Generadores de primos, identidades aproximadas y funciones multifractales

Serafín Ruiz Cabello

Tesis Doctoral
Departamento de Matemáticas
Universidad Autónoma de Madrid

Dirigida por Fernando Chamizo Lorente

道生一，一生二，二生三，三生万物。

El Tao engendra el uno,
El uno engendra el dos,
El dos engendra el tres,
Y el tres engendra a todos los seres.

Tao Thé Ching

Índice general

Prefacio v

Agradecimientos vii

Introducción 1

1. La sucesión de Rowland 13
1.1. Preliminares. Generalización 13
1.2. Conjeturas y relaciones entre ellas 16
1.3. Primos y Cadenas de Rowland 27

2. Identidades aproximadas y formas de Maass 31
2.1. Introducción 31
2.2. Resultados auxiliares 33
2.3. El caso no compacto 44
2.4. El caso compacto 53
2.5. Aplicación de los operadores de Hecke 60

3. Espectro de singularidades y formas modulares 63
3.1. Multifractales. El ejemplo de Riemann 63
3.2. Formas modulares. Resultado principal 68
3.3. Cálculo del orden Hölder 77
3.4. El espectro de singularidades 85
3.5. Futuras mejoras 97

Bibliografía 103

Prefacio

Esta memoria está compuesta por tres problemas diferentes cuyo nexo de unión es la teoría de números. Mientras que uno de ellos es de naturaleza combinatoria, el carácter de los otros dos es marcadamente analítico. De hecho, ambos comparten ciertas similaridades al hundir sus raíces conjuntamente en la teoría de formas automorfas.

La exposición está dividida en tres capítulos, cada uno de ellos correspondiente a uno de los citados problemas. Así mismo, existe un capítulo introductorio previo en el que se exponen brevemente las ideas que se desarrollarán con profunidad más adelante. Hemos preferido que en dicha introducción primen las ideas y los conceptos sobre el rigor matemático, esbozando las definiciones y resultados que luego aparecerán detallados en profunidad. Dada la disparidad de los problemas tratados, no se incluyen capítulos o apéndices exteriores con conceptos previos, conteniendo cada capítulo sus propios preliminares.

El primer capítulo trata acerca de una sucesión recurrente con una sorprendente propiedad; como reza el título, esta sucesión genera números primos. De hecho, una infinidad de ellos, arbitrariamente grandes. Una de sus peculiaridades es la sencilla expresión que la define. No en vano, las fórmulas para generar primos han estado en el imaginario matemático durante siglos, si bien la mayoría de las que se conocen son auténticas piezas de ingeniería compuestas por fórmulas o recurrencias muy elaboradas y que han sido expresamente diseñadas con el propósito de *fabricar primos*. La sucesión que vamos a ver, en cambio, los genera de forma natural.

Los otros dos capítulos tratan sobre formas automorfas. Éstas han causado una revolución en la teoría de números moderna y cosechado importantes resultados; entre ellos cabe destacar la famosa prueba del último teorema de Fermat, hace dos décadas. En el segundo capítulo se considerarán las formas no holomorfas, es decir, distintas de las clásicas. Introducidas por Hans Maass y desarrolladas por el medalla Fields noruego Atle Selberg han dado lugar a una teoría espectral de formas automorfas que estrecha los lazos entre el análisis armónico en superficies de Riemann y la aritmética. Emplearemos esta relación para demostrar que algunas series que involucran el número de representaciones como suma de dos cuadrados aproximan constantes conocidas.

En el tercer capítulo, empleamos propiedades de las formas modulares para construir funciones multifractales. Este tipo de funciones fueron introducidas por primera vez en el contexto de la mecánica de fluidos. Su particularidad es que clasifican los puntos de un intervalo en una colección no discreta de conjuntos, cada uno de ellos conteniendo un fractal de diferentes dimensiones. Para lograr funciones de este tipo a partir de formas modulares, utilizaremos aproximación diofántica, siendo clave el hecho de que los números irracionales pueden aproximarse por racionales con diferentes órdenes de precisión, tal y como expresa el Teorema de Jarník-Besicovitch.

Si las matemáticas fueran un continente, tal vez se podría decir que la teoría de números es un pequeño y joven país en el centro, rodeado por múltiples naciones que durante mucho tiempo han caminado por sus tierras y han plasmado su rúbrica sobre él a lo largo de la historia. Debido al carácter multidisciplinar de la teoría de números se hará uso de multitud de resultados y teorías previos, algunos de ellos con grandes nombres e historias a sus espaldas; muchos con resultados profundos y complejos que hacen imposible el que esta memoria sea autocontenida. Salvo en casos puntuales, se incluirán referencias adecuadas para completar y expandir tales resultados.

Agradecimientos

Completar este documento supone la síntesis de varios años de trabajo y, aunque sólo sea simbólicamente, es el fin de un largo camino. Llegar hasta aquí ha sido duro. Pero a medida que me acercaba al final estaba cada vez más seguro de lo que ahora sé; ha merecido la pena. No sólo por el premio de aportar una pequeña contribución al conocimiento matemático, sino también por el camino recorrido. Entre las muchas horas entre papeles y pantallas queda en el recuerdo lo aprendido, las personas, los momentos; queda lo bueno.

Lograrlo no habría sido posible sin la inestimable colaboración, de una u otra forma, de mucha gente. Seguramente haya dicho algo parecido varias veces, pero en pocas será tan cierto como en esta ocasión. Quería aprovechar este momento para recordar a algunas de esas personas, a vosotros, y daros las gracias.

Gracias a Fernando, mi director. Son muchas las razones que podría escoger y, pusiera las que pusiera, me quedaría corto. Gracias por todas las horas y el empeño que me has dedicado; por tu forma humilde de enseñarme, haciendo fáciles las explicaciones difíciles; por todos los grandes y pequeños detalles que has puesto de tu parte para que esto sea una realidad. Gracias por ser, más que un jefe, un amigo que siempre me ha hecho sentir que llegaríamos a buen puerto. Gracias porque te imagino pensando que exagero cuando digo todo esto, y eso hace que lo piense aún más. Gracias también por la mayoría de los dibujos de la tesis.

Gracias a Dulci, mi hermana de tesis. Parte de lo que hay en estas páginas lleva también tu firma. Y es mucho más divertido acotar integrales e irse de viaje en compañía. Por eso y por las palabras, gestos, y toda esa gran parte de ti que nos has pegado a todos, gracias.

Gracias a Adrián por tus sugerencias y correcciones del último capítulo, por concederme el honor de ser el lector de la tesis y por tus preguntas. A Javier, por la oportunidad que tuve de hacer el trabajo fin de Máster contigo y de aprender combinatoria. A Antonio, por sentarte en aquel sofá a escucharme hablar de los ceros de la función zeta, por contagiarnos tu amor por las matemáticas y por todas tus firmas.

Cuando me vine al Norte, fue extraño comenzar de cero en una ciudad tan grande, y enfrentarme a matemáticas más grandes aún. Empezamos en esto juntos. Si no hubierais estado, supongo que habría conseguido terminar, pero no habría sido lo

mismo. Así que, porque gracias a vosotros nunca me he sentido solo, por ser siempre un modelo en el que fijarme, por más razones de las que cabrían aquí... Ana, Félix, gracias.

Alguien dijo alguna vez que la gente se conoce de verdad no en los momentos especiales, sino en la rutina del día a día. Así que gracias a los que han sido mis compañeros en nuestro gallinero particular; el gran despacho 613. Además de los ya mencionados están Razvan (el chico latino), Pablo (¡qué bueno que viniste, reverendo pelotudo!), Sofi (gracias por los cafés, y las sonrisas), Su (*Dove si trova il Biscottino? Celo sul pavimento è l'emozione più grande che esiste*), Chao (*Thanks for translating the quote, you handsome guy!*), Ping (*waiting for your Chinese food*) y nuestro fichaje estrella de 2014, Irina (que tiene flechas y pronto tendrá un arco). Gracias a todos.

Gracias al gran elenco de becarios, no becarios, PIFs, PDIs, post-docs y jovenzuelos en general, porque pasarse el día entre cafés, charlas, comidas, deportes y algo de trabajo de vez en cuando con vosotros es uno de los mejores reclamos que tiene nuestro departamento. Entre los muchos que sois querría nombrar a unos cuantos. David, gracias por tus recomendaciones musicales, por nuestras bromas que nadie más entiende, por poder contar contigo siempre, por muchas más cosas, eres un grande; Jose, gracias por todos los buenos momentos, y por todo lo que he aprendido de ti; Beatriz, seguramente la más responsable y la que nos hace sensatos a los demás (gracias por aguantar todas nuestras tonterías); Luis Daniel, eres un modelo para (casi) todo, al menos para todo lo bueno; Ang, me enseñaste todos los secretos de los becarios, recuerdo muchas tardes de irme a casa y ver la puerta del 610 abierta cuando te tocaba a ti terminar; Soto, el gran maestro en la Teoría de la Aproximación; Carlos, gracias por abrirme las puertas de la Autónoma aquella mañana de septiembre y por aquel nefasto fichaje que hiciste para el *Lujo*; Pedro, eres lo más grande que ha *parío* Utrera; Enrique y Ernesto, oficialmente contáis como jovenzuelos; Javi, Charro, Marijose, Cristi, Nati, Ana Primo, Alberto, Bego, Mariluz, David F., Juanjo, Joan, Diana, Leyter (gracias por descubrirme la cocina peruana); Iason; Juan (te espera una derrota lenta y dolorosa en el ajedrez reciclado), Adri, Carlos A., Guille (eh oiga, soy ciudadano americano), Ángel (ja, ja, ja), María, Javi, David G., Felipe, y muchos otros a los que siento olvidar.

Gracias a todos los que habéis sido mis alumnos estos años. Vuestras palabras de agradecimiento y la sensación de haber podido ayudaros me ha servido de mucho, y me ha dado aliento en las peores etapas. Gracias también a los profesores con los que he compartido docencia estos años. Especialmente a Javi Cárcamo, a Tomeu y a Eugenio (gracias por hacerme sentir como en casa desde literalmente el primer día), además de algunos más que ya he nombrado. Gracias a Adolfo, me ayudaste mucho con pequeños detalles cuando empecé el máster y andaba un poco perdido. A Carmen, nuestra directora todos estos años, a la que he podido ver en primera línea defendiendo los intereses de nuestro departamento y de sus estudiantes y becarios. Gracias a toda la familia del C-XV.

Porque las buenas horas que pasamos mientras vosotros trabajáis, gracias también a Pili, la persona más simpática y con menos maldad que conozco; a Migue, por sacarnos una sonrisa todas las mañanas; a Nico, el mejor humorista de la facultad, a Jose, Cati, Javi y Antonio. Gracias también a Elisa, Antonio, Paloma y Cristina.

Gracias a Jorge por tu acogida en Barcelona y a Florian por las horas que compartimos en el curso de aproximación diofántica. Parte de lo que me contaste me ha servido para ilustrar la teoría del tercer capítulo. Gracias a Guillermo Curbera; a través de ti accedí a la beca que me trajo aquí. Gracias a Diana también por mostrarme esta puerta, y por convencerme de que la atravesara; gracias por todo. A Juan Arias de Reyna, por enseñarme con tanta dedicación teoría analítica de números y teoría de la medida (hay algo de las dos en estas páginas). Y también muchísimas gracias por tus innumerables comentarios y correcciones del manuscrito de la tesis, que ha mejorado mucho. Gracias a Rosario, porque me acercaste por primera vez al mundo de la investigación. Y a Mariví, porque me convenciste para que estudiara matemáticas.

Durante los años de la carrera, compartí clases, charlas, tardes al sol y días buenos y mejores con mucha gente. No habría podido dar el siguiente paso sin todo aquello. Gracias a Marta, Inma, Cristi, María, Verito, Jose, Nieves, Carmen, Belén, Correa, Rafa, Gentus, Carlis, Borri, Llors, Manu, Marisa, Antonio, las *spice*, Carlos *Poochie*, Pablo, Álex, Pallares, Pamos, Vane, Ali, Pilar, Sami, entre otros. También por supuesto a Anita y Antonio Herrera. Gracias a Manolo, David, Jesuli, Sergio, Benig, Rafa, Lamela, Jimmy, Alberto, Jesús... ahora estoy lejos y nos vemos menos que antes, pero aunque nos hayamos ido haciendo mayores siempre es especial cuando volvemos a vernos. Gracias también a Iván (*Jimmy*), Julio y Manuel. Gracias a Aida por enseñarme que las personas como tú existen de verdad y por todo lo que me diste. Aunque quedan un poco más lejos, no puedo evitar acordarme de mis años en Las Cumbres, donde todos nos conocíamos y éramos -somos- como una gran familia, y sé que una pequeña parte de la culpa de que haya llegado hasta aquí es vuestra también. Gracias a todos los que estabais allí.

Aunque vayáis al final, sois los más importantes. Gracias, de corazón, a toda mi familia. Hasta que no te vas tan lejos no te das cuenta de lo que significa volver a casa. Gracias a mis hermanas, Espe y Juli. Sois lo mejor que me ha pasado en la vida. Os quiero. A mi madre; seguramente me conoces mejor que yo mismo. Casi nada que escriba con palabras va a ser suficiente. Gracias por ser tan buena, tan cariñosa, tan luchadora, por ser mi madre, por todo lo bueno que me das y nos das siempre. *Tutem.* A mi padre; me parezco muchísimo a ti, y no podría elegir a alguien mejor para eso. Gracias por tu ejemplo, tu cariño, por hacerme mejor. Gracias por estar ahí siempre. Te quiero. Bram, ¿ya te puedo llamar cuñado? Gracias por tu calidez, y por las risas que nos echamos juntos. Edu, gracias por echarme de menos, por contar conmingo, por espabilarme, por todo lo que compartimos. Chari, gracias por escucharme y darme apoyo, en los buenos momentos y cuando me ha hecho más

falta. Gracias a mis abuelos Esperanza, Mª Jesús, Manolo y Serafín; todo lo bueno que tengo es por vosotros. También a mis abuelos *postizos*, Memi y Luis. A mís tíos Cabello (que como dice el villancico, son de oro), en especial a mi tía Reme, y a la tercera generación (*forever*). A mís tíos y primos Ruiz, expertos en generar *primitos*. A mi tío Serafín y un agradecimiento especial a mis primos madrileños: María, Cari, Eva, Miguel Ángel y Fernando, por vuestra cálida acogida cuando me vine aquí, y por nuestras comidas, cenas, bodas y espectáculos varios. Gracias a todos.

Por último, gracias a todos los que faltan en esta lista, que son muchos. Perdonad que no os haya incluido. Y gracias a Trufa, Puchi y Kika por vuestro amor incondicional.

Serafín Ruiz Cabello.
Madrid, 19 de marzo de 2014.

Introducción

El contenido de esta tesis está dividido en tres partes, ocupando cada una de ellas un capítulo. El primero de ellos, de naturaleza combinatoria y algo más alejado de los otros dos, se construye en torno a la sucesión de Rowland. Es ésta una sucesión recurrente de enteros positivos, que parte de una sencilla regla,

$$a_1 = 7, \qquad a_{k+1} = a_k + \operatorname{mcd}(k+1, a_k), \quad k \geq 1,$$

y posee una sorprendente propiedad: la diferencia entre dos términos consecutivos cualesquiera es siempre 1 o un número primo. Eric S. Rowland [Row08] descubrió este hecho cuando era estudiante de doctorado en Rutgers.

Surgen aquí una gran cantidad de cuestiones. ¿Qué tiene el 7 de especial? ¿Qué ocurre si es reemplazado por cualquier otra condición inicial? ¿Qué primos aparecen? ¿Con qué frecuencia y en qué orden? ¿Podemos utilizar la sucesión de Rowland como un generador natural de primos? Nuestra aportación comienza introduciendo dos sucesiones auxiliares que describen el comportamiento de la sucesión de Rowland e indican fácilmente cuándo aparecerán primos.

$$(1) \qquad c_1^* = 5, \quad c_n^* = c_{n-1}^* + \operatorname{mfp}(c_{n-1}^*) - 1, \qquad \text{y} \quad r_n^* = \frac{c_n^* + 1}{2},$$

Con estas dos sucesiones se obtiene una prueba muy corta de la propiedad arriba citada; además, también permiten demostrar que entre las distintas diferencias entre términos consecutivos aparecen una infinidad de primos distintos.

La *sucesión de Rowland generalizada* aparece cuando se reemplaza el 7 inicial por cualquier entero positivo (veremos que basta con estudiar los números impares, a partir del 5). Haciendo esto perdemos la garantía de que la diferencia entre términos consecutivos no sea nunca un número compuesto. Por ejemplo, $a_{18} - a_{17}$ es 9 si partimos de $a_1 = 533$. Aun así, a la vista de las pruebas efectuadas con los primeros millones de casos, hay hueco para la esperanza. Contraejemplos como el anterior son relativamente escasos (si bien su frecuencia aumenta cuando crece a_1, véase la tabla 1.3 en la página 16) e, incluso cuando se dan, parece que los números compuestos dejan de aparecer a partir de un cierto índice.

Esta intuición nos lleva a conjeturar que, *para cualquier condición inicial a_1 dada, existe un índice $k_0 \in \mathbb{N}$ a partir del cual la diferencia entre dos términos consecutivos cualesquiera es siempre 1 o un número primo.*

Generalizando adecuadamente las sucesiones auxiliares dadas por (1) es posible obtener análogos para cualquier condición inicial; a las sucesiones auxiliares generalizadas las denotaremos por $\{r_n\}$ y $\{c_n\}$. De ellas extraeremos gran cantidad de información; el hecho más importante es que siempre que en c_n aparezca un primo la conjetura será cierta, lo que lo convierte en una condición suficiente. Las pruebas efectuadas con ordenador parecen indicar que en todos los casos tal primo acaba apareciendo. Otra condición suficiente para que se tenga la conjetura es que la sucesión r_n, pequeña para los primeros valores de n y siempre acotada por $(c_n + 1)/2)$, crezca hasta alcanzar la igualdad en dicha cota, lo que en particular implica que dicha igualdad se mantendrá en todas las iteraciones posteriores. De nuevo los cálculos sugieren que este hecho no sólo se cumple siempre, sino que además va asociado a la aparición del primer primo en la sucesión c_n justo un paso después. Estos dos hechos dan lugar a una segunda conjetura, compuesta por tres apartados.

- *Siempre existe un índice n_0 en el que $c_{n_0} = 2r_{n_0} - 1$.*
- *Siempre existe un índice m_0 para el que c_{m_0} es primo.*
- *Más aún, estos dos índices aparecen por primera vez* de forma consecutiva.

Bastaría con demostrar cualquiera de las tres afirmaciones anteriores para probar la primera conjetura. Por desgracia, a día de hoy no sabemos si alguna de ellas es cierta. Su composición las coloca en situación análoga a otras famosas conjeturas de teoría de números cuyo denominador común es la idea de que en una sucesión estrictamente creciente siempre aparecerán números primos, salvo que condiciones de divisibilidad local lo impidan. Algunos ejemplos de esto son la hipótesis de Schinzel [SS58]; la conjetura de Hardy-Littlewood , que generaliza la conjetura de los primos gemelos [ORW99], [GBGL08, IV.2]; o de forma más general la conjetura de Bateman-Horn [BH62]. Un objetivo menos ambicioso es demostrar que los tres puntos de la segunda conjetura son equivalentes. En este sentido, presentamos una serie de resultados parciales.

La segunda parte de nuestro análisis sobre la sucesión de Rowland se centra en los primos que aparecen en las diferencias entre términos sucesivos. Uno de nuestros resultados es que la sucesión de Rowland contiene infinitos primos y la sucesión de Rowland generalizada también, siempre que la conjetura sea cierta. Por tanto, la sucesión de Rowland es un generador natural (y de aspecto muy sencillo, algo poco frecuente en la literatura) de primos arbitrariamente grandes, salvo en algunos casos triviales. La mala noticia es que un primo p requiere al menos $(p-1)/2$ iteraciones del algoritmo para aparecer, lo cual hace que el método sea demasiado costoso e inútil en la práctica para explicitar primos gigantes.

Otra cuestión es el orden en que aparecen los primos en la sucesión. En este sentido introducimos el concepto *cadena de Rowland* para denotar cualquier secuencia de primos que aparezca dentro de la sucesión generalizada de Rowland (una vez quitados

los unos, por supuesto). Por ejemplo, los primeros quince primos que aparecen en la sucesión original son

$$5, 3, 11, 3, 23, 3, 47, 3, 5, 3, 101, 3, 7, 11, 3.$$

Un rápido vistazo a ejemplos similares nos hace ver que, cuanto más pequeño es un primo, suele aparecer antes y con más frecuencia. Un análisis más conzienzudo nos convence de que muchas posibilidades no son válidas; la más sencilla es que nunca aparecerá el mismo primo dos veces seguidas (siempre habrá al menos otro primo entre dos treses, como ilustra el ejemplo de arriba). Aquí logramos una caracterización completa de las posibles cadenas de Rowland basada en las clases residuales que ocupan las sumas parciales de primos bajo ciertos módulos. Esta caracterización es muy potente y permite determinar algorítmicamente si una secuencia de primos es o no una cadena de Rowland; en particular, permite descartar muchas configuraciones sencillas de primos. También nos permite probar que, por ejemplo, ninguna cadena puede aparecer duplicada. Es decir, jamás podremos encontrar una secuencia como $3, 5, 3, 5$ en ninguna sucesión de Rowland. Por el contrario, sí parece posible dar cadenas largas formadas por muy pocos primos. Por ejemplo, la cadena

$$3, 5, 3, 23, 3, 5, 3, 653, 3, 5, 3, 23, 5, 3, 3603833, 3, 5, 3, 23, 5, 3, 653, 3, 5, 3$$

tiene 27 elementos con sólo 5 primos diferentes. Corresponde a la condición inicial $a_1 = 1550303031682205$.

El estudio de las cadenas de Rowland abre nuevas e interesantes vías de investigación que no han sido incluidos en esta memoria, pero que podrían formar parte de trabajos posteriores.

El segundo capítulo está dedicado a las identidades aproximadas. En la teoría de formas modulares existen multitud de ejemplos de estas identidades, siendo una de las más conocidas la que involucra a la denominada *constante de Ramanujan*,

$$e^{\pi\sqrt{163}} = 262537412640768743,99999999999925007\ldots,$$

que dista menos de 10^{-12} de un número entero y que curiosamente fue introducida por Hermite y no aparece en la obra de Ramanujan, aunque sí lo hacen otras cantidades parecidas [Ram00]. Un segundo ejemplo que nos ayudará a sentar las bases para ilustrar nuestro objetivo es:

$$\frac{1}{4}\left(\sum_{n=-15}^{15} e^{-n^2/4}\right)^2.$$

Esta cantidad *aproxima* al número π de modo que la diferencia entre ambos es positiva y menor que 10^{-15}. La serie aparece truncada porque su cola es de una magnitud mucho más pequeña que dicha diferencia. Los engranajes ocultos que explican tal precisión en la aproximación son la fórmula de sumación de Poisson y el hecho de que la transformada de Fourier de la función $f(x) = e^{-x^2/4}$ tiende a cero con mucha rapidez; por tanto, el valor de la serie puede aproximarse muy bien por el valor de dicha transformada en el cero.

Examinemos este ejemplo desde otro prisma: En el intervalo $[0, 1]$, las autofunciones del operador laplaciano habitual (imponiendo como condición de frontera que las soluciones valgan lo mismo en 0 y 1) son exponenciales complejas de la forma $\{e^{2\pi ikx}\}_{k\in\mathbb{Z}}$. Cualquier función real 1-periódica admitirá un desarrollo sobre la base ortonormal que forman dichas exponenciales una vez normalizadas. Esto supone una gran restricción, pues la mayoría de funciones reales no son periódicas; aunque bajo ciertas condiciones pueden *reformularse* para que lo sean. Dada una función f suficientemente regular y con decamiento exponencial, identificamos los puntos extremos del intervalo $[0, 1]$ para formar un toro y consideramos la suma de todas las traslaciones enteras actuando sobre f, forzando así a la nueva función a ser 1-periódica por construcción. En el ejemplo que acabamos de ver, la función $f(x) = e^{-x^2/4}$ se reemplazaría por $F(x, y) := \sum_{n=-\infty}^{\infty} f(d(x + n, y))$. Desarrollando F en la base ortonormal,

$$F(x, y) = 2\sqrt{\pi} \sum_{j=-\infty}^{\infty} e^{\lambda_j} e^{2\pi ijx} e^{-2\pi ijy},$$

donde $\lambda_j = -4\pi^2 j^2$ es el autovalor correspondiente a la autofunción $e^{2\pi ijx}$. Y, puesto que el primer autovalor no trivial es $\lambda_1 = \lambda_{-1} \simeq 39'47$, ahora es evidente ver que $F(0, 0)$ se aproxima con mucha precisión por el término correspondiente a $j = 0$ en la serie de la derecha, cuyo valor es $2\sqrt{\pi}$; esto a su vez demuestra por qué nuestro ejemplo aproxima a π con tanta precisión.

Las aproximaciones que ofrecemos se obtienen partiendo de esta misma idea, pero en un campo de batalla un tanto más *exótico*. Nuestro punto de partida es reemplazar $\mathbb{R}$ por el *semiplano de Poincaré*,

$$\mathbb{H} := \{x + iy \in \mathbb{C} : y > 0\},$$

que es el semiplano superior complejo dotado de una métrica especial de la que se deriva la denominada *distancia hiperbólica*, ρ, dada por

$$\rho(z, w) = \operatorname{arccosh}\left(1 + 2u(z, w)\right), \qquad \text{donde} \quad u(z, w) = \frac{|z - w|^2}{4\Im z \Im w}. \tag{2}$$

Generalizando la idea que exponíamos en el párrafo anterior, las autofunciones normalizadas de un operador diferencial autoadjunto constituyen una base ortonormal del espacio que alberga dichas funciones, siempre que éste sea de dimensión finita.

Para el caso infinito, el análisis funcional proporciona un análogo válido para determinados operadores elípticos de segundo orden. Aquí entra en juego el operador de Laplace-Beltrami, que no es más que la generalización natural del laplaciano convencional adaptado a $\mathbb{H}$. El grupo $G = \mathrm{SL}_2(\mathbb{R})$ de matrices reales regulares 2 por 2 con determinante 1 define una acción sobre $\mathbb{H}$ (a menudo identificando I con $-I$ para que dicha acción sea *fiel*; es decir, no haya matrices distintas que generen la misma acción sobre $\mathbb{H}$) con la propiedad de que la distancia hiperbólica es invariante por dicha acción.

Tal y como en el caso real las funciones a desarrollar debían en última instancia ser invariantes por traslaciones enteras, ahora buscamos que una función k definida sobre $\mathbb{H}$ (suficientemente regular y de cuadrado integrable) tenga las simetrías expresadas por un subgrupo discreto $F \subset G$ (en concreto, consideraremos grupos fuchsianos de primera especie) considerando la suma de las acciones de dichas simetrías sobre esa función. La suma resultante se denomina *núcleo automorfo*,

$$K(z,w) := \sum_{g \in F} k\left(u(gz,w)\right), \qquad z,w \in \mathbb{H}, \tag{3}$$

y tiene la propiedad básica de que es invariante por elementos g de F, ya que $K(gz,w) = K(z,w)$, al igual que la F del primer ejemplo verificaba $F(x+n,y) = F(x,y)$. Si $\mathbb{H}\backslash F$ es compacto (se dice entonces que F es *co-compacto*), el núcleo K admite un desarrollo en autofunciones del operador de Laplace-Beltrami,

$$K(z,w) = \sum_{j=0}^{\infty} h(t_j) u_j(z) \overline{u_j(w)}. \tag{4}$$

Dichas autofunciones se denominan *formas de Maass*, por el matemático Hans Maass que las introdujo a mediados del siglo pasado [Maa49]. La función h en (4) es un análogo a la transformada de Fourier en el caso real. Se conoce como la *transformada de Selberg* de k, en honor al noruego Atle Selberg que desarrolló y amplió la teoría espectral de formas automorfas. Por otro lado, $-(1/4+t_j^2)$ es el autovalor correspondiente a la forma de Maass u_j. Cabe destacar que el primer autovalor es cero y la primera autofunción está relacionada con el área del dominio fundamental de F. El objetivo es conseguir, mediante ejemplos *adecuados* de funciones k (en el sentido de que sus transformadas de Selberg tengan una descripción explícita y rápida convergencia) ejemplos de identidades aproximadas (entre el núcleo y la contribución a la serie del autovalor trivial igualando (3) y (4) en puntos z y w escogidos de manera conveniente) con significado aritmético.

La primera contrariedad que surge es que muchos de los grupos fuchsianos habituales con los que nos gustaría investigar no son compactos. El ejemplo más característico es $\Gamma = \mathrm{PSL}_2(\mathbb{Z})$, del cual se derivan muchos otros. Esta dificultad se puede solventar generalizando (4) para dar lugar a la llamada *fórmula de pretraza*

de Selberg [Sel56], válida también para grupos no co-compactos:
(5)

$$K(z,w) = \sum_{j=0} h(t_j) u_j(z) \overline{u_j(w)} + \frac{1}{4\pi} \sum_{\mathfrak{a}} \int_{-\infty}^{\infty} h(t) E_{\mathfrak{a}}(z, 1/2+it) \overline{E_{\mathfrak{a}}(w, 1/2+it)}\, dt.$$

Aquí, $\mathfrak{a}$ recorre las *cúspides* del grupo fuchsiano F (caracterizadas por los vértices del dominio fundamental de F que caen en la recta real o el punto $i\infty$) y $E_{\mathfrak{a}}$ es la *serie de Eisenstein* asociada a dicha cúspide. La fórmula (5) nos permite obtener un primer ejemplo de identidad aproximada, precisamente utilizando Γ como grupo fuchsiano. Sean

$$S = 8 \sum_{n=1}^{\infty} \xi_n \frac{r(n) r(n+4)}{(n+4)^2}, \qquad I = \int_{-\infty}^{\infty} \frac{|f(t)|^2}{\cosh(\pi t)} (1/4 + t^2)\, dt,$$

donde $f(t) = \zeta(1/2+it)\zeta^{-1}(1+2it)L(1/2+it,\chi)$, χ es el único carácter no principal módulo 4, $r(n)$ cuenta el número de expresiones de un entero n como suma de dos cuadrados y ξ_n vale $1/2$ en los pares y $1/4$ en los impares. Probaremos (véase la Proposición 2.15 en la página 51) que $(S-3)/I$ aproxima al número π de modo que la diferencia entre ambas cantidades es menor que $4 \cdot 10^{-14}$ y no nula. También obtendremos más ejemplos utilizando otros grupos diferentes.

Un comentario interesante es que la aparición de la función $r(n)$, con un fuerte significado aritmético, no es una casualidad ya que las matrices de Γ están formadas por números enteros. Concretamente, tomando $z = w = i$ en (3), la expresión $K(w,z)$ adquiere una estructura aritmética muy simple y la suma sobre los elementos de G se traduce en una suma sobre los enteros. El caso en que esta correspondencia se hace más palpable corresponde a tomar el subgrupo $\widetilde{\Gamma}$, formado por las matrices de Γ en las que los dos elementos de cada diagonal tienen la misma paridad. En ese caso se cumple:

$$2 \sum_{g \in \widetilde{\Gamma}} k\left(u(\gamma i, i)\right) = \sum_{n=0}^{\infty} r(n) r(n+1) k(n),$$

donde u viene dada por (2). Para otros grupos fuchsianos se tendrán análogos a éste, si bien no tan abrumadoramente simples.

El estudio de las aproximaciones para grupos no compactos incluye varias identidades aproximadas más, junto con una serie de lemas técnicos entre los que cabe destacar aquellos que relacionan los núcleos con series en las que aparece la función $r(n)$, y un análisis numérico del error cometido en las aproximaciones. Cabe destacar que el que se obtiene en el ejemplo es tan preciso debido en parte a que las dos autofunciones correspondientes a los dos autovalores no triviales más pequeños del operador de Laplace-Beltrami son impares, por lo que $u_1(i) = u_2(i) = 0$, y el error dependerá del al tercer autovalor. Esto situará a este ejemplo por delante de otros a priori más potentes (como en el caso compacto).

Seguidamente estudiaremos el caso compacto en el que, a pesar de partir de un desarrollo espectral más sencillo ((4) frente a (5)), nos enfrentaremos al reto de encontrar grupos fuchsianos válidos para nuestros propósitos. Los primeros que utilizaremos proceden del álgebra de cuaterniones y están definidos como sigue, para p y q primos con $p \equiv 3 \pmod 4$ y $q \equiv 5 \pmod 8$:

$$\begin{aligned} G_p &= \left\{ \frac{1}{2} \begin{pmatrix} a+b\sqrt{p} & c+d\sqrt{p} \\ -c+d\sqrt{p} & a-b\sqrt{p} \end{pmatrix} \in \mathrm{SL}_2(\mathbb{R}) : a \equiv b \equiv c \equiv d \pmod 2 \right\} / \{\pm I\} \\ G_{2,q} &= \left\{ \frac{1}{2} \begin{pmatrix} a+b\sqrt{2} & c+d\sqrt{2} \\ q(c-d\sqrt{2}) & a-b\sqrt{2} \end{pmatrix} \in \mathrm{SL}_2(\mathbb{R}) : a \equiv c, b \equiv d \pmod 2 \right\} / \{\pm I\}. \end{aligned}$$

La mejor aproximación que alcanzaremos será con G_3, cuyo primer autovalor no trivial es el de mayor tamaño entre todos los expuestos. Concretamente, para

$$S' := \sum_{n=1}^{\infty} r(n) r(3n+2) \sqrt{n} e^{-(\log n/4)^2},$$

demostraremos que S' aproxima bien a $72e^9\sqrt{\pi}$ en el sentido de que el error relativo es pequeño, concretamente (véase la Proposición 2.22 en la página 58)

$$1'29 \cdot 10^{-7} < 1 - \frac{S'}{72e^9\sqrt{\pi}} < 3 \cdot 10^{-7}.$$

Vemos que nuevamente aparece una expresión que involucra la función $r(n)$ y que, como ya anunciábamos, esta aproximación no es tan buena como la mejor que obteníamos en grupos fuchsianos no compactos. La razón, sobre la que hablaremos ampliamente en el segundo capítulo, es que ahora las primeras autofunciones no serán impares, y por tanto el error está relacionado con el tamaño del primer autovalor en lugar del tercero.

Hemos recogido más ejemplos de grupos fuchsianos y núcleos con los que se alcanzan identidades aproximadas destacables, si bien algunas de ellas no han llegado a formar parte del artículo en que se basa esta sección. Nuestro último caso de estudio corresponde a los operadores de Hecke, que son autoadjuntos actuando sobre $\mathbb{H}$ y tienen un comportamiento que en cierto modo generaliza al de grupos compactos sobre $\mathbb{H}$, al estar basados en matrices de determinante entero y no sólo de valor uno.

El tercer y último capítulo gira alrededor de dos conceptos de reciente aparición en la literatura matemática: el espectro de singularidades y las funciones multifractales. Introducidas originalmente en el contexto de problemas de fluidos [BPPV84], las funciones multifractales son aquellas tales que al asignar a cada exponente Hölder

el conjunto de puntos de la función donde dicho exponente se alcanza se obtiene un continuo de fractales de diferentes dimensiones. Esa asignación es conocida como espectro de singularidades y, expresado en términos matemáticos, una función será multifractal cuando la imagen de su espectro de singularidades no sea discreta. Uno de los ejemplos más conocidos es la función

$$R(x) = \sum_{n=1}^{\infty} \frac{\operatorname{sen}(2\pi n^2 x)}{n^2},$$

frecuentemente denominada *el ejemplo de Riemann* o, simplemente, la *función de Riemann* (véase la Figura 1). Según Weierstrass [Edg04], Riemann introdujo $R(x)$ como un ejemplo de función continua y al mismo tiempo no diferenciable en ningún punto (véase también [BS86]). Tal afirmación resultó ser falsa. Décadas más tarde Hardy [Har16] demostró que era no diferenciable en todos los irracionales, y también en ciertas clases racionales, pero fue J. Gerver quien siendo un estudiante de grado demostró en la década de los 70 del pasado siglo que sí era diferenciable en el resto de racionales.

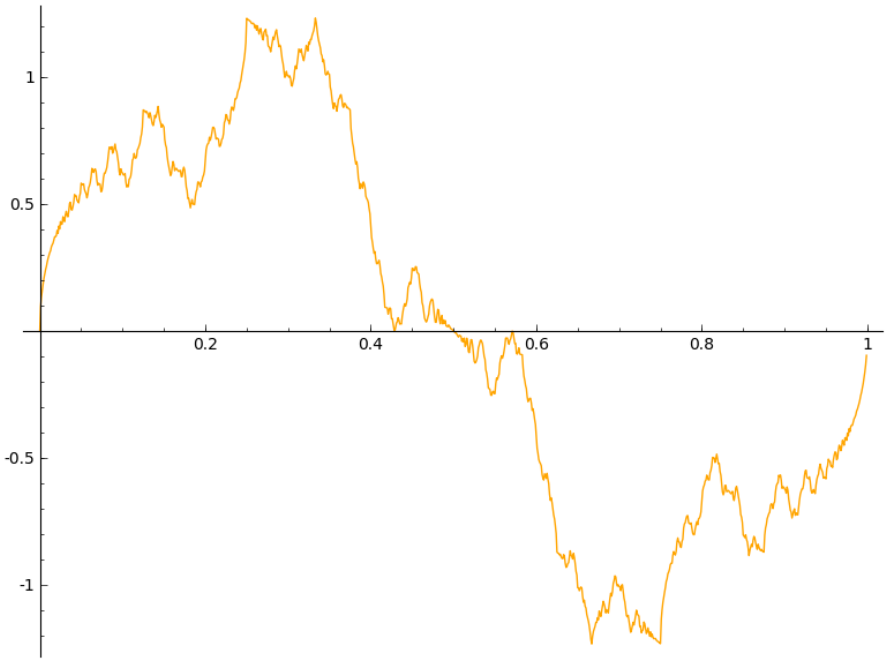

Figura 1: Gráfica de la función $R(x)$.

En cuanto al espectro de singularidades, el matemático francés Stéphane Jaffard lo determinó completamente [Jaf96] probando que, fijado $\beta \in [1/2, 3/4]$, el conjunto de puntos con exponente Hölder β tiene dimensión de Hausdorff $4(\beta - 1/2)$; y que el

resto de puntos (que son precisamente los racionales dados por Gerver) tiene orden Hölder 3/2, formando estos un conjunto de dimensión cero (véase el Teorema 3.3 en el tercer capítulo para más información). En particular, los puntos con exponente Hölder 3/4 son los únicos que dan lugar a un conjunto de medida positiva, por lo que el orden Hölder *típico* de $R(x)$ será 3/4. Esto es fácil de intuir a partir de la identidad de Parseval, pues

$$\begin{aligned}\int_0^1 |R(x+h)-R(x)|^2\,dx &= 4\int_0^1 \left|\sum_{n=1}^{\infty}\frac{\operatorname{sen}(\pi n^2 h)\cos(2\pi n^2 x+\pi n^2 h)}{n^2}\right|^2 dx\\ &= 2\sum_{n=1}^{\infty}\frac{\operatorname{sen}^2(\pi n^2 h)}{n^4}.\end{aligned}$$

El rango de valores de n de orden menor o igual a $h^{-1/2}$ dará la contribución principal que es comparable a $h^{3/2}$, por tanto cabría esperar que $R(x+h)-R(x)$ sea comparable a $h^{3/4}$. De hecho se puede probar que $R(x+h)-R(x)=O\big(h^{3/4}\big)$ se cumple para todo x, salvo en un conjunto de medida nula. La integración sólo *ve* conjuntos de medida positiva y por tanto es inútil para detectar las peculiaridades en conjuntos fractales, y es aquí donde toma valor el análisis multifractal. La prueba de Jaffard emplea la *transformada wavelet*.

La *notación de Landau* que aparece en el párrafo anterior es muy habitual para expresar relaciones asintóticas entre dos funciones, y será utilizada frecuentemente en el tercer capítulo. Dadas f y g, reales o complejas, se escribirá $f(x)=\mathcal{O}\left(g(x)\right)$ para indicar que el cociente $|f(x)/g(x)|$ está acotado por una constante absoluta cuando x tiende a infinito. Equivalentemente se escribirá $f(x)\ll g(x)$. Si la constante depende de una segunda variable t y no quiere mostrarse explícitamente la dependencia porque no sea relevante, se suele indicar con $f(x)=\mathcal{O}_t\left(g(x)\right)$ o $f(x)\ll_t g(x)$. La notación $f(x)=o\left(g(x)\right)$ indica que el cociente $f(x)/g(x)$ tiende a cero cuando x tiende a infinito, mientras que la menos habitual notación $f(x)=\Omega(g(x))$ indica que no se cumple $f(x)=o(g(x))$ (en otras palabras, que f es de orden igual o superior a g). Por último, $f(x)\asymp g(x)$ indica que se satisfacen simultáneamente $f(x)\ll g(x)$ y $f(x)\gg g(x)$.

