p es el polinomio definido anteriormente en (19), el algoritmo *greedy* aplicado al número n siempre se va a detener. Por claridad de exposición vamos a aislar previamente de la prueba de este resultado un pequeño detalle técnico.

Lema 4.1. *Sean $x, y \in \mathbb{N}$ con $x \leq y$. De las fracciones unitarias que son menores que la suma $s = \frac{1}{x} + \frac{1}{y}$, la fracción $1/x$ es la más próxima a s si y sólo si $x(x-1) \leq y$.*

Demostración. La fracción $1/x$ será la más próxima a s de todas las fracciones unitarias que quedan por debajo de ese valor si y sólo si $s < \frac{1}{x-1}$, con lo que la condición enunciada equivale a que sea

$$\left\lfloor \frac{xy}{x+y} \right\rfloor = x - 1,$$

lo que equivale a su vez a las desigualdades

$$x - 1 \leq \frac{xy}{x+y} < x,$$

equivalentes a la desigualdad única

$$x(x-1) \leq y. \qquad \square$$

Proposición 4.2. *El algoritmo* greedy *siempre se detiene para $n = p(x, y, z)$, siendo x, y, z números enteros no negativos y $p(x, y, z)$ el polinomio*

$$p(x, y, z) := (x+1)(4y+3)(4z+3) - (4y+3) - (x+1).$$

Demostración. Si $n = p(x, y, z)$, poniendo $a = x + 1$, $b = 4y + 3$ y $c = 4z + 3$ y usando (20) obtenemos una descomposición de tipo I de la fracción $4/n$. Por otra parte, para los denominadores de esta descomposición se verifica

$$a\frac{bc-1}{4} < a(ac-1)\frac{bc-1}{4} < (ac-1)\frac{bc-1}{4}n$$

ya que, como $a = x + 1 \geq 1$ y $c = 4z + 3 \geq 3$, se tiene $ac - 1 \geq 2a$, lo que da la primera desigualdad; y para obtener la segunda podemos considerar que $n = abc - a - b \geq a$, que equivale a $b(ac - 1) \geq 2a$.

Según el Lema 4.1, para comprobar que el algoritmo *greedy* aplicado a $4/n$ se detiene, basta demostrar que

$$a\frac{bc-1}{4}\Big(a\frac{bc-1}{4}-1\Big)\leq (ac-1)\frac{bc-1}{4}\,n$$

o, equivalentemente, que

$$a\Big(a\frac{bc-1}{4}-1\Big)\leq (ac-1)(abc-a-b).$$

Y esta última desigualdad se puede probar observando que las expresiones $r_1(b) := ba^2c/4 - a^2/4 - a$ y $r_2(b) := (ac-1)^2b - a(ac-1)$ son funciones lineales de b cuyas pendientes cumplen $r_1'(b) = a^2c/4 \leq (ac-1)^2 = r_2'(b)$, ya que $a \leq ac-1$ y $ac/4 \leq ac-1$, y que además sus valores para $b = 1$ son

$$r_1(1) = a\Big(a\frac{c-1}{4}-1\Big)\leq r_2(1) = (ac-1)\big((ac-1)-a\big),$$

ya que $a < ac-1$ y $\big(a(c-1)/4-1\big) < \big(a(c-1)-1\big) = ac-a-1$. □

El siguiente resultado caracteriza la detención del algoritmo *greedy*.

Proposición 4.3. *Sean $n = 4q+1$ y j números naturales. Sean $s = s(q,j)$ y $r = r(q,j)$ tales que $(4q+1)(q+j) = s(4j-1)+r$, $0 \leq r \leq 4j-2$.*

(i) *El algoritmo* greedy *se detiene en a lo sumo j pasos para $n = 4q+1$ si y sólo si*

$$(4j-1) - r \text{ divide a } (4q+1)(q+j)(s+1). \tag{29}$$

(ii) *Si $(r, 4j-1) = 1$, la condición* (29) *es equivalente a*

$$(4j-1) - r \text{ divide a } (4q+1)^2(q+j)^2.$$

(iii) *Si $4q+1$ es primo y $4j-1 < 4q+1$, entonces una condición necesaria y suficiente para que el algoritmo* greedy *se detenga es que* $(4j-1) - r$ *divida a* $(q+j)^2$.

