Departamento de Matemáticas
Facultad de Ciencias
Universidad Autónoma de Madrid

Tesis Doctoral

Métodos espectrales, combinatorios y analíticos en algunos problemas de teoría de números

Dulcinea Raboso Paniagua

Dirigida por
Fernando Chamizo Lorente

Madrid, 2014

Como todos los soñadores,
confundí el desencanto con la verdad.

J.P. Sartre

Índice general

Introducción

Al pensar que todo podía explicarse con los números, los Pitagóricos establecieron gran cantidad de clasificaciones entre estos y se dedicaron a descubrir sus propiedades. Así iniciaron una rama de las matemáticas que hoy se conoce como la teoría de números.

En la actualidad, son varias las áreas que engloba la teoría y existen centenares de problemas no resueltos, apareciendo nuevos problemas más rápidamente que se resuelven los antiguos, de temas tan dispares que debemos estar dispuestos a utilizar cualquier método que tengamos a mano. De este modo, podemos clasificarlos por los métodos utilizados y no por la forma en que se expresen. Con esta idea, el presente trabajo se divide en tres partes de acuerdo al punto de vista y a las herramientas usadas en cada una de ellas. Temas relacionados con formas automorfas, teoría espectral, teoría combinatoria, métodos de criba, sumas trigonométricas y puntos del retículo. Esta diversidad refleja mi gran interés en distintas áreas de la teoría de números y de las matemáticas en general.

Con esta introducción se intenta motivar los distintos resultados de la memoria. Una exposición indicando el origen del tema en la historia y sus principales protagonistas junto con un breve desarrollo de conceptos e ideas del mismo podría ser más que suficiente para este fin. Aun así, siempre y cuando sea posible, se intentará incluir algunos ejemplos e ideas generales de forma que sirvan al posible lector para acercarse a la teoría y al mismo tiempo, como invitación a seguir leyendo.

La primera parte trata sobre métodos espectrales y consta de tres capítulos. El primero de ellos a modo de introducción, es una recopilación de conceptos y resultados preliminares.

La teoría de formas automorfas tiene sus orígenes en los trabajos de Riemann, Klein y Poincaré con la introducción de funciones automorfas o fuchsianas (denominadas así por el propio Poincaré). Desde entonces ha experimentado un enorme desarrollo estableciendo conexiones con diferentes áreas. El estudio llevado por E. Hecke (1887–1947) abría las puertas a la teoría aritmética de las formas modulares, mientras que el trabajo de C.L. Siegel (1896–1981) sobre formas cuadráticas con coeficientes enteros puso de manifiesto la intervención de la teoría de los grupos de Lie. A principios de los años 80, N.V. Kuznetsov probó una fórmula espectral

con potenciales aplicaciones aritméticas que contenía unas sumas introducidas por H.D. Kloosterman más de cincuenta años atrás. Más recientemente, numerosos autores han proporcionado avances considerables en relación con la teoría analítica de números. Pero sin duda, es prácticamente imposible no hablar de la aportación de Maass y Selberg, cuyo trabajo supuso la introducción de la teoría espectral.

A pesar de que sería natural que las formas de Maass surgieran dentro del análisis armónico y ecuaciones diferenciales parciales, en 1949 H. Maass (1911–1992) las introduce para resolver un problema relacionado con funciones L en cuerpos cuadráticos reales [Maa49] (una idea al respecto se puede ver en [Rab13]). En los años siguientes A. Selberg (1917–2007) dirige su atención a estas nuevas formas automorfas no holomorfas, desarrollando la teoría y obteniendo el resultado que le ha dado más fama, la *fórmula de traza de Selberg*.

Nosotros nos quedaremos con una fórmula precedente a la anterior, basada en el desarrollo espectral de núcleos automorfos y conocida como fórmula de pretraza, en la que se basan los principales resultados de la Parte I.

Un tema básico en el análisis armónico es la expresión de una función como superposición de "tonos puros" que suelen ser autofunciones de un operador. Por ejemplo, en el caso de las series de Fourier clásicas,

$$f(x) = \sum a_n e(nx) \qquad \text{con} \qquad e(x) = e^{2\pi i x}$$

donde $e(nx)$ son autofunciones del operador laplaciano $\Delta f = -f''$, que está bien definido para funciones regulares 1-periódicas, es decir, invariantes por traslaciones enteras.

La teoría espectral de formas automorfas surge cuando se cambia $\mathbb{R}$ por el *semiplano de Poincaré* $\mathbb{H} = \{x + iy \ : \ x \in \mathbb{R},\ y \in \mathbb{R}^+\}$ y se consideran las funciones, llamadas automorfas, que son invariantes por un grupo fuchsiano (de primera especie) Γ. Asociado a la distancia hiperbólica en $\mathbb{H}$ hay un operador laplaciano natural Δ, el *operador de Laplace-Beltrami*

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

cuyas autofunciones bajo ciertas condiciones de crecimiento son las formas de Maass.

El conjunto de órbitas $\Gamma\backslash\mathbb{H}$ se puede interpretar geométricamente mediante un dominio fundamental con identificaciones en la frontera, de hecho siempre se puede elegir como dominio fundamental un polígono hiperbólico. Cuando es compacto, las formas de Maass son de cuadrado integrable y se tiene un desarrollo en autofunciones análogo al de Fourier clásico:

$$f(z) = \sum c_j u_j(z) \qquad \text{con} \qquad u_j \text{ formas de Maass en } L^2(\Gamma\backslash\mathbb{H}).$$

Por otro lado, cuando el dominio fundamental no es compacto, tiene vértices, llamados cúspides, en $\{\Im z = 0\} \cup \{\infty\}$. Asociadas a cada una de estas cúspides hay

unas formas de Maass, las series de Eisenstein, que no son de cuadrado integrable pero que también participan en la descomposición espectral. Tenemos, entonces, una situación más compleja que en las series de Fourier, pues ahora el desarrollo espectral de una función consta tanto de espectro discreto como de espectro continuo.

En la búsqueda de funciones que muestren las simetrías expresadas por un grupo finito podemos simplemente considerar la suma de las acciones de estas simetrías en la función. Esto es un hecho común en el caso euclídeo y que permite deducir la fórmula de sumación de Poisson. Para ello basta considerar las isometrías dadas por traslaciones enteras $T = \{x \to x+n \ : \ n \in \mathbb{Z}\}$ con la distancia usual $d(x,y) = |x-y|$. Dada una función $f \in \mathcal{C}_0^\infty(\mathbb{R}^+)$, la expresión $f(d(x,y))$ es invariante si se aplica la misma isometría (no necesariamente una traslación entera) a x e y. Entonces, el *núcleo automorfo* se define como

$$K(x,y) = \sum_{g \in T} f\big(d(gx,y)\big) = \sum_{n} f(|n+x-y|).$$

Por otro lado, es fácil comprobar usando la propiedad aditiva de las autofunciones, que

$$\int_{\mathbb{R}} f(|x-y|)e(nx)\,dx = \widehat{f_p}(\sqrt{\lambda_n})e(ny), \tag{1}$$

donde $\widehat{f_p}$ es la transformada de Fourier de la extensión par de f y $\lambda_n = 4\pi^2 n^2$ es el autovalor asociado a la autofunción $e(nx)$. A partir de este resultado y considerando $\mathbb{R}$ como unión de $g([0,1))$ con $g \in T$, se llega al desarrollo de Fourier de K,

$$K(x,y) = \sum_{n} \widehat{f_p}(\sqrt{\lambda_n})e(nx)\overline{e(ny)}.$$

La idea en el plano $\mathbb{R}^2$ es muy similar salvo porque (1) es más complicado ya que aparecen transformadas de Hankel [Ven90, Ch.3] [Iwa02, Ch.0].

En el semiplano de Poincaré, nuestro interés recae sobre núcleos automorfos del tipo

$$K(z,w) = \sum_{\gamma \in \Gamma} k\big(u(z,\gamma w)\big), \tag{2}$$

donde u es cierta función relacionada con la distancia hiperbólica. Bajo ciertas condiciones de regularidad y decaimiento en k, la definición anterior tiene sentido y su desarrollo espectral se conoce como *fórmula de pretraza*,

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

donde h es la transformada de Selberg de la función k, el análogo hiperbólico de la transformada de Fourier, y los valores t_j se relacionan con los autovalores de las

formas de Maass cuspidales $u_j(z)$, junto con la función constante u_0. Los puntos suspensivos representan la parte continua del espectro asociadas a las cúspides del grupo.

En el caso euclídeo, al considerar la traza del núcleo automorfo, integrando en $x = y$, obtenemos la fórmula de sumación de Poisson. Con un aumento considerable en cuanto a dificultad y trabajo, en el caso hiperbólico esto conduce a la fórmula de traza de Selberg la cual establece una relación clara entre los autovalores y las longitudes de las geodésicas cerradas y tiene algunas interpretaciones aritméticas directas (por ejemplo, [Sar82]). Este es un excelente resultado dentro de la teoría espectral de formas automorfas, pero la fórmula de Kuznetsov [Kuz80] ha sido la que ha proporcionado la interacción más profunda entre la teoría espectral y la teoría de números.

En el Capítulo 2, nuestro estudio se centra en esta fórmula. Con ella se establece una conexión entre objetos espectrales, coeficientes de Fourier de formas de Maass $\nu_j(n)$ normalizados, y objetos aritméticos, sumas de Kloosterman, $S(n, m; c)$.

La fórmula de Kuznetsov, principalmente a través de la obra de H. Iwaniec y sus colaboradores, se convirtió en una herramienta fundamental en la teoría analítica de números moderna. Supuso una gran revolución que dio en llamarse *Kloostermania*, sorprendiendo por sus numerosas aplicaciones. La representación en términos de sumas de Kloosterman permite el uso de la cota de Weil propia de la geometría algebraica, así como otras ideas de la teoría de sumas trigonométricas. Con esta fórmula a menudo se consigue mejorar términos de error en distintos problemas, ya que las sumas de Kloosterman aparecen de forma natural en muchas aplicaciones dentro de la teoría de números.

Para $\mathrm{PSL}_2(\mathbb{Z})$, la *fórmula de Kuznetsov* esencialmente establece que

$$\sum_j h(t_j)\nu_j(n)\nu_j(m) + \cdots = \sum_{c=1}^{\infty} \frac{1}{c} S(n, m; c)\ H\Big(\frac{4\pi\sqrt{|mn|}}{c}\Big) + \dots$$

donde H es cierta transformada integral de h, y los puntos suspensivos representan la contribución del espectro continuo.

El problema es que técnicamente es difícil de aplicar porque la transformada H es muy complicada y además asimétrica en los casos $mn > 0$ y $mn < 0$. Por otra parte, no es nada fácil dar una prueba completa. Una pregunta natural, y que surge en las aplicaciones, es si dada la función H se puede conseguir la correspondiente h, en otras palabras, si a partir de un promedio arbitrario de sumas de Kloosterman se recupera una suma espectral. El problema radica en si la trasformada integral $h \to H$ se puede invertir, y así ocurre para $mn < 0$, sin embargo para $mn > 0$ la transformada no es sobreyectiva en espacios razonables de funciones y esto no es posible. Curiosamente, en este caso, tomando h como cierta transformada de H,

ambos miembros de la fórmula de Kuznetsov difieren en una cantidad que depende de los coeficientes de Fourier de las formas modulares cuspidales clásicas. En las aplicaciones su contribución es menor pero necesaria si se quiere tener una igualdad.

Nuestra contribución resuelve estos problemas: En el Teorema 2.2.1 damos una nueva formulación de la fórmula de Kuznetsov cuya prueba es asombrosamente breve y accesible, no usa nada que vaya más allá de la fórmula de pretraza. En ella la única transformada integral es una sencilla transformada de Hankel (integración contra J_0, la función de Bessel más básica) esta vez del núcleo k asociado a h, y la única diferencia entre los casos $mn > 0$ y $mn < 0$ es que una constante sea 0 o 1. Concretamente

$$H(x) = 4\pi x \int_0^\infty k(r) J_0\big(x\sqrt{r+\epsilon_0}\big)\, dr \qquad \text{con} \quad 2\epsilon_0 = 1 + \operatorname{sgn}(mn).$$

El problema de la fórmula inversa, Teorema 2.3.1, admite ahora una solución más limpia y rápida. En el Teorema 2.4.1 probamos que nuestra formulación es equivalente a la clásica.

Por otro lado, ilustramos cómo el escribir la fórmula de esta forma sencilla en términos del núcleo es realmente útil no solo en su demostración, también facilita estimaciones deduciendo de manera muy simple la acotación de $\sum |\nu_j(n)|^2$, Corolario 2.5.3. Además, permite obtener ejemplos explícitos para la fórmula de Kuznetsov usando algunas fórmulas cerradas para pares k y h tratadas en la Sección 3.2, lo que enlaza con el siguiente capítulo.

El trabajo realizado en el Capítulo 3 conduce a la obtención de *identidades aproximadas*, partiendo de nuevo de la fórmula de pretraza. La teoría de formas modulares provee de numerosos ejemplos de identidades aproximadas. Como muestra, podemos considerar

$$\frac{1}{4}\Big(\sum_{n=-15}^{15} e^{-n^2/4}\Big)^2 = 3.141592653589793328\ldots$$

$$\pi = 3.141592653589793238\ldots$$

y

$$e^{\pi\sqrt{163}} = 262537412640768743.999999999999250\ldots$$

$$744 + 640320^3 = 262537412640768744$$

Ambas aproximaciones están ligadas al desarrollo de Fourier de formas modulares clásicas. El primero se trata de una aproximación de π, con el que se consiguen hasta 15 decimales de precisión a través de la función θ. El segundo es la conocida constante de Ramanujan que difiere de un entero menos que 10^{-12} y se basa en un valor especial del invariante j. Una demostración autocontenida se puede ver en [CR10].

Nuestra contribución es la de encontrar identidades de este tipo, identidades aproximadas a las que denominamos "exóticas" porque utilizamos la teoría de formas

automorfas en lugar del análisis armónico euclídeo. Para ello, y esto es algo que nos parece interesante, recurrimos a herramientas muy diversas. Se trabaja con formas de Maass, en lugar de con las clásicas formas modulares holomorfas, en el semiplano de Poincaré bajo la acción de grupos de congruencias y grupos asociados a álgebras de cuaterniones.

El estudio de grupos especiales permite dar un sentido aritmético a los núcleos automorfos. Por ejemplo, consideremos $\widetilde{\Gamma}$ el grupo definido como el subgrupo de $\mathrm{PSL}_2(\mathbb{Z})$ tal que $a_{11}+a_{22}$ y $a_{12}+a_{21}$ son ambos pares. Un cálculo prueba que para cualquier $\gamma=(a_{ij})\in \mathrm{PSL}_2(\mathbb{R})$

$$\begin{cases} 4u(\gamma i,i)=(a_{11}-a_{22})^2+(a_{12}+a_{21})^2 \\ 4u(\gamma i,i)+4=(a_{11}+a_{22})^2+(a_{12}-a_{21})^2 \end{cases}$$

y si $\gamma\in\widetilde{\Gamma}$, estas cantidades son múltiplos de 4, digamos $4n$ y $4n+4$. De modo que, tomando $z=w=i$, podemos escribir (2) como

$$K(i,i)=\frac{1}{2}\sum_{n=0}^{\infty} r(n)r(n+1)k(n),$$

donde $r(n)=\#\{(a,b)\in\mathbb{Z}^2 \ : \ a^2+b^2=n\}$. Además, $\widetilde{\Gamma}$ tiene solo dos cúspides y podemos relacionar las series de Eisenstein asociadas con una función L y la función zeta de Riemann, obteniendo el desarrollo espectral

$$K(i,i)=4\int_0^{\infty} k(x)\,dx+\sum_{j=1}^{\infty} h(\widetilde{t}_j)|u_j(i)|^2+\frac{2}{\pi}\int_{-\infty}^{\infty} h(t)\Big|\frac{f(t)}{1+2^{\frac{1}{2}+it}}\Big|^2\,dt,$$

donde $f(t)=\zeta(s)L(\chi,s)/\zeta(2s)$ con $s=1/2+it$ y χ es un carácter no principal módulo 4.

Típicamente, el término principal en el desarrollo espectral de núcleos automorfos viene dado por la autofunción constante u_0, y el término de error en esta aproximación se relaciona con el tamaño de los autovalores. Por ejemplo, si tomamos $k(u)=(u+1)^{-m}$ con m un entero mayor que 1, obtenemos aproximaciones de π cuya exactitud depende en este caso de $\widetilde{\lambda}_1$, el menor autovalor no trivial en $\widetilde{\Gamma}\backslash\mathbb{H}$.

Un argumento similar, considerando el grupo $\mathrm{PSL}_2(\mathbb{Z})$ en lugar de $\widetilde{\Gamma}$, da

$$\sum_{n=0}^{\infty}\big(3+(-1)^n\big)r(n)r(n+4)k\big(\frac{n}{4}\big)$$
$$=96\int_0^{\infty} k(x)\,dx+8\sum_{j=1}^{\infty} h(t_j)|u_j(i)|^2+\frac{8}{\pi}\int_{-\infty}^{\infty} h(t)|f(t)|^2\,dt$$

En este caso, probamos una aproximación de π que ahora depende del tercer autovalor λ_3, pues $u_1(i) = u_2(i) = 0$ debido a ciertas simetrías. Y utilizamos estas ideas para demostrar que, definiendo

$$S = \sum_{n=0}^{\infty} \big(3 + (-1)^n\big) \frac{r(n)r(n+4)}{2(n+4)^2} \qquad \text{y} \qquad I = \int_{-\infty}^{\infty} \frac{\frac{1}{4} + t^2}{\cosh(\pi t)} |f(t)|^2 \, dt,$$

se cumple que $(S-3)/I$ no es π pero sobrepasa este valor en una cantidad menor que $4 \cdot 10^{-14}$.

Si el grupo es compacto, como es el caso de los grupos asociados a álgebras de cuaterniones, el desarrollo espectral únicamente contará con la parte discreta del espectro lo que llevará a fórmulas visualmente más atractivas. Por ejemplo,

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

está muy cerca de $72e^9\sqrt{\pi}$. De hecho, veremos que el error relativo no es cero, pero es menor que $3 \cdot 10^{-7}$.

Finalizamos el capítulo y con ello también la primera parte, con los operadores de Hecke T_m. En cierto sentido, esto supone una generalización de lo anterior. Cuando aplicamos tal operador a un núcleo automorfo respecto al grupo modular completo $\Gamma_0(1)$, la suma queda

$$T_m\Big(\sum_{\gamma \in \Gamma_0(1)} k(\gamma(\cdot), w)\Big)(z) = \frac{1}{\sqrt{m}} \sum_{\gamma \in \Gamma_m} k(\gamma z, w),$$

donde Γ_m son matrices enteras con determinante m. Entonces, formalmente, la aplicación del operador de Hecke corresponde a considerar en los núcleos automorfos matrices enteras de determinante entero en lugar de solo considerar aquellas con determinante 1.

En la Parte II hacemos uso de métodos combinatorios en distintos problemas. Los números primos siempre han suscitado el interés matemático y como no podía ser de otro modo, tratándose de una tesis en teoría de números, estos tienen un papel destacado.

C.F. Gauss (1777–1855) observó con sus gigantescas tablas de primos, que la densidad de éstos en la sucesión de números naturales decae como el inverso del logaritmo, esto es, el famoso Teorema de los Números Primos que demostraron Hadamard y De la Vallée-Poussin setenta años después.

Hasta la fecha, la búsqueda de una fórmula que proporcione tales números parece algo imposible, sin embargo existen resultados más modestos de fórmulas que suministran una cantidad amplia de primos.

Un breve repaso a la historia nos lleva a M. Mersenne (1588–1648) que trabajó con números de la forma $M_n = 2^n - 1$, dando una lista de exponentes primos para los cuales M_n era primo. En 1883, Pervushin y Lucas dieron con un primer error en la lista. E. Lucas desarrolló un método, que se conoce como test de Lucas, mediante el cual se comprueba si un número de Mersenne es o no primo. Considerando la sucesión definida recursivamente como $r_{n+1} = r_n^2 - 3$ con $r_1 = 3$, el número de Mersenne con p de la forma $p = 4k + 3$, es primo, si y sólo si M_p divide a r_{p-1}. Este método fue mejorado por Lehmer en 1930, y actualmente sirve para comprobar la fiabilidad de los supercomputadores.

Existen más resultados al respecto, como la conjetura errónea de Fermat por la que todos los números de la forma $F_n = 2^{2^n} + 1$ son primos, y que encuentra el primer fallo con $n = 5$.

Una curiosa fórmula para encontrar números primos es la que se deduce de la espiral de Ulam, que resulta de escribir los números enteros en forma de espiral y donde los primos muestran una tendencia a alinearse en diagonales dentro del cuadrado obtenido. Estudiando estas espirales para valores iniciales distintos a 1, la que comienza en 41 presenta una perfecta diagonal de números primos.

121	90	91	92	93	94	95	96	97
120	89	66	67	68	69	70	71	98
119	88	65	50	51	52	53	72	99
118	87	64	49	42	43	54	73	100
117	86	63	48	41	44	55	74	101
116	85	62	47	46	45	56	75	102
115	84	61	60	59	58	57	76	103
114	83	82	81	80	79	78	77	104
113	112	111	110	109	108	107	106	105

S.M. Ulam (1909–1984) trabajó con una fórmula que ya había sido propuesta por Euler:

$$P(m) = m^2 + m + 41,$$

con la que pueden encontrarse números primos para los cuarenta primeros valores de m. Para $1 \leq m \leq 107$, la fórmula anterior proporciona un número primo prácticamente de cada dos. A pesar de que existen otras fórmulas parecidas bastante eficientes, ninguna fórmula polinómica puede proporcionar todos los números primos. Por otro lado, G. Rabinowitz encontró una sorprendente relación con el número de clases, de la que deduce que $P(m)$ es, en cierto sentido, el ejemplo óptimo.

Algunas sucesiones definidas recursivamente también tienen sorprendentes propiedades relacionadas de una forma u otra con números primos. Nosotros nos interesamos por una sucesión en particular,

$$a_k = a_{k-1} + \mathrm{mcd}(k, a_{k-1}) \quad \text{con} \quad a_1 = 7,$$

que E.S. Rowland introduce en [Row08] probando que la diferencia entre dos términos consecutivos de tal sucesión es siempre 1 o un número primo.

k	1	2	3	4	5	6	7	8	9	10	11	...
a_k	7	8	9	10	15	18	19	20	21	22	33	...
$a_k - a_{k-1}$		1	1	1	5	3	1	1	1	1	11	...
					$\triangle$	$\triangle$					$\triangle$	

A partir de unas sucesiones auxiliares, la propiedad probada por Rowland admite una sencilla y corta demostración (Proposición 4.1.3). La generalización del resultado pasa por considerar otros valores iniciales, hecho que estudiamos en la Sección 4.1 tomando como condición inicial $a_1 > 3$ impar. Para ello, introducimos dos sucesiones generales

$$\begin{cases} r_1 = 1 \\ r_{n+1} = \text{mín}\left\{k > r_n \ : \ \text{mcd}(c_n, k) \neq 1\right\} \end{cases} \quad \text{y} \quad \begin{cases} c_1 = a_1 - 2 \\ c_{n+1} = c_n + \text{mcd}(c_n, r_{n+1}) - 1 \end{cases}$$

y probamos que la diferencia entre dos términos consecutivos de la sucesión de Rowland generalizada $a_k - a_{k-1}$ o bien es 1 o bien coincide con $\text{mcd}(c_{n-1}, r_n)$ (Proposición 4.1.4). Ahora ya no está claro que vayamos a obtener primos en la sucesión formada por las diferencias, pues todo depende de los factores comunes entre c_{n-1} y r_n. De hecho, existen contraejemplos en los que $a_k - a_{k-1}$ no es primo, pero son muy poco frecuentes. Los cálculos sugieren:

Conjetura A

Para cada sucesión de Rowland generalizada, existe $N \geq 1$ tal que $a_k - a_{k-1}$ es 1 o bien un primo para todo $k > N$.