Nuestra contribución consiste en extender el resultado de Jaffard a otras funciones similares. Para describir estas funciones, primero debemos explorar un tercer punto de vista de la función de Riemann: su conexión con la también famosa función θ de Jacobi

$$\theta(z):=\sum_{n=-\infty}^{\infty} e(n^2 z),\quad z\in\mathbb{C},\ \Im z>0,$$

donde $e(z)=e^{2\pi i z}$. $\theta(z)$ es una *forma modular*, ya que verifica una cierta ecuación funcional (véase (3.4) en la página 71) con respecto de un grupo discreto de matrices

enteras. Concretamente, el grupo $\Gamma_0(4)$, donde

$$\Gamma_0(N) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) : N|c \right\}. \tag{6}$$

Aquí, $\mathrm{SL}_2(\mathbb{Z})$ denota las matrices enteras 2×2 con determinante 1. La *integral fraccionaria* de θ es una función definida sobre los reales que procede de la función θ:

$$\theta_2(x) = \sum_{n=1}^{\infty} \frac{e(n^2 x)}{n^2}, \quad x \in \mathbb{R}. \tag{7}$$

Por construcción, $R(x) = \Im\theta_2(x)$. Nosotros tomaremos una familia de formas modulares f sobre $\Gamma_0(N)$, que bajo ciertas condiciones admitirán un desarrollo de Fourier,

$$f(z) = \sum_{n=0}^{\infty} a_n e(nz), \quad z \in \mathbb{C},\ \Im z > 0,$$

y, para cada una de ellas, una colección de integrales fraccionarias,

$$f_\alpha(x) = \sum_{n=0}^{\infty} \frac{a_n}{n^\alpha} e(nx), \quad x \in \mathbb{R}, \tag{8}$$

donde el parámetro α (que generaliza el 2 de (7)) se acotará superior e inferiormente en función del *peso* r de la forma modular (véase la Definición 3.5 en la página 71) para que la serie en (8) sea convergente. En estas condiciones demostraremos que, si f no es una forma cuspidal, (véase el Teorema 3.7 en la página 73), entonces para $f_\alpha(x)$, los puntos con exponente Hölder β tienen dimensión de Hausdorff $2(\beta - \alpha + r)/r$, para $\alpha - r < \beta < \alpha - r/2$, lo que en particular demuestra que f_α es un multifractal..

Para demostrar nuestro citado Teorema, utilizaremos la relación existente entre f y f_α. Siempre que el exponente Hölder esperado sea menor que 1, como en nuestro caso, éste admite una descripción más sencilla de la habitual, siendo suficiente expresar $f_\alpha(x+h) - f_\alpha(x)$ como $\mathcal{O}(|h|^\gamma)$ para $h \neq 0$ arbitrariamente pequeño y algún $\gamma > 0$. La anterior diferencia puede expresarse como la integral compleja de la diferencia entre dos evaluaciones de la función f. Si x es un número irracional, un conocido resultado de Dirichlet nos dice que existirán infinitas fracciones a/q que aproximen x con precisión; concretamente, verificando $|x - a/q| < q^{-2}$. La teoría de formas modulares posee potentes herramientas para describir el comportamiento de f cerca de estos racionales o *cúspides*. A medida que h se acerque más a cero, tomaremos una sucesión de fracciones $\{a_n/q_n\}$ con denominadores cada vez más grandes, de modo que la distancia a x sea cada vez más pequeña. La elección adecuada de esta sucesión se obtendrá a través de la *fracción continua* de x, de la cual se obtienen sus *convergentes*, que son precisamente esas fracciones.

Hay último detalle crucial para lograr distintos exponentes Hölder en distintos puntos x. Es sabido que la mayoría de irracionales dejan de admitir infinitas aproximaciones por fracciones tales que $|x-a/q| < q^{-2}$ si se reemplaza el 2 por otro número real $c > 2$. Los que sí lo hacen tienen medida cero, pero se agrupan formando conjuntos de todas las posibles dimensiones comprendidas entre 0 y 1 al clasificarlos según el mayor exponente c para el que admiten infinitas aproximaciones. Esta afirmación queda cuantificada en el Teorema de Jarník-Besicovitch, que aqui utilizaremos y adaptaremos para obtener el espectro de singularidades de f_α. Concretamente, probraremos (véanse las Proposiciones 3.13 y 3.13 a partir de la página 88) que, fijado $c > 2$, existe un subconjunto de $[0,1]$ con dimensión $2/c$ tal que todos sus puntos tienen exponente Hölder $\alpha - r + r/c$. Recíprocamente, probaremos que todos los puntos de $[0,1]$ que tengan ese exponente Hölder deben estar contenidos en otro subconjunto de la misma dimensión.

Nuestros resultados son válidos para integrales fraccionarias procedentes de formas modulares con pesos comprendidos entre 0 y 1. Existen varios ejemplos explícitos de formas modulares con pesos comprendidos en este rango. La ya mencionada función θ de Jacobi tiene peso $1/2$, y con ese mismo peso existen muchas otras que en realidad son variantes de ella [BS86]. También existen formas modulares de peso $1/5$ relacionadas con trabajos de Klein y con las identidades de Rogers-Ramanujan ([Hub14],[Man02],[Kan06]). T. Ibukiyama dio una familia de formas modulares de peso $(N-3)/(2N)$ para cualquier N impar [Ibu00]. Están construidas como cocientes entre funciones θ y una función η de Dedekind.

El estudio iniciado con los resultados que se reflejan en este capítulo permanece abierto, y en futuras investigaciones planeamos obtener resultados similares para formas modulares con pesos mayores. Esto amplía el tamaño de los exponentes Hölder esperados. Como consecuencia, calcularlos se convierte en un problema más complejo, al aparecer nuevos términos englobando a las sucesivas derivadas de f.

No haremos ningún recopilatorio sobre notación, y habitualmente cada expresión se definirá en el momento en que se introduzca. Aun así conviene repasar varios términos que utilizaremos habitualmente y que aunque son muy utilizados, pueden dar lugar a confusión. Escribiremos $\Re z$ y $\Im z$ para expresar respectivamente las partes real e imaginaria de un número complejo, y abreviaremos $e^{2\pi i z}$ mediante la expresión $e(z)$. De igual manera, a veces emplearemos $a \equiv b\,(c)$ para denotar que a y b son congruentes módulo c.

Los resultados de la tesis están recogidos en los siguientes artículos:

- F. Chamizo, D. Raboso, and S. Ruiz-Cabello. *On Rowland's sequence*. Electron. J. Combin. 18 (2011), no. 2, Paper 10, 10 pp.
- F. Chamizo, D. Raboso, and S. Ruiz-Cabello. *Exotic approximate identities and Maass forms*. Acta Arith. 159 (2013), no. 1, 27–46.
- F. Chamizo and S. Ruiz-Cabello. *Modular forms and multifractal Fourier series*. En preparación.

Capítulo 1

La sucesión de Rowland

1.1. Preliminares. Generalización

El presente capítulo está centrado en el estudio de la sucesión

$$a_1 = 7, \qquad a_k = a_{k-1} + \mathrm{mcd}(k, a_{k-1}), \quad k > 1, \tag{1.1}$$

a la que nos referiremos como *Sucesión de Rowland* en adelante.

k	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	...
a_k	7	8	9	10	15	18	19	20	21	22	33	36	37	38	39	40	...
$a_k - a_{k-1}$		1	1	1	5	3	1	1	1	1	11	3	1	1	1	1	...

Tabla 1.1: Los primeros términos de la sucesión de Rowland.

Descubierta por primera vez por Matthew Frank en 2003, Eric S. Rowland la dio a conocer cinco años más tarde probando un resultado sorprendente:

Teorema 1.1 (Rowland, 2008 [Row08])**.** *Para cualquier índice $k \geq 2$, la diferencia $a_k - a_{k-1}$ dada por* (1.1) *es siempre* 1 *o un número primo.*

Como el mismo Rowland relata en su artículo, es infrecuente en la literatura matemática hallar ejemplos de funciones que produzcan números primos y tengan una estructura *natural*; es decir, que no hayan sido expresamente diseñadas para este propósito, lo que suele implicar que su definición sea bastante artificiosa. La mala noticia a cambio es que los primos generados no aparecen ordenados ni tienen estructura, sino que surgen de forma cáotica; algunos aparecen repetidas veces, y no está claro que tengan que aparecer todos.

Como muestra, veamos una lista algo más amplia de las diferencias entre términos consecutivos:

$\{a_k - a_{k-1}\}$ = 1, 1, 1, 5, 3, 1, 1, 1, 1, 11, 3, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 23, 3, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 47, 3, 1, 5, 3, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 101, 3, 1, 1, 7, 1, 1, 1, 1, 11, 3, 1, 1, 1, 1, 1, 13, 1, 233, 3, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, ...

Comenzamos nuestro análisis de la sucesión de Rowland introduciendo las dos sucesiones auxiliares siguientes.

$$c_1^* = 5, \quad c_n^* = c_{n-1}^* + \mathrm{mfp}(c_{n-1}^*) - 1, \qquad \text{y} \quad r_n^* = \frac{c_n^* + 1}{2}, \tag{1.2}$$

donde $\mathrm{mfp}(m)$ denota el menor primo que divide a m; bien definido siempre que m sea mayor que 1. Nótese que, con esta definición, c_n^* siempre es impar. Estas dos sucesiones nos van a permitir dar una caracterización de la sucesión $\{a_k - a_{k-1}\}$ que prueba el Teorema 1.1 de forma inmediata y sencilla:

Proposición 1.2.

$$a_k - a_{k-1} = \begin{cases} \mathrm{mfp}(c_{n-1}^*) & \textit{si } k = r_n^* \textit{ para algún índice } n > 1, \\ 1 & \textit{en el resto de casos.} \end{cases} \tag{1.3}$$

Demostración: Consideremos la sucesión $\{b_k\}_{k\geq 1}$ dada por

$$b_1 = 7, \quad b_2 = 8; \qquad\qquad b_k = c_n^* + k + 1, \quad k \in [r_n^*, r_{n+1}^*), \quad n \geq 1.$$

Vamos a demostrar que $\{a_k\}$ y $\{b_k\}$ describen exactamente la misma sucesión. Fijado n, tomemos cualquier $k \in [r_n^*, r_{n+1}^*)$. b_{k-1} será igual a $c_n^* + k$ salvo si $k = r_n^*$, siendo entonces igual a $c_{n-1}^* + k$. Por tanto $b_k - b_{k-1}$ equivale al lado derecho de (1.3) y basta con probar que $b_k - b_{k-1} = \mathrm{mcd}(k, b_{k-1})$. Hay dos posibilidades. Si k no coincide con ningún r_n^*,

$$\mathrm{mcd}(k, b_{k-1}) = \mathrm{mcd}(k, c_n^* + k) = \mathrm{mcd}(2k, c_n^*) = \mathrm{mcd}(2(k - r_n^*) + 1, c_n^*)$$

y el último término es 1, ya que $2(k - r_n^*) + 1 < 2(r_{n+1}^* - r_n^*) + 1 = \mathrm{mfp}(c_n^*)$. Y si $k = r_n^*$ se obtiene el mismo resultado reemplazando n por $n-1$. Por tanto, $2(k - r_{n-1}^*) + 1 = 2(r_n^* - r_{n-1}^*) + 1 = \mathrm{mfp}(c_{n-1}^*)$. □

Obsérvese la Tabla 1.2 que describe los primeros términos de las sucesiones auxiliares. Comparándola con la Tabla 1.1 puede verse que los números que aparecen en la sucesión r_n^* (salvo el primero) se corresponden exactamente con los índices k

n	1	2	3	4	5	6	7	8	9	10	...
c_n^*	5	9	11	21	23	45	47	93	95	99	...
$\mathrm{mfp}(c_n^*)$	5	3	11	3	23	3	47	3	5	3	...
r_n^*	3	5	6	11	12	23	24	47	48	50	...

Tabla 1.2: Las sucesiones auxiliares r_n^* y c_n^*.

en los que $a_k - a_{k-1}$ es mayor que 1, mientras que la sucesión $\{\mathrm{mfp}(c_n^*)\}$ recoge en orden esos valores de $a_k - a_{k-1}$.

Llegados a este punto, cabe hacerse varias preguntas que abren dos vías principales de investigación. Una de ellas es el análisis de los primos que aparecen entre términos consecutivos de la sucesión de Rowland: cuántos, con qué frecuencia y en qué orden. Este estudio tiene cabida en la tercera y última sección de este capítulo. La otra vía parte de nuestra tendencia natural a generalizar y hacer más ricos los problemas. ¿Qué ocurre si se reemplaza el 7 por cualquier otro entero positivo? ¿Podremos dar un resultado análogo al Teorema 1.1? La respuesta será que en general no, pero aún podremos decir bastante. El nuevo objeto de estudio es la *Sucesión de Rowland generalizada*:

$$a_1 \geq 5 \quad \text{impar}; \qquad a_k = a_{k-1} + \mathrm{mcd}(k, a_{k-1}), \quad k > 1, \tag{1.4}$$

Como puede verse en la definición, sólo consideraremos enteros impares mayores o iguales que 5. La razón es que tomar a_1 como 1 o 3 da lugar a sucesiones triviales ($a_k = k$ y $a_k = k + 2$, respectivamente) y las condiciones iniciales pares quedan caracterizadas por las impares, ya que $a_1 = 2n$ y $a_1 = 2n + 1$ producen el mismo a_2, y por tanto la misma sucesión a partir del segundo paso.

Tomando una condición inicial arbitraria, surgen contraejemplos en los que no se cumplirá el Teorema 1.1. Considérese, por ejemplo, $a_1 = 805$, que conduce a $a_{18} - a_{17} = 9$. Los cálculos efectuados con ordenador sugieren que aunque el número de estas condiciones iniciales problemáticas es escaso entre valores pequeños de a_1 (la primera que aparece es $a_1 = 533$, tras más de doscientos casos positivos), su proporción parece incrementarse lentamente a medida que crece el tamaño de a_1 (véase la Tabla 1.3). No es descabellado pensar que conforme se aumente el tamaño de a_1, la densidad de estos casos pueda tender a una constante positiva o incluso acercarse a 1. A pesar de esto, como adelantábamos antes, no todo está perdido. Aparezcan o no compuestos para una condición inicial fija, el número de estos parece ser siempre finito (ocurre así en asbolutamente todos los casos para $a_1 < 10^8$). Ésta es la gran conjetura sobre la sucesión de Rowland generalizada, y a la que está dedicada la siguiente sección.

Primeros N valores de a_1	Número de casos con contraejemplos	Porcentaje
100	0	0 %
500	22	4′4 %
1000	63	6′3 %
5000	447	8′94 %
10000	1142	11′42 %
50000	7577	15′15 %
100000	16218	16′21 %
500000	99419	19′88 %
1000000	211077	21′11 %
5000000	1099747	21′99 %

Tabla 1.3: Porcentaje de términos iniciales a_1 para los que aparecen números compuestos. Los N primeros casos corresponden a los N primeros impares mayores o iguales que 5.

1.2. Conjeturas y relaciones entre ellas

Comenzamos formalizando las ideas plasmadas en el último párrafo de la anterior sección.

Conjetura 1.3. *Fijemos a_1 impar y mayor o igual que 5. Sea $\{a_k\}$ la sucesión dada por (1.4). Entonces existe un índice k_0 tal que $a_k - a_{k-1}$ es 1 o un número primo para todo $k > k_0$.*

Es interesante recalcar que también puede plantearse, y así aparece en el artículo original de Rowland [Row08], una segunda generalización; que el término inicial de la serie no sea a_1 sino a_m para cualquier m entero. Al depender cada a_k fuertemente del índice del término anterior, esta segunda modificación cambia totalmente las reglas del juego (como ilustraremos más adelante con ejemplos). No la incluiremos en nuestro análisis.

Las sucesiones auxiliares que planteábamos en (1.2) para caracterizar el comportamiento de la sucesión de Rowland original también pueden generalizarse.

Definición 1.4. *Sea a_1 impar y mayor o igual que 5. Se definen por inducción simultánea las siguientes sucesiones:*

$$(1.5)\qquad \begin{cases} r_1 = 1, & r_{n+1} = \min\{k > r_n : \operatorname{mcd}(k, c_n) \neq 1\}, \quad n \geq 1 \\ c_1 = a_1 - 2, & c_{n+1} = c_n + \operatorname{mcd}(c_n, r_{n+1}) - 1, \quad n \geq 1. \end{cases}$$

Nótese que, como la sucesión $\{c_n\}$ es estrictamente creciente y sólo toma valores impares, el conjunto que define r_{n+1} será no vacío siempre que c_1 sea mayor que 1.

Por tanto, basta con pedir que a_1 no tome los valores 1 o 3 que, como ya dijimos, arrojan sucesiones triviales.

La Definición 1.4 nos resultará muy útil durante el resto de la exposición, aunque no se trata propiamente de una generalización de (1.2). En este sentido, la definición natural de $\{r_n\}$ y $\{c_n\}$ que se obtendría de la prueba de la Proposición 1.2 es la siguiente:

$$\text{(1.6)} \qquad \begin{cases} r_1 = 1, & r_{n+1} = \min\{p + p\lfloor r_n/p\rfloor : p|c_n\}, \quad n \geq 1 \\ c_1 = a_1 - 2, & c_{n+1} = c_n + \operatorname{mcd}(c_n, r_{n+1}) - 1, \quad n \geq 1, \end{cases}$$

donde $\lfloor x \rfloor$ denota la parte entera de un número x y p es un número primo cualquiera. Es fácil comprobar que r_n^* y c_n^*, tal y como están definidas en (1.2), satisfacen (1.6) para $n > 1$. Y, como probaremos a continuación, esta definición alternativa coincide con la de la Definición 1.4.

Lema 1.5. *Dados enteros positivos $m > 1$ y n,*

$$\min\left\{p + p\left\lfloor \frac{n}{p}\right\rfloor \ : \ p \mid m\right\} = \min\{k > n \ : \ \operatorname{mcd}(k, m) \neq 1\}.$$

Demostración: Basta considerar que $p+p\lfloor n/p\rfloor = p(1+\lfloor n/p\rfloor)$ es el primer múltiplo de p mayor que n. El lado derecho denota por su parte al primer entero mayor que n no coprimo con m; dicho entero será múltiplo de los primos que alcancen el mínimo en el lado izquierdo. Por tanto ambas expresiones describen al mismo número. Nótese que imponiendo que m no pueda valer 1 los dos conjuntos descritos para los mínimos serán siempre no vacíos. □

Por tanto las dos definiciones para las sucesiones auxiliares generalizadas, $\{r_n\}$ y $\{c_n\}$, coinciden. Es interesante notar que la segunda definición, (1.6), permite calcular las sucesiones r_n y c_n con mayor rapidez (la hemos utilizado para las gráficas de la página 25 y siguientes), ya que el cálculo de varios máximos comunes divisores consecutivos es más costoso computacionalmente que factorizar un único número para obtener el siguiente término. Estas sucesiones nos van a permitir obtener un resultado en cierto modo similar a la Proposición 1.2 para caracterizar los valores que toma la sucesión $\{a_k - a_{k-1}\}$.

Proposición 1.6. *Consideremos la sucesión de Rowland generalizada* (1.4) *para a_1 fijo y, a partir de ésta, las sucesiones $\{r_n\}$ y $\{c_n\}$ dadas por* (1.5)*. Se cumple, para cada índice $k \geq 1$*

$$\text{(1.7)} \qquad a_k = c_n + k + 1 \qquad \textit{para } k \in [r_n, r_{n+1}).$$

Además, si $k \neq 1$,

$$\text{(1.8)} \qquad a_k - a_{k-1} = \begin{cases} \operatorname{mcd}(c_{n-1}, r_n) & \textit{si } k = r_n \textit{ para algún índice } n > 1, \\ 1 & \textit{en el resto de casos.} \end{cases}$$

Demostración: Recordemos que, como (1.4) requiere que a_1 sea impar y mayor que 5, las dos sucesiones auxiliares (1.5) están bien definidas y son estrictamente crecientes. En particular, dado cualquier k natural existirá un único índice $n \geq 1$ tal que $r_n \leq k < r_{n+1}$. Vamos a probar (1.7) y (1.8) simultáneamente utilizando inducción fuerte sobre k. Supongamos que las dos fórmulas están demostradas para todo j menor que un k fijo. Distinguimos dos casos.

Si existe n tal que $k \in (r_n, r_{n+1})$, entonces por la definición de r_{n+1} en (1.5) se cumplirá $\text{mcd}(k, c_n) = 1$. Como k,$1 \geq r_n$, se cumplirá $a_{k-1} = c_n + k$ por hipótesis de inducción. Utilizando esto y las definiciones de a_k y r_{n+1},

$$a_k - a_{k-1} = \text{mcd}(k, a_{k-1}) = \text{mcd}(k, c_n + k) = \text{mcd}(k, c_n) = 1.$$

Esto prueba (1.8), y $a_k = a_{k-1} + 1 = (c_n + k) + 1 = c_n + k + 1$ prueba (1.7).

El otro caso posible es que k coincida con r_n para algún índice n. Si $n = 1$, entonces $k = 1$ y (1.7) es inmediato (nótese que en este caso (1.8) no procede), por lo que podemos suponer $n > 1$. Se verificarán $\text{mcd}(r_n, c_{n-1}) \neq 1$ por (1.5) y $a_{k-1} = c_{n-1} + k$ por hipótesis de inducción. De donde

$$a_k - a_{k-1} = \text{mcd}(k, a_{k-1}) = \text{mcd}(k, c_{n-1} + k) = \text{mcd}(k, c_{n-1}) = \text{mcd}(r_n, c_{n-1}).$$

Esto completa la prueba de (1.8). A su vez, se cumple $a_k = a_{k-1} + \text{mcd}(r_n, c_{n-1}) = c_{n-1} + k + \text{mcd}(r_n, c_{n-1}) = c_n + k + 1$, lo que prueba (1.7). Y con esto abarcamos todos los posibles casos. □

k	1	2	3	4	5	6	7	...	40	41	42	...	82	83	84	...
a_k	35	36	39	40	45	48	49	...	82	123	126	...	166	249	252	...

Tabla 1.4: La sucesión de Rowland generalizada, tomando $a_1 = 35$.

Como puede verse, hay una pequeña variación entre las fórmulas (1.3) y (1.8) que explica por qué ahora no siempre se obtienen primos al considerar diferencias entre términos adyacentes: donde antes aparecía el menor factor primo de c_{n-1}, ahora encontramos un máximo común divisor, que por supuesto no será primo en general.

n	1	2	3	4	5	6	7	8	9	10	...
r_n	1	3	5	6	41	42	83	84	167	168	...
c_n	33	35	39	41	81	83	165	167	333	335	...
$\text{mcd}(c_{n-1}, r_n)$		3	5	3	41	3	83	3	167	3	...

Tabla 1.5: Las sucesiones auxiliares para $a_1 = 35$.

Examinemos un ejemplo tomando $a_1 = 35$. Las Tablas 1.4 y 1.5 son los análogos respectivos de las Tablas 1.1 y 1.2 que veíamos al inicio de la primera sección, referidas

a la sucesión de Rowland original. De nuevo los números que aparecen en la fila correspondiente a r_n (salvo el primero) se corresponden con los índices k en los que $a_k - a_{k-1}$ es mayor que 1. El problema es que ahora dicho incremento (que aparece reflejado en la última fila de la tabla 1.5) ya no tiene por qué ser primo. Los indicios apuntan a que esta fila estará ocupada exclusivamente por primos, salvo en número finito de casos, pero ahora en principio la recorremos a ciegas.

¿Qué ocurría en el caso $a_1 = 7$ que nos garantizaba que sólo encontraríamos primos en la sucesión $\{a_k - a_{k-1}\}$? ¿Es posible dar con algún análogo en el caso general que nos asegure que, al menos a partir de cierto punto, no aparecerán diferencias compuestas? La respuesta es que sí. Existen dos *indicadores* tales que, una vez aparece alguno de ellos en las sucesiones auxiliares, nos indican que de ahí en adelante todos los incrementos superiores a 1 serán primos. Estos indicadores son, por tanto, condiciones suficientes. Para introducirlos, partimos del siguiente resultado:

Proposición 1.7. *Fijemos a_1 impar mayor o igual que 5 y consideremos la sucesión dada por (1.4). Si se cumple $r_{n_0} = (c_{n_0} + 1)/2$ para algún índice n_0, entonces*

$$c_n = c_{n-1} + \text{mfp}(c_{n-1}) - 1 \quad y \quad r_n = (c_n + 1)/2, \tag{1.9}$$

para todo $n > n_0$.

Demostración: Vamos a probar que si $r_m = (c_m+1)/2$ para cualquier $m \geq n_0$ dado, entonces se cumplirá (1.9) para $m+1$, y habremos probado la Proposición mediante inducción. Utilizando (1.5),

$$r_{m+1} = r_m + \text{mín}\{l \geq 1 \ : \ \text{mcd}(r_m + l, c_m) \neq 1\},$$

donde $\text{mcd}(r_m+l, c_m) = \text{mcd}((c_m+1+2l)/2, c_m) = \text{mcd}(1+2l, c_m)$, gracias a que c_m es siempre impar. Por tanto, $1+2l = \text{mfp}(c_m)$, luego $r_{m+1} = r_m + (\text{mfp}(c_m) - 1)/2$ y

$$c_{m+1} = c_m + \text{mcd}\Big(c_m, \frac{c_m + 1}{2} + \frac{\text{mfp}(c_m) - 1}{2}\Big) - 1 = c_m + \text{mfp}(c_m) - 1.$$

Esto prueba (1.9) para $m+1$ y concluye la demostración. □

El hecho de que aparezca un índice n_0 para el que se tenga la igualdad arriba mencionada es, de hecho, el primer indicador o condición suficiente. El segundo es que aparezca un número primo en la sucesión $\{c_n\}$. Cualquiera de estos dos hechos basta para que se tenga la conjetura:

Proposición 1.8. *Considérese la sucesión de Rowland generalizada con término inicial a_1. Supongamos que se cumple alguna de las dos siguientes condiciones:*

1. *Existe un entero positivo n_0 tal que $r_{n_0} = (c_{n_0} + 1)/2$.*

2. Existe un entero positivo m_0 tal que c_{m_0} es primo.

Entonces la Conjetura 1.3 es cierta.

Demostración: Podemos suponer que se cumple la primera de las dos condiciones, puesto que la segunda implica de forma inmediata la primera para $n_0 = m_0 + 1$. Las Proposiciones 1.6 y 1.7 implican que, si se toma $k = r_n$ con $n > n_0$, debe cumplirse

$$\begin{aligned} a_k - a_{k-1} = \mathrm{mcd}(c_{n-1}, r_n) &= \mathrm{mcd}\Big(c_n + 1 - \mathrm{mfp}(c_{n-1}), \frac{c_n + 1}{2}\Big) \\ &= \mathrm{mcd}(\mathrm{mfp}(c_{n-1}), c_n + 1) = \mathrm{mfp}(c_{n-1}). \end{aligned}$$

Esto concluye la prueba. □

n	1	2	3	4	5	6	7	8	9	10	...
r_n	1	5	6	11	12	23	24	47	48	50	...
c_n	*5*	9	11	21	23	45	47	93	95	99	...

n	1	2	3	4	5	6	7	8	9	10	...
r_n	1	3	5	6	41	42	83	84	167	168	...
c_n	33	35	39	*41*	81	83	165	167	333	335	...

n	1	2	3	4	5	6	7	8	9	10	11
r_n	1	7	11	17	18	20	21	29	30	35	587
c_n	511	517	527	543	545	549	551	579	581	*587*	1173

n	1	2	3	4	5	6	7	8	9	10	...
r_n	1	5	7	10	12	131	132	263	264	272	...
c_n	115	119	125	129	*131*	261	263	525	527	543	...

Tabla 1.6: Sucesiones auxiliares para $a_1 = 7, 35, 513$ y 117, respectivamente. En cursiva, el primer primo que aparece en la sucesión $\{c_n\}$ en cada caso.

En la Tabla 1.6 pueden verse una serie de ejemplos, cada uno de ellos correspondiente a tomar $a_1 = c_1 + 2$. Los dos primeros ya son conocidos, pero es interesante volver a contemplarlos desde el nuevo prisma que nos brinda la Proposición 1.8. Una vez aparece un primo en la sucesión $\{c_n\}$, ahora sí tenemos garantizado que todos los términos de la sucesión $\{\mathrm{mcd}(c_{n-1}, r_n)\}$ que aparezcan de ahí en adelante van a ser primos. Ahora podemos responder a la pregunta que planteábamos en la introducción acerca de qué tenía de especial el 7. No más que el hecho de que $c_1 = 7 - 2 = 5$ es primo.

Lo que ocurre en estos cuatro ejemplos parece probable, a la luz de los cálculos por ordenador, que ocurrirá siempre, se tome el valor inicial que se tome. No sólo los dos apartados de la Proposición 1.8, sino además, de forma *consecutiva*; es decir, la primera vez que tengan lugar ambos hechos es con un paso de diferencia. Para muestra, en cada uno de los cuatro ejemplos anteriores puede comprobarse que las sucesiones $\{r_n\}$ y $\{c_n\}$ nunca cumplen $r_n = (c_n + 1)/2$ hasta que aparece el primer primo en $\{c_n\}$. Formalizando esta idea, vamos a dar una segunda conjetura que implicaría la original que planteábamos al principio de este capítulo.

Definición 1.9. *Dada la sucesión* (1.4) *para un cierto* a_1*, definimos* n_0 *como el primer índice en el que se cumple* $r_{n_0} = (c_{n_0} + 1)/2$ *y* m_0 *como el primero en el que* c_{m_0} *es primo. En ambos casos, si el hecho correspondiente no llega a tener lugar, se define* n_0 *y/o* m_0 *como infinito.*

Conjetura 1.10. *Sea* a_1 *impar y mayor o igual que* 5*. Entonces*

- (I) $n_0 < \infty$.
- (II) $m_0 < \infty$.
- (III) $n_0 = m_0 + 1 < \infty$.

No nos ha sido posible demostrar esta conjetura. Aunque parece muy probable que dada cualquier condición inicial la sucesión $\{c_n\}$ siempre acabe pasando sobre algún primo, no se conoce una forma de demostrar esto en todos los casos. Existen otras conjeturas en la teoría de los números cuyo nexo común es la idea de que cualquier sucesión creciente debe tomar valores primos salvo que condiciones de divisibilidad local lo impidan. Destacan entre ellas la hipótesis de Schinzel [SS58]; la conjetura de Hardy-Littlewood, que generaliza la conjetura de los primos gemelos [ORW99], [GBGL08, IV.2]; o de forma más general la conjetura de Bateman-Horn [BH62]. Consúltese [Clo11] para más información en este aspecto.

n	1	2	3	4
r_n	59	60	65	66
c_n	93	95	99	131

Tabla 1.7: Un ejemplo comenzando en $a_{59} = 153$.

Es un buen momento para mostrar con un ejemplo por qué generalizar la sucesión de Rowland permitiendo que el primer elemento no sea a_1, sino a_k para k entero, es un problema más amplio. Comenzando por ejemplo en $a_{59} = 153$, se cumple la Proposición 1.6 si se toman $r_1 = 59$ y $c_1 = 93$. Con estas condiciones iniciales, las sucesiones auxiliares seguirían el comportamiento de la Tabla 1.7. El análogo a la

condición (I) se daría para $n_0 = 4$, ya que $c_4 = 2r_4 - 1$. Pero $c_3 = 99$ no es un número primo y la Conjetura 1.10 no puede aplicarse.

Durante el resto de esta sección nos centraremos en dar algunas aproximaciones a la conjetura, y estableceremos un objetivo algo menos ambicioso; probar que los tres puntos de la conjetura 1.10 son equivalentes. En adelante se dará por hecho que se parte de una sucesión de Rowland generalizada con a_1 arbitrario; y nos referiremos a los valores n_0 y m_0 que aparecen en la Definición 1.9.

Proposición 1.11. *Las sucesiones auxiliares* $\{r_n\}$ *y* $\{c_n\}$ *verifican* $r_n \leq (c_n + 1)/2$ *para cada entero positivo* n*. De hecho, para* $n > 1$ *la igualdad exacta ocurrirá si y sólo si* $\mathrm{mcd}(c_{n-1}, r_n)$ *es un primo* p *y* $p \lfloor r_{n-1}/p \rfloor = (c_{n-1} - p)/2$*.*

Demostración: Emplearemos inducción para probar la desigualdad. Que $2r_1 \leq c_1 + 1$ se cumple está claro. Supongamos que $r_{n-1} \leq (c_{n-1} + 1)/2$ para un cierto índice n. Por definición, $r_n = p + p \lfloor r_{n-1}/p \rfloor$ para algún primo $p \mid c_{n-1}$. Se tendrá entonces

$$r_n = p + p \left\lfloor \frac{r_{n-1}}{p} \right\rfloor \leq p + p \left\lfloor \frac{c_{n-1} + 1}{2p} \right\rfloor = p + \frac{c_{n-1} - p}{2} = \frac{c_{n-1} + p}{2}. \tag{1.10}$$

Por otro lado, utilizando que p es un divisor de $\mathrm{mcd}(c_{n-1}, r_n)$,

$$\frac{c_{n-1} + p}{2} \leq \frac{c_{n-1} + \mathrm{mcd}(c_{n-1}, r_n)}{2} = \frac{c_n + 1}{2}. \tag{1.11}$$

Combinando (1.10) y (1.11) se completa el paso inductivo.

Si $\mathrm{mcd}(c_{n-1}, r_n)$ no es primo, entonces habrá una desigualdad estricta en (1.11) y $r_n \neq (c_n + 1)/2$. Lo mismo ocurre si $p \lfloor r_{n-1}/p \rfloor \neq (c_{n-1} - p)/2$ empleando ahora (1.10). Por tanto, las propiedades citadas en el enunciado son condiciones necesarias para que se tenga la igualdad. Es fácil comprobar que en sentido contrario ocurre lo mismo. □

Ya adelantamos antes que uno de nuestros objetivos era tratar de probar que los tres hechos recogidos en la conjetura 1.10 son equivalentes. ¿Cómo están relacionados los tres puntos? Como vimos en la prueba de la Proposición 1.8, el segundo implica el primero, y está claro que el tercero implica los otros dos. Veremos ahora una serie resultados parciales para tratar de probar que (I) implica (III), lo que completaría la equivalencia. El primero de estos resultados se obtiene de la Proposición anterior:

Corolario 1.12. *Si se cumple* (I) y $\mathrm{mcd}(c_{n_0-1}, r_{n_0}) > r_{n_0-1}$, entonces (III) también debe cumplirse.

Demostración: Supongamos que (I) es cierto y que el máximo común divisor de c_{n_0-1} y r_{n_0} (al que llamaremos d) es mayor que r_{n_0-1}. Entonces $c_{n_0} = c_{n_0-1} + d - 1$

y $r_{n_0} = (c_{n_0-1} + d)/2$. Por otro lado, la diferencia entre r_{n_0} y r_{n_0-1} es menor o igual que d, ya que siempre algún número entre $r_{n_0-1}+1, \ldots, r_{n_0-1}+d$ ha de ser múltiplo de d. Por tanto, $(c_{n_0-1}+d)/2 = r_{n_0} \leq r_{n_0-1}+d < 2d$. Esto implica $c_{n_0-1} < 3d$. Como c_{n_0-1} es impar, cualquier divisor propio que tenga será menor o igual que su tercera parte. Por tanto, la única posibilidad es que d sea el propio c_{n_0-1}. Pero entonces $c_{n_0} = 2c_{n_0-1} - 1$ y por tanto c_{n_0-1} debe ser primo. Además, todos los anteriores a él deben ser compuestos (si no, se cumpliría (I) con un índice menor que n_0). Concluimos entonces que (III) es cierto. □

A continuación vamos a ver una manera de redefinir m_0 sin hacer referencia alguna a los números primos.

Proposición 1.13. *Para un $n > 1$ dado, $r_n = c_{n-1}$ si y sólo si c_{n-1} es primo.*

Demostración: Si c_{n-1} es primo, la Proposición 1.11 implica $r_{n-1} < c_{n-1}$ y utilizando (1.5) concluimos que r_n y c_{n-1} deben ser iguales.

Recíprocamente, supongamos que $r_n = c_{n-1}$ y tomemos $m = (c_{n-1}+\text{mfp}(c_{n-1}))/2 = (r_n+\text{mfp}(r_n))/2$. Se cumplirá entonces que $\text{mcd}(m, c_{n-1}) \neq 1$ y, apelando de nuevo a la Proposición 1.11, $r_{n-1} < m$. La definicion de r_n dada por (1.5) implica $r_n \leq m$ o, equivalentemente, $r_n = \text{mfp}(r_n)$. Luego $r_n = c_{n-1}$ es primo. □

La Proposición que acabamos de probar puede reformularse de la siguiente forma, lo que nos permite efectivamente redefinir m_0:

Corolario 1.14. *Si para algún $n > 1$ se cumple $r_n = c_{n-1}$ para algún $n > 1$, entonces* (I) *y* (II) *son ciertos.*

Proposición 1.15. *Suponiendo que* (III) *es cierto, existe un primo p tal que*

$$\text{ínf}\{k \,:\, a_k = 3k\} = \frac{p+1}{2} \qquad y \qquad \text{ínf}\{k \,:\, a_k = 3k,\ a_k - a_{k-1} > 1\} = p.$$

Demostración: Es fácil ver que $a_k = 3k$ equivale a $c_n = 2k - 1$. Si $a_k - a_{k-1} > 1$, entonces k debe ser igual a r_n para algún índice n, como consecuencia de la Proposición 1.6. Como r_n es una sucesión estrictamente creciente, su mínimo se alcanza en r_{n_0} que debe ser primo por la Proposición 1.13.

Tome el valor que tome $a_k - a_{k-1}$, la Proposición 1.6 garantiza que para $k \in [r_{n_0-1}, r_{n_0})$

$$a_k = 3k \;\Leftrightarrow\; k = \frac{c_{n_0-1}+1}{2} = \frac{p+1}{2},$$

y este valor está justamente en el intervalo $[r_{n_0-1}, r_{n_0})$, gracias a la Proposición 1.11.

Sólo falta comprobar que $a_k > 3k$ para todo $k \leq r_{n_0-1}$. De no ser así, si $a_{k-1} \leq 3(k-1)$ para algún k, entonces $3 \leq 3k - a_{k-1}$. Por la Proposición 1.6, $a_k - a_{k-1}$ equivale a $\text{mcd}(c_{n-1}, r_n)$ para $k = r_n$ y a 1 en el resto de casos, y por tanto es siempre

un divisor de $3k - a_{k-1}$, luego $a_k - a_{k-1} \leq 3k - a_{k-1}$, y por tanto $a_k \leq 3k$. Repitiendo este proceso se llega a una contradicción para $k = r_{n_0-1}$. □

Nuestros cálculos efectuados por ordenador indican que la cantidad $(c_n + 1)/r_n$, donde n recorre los índices menores que n_0, son mucho mayores que 2 cuando la condición inicial a_1 es suficientemente grande. Mejorar la Proposición 1.11 cambiando ese 2 por cualquier otra cantidad mayor supondría una enorme mejora, ya que la equivalencia entre (I) podría probarse con un número finito de cálculos. Para ilustrar esto, vamos a ver lo que ocurría si la Proposición 1.11 fuese cierta para $2 + \frac{1}{2500}$.

Proposición 1.16. *Supongamos que* (I) *es cierto y que* $\big(2 + \frac{1}{2500}\big) r_n < c_n + 1$ *para* $n < n_0$. *Entonces,* (III) *también es cierto.*

Demostración: De la Proposición 1.11 sabemos que $\mathrm{mcd}(c_{n_0-1}, r_{n_0}) = p$. Además, para ciertos j y l se debe cumplir

$$\begin{aligned} r_{n_0-1} &= pj + l, & r_{n_0} &= p(j+1), \\ c_{n_0-1} &= p(2j+1), & c_{n_0} &= 2p(j+1) - 1. \end{aligned}$$

Para simplificar, pongamos $K = 3500$. Si $j > K$,

$$\frac{c_{n_0-1} + 1}{r_{n_0-1}} \leq \frac{p(2j+1) + 1}{pj} = 2 + \frac{1}{j} + \frac{1}{3j} < 2 + \frac{1}{2500},$$

que no cumple la hipótesis del enunciado. Podemos entonces suponer $1 \leq j \leq K$, ya que $j = 0$ conduce inmediatamente a (III). Vamos a distinguir varios casos.

Si $p \leq 4K - 3$ entonces $c_{n_0-1} < 10^8 - 2$ y la condición inicial a_1 debe ser inferior a 10^8, para la que hemos comprobado mediante cálculos por ordenador que (III) se cumple.

Podemos tomar entonces $p > 4K - 3$. Si $l < p - 2K$, siempre ha de existir $r_{n_0-1} < m < r_{n_0}$ que sea múltiplo de $2j + 1$, de donde $\mathrm{mcd}(m, c_{n_0-1}) \neq 1$; esto entra en contradicción con la Definición 1.4. El último caso posible corresponde a $l \geq p - 2K$. Se tendrá lo siguiente:

$$\frac{c_{n_0-1} + 1}{r_{n_0-1}} \leq \frac{p(2j+1) + 1}{p(j+1) - 2K} = 2 + \frac{4K - p + 1}{p(j+1) - 2K}.$$

Introduciendo la desigualdad asumida en el enunciado, debería cumplirse

$$p(j+1) - 2K < 2500\big(4K - p + 1\big),$$

que no es posible tomando $j > 0$ y $p > 4K - 3$. □

En sentido contrario, puede probarse que la aparición del primer primo en la sucesión $\{c_n\}$ puede retrasarse arbitrariamente para alguna condición inicial a_1 suficientemente grande.

