TESIS DOCTORAL

Algunos problemas diofánticos

Manuel Benito Muñoz

UNIVERSIDAD DE LA RIOJA

TESIS DOCTORAL

Algunos problemas diofánticos

Manuel Benito Muñoz

Universidad de La Rioja
Servicio de Publicaciones
2004

Esta tesis doctoral, dirigida por el doctor D. Juan Luis Varona Malumbres, fue leida el 31 de mayo de 2002, y obtuvo la calificación de Sobresaliente Cum Laude Unanimidad.

Edita: Universidad de La Rioja
Servicio de Publicaciones

ISBN 84-688-6946-5

UNIVERSIDAD DE LA RIOJA
Departamento de Matemáticas y Computación

Algunos problemas diofánticos

Manuel Benito Muñoz

Memoria presentada para optar al grado de
Doctor en Ciencias Matemáticas

Dirigida por el
Dr. D. Juan Luis Varona Malumbres

Logroño, 2002

Durante el curso 2000-2001 disfruté de una licencia por estudios concedida por la Consejería de Educación, Cultura, Juventud y Deportes del Gobierno de La Rioja.

UNIVERSIDAD DE LA RIOJA
Departamento de Matemáticas y Computación

TESIS DOCTORAL

Autor: Manuel Benito Muñoz
Título: Algunos problemas diofánticos
Director: Dr. Juan Luis Varona Malumbres

TRIBUNAL

Presidente:
Dr. José Ignacio Extremiana Aldana, Profesor Titular de Geometría y Topología, Universidad de La Rioja.

Vocales:
Dr. Luis Manuel Navas Vicente, Profesor Titular de Análisis Matemático, Universidad de Salamanca.
Dr. Francisco Luquín Martínez, Profesor Titular de Análisis Matemático, Universidad del País Vasco.
Dr. Mario Pérez Riera, Profesor Titular de Análisis Matemático, Universidad de Zaragoza.

Secretario:
Julio Jesús Rubio García, Profesor Titular de Ciencias de la Computación e Inteligencia Artificial, Universidad de La Rioja.

Se efectuó la defensa de la Tesis el día 31 de mayo de 2002, obteniendo, por unanimidad, la calificación de SOBRESALIENTE "CUM LAUDE".

Índice general

Índice de figuras

Índice de tablas

Capítulo 1

Introducción. Dos breves notas históricas

El objetivo de esta tesis es el estudio de algunos problemas diofánticos. Unos relacionados con ternas pitagóricas, y otros con funciones aritméticas.

En concreto se empieza, en el capítulo 1, por dos breves notas históricas sobre la aritmética de Diofanto y la tablilla Plimpton 322, para seguir en el capítulo 2 con el estudio del número de ternas pitagóricas de catetos menores que n. Parte de este capítulo está recogido en el artículo *Pythagorean triangles with legs less than n*, que ha sido aceptado para su publicación en el **Journal of Computational and Applied Mathematics** [7].

En el capítulo 3 estudiamos la función $M(n) = \sum_{m=1}^{n} \mu(m)$. Sobre ella Mertens conjeturó que $M(x) < \sqrt{x}$. Odlyzco y te Riele en [35] demostraron que la conjetura es falsa, pero sin dar un contraejemplo explícito. Uno de los actuales retos computacionales es encontrar un contraejemplo explícito de la conjetura de Mertens. Odlyzco y te Riele pronosticaron que no existe un contraejemplo para valores de x menores que 10^{20}.

En el capítulo 4, basándonos en una de las fórmulas recurrentes establecidas en el capítulo 3, definimos funciones parecidas a las μ, M y φ que, en vez de tomar valores enteros, toman valores enteros gaussianos. Para estas nuevas funciones establecemos diversas fórmulas recurrentes y acotaciones.

El capítulo 5 recoge parte del trabajo que venimos realizando, desde hace siete años, en el estudio de las sucesiones alicuatorias. En el artículo *Advances in aliquot sequences*, publicado en el volumen 68, número 225, Enero de 1999, de la revista **Mathematics of Computation** [4], informábamos de los avances que habíamos conseguido hasta Junio de 1997. Los sucesivos avances que hemos ido realizando se han reflejado en [5] y [6]. A este respecto, el resultado más llamativo que hemos logrado es constatar que la sucesión alicuatoria correspondiente al número 3630 termina en 1 después

de alcanzar un número de 100 cifras. Este resultado aparecerá publicado en **Experimental Mathematics** [3].

1.1. Ternas pitagóricas en la aritmética de Diofanto

A una terna de números naturales no nulos (a, b, c) que satisface la ecuación $a^2+b^2 = c^2$ la llamamos una terna pitagórica. El correspondiente triángulo rectángulo de catetos a, b e hipotenusa c se llama triángulo pitagórico. Si además $\mathrm{mcd}(a, b, c) = 1$, decimos que la terna pitagórica es primitiva.

El problema número ocho del libro II de la aritmética de Diofanto de Alejandría dice:

"Descomponer un cuadrado dado en dos cuadrados."

Y lo resuelve de la siguiente manera:

Si queremos descomponer el número 16 en dos cuadrados y suponemos que el primero es el cuadrado de un aritmo, el otro tendrá 16 unidades menos un cuadrado de aritmo, y por tanto 16 unidades menos un cuadrado de aritmo, son un cuadrado.

Formamos el cuadrado de un conjunto cualquiera de aritmos disminuidos en tantas unidades como tiene la raíz de 16 unidades, y sea el cuadrado de 2 aritmos menos 4 unidades.

Este cuadrado tendrá, pues, 4 cuadrados de aritmo y 16 unidades menos 16 aritmos. Lo igualamos a 16 unidades menos un cuadrado de aritmo, y, sumando a uno y otro lado los términos negativos y restando los semejantes, resulta que 5 cuadrados de aritmo equivalen a 16 aritmos, y por tanto un aritmo vale $\frac{16}{5}$; luego uno de los números es $\frac{256}{25}$ y el otro $\frac{144}{25}$, números cuya suma es $\frac{400}{25}$, es decir, 16 unidades, y cada uno de ellos es un cuadrado.

$$16 = x^2 + (16 - x^2)$$
$$16 - x^2 = \square$$
$$\square = (2x-4)^2 = 4x^2+16-16x$$
$$4x^2 + 16 - 16x = 16 - x^2$$
$$5x^2 = 16x$$
$$x = \frac{16}{5}$$
$$16 = \frac{256}{25} + \frac{144}{25}$$
$$= \left(\frac{16}{5}\right)^2 + \left(\frac{12}{5}\right)^2$$

En resumen, lo que Diofanto hace es identificar $16-x^2$ con una expresión del tipo $(mx - \sqrt{16})^2$, en el caso $m = 2$.

En general se trata de hacer

$$\begin{aligned} n^2 &= x^2 + y^2\,, \\ n^2 - x^2 &= (mx - n)^2\,, \\ n^2 - x^2 &= m^2x^2 - 2mnx + n^2 \\ (m^2+1)x^2 &= 2mnx\,, \\ x &= \frac{2mn}{m^2+1}\,, \\ y^2 &= n^2 - \frac{4m^2n^2}{(m^2+1)^2} = n^2\,\frac{m^4+2m^2+1-4m^2}{(m^2+1)^2}\,, \\ y &= n\frac{m^2-1}{m^2+1}\,, \end{aligned}$$

obteniéndose la terna

$$\left(\frac{2mn}{m^2+1}, \frac{(m^2-1)n}{m^2+1}, n\right)\,,$$

que dividiendo por n y multiplicando por m^2+1 nos da

$$\left(2m, m^2-1, m^2+1\right)\,.$$

Si m es natural, es la parametrización atribuida a Platón.

Si m es racional, $m = \frac{p}{q}$, se tiene

$$\left(2\frac{p}{q}, \frac{p^2}{q^2} - 1, \frac{p^2}{q^2} + 1\right)\,,$$

que multiplicando por q^2 nos da

$$(2pq, p^2 - q^2, p^2 + q^2)\,,$$

parametrización atribuida a Diofanto.

Comenta F. Vera en su libro "Los científicos griegos" [42] que, en el manuscrito 48 de la Biblioteca Nacional —catálogo de Iriarte— del siglo XIII, que es el ejemplar de Diofanto más antiguo de los conocidos, una mano anónima ha escrito esta curiosa nota marginal:

"Que tu alma Diofanto sea con Satanás por la dificultad de los otros teoremas y, sobre todo, de la de éste."

Comentario muy exagerado ya que II.8 es uno de los problemas que podríamos catalogar de fáciles entre los 6 libros griegos de Diofanto.

Mucho más famosa es la nota marginal que Fermat anotó en su ejemplar de la edición de Bachet (1621), recogida en la reedición de su hijo Samuel de 1670.

"Por el contrario, es imposible descomponer un cubo en dos cubos, un bicuadrado en dos bicuadrados y, en general, una potencia cualquiera, aparte del cuadrado, en dos potencias del mismo exponente.

He encontrado una demostración realmente admirable, pero el margen de este libro es muy pequeño para ponerla."

El libro VI consta de 24 problemas sobre triángulos rectángulos de lados racionales que, además de satisfacer a la ecuación pitagórica, deben cumplir las condiciones que les imponen sus respectivos enunciados.

En alguno de ellos utiliza la parametrización

$$(2pq, p^2 - q^2, p^2 + q^2)\,.$$

Así por ejemplo el problema 1 dice:

"Encontrar un triángulo tal que la hipotenusa menos una y otra de las perpendiculares haga un cubo."

En la parametrización

$$a = 2pq,\ b = p^2 - q^2,\ c = p^2 + q^2\,,$$

intenta tomar

$$p = x,\ q = 3,\ a = 6x,\ b = x^2 - 9,\ c = x^2 + 9\,;$$

la diferencia $c - b = 18$ es $2 \cdot 3^2$, que no es un cubo.

Para conseguir que $2q^2 =$ cubo, toma $q = 2$. Ahora,

$$a = 4x,\ b = x^2 - 4,\ c = x^2 + 4,\ c - a = x^2 - 4x + 4 = (x - 2)^2\,.$$

Para que sea cubo, toma $x - 2 = 8$, o sea $x = 10$. Luego $a = 40$, $b = 96$, $c = 104$.

El problema 17 pide:

"Encontrar un triángulo rectángulo tal que su área más su hipotenusa sea un cuadrado y su perímetro sea un cubo."

Esto es:

$$\frac{1}{2}xy + z = \text{cuadrado}, \tag{1.1}$$

$$x + y + z = \text{cubo}. \tag{1.2}$$

La solución original no utiliza la parametrización, pero podemos recrear una solución con parametrización que no utiliza más cuentas que las que aparecen

en las soluciones de los problemas VI.3 y VI.19, aparte de las de este mismo problema VI.17.

En

$$\begin{cases} x = 2pq\lambda, \\ y = (p^2 - q^2)\lambda, \\ z = (p^2 + q^2)\lambda, \end{cases}$$

tomamos $q = 1$ y $\lambda = \frac{1}{p}$, dando

$$\begin{cases} x = 2\,, \\ y = p - \dfrac{1}{p}\,, \\ z = p + \dfrac{1}{p}\,. \end{cases}$$

Debe ser

$$2p = \text{cuadrado}, \tag{1.3}$$
$$2p + 2 = \text{cubo}, \tag{1.4}$$

de manera que llevando (1.3) a (1.4), se hace necesario encontrar una solución de

$$\text{cuadrado} + 2 = \text{cubo}. \tag{1.5}$$

Diofanto hace, para esto,

$$\text{cuadrado} = (\sigma + 1)^2,\ \text{cubo} = (\sigma - 1)^3\,,$$

con lo que

$$\begin{aligned} \sigma^2 + 2\sigma + 3 &= \sigma^3 - 3\sigma^2 + 3\sigma - 1\,, \\ 4\sigma^2 + 4 &= \sigma^3 + \sigma\,, \\ 4(\sigma^2 + 1) &= \sigma(\sigma^2 + 1)\,, \end{aligned}$$

luego $\sigma = 4$; cuadrado $= 5^2$ y cubo $= 3^3$, que sustituidos en (1.5) nos dan

$$5^2 + 2 = 3^3\,.$$

Entonces $p = \frac{25}{2}$ y la solución diofántica es

$$x = 2,\ y = \frac{621}{50},\ z = \frac{629}{50}\,.$$

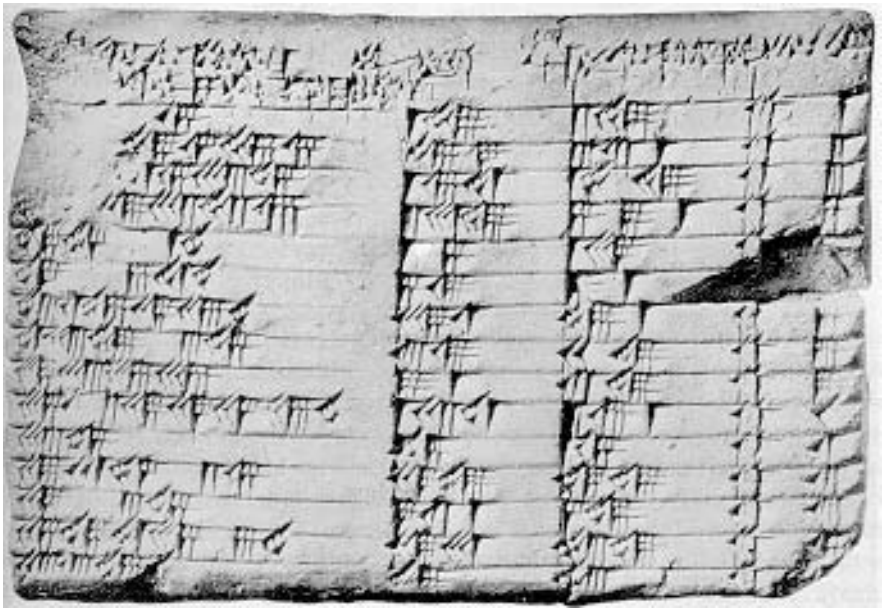

Figura 1.1: Tablilla Plimpton 322.

1.2. La tablilla Plimpton 322

Retrocedemos unos dos mil años, a la Babilonia antigua. En la figura 1.1 tenemos parte de una tablilla de arcilla, con escritura cuneiforme, perteneciente a la colección Plimpton de la Universidad de Columbia, en Nueva York, y catalogada con el número 322. La descripción que sigue está extraída de Neugebauer [33], con algunas interpretaciones propias y, posiblemente, novedosas.

Se conserva la parte derecha de la tablilla, en la que aparecen cuatro columnas, pues la que consta de solo números que parecen ser onces se considera un motivo de separación. La última columna esta encabezada por la expresión "sus nombres", y en ella aparecen los números del 1 al 15.

La segunda y tercera columnas están encabezadas por palabras que Neugebauer transcribió por "números solución de la anchura" y "números solución de la diagonal". En el encabezamiento de la primera columna aparece la palabra "diagonal", pero no consiguió descifrar el significado exacto de las otras palabras. En esta primera columna hay varios números que no se distinguen.

En la tabla 1.1 mostramos una transcripción de las cuatro columnas significativas de la tablilla (encabezadas por I, II, III y IV, junto con una descripción cuyo significado se aclarará más adelante). Esta transcripción

Tabla 1.1: Transcripción de la tablilla Plimpton 322.

$I, \quad (\frac{z}{x})^2$	$II, \quad y$	$III, \quad z$	IV	x	p	q	α
[1, 59, 0,]15 1.983402777	1, 59 119	2, 49 169	1	2, 0 120	12 12	5 5	$44^\circ 45' 37''$
[1, 56, 56,]58, 14, 50, 6, 15 1.949158552	56, 7 3367	**3, 12, 1** 1, 20, 25 11521 4825	2	57, 36 3456	1, 4 64	27 27	$44^\circ 15' 10''$
[1, 55, 7,]41, 15, 33, 45 1.918802127	1, 26, 41 4601	1, 50, 49 6649	3	1, 20, 0 4800	1, 15 75	32 32	$43^\circ 47' 14''$
[1,]5[3, 1]0, 29, 32, 52, 16 1.886247907	3, 31, 49 12709	5, 9, 1 18541	4	3, 45, 0 13500	2, 5 125	54 54	$43^\circ 16' 17''$
[1]48, 54, 1, 40 1.815007716	1, 5 65	1, 37 97	5	1, 12 72	9 9	4 4	$42^\circ 04' 30''$
[1]47, 6, 41, 40 1.785192901	5, 19 319	8, 1 418	6	6, 0 360	20 20	9 9	$41^\circ 32' 40''$
[1]43, 11, 56, 28, 26, 40 1.719983676	38, 11 2291	59, 1 3541	7	45, 0 2700	54 54	25 25	$40^\circ 18' 55''$
[1,]41, 33, 59, 3, 45 1.692773438	13, 19 799	20, 49 1249	8	16, 0 960	32 32	15 15	$39^\circ 46' 18''$
[1,]38, 33, 36, 36 1.642669445	**9, 1** 8, 1 541 481	12, 49 769	9	10, 0 600	25 25	12 12	$38^\circ 47' 5''$
1, 35, 10, 2, 28, 27, 24, 26, 40 1.586122566	1, 22, 41 4961	2, 16, 1 8161	10	1, 48, 0 6480	1, 21 81	40 40	$37^\circ 26' 14''$
1, 33, 45 1.5625	**45** 45, 0 45 2700	**1, 15** 1, 15, 0 75 4500	11	1, 0 60 3600	30 60	30 30	$36^\circ 52' 12''$
1, 29, 21, 54, 2, 15 1.489416843	27, 59 1679	48, 49 2929	12	40, 0 2400	48 48	25 25	$34^\circ 58' 34''$
[1,]27, 0, 3, 45 1.450017361	**7, 12, 1** 2, 41 25921 161	4, 49 289	13	4, 0 240	15 15	8 8	$33^\circ 51' 18''$
1, 25, 48, 51, 35, 6, 40 1.43023882	29, 31 1771	53, 49 3229	14	45, 0 2700	50 50	27 27	$33^\circ 15' 43''$
[1,]23, 13, 46, 40 1.387160494	**56** 28 56 28	**53** 1, 46 53 106	15	1, 30 90 45	9 9	5 5	$31^\circ 53' 27''$

está, también, extraída de [33]. En ella, en la primera columna aparecen, entre corchetes, lo que se supone que debería contener la parte de la primera columna que no se distingue. Además, nosotros hemos añadido, a la transcripción, cuatro columnas más en la parte de la derecha (las encabezadas por x, p, q y α). Más adelante las comentamos.

En bastantes casillas de la tabla, aparecen dos filas. En estos casos, el número superior está escrito con notación sexagesimal (transcripción directa de la original babilónica). Y el inferior corresponde a su conversión a la notación decimal moderna.

Los números de las columnas dos y tres corresponden al cateto y la hipotenusa de diversas ternas pitagóricas, con catetos x e y e hipotenusa z. Los marcados en negrita son, según Neugebauer, errores cometidos por el escriba. En estos, en la parte derecha de la correspondiente casilla aparece lo que, supuestamente, debería ser correcto.

La columna quinta, una de las que hemos añadido, contiene los correspondientes valores de x. Además, en las columnas sexta y séptima, hemos incluido los valores p y q de la parametrización diofántica $x = 2pq$, $y = p^2 - q^2$, $z = p^2 + q^2$.

Observamos que todas las ternas se pueden obtener con esta parametri-

zación, excepto la undécima. Pero al no haber ceros en la tablilla, en vez de leer $1,15_{(60} = 75_{(10}$ podríamos leer $1,15,0_{(60} = 4500_{(10}$; y en vez de leer $45_{(60} = 45_{(10}$, leer $45,0_{(60} = 2700_{(10}$, terna que se obtiene por la parametrización tomando $p = 60$ y $q = 30$. Aunque no sabemos por qué no tomó la terna $(4, 3, 5)$ que se obtiene de las anteriores dividiendo por 15 ó por 900.

Aparte de ésta y de la decimoquinta, todas las restantes ternas son primitivas, siendo esta última cuasiprimitiva, generada por $p = 9$, $q = 5$, primos entre sí.

Podemos observar que, en la descomposición en factores de todos los x de la tabla, sólo aparecen los primos 2, 3 y 5. Por tanto son números que en base 60 son fáciles de invertir (números regulares). El mayor valor que alcanza x es 13500. Además, los exponentes máximos de 2, 3 y 5 son 7, 4 y 3 respectivamente.

En la primera columna aparece $\frac{z^2}{x^2}$, esto es, la $(\sec\alpha)^2$, siendo α el ángulo comprendido entre la hipotenusa z y el cateto x. La última columna añadida, a la derecha, muestra los correspondientes valores de α en grados sexagesimales (con notación actual). Vemos que los ángulos están ordenados en orden decreciente.

Asimismo, hemos construido la tabla 1.2, en la que están calculadas todas las ternas con x regular, $x < 15000$, y exponentes no superiores a 7 para el 2, 4 para el 3, y 3 para el 5. Vemos que las 15 primeras son precisamente las que aparecen en la tablilla Plimpton.

Sobre los errores en la tablilla, Neugebauer supone que el II,9 (es decir, el que aparece —en negrita— en la fila 9 de la columna II) es debido a un simple error del escriba, quien escribió $9,1$ en vez de $8,1$. El error II,13, donde en el texto aparece $7,12,1$ en vez de $2,41$, lo atribuye a que el escriba puso el cuadrado de

$$2,41_{(60} = 161_{(10}\,,$$

esto es,

$$(161_{(10})^2 = 25921_{(10} = 7,12,1_{(60}\,.$$

El error III,15, donde aparece 53 en vez de $1,46$, que es el doble de 53, lo atribuye a que al escriba se le olvidó multiplicar por 2. Sin embargo, nosotros pensamos que el verdadero error es el 56 de II,15, que debería de ser la mitad, 28, quedando la terna $y = 28, z = 53, x = 45$, que es primitiva. Esto casaría con la forma en que Neugebauer supone que se construyó la tabla, calculando

$$d = \frac{p}{q},\ d^{-1} = \frac{q}{p},\ v = \frac{d - d^{-1}}{2},\ w = \frac{d + d^{-1}}{2}\,.$$

Tabla 1.2: Ternas pitagóricas con x regular, $x < 15000$, y exponentes no superiores a 7 para el 2, 4 para el 3, y 3 para el 5.

α	p	q	x	y	z	$\sec^2(\alpha)$
$44, 45, 36$	12	5	120	119	169	$\frac{28561}{14400}$
$44, 15, 9$	64	27	3456	3367	4825	$\frac{23280625}{11943936}$
$43, 47, 14$	75	32	4800	4601	6649	$\frac{44209201}{23040000}$
$43, 16, 16$	125	54	13500	12709	18541	$\frac{343768681}{182250000}$
$42, 4, 30$	9	4	72	65	97	$\frac{9409}{5184}$
$41, 32, 40$	20	9	360	319	481	$\frac{231361}{129600}$
$40, 18, 54$	54	25	2700	2291	3541	$\frac{12538681}{7290000}$
$39, 46, 13$	32	15	960	799	1249	$\frac{1560001}{921600}$
$38, 43, 4$	25	12	600	481	769	$\frac{591361}{360000}$
$37, 26, 13$	81	40	6480	4961	8161	$\frac{66601921}{41990400}$
$36, 52, 11$	2	1	4	3	5	$\frac{25}{16}$
$34, 58, 33$	48	25	2400	1679	2929	$\frac{8579041}{5760000}$
$33, 51, 18$	15	8	240	161	289	$\frac{83521}{57600}$
$33, 15, 42$	50	27	2700	1771	3229	$\frac{10426441}{7290000}$
$31, 53, 26$	9	5	90	56	106	$\frac{11236}{8100}$
$31, 17, 4$	16	9	288	175	337	$\frac{113569}{82944}$
$28, 41, 55$	27	16	864	473	985	$\frac{970225}{746496}$
$28, 4, 20$	5	3	30	16	34	$\frac{1156}{900}$
$26, 37, 38$	81	50	8100	4061	9061	$\frac{82101721}{65610000}$
$25, 59, 21$	8	5	80	39	89	$\frac{7921}{6400}$
$24, 45, 41$	25	16	800	369	881	$\frac{776161}{640000}$
$22, 37, 11$	3	2	12	5	13	$\frac{169}{144}$
$21, 57, 40$	40	27	2160	871	2329	$\frac{5424241}{4665600}$
$20, 26, 39$	36	25	1800	671	1921	$\frac{3690241}{3240000}$
$19, 46, 33$	64	45	5760	2071	6121	$\frac{37466641}{33177600}$
$19, 9, 57$	45	32	2880	1001	3049	$\frac{9296401}{8294400}$
$18, 29, 32$	25	18	900	301	949	$\frac{900601}{810000}$
$16, 56, 32$	27	20	1080	329	1129	$\frac{1274641}{1166400}$
$16, 15, 36$	4	3	24	7	25	$\frac{625}{576}$
$14, 0, 9$	32	25	1600	399	1649	$\frac{2719201}{2560000}$
$12, 40, 49$	5	4	40	9	41	$\frac{1681}{1600}$
$10, 23, 19$	6	5	60	11	61	$\frac{3721}{3600}$
$9, 41, 16$	32	27	1728	295	1753	$\frac{3073009}{2985984}$
$6, 43, 58$	9	8	144	17	145	$\frac{21025}{20736}$
$6, 1, 32$	10	9	180	19	181	$\frac{32761}{32400}$
$4, 24, 18$	27	25	1350	104	1354	$\frac{1833316}{1822500}$
$3, 41, 42$	16	15	480	31	481	$\frac{231361}{230400}$
$2, 20, 17$	25	24	1200	49	1201	$\frac{1442401}{1440000}$

Así, para $p = 9$ y $q = 5$ se tiene

$$w = \frac{\frac{9}{5} + \frac{5}{9}}{2} = \frac{106}{90} = \frac{53}{45}\,,$$

$$v = \frac{\frac{9}{5} - \frac{5}{9}}{2} = \frac{56}{90} = \frac{28}{45}\,,$$

obteniendo la terna $(45, 28, 53)$, en vez de la terna $(90, 56, 106)$.

Finalmente, para explicar el error III,2 sigue a R. J. Gillins, quien supone que el escriba cometió dos errores. Al calcular $z = p^2 + q^2 = (p+q)^2 - 2pq$ con

$$p = 1, 4_{(60} = 64_{(10},\ q = 27_{(60}$$

el escriba cambió $-2pq$ por $+2pq$ y, en vez de escribir $2 \cdot 27 \cdot 1, 4 = 57, 36$, escribió $2 \cdot 27 \cdot 1, 0 = 54, 0$. Hallando, por tanto,

$$z = 2, 18, 1 + 54, 0 = 3, 12, 1\,,$$

en vez de

$$z = 2, 18, 1 - 57, 36 = 1, 20, 25\,.$$

Capítulo 2

Ternas pitagóricas de catetos menores que n

2.1. Introducción

Recordemos que un trío (a, b, c) de enteros estrictamente positivos se denomina terna pitagórica si satisface $a^2+b^2 = c^2$. El correspondiente triángulo de catetos a, b e hipotenusa c es un triángulo pitagórico. Una terna (o un triángulo) pitagórica se dice primitiva si y sólo si a, b y c son primos entre sí.

Si fijamos un parámetro n, podemos contar el número de triángulos pitagóricos (primitivos o no) que tienen alguna propiedad o característica cuyo valor está acotado por el parámetro n; por ejemplo, área, hipotenusa, ... Así, hemos construido una función que depende de n. En la literatura matemática, se han estudiado estimaciones asintóticas para este tipo de funciones relacionadas con las ternas pitagóricas. Veamos, en primer lugar, algunos ejemplos.

D. N. Lehmer [28], en 1900, demostró que el número de ternas pitagóricas primitivas de hipotenusa menor que n, $P_h(n)$, verifica

$$P_h(n) \sim \frac{n}{2\pi},\ n \to \infty;$$

y que el número de ternas pitagóricas primitivas que forman triángulos de perímetro menor que n, $P_p(n)$, verifica

$$P_p(n) \sim \frac{\log 2}{\pi^2}\, n\,.$$

Posteriormente, D. H. Lehmer [27], en 1948, estableció que

$$P_p(n) = \frac{\log 2}{\pi^2}\, n + O\left(n^{\frac{1}{2}} \log n\right)\,.$$

J. Lambek y L. Moser [26] en 1955 probaron que el número de ternas pitagóricas primitivas que forman un triángulo de área menor que n es

$$P_a(n) = \kappa n^{\frac{1}{2}} + O\left(n^{\frac{1}{3}}\right) ,$$

con $\kappa = \Gamma\left(\frac{1}{4}\right)^2 2^{-\frac{1}{2}}\pi^{-\frac{5}{2}} = 0.531340\ldots$, y que

$$P_h(n) = \frac{1}{2\pi}\, n + O\left(n^{\frac{1}{2}} \log n\right) .$$

En el mismo año 1955, R. E. Wild [43] mejoró la estimación de Lambek y Moser para $P_a(n)$, estableciendo

$$P_a(n) = \kappa n^{\frac{1}{2}} - \kappa' n^{\frac{1}{3}} + O\left(n^{\frac{1}{4}} \log n\right) ,$$

con $\kappa = \Gamma\left(\frac{1}{4}\right)^2 2^{-\frac{1}{2}}\pi^{-\frac{5}{2}} = 0.531340\ldots$, y $\kappa' = -\frac{\zeta\left(\frac{1}{3}\right)\left(1+2^{-\frac{1}{3}}\right)}{\zeta\left(\frac{4}{3}\right)\left(1+4^{-\frac{1}{3}}\right)} \simeq 0.297.$

Respecto al número de ternas pitagóricas con hipotenusa menor o igual que n, $T_h(n)$, W. Sierpiński [39] probó que

$$T_h(n) = \frac{1}{\pi}\, n \log n + (B-1)n + E(n) ,$$

con $B = \frac{1}{\pi}(\gamma + \frac{K}{\pi} - \frac{12F}{\pi^2} + \frac{\log 2}{3} - \frac{1}{\pi})$, donde γ es la constante de Euler, $F = 0.9375482543\ldots$ y $K = 2.5849817596\ldots$ son constantes explícitamente dadas, siendo

$$E(n) = O\left(n^{\frac{2}{3}}\right) .$$

M. I. Stronina [40] precisó la estimación de $E(n)$, estableciendo

$$E(n) = O\left(n^{\frac{1}{2}} e^{-\kappa(\log n)^{\frac{3}{5}}(\log\log n)^{-\frac{1}{5}}}\right) \qquad \text{con un } \kappa > 0$$

y que

$$E(n) = \Omega(n^{\frac{1}{4}}) .$$

El símbolo Ω se define como la negación del símbolo o, así que $F(t) = \Omega\left(\phi(t)\right)$ significa que la desigualdad $|F(t)| > A\phi(t)$ se satisface para algunos valores arbitrariamente grandes de t.