Obviamente, esto equivale a probar que a partir de cierto valor, $\text{mcd}(c_{n-1}, r_n)$ es siempre primo. Fijado $a_1 > 3$ impar, para que la conjetura A sea cierta basta que se cumpla alguna de estas condiciones:

- ◊ Que exista n tal que $2r_n - 1 = c_n$.
- ⧫ Que exista m tal que c_m sea primo.

Un trabajo computacional sugiere que estos dos hechos ocurren siempre y, además, de forma consecutiva.

$a_1 = 7$

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	...

♦ ◊

$a_1 = 35$

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	...

♦ ◊

$a_1 = 117$

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	...

♦ ◊

Esto motiva las siguientes definiciones

$$n_0 = \text{ínf}\{n \in \mathbb{Z}^+ \,:\, c_n = 2r_n - 1\} \qquad \text{y} \qquad m_0 = \text{ínf}\{n \in \mathbb{Z}^+ \,:\, c_n \text{ es primo}\},$$

con $\text{ínf}\,\emptyset = \infty$, y nuestra segunda conjetura:

Conjetura B

$$\text{(i)} \quad n_0 < \infty, \qquad \text{(ii)} \quad m_0 < \infty, \qquad \text{(iii)} \quad n_0 = m_0 + 1 < \infty.$$

A pesar de no haber podido demostrar incondicionalmente la veracidad de estas conjeturas logramos establecer relaciones entre ellas, probando que las tres situaciones (i)-(iii) de la segunda guardan cierta jerarquía y que cualquiera de ellas daría lugar a la Conjetura A.

También nos interesamos por los primos que aparecen en la sucesión de diferencias de a_k, llegando a demostrar que estos son infinitos en la sucesión de Rowland, resultado que está sujeto a la Conjetura A para condiciones iniciales generales. Por otro lado, las sublistas finitas de primos que aparecen en $\{a_k - a_{k-1}\}$, a las que denominamos Cadenas de Rowland, admiten una caracterización que da lugar a interesantes observaciones sobre la frecuencia con la que aparecen ciertos primos, así como la imposición de restricciones en cuanto a su estructura.

El estudio de generadores de vectores pseudoaleatorios fue la principal motivación del Capítulo 5. Un número pseudoaleatorio es un número generado en un proceso que parece producir números aleatorios, sucesiones que a pesar de ser generadas por un algoritmo determinista, desde el punto de vista estadístico, no muestran un patrón aparente.

La función $k \mapsto g^k \pmod p$ con g un generador de $\mathbb{F}_p^*$ se emplea en la práctica como generador de números pseudoaleatorios. Nosotros buscamos un resultado análogo con matrices enteras no singulares de dimensión 2 y hacemos uso de métodos de criba para asegurar la existencia de buenos generadores.

La teoría de criba moderna tuvo un desarrolló espectacular durante la década de 1950, con la criba de Selberg y la gran criba, mostrándose como herramientas poderosas en teoría de números. En líneas generales, con los métodos de criba se estudia cómo se modifica el cardinal de un conjunto al eliminar clases de congruencia módulo ciertos primos. Esto es, para $\mathcal{A}$ un conjunto finito de enteros positivos y $\mathcal{P}$ un conjunto de primos, considerando el subconjunto $\mathcal{A}_p$ de los elementos de $\mathcal{A}$ correspondientes a ciertas clases de congruencia módulo p, el problema de criba consiste en estimar

$$\mathcal{Z} = \mathcal{A} \setminus \bigcup_{p \in \mathcal{P}} \mathcal{A}_p.$$

Seguramente, el procedimiento más básico que a uno se le ocurre cuando pretende encontrar los números primos contenidos en un determinado intervalo es la conocida criba de Eratóstenes. Este es un método muy popular para encontrar primos sucesivos eliminando los números divisibles por ciertos primos, o en relación a lo anterior, tomando $\mathcal{A}$ como los enteros positivos menores que cierto x y $\mathcal{A}_p$ aquellos pertenecientes a la clase del cero módulo ciertos primos, aunque por supuesto, el método no proporciona una regla para obtener ordenadamente una relación de todos ellos.

En diversos problemas de teoría analítica de números aparece el problema de obtener cancelación en una forma bilineal

$$\mathcal{B}(\vec{x}, \vec{y}) = \sum_{m=1}^{M} \sum_{n=1}^{N} x_m b_{mn} y_n \quad \text{con} \quad \vec{x} = (x_m)_{m=1}^{M},\ \vec{y} = (y_n)_{n=1}^{N} \ \text{ y } \ B = (b_{mn})_{m,n=1}^{M,N}$$

donde las coordenadas $\vec{x}$ e $\vec{y}$ tienen significado demasiado aritmético como para tratar de atacar directamente las sumas con métodos analíticos. La cota trivial aplicando dos veces la desigualdad de Cauchy-Schwarz es

$$\mathcal{B}(\vec{x}, \vec{y}) \leq \|\vec{x}\| \|\vec{y}\| \|B\|_2 \quad \text{con} \quad \|B\|_2 = \Big(\sum_{m=1}^{M} \sum_{n=1}^{N} |b_{mn}|^2 \Big)^{1/2}.$$

En términos generales se llama *desigualdad de gran criba* a una mejora de esta acotación para cierta B con $\vec{x}$ e $\vec{y}$ arbitrarios. Se busca extraer la cancelación inducida por la estructura de la forma bilineal con la idea de que la debida elección particular de $\vec{x}$ e $\vec{y}$ es intratable.

El nombre apareció por primera vez en el trabajo de Yu.V. Linnik (1915–1972) en 1941 y proviene de que algunas de estas desigualdades fueron fundamentales para

construir métodos de criba que permitían eliminar muchas clases de congruencia por primo.

Distintos autores han seguido desarrollando y simplificando estas técnicas, tales como Bombieri, Davenport, Montgomery, Selberg y Gallagher entre otros. La gran criba es un método útil para cribar sucesiones en las que se elimina muchas clases residuales por primo. Sin embargo, para sucesiones en las que se elimina en promedio más de la mitad de las clases residuales, es preferible utilizar la criba mayor introducida por P.X. Gallagher [FI10]. En [Gal71], la aplicó eliminando un número de clases residuales módulo p próximo al propio primo p. De estas cotas se desprende que, definiendo $\exp_p(n)$ como el orden de n en $\mathbb{F}_p^*$ e igual a 0 si $p \mid n$, es poco probable encontrar un n tal que $\exp_p(n)$ sea pequeño para muchos primos consecutivos, por lo que se espera que el uso de $k \mapsto n^k \pmod p$ como generador de números pseudoaleatorios, para p en un rango considerablemente grande, proporcione buenos resultados para casi cualquier elección de n.

En un contexto matricial, fijado un primo p, dada una matriz $M \in \mathrm{GL}_2(\mathbb{Z})$ tomamos los puntos

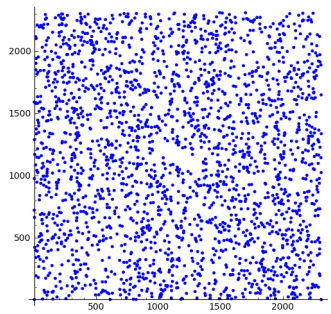
$$\begin{pmatrix} x_n \\ y_n \end{pmatrix} = M^n \begin{pmatrix} x_0 \\ y_0 \end{pmatrix},$$

siempre trabajando módulo p. Escribimos $\exp_p(M)$ para denotar el orden de la matriz M en $\mathrm{GL}_2(\mathbb{F}_p)$ cuando se reduce módulo p si $p \nmid \det(M)$ y $\exp_p(M) = 0$ si $p \mid \det(M)$.

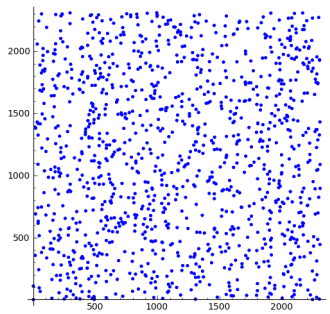
Por ejemplo, para el primo $p = 2311$, las matrices

$$A = \begin{pmatrix} 703 & 633 \\ 934 & 841 \end{pmatrix}, \quad B = \begin{pmatrix} 704 & 635 \\ 653 & 589 \end{pmatrix} \quad \text{y} \quad C = \begin{pmatrix} 703 & 787 \\ 862 & 965 \end{pmatrix}$$

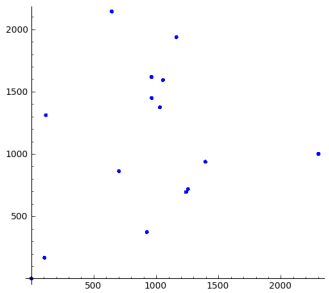
tienen ordenes $2310, 1155$ y 15 módulo p, respectivamente, y al tomar repetidas iteraciones se obtiene



$\exp_p(A) = p - 1$

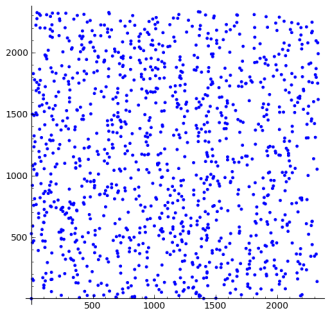


$\exp_p(B) = (p-1)/2$

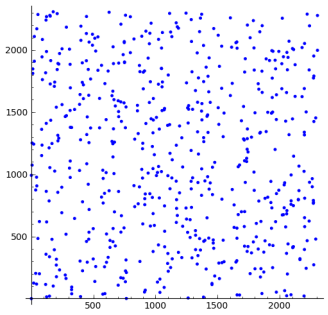


$\exp_p(C) = (p-1)/154$

Las imágenes muestran a la matriz C como un mal generador para $p = 2311$. Sin embargo, para $p = 2333$ y 2309 el orden de C pasa a ser 1167 y 577 respectivamente, obteniendo mejores resultados.



$\exp_p(C) = (p+1)/2$
$p = 2333$



$\exp_p(C) = (p-1)/4$
$p = 2309$

El análogo natural del intervalo $[0, N]$ en $\mathrm{SL}_2(\mathbb{Z})$ es el conjunto

$$\mathcal{I}_N = \left\{ A \in \mathrm{SL}_2(\mathbb{Z}) \ : \ 0 \leq a_{ij} \leq N \right\}.$$

Permitimos intervalos cortos de primos I, siempre que tengan densidad positiva y sean lo suficientemente grandes, mostrando que hay un valor x muy cercano al tamaño del intervalo tal que son pocas las matrices cuyo orden es menor que x. En concreto, probamos que si $|I| = N^\delta \geq 3$, entonces el número de matrices en $\mathcal{I}_N$ tales que

$$\exp_p(A) \leq CN^\delta \frac{\log\log N}{\delta(\log N)^2}$$

para todo $p \in I$ es menor que $N^{\delta+1} \log N (\log\log N)^2$. Resultado que generalizamos a matrices enteras no singulares arbitrarias, y que asegura la obtención de buenos generadores de vectores pseudoaleatorios.

En la Sección 5.4 tratamos cuestiones acerca de la distribución, obteniendo resultados sobre un tipo de discrepancia de estas matrices y sobre la distribución de sus potencias.

En la última parte de esta tesis cambiamos de registro, estando más centrada en los temas analíticos clásicos de la teoría de números.

Las sumas trigonométricas (o exponenciales) han desempeñado un importante papel en la teoría de números desde tiempos de Gauss, cuando fueron utilizadas para probar la ley de reciprocidad cuadrática.

En la solución de problemas particulares se utilizan distintos tipos de sumas que, en general, requieren algún tipo de reducción y que a menudo implican ingeniosas manipulaciones. La primera distinción básica se da entre una suma trigonométrica completa, típicamente una suma sobre todas las clases de residuos módulo algún entero N, y una suma incompleta donde el rango de la suma está restringido por alguna desigualdad.

Ejemplos de sumas trigonométricas completas son las sumas de Gauss y sumas de Kloosterman. Un ejemplo de suma incompleta es la suma parcial de las sumas

cuadráticas de Gauss. Una generalización natural de estas sumas son las sumas de Weyl:

$$\sum_{1\leq n\leq N} e\big(P(n)\big),$$

donde P es un polinomio con coeficientes reales. Las primeras estimaciones de este tipo de sumas aparecen en el famoso trabajo de H. Weyl (1885-1955) [Wey16] sobre distribución uniforme. Las sumas de Weyl desempeñan un papel fundamental en el estudio del problema de Waring. Éste consiste en probar que para cualquier entero $k \geq 2$ existe un entero $s = s(k) \in \mathbb{Z}^+$ tal que todo número natural N se puede expresar como $n_1^k + n_2^k + \cdots + n_s^k$ con n_i enteros no negativos. Aunque este hecho fue probado por Hilbert, su demostración combinatoria no daba idea acerca del mínimo valor de s ni del número de representaciones. Este último se relaciona con las sumas de Weyl mediante la fórmula

$$r_k(N) = \int_0^1 \Big(\sum_{n\leq N} e\big(\alpha n^k\big)\Big)^s e\big(-N\alpha\big)\, d\alpha.$$

G.H. Hardy (1877–1947) y J.E. Littlewood (1885–1977) tomaron una versión algo más compleja de esta identidad como punto de partida para el método del círculo. El tratamiento de los arcos mayores por este método implica el uso de sumas trigonométricas completas. I.M. Vinogradov (1891–1983) obtuvo avances importantes sobre el mínimo valor de s para enteros grandes con su método de sumas trigonométricas.

En general, uno puede elegir como fase cualquier función real f en lugar de un polinomio,

$$S = \sum_{a\leq n\leq b} e\big(f(n)\big).$$

Un caso importante se da al tomar f de tipo logarítmico, relacionado con la función zeta de Riemann.

El problema de conseguir acotaciones no triviales para este tipo de sumas aparece en teoría analítica de números en numerosas ocasiones tras utilizar el análisis de Fourier para escribir una función como superposición de ondas. Después de separar una amplitud no oscilatoria mediante sumación por partes, el estudio del promedio de la función en $[a, b] \cap \mathbb{Z}$ lleva a sumas como la anterior.

Los principales avances en el tema fueron el método de van der Corput (1920), y el método de Vinogradov (1930). La acotación más básica del método de van der Corput permite obtener acotaciones no triviales en rangos en los que la derivada segunda de la fase es moderadamente pequeña. La base del método de van der Corput [GK91] para estimar sumas trigonométricas es dividir el rango de sumación y aplicar una o varias veces la desigualdad de Cauchy para reducir la oscilación (Proceso

A) y transformar la nueva suma por medio de la fórmula de sumación de Poisson combinada con el método de fase estacionaria (Proceso B).

La sumación de Poisson es un arma fundamental que transforma cualquier suma suficientemente regular en una suma de integrales oscilatorias y la idea detrás del principio de fase estacionaria es que la mayor contribución de una integral oscilatoria proviene de los puntos en los que, en algún sentido, la frecuencia es nula.

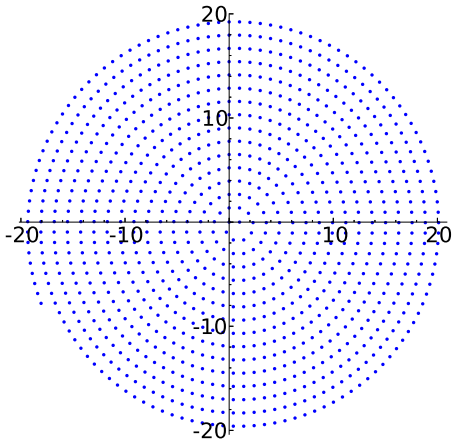
Para aplicar las ideas de método de van der Corput, se debe tener cierto control sobre alguna derivada de f. Por ejemplo, si $f'' \asymp \lambda$, se tiene

$$\sum_{n=1}^{N} e\big(f(n)\big) \ll N\lambda^{1/2} + \lambda^{-1/2}.$$

Entonces, cuando la derivada segunda es comparable a N^{-1}, la suma es menor que la raíz cuadrada del número de términos. Otro ejemplo, es que si f' es monótona y $|f'| \leq 1/2$,

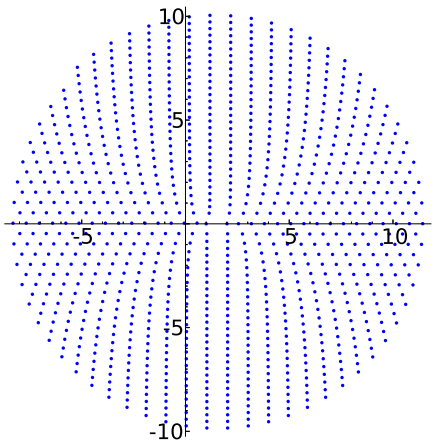
$$\sum_{n=1}^{N} e\big(f(n)\big) = \int_{1}^{N} e\big(f(x)\big)\, dx + O(1). \tag{3}$$

Un ejemplo curioso [Cha11] es el que ocurre al dibujar los números complejos $z_N = \sum_{n=1}^{N} e\big(\frac{1}{2}\sqrt{n}\big)$. El resultado revela una estructura de espiral que es inesperada si se desconoce el método de van der Corput.

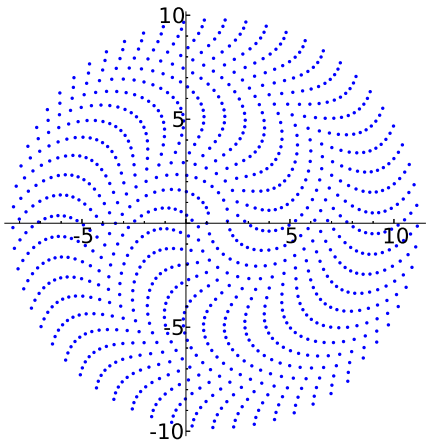


$\alpha = 1/2$

Escribiendo $S(N;\alpha) = \sum_{n=1}^{N} e\big(\alpha\sqrt{n}\big)$, uno podría esperar que este patrón se repitiese cuando α varía, sin embargo, la sorpresa va *in crescendo*, y ya no tiene explicación dentro del método de van der Corput, cuando observamos los dibujos resultantes para otro valores. Por ejemplo, para $\alpha = 1$ y $\alpha = 65/64$, se tiene



$\alpha = 1$



$\alpha = 65/64$

En el Capítulo 6 se estudian los patrones que aparecen al dibujar $\{S(n;\alpha)\}_{n=1}^{N}$ para algunos valores de α.

Como la derivada de $\alpha\sqrt{x}$ decrece, para α razonablemente pequeño podemos considerar el término principal dado por (3), por lo que la sucesión finita debería aproximarse por una espiral de Arquímedes

$$\frac{1}{2}(\pi\alpha)^{-2}t(\operatorname{sen} t, -\cos t) \qquad \text{con} \quad t \in [1, 2\pi\alpha\sqrt{N}]$$

cuando N crece (salvo por una traslación). A pesar de que este análisis no es riguroso, debido a que el término de error en la aproximación es comparable a la separación entre los puntos, un estudio teórico detallado nos sigue llevando a una estructura en espiral, surgiendo así la paradoja.

Para explicar este fenómeno, establecemos una relación de recurrencia de naturaleza aritmética para puntos cercanos,

$$t_{k+1} = t_k + \left\lfloor \frac{2\alpha\sqrt{t_k}+1}{\alpha^2} + \frac{1}{2} \right\rfloor.$$

Los distintos valores de la recurrencia dan las "ramas" del patrón, en el sentido de que las curvas que se observan en las figuras de las sumas parciales $\{S(n;\alpha)\}_{n=1}^{N}$ corresponden a porciones de ramas. La aparente pérdida de dicha estructura en espiral se debe a que nuestra vista tiende a conectar puntos cercanos en vueltas consecutivas, que corresponden a puntos en las ramas antes indicadas. El capítulo finaliza mostrando que la recurrencia puede ser resuelta para algunos valores de α, dando una explicación completa del patrón.

En el Capítulo 7, nos interesamos por un problema clásico en teoría de números: contar puntos de coordenadas enteras (puntos del retículo) en un dominio que se

expande. Este tipo de problemas tiene una larga tradición en teoría analítica de números, de hecho dos problemas famosos todavía abiertos, el del círculo y el del divisor, tienen su origen en trabajos de C.F. Gauss y de P.G.L. Dirichlet (1805–1859).

Consideremos la función aritmética $r(n)$ que da el número de representaciones de n como suma de dos cuadrados. Es obvio que su suma coincide con el número de puntos en el interior de un círculo y que éste debiera aproximarse bien por el área:

$$\sum_{n\leq R^2} r(n) = \#\{(a,b)\in\mathbb{Z}^2 \ : \ a^2+b^2\leq R^2\} \sim \pi R^2$$

El problema del círculo consiste en hallar el orden del término de error. Con métodos muy sofisticados de sumas trigonométricas, M.N. Huxley [Hux03] consiguió en 2003 el mejor resultado conocido hasta la fecha

$$\sum_{n\leq R^2} r(n) = \pi R^2 + O_\epsilon\big(R^{131/208+\epsilon}\big) \qquad \text{para todo } \ \epsilon>0.$$

Por otro lado, según una conjetura de Hardy, 131/208 se debería poder reemplazar por 1/2.

Si prescindimos de la función aritmética $r(n)$ y pensamos el problema desde el punto de vista geométrico, cabe fijar un dominio $D\in\mathbb{R}^2$ y plantearse el estudio del número de puntos de $\mathbb{Z}^2$ en RD cuando $R\in\mathbb{R}^+$ crece. El término principal es $R^2|D|$ y el término de error conduce a sumas trigonométricas. La explicación intuitiva es asequible a partir de la fórmula de sumación de Poisson. Despreocupándose de cuestiones de convergencia, si χ es la función característica de D, se tiene que el número de puntos de coordenadas enteras en RD es

$$\sum_{\vec{n}\in\mathbb{Z}^2} \chi(R^{-1}\vec{n}) = R^2 \sum_{\vec{n}\in\mathbb{Z}^2} \widehat{\chi}(R\vec{n}).$$

El sumando correspondiente a $\vec{n}=\vec{0}$ en el segundo miembro da el término principal $R^2|D|$, mientras que el resto de los términos oscilan de una manera que se puede aproximar con el principio de fase estacionaria. Finalmente, la estimación de sumas trigonométricas permite cuantificar la cancelación entre estos términos.

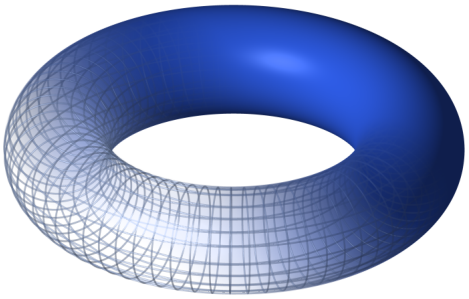
El problema también se generaliza naturalmente a más dimensiones. Así se tiene el problema de la esfera, para el que el mejor resultado conocido se debe a D.R. Heath-Brown [HB99]

$$\#\{\vec{n}\in\mathbb{Z}^2 \ : \ \|\vec{n}\|\leq R\} = \frac{4}{3}\pi R^3 + O_\epsilon\big(R^{12/16+\epsilon}\big) \qquad \text{para todo } \ \epsilon>0,$$

y que se extiende también a elipsoides racionales [CCU09]. Una particularidad de estos problemas es que hay que suplementar las sumas trigonométricas con técnicas bien distintas, que no se aplican a otros dominios.