Proposición 1.17. *Dado un entero N arbitrariamente grande, siempre existe una condición inicial a_1 tal que $m_0 > N$.*

Demostración: Tómese cualquier a_1 que cumpla (II) (está claro por lo estudiado hasta ahora que hay muchos casos en los que se cumple). Sea $m_0 < \infty$ el mínimo índice tal que c_{m_0} es primo. Sea ahora $a_1' = a_1 + M$ con $M = c_{m_0}!$. Afirmamos que, para $j \leq m_0$, las sucesiones auxiliares (1.5) correspondientes a a_1' son

$$r_j' = r_j \qquad \text{y} \qquad c_j' = c_j + M.$$

En efecto, como $\text{mcd}(k, c_j + M) = \text{mcd}(k, c_j)$ para cada $k \leq r_{m_0}$, la igualdad anterior es consecuencia de la Definición 1.4 y del hecho de que k es un divisor de M.

Como c_j es claramente un factor no trivial de c_j', debe cumplirse $m_0' > m_0$. Este proceso puede iterarse cuantas veces se quiera; si se hace N veces, obtendremos una condición inicial cuyo índice m_0 será al menos N unidades mayor que el m_0 correspondiente al a_1 original. □

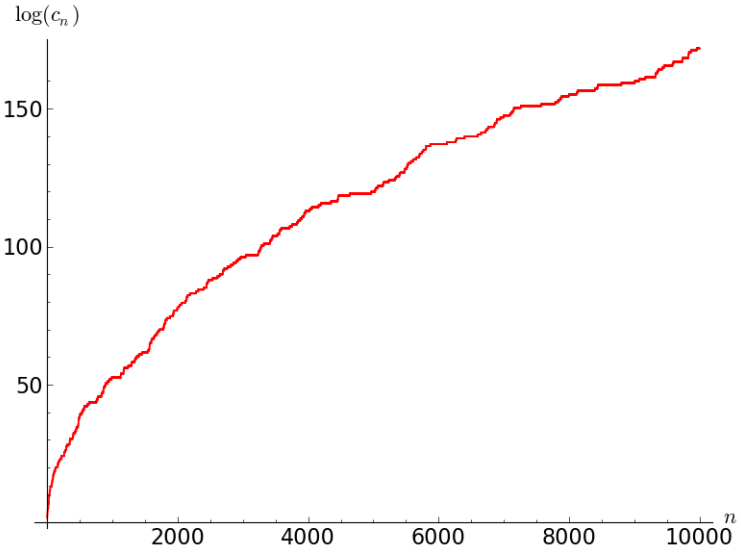

Figura 1.1: Gráfica logarítmica de c_n para $c_1 = 5$.

Finalizamos esta sección con un apunte sobre el crecimiento de la sucesión c_n. Nuestros cálculos están basados en la sucesión de Rowland original, aunque no es aventurado suponer que debe ocurrir algo parecido en otros casos. Contemplando de nuevo la definición recursiva de $\{c_n\}$, ya se intuye que a medida que n crezca y c_n sea grande, la diferencia entre c_{n-1} y c_n será mínima si c_{n-1} tiene divisores primos pequeños y muy grande si es el producto de unos pocos primos grandes o es de hecho un número primo. En este último caso, c_n duplicará a su predecesor. En general,

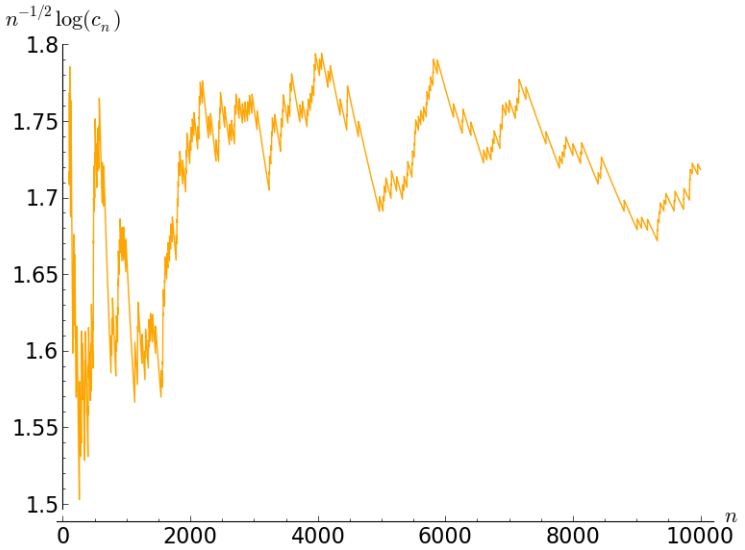

Figura 1.2: Gráfica de $n^{-1/2}\log(c_n)$ para $c_1 = 5$ y $100 < n \leq 10000$.

$C_1 n \leq c_n \leq C_2 2^n$, A efectos de orden de magnitud, puede estimarse el crecimiento de la sucesión $\{c_n\}$ diciendo que su tamaño se multiplicará por dos cada vez que pase por un primo y permanecerá prácticamente constante en el resto de casos. Puesto que la probabilidad de que un número N sea primo es aproximadamente $(\log N)^{-1}$ (gracias al Teorema del número primo), la sucesión c_n se puede estimar como un proceso aleatorio que parte de $c_1 = 5$ y viene dado por

$$\log c_n = \begin{cases} \log c_{n-1} + \log 2, & \text{con probabilidad } \frac{1}{\log c_{n-1}} \\ \log c_{n-1}, & \text{con probabilidad } 1 - \frac{1}{\log c_{n-1}}. \end{cases}$$

En base a lo anterior, el valor esperado de $\log c_n$ en función del de su predecesor será $1 + \log 2/\log c_{n-1} + \log c_{n-1} - 1 = \log 2/\log c_{n-1} + \log c_{n-1}$. Esto sugiere que el orden de crecimiento de $\log c_n$ será similar al de $\sqrt{n}$, ya que para valores suficientemente grandes de n

$$\sqrt{n} = \sqrt{n-1}\sqrt{1 + \frac{1}{n-1}} \sim \sqrt{n-1}\left(1 + \frac{1}{2(n-1)}\right) = \sqrt{n-1} + \frac{1}{2\sqrt{n-1}}.$$

La representación de la gráfica del logaritmo de c_n para los primeros 10000 términos corrobora esta idea (véase la Figura 1.1), apreciándose aún mejor al representar el cociente entre ambas sucesiones (véase la Figura 1.2).

1.3. Primos y Cadenas de Rowland

Proposición 1.18. *Si cualquiera de las condiciones* (I), (II) *o* (III) *de la Conjetura 1.10 fuera cierta, entonces la Conjetura 1.3 también lo sería; de hecho, en ese caso la sucesión* $\{a_k - a_{k-1}\}_{k=1}^{\infty}$ *contendría infinitos primos diferentes.*

Demostración: Parte de lo que queremos demostrar ya se vio en la prueba de la Proposición 1.8. Concretamente, como cualquiera de las tres condiciones implica que se cumpla la primera, podemos suponer sin perdida de generalidad que (I) es cierto. Ya vimos que, en ese caso, $a_k - a_{k-1}$ siempre sería o bien 1 o bien un número primo. Resta entonces probar que la sucesión $\{a_k - a_{k-1}\}_{k=1}^{\infty}$ contiene infinitos elementos diferentes, que en particular serán primos. Sea P el producto de todos los primos menores que N, con N escogido de forma que se tenga $P > c_{n_0}$. Sea n el único entero tal que $c_n < P \leq c_{n+1}$. Si escribimos $c_n = pq$, donde $p = \text{mfp}(c_n)$ y empleamos la Proposición 1.7, entonces $pq < P \leq pq + p - 1$, y por tanto $0 < P - pq < p$. Finalmente, como $P - pq$ no puede ser múltiplo de p, deducimos que p debe ser mayor que N.

Hemos visto que dado N arbitrario suficientemente grande, siempre puede hallarse n tal que $a_{r_n+1} - a_{r_n} = \text{mfp}(c_n) = p > N$. Basta hacer tender N a infinito para conseguir el resultado. □

En particular, la Sucesión de Rowland y muchas de sus generalizaciones (si no todas) son generadores naturales de primos tales que si su algoritmo se ejecuta un número suficientemente grande de pasos, producirá primos arbitrariamente grandes. Por desgracia, su aplicación práctica en ese sentido es relativamente escasa: de (1.4) es inmediato deducir que para que un primo p aparezca como diferencia entre dos términos consecutivos de la sucesión de Rowland, el índice de esos términos será mayor que p, con lo que habrá que ejecutar al menos p pasos de un algoritmo relativamente lento para un ordenador.

Ya mencionábamos en la primera sección que no todas las sucesiones de primos (eliminando los unos intermedios) iban a poder aparecer. El primer y sencillo ejemplo es que un mismo primo nunca podrá aparecer dos veces de forma consecutiva, lo cual es una consecuencia inmediata de (1.5) y (1.8). Con la motivación de explorar con más profundidad qué secuencias de primos aparecen y cuáles no, introducimos el siguiente concepto.

Definición 1.19. *Diremos que una sucesión finita* $C_k = \{p_1, p_2, \ldots, p_k\}$ *de primos impares es una* cadena de Rowland *si existe* $a_1 \geq 5$ *impar tal que* $p_n = c_n$ *para* $1 \leq n \leq k$*, donde* $\{c_n\}$ *viene dada por (1.5).*

Dada una sucesión finita de primos cualesquiera C_k, definimos las siguientes sumas parciales:

$$S(1) = 0; \qquad S(n) = \sum_{j<n}(p_j - 1), 1 \leq n \leq k,$$

que nos van a permitir caracterizar las cadenas de Rowland, por medio del siguiente resultado:

Proposición 1.20. *Una sucesión finita de primos impares $C_k = \{p_1, p_2, \ldots, p_k\}$ es una cadena de Rowland si y sólo si se cumplen las tres siguientes condiciones:*

a) $S(m) \equiv S(n) \pmod{p_n}$ *siempre que* $p_n = p_m$.

b) $S(m) \not\equiv S(n) \pmod{p_n}$ *siempre que* $p_n < p_m$.

c) *Para todo primo q, el conjunto $\{S(j) \pmod{q} : p_j > q\}$ no contiene todas las clases de residuos módulo q.*

Demostración: Comenzamos notando que, por construcción, $c_n^* = c_1^* + S(n)$ y C_k será una cadena de Rowland si y sólo si existe c_1^* cumpliendo para cada $1 \leq n \leq k$

$$(1.12) \quad c_1^* + S(n) \equiv 0 \pmod{p_n} \quad \text{y} \quad c_1^* + S(n) \not\equiv 0 \pmod{q} \quad \text{para todo } q < p_n.$$

Si $p_n = p_m$, entonces $c_1^* + S(n) \equiv c_1^* + S(m) \equiv 0 \pmod{p_n}$ implica a). En sentido contrario, el Teorema chino del resto garantiza la existencia de solución para el primer conjunto de ecuaciones de (1.12) bajo estas condiciones.

Sea ahora q un primo no superior al máximo de todos los que hay en C_k. Las ecuaciones de (1.12) que involucran a q serán

$$c_1^* + S(m) \not\equiv 0 \pmod{q} \quad \text{para } m \in \{j : p_j > q\};$$

además, si q forma parte de C_k, por ejemplo $q = p_n$, debe añadirse

$$c_1^* + S(n) \equiv 0 \pmod{q}.$$

En el primer caso existirá solución módulo q si y sólo si $S(m)$ no abarca todas las clases residuales, de donde sale c). En el segundo caso también necesitamos $S(m) \not\equiv S(n) \pmod{p_n}$, de donde sale b). □

Nótese que en la tercera condición sólo es necesario comprobar un número finito de primos; concretamente, si q es mayor que todos los elementos de C_k, el conjunto descrito será vacío. De igual forma, dicha tercera condición se cumplirá de forma trivial siempre que q sea mayor que k. Por tanto, esta caracterización permite comprobar de forma efectiva si cualquier sucesión de primos finita es o no una cadena de Rowland. Por ejemplo, $\{3, 19, 5, 3\}$ es una cadena de Rowland ya que $S(1) = 0$ y $S(4) = 24$ implican a). El resto de valores, $S(2) = 2$, $S(3) = 20$ implican que ni

$S(1)$ ni $S(4)$ son congruentes con $S(2)$ o $S(3)$ (mód 3), y $S(2) \not\equiv S(3)$ (mód 5), lo que prueba b). Por último, c) no requiere ninguna verificación adicional (más allá del caso trivial $q = 2$) porque si el conjunto es no vacío $q \geq 5$ y sólo tenemos 4 clases residuales. Por otro lado, $\{17, 5, p\}$ nunca será una cadena de Rowland para ningún $p > 3$ al no cumplirse la condición c) para $q = 3$.

Sabemos, gracias a la segunda parte de la Proposición 1.18, que la sucesión de primos no puede ser periódica; pero de hecho la realidad es aún más restrictiva, ya que tampoco pueden repetirse bloques.

Corolario 1.21. *Si $p_1, \ldots, p_k$ son primos distintos, entonces*

$$C_{2k} = \{p_1, p_2, \ldots, p_k, p_1, p_2, \ldots, p_k\}$$

no es una cadena de Rowland.

Demostración: Nótese que $\lambda = S(n + k) - S(n)$ es constante para $1 \leq n \leq k$. Por lo tanto, la primera condición de la caracterización implica que tal valor es divisible por todos los p_n, y por tanto λ es un múltiplo de $p_1 p_2 \ldots p_k$. Pero esto no es posible, al ser el producto mayor que λ. □

En la mayoría de casos, la Proposición 1.20 impone grandes restricciones para construir cadenas de Rowland de gran tamaño con sólo unos pocos primos dados diferentes. Aunque por otro lado es posible hallar cadenas de gran longitud para selecciones especiales de primos. Por ejemplo, utilizando sólo los primeros cinco primos impares no pueden construirse cadenas de longitud superior a 10, pero se tiene que

$$C_{27} = \{3, 5, 3, 23, 3, 5, 3, 653, 3, 5, 3, 23, 3, 5, 3, 3603833, 3, 5, 3, 23, 3, 5, 3, 653, 3, 5, 3\}$$

es una cadena de Rowland de 27 elementos que tan sólo involucra a cinco primos: $3, 5, 23, 653$ y 3603833. Es, de hecho, maximal para este conjunto de primos (existe otra válida de la misma longitud). Corresponde a $c_1^* = 1550303031682203$.

Nótese que La prueba del Corolario 1.21 nos dice que

$$\text{mcm}(p_1, p_2, \ldots, p_k) \mid \sum_{j=1}^{k} (p_j - 1),$$

incluso admitiendo que se repitan primos. Esperamos que tampoco en este caso puedan aparecer bloques consecutivos idénticos, ya que la Proposición 1.20 impondría condiciones muy restrictivas. Por otro lado, pensamos que es posible concatenar grandes bloques idénticos insertando otro primo entre ellos, como en el último ejemplo.

Los resultados expuestos en este capítulo aparecieron recogidos originalmente en [CRRC11].

Capítulo 2

Identidades aproximadas y formas de Maass

2.1. Introducción

El capítulo que nos ocupa a continuación es, notablemente, más técnico que el anterior; lo cual implica que debemos presentar y exponer nuestras herramientas de trabajo antes de poder empezar a obtener resultados satisfactorios con ellas. Por este motivo, nos tomaremos la licencia de comenzar con un ejemplo que aun estando en otro plano totalmente distinto, ilustra con fuerza las ideas principales en las que nos basaremos más adelante. Se trata del ejemplo que expusimos con brevedad en la introducción, si bien ahora lo trataremos de forma más minuciosa. El ejemplo en cuestión es la siguiente serie truncada:

$$S = \frac{1}{4}\left(\sum_{n=-15}^{15} e^{-n^2/4}\right)^2. \tag{2.1}$$

Si alguien se toma la molestia de usar un ordenador o una calculadora para escribir la expresión decimal de (2.1), encontrará una secuencia que le resultará familiar. No en vano, S aproxima al número π con algo más de una docena de cifras decimales. Concretamente, es fácil probar que la diferencia entre S y π es menor que 10^{-15} y, por supuesto, positiva. La expresión que define S es, por tanto, una *identidad aproximada* para π.

Que esto ocurra no es, por supuesto, una casualidad. El bosque oculto tras los árboles es la famosa fórmula de sumación de Poisson,

$$\sum_{n=-\infty}^{\infty} f(n) = \sum_{n=-\infty}^{\infty} \widehat{f}(n),$$

válida entre otros casos cuando f es una función de *decaimiento rápido*, como lo es por ejemplo la gaussiana $f(x) = e^{-\lambda x}$. Tomando $\lambda = 1/4$, la transformada de f tendrá un exponente grande y ya el término en $n = 1$ será significativamente pequeño. Bajo este nuevo prisma, la fórmula (2.1) puede reescribirse para mostrarnos toda la maquinaria oculta que había tras el telón.

$$S = \widehat{f}(0) - 2\sum_{n\geq 16} e^{-n^2/4} + \sum_{n\neq 0} \sqrt{4\pi} e^{-4\pi^2 n^2} \approx \widehat{f}(0) = 2\sqrt{\pi}. \tag{2.2}$$

Nótese que la elección del número 15 para truncar la serie no es arbitraria; para ese valor, las dos series en (2.2) tienen prácticamente el mismo orden de magnitud, y no aporta nada el reemplazar 15 por cualquier otro entero mayor.

Este mismo ejemplo que acabamos de ver puede interpretarse de otra manera que nos acercará al contenido de las próximas secciones. Si consideramos el operador laplaciano en una dimensión, $\Delta = -d^2/dx^2$, algunas de sus autofunciones son senos y cosenos. De hecho todas las posibles son exponenciales complejas. Ahora, de entre las autofunciones $f : [0,1] \longrightarrow \mathbb{C}$, vamos a imponer como condiciones de contorno que tengan el mismo valor en los extremos del intervalo. Es decir, soluciones de la siguiente ecuación diferencial:

$$\begin{cases} \Delta f &= \lambda f \\ f(0) &= f(1). \end{cases}$$

La condición de contorno sólo se cumple cuando el exponente es un múltiplo entero de 2π. Por tanto, las autofunciones son $\{e^{2\pi i j x}\}_{j\in\mathbb{Z}}$, con sendos autovalores $\lambda_j = 4\pi^2 j^2$. Al ser el laplaciano un operador diferencial lineal autoadjunto estas funciones, convenientemente normalizadas, forman una base ortonormal del espacio de funciones $\{f : [0,1] \longrightarrow \mathbb{C}\}$, y la teoría nos dice que cualquier función suficientemente regular que se anule en los bordes admitirá un desarrollo en esta base. Esto es una restricción significativa, puesto que nos gustaría tratar con funciones definidas sobre toda la recta real y, en general, la mayoría de estas funciones toman valores arbitrarios en 0 y en 1. Existe una manera de proceder para suavizar esto, reformulando cualquier función real f para obtener otra 1-periódica. Esto se hace considerando la suma de todas las traslaciones enteras actuando sobre f. Con estas ideas en mente definimos, siempre que se tenga la convergencia, el *núcleo automorfo*:

$$F(x,y) := \sum_{n\in\mathbb{Z}} f\left(d(x+n,y)\right) = \sum_{n\in\mathbb{Z}} f(|x+y-n|), \qquad x,y\in\mathbb{R}, \tag{2.3}$$

donde d es la distancia euclídea habitual. La nueva función es invariante por traslaciones enteras en cada uno de sus dos parámetros; es decir, $F(x+n,y) = F(x,y) = F(x,y+m)$ para cualesquiera n y m enteros. En particular se tiene la 1-periodicidad

que buscábamos. Lo cual nos permite adaptar $f(x) = e^{-x^2/4}$ a un núcleo que se escribe en función de la base dada por las autofunciones $\phi_j(x) := e^{-2\pi i j x}$. Los coeficientes serán precisamente los coeficientes de Fourier de f:

(2.4)
$$F(x,y) = \sum_{n\in\mathbb{Z}} e^{(x+n-y)^2/4} = 2\sqrt{\pi}\sum_{j\in\mathbb{Z}} e^{\lambda_j}\phi_j(x)\overline{\phi_j(y)} = 2\sqrt{\pi}\sum_{j\in\mathbb{Z}} e^{-4\pi^2 j^2} e^{2\pi i j x} e^{-2\pi i j y}.$$

Ahora basta tomar $x = y = 0$ y truncar la serie a la izquierda de (2.4) para llegar al mismo punto que en (2.2). El primer autovalor no trivial es $\lambda_1 > 39$, lo que explica la escasa contribución de todos los términos de la serie a la derecha, salvo la de λ_0. Y por tanto el valor de $F(0,0)$ está muy bien aproximado por $2\sqrt{\pi}$.

Esto concluye nuestro acercamiento a la puerta de entrada del sugerente mundo de las identidades aproximadas. Muchas de ellas, como la que acabamos de ver, tienen en común el desarrollo de Fourier de expresiones con un cierto significado aritmético y la rápida convergencia de sus transformadas. No se encuentra en esta categoría el probablemente ejemplo más famoso y que no nos resistimos a volver a mencionar; la llamada constante de Ramanujan, $e^{\pi\sqrt{163}}$, que dista de un entero menos de 10^{-12} y que justifica por sí misma el interés en este área (la referencia [CR10] contiene una detallado explicación autocontenida de por qué esta constante está tan cerca de un entero).

En el resto de este capítulo nos adentraremos más profundamente para obtener identidades aproximadas algo menos habituales, procedentes de la teoría espectral de formas automorfas. Sustituiremos nuestro espacio de trabajo original, la recta real, por el semiplano de Poincaré. En este contexto resulta natural utilizar un sustituto del laplaciano habitual: el operador de Laplace-Beltrami. Las autofunciones con las que formaremos una base se llaman *formas de Maass*, y nos permitirán dar un análogo al desarrollo de un núcleo automorfo (la llamada fórmula de pretraza). El papel de las traslaciones enteras lo desempeñarán subgrupos discretos de matrices 2×2 que, como veremos, actúan sobre el semiplano de Poincaré y son invariantes por la métrica y la distancia de éste. El papel aritmético lo tomará la función $r(n)$ que cuenta el número de formas de expresar un entero n como suma de dos cuadrados. Todos los preliminares necesarios se expondrán con suficiente detalle en la siguiente sección, así como una serie de resultados de apoyo que utilizaremos más adelante. Los resultados y conclusiones aparecen en las tres últimas secciones. Una lectura agradable y algo antigua sobre teoría espectral en general es [Ter85]

2.2. Resultados auxiliares

Esta sección recoge la notación y resultados previos sobre teoría espectral de formas automorfas que necesitamos, así como algunos lemas técnicos a los que se apelará en posteriores secciones. La complejidad y extensión de algunos de los re-

sultados clásicos que utilizaremos obliga a que el capítulo no sea autocontenido. Así mismo, algunos cálculos son suficientemente conocidos o fáciles de completar, y no siempre se incluirán con todo detalle. Dichos resultados pueden consultarse en [Iwa02] con más profundidad.

En el últimos párrafo de la introducción habíamos presentado brevemente parte de los elementos que vamos a utilizar. La recta real será sustituida por el *semiplano de Poincaré*, que está formado por el semiplano complejo superior,

$$\mathbb{H} := \{z \in \mathbb{C} : \Im z > 0\},$$

junto con la métrica de Poincaré, $ds^2 = (dx^2 + dy^2)y^{-2}$, para $z = x + iy \in \mathbb{H}$. De esta métrica se infieren la *medida hiperbólica*,

$$\mu(A) = \int_A d\mu(z), \quad A \subset \mathbb{H}; \qquad d\mu(z) = y^{-2}dxdy, \tag{2.5}$$

y la *distancia hiperbólica* ρ, que puede definirse de la siguiente forma:

$$\rho(z,w) = \operatorname{arccosh}\left(1 + 2u(z,w)\right), \qquad \text{donde} \quad u(z,w) = \frac{|z-w|^2}{4\Im z \Im w}. \tag{2.6}$$

Nótese que, dado $t \geq 1$, arccosh t se escoge como la única solución no negativa de $\cosh x = t$. Cabe destacar que la geodésica entre dos puntos será un arco de circunferencia con centro en el eje real, salvo si los dos puntos tienen la misma parte real. En este último caso la geodésica será un segmento rectilíneo vertical. Un polígono hiperbólico se formará uniendo dos vértices consecutivos mediante la correspondiente geodésica. Por último, el conjunto de puntos a la misma distancia de uno dado será una circunferencia euclídea, cuyo centro no coincidirá con dicho punto dado.

El segundo objeto que vamos a emplear es el grupo de matrices reales 2×2 con determinante 1, habitualmente denotado por $\mathrm{SL}_2(\mathbb{R})$. En lo sucesivo lo llamaremos G para abreviar. Entre G y $\mathbb{H}$ existe una conocida correspondencia $G \times \mathbb{H} \longrightarrow \mathbb{H}$, dada por

$$\big(g, z\big) \mapsto gz := \frac{az+b}{cz+d}, \qquad \text{para} \quad g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in G \quad \text{y} \quad z \in \mathbb{H}.$$

Esta conocida aplicación está bien definida y posee un elemento unidad. Además es asociativa en G; dos matrices $g, h \in \mathbb{H}$ cualesquiera siempre cumplirán $g(hz) = (gh)(z)$ para cada $z \in \mathbb{H}$. Por tanto, el grupo G define una *acción* sobre $\mathbb{H}$. De entre los tipos de acciones que existen, nos gustaría que la nuestra fuese *fiel*; es decir, que dos matrices distintas de g no definan la misma biyección sobre $\mathbb{H}$. Esto no ocurre a priori, pero es fácil lograrlo redefiniendo G identificando matrices opuestas; esto es, tomando $G = \mathrm{PSL}_2(\mathbb{R}) = \mathrm{SL}_2(\mathbb{R})/\{\pm I\}$. En adelante supondremos que G

está definido de esta última forma, siempre que no se indique otra cosa. También emplearemos de forma habitual la notación a, b, c, d para indicar los coeficientes ordenados de una matriz de G sin haberla definido así de forma explícita.

La métrica de Poincaré es *invariante* respecto de G. Es decir,

$$ds^2 = \frac{|dz|^2}{(\Im z)^2} = \frac{|dgz|^2}{(\Im gz)^2}. \tag{2.7}$$

Para verlo, tomemos una matriz $g \in G$ arbitraria. Denotaremos por $j_g(z)$ a $cz + d$. Se cumple

$$\frac{dgz}{dz} = \frac{a(cz+d) - (az+b)c}{(cz+d)^2} = \frac{1}{(cz+d)^2} = (j_g(z))^{-2},$$

y por tanto $dgz = dz\,(j_g(z))^{-2}$. Tomando conjugados y multiplicando ambas ecuaciones se obtiene $|dgz|^2 = |dz|^2 |j_g(z)|^{-4}$, de donde (2.7) es inmediato gracias a que $\Im gz = \Im z |j_g(z)|^{-2}$. Como la métrica es invariante por G, la distancia y medida hiperbólicas dadas por (2.6) y (2.5), también lo serán. Cada g se convierte, por tanto, en una isometría al actuar sobre $\mathbb{H}$.

El papel que desempeñaban las traslaciones enteras en aquel ejemplo que veíamos en la introducción lo interpretarán ahora subgrupos discretos F de G, que son conocidos como *grupos fuchsianos*. Para evitar complicaciones topológicas añadiremos una restricción técnica, pidiendo que las órbitas de tales subgrupos tengan la recta real extendida, $\widehat{\mathbb{R}} := (-\infty, \infty) \cup \{i\infty\}$, como límite. Estos últimos se denominan *grupos fuchsianos de primera especie*. Todos los que mencionamos en este capítulo lo son, y a veces por abuso de notación no lo especificaremos. El ejemplo más conocido es $\Gamma := \mathrm{PSL}_2(\mathbb{Z})$, formado por las matrices de G cuyas entradas son enteras. A partir de este grupo surgirán muchos otros (véase el principio de la siguiente sección, correspondiente al caso no compacto). Entre ellos $\widetilde{\Gamma}$, formado por las matrices de Γ tales que la suma de sus elementos en cada diagonal es par. Más adelante estudiaremos otros de naturaleza muy distinta, la mayoría de ellos procedentes de álgebras de cuaterniones (véase el principio de la cuarta sección, correspondiente al caso compacto).

Cada grupo fuchsiano F lleva asociado un *dominio fundamental*, que es a $\mathbb{H}$ lo mismo que el intervalo $[0, 1]$ a la recta real cuando el grupo son las traslaciones enteras. Concretamente, un dominio fundamental de F es cualquier subconjunto $D \subset \mathbb{H}$ tal que:

- Dos puntos distintos del interior de D no pertenezcan a la misma órbita; equivalentemente, que no exista $g \in F$ que lleve uno de los dos puntos en el otro.

- Toda órbita contenga un punto en el cierre de D. Es decir, para cada punto de $\mathbb{H}$ ha de existir $g \in F$ que lleve dicho punto a uno localizado en el cierre de D.

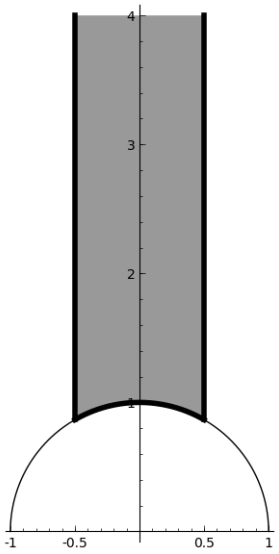

Figura 2.1: Dominio fundamental D para Γ.

Por supuesto, el dominio fundamental de un grupo no es único. Basta trasladarlo por cualquier matriz de dicho grupo para obtener otro análogo válido. En el caso de Γ, es costumbre escoger como dominio el triángulo hiperbólico D de vértices $i\infty$ y $(\pm 1 + i\sqrt{3})/2$, es decir, $D = \{z \in \mathbb{H} : |\Re z| \leq 1/2, |z| \geq 1\}$ (véase la Figura 2.1). Otra posibilidad es tomar $D' = \{z \in \mathbb{H} : |z| < 1, |z-1|, |z+1| > 1\}$ (véase la Figura 2.2).

Se dirá que un grupo fuchsiano F es *co-compacto* si ninguno de los vértices de su dominio fundamental está en la recta real extendida. Γ no es por tanto co-compacto, al ser el punto del infinito $(i\infty)$ uno de los vértices de D. Esta definición es coherente ya que cualquier matriz $g \in G$ es una biyección de dicha recta en sí misma, y por tanto cualquier dominio que escojamos tendrá el mismo número de estos vértices

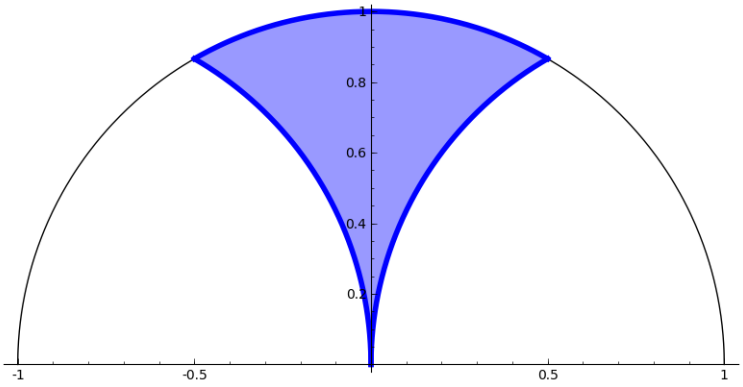

Figura 2.2: Dominio fundamental D' para Γ.

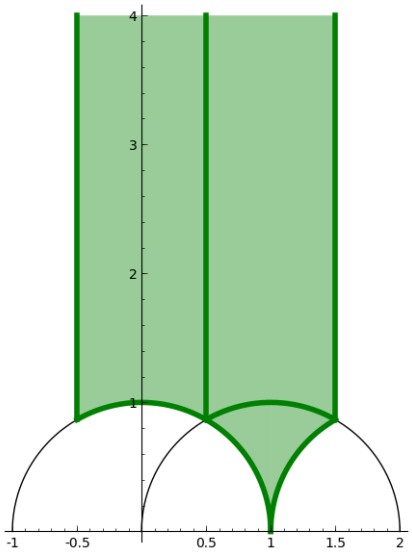

Figura 2.3: Un ejemplo de dominio fundamental para $\widetilde{\Gamma}$, con dos cúspides.

conflictivos, a los que se denomina *cúspides*. Es importante recalcar que el conjunto de cúspides no estará fijado para un grupo fuchsiano , al poder variar si se cambia el dominio fundamental. Por este motivo se suelen tomar clases de equivalencia; identificaremos dos cúspides si ambas están en la misma órbita; es decir, si puede llevarse una en otra mediante algún elemento del grupo fuchsiano en cuestión. Con esta relación, el conjunto de las cúspides sí será invariante. A menudo, por abuso de notación, llamaremos cúspide a toda la clase de equivalencia de un representante concreto. En el caso de Γ, existirá una única cúspide que agrupe todos los racionales junto con el punto del infinito. Para $\widetilde{\Gamma}$ habrá dos diferentes, distinguiendo racionales cuyo denominador (en forma irreducible) sea par o impar (véase la Figura 2.3, en la que el dominio fundamental escogido tiene efectivamente dos cúspides.)

Nuestro objetivo es replicar el ejemplo que estudiamos sobre una función real en el semiplano de Poincaré. Es decir, queremos poder expresar cualquier función $k : [0, \infty) \longrightarrow$ sobre una base ortonormal de autofunciones de algún operador. El reemplazo natural del laplaciano habitual es el *operador de Laplace-Beltrami*,

$$\Delta = y^2 \left(\frac{\partial^2}{\partial x^2} + \frac{\partial^2}{\partial y^2} \right),$$

que también es invariante por la métrica ds. La existencia de un sistema ortonormal completo de autofunciones para el laplaciano puede extenderse a ciertos operadores elípticos de segundo orden sobre variedades de Riemann compactas; en el caso que nos ocupa, si F es co-compacto, tales autofunciones (convenientemente normalizadas) se denominan *formas de Maass*, $\{u_j\}_{j=0}^{\infty}$, denominadas así en honor al matemático

alemán Hans Maass, que las introdujo por primera vez en 1949 [Maa49]. Las formas de Maass dependen del grupo fuchsiano F que hayamos fijado. Es interesante destacar que u_0 es constante y su valor es $|\mu(D)|^{-1/2}$, siendo $\mu(D)$ el área de cualquier dominio fundamental de F. Remitimos al lector a [HR92], que contiene algunos dibujos e información adicional.

Para poder expresar funciones complejas sobre la base de las formas de Maass, es necesario que éstas verifiquen ciertas condiciones de contorno, que pueden traducirse en que la función valga lo mismo en puntos que pertenezcan a una misma órbita. Tal y como hicimos con las funciones f reales para que fueran 1-periódicas, ahora queremos reformular $k : [0, \infty) \longrightarrow \mathbb{C}$ para que tenga las simetrías expresadas por F. Para ello, simplemente consideraremos la suma de las acciones de dichas simetrías sobre k. De forma análoga a (2.3) definimos en nuestro contexto, siempre suponiendo la convergencia, el *núcleo automorfo*:

$$K(z, w) := \sum_{g \in F} k\left(u(gz, w)\right), \tag{2.8}$$

que es por construcción invariante por F en sus dos variables; es decir, se cumple $K(gz, w) = K(z, w) = K(z, g'w)$ para cualesquiera $g, g' \in F$. Si el grupo F que hemos escogido es co-compacto y la función k suficientemente regular, entonces tenemos el ansiado desarrollo espectral:

$$\sum_{g \in F} k\left(u(gz, w)\right) = \sum_{j=0}^{\infty} h(t_j) u_j(z) \overline{u_j(w)}, \tag{2.9}$$

donde $-(1/4 + t_j^2)$ es el autovalor correspondiente a u_j (se cumple $t_0 = \pm i/2$), y $h(t)$ es la *transformada de Selberg* de k, que se define como sigue:

$$h(t) = \int_0^{\infty} \int_{-\infty}^{\infty} k\left(\frac{x^2 + (y-1)^2}{4y}\right) y^{-3/2+it} dx dy. \tag{2.10}$$

En cierto sentido, h es el análogo natural de la transformada de Fourier para el caso euclídeo. Esta expresión nos va a permitir obtener identidades aproximadas para grupos co-compactos (en la cuarta sección), pero quedarnos aquí supondría una importante restricción, ya que gran parte de los grupos que se conocen y sobre los que se tienen información valiosa no son co-compactos . Por fortuna, esta salvedad aún puede evitarse. En el caso no compacto se sabe que además de una cantidad numerable de formas de Maass de cuadrado integrable y con decaimiento exponencial en las cúspides, hay otras que no son de cuadrado integrable y que participan en desarrollos espectrales generalizados, reemplazando sumas por integrales. Estas autofunciones son las *series de Eisenstein*, definidas como la continuación analítica de

$$E_{\mathfrak{a}}(z, s) = \sum_{g \in F_{\mathfrak{a}} \backslash F} \left(\Im(\sigma_{\mathfrak{a}}^{-1} gz)\right)^s, \tag{2.11}$$

para una cúspide $\mathfrak{a}$ de F y un $s \in \mathbb{H}$ fijo que asegure la convergencia. Aquí, $\sigma_\mathfrak{a}$ es una *matriz de escala* para $\mathfrak{a}$; es decir, una matriz de G tal que $\sigma_\mathfrak{a}\infty = \mathfrak{a}$ y $\sigma_\mathfrak{a}^{-1} F_\mathfrak{a} \sigma_\mathfrak{a}$ está generado por la traslación unidad, donde $F_\mathfrak{a}$ comprende a los elementos (parabólicos) de F que dejan $\mathfrak{a}$ fija[1]. En general, y para el caso no compacto en particular, gran cantidad de funciones k de cuadrado integrable admiten un desarrollo en autofunciones (incluyendo el espectro discreto y el continuo) y, generalizando (2.9), es posible dar un análogo válido para todos los grupos fuchsianos; la llamada *fórmula de pretraza*:

$$\begin{aligned}(2.12)\quad \sum_{g\in F} k\left(u(gz,w)\right) &= \sum_{j=0}^{\infty} h(t_j) u_j(z)\overline{u_j(w)} \\ &\quad + \frac{1}{4\pi}\sum_{\mathfrak{a}} \int_{-\infty}^{\infty} h(t) E_\mathfrak{a}(z, 1/2+it)\overline{E_\mathfrak{a}(w,1/2+it)}\, dt.\end{aligned}$$

Aquí, el sumatorio recorre las clases de equivalencia de la cúspides y es vacío si F es co-compacto. Es interensate recalcar que la fórmula (2.12), introducida [Sel56] por el matemático noruego Atle Selberg, es el paso previo a la famosa *fórmula de traza* del mismo autor, que relaciona con maestría el tamaño de los autovalores con la longitud de las geodésicas.

Una vez llegados a esta crucial fórmula, una parte importante de nuestro trabajo consiste en hallar ejemplos explícitos de funciones k para las que exista transformada de Selberg con una descripción explícita (lo cual no siempre es fácil) y rápido decaimiento, para que la contribución de los autovalores no triviales sea lo menor posible. A continuación incluimos una serie de resultados auxiliares que utilizaremos más adelante. El primero de ellos tiene la gran utilidad de permitirnos calcular el valor de una transformada de Selberg en t_0 sin necesidad de describir h con exactitud.

Lema 2.1. *Dada una función $k : [0,\infty) \longrightarrow \mathbb{C}$ con transformada de Selberg h,*

$$h(i/2) = 4\pi \int_0^\infty k(x)\, dx.$$

Demostración: Tomando $t = i/2$ en (2.10) queda una función sencilla en términos de $u(i,z)$, para $z = x + iy$.

$$h(i/2) = \int_0^\infty \int_{-\infty}^\infty k\left(\frac{x^2+(y-1)^2}{4y}\right)\frac{dxdy}{y^2} = \int_{\mathbb{H}} k(u(i,z))\, d\mu(z).$$

La función $u(i,z)$ es i-radial, lo cual sugiere utilizar coordenadas polares hiperbólicas. Dado $r \in (0,+\infty)$, el punto $e^r i$ verifica $\rho(i, e^r i) = r$ por (2.6), luego está

[1]Son parabólicos aquellos que fijan un único punto en la recta real extendida. La notación $F_\mathfrak{a}\backslash F$ simplemente indica las órbitas de los elementos de $F_\mathfrak{a}$ actuando sobre F.

situado en la circunferencia hiperbólica de centro i y radio r. La transformación

$$g_\theta(e^r i) = \frac{\cos\theta \cdot e^r i + \operatorname{sen}\theta}{-\operatorname{sen}\theta \cdot e^r i + \cos\theta}, \quad \theta \in [0, \pi),$$

da un punto de la misma circunferencia, girado un ángulo de 2θ en sentido antihorario. El cambio de coordenadas se puede escribir como

$$\left\{ \begin{array}{rcl} y & = & 1/(\cosh r + \operatorname{senh} r \cos(2\theta)) \\ x & = & y \cdot \operatorname{senh} r \operatorname{sen}(2\theta). \end{array} \right. ,$$

de donde $d\mu z = 2 \operatorname{senh} r dr d\theta$. Por último, mediante el cambio $\cosh r = 1 + 2u$, se obtiene $d\mu z = 4 du d\theta$, y entonces

$$\int_{\mathbb{H}} k(u(i,z)) d\mu(z) = \int_0^\infty \int_0^\pi k(u) 4 du d\theta = 4\pi \int_0^\infty k(u) du.$$

Esto completa la prueba. Los detalles específicos sobre el cambio de coordenadas pueden consultarse en [Iwa02, §1.3] □

El siguiente es un resultado clásico, que de hecho aparece de forma explícita en la prueba de (2.9). Suele denominarse *Fundamental Lemma* (véase por ejemplo [Hej76]), aunque hay resultados más famosos que comparten la misma denominación.