Condicionado a la hipótesis de Riemann, W. G. Nowak y W. Recknagel [34] demostraron que

$$E(n) = O\left(n^{\frac{53}{116}+\varepsilon}\right) .$$

Y, más tarde, M. Kühleitner [25] probó que, para $n \to \infty$, es

$$E(n) = \Omega\left(n^{\frac{1}{3}}\right) .$$

A. Fässler [16] da, para el número de hipotenusas $c \leq n$ tales que existen exactamente 2^{k-1} ternas pitagóricas distintas (a, b, c), la estimación

$$H_k(n) \sim \frac{1}{2^k} \frac{1}{(k-1)!} \frac{n(\log\log n)^{k-1}}{\log n} \text{ cuando } n \to \infty .$$

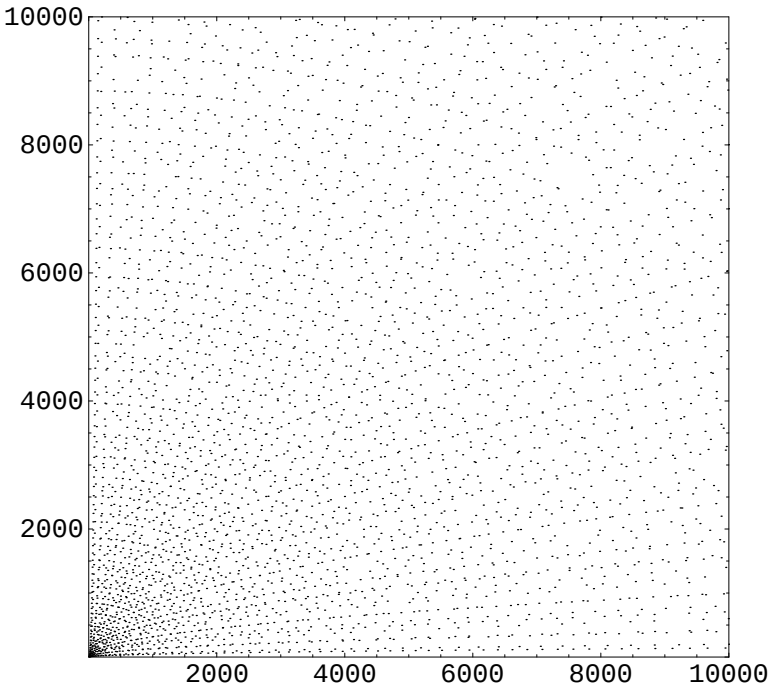

Figura 2.1: Catetos de las ternas pitagóricas primitivas del cuadrado $(0, 10000) \times (0, 10000)$.

Sin embargo, por lo que nosotros sabemos, todavía no se había estudiado el problema de estimar el número de triángulos pitagóricos de catetos menores que n. Esto es lo que queremos hacer en este capítulo, encontrar estimaciones asintóticas para el número de triángulos pitagóricos con catetos menores que n. Las estudiamos en ambos casos: triángulos primitivos y triángulos generales.

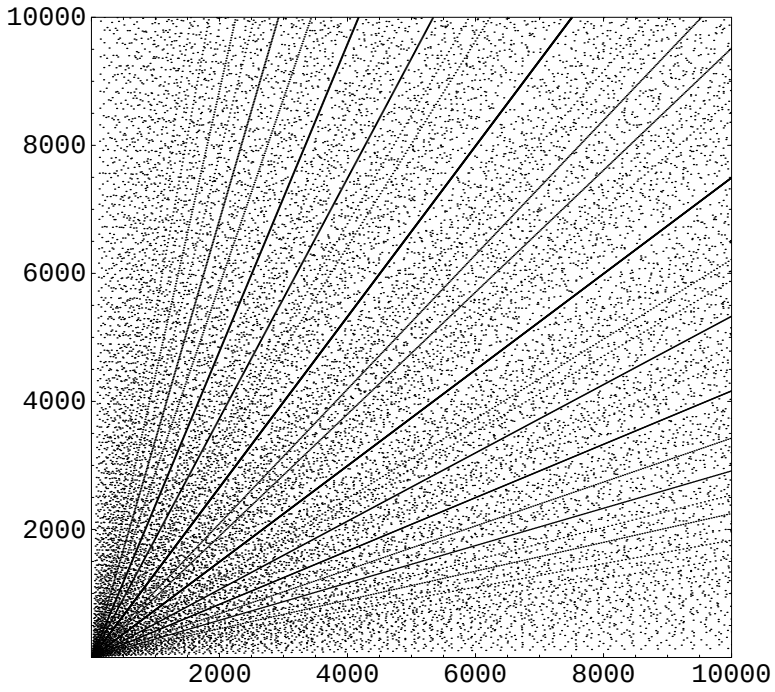

Figura 2.2: Catetos de las ternas pitagóricas del cuadrado $(0, 10000) \times (0, 10000)$.

Los principales resultados de este capítulo son los teoremas 2.2.7 y 2.2.8, así como el teorema 2.3.11; este último supone una mejora en la cota del error mostrada en el teorema 2.2.7, aunque a costa de tener una demostración mucho más complicada. De todas formas, y como comentamos en la última sección de este capítulo, basada en datos experimentales, resulta bastante plausible pensar que la estimación asintótica es, en realidad, mucho más precisa de lo que sugiere la cota del error del teorema 2.3.11.

En la figura 2.1, representamos, en el plano ab, los pares (a, b) de las ternas primitivas (a, b, c) que verifican las condiciones $a < n$, $b < n$ (considerando (a, b) distinto de (b, a)) para $n = 10000$. Análogamente, representamos en la figura 2.2 las ternas pitagóricas generales. De esta forma, podemos decir que estamos contando (y estimando) el número de triángulos pitagóricos del cuadrado $(0, n) \times (0, n)$.

Designamos por $P(n)$ el número de ternas pitagóricas primitivas (a, b, c) con catetos $a < n$, $b < n$; y por $T(n)$ el número de ternas pitagóricas ge-

nerales con $a < n$, $b < n$. Tanto en $P(n)$ como en $T(n)$ consideramos que la terna (a, b, c) es la misma que (b, a, c). Si consideramos (a, b, c) y (b, a, c) como ternas distintas, designamos los números correspondientes de ternas pitagóricas primitivas y generales por $\widetilde{P}(n)$ y $\widetilde{T}(n)$ respectivamente. Es claro que $\widetilde{P}(n) = 2P(n)$ y $\widetilde{T}(n) = 2T(n)$.

Para las ternas pitagóricas primitivas (a, b, c), se conoce la siguiente parametrización atribuida a Diofanto:

$$a = x^2 - y^2\,,\ b = 2xy\,,\ c = x^2 + y^2\,,$$

con x, y enteros positivos, primos entre sí y de distinta paridad. Esta fórmula genera todas las ternas pitagóricas primitivas con a impar y b par. Obviamente, el número de tales ternas es, $P(n)$.

Así, el problema de encontrar el número $P(n)$ se reduce al problema de contar los puntos (x, y) de coordenadas enteras, primas entre sí y de distinta paridad, de la región del plano xy definida por

$$\begin{cases} x^2 - y^2 < n, \\ 2xy < n, \\ x > y > 0. \end{cases} \tag{2.1}$$

2.2. Una primera estimación

Dado un entero positivo n, designamos por P_n y Q_n a los conjuntos siguientes:

$$\begin{aligned} P_n &= \{(x, y) \text{ que verifican (2.1) } :\ \operatorname{mcd}(x, y) = 1,\ \text{de paridades opuestas}\}\,, \\ Q_n &= \{(x, y) \text{ que verifican (2.1) } :\ \operatorname{mcd}(x, y) = 1\} \end{aligned}$$

(desde luego que x e y son números enteros positivos). Así, el $P(n)$ de la sección anterior es $P(n) = \#P_n$; análogamente definimos $Q(n) = \#Q_n$.

De esta forma, tenemos

Lema 2.2.1. *De acuerdo con la notación anterior,*

$$P(n) = \sum_{k \geq 0} (-1)^k Q\Big(\frac{n}{2^k}\Big). \tag{2.2}$$

Demostración. Si $(x, y) \in Q_n$, hay dos posibilidades: (i) x e y tienen paridades opuestas; o (ii) x e y son números impares. En el caso (i), $(x, y) \in P_n$. Analizamos el caso (ii): para un tal (x, y), sea (a, b, c) su correspondiente terna pitagórica de acuerdo con la parametrización de Diofanto.

Es fácil comprobar que, si x e y son números impares primos entre sí, entonces $\mathrm{mcd}(a,b,c)=2$; recíprocamente, si $\mathrm{mcd}(a,b,c)=2$, entonces existen x e y números impares primos entre sí tales que $a=x^2-y^2$, $b=2xy$, y $c=x^2+y^2$. Así, en el caso (ii), (x,y) genera una terna pitagórica (a,b,c) con $a<n$, $b<n$ y $\mathrm{mcd}(a,b,c)=2$. Por tanto, $(\frac{a}{2},\frac{b}{2},\frac{c}{2})$ es una terna pitagórica primitiva con $\frac{a}{2}<\frac{n}{2}$, $\frac{b}{2}<\frac{n}{2}$; esto es, $(x,y)\in P_{n/2}$.

De esta forma, hemos probado que $Q(n)=P(n)+P(\frac{n}{2})$. Ahora, es evidente que $P(n)=Q(n)-Q(\frac{n}{2})+Q(\frac{n}{2^2})-\ldots$. □

Por conveniencia, reescribimos (2.1) haciendo $n=t^2$, $t\in[1,\infty)$. Entonces, se transforma en

$$\begin{cases} x^2-y^2<t^2, \\ \quad 2xy<t^2, \\ x>y>0. \end{cases} \tag{2.3}$$

Para $t=1$, designamos por R la región del plano xy acotada por las ecuaciones (2.3). Para un t general, cada región Rt (homotética con R), se obtiene aplicando una semejanza de centro $(0,0)$ y razón t. Mostramos esta región Rt en la figura 2.3, con su borde marcado con una línea gruesa.

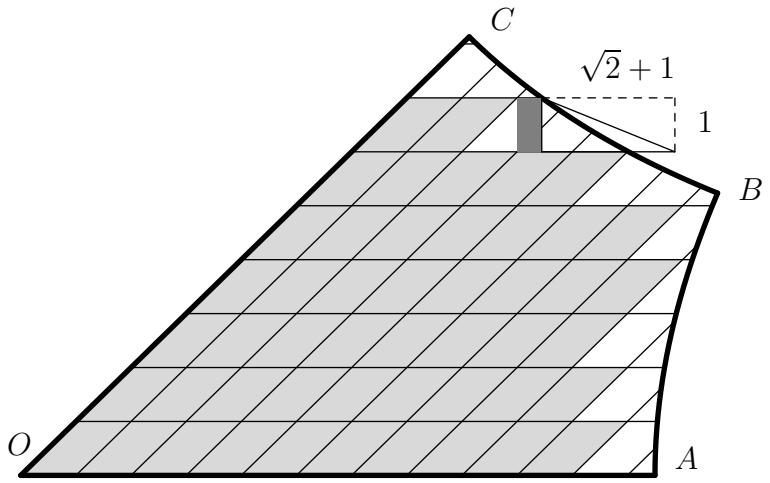

Figura 2.3: Región del plano xy definida por $x^2-y^2<t^2$, $2xy<t^2$, $x>y>0$.

Ahora, utilizamos $L(Rt)$ para designar el número de puntos de coordenadas enteras (x,y) de la región Rt; en la figura 2.3, estos puntos corresponden a las intersecciones entre las líneas horizontales y las inclinadas. También, designamos por $L'(Rt)$ el número de puntos de Rt cuyas coordenadas son primas entre sí. Establecemos el siguiente

Lema 2.2.2. *Tenemos la relaciones*

$$L(Rt) = \sum_{d\geq 1} L'\Big(R\frac{t}{d}\Big) = \sum_{t\geq d\geq 1} L'\Big(R\frac{t}{d}\Big) \tag{2.4}$$

y

$$L'(Rt) = \sum_{d\geq 1} \mu(d) L\Big(R\frac{t}{d}\Big) = \sum_{t\geq d\geq 1} \mu(d) L\Big(R\frac{t}{d}\Big)\,, \tag{2.5}$$

siendo $\mu(d)$ la función de Möbius.

Demostración. Observamos primero que $L(R\lambda) = L'(R\lambda) = 0$ para $\lambda < 1$, por esto las sumas finitas e infinitas son equivalentes.

Con un pequeño abuso de notación, utilizamos L tanto para designar el conjunto como su cardinal; y lo mismo para L'. Sea $(x, y) \in L(Rt)$ con $\mathrm{mcd}(x, y) = d$. Entonces, $x = x_1 d$, $y = y_1 d$ con $\mathrm{mcd}(x_1, y_1) = 1$; esto es, $(x_1, y_1) \in L'(R\frac{t}{d})$. Por lo tanto, existen tantos puntos en $L(Rt)$ cuyo mcd es d, como puntos en $L'(R\frac{t}{d})$. Así se sigue (2.4).

Para establecer (2.5), sólo tenemos que aplicar la fórmula de inversión de Möbius (ver, por ejemplo, [21, teorema 268]). □

Un poco de notación: utilizaremos $M(Rt)$ para designar el área de la región Rt. Así, tenemos el siguiente

Lema 2.2.3. *De acuerdo con la notación previa, tenemos*

$$0 \leq M(Rt) - L(Rt) < \Big(\sqrt{2} + \frac{1}{2}\Big)\, t + 3\,. \tag{2.6}$$

En particular, $M(Rt) - L(Rt) = O(t)$.

Demostración. Ilustramos la demostración con la figura 2.3. Aquí, en el plano xy, la recta OA es el eje $y = 0$, y OC es la recta $y = x$. Análogamente, los arcos AB y BC representan, respectivamente, $x^2 - y^2 = t^2$ y $2xy = t^2$. Así, el borde de Rt es la línea gruesa (recordemos que $M(Rt)$ es, por definición, su área interior).

En la figura, también representamos las rectas $y = j$ (rectas horizontales) e $y = x - i$ (rectas inclinadas) para números enteros positivos j e i. Con sus intersecciones, formamos un retículo; $L(Rt)$ es el número de puntos del retículo. Con estos puntos, formamos paralelogramos disjuntos. Pintamos de gris los que están contenidos en la región Rt. Es evidente que el área de cada uno de estos paralelogramos es 1.

Fijemos uno de estos paralelogramos. Afirmamos que está incluido en Rt si y sólo si su vértice superior derecho está en Rt (y así, es uno de los puntos contados por $L(Rt)$). De esta forma, concluimos $L(Rt) < M(Rt)$.

Para probar la afirmación, desde luego, sólo necesitamos estudiar los paralelogramos de la derecha de $y = x$, para cualquier banda entre $y = j$ e $y = j + 1$. Para cualquier paralelogramo con su vértice inferior derecho por encima de B, la afirmación es clara. Cuando el vértice inferior derecho no está por encima de B, también es cierta, pues la pendiente en el arco AB siempre es mayor que 1 (la pendiente de $y = x - i$).

Ahora, probaremos la cota superior de $M(Rt) - L(Rt)$ en (2.6). Tenemos que estimar el área blanca de la figura. Para cualquiera de las bandas horizontales entre $y = j$ e $y = j + 1$, acotamos el tamaño de la parte blanca. Primero, estudiamos una banda por encima de B.

En la figura, para una de tales bandas, hemos partido el área blanca en tres partes: el rectángulo gris del medio (con su vértice superior izquierdo en el retículo y su vértice superior derecho en el arco BC), el triángulo de la izquierda (que es medio paralelogramo) y el triángulo con un lado curvo de la derecha (siendo el arco BC uno de sus lados). Es claro que el área del rectángulo gris es menor o igual que 1, y que el área del triángulo de la izquierda siempre es $1/2$. También vamos a encontrar una cota para el área del triángulo mixtilíneo de la derecha. Para esto, teniendo en cuenta la pendiente en el arco BC, es fácil ver que el triángulo mixtilíneo siempre está incluido en un triángulo rectángulo de catetos 1 y $1 + \sqrt{2}$, como se muestra en la figura. El área de este triángulo es $\frac{1+\sqrt{2}}{2}$, un número fijo. Entonces, el área de la parte blanca de esta banda es menor que

$$1 + \frac{1}{2} + \frac{1+\sqrt{2}}{2} = 2 + \frac{\sqrt{2}}{2}\,. \tag{2.7}$$

Para una banda por debajo de B, o para la banda que contiene el punto B, podemos utilizar argumentos parecidos para encontrar cotas mejores. En particular, también se cumple la cota (2.7) para el área de su parte blanca.

Notemos finalmente que tenemos, a lo sumo, $\frac{t}{\sqrt{2}} + 1$ bandas horizontales, pues el punto C es $C = (\frac{t}{\sqrt{2}}, \frac{t}{\sqrt{2}})$. Entonces se sigue (2.6). (Realmente, utilizando una cota más precisa para la parte blanca de las bandas inferiores a B, se puede encontrar una estimación mejor de la cota superior de $M(Rt) - L(Rt)$; aunque también será $O(t)$.) □

Por integración, obtenemos que el área $M(Rt)$ es

$$M(Rt) = \frac{\log(1+\sqrt{2})}{2}\, t^2\,,$$

y por tanto, por el lema 2.2.3, podemos escribir

$$L(Rt) = \frac{\log(1+\sqrt{2})}{2}\, t^2 + O(t)\,. \tag{2.8}$$

Antes de proseguir recordaremos algunos resultados conocidos que utilizaremos en la demostración del teorema 2.2.7.

Teorema 2.2.4. *[21, página 245]*

$$\zeta(2) = \sum_{n=1}^{\infty} \frac{1}{n^2} = \frac{\pi^2}{6}\,.$$

Teorema 2.2.5. *[21, teorema 287]*

$$\frac{1}{\zeta(s)} = \sum_{n=1}^{\infty} \frac{\mu(n)}{n^s} \quad (s > 1)\,.$$

Teorema 2.2.6. *[2, teorema 3.2 de la página 69] Si $x \geq 1$ tenemos:*

(a) $\sum_{n\leq x} \frac{1}{n^s} = \frac{x^{1-s}}{1-s} + \zeta(s) + O(x^{-s})$ *si* $s > 0$, $s \neq 1$.

(b) $\sum_{n>x} \frac{1}{n^s} = O(x^{1-s})$ *si* $s > 1$.

(c) $\sum_{n\leq x} n^{\alpha} = \frac{x^{\alpha+1}}{\alpha+1} + O(x^{\alpha})$ *si* $\alpha \geq 0$.

Teorema 2.2.7. *El número de ternas pitagóricas primitivas (a, b, c) que verifican la condición $a < n$, $b < n$ (considerando la terna (a, b, c) como distinta de la (b, a, c)) es*

$$\widetilde{P}(n) = \frac{4\log\left(1+\sqrt{2}\right)}{\pi^2}\, n + O\left(n^{\frac{1}{2}}\log n\right)\,.$$

Demostración. Por integración se obtiene que

$$M(R) = \frac{1}{2}\log\left(1+\sqrt{2}\right), \tag{2.9}$$

y por tanto

$$L(Rt) = \frac{1}{2}\, t^2 \log\left(1+\sqrt{2}\right) + O(t)\,.$$

Sustituyendo en (2.5) tenemos

$$L'(Rt) = \sum_{t>d\geq 1} \mu(d) L\left(R\frac{t}{d}\right)$$

$$= \sum_{t>d\geq 1} \mu(d)\left(\frac{1}{2}\,\frac{t^2}{d^2}\log\left(1+\sqrt{2}\right) + O\left(\frac{t}{d}\right)\right)$$

$$= \frac{1}{2}\, t^2 \log\left(1+\sqrt{2}\right) \sum_{d=1}^{\infty} \frac{\mu(d)}{d^2} + O(t\log t)$$

$$= \frac{3}{\pi^2}\, t^2 \log\left(1+\sqrt{2}\right) + O(t\log t)\,.$$

Deshaciendo el cambio $n = t^2$ se tiene

$$Q(n) = \frac{3}{\pi^2}\, n \log\left(1+\sqrt{2}\right) + O(\sqrt{n}\log n)\,. \tag{2.10}$$

Recordando la igualdad (2.2), podemos escribir

$$P(n) = \sum_{j\geq 0} (-1)^j Q\left(\frac{n}{2^j}\right) = \frac{3}{\pi^2}\, n \log\left(1+\sqrt{2}\right) \sum_{j\geq 0} \left(-\frac{1}{2}\right)^j + O\left(\sqrt{n}\log n\right)$$

$$= \frac{2}{\pi^2}\, n \log\left(1+\sqrt{2}\right) + O\left(\sqrt{n}\log n\right)\,.$$

Como $P(n)$ es el número de ternas primitivas con b par, el número total de ternas primitivas, considerando como distintas (a,b,c) y (b,a,c) (figura 2.1), será

$$\widetilde{P}(n) = \frac{4\log\left(1+\sqrt{2}\right)}{\pi^2}\, n + O\left(\sqrt{n}\log n\right)\,.$$

□

Teorema 2.2.8. *Si $\widetilde{T}(n)$ es el número de ternas primitivas o no, cuyos catetos son menores que n (figura 2.2), entonces se verifica*

$$\widetilde{T}(n) = \frac{4\log\left(1+\sqrt{2}\right)}{\pi^2}\, n\log n + O(n)\,.$$

Demostración. Tenemos que

$$T(n) = \sum_{d=1}^{n} \widetilde{P}\left(\frac{n}{d}\right) = \sum_{d=1}^{n} \left(\frac{4}{\pi^2}\frac{n}{d}\log\left(1+\sqrt{2}\right) + O\left(\sqrt{\frac{n}{d}}\log\left(\frac{n}{d}\right)\right)\right)$$

$$= \frac{4\log\left(1+\sqrt{2}\right)}{\pi^2}\, n \sum_{d=1}^{n} \frac{1}{d} + \sum_{d=1}^{n} O\left(\left(\frac{n}{d}\right)^{\frac{1}{2}} \log\frac{n}{d}\right)$$

$$= \frac{4\log\left(1+\sqrt{2}\right)}{\pi^2}\, n\log n + O(n)\,.$$

□

2.3. Intentando mejorar la estimación

El objetivo de esta sección es mejorar el término del error $O(n^{\frac{1}{2}} \log n)$ que aparece en el teorema 2.2.7: lo lograremos rebajar hasta $O(n^{\frac{1}{2}})$ (ver teorema 2.3.11). Utilizaremos diversas técnicas de Vinogradov y Sierpiński para la estimación de sumas de partes fraccionarias, adaptadas a nuestros propósitos. Una exposición detallada de tales técnicas puede encontrarse en [23] y [17].

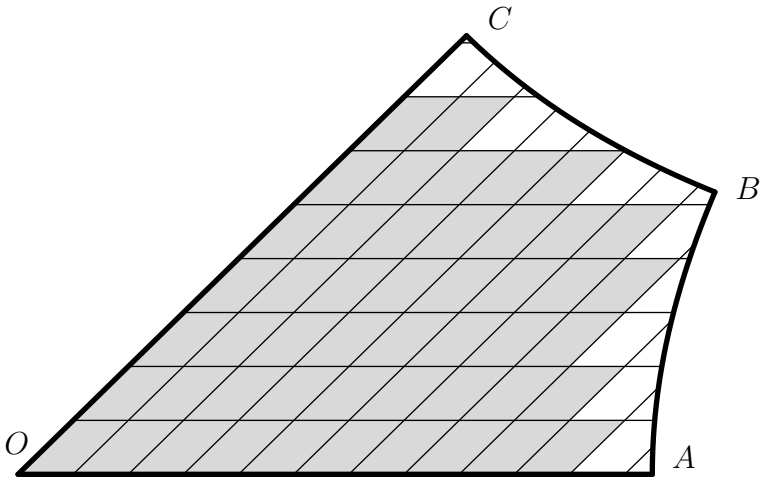

Figura 2.4: Región Rt del plano xy, siendo $R_b(t)$ su parte no sombreada.

Observemos la figura 2.4. Vemos que, al tomar como aproximación del número de puntos de coordenadas enteras de la región, $L(Rt)$, el área de la región, $M(Rt)$, el error cometido es el área de la parte blanca. Nuestro primer propósito va a ser estimar el valor de este área para conseguir establecer el siguiente teorema:

Teorema 2.3.1.

$$L(Rt) = \frac{\log\left(1+\sqrt{2}\right)}{2}\, t^2 - \frac{2+\sqrt{2}}{4}\, t + O\left(t^{\frac{2}{3}} \log t\right) .$$

Este resultado será clave en la demostración del teorema 2.3.11, en el que mostramos la perseguida mejora del término del error que aparece en el teorema 2.2.7.

Introduzcamos un poco de notación basada en la figura 2.4 (ó 2.3). Como vemos, los vértices de la región son O, A, B y C. Las coordenadas de A son $(t, 0)$, las de B son $\left(t\sqrt{\frac{\sqrt{2}+1}{2}}, t\sqrt{\frac{\sqrt{2}-1}{2}}\right)$ y las de C son $\left(\frac{t}{\sqrt{2}}, \frac{t}{\sqrt{2}}\right)$.

Designamos por (x_1, y_1), (x_2, y_2), (x_3, y_3) las partes enteras de las coordenadas de A, B y C respectivamente. Así,

$$x_1 = \lfloor t \rfloor\,,\ y_1 = 0,\ x_2 = \left\lfloor t\sqrt{\frac{\sqrt{2}+1}{2}} \right\rfloor\,,$$

$$y_2 = \left\lfloor t\sqrt{\frac{\sqrt{2}-1}{2}} \right\rfloor\,,\ x_3 = y_3 = \left\lfloor \frac{t}{\sqrt{2}} \right\rfloor\,.$$

Abordemos ya la demostración del teorema 2.3.1. Para ello necesitaremos bastantes resultados previos. Vamos con ello.

Lema 2.3.2. *El área $E_1(t)$, de la región limitada por el arco de curva CB y la poligonal de vértices en los puntos de intersección de las rectas $x =$ entero con el arco de curva CB, verifica*

$$E_1(t) = O(1)\,.$$

Demostración. Sea $e(x_0)$ el área de la región limitada por el arco de curva CB y el segmento que une los puntos de intersección de la curva con las rectas $x = x_0$ y $x = x_0 + 1$ es

$$\begin{aligned} e(x_0) &= \frac{1}{2}\left(\frac{t^2}{2x_0} + \frac{t^2}{2(x_0+1)}\right) - \int_{x_0}^{x_0+1} \frac{t^2}{2x}\,dx \\ &= \frac{t^2}{2}\left(\frac{2x_0+1}{2(x_0+1)x_0} - \log\left(1+\frac{1}{x_0}\right)\right) \\ &\le \frac{t^2}{2}\left(\frac{2x_0+1}{2x_0^2+2x_0} - \frac{1}{x_0} + \frac{1}{2x_0^2}\right) = \frac{t^2}{4(x_0^3+x_0^2)}\,. \end{aligned}$$

Sumando convenientemente a lo largo de la poligonal tenemos

$$\begin{aligned} E_1(t) &= \sum_{x_0=x_3+1}^{x_2-1} e(x_0) \le \sum_{x_0=x_3+1}^{x_2-1} \frac{t^2}{4(x_0^3+x_0^2)} \\ &< \frac{t^2}{4\left(\frac{t^3}{2\sqrt{2}} + \frac{t^2}{2}\right)}\left(\sqrt{\frac{\sqrt{2}+1}{2}}\,t - \frac{t}{\sqrt{2}}\right) < k\,, \end{aligned}$$

donde k es una constante que no depende de t; por tanto $E_1(t) = O(1)$. □

Como es habitual, $\{x\}$ designa la parte decimal de x, esto es, $\{x\} = x - \lfloor x \rfloor$.

En la demostración del lema 2.3.4 utilizaremos la fórmula de sumación de Euler–Maclaurin. Esta fórmula puede encontrarse en [22, capítulo 4, pág. 104], aunque a nosotros nos bastará la siguiente versión simplificada que aparece en [23, teorema 12.2 de la pág. 134]:

Teorema 2.3.3. *Sea $f(x)$ una función con derivada segunda continua en el intervalo $Q \le x \le R$, y sea*

$$\sigma(x) = \int_0^x \left(\frac{1}{2} - \{t\}\right) dt\,.$$

Entonces

$$\sum_{Q<x\le R} f(x) = \int_Q^R f(x)\,dx + \left(\frac{1}{2} - \{R\}\right) f(R) - \left(\frac{1}{2} - \{Q\}\right) f(Q)$$

$$-\sigma(R)f'(R) + \sigma(Q)f'(Q) + \int_Q^R \sigma(x)f''(x)\,dx\,.$$

El valor de $\sigma(x)$ está comprendido entre 0 y $\frac{1}{8}$; ver la figura 2.5.

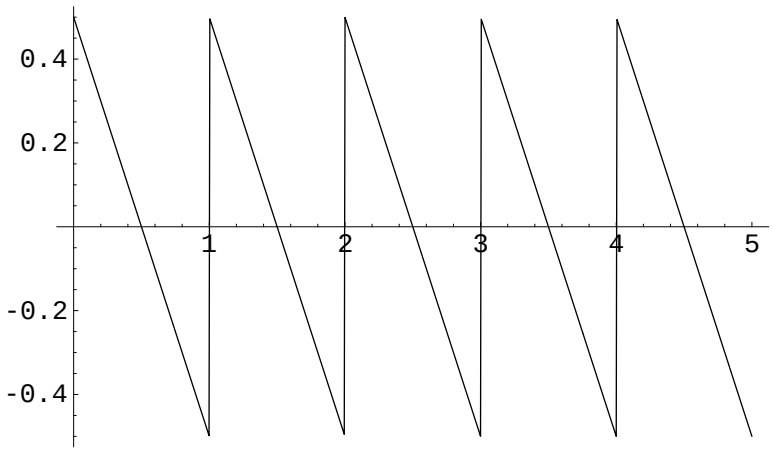

Figura 2.5: La función $\frac{1}{2} - \{t\}$.