Los métodos analíticos empleados en 2 y 3 dimensiones exigen naturalmente la convexidad, entendiendo por esta que la curvatura (gaussiana, en el caso tridimensional) de la frontera sea positiva. Sin embargo, en principio no hay razones geométricas o aritméticas para ello. Un análisis más cuidadoso muestra que cuando no se requiere la convexidad, pueden aparecer términos principales secundarios. Sobre todo en las últimas dos décadas ha habido interés por el estudio de estos problemas no convexos [Krä02b], [Now08b], [Guo13].

El Capítulo 7 está dedicado al problema de puntos del retículo asociado al sólido no convexo posiblemente más cotidiano en el ámbito matemático: el toro obtenido por la revolución de un círculo alrededor del eje z.



Probamos que el número de puntos de $\mathbb{Z}^3$ en el toro R-dilatado es

$$VR^3 + M_R R^{3/2} + O_\epsilon\big(R^{4/3+\epsilon}\big) \qquad \text{para todo } \ \epsilon > 0,$$

donde V es el volumen del toro original y M_R es una función periódica acotada. Esto mejora un resultado anterior de W.G. Nowak [Now08a]. Aunque dentro de las conjeturas habituales uno esperaría poder cambiar $4/3$ por 1, nuestro resultado parece establecer un límite sobre lo que se puede obtener utilizando únicamente sumas trigonométricas. La razón para ello es que el error proviene de un término diagonal.

Los resultados de las distintas partes de la tesis están recogidos en:

Parte I

- 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 D. Raboso. *On the Kuznetsov formula*. Preprint 2013. Submitted.
- D. Raboso. *When the modular world becomes non-holomorphic*. Preprint 2013. To appear in Contemporary Mathematics.

Parte II

- 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 and D. Raboso. *Distributional properties of powers of matrices*. Preprint, 2013. To appear in Czechoslovak Mathematical Journal.

Parte III

- F. Chamizo and D. Raboso. *Van der Corput method and optical illusions*. Preprint 2014.
- F. Chamizo and D. Raboso. *Lattice points in the 3-dimensional torus*. Preprint 2014.

Parte I

Métodos espectrales

Capítulo 1

Conceptos preliminares

A finales del siglo XVII, algunos matemáticos intentaron demostrar el quinto postulado de Euclides mediante reducción al absurdo, sin darse cuenta del alcance que podría tener el resultado: varios teoremas pertenecientes a lo que hoy conocemos como geometrías no euclidianas. Gauss fue el primero en enfocar el problema de forma correcta refutando la creencia sobre la posibilidad de demostrar el postulado de las paralelas y, a pesar de no publicarlos, de parte de su correspondencia se deduce que llegó a resultados verdaderamente interesantes.

Los primeros matemáticos que publicaron trabajos sobre geometría hiperbólica fueron Lobachevsky y Bolyai de forma independiente a principios del siglo XIX, aunque los de Lobachevsky, dando un mayor desarrollo desde el punto de vista analítico, tuvieron más trascendencia.

El problema de dar sentido a esta nueva geometría se traduce en la búsqueda de modelos. Para ello se recurre a las superficies, cambiando la noción de recta por la de "andar" en línea recta por la superficie. Este andar en línea recta se denomina geodésica. La mayoría de los modelos de geometría hiperbólica fueron establecidos entre 1869 y 1881.

Los diferentes modelos son equivalentes, en el sentido de que existen funciones que transforman un modelo en otro, de manera que las nociones de objetos geométricos como puntos, rectas, ángulos y distancias se preservan.

El semiplano superior $\mathbb{H} = \{x + iy \ : \ x \in \mathbb{R}, \ y \in \mathbb{R}^+\}$, es una superficie de Riemann simplemente conexa y un modelo del plano hiperbólico cuando se equipa con la *métrica de Poincaré*

$$ds^2 = \frac{dx^2 + dy^2}{y^2}.$$

Esta métrica induce una *distancia* dada por

$$\rho(z, w) = \log \frac{|z - \overline{w}| + |z - w|}{|z - \overline{w}| - |z - w|}. \tag{1.1}$$

Sin embargo, en la práctica, existe otra fórmula más útil

$$u(z,w) = \frac{|z-w|^2}{4\Im(z)\Im(w)} \qquad \text{donde} \quad \cosh\rho(z,w) = 1 + 2u(z,u). \tag{1.2}$$

Las geodésicas serán entonces semicircunferencias con centro en el eje x o bien, semirectas verticales.

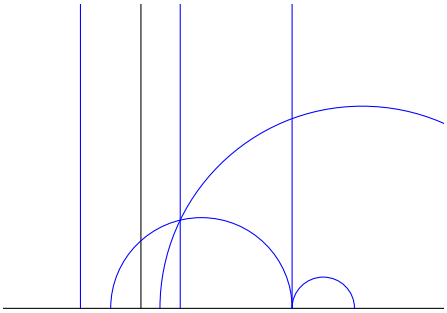


Figura 1.1: Geodésicas en $\mathbb{H}$.

En geometría riemaniana, hay una manera de asignar a cada métrica un elemento de volumen. En otras palabras, una vez que sabemos cómo medir longitudes, sólo hay una manera coherente para medir áreas o volúmenes. En el semiplano de Poincaré, el elemento de volumen es la *medida hiperbólica*

$$d\mu(z) = y^{-2}dxdy,$$

con la que podemos calcular el área de una región en $\mathbb{H}$, que no tiene por qué parecerse al área euclídea porque cuando cuando y crece, las distancias y áreas disminuyen con respecto a las euclídeas.

La acción del grupo $G = \mathrm{SL}_2(\mathbb{R})$ en $\mathbb{H}$ da lugar a todas las isometrías directas del semiplano de Poincaré. Dado $g \in G$ y $z \in \mathbb{H}$ se define gz como

$$gz = \frac{az+b}{cz+d} \qquad \text{donde} \quad g = \begin{pmatrix} a & b \\ c & d \end{pmatrix}.$$

Esta acción no es fiel porque g y $-g$ actúan de la misma forma, de modo que a menudo se piensa en G como el grupo $\mathrm{PSL}_2(\mathbb{R}) = \mathrm{SL}_2(\mathbb{R})/\{\pm I\}$ de todas las transformaciones de Möbius. Al ser la métrica de Poincaré invariante por la acción de G, también lo es la distancia y la medida hiperbólicas.

Los subgrupos discretos de G reciben el nombre de *grupos fuchsianos*. Entre ellos destacan el grupo modular completo $\mathrm{PSL}_2(\mathbb{Z})$, y los subgrupos de congruencias.

Se define el grupo principal de congruencias de nivel N como

$$\Gamma(N) = \{\gamma \in \mathrm{SL}_2(\mathbb{Z}) \ : \ \gamma \equiv I \pmod{N}\},$$

donde I es la matriz identidad. Un subgrupo Γ de $\mathrm{SL}_2(\mathbb{Z})$ se dice que es un subgrupo de congruencias de nivel N si contiene a $\Gamma(N)$. El ejemplo más destacado es

$$\Gamma_0(N) = \left\{\gamma \in \mathrm{SL}_2(\mathbb{Z}) \ : \ \gamma \equiv \left(\begin{smallmatrix} * & * \\ 0 & * \end{smallmatrix}\right) \pmod{N}\right\}.$$

Con un abuso de notación obvio, escribiremos $\Gamma_0(1) = \mathrm{PSL}_2(\mathbb{Z})$.

Análogamente al estudio de funciones periódicas en $\mathbb{R}$, se consideran funciones en $\mathbb{H}$ que son periódicas respecto a un grupo Γ, es decir, funciones en el espacio cociente $\Gamma\backslash\mathbb{H}$.

Una función $f \ : \ \mathbb{H} \to \mathbb{C}$ se dice *automorfa* respecto a un grupo Γ, si es Γ-invariante, es decir, si $f(\gamma z) = f(z)$ para todo $\gamma \in \Gamma$.

Nótese que aquí no se requiere que f sea holomorfa.

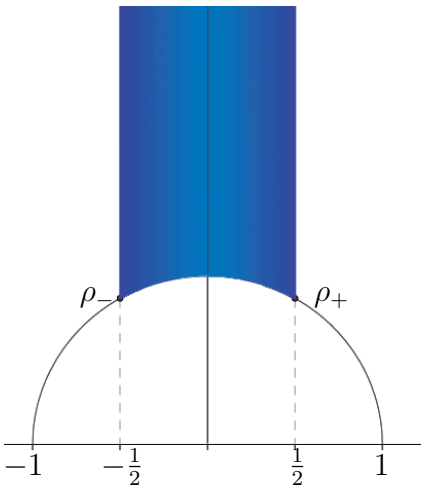
Nuestro interés recae sobre grupos fuchsianos de primera especie para los cuales $\Gamma\backslash\mathbb{H}$ tiene área finita. De este modo se puede escoger el *dominio fundamental* del cociente como un polígono convexo, cuyos lados son arcos de semicircunferencias o rectas verticales (los dos tipos de geodésicas) y $\Gamma\backslash\mathbb{H}$ puede ser interpretado como dicho polígono con una regla para identificar los lados.

En el caso de $\Gamma_0(1)$, su dominio fundamental es el triángulo hiperbólico de vértices $i\infty$ y $\rho_\pm = (i\sqrt{3} \pm 1)/2$,

$$D_1 = \{z \in \mathbb{H} \ : \ |z| \geq 1, \ |\Re z| \leq 1/2\},$$

y se tiene

$$|D_1| = \int_{D_1} d\mu(z) = \frac{\pi}{3}.$$



Los puntos del infinito de $\Gamma\backslash\mathbb{H}$ se denominan *cúspides*, vértices del dominio fundamental en $\{\Im z = 0\} \cup \{\infty\}$. En términos de teoría de grupos, la cúspide $\mathfrak{a}$ es el único punto fijo de algún $\gamma \in \Gamma$ denominado *parabólico*. Si $|\Gamma\backslash\mathbb{H}|$ es finito, entonces tiene un número finito de cúspides. De hecho, no habrá cúspides si y solo si $\Gamma\backslash\mathbb{H}$ es compacto y en ese caso diremos que Γ es *cocompacto*.

En el caso no compacto, cada cúspide $\mathfrak{a}$ tiene asociada una *matriz de escala* $\sigma_\mathfrak{a} \in G$ tal que

$$\sigma_\mathfrak{a} \, \infty = \mathfrak{a} \qquad \text{y} \qquad \sigma_\mathfrak{a}^{-1} \Gamma_\mathfrak{a} \, \sigma_\mathfrak{a} = T,$$

donde $\Gamma_\mathfrak{a} = \{\gamma \in \Gamma \ : \ \gamma\mathfrak{a} = \mathfrak{a}\}$ es el *estabilizador* de la cúspide y T es el grupo de

traslaciones enteras,

$$T = \Big\{ \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} \ : \ n \in \mathbb{Z} \Big\}. \tag{1.3}$$

El efecto geométrico de $\sigma_{\mathfrak{a}}^{-1}$ es mandar la parte del dominio fundamental cercana a la cúspide $\mathfrak{a}$ a la parte del dominio fundamental de $\Gamma_0(1)$ cercana al ∞. Podemos pensar entonces en la matriz de escala como un tipo de normalización.

Por otro lado, la *descomposición en cogrupos dobles* de $\Gamma_0(1)$ respecto al grupo de estabilidad de la única cúspide ∞, da una especie de parametrización en el sentido de que

$$\Gamma_0(1) = T \cup \bigcup_{\substack{c=1 \\ \mathrm{mcd}(c,d)=1}}^{\infty} \bigcup_{d=0}^{c-1} T\omega_{d/c}T \qquad \text{donde} \quad \omega_{d/c} = \begin{pmatrix} * & * \\ c & d \end{pmatrix} \in \Gamma_0(1). \tag{1.4}$$

La descomposición en cogrupos dobles es una herramienta para estudiar un grupo Γ por medio de caracteres aditivos [Iwa02]. Con ello, se obtienen las clásicas *sumas de Kloosterman* definidas por

$$S(m,n;c) = \sum_{ad \equiv 1 \ \mathrm{mód}\ c} e\Big(\frac{ma+nd}{c}\Big) \qquad \text{donde} \quad e(x) = e^{2\pi i x}. \tag{1.5}$$

El análisis armónico en $\mathbb{H}$ se asocia con el *operador de Laplace-Beltrami*, o Laplaciano hiperbólico

$$\Delta = -y^2\Big(\frac{\partial^2}{\partial x^2} + \frac{\partial^2}{\partial y^2}\Big).$$

Una función Γ-automorfa f es una *forma de Maass* si f es una autofunción de Δ y tiene crecimiento polinomial en las cúspides, es decir, si satisface

$$\Delta f = \lambda f \quad \text{ con } \lambda \in \mathbb{C} \qquad \text{y} \qquad f(\sigma_{\mathfrak{a}} iy) = O(y^n) \quad \text{cuando } y \to \infty.$$

Además, se dice que f es una *forma de Maass cuspidal* si

$$\int_0^1 f(\sigma_{\mathfrak{a}} z)\, dx = 0,$$

para toda cúspide $\mathfrak{a}$ en Γ.

A veces, una forma de Maass se define con la condición adicional $f \in L^2(\Gamma\backslash\mathbb{H})$ (cf. [Gol06]). En este contexto, las formas modulares clásicas corresponden a $\lambda = 0$ ya que son armónicas por las ecuaciones de Cauchy-Riemann. La condición de ser autofunción reemplaza aquí la condición de holomorfía, dando una función analítica real. Ahora podemos considerar otros valores de λ.

Por definición, el operador de Laplace solo depende de la métrica y por tanto es un operador diferencial G-invariante, i.e., para toda función f que sea dos veces diferenciable se tiene que $(\Delta f)\circ g = \Delta(f\circ g)$ para todo $g\in G$. El subgrupo de traslaciones de G actúa por $z = x+iy \mapsto (x+r)+iy$ con $r\in\mathbb{R}$. Por lo tanto, las autofunciones invariantes por traslaciones serán autofunciones que solo dependen de la parte imaginaria de z. Dada una función f que dependa únicamente de $y = \Im z$, la condición es

$$y^2 f'' + \lambda f = 0. \tag{1.6}$$

La solución general de la ecuación, para $\lambda\neq 0$, es de la forma $ay^s + by^{1-s}$ con $a,b\in\mathbb{C}$. Si $\lambda = 0$, esto es, cuando $s = 1-s = 1/2$, además de $y^{1/2}$ existe una segunda solución: $y^{1/2}\log y$.

Es posible obtener formas de Maass a partir de autofunciones del Laplaciano en $\mathbb{H}$ forzando a que estas funciones sean automorfas. La G-invariancia de Δ asegura que para todo $g\in G$ la acción de y^s por g es también una autofunción con el mismo autovalor. Por lo tanto,

$$\big(\Im gz\big)^s = \Big(\frac{y}{|cz+d|^2}\Big)^s \qquad \text{con } g = \begin{pmatrix} * & * \\ c & d\end{pmatrix}\in G \tag{1.7}$$

es autofunción de Δ con autovalor $\lambda = s(1-s)$. Si consideramos el grupo $\Gamma_0(1)$, un candidato a forma de Maass es $\sum_{\gamma\in\Gamma_0(1)}(\Im\gamma z)^s$, pero esta suma diverge pues y^s es invariante por Γ_∞, el estabilizador de la única cúspide de $\Gamma_0(1)$. Por lo tanto, la suma no debería incluir estos elementos. Esto conduce a la definición de *serie de Eisentein*, una variante espectral de sus homónimas holomorfas clásicas [Shi71],

$$E(z,s) = \sum_{\gamma\in\Gamma_\infty\backslash\Gamma_0(1)} \big(\Im\gamma z\big)^s = \frac{1}{2}\sum_{\substack{c,d=-\infty\\(c,d)=1}}^{\infty} \frac{y^s}{|cz+d|^{2s}}. \tag{1.8}$$

Para grupos generales, las series de Eisenstein no holomorfas asociadas a la cúspide $\mathfrak{a}$ vienen dadas por

$$E_{\mathfrak{a}}(z,s) = \sum_{\gamma\in\Gamma_{\mathfrak{a}}\backslash\Gamma} \big(\Im\sigma_{\mathfrak{a}}^{-1}\gamma z\big)^s, \tag{1.9}$$

las cuales son absoluta y uniformemente convergentes en conjuntos compactos para cada $s\in\mathbb{C}$ con $\Re s > 1$. Por (1.7) se tiene $\Delta E_{\mathfrak{a}}(\cdot,s) = s(1-s)E_{\mathfrak{a}}(\cdot,s)$, es decir, son autofunciones de Δ pero desafortunadamente no son de cuadrado integrable.

Para cualquier función f en $\Gamma\backslash\mathbb{H}$, la función $f\circ\sigma_{\mathfrak{a}}$ es 1-periódica. En particular, tiene un desarrollo de Fourier

$$f(\sigma_{\mathfrak{a}}z) = \sum_n \widehat{f}_{\mathfrak{a}n}(y)e(nx) \qquad \text{con} \quad z = x+iy \tag{1.10}$$

y

$$\widehat{f}_{\mathfrak{a}n}(y) = \int_0^1 f(\sigma_{\mathfrak{a}} z) e(-nx)\, dx.$$

Si f es una autofunción con autovalor λ entonces, aplicando el operador de Laplace-Beltrami, los coeficientes $\widehat{f}_{\mathfrak{a}n}$ son soluciones de la ecuación diferencial ordinaria

$$g'' + \Big(\frac{\lambda}{y^2} - 4\pi^2 n^2\Big) g = 0.$$

Para $n = 0$, la solución coincide con la de (1.6), mientras que para $n \neq 0$ existen dos soluciones linealmente independientes que vienen dadas por funciones de Bessel, pero una de ellas tiene crecimiento exponencial [Wat44]. Por lo tanto, de (1.10) se llega a

$$f(\sigma_{\mathfrak{a}} z) = a y^s + b y^{1-s} + y^{1/2} \sum_{n \neq 0} a_n K_{s-1/2}(2\pi |n| y) e^{2\pi i n x}$$

donde f satisface

$$\Delta f = \lambda f \qquad \text{con} \quad \lambda = s(1-s). \tag{1.11}$$

Si $s = 1/2$, se debe reemplazar y^{1-s} por $y^{1/2} \log y$.

Siguiendo la misma idea, si consideramos $\mathfrak{a}$, $\mathfrak{b}$ dos cúspides (no necesariamente distintas) entonces $E_{\mathfrak{a}}(\cdot, s)$ tiene un desarrollo de Fourier en la cúspide $\mathfrak{b}$ de la forma

$$E_{\mathfrak{a}}(\sigma_{\mathfrak{b}} z, s) = \delta_{\mathfrak{a}\mathfrak{b}} y^s + \varphi_{\mathfrak{a}\mathfrak{b}}(s) y^{1-s} + y^{1/2} \sum_{n \neq 0} \varphi_{\mathfrak{a}\mathfrak{b}n}(s) K_{s-1/2}(2\pi |n| y) e^{2\pi i n x}, \tag{1.12}$$

donde los coeficientes $\varphi_{\mathfrak{a}\mathfrak{b}}(s)$ y $\varphi_{\mathfrak{a}\mathfrak{b}n}(s)$ vienen dados por series de Dirichlet. El problema es que para grupos generales no se puede evaluar explícitamente estos coeficientes. Sin embargo, para grupos de congruencias esto es más simple usando propiedades de la función ζ de Riemann y de funciones L. De hecho, $\varphi_{\mathfrak{a}\mathfrak{b}}(s)$ se identifica estrechamente con la función zeta de un cuerpo de números, por lo que $\varphi_{\mathfrak{a}\mathfrak{b}}(s)$ es meromorfa de orden 1. Para $\Gamma_0(1)$, los coeficientes de Fourier son explícitos [Iwa02], funciones meromorfas en todo el s-plano complejo, dando una continuación meromorfa de $E(z, s)$ para todo $s \in \mathbb{C}$.

En el caso general, tenemos varias cúspides y a través de la matriz de términos constantes $\Phi(s) = (\varphi_{\mathfrak{a}\mathfrak{b}}(s))$, se puede obtener una ecuación funcional con el vector columna de la serie de Eisenstein del tipo

$$[E_{\mathfrak{a}}(z, s)] = \Phi(s)[E_{\mathfrak{a}}(z, 1-s)].$$

Es importante notar que probar la continuación meromorfa de $E_{\mathfrak{a}}$ no es en absoluto fácil en el caso general, y esta se debe a Selberg [Sel63] [Iwa02].

En el semiplano $\Re s \geq 1/2$ los polos de $\Phi(s)$ y $E_{\mathfrak{a}}(z, s)$ son los mismos, simples y reales. Para grupos de congruencias no hay más polos que los triviales, pero en

general, existe un número finito de otros polos, s_j con $1/2 < s_j \leq 1$. Los residuos de la serie de Eisentein $E_{\mathfrak{a}}(z,s)$ en $s = s_j$ satisfacen (1.11) con $0 \leq \lambda_j < 1/4$. Estas funciones son de cuadrado integrable (en contraste con las series de Eisentein) y pertenecen al subespacio del espectro discreto de Δ. En la línea crítica $s = 1/2 + it$, la matriz $\Phi(1/2+it)$ es unitaria y las series de Eisentein $E_{\mathfrak{a}}(z, 1/2+it)$ forman un autoespacio del espectro continuo.

Una descripción explícita de la descomposición de $L^2(\Gamma\backslash\mathbb{H})$ en términos espectrales es fundamental en la teoría de funciones automorfas. Si Γ es cocompacto, entonces la teoría de espacios de Hilbert implica que Δ tiene un sistema ortonormal completo de autofunciones u_j con autovalores $\lambda_j \geq 0$ [CH53]. La descomposición espectral asegura que toda $f \in L^2(\Gamma\backslash\mathbb{H})$ se puede escribir como combinación lineal de u_j,

$$f(z) = \sum_{j=0}^{\infty} \langle f, u_j \rangle u_j(z)$$

donde

$$\langle f, g \rangle = \int_{\Gamma\backslash\mathbb{H}} f(z)\overline{g(z)}\, d\mu(z) \tag{1.13}$$

es el el *producto de Petersson*, el producto escalar natural.

En el caso no compacto, la teoría es más complicada porque Δ tiene un espectro continuo que cubre el intervalo $[1/4, \infty)$ cuya multiplicidad (finita) coincide con el número de cúspides no equivalentes en Γ.

Por lo tanto, podemos pensar que la descomposición de $L^2(\Gamma\backslash\mathbb{H})$ es un tipo de mezcla entre el análisis de Fourier clásico de $\mathbb{R}/\mathbb{Z}$ y $\mathbb{R}$, ya que tendrá un espectro discreto formado por autofunciones, y un espectro continuo en que se reemplaza sumas por integrales. Formalmente, el resultado es

$$L^2(\Gamma\backslash\mathbb{H}) = \mathcal{D} \oplus \mathcal{C},$$

donde la parte discreta $\mathcal{D}$ es la clausura, en $L^2(\Gamma\backslash\mathbb{H})$, del espacio generado por las formas cuspidales y por los residuos de las series de Eisenstein, y la parte continua $\mathcal{C}$ es una suma directa de $E_{\mathfrak{a}}(z, 1/2+it)$. Por otro lado, con el producto escalar (1.13), la parte discreta es el complemento ortogonal de la parte continua, y los dos espacios que forman $\mathcal{D}$ son ortogonales entre sí.