Demostración. (i) El algoritmo *greedy* se detiene en a lo sumo j pasos para $n = 4q+1$ si y sólo si existen $r, s, t \in \mathbb{N}$ tales que $0 \leq r \leq 4j-2$ y

$$\frac{4}{4q+1} - \frac{1}{q+j} = \frac{4j-1}{(4q+1)(q+j)} = \frac{4j-1}{s(4j-1)+r} = \frac{1}{s+1} + \frac{1}{t},$$

Zubía | núm. 37-38 (2019-2020), pp. 149-176
ISSN 0213-4306

lo que es equivalente a que

$$\frac{4j-1-r}{(4q+1)(q+j)(s+1)} = \frac{1}{t},$$

o sea, a que $4j-1-r$ divida a $(4q+1)(q+j)(s+1)$, que es la condición (29).

(ii) Observemos que

$$(4q+1)(q+j) = s(4j-1)+r = (s+1)(4j-1)+r-(4j-1),$$

igualdad equivalente, multiplicando ambos lados por $(4q+1)(q+j)$, a

$$(4q+1)^2(q+j)^2 = (s+1)(4q+1)(q+j)(4j-1) + \big(r-(4j-1)\big)(4q+1)(q+j)$$

Si $(r, 4j-1) = (4j-1-r, 4j-1) = 1$, entonces $\big(r-(4j-1)\big)$ divide a $(s+1)(4q+1)(q+j)$ si y sólo si divide a $(4q+1)^2(q+j)^2$.

(iii) Si $4q+1$ es primo y $4j-1 < 4q+1$, entonces de la relación

$$(4q+1)(q+j+1) = (4j-1)s + r,$$

equivalente a

$$(4q+1)(4q+1+4j-1) = 4(4j-1)s + 4r,$$

se sigue que $(4j-1, r) = 1$. Para concluir basta aplicar (ii). □

Hasta la cota alcanzada en los experimentos numéricos que hemos realizado, el algoritmo *greedy* se detiene para todos los números naturales, lo que incluye en particular a los cuadrados perfectos, que no están en $\mathcal{N}_1$ como se ha visto. Pero la detención del algoritmo cuando se aplica a un cierto n de entrada puede requerir muchos pasos, como se prueba en el siguiente resultado.

PROPOSICIÓN 4.4. *Dado $m \in \mathbb{N}$ existe $n \in \mathbb{N}$ tal que el algoritmo* greedy *para CES, aplicado al número n, no se detiene antes de m pasos.*

DEMOSTRACIÓN. Sean $m \geq 3$ un número natural y n el mínimo común múltiplo de $4j-1$ y $3j-1$, con j recorriendo los números desde 1 hasta m. Entonces para cada $j = 1, 2, \ldots, n$ existe $s = s(n, j) \in \mathbb{N}$ tal que

$$(n+1)(n/4+j) = s(4j-1) + j,$$

y

$$4j-1-j = 3j-1 \quad \text{no divide a} \quad (n+1)^2(n/4+j)^2.$$

Por lo tanto, según la caracterización dada en la Proposición 4.3 (ii), el algoritmo *greedy* aplicado a $(n+1)$ se detiene, si lo hace, en más de m pasos. □

Zubía | núm. 37-38 (2019-2020), pp. 149-176
ISSN 0213-4306

AGRADECIMIENTOS

Los autores deseamos agradecer en primer lugar la gran ayuda recibida de nuestros colegas del Departamento de Matemáticas y Computación de la Universidad de La Rioja Jónathan Heras Vicente, José Antonio Martínez Muñoz y Juan Luis Varona Malumbres, que nos permitieron usar hasta sus propias computadoras (en los años 2008–2012, cuando preparábamos el artículo Bello-Hernández *et al.* 2012) para llevar a cabo la ejecución de muchos de los programas que constituyeron el soporte empírico básico que permitió avanzar en la elaboración del trabajo que se presenta aquí.