Lema 2.3.4. *El área $E_2(t)$, de la región limitada por el arco de curva AB y la poligonal de vértices en los puntos de intersección de las rectas $y =$ entero con el arco de curva AB, verifica*

$$E_2(t) = O(1)\,.$$

Demostración.

$$E_2(t) = \sum_{y=0}^{y_2-1} \left(\frac{\sqrt{t^2+y^2} + \sqrt{t^2+(y+1)^2}}{2} - \int_y^{y+1} \sqrt{y^2+t^2}\, dy \right)$$

$$= -\int_0^{y_2} \sqrt{y^2+t^2}\, dy + \sum_{y=0}^{y_2-1} \frac{\sqrt{y^2+t^2}}{2} + \sum_{y=0}^{y_2-1} \frac{\sqrt{(y+1)^2+t^2}}{2}$$

$$= -\int_0^{y_2} \sqrt{y^2+t^2}\, dy + \frac{t}{2} - \frac{\sqrt{y_2^2+t^2}}{2} + \sum_{y=1}^{y_2} \sqrt{t^2+y^2}\,.$$

Aplicando el teorema 2.3.3 al cálculo de

$$\sum_{y=1}^{y_2} \sqrt{t^2+y^2}\,,$$

siendo, aquí,

$$f(y) = \sqrt{y^2+t^2}\,,\ f'(y) = \frac{y}{\sqrt{t^2+y^2}}\,,\ f''(y) = \frac{t^2}{(t^2+y^2)^{\frac{3}{2}}}\,,$$

tenemos

$$E_2(t) = -\int_0^{y_2} \sqrt{y^2+t^2}\, dy + \frac{t}{2} - \frac{\sqrt{y_2^2+t^2}}{2} + \int_0^{y_2} \sqrt{y^2+t^2}\, dy$$

$$+\frac{\sqrt{y_2^2+t^2}}{2} - \frac{t}{2} + \int_0^{y_2} \sigma(y) \frac{t^2}{(t^2+y^2)^{\frac{3}{2}}}\, dy$$

$$= \int_0^{y_2} \sigma(y) \frac{t^2}{(t^2+y^2)^{\frac{3}{2}}}\, dy \le \int_0^{y_2} \frac{t^2}{(t^2+y^2)^{\frac{3}{2}}}\, dy$$

$$= \frac{1}{t} \int_0^{y_2} \frac{1}{(1+(\frac{y}{t})^2)^{\frac{3}{2}}}\, dy\,.$$

Con el cambio

$$\frac{y}{t} = \operatorname{sh}\alpha\,,$$

$$y = t \operatorname{sh}\alpha\,,$$

$$dy = t \operatorname{ch}\alpha\, d\alpha\,,$$

$$\operatorname{ch}\alpha = \sqrt{1+\left(\frac{y}{t}\right)^2}\,,$$

tenemos

$$\int \frac{1}{(1+(\frac{y}{t})^2)^{\frac{3}{2}}}\,dy = \int \frac{1}{\operatorname{ch}^3\alpha}\,t\operatorname{ch}\alpha\,d\alpha = t\int \frac{1}{\operatorname{ch}^2\alpha}\,d\alpha$$

$$= t\,\frac{\operatorname{sh}\alpha}{\operatorname{ch}\alpha} + K = t\,\frac{y}{\sqrt{t^2+y^2}} + K\,.$$

Y de aquí

$$E_2(t) \le \frac{1}{t}\left[t\,\frac{y}{\sqrt{t^2+y^2}}\right]_{y=0}^{y_2} = \frac{y_2}{\sqrt{t^2+y_2^2}}\,,$$

esto es

$$E_2(t) = O(1)\,.$$

□

Observemos las figuras 2.6 y 2.7. Designamos por $C(t)$ el área de la región limitada por $y=x$, $y=\frac{t^2}{2x}$, $x=\left\lfloor\frac{t}{\sqrt{2}}\right\rfloor$, $x=\left\lceil\frac{t}{\sqrt{2}}\right\rceil$, y

- la recta $y=\left\lfloor\frac{t}{\sqrt{2}}\right\rfloor$, si el punto $\left(\left\lceil\frac{t}{\sqrt{2}}\right\rceil,\left\lfloor\frac{t}{\sqrt{2}}\right\rfloor\right)$ pertenece a la región (2.3).

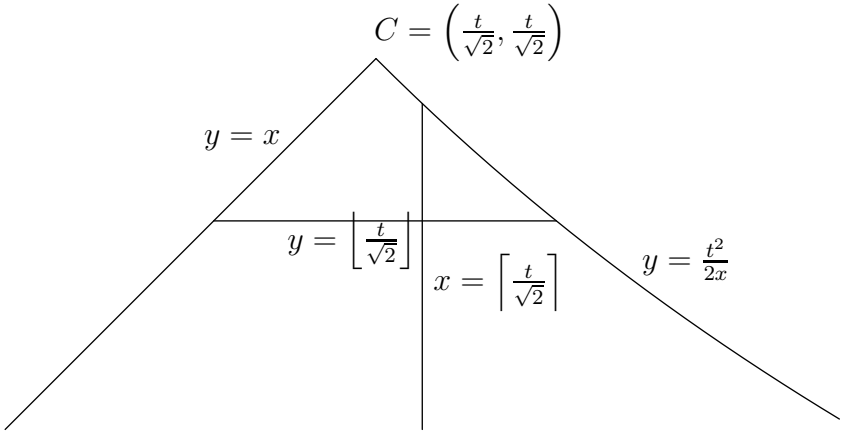

Figura 2.6: La región $C(t)$, cuando el punto $\left(\left\lceil\frac{t}{\sqrt{2}}\right\rceil,\left\lfloor\frac{t}{\sqrt{2}}\right\rfloor\right)$ pertenece a la región (2.3).

- la recta $y=\left\lfloor\frac{t}{\sqrt{2}}\right\rfloor-1$, si el punto $\left(\left\lceil\frac{t}{\sqrt{2}}\right\rceil,\left\lfloor\frac{t}{\sqrt{2}}\right\rfloor\right)$ no pertenece a la región (2.3).

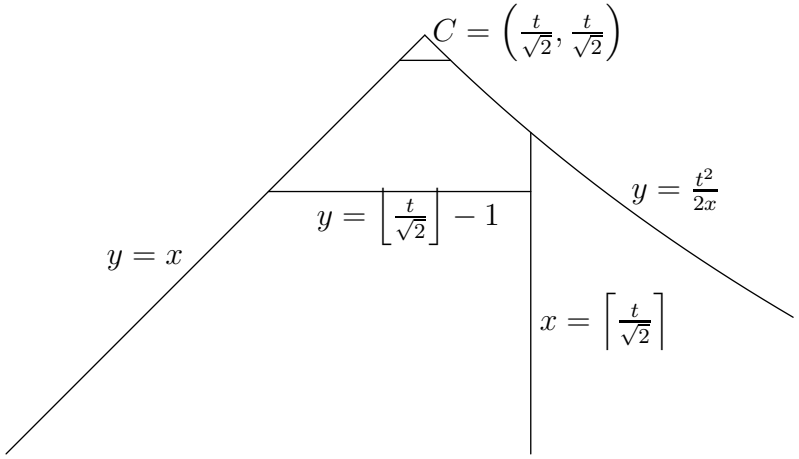

Figura 2.7: La región $C(t)$, cuando el punto $\left(\left\lceil \frac{t}{\sqrt{2}} \right\rceil, \left\lfloor \frac{t}{\sqrt{2}} \right\rfloor\right)$ no pertenece a la región (2.3).

Observemos la figura 2.8. Designamos por $B(t)$ el área de la región limitada por $y = \sqrt{x^2 - t^2}$, $y = \frac{t^2}{2x}$, $y = \left\lfloor \sqrt{\frac{\sqrt{2}-1}{2}}\, t \right\rfloor$ y

- la recta $x = \left\lfloor \sqrt{\frac{\sqrt{2}+1}{2}}\, t \right\rfloor$, si el punto $\left(\left\lfloor \sqrt{\frac{\sqrt{2}+1}{2}}\, t \right\rfloor, \left\lfloor \sqrt{\frac{\sqrt{2}-1}{2}}\, t \right\rfloor\right)$ pertenece a la región (2.3).
- la recta $x = \left\lfloor \sqrt{\frac{\sqrt{2}+1}{2}}\, t \right\rfloor - 1$, si el punto $\left(\left\lfloor \sqrt{\frac{\sqrt{2}+1}{2}}\, t \right\rfloor, \left\lfloor \sqrt{\frac{\sqrt{2}-1}{2}}\, t \right\rfloor\right)$ no pertenece a la región (2.3).

Obviamente las áreas de las regiones $C(t)$ y $B(t)$ son $O(1)$.
Designamos por $R_b(t)$ a la región no sombreada en la figura 2.4.

Lema 2.3.5. *El área $S(t)$, de $R_b(t)$, verifica*

$$S(t) = \frac{1}{2}\left(\frac{t^2}{2(x_3+1)} - \frac{t^2}{2x_2}\right) + \frac{1}{2}\left(\sqrt{t^2+y_2^2} - t\right) - x_2 + \lfloor t \rfloor + \frac{1}{2}\frac{t}{\sqrt{2}} + \sum_{x=x_3+1}^{x_2-1} \left\{\frac{t^2}{2(x+1)}\right\} + \sum_{y=0}^{y_2-1} \left\{\sqrt{t^2+y^2}\right\} + O(1)\,. \tag{2.11}$$

Demostración. Las partes de la región $R_b(t)$ contenidas en las franjas $y = k$, $y = k+1$, con k entero, tienen en su parte izquierda un triángulo de área $\frac{1}{2}$, salvo aquellas franjas que contienen puntos de corte de las rectas $x =$ entero

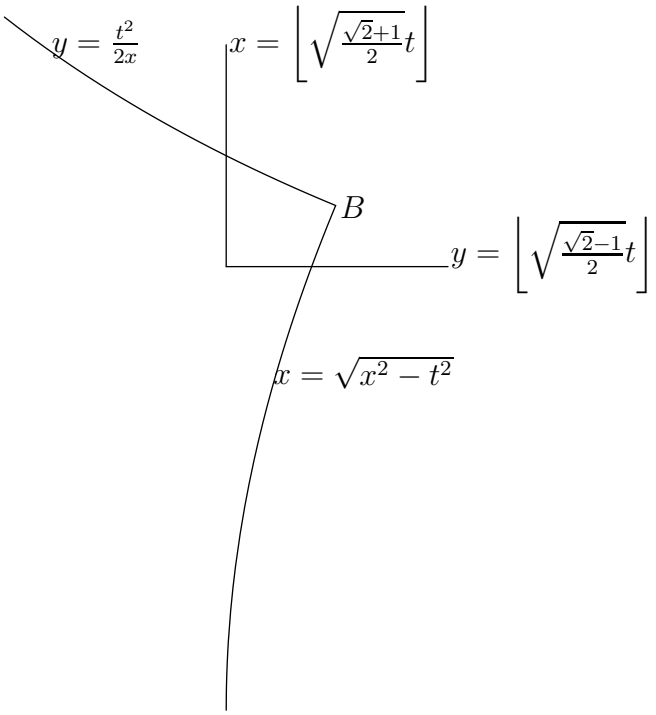

Figura 2.8: La región $B(t)$.

con el arco de curva AB (ver la figura 2.11), y eventualmente las zonas que contienen a los vértices. Su contribución al área de $R_b(t)$ viene reflejada por los tres últimos sumandos de (2.12).

Sea $x_4 = x_2 - 1$, si el punto (x_2, y_2) pertenece a la región (2.3), y $x_4 = x_2 - 2$, si no pertenece.

Observando las figuras 2.9, 2.10 y 2.11 vemos que podemos escribir

$$S(t) + E_1(t) + E_2(t) = C(t) + \sum_{x=x_3+1}^{x_4} \left(\frac{1}{2} \left(\frac{t^2}{2x} - \frac{t^2}{2(x+1)} \right) + \left\{ \frac{t^2}{2(x+1)} \right\} \right)$$

$$+B(t) + \sum_{y=0}^{y_2-1} \left(\frac{1}{2} \left(-\sqrt{t^2+y^2} + \sqrt{t^2+(y+1)^2} \right) + \left\{ \sqrt{t^2+y^2} \right\} \right)$$

$$+\frac{1}{2} \left\lfloor \frac{t}{\sqrt{2}} \right\rfloor - (x_2 - \lfloor t \rfloor) + O(1)\,. \tag{2.12}$$

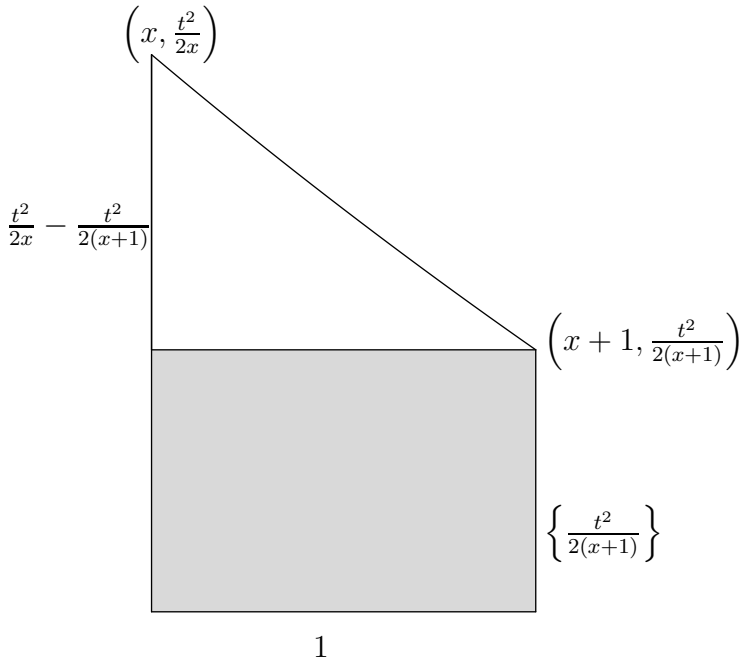

Figura 2.9: Auxiliar en la demostración del lema 2.3.5.

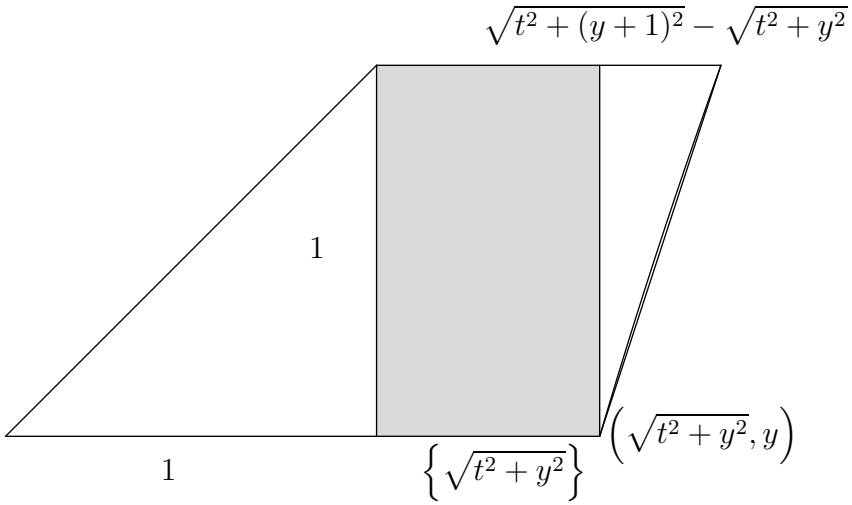

Figura 2.10: Auxiliar en la demostración del lema 2.3.5.

Dado que para $x > \frac{t}{\sqrt{2}}$, el área encerrada en la figura 2.9 es

$$\frac{1}{2}\left(\frac{t^2}{2x} - \frac{t^2}{2(x+1)}\right) + \left\{\frac{t^2}{2(x+1)}\right\} \leq \frac{1}{2}t^2\frac{2}{2x(x+1)} + 1 = \frac{\frac{t}{\sqrt{2}}}{\frac{t}{\sqrt{2}}+1} + 1 < 2\,,$$

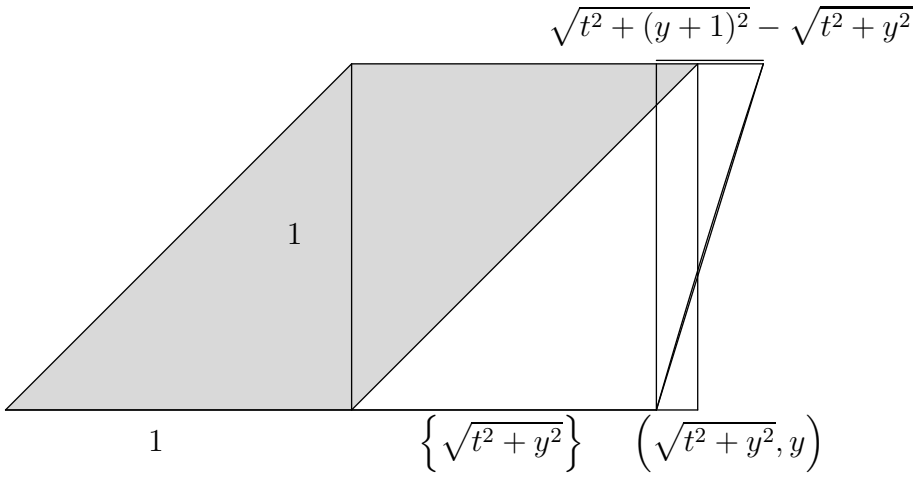

Figura 2.11: Auxiliar en la demostración del lema 2.3.5.

el posible error cometido al cambiar en el primer sumatorio de (2.12), x_4 por x_2-1 es un $O(1)$.

Operando convenientemente y teniendo en cuenta que $E_1(t)$, $E_2(t)$, $C(t)$ y $B(t)$ son $O(1)$ tenemos

$$S(t)=\frac{1}{2}\left(\frac{t^2}{2(x_3+1)}-\frac{t^2}{2x_2}\right)+\frac{1}{2}\left(\sqrt{t^2+y_2^2}-t\right)-x_2+\lfloor t\rfloor+\frac{1}{2}\frac{t}{\sqrt{2}}$$
$$+\sum_{x=x_3+1}^{x_2-1}\left\{\frac{t^2}{2(x+1)}\right\}+\sum_{y=0}^{y_2-1}\left\{\sqrt{t^2+y^2}\right\}+O(1)\,.$$

□

A la vista de la expresión (2.11), vamos a estimar los valores de

$$\sum_{x=x_3+1}^{x_2-1}\left\{\frac{t^2}{2(x+1)}\right\}$$

y de

$$\sum_{y=0}^{y_2-1}\left\{\sqrt{t^2+y^2}\right\}\,.$$

Para ello utilizaremos el siguiente resultado conocido que se puede encontrar en [23, teorema 11.3, pág. 132]:

Teorema 2.3.6. *Si $k\geq 1$ y $f(x)$ es una función con derivada segunda continua en $M\leq x\leq M+m$, que verifica*

$$\frac{1}{A}\leq|f''(x)|\leq\frac{k}{A}\,.$$

Entonces

$$S = \sum_{x=M}^{M+m-1} \{f(x)\} = \frac{1}{2}\, m + O(\Delta)\,,$$

donde

$$\Delta = (k^2 m \log A + kA)A^{-\frac{1}{3}}\,.$$

Aplicando este resultado vamos a establecer los dos lemas siguientes.

Lema 2.3.7.

$$\sum_{x=x_3+1}^{x_2-1} \left\{ \frac{t^2}{2(x+1)} \right\} = \frac{1}{2} \left(\sqrt{\frac{\sqrt{2}+1}{2}} - \frac{1}{\sqrt{2}} \right) t + O(t^{\frac{2}{3}} \log t)\,.$$

Demostración. Para aplicar el teorema 2.3.6 tomamos

$$\begin{gathered} f(x) = \frac{t^2}{2(x+1)}\,, \\ f'(x) = \frac{-t^2}{2(x+1)^2}\,, \\ f''(x) = \frac{t^2}{(x+1)^3}\,, \qquad (2.13) \\ M = x_3 + 1,\ M + m = x_2\,, \end{gathered}$$

luego $m = x_2 - x_3 - 1$. Para $x > 0$, se tiene $f'''(x) < 0$; luego $f''(x)$ es decreciente y para $M \le x \le M + m$ verifica

$$f''\left(\frac{t}{\sqrt{2}}\right) > f''(x_3+1) \ge f''(x) \ge f''(x_2) > f''\left(\sqrt{\frac{1+\sqrt{2}}{2}}\, t\right)\,.$$

Sustituyendo en la expresión (2.13) por los valores correspondientes, tenemos

$$\frac{t^2}{\left(\frac{t}{\sqrt{2}}+1\right)^3} > f''(x) > \frac{t^2}{\left(\sqrt{\frac{1+\sqrt{2}}{2}}\, t + 1\right)^3}\,.$$

Si $t \ge 1$, se tiene $\sqrt{\frac{1+\sqrt{2}}{2}} + \frac{1}{t} < 3$; por tanto

$$\frac{t^2}{\left(\sqrt{\frac{1+\sqrt{2}}{2}}\, t + 1\right)^3} = \frac{1}{t} \left(\frac{1}{\sqrt{\frac{1+\sqrt{2}}{2}} + \frac{1}{t}} \right)^3 > \frac{1}{27t}\,.$$

Además se verifica que

$$\frac{t^2}{\left(\frac{t}{\sqrt{2}}+1\right)^3} = \frac{1}{t}\frac{1}{\frac{1}{\sqrt{2}}+\frac{1}{t}} < \frac{1}{t}\sqrt{2} = \frac{27\sqrt{2}}{27t}\,,$$

lo que nos permite estimar $f''(x)$ mediante

$$\frac{1}{27t} < f''(x) < \frac{27\sqrt{2}}{27t}\,.$$

Para aplicar el teorema 2.3.6 tomamos $A = 27t$, $k = 27\sqrt{2}$,

$$\Delta = \left(\left(27\sqrt{2}\right)^2 (x_2 - x_3 - 1)\log(27t) + 729\sqrt{2}\,t\right)(27t)^{-\frac{1}{3}}\,.$$

Así, el teorema 2.3.6 nos permite asegurar que

$$\sum_{x=x_3+1}^{x_2-1}\left\{\frac{t^2}{2(x+1)}\right\} = \frac{1}{2}(x_2 - x_3 - 1) + O\left(t^{\frac{2}{3}}\log t\right)$$

$$= \frac{1}{2}\left(\sqrt{\frac{\sqrt{2}+1}{2}} - \frac{1}{\sqrt{2}}\right)t + O\left(t^{\frac{2}{3}}\log t\right)\,.$$

□

Lema 2.3.8.

$$\sum_{y=0}^{y_2-1}\left\{\sqrt{t^2+y^2}\right\} = \frac{\sqrt{\frac{\sqrt{2}-1}{2}}}{2}\,t + O\left(t^{\frac{2}{3}}\log t\right)\,.$$

Demostración. Tomamos

$$f(y) = \sqrt{t^2+y^2}\,,$$

$M = 0$ y $m = y_2$. Las dos primeras derivadas de la función $f(y)$ son

$$f'(y) = \frac{y}{\sqrt{t^2+y^2}}$$

y

$$f''(y) = \frac{t^2}{(t^2+y^2)^{\frac{3}{2}}}\,.$$

Además, si $0 \leq y \leq y_2$, es

$$\frac{1}{t} \geq f''(y) \geq \frac{t^2}{(t^2+y_2^2)^{\frac{3}{2}}} > \frac{t^2}{\left(t^2+\sqrt{\frac{\sqrt{2}-1}{2}}t^2\right)^{\frac{3}{2}}}\,.$$

Simplificando, queda

$$\frac{1}{\left(1+\sqrt{\frac{\sqrt{2}-1}{2}}\right)^{\frac{3}{2}}t} < f''(y) \leq \frac{1}{t}\,.$$

Tomando

$$A = \left(1+\sqrt{\frac{\sqrt{2}-1}{2}}\right)^{\frac{3}{2}} t$$

y

$$k = \left(1+\sqrt{\frac{\sqrt{2}-1}{2}}\right)^{\frac{3}{2}} > 1\,,$$

el teorema 2.3.6 afirma que

$$\sum_{y=0}^{y_2-1} \left\{\sqrt{t^2+y^2}\right\} = \frac{1}{2}y_2 + O(\Delta)\,,$$

con

$$\Delta = \left(\left(1+\sqrt{\frac{\sqrt{2}-1}{2}}\right)^3 y_2 \log\left(\left(1+\sqrt{\frac{\sqrt{2}-1}{2}}\right)^{\frac{3}{2}} t\right)\right.$$
$$\left. + \left(1+\sqrt{\frac{\sqrt{2}-1}{2}}\right)^3 t\right)\left(1+\sqrt{\frac{\sqrt{2}-1}{2}}\right)^{\frac{-1}{2}} t^{\frac{-1}{3}}\,.$$

Por tanto tenemos probado que

$$\sum_{y=0}^{y_2-1} \left\{\sqrt{t^2+y^2}\right\} = \frac{\sqrt{\frac{\sqrt{2}-1}{2}}}{2}\,t + O\left(t^{\frac{2}{3}}\log t\right)\,.$$

□

Así, ya podemos abordar lo siguiente:

Demostración del teorema 2.3.1. Sustituyendo, en la expresión (2.11), los sumandos

$$\sum_{x=x_3+1}^{x_2-1}\left\{\frac{t^2}{2(x+1)}\right\} \quad \text{y} \quad \sum_{y=0}^{y_2-1}\left\{\sqrt{t^2+y^2}\right\}$$

por los correspondientes valores obtenidos en los lemas 2.3.7 y 2.3.8, podemos escribir

$$S(t)=\frac{1}{2}\left(\frac{t^2}{2(x_3+1)}-\frac{t^2}{2x_2}\right)+\frac{1}{2}\left(\sqrt{t^2+y_2^2}-t\right)-x_2+\lfloor t\rfloor+\frac{1}{2}\frac{t}{\sqrt{2}}$$

$$+\frac{1}{2}\left(\sqrt{\frac{\sqrt{2}+1}{2}}-\frac{1}{\sqrt{2}}\right)t+\frac{\sqrt{\frac{\sqrt{2}-1}{2}}t}{2}+O\left(t^{\frac{2}{3}}\log t\right).$$

De aquí,

$$S(t)=\frac{1}{2}\left(\frac{t}{\sqrt{2}}-\frac{t}{2\sqrt{\frac{\sqrt{2}+1}{2}}}\right)+\frac{1}{2}\left(\sqrt{1+\frac{\sqrt{2}-1}{2}}-1\right)t-\sqrt{\frac{\sqrt{2}+1}{2}}\,t$$

$$+t+\frac{1}{2\sqrt{2}}\,t+\frac{1}{2}\frac{\sqrt{\sqrt{2}+1}-1}{\sqrt{2}}\,t+\frac{\sqrt{\sqrt{2}-1}}{2\sqrt{2}}\,t+O\left(t^{\frac{2}{3}}\log t\right),$$

y operando convenientemente obtenemos

$$S(t)=\frac{2+\sqrt{2}}{4}\,t+O\left(t^{\frac{2}{3}}\log t\right).$$

Dado que

$$L(Rt)+S(t)=M(Rt),$$

tenemos

$$L(Rt)+\frac{2+\sqrt{2}}{4}\,t=M(Rt)+O\left(t^{\frac{2}{3}}\log t\right).$$

Recordando (2.9), podemos escribir

$$L(Rt)=\frac{\log(1+\sqrt{2})}{2}\,t^2-\frac{2+\sqrt{2}}{4}\,t+O\left(t^{\frac{2}{3}}\log t\right). \tag{2.14}$$

□

Queremos hacer notar que, adaptando a nuestro recinto los resultados obtenidos en [32] a partir de las técnicas desarrolladas por M. N. Huxley [24], es posible conseguir rebajar nuestro exponente $\frac{2}{3}$, en la estimación del error del teorema 2.3.1, estableciendo

$$L(Rt) = \frac{\log(1+\sqrt{2})}{2}\, t^2 - \frac{2+\sqrt{2}}{4}\, t + O\left(t^{\frac{46}{73}} \log^{\frac{315}{146}}(t)\right) .$$

No hemos optado por seguir este camino, muy distinto al utilizado aquí, dado que para nuestros propósitos nos basta con un error $O(t^\alpha)$ con $\alpha < 1$, sin que un exponente menor pueda aportar una mejora a la cota de error del teorema 2.3.10.

En nuestro afán por encontrar una cota del error más precisa para la expresión $\widetilde{P}(n)$ del teorema 2.2.7, buscamos ahora una mejora de la estimación (2.10). Esta es la que aparecerá en el teorema 2.3.10. En su demostración, utilizamos el siguiente resultado conocido, que se puede encontrar en [2, teorema 3.13]:

Teorema 2.3.9. *Para todo $x \geq 1$, se cumple*

$$\left| \sum_{n \leq x} \frac{\mu(n)}{n} \right| \leq 1 ,$$

y la igualdad se verifica únicamente si $x < 2$.