Lema 2.2. *$k : [0, \infty) \longrightarrow \mathbb{C}$ con transformada de Selberg h. Sea $\phi(z)$ una autofunción del operador de Laplace-Beltrami con autovalor $s(1-s)$ donde $s = 1/2 + it$ y $t \in \mathbb{C}$. Se cumple entonces*

$$\int_{\mathbb{H}} k\big(u(z,w)\big) \phi(z) \, d\mu(z) = h(t)\phi(w).$$

Este lema va a permitirnos dar el siguiente resultado en el que interviene la *convolución hiperbólica* de dos funciones k_1 y k_2, definida como sigue:

$$(k_1 * k_2)\,(u(z,w)) = \int_{\mathbb{H}} k_1\,(u(z,v))\, k_2\,(u(v,w)) \; d\mu(v).$$

Lema 2.3. *Sean k_1 y k_2 dos funciones suficientemente regulares con transformadas de Selberg h_1 y h_2. Entonces el producto $h_1 h_2$ es a su vez la transformada de Selberg de $k_1 * k_2$.*

Demostración: Utilizando que $\phi(z) = \Im z$ es una autofunción del operador de Laplace-Beltrami (con autovalor $s(1-s) = 1/4 + t^2$ si escogemos $s = 1/2 + it$)

sobre el lema anterior,

$$\begin{aligned}\int_{\mathbb{H}} (k_1 * k_2)(u(z,i))(\Im z)^{1/2+it} d\mu(z) & \\ &= \int_{\mathbb{H}} \left[\int_{\mathbb{H}} k_1(u(z,v)) k_2(u(v,i)) d\mu(v) \right] (\Im z)^{1/2+it} d\mu(z) \\ &= \int_{\mathbb{H}} k_2(u(v,i)) \left[\int_{\mathbb{H}} k_1(u(z,v))(\Im z)^{1/2+it} d\mu(z) \right] d\mu(v) \\ &= \int_{\mathbb{H}} k_2(u(v,i)) \left[h_1(t) \cdot (\Im v)^{1/2+it} \right] d\mu(v) \\ &= h_1(t) h_2(t).\end{aligned}$$

□

Lema 2.4. *Sea $\mu \in \mathbb{C}$ una constante compleja tal que $\Re\mu > 1$. Consideremos la función $k(u) = (u+1)^{-\mu}$. Entonces, su transformada de Selberg es*

$$h(t) = \frac{4\pi}{\Gamma^2(\mu)} \Gamma\left(\mu - 1/2 + it\right) \Gamma\left(\mu - 1/2 - it\right). \tag{2.13}$$

Demostración: En esta demostración juega un importante papel la función Beta, $B(a,b) := \Gamma(a)\Gamma(b)/\Gamma(a+b)$, que entre otras muchas otras admite [GR07] la siguiente definición:

$$B(a,b) = \int_0^\infty \frac{t^{b-1}}{(1+t)^{a+b}}\, dt, \quad \Re a, \Re b > 0 \tag{2.14}$$

La función Beta guarda una estrecha relación con Gamma. Concretamente, se cumple $\Gamma(a)\Gamma(b)\Gamma^{-1}(a+b) = B(a,b)$. Ahora basta escribir la expresión de la transformada de Selberg de k y, mediante el cambio de variables $x \mapsto (y+1)\sqrt{x}$, se concluye el resultado que buscábamos.

$$\begin{aligned} h(t) &= 2\int_0^\infty \int_0^\infty \Big(\frac{x^2 + (y-1)^2}{4y} + 1 \Big)^{-\mu} y^{-3/2+it}\, dxdy \\ &= 4^\mu \int_0^\infty \frac{y^{\mu-3/2+it}}{(1+y)^{2\mu-1}}\, dy \int_0^\infty \frac{x^{-1/2}}{(1+x)^\mu}\, dx \\ &= 4^\mu B(1/2, \mu - 1/2) B(\mu - 1/2 + it, \mu - 1/2 - it). \end{aligned}$$

□

Corolario 2.5. *Si 2μ es un entero mayor que 2, entonces la función $k(u)$ dada por el Lema 2.4 tiene la siguiente transformada de Selberg:*

$$h(t) = \begin{cases} \dfrac{4\pi^2}{(\mu-1)!^2\cosh(\pi t)} \displaystyle\prod_{n=1}^{\mu-1} \Big(\big(n-1/2\big)^2 + t^2 \Big) & \text{para} \quad \mu \in \mathbb{Z} \\ \dfrac{\big(\mu-3/2\big)!^2\, 4^{2\mu-1}\, \pi t}{(2\mu-2)!^2 \sinh(\pi t)} \displaystyle\prod_{n=1}^{\mu-3/2} (n^2+t^2) & \text{para} \quad \mu+\tfrac{1}{2} \in \mathbb{Z} \end{cases}$$

Demostración: Basta utilizar sobre (2.13) las siguientes fórmulas clásicas (consultar [WW62, §12]) relativas a la función Gamma:

$$|\Gamma\left(1/2+it\right)|^2 = \frac{\pi}{\cosh(\pi t)}, \quad \big|\Gamma\big(1+it\big)\big|^2 = \frac{\pi t}{\operatorname{senh}(\pi t)}, \quad \Gamma\left(n+1/2\right) = \frac{(2n-1)!\sqrt{\pi}}{2^{n-1}(n-1)!}.$$

□

Los siguientes ejemplos de funciones con transformadas explícitas de Selberg que vamos a introducir hacen uso de cierta clase de funciones de Bessel, en concreto dentro de las funciones de Bessel modificadas. Son éstas soluciones de la siguiente familia de ecuaciones diferenciales,

$$x^2\frac{d^2y}{dx^2} + x\frac{dy}{dx} - (x^2+\alpha^2)y = 0,$$

donde α es un parámetro complejo. Las soluciones a la ecuación anterior que presentan una singularidad en el cero se denominan *funciones de Bessel modificadas de segunda especie*, y son las que van a aparecer en nuestro estudio. Dichas funciones pueden escribirse como

$$K_\nu(x) = \int_0^\infty e^{-x\cosh t}\cosh(\nu t)\,dt, \quad x \in \mathbb{R}^+, \nu \in \mathbb{C}.$$

Cuando ν es imaginario puro, el módulo de $K_\nu(z)$ puede acotarse por una exponencial negativa en cada uno de los dos argumentos.

Para el siguiente lema, vamos a emplear una definición alternativa de K_ν. Mediante el cambio $t \to \log t$ y una reordenación adecuada se verifica ([GR07, §8]) que

$$K_\nu(x) = \frac{1}{2}\int_0^\infty e^{-x(t+1/t)/2} t^{-\nu-1}\,dt. \tag{2.15}$$

Lema 2.6. *Dado un número real positivo μ, la transformada de Selberg de la función $k(u) = e^{-\mu u}$ es $4e^{\mu/2}\sqrt{\pi/\mu}\,K_{it}(\mu/2)$.*

Demostración: Basta emplear la definición de la transformada de Selberg sobre $k(u)$:

$$\begin{aligned} h(t) &= \int_0^\infty e^{-\mu\frac{(y-1)^2}{4y}}\Big(\int_{-\infty}^\infty e^{-\mu\frac{x^2}{4y}}\,dx\Big)y^{-\frac{3}{2}+it}\,dy \\ &= (4\pi e^\mu)^{1/2}\mu^{-1/2}\int_0^\infty e^{-\frac{\mu}{4}(y+\frac{1}{y})}y^{-1+it}\,dy. \end{aligned}$$

Comparando lo que hemos obtenido con (2.15), se completa la prueba. □

Para el siguiente lema utilizaremos el siguiente hecho: dados $z, w \in \mathbb{H}$ arbitrarios, siempre existirá una matriz $g \in G$ tal que $gz = i$ y $\Im(gw) = 1$. No mostraremos la demostración de forma rigurosa, puesto que es fácil comprobar las cuentas. Baste decir que para $z \in \mathbb{H}$ el sistema $az + b = i(cz + d)$ tiene un conjunto de soluciones S de dimensión 1 sobre los reales, y siempre puede escogerse un $(a', b', c', d') \in S$ tal que la parte imaginaria de $(a'w + b')/(c'z + d')$ (que es $(c'^2 + d'^2)^{-1}$) sea 1, gracias a que $c'd' \neq 0$.

Lema 2.7. *Dados $\alpha, \beta > 0$, la transformada de Selberg de la función*

$$k(u) = \frac{\sqrt{\alpha\beta}}{4\sqrt{(\alpha+\beta)^2 + 4\alpha\beta u}}\, e^{-\sqrt{(\alpha+\beta)^2+4\alpha\beta u}}$$

es $K_{it}(\alpha)K_{it}(\beta)$.

Demostración: Dado $\mu > 0$, definamos $k_\mu(u) = \sqrt{\mu/(8\pi)}\, e^{-\mu(1+2u)}$. Por el Lema 2.6, la transformada de Selberg de $k_\mu(u)$ es $K_{it}(\mu)$. Luego, por el Lema 2.3, basta con probar $(k_\alpha * k_\beta)(u) = k(u)$. Por (2.10), podemos escribir $u = u(z, w)$. Esta última expresión es invariante por elementos de G; es decir, $u(gz, gw) = u(z, w)$. En virtud del párrafo anterior a este Lema, podemos suponer sin pérdida de generalidad que $z = i$, $w = \lambda i$, y entonces $u(z, w) = (\lambda - 1)^2/4\lambda$, de donde

$$\begin{aligned} & (k_\alpha * k_\beta)(u(z,w)) \\ = \;& \frac{\sqrt{\alpha\beta}}{8\pi e^{\,\alpha+\beta}}\int_0^\infty \Big(\int_{-\infty}^\infty e^{-(\alpha/\lambda+\beta)x^2/2y}\,dx\Big)e^{-\left((\alpha(y-\lambda)^2)/\lambda+\beta(y-1)^2\right)/2y}y^{-2}\,dy \\ = \;& \frac{\sqrt{2\pi\alpha\beta}}{8\pi\sqrt{\alpha/\lambda+\beta}}\int_0^\infty e^{-(\alpha/\lambda+\beta)y/2-(\beta+\alpha\lambda)/2y}y^{-3/2}\,dy \\ = \;& \frac{\sqrt{\alpha\beta}}{4\sqrt{(\alpha/\lambda+\beta)(\beta+\alpha\lambda)}}\, e^{\sqrt{(\alpha/\lambda+\beta)(\beta+\alpha\lambda)}}. \end{aligned}$$

Por (2.15), la última integral coincide con $K_{1/2}(z)$, que también puede escribirse como $e^{-z}\sqrt{\pi/2z}$ (consúltese [GR07, §8]). □

Lema 2.8. *Consideremos la función* $k(u) = u^{-2}\big((1+2/u)\log(1+u) - 2\big)$, *con* $k(0) = 1/6$ *para que sea continua. Su transformada de Selberg es*

$$h(t) = 2\pi^3 \left(\frac{1/4 + t^2}{\cosh(\pi t)}\right)^2.$$

Nótese que k es la derivada de $u^{-2}\big(u - (1+u)\log(1+u)\big)$.

Demostración: Utilizando los Lemas 2.3 y 2.4 sabemos que la transformada de Selberg de $(u+1)^{-2} * (u+1)^{-2}$ será $8\pi h(t)$. Luego es suficiente probar que

$$8\pi k\big(u(z,w)\big) = \int_{\mathbb{H}} \big(u(z,v)+1\big)^{-2}\big(u(v,w)+1\big)^{-2}\, d\mu(v). \tag{2.16}$$

Podemos, al igual que en la demostración precedente, suponer $z = i$ y $w = (2c+1)i$, donde $c > -1/2$. Para estos valores, $u(z,w) = c^2/(2c+1)$ y

$$k\big(u(z,w)\big) = \frac{(2c+1)^2}{c^4}\Big(\frac{c^2+4c+2}{c^2}\,\log\frac{(c+1)^2}{2c+1} - 2\Big).$$

Por otro lado, la integral de (2.16) es

$$I = 256(2c+1)^2 \int_0^\infty y^2 J(y+1, y+2c+1)\, dy,$$

donde

$$J(A,B) = \int_{-\infty}^{\infty} \frac{dx}{(x^2+A^2)^2(x^2+B^2)^2} = \frac{\pi}{2}\,\frac{A^2+3AB+B^2}{A^3B^3(A+B)^3}.$$

Empleando el cambio de variables $y \mapsto y - c - 1$ obtenemos

$$I = 16\pi(2c+1)^2 \int_{c+1}^\infty \frac{(5y^2-c^2)(y-c-1)^2}{y^3(y^2-c^2)^3}\, dy.$$

Al evaluar esta integral racional, se obtiene la misma expresión que la que describe $8\pi k\big(u(z,w)\big)$, y esto prueba (2.16). □

2.3. El caso no compacto

Como ya hemos mencionado anteriormente los grupos fuchsianos más conocidos y, por diversos motivos, sobre los que tenemos mayor control suelen ser no cocompactos. Destaca por encima del resto el grupo $\Gamma := \mathrm{PSL}_2(\mathbb{Z})$ que introducíamos en la sección anterior. Añadiendo una condición de divisibilidad a una de las casillas

de las matrices, se deriva toda una familia de grupos fuchsianos de primera especie contenidos en Γ. Fijado un entero positivo N, se define[2]

$$\Gamma_0(N) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{PSL}_2(\mathbb{Z}) : N|c \right\}.$$

Nótese que, en particular, $\Gamma = \Gamma_0(1)$ y $\Gamma_0(N') \supset \Gamma_0(N)$ para $N'|N$. El grupo $\widetilde{\Gamma}$ que habíamos introducido junto con Γ (compuesto por las matrices de Γ tales que los elementos de cada diagonal tienen la misma paridad) es en realidad un conjugado de $\Gamma_0(2)$; si consideramos la matriz $A = \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}$, se cumple $\widetilde{\Gamma} = A^{-1}\Gamma_0(2)A$.

Una de las ventajas que proporcionan Γ y $\widetilde{\Gamma}$ es la interpretación aritmética directa de (2.8) para estos grupos a través de la función $r(n)$, que cuenta el número de representaciones de n como suma de dos cuadrados:

$$r(n) := \left|\left\{(a,b) \in \mathbb{Z}^2 : a^2 + b^2 = n\right\}\right|.$$

Esta conocida función aritmética toma valores múltiplos de 4 para todos los enteros no negativos salvo el cero, debido a la simetría al tomar cuadrados de números positivos y negativos. De hecho, la función $r(n)$ no es multiplicativa como tal, pero $r(n)/4$ sí lo es. Esta última puede expresarse como convolución de la función constantemente 1 con el único carácter no trivial módulo 4, que vale $(-1)^{(n-1)/2}$ para n impar y 0 en los pares. Denotaremos por χ_4 a éste carácter. Utilizando esto, podemos dar una expresión explícita para $r(n)$:

$$r(n) = 4\left(d_1(n) - d_3(n)\right), \qquad \text{para} \quad d_m(n) = \left|\{d \mid n : d \equiv m\,(4)\}\right|.$$

Esta igualdad caracteriza en particular los enteros en los que $r(n)$ es positiva; son aquellos en los que todo divisor congruente con 3 módulo 4 aparece con multiplicidad par. Por tanto, $r(4k+3)$ siempre valdrá cero. También es fácil comprobar que $r(2^k n) = r(n)$ para cualesquiera n y k. Todas estas propiedades de $r(n)$ serán utilizadas más adelante.

Para poder lograr esta interpretación aritmética del núcleo automorfo en función de $r(n)$ es clave escoger adecuadamente dos puntos $z, w \in \mathbb{H}$ para los que $\big(u(\gamma z, w)\big)$ tenga una descripción sencilla en función de los coeficientes de una matriz genérica γ de Γ o $\widetilde{\Gamma}$. Tomemos $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma$. Se cumple que, para $z = w = i$,

$$4\big(u(\gamma i, i)\big) = \left|\frac{ai-b}{ci-d} - i\right|^2 (c^2+d^2) = |(a-d)i+(b+c)|^2 = (a-d)^2+(b+c)^2. \tag{2.17}$$

Manipulando adecuadamente esta fórmula vamos a lograr describir (2.8) en función de $r(n)$, independientemente de quién sea la función k. El resultado es el siguiente.

[2]Esta definición difiere de la habitual, en la que no consideran matrices de $\mathrm{SL}_2(\mathbb{Z})$ sin identificar I con $-I$. Nuestra variante no modifica la acción sobre $\mathbb{H}$.

Lema 2.9. *Sea $k : [0, \infty) \longrightarrow \mathbb{C}$ una función arbitraria. Se cumplen las siguientes identidades:*

$$\sum_{\gamma \in \widetilde{\Gamma}} k\big(u(\gamma i, i)\big) = \sum_{n=0}^{\infty} \frac{1}{2} r(n) r(n+1) k(n) \tag{2.18}$$

$$\sum_{\gamma \in \Gamma} k\big(u(\gamma i, i)\big) = \sum_{n=0}^{\infty} \xi_n r(n) r(n+4) k(n/4), \tag{2.19}$$

donde ξ_n toma el valor $1/2$ para n par y $1/4$ para n impar.

Demostración: Comenzamos suponiendo que γ pertenece a $\widetilde{\Gamma}$, en el que el resultado se logra de forma más sencilla. Utilizando la notación habitual para γ, los coeficientes a y d tendrán la misma paridad, así como b y c. Observando (2.17) esto implica que, para $\gamma \in \widetilde{\Gamma}$, $4u(\gamma i, i)$ siempre será un múltiplo de 4 no negativo. Utilizando $ad - bc = 1$ en (2.17) se obtiene el siguiente sistema:

$$4u(\gamma i, i) = (a-d)^2 + (b+c)^2 = (a+d)^2 + (b-c)^2 - 4. \tag{2.20}$$

Escribamos ahora $u(\gamma i, i) = n$, para n fijo. ¿Cuántas matrices $\gamma \in \widetilde{\Gamma}$ existen para las que $u(\gamma i, i)$ tome exactamente el valor n? Es fácil comprobar que la correspondencia

$$\begin{array}{rcl} \left\{(a,b,c,d) \in \mathbb{Z}^4 : \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \widetilde{\Gamma}\right\} & \to & \big\{(r,s,t,u) \in (2\mathbb{Z})^4 : r^2 + s^2 = t^2 + u^2 - 4\big\} \\ (a,b,c,d) & \mapsto & (a-d, b+c, a+d, b-c) \end{array} \tag{2.21}$$

admite inversa y es claramente una biyección (la notación $(2\mathbb{Z})$ denota a los enteros pares); por tanto, cada valor $4n$ aparecerá exactamente $r(4n)r(4n+4)$ veces. Recordando que $r(n)$ no varía al multiplicar por potencias de 2, se obtiene (2.18). La división por 2 proviene de la identificación de I con $-I$.

La demostración para Γ es ligeramente más complicada debido a que, aunque (2.20) sigue siendo válida, la expresión a la derecha no siempre será un múltiplo de 4, ya que $u(\gamma i, i)$ tomará valores racionales para $\gamma \in \Gamma \setminus \widetilde{\Gamma}$. De hecho, la parte fraccionaria de $u(\gamma i, i)$ será siempre $1/4$ para estas matrices, como veremos a continuación. En primer lugar descomponemos la suma sobre Γ en dos partes, distinguiendo las matrices que pertenecen a $\widetilde{\Gamma}$ de las que no. El primero de estos conjuntos dará los términos pares del sumatorio en la parte derecha de (2.19) gracias a que, mediante

el cambio $n \mapsto m/4$,

$$\begin{aligned}\sum_{n=0}^{\infty}\frac{1}{2}r(n)r(n+1)k(n) &= \sum_{n=0}^{\infty}\frac{1}{2}r(4n)r(4n+4)k(n)\\ &= \sum_{\substack{m=0\\4|m}}^{\infty}\frac{1}{2}r(m)r(m+4)k\left(\frac{m}{4}\right)\\ &= \sum_{\substack{m=0\\2|m}}^{\infty}\frac{1}{2}r(m)r(m+4)k\left(\frac{m}{4}\right). \qquad (2.22)\end{aligned}$$

La última igualdad es consecuencia inmediata de que todo n de la forma $4k+2$ verifica $r(n)r(n+4)=0$, y por tanto todos los términos que se añaden en la última igualdad son nulos. Luego sólo nos queda analizar matrices de $\Gamma \setminus \widetilde{\Gamma}$, que siempre tienen tres entradas impares y una par, por lo que podemos escribir $4u(\gamma i, i) = 4n+1$, con $n \geq 0$. Para ver cuántas matrices $\gamma \in \Gamma \setminus \widetilde{\Gamma}$ cumplen $u(\gamma i, i) = n + 1/4$, establecemos la siguiente correspondencia, parecida a (2.21):

$$\begin{aligned}\left\{(a,b,c,d)\in\mathbb{Z}^4 : \begin{pmatrix}a & b\\ c & d\end{pmatrix}\in\Gamma\setminus\widetilde{\Gamma}\right\} &\to \left\{(r,s,t,u)\in\widetilde{\mathbb{Z}^4} : r^2+s^2=t^2+u^2-4\right\}\\ (a,b,c,d) &\mapsto (a-d, b+c, a+d, b-c),\end{aligned}$$

donde $\widetilde{\mathbb{Z}^4} := \{(r,s,t,u) \equiv (1,0,1,0), (0,1,0,1) \text{ (mód 2)}\} \subset \mathbb{Z}^4$. De nuevo es fácil comprobar que se trata de una biyección. El número de matrices para los que se alcanza el valor $4n+1$ será exactamente $r(4n+1)r(4n+5)/2$. La razón por la que se divide por 2 es que al restringir el segundo conjunto a $\widetilde{\mathbb{Z}^4}$ la paridad de r y s fuerza la de t y u. Es decir, el par (r,s) tendrá un elemento par y como $t = a+d$, tendrá la misma paridad que r, así como u tendrá la misma que s; por este motivo sólo se alcanzan la mitad de soluciones posibles que si tomáramos todo $\mathbb{Z}^4$. Utilizando el mismo cambio de antes, se concluye

$$\sum_{n=0}^{\infty}\frac{1}{4}k(n+1/4)r(4n+1)r(4n+5) = \sum_{\substack{n=0\\2\nmid n}}^{\infty}\frac{1}{4}k\left(\frac{n}{4}\right)r(n)r(n+4), \qquad (2.23)$$

gracias a que $r(n)$ se anula si n es congruente con 3 módulo 4. Sumando (2.22) y (2.23) y teniendo en cuenta de nuevo la identificación $\pm I$, se obtiene (2.19). □

Por supuesto, para otros de los grupos fuchsianos de primera especie que hemos mencionado es posible obtener fórmulas en cierto modo similares a las que tenemos para Γ y $\widetilde{\Gamma}$, pero que no parecen poder expresarse claramente en función de $r(n)$.

Lema 2.10. *Sea E la serie de Eisenstein asociada a la única cúspide de Γ, tal y como se definió en (2.11); y sean $E_{\mathfrak{a}}$, $E_{\mathfrak{b}}$ las series correspondientes a $\mathfrak{a}=\infty$ y $\mathfrak{b}=1$ de $\widetilde{\Gamma}$, respectivamente. Se verifican las siguientes igualdades:*

$$E(i,s)=(2^s+1)E_{\mathfrak{a}}(i,s)=(2^s+1)E_{\mathfrak{b}}(i,s)=\frac{2\zeta(s)L(s,\chi_4)}{\zeta(2s)}. \tag{2.24}$$

Demostración: Escribiendo la serie de Eisenstein para $z=i$,

$$E(i,s)=\sum_{\gamma\in\Gamma_\infty\backslash\Gamma}\frac{(\Im i)^s}{|j_{\sigma_\infty^{-1}\gamma}(i)|^{2s}}=\frac{1}{2}\sum_{\substack{c,d=-\infty\\ \mathrm{mcd}(c,d)=1}}^{\infty}\frac{1}{(c^2+d^2)^s}=\frac{1}{2\zeta(2s)}\sum_{n=1}^{\infty}\frac{r(n)}{n^s}.$$

El que $E(i,s)$ pueda escribirse como la última expresión de (2.24) es conocido y consecuencia de que, como ya vimos, la función $r(n)/4$ se obtenía como convolución de $1(n)$ y $\chi_4(n)$. Pasemos ahora a las dos cúspides de $\widetilde{\Gamma}$, que tienen como matrices de escala las siguientes.

$$\sigma_{\mathfrak{a}}=\begin{pmatrix}\sqrt{2}&0\\0&1/\sqrt{2}\end{pmatrix}\qquad \sigma_{\mathfrak{b}}=\begin{pmatrix}1&0\\1&1\end{pmatrix}.$$

Ambas matrices verifican $\sigma_{\mathfrak{a}}^{-1}\widetilde{\Gamma}\sigma_{\mathfrak{a}}=\sigma_{\mathfrak{b}}^{-1}\widetilde{\Gamma}\sigma_{\mathfrak{b}}=\Gamma_0(2)$; por tanto,

$$E_{\mathfrak{a}}(i,s)=\sum_{g\in\widetilde{\Gamma}_{\mathfrak{a}}\backslash\widetilde{\Gamma}}\left(\Im(\sigma_{\mathfrak{a}}^{-1}gi)\right)^s=\sum_{\gamma\in\Gamma_\infty\backslash\sigma_{\mathfrak{a}}^{-1}\widetilde{\Gamma}\sigma_{\mathfrak{a}}}\left(\Im(\gamma\sigma_{\mathfrak{a}}^{-1}i)\right)^s=\frac{1}{2^{s+1}}\sum_{\substack{m,n\in\mathbb{Z}\\ \mathrm{mcd}(m,n)=1\\ 2\nmid m-n}}^{\infty}\frac{1}{\left(m^2+n^2\right)^s},$$

de donde

$$2(2^s+1)E_{\mathfrak{a}}(i,s)=\sum_{\substack{m,n\in\mathbb{Z}\\ \mathrm{mcd}(m,n)=1\\ 2\nmid m-n}}^{\infty}\frac{1}{(m^2+n^2)^s}+\sum_{\substack{m,n\in\mathbb{Z}\\ \mathrm{mcd}(m,n)=1\\ 2\mid m-n}}^{\infty}\frac{1}{(m^2+n^2)^s}=2E(i,s).$$

Para $\mathfrak{b}$ se obtiene el mismo resultado empleando esencialmente el mismo procedimiendo que acabamos de utilizar. Esto concluye la prueba. □

Los Lemas 2.9 y 2.10 son la clave para dar una primera expresión satisfactoria de la fórmula de pretraza (2.12) para el caso no compacto.

Proposición 2.11. *Se tienen los dos siguientes desarrollos espectrales.*

$$\sum_{n=0}^{\infty} r(n)r(n+1)k(n) = 8\int_0^{\infty} k(x)\,dx + 2\sum_{j=1}^{\infty} h(\widetilde{t}_j)|u_j(i)|^2 + \frac{4}{\pi}\int_{-\infty}^{\infty} h(t)\left|\frac{f(t)}{1+2^{\frac{1}{2}+it}}\right|^2 dt \tag{2.25}$$

$$\sum_{n=0}^{\infty} \xi_n r(n)r(n+4)k(n/4) = 12\int_0^{\infty} k(x)\,dx + \sum_{j=1}^{\infty} h(t_j)|u_j(i)|^2 + \frac{1}{\pi}\int_{-\infty}^{\infty} h(t)|f(t)|^2\,dt, \tag{2.26}$$

donde ξ_n se define como en el Lema 2.9, $f(t) := \zeta(s)\zeta^{-1}(2s)L(s,\chi_4)$, $s = 1/2+it$ y $-(1/4+\widetilde{t}_j^2)$, $-(1/4+t_j^2)$ son los autovalores no triviales asociados a $\widetilde{\Gamma}\backslash\mathbb{H}$ y $\Gamma\backslash\mathbb{H}$, respectivamente. $h(t)$ es la transformada de Selberg de k dada por (2.10).

Demostración: La prueba es inmediata utilizando los Lemas 2.9 y 2.10 sobre (2.12). Nótese que en ambos casos hemos aislado el término correspondiente al autovalor trivial y utilizado que el área del dominio fundamental de Γ es $\pi/3$ y el de $\widetilde{\Gamma}$, π. Esto implica que u_0 es constante y vale $\sqrt{3/\pi}$ en el primer caso y $\sqrt{1/\pi}$ en el segundo. □

La anterior Proposición abre el camino a muchas posibles identidades aproximadas, siendo ahora la clave utilizar la funciones k adecuadas, estando entre ellas las que expusimos al final de la sección precedente. Uno de los ejemplos más satisfactorios va a ser la familia de funciones $\{k(u) = (u+1)^{-m}\}$, para cualquier entero $m \geq 2$, que nos van a permitir aproximar el número π. A continuación incluimos un estudio sobre el error cometido al realizar tales aproximaciones.

Definición 2.12. *De acuerdo a la notación de la Proposición 2.11 definimos las siguientes sucesiones, relativas a Γ.*

$$s_m = 4\sum_{n=0}^{\infty} \xi_n \frac{r(n)r(n+4)}{(n+4)^m}; \qquad \gamma_m = \int_{-\infty}^{\infty} g_m(t)|f(t)|^2\,dt.$$

$$e_m = (m-1)!^2\,\frac{2^{2m-4}(m-1)s_m - 3}{(m-1)\gamma_m} - \pi \tag{2.27}$$

Y, de forma paralela, las siguientes, relativas a $\widetilde{\Gamma}$.

$$\widetilde{s}_m = \sum_{n=0}^{\infty} \frac{r(n)r(n+1)}{(n+1)^m}; \qquad \widetilde{\gamma}_m = \int_{-\infty}^{\infty} g_m(t)\left|\frac{f(t)}{1+2^{\frac{1}{2}+it}}\right|^2 dt,$$

$$\widetilde{e}_m = (m-1)!^2\,\frac{(m-1)\widetilde{s}_m - 8}{16(m-1)\widetilde{\gamma}_m} - \pi.$$

Donde, en ambos casos, m es un entero mayor o igual que 2 y

$$g_m(t) = \operatorname{sech}(\pi t)\prod_{j=1}^{m-1}\left((j-1/2)^2+t^2\right).$$

Como probaremos a continuación, los términos e_m serán de pequeña magnitud, por lo que el primer sumando a la derecha en (2.27) será una aproximación de π para cada m. La función $g_m(t)$ es creciente en términos de m, por lo que a priori escoger $m = 2$ debería proporcionar la mejor aproximación de π. Es cierto que, partiendo del Corolario 2.5, la Definición 2.12 puede generalizarse cuando m es un semientero y tomar $m = 3/2$ podría dar una aproximación aún mejor, pero desafortunadamente el análogo de (2.27) para $m = 3/2$ no aproxima a π. En ambos casos, la convergencia de las series implicadas es relativamente lenta, haciendo inasequible estimarlas con mucha precisión con ordenador. Por ello, vamos a introducir los dos siguientes teoremas, que nos permitirán obtener tales cotas de manera satisfactoria.

Teorema 2.13. *Sea m un entero mayor que 1. Se cumple*

$$0 < e_m < \frac{\gamma_{m+1}}{\left((m-1/2)^2+t_3^2\right)\gamma_m}\,e_{m+1}.$$

donde $\lambda_3 = \frac{1}{4} + t_3^2$ es el tercer autovalor no trivial en $\Gamma\backslash\mathbb{H}$, y $t_3 = 13'77975\ldots$.

Demostración: Utilizaremos (2.26) sobre la función $k_m(u) = 4^{-m}(u+1)^{-m}$. Gracias al Lema 2.4, podemos dar explícitamente la transformada de Selberg de dicha función. Por último, el Lema 2.1 nos permite expresar $h(t_0)$ como una integral que se resuelve de forma inmediata. Uniendo todo esto, podemos escribir

$$s_m = \frac{48}{4^m(m-1)} + 4\sum_{j=1}^{\infty} h_m(t_j)|u_j(i)|^2 + \frac{4\pi}{4^{m-1}(m-1)!^2}\int_{-\infty}^{\infty} g_m(t)|f(t)|^2\,dt,$$

donde hemos aislado el término correspondiente al autovalor trivial t_0. El término de error e_m puede ahora expresarse de la siguiente forma:

$$e_m = \frac{4^{m-2}(m-1)s_m - 3}{(m-1)\gamma_m}(m-1)!^2 - \pi = \frac{\pi^2}{\gamma_m}\sum_{j=1}^{\infty} g_m(t_j)|u_j(i)|^2. \tag{2.28}$$

Esta última cantidad será estrictamente positiva gracias a que existen infinitos valores de j para los que u_j no se anula en i (véase [Iwa02, §13.2]). Utilizando ahora la

recurrencia $g_{m+1}(t) = \big((m-1/2)^2+t^2\big)g_m(t)$ y el hecho de que tanto u_1 como u_2 son impares [BSV06] (y en consecuencia, $u_1(i) = u_2(i) = 0$), deducimos

$$\frac{e_m}{e_{m+1}} = \frac{\gamma_{m+1}\sum_{j=1}^{\infty} g_m(t_j)|u_j(i)|^2}{\gamma_m \sum_{j=1}^{\infty} g_{m+1}(t_j)|u_j(i)|^2} \leq \frac{\gamma_{m+1}/\gamma_m}{(m-1/2)^2+t_3^2}.$$

El autovalor λ_3, por contra, está asociado a una función par [BSV06] y por tanto es el más relevante en el término de error. □

Por supuesto, el Teorema precedente tiene una versión similar referente a $\widetilde{\Gamma}$.

Teorema 2.14. *Sea m un entero mayor que 1. Se cumple*

$$0 < \widetilde{e}_m < \frac{\widetilde{\gamma}_{m+1}}{\big((m-1/2)^2+\widetilde{t}_1^{\,2}\big)\widetilde{\gamma}_m}\,\widetilde{e}_{m+1},$$

donde $\widetilde{\lambda}_1 = \frac{1}{4} + \widetilde{t}_1^{\,2}$ es el primer y más pequeño autovalor no trivial en $\widetilde{\Gamma}\backslash\mathbb{H}$, con $\widetilde{t}_1 = 8'92287\ldots$.

Demostración: Esta demostración procede de forma similar a la correspondiente al Teorema 2.13. Apelando a (2.25) y utilizando de nuevo los mismos dos lemas que antes, tenemos la siguiente expresión:

$$\widetilde{s}_m = \frac{8}{m-1} + 2\sum_{j=1}^{\infty} h_m(\widetilde{t}_j)|u_j(i)|^2 + \frac{16\pi}{(m-1)!^2}\int_{-\infty}^{\infty} g_m(t)\,\left|\frac{f(t)}{1+2^{\frac{1}{2}+it}}\right|^2 dt,$$

de donde

$$\widetilde{e}_m = \frac{\pi^2}{2\widetilde{\gamma}_m}\sum_{j=1}^{\infty} g_m(\widetilde{t}_j)|u_j(i)|^2 > 0, \qquad \text{y} \qquad \frac{\widetilde{e}_m}{\widetilde{e}_{m+1}} \leq \frac{\widetilde{\gamma}_{m+1}/\widetilde{\gamma}_m}{(m-1/2)^2+\widetilde{t}_1^{\,2}}$$

Y con esto se obtiene el resultado buscado. □

Ahora sí podemos, mediante el Teorema 2.13, acotar satisfactoriamente e_2. También podremos decir algo en el caso $m = 3/2$ para el que, como mencionamos antes, la Definición 2.12 admitía una generalización.

Proposición 2.15. *Sea e_2 dado por la Definición 2.12. Sea también $s_{3/2}$ correspondiente a generalizar esa misma definición para el caso en que m es un semientero. Se cumplen*

$$0 < e_2 < 3'62\cdot 10^{-14}, \qquad 0 < s_{3/2} - 12 - 8\int_{-\infty}^{\infty}\frac{t|f(t)|^2}{\operatorname{senh}(\pi t)}\,dt < 1'55\cdot 10^{-15}.$$

Demostración: Gracias a que se conocen métodos para estimar $|f(t)|$ con la precisión necesaria (véase [Bor00]), las integrales que definen γ_2 y γ_3 convergen con rapidez, y podemos estimar sus valores mediante cálculos con ordenador. Concretamente, $\gamma_2 = 0'23223\ldots$ y $\gamma_3 = 0'80239\ldots$. De la misma forma, e_3 se puede aproximar con la precisión necesaria, $e_3 = 2'0086 \cdot 10^{-12}$. Utilizando el Teorema 2.13 con estos valores, se obtiene la cota de e_2.

Para $e_{3/2}$, utilizamos la función $k(u) = (u+1)^{-3/2}$ sobre (2.26), obteniendo

$$16s_{3/2} = 192 + 128\pi \sum_{j=1}^{\infty} \frac{t_j}{\operatorname{sinh}(\pi t_j)} |u_j(i)|^2 + 128 \int_{-\infty}^{\infty} \frac{t|f(t)|^2}{\operatorname{senh}(\pi t)}\, dt.$$

La función $g(t) = t^{-1}(1/4+t^2)(9/4+t^2)\tanh(\pi t)$ es creciente para $t > t_3 = 13'77975$. Como además u_1 y u_2 se anulan en $t = i$,

$$0 < s_{3/2} - 12 - 8\int_{-\infty}^{\infty} \frac{t|f(t)|^2}{\operatorname{senh}(\pi t)}\, dt < \frac{8\pi}{g(t_3)} \sum_{j=3}^{\infty} \frac{(1/4+t_j^2)(9/4+t_j^2)}{\cosh(\pi t_j)} |u_j(i)|^2.$$

Por (2.28), el último sumatorio equivale a $\gamma_3 e_3/\pi^2$. Sustituyendo los valores numéricos de las cantidades involucradas, se obtiene la segunda parte del resultado. □

Nuestra mejor aproximación por tanto, difiere de π una cantidad menor que $4{\cdot}10^{-14}$ ¿Por qué tal aproximación se consigue con Γ y no con $\widetilde{\Gamma}$? Si se supone ([Iwa02, §13], [IS95]) que $u_j(t_j)$ puede acotarse esencialmente en términos del autovalor, a priori e_m debería ser comparable a $g_m(t_1)/\gamma_m$, y a $\widetilde{e}_m$ le debería ocurrir lo mismo en función de $\widetilde{\gamma}_m$, pero el análisis numérico de los primeros casos muestra que esto no ocurre en absoluto y ambas cantidades (e_m y $\widetilde{e}_m$) difieren en varios órdenes de magnitud. Si truncamos los valores correspondientes a $m = 3$ y 4,

$$e_3 = 2'0086 \cdot 10^{-12}, \quad \widetilde{e}_3 = 7'2745 \cdot 10^{-7}, \quad e_4 = 4'9016 \cdot 10^{-11}, \quad \widetilde{e}_4 = 6'7890 \cdot 10^{-6}.$$

La justificación de esta discrepancia ya ha aparecido, en la demostración del Teorema 2.13. Los dos primeros autovalores no triviales (y de menor tamaño) relativos Γ corresponden a autofunciones impares, y en consecuencia $u_1(i) = u_2(i) = 0$. Sin embargo, $\lambda_3 = \frac{1}{4} + t_3^2$, donde $t_3 = 13'77975\ldots$, está asociado a una autofunción par que no se anula en i (consúltese [BSV06]). El grupo $\widetilde{\Gamma}$ no corre esta misma suerte y ya su primer autovalor no trivial está asociado a una función par (consúltese [FL]). El gran tamaño del cociente $\cosh(\pi t_3)/\cosh(\pi \widetilde{t}_1) = 4'23 \cdot 10^6$ justifica por qué las aproximaciones de π derivadas de $\widetilde{\Gamma}$ son seis órdenes de magnitud menos precisas que las de Γ.

Es interesante notar que es posible extender los Teoremas 2.13 y 2.14 para albergar también el caso $m = 1$, que es en principio no convergente. Redefiniendo

$e_1 = s_1/4\gamma_1$ y $\widetilde{e}_1 = \widetilde{s}_1/16\widetilde{\gamma}_1$ para

$$s_1 = \sum_{n=0}^{\infty} \frac{\big(3+(-1)^n\big)r(n)r(n+4) - 24}{2(n+4)} \qquad \text{y} \qquad \widetilde{s}_1 = \sum_{n=0}^{\infty} \frac{r(n)r(n+1)-8}{n+1},$$

se puede probar que los dos sumatorios convergen.

Aunque el análisis se ha centrado en el estudio de la función $(u+1)^{-m}$, todavía es interesante ver lo que ocurre tomando otras.

Proposición 2.16. *Consideremos la serie*

$$S := \sum_{n=1}^{\infty} r(n)r(n+1)\,\frac{e^{1-\sqrt{n+1}}}{\sqrt{n+1}}$$

y la integral

$$I := \int_{-\infty}^{\infty} K_{it}^2(1/2)\left|\frac{f(t)}{1+2^{\frac{1}{2}+it}}\right|^2 dt.$$

Entonces, $(S-16)/(32I) = 0'8652559794526\ldots$ *supera a* e/π *en una cantidad positiva y menor que* $2'04\cdot 10^{-11}$.