En segundo lugar agradecemos al Instituto de Estudios Riojanos la oportunidad que nos ha brindado para ver este artículo publicado en *Zubía*, y a los revisores por su lectura tan minuciosamente atenta; tanto sus correcciones como sus pertinentes sugerencias han permitido mejorar ostensiblemente la versión final.

BIBLIOGRAFÍA

Babai, L. (1996) In and out of Hungary: Paul Erdős, his friends and times. En *Combinatorics: Paul Erdős is Eighty* (Vol. 2), Bolyai Soc. Math. Stud., 7–95.

Bello-Hernández, M., Benito, M. y Fernández, E. (2012) On egyptian fractions (preprint). `arXiv:1010.2035v2 [math.NT] 30 Apr 2012`.

Bernstein, L. (1962) Zur Lösung der diophantischen Gleichung $\frac{m}{n}$, insbesondere im Fall $m = 4$. *J. Reine Angew. Math.* **211**, 1–10.

Cantor, D., Gordon, B., Hales, A. y Schacher, M. (1985) Ernst G. Straus, 1922–1983. *Pacific J. Math.* **118** No. 2, i–xx.

Croot III, E. S., Dobbs, D. E., Friedlander, J. B., Hetzel, A. J. y Pappalardi, F. (2000) Binary Egyptian fractions. *J. Number Theory* **84**, 63–79.

Elsholtz, C. y Tao, T. (2013) Counting the number of solutions to the Erdős-Straus equation on unit fractions. *J. Aust. Math. Soc.* **94**, 50–105.

Erdős, P. (1950) Az $\frac{1}{x_1} + \frac{1}{x_2} + \ldots + \frac{1}{x_n} = \frac{a}{b}$ egyenlet egész számú megoldásairol. *Mat. Lapok* **1**, 192–210.

Erdős, P. (1956) Recensión de (Sierpiński 1956). *MathSciNet*, Mathematical Reviews on the Web, MR0078385 (17,1185d).

Fraleigh, J. B. y Katz, V. J. (2003) *A First Course in Abstract Algebra*, Seventh Edition. Addison-Wesley.

Guy, R. K. (1994) *Unsolved Problems in Number Theory*, Second edition. Springer-Verlag.

Hardy, G. H. (1940) *Ramanujan: Twelve Lectures on Subjects Suggested by his Life and Work*. Cambridge Univ. Press.

Hua, L. (1982) *Introduction to Number Theory*. Springer.

Huang, J. y Vaughan, R. C. (2011) Mean value theorems for binary Egyptian fractions. *J. Number Theory* **131**, 1641–1656.

Landau, E. (1908) Über die Einteilung der positiven ganzen Zahlen in vier Klassen nach der Mindestzahl der zu ihrer additiven Zusammensetzung erforderlichen Quadrate. *Arch. Math. Phys.* (3) **13**, 305–312.

Montgomery, H. L. y Vaughan, R. C. (2007) *Multiplicative number theory I. Classical theory*. Cambridge Tracts in Advanced Mathematics 97, Cambridge Univ. Press.

Mordell, L. J. (1969) *Diophantine Equations*. Academic Press.

Nešetřil, J. (2000) Paul Erdős: El arte de conjeturar y demostrar. En A. Martinón, ed-coord., *Las matemáticas del siglo XX. Una mirada en 101 artículos*, Sociedad Canaria *Isaac Newton* de Profesores de Matemáticas y Nivola libros y ediciones S. L., no. 92, 449–454.

Niven, I., Zuckerman, H. S. y Montgomery, H. L. (1991) *An Introduction to Theory of Numbers*, Fifth Edition. John Wiley & Sons.

Schinzel, A. (2000) On sums of three unit fractions with polynomial denominators. *Funct. Approx. Comment. Math.* **28**, 187–194.

Sierpiński, W. (1956) Sur les décompositions de nombres rationnels en fractions primaires. *Mathesis* **65**, 16–32.

Vaughan, R. C. (1970) On a problem of Erdős, Straus, and Schinzel. *Mathematika* **17**, 193–198.

Yamamoto, K. (1965) On the diophantine equation $\frac{4}{n} = \frac{1}{x} + \frac{1}{y} + \frac{1}{z}$. *Mem Fac. Sci. Kyushu Univ. Ser. A* **19**, 37–47.