Esto nos permite escribir, para un sistema ortonormal completo de autofunciones propias en $\mathcal{D}$, $\{u_j(z)\}$, y para toda $f \in L^2(\Gamma\backslash\mathbb{H})$, la siguiente descomposición espectral

$$f(z) = \sum_{j\geq 0} \langle f, u_j \rangle u_j(z) + \sum_{\mathfrak{a}} \frac{1}{4\pi} \int_{\mathbb{R}} \langle f, E_{\mathfrak{a}}(z, \frac{1}{2}+it) \rangle E_{\mathfrak{a}}(z, \frac{1}{2}+it)\, dt,$$

donde la igualdad y la convergencia se entienden en sentido $L^2(\Gamma\backslash\mathbb{H})$. Este es el análogo hiperbólico del desarrollo de Fourier.

Dada una función $k : [0,\infty) \to \mathbb{C}$, se define el *núcleo automorfo* como

$$K(z,w) = \sum_{\gamma\in\Gamma} k\big(u(z,\gamma w)\big), \tag{1.14}$$

donde u está definida en (1.2). Bajo condiciones adecuadas de regularidad y de decaimiento en k, la definición anterior tiene sentido. Imponiendo condiciones de simetría radial, se obtiene un resultado básico (el *Lema Fundamental* en [Hej76]) por el que para cualquier autofunción $\phi(z)$ del Laplaciano hiperbólico se tiene

$$\int_{\mathbb{H}} k\big(u(z,w)\big)\phi(z)\, d\mu(z) = h(t)\phi(w), \tag{1.15}$$

donde h es la *transformada de Selberg* de k definida por

$$h(t) = \int_{\mathbb{H}} k\big(u(z,i)\big)(\Im z)^{1/2+it}\, d\mu(z) = \int_0^\infty \int_{-\infty}^\infty k\left(\frac{x^2+(y-1)^2}{4y}\right) y^{-\frac{3}{2}+it}\, dxdy, \tag{1.16}$$

y que podemos considerar el análogo hiperbólico de la transformada de Fourier. Con un simple cambio de variable [Iwa02, §1.8] también podemos considerar los siguientes tres pasos

$$q(v) = \int_v^\infty \frac{k(u)\, du}{\sqrt{u-v}}, \qquad g(r) = 2q\big(\operatorname{senh}^2 \frac{r}{2}\big), \qquad h(t) = \int_{-\infty}^\infty e^{irt} g(r)\, dr, \tag{1.17}$$

que se pueden invertir usando

$$g(r) = \frac{1}{2\pi}\int_{-\infty}^\infty e^{irt} h(t)\, dt,\ q(v) = \frac{1}{2} g\big(2\log(\sqrt{v+1}+\sqrt{v})\big),\ k(u) = \int_u^\infty \frac{-q'(v)\, dv}{\pi\sqrt{v-u}}. \tag{1.18}$$

Para $u = 0$ esto implica [Kub73]

$$k(0) = \frac{1}{4\pi}\int_{-\infty}^\infty th(t)\tanh(\pi t)\, dt. \tag{1.19}$$

De lo anterior se desprende el desarrollo espectral de núcleos automorfos conocido como *fórmula de pretraza* [Sel56]

$$K(z,w) = \sum_{j=0}^\infty h(t_j) u_j(z)\overline{u_j(w)} + \frac{1}{4\pi}\sum_{\mathfrak{a}} \int_{-\infty}^\infty h(t) E_{\mathfrak{a}}(z,1/2+it)\overline{E_{\mathfrak{a}}(w,1/2+it)}\, dt, \tag{1.20}$$

donde h es la transformada de Selberg de la función k, y las funciones $u_j(z)$ tienen autovalores ordenados $\lambda_j = -(1/4+t_j^2)$.

Capítulo 2

Sobre la fórmula de Kuznetsov

2.1. Introducción

El desarrollo espectral del núcleo automorfo

$$K(z,w) = \sum_{\gamma\in\Gamma_0(1)} k\big(u(z,\gamma w)\big), \tag{2.1}$$

es

$$K(z,w) = \sum_j h(t_j)u_j(z)\overline{u_j(w)} + \frac{1}{4\pi}\int_{-\infty}^{\infty} h(t)E(z,1/2+it)\overline{E(w,1/2+it)}\,dt, \tag{2.2}$$

y una vez que sabemos que k se pueden recuperar de h, los problemas de convergencia en (2.1) y (2.2) se evitan exigiendo las siguientes condiciones de regularidad en h:

RC. *Para cierto $\eta\in\mathbb{R}^+$, la función h es holomorfa en la banda $|\Im(t)|\le 1/2+\eta$, y satisface $h(t) = O\big(|t|^{-2-\eta}\big)$ en ella.*

La fórmula de Kuznetsov se generaliza a grupos fuchsianos arbitrarios de primera especie. En teoría de números, sin embargo, se usa fundamentalmente para $\Gamma_0(1)$ y $\Gamma_0(N)$. En aras de la simplicidad sólo hemos considerado el caso del grupo modular completo $\Gamma_0(1)$, como hizo el propio Kuznetsov. En el caso general, simplemente hay que añadir la contribución de las series de Eisenstein correspondientes a las diferentes cúspides y en consecuencia, cambiar la definición de la suma de Kloosterman (véase [Iwa02] para el caso general y [DI83] para el caso $\Gamma_0(N)$ plenamente desarrollado).

Esta fórmula proporciona una expresión aritmética para sumas espectrales las cuales involucran coeficientes de Fourier normalizados de formas de Maass cuspidales $\{\nu_j(n)\}$ y de series de Eisenstein $\{\eta_t(n)\}$, definidos más adelante. Simbólicamente, la fórmula de Kuznetsov es

$$S_{mn} = A_{mn} \qquad \text{para} \quad m,n\in\mathbb{Z}-\{0\}$$

donde S_{mn} es la expresión espectral

$$\sum_j h(t_j)\nu_j(n)\overline{\nu_j(m)} + \frac{1}{4\pi}\int_{-\infty}^{\infty} h(t)\eta_t(n)\overline{\eta_t(m)}\,dt, \tag{2.3}$$

con h satisfaciendo **RC**, y A_{mn} es la expresión aritmética

$$\frac{\delta_{mn}}{\pi}\int_{-\infty}^{\infty} t\tanh(\pi t)h(t)\,dt + \sum_{c=1}^{\infty}\frac{1}{c}\,S(m,n;c)\,H\Big(\frac{4\pi\sqrt{|mn|}}{c}\Big), \tag{2.4}$$

donde $S(m,n;c)$ son sumas de Kloosterman (1.5), $\delta_{mn} = 1$ si $m = n$ y es cero en otro caso, y H es la transformación integral dada por

$$H(x) = 2i\int_{-\infty}^{\infty}\frac{th(t)}{\cosh(\pi t)}J_{2it}(x)\,dt \qquad \text{si} \quad mn > 0 \tag{2.5}$$

y

$$H(x) = \frac{4}{\pi}\int_{-\infty}^{\infty} th(t)K_{2it}(x)\operatorname{senh}(\pi t)\,dt \qquad \text{si} \quad mn < 0, \tag{2.6}$$

con J_ν y K_ν funciones de Bessel, con representaciones integrales

$$K_\nu(x) = \int_0^\infty e^{-x\cosh v}\cosh(\nu v)\,dv \tag{2.7}$$

y

$$J_\nu(x) = \frac{1}{\pi}\int_0^\pi \cos(\nu\theta - x\operatorname{sen}\theta)\,d\theta - \frac{\operatorname{sen}(\nu\pi)}{\pi}\int_0^\infty e^{\nu\theta - x\operatorname{senh}\theta}\,d\theta. \tag{2.8}$$

Las sucesiones $\{\nu_j(n)\}_{n\neq 0}$ y $\{\eta_t(n)\}_{n\neq 0}$ son los coeficientes de Fourier normalizados en el sentido de que

$$\nu_j(n) = \rho_j(n)\sqrt{\frac{\pi}{\cosh(\pi t_j)}} \qquad \text{y} \qquad \eta_t(n) = \tau_t(n)\sqrt{\frac{\pi}{\cosh(\pi t_j)}}, \tag{2.9}$$

donde $\rho_j(n)$ y $\eta_t(n)$ son los coeficientes naturales de Fourier:

$$\int_0^1 u_j(z)e(-nx)\,dx = c_{nt_j}(y)\rho_j(n), \qquad \int_0^1 E(z,\frac{1}{2}+it)e(-nx)\,dx = c_{nt}(y)\tau_t(n), \tag{2.10}$$

con $z = x+iy$ y $c_{nt}(y) = y^{1/2}K_{it}(2\pi|n|y)$. En otras palabras, los desarrollos completos de Fourier de u_j y E son

$$u_j(z) = \sum_{n\neq 0}\rho_j(n)c_{nt_j}(y)e(nx)$$

y

$$E\big(z, \frac{1}{2} + it\big) = y^{1/2+it} + \eta(t) y^{1/2-it} + \sum_{n \neq 0} \tau_t(n) c_{nt}(y) e(nx).$$

Hasta donde sabemos, hay tres modelos de prueba de la fórmula de Kuznetsov. En primer lugar la que se da en el artículo original [Kuz80] (véase también el trabajo independiente [Bru78]) que usa series de Poincaré (ver Capítulo 16 de [IK04] para una versión corta). Una interesante variación se debe a Motohashi [Mot96] [Mot97] que emplea algunas integrales de Barnes (productos de funciones Γ). Otra demostración utiliza la función automorfa de Green, el núcleo del operador resolvente, como en [Iwa02]. Finalmente, hay una prueba [CPS90] en el marco de la teoría de representaciones, revelando la fórmula de Kuznetsov como una "fórmula de traza relativa".

Todas estas pruebas dependen en gran medida de las propiedades de las funciones especiales involucradas. En principio esto es natural porque la propia fórmula de Kuznetsov contiene transformaciones de Bessel de orden imaginario. El inconveniente de la presencia de estas funciones especiales es que en las aplicaciones uno tiene que hacer frente a integrales oscilatorias engorrosas.

En la sección 2.2 planteamos la fórmula de Kuznetsov en una forma que admite una corta derivación a partir de la fórmula de pretraza e implica casi ningún uso de funciones especiales. De hecho, sólo utilizamos como definiciones

$$K_{it}(x) = \int_0^\infty e^{-x \cosh v} \cos(tv)\, dv \quad \text{y} \quad J_0(x) = \frac{1}{2\pi} \int_0^{2\pi} \cos(x \cos\theta)\, d\theta, \tag{2.11}$$

y no se necesita conocimiento previo acerca de estas funciones especiales, pues solo apelamos a argumentos básicos del análisis real.

Más allá del posible interés educativo de introducir rápidamente la fórmula de Kuznetsov, creemos que tiene ventajas teóricas, tal vez la más obvia sea la simetría entre los casos $mn > 0$ y $mn < 0$. Otra característica positiva es que la fórmula inversa, tratada en la sección 2.3, admite una prueba más limpia y más corta. El enfoque típico apela a la falta inesperada de sobreyectividad cuando $mn > 0$ de los operadores integrales involucrados (la integral de Titchmarsh [Iwa02, B5]). También creemos que se podría flexibilizar las condiciones de regularidad con respecto a trabajos anteriores, pero no hemos seguido esta línea, al ser menos importante para las aplicaciones.

En la sección 2.4 demostramos la equivalencia entre nuestra formulación y la clásica. Ponemos especial cuidado en usar únicamente las representaciones integrales (2.7) y (2.8) junto con argumentos que involucran análisis de Fourier básico y análisis complejo en forma del teorema de los residuos.

Nuestro resultado se basa en la sustitución de la original transformada de Bessel por una transformada de Hankel de una transformación de Selberg (la transformada

de Hankel ha aparecido en trabajos anteriores como herramienta analítica para hacer frente a una parte de ciertos términos en la prueba de la fórmula inversa cuando $mn > 0$).

Este cambio de una transformada integral como composición de dos no es sólo estético, pues ofrece una ganancia ya que la transformada de Selberg se comporta como una transformada de Fourier y admite estimaciones similares, como se muestra en el Lema 2.5.1. Por otro lado, cuando c es grande, la transformada de Hankel tiende a una integral simple. Ilustramos estas ideas con un ejemplo estimando un valor medio regularizado de los coeficientes de Fourier.

2.2. Una nueva forma de la fórmula de Kuznetsov

Teorema 2.2.1. *Bajo la condición de regularidad* **RC**, *para m y n enteros no nulos, se tiene*

$$S_{mn} = \frac{\delta_{mn}}{\pi} \int_{-\infty}^{\infty} t \tanh(\pi t) h(t)\, dt + \sum_{c=1}^{\infty} \frac{1}{c}\, S(m,n;c)\, G\Big(\frac{4\pi\sqrt{|mn|}}{c}\Big),$$

donde

$$G(x) = 4\pi x \int_0^{\infty} k(r) J_0\big(x\sqrt{r+\epsilon_0}\big)\, dr$$

con $\epsilon_0 = 0$ si $mn < 0$ y $\epsilon_0 = 1$ si $mn > 0$.

Para la demostración del teorema necesitamos un lema conocido cuya demostración se reduce a un calculo de [Iwa02, §5.2] y que incluimos por completitud.

Lema 2.2.2. *Los coeficientes de Fourier a_{mn} del núcleo automorfo* (2.1) *como función de $\Re(z)$ y $-\Re(w)$ son*

$$a_{mn} = \delta_{mn} \int_{-\infty}^{\infty} e(-nx) k\big(u(x + \Im(z)i, \Im(w)i\big)\, dx + \sum_{c=1}^{\infty} \frac{1}{c}\, S(n,m;c)\, b_{mn},$$

donde

$$b_{mn} = c \int_{-\infty}^{\infty} \int_{-\infty}^{\infty} e(-nx + mx') k\Big(u\big(\frac{-c^{-2}}{x + \Im(z)i}, x' + \Im(w)i\big)\Big)\, dx dx'.$$

Demostración. Los términos asociados a las traslaciones se pueden manipular de forma sencilla. Tomando $t = \Re(z - w)$, la fórmula de sumación de Poisson da

$$\begin{aligned}\sum_{\gamma \in T} k\big(u(\gamma z, w)\big) &= \sum_{n=-\infty}^{\infty} k\big(u(z+n, w)\big) = \sum_{n=-\infty}^{\infty} k\big(u(t + \Im(z)i + n, \Im(w)i)\big) \\ &= \sum_{n=-\infty}^{\infty} e(nt) \int_{-\infty}^{\infty} e(-nx) k\big(u(x + \Im(z)i, \Im(w)i)\big)\, dx,\end{aligned}$$

con lo que se obtiene la primera parte de la fórmula en a_{mn}. En el resto de casos, por la descomposición en cogrupos dobles de $\Gamma_0(1)$, (1.4), y la fórmula de sumación de Poisson se tiene

$$\sum_{\gamma\in\,\Gamma-T} k\big(u(\gamma z,w)\big) = \sum_{m,n=-\infty}^{\infty} \sum_{\substack{c=1\\ \gcd(c,d)=1}}^{\infty}\sum_{d=0}^{c-1} k\big(u(\omega_{d/c}(z+n),w-m)\big)$$

$$= \sum_{m,n=-\infty}^{\infty} e(n\Re(z)-m\Re(w)) \sum_{\substack{c=1\\ \gcd(c,d)=1}}^{\infty}\sum_{d=0}^{c-1} \int_{-\infty}^{\infty}\int_{-\infty}^{\infty} e(-nx+mx')\mathcal{K}_{cd}(x,x')dxdx',$$

donde

$$\mathcal{K}_{cd}(x,x') = k\Big(u\big(\frac{-c^{-2}}{x+d/c+i\Im(z)}, x'-\overline{d}/c+i\Im(w)\big)\Big)$$

y $\overline{d}$ es el inverso de d modulo c. Tras efectuar una traslación se llega al resultado. □

Lema 2.2.3. *Se tiene*

$$\int_0^\infty K_{it}^2(2\pi y)\, dy = \frac{\pi}{8\cosh(\pi t)}.$$

Demostración. Por (2.11), la integral es

$$\frac{1}{8\pi}\int_{-\infty}^{\infty}\int_{-\infty}^{\infty} \frac{\cos\big(t(u+v)\big)}{\cosh u+\cosh v}\, dudv.$$

Ahora, tras efectuar el cambio $u=\pi(r+s)$ y $v=\pi(r-s)$, podemos separar variables obteniendo unas integrales simples conocidas llegando así al resultado esperado. □

Demostración del Teorema 2.2.1. Comenzamos tomando $z=x+iy/|n|$ y $w=x'+iy/|m|$ en la fórmula de la pretraza (2.2). Por (2.9), (2.10) y el Lema 2.2.3 los coeficientes del término $e(nx-mx')$ en el desarrollo de Fourier de $8\sqrt{|mn|}\int_0^\infty y^{-1}K(z,w)\,dy$ son iguales a S_{mn}. Entonces, con la notación del Lema 2.2.2 tenemos que probar que

$$8\sqrt{|mn|}\int_0^\infty a_{mn}\,\frac{dy}{y} = \frac{\delta_{mn}}{\pi}\int_{-\infty}^{\infty} t\tanh(\pi t)h(t)\,dt + \sum_{c=1}^{\infty}\frac{1}{c}S(m,n;c)\,G\Big(\frac{4\pi\sqrt{|mn|}}{c}\Big)$$

para $m,n\neq 0$. El término con el coeficiente δ_{mn} proviene de la parte correspondiente en la fórmula para a_{mn} en el Lema 2.2.2 con un cambio de variable $x=2|n|^{-1}yv$

$$8|n|\int_0^\infty\int_{-\infty}^{\infty} e(-nx)k\big(u(x+i\frac{y}{|n|},i\frac{y}{|n|}\big)\,\frac{dxdy}{y} = 16\int_0^\infty\int_{-\infty}^{\infty} e(-2yv)k(v^2)\,dvdy$$

que es igual a $4k(0)$ a través de una inversión de Fourier, como se esperaba por (1.19). Consideramos ahora la contribución de b_{mn} en el Lema 2.2.2. Tomando $\lambda = \sqrt{|mn|}/c$, con un simple cambio de variable dicha contribución en $8\sqrt{|mn|}\int_0^\infty y^{-1}a_{mn}\,dy$ es

$$\frac{8}{\lambda}\int_0^\infty\int_{-\infty}^\infty\int_{-\infty}^\infty y^{-1}e\big(-\frac{n}{|n|}x+\frac{m}{|m|}x'\big)k\Big(u\big(\frac{-\lambda^2}{x+iy},x'+iy\big)\Big)dxdx'dy$$
$$=16\lambda\int_{-\frac{\pi}{2}}^{\frac{\pi}{2}}\int_0^\infty\int_{-\infty}^\infty\cos\Big(2\pi\lambda\big(2s\cos\theta-\big(\frac{mn}{|mn|}v+v^{-1}\big)\operatorname{sen}\theta\big)\Big)k\Big(s^2+\frac{(1-v^2)^2}{4v^2}\Big)dsdvd\theta,$$

donde la última expresión se obtiene tomando

$$x=\lambda v\operatorname{sen}\theta,\qquad y=\lambda v\cos\theta\qquad\text{y}\qquad x'=\frac{2syv-x}{v^2}.$$

Si $mn>0$, tras aplicar el cambio $v=w+\sqrt{w^2+1}$, podemos escribir la integral anterior como

$$\int_{-\frac{\pi}{2}}^{\frac{\pi}{2}}\int_{-\infty}^\infty\int_{-\infty}^\infty\cos\big(4\pi\lambda(s\cos\theta-\sqrt{w^2+1}\operatorname{sen}\theta)\big)k\big(s^2+w^2\big)dsdwd\theta$$
$$=\frac{1}{2}\int_0^{2\pi}\int_{-\infty}^\infty\int_{-\infty}^\infty\cos\big(4\pi\lambda\sqrt{s^2+w^2+1}\cos\theta\big)k(s^2+w^2)dsdwd\theta.$$

Cuando $mn<0$, el mismo cambio da la integral

$$\int_{-\frac{\pi}{2}}^{\frac{\pi}{2}}\int_{-\infty}^\infty\int_{-\infty}^\infty\cos\big(4\pi\lambda(s\cos\theta+w\operatorname{sen}\theta)\big)k(s^2+w^2)dsdvd\theta$$
$$=\frac{1}{2}\int_0^{2\pi}\int_{-\infty}^\infty\int_{-\infty}^\infty\cos\big(4\pi\lambda\sqrt{s^2+w^2}\cos\theta\big)k(s^2+w^2)dsdwd\theta.$$

Por último, es suficiente usar coordenadas polares y la representación integral de J_0 en (2.11) para obtener $G(x)$. □

2.3. La fórmula de Kuznetsov inversa

Es un hecho elemental que la transformada de Fourier de $f\big(\sqrt{x^2+y^2}\big)$ viene dada por $2\pi\int_0^\infty rf(r)J_0\big(2\pi r\sqrt{\xi^2+\eta^2}\big)\,dr$. Renombrando las variables se consigue la fórmula de inversión para la transformada de Hankel a partir de la correspondiente para la transformada de Fourier,

$$F(x)=\int_0^\infty rf(r)J_0(rx)\,dr\quad\text{implica}\quad f(r)=\int_0^\infty xF(x)J_0(rx)\,dx.\tag{2.12}$$

Nótese que la función G en el Teorema 2.2.1 puede ser escrita como una transformada de este tipo

$$G(x) = 8\pi x \int_{\epsilon_0}^{\infty} r\, k(r^2 - \epsilon_0) J_0(rx)\, dr.$$

La asimetría de la fórmula inversa para $mn > 0$ viene del hecho de que para $\epsilon_0 = 1$ el intervalo $[0, 1]$ no se considera en la integración. Esto aparece en el enfoque original de Kuznetsov [Kuz80, (6.19)] pero se oculta bajo transformaciones integrales complicadas. Con nuestra formulación, este hecho aparece más transparente y natural.

En este caso asimétrico $mn > 0$ de la fórmula inversa, es conveniente considerar funciones de Bessel de orden entero $J_n(t)$ que, de acuerdo con (2.8), se definen como coeficientes de Fourier de $e^{it\,\mathrm{sen}(2\pi\theta)}$; i.e.,

$$J_n(t) = \int_0^1 e^{it\,\mathrm{sen}(2\pi\theta)} e(-n\theta)\, d\theta.$$

Para garantizar la convergencia en la fórmula inversa, se necesitan algunas condiciones de regularidad sobre la función test f y $f(0) = 0$. Kuznetsov también impone $f'(0) = 0$ pero esto parece ser innecesario [Iwa02]. Aquí imponemos fuertes condiciones de regularidad, a pesar de que estas pueden ser en gran medida debilitadas.