Demostración: La transformada de Selberg de la función $k(u) = e^{1-\sqrt{u+1}}/\sqrt{u+1}$ es $h(t) = 8e\,K_{it}^2(1/2)$, gracias al Lema 2.7 tomando $\alpha = \beta = 1$. Por tanto,

$$S = 64e\int_0^{\infty} k(x)\,dx + 16e\sum_{j=1}^{\infty} h(\widetilde{t}_j)|u_j(i)|^2 + \frac{32e}{\pi}I.$$

Computando un número suficientemente grande de términos de S, se llega a la cota buscada. □

2.4. El caso compacto

Volvamos la vista atrás unos instantes, cuando definimos los grupos fuchsianos y llegábamos al desarrollo espectral (2.9) para núcleos automorfos. Aquella fórmula sólo era válida para grupos fuchsianos co-compactos (sin cúspides), y si no la fórmula anterior debía ser reemplazada por (2.12), que albergaba más términos. Ahora es el momento de explorar (2.9) sin preocuparnos por las series de Eisenstein. Siendo este caso a priori más sencillo por la simpleza de la fórmula, en la práctica surge sin embargo la dificultad de que los ejemplos de grupos co-compactos son menos frecuentes. Los que vamos a ver proceden del álgebra de cuaterniones, por ello comenzaremos esta sección introduciendo una serie de conceptos y resultados previos. Es de destacar que, como veremos a continuación, nuestro estudio es susceptible de

ser continuado buscando otros ejemplos de grupos fuchsianos válidos. Comenzamos considerando un cuerpo k de característica 0 y dos unidades $a, b \in k$. Se define el álgebra de cuaterniones A como

$$A := \{x_0 + x_1 i + x_2 j + x_3 ij : i^2 = a, j^2 = b, ij = -ji; x_0, x_1, x_2, x_3 \in k\},$$

donde i y j son dos elementos que permanecen indeterminados. Habitualmente se empleará la notación $\left(\frac{a,b}{k}\right)$ para referirse a A, ya que explicita los elementos que definen al álgebra. Por construcción, A es un k-espacio vectorial de dimensión 4 y puede suponerse sin pérdida de generalidad que a y b son libres de cuadrados. Si se toma $k = \mathbb{R}$, es sabido que las dos únicas álgebras de cuaterniones diferentes (no isomorfas) posibles son $\left(\frac{1,1}{\mathbb{R}}\right) \cong \mathcal{M}_2(\mathbb{R})$ y $\left(\frac{-1,-1}{\mathbb{R}}\right) =: \mathcal{H}$, esta última conocida habitualmente como los cuaterniones de Hamilton. La notación $\mathcal{M}_2(\mathbb{R})$ indica el conjunto de las matrices reales 2×2. Para un cuerpo cualquiera k toda álgebra de cuaterniones será o bien isomorfa a $\mathcal{M}_2(k)$ o bien un álgebra de división (no contendrá divisores de cero); pudiendo haber muchas distintas, en el sentido de que no serán isomorfas entre ellas.

Dado $x = x_0 + x_1 i + x_2 j + x_3 ij$, se definen el conjugado de x, su norma y su traza como $\overline{x} = x_0 - x_1 i - x_2 j - x_3 ij$, $n(x) := x \cdot \overline{x} = x_0^2 - a x_1^2 - b x_2^2 + ab x_3^2$ y $\mathrm{tr}(x) := x + \overline{x} = 2x_0$, respectivamente. Toda álgebra A se puede inyectar de forma natural sobre un álgebra de matrices. En concreto, siempre se tiene la inyección $\rho : A \longrightarrow \mathcal{M}_2\left(k(\sqrt{a})\right)$ dada por

$$1 \to I, \quad i \to \begin{pmatrix} \sqrt{a} & 0 \\ 0 & -\sqrt{a} \end{pmatrix}, \quad j \to \begin{pmatrix} 0 & 1 \\ b & 0 \end{pmatrix}, \quad ij \to \begin{pmatrix} 0 & \sqrt{a} \\ -b\sqrt{a} & 0 \end{pmatrix}.$$

Esta inyección es coherente con el producto definido dentro del álgebra, cumpliéndose $n(x) = \det\left(\rho(x)\right)$ y $\mathrm{tr}(x) = \mathrm{tr}\left(\rho(x)\right)$. El papel que en cierto modo desempeñan los grupos discretos de matrices en el lado derecho lo van a tomar los *órdenes* dentro de las álgebras, al tratarse desde cierto punto de vista en objetos discretos. Denotemos por R_k al anillo de enteros de k, que sabemos es único. Un orden va a ser al álgebra de cuaterniones lo que el anillo de enteros al cuerpo, sin embargo, no habrá un único orden a partir de un álgebra de cuaterniones dada:

Definición 2.17. *Sea A un álgebra de cuaterniones sobre un cuerpo k. Un* orden $\mathcal{O}$ *es un R_k-módulo finitamente generado cumpliendo las siguientes condiciones:*

1. $\mathcal{O} \bigotimes_{R_k} k = A$.
2. $\mathcal{O}$ *es un anillo que contiene al* 1.

Por ejemplo, dada cualquier álgebra de cuaterniones $A = \left(\frac{a,b}{\mathbb{Q}}\right)$, consideremos los conjuntos $\mathcal{O}_1 := \mathbb{Z}[1, i, j, ij]$ y $\mathcal{O}_2 := \mathbb{Z}[1/2, i/2, j/2, ij/2]$. Ambos son órdenes,

porque al tensorizar respecto de $\mathbb{Q}$ se obtiene todo A. Entre los órdenes existirá, valga la redundancia, un orden parcial (en este caso $\mathcal{O}_1 \subset \mathcal{O}_2$) y estaremos interesados en los maximales.

Por supuesto, va a ser posible extraer grupos discretos a partir de órdenes mediante la inyección ρ, pero nuestro objetivo es extraer grupos fuchsianos (de primera especie). A partir de ahora supongamos que $\mathbb{Q} \subset k \subset \mathbb{R}$ es un cuerpo de números. Dada un álgebra de cuaterniones sobre k, denotaremos por A^1 a los elementos que tienen norma 1, que irán a parar por ρ a $\mathrm{SL}_2(\mathbb{R})$ siempre que se asuma $a > 0$. A^1 no será un álgebra, pero sí un grupo; eso sí, no será discreto, y de hecho se puede probar que su imagen será densa en $\mathrm{SL}_2(\mathbb{R})$. Dado ahora un orden, denotamos por $\mathcal{O}^1$ a los elementos de norma 1 y consideramos el grupo $P(\rho(\mathcal{O}^1))$ (la P sirve para indicar que se identifica I con $-I$). El siguiente resultado caracteriza los casos en los que tal grupo es discreto (y, por tanto, fuchsiano).

Teorema 2.18 (Armand Borel y Harish-Chandra, [BHC62])**.** *Sea $\mathcal{O}$ un orden contenido en un álgebra de cuaterniones $A = \left(\frac{a,b}{k}\right)$, para un cuerpo de números k. El grupo $P(\rho(\mathcal{O}^1))$ es discreto si y sólo si se cumple una de las siguientes propiedades*

1. *k es totalmente real (es decir, todas sus inmersiones son reales).*
2. *$A \bigotimes_k \mathbb{R} = \mathcal{M}_2(\mathbb{R})$.*
3. *Todo $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}) \setminus \{Id\}$ cumple $A^\sigma \bigotimes_{\sigma(k)} \mathbb{R} = \mathcal{H}$, donde $\mathcal{H}$ representa los cuaterniones de Hamilton.*

Nótese que $A^\sigma = \left(\frac{\sigma(a),\sigma(b)}{\sigma(k)}\right)$, lo que permite escribir el producto tensorial del tercer punto como $\left(\frac{\sigma(a),\sigma(b)}{\mathbb{R}}\right)$. La segunda condición equivale a que a o b sean positivos (al menos uno de los dos).

Si se toma por ejemplo $A = \left(\frac{1,1}{\mathbb{Q}}\right)$ y se considera el orden $\mathcal{O} = \mathbb{Z}[1, i, j, ij]$, de $\mathcal{O}^1$ se obtiene el grupo Γ mediante el procedimiento anterior. Sin embargo éste es un caso aislado, ya que salvo que se parta de un álgebra de cuaterniones de la forma $\left(\frac{1,1}{k}\right)$ el grupo obtenido será co-compacto. Los órdenes que vamos a utilizar son los llamados *órdenes de Eichler*, definidos como la intersección de dos órdenes maximales. Nuestros ejemplos son de este tipo. Consideremos, para primos $p \equiv 3\,(4)$ y $q \equiv 5\,(8)$,

$$\begin{aligned} \mathcal{O}_1 := \mathbb{Z}\left[1, i, j, \frac{1}{2}(1+i+j+ij)\right] &\subset \left(\frac{p,-1}{\mathbb{Q}}\right) \\ \mathcal{O}_2 := \mathbb{Z}\left[1, i, \frac{1}{2}(1+j), \frac{1}{2}(i+ij)\right] &\subset \left(\frac{2,q}{\mathbb{Q}}\right). \end{aligned}$$

Ambos son órdenes de Eichler maximales (véase [AB04]) y sus imágenes por ρ darán lugar a dos familias de grupos fuchsianos co-compactos,

$$\begin{aligned} G_p &= \left\{ \frac{1}{2}\begin{pmatrix} a+b\sqrt{p} & c+d\sqrt{p} \\ -c+d\sqrt{p} & a-b\sqrt{p} \end{pmatrix} \in \mathrm{SL}_2(\mathbb{R}) : a \equiv b \equiv c \equiv d \pmod 2 \right\} / \{\pm I\} \\ G_{2,q} &= \left\{ \frac{1}{2}\begin{pmatrix} a+b\sqrt{2} & c+d\sqrt{2} \\ q(c-d\sqrt{2}) & a-b\sqrt{2} \end{pmatrix} \in \mathrm{SL}_2(\mathbb{R}) : a \equiv c, b \equiv d \pmod 2 \right\} / \{\pm I\}, \end{aligned}$$

para primos p y q verificando las mismas condiciones de congruencia que se usaron para introducir $\mathcal{O}_1$ y $\mathcal{O}_2$. Remitimos al lector a [Vig80] para profundizar en la teoría de los órdenes de Eichler. Las familias G_p y $G_{2,q}$ nos permitirán utilizar (2.9) de forma satisfactoria. Vamos a emplear la siguiente generalización de la función $r(n)$, para enteros arbitrarios s y t:

$$r_{s,t}(n) = \left| \left\{ (x,y) \in \mathbb{Z}^2 : rx^2 + st^2 = n \right\} \right|.$$

Utilizando esta generalización vamos a poder dar un significado aritmético a los desarrollos espectrales para G_p y $G_{2,q}$ en determinadas parejas de puntos.

Lema 2.19. *Para los grupos G_p y $G_{2,q}$ se verifican las siguientes identidades:*

$$\sum_{\gamma \in G_p} k\left(u(\gamma i, i)\right) = \frac{1}{2}\sum_{n=0}^{\infty} r(n) r(pn+2) k\left(\frac{pn}{2}\right) \tag{2.29}$$

$$\sum_{\gamma \in G_{2,q}} k\left(u\big(\gamma(i/\sqrt{q}), i/\sqrt{q}\big)\right) = \frac{1}{2}\sum_{n=0}^{\infty} r_{2,q}(n) r_{1,2q}(n+4) k\left(\frac{n}{4}\right). \tag{2.30}$$

Demostración: Esta demostración se basa en las mismas ideas que las del Lema 2.9. Comenzamos tomando una matriz $\gamma \in G_p$, dada por los coeficientes a, b, c, d en el orden correcto. En particular, $ad - bc = 1$ y, por analogía con (2.17), se tiene la siguiente doble igualdad:

$$4u(\gamma i, i) = p(b^2 + d^2) = a^2 + c^2 - 4.$$

La suma $b^2 + d^2$ siempre ha de ser par por definición, por lo que $u(\gamma i, i)$ será siempre un múltiplo entero de $p/2$. Queremos entonces contar el número exacto de matrices de G_p para las que $u(\gamma i, i)$ valdrá $pn/2$, para cada n. De nuevo empleando la analogía con (2.17), está claro que la correspondencia

$$\begin{aligned} \left\{ (a,b,c,d) \in \mathbb{Z}^4 : \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in G_p \right\} &\to \left\{ (r,s,t,u) \in \mathbb{Z}^4 : p(s^2+u^2) = r^2 + t^2 - 4 \right\} \\ (a,b,c,d) &\mapsto (b,d,a,c) \end{aligned}$$

es una biyección (gracias a que p es congruente con 3 módulo 4); por tanto, escribiendo $u(\gamma i, i) = 4m$ para m un múltiplo entero de $p/2$, cada valor $4m$ se tomará para exactamente $r(4m/p)r(4m+4)$ matrices. Mediante el cambio $4m \to pn/2$, cada valor $pn/2$ se tomará para $r(2n)r(pn+2)$ matrices, de donde se concluye (2.29) gracias a que $r(2n) = r(n)$ y a la identificación de I con $-I$. Para (2.30), evaluando $u(\gamma z, w)$ en $z = w = i/\sqrt{q}$ se obtienen las siguientes dos igualdades:

$$4u\big(\gamma(i/\sqrt{q}), i/\sqrt{q}\big) = a^2 + 2qd^2 - 4 = 2b^2 + qc^2.$$

El proceso es esencialmente igual al caso anterior y no lo volveremos a desarrollar. Esencialmente, escribiendo $n = u\left(\gamma(i/\sqrt{q})\right)$, el número de matrices de $G_{2,q}$ para las que $u\big(\gamma(i/\sqrt{q}), i/\sqrt{q}\big)$ vale n equivaldrá a $r_{2,q}(4n)r_{1,2q}(4n+4)$, de donde identificando de nuevo I con $-I$ y tomando $n' = n/4$ se completa la prueba de (2.30). □

Proposición 2.20. *Se tienen los dos siguientes desarrollos espectrales.*

$$\sum_{n=0}^{\infty} r(n)r(pn+2)k(pn/2) = \frac{24}{p-1}\int_0^{\infty} k(x)\,dx + 2\sum_{j=1}^{\infty} h(t_j)|u_j(i)|^2$$
$$\sum_{n=0}^{\infty} r_{2,q}(n)r_{1,2q}(n+4)k(n/4) = \frac{24}{q-1}\int_0^{\infty} k(x)\,dx + 8\sum_{j=1}^{\infty} h(t_j)|u_j(i/\sqrt{q})|^2,$$

Demostración: Basta utilizar el Lema 2.19 en el desarrollo 2.9 y tener en cuenta (véase [BJ99],(2.1)) que el área del dominio fundamental de G_p es $(p-1)\pi/3$, mientras que la de $G_{2,q}$ es $(q-1)\pi/3$. □

Se ha demostrado (véanse [BJ99], [Str01]) que cada grupo entre los que forman G_p y $G_{2,q}$ tienen los mismos autovalores que $\Gamma_0(D)$, donde D es el discriminante asociado a cada grupo. Éste viene definido por el producto de los primos tales que $ax^2 + by^2 \equiv z^2 \pmod{p^k}$ no tiene solución no trivial para algún k, donde a y b son los generadores del álgebra de cuaterniones sobre la que se define el grupo. Debido a esto, la mejor identidad aproximada que vamos a obtener con estos grupos procede de G_3. Para poder obtener cotas superiores explícitas para del error cometido al utilizar tal identidad aproximada, necesitamos el resultado que sigue a continuación.

Proposición 2.21. *Sea $A = \{\gamma \in G_3 : \rho(\gamma i, i) < R\}$, para $R > 0$ arbitrario y donde ρ es la distancia hiperbólica dada por* (2.6)*. Se cumple*

$$|A| \leq 3(2+\sqrt{3})\cosh R.$$

Demostración: Para la prueba, necesitamos un dominio fundamental de G_3. El Teorema 5.46 de [AB04] nos dice que una posible representación de dicho dominio viene

dada por el hexágono hiperbólico D (véase la Figura 2.4), cuyos lados son geodésicas que unen sus vértices:

$$\begin{array}{lllllllll} v_1 & = & \dfrac{-\sqrt{3}+2}{2}, & v_2 & = & \dfrac{-1+i}{1+\sqrt{3}}, & v_3 & = & (2-\sqrt{3})i, \\ v_4 & = & -\overline{v_2}, & v_5 & = & -\overline{v_1}, & v_6 & = & i. \end{array}$$

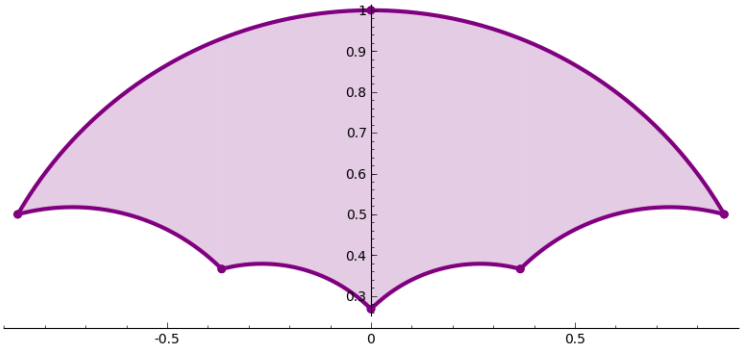

Figura 2.4: El dominio fundamental D de G_3 descrito en la Proposición 2.21.

Es fácil comprobar que la distancia entre v_6 y cualquier otro vértice es no superior a $\cosh^{-1} 2$, y por tanto el dominio fundamental estará contenido en el disco hiperbólico de centro i y radio $\cosh^{-1} 2$. Así mismo, si consideramos todos los $\gamma \in A$, la unión $\bigcup \gamma D$ estará contenida en el disco de centro y y radio $R + \cosh^{-1} 2$, al que llamaremos B. Dados $\gamma, \gamma' \in A$, los conjuntos γD y $\gamma' D$ tendrán interior disjunto. Por tanto,

$$|A| \leq |B|/|D| = 3(2\cosh R + \sqrt{3}\,\mathrm{senh}\, R - 1).$$

En el último paso hemos utilizado que el área del dominio fundamental es $2\pi/3$, y que el área del círculo hiperbólico de radio r es $4\pi\,(\mathrm{senh}(r/2))^2$ (consúltese el capítulo 1 de [Iwa02]). □

Ahora podemos dar la principal identidad aproximada de esta sección.

Proposición 2.22. *Consideremos la serie*

$$S = \sum_{n=1}^{\infty} r(n) r(3n+2) \sqrt{n} e^{-((\log n)/4)^2}. \tag{2.31}$$

Se verifica

$$1'29 \cdot 10^{-7} < 1 - \frac{S}{72 e^9 \sqrt{\pi}} < 3 \cdot 10^{-7}.$$

Demostración: Vamos a extraer la parte inicial de la serie, que acotaremos con ordenador. Concretamente, si consideramos S' como la suma de los $N = 2'2 \cdot 10^{12}$ primeros términos de (2.31), se prueba que

$$2 \cdot 10^{-7} < 1 - \frac{S'}{72e^9\sqrt{\pi}} < 3 \cdot 10^{-7}.$$

Sea S'' el resto de la serie. Empleando la Proposición 2.21 con $\cosh R = 1 + 3x$ y la Proposición 2.20 se obtiene

$$\sum_{n \le x} r(n)r(3n+2) \le 18(2+\sqrt{3})x - 6(1+\sqrt{3}).$$

Ahora dividimos la serie en intervalos diádicos:

$$\begin{aligned} S'' &\le \sum_{j=0}^{\infty} \sqrt{2^j N} e^{-(\log(2^j N))^2/16} \sum_{n \le 2^{j+1}N} r(n)r(3n+2) \\ &\le 36(2+\sqrt{3}) \sum_{j=0}^{\infty} (2^j N)^{3/2} e^{-(\log 2^j N)^2/16}. \end{aligned}$$

Extrayendo los términos correspondientes a $j = 0, 1$ y acotando el resto con una integral, se obtiene

$$\begin{aligned} S'' &\le 36(2+\sqrt{3}) \left(3'8977 \cdot 10^{-4} + 9'1185 \cdot 10^{-5} + \frac{1}{\log 2} \int_{\log(2N)}^{\infty} e^{3x/2 - x^2/16}\, dx \right) \\ &\le 6'4619 \cdot 10^{-2} + \frac{36(2+\sqrt{3}}{\log 2} \cdot \frac{8}{\log(2N) - 12} \int_{\log(2N)}^{\infty} \frac{x-12}{8} e^{3x/2 - x^2/16}\, dx. \end{aligned}$$

De donde se concluye

$$0 < 1 - \frac{S''}{72e^9\sqrt{\pi}} < 7'0479 \cdot 10^{-9}.$$

Uniendo las cotas sobre S' y S'' se completa la prueba. □

Un pequeño comentario para finalizar esta sección es que, utilizando los resultados que hemos visto, es posible *fabricar* funciones k que permitan dar cotas superiores para el primer autovalor en G_p tal que $u_j(i)$ sea no nulo. Por ejemplo, consideremos

$$k(u) = \frac{0'7676}{(u+1)^{3/2}} - \frac{1'6153}{(u+1)^2} + \frac{0'6550}{(u+1)^{5/2}}.$$

Utilizando esta función en la Proposición 2.20 para $p = 3$, el lado izquierdo de la igualdad se cancela con la integral. Además, por el Lema 2.4, la transformada de Selberg es positiva para $t > 3'377$. Por tanto, esto nos permite demostrar que el primer autovalor en G_3 para el que $u_j(i)$ no se anula es menor que $3'377$ (nótese que su valor real es aproximadamente $2'592$).

2.5. Aplicación de los operadores de Hecke

De acuerdo a la teoría clásica [Miy06], podemos introducir los operadores de Hecke [Iwa02, §8.5] en nuestro contexto. Sea m un entero positivo. Definimos Γ_m como el conjunto de matrices enteras 2×2 con determinante m. El operador de Hecke T_m viene dado por

$$T_m f(z) = \frac{1}{\sqrt{m}} \sum_{\gamma \in \Gamma \backslash \Gamma_m} f(\gamma z)$$

para funciones $f \in L^2(\Gamma\backslash\mathbb{H})$ no holomorfas. Este operador será autoadjunto y conmutará por ello con Δ. Las formas de Maass $\{u_j(z)\}_{j=0}^{\infty}$ pueden escogerse de forma que también sean autofunciones de T_m con autovalores que denotaremos por $\{\lambda_j(m)\}_{j=0}^{\infty}$. En $\Gamma_0(N)$, lo ya visto sigue siendo válido si N y m son coprimos; para el resto de casos puede utilizarse teoría de Atkin-Lehner.

Los operadores de Hecke también se pueden definir de la misma manera en los grupos co-compactos procedentes de álgebras de cuaterniones sobre $\mathbb{Q}$ (consúltense [Are05] y [Miy06, §5.3]), pero ahora la suma recorre las matrices de $\gamma \in R(1)\backslash R(m)$, donde $R(m)$ indica la imagen por ρ (véase la sección anterior) de los elementos de norma m de un orden R. Si se aplica T_m a un núcleo automorfo con respecto de Γ, el desarrollo obtenido es

$$T_m\Big(\sum_{\gamma\in\Gamma} k(\gamma(\cdot), w)\Big)(z) = \frac{1}{\sqrt{m}} \sum_{\gamma\in\Gamma_m} k(\gamma z, w).$$

Luego, formalmente, aplicar un operador de Hecke se correponde con considerar matrices enteras de determinante m en lugar de las de determinante unitario. Por otro lado, la acción de T_m sobre (2.12) es

$$\sum_{j=0}^{\infty} \lambda_j(m) h(t_j) u_j(z) \overline{u_j(w)} + \frac{1}{4\pi} \int_{-\infty}^{\infty} \eta_t(m) h(t) E(z, 1/2+it) \overline{E(w, 1/2+it)}\, dt \tag{2.32}$$

donde $\eta_t(m)$ viene dada por $\sum_{ab=m} (a/b)^{it}$ (véase [Iwa02]).

Se tiene fórmulas similares para el caso asociado a las álgebras de cuaterniones cuando m es coprimo con el discriminante del álgebra (véase la sección anterior) y con el nivel del orden (véanse [BHC62], [Hej85]). Nos restringiremos al grupo Γ y al orden $\mathcal{O}_1 = \mathbb{Z}\left[1, i, j, \frac{1}{2}(1+i+j+k)\right]$ que habíamos utilizado para definir G_p.

Lema 2.23. *Para Γ_m definida como antes y ξ_n como en el Lema 2.9, se cumple*

$$\sum_{\gamma\in\Gamma_m} k\big(u(\gamma i, i)\big) = \sum_{n=0}^{\infty} \xi_n r(n) r(n+4m) k\big(\frac{n}{4m}\big).$$

Y, para el orden $\mathcal{O}_1 = \mathbb{Z}\left[1, i, j, \frac{1}{2}(1+i+j+k)\right]$,

$$2\sum_{\gamma\in R(m)} k\big(u(\gamma i, i)\big) = \sum_{n=0}^{\infty} r(n)r(pn+2m)k\big(\frac{pn}{2m}\big),$$

para $p \equiv 3 \pmod 4$.

Demostración: La demostración es, de nuevo, muy similar a las de las Proposiciones 2.9 y 2.19. Tomando γ de determinante m,

$$\begin{cases} 4m\, u(\gamma i, i) = (a-d)^2 + (b+c)^2 \\ 4m\, u(\gamma i, i) + 4m = (a+d)^2 + (b-c)^2 \end{cases}$$

A partir de este sistema, la primera fórmula se obtiene siguiendo el mismo proceso que en la primera de las dos citadas demostraciones. Para la segunda fórmula se utiliza la segunda demostración, partiendo de que $4u(\gamma i, i) = p(b^2+d^2)/m$ para $\gamma \in R(m)$ y $p(b^2+d^2) + 4m = a^2 + c^2$. □

Se cumple $|\Gamma\backslash\Gamma_m| = \sigma(m)$, donde $\sigma(m)$ denota la suma de todos los divisores de m. De forma análoga, si m y $2p$ son coprimos, entonces $|R(1)\backslash R(m)| = \sigma(m)$ (véase la página 217 de [Miy06]). Y si la transformada de Selberg de k decae con suficiente rapidez, esperamos que, de forma similar a las Proposiciones 2.11 y 2.20, se cumplan

$$\sum_{n=0}^{\infty} \big(4\chi_n r(n)r(n+4m)k\big(\frac{n}{4m}\big) \approx 96\sigma(m)\int_0^{\infty} k(x)\,dx + \frac{8\sqrt{m}}{\pi}\int_{-\infty}^{\infty} \eta_t(m)h(t)|f(t)|^2\,dt \tag{2.33}$$

y

$$\sum_{n=0}^{\infty} r(n)r(pn+2m)k\big(\frac{pn}{2m}\big) \approx \frac{24\sigma(m)}{p-1}\int_0^{\infty} k(x)\,dx \qquad \text{para } 2\nmid m,\ p\nmid m. \tag{2.34}$$

Tomemos por ejemplo

$$S = \sum_{n=0}^{\infty} \big(3+(-1)^n\big) r(n)r(n+2012)\frac{2012^3}{(n+2012)^3}$$

junto con

$$I = \int_{-\infty}^{\infty} \frac{\cos(t\log 503)}{\cosh(\pi t)}(1/4+t^2)(9/4+t^2)|f(t)|^2\,dt.$$

De (2.33) y del Lema 2.4 para $m = 503$ y $k(u) = (u+1)^{-3}$, deducimos

$$S \approx 24192 + 16\pi\sqrt{503}\, I.$$

De los valores numéricos aproximados ($S = 24144'020885716756651$ e $I = -0'042559682395475411270$) se obtiene

$$\frac{S - 24192}{16I} = 70'45857658\ldots$$

que coincide con $\pi\sqrt{503}$ en al menos todos los dígitos mostrados. El error cometido debería de hecho ser comparable a 10^{-12}.

A pesar de la precisión lograda con este ejemplo, las fórmulas (2.33) y (2.34) no deberían ser uniformes en m, por el errático comportamiento de $\lambda_j(m)$ sobre el número de divisores de m. Véase [Cha99] para un análisis de la uniformidad.

Es interesante notar que las propiedades multiplicativas de los autovalores de Hecke pueden observarse numéricamente para mejorar las aproximaciones. Considérese por ejemplo

$$S_m = \sum_{n=0}^{\infty} r(n)r(7n+2m)g(7n/2m),$$

donde g es la función k del Lema 2.8. Según (2.34), debería aproximar a $2\sigma(m)$, pero tal aproximación es pobre debido a la existencia de pequeños autovalores al principio. De hecho se cumplen

$$S_1 - 2 = 0'047039, \qquad S_3 - 8 = -0'109461 \qquad \text{y} \qquad S_9 - 26 = 0'119267.$$

El desarrollo espectral (2.32) y el Lema 2.23 sugieren que

$$S_m \approx 2\sigma(m) + 2\sqrt{m}\lambda_1(m)h(t_1)|u_1(i)|^2$$

donde h viene dada por el Lema 2.8, es una mejor aproximación. Por otro lado, las propiedades multiplicativas de los autovalores de Hecke (véase [Iwa02, §8.5]) aseguran que $\big(\lambda_j(3)\big)^2 = 1 + \lambda_j(9)$, que se traduce en $(8 - S_3)^2 \approx 3(2 - S_1)^2 + (26 - S_9)(2 - S_1)$. Esperamos por tanto, la siguiente aproximación mejorada:

$$S_3 + \sqrt{3(2 - S_1)^2 + (26 - S_9)(2 - S_1)} \approx 8.$$

El lado izquierdo vale de hecho $8'001211$, mejorando la aproximación precedente $S_3 \approx 8$ en dos órdenes de magnitud.

Los resultados expuestos en este capítulo aparecieron recogidos originalmente en [CRRC13].

Capítulo 3

Espectro de singularidades y formas modulares

3.1. Multifractales. El ejemplo de Riemann

El capítulo final se centra en el análisis de las propiedades multifractales de ciertas familias de formas modulares. Tanto el concepto de función multifractal como el de espectro de singularidades, los dos términos en torno a los que orbita toda nuestra exposición, fueron introducidos hace relativamente poco tiempo. Los multifractales aparecen por primera vez en el campo de la física; más concretamente, en el estudio de la mecánica de fluidos [BPPV84]. En esta primera sección definiremos ambos conceptos, previo recordatorio de algunos términos propios del análisis y de la teoría de la medida. También veremos con detalle una conocida función que es además un ejemplo de multifractal.

Como vamos a trabajar con formas modulares, dedicaremos una segunda sección de preliminares a introducirlas y repasar algunas de sus más relevantes propiedades, que utilizaremos más adelante. Parte de lo que aquí vamos a ver ya apareció en el capítulo anterior; concretamente, el semiplano de Poincaré y la acción de grupos fuchsianos de primera especie sobre él, así como los dominios fundamentales y las cúspides de estos grupos. Hemos considerado adecuado desarrollar las dos exposiciones por separado en cada capítulo a pesar de la presencia de estos elementos comunes. El motivo, además de que el nivel de intersección no es muy significativo, es que el contexto del que partimos ahora es notablemente diferente del que teníamos en el capítulo anterior, y tal exposición en común podría dar lugar a confusión. En cualquier caso, cuando en lo sucesivo aparezcan términos previamente introducidos en el segundo capítulo se detallarán claramente las diferencias existentes. En lo que sigue, a menudo utilizaremos la conocida notación de Landau que introdujimos en la página 9.

Dado cualquier conjunto no vacío $X \subset \mathbb{R}$ y $s > 0$, la *medida s-dimensional de*

Hausdorff de X viene dada por

$$\mathcal{H}^s(X) := \lim_{\delta\to 0} \inf\left\{\sum_{i=1}^{\infty} |U_i|^s : \{U_i\}_{i\in\mathbb{N}} \text{ es un } \delta\text{-recubrimiento de } X\right\},$$

donde un δ-recubrimiento de X es cualquier colección numerable de conjuntos $\{U_i\}$ tales que el diámetro de cada uno de ellos sea menor que δ y X esté contenido en la unión de todos ellos. La *dimensión de Hausdorff* de $X \subset \mathbb{R}^n$ viene a su vez dada por

$$\dim_{\mathcal{H}}(X) := \inf\{s > 0 : \mathcal{H}^s(X) = 0\} = \sup\{s > 0 : \mathcal{H}^s(X) = \infty\}.$$

Es un hecho conocido que la anterior definición es consistente, y que cualquier conjunto con dimensión de Hausdorff menor que 1 tiene medida nula[1]. Nótese que la medida de Hausdorff está definida para cualquier subconjunto no vacío de $\mathbb{R}^n$ donde n es cualquier entero positivo, pero aquí sólo utilizaremos $n = 1$. En adelante, si no se indica otra cosa nos referiremos a la dimensión de Hausdorff cuando digamos *dimensión* a secas. Siguiendo la notación de [CU12], tomemos una función $f : [0, 1] \longrightarrow \mathbb{C}$, y un punto $x \in [0, 1]$. Se define el *exponente Hölder* u *orden Hölder* de f en x como el supremo de todos los $\alpha \geq 0$ tales que f pertenece a $C^\alpha(x)$, donde

$$C^\alpha(x) := \{f : |f(x + h) - P(h)| = \mathcal{O}\left(|h|^\alpha\right) \text{ para algún } P \in \mathbb{C}[x] : \deg(P) \leq \alpha\}$$

Denotaremos al exponente Hölder en x por $\beta_f(x)$. Si $\beta_f(x) \leq 1$, dicho exponente puede definirse equivalentemente [CU12] de la siguiente forma

$$\beta_f(x) := \sup\{\alpha \leq 1 : |f(x + h) - f(x)| = \mathcal{O}\left(|h|^\alpha\right)\}. \tag{3.1}$$

Ya estamos en condiciones de definir el espectro de singularidades de una función f.

Definición 3.1 (Espectro de singularidades)**.** *Dada una función $f : [0, 1] \longrightarrow \mathbb{C}$, se denomina* espectro de singularidades de f *a la correspondencia $d_f : [0, \infty) \longrightarrow [0, \infty)$ dada por*

$$d_f(\delta) := \begin{cases} \dim_{\mathcal{H}}\{x \in [0, 1] : \beta_f(x) = \delta\}, & si\ \{x \in [0, 1] : \beta_f(x) = \delta\} \neq \emptyset. \\ indefinido, & si\ \{x \in [0, 1] : \beta_f(x) = \delta\} = \emptyset. \end{cases}$$

En otras palabras, el espectro de singularidades de f asigna a cada posible exponente Hölder la dimensión de Hausdorff del subconjunto de $[0, 1]$ formado por todos los puntos que tienen ese exponente Hölder, en caso de que ese conjunto sea no vacío. Si se consideran la mayoría de funciones de uso habitual, sus espectros de singularidades tendrán descripciones muy simples al estar definidos en un número finito de puntos. Pero existirán ejemplos en los que estos espectros sean mucho más elaborados: las funciones multifractales.

[1]Cuando indiquemos medida nula nos referiremos implícitamente a la medida de Lebesgue.

Definición 3.2 (Función multifractal)**.** *Considérese la función f de la definición anterior. Si la imagen de su espectro de singularidades es un conjunto no discreto, se dice que f es una* función multifractal.

La nomenclatura escogida para estas funciones no es una casualidad. Si se considera un conjunto de puntos $F \subset [0,1]$ con dimensión de Hausdorff comprendida estrictamente entre 0 y 1, tal conjunto estará describiendo un fractal en el más amplio sentido de la palabra. Este término, acuñado por Benoit Mandelbrot, procede del latín *fractus* (roto) y hace referencia a la imposibilidad de describir estos conjuntos con las técnicas geométricas habituales. En palabras de Kenneth Falconer [Fal90], aunque hay varias definiciones diferentes de fractales según el contexto en que nos movamos, éstas suelen compartir varios puntos sobre lo que debe cumplir un fractal:

- Un fractal está dotado de cierta *estructura* a cualquier nivel; es decir, tiene detalle a escala arbitrariamente pequeña.
- La estructura de un fractal es demasiado irregular para describirlo en el lenguaje geométrico tradicional, tanto local como globalmente.
- A menudo los fractales verifican algún tipo de autosemejanza, aproximada o estadística.
- Habitualmente su *dimensión fractal* (la dimensión de Hausdorff, en nuestro caso) es mayor que su *dimensión topológica* (se trata de conjuntos de medida nula).
- Es frecuente que un fractal se defina de forma sencilla, por ejemplo recursivamente.

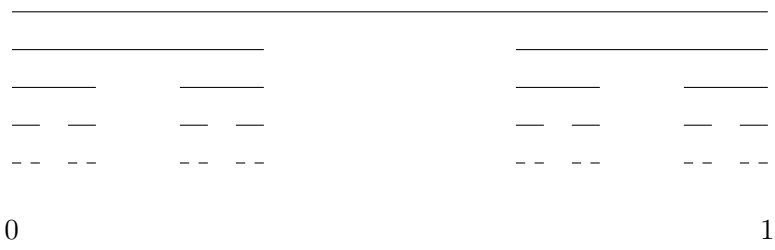

Figura 3.1: De arriba a abajo, los primeros cinco niveles del proceso iterativo que conduce al conjunto de Cantor.

El ejemplo arquetípico es el famoso conjunto de Cantor (véase la Figura 3.1). Es éste un subconjunto del intervalo $[0,1]$ con cardinal no numerable sin ser denso, y

con dimensión de Hausdorff $0 < \log 2/\log 3 < 1$ [Fal90, §2.3]. Se define de forma iterativa partiendo de $C_0 = [0, 1]$ y, en la etapa k-ésima, eliminando de cada uno de los 2^{k-1} intervalos de C_{k-1} el tercio central y dejando dos intervalos (cerrados) que miden cada uno la tercera parte del original. El conjunto de Cantor es la intersección infinita de todos los C_k. Es un conjunto autosemejante, y dotado de estructura no trivial en cualquier escala. Salvando las distancias, cualquier conjunto de la forma que describíamos arriba (con dimensión de Hausdorff comprendida entre 0 y 1) va a ser un fractal como éste. Y la Definición 3.2 nos dice que, si tomamos una función multifractal, clasificando los puntos del intervalo $[0, 1]$ en base a su exponente Hölder obtendremos una colección no numerable de fractales distintos. Por tanto, la elección del término *multifractal* está más que justificada.

Por supuesto, no queremos desaprovechar la oportunidad de introducir un ejemplo significativo que ilustre tanto los nuevos conceptos como nuestros objetivos. En este caso se trata de uno bastante famoso, habitualmente denominado *ejemplo de Riemann*:

$$R(x) := \sum_{n=1}^{\infty} \frac{\operatorname{sen}(2\pi n^2 x)}{n^2}, \ x \in \mathbb{R}. \tag{3.2}$$

Puede verse su representación gráfica en la Figura 3.2. Esta función, en ocasiones presentada en forma compleja (sustituyendo el seno por una exponencial), tiene una gran historia. Se denomina ejemplo de Riemann porque, según Karl Weierstrass [Edg04], Bernhard Riemann la citó a mediados del siglo XIX como ejemplo de función continua en todo $\mathbb{R}$ y al mismo tiempo no diferenciable en ningún punto, afirmación que a la postre resultaría ser errónea. Es fácil deducir la continuidad, pero la diferenciabilidad no se supo demostrar o refutar hasta mucho después. Godfrey H. Hardy allanó el terreno probando [Har16] en 1916 que R era no diferenciable en todos los irracionales, y en ciertas familias de racionales (véanse las Figuras 3.3 y 3.8 en las páginas 68 y 91). Fue Joseph Gerver quien en 1970, siendo un estudiante, demostró [Ger70] que R era diferenciable en una colección numerable de racionales, concretamente en los de la forma a/b, con a impar y b par no múltiplo de 4 (véase la Figura 3.7 en la página 90), que eran justamente los únicos que no habían entrado en el resultado de Hardy. Por tanto, la unión de ambos trabajos caracterizaba completamente la derivabilidad de la función R en todos sus puntos. El grafo de R también es un fractal, cuya dimensión de Minkowski es $5/4$ (este resultado generalizado aparece en [CC92]). La función R es por construcción 1-periódica y basta estudiar lo que ocurre en el intervalo $[0, 1]$.

Por supuesto, R no es sólo interesante por sus propiedades de diferenciabilidad, sino también por las de sus propiedades multifractales, demostradas por el matemático francés Stéphane Jaffard en 1996.

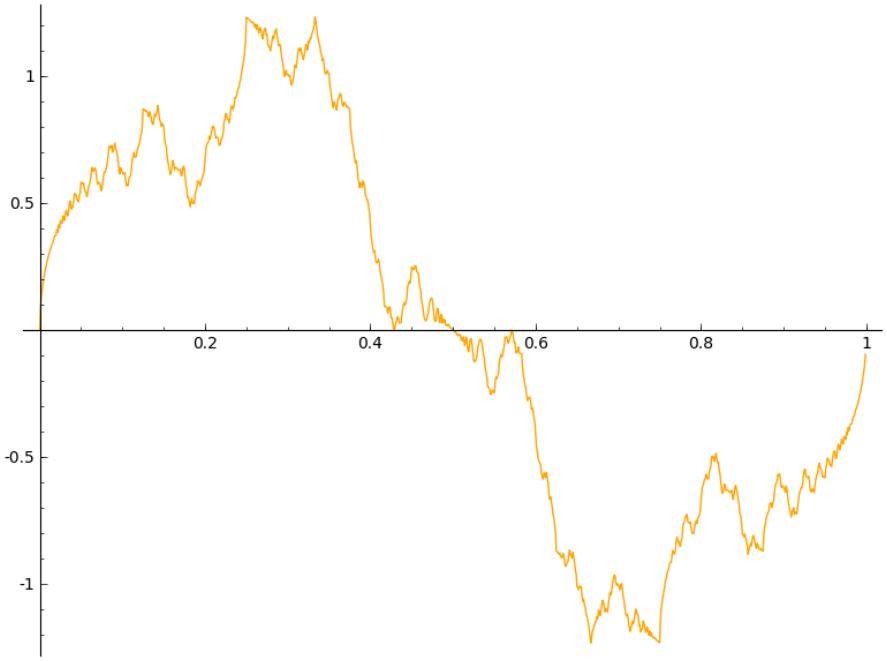

Figura 3.2: Gráfica de la función $R(x)$, conocida como *Ejemplo de Riemann*.