Así, tenemos

Teorema 2.3.10. *El número $Q(n)$ de puntos de coordenadas enteras primas entre sí de la región de la figura 2.3 verifica*

$$Q(n) = \frac{3\log(1+\sqrt{2})}{\pi^2}\, n + O\left(\sqrt{n}\right) .$$

Demostración. Como $L(R2) = 1$ y, si $t < 2$, es $L(Rt) = 0$, aplicando la fórmula de inversión de Möbius tenemos que el número de puntos de la región Rt que tienen coordenadas enteras primas entre sí, $L'(Rt)$ verifica

$$L'(Rt) = \sum_{j=1}^{t} \mu(j) L\left(R\,\frac{t}{j}\right)$$

$$= \sum_{j=1}^{t} \mu(j) \left(\frac{\log(1+\sqrt{2})}{2} \frac{t^2}{j^2} - \frac{2+\sqrt{2}}{4} \frac{t}{j} + O\left(\left(\frac{t}{j}\right)^{\frac{2}{3}} \log\left(\frac{t}{j}\right) \right) \right)$$

$$= \frac{\log\left(1+\sqrt{2}\right)}{2} t^2 \sum_{j=1}^{\infty} \frac{\mu(j)}{j^2} - \frac{\log\left(1+\sqrt{2}\right)}{2} t^2 \sum_{j=t+1}^{\infty} \frac{\mu(j)}{j^2}$$

$$-\frac{2+\sqrt{2}}{4} t \sum_{j=1}^{t} \frac{\mu(j)}{j} + \sum_{j=1}^{t} \mu(j) O\left(\left(\frac{t}{j}\right)^{\frac{2}{3}} \log\left(\frac{t}{j}\right)\right). \qquad (2.15)$$

Por el teorema 2.2.4 tenemos

$$\frac{\log\left(1+\sqrt{2}\right)}{2} t^2 \sum_{j=1}^{\infty} \frac{\mu(j)}{j^2} = \frac{\log\left(1+\sqrt{2}\right)}{2} \frac{6}{\pi^2} t^2 .$$

Aplicando el teorema 2.2.6(b) llegamos a

$$-\frac{\log\left(1+\sqrt{2}\right)}{2} t^2 \sum_{j=t+1}^{\infty} \frac{\mu(j)}{j^2} = -\frac{\log\left(1+\sqrt{2}\right)}{2} t^2 O\left(t^{1-2}\right) = O(t) .$$

Y por el teorema 2.3.9 sabemos

$$\left| -\frac{2+\sqrt{2}}{4} t \sum_{j=1}^{t} \frac{\mu(j)}{j} \right| \leq \frac{2+\sqrt{2}}{4} t .$$

Para acotar el último sumando, sea $\frac{2}{3} < \alpha < 1$. Así,

$$\left| \sum_{j=1}^{t} \mu(j) O\left(\left(\frac{t}{j}\right)^{\frac{2}{3}} \log\left(\frac{t}{j}\right)\right) \right| \leq \sum_{j=1}^{t} \left| O\left(\left(\frac{t}{j}\right)^{\frac{2}{3}} \log\left(\frac{t}{j}\right)\right) \right| ,$$

y al ser $\alpha > \frac{2}{3}$, existe un k tal que

$$\sum_{j=1}^{t} \left| O\left(\left(\frac{t}{j}\right)^{\frac{2}{3}} \log\left(\frac{t}{j}\right)\right) \right| < k \sum_{j=1}^{t} \frac{t^\alpha}{j^\alpha} .$$

Usando el teorema 2.2.6(a) deducimos

$$k \sum_{j=1}^{t} \frac{t^\alpha}{j^\alpha} = k t^\alpha \left(\frac{t^{1-\alpha}}{1-\alpha} + \zeta(\alpha) + O\left(t^{-\alpha}\right) \right)$$

$$= \frac{kt}{1-\alpha} + k\zeta(\alpha) t^\alpha + O(1) = O(t) .$$

Y de aquí

$$L'(Rt) = \frac{\log\left(1+\sqrt{2}\right)}{2} \frac{6}{\pi^2} t^2 + O(t) .$$

Deshaciendo el cambio $n = t^2$ llegamos a

$$Q(n) = \frac{\log\left(1+\sqrt{2}\right)}{2}\frac{6}{\pi^2}\, n + O\left(\sqrt{n}\right) . \tag{2.16}$$

□

Nótese que, para el último sumando de (2.15), aunque en vez del exponente $\frac{2}{3}$ en (2.14), partamos de un exponente menor, como $\frac{46}{73}$, sólo podemos asegurar que este sumando es un $O(t)$. Por lo tanto la estimación (2.16) no se mejora.

Con todo esto, ya estamos en condiciones de establecer una versión más precisa del teorema 2.2.7:

Teorema 2.3.11. *El número total $\widetilde{P}(n)$ de ternas pitagóricas primitivas, considerando como distintas las ternas (a, b, c) y (b, a, c), que hay en el cuadrado $(0, n) \times (0, n)$ es igual a*

$$\widetilde{P}(n) = \frac{4\log\left(1+\sqrt{2}\right)}{\pi^2}\, n + O\left(\sqrt{n}\right) .$$

Demostración. Recordando la igualdad (2.2), tenemos

$$P(n) = \sum_{j\geq 0}(-1)^j Q\left(\frac{n}{2^j}\right)$$

$$= \sum_{j\geq 0}(-1)^j\, \frac{6}{\pi^2}\frac{\log\left(1+\sqrt{2}\right)}{2}\frac{n}{2^j} + \sum_{j\geq 0}(-1)^j O\left(\sqrt{\frac{n}{2^j}}\right)$$

$$= \frac{2\log\left(1+\sqrt{2}\right)}{\pi^2}\, n + O\left(\sqrt{n}\right) .$$

El número total de ternas primitivas $\widetilde{P}(n)$ es el doble de $P(n)$, pues en $\widetilde{P}(n)$ consideramos como distintas la terna (a, b, c) de la terna (b, a, c). Por tanto,

$$\widetilde{P}(n) = \frac{4\log\left(1+\sqrt{2}\right)}{\pi^2}\, n + O\left(\sqrt{n}\right) .$$

□

Tabla 2.1: Valores exactos de $\widetilde{P}(n)$ y $\widetilde{T}(n)$ y sus estimaciones.

n	$\widetilde{P}(n)$	$\frac{4\log(1+\sqrt{2})}{\pi^2}\,n$	$\widetilde{T}(n)$	$\frac{4\log(1+\sqrt{2})}{\pi^2}\,n\log n$
10	2	4	4	8
100	36	36	124	165
1 000	358	357	2 064	2 468
5 000	1 780	1 786	13 228	15 212
10 000	3 576	3 572	28 942	32 900
50 000	17 856	17 860	173 494	193 245
100 000	35 722	35 721	371 720	411 250
500 000	178 600	178 604	2 145 994	2 343 702
1 000 000	357 200	357 207	4 539 566	4 935 001
2 000 000	714 408	714 415	9 574 182	10 365 196
3 000 000	1 071 656	1 071 622	14 795 842	15 982 299
4 000 000	1 428 882	1 428 829	20 138 896	21 720 780
5 000 000	1 786 016	1 786 036	25 572 200	27 549 518
6 000 000	2 143 200	2 143 244	31 077 182	33 450 181
7 000 000	2 500 440	2 500 451	36 641 876	39 410 657
8 000 000	2 857 660	2 857 658	42 258 408	45 422 338
9 000 000	3 214 852	3 214 865	47 919 274	51 478 787
10 000 000	3 572 022	3 572 073	53 619 836	57 575 008
20 000 000	7 144 150	7 144 145	112 191 874	120 101 960
$30\dot{0}00\,000$	10 716 254	10 716 218	172 632 656	184 497 992
40 000 000	14 288 252	14 288 290	234 287 284	250 107 808
50 000 000	17 860 382	17 860 363	296 845 152	316 620 185
60 000 000	21 432 326	21 432 436	360 121 156	383 851 817
70 000 000	25 004 490	25 004 508	423 995 102	451 681 581
80 000 000	28 576 662	28 576 581	488 382 804	520 023 392
90 000 000	32 148 616	32 148 653	553 217 166	588 812 882
100 000 000	35 720 710	35 720 726	618 449 498	658 000 090
200 000 000	71 441 356	71 441 452	1 286 418 190	1 365 519 621
300 000 000	107 162 112	107 162 178	1 973 076 850	2 091 729 956
400 000 000	142 882 968	142 882 904	2 671 874 926	2 830 078 125
500 000 000	178 603 536	178 603 630	3 379 697 288	3 577 451 904
600 000 000	214 324 350	214 324 356	4 094 712 042	4 332 018 235
700 000 000	250 045 106	250 045 082	4 815 708 888	5 092 565 894
800 000 000	285 765 804	285 765 808	5 541 827 134	5 858 234 014
900 000 000	321 486 520	321 486 534	6 272 419 600	6 628 378 925
1 000 000 000	357 207 278	357 207 260	7 006 991 998	7 402 501 013

2.4. Valores exactos de $\widetilde{P}(n)$ y $\widetilde{T}(n)$

Hemos calculado los números exactos $\widetilde{P}(n)$ y $\widetilde{T}(n)$ para algunos valores de n, y comparado estos valores con las estimaciones (redondeando al entero más próximo) dadas por los teoremas 2.2.7 (ó 2.3.11) y 2.2.8. Esto se muestra en la tabla 2.1.

Podemos ver que la precisión de las estimaciones para $\widetilde{P}(n)$ dadas por $\frac{4\log(1+\sqrt{2})}{\pi^2}\,n$ son excelentes, siendo unas veces el valor estimado superior al real, como ocurre para $n = 900\,000\,000$, y en otras inferior, como para $n = 1\,000\,000\,000$. Los valores correspondientes parecen ser mucho más ajustados que lo sugerido por el término de error $O(\sqrt{n})$ que aparece en el teorema 2.3.11. Por esto, conjeturamos que el teorema se puede mejorar encontrando menores cotas asintóticas para el término del error.

Capítulo 3

La función M

3.1. Introducción

Recordemos que se conoce como la función de Möbius $\mu(n)$ a la función

$$\mu(n) := \begin{cases} 1 & \text{si } n = 1\,, \\ (-1)^k & \text{si } n \text{ es producto de } k \text{ primos distintos,} \\ 0 & \text{si } n \text{ tiene un divisor primo elevado al cuadrado.} \end{cases}$$

Para cada número real $x \geq 0$ podemos definir la función $M(x)$, suma de la función de Möbius, mediante

$$M(x) := \sum_{n \leq x} \mu(n)\,.$$

Así $M(1) = 1,\ M(2) = 0,\ M(3) = -1,\ \ldots,\ M(100) = 1,\ \ldots$

El comportamiento de $M(x)$ es bastante errático y difícil de estudiar. En [29], J. E. Littlewood probó el siguiente resultado:

Teorema 3.1.1. *La conjetura de Riemann es equivalente a la afirmación de que para cada $\varepsilon > 0$ la función $M(x)x^{-\frac{1}{2}-\varepsilon}$ tiende a cero cuando $x \to \infty$.*

Como hace E. C. Titchmarsh, en [41], ese resultado a menudo se enuncia de la siguiente forma, también equivalente:

$$M(x) = O\left(x^{\frac{1}{2}+\varepsilon}\right) \quad \text{para todo } \varepsilon > 0\,.$$

En 1897, F. Mertens publicó el artículo [30], donde da una tabla de los valores de $M(n)$ para $1 \leq n \leq 10000$. Basándose en ella, conjetura que, para $x > 1$,

$$|M(x)| < \sqrt{x}\,.$$

Esta conjetura fue refutada, en 1985, por A. M. Odlyzko y H. J. J. te Riele en [35], aunque de momento no se conoce un contraejemplo explícito. Para todos los valores calculados hasta entonces, se verificaba que $|M(n)| < 0.6\sqrt{n}$. Ellos creen que no se encontrarán contraejemplos para valores de n menores que 10^{20}.

Nuestro propósito es dar algunas fórmulas recursivas que pueden ser útiles para el cálculo efectivo de $M(x)$. En particular, la fórmula (3.10), consecuencia directa del teorema 3.4.3.

3.2. Fórmulas en las que sólo interviene M

Comenzamos recordando una conocida propiedad de la función de Möbius.

Lema 3.2.1. *La función de Möbius verifica que*

$$\sum_{d|n} \mu(d) = \begin{cases} 1 & si \quad n = 1\,, \\ 0 & si \quad n > 1\,. \end{cases} \tag{3.1}$$

Demostración. Si $n = \prod_{j=1}^{k} p_j^{\alpha_j} > 1$ entonces

$$\sum_{d|n} \mu(d) = \binom{k}{0} - \binom{k}{1} + \cdots + (-1)^k \binom{k}{k} = (1-1)^k = 0\,.$$

Si $n = 1$, $\mu(1) = 1$. □

Este lema nos permite probar una fórmula, también conocida, que nos relaciona el valor de $M(n)$ con valores de $M(m)$, para m menores que n.

Proposición 3.2.2.

$$1 = \sum_{a=1}^{n} M\left(\frac{n}{a}\right)\,. \tag{3.2}$$

Demostración. Por la definición de $M(x) = \sum_{n\le x} \mu(n)$, podemos escribir

$$\sum_{a=1}^{\lfloor x\rfloor} M\left(\frac{x}{a}\right) = \sum_{a=1}^{\lfloor x\rfloor} \sum_{b=1}^{\lfloor \frac{x}{a}\rfloor} \mu(b)\,.$$

Si $ab = k$ entonces $a|k$ y además, al variar los valores de a y b, k toma los valores $1, 2, \ldots, \lfloor x\rfloor$. Así, podemos escribir la igualdad

$$\sum_{a=1}^{\lfloor x\rfloor} \sum_{b=1}^{\lfloor \frac{x}{a}\rfloor} \mu(b) = \sum_{1\le k\le \lfloor x\rfloor} \sum_{a|k} \mu(a)\,.$$

Aplicando el lema 3.2.1 tenemos

$$\sum_{a=1}^{n} M\left(\frac{n}{a}\right) = 1\,.$$

□

Despejando $M(n)$ en (3.2) tenemos una primera fórmula recursiva para el cálculo de $M(n)$:

$$M(n) = 1 - \sum_{a=2}^{n} M\left(\frac{n}{a}\right)\,. \tag{3.3}$$

Esta fórmula ha sido utilizada por M. Deléglise y J. Rivat en [11] para calcular

$$M(10^{16}) = -3195437\,.$$

En (3.3) intervienen n sumandos. En la siguiente proposición reducimos el número de sumandos a $\left\lfloor \frac{n-1}{2} \right\rfloor$.

Proposición 3.2.3. *Si $n \geq 3$ entonces*

$$M(n) = -\sum_{a=1}^{\left\lfloor \frac{n-1}{2} \right\rfloor} M\left(\frac{n}{2a+1}\right)\,.$$

Demostración. Si $n = 2m$ con $m > 1$, aplicando sucesivamente las fórmulas (3.3) y (3.2), podemos escribir

$$M(2m) = 1 - \sum_{a=2}^{2m} M\left(\frac{2m}{a}\right) = \sum_{a=1}^{m} M\left(\frac{m}{a}\right) - \sum_{a=2}^{2m} M\left(\frac{2m}{a}\right)$$

$$= -\sum_{a=1}^{m-1} M\left(\frac{2m}{2a+1}\right) = -\sum_{a=1}^{\left\lfloor \frac{n-1}{2} \right\rfloor} M\left(\frac{n}{2a+1}\right)\,.$$

Para probar el caso $n = 2m+1$ empezamos por observar que el máximo resto que se puede obtener al dividir m por a es $a-1$. Así, tenemos

$$\frac{a-1}{a} + \frac{1}{2a} = \frac{2a-2+1}{2a} = \frac{2a-1}{2a} < 1\,,$$

y por tanto

$$M\left(\frac{2m+1}{2a}\right) = M\left(\frac{m}{a} + \frac{1}{2a}\right) = M\left(\frac{m}{a}\right)\,.$$

Recordando que la proposición 3.2.2 establece que $1 = \sum_{a=1}^{n} M\left(\frac{n}{a}\right)$, podemos escribir

$$M(2m+1) = 1 - \sum_{a=2}^{2m+1} M\left(\frac{2m+1}{a}\right)$$

$$= \sum_{a=1}^{m} M\left(\frac{m}{a}\right) - \sum_{a=2}^{2m+1} M\left(\frac{2m+1}{a}\right) = -\sum_{a=1}^{m} M\left(\frac{2m+1}{2a+1}\right)$$

$$= -\sum_{a=1}^{\lfloor\frac{n-1}{2}\rfloor} M\left(\frac{n}{2a+1}\right).$$

□

3.3. Fórmulas en las que sólo interviene μ

En la proposición siguiente, expresamos $M(n)$ como suma de $\lfloor\frac{n}{3}\rfloor$ sumandos en los que sólo intervienen las funciones μ y parte entera.

Proposición 3.3.1. *Si $n \geq 3$ entonces*

$$M(n) = -\sum_{k=1}^{\lfloor\frac{n}{3}\rfloor} \left\lfloor \frac{n-k}{2k} \right\rfloor \mu(k)\,.$$

Demostración. Por la proposición 3.2.3 se tiene

$$M(n) = -\sum_{a=1}^{\lfloor\frac{n-1}{2}\rfloor} M\left(\frac{n}{2a+1}\right).$$

El mayor valor que alcanza $\lfloor\frac{n}{2a+1}\rfloor$ es $\lfloor\frac{n}{3}\rfloor$.
La expresión $\lfloor\frac{n}{2a+1}\rfloor$ toma el valor k si

$$k \leq \frac{n}{2a+1} < k+1\,,$$

$$2ak + k \leq n < 2a(k+1) + k + 1\,,$$

$$\frac{n-(k+1)}{2(k+1)} < a \leq \frac{n-k}{2k}\,,$$

o sea para $\lfloor\frac{n-k}{2k}\rfloor - \left\lfloor\frac{n-(k+1)}{2(k+1)}\right\rfloor$ valores de a.

Por tanto

$$M(n) = -\sum_{k=1}^{\lfloor \frac{n}{3} \rfloor} \left(\left\lfloor \frac{n-k}{2k} \right\rfloor - \left\lfloor \frac{n-(k+1)}{2(k+1)} \right\rfloor \right) M(k)$$

$$= -\left(\left(\left\lfloor \frac{n-1}{2} \right\rfloor - \left\lfloor \frac{n-2}{2\cdot 2} \right\rfloor \right) M(1) + \left(\left\lfloor \frac{n-2}{2\cdot 2} \right\rfloor - \left\lfloor \frac{n-3}{2\cdot 3} \right\rfloor \right) M(2) + \cdots \right.$$
$$\left. + \left(\left\lfloor \frac{n-\left\lfloor \frac{n}{3} \right\rfloor}{2\left\lfloor \frac{n}{3} \right\rfloor} \right\rfloor - \left\lfloor \frac{n-\left\lfloor \frac{n}{3} \right\rfloor - 1}{2\left(\left\lfloor \frac{n}{3} \right\rfloor + 1\right)} \right\rfloor \right) M\left(\left\lfloor \frac{n}{3} \right\rfloor \right) \right)$$
$$= -\left(\left\lfloor \frac{n-1}{2} \right\rfloor \mu(1) + \left\lfloor \frac{n-2}{2\cdot 2} \right\rfloor \mu(2) + \left\lfloor \frac{n-3}{2\cdot 3} \right\rfloor \mu(3) + \cdots \right.$$
$$\left. + \left\lfloor \frac{n-\left\lfloor \frac{n}{3} \right\rfloor}{2\left\lfloor \frac{n}{3} \right\rfloor} \right\rfloor \mu\left(\left\lfloor \frac{n}{3} \right\rfloor \right) - \left\lfloor \frac{n-\left\lfloor \frac{n}{3} \right\rfloor - 1}{2\left(\left\lfloor \frac{n}{3} \right\rfloor + 1\right)} \right\rfloor M\left(\left\lfloor \frac{n}{3} \right\rfloor \right) \right) .$$

Observemos ahora que

$$\frac{n-\left\lfloor \frac{n}{3} \right\rfloor - 1}{2\left(\left\lfloor \frac{n}{3} \right\rfloor + 1\right)} = \begin{cases} \frac{3m-m-1}{2m+2} = \frac{2m-1}{2m+2} < 1 & \text{si} \quad n = 3m\,, \\ \frac{3m+1-m-1}{2m+2} < 1 & \text{si} \quad n = 3m+1\,, \\ \frac{3m+2-m-1}{2m+2} = \frac{2m+1}{2m+2} < 1 & \text{si} \quad n = 3m+2\,, \end{cases}$$

luego

$$\left\lfloor \frac{n-\left\lfloor \frac{n}{3} \right\rfloor - 1}{2\left(\left\lfloor \frac{n}{3} \right\rfloor + 1\right)} \right\rfloor = 0\,.$$

Lo que nos permite afirmar que

$$M(n) = -\sum_{k=1}^{\lfloor \frac{n}{3} \rfloor} \left\lfloor \frac{n-k}{2k} \right\rfloor \mu(k)\,.$$

□

El siguiente resultado, ya conocido (ver [2, teorema 3.12, pág. 83], aunque la demostración que damos aquí es distinta y, quizás, nueva), nos liga el valor de $\mu(n)$ con los valores de $\mu(m)$ para $1 \leq m < n$:

Proposición 3.3.2.

$$1 = \sum_{k=1}^{n} \left\lfloor \frac{n}{k} \right\rfloor \mu(k)\,.$$

Demostración. Por la proposición 3.2.2 sabemos que $1 = \sum_{a=1}^{n} M\left(\frac{n}{a}\right)$.

Se verifica $\left\lfloor \frac{n}{a} \right\rfloor = k$ si y sólo si

$$k \leq \frac{n}{a} < k+1\,,$$

que multiplicando por a se transforma en

$$ka \leq n < ka + a\,,$$

siendo esta última expresión equivalente a

$$\frac{n}{k+1} < a \leq \frac{n}{k}\,,$$

luego $M\left(\frac{n}{a}\right) = M\left(\left\lfloor \frac{n}{a} \right\rfloor\right) = M(k)$ para $\left\lfloor \frac{n}{k} \right\rfloor - \left\lfloor \frac{n}{k+1} \right\rfloor$ valores de a.

Por tanto

$$1 = \sum_{a=1}^{n} M\left(\frac{n}{a}\right) = \sum_{a=1}^{n} \left(\left\lfloor \frac{n}{k} \right\rfloor - \left\lfloor \frac{n}{k+1} \right\rfloor \right) M(k)$$

$$= \left(\left\lfloor \frac{n}{1} \right\rfloor - \left\lfloor \frac{n}{2} \right\rfloor \right) M(1) + \left(\left\lfloor \frac{n}{2} \right\rfloor - \left\lfloor \frac{n}{3} \right\rfloor \right) M(2) + \cdots + \left(\left\lfloor \frac{n}{n} \right\rfloor - \left\lfloor \frac{n}{n+1} \right\rfloor \right) M(n)$$

$$= \left\lfloor \frac{n}{1} \right\rfloor + \left\lfloor \frac{n}{2} \right\rfloor (M(2) - M(1)) + \cdots + \left\lfloor \frac{n}{n} \right\rfloor (M(n) - M(n-1)) - \left\lfloor \frac{n}{n+1} \right\rfloor M(n)$$

$$= \left\lfloor \frac{n}{1} \right\rfloor \mu(1) + \left\lfloor \frac{n}{2} \right\rfloor \mu(2) + \cdots + \left\lfloor \frac{n}{n} \right\rfloor \mu(n)$$

$$= \sum_{k=1}^{n} \left\lfloor \frac{n}{k} \right\rfloor \mu(k)\,.$$

□

En la fórmula dada por la proposición 3.3.2, intervienen n sumandos. La proposición siguiente nos permite reducir el número de sumandos a $\lfloor \frac{n}{3} \rfloor$.

Proposición 3.3.3.

$$1 = \sum_{k=1}^{\lfloor \frac{n}{3} \rfloor} \left\lfloor \frac{n}{3k} \right\rfloor \mu(k)\,.$$

Demostración. Si $n = 3m$, por la proposición 3.3.2 tenemos

$$1 = \sum_{k=1}^{m} \left\lfloor \frac{m}{k} \right\rfloor \mu(k) = \sum_{k=1}^{\frac{n}{3}} \left\lfloor \frac{3m}{3k} \right\rfloor \mu(k) = \sum_{k=1}^{\lfloor \frac{n}{3} \rfloor} \left\lfloor \frac{n}{3k} \right\rfloor \mu(k)\,.$$

Si $n = 3m + 1$,

$$\sum_{k=1}^{\lfloor \frac{n}{3} \rfloor} \left\lfloor \frac{n}{3k} \right\rfloor \mu(k) = \sum_{k=1}^{m} \left\lfloor \frac{3m+1}{3k} \right\rfloor \mu(k) = \sum_{k=1}^{m} \left\lfloor \frac{m}{k} \right\rfloor \mu(k) = 1\,,$$

pues, al ser

$$\left\lfloor \frac{3m+1}{3k} \right\rfloor = \left\lfloor \frac{m}{k} + \frac{1}{3k} \right\rfloor\,,$$

el mayor resto posible al dividir m entre k es $k-1$, y como

$$\frac{k-1}{k} + \frac{1}{3k} = \frac{3k-2}{3k} < 1$$

se verifica que

$$\left\lfloor \frac{3m+1}{3k} \right\rfloor = \left\lfloor \frac{m}{k} \right\rfloor\,.$$

Si $n = 3m + 2$

$$\left\lfloor \frac{3m+2}{3k} \right\rfloor = \left\lfloor \frac{m}{k} + \frac{2}{3k} \right\rfloor\,,$$

$$\frac{k-1}{k} + \frac{2}{3k} = \frac{3k-1}{3k} < 1\,,$$

luego

$$\left\lfloor \frac{3m+2}{3k} \right\rfloor = \left\lfloor \frac{m}{k} \right\rfloor\,,$$

y por tanto

$$\sum_{k=1}^{\lfloor \frac{n}{3} \rfloor} \left\lfloor \frac{n}{3k} \right\rfloor \mu(k) = \sum_{k=1}^{m} \left\lfloor \frac{3m+2}{3k} \right\rfloor \mu(k) = \sum_{k=1}^{m} \left\lfloor \frac{m}{k} \right\rfloor \mu(k) = 1\,.$$

□

Proposición 3.3.4.

$$2M(n) + 3 = \sum_{k=1}^{\lfloor \frac{n}{3} \rfloor} \left(3 \left\lfloor \frac{n}{3k} \right\rfloor - 2 \left\lfloor \frac{n}{2k} - \frac{1}{2} \right\rfloor \right) \mu(k)\,. \tag{3.4}$$

Demostración. Por la proposición 3.3.1 sabemos que

$$M(n) = -\sum_{k=1}^{\lfloor \frac{n}{3} \rfloor} \left\lfloor \frac{n-k}{2k} \right\rfloor \mu(k)$$

y por la proposición 3.3.3 es

$$1 = \sum_{k=1}^{\lfloor \frac{n}{3} \rfloor} \left\lfloor \frac{n}{3k} \right\rfloor \mu(k)\,,$$

luego

$$2M(n) + 3 = \sum_{k=1}^{\lfloor \frac{n}{3} \rfloor} \left(3 \left\lfloor \frac{n}{3k} \right\rfloor - 2 \left\lfloor \frac{n}{2k} - \frac{1}{2} \right\rfloor \right) \mu(k)\,.$$

□

Designamos por $g(n,k)$ a los coeficientes de $\mu(k)$ en la ecuación (3.4). La proposición siguiente da una forma alternativa de calcular $g(n,k)$.

Proposición 3.3.5. *Sean $k > 0$, $n \geq 0$,*

$$g(n,k) = 3 \left\lfloor \frac{n}{3k} \right\rfloor - 2 \left\lfloor \frac{n}{2k} - \frac{1}{2} \right\rfloor$$

y tomemos n_0 tal que

$$n \equiv n_0 \mod 6k, \quad 0 \leq n_0 < 6k\,.$$

Entonces

$$g(n,k) = \begin{cases} 2 & si \quad 0 \leq n_0 < k\,, \\ 0 & si \quad k \leq n_0 < 3k\,, \\ 1 & si \quad 3k \leq n_0 < 5k\,, \\ -1 & si \quad 5k \leq n_0 < 6k\,. \end{cases}$$

Demostración. Sea $n = n_0 + n_1 6k$, con $0 \leq n_0 < 6k$. Entonces

$$g(n,k) = 3 \left\lfloor \frac{n_0 + n_1 6k}{3k} \right\rfloor - 2 \left\lfloor \frac{n_0 + n_1 6k - k}{2k} \right\rfloor .$$

Así,

$$\begin{array}{lll} \text{si} & 0 \leq n_0 < k, & g(n,k) = 6n_1 - 2 \left\lfloor \frac{6k(n_1-1)}{2k} + \frac{5k+n_0}{2k} \right\rfloor = 2\,; \\ \text{si} & k \leq n_0 < 3k, & g(n,k) = 6n_1 - 6n_1 = 0\,; \\ \text{si} & 3k \leq n_0 < 5k, & g(n,k) = 3 + 6n_1 - 6n_1 - 2 = 1\,; \\ \text{si} & 5k \leq n_0 < 6k, & g(n,k) = 3 + 6n_1 - 6n_1 - 4 = -1\,. \end{array}$$

□

Esta proposición nos permite enunciar la proposición 3.3.4 en la siguiente forma:

$$2M(n) + 3 = \sum_{k=1}^{\lfloor \frac{n}{3} \rfloor} g(n,k)\mu(k)\,. \tag{3.5}$$

3.4. Fórmulas en las que intervienen las funciones M y μ

En la proposición siguiente estudiamos la constancia de $g(n,k)$ en determinados intervalos.

Proposición 3.4.1. *Sean a y n números enteros positivos, con $a < n$. Al variar el número entero k en el intervalo $\frac{n}{a+1} < k \leq \frac{n}{a}$, el valor de $g(n,k)$ permanece constante. Este valor sólo depende del resto de a módulo 6.*

Demostración. Sea $a = a_0 + 6a_1$ con $0 \leq a_0 < 6$. Si

$$\frac{n}{a+1} < k \leq \frac{n}{a}\,,$$

entonces

$$ka \leq n < k(a+1)\,. \tag{3.6}$$

Sustituyendo el valor de a tenemos

$$ka_0 + 6ka_1 \leq n < k(a_0 + 6a_1 + 1)\,,$$

por lo que existe un n_0 tal que $n = n_0 + 6ka_1$, con $0 \leq n_0 < 6k$. Por tanto

$$ka_0 + 6ka_1 \leq n_0 + 6ka_1 < ka_0 + k + 6ka_1\,.$$

Restando $6ka_1$ a los miembros de esta desigualdad tenemos

$$ka_0 \leq n_0 < ka_0 + k\,.$$

Por la proposición 3.3.5, $g(n,k)$ es constante para estos valores de n_0, luego $g(n,k)$ es constante en

$$\frac{n}{a+1} < k \leq \frac{n}{a}\,,$$

y su valor sólo depende de a_0. □

Como consecuencia de la proposición 3.4.1, podemos definir

$$h(a) = g(n,k) \quad \text{para} \quad \frac{n}{a+1} < k \leq \frac{n}{a}\,.$$

Los valores de $h(a)$ son

$$\begin{array}{llll} \text{si} & a \equiv 0 & \text{mód } 6, & h(a) = 2\,, \\ \text{si} & a \equiv 1 & \text{mód } 6, & h(a) = 0\,, \\ \text{si} & a \equiv 2 & \text{mód } 6, & h(a) = 0\,, \\ \text{si} & a \equiv 3 & \text{mód } 6, & h(a) = 1\,, \\ \text{si} & a \equiv 4 & \text{mód } 6, & h(a) = 1\,, \\ \text{si} & a \equiv 5 & \text{mód } 6, & h(a) = -1\,. \end{array} \tag{3.7}$$

Partiremos ahora el sumatorio de (3.5) en dos partes. Dado un número b, la primera parte estará formada por el sumatorio de los $\lfloor \frac{n}{b+1} \rfloor$ primeros términos del sumatorio de (3.5), la segunda parte estará formada por b sumandos en los que intervienen valores de M.