Teorema 2.3.1. *Sea $f \in C_0^\infty(\mathbb{R})$ impar y ϵ_0 como en el Teorema 2.2.1. Entonces*

$$\sum_{c=1}^{\infty} \frac{1}{c}\, S(m,n;c)\, f\Big(\frac{4\pi\sqrt{|mn|}}{c}\Big) = S_{mn} - \frac{\delta_{mn}}{2\pi} \int_0^\infty f(t) J_0(t)\, dt + \epsilon_0 \sum_{c=1}^{\infty} \frac{1}{c}\, S(m,n;c)\, V\Big(\frac{4\pi\sqrt{|mn|}}{c}\Big),$$

donde h es la transformada de Selberg de $\frac{1}{8\pi}\int_0^\infty f(x) J_0\big(x\sqrt{r+\epsilon_0}\big)\, dx$ y V, que solo aparece en el caso $mn > 0$, admite las representaciones

$$V(x) = x \int_0^\infty \int_0^1 r f(t) J_0(rt) J_0(rx)\, drdt$$

y

$$V(x) = 2\sum_{j=1}^{\infty} (2j-1) J_{2j-1}(x) \int_0^\infty t^{-1} f(t) J_{2j-1}(t)\, dt.$$

Por una fórmula debida a H. Petersson [Iwa02], para $m, n > 0$ se tiene

$$\delta_{mn} + 2\pi(-1)^j \sum_{c=1}^{\infty} \frac{1}{c} S(m,n;c) J_{2j-1}\Big(\frac{4\pi\sqrt{mn}}{c}\Big) = \frac{(2j-2)!}{\big(4\pi\sqrt{mn}\big)^{2j-1}} \sum_l \overline{a}_{lj}(m) a_{lj}(n),$$

donde $a_{lj}(n)$ es el n-ésimo coeficiente de Fourier del l-ésimo elemento en una base ortonormal (con respecto al producto de Petersson) de las formas cuspidales clásicas de peso $2j$. Usando esta fórmula, se pueden descartar por completo las sumas de Kloosterman en el término que contiene V. Si pensamos en las formas modulares clásicas como funciones armónicas (correspondientes al autovalor cero del Laplaciano), se obtiene una fórmula inversa que contiene sumas de Kloosterman a un lado e información espectral a otro. En la práctica, el término relacionado con V da una contribución menor.

Demostración. Comenzamos definiendo $k(r) = \frac{1}{8\pi}\int_0^\infty f(x)J_0\big(x\sqrt{r+\epsilon_0}\big)\,dx$, y recordando que $k(r)$ es (salvo una constante) la componente radial de la transformada de Fourier de la función $f\big(\sqrt{x^2+y^2}\big)/\sqrt{x^2+y^2} \in C_0^\infty$ evaluada en $\sqrt{r+\epsilon_0}$. Entonces la función k es de decrecimiento rápido, y consecuentemente g en (1.17) también tiene decrecimiento rápido, de hecho, con decaimiento exponencial, y con una integración por partes se concluye que **RC** se cumple para la correspondiente transformada de Selberg h. Nótese que para $\epsilon_0 = 1$, (1.19) asegura que $\int_{-\infty}^\infty th(t)\tanh(\pi t)\,dt = \frac{1}{2}\int_0^\infty f(x)J_0(x)\,dx$. En cualquier caso, por (2.12), f se puede recuperar como

$$f(x) = 4\pi x\int_{-\epsilon}^\infty k(r)J_0\big(x\sqrt{r+\epsilon_0}\big)\,dr,$$

y por el Teorema 2.2.1 sólo queda demostrar, cuando $\epsilon_0 = 1$, que

$$V(x) = 4\pi x\int_{-1}^0 k(r)J_0\big(x\sqrt{r+1}\big)\,dr$$

para las dos expresiones de V. Tal y como hemos definido k, después de un cambio de variable, obtenemos

$$4\pi x\int_{-1}^0 k(r)J_0\big(x\sqrt{r+1}\big)\,dr = x\int_0^\infty\int_0^1 rf(y)J_0(ry)J_0(rx)\,drdy,$$

que coincide con la primera expresión. La segunda se consigue a partir de la siguiente identidad de funciones de Bessel,

$$xy\int_0^1 rJ_0(rx)J_0(ry)\,dr = 2\sum_{j=1}^\infty (2j-1)J_{2j-1}(x)J_{2j-1}(y). \tag{2.13}$$

De hecho, la definición de $J_n(t)$ implica $e^{iy\,\mathrm{sen}\,\theta} = \sum J_n(y)e(n\theta)$, y el uso de este desarrollo de Fourier como función generatriz, permite deducir fácilmente que

$$J_{n-1}(y) - J_{n+1}(y) = 2J_n'(y) \qquad \text{y} \qquad J_{n-1}(y) + J_{n+1}(y) = \frac{2n}{y}J_n(y),$$

lo que conduce a la relación

$$J_{n-1}(z)J_{n-1}(w) - J_{n+1}(z)J_{n+1}(w) = \frac{2n}{w}J_n(w)J_n'(z) + \frac{2n}{z}J_n(z)J_n'(w)$$

que da una serie telescópica cuando sumamos sobre impares (positivos). A saber,

$$zwJ_0(z)J_0(w) = 2\sum_{n \text{ odd}} n\big(zJ_n(w)J_n'(z) - wJ_n(z)J_n'(w)\big).$$

Sustituyendo $z = ry$, $w = rx$, e integrando por r^{-1} en el intervalo $[0, 1]$, obtenemos (2.13). □

2.4. Equivalencia con la formulación clásica

Esta sección está dedicada a la demostración de la equivalencia entre la fórmula de Kuznetsov y el Teorema 2.2.1. Para ello, basta probar que H es igual a G, por la definición misma de H nos vemos obligados a utilizar algunas funciones especiales.

Teorema 2.4.1. *Se tiene que $G(x) = H(x)$, para todo $x > 0$.*

Demostración. Definimos la transformada seno como $S_F(\xi) = \int_0^\infty F(x)\operatorname{sen}(\xi x)\, dx$. Por inversión de Fourier es suficiente probar que $S_G = S_H$. Para ello es conveniente considerar la fórmula

$$S_G(f(\xi))f'(\xi) = -\frac{d}{d\xi}\int_0^\infty G(x)\cos(xf(\xi))\,\frac{dx}{x}. \tag{2.14}$$

Si $mn < 0$, usando

$$\int_0^\infty J_0(x\beta)\cos(\alpha x)\, dx = \begin{cases} \frac{1}{\sqrt{\beta^2-\alpha^2}}, & 0 < \alpha^2 < \beta^2 \\ \infty, & \beta^2 = \alpha^2 \\ 0, & 0 < \beta^2 < \alpha^2 \end{cases}$$

y (1.17), podemos manipular (2.14) con $f(\xi) = \operatorname{senh}\xi$, cambiando el orden de integración para obtener

$$S_G(\operatorname{senh}\xi)\cosh\xi = -4\pi\frac{d}{d\xi}\int_{\operatorname{senh}^2\xi}^\infty \frac{k(r)}{\sqrt{r - \operatorname{senh}^2\xi}}\, dr = -4\pi g'(2\xi). \tag{2.15}$$

Si $mn > 0$, consideramos dos casos. Primero, si $\xi > 1$ entonces $f(\xi) = \cosh\xi$ en (2.14) también conduce a $-4\pi g'(2\xi)$, como en (2.15), y un procedimiento similar con $\xi < 1$ y $f(\xi) = \operatorname{sen}\xi$, da

$$S_G(\operatorname{sen}\xi)\cos\xi = -4\pi\frac{d}{d\xi}\int_0^\infty \frac{k(r)}{\sqrt{r + \cos^2\xi}}\, dr. \tag{2.16}$$

Una vez que hemos simplificado S_G, vamos a comprobar que coincide con S_H.

Para $mn < 0$, usando la definición (2.6),

$$S_H(\operatorname{senh}\xi) = \frac{4}{\pi}\int_{-\infty}^{\infty} th(t)\Big(\operatorname{senh}(\pi t)\int_0^{\infty} K_{2it}(x)\operatorname{sen}(x\operatorname{senh}\xi)\,dx\Big)dt.$$

Por (2.7), el término entre paréntesis es igual a

$$2\operatorname{senh}\xi\int_0^{\infty}\frac{\cos(2tv)\operatorname{senh}(\pi t)}{\cosh(2v)+\cosh(2\xi)}\,dv = \frac{\pi}{2}\frac{\operatorname{sen}(2t\xi)}{\cosh\xi}, \tag{2.17}$$

donde la última igualdad se obtiene tras realizar el cambio $w = e^{2v}$ y usar el teorema de los residuos sobre un contorno de tipo ojo de cerradura. El caso $mn < 0$, se tiene a través de

$$S_H(\operatorname{senh}\xi)\cosh\xi = 2\int_{-\infty}^{\infty} th(t)\operatorname{sen}(2t\xi)\,dt = -4\pi g'(2\xi).$$

Si $mn > 0$, la definición (2.5) da

$$S_H(\eta) = \int_{-\infty}^{\infty} th(t)\Big(\frac{i}{\cosh(\pi t)}\int_0^{\infty}\big(J_{2it}(x) - J_{-2it}(x)\big)\operatorname{sen}(x\eta)\,dx\Big)\,dt$$

y por (2.8), podemos escribir la expresión entre paréntesis como

$$\begin{aligned}\frac{2}{\pi\cosh(\pi t)}\frac{d}{d\eta}\int_0^{\pi}\int_0^{\infty}\operatorname{senh}(2t\theta)\operatorname{sen}(x\operatorname{sen}\theta)\cos(x\eta)\frac{dx}{x}\,d\theta \\ +\frac{4\eta}{\pi}\int_0^{\infty}\frac{\cos(2t\theta)\operatorname{senh}(\pi t)}{\operatorname{senh}^2\theta+\eta^2}\,d\theta.\end{aligned} \tag{2.18}$$

Si $\eta > 1$, la primera integral desaparece y escribiendo $\eta = \cosh\xi$, la segunda es la misma integral que aparecía en (2.17). Por tanto

$$S_H(\cosh\xi)\operatorname{senh}\xi = -4\pi g'(2\xi).$$

Si $0 < \eta < 1$, tomando $\eta = \operatorname{sen}\xi$, (2.18) es igual a

$$\frac{2}{\cosh(\pi t)\cos\xi}\frac{d}{d\xi}\int_{\xi}^{\pi-\xi}\operatorname{senh}(2t\theta)\,d\theta + \frac{4\operatorname{senh}(\pi t)}{\pi}\int_0^{\infty}\frac{\cos(2t\theta)}{\operatorname{senh}^2\theta+\operatorname{sen}^2\xi}\,d\theta.$$

Ahora, la primera integral es inmediata y la segunda se puede calcular siguiendo los mismos pasos que en (2.17). Combinando estos resultados se llega a

$$S_H(\operatorname{sen}\xi)\cos\xi = -\int_{-\infty}^{\infty} th(t)\frac{\operatorname{senh}(2t\xi)}{\cosh(\pi t)}\,dt = -\frac{d}{d\xi}\int_{-\infty}^{\infty} h(t)\frac{\cosh(2t\xi)}{\cosh(\pi t)}\,dt.$$

Por (1.17), la integral anterior es

$$\int_{-\infty}^{\infty} g(r) \int_{-\infty}^{\infty} \frac{\cos(rt)\cosh(2t\xi)}{\cosh(\pi t)}\, dtdr = 8\int_{-\infty}^{\infty} \frac{q\big(\operatorname{senh}^2 r\big)\cos\xi\cosh r}{\cosh(2r)+\cos(2\xi)}\, dr$$
$$= 4\int_0^{\infty}\int_w^{\infty} \frac{k(r)\cos\xi}{(w+\cos^2\xi)\sqrt{w(r-w)}}\, drdw.$$

Cambiando el orden de integración, la integral interior se puede calcular utilizando el teorema de los residuos lo que conduce a (2.16), y esto termina la prueba. □

2.5. Algunas estimaciones y ejemplos

Nuestra nueva formulación para la fórmula Kuznetsov no sólo muestra ventajas en su demostración, también facilita estimaciones en la práctica y en la búsqueda de ejemplos explícitos.

El siguiente resultado muestra que la transformada de Selberg se puede estimar como una transformada de Fourier con la distancia hiperbólica.

Lema 2.5.1. *Sea h una función que satisface* **RC** *y supongamos $\int_{-\infty}^{\infty} t^j h(t)e^{irt}\, dt \ll B_j(r)$ para $j = 0, 1$, donde $B_0(r)$ y $B_1(r)/\operatorname{senh} r$ son funciones no decrecientes para $r > 0$, entonces*

$$k^2(u) \ll B_0(\rho)B_1(\rho)/\operatorname{senh}\rho,$$

donde ρ y u se definen como en (1.2).

Demostración. A partir de (1.18), se deduce $q\big(\operatorname{senh}^2\frac{v}{2}\big) \ll B_0(v)$ y $q'\big(\operatorname{senh}^2\frac{v}{2}\big) \ll B_1(v)/\operatorname{senh} v$. Para $\xi > u$, escribimos

$$k(u) = \int_u^{\infty} \frac{-q'(v)\, dv}{\pi\sqrt{v-u}} = \int_{\xi}^{\infty} + \int_u^{\xi} = I_0(\xi) + I_1(\xi).$$

Por el teorema del valor medio

$$I_0(\xi) \ll \frac{1}{\sqrt{\xi-u}}\int_{\xi}^{\xi'} q'(v)\, dv \ll \frac{B_0(\rho)}{\sqrt{\xi-u}}$$

y

$$I_1(\xi) \ll \frac{B_1(\rho)}{\operatorname{senh}\rho}\int_u^{\xi} \frac{dv}{\sqrt{v-u}} \ll \frac{B_1(\rho)}{\operatorname{senh}\rho}\sqrt{\xi-u}.$$

Escogiendo $\xi = u + \frac{B_0}{B_1}\operatorname{senh}\rho$ se llega al resultado. □

Por ejemplo, para la gaussiana $h(t) = e^{-t^2/T^2}$ podemos tomar $B_0(r) = Te^{-T^2r^2/4}$ y $B_1(r) = rT^3e^{-T^2r^2/4}$, obteniendo

$$k\big(\frac{\cosh r - 1}{2}\big) \ll T^2 e^{-T^2r^2/4}\sqrt{\frac{u}{\operatorname{senh} u}}, \tag{2.19}$$

que es, de hecho, óptima y desempeña un papel importante en las desigualdades de gran criba de [Cha96].

En general, usando la cota de Weil [IK04, Corolario 11.12] y $J_0(t) \ll (1+|t|)^{-1/2}$, se deduce

Proposición 2.5.2. *Tomando S_{mn} como en (2.3) y con la notación del Lema 2.5.1, se tiene*

$$S_{mn} - \frac{\delta_{mn}}{\pi}\int_{-\infty}^{\infty} t\tanh(\pi t)h(t)\,dt \ll |mn|^{1/2}\sum_{c=1}^{\infty}\frac{\tau(c)}{c^{3/2}}(m,n,c)^{1/2}\,I\big(\frac{mn}{c^2}\big)$$

donde

$$I(\lambda) = \int_0^{\infty}\sqrt{\frac{B_0(v)B_1(v)\operatorname{senh} v}{1+(|\lambda|\cosh v+\lambda)^{1/2}}}\,dv,$$

con $\tau(c)$ el número de divisores de c y (m,n,c) el máximo común divisor.

Para ilustrar la aplicabilidad del resultado damos una estimación de sumas suavizadas de los coeficientes de Fourier.

Corolario 2.5.3. *Dado $\delta > 0$, se tiene*

$$\sum_j |\nu_j(n)|^2 e^{-t_j^2/T^2} + \frac{1}{4\pi}\int_{-\infty}^{\infty}|\eta_t(n)|^2 e^{-t^2/T^2}\,dt = \pi^{-1}T^2 + O\big(|n|^{1/2+\delta}T\big),$$

para cualquier $n \neq 0$ y $T > 1$.

Esto mejora (16.56) en [IK04]. Creemos que el argumento empleado allí no concuerda con el exponente indicado en (16.55), que se puede bajar, aun así nuestra aplicación de la Proposición 2.5.2 da de todos modos un resultado mejor.

Demostración. Escogiendo $h(t) = e^{-t^2/T^2}$ y $m = n$ en la Proposición 2.5.2, al igual que en (2.19), podemos tomar $B_0(r) = Te^{-T^2r^2/4}$ y $B_1(r) = rT^3e^{-T^2r^2/4}$. Entonces

$$I\big(\frac{n^2}{c^2}\big) \ll T^2\int_0^{\infty}\frac{v^{1/2}e^{-T^2v^2+v}}{1+e^{v/2}(n/c)^{1/2}}\,dv \ll T^{1/2}\min\big(1,\ c^{1/2}n^{-1/2}\big)$$

que da el término de error esperado.

Por último, teniendo en cuenta que $\tanh(\pi t) = \pm 1 + O\big(e^{-\pi|t|}\big)$ donde el signo de ± 1 coincide con el de t se llega a que el término principal es $\pi^{-1}T^2 + O(1)$. □

Otra ventaja que proporciona la nueva expresión es obtener algunos casos explícitos para la fórmula de Kuznetsov. Es decir, dado k y su transformada de Selberg, poder encontrar la función G correspondiente.

Hay algunos pares de k y h que tienen fórmulas cerradas, esto se usa en el Capítulo 3 para producir algunas fórmulas aproximadas inusuales, y de donde extraemos los ejemplos que se muestran a continuación, con especial interés en dar demostraciones simples y autocontenidas.

Por ejemplo, por el Lema 3.2.5, la transformada de Selberg de $k(r) = e^{-\mu r}$ con $\mu > 0$, es $4e^{\mu/2}\sqrt{\pi/\mu}\, K_{it}(\mu/2)$ y usando el desarrollo de Taylor del coseno en (2.11) se tiene

$$G(x) = 2x \sum_{n=0}^{\infty} (-1)^n \frac{x^{2n}}{(2n)!} \int_0^{\infty} e^{-\mu r} r^n \, dr \int_0^{2\pi} \cos^{2n}\theta \, d\theta.$$

Ambas integrales son sencillas, lo que permite obtener el desarrollo de Taylor $G(x) = 4\pi x \mu^{-1} e^{-x^2/4\mu}$.

Si consideramos funciones del tipo

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

donde $\alpha, \beta > 0$, usando el Lema 3.2.6 se tiene que $h(t) = K_{it}(\alpha)K_{it}(\beta)$ y tras un cambio de variable podemos escribir G como

$$\frac{\pi x(\alpha+\beta)}{2\sqrt{\alpha\beta}} \int_1^{\infty} e^{-\beta(\alpha+\beta)y} J_0\Big(\frac{x(\alpha+\beta)}{2\sqrt{\alpha\beta}}\sqrt{y^2-1}\Big)\, dy.$$

A partir de (2.11) se deduce que

$$J_0\big(\gamma\sqrt{y^2-1}\big) = \frac{1}{2\pi}\int_0^{2\pi} e^{i\gamma y\cos\theta - \gamma \operatorname{sen}\theta}\, d\theta$$

y por tanto, después de integrar en y, es suficiente usar el teorema de los residuos para obtener

$$G(x) = \frac{\pi x}{\sqrt{4\alpha\beta + x^2}}\, e^{-\frac{(\alpha+\beta)}{2\sqrt{\alpha\beta}}\sqrt{4\alpha\beta+x^2}}.$$

En otros ejemplos, con funciones del tipo $k(r) = (1+r)^{-\mu}$ con $\mu > 1$, puede ser útil usar la transformada de Hankel. En este caso, el Lema 3.2.4 da

$$h(t) = \frac{4\pi}{\Gamma^2(\mu)}\Gamma\big(\mu - \frac{1}{2} + it\big)\Gamma\big(\mu - \frac{1}{2} - it\big).$$

Por un lado, el binomio de Newton generalizado implica

$$(1+r^2)^{-\mu} = \sum_{n=0}^{\infty} \frac{\Gamma(\mu+n)}{n!\Gamma(\mu)}(-1)^n r^{2n}. \tag{2.20}$$

Por otro lado, a partir de (2.7) se llega a que

$$\int_0^\infty x^{\mu+2n} K_{\mu-1}(x)\, dx = \Gamma(\mu+2n+1) \int_0^\infty \frac{\cosh\big((\mu-1)v\big)}{(\cosh v)^{\mu+2n+1}} dv = 2^{\mu+2n-1} n!\, \Gamma(\mu+n).$$

Para ver esto último, basta escribir el coseno hiperbólico como una suma de exponenciales y hacer el cambio $v = \pm\frac{1}{2}\log\frac{1-y}{y}$ en las integrales resultantes.

Combinando esta expresión con (2.20), se obtiene el desarrollo de J_0 (o la serie de Taylor del coseno como se hizo en el primer ejemplo) de modo que

$$(1+r^2)^{-\mu} = \int_0^\infty \frac{x^\mu}{2^{\mu-1}\Gamma(\mu)}\, K_{\mu-1}(x) J_0(xr)\, dx.$$

Ahora, la fórmula de inversión de la transformada de Hankel da

$$G(x) = \frac{\pi x^\mu}{2^{\mu-4}\,\Gamma(\mu)} K_{\mu-1}(x).$$

En particular, si $\mu - \frac{1}{2} \in \mathbb{Z}^+$, el desarrollo de la serie de la función de Bessel permite escribir lo anterior como

$$\frac{\pi e^{-x}(\mu-1/2)!}{8(2\mu-1)!} \sum_{k=0}^{\mu-3/2} \frac{(\mu-3/2+k)!}{k!(\mu-3/2-k)!} (2x)^{\mu-1/2-k}.$$

Existen otros casos de transformadas "exactas" de Hankel que se pueden encontrar en tablas matemáticas, pero rara vez estas corresponden a una función explícita h.

Capítulo 3

Identidades aproximadas y formas de Maass

3.1. Introducción

Muchas identidades aproximadas proceden de la teoría de las formas modulares. Probablemente la más conocida es la llamada constante Ramanujan $e^{\pi\sqrt{163}}$ que difiere de $744 + 640320^3$ menos de 10^{-12}.

El punto común en la mayor parte de estas identidades aproximadas, cuando aparecen en teoría de números, es que aprovechan la rápida convergencia de un desarrollo de Fourier con cierto sentido aritmético. En el caso de la constante de Ramanujan (que, por cierto, se debe a Hermite y no parece en el trabajo de Ramanujan, aunque hay algunas cantidades relacionadas en [Ram00]), se emplea el desarrollo de Fourier del invariante j junto con la interpretación de valores especiales de j como raíces de la ecuación modular (una demostración autocontenida se puede ver en [CR10]). La aproximación a un entero de la constante de Ramanujan corresponde a tomar dos términos en el desarrollo de Fourier.

En este capítulo obtenemos algunas identidades aproximadas asociadas al desarrollo espectral del operador de Laplace-Beltrami en superficies de Riemann. En comparación con las aproximaciones derivadas del análisis de Fourier clásico, el papel desempeñado por los enteros positivos pasa ahora al espectro discreto, en particular, al tamaño de los autovalores. El espectro continuo, cuando existe, contribuye con una suma finita de integrales.

Para ilustrar nuestras identidades aproximadas, mencionamos aquí dos ejemplos. Consideremos la serie y la integral dadas por

$$S = \sum_{n=0}^{\infty} \big(3 + (-1)^n\big) \frac{r(n)r(n+4)}{2(n+4)^2} \qquad \text{y} \qquad I = \int_{-\infty}^{\infty} \frac{\frac{1}{4} + t^2}{\cosh(\pi t)} |f(t)|^2 \, dt$$

donde $r(n) = \#\big\{(a,b) \in \mathbb{Z}^2 \ : \ a^2 + b^2 = n\big\}$ y $f(t) = \zeta(s)L(s,\chi)/\zeta(2s)$, $s = \frac{1}{2} + it$,

con $L(s,\chi)$ la función L de Dirichlet para el carácter no principal χ módulo 4 (nótese que f se relaciona con facilidad con la función zeta de Epstein para x^2+y^2). Existen métodos numéricos eficientes para aproximar $f(t)$ (véase por ejemplo [Bor00]) e I. Usando varios millones de términos en S se puede comprobar que

$$\frac{S-3}{I} = 3.141592\ldots$$

Cabría sospechar que esta cantidad es π, lo cual está en consonancia con los límites razonables de los métodos numéricos, pero nosotros probaremos que en realidad es superior a π en una cantidad menor de $4\cdot 10^{-14}$. Esta precisión se relaciona con el tamaño del tercer autovalor del operador de Laplace-Beltrami en $\mathrm{PSL}_2(\mathbb{Z})\backslash\mathbb{H}$ y de un valor especial de la correspondiente autofunción. De hecho, es una relación en los dos sentidos: el valor de $\pi-(S-3)/I$ da una aproximación para una determinada expresión que involucra estas cantidades espectrales.