Teorema 3.3 (Stéphane Jaffard, [Jaf96])**.** *R es una función multifractal. En concreto, su espectro de singularidades cumple*

$$d_R(\beta) = \begin{cases} 4(\beta - 1/2), & si \quad \beta \in [1/2, 3/4] \\ 0 & si \quad \beta = 3/2 \\ indefinido, & en\ cualquier\ otro\ caso \end{cases}$$

Como puede verse en el enunciado del Teorema, la mayoría de puntos tienen exponente Hölder 3/4, pues es el único exponente cuyo conjunto de puntos tiene dimensión 1. Para exponentes entre 1/2 y 3/4, la imagen del espectro de singularidades abarca por completo el intervalo $[0, 1]$, y finalmente hay un conjunto de dimensión 0 que tiene exponente Hölder 3/2. En particular, estos serán los únicos puntos en los que la función será derivable, luego está claro que corresponden al subconjunto de los racionales que mencionábamos acerca del artículo de Gerver.

Las propiedades multifractales y de diferenciabilidad del ejemplo de Riemann son sólo la punta de un gran iceberg que ha ido emergiendo durante las últimas décadas. El mismo Jaffard amplió el cálculo del espectro de singularidades ([Jaf97], [Jaf94]) a otras funciones clásicas como la de Jordan o la de Lévy. Fernando Chamizo y Adrián Ubis estudiaron el espectro de singularidades de series exponenciales de la forma $\sum_{n=1}^{\infty} e(n^k x) n^{-\alpha}$ para enteros k mayores que 2 [CU07] y posteriormente generalizaron este problema a $\sum_{n=1}^{\infty} e\left(P(n)x\right) n^{-\alpha}$, con P un polinomio de coeficientes enteros

y grado mayor que 1 [CU12], demostrando a su vez su naturaleza multifractal. Recientemente esta propiedad ha aparecido en un trabajo [dlHV13] sobre la ecuación de filamentos de vorticidad, que está relacionada con la ecuación no lineal de Schrödinger. Las propiedades de diferenciabilidad también se han expandido a otras series de Fourier y formas automorfas ([CC99], [Cha04], [MS04]).

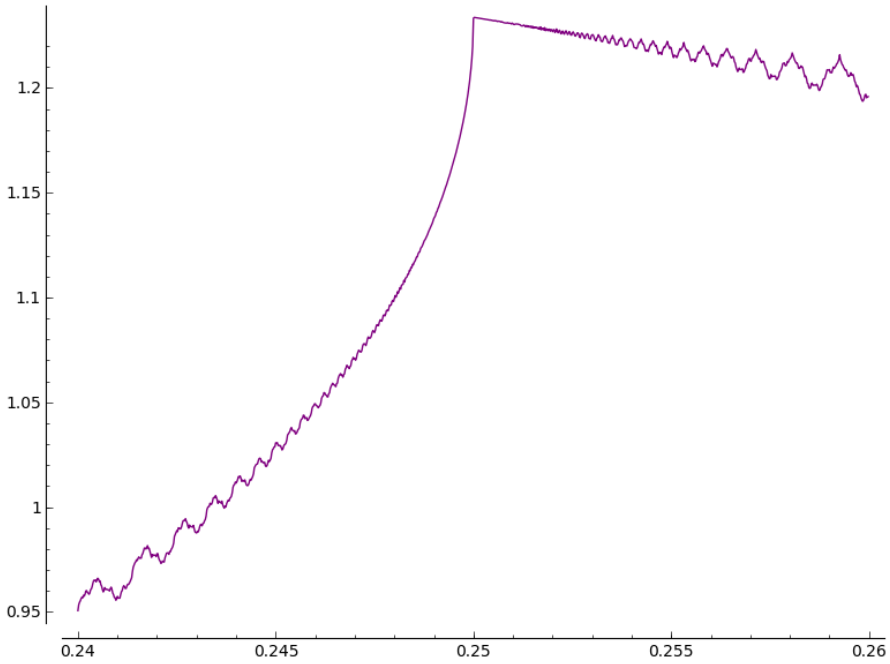

Figura 3.3: Detalle de la función $R(x)$ alrededor del punto $x = 1/4$, donde es no diferenciable.

3.2. Formas modulares. Resultado principal

A continuación haremos un breve repaso por la teoría de formas automorfas, orientada a las formas modulares clásicas que utilizaremos más adelante. Como adelantábamos al inicio de este capítulo, algunas de las definiciones que vamos a ver aparecen también, con mayor o igual detalle, al principio de la sección 2.2 del capítulo anterior, desde la página 33 hasta donde se definen las cúspides, en la página 37. Aunque los dos capítulos están diseñados para ser leídos de forma independiente, el lector puede dirigirse a tales páginas si lo desea para completar algunos detalles. A veces se apelará a resultados que aparecen allí y que ahora no serán necesarios más allá de una breve mención, como el concepto de distancia hiperbólica. Una referencia más completa sobre la estructura de los grupos $\Gamma_0(N)$ y las formas modulares asociadas a ellos es [Iwa97, §2].

Nuestro objetivo es extender el Teorema 3.3 a ciertas familias de integrales fraccionarias de formas modulares. No en vano, el ejemplo de Riemann (3.2) es precisamente la parte imaginaria de una de esas integrales fraccionarias, como veremos más adelante. Esencialmente, una forma modular es una función definida en el semiplano complejo superior $\mathbb{H} := \{z \in \mathbb{C} : \Im z > 0\}$ que verifica una identidad funcional consigo misma respecto de la acción de ciertos grupos discretos de matrices.

El *semiplano de Poincaré* es el citado semiplano $\mathbb{H}$ dotado de una métrica distinta de la euclídea (véase la página 34) de la que deriva la distancia hiperbólica ρ dada por (2.6). Constituye un modelo de variedad riemanniana compleja unidimensional con curvatura negativa. Asociado a $\mathbb{H}$, vamos a considerar el grupo $G := \mathrm{PSL}_2(\mathbb{R}) = \mathrm{SL}_2(\mathbb{R})/\{\pm I\}$ de matrices reales 2×2 con determinante 1 identificando I con $-I$. Este grupo define una acción sobre los puntos de $\mathbb{H}$, dada por

$$gz := \frac{az+b}{cz+d}, \qquad \text{para} \quad g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in G \quad \text{y} \quad z \in \mathbb{H}.$$

Esta acción está bien definida[2] y es asociativa, ya que $g(hz) = (gh)(z)$ para cualesquiera $g, h \in G$ y $z \in \mathbb{H}$. Además, toda matriz g define una isometría en $\mathbb{H}$ mediante esta acción. Denotaremos por $j_g(z)$ a la expresión $cz + d$, donde c y d dependen implícitamente de la matriz g escogida. Es fácil comprobar que, si $g, g_1 \in G$, entonces

$$\Im(gz) = \frac{\Im z}{|j_g(z)|^2} \qquad \text{y} \qquad j_g(z) j_{g_1}(gz) = j_{gg_1}(z). \tag{3.3}$$

Un *grupo fuchsiano de primera especie* es cualquier subgrupo discreto $F \subset G$ es aquel tal que todo punto de la *recta real extendida* $\widehat{\mathbb{R}} = \mathbb{R} \cup \{i\infty\}$ (que es la frontera de $\mathbb{H}$) es el punto límite (con la topología de $\mathbb{H}$) de la órbita $Fz := \{\gamma z : \gamma \in F\}$ para algún $z \in \mathbb{H}$. Un dominio fundamental de F es cualquier subconjunto conexo de $D \subset \mathbb{H}$ tal que dos puntos z_1, z_2 del interior de D no pertenezcan a la misma órbita (es decir, $\gamma z_1 \neq z_2$ para cada $\gamma \in F$) y tal que para todo punto $z \in \mathbb{H}$ exista z' en el cierre de D y $\gamma \in F$ tales que $\gamma z = z'$. Siempre se puede escoger D de modo que sea un polígono hiperbólico[3] y tal que su área sea finita, aunque no siempre D será compacto. Si no lo es, entonces tendrá al menos un vértice en la recta real extendida. A estos vértices los llamaremos *cúspides*. Fijado F, determinar sus cúspides es en principio ambiguo, ya que dependen del dominio fundamental escogido. Pero si se establece la relación de equivalencia según la cual se identifican dos cúspides $\mathfrak{a}$ y $\mathfrak{b}$ que pertenezcan a la misma órbita (es decir, tales que existe $\gamma \in F$ con $\gamma\mathfrak{a} = \mathfrak{b}$),

[2]Esta misma acción se definió en la página 34. La identificación de I y $-I$ tiene como objetivo que la acción sea fiel, es decir, que dos matrices distintas no definan la misma acción.

[3]Un polígono hiperbólico es el subconjunto de $\mathbb{H}$ delimitado por los vértices del polígono y sus lados, dados por geodésicas hiperbólicas. El lado que une dos vértices es un arco de circunferencia centrado en la recta real o, si ambos tienen la misma parte real, una recta vertical. Todos los puntos de $\mathbb{H}$ se suponen alineados verticalmente con $i\infty$.

entonces las clases de equivalencia generadas sí que dependen exclusivamente del grupo escogido F. Habitualmente representaremos una cúspide por medio de la letra $\mathfrak{a}$, y a su clase de equivalencia la denominaremos $[\mathfrak{a}]$. En este capítulo trabajaremos casi exclusivamente con la siguiente familia de grupos fuchsianos (de primera especie): Fijado un entero positivo N, se define[4]

$$\Gamma_0(N) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{PSL}_2(\mathbb{Z}) : N|c \right\}.$$

Vimos algunos ejemplos concretos de estos grupos en el capítulo anterior. En particular, $\Gamma_0(1)$ equivale a $\mathrm{PSL}_2(\mathbb{Z})$. Además es interesante notar que $\Gamma_0(N)$ estará contenido en $\Gamma_0(N')$ para $N'|N$. Para estos grupos, se sabe (véase por ejemplo [Iwa97, §2]) que el conjunto de cúspides viene dado por los racionales junto con el punto del infinito $i\infty$. Existe una fórmula para calcular el número exacto de cúspides para N arbitrario.

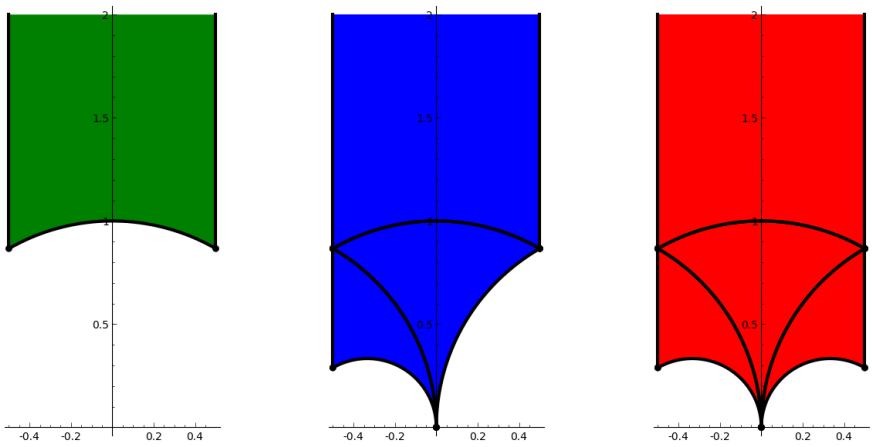

Figura 3.4: Dominios fundamentales para $\Gamma_0(1)$, $\Gamma_0(2)$ y $\Gamma_0(3)$, respectivamente.

Proposición 3.4. *Dado un entero positivo N, el grupo $\Gamma_0(N)$ posee exactamente $\sum_{vw=N} \varphi(\mathrm{mcd}(v,w))$ cúspides, donde $\varphi(n)$ es la función φ de Euler, que cuenta el número de enteros positivos menores que n y coprimos con n. Un conjunto de posibles representantes de estas clases de equivalencia viene dado por las fracciones*

$$\left\{ \frac{u}{v} : v \mid N,\ \mathrm{mcd}(u,v) = 1, u < \mathrm{mcd}(v, N/v) \right\}.$$

[4]Como ya comentábamos en el capítulo anterior, $\Gamma_0(N)$ se define habitualmente sin identificar I con $-I$. La diferencia no es significativa, al no modificarse la acción sobre $\mathbb{H}$.

En particular, si N es primo, $\Gamma_0(N)$ tendrá exactamente dos clases de equivalencia de cúspides; el único grupo que tiene una sola es $\Gamma_0(1)$ (véanse las Figuras 3.4 sobre estas línea y 3.6 en la página 90). Esta Proposición es un resultado conocido y puede consultarse por ejemplo en [Iwa97, §2.4].

Ya estamos preparados para introducir de forma rigurosa las formas modulares en nuestro contexto.

Definición 3.5. *Dado $r > 0$ y un entero positivo N, una* forma modular *de peso r con respecto del grupo $\Gamma_0(N)$ es una función $f : \mathbb{H} \longrightarrow \mathbb{C}$ holomorfa en $\mathbb{H}$ y en todas las cúspides*[5] *de $\Gamma_0(N)$ que verifica la siguiente identidad:*

$$f(\gamma z) = w_\gamma \left(j_\gamma(z)\right)^r f(z), \qquad \textit{para} \quad \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N), z \in \mathbb{H}. \tag{3.4}$$

Donde w_γ es un sistema de multiplicadores *que en particular siempre toma valores complejos de módulo* 1 [Iwa97, §2.6].

Definición 3.6. *En las condiciones de la Definición anterior, se dirá que f es* cuspidal *en una cúspide $\mathfrak{a}$ si la función decae exponencialmente al ser evaluada arbitrariamente cerca de dicha cúspide. Si f es cuspidal en todas las cúspides de $\Gamma_0(N)$, se dice que f es una* forma cuspidal.

Bajo las hipótesis de la Definición 3.5, la función f admitirá [Iwa97, §2.7] el siguiente desarrollo de Fourier:

$$f(z) = \sum_{n=0}^{\infty} a_n e(nz), \tag{3.5}$$

para ciertos coeficientes complejos $\{a_j\}_{j\geq 0}$. Con este desarrollo está claro que f será cuspidal en $i\infty$ si y sólo si el coeficiente a_0 es igual a cero. Siempre que f no sea idénticamente nula, podemos definir su integral fraccionaria, $f_\alpha : \mathbb{R} \longrightarrow \mathbb{C}$, de la siguiente forma:

$$f_\alpha(x) = \sum_{n=1}^{\infty} \frac{a_n}{n^\alpha} e(nx), \qquad r < \alpha < r + 1/2. \tag{3.6}$$

La condición de que α sea mayor que r resulta natural para que la serie que define a f_α sea convergente, ya que los coeficientes de f verifican [Cha04]

$$\sum_{n\leq N} a_n e(nx) = \mathcal{O}\left(N^r \log N\right)$$

[5] Consúltese la fórmula (3.13).

uniformemente en x. Esta cota puede mejorarse si se imponen condiciones adicionales a f, como por ejemplo, que sea una forma cuspidal, pero no el caso general. La cota superior $\alpha < r + 1/2$ no es estrictamente necesaria y puede ampliarse, a costa de modificar sensiblemente las condiciones a las que nos enfrentaremos en las siguientes secciones. Es el momento de aclarar por qué dijimos que queríamos *extender* el resultado de Jaffard a otras funciones similares. La función R está relacionada con una forma modular como las que hemos descrito; la función θ de Jacobi[6]:

$$\theta(z) := \sum_{n=-\infty}^{\infty} e(n^2 z), z \in \mathbb{H}.$$

Es ésta una forma modular de peso $1/2$ sobre el grupo $\Gamma_0(4)$ [BS86]. Y puede expresarse como en la Definición 3.5 sin más que tomar $a_0 = 1$, $a_n = 2$ en los cuadrados perfectos y 0 en el resto de enteros. Tras escribirla de esta forma, R corresponde a la mitad de la parte imaginaria de la integral fraccionaria de θ que se obtiene tomando[7] $\alpha = 1$.

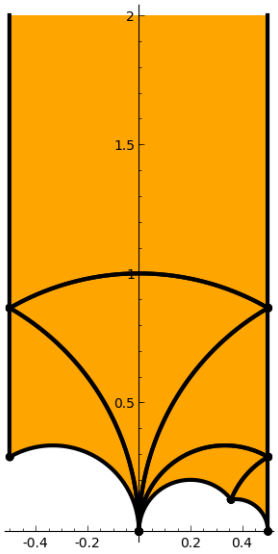

Figura 3.5: Un dominio fundamental para el grupo $\Gamma_0(4)$. Este grupo posee tres clases de equivalencia de cúspides, representadas aquí por los vértices 0, $1/2$ e $i\infty$.

Con la introducción de las formas modulares hemos recopilado todas las herramientas que necesitábamos para poder enunciar el Teorema principal de este capítulo.

[6]Frecuentemente, la función θ aparece normalizada de otras formas diferentes a la que hemos utilizado aquí.

[7]En la Introducción tomábamos $\alpha = 2$ para obtener la función R, pero no hay contradicción. Al escribir la función θ como en (3.5), el parámetro α se divide por 2.

Teorema 3.7. *Sea f una forma modular* no cuspidal *de peso $r \in (0,1)$ con respecto al grupo $\Gamma_0(N)$, para un entero positivo fijado N. Sea $\alpha < 1$ verificando $r < \alpha < r + 1/2$ y sea f_α la integral fraccionaria de f dada por* (3.6)*. Entonces, el espectro de singularidades de f_α cumple lo siguiente:*

$$d_{f_\alpha}(\beta) = \frac{2(\beta - \alpha + r)}{r}, \qquad \textit{para} \qquad \alpha - r < \beta < \alpha - r/2. \tag{3.7}$$

Luego bajo ciertas restricciones de tamaño para α y r, todas las integrales fraccionarias que se obtengan de formas modulares con peso menor que 1 verifican un resultado similar al Teorema 3.3. Las formas cuspidales se excluyen porque no son multifractales; por el Teorema 2.1 de [Cha04], si f es una forma cuspidal de peso r y $\alpha - r/2 < 1$, entonces todo x verifica[8]

$$\begin{aligned} f_\alpha(x+h) - f_\alpha(x) &= \mathcal{O}\left(|h|^{\alpha - r/2} \log |h|\right), \\ f_\alpha(x+h) - f_\alpha(x) &= \Omega\left(|h|^{\alpha - r/2}\right). \end{aligned}$$

Por tanto, el orden Hölder de f_α es $\alpha - r/2$ en todos los puntos, y el espectro de singularidades toma un único valor.

A lo largo de las dos siguientes secciones probaremos el Teorema 3.7, en dos etapas bien diferenciadas.

- En primer lugar, valiéndolos de las propiedades modulares de f y de su relación con f_α deduciremos varias fórmulas asintóticas para el incremento $f_\alpha(x+h) - f_\alpha(x)$ cuando x es cualquier número irracional y h tiende a 0. Estas fórmulas aparecen en la Proposición 3.9 (página 77).

- A continuación, nos valdremos de la teoría de aproximación diofántica y del Teorema de Jarník-Besicovitch para obtener de esas fórmulas el exponente Hölder de cada posible punto x, en las Proposiciones 3.13 y 3.17 (a partir de la página 88).

Estas tres Proposiciones son los resultados clave que nos permitirán demostrar el Teorema 3.7 al final del capítulo (página 96), junto con algunas observaciones sobre qué podría ocurrir con otros valores de r y α y ejemplos de algunas formas modulares de peso comprendido entre 0 y 1. Antes de finalizar esta sección, vamos a ver un Lema técnico que contiene varios resultados sobre el tamaño de las formas modulares.

[8] La notación $f(x) = \Omega(g(x))$ indica que no se cumple $f(x) = o(g(x))$, y por tanto f no puede ser de orden inferior a g.

Lema 3.8. *Sea $z := x + iy \in \mathbb{H}$ y f una forma modular cumpliendo las hipótesis de la Definición 3.5. Sea $[\mathfrak{a}]$ una clase de equivalencia de cúspides y a/q una fracción irreducible perteneciente a dicha clase. Existe entonces una matriz $M \in \mathrm{PSL}_2(\mathbb{R})$ tal que $\Im Mz = Ky|qz-a|^{-2}$ con K una constante no nula que sólo depende de la clase $[\mathfrak{a}]$ y tal que $f(z)$ puede expresarse como*

$$f(z) = (qz-a)^{-r} F(Mz), \tag{3.8}$$

donde $F : \mathbb{H} \longrightarrow \mathbb{C}$ es una función que verifica las siguientes cotas:

$$F(z) \ll 1 + (\Im z)^{-r}, \tag{3.9}$$

$$F'(z) \ll 1 + (\Im z)^{-r-1}. \tag{3.10}$$

Además, existen constantes $A \in \mathbb{C}$ y $C > 0$ que sólo dependen de la clase $[\mathfrak{a}]$ tales que A es nula si y sólo si f es cuspidal en la clase $[\mathfrak{a}]$ y

$$F(z) - A, F'(z) \ll e^{-C(\Im z)} \qquad si\ \Im z \leq 1. \tag{3.11}$$

Demostración: Como vimos en la Proposición 3.4, el número de clases de equivalencia de cúspides para $\Gamma_0(N)$ es finito. Podemos tomar para cada una de estas clases un representante, siendo necesario que estén fijado de antemano. Llamaremos a'/q' al representante de la clase $[\mathfrak{a}]$ a la que pertenece a/q. Si $\Gamma_0(N)$ tuviera una sola clase de equivalencia de cúspides, en particular existiría una matriz $\gamma \in \Gamma_0(N)$ que llevase a/q al punto del infinito. Y aprovechando la relación modular,

$$f(z) = w_\gamma \left(j_\gamma(z)\right)^{-r} f(\gamma z) \tag{3.12}$$

$\Im(\gamma z)$ sería proporcional a $|z - a/q|^{-1}$, por lo que debería tomar valores arbitrariamente grandes. Como ya sabemos, que haya una sola cúspide sólo es posible en el caso $N = 1$, luego no podemos tomarlo como hipótesis. Por ello vamos a utilizar el *desarrollo en la cúspide*, que en cierto sentido generaliza (3.12). Dada una cúspide $\mathfrak{a} \in \{\mathbb{Q} \cup i\infty\}$, se dirá que $\sigma_\mathfrak{a} \in PSL_2(\mathbb{R})$ es una *matriz de escala* para $\mathfrak{a}$ si $\sigma_\mathfrak{a}\infty = \mathfrak{a}$ y si existe algún generador g del grupo de estabilidad $F_\mathfrak{a} = \{\gamma \in \Gamma_0(N) : \gamma\mathfrak{a} = \mathfrak{a}\}$ tal que $\sigma_\mathfrak{a}^{-1} g \sigma_\mathfrak{a} = T$, donde T es la traslación unidad. Para cada matriz de escala $\sigma_\mathfrak{a}$, la función f admite el siguiente desarrollo[9] [Cha04]:

$$f(\sigma_\mathfrak{a} z) = \left(j_{\sigma_\mathfrak{a}}(z)\right)^r \sum_{n=0}^{\infty} a_n^\mathfrak{a} e\left((n + \kappa_\mathfrak{a})z\right). \tag{3.13}$$

Los coeficientes $a_n^\mathfrak{a}$ no varían dentro de una misma clase de equivalencia, salvo por un factor de módulo 1 constante para todo n que depende de la matriz de escala escogida.

[9] La fórmula (3.13) corresponde al desarrollo de la función $g(q)$ de [Iwa97, §2.7]. La función f es holomorfa en la cúspide $\mathfrak{a}$ si g lo es en $q = 0$.

El factor $\kappa_{\mathfrak{a}}$ sí es constante dentro de cada clase de equivalencia, y cumple $0 \leq \kappa_{\mathfrak{a}} < 1$. Vamos a utilizar de forma conjunta (3.12) y (3.13), y para ello nos apoyaremos en el representante fijo a'/q' de $[\mathfrak{a}]$ que mencionábamos antes. Tomemos una matriz $\gamma \in \Gamma_0(N)$ tal que $\gamma \frac{a}{q} = \frac{a'}{q'}$. La existencia de γ está garantizada por pertenecer a/q y a'/q' a la misma clase de equivalencia. Ahora bien, si z está cerca de a/q, entonces en (3.12), $f(\gamma z)$ ha de estar cerca de a'/q' y vamos a ser capaces de acotar el valor de $f(\gamma z)$ a partir de (3.13). Denotando $\mathfrak{a} := a'/q'$ se cumple $\sigma_{\mathfrak{a}}^{-1} \frac{a'}{q'} = \infty$. Cambiando z por $\sigma_{\mathfrak{a}}^{-1}(z)$ a ambos lados en (3.13) y utilizando que $j_{\sigma_{\mathfrak{a}}}(\sigma_{\mathfrak{a}}^{-1} z) = \left(j_{\sigma_{\mathfrak{a}}^{-1}}(z)\right)^{-1}$ (que es consecuencia de (3.3)), se tiene

$$f(z) = \left(j_{\sigma_{\mathfrak{a}}^{-1}}(z)\right)^{-r} \sum_{n=0}^{\infty} a_n^{\mathfrak{a}} e((n+\kappa_{\mathfrak{a}})\sigma_{\mathfrak{a}}^{-1} z). \tag{3.14}$$

Ahora desarrollamos $f(\gamma z)$ utilizando (3.14), con lo que (3.12) se convierte en

$$f(z) = w_\gamma \left(j_\gamma(z)\right)^{-r} \left(j_{\sigma_{\mathfrak{a}}^{-1}}(\gamma z)\right)^{-r} \sum_{n=0}^{\infty} a_n^{\mathfrak{a}} e\left((n+\kappa_{\mathfrak{a}})\sigma_{\mathfrak{a}}^{-1}(\gamma z)\right). \tag{3.15}$$

El producto de los dos operadores j equivale, gracias a (3.3), a $\left(j_{\sigma_{\mathfrak{a}}^{-1}\gamma}(z)\right)^{-r}$. La matriz $\sigma_{\mathfrak{a}}^{-1}\gamma$ lleva a/q al punto del infinito, por lo que $j_{\sigma_{\mathfrak{a}}^{-1}\gamma}(z)$ debe ser igual a $qz - a$, salvo el producto por una constante. Las posibles matrices $\sigma_{\mathfrak{a}}^{-1}$ vienen dadas [Cha04] por

$$\sigma_{\mathfrak{a}}^{-1} = \begin{pmatrix} Cp & Cs \\ q'/C & -a'/C \end{pmatrix},$$

donde p y s son enteros cualesquiera tales que $pa' + sq' = -1$ y C es un parámetro denominado *anchura* de la cúspide a/q, cuyo valor viene dado por [Iwa97, §2.4] $C^2 = N/\mathrm{mcd}(N, q'^2)$. En particular es no nulo y a todos los efectos lo podemos considerar como una constante acotada de forma asboluta por N. Utilizando esto, es fácil comprobar que $j_{\sigma_{\mathfrak{a}}^{-1}\gamma}(z) = C^{-1}(qz - a)$. Así pues,

$$f(z) = (qz-a)^{-r}(C^r w_\gamma) \sum_{n=0}^{\infty} a_n^{\mathfrak{a}} e\left((n+\kappa_{\mathfrak{a}})\sigma_{\mathfrak{a}}^{-1}(\gamma z)\right) =: (qz-a)^{-r} F(z),$$

para

$$F(z) = (C^r w_\gamma) \sum_{n=0}^{\infty} a_n^{\mathfrak{a}} e((n+\kappa_{\mathfrak{a}})z) \quad \text{y} \quad M = \sigma_{\mathfrak{a}}^{-1}\gamma. \tag{3.16}$$

Esto coincide con (3.8). Puesto que la serie que define a F ha de ser convergente por su relación con $f(z)$ en (3.8), es evidente que $F(z) \ll 1$. Utilizando esto en (3.8), debe cumplirse

$$f(z) \ll |qz-a|^{-r} \qquad \text{si} \quad \Im(Mz) = \frac{y}{|qz-a|^2} \geq 1. \tag{3.17}$$

En particular, tomando $a/q = 0/1$, de (3.17) se deduce $f(x+iy) \ll y^{-r}$ cuando y sea menor que 1. Esto nos va a permitir dar también una cota para $f'(x+iy)$, de nuevo para valores pequeños de y. Sea C la circunferencia centrada en $x+iy$ y de radio $y/2$. Utilizando la Fórmula integral de Cauchy,

$$f'(x+iy) \ll \int_C \frac{f(w)}{(w-z)^2}\, dw \ll 2\pi \frac{y}{2} \frac{(y/2)^{-r}}{(y/2)^2} \ll y^{-r-1}. \tag{3.18}$$

Empleando (3.18), ahora vamos a ver que se cumplen las distintas cotas especificadas sobre F y su derivada. Para probar (3.9), basta ver entonces que $F(z) \ll (\Im z)^{-r}$ cuando $\Im z \ll 1$. Tomemos, para cada representante de una de las clases de equivalencia de cúspides, una matriz de escala fija. Tomando una genérica σ_0 y por la definición de F, por (3.13) se cumple

$$F(z) = (j_{\sigma_0}(z))^{-r}\, f(\sigma_0 z). \tag{3.19}$$

Utilizando que $j_{\sigma_0}(z)$ y $f(\sigma_0 z)$ son 1-periódicos y que el primero de ellos se puede expresar como $Cz+D$ para ciertos coeficientes reales C y D, puede entonces tomarse un entero k tal que, si $y \ll 1$, $j_{\sigma_0}(z+k) = (C(x+k)+D)^2 + (Cy)^2 \asymp 1$ (siendo aquí esencial el que el número de matrices de escala y por tanto de sus coeficientes es finito y están además fijadas de antemano) y, por tanto $\Im \sigma_0(z+k) \asymp y$. De (3.19) se deduce $F(z) \ll y^{-r}$, que completa la prueba de (3.9). Por otro lado, la derivada de F es

$$F'(z) = rC \left(j_{\sigma_0(z)}\right)^{-r-1} f(\sigma_0 z) + \left(j_{\sigma_0(z)}\right)^{-r-2} f'(\sigma_0 z). \tag{3.20}$$

Replicando el proceso del párrafo anterior, el primer sumando de (3.20) se acota de nuevo por $(\Im z)^{-r}$. El segundo, utilizando (3.18), se acota por $(\Im z)^{-r-1}$. Y la cota $F'(z) \ll 1$ es inmediata al derivar (3.16), gracias a que el factor n que aparece al derivar es de orden claramente inferior al de la exponencial que aparece en la serie.

Queda únicamente por probar (3.11). En la expresión (3.16) puede apreciarse que, si la clase $[\mathfrak{a}]$ verifica $\kappa_{\mathfrak{a}} \neq 0$ o $a_0^{\mathfrak{a}} = 0$, f tendrá decaimiento exponencial en a/q (será por tanto cuspidal en $[\mathfrak{a}]$). En ese caso, la cota exponencial para $F(z)$ será inmediata. Si f es no cuspidal en $\mathfrak{a}$, entonces $\kappa_{\mathfrak{a}} = 0 \neq a_0^{\mathfrak{a}}$ con lo que el término con $n = 0$ en (3.16) será una constante que evitará el decaimiento exponencial. Cuando estemos en ese caso, es preciso extraer tal término y para ello definimos

$$A = \begin{cases} w_\gamma a_0^{\mathfrak{a}}, & \text{si } \kappa_{\mathfrak{a}} = 0, \text{ y } a_0^{\mathfrak{a}} \neq 0 \\ 0 & \text{en cualquier otro caso.} \end{cases} \tag{3.21}$$

Una vez hecho esto, está claro que la serie que define $F(z) - A$ puede acotarse por una exponencial que depende del tamaño de $\Im z$. En el caso de la derivada, basta con notar que el término en $n = 0$ desaparece al derivar, y añadir un factor n no modifica la convergencia. Esto concluye la prueba de la cota (3.11) y completa la demostración del Lema. □

3.3. Cálculo del orden Hölder

Obsérvese que para todas las funciones f_α que verifiquen las hipótesis del Teorema 3.7, los exponentes Hölder involucrados estarán acotados por $\alpha - r + r/2 < (1+r)/2$. En particular, todos serán menores que 1, y por tanto podremos utilizar la fórmula (3.1) para calcularlos. Es decir, queremos estudiar el comportamiento de la diferencia

$$f_\alpha(x+h) - f_\alpha(x) \tag{3.22}$$

cuando h tiende a 0 por la izquierda o por la derecha y x es cualquier irracional (los racionales constituyen un conjunto numerable y por tanto de dimensión cero). Para ello, a lo largo de este capítulo probaremos el siguiente resultado:

Proposición 3.9. *Sea f_α una integral fraccionaria dada por (3.6) para una forma modular f de peso $0 < r < 1$ con respecto al grupo $\Gamma_0(N)$. Sea $1/2 < \alpha < 1$ dado, con $r < \alpha < r + 1/2$. Sea $x \in [0,1] \setminus \mathbb{Q}$ y $h \neq 0$. Sea $[\mathfrak{a}]$ una clase de equivalencia de cúspides de $\Gamma_0(N)$ y a/q una fracción irreducible perteneciente a esta clase tal que $|h|, |\delta| \leq q^{-2}$, donde $\delta := x - a/q$. Entonces se cumple la siguiente fórmula asintótica*

$$f_\alpha(x+h) - f_\alpha(x) = \Lambda \frac{(\delta+h)^{\alpha-r} - \delta^{\alpha-r}}{q^r} + \mathcal{O}\left(|h|^{2\alpha-2r} q^{2\alpha-3r}\right), \tag{3.23}$$

donde $\Lambda = \Lambda_{\alpha,r,\mathfrak{a}}$ es una constante que sólo depende de α, r y la clase de equivalencia $[\mathfrak{a}]$ a la que pertenece a/q y que es nula si y sólo si f es cuspidal en a/q. En las mismas condiciones también se cumple

$$f_\alpha(x+h) - f_\alpha(x) = \mathcal{O}\left(|h||\delta|^{\alpha-r-1} q^{-r} + |h|^{2\alpha-2r} |\delta|^r q^{2\alpha-r}\right), \qquad \text{si } |h| < |\delta|. \tag{3.24}$$

Aunque (3.23) es válida sin suponer ninguna relación de tamaño entre h y δ, en la práctica no resultará útil cuando $|h|$ sea menor que $|\delta|$ (véase la prueba de la Proposición 3.13 en la página 88), y por ello será necesario recurrir también a (3.24), en la que se esquiva el término de error de (3.23). Demostraremos estas dos fórmulas al final de esta sección (a partir de la página 84) a través de dos Lemas intermedios que demostraremos antes.

Se dan dos hechos que resultarán cruciales para llegar a las fórmulas de la Proposición 3.9. El primero de ellos es la estrecha relación que guarda cada f_α con la función de la que proviene, f. Partiendo de la llamada *integral Gamma*,

$$\frac{\Gamma(\alpha)}{(2\pi n)^\alpha} = \int_0^\infty t^{\alpha-1} e^{-2\pi n t}\, dt, \quad \alpha > 0,$$

(que se obtiene mediante un cambio de variable en la definición habitual de la función Gamma), se puede introducir $n^{-\alpha}$ en cada coeficiente de la forma modular f [Cha04] y llegar a la relación

$$f_\alpha(x) = \frac{\Gamma(\alpha)}{(2\pi)^\alpha} \int_0^\infty t^{\alpha-1} f(x+it)\, dt, \quad x \in \mathbb{R}. \tag{3.25}$$

Esto nos permite expresar la diferencia (3.22) como una integral que engloba a f evaluada en dos puntos diferentes. El segundo hecho clave es que todo número irracional *se aproxima bien* por racionales. En concreto, siguiendo la notación del enunciado de la Proposición 3.9, fijado x irracional siempre habrá fracciones tales a/q que $|\delta|$ sea menor q^{-2}. Ahondaremos más sobre este hecho en la cuarta sección, pero es importante mencionarlo ahora porque desde el principio nuestro objetivo será buscar fracciones cuya distancia a x sea suficientemente pequeña para reescribir (3.22) únicamente en términos de evaluaciones de f_α muy cerca de valores racionales, o dicho de otro modo, muy cerca de *cúspides*. En este sentido, dada una fracción irreducible a/q cualquiera y suponiendo fijos x y h, definimos la siguiente expresión:

$$\Delta \;:=\; f_\alpha\left(\frac{a}{q}+(\delta+h)\right)-f_\alpha\left(\frac{a}{q}+\delta\right), \qquad \text{para } \delta := x-a/q. \tag{3.26}$$

Δ no es más que una forma compacta de escribir $f_\alpha(x+h)-f_\alpha(x)$. Depende implícitamente de f_α, así como de x, h y la fracción a/q, pero resulta útil para simplificar una notación que de otro modo llegaría a ser algo farragosa. La fracción a/q se escoge a posteriori en función del valor de x y de h, debiendo cumplir una serie de requisitos (los mencionados en la Proposición 3.9). De hecho, a medida que se haga tender a h a 0, en realidad se escogerá toda una sucesión de fracciones $\{a_n/q_n\}_{n\geq 1}$ relacionadas con la fracción continua y los convergentes de x. Las sucesivas diferencias δ_n que se generen no serán necesariamente menores o mayores que h; lo normal es que ambas posibilidades ocurran infinitas veces. Además, al igual que h, δ tampoco tendrá un signo concreto al poder aproximarse a x por la derecha o por la izquierda. Por tanto, $h+\delta$ y δ, pueden también tener signos distintos. Estas varaciones (especilamente las de tamaño) causarán que sea necesario adoptar simultáneamente dos estrategias, dadas por las fórmulas (3.23) y (3.24). Utilizando (3.25), podemos describir Δ como una integral compleja que depende de la función f. Abreviando $C_\alpha = (2\pi)^\alpha/\Gamma(\alpha)$,

$$\Delta \;=\; C_\alpha \int_0^\infty t^{\alpha-1}\left[f\left(\frac{a}{q}+(\delta+h)+it\right)-f\left(\frac{a}{q}+\delta+it\right)\right]dt \tag{3.27}$$

En primer lugar, vamos a demostrar que el peso de la integral está concentrado en el intervalo $[h^2q^2, q^{-2}]$. Sea

$$\Delta' \;=\; C_\alpha \int_{h^2q^2}^{q^{-2}} t^{\alpha-1}\left[f\left(\frac{a}{q}+(\delta+h)+it\right)-f\left(\frac{a}{q}+\delta+it\right)\right]dt$$

La razón básica para que se hayan escogido estos límites de integración es que el primero de ellos es h multiplicado por hq^2 y el segundo es h dividido por esa misma cantidad; la utilidad de esto puede aprecirse sobre todo en la demostración de la Proposición 3.11 (concretamente, véase la fórmula (3.36)). En primer lugar, vamos a ver el siguiente resultado:

Lema 3.10. *Bajo las hipótesis de la Proposición 3.9,* Δ *y* Δ' *verifican*

$$\Delta = \Delta' + \mathcal{O}\left(|h|^{2\alpha-2r}|\delta|^r q^{2\alpha-r} + |h|q^{2-2\alpha+r}\right). \tag{3.28}$$

Demostración: Comenzamos acotando (3.27) en el rango $0 \leq t \leq h^2q^2$. Nótese que, como estamos suponiendo $|h| \leq q^{-2}$, en particular todos los valores de t serán menores que $|h|$. Para dichos valores vamos a acotar individualmente cada uno de los dos sumandos dentro de la integral. Probaremos, en primer lugar,

$$f(z) \ll \begin{cases} |qz-a|^{-r} & \text{si } y \geq |qz-a|^2 \\ |qz-a|^r y^{-r} & \text{si } y \leq |qz-a|^2, \end{cases} \tag{3.29}$$

de donde se deduce que, sin restricciones sobre t,

$$f(a/q + \varepsilon + it) \ll q^{-r}|\varepsilon + it|^{-r} + q^r|\varepsilon + it|^r t^{-r}. \tag{3.30}$$

La primera desigualdad ya apareció en la Demostración del Lema 3.8. Partiendo de (3.8), se tiene que $\Im Mz \geq 1$ equivale a $y \geq |qz-a|^2$, y en ese caso se cumplirá $F(Mz) \ll 1$. Para la segunda utilizamos que, si $\Im Mz$ es menor que 1 (o lo que es lo mismo, si y es menor que $|qz-a|^2$), entonces $F(Mz)$ podrá acotarse por $(\Im Mz)^{-r}$. Sustituyendo el valor de $\Im Mz$ en (3.8), se prueba la segunda desigualdad y se completa la prueba de (3.29).