Proposición 3.4.2. *Si* $3 \leq b \leq n-1$ *entonces*

$$2M(n)+3 = \sum_{k=1}^{\lfloor \frac{n}{b+1} \rfloor} g(n,k)\mu(k) + \sum_{a=3}^{b} h(a)\left(M\left(\frac{n}{a}\right) - M\left(\frac{n}{a+1}\right)\right). \quad (3.8)$$

Demostración. Por la proposición 3.4.1,

$$2M(n)+3 = \sum_{k=1}^{\lfloor \frac{n}{3} \rfloor} g(n,k)\mu(k) = \sum_{k=1}^{\lfloor \frac{n}{b+1} \rfloor} g(n,k)\mu(k) + \sum_{a=3}^{b} \sum_{k=\lfloor \frac{n}{a+1} \rfloor + 1}^{\lfloor \frac{n}{a} \rfloor} g(n,k)\mu(k)$$

$$= \sum_{k=1}^{\lfloor \frac{n}{b+1} \rfloor} g(n,k)\mu(k) + \sum_{a=3}^{b} h(a) \sum_{k=\lfloor \frac{n}{a+1} \rfloor + 1}^{\lfloor \frac{n}{a} \rfloor} \mu(k)$$

$$= \sum_{k=1}^{\lfloor \frac{n}{b+1} \rfloor} g(n,k)\mu(k) + \sum_{a=3}^{b} h(a)\left(M\left(\frac{n}{a}\right) - M\left(\frac{n}{a+1}\right)\right).$$

□

Partiendo el segundo sumatorio de la parte derecha de (3.8) tenemos el siguiente

Teorema 3.4.3. *Sean* n, b *y* c *tres números enteros no negativos tales que* $9 \leq b \leq n-1$ *y* $c \leq \left\lfloor \frac{b-7}{6} \right\rfloor$. *Se verifica que*

$$2M(n)+3 = \sum_{k=1}^{\lfloor \frac{n}{b+1} \rfloor} g(n,k)\mu(k)$$
$$+ \sum_{\lambda=0}^{c}\left(M\left(\frac{n}{3+6\lambda}\right) - 2M\left(\frac{n}{5+6\lambda}\right) + 3M\left(\frac{n}{6+6\lambda}\right) - 2M\left(\frac{n}{7+6\lambda}\right)\right)$$
$$+ \sum_{a=6c+9}^{b} h(a) \sum_{k=\lfloor \frac{n}{a+1} \rfloor + 1}^{\lfloor \frac{n}{a} \rfloor} \mu(k). \quad (3.9)$$

Demostración. Por la proposición 3.4.2 sabemos que

$$2M(n)+3=\sum_{k=1}^{\lfloor \frac{n}{b+1}\rfloor} g(n,k)\mu(k)+\sum_{a=3}^{b} h(a)\left(M\left(\frac{n}{a}\right)-M\left(\frac{n}{a+1}\right)\right).$$

Desarrollando el segundo sumando podemos escribir

$$2M(n)+3=\sum_{k=1}^{\lfloor \frac{n}{b+1}\rfloor} g(n,k)\mu(k)+h(3)M\left(\frac{n}{3}\right)-h(3)M\left(\frac{n}{4}\right)$$

$$+h(4)M\left(\frac{n}{4}\right)-h(4)M\left(\frac{n}{5}\right)+h(5)M\left(\frac{n}{5}\right)-h(5)M\left(\frac{n}{6}\right)$$

$$+h(6)M\left(\frac{n}{6}\right)-h(6)M\left(\frac{n}{7}\right)+h(7)M\left(\frac{n}{7}\right)-h(7)M\left(\frac{n}{8}\right)$$

$$+h(8)M\left(\frac{n}{8}\right)-h(8)M\left(\frac{n}{9}\right)+\cdots$$

$$+h(6c+8)M\left(\frac{n}{6c+8}\right)-h(6c+8)M\left(\frac{n}{6c+9}\right)$$

$$+\sum_{a=6c+9}^{b} h(a)\left(M\left(\frac{n}{a}\right)-M\left(\frac{n}{a+1}\right)\right).$$

Sustituyendo los valores de $h(a)$ tenemos

$$2M(n)+3=\sum_{k=1}^{\lfloor \frac{n}{b+1}\rfloor} g(n,k)\mu(k)$$

$$+\sum_{\lambda=0}^{c}\left(M\left(\frac{n}{3+6\lambda}\right)-2M\left(\frac{n}{5+6\lambda}\right)+3M\left(\frac{n}{6+6\lambda}\right)-2M\left(\frac{n}{7+6\lambda}\right)\right)$$

$$+\sum_{a=6c+9}^{b} h(a)\sum_{k=\lfloor \frac{n}{a+1}\rfloor+1}^{\lfloor \frac{n}{a}\rfloor}\mu(k).$$

□

Despejando $M(n)$ en la expresión (3.9), tenemos la fórmula recursiva

$$M(n) = \frac{1}{2}\left(\sum_{k=1}^{\lfloor \frac{n}{b+1} \rfloor} g(n,k)\mu(k) \right.$$
$$+ \sum_{\lambda=0}^{c}\left(M\left(\frac{n}{3+6\lambda}\right) - 2M\left(\frac{n}{5+6\lambda}\right) + 3M\left(\frac{n}{6+6\lambda}\right) - 2M\left(\frac{n}{7+6\lambda}\right)\right)$$
$$\left. + \sum_{a=6c+9}^{b} h(a) \sum_{k=\lfloor \frac{n}{a+1} \rfloor + 1}^{\lfloor \frac{n}{a} \rfloor} \mu(k) - 3 \right) . \quad (3.10)$$

Una acertada elección de los parámetros b y c nos permitirá obtener buenos tiempos de ejecución, siempre dependientes de la implementación que se haga. Computacionalmente hablando, la fórmula (3.10) parece prometedora, pues pruebas preliminares, con una implementación directa, nos han permitido comprobar que el tiempo de ejecución que requiere es mucho menor que el correspondiente a la fórmula (3.3), la utilizada por M. Deléglise y J. Rivat [11] para evaluar $M(10^{16})$. En estas pruebas, una buena elección ha sido tomar valores de b del orden de $n^{\frac{2}{5}}$, y valores de c del orden de $n^{\frac{1}{5}}$.

3.5. La función $H(n,m)$. Periodicidad

En esta sección vamos a analizar algunas propiedades de la función $H(n,m)$ definida por el sumatorio

$$H(n,m) := \sum_{k=1}^{m} g(n,k)\mu(k) .$$

Además, utilizaremos la siguiente notación:

$$C_m := 6 \cdot (\text{mcm}\{1,2,\ldots,m\}) .$$

En primer lugar vamos a ver que fijado un valor m de la segunda variable, la función es periódica de periodo C_m.

Proposición 3.5.1. *Para todo número natural t se verifica*

$$H(n + tC_m, m) = H(n,m) .$$

Demostración. Como $g(n + 6\dot{k}, k) = g(n,k)$ para $k = 1,2,\ldots,m$, se tiene que $g(n + \dot{C}_m, k) = g(n,k)$. □

La proposición siguiente nos da el valor de $H(n,m)$ en función de $M(m)$.

Proposición 3.5.2. *Se verifica*

$$\begin{aligned}
&H(0+\dot{C}_m, m) = 2M(m)\,,\\
&H(1+\dot{C}_m, m) = 2M(m) - 2\,,\\
&H(2+\dot{C}_m, m) = 2M(m)\,,\\
&H(n+\dot{C}_m, m) = 2M(m) + 3, \qquad \textit{si } 2 < n \le m\,.
\end{aligned}$$

Demostración.

$$H(0,m) = \sum_{k=1}^{m} g(0,k)\mu(k) = 2\sum_{k=1}^{m}\mu(k) = 2M(m)\,.$$

$$H(1,m) = \sum_{k=1}^{m} g(1,k)\mu(k) = 0\cdot\mu(1) + 2\sum_{k=2}^{m}\mu(k) = 2M(m) - 2\,.$$

$$H(2,m) = \sum_{k=1}^{m} g(2,k)\mu(k) = 0\cdot\mu(1) + 0\cdot\mu(2) + 2\sum_{k=3}^{m}\mu(k) = 2M(m)\,.$$

$$\begin{aligned}
H(3,m) &= \sum_{k=1}^{m} g(3,k)\mu(k)\\
&= 1\cdot\mu(1) + 0\cdot\mu(2) + 0\cdot\mu(3) + 2\sum_{k=1}^{m}\mu(k) = 2M(m) + 3\,.
\end{aligned}$$

Si $2 < n \le m$ entonces

$$H(n,m) = \sum_{k=1}^{m} g(n,k)\mu(k) = \sum_{k=1}^{n} g(n,k)\mu(k) + \sum_{k=n+1}^{m} g(n,k)\mu(k)\,.$$

Por tanto, dado que para $0 \le n < n+1 \le k$ es $g(n,k) = 2$, tenemos

$$H(n,m) = \sum_{k=1}^{\lfloor \frac{n}{3} \rfloor} g(n,k)\mu(k) + \sum_{k=\lfloor \frac{n}{3} \rfloor + 1}^{n} g(n,k)\mu(k) + 2\sum_{k=n+1}^{m}\mu(k)\,.$$

Por las proposiciones 3.3.4 y 3.3.5 sabemos que

$$\sum_{k=1}^{\lfloor \frac{n}{3} \rfloor} g(n,k)\mu(k) = 2M(n) + 3\,.$$

Si $\left\lfloor \frac{n}{3} \right\rfloor \leq k \leq n$ entonces $k \leq n < 3k$ y en estos casos es $g(n,k) = 0$. Por tanto podemos escribir

$$H(m,n) = 2M(n) + 3 + 2\left(M(m) - M(n)\right) = 2M(m) + 3\,.$$

□

Capítulo 4

Las funciones $\overline{\mu}$, $\overline{M}$ y $\overline{\varphi}$

4.1. Introducción

En el capítulo anterior hemos dado algunas fórmulas que nos permiten calcular $M(n)$. En este capítulo vamos a utilizar una de ellas (la que luego citamos como (4.1)) para definir tres funciones aritméticas, similares a las funciones μ, M y φ. Estas nuevas funciones aritméticas, que denotaremos $\overline{\mu}$, $\overline{M}$ y $\overline{\varphi}$, en vez de tomar los valores enteros -1, 0 y 1, toman valores en el conjunto de los enteros gaussianos.

El objetivo de este capítulo es demostrar, para las funciones $\overline{\mu}$, $\overline{M}$ y $\overline{\varphi}$, diversos resultados análogos a los correspondientes para μ, M y φ. Además, veremos varias fórmulas que relacionan unas funciones con otras.

Tal como hicimos en el capítulo anterior, si $n \geq 2$, podemos despejar $M(n)$ en la ecuación

$$1 = \sum_{a=1}^{n} M\left(\frac{n}{a}\right) , \tag{4.1}$$

obteniendo una fórmula recurrente para el cálculo de $M(n)$:

$$M(n) = 1 - \sum_{a=2}^{n} M\left(\frac{n}{a}\right) ,$$

que nos permite calcular $M(n)$ en función de $M(1)$.

Así, $M(2) = 1 - M(1)$, $M(3) = 1 - 2M(1)$, $M(4) = -M(1)$, $M(5) = -2M(1)$, $M(6) = -1$, $M(7) = -1 - M(1)$, ...

Dado que $\mu(n) = M(n) - M(n-1)$ tenemos $\mu(1) = M(1)$, $\mu(2) =$

$1-2M(1)$, $\mu(3)=-M(1)$, $\mu(4)=-1+M(1)$, ...,

$$\mu(n)=\begin{cases} 0 & \text{si } n=\dot{p}^2, & \text{con } p \text{ primo impar,}\\ 0 & \text{si } n=\dot{8}\,, & \\ (-1)^k M(1) & \text{si } n=\prod_{j=1}^{k} p_j, & \text{con } p_j \text{ primos impares distintos,}\\ (-1)^k\,(1-2M(1)) & \text{si } n=2\prod_{j=1}^{k} p_j, & \text{con } p_j \text{ primos impares distintos,}\\ (-1)^k\,(-1+M(1)) & \text{si } n=4\prod_{j=1}^{k} p_j, & \text{con } p_j \text{ primos impares distintos,}\\ M(1) & \text{si } n=1\,. & \end{cases}$$

Al dar distintos valores a $M(1)$ se obtienen distintas funciones parecidas a $\mu(n)$, pero si se pretende que la función definida sea multiplicativa, debe ser $M(1)=1$.

En todo el capítulo utilizaremos i para designar la unidad imaginaria.

4.2. La función $\overline{\mu}$

Lo anterior nos da pie para definir la función aritmética $\overline{\mu}$ como sigue:

Definición 4.2.1. Para $n\in\mathbb{N}$ definimos

$$\overline{\mu}\,(n):=\begin{cases} 1 & \text{si} \quad n=1\,, & \\ -2+i & \text{si} \quad n=2\,, & \\ 1-i & \text{si} \quad n=4\,, & \\ 0 & \text{si} \quad n=\dot{p}^2, & \text{con } p \text{ primo impar,}\\ 0 & \text{si} \quad n=\dot{8}\,, & \\ (-1)^k & \text{si} \quad n=\prod_{j=1}^{k} p_j, & \text{con } p_j \text{ primos impares distintos,}\\ (-1)^k(-2+i) & \text{si} \quad n=2\prod_{j=1}^{k} p_j, & \text{con } p_j \text{ primos impares distintos,}\\ (-1)^k(1-i) & \text{si} \quad n=4\prod_{j=1}^{k} p_j, & \text{con } p_j \text{ primos impares distintos.}\\ & & \end{cases}$$

En las proposiciones siguientes vamos a establecer para la función $\overline{\mu}$ una serie de propiedades parecidas a las que verifica la μ ordinaria.

Proposición 4.2.1. *La función $\overline{\mu}$ de la definición 4.2.1 es multiplicativa.*

Demostración. Si a es un número impar se tiene $\overline{\mu}(a) = \mu(a)$, luego si a y b son dos números impares primos entre sí, entonces

$$\overline{\mu}(a \cdot b) = \overline{\mu}(a) \cdot \overline{\mu}(b).$$

Además, es claro que

$$\overline{\mu}(8 \cdot a) = 0 = \overline{\mu}(8) \cdot \overline{\mu}(a).$$

Por último, si a es un número impar,

$$\overline{\mu}(2 \cdot a) = (-2+i) \cdot \overline{\mu}(a) = \overline{\mu}(2) \cdot \overline{\mu}(a)$$

y

$$\overline{\mu}(4 \cdot a) = (1-i) \cdot \overline{\mu}(a) = \overline{\mu}(4) \cdot \overline{\mu}(a).$$

□

La notación $p^\alpha || n$ significa que $p^\alpha | n$ y $p^{\alpha+1} \nmid n$. Con ella podemos enunciar el siguiente

Corolario 4.2.2.

$$\overline{\mu}(n) = \begin{cases} \mu(n) & si \;\; n \; impar. \\ (2-i)\mu(n) & si \;\; 2||n. \\ (1-i)\mu(\frac{n}{4}) & si \;\; 4||n. \\ 0 & si \;\; 8|n. \end{cases} \tag{4.2}$$

En la siguiente proposición damos una nueva relación entre la función μ ordinaria y la función $\overline{\mu}$.

Proposición 4.2.3.

$$\mu(n) = \mathrm{Re}(\overline{\mu}(n)) + \mathrm{Im}(\overline{\mu}(n)).$$

Demostración. Es suficiente comprobar que se verifica para $n = 2$ y $n = 4$.

Para $n = 2$,

$$\mu(2) = -1 = -2 + 1 = \mathrm{Re}(\overline{\mu}(2)) + \mathrm{Im}(\overline{\mu}(2)).$$

Para $n = 4$,

$$\mu(4) = 0 = 1 - 1 = \mathrm{Re}(\overline{\mu}(4)) + \mathrm{Im}(\overline{\mu}(4)).$$

□

La función $\overline{\mu}$ verifica una fórmula parecida a la conocida fórmula verificada por μ:

$$\sum_{d|n} \mu(d) = \begin{cases} 1 & \text{si} \quad n = 1\,, \\ 0 & \text{si} \quad n > 1\,, \end{cases}$$

que puede verse, por ejemplo, en [21, teorema 263].

Proposición 4.2.4.

$$\sum_{d|n} \overline{\mu}\,(d) = \begin{cases} 1 & si \quad n = 1\,, \\ -1+i & si \quad n = 2\,, \\ 0 & si \quad n > 2\,. \end{cases} \tag{4.3}$$

Demostración. Analicemos todos los casos posibles:

Si $n = 1$, es $\overline{\mu}\,(1) = 1$.

Si $n = 2$, es $\overline{\mu}\,(1) + \overline{\mu}\,(2) = 1 + (-2+i) = -1+i$.

Si $n = 4$, es $\overline{\mu}\,(1) + \overline{\mu}\,(2) + \overline{\mu}\,(4) = 1 + (-2+i) + 1 - i = 0$.

Si $n = \prod p_k^{a_k}$ (todos los p_k primos impares), entonces

$$\sum_{d|n} \overline{\mu}\,(d) = \sum_{l=0}^{k} \binom{k}{l} (-1)^l = (1-1)^k = 0\,.$$

Si $n = 2 \cdot \prod p_k^{a_k}$, entonces

$$\sum_{d|n} \overline{\mu}\,(d) = \sum_{l=0}^{k} \binom{k}{l} (-1)^l + \overline{\mu}\,(2) \sum_{l=0}^{k} \binom{k}{l} (-1)^l = 0 + 0 = 0\,.$$

Si $n = 2^{a_0} \cdot \prod p_k^{a_k}$ (con $a_0 \geq 2$), entonces

$$\sum_{d|n} \overline{\mu}\,(d) = \sum_{l=0}^{k} \binom{k}{l} (-1)^l + \overline{\mu}\,(2) \sum_{l=0}^{k} \binom{k}{l} (-1)^l + \overline{\mu}\,(4) \sum_{l=0}^{k} \binom{k}{l} (-1)^l = 0\,.$$

□

La proposición 4.2.3 nos daba el valor de $\mu(n)$ en función del valor de $\overline{\mu}\,(n)$. La proposición siguiente nos muestra el valor de $\overline{\mu}\,(n)$ en función del valor de $\mu(n)$.

Proposición 4.2.5.

$$\overline{\mu}\,(n) = \mu(n) - \cos^2\left(\frac{\pi n}{2}\right)(1-i)\mu\left(\left\lfloor \frac{n}{2} \right\rfloor\right)\,.$$

Demostración. Si n es impar entonces $\cos(\frac{\pi n}{2}) = 0$, por tanto

$$\mu(n) - \cos^2\left(\frac{\pi n}{2}\right)(1-i)\mu\left(\left\lfloor\frac{n}{2}\right\rfloor\right) = \mu(n) = \overline{\mu}\,(n)\,.$$

Si $n = 2m$, m impar,

$$\mu(n) - \cos^2\left(\frac{\pi n}{2}\right)(1-i)\mu\left(\left\lfloor\frac{n}{2}\right\rfloor\right)$$

$$= -\mu(m) - (1-i)\mu(m) = \mu(m)(-2+i) = \overline{\mu}\,(n)\,.$$

Si $n = 4m$, m impar,

$$\mu(n) - \cos^2\left(\frac{\pi n}{2}\right)(1-i)\mu\left(\left\lfloor\frac{n}{2}\right\rfloor\right) = (1-i)\mu(m) = \overline{\mu}\,(n)\,.$$

Si $n = \dot{8}$, tanto $\mu(n)$ como $\mu\left(\left\lfloor\frac{n}{2}\right\rfloor\right)$ son 0, por tanto

$$\overline{\mu}\,(n) = 0 = \mu(n) - \cos^2\left(\frac{\pi n}{2}\right)(1-i)\mu\left(\left\lfloor\frac{n}{2}\right\rfloor\right)\,.$$

□

Este resultado nos permite adaptar la conocida fórmula de J. C. Kluyver

$$\mu(n) = \sum_{\substack{\nu=1\\ \mathrm{mcd}(\nu,n)=1}}^{n} \cos\frac{2\pi\nu}{n}\,, \tag{4.4}$$

a una fórmula válida para $\overline{\mu}$:

$$\overline{\mu}\,(n) = \sum_{\substack{\nu=1\\ \mathrm{mcd}(\nu,n)=1}}^{n} \cos\frac{2\pi\nu}{n} - \cos^2\left(\frac{\pi n}{2}\right)(1-i) \sum_{\substack{\nu=1\\ \mathrm{mcd}(\nu,\lfloor\frac{n}{2}\rfloor)=1}}^{\lfloor\frac{n}{2}\rfloor} \cos\frac{4\pi\nu}{n}\,.$$

La proposición siguiente es análoga a la proposición 3.3.2.

Proposición 4.2.6.

$$\sum_{k=1}^{n}\left\lfloor\frac{n}{k}\right\rfloor\overline{\mu}\,(k) = \begin{cases} i & si \quad n > 1\,,\\ 1 & si \quad n = 1\,. \end{cases}$$

Demostración. Para demostrar este resultado, empezamos por partir el sumatorio en cuatro partes, la primera formada por los términos para los que k es impar, la segunda formada por los términos para los que k es múltiplo

de dos y no de cuatro, la tercera formada por los términos para los que k es múltiplo de cuatro y no de ocho, los restantes términos valen cero. Así,

$$\sum_{k=1}^{n} \left\lfloor \frac{n}{k} \right\rfloor \overline{\mu}\,(k)$$

$$= \sum_{\substack{k=1 \\ \mathrm{mcd}(k,2)=1}}^{n} \left\lfloor \frac{n}{k} \right\rfloor \overline{\mu}\,(k) + \sum_{\substack{k=1 \\ \mathrm{mcd}(k,4)=2}}^{n} \left\lfloor \frac{n}{k} \right\rfloor \overline{\mu}\,(k) + \sum_{\substack{k=1 \\ \mathrm{mcd}(k,8)=4}}^{n} \left\lfloor \frac{n}{k} \right\rfloor \overline{\mu}\,(k)$$

$$= \sum_{\substack{k=1 \\ \mathrm{mcd}(k,2)=1}}^{n} \left\lfloor \frac{n}{k} \right\rfloor \mu(k) + (-2+i) \sum_{\substack{k=1 \\ \mathrm{mcd}(k,4)=2}}^{n} \left\lfloor \frac{n}{k} \right\rfloor \mu\left(\frac{k}{2}\right) + (1-i) \sum_{\substack{k=1 \\ 4||k}}^{n} \left\lfloor \frac{n}{k} \right\rfloor \mu\left(\frac{k}{4}\right)$$

$$= \sum_{\substack{k=1 \\ \mathrm{mcd}(k,2)=1}}^{n} \left\lfloor \frac{n}{k} \right\rfloor \mu(k) - \sum_{\substack{k=1 \\ \mathrm{mcd}(k,4)=2}}^{n} \left\lfloor \frac{n}{k} \right\rfloor \mu\left(\frac{k}{2}\right)$$

$$+(-1+i) \sum_{\substack{k=1 \\ \mathrm{mcd}(k,4)=2}}^{n} \left\lfloor \frac{n}{k} \right\rfloor \mu\left(\frac{k}{2}\right) + (1-i) \sum_{\substack{k=1 \\ 4||k}}^{n} \left\lfloor \frac{n}{k} \right\rfloor \mu\left(\frac{k}{4}\right)$$

$$= \sum_{k=1}^{n} \left\lfloor \frac{n}{k} \right\rfloor \mu(k) + (-1+i) \sum_{\substack{k=1 \\ k=2\dot{}}}^{n} \left\lfloor \frac{n}{k} \right\rfloor \mu\left(\frac{k}{2}\right) .$$

Teniendo en cuenta que $\left\lfloor \frac{n}{2k} \right\rfloor = \left\lfloor \frac{\left\lfloor \frac{n}{2} \right\rfloor}{k} \right\rfloor$ y la proposición 3.3.2 podemos escribir

$$\sum_{k=1}^{n} \left\lfloor \frac{n}{k} \right\rfloor \overline{\mu}\,(k) = 1 + (-1+i) \sum_{k=1}^{\left\lfloor \frac{n}{2} \right\rfloor} \left\lfloor \frac{\left\lfloor \frac{n}{2} \right\rfloor}{k} \right\rfloor \mu(k) = 1 + (-1+i) = i\,.$$

□

En la demostración de la proposición 4.2.8 utilizaremos el siguiente teorema, que puede verse en [2, teorema 11.7]. Como es habitual, aquí y en el resto del capítulo usaremos σ para denotar $\sigma = \mathrm{Re}(s)$.

Teorema 4.2.7. *Suponemos que $\sum_{n=1}^{\infty} \frac{f(n)}{n^s}$ converge absolutamente para $\sigma > \sigma_a$. Si f es multiplicativa tenemos*

$$\sum_{n=1}^{\infty} \frac{f(n)}{n^s} = \prod_{p} \left\{ 1 + \frac{f(p)}{p^s} + \frac{f\left(p^2\right)}{p^{2s}} + \cdots \right\} , \qquad \sigma > \sigma_a\,.$$

Para la función μ, es conocido que se verifica

$$\sum_{n=1}^{\infty} \frac{\mu(n)}{n^s} = \frac{1}{\zeta(s)}\,,$$

para $\sigma > 1$. Ver, por ejemplo, [21, teorema 287] (s real) o [2, sección 11.5, pág. 285]. La correspondiente fórmula para $\overline{\mu}$ viene dada por la proposición siguiente.

Proposición 4.2.8. *Si* $\mathrm{Re}(s) > 1$ *entonces*

$$\sum_{n=1}^{\infty} \frac{\overline{\mu}\,(n)}{n^s} = \frac{2^s - 1 + i}{2^s} \cdot \frac{1}{\zeta(s)}\,. \tag{4.5}$$

Demostración. Dado que $|\,\overline{\mu}\,(n)| \leq \sqrt{5}$, para $\mathrm{Re}(s) > 1$, la serie $\sum_{n=1}^{\infty} \frac{\overline{\mu}\,(n)}{n^s}$ es absolutamente convergente. Por tanto, por el teorema 4.2.7, tenemos

$$\sum_{n=1}^{\infty} \frac{\overline{\mu}\,(n)}{n^s} = \prod_{p} \left(1 + \frac{\overline{\mu}\,(p)}{p^s} + \frac{\overline{\mu}\,(p^2)}{p^{2s}} + \cdots\right)$$

$$= \left(1 + \frac{-2+i}{2^s} + \frac{1-i}{4^s}\right) \prod_{p \text{ primo impar}} \left(1 - \frac{1}{p^s}\right)$$

$$= \frac{2^{2s} - 2^{s+1} + 2^s i + 1 - i}{2^{2s}} \frac{1}{1 - \frac{1}{2^s}} \prod_{p \text{ primo}} \left(1 - \frac{1}{p^s}\right)$$

$$= \frac{((2^s)^2 - 2 \cdot 2^s + 1) + (2^s - 1)i}{2^s(2^s - 1)} \frac{1}{\zeta(s)} = \frac{2^s - 1 + i}{2^s} \frac{1}{\zeta(s)}\,.$$

□

Finalmente, tenemos

Corolario 4.2.9.

$$\sum_{n=1}^{\infty} \frac{\overline{\mu}\,(n)}{n^2} = \frac{3+i}{4} \cdot \frac{6}{\pi^2} = \frac{3+i}{2} \cdot \frac{3}{\pi^2}\,.$$

4.3. La función $\overline{\varphi}$

En esta sección, a partir de la función $\overline{\mu}$ definimos la función aritmética $\overline{\varphi}$, análoga a la función φ de Euler, y establecemos algunas de sus propiedades. La definición de $\overline{\varphi}$ la damos imitando una conocida propiedad de φ:

$$\varphi(n) = \sum_{d|n} \mu(d)\frac{n}{d}\,.$$

(ver, por ejemplo, [2, teorema 2.3, pág. 32]). Así, tomamos

Definición 4.3.1. Para $n \in \mathbb{N}$ definimos

$$\overline{\varphi}\,(n) := \sum_{d|n} \overline{\mu}\,(d)\frac{n}{d}\,. \tag{4.6}$$

Por ejemplo, se tiene

$$\overline{\varphi}\,(1) = 1,\ \ \overline{\varphi}\,(2) = 2\,\overline{\mu}\,(1) + \overline{\mu}\,(2) = 2 - 2 + i = i\,,$$

$$\overline{\varphi}\,(4) = 4\,\overline{\mu}\,(1) + 2\,\overline{\mu}\,(2) + \overline{\mu}\,(4) = 4 - 4 + 2i + 1 - i = 1 + i\,.$$

La proposición siguiente nos relaciona los valores de $\overline{\varphi}$ con los valores de φ.