Nuestro segundo ejemplo es la serie

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

Resulta que S está muy cerca de $72e^9\sqrt{\pi}$. De hecho, veremos que el error relativo es no nulo y menor que $3\cdot 10^{-7}$. Esta cifra está relacionada con el tamaño del primer autovalor no trivial del operador de Laplace-Beltrami en la curva de Shimura $X(6,1)$, con la notación de [AB04], la que corresponde a un álgebra de cuaterniones con menor discriminante.

3.2. Resultados auxiliares

De nuevo, vamos a considerar núcleos automorfos del tipo (1.14), asumiendo en todo momento buenas condiciones de regularidad y decaimiento para k [Iwa02, (1.63)]. Para mayor comodidad recordamos aquí la fórmula de pretraza (1.20).

Lema 3.2.1. *Sea h la transformada de Selberg de k tal que es holomorfa en $|\Im(t)| \le 1/2+\eta$ con $h(t) = O\big(|t|^{-2-\eta}\big)$, entonces*

$$\begin{aligned}\sum_{\gamma\in\Gamma} k\big(u(z,\gamma w)\big) = &\sum_{j=0}^{\infty} h(t_j)u_j(z)\overline{u_j(w)} \\ &+ \frac{1}{4\pi}\sum_{\mathfrak{a}}\int_{-\infty}^{\infty} h(t)E_{\mathfrak{a}}(z,1/2+it)\overline{E_{\mathfrak{a}}(w,1/2+it)}\,dt\end{aligned}$$

Si Γ es cocompacto el último término en el desarrollo no aparece. Típicamente, el término principal en la fórmula de pretraza viene de la autofunción constante $u_0(z) = |\Gamma\backslash\mathbb{H}|^{-1/2}$, donde $|\Gamma\backslash\mathbb{H}|$ es el área del dominio fundamental de Γ.

En esta sección, nuestro trabajo se centra en la búsqueda de transformadas de Selberg explícitas. En primer lugar, planteamos dos resultados principales

Lema 3.2.2. *Dada una función k y su transformada de Selberg h, se tiene*

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

Demostración. El resultado se deduce a partir de las igualdades

$$h(i/2) = \int_{\mathbb{H}} k\big(u(i,z)\big)\, d\mu(z) = 4\int_0^\infty \int_0^\pi k(u)\, du d\varphi = 4\pi \int_0^\infty k(u)\, du,$$

donde hemos empleado coordenadas polares hiperbólicas (u, φ) (veáse [Iwa02, §1.3]). □

Dadas dos funciones k_1 and k_2, definimos su *convolución hiperbólica* $k_1 * k_2$, como

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

La integral depende sólo de $u(z,w)$ ya que $z \mapsto gz$, $w \mapsto gw$ con $g \in G$ la deja invariante.

Lema 3.2.3. *Si h_1 y h_2 son las transformadas de Selberg de k_1 y k_2, entonces su producto $h_1 h_2$ es la transformada de Selberg de $k_1 * k_2$.*

Demostración. La prueba se reduce a una doble aplicación de la fórmula (1.15), para $\phi(z) = (\Im z)^s$,

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

Por supuesto, se asume implícitamente que la regularidad de k_1 y k_2 asegura la convergencia de las integrales. □

Debido a la definición de la fórmula inversa para la transformada de Selberg no es fácil encontrar ejemplos que den resultados explícitos.

Lema 3.2.4. *Sea $\mu \in \mathbb{C}$ con $\Re\mu > 1$. Entonces, la transformada de Selberg de $k(u) = (u+1)^{-\mu}$ es*

$$h(t) = \frac{4\pi}{\Gamma^2(\mu)}\Gamma\big(\mu - \frac{1}{2} + it\big)\Gamma\big(\mu - \frac{1}{2} - it\big).$$

En particular,

$$h(t) = \frac{4\pi^2}{(\mu-1)!^2\cosh(\pi t)}\prod_{n=1}^{\mu-1}\Big(\big(n-\frac{1}{2}\big)^2 + t^2\Big), \qquad si\ \ \mu \in \mathbb{Z},\ \mu > 1,$$

y

$$h(t) = \frac{\big(\mu - \frac{3}{2}\big)!^2\, 4^{2\mu-1}\,\pi t}{(2\mu-2)!^2\,\mathrm{senh}(\pi t)}\prod_{n=1}^{\mu-\frac{3}{2}}(n^2+t^2), \qquad si\ \ \mu - \frac{1}{2} \in \mathbb{Z},\ \mu > 1.$$

Demostración. A partir de la definición de transformada de Selberg y mediante el cambio de variable $x \mapsto (y+1)\sqrt{x}$, se tiene

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

donde B es la función especial clásica Beta, que admite la representación integral [GR07],

$$B(z_1,z_2) = \int_0^\infty \frac{u^{z_2-1}}{(1+u)^{z_1+z_2}}\,du$$

y satisface $\Gamma(z_1)\Gamma(z_2) = \Gamma(z_1+z_2)B(z_1,z_2)$. El resultado se obtiene usando estas relaciones, así como la fórmula de duplicación de la función Gamma.

Por otro lado, las conocidas fórmulas [GR07]

$$\Big|\Gamma\big(\tfrac{1}{2}+it\big)\Big|^2 = \frac{\pi}{\cosh(\pi t)}, \quad \Big|\Gamma\big(1+it\big)\Big|^2 = \frac{\pi t}{\mathrm{senh}(\pi t)} \quad \text{y} \quad \Gamma\big(n+\tfrac{1}{2}\big) = \frac{(2n-1)!}{2^{n-1}(n-1)!}\sqrt{\pi},$$

dan las expresiones particulares para μ entero y semi-entero. □

Lema 3.2.5. *La transformada de Selberg de $k(u) = e^{-\mu u}$, con $\mu > 0$, es la función $4e^{\mu/2}\sqrt{\pi/\mu}\,K_{it}(\mu/2)$, donde $K_\nu(z)$ es la función de Bessel modificada de segunda especie.*

Demostración. Manipulando la definición (1.16), se tiene

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

Un cambio de variable en (2.7) da la representación integral

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

La demostración concluye combinando ambos resultados. □

Lema 3.2.6. *Para $\alpha, \beta > 0$, 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. Para $\mu > 0$, definimos la función $k_\mu(u) = \sqrt{\mu/(8\pi)}\, e^{-\mu(1+2u)}$. Usando el lema previo, la transformada de Selberg de $k_\mu(u)$ es $K_{it}(\mu)$. Por lo tanto, de acuerdo con el Lema 3.2.3, sólo tenemos que demostrar que $(k_\alpha * k_\beta)\big(u(z,w)\big) = k\big(u(z,w)\big)$. Como ambos términos son $\mathrm{SL}_2(\mathbb{R})$ invariantes, podemos limitarnos a considerar los puntos $z = i$ y $w = \lambda i$, para algún $\lambda > 0$. Entonces $u(z,w) = (\lambda-1)^2/4\lambda$, y se tiene que

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

La última integral se puede expresar como $K_{1/2}(z)$, que es la función elemental $e^{-z}\sqrt{\pi/2z}$ (véase, por ejemplo [GR07, §8]). □

Lema 3.2.7. *La transformada de Selberg de $k(u) = u^{-2}\big((1+2/u)\log(1+u) - 2\big)$, con $k(0)$ definido por continuidad como $k(0) = 1/6$, es*

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

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

Demostración. A partir de los Lemas 3.2.3 y 3.2.4, la transformada de Selberg de $(u+1)^{-2} * (u+1)^{-2}$ es exactamente $8\pi h(t)$. Entonces es suficiente ver que

$$8\pi k\big(u(z,w)\big) = \int_{\mathbb{H}} \big(u(z,v)+1\big)^{-2}\big(u(v,w)+1\big)^{-2}\, d\mu(v). \tag{3.1}$$

Al igual que en la prueba anterior, podemos limitarnos a tomar $z=i$ y $w=(2c+1)i$, con $c>-1/2$. Con esta elección, $u(z,w)=c^2/(2c+1)^2$ 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 otra lado, la integral en (3.1) es

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

donde

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

Tras realizar el cambio de variable $y \mapsto y-c-1$, se obtiene

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

y la evaluación de esta integral racional conduce a la misma expresión que para $8\pi k\big(u(z,w)\big)$ de modo que (3.1) queda probado. □

3.3. El caso no compacto

En el Capítulo 1 mencionamos los ejemplos más notables de grupos fuchsianos, el grupo modular completo $\Gamma_0(1)$, y el grupo modular de congruencias $\Gamma_0(N)$. Además, será conveniente considerar también el grupo $\widetilde{\Gamma}$, definido como el subgrupo de $\Gamma_0(1)$ tal que $a_{11}+a_{22}$ y $a_{12}+a_{21}$ son ambos pares. Es fácil comprobar que de hecho $\widetilde{\Gamma}$ es un conjugado de $\Gamma_0(2)$.

$$\widetilde{\Gamma} = \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}^{-1} \Gamma_0(2) \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix} \Big/ \{\pm \mathrm{Id}\}.$$

Una característica especial de $\Gamma_0(1)$ y $\widetilde{\Gamma}$ es que los núcleos automorfos tienen una interpretación aritmética directa y el Lema 3.2.1 proporciona una especie de desarrollo de Fourier para estas cantidades.

Proposición 3.3.1. *Se tienen los siguientes desarrollos espectrales*

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

b) $$\sum_{n=0}^{\infty} \big(3+(-1)^n\big)r(n)r(n+4)k\big(\frac{n}{4}\big)$$
$$= 96\int_0^{\infty} k(x)\,dx + 8\sum_{j=1}^{\infty} h(t_j)|u_j(i)|^2 + \frac{8}{\pi}\int_{-\infty}^{\infty} h(t)|f(t)|^2\,dt$$

donde h es la transformada de Selberg de k, $f(t) = \zeta(s)L(s,\chi)/\zeta(2s)$ con $s = \frac{1}{2}+it$, y $\frac{1}{4}+\widetilde{t}_j^{\,2}$, $\frac{1}{4}+t_j^2$ son los autovalores no triviales en $\widetilde{\Gamma}\backslash\mathbb{H}$ y $\Gamma_0(1)\backslash\mathbb{H}$, respectivamente.

Para la prueba necesitamos dos fórmulas (cf. [Iwa02, §12]) y una descripción explícita de la serie de Eisentein para $\Gamma_0(1)$ y $\widetilde{\Gamma}$.

Lema 3.3.2. *Se tienen las siguiente identidades*

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

b) $$8\sum_{\gamma\in\Gamma_0(1)} k\big(u(\gamma i,i)\big) = \sum_{n=0}^{\infty} \big(3+(-1)^n\big)r(n)r(n+4)k\big(\frac{n}{4}\big).$$

Lema 3.3.3. *Sea E la serie de Eisenstein para $\Gamma_0(1)$ y $E_{\mathfrak{a}}$, $E_{\mathfrak{b}}$ las correspondientes series asociadas a las cúspides $\mathfrak{a}=\infty$ y $\mathfrak{b}=1$ de $\widetilde{\Gamma}$. Entonces*

$$E(i,s) = (2^s+1)E_{\mathfrak{a}}(i,s) = (2^s+1)E_{\mathfrak{b}}(i,s) = \frac{2\zeta(s)L(s,\chi)}{\zeta(2s)}, \tag{3.2}$$

donde χ es el carácter no principal módulo 4.

Demostración del Lema 3.3.2. Sea $\gamma = (a_{ij}) \in G$, entonces

$$\begin{cases} 4u(\gamma i,i) = (a_{11}-a_{22})^2 + (a_{12}+a_{21})^2 \\ 4u(\gamma i,i)+4 = (a_{11}+a_{22})^2 + (a_{12}-a_{21})^2 \end{cases} \tag{3.3}$$

Si $\gamma \in \widetilde{\Gamma}$ estas cantidades son ambas múltiplos de 4, digamos $4n$ y $4n+4$, y recordando que $r(n) = r(4n)$, la identidad en a) queda demostrada.

Para $\gamma \in \Gamma_0(1)$, si $n = 4u(\gamma i, i)$ satisface $n \equiv 1 \pmod 4$ entonces los cuadrados en cada ecuación de (3.3) tienen distinta paridad. La elección de paridad en la primera ecuación, fija el orden de los cuadrados en la segunda, contribuyendo $\frac{1}{2}r(n)r(n+4)$ al número total de soluciones. Si $n \equiv 0, 2 \pmod 4$ entonces los cuadrados tienen la misma paridad y se obtienen $r(n)r(n+4)$ soluciones. Por lo tanto

$$2\sum_{\gamma\in\Gamma_0(1)} k\big(u(\gamma i, i)\big) = \frac{1}{2}\sum_{n\equiv 1\ (4)}^{\infty} r(n)r(n+4)k\big(\frac{n}{4}\big) + \sum_{n\not\equiv 1\ (4)}^{\infty} r(n)r(n+4)k\big(\frac{n}{4}\big).$$

Nótese que $r(n) = 0$ para $n \equiv 3 \pmod 4$, con lo que finalmente se consigue probar b). □

Demostración del Lema 3.3.3. Tomando $z = i$ en la definición de serie de Eisentein (1.8), tenemos

$$E(i,s) = \sum_{\gamma\in\Gamma_\infty\backslash\Gamma_0(1)} \frac{(\Im i)^s}{|j_{\sigma_\infty^{-1}\gamma}(i)|^{2s}} = \frac{1}{2}\sum_{\substack{c,d=-\infty\\(c,d)=1}}^{\infty} \frac{1}{(c^2+d^2)^s} = \frac{1}{2\zeta(2s)}\sum_{n=1}^{\infty}\frac{r(n)}{n^s},$$

donde $r(n)$, el número de representaciones de n como suma de dos cuadrados, satisface $\frac{1}{4}r(n) = 1 * \chi(n)$ y esto da la igualdad entre los extremos de (3.2) que es un resultado clásico.

En el caso del grupo $\widetilde{\Gamma}$, las matrices de escala son

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

que dan lugar a los mismos grupos conjugados

$$\sigma_{\mathfrak{a}}^{-1}\widetilde{\Gamma}\sigma_{\mathfrak{a}} = \left\{ \begin{pmatrix} * & * \\ 2n & m \end{pmatrix} \in \Gamma_0(1) \right\} = \sigma_{\mathfrak{b}}^{-1}\widetilde{\Gamma}\sigma_{\mathfrak{b}}.$$

Por lo tanto

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

y, usando argumentos similares, se obtiene idéntico resultado para la correspondiente serie asociada a la cúspide $\mathfrak{b}$ de $\widetilde{\Gamma}$. Además

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

lo que finaliza la demostración. □

Demostración de la Proposición 3.3.1. Basta usar los lemas anteriores junto con el Lema 3.2.1. La contribución del autovalor trivial se evalúa utilizando el Lema 3.2.2, y teniendo en cuenta que $|\Gamma_0(1)\backslash\mathbb{H}| = \pi/3$, y $|\widetilde{\Gamma}\backslash\mathbb{H}| = \pi$. □

Tomando $k(u) = (u+1)^{-m}$ en la Proposición 3.3.1, con m un entero mayor que 1, se consiguen aproximaciones de π cuya exactitud depende de cantidades espectrales. Consideremos

$$s_m = \sum_{n=0}^{\infty} \big(3 + (-1)^n\big) \frac{r(n)r(n+4)}{2(n+4)^m} \qquad \text{y} \qquad \widetilde{s}_m = \sum_{n=0}^{\infty} \frac{r(n)r(n+1)}{(n+1)^m}.$$

además de las integrales

$$\gamma_m = \int_{-\infty}^{\infty} g_m(t)|f(t)|^2\, dt \qquad \text{y} \qquad \widetilde{\gamma}_m = \int_{-\infty}^{\infty} g_m(t)\Big|\frac{f(t)}{1+2^{\frac{1}{2}+it}}\Big|^2\, dt,$$

donde

$$g_m(t) = \operatorname{sech}(\pi t) \prod_{j=1}^{m-1} \Big(\big(j-\frac{1}{2}\big)^2 + t^2\Big),$$

y $f(t)$ definido como en la Proposición 3.3.1. Entonces, definimos

$$e_m = (m-1)!^2\, \frac{2^{2m-4}(m-1)s_m - 3}{(m-1)\gamma_m} - \pi \qquad \text{y} \qquad \widetilde{e}_m = (m-1)!^2\, \frac{(m-1)\widetilde{s}_m - 8}{16(m-1)\widetilde{\gamma}_m} - \pi.$$

Teorema 3.3.4. *Para todo entero $m > 1$,*

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

donde $\lambda_3 = \frac{1}{4} + t_3^2$ con $t_3 = 13.77975\ldots$, es el tercer autovalor no trivial en $\Gamma_0(1)\backslash\mathbb{H}$.

Demostración. Usando la Proposición 3.3.1 a), con $k_m(u) = 4^{-m}(u+1)^{-m}$, y los Lemas 3.2.4 y 3.2.2, se tiene

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

donde se ha usado que el área del dominio fundamental de $\Gamma_0(1)$ es $\pi/3$. También tenemos una expresión para el término de error dada por

$$e_m = \frac{4^{m-2}(m-1)s_m - 3}{(m-1)\gamma_m}(m-1)!^2 - \pi = \frac{\pi^2}{\gamma_m} \sum_{j=1}^{\infty} g_m(t_j)|u_j(i)|^2, \tag{3.4}$$

que es positivo ya que $u_j(i) \neq 0$ infinitas veces (de hecho se sabe que el conjunto de estos valores es infinito [Iwa02, §13.2]). Finalmente, notando que $g_{m+1}(t) = \big((m-1/2)^2+t^2\big)g_m(t)$, se llega a

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

donde u_1 y u_2 son autofunciones impares por lo que $u_j(i)=0$, mientras que $\lambda_3 = \frac{1}{4}+t_3^2$ con $t_3 = 13.77975\ldots$ corresponde a una autofunción par [BSV06]. □

Teorema 3.3.5. *Para cualquier entero $m>1$,*

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

donde $\widetilde{\lambda}_1 = \frac{1}{4}+\widetilde{t}_1{}^2$ con $\widetilde{t}_1 = 8.92287\ldots$, es el menor autovalor no trivial en $\widetilde{\Gamma}\backslash\mathbb{H}$.

Demostración. La prueba es similar a la del Teorema 3.3.4, pero en este caso $k_m(u) = (u+1)^{-m}$ y el área del domino fundamental de $\widetilde{\Gamma}$ es π. Esto da

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

y se tiene que

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

procediendo como en el caso anterior. □

Análisis numérico y ejemplos en el caso no compacto

Si pensamos en $u_j(z)$ esencialmente acotada [Iwa02, §13] en términos del autovalor, entonces, a primera vista uno puede esperar que e_m sea comparable a $g_m(t_1)/\gamma_m$, pero los cálculos numéricos muestran una mejor aproximación y una diferencia sustancial entre e_m y $\widetilde{e}_m$. Por ejemplo, los valores para $m=3$ y 4 con un truncamiento de 4 cifras decimales, son

$$e_3 = 2.0086\cdot 10^{-12}, \quad \widetilde{e}_3 = 7.2745\cdot 10^{-7}, \quad e_4 = 4.9016\cdot 10^{-11} \quad \text{y} \quad \widetilde{e}_4 = 6.7890\cdot 10^{-6}.$$

La explicación es, como se menciona en la demostración del Teorema 3.3.4, que el primer y segundo autovalor no trivial corresponden en $\Gamma_0(1)$ a autofunciones impares de manera que $u_1(i) = u_2(i) = 0$, mientras que $\lambda_3 = \frac{1}{4}+t_3^2$ con $t_3 = 13.77975\ldots$

proviene de una autofunción par [BSV06]. Por otro lado, para $\widetilde{\Gamma}\backslash\mathbb{H}$ el primer autovalor no trivial $\widetilde{\lambda}_1$ corresponde a una autofunción par (véase [FL]). El tamaño del cociente $\cosh(\pi t_3)/\cosh(\pi\widetilde{t}_1) = 4.23 \cdot 10^6$ explica el por qué la aproximación de π es peor en alrededor 6 órdenes de magnitud.

Nótese que g_m es creciente en m. Entonces, el mejor ejemplo para aproximar π es s_2. En principio, el caso semientero $s_{3/2}$ sería mejor, pero en realidad da una forma aproximada que no involucra a π. En ambos casos, la convergencia de la serie es muy lenta y un cálculo directo es inviable para controlar el término de error. Con el análisis previo, puede deducirse un resultado en esta dirección.

Proposición 3.3.6. *Sea e_m y s_m como antes, entonces*

$$0 < e_2 < 3.62 \cdot 10^{-14} \qquad y \qquad 0 < s_{3/2} - 12 - 8\int_{-\infty}^{\infty} \frac{t|f(t)|^2}{\operatorname{senh}(\pi t)}\, dt < 1.55 \cdot 10^{-15}.$$

Demostración. Las integrales γ_2 y γ_3 convergen rápidamente y el cálculo numérico da $\gamma_2 = 0.23223\ldots$ y $\gamma_3 = 0.80239\ldots$. Cálculos más extensos dan el valor de e_3 mencionado antes, y la sustitución de estos datos en el Teorema 3.3.4 con $m = 2$, permiten llegar a la primera parte del resultado.

Para la segunda parte, la Proposición 3.3.1 b) con $k(u) = (u+1)^{-3/2}$ da

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

La función $g(t) = t^{-1}(1/4+t^2)(9/4+t^2)\tanh(\pi t)$ es creciente para $t > t_3 = 13.77975$ y $u_1(i) = u_2(i) = 0$. Entonces,

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

La última suma es igual a $\gamma_3 e_3/\pi^2$ por (3.4). El resultado se obtiene sustituyendo los valores numéricos de las cantidades involucradas. □

Los Teoremas 3.3.4 y 3.3.5 se extienden también al caso no convergente $m = 1$ redefiniendo $e_1 = s_1/4\gamma_1$ y $\widetilde{e}_1 = \widetilde{s}_1/16\widetilde{\gamma}_1$ donde

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

cuya convergencia puede ser demostrada.

Podemos utilizar la misma idea con otros núcleos, por ejemplo

$$\sum_{n=0}^{\infty} r(n)r(n+1)\,\frac{e^{1-\sqrt{n+1}}}{\sqrt{n+1}}.$$

La transformada de Selberg de $k(u) = e^{1-\sqrt{u+1}}/\sqrt{u+1}$ es $h(t) = 8e\,K_{it}^2(1/2)$ por el Lema 3.2.6 con $\alpha = \beta = 1/2$. Ahora, denotando la suma previa por S, obtenemos

$$S = 64e\int_0^{\infty} k(x)\,dx + 16e\sum_{j=1}^{\infty} h(\widetilde{t}_j)|u_j(i)|^2 + \frac{32e}{\pi}\int_{-\infty}^{\infty} K_{it}^2(1/2)\Big|\frac{f(t)}{1+2^{\frac{1}{2}+it}}\Big|^2\,dt.$$

Sea I la última integral. Con millones de términos en S y aproximando I, finalmente se llega a que

$$\frac{S-16}{32I} = 0.8652559794526\ldots$$

difiere de e/π menos de $2.04\cdot 10^{-11}$.