Volvamos a (3.30), donde distinguiremos casos según el tamaño de $|h|$ y $|\delta|$. Si $|\delta|$ es mayor que h^2q^2, entonces $|\delta + h + it|, |\delta + it| \sim \delta$. Y en ese caso:

$$f(a/q + (\delta+h) + it) - f(a/q + \delta + it) \ll (q|\delta|)^{-r} + (q|\delta|)^r t^{-r} \ll (q|\delta|)^r t^{-r},$$

siendo la última iguladad consecuencia de que $t < (q|h|)^2 < (q|\delta|^2)$. Por tanto,

$$C_\alpha \int_0^{h^2q^2} t^{\alpha-1}\left[f\left(\frac{a}{q} + (\delta+h) + it\right) - f\left(\frac{a}{q} + \delta + it\right)\right] dt \ll_\alpha |h|^{2\alpha-2r}|\delta|^r q^{2\alpha-r},$$

que es coherente con (3.28). Por otro lado, si $|\delta| \leq h^2q^2$ (que en particular implica $|\delta| \leq |h|$), se tiene

$$f(a/q + (\delta+h) + it) \ll q^{-r}|h|^{-r} + q^r|h|^r t^{-r} \ll q^r|h|^r t^{-r} \tag{3.31}$$

y

$$f(a/q + \delta + it) \ll \begin{cases} q^{-r}|\delta|^{-r} + q^r|\delta|^r t^{-r} \ll q^r|\delta|^r t^{-r} \ll q^r & \text{si } t < |\delta| \\ q^{-r}t^{-r} + q^r \ll q^r & \text{si } t \geq |\delta| \end{cases}$$

Como $|h| \geq t$, claramente (3.31) es de orden mayor. Por tanto, sólo hace falta que integremos ése término, obteniendo

$$C_\alpha \int_0^{h^2q^2} t^{\alpha-1}\left[f\left(\frac{a}{q} + (\delta+h) + it\right) - f\left(\frac{a}{q} + \delta + it\right)\right] dt \ll_\alpha |h|^{2\alpha-r}q^{2\alpha-r},$$

y este término de error es de orden inferior al primero de (3.28), pues $|h|^{-r} < |\delta|^{-r}$.

Veamos ahora cómo acotar (3.27) en el otro rango exterior, $q^{-2} \leq t < \infty$. En primer lugar, representamos la diferencia entre los dos sumandos como la integral de f', de la siguiente forma:

$$C_\alpha \int_{q^{-2}}^{\infty} t^{\alpha-1} \left[f\left(\frac{a}{q} + (\delta+h) + it\right) - f\left(\frac{a}{q} + \delta + it\right)\right] dt = C_\alpha \int_{\delta}^{\delta+h} \left[\int_{q^{-2}}^{\infty} t^{\alpha-1} f'\left(\frac{a}{q} + u + it\right) dt \right] du. \tag{3.32}$$

Para acotar $f'(a/q+u+it)$ vamos a representar f como en la fórmula (3.8) del Lema 3.8. Derivando esa fórmula se cumple

$$f'(z) = -rq(qz-a)^{-r-1}F(Mz) + (qz-a)^{-r-2}F'(Mz),$$

donde $q(a/q+u+it)-a = q(u+it) \asymp qt$. Como $\Im M(a/q+u+it) = t\,(q(u+it))^{-2} \asymp q^{-2}t^{-1} \leq 1$ podemos utilizar (3.9) y deducir

$$f'\left(\frac{a}{q} + u + it\right) \ll q(qt)^{-r-1}(q^2t)^r + (qt)^{-r-2}(q^2t)^{r-1} \ll q^r t^{-1}.$$

Y por tanto, (3.32) puede acotarse por $|h|q^{-r}\int_{q^{-2}}^{\infty} t^{\alpha-2}\,dt \ll |h|q^{2-2\alpha+r}$, que es uno de los términos de error que figuran en (3.28). □

Lema 3.11. *Bajo las hipótesis de la Proposición 3.9, Δ' verifica*

$$\Delta' = \Lambda \frac{(\delta+h)^{\alpha-r} - \delta^{\alpha-r}}{q^r} + \mathcal{O}\left(|h|^{2\alpha-2r}q^{2\alpha-3r} + |h|q^{2-2\alpha+r}\right), \tag{3.33}$$

donde Λ es la misma constante que en la Proposición 3.9. En las mismas condiciones, también se cumple

$$\Delta' = \mathcal{O}\left(|h||\delta|^{\alpha-r-1}q^{-r} + |h|^{2\alpha-2r}|\delta|^r q^{2\alpha-r}\right), \qquad si\ |h| < |\delta|. \tag{3.34}$$

Demostración: De forma análoga a (3.32), se tiene

$$\Delta = C_\alpha \int_{h^2q^2}^{q^{-2}} t^{\alpha-1} \left[f\left(\frac{a}{q} + (\delta+h) + it\right) - f\left(\frac{a}{q} + \delta + it\right)\right] dt = C_\alpha \int_{\delta}^{\delta+h} \left[\int_{h^2q^2}^{q^{-2}} t^{\alpha-1} f'\left(\frac{a}{q} + u + it\right) dt \right] du. \tag{3.35}$$

Según la notación del Lema 3.8, volvemos a expresar la derivada $f'(z)$ como $rq(qz-a)^{-r-1}F(Mz)+(qz-a)^{-r-2}F'(Mz)$. Esta expresión podrá acotarse satisfactoriamente para $h^2q^2 \leq t \leq q^{-2}$, gracias a que

$$\Im\left(M(\frac{a}{q}+u+it)\right) = \frac{t}{q^2|u+it|^2} \sim \begin{cases} \frac{t}{q^2|h|^2} \geq \frac{1}{|h|q^2} & \text{, si } t \leq |h| \\ \frac{1}{q^2 t} & \text{, si } t \geq |h|. \end{cases} \tag{3.36}$$

Como vimos en la prueba de la fórmula (3.11) del Lema 3.8, la serie que define a $F(Mz)$ podrá acotarse por una exponencial siempre que $\Im(Mz)$ sea suficientemente grande (como es nuestro caso) y que f sea cuspidal en $[\mathfrak{a}]$. Incluso si no lo es, podremos conseguir esa misma cota sustrayendo la constante A dada por (3.21) (que recordemos, se define como cero para el caso cuspidal). Por tanto, partiremos de

$$f'(z) = rq(qz-a)^{-r-1}A + rq(qz-a)^{-r-1}\left[F(Mz)-A\right] + (qz-a)^{-r-2}F'(Mz).$$

Es importante separar el primero de estos tres sumandos. Bajo ciertas condiciones especiales (que A sea distinta de cero y que h tome una serie de valores especiales para los que $(|h|q^2)^{-1}$ sea arbitrariamente grande), esa separación será crucial para demostrar la Proposición 3.17. Gracias a (3.11) y (3.36),

$$f'\left(\frac{a}{q}+u+it\right) = Arq^{-r}\frac{1}{(u+it)^{r+1}} + \mathcal{O}\left(\frac{e^{q^{-2}t^{-1}}}{q^r(u+it)^{r+1}}\right) \tag{3.37}$$

Utilizando esta fórmula asintótica en (3.35), se obtiene un término principal,

$$\begin{aligned} \Delta'' &= \frac{Ar}{q^r}\int_{\delta}^{\delta+h}\left(\int_{h^2q^2}^{q^{-2}}\frac{t^{\alpha-1}}{(u+it)^{1+r}}\,dt\right)du \\ &= \frac{Ar}{q^r}\int_{\delta}^{\delta+h} u^{\alpha-r-1}\left(\int_{h^2q^2u^{-1}}^{q^{-2}u^{-1}}\frac{t^{\alpha-1}}{(1+it)^{1+r}}\,dt\right)du, \end{aligned} \tag{3.38}$$

más otro de error que acotaremos más tarde. Por analogía con (2.14) la integral interior en la expresión de la derecha, $\int_0^\infty t^{\alpha-1}(1+it)^{-1-r}\,dt$, define algo muy similar a una función Beta, salvo porque los límites de integración no son 0 e ∞ y por la presencia de una i multiplicando a t en el denominador. Aun así, parece asequible modificar (3.38) para conseguir un término exacto que dependa de esa función Beta, junto con algunos términos de error que deberían ser de orden inferior. En primer lugar, vamos a realizar el cambio de variable que lleva t a it para librarnos de la i. Como la función dentro de la integral únicamente tiene un polo en $t=iu$, podemos escribir

$$\int_0^R \frac{t^{\alpha-1}}{(1+it)^{1+r}}\,dt = -\int_{-iR}^0 \frac{t^{\alpha-1}}{(1+it)^{1+r}}\,dt - \int_{\gamma_R}\frac{t^{\alpha-1}}{(1+it)^{1+r}}\,dt,$$

donde γ_R recorre el arco $Re^{i\theta}$ para $\theta \in [0, -\pi/2]$. Escribiendo $1 + it = Re^{i\theta}$, se tiene $|t| = |R\cos\theta| \leq R$; por tanto, la última integral está acotada en módulo por $C_\alpha R^{\alpha-r-1}$ para valores grandes de R. Tomando ahora $R = \infty$ dicha cota tenderá a cero. Mediante $t \to -it$, se llega a

$$\begin{aligned}\int_0^\infty \frac{t^{\alpha-1}}{(1+it)^{1+r}}\,dt = \int_0^{-i\infty} \frac{t^{\alpha-1}}{(1+it)^{1+r}}\,dt &= (-i)^{\alpha-1}\int_{-}0^\infty \frac{t^{\alpha-1}}{(1+t)^{1+r}}\,dt \\ &= (-i)^{\alpha-1}B\left(\alpha, 1-\alpha+r\right). \end{aligned} \tag{3.39}$$

Como α y $1-\alpha+r$ son positivos, la integral que define la función Beta en (3.39) es convergente. De la unión de (3.38) y (3.39), y utilizando que $(-i)^{\alpha-1} = -(-i)^{\alpha+1}$ deducimos

$$\begin{aligned}\Delta'' = (-i)^{\alpha-1}Ar(\alpha-r)^{-1}B\left(\alpha, 1-\alpha+r\right)\left((\delta+h)^{\alpha-r} - \delta^{\alpha-r}\right)q^{-r} \\ + \mathcal{O}_{\alpha,r}\left(q^{-r}\int_\delta^{\delta+h} u^{\alpha-r-1}\left(\int_0^{h^2q^2u^{-1}} \frac{t^{\alpha-1}}{|1+it|^{1+r}}\,dt\right)du\right) \\ + \mathcal{O}_{\alpha,r}\left(q^{-r}\int_\delta^{\delta+h} u^{\alpha-r-1}\left(\int_{q^{-2}u^{-1}}^\infty \frac{t^{\alpha-1}}{|1+it|^{1+r}}\,dt\right)du\right)\end{aligned} \tag{3.40}$$

De la primera línea se obtiene uno de los términos de la Proposición 3.9; ahora sólo queda acotar los dos términos de error de (3.40). El segundo de ellos es bastante fácil de controlar. Como $q^{-2}u^{-1}$ es mayor que 1 para $u \ll |\delta| + |h|$, la integral interior es comparable a $t^{\alpha-2-r}$ y

$$\frac{1}{q^r}\int_\delta^{\delta+h} u^{\alpha-r-1}\left(\int_{q^{-2}u^{-1}}^\infty t^{\alpha-2-r}\,dt\right)du \ll \frac{q^{-2(\alpha-r-1)}}{q^r}\int_\delta^{\delta+h} dt = |h|q^{2-2\alpha+r}.$$

Para el otro término de error es necesario un análisis más elaborado. Comenzamos suponiendo que $|\delta|$ es menor que h^2q^2. Entonces t será mayor o menor que 1 en función de si u es mayor o menor que h^2q^2. Por tanto, vamos a separar la integral doble en tres partes: Primero separararemos el rango de u entre valores mayores y menores que h^2q^2. Para los menores, separaremos los valores de t entre 0 y 1 (para los cuales $|1+it| \sim 1$) y el resto (para los cuales $|1+it| \sim t$). Para los mayores, t

siempre será menor que 1 y no habrá que distinguir casos. Haciendo esto concluimos

$$\begin{aligned}\frac{1}{q^r}\int_\delta^{\delta+h} u^{\alpha-r-1}\left(\int_0^{h^2q^2u^{-1}} \frac{t^{\alpha-1}}{|1+it|^{1+r}}\,dt\right)du \\ &\ll \frac{1}{q^r}\int_\delta^{h^2q^2} u^{\alpha-r-1}\,du + \frac{1}{q^r}\int_\delta^{h^2q^2} u^{\alpha-r-1}\left(\int_1^{h^2q^2u^{-1}} t^{\alpha-2-r}\,dt\right)du \\ &\quad + \frac{1}{q^r}\int_{h^2q^2}^{\delta+h} u^{\alpha-r-1}\left(\int_0^{h^2q^2u^{-1}} t^{\alpha-1}\,dt\right)du \\ &\ll |h|^{2\alpha-2r}q^{2\alpha-3r}.\end{aligned}$$

Nótese que los tres sumandos dan el mismo término de error. Supongamos ahora que $|\delta|$ es mayor que h^2q^2. Entonces $h^2q^2u^{-1} \le h^2q^2|\delta|^{-1} \le 1$, y podemos sustituir $|1+it|$ por 1 sin distinguir casos. En este caso la integral que queda es $q^{-r}\int_\delta^{\delta+h} u^{\alpha-r-1}\left[\int_0^{h^2q^2u^{-1}} t^{\alpha-1}\,dt\right]du \ll |h|^{2\alpha}q^{2\alpha-r}|\delta|^{-r} \ll |h|^{2\alpha-2r}q^{2\alpha-3r}$.

Para completar la prueba de (3.33), necesitamos acotar el término de error de (3.37) en (3.35). A la vista de (3.36), el tramo para el que t es mayor que h tiene mucho más peso que el otro; y debido a que la exponencial alcanza su máximo en q^{-2} dentro de la integral, podemos simplemente acotar

$$\begin{aligned}\frac{1}{q^r}\int_\delta^{\delta+h}\left(\int_{\delta+h}^{q^{-2}} t^{\alpha-1}|u+it|^{-r-1}e^{q^{-2}t^{-1}}\,dt\right)du &\ll \frac{h}{q^r}\int_{\delta+h}^{q^{-2}} t^{\alpha-2-r}e^{q^{-2}t^{-1}}\,dt \\ &\ll \frac{|h|}{q^r}\int_{q^2}^{(\delta+h)^{-1}} t^{-\alpha+r}e^{t/q^2}\,dt \\ &\ll \frac{|h|}{q^r}q^2q^{-2\alpha+2r},\end{aligned}$$

utilizando el cambio de variable $t \to 1/t$ y el hecho de que el integrando final decae exponencialmente y es comparable al valor en el extremo inferior. Este término de error aparece en el enunciado de la Proposición y con esto se completa la prueba de (3.33).

Pasamos a probar (3.34). Como adelantábamos antes, por motivos que quedarán claros en la siguiente sección, estos términos de error no van a funcionar cuando $|\delta|$ sea mayor que $|h|$. La ventaja que tenemos es que en estos casos no será necesaria una fórmula asintótica que distinga un término de los demás, y por tanto no será necesario insertar varios términos *fantasma* de error en (3.38) para completar la función Beta. Por tanto, ahora podemos acotar

$$\Delta'' = \frac{\Lambda_{\alpha,r}}{q^r}\int_\delta^{\delta+h}\left(\int_{h^2q^2}^{q^{-2}} \frac{t^{\alpha-1}}{(u+it)^{1+r}}\,dt\right)du$$

sin las precauciones que tuvimos antes. Por construcción, $h^2q^2 \leq |h| \leq |\delta| \leq q^{-2}$, por lo que δ siempre estará contenido en el intervalo $[h^2q^2, q^{-2}]$. En particular, $u \asymp \delta$ y podemos aproximar $(u+it)$ por $(\delta+it)$. Separando la integral en dos partes, según sea t mayor o menor que δ, se obtiene

$$\begin{aligned}\Delta'' &\ll_{\alpha,r} \frac{|h|}{q^r}\left[\int_{h^2q^2}^{\delta}\frac{t^{\alpha-1}}{|\delta+it|^{1+r}}\,dt + \int_{\delta}^{q^{-2}}\frac{t^{\alpha-1}}{|\delta+it|^{1+r}}\,dt\right]\\ &\ll \frac{|h|}{q^r}|\delta|^{-r-1}\left(\int_{h^2q^2}^{\delta} t^{\alpha-1}\,dt\right) + \frac{|h|}{q^r}\int_{\delta}^{q^{-2}} t^{\alpha-r-2}\,dt\\ &\ll |h||\delta|^{\alpha-r-1}q^{-r}.\end{aligned}$$

Estas desigualdades completan la prueba de (3.34) y del Lema. □

Una vez demostrados los Lemas 3.10 y 3.11, podemos demostrar la Proposición 3.9 sin más que relacionar adecuadamente todos los términos de (3.28), (3.33) y (3.34).

Demostración de la Proposición 3.9: Nuestro objetivo es demostrar las fórmulas (3.23) y (3.24) bajo las hipótesis de la Proposición 3.9; en particular, r y α son menores que 1 y $r < \alpha < r+1/2$. Para probar (3.23) (que, recordemos, se cumple sin condiciones adicionales sobre el tamaño de h y δ) unimos (3.28) y (3.33), deduciendo

$$\begin{aligned}(3.41)\quad f_\alpha(x+h) - f_\alpha(x) = \Lambda\frac{(\delta+h)^{\alpha-r}-\delta^{\alpha-r}}{q^r}\\ + \mathcal{O}\left(|h|^{2\alpha-2r}|\delta|^r q^{2\alpha-r} + |h|q^{2-2\alpha+r} + |h|^{2\alpha-2r}q^{2\alpha-3r}\right).\end{aligned}$$

Los términos principales de (3.23) y (3.41) coinciden, por tanto resta probar que los tres términos de error de (3.41) pueden acotarse por el último de ellos, que es el único presente en (3.23). En otras palabras, queremos ver que se cumple la desigualdad

$$|h|^{2\alpha-2r}|\delta|^r q^{2\alpha-r} + |h|q^{2-2\alpha+r} \ll |h|^{2\alpha-2r}q^{2\alpha-3r}.$$

Para el primer sumando es cierto sin más que utilizar $|\delta| \leq q^{-2}$. Para el segundo, es equivalente comprobar que se cumple $|h|^{1-2\alpha+2r} \ll q^{-2+4\alpha-4r}$, y esto es consecuencia de que $|h| \leq q^{-2}$ y de que $1-2\alpha+2r$ es estrictamente positivo.

Pasamos a demostrar (3.24), con lo cual en lo que resta de la demostración añadimos la hipótesis de que $|h| < |\delta|$. Utilizando (3.28) de nuevo junto con (3.34) obtenemos la siguiente fórmula:

$$f_\alpha(x+h) - f_\alpha(x) = \mathcal{O}\left(|h|^{2\alpha-2r}|\delta|^r q^{2\alpha-r} + |h|q^{2-2\alpha+r} + |h||\delta|^{\alpha-r-1}q^{-r}\right).$$

Para equiparar esta fórmula con (3.24), únicamente hemos de acotar el término de error del centro por uno de los otros dos. Utilizaremos el último de ellos. Como $2-2\alpha+r$ es estrictamente positivo,

$$|h|q^{2-2\alpha+r} = |h|q^{2-2\alpha+2r}q^{-r} \leq |h||\delta|^{\alpha-r-1}q^{-r}.$$

Esto prueba (3.24) y completa la prueba de la Proposición. □

3.4. El espectro de singularidades

En la sección anterior, aprovechando la relación de f_α con f dada por (3.25) y las propiedades modulares de f, conseguimos las fórmulas (3.23) y (3.24) para obtener varias expresiones satisfactorias de $f_\alpha(x+h)-f_\alpha(x)$. Para ello, era necesario hallar una fracción a/q irreducible que verificase dos hipótesis:

- Que el denominador de la fracción fuese lo bastante grande en comparación con $|h|$; concretamente, debía cumplirse $|h|q^2 \leq 1$.
- Que la fracción a/q aproximase a x con suficiente precisión, siendo la diferencia $\delta := x - a/q$ menor que q^{-2} en valor absoluto.

Hallar fracciones que cumplan esta segunda propiedad es sencillo. Por el Teorema de aproximación de Dirichlet [Dir69], si consideramos cualquier $x \in \mathbb{R} \setminus \mathbb{Q}$ y un entero positivo Q, entonces siempre existe una fracción irreducible a/q con $1 \leq q \leq Q$ tal que $0 < |x-a/q| < (qQ)^{-1}$. Una consecuencia inmediata de este Teorema [Cas72] es que dado cualquier número irracional x, existen infinitas fracciones a/q tales que $0 < |x-a/q| < q^{-2}$. Además, disponemos de un método explícito para hallar una subsucesión infinita $\{a_n/q_n\}_{n\geq 1}$ de estas fracciones; los convergentes de la fracción continua de x:

$$x = x_0 + \cfrac{1}{x_1 + \cfrac{1}{x_2 + \cfrac{1}{x_3 + \cfrac{1}{\cdots}}}} \tag{3.42}$$

Siempre que x sea irracional, esta construcción es única y genera una sucesión infinita de enteros positivos $x_0, x_1, x_2, \ldots$ (salvo el primero, que puede tomar cualquier valor entero). La sucesión viene dada por la recurrencia:

$$r_0 = x, x_n = \lfloor r_n \rfloor, r_{n+1} = (r_n - x_n)^{-1}, \quad n \geq 0.$$

El n-ésimo convergente de x, a_n/q_n, corresponde a truncar la estructura (3.42), esencialmente reemplazando $x_n + \frac{1}{\cdots}$ por x_n. Esto genera dos sucesiones infinitas de enteros

positivos estrictamente crecientes[10] $\{a_n\}_{n\geq 0}$ y $\{q_n\}_{n\geq 0}$ tales que $|x - a_n/q_n| \leq q_n^{-2}$. Estas dos series admiten la siguiente construcción explícita [CC92]:

$$\begin{aligned} a_{-2} = 0, a_{-1} = 1, \qquad & a_{n+2} = x_{n+2}p_{n+1} + p_n, \quad n \geq 0 \\ q_{-2} = 1, q_{-1} = 0, \qquad & q_{n+2} = x_{n+2}q_{n+1} + q_n, \quad n \geq 0. \end{aligned} \tag{3.43}$$

Existen innumerables propiedades interesantes sobre los convergentes. Entre ellas, una de las que más útil nos va a resultar es que cada uno de ellos da *la mejor aproximación posible* de x hasta q_n. Es decir, cualquier otra fracción a'/q' con $q' < q_n$ cumple $|x - a'/q'| > |x - a_n/q_n|$ (aunque no todas las mejores proximaciones son convergentes). En sentido contrario, toda aproximación de x *suficientemente buena* debe ser un convergente. Esta afirmación inconclusa queda cuantificada por el criterio de Legendre, según el cual [Lan66] si una fracción arbitraria a/q cumple $|x - a/q| < 2q^{-2}$, entonces dicha fracción coincide con un convergente de x. Fatou amplió este resultado probando [Fat04] que si tal fracción verifica $|x - a/q| < q^{-2}$, entonces a/q es o bien un convergente de x o un *intermediario*; es decir, a/b es expresable en la forma $(a_n \pm a_{n-1})/(q_n \pm q_{n-1})$. Worley obtuvo un resultado más débil, pero válido reemplazando 1 por cualquier constante positiva fijada a priori [Wor81]. En sentido contrario, se verifica [CC92] para todo $n \geq 0$:

$$\frac{1}{(x_{n+1}+2)q_n^2} < \left| x - \frac{a_n}{q_n} \right| < \frac{1}{x_{n+1}q_n^2}.$$

En particular, todo convergente cumple $|x - a_n/q_n| \leq q_n^{-2}$. Otra observación importante es la alternancia de los convergentes. Los pares, a_{2n}/q_{2n}, siempre serán menores que x, mientras que los impares serán mayores.

Ya sabemos por tanto que para aproximar un irracional x fijo tendremos a nuestra disposición una sucesión infinita de fracciones $\{a_n/q_n\}$ cuya distancia a x se acerque arbitrariamente a cero y tal que el denominador sea grande en función de un h pequeño fijado de antemano. El objetivo ahora es convertir (3.23) en una fórmula asintótica que dependa exclusivamente de ese valor h, sin presencia alguna del denominador q_n ni del tamaño de la diferencia $\delta := x - a_n/q_n$. Para ello necesitamos ahondar en la teoría de aproximación diofántica. Hay un hecho clave para ello: aunque como acabamos de ver, todos los irracionales se aproximan *bien* por fracciones, unos lo hacen mejor que otros. Cualquier fracción irreducible a/q que verifique $|x - a/q| < q^{-k}$ para un irracional x dado y $k > 0$ se denominará una *aproximación diofántica de x de orden k*. Obviamente, una aproximación diofántica de orden k_0 lo es también de orden k para cualquier otro $k < k_0$. Los racionales tienen malas aproximaciones diofánticas, pues si se aproxima una fracción por otras diferentes, el orden no puede

[10] Obviamente, si x es negativo, cada fracción lo será también. En ese caso tomaremos la convención de asignar el signo menos a la sucesión de los numeradores, $\{a_n\}$, con lo que esta sucesión será estrictamente decreciente.

ser mejor que lineal a medida que el denominador de éstas tiende a infinito. Con los irracionales acabamos de ver que esto mejora mucho al existir siempre infinitas aproximaciones diofánticas de orden 2, pero ¿es éste el mejor orden de aproximación que se puede alcanzar? La respuesta es que en general sí, puesto que el conjunto de números que poseen infinitas aproximaciones diofánticas de orden mayor que 2 tiene medida de Lebesgue nula[11]. Pero utilizando una lente más precisa, la que nos brinda la dimensión de Hausdorff, somos capaces de apreciar la insondable riqueza de ese pequeño conjunto; si clasificamos los irracionales en base al máximo grado k tales que admiten infinitas aproximaciones diofánticas de grado k, vamos a obtener conjuntos con todas las dimensiones posibles comprendidas entre 0 y 1. Este precioso resultado fue demostrado de forma independiente[12] por el checo Vojtěc Jarník y el ruso Abram Samoilovitch Besicovitch.

Teorema 3.12 (Teorema de Jarník-Besicovitch)**.** *Sea $c \geq 2$ un número real. Consideremos el conjunto F_c dado por todos los elementos $x \in [0,1] \setminus \mathbb{Q}$ tales que existen infinitas fracciones irreducibles a/q verificando $|x - a/q| \leq q^{-c}$. Entonces, la dimensión de Hausdorff de F_c es $2/c$.*

Un ejemplo notable son los llamados números de Liouville, que son aquellos que cumplen la hipótesis del teorema para c arbitrariamente grande. Estos números forman un conjunto de dimensión cero, pero denso [Lio44] en el intervalo $[0,1]$. El primero de ellos que se construyó explícitamente [Lio51] se denomina precisamente *constante de Liouville*, y puede expresarse mediante la serie $\sum_{n=1}^{\infty} 10^{-n!}$.

A la vista del Teorema 3.12, es necesario clasificar x en función del *nivel de aproximación* que admita por racionales para convertir la fórmula (3.23) en un cálculo efectivo del exponente Hölder con el que obtener el espectro de singularidades de f_α. El problema es que los conjuntos F_c tal y como se definen en ese teorema no son disjuntos, sino que están encajados unos en otros. Es decir, verifican $F_c \supset F_c'$ para $c \leq c'$. Como deseamos asignar a cada punto x el nivel adecuado dentro del conjunto, vamos a considerar *secciones* de F_c; es decir, el subconjunto de F_c para el que el exponente c es crítico en algún sentido. Para ello, siguiendo de nuevo la notación de [CU12], definimos el siguiente conjunto:

$$A_c := \left\{ x \in [0,1] \setminus \mathbb{Q} : \left| x - \frac{a_n}{q_n} \right| = \frac{1}{q_n^{c_n}} \quad \text{con} \quad \limsup c_n = c \right\}, \tag{3.44}$$

[11] En particular, todo número algebraico admite un número finito de aproximaciones diofánticas de orden $2+\varepsilon$, para cualquier $\varepsilon > 0$ fijado. Este famoso resultado se denomina teorema de Roth, o teorema de Thue-Siegel-Roth [DR55].

[12] Jarník [Jar31] demostró el resultado del teorema en primer lugar, por ello a veces el resultado se conoce simplemente como Teorema de Jarník. En nuestra exposición utilizaremos la prueba de Besicovitch [Bes] para generalizar el resultado. Una versión más moderna de la prueba puede encontrarse en [Fal90, §10].

donde para cada x, la sucesión $\{a_n/q_n\}_{n\geq 1}$ está formada por sus convergentes. Obviamente, A_c está contenido en F_c, y éste a su vez estará contenido en $\bigcup_{s\geq c} A_s$. El conjunto A_c tendrá dimensión de Hausdorff $2/c$. Una forma de verlo es utilizar que para todo $\varepsilon > 0$ se verifica

$$A_c \subset \bigcup_{s\geq c} A_s \setminus \bigcup_{s\geq c+\varepsilon} A_s.$$

El conjunto de la izquierda tiene dimensión $2/c$ y el de la derecha $2/(c+\varepsilon) < 2/c$, luego el conjunto diferencia tendrá dimensión $2/c$ por propiedades elementales de una medida. Así pues, A_c es un subconjunto de F_c con su misma dimensión y, lo que es más importante, cada irracional x puede asignarse unívocamente a A_c para algún $c \geq 2$. Esto va a permitirnos dar el primer resultado que buscamos.

Proposición 3.13. *Considérese la función f_α satisfaciendo las hipótesis del Teorema 3.9. Sean $c > 2$ y $x \in A_c$ donde A_c viene dado por* (3.44)*. Entonces, todo $h \neq 0$ suficientemente pequeño verifica*

$$f_\alpha(x+h) - f_\alpha(x) \ll |h|^{\alpha - r + r/c} \tag{3.45}$$

Demostración: Fijado $x \in A_c$, consideramos la sucesión formada por sus convergentes $\{a_n/q_n\}$, que como vimos antes está definida de manera unívoca. Dado cualquier $h \neq 0$ suficientemente pequeño, siempre existirá un índice n tal que h esté encajado entre las diferencias de aproximación a x de dos convergentes sucesivos; es decir,

$$\frac{1}{q_n^{c_n}} = \left| x - \frac{a_n}{q_n} \right| \leq |h| < \left| x - \frac{a_{n-1}}{q_{n-1}} \right| = \frac{1}{q_{n-1}^{c_{n-1}}}. \tag{3.46}$$

Nótese que $c_{n-1}, c_n > 2$ gracias a que $q_j^{-c_j} = |x - a_j/q_j| \leq q_j^{-2}$ para $j = n-1, n$, por las propiedades de los convergentes que vimos en la página 86. En particular ambas fracciones aproximan lo bastante a x como para poder utilizarlas en (3.23). Pero, ¿qué ocurre con h? No habrá problemas para utilizar q_{n-1}, puesto que $|h|q_{n-1}^2 < |h|q_{n-1}^{c_{n-1}} < 1$. El problema viene con q_n, ya que a la vista de (3.43), su valor es esencialmente q_{n-1} multiplicado por el inverso de la parte fraccionaria de un número de carácter aleatorio. Por tanto, q_n puede ser muchísimo mayor que q_{n-1}, y en consecuencia q_n^{-2} puede ser mayor que $q_{n-1}^{c_{n-1}}$. Por cuestiones de magnitud, es recomendable utilizar la fracción a_n/q_n siempre que sea posible, y cambiar a a_{n-1}/q_{n-1} cuando ocurra se dé el caso que acabamos de exponer. Por tanto, distinguiremos dos casos según el valor de h. Si $q_n^{-c_n} \leq |h| \leq q_n^{-2}$, entonces $|h| > |\delta|$ para $\delta := x - a_n/q_n$, y de (3.23) se deduce

$$f_\alpha(x+h) - f_\alpha(x) \ll h^{\alpha-r} q_n^{-r}(1 + hq_n^2) \leq h^{\alpha-r} q_n^{-r} \leq h^{\alpha - r + r/c_n}.$$

Supongamos ahora que $q_n^{-2} \leq |h| \leq q_{n-1}^{-c_{n-1}}$ (como dijimos antes, esto sólo puede ocurrir cuando $q_n^{-2} \leq q_{n-1}^{-c_{n-1}}$; si no, siempre estaríamos en el primer caso). Bajo este

supuesto, tenemos automáticamente una cota superior para q_{n-1} con respecto a h^{-1}. Para dar una cota inferior, utilizamos

$$\frac{2}{q_{n-1}^{c_{n-1}}} < \frac{1}{q_{n-1}^{c_{n-1}}} - \frac{1}{q_n^{c_n}} = \left|x - \frac{a_{n-1}}{q_{n-1}}\right| + \left|x - \frac{a_n}{q_n}\right| = \left|\frac{a_{n-1}}{q_{n-1}} - \frac{a_n}{q_n}\right| < \frac{1}{q_{n-1}q_n},$$

de donde $q_{n-1}^{-c_{n-1}} \ll (q_n q_{n-1})^{-1}$. Nótese que hemos utilizado que dos convergentes consecutivos han de estar uno a cada lado de x. Por tanto, $q_{n-1}^{c_{n-1}-1} > q_n$ y de aquí deducimos $q_{n-1}^{2(c_{n-1}-1)} > |h|^{-1}$. Si tomamos $\delta = x - a_{n-1}/q_{n-1}$, entonces $|\delta| = q_{n-1}^{-c_{n-1}}$ y se tiene

$$1 < |\delta h^{-1}| < |\delta|^{(2-c_{n-1})/c_{n-1}}. \tag{3.47}$$

Puesto que ahora $\delta := |x - a_{n-1}/q_{n-1}|$ es mayor que h, utilizaremos (3.24) para acotar $f_\alpha(x+h) - f_\alpha(x)$, obteniendo

$$\begin{aligned} f_\alpha(x+h) - f_\alpha(x) &\ll |h| \left|x - \frac{a_{n-1}}{q_{n-1}}\right|^{\alpha-r-1} q_{n-1}^{-r} + |h|^{2\alpha-2r} \left|x - \frac{a_{n-1}}{q_{n-1}}\right|^{r} q_{n-1}^{2\alpha-r} \\ &= |h||\delta|^{\alpha-r-1+r/c_{n-1}} + |h|^{2\alpha-2r}|\delta|^{r+(r-2\alpha)/c_{n-1}} \\ &= |h|^{\alpha-r+r/c_{n-1}} \left[\left|\frac{\delta}{h}\right|^{\alpha-r+r/c_{n-1}-1} + |\delta|^{\frac{(c_{n-1}-2)\alpha}{c_{n-1}}} \left|\frac{\delta}{h}\right|^{-\alpha+r+r/c_{n-1}}\right] \\ &\ll |h|^{\alpha-r+r/c_{n-1}} \left[1 + \left|\frac{\delta}{h}\right|^{-2\alpha+r+r/c_{n-1}}\right]. \end{aligned} \tag{3.48}$$

Para la última desigualdad hemos utilizado $r < \alpha < 1$ y (3.47). El término entre corchetes es claramente menor o igual que 1, y por tanto esto completa la prueba de (3.45). □

Ahora queremos obtener una cota inferior de la Proposición 3.9, y es preciso proceder con mayor delicadeza. En primer lugar, está claro que para lograr una cota superior necesitaremos (3.23) y conseguir que su término principal sea de orden superior al de error. Para ello es necesario que el denominador q escogido sea bastante grande, para que se cumpla $hq^2 = o(1)$ y no sólo $hq^2 = \mathcal{O}(1)$ como veníamos pidiendo hasta ahora. Y también necesitamos, por supuesto, que la constante Λ sea no nula, lo que ocurrirá *cuando f no sea cuspidal en $\mathfrak{a} = a/q$*. Esto a priori supone un problema, puesto que ahora no podremos considerar todos los convergentes de x, sino únicamente los que pertenezcan a clases de equivalencia de cúspides en los que f sea no cuspidal.

Lo que vamos a demostrar a continuación es que basta garantizar que f no sea una forma cuspidal (es decir, que como mínimo exista una clase de equivalencia de cúspides sobre la que f sea no cuspidal) para obtener un resultado satisfactorio:

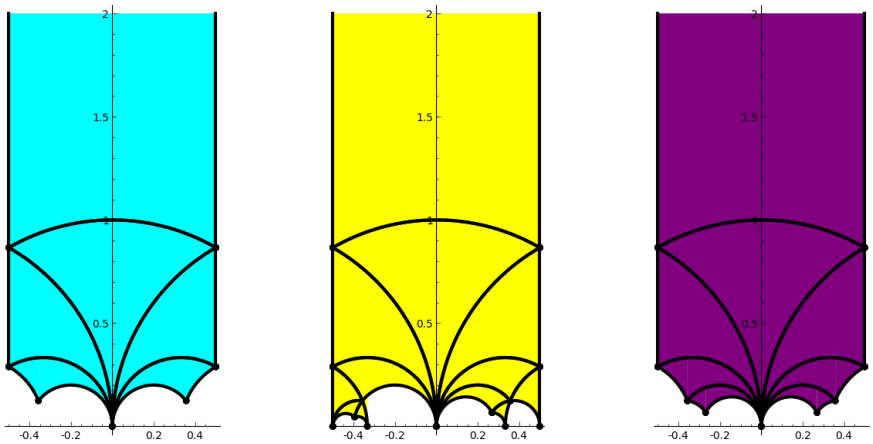

Figura 3.6: Dominios fundamentales para $\Gamma_0(5)$, $\Gamma_0(6)$ y $\Gamma_0(7)$, respectivamente.

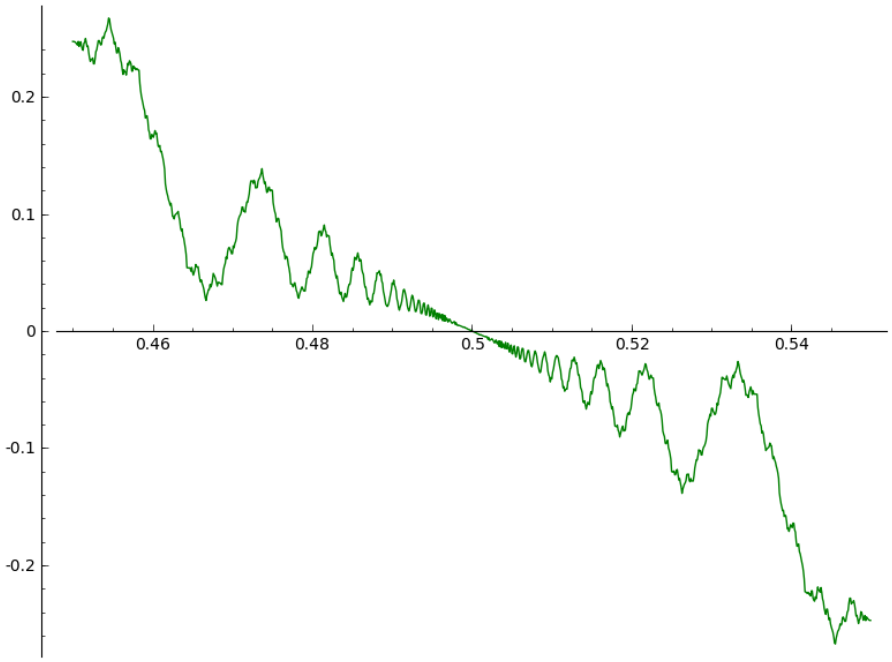

Figura 3.7: Detalle de la función $R(x)$ alrededor de $x = 1/2$.

los puntos x de A_c tales que sus convergentes no pasen infinitas veces sobre una clase de equivalencia de cúspides concreta no pueden ser muchos. Probaremos que los que sí lo hagan tendrán la misma dimensión que el conjunto completo. Para ello, vamos a utilizar una interesante propiedad que cumple $\Gamma_0(N)$, y es que *las clases de equivalencia de cúspides pueden describirse mediante clases de congruencia* [Iwa97,

§2.4]. Por ejemplo, $\Gamma_0(4)$ tiene tres clases de equivalencia de cúspides diferentes :

$$\begin{aligned}
[\mathfrak{a}] &= \left[\frac{1}{2}\right] = \left\{\frac{a}{q} \in \mathbb{Q} : \operatorname{mcd}(a,q) = 1, q \equiv 2\,(4)\right\}. \\
[\mathfrak{b}] &= \left[\frac{1}{3}\right] = \left\{\frac{a}{q} \in \mathbb{Q} : \operatorname{mcd}(a,q) = 1, q \equiv 1\,(2)\right\}. \\
[\mathfrak{c}] &= \left[\frac{1}{4}\right] = \left\{\frac{a}{q} \in \mathbb{Q} : \operatorname{mcd}(a,q) = 1, q \equiv 0\,(4)\right\} \cup \{i\infty\}.
\end{aligned}$$

Puede verse un dominio fundamental de $\Gamma_0(4)$ en la Figura 3.5 de la página 72, donde $i\infty \in [\mathfrak{c}]$ y $0 \in [\mathfrak{b}]$. La función R que vimos en (3.2) es cuspidal en $1/2$ (donde también es diferenciable, véase la Figura 3.7) y no lo es en $1/3$ y $1/4$ (donde tampoco es diferenciable, véanse las Figuras 3.3 y 3.8).