Proposición 4.3.1.

$$\textit{Si } n \textit{ es impar}, \qquad \overline{\varphi}\,(n) = \varphi(n)\,; \tag{4.7}$$

$$\textit{si } n = 2m, \ \textit{con } m \textit{ impar}, \qquad \overline{\varphi}\,(2m) = \varphi(m)\cdot i\,; \tag{4.8}$$

$$\textit{si } n = 2^k m, \ \textit{con } k \geq 2, \ m \textit{ impar}, \qquad \overline{\varphi}\,(2^k m) = 2^{k-2}(1+i)\varphi(m)\,. \tag{4.9}$$

Demostración. Si n es impar, todos sus divisores son impares; por tanto

$$\overline{\varphi}\,(n) = \sum_{d|n} \overline{\mu}\,(d)\frac{n}{d} = \sum_{d|n} \mu(d)\frac{n}{d} = \varphi(n)\,.$$

Si $n = 2m$,

$$\begin{aligned}\overline{\varphi}\,(n) &= \sum_{d|n} \overline{\mu}\,(d)\frac{n}{d} = \sum_{d|m} \overline{\mu}\,(d)\frac{2m}{d} + \sum_{d|m} \overline{\mu}\,(2d)\frac{2m}{2d} \\ &= 2\varphi(m) + (-2+i)\varphi(m) = i\varphi(m)\,.\end{aligned}$$

Si $n = 2^k m$, con $k \geq 2$ y m impar

$$\overline{\varphi}\,(n) = \sum_{d|n} \overline{\mu}\,(d)\frac{n}{d} = \sum_{d|m} \overline{\mu}\,(d)\frac{2^k m}{d} + \sum_{d|m} \overline{\mu}\,(2d)\frac{2^k m}{2d} + \sum_{d|m} \overline{\mu}\,(4d)\frac{2^k m}{4d}$$

$$= 2^k\varphi(m) + (-2+i)2^{k-1}\varphi(m) + (1-i)2^{k-2}\varphi(m) = (1+i)2^{k-2}\varphi(m)\,.$$

□

Corolario 4.3.2. *$\overline{\varphi}$ es multiplicativa.*

Demostración. Si $(m,n)=1$ y ambos son impares entonces

$$\overline{\varphi}\,(mn)=\varphi(mn)=\varphi(m)\cdot\varphi(n)=\overline{\varphi}\,(m)\cdot\overline{\varphi}\,(n)\,.$$

Si $(m,n)=1$ y $m=2m_1$ con m_1 impar, entonces

$$\overline{\varphi}\,(mn)=i\varphi(m_1n)=i\varphi(m_1)\cdot\varphi(n)=\overline{\varphi}\,(m)\cdot\overline{\varphi}\,(n)\,.$$

Si $(m,n)=1$ y $m=2^km_1$ con m_1 impar y $k\geq 2$, entonces

$$\overline{\varphi}\,(mn)=2^{k-2}(1+i)\varphi(m_1n)=2^{k-2}(1+i)\varphi(m_1)\cdot\varphi(n)=\overline{\varphi}\,(m)\cdot\overline{\varphi}\,(n)\,.$$

□

Ahora vamos a probar una serie de resultados que verifica la función $\overline{\varphi}$, análogos a los que verifica φ. En primer lugar, la conocida igualdad

$$\varphi(n)=n\prod_{\substack{p\text{ primo}\\ p|n}}\left(1-\frac{1}{p}\right)$$

(ver [2, teorema 2.4, pág. 33]) queda ahora del siguiente modo:

Proposición 4.3.3. *Si n es impar, entonces*

$$\overline{\varphi}\,(n)=n\prod_{\substack{p\ primo\\ p|n}}\left(1-\frac{1}{p}\right)\,.$$

Si $n=2m$, con m impar, entonces

$$\overline{\varphi}\,(n)=i\cdot n\prod_{\substack{p\ primo\\ p|n}}\left(1-\frac{1}{p}\right)\,.$$

Si n es múltiplo de 4, entonces

$$\overline{\varphi}\,(n)=\frac{1+i}{2}\,n\prod_{\substack{p\ primo\\ p|n}}\left(1-\frac{1}{p}\right)\,.$$

Demostración. Si n es impar, entonces

$$\overline{\varphi}\,(n)=\varphi(n)=n\prod_{\substack{p\text{ primo}\\ p|n}}\left(1-\frac{1}{p}\right)\,.$$

Si $n = 2m$, con m impar, entonces

$$\overline{\varphi}(n) = i\,\overline{\varphi}(m) = i \cdot m \prod_{\substack{p \text{ primo} \\ p|m}} \left(1 - \frac{1}{p}\right)$$

$$= i \cdot 2m \left(1 - \frac{1}{2}\right) \prod_{\substack{p \text{ primo} \\ p|m}} \left(1 - \frac{1}{p}\right) = i \cdot n \prod_{\substack{p \text{ primo} \\ p|n}} \left(1 - \frac{1}{p}\right).$$

Si $n = 2^k m$ con $k \geq 2$ y m impar, entonces

$$\overline{\varphi}(n) = 2^{k-2}(1+i)\varphi(m) = \frac{1+i}{2}\, 2^k m \left(1 - \frac{1}{2}\right) \prod_{\substack{p \text{ primo} \\ p|m}} \left(1 - \frac{1}{p}\right)$$

$$= \frac{1+i}{2}\, n \prod_{\substack{p \text{ primo} \\ p|n}} \left(1 - \frac{1}{p}\right).$$

□

La función φ verifica

$$\sum_{d|n} \varphi(d) = n$$

(ver, por ejemplo, [2, teorema 2.2, pág. 3]). Ahora, tenemos

Proposición 4.3.4.

$$\sum_{d|n} \overline{\varphi}(d) = \begin{cases} n & \textit{si } n \textit{ es impar,} \\ \frac{n}{2} + \frac{n}{2}\, i & \textit{si } n \textit{ es par.} \end{cases}$$

Demostración. Si n es impar, los divisores d de n son impares y $\overline{\varphi}(d) = \varphi(d)$; por tanto

$$\sum_{d|n} \overline{\varphi}(d) = \sum_{d|n} \varphi(d) = n\,.$$

Si n es par, $n = 2^k m$ con m impar, entonces

$$\sum_{d|n} \overline{\varphi}(d) = \sum_{d|m} \overline{\varphi}(d) + \sum_{j=1}^{k} \sum_{d|m} \overline{\varphi}(2^j d)$$

$$= \sum_{d|m} \overline{\varphi}(d) + i \sum_{d|m} \overline{\varphi}(d) + \sum_{j=2}^{k} 2^{j-2}(1+i) \sum_{d|m} \overline{\varphi}(d)$$

$$= \left(\sum_{d|m} \overline{\varphi}\,(d) \right) \left(1 + i + \sum_{j=2}^{k} 2^{j-2}(1+i) \right)$$

$$= m\left(1 + i + (1+i)\left(2^{k-1} - 1\right)\right) = m2^{k-1}(1+i) = \frac{n}{2}(1+i)\,.$$

□

En la demostración de la siguiente proposición utilizamos el conocido resultado, que damos en la forma como aparece en [2, teorema 11.5].

Teorema 4.3.5. *Sean dos funciones $F(s)$ y $G(s)$ representadas por dos series de Dirichlet,*

$$F(s) = \sum_{n=1}^{\infty} \frac{f(n)}{n^s} \quad \textit{para } \sigma > a\,,$$

y

$$G(s) = \sum_{n=1}^{\infty} \frac{g(n)}{n^s} \quad \textit{para } \sigma > b\,.$$

Entonces, en el semiplano en el que ambas series convergen absolutamente, tenemos

$$F(x)G(x) = \sum_{n=1}^{\infty} \frac{h(n)}{n^s}\,,$$

donde $h = f * g$, es la convolución de Dirichlet de f y g:

$$h(n) = \sum_{d|n} f(d)g\left(\frac{n}{d}\right)\,.$$

Recíprocamente, si $F(s)G(s) = \sum \alpha(n)n^{-s}$ para todo s de una sucesión $\{s_k\}$ cuya parte real σ_k verifica $\sigma_k \to +\infty$ cuando $k \to \infty$, entonces $\alpha = f * g$.

Proposición 4.3.6. *Si* $\mathrm{Re}(s) > 2$, *entonces*

$$\sum_{n=1}^{\infty} \frac{\overline{\varphi}\,(n)}{n^s} = \frac{\zeta(s-1)}{\zeta(s)} \left(\frac{2^s - 1 + i}{2^s} \right)\,. \tag{4.10}$$

Demostración. En el teorema 4.3.5 tomamos $f(n) = 1$ y $g(n) = \overline{\varphi}\,(n)$, con lo que

$$F(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$$

y

$$G(s) = \sum_{n=1}^{\infty} \frac{\overline{\varphi}\,(n)}{n^s}\,.$$

Por la proposición 4.3.4, $h = f * g$ verifica

$$h(n) := \sum_{d|n} \overline{\varphi}(d) = \begin{cases} n & \text{si} \quad n \text{ es impar,} \\ \frac{n}{2} + \frac{n}{2}i & \text{si} \quad n \text{ es par.} \end{cases}$$

Por tanto para $\mathrm{Re}(s) > 2$ se tiene

$$\left(\sum_{n=1}^{\infty} \frac{1}{n^s}\right)\left(\sum_{n=1}^{\infty} \frac{\overline{\varphi}(n)}{n^s}\right) = \sum_{n=1}^{\infty} \frac{h(n)}{n^s}$$

$$= \sum_{\substack{n=1 \\ \mathrm{mcd}(n,2)=1}}^{\infty} \frac{1}{n^{s-1}} + \sum_{\substack{n=1 \\ \mathrm{mcd}(n,2)=2}}^{\infty} \frac{\frac{1}{2} + \frac{1}{2}i}{n^{s-1}}$$

$$= \sum_{n=1}^{\infty} \frac{1}{n^{s-1}} - \frac{1}{2} \sum_{\substack{n=1 \\ \mathrm{mcd}(n,2)=2}}^{\infty} \frac{1}{n^{s-1}} + \frac{1}{2}i \sum_{\substack{n=1 \\ \mathrm{mcd}(n,2)=2}}^{\infty} \frac{1}{n^{s-1}}$$

$$= \zeta(s-1) + \left(-\frac{1}{2} + \frac{1}{2}i\right) \frac{1}{2^{s-1}} \zeta(s-1) = \left(-\frac{1}{2^s} + \frac{1}{2^s}i + 1\right) \zeta(s-1)$$

$$= \frac{2^s - 1 + i}{2^s} \zeta(s-1)\,,$$

luego

$$\sum_{n=1}^{\infty} \frac{\overline{\varphi}(n)}{n^s} = \frac{\zeta(s-1)}{\zeta(s)} \left(\frac{2^s - 1 + i}{2^s}\right).$$

□

Terminamos esta sección estudiando el comportamiento asintótico de la función de las sumas de $\overline{\varphi}(n)$, para $n \leq x$.

Proposición 4.3.7. *Cuando $x \to \infty$, se verifica*

$$\sum_{n \leq x} \overline{\varphi}(n) - \frac{9 + 3i}{4\pi^2} x^2 = O(x \log x)\,. \tag{4.11}$$

Demostración.

$$\sum_{n \leq x} \overline{\varphi}(n) = \sum_{n \leq x} \sum_{d|n} \overline{\mu}(d) \frac{n}{d} = \sum_{\substack{q,d \\ q \cdot d \leq x}} \overline{\mu}(d) q$$

$$= \sum_{d \leq x} \overline{\mu}(d) \sum_{q \leq \frac{x}{d}} q = \sum_{d \leq x} \overline{\mu}(d) \frac{\left(1 + \left\lfloor \frac{x}{d} \right\rfloor\right) \left\lfloor \frac{x}{d} \right\rfloor}{2}$$

$$= \sum_{d\leq x} \overline{\mu}\,(d) \frac{\left(1+\frac{x}{d}-\left\{\frac{x}{d}\right\}\right)\left(\frac{x}{d}-\left\{\frac{x}{d}\right\}\right)}{2}$$

$$= \sum_{d\leq x} \frac{x^2}{2}\frac{\overline{\mu}\,(d)}{d^2} + \sum_{d\leq x} \frac{x}{2}\frac{\overline{\mu}\,(d)}{d} + \sum_{d\leq x} \frac{-1-\frac{2x}{d}}{2}\,\overline{\mu}\,(d)\left\{\frac{x}{d}\right\} + \sum_{d\leq x}\frac{1}{2}\left\{\frac{x}{d}\right\}^2 \overline{\mu}\,(d)$$

$$= \frac{x^2}{2}\sum_{d=1}^{\infty}\frac{\overline{\mu}\,(d)}{d^2} - \frac{x^2}{2}\sum_{d>x}\frac{\overline{\mu}\,(d)}{d^2} + \frac{x}{2}\sum_{d\leq x}\frac{\overline{\mu}\,(d)}{d} - x\sum_{d\leq x}\left\{\frac{x}{d}\right\}\frac{\overline{\mu}\,(d)}{d}$$

$$-\frac{1}{2}\sum_{d\leq x}\left\{\frac{x}{d}\right\}\overline{\mu}\,(d) + \frac{1}{2}\sum_{d\leq x}\left\{\frac{x}{d}\right\}^2\overline{\mu}\,(d)\,,$$

luego, por el corolario 4.2.9,

$$\left|\sum_{n\leq x}\overline{\varphi}\,(n) - \frac{9+3i}{4\pi^2}x^2\right| = \left|-\frac{x^2}{2}\sum_{d>x}\frac{\overline{\mu}\,(d)}{d^2} + \frac{x}{2}\sum_{d\leq x}\frac{\overline{\mu}\,(d)}{d}\right.$$

$$\left. -x\sum_{d\leq x}\left\{\frac{x}{d}\right\}\frac{\overline{\mu}\,(d)}{d} - \frac{1}{2}\sum_{d\leq x}\left\{\frac{x}{d}\right\}\overline{\mu}\,(d) + \frac{1}{2}\sum_{d\leq x}\left\{\frac{x}{d}\right\}^2\overline{\mu}\,(d)\right| < kx\log x\,.$$

□

4.4. La función $\overline{M}$

De forma análoga a como hemos definido la función M, a partir de la función $\overline{\mu}$ podemos definir la nueva función aritmética

Definición 4.4.1.

$$\overline{M}(n) := \sum_{k=1}^{n}\overline{\mu}\,(k)\,. \tag{4.12}$$

Obviamente, por la proposición 4.2.3, se cumple

$$M(n) = \mathrm{Re}\left(\overline{M}(n)\right) + \mathrm{Im}\left(\overline{M}(n)\right)\,. \tag{4.13}$$

Veamos ahora cómo obtener $\overline{M}$ a partir de M:

Proposición 4.4.1.

$$\overline{M}(n) = M(n) - M\left(\frac{n}{2}\right) + iM\left(\frac{n}{2}\right)\,.$$

Demostración. En el sumatorio de la parte derecha de (4.12), los sumandos correspondientes a $k = \dot{8}$ son cero. Agrupamos los restantes sumandos en tres sumatorios, lo que operando convenientemente nos permite establecer el resultado enunciado.

$$\overline{M}(n) = \sum_{k=1}^{n} \overline{\mu}\,(k) = \sum_{\substack{k=1\\ \text{impar}}}^{n} \overline{\mu}\,(k) + \sum_{\substack{k=1\\ 2||k}}^{n} \overline{\mu}\,(k) + \sum_{\substack{k=1\\ 4||k}}^{n} \overline{\mu}\,(k)$$

$$= \sum_{\substack{k=1\\ \text{impar}}}^{n} \mu(k) + 2\sum_{\substack{k=1\\ 2||k}}^{n} \mu(k) - i\sum_{\substack{k=1\\ 2||k}}^{n} \mu(k) + \sum_{\substack{k=1\\ 4||k}}^{n} \mu\left(\frac{k}{4}\right) - i\sum_{\substack{k=1\\ 4||k}}^{n} \mu\left(\frac{k}{4}\right)$$

$$= \sum_{k=1}^{n} \mu(k) + \sum_{\substack{k=1\\ 2||k}}^{n} \mu(k) + \sum_{\substack{k=1\\ 4||k}}^{n} \mu\left(\frac{k}{4}\right) - i\left(\sum_{\substack{k=1\\ 2||k}}^{n} \mu(k) + \sum_{\substack{k=1\\ 4||k}}^{n} \mu\left(\frac{k}{4}\right)\right)$$

$$= \sum_{k=1}^{n} \mu(k) + \sum_{\substack{l=1\\ l \text{ impar}}}^{\frac{n}{2}} \mu(2l) + \sum_{\substack{l=1\\ l \text{ impar}}}^{\frac{n}{4}} \mu(l) - i\left(\sum_{\substack{l=1\\ l \text{ impar}}}^{\frac{n}{2}} \mu(2l) + \sum_{\substack{l=1\\ l \text{ impar}}}^{\frac{n}{4}} \mu(l)\right)$$

$$= \sum_{k=1}^{n} \mu(k) - \sum_{\substack{l=1\\ l \text{ impar}}}^{\frac{n}{2}} \mu(l) - \sum_{\substack{l=1\\ l \text{ impar}}}^{\frac{n}{4}} \mu(2l) + i\left(\sum_{\substack{l=1\\ l \text{ impar}}}^{\frac{n}{2}} \mu(l) + \sum_{\substack{l=1\\ l \text{ impar}}}^{\frac{n}{4}} \mu(2l)\right)$$

$$= \sum_{k=1}^{n} \mu(k) - \sum_{k=1}^{\frac{n}{2}} \mu(k) + i\sum_{k=1}^{\frac{n}{2}} \mu(k)$$

$$= M(n) - M\left(\frac{n}{2}\right) + iM\left(\frac{n}{2}\right).$$

□

En la demostración de la proposición 4.4.3 hay que tener en cuenta que si $\frac{n}{2} < k \leq n$ entonces $\left\lfloor \frac{n}{k} \right\rfloor = 1$. Y la fórmula de inversión de Chebyshev, en la forma que se encuentra en [1, pág. 370].

Teorema 4.4.2 (Fórmula de inversión de Chebyshev). *Si*

$$F(x) = \sum_{n \leq x} G\left(\frac{x}{n}\right),$$

entonces

$$G(x) = \sum_{n \leq x} \mu(n) F\left(\frac{x}{n}\right)$$

y recíprocamente.

De este modo, obtenemos

Proposición 4.4.3. *Si $n > 1$, entonces*

$$\sum_{k=1}^{n} \overline{M}\left(\frac{n}{k}\right) = i\,. \tag{4.14}$$

Demostración. Tomemos

$$F(x) := \begin{cases} 1 & \text{si} \quad \lfloor x \rfloor = 1\,, \\ i & \text{si} \quad \lfloor x \rfloor > 1\,. \end{cases} \tag{4.15}$$

Esto nos permite escribir

$$\overline{M}(n) = M(n) - M\left(\frac{n}{2}\right) + iM\left(\frac{n}{2}\right) = \sum_{k=\lfloor \frac{n}{2} \rfloor + 1}^{n} \mu(k) + i \sum_{k=1}^{\frac{n}{2}} \mu(k)$$

$$= \sum_{k=1}^{n} F\left(\frac{n}{k}\right) \mu(k)\,.$$

Aplicando la fórmula de inversión de Chebyshev llegamos a

$$F(n) = \sum_{k=1}^{n} \overline{M}\left(\frac{n}{k}\right)\,.$$

□

Despejando $\overline{M}(n)$ en el resultado anterior se obtiene, de manera inmediata, una fórmula recursiva para $\overline{M}$. Pero podemos encontrar también esta otra, en la que aparecen menos sumandos:

Proposición 4.4.4. *Si $n > 3$, entonces*

$$\overline{M}(n) = -\sum_{a=1}^{\left\lfloor \frac{n-1}{2} \right\rfloor} \overline{M}\left(\frac{n}{2a+1}\right)\,. \tag{4.16}$$

Demostración. Si $n = 2m$ (con $m > 1$), entonces, por la proposición 4.4.3,

$$\overline{M}(2m) = i - \sum_{a=2}^{2m} \overline{M}\left(\frac{2m}{a}\right)$$

e

$$i = \sum_{a=1}^{m} \overline{M}\left(\frac{m}{a}\right)\,,$$

luego

$$\overline{M}(2m) = \sum_{a=1}^{m} \overline{M}\left(\frac{m}{a}\right) - \sum_{a=2}^{2m} \overline{M}\left(\frac{2m}{a}\right) = \sum_{a=1}^{m} \overline{M}\left(\frac{2m}{2a}\right) - \sum_{a=2}^{2m} \overline{M}\left(\frac{2m}{a}\right)$$

$$= -\sum_{a=1}^{m-1} \overline{M}\left(\frac{n}{2a+1}\right) = -\sum_{a=1}^{\left\lfloor \frac{n-1}{2} \right\rfloor} \overline{M}\left(\frac{n}{2a+1}\right).$$

Si $n = 2m+1$, con $m > 1$, despejando $\overline{M}(n)$ en (4.14) tenemos que

$$\overline{M}(2m+1) = i - \sum_{a=2}^{2m+1} \overline{M}\left(\frac{2m+1}{a}\right). \tag{4.17}$$

Al ser $m > 1$, en (4.17) podemos cambiar i por la expresión obtenida en (4.14), para obtener

$$\overline{M}(2m+1) = \sum_{a=1}^{m} \overline{M}\left(\frac{m}{a}\right) - \sum_{a=2}^{2m+1} \overline{M}\left(\frac{2m+1}{a}\right).$$

Observamos que

$$\frac{a-1}{a} + \frac{1}{2a} = \frac{2a-1}{2a} < 1\,.$$

Al ser $a-1$ el mayor resto que se obtiene al dividir m por a, tenemos que

$$\left\lfloor \frac{2m+1}{2a} \right\rfloor = \left\lfloor \frac{m}{a} + \frac{1}{2a} \right\rfloor = \left\lfloor \frac{m}{a} \right\rfloor.$$

Esto nos permite escribir

$$\overline{M}(2m+1) = \sum_{a=1}^{m} \overline{M}\left(\frac{2m+1}{2a}\right) - \sum_{a=2}^{2m+1} \overline{M}\left(\frac{2m+1}{a}\right)$$

$$= -\sum_{a=1}^{m} \overline{M}\left(\frac{2m+1}{2a+1}\right) = -\sum_{a=1}^{\left\lfloor \frac{n-1}{2} \right\rfloor} \overline{M}\left(\frac{n}{2a+1}\right).$$

□

Proposición 4.4.5. *Si $n > 3$, entonces*

$$\overline{M}(n) = -\sum_{k=1}^{\left\lfloor \frac{n}{3} \right\rfloor} \left\lfloor \frac{n-k}{2k} \right\rfloor \overline{\mu}(k)\,. \tag{4.18}$$

Demostración. En

$$\overline{M}(n) = -\sum_{a=1}^{\left\lfloor \frac{n-1}{2} \right\rfloor} \overline{M}\left(\frac{n}{2a+1}\right),$$

el mayor valor que alcanza $\left\lfloor \frac{n}{2a+1} \right\rfloor$ es $\left\lfloor \frac{n}{3} \right\rfloor$.

Estudiemos cuándo $\left\lfloor \frac{n}{2a+1} \right\rfloor = k$. Esto ocurre si

$$k \leq \frac{n}{2a+1} < k+1\,,$$
$$2ak + k \leq n < 2a(k+1) + k + 1\,,$$
$$\frac{n-(k+1)}{2(k+1)} < a \leq \frac{n-k}{2k}\,.$$

Por tanto

$$\overline{M}(n) = -\sum_{k=1}^{\left\lfloor \frac{n}{3} \right\rfloor} \left(\left\lfloor \frac{n-k}{2k} \right\rfloor - \left\lfloor \frac{n-(k+1)}{2(k+1)} \right\rfloor \right) \overline{M}(k)$$

$$= -\Bigg(\left(\left\lfloor \frac{n-1}{2} \right\rfloor - \left\lfloor \frac{n-2}{2\cdot 2} \right\rfloor \right) \overline{M}(1) + \left(\left\lfloor \frac{n-2}{2\cdot 2} \right\rfloor - \left\lfloor \frac{n-3}{2\cdot 3} \right\rfloor \right) \overline{M}(2) + \cdots$$
$$+ \left(\left\lfloor \frac{n-\left\lfloor \frac{n}{3} \right\rfloor}{2\cdot \left\lfloor \frac{n}{3} \right\rfloor} \right\rfloor - \left\lfloor \frac{n-\left\lfloor \frac{n}{3} \right\rfloor - 1}{2\cdot \left(\left\lfloor \frac{n}{3} \right\rfloor + 1 \right)} \right\rfloor \right) \overline{M}\left(\left\lfloor \frac{n}{3} \right\rfloor \right) \Bigg)$$

$$= -\Bigg(\left\lfloor \frac{n-1}{2} \right\rfloor \overline{\mu}\,(1) + \left\lfloor \frac{n-2}{2\cdot 2} \right\rfloor \overline{\mu}\,(2) + \left\lfloor \frac{n-3}{2\cdot 3} \right\rfloor \overline{\mu}\,(3) + \cdots$$
$$+ \left\lfloor \frac{n-\left\lfloor \frac{n}{3} \right\rfloor}{2\cdot \left\lfloor \frac{n}{3} \right\rfloor} \right\rfloor \overline{\mu}\left(\left\lfloor \frac{n}{3} \right\rfloor \right) - \left\lfloor \frac{n-\left\lfloor \frac{n}{3} \right\rfloor - 1}{2\cdot \left(\left\lfloor \frac{n}{3} \right\rfloor + 1 \right)} \right\rfloor \overline{M}\left(\left\lfloor \frac{n}{3} \right\rfloor \right) \Bigg)$$

$$= -\sum_{k=1}^{\left\lfloor \frac{n}{3} \right\rfloor} \left\lfloor \frac{n-k}{2k} \right\rfloor \overline{\mu}\,(k)\,,$$

pues

$$\left\lfloor \frac{n-\left\lfloor \frac{n}{3} \right\rfloor - 1}{2\cdot \left\lfloor \frac{n}{3} \right\rfloor + 2} \right\rfloor = 0$$

ya que

$$\begin{cases} \frac{3m-m-1}{2m+2} = \frac{2m-1}{2m+2} < 1 & \text{si} \quad n = 3m\,, \\ \frac{3m+1-m-1}{2m+2} = \frac{2m}{2m+2} < 1 & \text{si} \quad n = 3m+1\,, \\ \frac{3m+2-m-1}{2m+2} = \frac{2m+1}{2m+2} < 1 & \text{si} \quad n = 3m+2\,. \end{cases}$$

□

Proposición 4.4.6. *Si $n \geq 6$, entonces*

$$i = \sum_{k=1}^{\lfloor \frac{n}{3} \rfloor} \left\lfloor \frac{n}{3k} \right\rfloor \overline{\mu}(k) . \tag{4.19}$$

Demostración. Si $n = 3m$ (lógicamente, $m \geq 2$, pues $n \geq 6$) entonces, por la proposición 4.2.6, se tiene

$$i = \sum_{k=1}^{m} \left\lfloor \frac{m}{k} \right\rfloor \overline{\mu}(k) = \sum_{k=1}^{\frac{n}{3}} \left\lfloor \frac{3m}{3k} \right\rfloor \overline{\mu}(k) = \sum_{k=1}^{\lfloor \frac{n}{3} \rfloor} \left\lfloor \frac{n}{3k} \right\rfloor \overline{\mu}(k) .$$

Si $n = 3m + 1$, comprobemos en primer lugar, que

$$\left\lfloor \frac{3m+1}{3k} \right\rfloor = \left\lfloor \frac{m}{k} + \frac{1}{3k} \right\rfloor = \left\lfloor \frac{m}{k} \right\rfloor . \tag{4.20}$$

En efecto, el mayor resto posible al dividir m entre k es $k - 1$, y entonces

$$\frac{k-1}{k} + \frac{1}{3k} = \frac{3k-2}{3k} < 1 ,$$

de donde se sigue nuestra afirmación (4.20). Con esto, tenemos

$$\sum_{k=1}^{\lfloor \frac{n}{3} \rfloor} \left\lfloor \frac{n}{3k} \right\rfloor \overline{\mu}(k) = \sum_{k=1}^{m} \left\lfloor \frac{3m+1}{3k} \right\rfloor \overline{\mu}(k) = \sum_{k=1}^{m} \left\lfloor \frac{m}{k} \right\rfloor \overline{\mu}(k) = i .$$

Si $n = 3m + 2$,

$$\sum_{k=1}^{\lfloor \frac{n}{3} \rfloor} \left\lfloor \frac{n}{3k} \right\rfloor \overline{\mu}(k) = \sum_{k=1}^{m} \left\lfloor \frac{3m+2}{3k} \right\rfloor \overline{\mu}(k) = \sum_{k=1}^{m} \left\lfloor \frac{m}{k} \right\rfloor \overline{\mu}(k) = i ,$$

pues

$$\left\lfloor \frac{3m+2}{3k} \right\rfloor = \left\lfloor \frac{m}{k} + \frac{2}{3k} \right\rfloor = \left\lfloor \frac{m}{k} \right\rfloor ,$$

dado que

$$\frac{k-1}{k} + \frac{2}{3k} = \frac{3k-1}{3k} < 1 .$$

□

Proposición 4.4.7. *Si $n \geq 6$, entonces*

$$2\overline{M}(n) + 3i = \sum_{k=1}^{\lfloor \frac{n}{3} \rfloor} g(n,k)\,\overline{\mu}\,(k)\,, \tag{4.21}$$

donde

$$g(n,k) = 3\left\lfloor \frac{n}{3k} \right\rfloor - 2\left\lfloor \frac{n}{2k} - \frac{1}{2} \right\rfloor .$$

Demostración. Por la proposición 4.4.5 se tiene

$$\overline{M}(n) = -\sum_{k=1}^{\lfloor \frac{n}{3} \rfloor} \left\lfloor \frac{n-k}{2k} \right\rfloor \overline{\mu}\,(k)$$

y, por la proposición 4.4.6,

$$i = \sum_{k=1}^{\lfloor \frac{n}{3} \rfloor} \left\lfloor \frac{n}{3k} \right\rfloor \overline{\mu}\,(k)\,.$$

Por tanto

$$\begin{aligned} 2\overline{M}(n) + 3i &= \sum_{k=1}^{\lfloor \frac{n}{3} \rfloor} \left(3\left\lfloor \frac{n}{3k} \right\rfloor - 2\left\lfloor \frac{n-k}{2k} \right\rfloor \right) \overline{\mu}\,(k) \\ &= \sum_{k=1}^{\lfloor \frac{n}{3} \rfloor} g(n,k)\,\overline{\mu}\,(k)\,. \end{aligned}$$

□

Proposición 4.4.8. *Si $3 \leq b \leq n-1$, entonces*

$$2\overline{M}(n) + 3i = \sum_{k=1}^{\lfloor \frac{n}{b+1} \rfloor} g(n,k)\,\overline{\mu}\,(k) + \sum_{a=3}^{b} h(a)\left(\overline{M}\left(\frac{n}{a}\right) - \overline{M}\left(\frac{n}{a+1}\right) \right), \tag{4.22}$$

donde $h(a)$ es la función definida en (3.7).

Demostración. Partimos el sumatorio de la parte derecha de (4.21) en dos sumatorios y operamos convenientemente. Así,

$$2\overline{M}(n) + 3i = \sum_{k=1}^{\lfloor \frac{n}{3} \rfloor} g(n,k)\,\overline{\mu}\,(k)$$

$$= \sum_{k=1}^{\left\lfloor \frac{n}{b+1} \right\rfloor} g(n,k)\,\overline{\mu}\,(k) + \sum_{a=3}^{b} \sum_{k=\left\lfloor \frac{n}{a+1} \right\rfloor + 1}^{\left\lfloor \frac{n}{a} \right\rfloor} g(n,k)\,\overline{\mu}\,(k)$$

$$= \sum_{k=1}^{\left\lfloor \frac{n}{b+1} \right\rfloor} g(n,k)\,\overline{\mu}\,(k) + \sum_{a=3}^{b} h(a) \sum_{k=\left\lfloor \frac{n}{a+1} \right\rfloor + 1}^{\left\lfloor \frac{n}{a} \right\rfloor} \overline{\mu}\,(k)$$

$$= \sum_{k=1}^{\left\lfloor \frac{n}{b+1} \right\rfloor} g(n,k)\,\overline{\mu}\,(k) + \sum_{a=3}^{b} h(a) \left(\overline{M}\left(\left\lfloor \frac{n}{a} \right\rfloor \right) - \overline{M}\left(\left\lfloor \frac{n}{a+1} \right\rfloor \right) \right) .$$

□

Despejando $\overline{M}(n)$ en (4.22) obtenemos una fórmula, análoga a la establecida en el capítulo anterior para $M(n)$, que nos permite calcular $\overline{M}(n)$.