También es posible probar fórmulas aproximadas asociadas a grupos de congruencias generales, pero tienen una interpretación aritmética menos directa.

3.4. El caso compacto

Sea H un álgebra de cuaterniones indefinida $\left(\frac{A,B}{\mathbb{Q}}\right)$ con A y B libres de cuadrados y $A > 0$. Entonces, existe una inmersión de H en $M_2(\mathbb{R})$, dada por

$$\Phi(\lambda_1+\lambda_2 i+\lambda_3 j+\lambda_4 k) = \begin{pmatrix} \lambda_1+\lambda_2\sqrt{A} & \lambda_3+\lambda_4\sqrt{A} \\ B(\lambda_3-\lambda_4\sqrt{A}) & \lambda_1-\lambda_2\sqrt{A}\end{pmatrix}.$$

Por el Teorema 5.2.13 de [Miy06], dado un orden $\mathcal{O} \subset H$, la imagen por Φ de los elementos de norma uno en $\mathcal{O}$, es un grupo fuchsiano de primera especie. Además, será cocompacto si H es un álgebra de división.

El espectro de estos grupos coincide, bajo ciertas condiciones, con el espectro discreto de $\Gamma_0(N)$ donde N depende del discriminante y del nivel del orden [BJ99], [Hej85]. Por otro lado, la fórmula de traza de Selberg prueba que los autovalores para $\Gamma_0(N)$ se agrupan en torno al autovalor $1/4$ cuando N crece [Iwa02, (11.18)]. Por lo tanto, para obtener fórmulas aproximadas como antes lo más sensato es considerar discriminantes y niveles pequeños.

Siguiendo [AB04], especialmente la Proposición 1.60, consideramos los ordenes de Eichler

$$\mathbb{Z}\big[1,i,j,\frac{1}{2}(1+i+j+k)\big] \subset \left(\frac{p,-1}{\mathbb{Q}}\right) \quad \text{y} \quad \mathbb{Z}\big[1,i,\frac{1}{2}(1+j),\frac{1}{2}(i+k)\big] \subset \left(\frac{2,q}{\mathbb{Q}}\right)$$

con $p \equiv 3$ (mód 4) y $q \equiv 5$ (mód 8) primos, que corresponden a las curvas de Shimura $X(2p,1)$ y $X(2q,1)$ con la notación de [AB04].

Un cálculo muestra que los correspondientes grupos cocompactos por Φ son, respectivamente,

$$G_p = \Big\{ \frac{1}{2} \begin{pmatrix} a+b\sqrt{p} & c+d\sqrt{p} \\ -c+d\sqrt{p} & a-b\sqrt{p} \end{pmatrix} \in \mathrm{SL}_2(\mathbb{R}) : \ a \equiv b \equiv c \equiv d \pmod 2 \Big\} \Big/ \{\pm \mathrm{Id}\}$$

y

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

Los desarrollos espectrales recuerdan al de $\Gamma_0(1)$ pero son más atractivos porque no aparecen las integrales asociadas al espectro continuo.

Proposición 3.4.1. *Sean $p \equiv 3$ (mód 4) y $q \equiv 5$ (mód 8) primos, entonces se tienen los siguientes desarrollos espectrales*

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

y

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

donde h es la transformada de Selberg de k y $r_{s,t}(n)$ denota el número de pares $(a,b) \in \mathbb{Z}^2$ tales que $n = sa^2 + tb^2$.

Para la demostración necesitamos de nuevo una expresión aritmética para núcleos automorfos.

Lema 3.4.2. *Tomando p y q como antes, se tiene*

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

y

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

Demostración. Nótese que para $\gamma \in G_p$, $4u(\gamma i, i) = p(b^2+d^2)$. Además, $\gamma \in \mathrm{SL}_2(\mathbb{R})$ implica $p(b^2+d^2)+4 = a^2+c^2$. Como a, b, c, d tienen la misma paridad, $2 \mid b^2+d^2$. Por otra parte, esta condición determina G_p hasta el signo $\pm\gamma$. Por lo tanto

$$2\sum_{\gamma\in G_p} k\big(u(\gamma i, i)\big) = \sum_{n=0}^{\infty} r(2n)r(2pn+4)k\big(\frac{pn}{2}\big),$$

y, notando que $r(n) = r(2n)$ se llega a la demostración de la primera igualdad.

Para la segunda, dado n, el número de soluciones $(a, b, c, d) \in \mathbb{Z}^4$ de

$$\begin{cases} n = 2b^2 + qc^2 \\ n+4 = a^2 + 2qd^2 \end{cases}$$

es $r_{2,q}(n)r_{1,2q}(n+4)$. Es claro que a y c tienen la misma paridad, y esto implica que b y d tienen la misma paridad también. Entonces, (a, b, c, d) da lugar a un $\gamma \in G_{2,q}$, con $4u\big(\gamma(i/\sqrt{q}), i/\sqrt{q}\big) = 2b^2 + qc^2$. Recíprocamente, $\gamma \in G_{2,q}$ da dos soluciones $\pm(a, b, c, d)$ de las ecuaciones anteriores con $n = 4u\big(\gamma(i/\sqrt{q}), i/\sqrt{q}\big)$. □

Demostración de la Proposición 3.4.1. Basta usar el lema previo en la fórmula de pretraza, Lema 3.2.1, notando que de acuerdo con [BJ99, (2.1)], el área del dominio fundamental es $|G_p\backslash\mathbb{H}| = (p-1)\pi/3$ en el primer caso y $|G_{2,q}\backslash\mathbb{H}| = (q-1)\pi/3$, en el segundo. □

Análisis numérico y ejemplos en el caso compacto

Ilustramos la Proposición 3.4.1 con un ejemplo explícito (mencionado en la introducción), en el que los argumentos numéricos y teóricos se combinan para controlar la precisión de la aproximación. El grupo subyacente es G_3, que es óptimo en el sentido de que tiene el mayor salto espectral entre las posibles elecciones de p.

Proposición 3.4.3. *Sea*

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

Entonces

$$1.29\cdot 10^{-7} < 1 - \frac{S}{72e^9\sqrt{\pi}} < 3\cdot 10^{-7}.$$

Para la prueba emplearemos una cota superior explícita en el problema del círculo hiperbólico (el análisis espectral da fórmulas asintóticas pero los términos de error no son explícitos [Iwa02, §12]).

Lema 3.4.4. *Se tiene que*

$$\#\{\gamma \in G_3 : \rho(\gamma i, i) < R\} \leq 3(2+\sqrt{3})\cosh R,$$

donde ρ es la distancia hiperbólica definida en (1.1).

Demostración. Sea D el dominio fundamental de $G_3\backslash\mathbb{H}$. Por el Teorema 5.46 de [AB04], D es el polígono con vértices

$$v_1 = \frac{-\sqrt{3}+i}{2},\ v_2 = \frac{-1+i}{1+\sqrt{3}},\ v_3 = (2-\sqrt{3})i,\ v_4 = \frac{1+i}{1+\sqrt{3}},\ v_5 = \frac{\sqrt{3}+i}{2},\ v_6 = i.$$

Usando (1.2), la distancia hiperbólica desde v_6 a cualquier otro vértice es como máximo $\cosh^{-1} 2$. Por lo tanto, $D \subset B(i, \cosh^{-1} 2)$, donde $B(z_0, r) = \{z \in \mathbb{H} : \rho(z, z_0) \leq r\}$.

Sea $\mathcal{A} = \{\gamma \in G_3 : \rho(\gamma i, i) < R\}$. Entonces

$$\bigcup_{\gamma\in\mathcal{A}} \gamma D \subset B(i, R + \cosh^{-1} 2).$$

Por la definición de dominio fundamental, los interiores de los conjuntos en la parte izquierda son disjuntos. Por lo tanto

$$\#\mathcal{A} \leq \frac{|B(i, R+\cosh^{-1} 2)|}{|D|} = 3(2\cosh R + \sqrt{3}\,\mathrm{senh}\, R - 1),$$

donde hemos usado la fórmula para el área del círculo hiperbólico [Iwa02, §1.1] y que $|D| = 2\pi/3$. □

Demostración de la Proposición 3.4.3. Dividimos S en dos sumas tales que

$$S = \sum_{n<N} + \sum_{n\geq N} = S_1 + S_2, \qquad \text{con} \quad N = 2.2 \cdot 10^{12}.$$

Un cálculo numérico extenso muestra que

$$2 \cdot 10^{-7} < 1 - \frac{S_1}{72e^9\sqrt{\pi}} < 3 \cdot 10^{-7}. \tag{3.5}$$

Para S_2, el Lema 3.4.2 con $\cosh R = 1 + 3X$ junto con el Lema 3.4.4 implican

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

Subdividiendo la suma en intervalos diádicos,

$$S_2 \leq \sum_{M=2^j N} \sqrt{M} e^{-(\log M)^2/16} \sum_{n\leq 2M} r(n)r(3n+2) \leq 36(2+\sqrt{3}) \sum_{M=2^j N} M^{3/2} e^{-(\log M)^2/16}.$$

Extraemos los términos correspondientes a $j = 0, 1$, y acotamos el resto con una integral.

$$S_2 \leq 36(2+\sqrt{3})\Big(3.8977 \cdot 10^{-4} + 9.1185 \cdot 10^{-5} + \frac{1}{\log 2}\int_{\log 2N}^{\infty} e^{3x/2-x^2/16}\, dx\Big)$$
$$\leq 6.4619 \cdot 10^{-2} + \frac{36(2+\sqrt{3})}{\log 2} \cdot \frac{8}{\log 2N - 12}\int_{\log 2N}^{\infty} \frac{x-12}{8}\, e^{3x/2-x^2/16}\, dx.$$

De donde

$$0 < \frac{S_2}{72e^9\sqrt{\pi}} < 7.0479 \cdot 10^{-8}.$$

El resultado se sigue de estas desigualdades y de (3.5). □

Con la elección de núcleos adecuados se pueden conseguir cotas superiores para el primer autovalor no trivial en G_p con $u_j(i) \neq 0$. Por ejemplo, tomando el núcleo

$$k(u) = \frac{4603.9844}{(u+1)^{3/2}} - \frac{4247.8634}{(u+1)^2} + \frac{1272.2748}{(u+1)^{5/2}}$$

en la Proposición 3.4.1, con $p = 3$, la parte izquierda y la integral se cancelan, y la transformada de Selberg, por el Lema 3.2.4, es positiva para $t > 3.13$. Por lo tanto, el primer autovalor en G_3 con $u_j(i) \neq 0$ es menor que 3.13. El valor real es aproximadamente 2.59.

3.5. Aplicación de los operadores de Hecke

En analogía con la teoría clásica [Miy06] se introducen operadores de Hecke [Iwa02, §8.5]

$$T_m f(z) = \frac{1}{\sqrt{m}} \sum_{\gamma \in \Gamma_0(1)\backslash\Gamma_m} f(\gamma z)$$

actuando sobre funciones (no holomorfas) $f \in L^2(\Gamma\backslash\mathbb{H})$, donde Γ_m son matrices enteras con determinante m. Nótese que estas matrices conmutan claramente con Δ. Estos operadores son auto-adjuntos y las formas de Maass cuspidales $\{u_j(z)\}_{j=0}^{\infty}$ pueden elegirse de forma que también sean autofunciones de T_m con autovalores que denotamos por $\{\lambda_j(m)\}_{j=0}^{\infty}$. En $\Gamma_0(N)$, la teoría es idéntica cuando $\mathrm{mcd}(N, m) = 1$ y existe una teoría de Atkin-Lehner para cubrir el resto de casos.

Los operadores de Hecke también se definen de la misma forma en grupos cocompactos correspondientes a álgebras de cuaterniones indefinidas sobre $\mathbb{Q}$ (véase [Are05], [Miy06, §5.3]), donde ahora la suma toma $\gamma \in R(1)\backslash R(m)$ y $R(k)$ es la imagen de la aplicación en $M_2(\mathbb{R})$ de los elementos de norma k de un orden R.

Cuando aplicamos T_m a un núcleo automorfo con respecto al grupo modular completo $\Gamma_0(1)$, la suma queda

$$T_m\Big(\sum_{\gamma\in\Gamma_0(1)} k(\gamma(\cdot),w)\Big)(z) = \frac{1}{\sqrt{m}}\sum_{\gamma\in\Gamma_m} k(\gamma z,w).$$

Entonces, formalmente, la aplicación del operador de Hecke corresponde a considerar en los núcleos automorfos, matrices enteras de determinante m en vez de 1.

Por otro lado, la acción de T_m en la fórmula de pretraza, Lema 3.2.1, es

$$\sum_{j=0}^{\infty}\lambda_j(m)h(t_j)u_j(z)\overline{u_j(w)} + \frac{1}{4\pi}\int_{-\infty}^{\infty}\eta_t(m)h(t)E(z,1/2+it)\overline{E(w,1/2+it)}\,dt \quad (3.6)$$

donde $\eta_t(m)$ es la función divisor $\sum_{ab=m}(a/b)^{it}$ (véase [Iwa02]).

Fórmulas similares se usan en el caso asociado a álgebras de cuaterniones cuando m es coprimo con el discriminante del álgebra y con el nivel del orden (por supuesto la integral correspondiente al espectro continuo no aparecerá).

Nos centramos aquí en el grupo $\Gamma_0(1)$ y en el orden $R=\mathbb{Z}\big[1,i,j,\frac{1}{2}(1+i+j+k)\big]$ que se empleó para definir G_p. En este último caso, se describe el núcleo automorfo en términos de la correlación de $r(n)$ consigo mismo en progresiones aritméticas.

Lema 3.5.1. *Con Γ_m como antes, se tiene*

$$8\sum_{\gamma\in\Gamma_m} k\big(u(\gamma i,i)\big) = \sum_{n=0}^{\infty}\big(3+(-1)^n\big)r(n)r(n+4m)k\big(\frac{n}{4m}\big).$$

Y para el orden $R=\mathbb{Z}\big[1,i,j,\frac{1}{2}(1+i+j+k)\big]$

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

donde, como antes $p\equiv 3 \pmod 4$ es primo y $R(m)$ denota la imagen de los elementos de norma m.

Demostración. Para $\gamma\in(a_{ij})$ con determinante m,

$$\begin{cases} 4m\,u(\gamma i,i) = (a_{11}-a_{22})^2+(a_{12}+a_{21})^2 \\ 4m\,u(\gamma i,i)+4m = (a_{11}+a_{22})^2+(a_{12}-a_{21})^2 \end{cases}$$

Usando esto, la primera fórmula se sigue modificando consecuentemente la demostración del Lema 3.3.2.

De la misma manera, la segunda se obtiene como en la demostración del Lema 3.4.2 notando 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 tiene que $|\Gamma\backslash\Gamma_m| = \sigma(m)$, la suma de los divisores de m. Análogamente, si m y $2p$ son primos entre sí (véase p.217 de [Miy06]) $|R(1)\backslash R(m)| = \sigma(m)$. Entonces si la transformada de Selberg de k decae rápidamente se espera que (cf. Proposición 3.3.1 y Proposición 3.4.1)

$$\sum_{n=0}^{\infty} \big(3+(-1)^n\big) r(n)r(n+4m)k\big(\frac{n}{4m}\big) \approx 96\sigma(m)\int_0^\infty k(x)\,dx + \frac{8\sqrt{m}}{\pi}\int_{-\infty}^{\infty} \eta_t(m)h(t)|f(t)|^2\,dt \tag{3.7}$$

y

$$\sum_{n=0}^{\infty} r(n)r(pn+2m)k\big(\frac{pn}{2m}\big) \approx \frac{24\sigma(m)}{p-1}\int_0^\infty k(x)\,dx \qquad \text{para} \quad 2\nmid m,\ p\nmid m. \tag{3.8}$$

Por ejemplo, consideremos

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

y

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

Entonces, por (3.7) y el Lema 3.2.4 con $m = 503$ y $k(u) = (u+1)^{-3}$, se tiene

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

Los valores numéricos reales dan

$$\frac{S-24192}{16I} = 70.45857658\ldots$$

que coincide con $\pi\sqrt{503}$ en todos los dígitos mostrados. De hecho, el error real parece ser comparable a 10^{-12}.

Aunque se consigue gran precisión en este ejemplo no se espera que las fórmulas (3.7) y (3.8) sean uniformes en m por el comportamiento irregular de $\lambda_j(m)$. Véase [Cha99] para un análisis de la uniformidad en un contexto cercano.

Es interesante notar que las propiedades multiplicativas de los autovalores de Hecke se pueden observar numéricamente y emplearse para mejorar las aproximaciones. Consideremos por ejemplo

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

donde g es la función k del Lema 3.2.7. Según (3.8), debe aproximar $2\sigma(m)$ pero esta aproximación es pobre debido a la existencia de autovalores pequeños en la parte inferior del espectro. De hecho, se tiene que

$$S_1 - 2 = 0.047039, \qquad S_3 - 8 = -0.109461 \qquad \text{y} \qquad S_9 - 26 = 0.119267.$$

El desarrollo espectral (3.6) y el Lema 3.5.1 sugieren que

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

con h como en el Lema 3.2.7 es la mejor aproximación. Por otro lado, las propiedades multiplicativas de los autovalores de Hecke [Iwa02, §8.5] aseguran que $\big(\lambda_j(3)\big)^2 = 1 + \lambda_j(9)$ que se traduce en $(8 - S_3)^2 \approx 3(2 - S_1)^2 + (26 - S_9)(2 - S_1)$. Por lo tanto, se espera una aproximación mejorada

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

De hecho, el lado izquierdo es 8.001211, mejorando la anterior aproximación $S_3 \approx 8$ en dos órdenes de magnitud.

Parte II

Métodos combinatorios

Capítulo 4

La sucesión de Rowland

4.1. Introducción

En [Row08] E.S. Rowland introdujo la siguiente sucesión definida recursivamente

$$a_k = a_{k-1} + \text{mcd}(k, a_{k-1}) \quad \text{con} \quad a_1 = 7, \tag{4.1}$$

probando el sorprendente resultado:

Teorema 4.1.1 (Rowland [Row08]). *Sea $\mathcal{P}$ el conjunto de primos y $\mathcal{P}_1 = \mathcal{P} \cup \{1\}$. Entonces $a_k - a_{k-1} \in \mathcal{P}_1$ para todo $k > 1$.*

k	1	2	3	4	5	6	7	8	9	10	11	...
a_k	7	8	9	10	15	18	19	20	21	22	33	...
$a_k - a_{k-1}$		1	1	1	5	3	1	1	1	1	11	...
					△	△					△	

Por desgracia, no está claro si la prueba se aplica a todos los posibles valores a_1. Nótese que $a_1 = 2A$ y $a_1 = 2A + 1$ dan lugar al mismo término a_2, por lo que podemos limitarnos a condiciones iniciales impares para estudiar este problema. Por otro lado, es fácil comprobar que $a_1 = 1$ y $a_1 = 3$ conducen a las mismas sucesiones $a_k = k$ y $a_k = k+2$, respectivamente. Por lo tanto, solo consideraremos las sucesiones

$$a_k = a_{k-1} + \text{mcd}(k, a_{k-1}) \quad \text{con} \quad a_1 > 3 \quad \text{impar}. \tag{4.2}$$

Conjetura 4.1.2. *Para toda sucesión de la forma* (4.2)*, existe un entero positivo N tal que $a_k - a_{k-1} \in \mathcal{P}_1$ para todo $k > N$.*

En realidad, en [Row08], esta conjetura se menciona para valores iniciales de la forma $a_{k_0} = A$ con k_0 no necesariamente 1. Nosotros consideramos que la formulación anterior es más natural (aunque menos general) y, como veremos más adelante,

existen diferencias entre las dos situaciones. En [Clo11] aparecen otras conjeturas acerca de sucesiones relacionadas.

Nuestro enfoque depende de la introducción de dos recurrencias auxiliares. Se trata de una versión del atajo mencionado en [Row08]. Antes de dar las definiciones concretas, intentamos motivarlas incluyendo aquí una demostración muy sencilla del Teorema 4.1.1 en una forma más fuerte, utilizando las sucesiones

$$c_n^* = c_{n-1}^* + \operatorname{mfp}(c_{n-1}^*) - 1 \quad \text{y} \quad r_n^* = \frac{c_n^* + 1}{2} \quad \text{con} \quad c_1^* = 5, \tag{4.3}$$

donde $\operatorname{mfp}(\cdot)$ denota el menor factor primo. Nótese que c_n^* es impar para todo n.

Proposición 4.1.3. *Sea $\{a_k\}_{k=1}^{\infty}$ la sucesión de Rowland* (4.1)*. Entonces*

$$a_k - a_{k-1} = \begin{cases} \operatorname{mfp}(c_{n-1}^*) & \textit{si } \ k = r_n^* \ \textit{ para algún } \ n > 1, \\ 1 & \textit{en otro caso.} \end{cases} \tag{4.4}$$

Demostración. Definimos $x_1 = 7$, $x_2 = 8$, y $x_k = c_n^* + k + 1$ para $k \in [r_n^*, r_{n+1}^*)$, $n \geq 1$. Si $k \in (r_n^*, r_{n+1}^*)$ es fácil ver que los valores $x_k - x_{k-1}$ son siempre iguales a 1, pues en los dos miembros de la diferencia se considera el mismo término c_n^*. Cuando $k = r_n^* > 3$, se tiene $x_{k-1} = c_{n-1}^* + k$, y la diferencia pasa a ser $\operatorname{mfp}(c_{n-1}^*)$. Para ver que $a_k = x_k$, y consecuentemente obtener el resultado, basta probar que este valor coincide con $\operatorname{mcd}(k, x_{k-1})$. De nuevo, si $k \in (r_n^*, r_{n+1}^*)$,

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

y esto es 1 pues $2(k - r_n^*) + 1 < 2(r_{n+1}^* - r_n^*) + 1 = \operatorname{mfp}(c_n^*)$, mientras que si $k = r_n^*$, tenemos $\operatorname{mcd}(k, x_{k-1}) = \operatorname{mcd}(r_n^*, c_{n-1}^* + r_n^*) = \operatorname{mcd}(c_n^* + 1, c_{n-1}^*) = \operatorname{mfp}(c_{n-1}^*)$. □

Esta breve demostración del Teorema 4.1.1 sugiere la introducción de unas sucesiones generales

$$\begin{cases} r_1 = 1 \\ r_{n+1} = \min\left\{p + p\lfloor r_n/p \rfloor \ : \ p \mid c_n\right\} \end{cases} \quad \text{y} \quad \begin{cases} c_1 = a_1 - 2 \\ c_{n+1} = c_n + \operatorname{mcd}(c_n, r_{n+1}) - 1 \end{cases} \tag{4.5}$$

donde $\lfloor \cdot \rfloor$ denota la parte entera y p es primo. Es fácil comprobar que $r_n = r_n^*$ y $c_n = c_n^*$ satisfacen esta recurrencia para $n > 1$, donde r_n^* y c_n^* se toman como en (4.3). De nuevo, c_n es impar para todo n. Un argumento elemental da una expresión alternativa para r_n mostrando que r_{n+1} es el menor número mayor que r_n que no es coprimo con c_n (véase el Lema 4.2.1 más adelante y cf. Proposición 3 [Row08]).