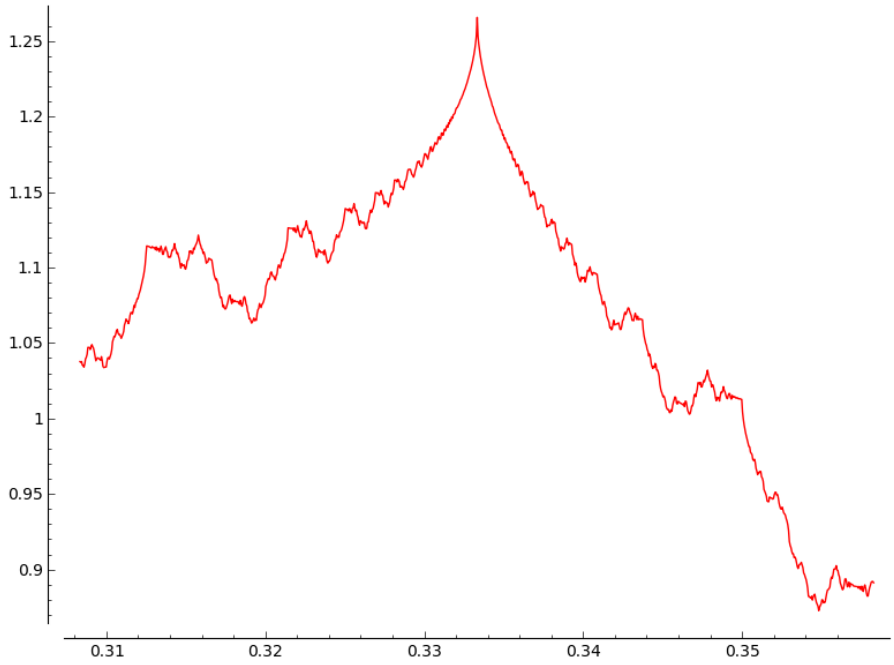

Figura 3.8: Detalle de la función $R(x)$ alrededor de $x = 1/3$.

Ahora bien, no está claro cómo traducir este ejemplo al caso general, ya que la afirmación de que las cúspides pueden agruparse por clases de congruencia resulta algo inconclusa. Como no necesitamos una descripción completa, únicamente probaremos el siguiente resultado:

Proposición 3.14. *Dado un entero positivo N, sean dos fracciones irreducibles m/n y m'/n' que verifiquen $m \equiv m'\,(N)$ y $n \equiv n'\,(N)$. Entonces existe una matriz $g \in$*

$\Gamma_0(N)$ tal que $g\frac{m}{n} = \frac{m'}{n'}$. En particular, las cúspides m/n y m'/n' pertenecen a la misma clase de congruencia.

Demostración: Siempre existirá $\gamma := \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(1)$ tal que $m' = am + bn$ y $n' = cm+dn$, puesto que en ese grupo todos los racionales están en la misma clase de equivalencia. Dados enteros λ y μ, se cumplirán también $m' = (a-\lambda n)m+(b+\lambda m)n$ y $n' = (c-\mu n)m+(d+\mu m)n$, pero en este caso los coeficientes no tienen por qué formar una matriz de determinante 1. Esto ocurrirá si y sólo si $a\mu m + b\mu n - c\lambda m - d\lambda n = \mu m' - \lambda n' = 0$. Tomando entonces $\lambda = \mu m'/n'$ y mediante el cambio $\mu \to \mu n'$ para que los parámetros sean enteros, nos queda la matriz

$$g = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} = \begin{pmatrix} a - \mu m'n & b + \mu m'm \\ c - \mu n'n & d + \mu n'm \end{pmatrix}$$

que, por construcción, está en $\Gamma_0(1)$. Vamos a demostrar que podemos escoger μ tal que esté además en $\Gamma_0(N)$, para lo que basta probar que γ es un múltiplo de N. Como m/n es irreducible, al menos uno de los dos debe ser coprimo con N. Podemos suponer $\mathrm{mcd}(m, N) = 1$ (el caso $\mathrm{mcd}(n, N)$ es análogo). Se cumple entonces $\mathrm{mcd}(m', N) = 1$ y puede tomarse μ tal que $\beta \equiv 0\,(N)$. Como $\alpha m + \beta n = m'$, α debe ser congruente con 1 módulo N, y entonces δ también, por ser g de determinante 1. Utilizando esto último en $\gamma m + \delta n = n'$, se concluye que $\gamma \equiv 0\,(N)$, que es lo que queríamos demostrar. □

Con la Proposición anterior y la hipótesis de que f es no cuspidal en al menos una clase de equivalencia de cúspides $[\mathfrak{a}]$, tenemos garantizado que existen a' y q' coprimos tales que todos los convergentes a_n/q_n con $a_n \equiv a'\,(N)$ y $q_n \equiv q'\,(N)$ cumplirán que el término principal de (3.23) sea no nulo. A partir de estos elementos, vamos a definir la anunciada refinación de A_c. Fijado $c \geq 2$, definimos

$$A_c^* := \{x \in A_c : \exists \{n_k\}_{k\geq 1} : a_{n_k} \equiv a'\,(N); q_{n_k} \equiv q'\,(N) \text{ para cada } k\}, \tag{3.49}$$

donde de nuevo $\{a_n/q_n\}_{n\geq 1}$ representa la sucesión de los convergentes del valor x fijado y, por supuesto, A_c^* depende implícitamente de la clase $[\mathfrak{a}]$ que hayamos escogido, así como de a' y q'. Para demostrar que este conjunto tiene la misma dimensión que A_c vamos a replicar el argumento de la página 87 que relacionaba A_c y F_c. Por ello, en primer lugar, necesitamos redefinir F_c de la misma forma que hemos hecho con A_c. Partiendo del conjunto original,

$$F_c := \{x \in [0,1] :\ |x - a/q| < 1/q^c \text{ para infinitos } (a,q) = 1\}, \tag{3.50}$$

definimos, para $c \geq 2$ fijo,

$$F_c^* := \{x \in [0,1] :\ |x - a/q| < 1/q^c \text{ para infinitos } (a,q) = 1; a \equiv a', q \equiv q'\,(N)\}.$$

Vamos a demostrar que, con esta elección, este conjunto tiene la misma dimensión que F_c.

Proposición 3.15. *El conjunto F_c^* tiene dimensión de Hausdorff $2/c$.*

La prueba se basa en ciertas modificaciones sobre la demostración original de A.S. Besicovitch [Bes]. Al tratarse ésta de una prueba considerablemente larga y técnica, hemos optado por mostrar aquí las modificaciones más importantes, conservando la notación original. Remitimos al lector a la fuente para completar los posibles detalles.

Demostración: Como F_c^* es claramente un subconjunto de F_c, únicamente hemos de probar que su dimensión de Hausdorff es no inferior a $2/c$. Para ello, basta con demostrar que ningún conjunto numerable de intervalos $\mathcal{I} \in [0,1]$ que verifique

$$\sum_{I\in\mathcal{I}} |I|^{(2-\varepsilon)/c} < 1, \qquad |I| \leq \lambda, \tag{3.51}$$

para $\varepsilon > 0$ suficientemente pequeño puede contener por completo a F_c^*, y en consecuencia, $\dim_{\mathcal{H}} S \geq (2-\varepsilon)/r$ para cada $\varepsilon > 0$. Puede suponerse que los intervalos que componen $\mathcal{I}$ son disjuntos. Para verlo, dada una colección de intervalos $\mathcal{I}$ como en (3.51), vamos a definir $\mathcal{J}$ como la versión *refinada* de $\mathcal{I}$ de la siguiente forma: si $I_1, I_2 \in \mathcal{I}$ tienen intersección común, se definen $J_1, J_2 \in \mathcal{J}$ como $J_1 := I_1$, $J_2 = I_2 \setminus (I_1 \cup I_2)$. Como $\mathcal{I}$ es numerable, siempre se puede obtener una colección de intervalos disjuntos $\mathcal{J} = \bigcup J = \bigcup I$ cuyo número es menor o igual que los de $\mathcal{I}$ y cuya longitud es no superior a λ. Si $\mathcal{J}$ verifica

$$S \not\subset \bigcup_{J\in\mathcal{J}} \Rightarrow \sum_{J\in\mathcal{J}} |J| \geq 1 \tag{3.52}$$

entonces $\sum_I |I| \geq 1$. Pero $\bigcup I$ no puede contener a S porque hemos supuesto que $\bigcup J$ tampoco lo hace, y son iguales. Luego si $\mathcal{J}$ cumple (3.52), también lo cumple $\mathcal{I}$. Por tanto, a partir de ahora supondremos que los intervalos que componen $\mathcal{I}$ son disjuntos. Consideramos, como Besicovitch, la sucesión creciente $n_0, n_1, n_2, \ldots$, para n_0 suficientemente grande y de modo que el cociente entre dos términos consecutivos también sea suficientemente grande, en un sentido que precisaremos varias veces. Fijemos $\lambda = 1/n_0^c$, y tomemos $q'' = \mathrm{mcd}(q', N)$ (entendiendo que $0 \leq q' < N$). Vamos a construir el siguiente conjunto:

$$F_1 := \left\{ \left(\frac{a}{q} - \frac{1}{q^c}, \frac{a}{q} + \frac{1}{q^c} \right) : (a,q) = 1; a \in \mathcal{A} \cap [0,q]; q \in \mathcal{Q} \cap [n_1, 2n_1), q/q'' \in \mathcal{P} \right\},$$

donde $\mathcal{P}$ es el conjunto de los números primos y $\mathcal{A}$ y $\mathcal{Q}$ denotan los enteros congruentes con a' y con q' módulo N, respectivamente. Todos los intervalos que forman F_1 son trivialmente disjuntos entre sí (ya que $x^{-r} + y^{-r} < (xy)^{-1}$ para $n_1 \leq x, y < 2n_1$). Estrictamente, en los intervalos de los extremos (correspondientes a $a = 0, 1$) sólo se cuenta la mitad que está en $[0,1]$, aunque esto no es relevante para lo que vamos

a hacer. Uno de los pasos más importantes y que más cambia con respecto a la demostración original es dar una cota inferior del número de intervalos que forman F_1, cantidad que denotaremos por $|F_1|$. Fijado un $q \in [n_1, 2n_1)$ válido, queremos contar los $a = 1, 2, \ldots, q-1$ que sean coprimos con q/q_1 y estén en $\mathcal{A}$. Equivalentemente, $(a, q/q'') = \mathrm{mcd}(a, q'') = 1, a \equiv a'\,(N)$, por lo tanto el número de valores de a válidos es aproximadamente igual a $q(1-q''/q)(\varphi(q'')/q'')a^{-1} \geq (q-q'')/(aq'')$, donde $\varphi(n)$ es la función φ de Euler. Como $q \geq n_1$ es muchísimo mayor que a' y q', el número de valores de a será mayor que $q/(2aq'')$. Sumando ahora en q,

$$|F_1| \geq \sum_{\substack{q\in[n_1,2n_1)\\ q\in\mathcal{Q}\cap q''\mathcal{P}}} \frac{q}{2aq''} \geq \frac{n_1}{2aq''} \sum_{\substack{n_1\leq q<2n_1\\ q\equiv q'\,(N)\\ q/q''\in\mathcal{P}}} 1 = \frac{n_1}{2aq''} \sum_{\substack{(q'')^{-1}n_1\leq q<2(q'')^{-1}n_1\\ q\equiv q'(q'')^{-1}\,(N(q'')^{-1})\\ q\in\mathcal{P}}} 1.$$

Por comodidad, escribiremos $\overline{n_1} := n_1 q_1^{-1}$, $\overline{N} := q_0(q'')^{-1}$ y $\overline{q'} := q'(q'')^{-1}$. El último sumatorio es $\pi(2\overline{n_1}; \overline{N}, \overline{q'}) - \pi(\overline{n_1}; \overline{N}, \overline{q'}) + \epsilon$ donde $\pi(x; q, a) = |\{p \in \mathcal{P} : p \leq x,\, p \equiv a\,(q)\}|$ y ϵ es una constante entera absoluta que depende de si los extremos del intervalo son enteros o no. Como N está fijado de antemano, puede tomarse n_1 suficientemente grande para que $q', q'' \leq N = o(n_1)$; entonces, por el teorema de los números primos en progresiones aritméticas, la diferencia de arriba es asintóticamente $\overline{n_1}(\varphi(\overline{N})\log\overline{n_1})^{-1}$, gracias a que $\overline{N}$ y $\overline{q'}$ son coprimos. De nuevo, puede tomarse n_1 todo lo grande que sea necesario, y siempre debe existir algún valor para el que la diferencia sea mayor o igual que $\overline{n_1}(2\varphi(\overline{N})\log\overline{n_1})^{-1}$. Por tanto,

$$|F_1| \geq \frac{n_1}{2a_0q''} \cdot \frac{n_1}{2q''\varphi(N/q'')\log n_1/q''} \geq \frac{n_1^2}{(4a_0Nq'')\log n_1}. \tag{3.53}$$

Y ésta es quizás la diferencia más significativa. En el original, la ecuación análoga a (3.53) es $|F_1| \geq n_1^2/(\log n_1)$. Aquí, únicamente dividimos por una constante que es arbitrariamente pequeña en relación con el tamaño de n_1. Descomponiendo F_1 en F_1' y F_1'' y procediendo como en el original, se demuestra

$$|F_1''| \geq \frac{n_1^2}{(32N^2q'')\log n_1}$$

siempre que n_1 sea suficientemente grande en comparación con n_0. Ahora se define G_1 a partir de los intervalos de F_1'', verificándose por construcción que todo intervalo de G_1 tiene diámetro menor que n_1^{-c}. Procediendo como en [Bes] y utilizando (3.53), se deduce

$$\sum_{I\in G_1} |I| > \frac{|F_1''|}{(2n_1)^c} > \frac{n_1^2}{(8N^2q'')(2n_1)^c\log n_1}.$$

A continuaciónse inicia un proceso iterativo definiendo

$$F_2 := \left\{ \left(\frac{a}{q} - \frac{1}{q^c}, \frac{a}{q} + \frac{1}{q^c} \right) : (a,q) = 1; a \in \mathcal{A}\cap[0,q]; q \in \mathcal{Q}\cap[n_2, 2n_2), q/q'' \in \mathcal{P} \right\},$$

de donde

$$|G_2| > \frac{n_2^2}{(4N^2q'')\log n_2}\cdot\frac{n_1^2}{2(8N^2q'')(2n_1)^c\log n_1} = \frac{1}{4}\cdot\frac{(n_2n_1)^2}{(4N^2q'')^2(2n_1)^c\log n_2\log n_1}.$$

y

$$\sum_{I\in G_2}|I| > \frac{1}{4}\cdot\frac{(n_2n_1)^2}{(4N^2q'')^2(2n_2 2n_1)^c\log n_2\log n_1}.$$

Realizando esto infinitas veces, conseguimos una sucesión de conjuntos $\{G_k\}_{k=1}^{\infty}$ de tal manera que cada uno está contenido en el anterior y que cada G_k no contiene ningún intervalo de $\mathcal{I}$ de longitud mayor o igual que n_k^{-c} y además verifica

$$\sum_{I\in G_k}|I| > \frac{1}{4}\cdot\frac{(n_kn_{k-1}\dots n_2n_1)^2}{(4N^2q'')^k(2n_k2n_{k-1}\dots 2n_22n_1)^c\log n_k\log n_{k-1}\dots\log n_2\log n_1} \tag{3.54}$$

para cada $k\in\mathbb{Z}^+$. Luego son todos no vacíos y compactos. Por tanto $G := \bigcap_{k=1}^{\infty}G_k$ es no vacío, no tiene ningún punto en común con $\mathcal{I}$ y $G\subset\bigcap_{k=1}^{\infty}F_k\subset F_c^*$. Esto basta para completar la prueba. Nótese que la fórmula final que aparece en [Bes] difiere de (3.54) únicamente en el factor $(4N^2q'')^k$ □

Corolario 3.16. *El conjunto A_c^* tiene dimensión de Hausdorff $2/c$.*

Demostración: La relación entre A_c^* y F_c^* es análoga a la que hay entre A_c y F_c, que expusimos en la página 87 bajo la definición de A_c. Básicamente F_c^* estará compuesto por la unión de todos los A_s^* con $s\geq c$, y A_c^* será de algún modo el conjunto de los $x\in F_c^*$ para los que c es el exponente crítico. Por construcción, A_c^* está contenido en F_c^*, y éste a su vez $\bigcup_{s\geq c}A_s^*$, como acabamos de ver. Para todo $\varepsilon>0$ se verificará

$$A_c^*\subset\bigcup_{s\geq c}A_s^*\setminus\bigcup_{s\geq c+\varepsilon}A_s^*.$$

El conjunto de la izquierda tiene dimensión $2/c$ y el de la derecha $2/(c+\varepsilon)<2/c$, luego el conjunto diferencia tendrá dimensión $2/c$ por propiedades elementales de una medida. □

Una vez completada la definición de F_c^*, estamos en condiciones de dar un análogo a la Proposición 3.13 que dé una cota inferior; eso sí, para una sucesión seleccionada de valores de h.

Proposición 3.17. *Considérese la función f_α satisfaciendo las hipótesis del Teorema 3.9. Supongamos además que f no es una forma cuspidal. Sea $c>2$ y $x\in A_c^*$, donde A_c^* viene dado por* (3.49)*. Entonces existe una sucesión $\{h_n\}$ convergente a cero y tal que*

$$f_\alpha(x+h_n)-f_\alpha(x)\gg h^{\alpha-r+r/c}.$$

Demostración: Para la cota inferior necesitamos que la asintótica principal sea de hecho mayor que el término de error, por lo que ahora no es suficiente con que hq_n^2 esté acotado (ahora sólo vamos a trabajar con q_n), sino que además debe ser muy pequeño. Para ello vamos a definir la siguiente variante de (3.44) (se sobreentiende que depende implícitamente de la f escogida):

Dado $x \in A_c^*$, tomamos h como en (3.46) y consideramos la subsucesión $h_n := x - a_n/q_n = q_n^{-c_n}$ para aquellos q_n que cumplan la condición de congruencia (es decir, $a_0^{\mathfrak{a}} \neq 0$ para $\mathfrak{a} = a_n/q_n$. Existen infinitos de estos q_n, y además con esta definición h_n tiende a cero. Tomando pues $x \in A_c^*$ y la subsucesión citada se cumple, haciendo lo mismo que antes y utilizando (3.23),

$$\begin{aligned} f_\alpha(x+h_n) - f_\alpha(x) &\gg h_n^{\alpha-r} q_n^{-r} \left(1 + (h_n q_n^2)^{\alpha-r}\right) \\ &\gg h_n^{\alpha-r} q_n^{-r} \\ &= h_n^{\alpha-r+r/c_n} \end{aligned} \tag{3.55}$$

Y esto prueba la Proposición 3.17. Para la penúltima desigualdad se utiliza que c_n es siempre mayor que 2 y, para n suficientemente grande, $q_n^{2-c_n}$ puede acotarse inferiormente con precisión arbitraria para lograr $h_n q_n^2 = o(1)$. □

Ya podemos concluir la prueba del Teorema principal.

Demostración del Teorema 3.7: Vamos a demostrar la fórmula (3.7). Con la Proposición 3.13 demostramos que el exponente Hölder de x debía ser, a lo más, $\alpha - r + r/c$ para cada $x \in A_c$. Y con la Proposición 3.17 acabamos de ver que para una sucesión convergente a cero de valores de h, dicho exponente se alcanza explícitamente, siempre que x esté en A_c^*, que es un subconjunto de A_c con la misma dimensión. Así pues, dado $c > 2$ todo $x \in A_c^*$ tiene exponente Hölder exactamente $\alpha - r + r/c$, y por tanto, el subconjunto de puntos de $[0,1]$ con orden Hölder $\beta := \alpha - r + r/c$ tiene dimensión al menos $2/c = 2(\beta - \alpha + r)/r$. En términos del espectro de singularidades, este hecho se expresa equivalentemente como $d_{f_\alpha}(\beta) \geq 2(\beta - \alpha + r)/r$, para $\alpha - r < \beta < \alpha - r/2$ (este rango surge haciendo variar c entre 2 e ∞).

Por otro lado, de (3.45) se deduce que todo $x \in [0,1]$ irracional con exponente Hölder exactamente $\alpha - r + r/c$ debe estar contenido o bien en A_c o bien en algún A_s con $s > c$ (incluyendo la posibilidad $s = \infty$). En particular, x estará contenido en $\bigcup_{s \geq c} A_s = F_c$, donde F_c viene dado por (3.50) y tiene dimensión $2/c$ por el Teorema 3.12. Por tanto, tenemos la desigualdad contraria, $d_{f_\alpha}(\beta) \leq 2(\beta - \alpha + r)/r$, para $\alpha - r < \beta < \alpha - r/2$. De la unión de ambas conseguimos la igualdad y completamos la prueba del Teorema 3.7. □

3.5. Futuras mejoras

Los resultados expuestos en este capítulo forman parte de un artículo en preparación que podría contener resultados adicionales a los que figuran en la tesis, o ser el primero de varios artículos relacionados. En particular, sería deseable generalizar el Teorema 3.7 en varios sentidos:

- Para caracterizar completamente el espectro $d_{f_\alpha}(\beta)$ (3.7), falta incluir los casos límite en que β toma los valores $\alpha - r$ (para el que se espera el valor cero) y $\alpha - r/2$ (para el que se espera el valor uno). En estos casos, especialmente en el segundo, es preciso operar con más cuidado, ya que aparecen términos de error logarítmicos para los que nuestras cotas no son válidas a priori, aunque parece razonable que puedan acotarse satisfactoriamente. También falta estudiar qué ocurre con los racionales, puesto que aunque constituyen un conjunto de medida cero, pueden aportar nuevos valores al espectro. De hecho, para las clases de equivalencia de cúspides en las que f sea cuspidal, f_α será diferenciable en los racionales que pertenezcan a esa clase [Cha04], y por tanto existirán valores $\beta \geq 1$ para los que $d_{f_\alpha}(\beta)$ tome el valor cero, como ocurría con el ejemplo de Riemann (véase el Teorema 3.3 en la página 66) en el que $d_R(3/2)$ estaba definido.

- Cuando introducíamos f_α en la Definición 3.6, ya indicábamos que la cota $\alpha < r + 1/2$ no tenía por qué ser insalvable. De hecho, el ejemplo de Riemann nace tomando exactamente $\alpha = r + 1/2$ a partir de la función θ. La evidencia muestra de nuevo que sería posible extender el Teorema 3.7 a ese caso límite (de nuevo aparecerían términos de error que estarían justo en el caso extremo en que aún se podrían acotar, aunque con algo más de esfuerzo). Y tomar valores incluso mayores de α aún podría ser un tema de estudio, si bien en ese caso la descomposición de Δ sería totalmente diferente y aparecerían nuevos términos principales.

- Aunque existen ejemplos explícitos de formas modulares de pesos menores que 1 (la ya mencionada función θ de Jacobi, de peso $1/2$; otras de peso $1/5$ relacionadas con trabajos de Klein y con las identidades de Rogers-Ramanujan ([Hub14],[Man02],[Kan06]), y existe una familia de formas modulares de peso $(N-3)/(2N)$ para cualquier N impar [Ibu00]), sería deseable extender el resultado a pesos mayores. La principal limitación y al mismo tiempo el hecho que cambiaría completamente las reglas del juego es la posibilidad de que el exponente Hölder esperado sea mayor que 1. Si nuestras conjeturas son ciertas, el Teorema 3.7 debería seguir siendo cierto sin pedir que α y r sean menores que 1 (únicamente bajo $r < \alpha < r + 1/2$), teniendo los puntos $x \in A_c^*$ exponente Hölder $\alpha - r + r/1$. Esta cantidad será menor que 1 si y sólo si $c > r(1-\alpha+r)^{-1}$

(nótese que la expresión de la derecha toma valores entre r y $2r$). Para que esto ocurra para todo $c \geq 2$, la restricción que se impone es $\alpha < r + 1/2$ (que es ligeramente menos fuerte que la que tomamos nosotros, $\alpha, r < 1$). Para valores mayores, el exponente Hölder esperado podrá ser mayor que 1 y la fórmula $f_\alpha(x+h) - f_\alpha(x)$ ya no será válida para obtenerlo (recordemos que sólo servía si tal exponente era menor que 1). En ese caso la función f podría admitir una o varias derivadas en x (dependiendo del tamaño del exponente Hölder), y el problema cambiaría notablemente. Para el caso de series de Eisenstein, recientemente se han obtenido resultados parciales para pesos pares, utilizando las técnicas de Jaffard [Pet13].

- Para $1 \leq \alpha < r + 1/2$, el exponente Hölder esperado sería aún menor que 1, pero no nos ha sido posible obtener el espectro de singularidades en ese caso, porque el Lema 3.10 no es suficiente tal y como está planteado. Es posible que el hecho de que α sea mayor que 1 cambie radicalmente la composición de la integral Gamma y el problema deba estudiarse desde otro ángulo.

- Incluso cuando no se cumple $2 > r(1 - \alpha + r)^{-1}$, el Teorema 3.7 sería cierto para valores de c grandes; es decir, sean lo grandes que sean α y δ, el Teorema sería cierto para $c \gg r$. Con lo cual, en todos esos casos hemos ya demostrado que f_α es un multifractal, si bien la caracterización de su espectro está mucho más incompleta.

Bibliografía

[AB04] M. Alsina and P. Bayer. *Quaternion orders, quadratic forms, and Shimura curves*, volume 22 of *CRM Monograph Series*. American Mathematical Society, Providence, RI, 2004.

[Are05] A. Arenas. Operadors de Hecke. Fórmula de les traces. In *Corbes de Shimura*, pages 75–90. Publicacions de la Universitat de Barcelona, 2005.

[Bes] A. S. Besicovitch. Sets of Fractional Dimensions (IV): On Rational Approximation to Real Numbers. *J. London Math. Soc.*, S1-9(2):126.

[BH62] P. T. Bateman and R. A. Horn. A heuristic asymptotic formula concerning the distribution of prime numbers. *Math. Comp.*, 16:363–367, 1962.

[BHC62] A. Borel and Harish-Chandra. Arithmetic subgroups of algebraic groups. *Ann. of Math. (2)*, 75:485–535, 1962.

[BJ99] J. Bolte and S. Johansson. A spectral correspondence for Maaß waveforms. *Geom. Funct. Anal.*, 9(6):1128–1155, 1999.

[Bor00] P. Borwein. An efficient algorithm for the Riemann zeta function. In *Constructive, experimental, and nonlinear analysis (Limoges, 1999)*, volume 27 of *CMS Conf. Proc.*, pages 29–34. Amer. Math. Soc., Providence, RI, 2000.

[BPPV84] R. Benzi, G. Paladin, G. Parisi, and A. Vulpiani. On the multifractal nature of fully developed turbulence and chaotic systems. *J. Phys. A*, 17(18):3521–3531, 1984.

[BS86] P. L. Butzer and E. L. Stark. "Riemann's example" of a continuous nondifferentiable function in the light of two letters (1865) of Christoffel to Prym. *Bull. Soc. Math. Belg. Sér. A*, 38:45–73 (1987), 1986.

[BSV06] A. R. Booker, A. Strömbergsson, and A. Venkatesh. Effective computation of Maass cusp forms. *Int. Math. Res. Not.*, pages Art. ID 71281, 34, 2006.

[Cas72] J. W. S. Cassels. *An introduction to Diophantine approximation*. Hafner Publishing Co., New York, 1972. Facsimile reprint of the 1957 edition, Cambridge Tracts in Mathematics and Mathematical Physics, No. 45.

[CC92] J. Cilleruelo and A. Córdoba. *La teoría de los números*. Bilbiloteca Mondadori. Mondadori España, Madrid, 1992.

[CC99] F. Chamizo and A. Córdoba. Differentiability and dimension of some fractal Fourier series. *Adv. Math.*, 142(2):335–354, 1999.

[Cha99] F. Chamizo. Correlated sums of $r(n)$. *J. Math. Soc. Japan*, 51(1):237–252, 1999.

[Cha04] F. Chamizo. Automorphic forms and differentiability properties. *Trans. Amer. Math. Soc.*, 356(5):1909–1935 (electronic), 2004.

[Clo11] B. Cloitre. 10 conjectures in additive number theory. ArXiv:1101.4274, 2011.

[CR10] F. Chamizo and D. Raboso. Modular forms and quasi-integers (Spanish). *Gac. R. Soc. Mat. Esp.*, 13(3):539–555, 2010.

[CRRC11] F. Chamizo, D. Raboso, and S. Ruiz-Cabello. On Rowland's sequence. *Electron. J. Combin.*, 18(2):Paper 10, 10, 2011.

[CRRC13] F. Chamizo, D. Raboso, and S. Ruiz-Cabello. Exotic approximate identities and Maass forms. *Acta Arith.*, 159(1):27–46, 2013.

[CU07] F. Chamizo and A. Ubis. Some Fourier series with gaps. *J. Anal. Math.*, 101:179–197, 2007.

[CU12] F. Chamizo and A. Ubis. Multifractal behavior of polynomial fourier series. To appear in *Advances in Mathematics*, 2012.

[Dir69] G. L. Dirichlet. *Mathematische Werke. Bände I, II*. Herausgegeben auf Veranlassung der Königlich Preussischen Akademie der Wissenschaften von L. Kronecker. Chelsea Publishing Co., Bronx, N.Y., 1969.

[dlHV13] F. de la Hoz and L. Vega. Vortex filament equation for a regular polygon. arXiv:1304.5521, 2013.

[DR55] H. Davenport and K. F. Roth. Rational approximations to algebraic numbers. *Mathematika*, 2:160–167, 1955.

[Edg04] G. A. Edgar, editor. *Classics on fractals*. Studies in Nonlinearity. Westview Press. Advanced Book Program, Boulder, CO, 2004.

[Fal90] K. Falconer. *Fractal geometry*. John Wiley & Sons Ltd., Chichester, 1990. Mathematical foundations and applications.

[Fat04] P. Fatou. Sur l'approximation des incommenurables et les series trigonométriques. *C. R. Acad. Sci. Paris*, 139:1019–1021, 1904.

[FL] D. W. Farmer and S. Lemurell. Maass forms and their L-functions. *Preprint* `http://www.math.chalmers.se/~sj/forskning.html`.

[GBGL08] T. Gowers, J. Barrow-Green, and I. Leader, editors. *The Princeton companion to mathematics*. Princeton University Press, Princeton, NJ, 2008.

[Ger70] J. Gerver. The differentiability of the Riemann function at certain rational multiples of π. *Amer. J. Math.*, 92:33–55, 1970.

[GR07] I. S. Gradshteyn and I. M. Ryzhik. *Table of integrals, series, and products*. Elsevier/Academic Press, Amsterdam, seventh edition, 2007. Translated from the Russian, Translation edited and with a preface by Alan Jeffrey and Daniel Zwillinger, With one CD-ROM (Windows, Macintosh and UNIX).

[Har16] G. H. Hardy. Weierstrass's non-differentiable function. *Trans. Amer. Math. Soc.*, 17(3):301–325, 1916.

[Hej76] D. A. Hejhal. The Selberg trace formula and the Riemann zeta function. *Duke Math. J.*, 43(3):441–482, 1976.

[Hej85] D. A. Hejhal. A classical approach to a well-known spectral correspondence on quaternion groups. In *Number theory (New York, 1983–84)*, volume 1135 of *Lecture Notes in Math.*, pages 127–196. Springer, Berlin, 1985.

[HR92] D. A. Hejhal and B. N. Rackner. On the topography of Maass waveforms for PSL$(2, \mathbf{Z})$. *Experiment. Math.*, 1(4):275–305, 1992.

[Hub14] T. Huber. A theory of theta functions to the quintic base. *J. Number Theory*, 134:49–92, 2014.

[Ibu00] T. Ibukiyama. Modular forms of rational weights and modular varieties. *Abh. Math. Sem. Univ. Hamburg*, 70:315–339, 2000.

[IS95] H. Iwaniec and P. Sarnak. L^∞ norms of eigenfunctions of arithmetic surfaces. *Ann. of Math. (2)*, 141(2):301–320, 1995.

[Iwa97] H. Iwaniec. *Topics in classical automorphic forms*, volume 17 of *Graduate Studies in Mathematics*. American Mathematical Society, Providence, RI, 1997.

[Iwa02] H. Iwaniec. *Spectral methods of automorphic forms*, volume 53 of *Graduate Studies in Mathematics*. American Mathematical Society, Providence, RI, second edition, 2002.

[Jaf94] S. Jaffard. Some mathematical results about the multifractal formalism for functions. In *Wavelets: theory, algorithms, and applications (Taormina, 1993)*, volume 5 of *Wavelet Anal. Appl.*, pages 325–361. Academic Press, San Diego, CA, 1994.

[Jaf96] S. Jaffard. The spectrum of singularities of Riemann's function. *Rev. Mat. Iberoamericana*, 12(2):441–460, 1996.

[Jaf97] S. Jaffard. Old friends revisited: the multifractal nature of some classical functions. *J. Fourier Anal. Appl.*, 3(1):1–22, 1997.

[Jar31] V. Jarník. Über die simultanen diophantischen Approximationen. *Math. Z.*, 33(1):505–543, 1931.

[Kan06] M. Kaneko. On modular forms of weight $(6n + 1)/5$ satisfying a certain differential equation. In *Number theory*, volume 15 of *Dev. Math.*, pages 97–102. Springer, New York, 2006.

[Lan66] S. Lang. *Introduction to diophantine approximations*. Addison-Wesley Publishing Co., Reading, Mass.-London-Don Mills, Ont., 1966.

[Lio44] J. Liouville. Nouvelle démonstration d'un théorème sur les irrationalles algébriques, inséré dans le *compte rendu* de la dernière séance. *C. R. Acad. Sci. Paris*, 18:910–911, 1844.

[Lio51] J. Liouville. Sur des classes très-étendues de quantités dont la valeur n'est ni algébrique, ni même réductible à des irrationelles algébriques. *J. Math. pures appl*, 16:133–142, 1851.

[Maa49] H. Maass. Über eine neue Art von nichtanalytischen automorphen Funktionen und die Bestimmung Dirichletscher Reihen durch Funktionalgleichungen. *Math. Ann.*, 121:141–183, 1949.

[Man02] T. Mano. Differential relations for modular forms of level five. *J. Math. Kyoto Univ.*, 42(1):41–55, 2002.

[Miy06] T. Miyake. *Modular forms*. Springer Monographs in Mathematics. Springer-Verlag, Berlin, english edition, 2006. Translated from the 1976 Japanese original by Yoshitaka Maeda.

[MS04] S. D. Miller and W. Schmid. The highly oscillatory behavior of automorphic distributions for SL(2). *Lett. Math. Phys.*, 69:265–286, 2004.

[ORW99] A. Odlyzko, M. Rubinstein, and M. Wolf. Jumping champions. *Experiment. Math.*, 8(2):107–118, 1999.

[Pet13] I. Petrykiewicz. Hölder regularity of arithmetic fourier series arising from modular forms. arXiv:1311.0655v2, 2013.

[Ram00] S. Ramanujan. Modular equations and approximations to π [Quart. J. Math. **45** (1914), 350–372]. In *Collected papers of Srinivasa Ramanujan*, pages 23–39. AMS Chelsea Publ., Providence, RI, 2000.

[Row08] E. S. Rowland. A natural prime-generating recurrence. *J. Integer Seq.*, 11(2):Article 08.2.8, 13, 2008.

[Sel56] A. Selberg. Harmonic analysis and discontinuous groups in weakly symmetric Riemannian spaces with applications to Dirichlet series. *J. Indian Math. Soc. (N.S.)*, 20:47–87, 1956.

[SS58] A. Schinzel and W. Sierpiński. Sur certaines hypothèses concernant les nombres premiers. *Acta Arith. 4 (1958), 185–208; erratum*, 5:259, 1958.

[Str01] A. Strömbergsson. Some remarks on a spectral correspondence for Maass waveforms. *Internat. Math. Res. Notices*, (10):505–517, 2001.

[Ter85] A. Terras. *Harmonic analysis on symmetric spaces and applications. I*. Springer-Verlag, New York, 1985.

[Vig80] M.-F. Vignéras. *Arithmétique des algèbres de quaternions*, volume 800 of *Lecture Notes in Mathematics*. Springer, Berlin, 1980.

[Wor81] R. T. Worley. Estimating $\alpha - p/q$. *J. Austral. Math. Soc. Ser. A*, 31(2):202–206, 1981.

[WW62] E. T. Whittaker and G. N. Watson. *A course of modern analysis. An introduction to the general theory of infinite processes and of analytic functions: with an account of the principal transcendental functions*. Fourth edition. Reprinted. Cambridge University Press, New York, 1962.

Índice alfabético

acción de grupo, 5, 34, 63, 69
aleatorio, 88
álgebra, 54, 55
álgebra de división, 54
algebraico, número, 87
aproximación diofántica, 73, 86, 87
asintótica, fórmula, 9, 73, 77, 81, 83, 86, 94, 96
autosemejanza, 65, 66

Bessel, funciones de, 42
Beta, función, 41, 81–83

Cantor, conjunto de, 65, 66
Cauchy, Fórmula integral de, 76
clase de congruencia, 91, 92, 96
combinatoria, 1
convergentes de la fracción continua, 10, 78, 85, 86, 88, 89, 92
convolución hiperbólica, 40
coordenadas polares hiperbólicas, 39, 40
cuaterniones, álgebra de, 7, 35, 53–55, 57, 60
cúspide, 6, 10, 37–39, 48, 53, 63, 68–72, 74, 75, 78, 91
cúspide, anchura de, 75
cúspides, clase de equivalencia de, 37, 70, 74, 75, 77, 89–92, 97

Dedekind, función η de, 11
desarrollo espectral, 7, 38, 49, 53, 57, 60, 62
Dirichlet, Peter G.L. (1805–1859), 10, 85
discriminante, 57
distancia hiperbólica, 4, 5, 34, 35, 57, 58, 68, 69
dominio fundamental, 5, 6, 35–38, 57, 58, 63, 69, 72

Eichler maximales, órdenes de, 56
Eichler, órdenes de, 55, 56
Eisenstein, series de, 6, 38, 48, 53, 98
espectro de singularidades, 7, 8, 11, 63–65, 67, 73, 85, 87, 96, 97
Euler, función φ de, 70, 94

formas cuspidales, 10, 71–73, 76, 89, 91, 95
formas modulares, 3, 9–11, 63, 68, 69, 71–74, 77, 97
fórmula de pretraza, 33, 39
Fourier, desarrollo de, 10, 33, 71, 74
Fourier, transformada de, 4, 5, 32, 33, 38
fracción continua, 10, 78, 85
fractal, 8, 9, 65, 66
función de decaimiento rápido, 4, 5, 32, 38, 61, 71, 76

Gamma, función, 41, 42, 77
gaussiana, 32
generadores de primos, 1, 13, 27
geodésica, 34, 39, 58, 69
grupo de estabilidad, 74
grupo fuchsiano, 5–7, 35–39, 44, 53–55
grupo fuchsiano co-compacto, 5, 6, 36–39, 44, 53, 55, 56, 60, 69
grupo fuchsiano de primera especie, 5, 35, 45, 47, 55, 63, 69, 70

Hamilton, cuaterniones de, 54, 55
Hardy, Godfrey H. (1877–1947), 2, 8, 21, 66
Hausdorff, dimensión de, 8–11, 64–67, 87, 88, 90, 92, 93, 95, 96
Hausdorff, medida de, 64
Hecke, operadores de, 7, 60
Hölder, exponente, 7–11, 64, 66, 67, 73, 77, 87, 96–98

identidades aproximadas, 3, 5–7, 31, 33, 49, 57, 58, 62
integral fraccionaria, 10, 11, 69, 71–73, 77
integral Gamma, 77, 98
isometría, 35, 69

Jacobi, función θ de, 9–11, 72, 97
Jarník-Besicovitch, Teorema de, 11, 73, 87

Landau, notación de, 9, 63
Laplace-Beltrami, operador de, 5, 6, 33, 37, 40
laplaciano, operador, 4, 5, 32, 37
Lebesgue, medida de, 64, 87, 97
Legendre, criterio de, 86
Liouville, constante de, 87
Liouville, números de, 87

Maass, formas de, 5, 31, 33, 37, 38, 60
Maass, Hans (1911-1992), 5, 38
Mandelbrot, Benoit (1924–2010), 65
matriz de escala, 39, 74
medida, 88, 95
medida hiperbólica, 34, 35
Minkowski, dimensión de, 66
multifractal, 7–10, 63–68, 98

núcleo automorfo, 5, 7, 32, 33, 38, 45, 53, 60
número primo, Teorema del, 26

órbita, 35, 37, 38, 69
orden, 54, 55, 60, 61

Parseval, identidad de, 9
peso de una forma modular, 10, 11, 71–73, 77, 97, 98
Poincaré, métrica de, 4, 34, 35, 37, 69
Poincaré, semiplano de, 4, 33, 34, 37, 63
Poisson, fórmula de sumación de, 4, 31
polígono hiperbólico, 34, 69
polo, 81
primos en progresiones aritméticas, Teorema de los, 94
primos gemelos, 2
punto del infinito, 6, 36, 37, 70, 74, 75

Ramanujan, constante de, 3, 33
recta real extendida, 35, 36, 39, 69
recurrencia, 1, 65, 66, 85, 94
Riemann, Bernhard (1828–1866), 8, 37, 66
Riemann, ejemplo de, 8, 9, 63, 66, 67, 69, 97
Roth, Teorema de, 87
Rowland generalizada, sucesión de, 1, 2, 15, 17–19
Rowland, cadena de, 2, 3, 27–29
Rowland, sucesión de, 1–3, 13–16, 19, 25, 27

Selberg, Atle (1917-2007), 5, 39
Selberg, transformada de, 5, 38–44, 49, 53, 59, 61
sistema de multiplicadores, 71

teorema chino del resto, 28
teoría de números, 2, 21
teoría espectral de formas automorfas, 5, 33

variedad riemanniana, 69

Weierstrass, Karl (1815–1897), 8, 66