Designamos

$$\overline{H}(n,m) := \sum_{k=1}^{m} g(n,k)\,\overline{\mu}\,(k)\,,$$

y

$$C_m := 6 \cdot (\operatorname{mcm}\{1,2,\ldots,m\})\ .$$

Con esta notación, tenemos

Proposición 4.4.9.

$$\overline{H}(n + tC_m, m) = \overline{H}(n,m)\,, \tag{4.23}$$

donde t es un entero tal que $n + tC_m > 0$.

Demostración. Como $g(n + \dot{\overline{6k}}, k) = g(n,k)$, para $k = 1,2,\ldots,m$ se tiene que $g(n + \dot{\overline{C_m}}, k) = g(n,k)$, luego

$$\overline{H}(n + tC_m, m) = \sum_{k=1}^{m} g(n + tC_m, k)\,\overline{\mu}\,(k) = \sum_{k=1}^{m} g(n,k)\,\overline{\mu}\,(k) = \overline{H}(n,m)\,.$$

□

La proposición siguiente nos relaciona el valor de $\overline{H}(n,m)$ con el valor de $\overline{M}(m)$.

Proposición 4.4.10.

$$\overline{H}(0+\dot{\overline{C_m}},m)=2\overline{M}(m)\,, \tag{4.24}$$

$$\overline{H}(1+\dot{\overline{C_m}},m)=2\overline{M}(m)-2\,, \tag{4.25}$$

$$\overline{H}(2+\dot{\overline{C_m}},m)=2\overline{M}(m)+2-2i\,, \tag{4.26}$$

$$\overline{H}(n+\dot{\overline{C_m}},m)=2\overline{M}(m)+3i\,,\ \ si\ 2<n\leq m\,. \tag{4.27}$$

Demostración. Para probar (4.24), basta usar

$$\overline{H}(0,m)=\sum_{k=1}^{m}g(0,k)\,\overline{\mu}\,(k)=2\sum_{k=1}^{m}\overline{\mu}\,(k)=2\overline{M}(m)\,.$$

La fórmula (4.25) se obtiene como sigue:

$$\overline{H}(1,m)=\sum_{k=1}^{m}g(1,k)\,\overline{\mu}\,(k)=0\cdot\,\overline{\mu}\,(1)+2\sum_{k=2}^{m}\overline{\mu}\,(k)=2\sum_{k=1}^{m}\overline{\mu}\,(k)-2$$

$$=2\overline{M}(m)-2\,.$$

Y (4.26) se obtiene así:

$$\overline{H}(2,m)=\sum_{k=1}^{m}g(2,k)\,\overline{\mu}\,(k)=0\cdot\,\overline{\mu}\,(1)+0\cdot\,\overline{\mu}\,(2)+2\sum_{k=3}^{m}\overline{\mu}\,(k)$$

$$=2\sum_{k=1}^{m}\overline{\mu}\,(k)-2\,\overline{\mu}\,(1)-2\,\overline{\mu}\,(2)=2\overline{M}(m)-2+4-2i=2\overline{M}(m)+2-2i\,.$$

Finalmente, para probar (4.27), vemos que si $2<n\leq m$, entonces

$$\overline{H}(n,m)=\sum_{k=1}^{m}g(n,k)\,\overline{\mu}\,(k)=\sum_{k=1}^{n}g(n,k)\,\overline{\mu}\,(k)+\sum_{k=n+1}^{m}g(n,k)\,\overline{\mu}\,(k)$$

$$=\sum_{k=1}^{\lfloor\frac{n}{3}\rfloor}g(n,k)\,\overline{\mu}\,(k)+\sum_{k=\lfloor\frac{n}{3}\rfloor+1}^{n}g(n,k)\,\overline{\mu}\,(k)+\sum_{k=n+1}^{m}g(n,k)\,\overline{\mu}\,(k)$$

$$=2\overline{M}(n)+3i+2\sum_{k=n+1}^{m}\overline{\mu}\,(k)=2\overline{M}(n)+3i+2\overline{M}(m)-2\overline{M}(n)=2\overline{M}(m)+3i\,.$$

Si

$$\left\lfloor\frac{n}{3}\right\rfloor+1\leq k\leq n\,,$$

es claro que

$$k \le n < 3\left(\left\lfloor \frac{n}{3} \right\rfloor + 1\right) \le 3k$$

y por lo tanto se verifica $g(n,k) = 0$. Si

$$n+1 \le k \le m\,,$$

se tiene

$$0 \le n < k$$

y ahora $g(n,k) = 2$. □

Proposición 4.4.11. *Sea*

$$\overline{G}\,(n,b) := \sum_{a=3}^{b} h(a)\left(\overline{M}\left(\frac{n}{a}\right) - \overline{M}\left(\frac{n}{a+1}\right)\right)$$

y sea $b = b_0 + 6b_1$ *con* $0 \le b_0 < 6$. *Entonces*

$$\begin{aligned}\overline{G}\,(n,b) &= \overline{M}\left(\frac{n}{3}\right) - 2\overline{M}\left(\frac{n}{5}\right)\\ &\quad + \sum_{t=1}^{b_1-1}\left(3\overline{M}\left(\frac{n}{6t}\right) - 2\overline{M}\left(\frac{n}{6t+1}\right) + \overline{M}\left(\frac{n}{6t+3}\right) - 2\overline{M}\left(\frac{n}{6t+5}\right)\right)\\ &\quad + \overline{M}\left(\frac{n}{6b_1}\right) + \sum_{r=0}^{b_0} h(r)\left(\overline{M}\left(\frac{n}{6b_1+r}\right) - \overline{M}\left(\frac{n}{6b_1+r+1}\right)\right)\,.\end{aligned} \tag{4.28}$$

Demostración. En la definición de $\overline{G}$ sustituimos $h(a)$ por sus valores

$$\begin{aligned}\overline{G}\,(n,b) &= \sum_{a=3}^{b_0+6b_1} h(a)\left(\overline{M}\left(\frac{n}{a}\right) - \overline{M}\left(\frac{n}{a+1}\right)\right) = \overline{M}\left(\frac{n}{3}\right) - \overline{M}\left(\frac{n}{4}\right)\\ &+\overline{M}\left(\frac{n}{4}\right) - \overline{M}\left(\frac{n}{5}\right) - \overline{M}\left(\frac{n}{5}\right) + \overline{M}\left(\frac{n}{6}\right) + 2\overline{M}\left(\frac{n}{6}\right) - 2\overline{M}\left(\frac{n}{7}\right) + \overline{M}\left(\frac{n}{9}\right)\\ &-\overline{M}\left(\frac{n}{10}\right) + \overline{M}\left(\frac{n}{10}\right) - \overline{M}\left(\frac{n}{11}\right) - \overline{M}\left(\frac{n}{11}\right) + \overline{M}\left(\frac{n}{12}\right) + 2\overline{M}\left(\frac{n}{12}\right) + \cdots\\ &= \overline{M}\left(\frac{n}{3}\right) - 2\overline{M}\left(\frac{n}{5}\right)\\ &\quad + \sum_{t=1}^{b_1-1}\left(3\overline{M}\left(\frac{n}{6t}\right) - 2\overline{M}\left(\frac{n}{6t+1}\right) + \overline{M}\left(\frac{n}{6t+3}\right) - 2\overline{M}\left(\frac{n}{6t+5}\right)\right)\\ &\quad + \overline{M}\left(\frac{n}{6b_1}\right) + \sum_{r=0}^{b_0} h(6b_1+r)\left(\overline{M}\left(\frac{n}{6b_1+r}\right) - \overline{M}\left(\frac{n}{6b_1+r+1}\right)\right)\,,\end{aligned}$$

y la demostración se completa recordando que $h(6b_1 + r) = h(r)$. □

Al igual que se hace en [13, 38], utilizaremos la notación

$$Q(n) := \sum_{k=1}^{n} |\mu(k)| \,.$$

Más adelante, nos resultará útil la siguiente propiedad, que resulta ser una ligera modificación sobre una propiedad ya conocida para Q:

Proposición 4.4.12. *Si $n \geq 1$ entonces*

$$\left| Q(n) - \frac{6n}{\pi^2} \right| < \sqrt{n} \,.$$

Demostración. Moser y MacLeod, en [31], probaron que, si $n > 0$, entonces

$$\left| Q(n) - \frac{6n}{\pi^2} \right| \leq \frac{13}{18}\sqrt{n} + \frac{9}{2} \,.$$

Dado que si $\frac{5}{18}\sqrt{n} > \frac{9}{2}$ entonces $\frac{13}{18}\sqrt{n} + \frac{9}{2} < \sqrt{n}$, tenemos la proposición probada para todos los valores de n que verifican $n > \left(\frac{81}{5}\right)^2 = 262.44$, esto es, para todos los valores de $n \geq 263$.

Por simple comprobación directa se tiene que la proposición es cierta para $1 \leq n \leq 263$. □

La función análoga a Q será

$$\overline{Q}(n) := \sum_{k=1}^{n} |\,\overline{\mu}\,(k)| \,.$$

Ahora vamos a probar algunas propiedades sobre dicha función $\overline{Q}$.

Proposición 4.4.13.

$$\left| \overline{Q}(n) - \frac{4 + 2\sqrt{5} + \sqrt{2}}{\pi^2} n \right| < \left(3 + \sqrt{2} - \sqrt{5}\right) \sqrt{n} \,. \tag{4.29}$$

Demostración. En la definición de $\overline{Q}$ los sumandos correspondientes a $k = \dot{8}$ son cero. Agrupamos los restantes sumandos en tres sumatorios y operamos convenientemente. Así,

$$\overline{Q}(n) = \sum_{k=1}^{n} |\,\overline{\mu}\,(k)| = \sum_{\substack{k=1 \\ (k,2)=1}}^{n} |\,\overline{\mu}\,(k)| + \sqrt{5} \sum_{\substack{k=1 \\ (k,2)=1}}^{\frac{n}{2}} |\,\overline{\mu}\,(k)| + \sqrt{2} \sum_{\substack{k=1 \\ (k,2)=1}}^{\frac{n}{4}} |\,\overline{\mu}\,(k)|$$

$$= Q(n) + (\sqrt{5}-1)Q\left(\frac{n}{2}\right) + \left(\sqrt{2}+1-\sqrt{5}\right) \sum_{\substack{k=1 \\ (k,2)=1}}^{\frac{n}{4}} |\,\overline{\mu}\,(k)| = Q(n)$$

$$+(\sqrt{5}-1)Q\left(\frac{n}{2}\right) + \left(\sqrt{2}+1-\sqrt{5}\right)\left(Q\left(\frac{n}{4}\right) - Q\left(\frac{n}{8}\right) + Q\left(\frac{n}{16}\right) + \cdots\right),$$

$$\overline{Q}(n) < \frac{6}{\pi^2}n + \sqrt{n} + (\sqrt{5}-1)\left(\frac{6}{\pi^2}\frac{n}{2} + \sqrt{\frac{n}{2}}\right)$$

$$+\left(\sqrt{2}+1-\sqrt{5}\right)\left(\frac{6}{\pi^2}\frac{n}{4} + \sqrt{\frac{n}{4}} - \frac{6}{\pi^2}\frac{n}{8} + \sqrt{\frac{n}{8}} + \frac{6}{\pi^2}\frac{n}{16} + \sqrt{\frac{n}{16}} + \cdots\right)$$

$$= \frac{6}{\pi^2}n\left(1 + \frac{\sqrt{5}-1}{2} + \left(\sqrt{2}+1-\sqrt{5}\right)\frac{\frac{1}{4}}{1+\frac{1}{2}}\right)$$

$$+\sqrt{n}\left(1 + \frac{\sqrt{5}-1}{\sqrt{2}} + \left(\sqrt{2}+1-\sqrt{5}\right)\frac{\frac{1}{2}}{1-\frac{1}{\sqrt{2}}}\right)$$

$$= \frac{4+2\sqrt{5}+\sqrt{2}}{\pi^2}n + \left(3+\sqrt{2}-\sqrt{5}\right)\sqrt{n}\,,$$

$$\overline{Q}(n) > \frac{6}{\pi^2}n - \sqrt{n} + (\sqrt{5}-1)\left(\frac{6}{\pi^2}\frac{n}{2} - \sqrt{\frac{n}{2}}\right)$$

$$+\left(\sqrt{2}+1-\sqrt{5}\right)\left(\frac{6}{\pi^2}\frac{n}{4} - \sqrt{\frac{n}{4}} - \frac{6}{\pi^2}\frac{n}{8} - \sqrt{\frac{n}{8}} + \frac{6}{\pi^2}\frac{n}{16} - \sqrt{\frac{n}{16}} - \cdots\right)$$

$$= \frac{4+2\sqrt{5}+\sqrt{2}}{\pi^2}n - \left(3+\sqrt{2}-\sqrt{5}\right)\sqrt{n}\,.$$

□

Corolario 4.4.14. *Si $n > 2179$, entonces $\overline{Q}(n) > n$.*

Demostración. El coeficiente de n en (4.29) verifica

$$\frac{4+2\sqrt{5}+\sqrt{2}}{\pi^2} > 1.001696635\,,$$

y el coeficiente de $\sqrt{n}$ verifica

$$3+\sqrt{2}-\sqrt{5} < 2.178145585\,.$$

Aplicando estas desigualdades a (4.29) tenemos

$$1.001696635n - 2.178145585\sqrt{n} < \overline{Q}(n)\,,$$

$$\sqrt{n}(0.001696635\sqrt{n} - 2.178145585) < \overline{Q}(n) - n\,.$$

Con todo esto es fácil comprobar que si $n > 1648150$ entonces $\overline{Q}(n) - n > 0$.

Finalmente, un laborioso cálculo directo (con ayuda de un manipulador algebraico) nos permite establecer que, para $2179 < n < 1648151$,

$$\overline{Q}(n) > n\,.$$

□

Corolario 4.4.15. *Si $n > 55448$, entonces $\overline{Q}(n) < 1.002n$.*

Demostración. Como consecuencia de (4.29), tenemos

$$\overline{Q}(n) < 1.001696635003n + 2.178145584874\sqrt{n}\,.$$

Si $n > 51551685$, entonces

$$1.001696635003n + 2.178145584874\sqrt{n} < 1.002n\,;$$

por lo tanto si $n > 51551685$, se verifica

$$\overline{Q}(n) < 1.002n\,.$$

Para $55448 < n < 51551686$, un manipulador algebraico nos sirve para comprobar, de manera directa, que

$$\overline{Q}(n) < 1.002n\,.$$

□

Corolario 4.4.16. *Si $n > 46$, entonces $\overline{Q}(n) < 1.1n$.*

Demostración. Si $n > 491$, entonces

$$1.001696635003n + 2.178145584874\sqrt{n} < 1.1n\,,$$

luego, en este caso,

$$\overline{Q}(n) < 1.1n\,.$$

Por comprobación directa se establece que, para $46 < n < 492$,

$$\overline{Q}(n) < 1.1n\,.$$

□

En [13, pág. 49], se establece el siguiente resultado:

Lema 4.4.17. *La función*

$$f(x) := \lfloor x \rfloor - \left\lfloor \frac{x}{2} \right\rfloor - \left\lfloor \frac{x}{3} \right\rfloor - \left\lfloor \frac{x}{6} \right\rfloor$$

es periódica de periodo 6 *y verifica que*

$$\begin{array}{llll} si & 1 \leq x < 5 & es & f(x) = 1\,, \\ si & 1 \leq x & es & |1 - f(x)| \leq 1\,. \end{array}$$

Utilizaremos esta propiedad para demostrar lo siguiente:

Proposición 4.4.18. *Si* $n > 5$, $|\overline{M}(n)| < 0.225n$.

Demostración. Sea

$$S(x) = \sum_{n \leq x} \overline{\mu}\,(n) \left(1 - f\left(\frac{x}{n}\right)\right)\,. \tag{4.30}$$

Entonces

$$S(x) = \sum_{n \leq x} \left(\overline{\mu}\,(n) - \left\lfloor \frac{x}{n} \right\rfloor \overline{\mu}\,(n) + \left\lfloor \frac{x}{2n} \right\rfloor \overline{\mu}\,(n) + \left\lfloor \frac{x}{3n} \right\rfloor \overline{\mu}\,(n) + \left\lfloor \frac{x}{6n} \right\rfloor \overline{\mu}\,(n) \right)$$

y por la proposición 4.2.6 tenemos

$$S(x) = \overline{M}(x) - i + i + i + i = \overline{M}(x) + 2i\,. \tag{4.31}$$

Por otra parte, tomando módulos en (4.30), tenemos

$$|S(x)| = \left| \sum_{n \leq x} \overline{\mu}\,(n) \left(1 - f\left(\frac{x}{n}\right)\right) \right|$$

$$= \left| \sum_{n \leq \frac{x}{5}} \overline{\mu}\,(n) \left(1 - f\left(\frac{x}{n}\right)\right) \right| \leq \sum_{n \leq \frac{x}{5}} |\,\overline{\mu}\,(n)| = \overline{Q}\left(\frac{x}{5}\right)\,,$$

esto es

$$|S(x)| \leq \overline{Q}\left(\frac{x}{5}\right)\,. \tag{4.32}$$

A partir de (4.31) y (4.32) se sigue

$$\left|\overline{M}(x) + 2i\right| \leq \overline{Q}\left(\frac{x}{5}\right)\,.$$

Dado que si $x > 400$, entonces $\frac{x}{5} > 80 > 46$, utilizando la desigualdad triangular y el corolario 4.4.16, tenemos que para $x > 400$ se verifica

$$\left|\overline{M}(x)\right| \leq 2 + \overline{Q}\left(\frac{x}{5}\right) < 0.22x + 2\,.$$

Por otra parte, si $x > 400$,

$$0.225x > 0.22x + 2\,.$$

Así, tenemos probado que si $x > 400$, entonces se verifica

$$\left|\overline{M}(x)\right| < 0.225x\,.$$

Finalmente, por comprobación directa se establece que, para $6 \leq x < 401$,

$$\left|\overline{M}(x)\right| < 0.225x\,.$$

□

Capítulo 5

Sucesiones alicuatorias

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

$$\sigma(p_1^{a_1} \cdots p_k^{a_k}) = (1 + p_1 + \cdots + p_1^{a_1}) \cdots (1 + p_k + \cdots + p_k^{a_k}). \tag{5.1}$$

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:

$$\sigma(n) = \frac{p_1^{a_1+1} - 1}{p_1 - 1} \cdots \frac{p_k^{a_k+1} - 1}{p_k - 1}. \tag{5.2}$$

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 sobre el tema, y que incide en su aspecto computacional, es [44]):

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 39; el mayor, encontrado el 14 de Noviembre de 2001, es $2^{13466917}-1$, que tiene 4053946 cifras (existe un premio de 100000 dólares para la primera persona que encuentre un primo de diez millones 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 cinco últimos primos de Mersenne conocidos han sido descubiertos 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 (ver, por ejemplo, [37]). 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 diciembre de 2001, se han encontrado 110 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. Un listado de todos puede encontrarse en `http://xraysgi.ims.uconn.edu:8080/sociable.txt`

Intocables de Erdős: Se llaman así a los n tales que $n \neq s(m)$ para todo m. Por ejemplo, 2 y 5. En 1973, el mismo Erdős probó en [14] que existen infinitos de ellos y que su densidad inferior es positiva.

5.1. 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 [8] en 1887 y L. E. Dickson [12] 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. P. Erdős, en [15], afirma que H. W. Lenstra probó el siguiente resultado:

Teorema 5.1.1. *Para todo número natural k, existe un número natural m, tal que*

$$m = s^0(m) < s^1(m) < \cdots < s^k(m)\,.$$

En el artículo de Erdős aparece la demostración, que Lenstra no había publicado previamente, y que reproducimos aquí. Antes de empezar la demostración, vamos a dar algunos lemas previos y fijar algunas notaciones.

Designamos por p_i al i-ésimo primo. Así, $p_1 = 2$, $p_2 = 3$, $p_3 = 5$, ...

Usaremos $\varphi(n)$ para denotar la función característica de Euler, esto es, $\varphi(n)$ es el número de números naturales menores que n que son primos con n.

La notación $p^\alpha || n$ significa que $p^\alpha | n$ y $p^{\alpha+1} \nmid n$.

Lema 5.1.2. *Los múltiplos propios de un número perfecto o abundante son abundantes.*

Demostración. Sea n un número perfecto ($\sigma(n) = 2n$) o abundante ($\sigma(n) > 2n$), esto es, $\sigma(n) \geq 2n$; y sea $l > 1$ un número natural.

Si los divisores de n son $1, d_1, d_2, \ldots, d_k$, los números $l, ld_1, ld_2, \ldots, ld_k$, son divisores de ln, por tanto

$$\sigma(ln) \geq 1 + l + ld_1 + ld_2 + \cdots + ld_k > l(1 + d_1 + d_2 + \cdots + d_k) = l\sigma(n) \geq 2ln\,,$$

luego ln es abundante. □

Lema 5.1.3. *La sucesión $\{t_i\}_{i\in\mathbb{N}}$ definida mediante $t_1 = 2$,*

$$t_{i+1} = \varphi\left(p_i^{t_i+1}\,(p_{i+1} - 1)\right) - 1\,,$$

verifica la propiedad de que

$$p_i^{t_i+1} | \sigma\left(p_{i+1}^{t_{i+1}}\right) \qquad \text{para } i \geq 1\,. \tag{5.3}$$

Demostración. Por el teorema de Euler-Fermat sabemos que

$$p_{i+1}^{t_{i+1}+1} = p_{i+1}^{\varphi\left(p_i^{t_i+1}(p_{i+1}-1)\right)} \equiv 1 \mod \left(p_i^{t_i+1}(p_{i+1}-1)\right).$$

Por tanto

$$p_{i+1}^{t_{i+1}+1} - 1 = \overline{p_i^{t_i+1}(p_{i+1}-1)},$$

luego

$$\sigma\left(p_{i+1}^{t_{i+1}}\right) = \frac{p_{i+1}^{t_{i+1}+1}-1}{p_{i+1}-1} = \overline{p_i^{t_i+1}}.$$

□

Lema 5.1.4. *Para $l \geq 1$, sea*

$$A_l = \left\{m \in \mathbb{N} \ : \ p_i^{t_i} || m, \ 1 \leq i \leq l\right\}.$$

Si $m \in A_l$, $l \geq 2$, entonces $s(m) > m$ y $s(m) \in A_{l-1}$.

Demostración. Para $l \geq 2$, tenemos que $6|m$. Como 6 es perfecto, por el lema 5.1.2, m es abundante. O sea, $s(m) > m$.

Si $m \in A_l$ entonces existe un número natural B tal que $m = p_1^{t_1} \cdot \ldots \cdot p_l^{t_l} \cdot B$, con mcd $\left(B, \frac{m}{B}\right) = 1$. Además, para $1 \leq i \leq l$, tenemos $p_i^{t_i} || m$.

Por la propiedad (5.3), existen l números naturales δ_i con $\sigma\left(p_{i+1}^{t_{i+1}}\right) = \delta_i \cdot p_i^{t_i+1}$, luego

$$s(m) = \sigma(m) - m = \sigma\left(p_1^{t_1}\right) \cdot \ldots \cdot \sigma\left(p_l^{t_l}\right) \cdot \sigma(B) - p_1^{t_1} \cdot \ldots \cdot p_l^{t_l} \cdot B.$$

Como $\sigma\left(p_1^{t_1}\right) = \sigma\left(2^2\right) = 7$, tenemos que

$$s(m) = 7 \cdot \delta_1 \cdot p_1^{t_1+1} \cdot \delta_2 \cdot p_2^{t_2+1} \cdot \ldots \cdot \delta_{l-1} \cdot p_{l-1}^{t_{l-1}+1} \cdot \sigma(B) - p_1^{t_1} \cdot \ldots \cdot p_l^{t_l} \cdot B$$

$$= p_1^{t_1} \cdot p_2^{t_2} \cdot \ldots \cdot p_{l-1}^{t_{l-1}} \left(7 \cdot \delta_1 \cdot \delta_2 \cdot \ldots \cdot \delta_{l-1} \cdot p_1 \cdot p_2 \cdot \ldots \cdot p_{l-1} \cdot \sigma(B) - p_l^{t_l} B\right).$$

Finalmente, al ser B primo con $p_1 \cdot p_2 \cdot \ldots \cdot p_l$, tenemos

$$p_1^{t_1} || s(m), \quad p_2^{t_2} || s(m), \quad \ldots, \quad p_{l-1}^{t_{l-1}} || s(m),$$

luego $s(m) \in A_{l-1}$. □

Estamos ya en condiciones de demostrar el teorema de Lenstra:

Demostración del teorema 5.1.1. Dado $m \in A_{k+1}$, tenemos

$$s(m) \in A_k,\ s^2(m) \in A_{k-1},\ \ldots,\ s^{k-1}(m) \in A_2,\ s^k(m) \in A_1$$

y

$$m < s(m) < s^2(m) < \cdots < s^k(m)\,.$$

□

A primera vista, este teorema parece ser un argumento en contra de la certeza de la conjetura de Catalan-Dickson, pero el rápido crecimiento de los términos de la sucesión $\{t_i\}_{i\in\mathbb{N}}$ diluye la fuerza de este argumento. Los primeros cuatro términos de la sucesión $\{t_i\}_{i\in\mathbb{N}}$ son

$$\begin{aligned} t_1 &= 2\,,\\ t_2 &= \varphi\left(2^3(3-1)\right) - 1 = 7\,,\\ t_3 &= \varphi\left(3^8(5-1)\right) - 1 = 8747\,,\\ t_4 &= \varphi\left(5^{8748}(7-1)\right) - 1\,. \end{aligned}$$

Expresado en base diez, t_4 es un número de 6115 dígitos. Sin embargo, el número más pequeño para el que se verifica $m < s(m) < s^2(m) < s^3(m)$, es 30. La sucesión alicuatoria de 30 es

$$30, 42, 54, 66, 78, 90, 144, 259, 45, 33, 15, 9, 4, 3, 1\,.$$

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 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 sobre el final de la sucesión que comienza en él fue $n = 138$ (Poulet, 1918). La incertidumbre fue resuelta 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, W. Creyaufmüller y nosotros. Además, en algunas factorizaciones se ha contado con la colaboración de S. Wagstaff, A. Lenstra y Yuji Kida. Actualmente, se ha llegado hasta $s^{1283}(276)$, un número de 117 cifras.

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 (5.2). Pero la dificultad radica en que la sucesión puede alcanzar términos muy grandes. Para poder seguir, (5.2) 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 [19, capítulo 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, se han estudiado todas las sucesiones que comienzan en un número n menor de 10000. En todas ellas, se ha avanzado hasta términos mayores que 10^{96} y se ha encontrado el final de algunas que anteriormente estaban en duda. Más adelante comentamos con mayor detalle nuestro trabajo con estas sucesiones.

Por último, W. Creyaufmüller [10] 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. Puede encontrarse información actualizada en `http://home.t-online.de/home/Wolfgang.Creyaufmueller/aliquote.htm`.

Además de esta página web, existen otras tres dedicadas a los progresos en sucesiones alicuatorias: La mantenida por J. L. Varona, `http://www.unirioja.es/dptos/dmc/jvarona/aliquot.html`, la de W. Bosma, `http://www-math.sci.kun.nl/math/~bosma/nuth/ali.html`, y la de P. Zimmermann `http://www.loria.fr/~zimmerma/records/aliquot.html`.

Todo el esfuerzo computacional para ir calculando términos de una sucesión alicuatoria se hace aplicando las fórmulas (5.1) o (5.2). Como comentábamos anteriormente, 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 [36, capítulo 6].

5.2. 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 (5.1), $s(n) = (1+2+4+8) \cdot 4 \cdot 6 \cdot (p+1) \cdot (q+1) - 2^3 \cdot 3 \cdot 5 \cdot p \cdot q = 15 \cdot 2^2 \cdot 2 \cdot 3 \cdot (p+1) \cdot (q+1) - 2^3 \cdot 3 \cdot 5 \cdot p \cdot q = 2^3 \cdot 3 \cdot 5 \cdot [3 \cdot (p+1) \cdot (q+1) - p \cdot q] = 2^3 \cdot 3 \cdot 5 \cdot m$, 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. Recordemos, además, que (tal como hemos comprobado en el lema 5.1.2) si m es un número perfecto (o abundante) y m divide propiamente a n, entonces $s(n) > n$.

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 $p, q \equiv 1 \bmod 4$, entonces desaparece el 2^3 y surge, en su lugar, 2^2. Si $p, q \equiv 3 \bmod 4$, se mantiene el 2^3. Si $p \equiv 1$ y $q \equiv 3 \bmod 4$, entonces al menos aparece el factor 2^3; pero la potencia de 2 aumenta si 8 no divide a $q+1$, es decir, si $q \equiv 3 \bmod 8$.

La existencia de estructuras estables ha sido analizada rigurosamente y plasmada en forma de definiciones generales. Así, Guy y Selfridge [20] 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 $\mathrm{mcd}(m, 15) \neq 1$.

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 (ver [20]): 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 posibilidad 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.

5.3. Nuestros progresos con sucesiones alicuatorias

Tal como comentábamos anteriormente, nos hemos preocupado en estudiar computacionalmente las sucesiones alicuatorias que comienzan en $n < 10000$. Este trabajo ha supuesto avances 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 [18], que habían analizado las sucesiones que comenzaban en $n \leq 7044$. Fruto de este trabajo, hemos hallado el final de varias sucesiones, concretamente las que comienzan en $n = 6792$, 8262, 7080, 3556, 4170, 3630, 6160 y 7422. Para cada una de estas sucesiones $\{s^k(n)\}_{k\in\mathbb{N}}$, en las figuras 5.1, 5.2, 5.3, 5.4, 5.5, 5.6, 5.7 y 5.8 representamos, en abscisas, el número de iteración k y, en ordenadas, el logaritmo en base 10 del número $s^k(n)$ alcanzado. Comentemos a continuación estos resultados:

- La sucesión que comienza en 6792 alcanza el 1 después de 1341 iteraciones, siendo 59 el primo previo. El máximo alcanzado es

$$\begin{aligned} s^{659}(6792) &= 894638342683032483224656500048971888841494754216 \\ &= 2\cdot 2\cdot 2\cdot 83\cdot 5851\cdot 13001 \\ &\cdot 177122026153789678892954905119357626 9\,, \end{aligned}$$

  un número de 47 cifras.

- La sucesión que comienza en 8262 alcanza el 1 después de 773 iteraciones, siendo 317 el primo previo. El máximo alcanzado es

$$\begin{aligned} & s^{444}(8262) \\ &= 10581239574507789499350951865022410233252169593450 26 \\ &= 2\cdot 223\cdot 8831\cdot 1256153653\cdot 7873472183 \\ &\cdot 27163313185808805688909099\,, \end{aligned}$$

  un número de 52 cifras.

- La sucesión que empieza en 7080 alcanza el 1 después de 1264 iteraciones, siendo 37 el primo previo. Aquí y en lo sucesivo, el símbolo \ significa que la expresión decimal del número continúa en la línea siguiente. Así, el máximo alcanzado es

$$\begin{aligned} s^{539}(7080) &= 335667604077269949393384678421830608905222618241\backslash \\ &\qquad 8412008219112234936 \\ &= 2\cdot 2\cdot 2\cdot 419\cdot 34110465457\cdot 1418417145283289 \\ &\cdot 20697305061593509314923291434129565941\,, \end{aligned}$$

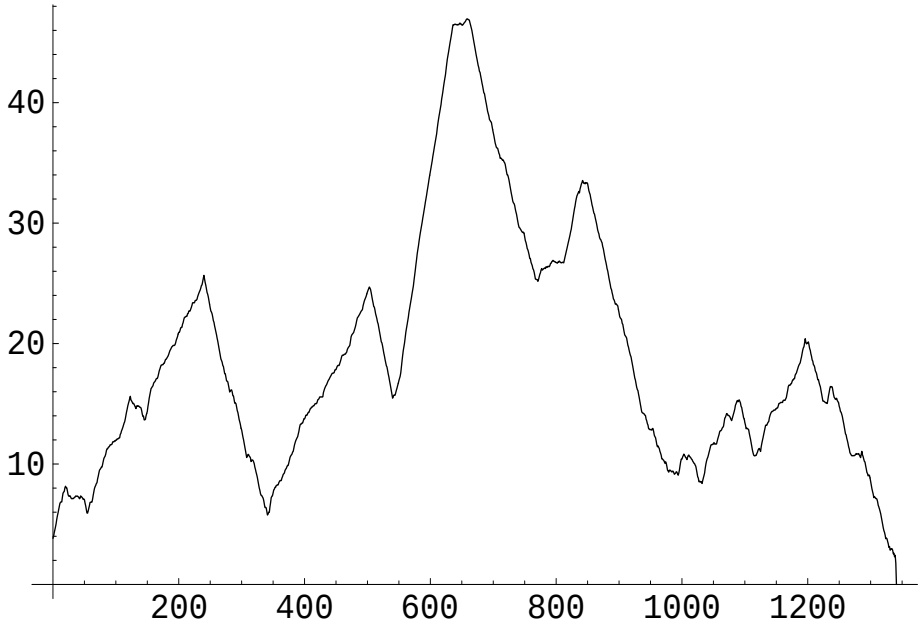

Figura 5.1: Sucesión alicuatoria 6792.

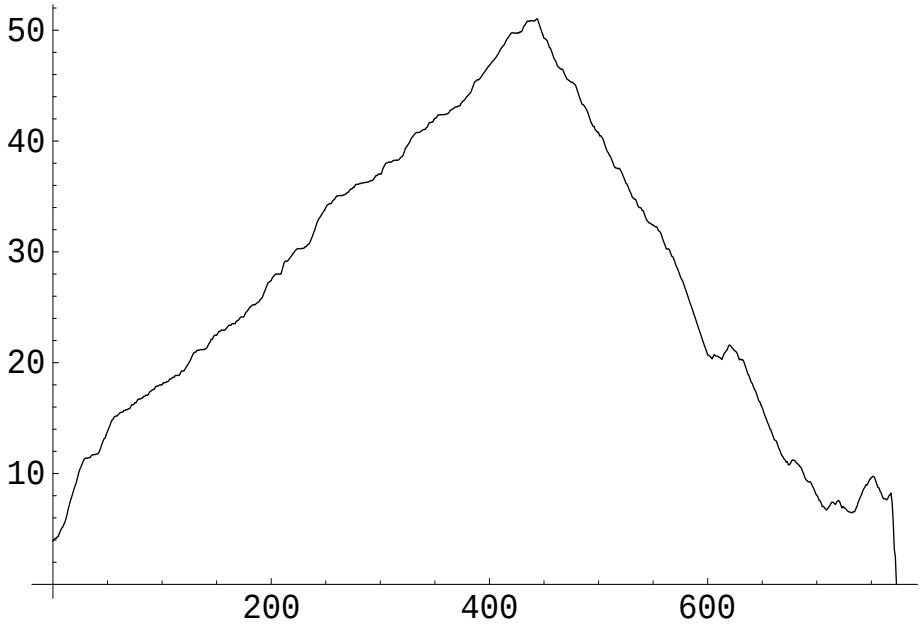

Figura 5.2: Sucesión alicuatoria 8262.

un número de 67 cifras.

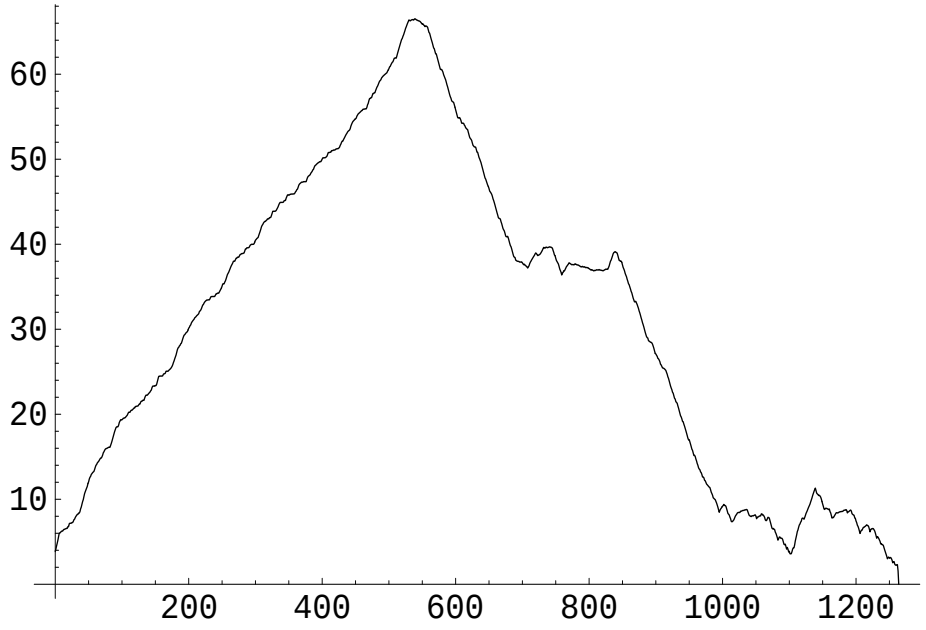

Figura 5.3: Sucesión alicuatoria 7080.

- La sucesión que empieza en 3556 alcanza el 1 después de 2058 iteraciones, siendo 59 el primo previo. El máximo alcanzado es

$$s^{551}(3556) = 476372841845828677729108156155573671704082265291532247964505425538142202028 = 2 \cdot 2 \cdot 503 \cdot 24359 \cdot 7455102267576203135197 \cdot 100819403542569743 \cdot 1293188498225949716200056532 1,$$

un número de 75 cifras.

- La sucesión que empieza en 4170 alcanza el 1 después de 869 iteraciones, siendo 79 el primo previo. El máximo alcanzado es

$$s^{289}(4170) = 32956108034247721274720369286336621383383870315885822327064032192093690321488891836 = 2 \cdot 2 \cdot 41 \cdot 97 \cdot 20374357 \cdot 1559593537 \cdot 651966073954976081342107597832287652091395156174990523498331163,$$

un número de 84 cifras.

Figura 5.4: Sucesión alicuatoria 3556.

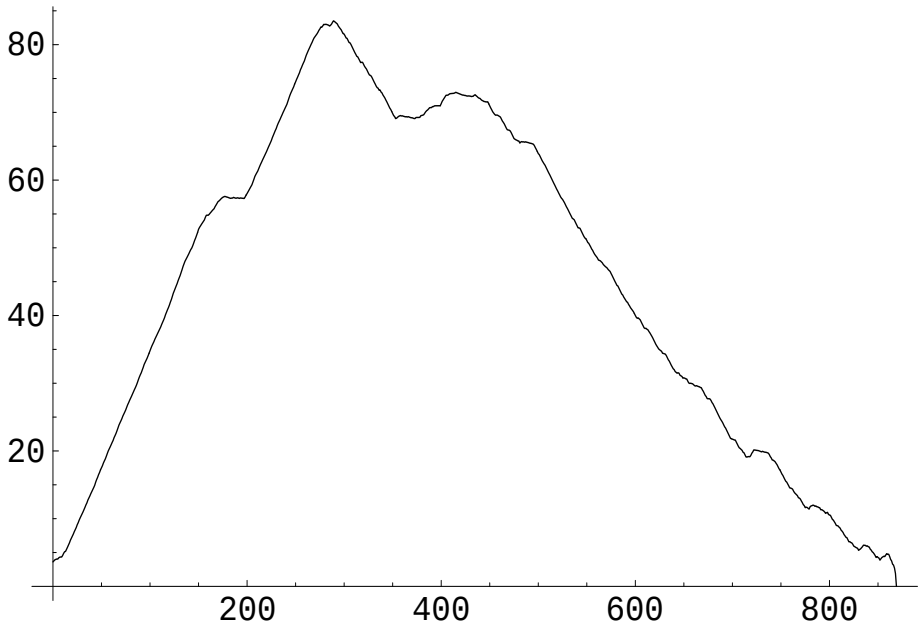

Figura 5.5: Sucesión alicuatoria 4170.

Ésta fue, desde el 22 de Diciembre de 1996 hasta Octubre de 1999, la sucesión con final conocido que alcanzaba un término mayor.

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 [4]. Allí, además, se muestra el estado de todas las sucesiones principales que comienzan en $n < 10000$ hasta alcanzar términos de, al menos, 75 dígitos.

En Octubre de 1999, W. Bosma batió el *record* computacional establecido con la sucesión 4170: encontró que la sucesión que empieza en 42922 termina en 1 después de 1689 iteraciones, alcanzando un número de 85 cifras en el paso 1167. Y el 3 de Diciembre de 1999, el mismo W. Bosma encontró que la sucesión que empieza en 43230 termina en 1 después de 4357 iteraciones, alcanzando un número de 91 cifras en el paso 967. Pero, más adelante, obtuvimos el siguiente resultado:

- La sucesión que empieza en 3630 alcanza el 1 después de 2624 iteraciones, siendo 59 el primo previo. El máximo alcanzado es

$$\begin{aligned} s^{1263}(3630) &= 564396949893122558135271017322933689733637831793303449101418864382611123836555856019471943153476813\backslash \\ &= 2\cdot 2\cdot 2\cdot 705496187366403197669088771653667112167047289741629311376773580478263904795694820024339928941846017\,, \end{aligned}$$

un número de 100 cifras. Ésta es, hasta ahora, la sucesión con final conocido que alcanza un término mayor [3]. Encontramos su final el 10 de Junio de 2001.

- Recientemente, hemos encontrado que la sucesión que empieza en 6160 alcanza el 1 después de 3027 iteraciones, siendo 601 el primo previo. El máximo alcanzado es

$$\begin{aligned} s^{1631}(6160) &= 373179927828460325924851053974707693012492152194092977359908491036050349027883112741134921829284\backslash \\ &= 2\cdot 2\cdot 59\cdot 3009605537\cdot 525408018156855609761484153\backslash \\ &\quad 436400277245983848851931164029617450550864290479346157387\,, \end{aligned}$$

un número de 96 cifras. La completamos el 25 de Diciembre de 2001.

- De las sucesiones que empiezan en un número menor que 10000 y terminan en un ciclo, la que hasta ahora alcanza un mayor máximo es la

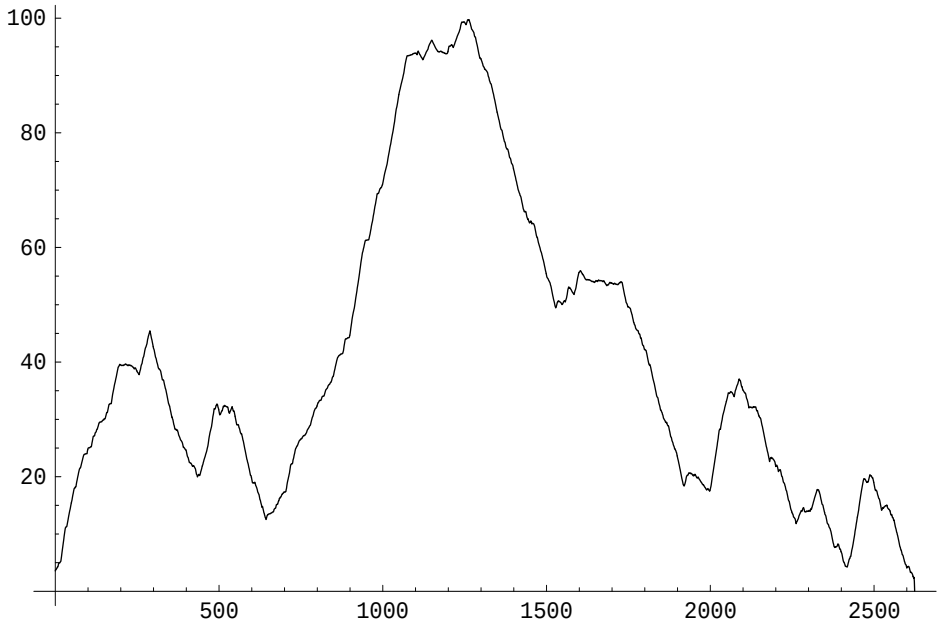

Figura 5.6: Sucesión alicuatoria 3630.

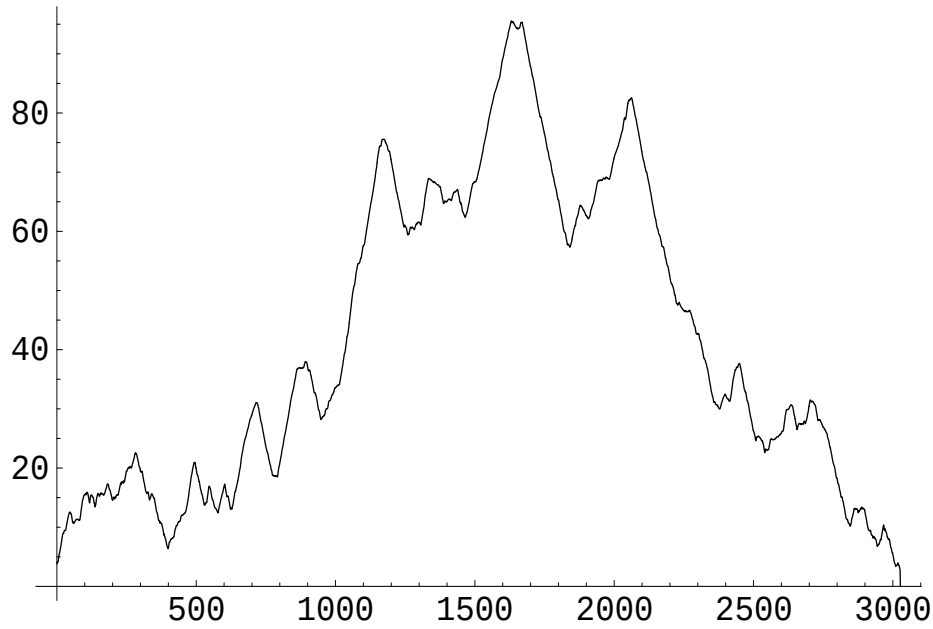

Figura 5.7: Sucesión alicuatoria 6160.

que empieza en 7422. Para esta sucesión, tenemos $s^{332}(7422) = 2924$ y $s^{333}(7422) = 2620$, siendo $(2620, 2924)$ un par de números amigos. El máximo alcanzado por esta sucesión es

$$\begin{aligned} s^{156}(7422) &= 1269528720481893811316 \\ &= 2^2 \cdot 13 \cdot 109 \cdot 131 \cdot 110323 \cdot 15497988349\,, \end{aligned}$$

un número de 22 cifras.

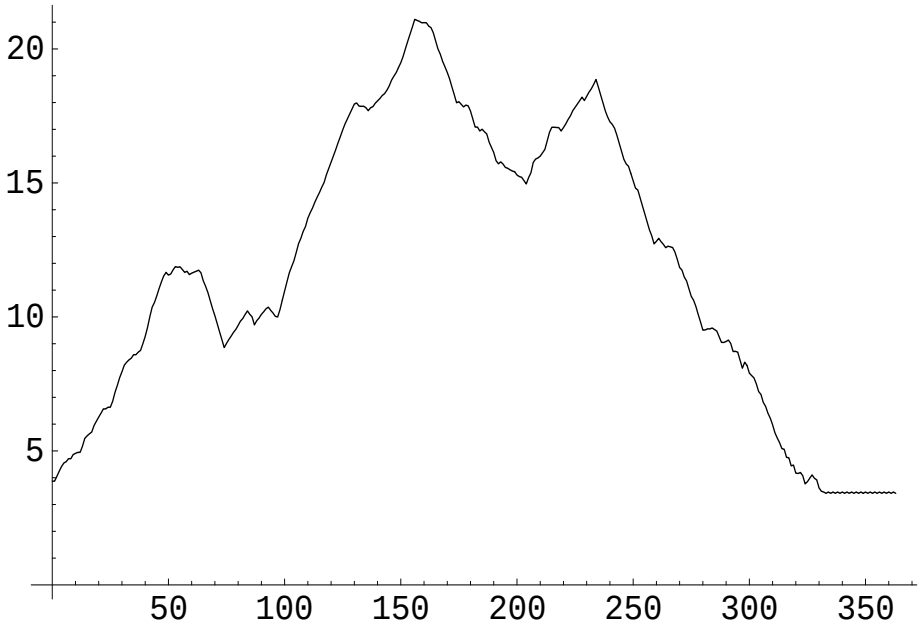

Figura 5.8: Sucesión alicuatoria 7422.

Lo mismo le ocurre a las sucesiones que empiezan en 7434 y 9894, que coinciden con la sucesión que empieza en 7422 después de unas cuantas iteraciones.

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 (ver [9]). 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

Tabla 5.1: Sucesiones alicuatorias cuyo final está en duda.

n	276	552	564	660	966	1074	1134	1464	1476
k	1284	818	3048	468	526	1585	2249	1897	1055
dígitos	117	118	115	112	114	105	127	101	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	824	1632	1336	1109	713	1404	1992	985	390
dígitos	103	101	101	104	102	103	108	102	102
guía	$2^2\cdot7$	$2^2\cdot7$	$2^5\cdot3\cdot7$	$2^{2(*)}$	$2^3\cdot3\cdot5$	$2^2\cdot7$	$2^2\cdot7$	$2^3\cdot3\cdot5$	$2^{6(*)}$
n	2340	2360	2484	2514	2664	2712	2982	3270	3366
k	471	1025	796	2866	761	1408	826	417	1062
dígitos	99	107	97	105	100	102	97	98	100
guía	$2^3\cdot3\cdot5$	$2^2\cdot7$	$2^3\cdot3$	$2^3\cdot3\cdot5$	$2^2\cdot7$	$2^{4(*)}$	$2^4\cdot31$	$2^5\cdot3\cdot7$	$2^{3(*)}$
n	3408	3432	3564	3678	3774	3876	3906	4116	4224
k	889	933	779	1201	1253	830	704	1192	519
dígitos	111	103	100	98	105	96	100	105	98
guía	$2^3\cdot3\cdot5$	$2^3\cdot3\cdot5$	$2^3\cdot3$	$2^2\cdot7$	$2^{2(*)}$	$2^2\cdot7$	$2^2\cdot7$	$2^3\cdot3$	$2^3\cdot3\cdot5$
n	4290	4350	4380	4788	4800	4842	5148	5208	5250
k	953	1165	980	2152	1135	473	1623	1710	1567
dígitos	106	97	104	105	101	98	102	96	100
guía	$2^2\cdot7$	$2^2\cdot7$	$2^2\cdot7$	$2^3\cdot3\cdot5$	$2^4\cdot31$	$2^2\cdot7$	$2\cdot3$	$2^3\cdot3\cdot5$	$2^{4(*)}$
n	5352	5400	5448	5736	5748	5778	6396	6552	6680
k	746	2776	1209	1093	1091	765	1272	932	1880
dígitos	106	102	104	100	108	101	105	102	106
guía	$2^2\cdot7$	$2^2\cdot7$	$2^3\cdot3\cdot5$	$2^2\cdot7$	$2^2\cdot7$	$2^4\cdot31$	$2^3\cdot3\cdot5$	$2^3\cdot3$	$2^4\cdot31$
n	6822	6832	6984	7044	7392	7560	7890	7920	8040
k	1177	885	1764	1113	498	846	891	1014	2240
dígitos	97	104	96	102	96	97	99	109	106
guía	$2^4\cdot31$	$2^3\cdot3$	$2^4\cdot31$	$2^4\cdot31$	$2^3\cdot3\cdot5$	$2^3\cdot5^{(*)}$	$2^2\cdot7$	$2^6\cdot127$	$2^3\cdot3\cdot5$
n	8154	8184	8288	8352	8760	8844	8904	9120	9282
k	647	1241	849	1291	2157	1184	1025	580	556
dígitos	96	102	103	96	97	101	110	103	106
guía	$2^2\cdot7$	$2^2\cdot7$	$2^{8(*)}$	$2^2\cdot7$	$2^{4(*)}$	$2^4\cdot31$	$2^2\cdot7$	$2^3\cdot3$	$2^3\cdot3$
n	9336	9378	9436	9462	9480	9588	9684	9708	9852
k	645	2198	638	447	1028	1848	643	710	669
dígitos	104	101	102	97	98	103	101	106	105
guía	$2^6\cdot127$	$2^2\cdot7$	$2\cdot3$	$2^3\cdot3\cdot5$	$2\cdot3$	$2^5\cdot3\cdot7$	$2^5\cdot3\cdot7$	$2^2\cdot7$	$2^2\cdot7$

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 que hemos empleado han sido PARI[1], KASH[2], MIRACL[3] y, fundamentalmente, UBASIC[4].

Queremos señalar que, tras enviar a publicar nuestro artículo [4], tuvimos conocimiento de que P. Zimmermann, W. Bosma y W. Creyaufmüller estaban realizando, en parte, el mismo trabajo. Concretamente, P. Zimmermann estaba analizando las cinco sucesiones de Lehmer y las que comienzan por 1074 y 1134; 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 nosotros independientemente); y W. Creyaufmüller se estaba dedicando a alcanzar 60 cifras para las sucesiones que empiezan en números menores que 10^6. Lógicamente, cuantas más sucesiones se abarcan, menos tiempo computacional es posible dedicar a cada una. Se hizo inevitable la coordinación de nuestros trabajos a fin de unificar las notaciones y evitar repeticiones innecesarias. Parte del fruto de nuestra colaboración se recoge en el artículo [3].

El estado actual de los cálculos para sucesiones alicuatorias que comienzan en $n < 10000$ es el que aparece resumido en la tabla 5.1. En ella mostramos las 81 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. En todas ellas, el guía del último término es, además, un conductor, salvo en las marcadas con $^{(*)}$. Los datos de las 7 primeras sucesiones son de W. Creyaufmüller, P. Zimmermann y J. Howell, y pueden encontrarse en sus respectivas páginas web[5]. Es de destacar que en

[1]Inicialmente desarrollado por C. Batut, D. Bernardi, H. Cohen y M. Olivier, actualmente está mantenido por Karim Belabas. Ver `http://www.parigp-home.de/`.

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

[3]M. Scott, disponible en `http://indigo.ie/~mscott/`.

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

[5]La de J. Howell es `http://home.netcom.com/~jrhowell/math/aliquot.htm`; las demás ya nos han aparecido anteriormente.

todas las sucesiones se ha llegado a términos mayores que 10^{96}; en bastantes 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://mat.unirioja.es/pub/aliquot`.

Bibliografía

[1] E. Aparicio, *Teoría de los números*, Servicio Editorial de la Universidad del País Vasco, Bilbao, 1993.

[2] T. M. Apostol, *Introducción a la teoría analítica de números*, Reverté, Barcelona, 1984.

[3] M. Benito, W. Creyaufmüller, J. L. Varona y P. Zimmermann, Aliquot sequence 3630 ends after reaching 100 digits, *Experimental Mathematics*, próxima aparición.

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

[5] M. Benito y J. L. Varona, Sucesiones alicuatorias, *Gac. R. Soc. Mat. Esp.* **2** (1999), 357–365.

[6] M. Benito y J. L. Varona, Aliquot sequences starting with a number under 10000, en *Actas EACA 2001*, Universidad de La Rioja, Logroño, 2001, pp. 90–94.

[7] M. Benito y J. L. Varona, Pythagorean triangles with legs less than n, *J. Comput. Appl. Math.*, próxima aparición.

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

[9] H. Cohen, *A Course in Computational Algebraic Number Theory*, Springer Verlag, 1993.

[10] W. Creyaufmüller, *Primzahlfamilien* (3.ª ed.), Verlagsbuchhandlung Creyaufmüller, Stuttgart, 2000.

[11] M. Deléglise y J. Rivat, Computing the summation of the Möbius function, *Experimental Mathematics* **5** (1996), 291–295.

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

[13] F. Dress, Majorations de la fonction sommatorie de la fonction de Möbius, *Bull. Soc. Math. France Mém.* **49-50** (1977), 47–52.

[14] P. Erdős, Über die Zhalen der Form $\sigma(n) - n$ und $n - \varphi(n)$, *Elem. Math.* **28** (1973), 83–86.

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

[16] A. Fässler, Multiple Pythagorean number triples, *Amer. Math. Monthly* **98** (1991), 505–517.

[17] A. Gelfond y Y. Linnik, *Méthodes élémentaires dans la théorie analitique des nombres*, Gauthier-Villars, París, 1965.

[18] A. W. P. Guy y R. K. Guy, A record aliquot sequence, en *Computation 1943–1993: A Half-Century of Computational Mathematics* (Vancouver, 1993), *Proc. Sympos. Appl. Math.* **48** (1994), Amer. Math. Soc., Providence, RI, 1994, pp. 557–559.

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

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

[21] G. H. Hardy y E. M. Wright, *An Introduction to the Theory of Numbers* (5.ª ed.), The Clarendon Press, Oxford University Press, Nueva York, 1979.

[22] E. Hlawka, J. Schoissengeier y R. Taschner, *Geometric and Analytic Number Theory*, Springer, 1991.

[23] L. K. Hua, *Introduction to Number Theory*, Springer, 1982.

[24] M. N. Huxley, *Area, Lattice Points and Exponential Sums*, The Clarendon Press, Oxford University Press, Nueva York, 1996.

[25] M. Kühleitner, An omega theorem on Pythagorean triples, *Abh. Math. Sem. Univ. Hamburg* **63** (1993), 105–113.

[26] J. Lambek y L. Moser, On the distribution of Pythagorean triangles, *Pacific J. Math.* **5** (1955), 73–83.

[27] D. H. Lehmer, A conjecture of Krishnaswami, *Bull. Amer. Math. Soc.* **54** (1948), 1185–1190.

[28] D. N. Lehmer, Asymptotic evaluation of certain totient sums, *Amer. J. Math.* **22** (1900), 293–335.

[29] J. E. Littlewood, Quelques conséquences de l'hypothèse que la fonction $\zeta(s)$ n'a pas de zéros dans le demi-plan $Re(s) > \frac{1}{2}$, *C. R. Acad. Sci. Paris* **154** (1912), 263–266.

[30] F. Mertens, Übereine zahlentheoretische Funktion, *Sitzungsherichte Akad. Wiss. Wien* **IIa 106** (1897), 761–830.

[31] L. Moser y R. A. MacLeod, The error term for the squarefree integers, *Canad. Math. Bull.* **9** (1966), 303–306.

[32] H. Müller y W. G. Nowak, Potenzen von Gaußschen ganzen Zhalen in Quadraten, *Mitt. Math. Ges. Hamburg* **18** (1999), 119–126.

[33] O. Neugebauer, *The Exact Sciences in Antiquity*, Dover, 1969.

[34] W. G. Nowak y W. Recknagel, The distribution of Pythagorean triples and three-dimensional divisor problem, *Math. J. Okayama Univ.* **31** (1989), 213–220.

[35] A. M. Odlyzko y H. J. J. te Riele, Disproof of the Mertens conjecture, *J. Reine Angew. Math.* **357** (1985), 138–160.

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

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

[38] L. Scoenfeld, An improved estimate for the summatory function of the Möbius function, *Acta Arithmetica* **15** (1969), 221–233.

[39] W. Sierpiński, Sur la sommation de la série $\sum_{a<n\leq b} \tau(n)F(n)$, où $\tau(n)$ signifie le nombre de décompositions du nombre n en une somme de deux carrés de nombres entiers, *Prace Mat. Fiz.* **18** (1908), 1–59 (en polaco); *Œuvres choises*, Vol. 1, Varsovia, 1974, pp. 109–154 (en francés).

[40] M. I. Stronina, Lattice points on circular cones (en ruso), *Izv. Vysš. Učebn. Zaved. Matematika* **87** (1969), 112–116.

[41] E. C. Titchmarsh, *The Theory of the Riemann Zeta-Function*, Oxford at the Clarendon Press, 1967.

[42] F. Vera, *Los científicos griegos*, Aguilar, 1970.

[43] R. E. Wild, On the number of primitive Pythagorean triangles with area less than n, *Pacific J. Math.* **5** (1955), 85–91.

[44] S. Y. Yan, *Perfect, Amicable and Sociable Numbers. A Computacional Approach*, World Scientific, Singapur, 1996.