La sucesión (4.2) está determinada por (4.5). De hecho, r_n da los índices k para los cuales $a_k - a_{k-1} \neq 1$. El análogo a la Proposición 4.1.3 es

Proposición 4.1.4. *La sucesión* (4.2) *satisface*

$$a_k = c_n + k + 1 \qquad \textit{para} \qquad r_n \leq k < r_{n+1}, \tag{4.6}$$

donde r_n *y* c_n *se definen como en* (4.5). *Además,* $a_k - a_{k-1}$ *es igual a* $\operatorname{mcd}(c_{n-1}, r_n)$ *si* $k = r_n$ *para algún* $n > 1$, *e igual a* 1 *en otro caso.*

Rowland señala que su prueba se puede aplicar cuando $a_k = 3k$ para algún k (esto ocurre en (4.1) cuando $k = 3$). Con nuestra prueba, esto corresponde a que $c_n = 2r_n - 1$ para algún n, lo que de hecho implica que $c_l = 2r_l - 1$ para $l > n$. Por otro lado, la idea subyacente en gran número de conjeturas (por ejemplo, la hipótesis de Schinzel [SS58], las conjeturas de k-uplas de Hardy-Littlewood [ORW99], [GBGL08, IV.2] o de forma más general la conjetura de Bateman-Horn [BHC61]) es que los primos deben aparecer en una sucesión si ninguna condición de divisibilidad local lo impide, por lo que una suposición natural es que c_m es primo para algún m. Curiosamente, parece que las menores elecciones de m y n en estas afirmaciones son siempre consecutivas.

Por ejemplo, si $a_1 = 117$ se tiene

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	...
					♦	◊					

En este caso, $c_n = 2r_n - 1$ por primera vez cuando $n = 6$, y el primer valor tal que c_m es primo ocurre para $m = 5$. Hemos comprobado cada $a_1 < 10^8$ y los experimentos sugieren:

Conjetura 4.1.5. *Consideremos la sucesión* (4.5) *con* $a_1 > 3$ *impar. Se define*

$$n_0 = \text{ínf}\{n \in \mathbb{Z}^+ \,:\, c_n = 2r_n - 1\} \qquad y \qquad m_0 = \text{ínf}\{n \in \mathbb{Z}^+ \,:\, c_n \textit{ es primo}\},$$

escribiendo como de costumbre $\text{ínf}\,\emptyset = \infty$. *Entonces*

$$\text{(i)} \quad n_0 < \infty, \qquad \text{(ii)} \quad m_0 < \infty, \qquad \text{(iii)} \quad n_0 = m_0 + 1 < \infty.$$

En la Sección 4.2 se dan evidencias teóricas y equivalencias entre las conjeturas. En la Sección 4.3 se obtienen algunas propiedades del conjunto de primos generado por las sucesiones (4.2). Cualquiera de los tres enunciados en la Conjetura 4.1.5 implica la Conjetura 4.1.2 (Proposición 4.3.2). En términos de a_k, (iii) implica que el primer k para el cual $a_k - a_{k-1} \neq 1$ y $a_k = 3k$ es necesariamente primo (Proposición 4.2.6).

Para sucesiones con valor inicial distinto a a_1, la última propiedad de primalidad (iii) admite contraejemplos. Uno de los más simples es $a_{59} = 153$, que satisface la Proposición 4.1.4 dando en (4.5) los valores iniciales $r_1 = 59$ y $c_1 = 93$. Los siguientes términos

$$\begin{aligned} r_1 &= 59, \quad r_2 = 60, \quad r_3 = 65, \quad r_4 = 66, \quad \ldots \\ c_1 &= 93, \quad c_2 = 95, \quad c_3 = 99, \quad c_4 = 131, \quad \ldots \end{aligned}$$

muestran que se tiene $a_k = 3k$ por primera vez cuando $k = 66$, que corresponde a $c_4 = 2r_4 - 1$, pero ni $r_4 = 66$ ni $c_3 = 99$ son primos.

4.2. Relación entre las conjeturas

Comenzamos dando una fórmula alternativa para r_{n+1} y la prueba de la Proposición 4.1.4.

Lema 4.2.1. *Para $m, n \in \mathbb{Z}^+$*

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

Demostración. El resultado se sigue del hecho de que

$$p + p\left\lfloor \frac{n}{p} \right\rfloor = p\left(1 + \left\lfloor \frac{n}{p} \right\rfloor\right)$$

es el primer múltiplo de p que es mayor que n, y cumple $p \mid \text{mcd}(p + p\lfloor n/p \rfloor, m)$. □

Demostración de la Proposición 4.1.4. Si $k \in (r_n, r_{n+1})$ entonces, por el Lema 4.2.1, se tiene $\text{mcd}(k, c_n) = 1$, de donde

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

Por otro lado, si $k = r_n$, entonces $\text{mcd}(k, c_{n-1}) \neq 1$ y por (4.5) se llega a que

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

Esto prueba (4.6), y de hecho, también que $a_k - a_{k-1}$ es $\text{mcd}(c_{n-1}, r_n)$ si $k = r_n$ y 1 en otro caso. □

La siguiente relación incondicional entre r_n y c_n desempeña un papel importante a la hora de relacionar las conjeturas. Compárese este resultado con la Proposición 1 y 2 en [Row08] y los comentarios que dan allí. Nótese, por ejemplo, que por (4.6), $a_k \geq 3k$ para $k = r_n$.

Proposición 4.2.2. *Sea r_n y c_n definidos como en (4.5) con $a_1 > 3$ impar. Entonces, $r_n \leq (c_n + 1)/2$ para todo $n \in \mathbb{Z}^+$. Además, la igualdad para $n > 1$ ocurre 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. La desigualdad se prueba por inducción. Es evidente que para $n = 1$ es cierta. Supongamos $r_{n-1} \leq (c_{n-1} + 1)/2$. Por definición, $r_n = p + p\lfloor r_{n-1}/p \rfloor$ para algún primo $p \mid c_{n-1}$, y usando la hipótesis de inducción, tenemos

$$r_n = p + p\left\lfloor \frac{r_{n-1}}{p} \right\rfloor \leq p + p\left\lfloor \frac{c_{n-1}+1}{2p} \right\rfloor = p + \frac{c_{n-1} - p}{2} = \frac{c_{n-1} + p}{2}. \tag{4.7}$$

Por otro lado, como $p \mid \mathrm{mcd}(c_{n-1}, r_n)$, entonces

$$\frac{c_{n-1} + p}{2} \leq \frac{c_{n-1} + \mathrm{mcd}(c_{n-1}, r_n)}{2} = \frac{c_n + 1}{2}. \tag{4.8}$$

Combinando (4.7) y (4.8) se concluye el resultado.

Si $\mathrm{mcd}(c_{n-1}, r_n)$ no es primo, entonces tenemos una desigualdad estricta en (4.8) y $r_n \neq (c_n + 1)/2$. Se llega a la misma conclusión si $p\lfloor r_{n-1}/p \rfloor \neq (c_{n-1} - p)/2$ usando (4.7). Entonces, las propiedades del enunciado son condiciones necesarias para la igualdad. Es sencillo ver que lo contrario también es cierto. □

Usando el Lema 4.2.1, es fácil comprobar que (ii) implica (i). También, trivialmente (iii) implica (i) y (ii).

Corolario 4.2.3. *Si se cumple* (i) *y* $\mathrm{mcd}(c_{n_0-1}, r_{n_0}) > r_{n_0-1}$, *entonces* (iii) *es cierto.*

Demostración. La Proposición 4.2.2 asegura que en esta situación se tiene

$$\mathrm{mcd}(c_{n_0-1}, r_{n_0}) = p \quad \text{primo} \quad \text{y} \quad p\left\lfloor \frac{r_{n_0-1}}{p} \right\rfloor = \frac{c_{n_0-1} - p}{2}.$$

Como $p > r_{n_0-1}$, necesariamente $c_{n_0-1} = p$ y es la primera vez que sucede pues en caso contrario se llegaría una contradicción con la hipótesis (i). □

Podemos redefinir m_0 sin hacer referencia a primos gracias al siguiente resultado.

Proposición 4.2.4. *Dado $n > 1$, $r_n = c_{n-1}$ si y sólo si c_{n-1} es primo.*

Que puede ser reformulada como

Corolario 4.2.5. *Si $r_n = c_{n-1}$ para algún $n > 1$, entonces se cumplen* (i) *y* (ii)

Demostración de la Proposición 4.2.4. Supongamos primero que c_{n-1} es primo. Entonces la Proposición 4.2.2 implica que $r_{n-1} < c_{n-1}$ y, de acuerdo con el Lema 4.2.1, se concluye que r_n tiene que ser c_{n-1}.

Para demostrar el recíproco, supongamos ahora que $r_n = c_{n-1}$ y sea $m = (c_{n-1} + \mathrm{mfp}(c_{n-1}))/2 = (r_n + \mathrm{mfp}(r_n))/2$. Se tiene que $\mathrm{mcd}(m, c_{n-1}) \neq 1$ y, de nuevo por la Proposición 4.2.2, $r_{n-1} < m$. La definición alternativa de r_n dada en el Lema 4.2.1 implica que $r_n \leq m$, o de forma equivalente, $r_n = \mathrm{mfp}(r_n)$. Por lo tanto, $r_n = c_{n-1}$ es primo. □

Proposición 4.2.6. *Suponiendo* (iii)*, existe un primo p tal que*

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

Demostración. Claramente $a_k = 3k$ equivale a $c_n = 2k-1$. Si $a_k - a_{k-1} > 1$, entonces la Proposición 4.1.4 muestra que $k = r_n$ para algún n. Como r_n es creciente, el mínimo se alcanza en r_{n_0} que es primo por la Proposición 4.2.4.

Sin ningún tipo de hipótesis en $a_k - a_{k-1}$, la Proposición 4.1.4 para $r_{n_0-1} \leq k < r_{n_0}$ da

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

y sabemos, por la Proposición 4.2.2, que este valor se encuentra en el intervalo $[r_{n_0-1}, r_{n_0})$.

Sólo queda probar que $a_k > 3k$ para todo $k \leq r_{n_0-1}$. En caso contrario, si $a_{k-1} \leq 3(k-1)$ para algún k, entonces $3 \leq 3k - a_{k-1}$. Por la Proposición 4.1.4, $a_k - a_{k-1}$ es igual a $\mathrm{mcd}(c_{n-1}, r_n)$ para $k = r_n$ e igual a 1 en otro caso, por lo tanto, siempre divide a $3k - a_{k-1}$, de donde $a_k - a_{k-1} \leq 3k - a_{k-1}$, y entonces $a_k \leq 3k$. La iteración del proceso llevaría a una contradicción para $k = r_{n_0-1}$. □

Extensos cálculos muestran que

$$Q_k = \min_{n<n_0} \frac{c_n + 1}{r_n}$$

es, con mucho, superior a 2 cuando a_1 es grande. Por ejemplo, cuando $2^{20} < a_1 < 2^{21}$, el mínimo es 340.56. Cualquier mejora de la Proposición 4.2.2 en esta dirección reduce la equivalencia entre (i) y (iii) a un número finito de cálculos. Computacionalmente, la Conjetura 4.1.5 se verifica para $a_1 < 10^8$.

Proposición 4.2.7. *Supongamos* (i) *y que* $\left(2 + \frac{1}{2500}\right) r_n < c_n + 1$ *para* $n < n_0$. *Entonces también se cumple* (iii).

Demostración. Por la Proposición 4.2.2 se tiene $\mathrm{mcd}(c_{n_0-1}, r_{n_0}) = p$. También, para algún j y l,

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

Para abreviar escribiremos $K = 3500$. Si $j > K$, entonces

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

que no coincide con nuestra hipótesis. De modo que podemos suponer $1 \leq j \leq K$, ya que $j = 0$ implica claramente (iii). Se distinguen varios casos.

Si $p \leq 4K - 3$ entonces $c_{n_0-1} < 10^8 - 2$ que corresponde a algún $a_1 < 10^8$ para el cual (iii) se comprobó de forma computacional.

En otro caso se tiene $p > 4K - 3$. Si $l < p - 2K$, existirá $r_{n_0-1} < m < r_{n_0}$ que es múltiplo de $2j + 1$, por lo tanto $\mathrm{mcd}(m, c_{n_0-1}) \neq 1$, y esto contradice el Lema 4.2.1. Entonces, necesariamente $l \geq p - 2K$ y

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

Comparándolo con la desigualdad que hemos supuesto, se debe cumplir que

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

lo cual es imposible para $j > 0$ y $p > 4K - 3$. □

Proposición 4.2.8. *Dado N, existe a_1 tal que $m_0 > N$.*

Demostración. Sea a_1 tal que $m_0 < \infty$. Tomando $a_1' = a_1 + M$ con $M = c_{m_0}!$, afirmamos que las sucesiones (4.5) correspondientes a a_1' son

$$r_j' = r_j \qquad \text{y} \qquad c_j' = c_j + M \qquad \text{para} \quad j \leq m_0.$$

Claramente c_j es un factor no trivial de c_j' entonces $m_0' > m_0$ e iterando el proceso N veces se obtiene $a_1^{(N)}$ cuyo m_0 supera al menos en N al m_0 correspondiente a a_1.

Para probar la afirmación, basta notar que $\mathrm{mcd}(k, c_j + M) = \mathrm{mcd}(k, c_j)$ para todo $k \leq r_{m_0}$ porque de hecho k divide a M, y usar el Lema 4.2.1. □

4.3. Primos en la sucesión de Rowland

Proposición 4.3.1. *Suponiendo cierto* (i) *se tiene*

$$c_n = c_{n-1} + \mathrm{mfp}(c_{n-1}) - 1 \qquad y \qquad r_n = (c_n + 1)/2,$$

para $n > n_0$.

Demostración. El resultado se alcanza mediante un argumento inductivo para $n \geq n_0$. A partir de (i) se tiene $r_{n_0} = (c_{n_0} + 1)/2$, y por el Lema 4.2.1,

$$r_{n+1} = \text{mín}\{l \geq 1 \ : \ \text{mcd}(r_n + l, c_n) \neq 1\},$$

donde $\text{mcd}(r_n + l, c_n) = \text{mcd}((c_n + 1 + 2l)/2, c_n) = \text{mcd}(1 + 2l, c_n)$, pues c_n es impar. Por lo tanto, $1 + 2l = \text{mfp}(c_n)$. Entonces $r_{n+1} = r_n + (\text{mfp}(c_n) - 1)/2$ y

$$c_{n+1} = c_n + \text{mcd}\Big(c_n, \frac{c_n + 1}{2} + \frac{\text{mfp}(c_n) - 1}{2}\Big) - 1 = c_n + \text{mfp}(c_n) - 1,$$

de donde se concluye el resultado. □

Proposición 4.3.2. *Suponiendo* (i), (ii) *o* (iii), *la Conjetura 4.1.2 es cierta. Además,* $\{a_k - a_{k-1}\}_{k=1}^{\infty}$ *contiene infinitos primos distintos.*

Demostración. Siempre podemos suponer que (i) es cierta ya que es, en principio, menos general. Por las Proposiciones 4.1.4 y 4.3.1, para $k = r_n$ con $n > n_0$, se tiene

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

De este modo, basta demostrar que el conjunto $\{a_k - a_{k-1}\}_{k=1}^{\infty}$ contiene infinitos primos distintos. Sea P el producto de primos menores que N, con N tal que $P > c_{n_0}$. Sea n el único entero que satisface $c_n < P \leq c_{n+1}$. Si se escribe $c_n = pq$ con $p = \text{mfp}(c_n)$, la Proposición 4.3.1 da $pq < P \leq pq + p - 1$, y por tanto $0 < P - pq < p$. Entonces, como $P - pq$ no puede ser un múltiplo de p, se deduce que p tiene que ser mayor que N.

Por lo tanto, dado N hemos encontrado un n tal que $a_{r_n+1} - a_{r_n} = \text{mfp}(c_n) = p > N$. Cuando N tiende a infinito obtenemos una sucesión no acotada de primos, lo que finaliza la demostración. □

No todas las posibles sucesiones de primos pueden darse. Por ejemplo, es obvio que (4.4) y (4.3) impiden que aparezca el mismo primo en valores consecutivos de $a_k - a_{k-1} \neq 1$. Esto motiva la siguiente definición.

Definition 4.3.1. Decimos que una sucesión finita de k primos impares $C_k = \{p_1, p_2, \ldots, p_k\}$ es una *cadena de Rowland* si existe $c_1^* > 1$ tal que $p_n = \text{mfp}(c_n^*)$ para $1 \leq n \leq k$, donde $c_n^* = c_{n-1}^* + \text{mfp}(c_{n-1}^*) - 1$. Para cada cadena C_k definimos la suma parcial

$$S(n) = \sum_{j<n} (p_j - 1) \qquad \text{y} \qquad S(1) = 0.$$

Lo que sigue, es una caracterización de cadenas de Rowland.

Proposición 4.3.3. *Una sucesión finita de primos impares $C_k = \{p_1, p_2, \ldots, p_k\}$ es una cadena de Rowland si y solo si las siguientes tres condiciones se verifican:*

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

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

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

Por supuesto, en la tercera condición el conjunto es vacío excepto para los q menores que el máximo de C_k y esto también se cumple de forma trivial si $q > k$, por lo que esta caracterización permite verificar si C_k es una cadena de Rowland en un número finito de pasos. Por ejemplo, $\{3, 19, 5, 3\}$ es una cadena de Rowland porque $S(1) = 0$, $S(4) = 24$ 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 $S(3) \pmod 3$, y $S(2) \not\equiv S(3) \pmod 5$, lo que da b). Finalmente c) no necesita verificación debido a que (excluyendo el caso trivial $q = 2$) si el conjunto no es vacío $q \geq 5$, y solo tenemos 4 clases residuales. Por otro lado, $\{17, 5, p\}$ no es una cadena de Rowland para cualquier $p > 3$ pues viola c) para $q = 3$.

Demostración. Nótese que, de acuerdo con la definición de cadena de Rowland, $c_n^* = c_1^* + S(n)$ y C_k es una cadena de Rowland si y solo si existe c_1^* tal que para $1 \leq n \leq k$

$$c_1^* + S(n) \equiv 0 \pmod{p_n} \quad \text{y} \quad c_1^* + S(n) \not\equiv 0 \pmod{q} \qquad \text{para todo} \quad q < p_n. \tag{4.9}$$

Si $p_n = p_m$ entonces $c_1^* + S(n) \equiv c_1^* + S(m) \equiv 0 \pmod{p_n}$ implica a). Por otro lado, el teorema chino del resto asegura que bajo estas condiciones existe una solución del sistema formado por el primer conjunto de ecuaciones de (4.9).

Sea q cualquier primo menor que el máximo de C_k. Entonces, las ecuaciones en (4.9) que involucran a q son

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

y si $q \in C_k$, digamos $q = p_n$, hay que añadir también

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

En el primer caso, existe solución $\bmod q$ si y solo si $S(m)$ no cubre todas las clases residuales. Esto es c). En el segundo caso, también necesitamos $S(m) \not\equiv S(n) \pmod{p_n}$ y esto es b).

Por último, nótese que una vez hemos comprobado que las ecuaciones repetidas son coherentes, el teorema chino del resto se puede usar para encontrar una progresión aritmética de posibles c_1^*. □

Sabemos, gracias a la segunda parte de la Proposición 4.3.2, que la sucesión de primos no puede ser periódica. Pero la situación es aún más restrictiva: no puede repetir bloques.

Corolario 4.3.4. *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 $1 \leq n \leq k$. Entonces, la Proposición 4.3.3 a) implica que este valor es divisible por cada uno de los p_n, y por tanto λ es múltiplo de $p_1 p_2 \ldots p_k$. Pero esto es imposible ya que el producto es mayor que λ. □

En la mayoría de los casos, la Proposición 4.3.3 impone fuertes restricciones a la hora de construir cadenas de Rowland con unos pocos primos distintos dados y k grande. Pero por otro lado, es posible encontrar cadenas largas a partir de elecciones especiales de primos. Por ejemplo, usando los primeros cinco primos impares, no hay cadenas de longitud mayor que 10 pero se tiene

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

de longitud 27 y que sólo involucra a los primos $3, 5, 23, 653$ y 3603833. De hecho, es máximal para este conjunto de números primos (hay otra cadena maximal válida de la misma longitud). Corresponde a tomar $c_1^* = 1550303031682203$.

Capítulo 5

Distribución de potencias de matrices

5.1. Introducción y resultados principales

Un número pseudoaleatorio es un número generado en un proceso que parece producir números aleatorios. Estas sucesiones no muestran un patrón aparente desde el punto de vista estadístico, a pesar de haber sido generadas por un algoritmo completamente determinista (por lo general, un programa de ordenador) el cual tiene por entrada dígitos realmente aleatorios. En las últimas décadas, los generadores lineales recursivos han sido muy usados a la hora de generar números pseudoaleatorios dentro de un determinado rango. Los algoritmos producen una sucesión de números que se asemeja a una muestra de una distribución uniforme $U(0;1)$, aunque realmente no lo sea.

En la práctica, la función $k \mapsto g^k \pmod p$ con g un generador de $\mathbb{F}_p^*$ se emplea como generador de números pseudoaleatorios. En general, la aplicación de generadores lineales recursivos [L'E94] sugiere que se deben buscar matrices en $\mathrm{GL}_n(\mathbb{F}_p)$ con orden maximal y existe algo de literatura acerca de la elección de estas matrices y de las propiedades estadísticas de los generadores correspondientes [EHGL89], [Nie90].

En aplicaciones informáticas, por lo general, hay integrada una función generadora de números pseudoaleatorios cuya salida se reduce modulo m para obtener un número pseudoaleatorio en el rango $[1, m)$.

Estos rangos aparecen muy a menudo en tiempo de ejecución y es imposible elegir de antemano un elemento de orden grande común para todos los módulos correspondientes. Desde un punto de vista matemático, se espera que el uso de $k \mapsto n^k \pmod p$ como generador de números pseudoaleatorios con p en un rango considerablemente grande, proporcione buenos resultados para casi cualquier elección de n. En otras palabras, si $\exp_p(n)$ se define como el orden de n en $\mathbb{F}_p^*$ e igual a 0 si $p \mid n$, entonces es poco probable encontrar un n tal que $\exp_p(n)$ sea pequeño para muchos primos consecutivos. Este hecho fue demostrado por P.X. Gallagher como una aplicación de su criba mayor.

Teorema 5.1.1 ([Gal71, Th.2]). *Dado $\epsilon > 0$, el número de enteros $n \leq N$ para los cuales $\exp_p(n) \leq N^\theta$ para todo primo $p \leq N^{\theta+\epsilon}$ es $O(N^\theta)$, uniformemente para $0 \leq \theta \leq 1$.*

En conexión con este resultado, P.J. Stephens anteriormente había probado que la conjetura de Artin se cumple en promedio, dando una cota no trivial para el número de posibles excepciones [Ste69]. En la práctica no hay diferencia entre elementos de orden maximal y orden grande a la hora de generar números pseudoaleatorios.

Aunque los generadores lineales recursivos se han utilizado desde los años 80, parece que la conjetura de Artin en $\mathrm{GL}_n(\mathbb{F}_p)$ no ha recibido mucha atención hasta hace poco. El caso $n = 2$ parece distinguirse del resto. En [KR01] y [KRR07] (véase también [Kur03]) se muestra la relación existente con la ergodicidad cuántica en toros planos (un ejemplo de caos cuántico aritmético). En [Ros00] se estudia también en conexión con el orden de la reducción de unidades en cuerpos cuadráticos. Por otro lado, nuestro conocimiento acerca de la distribución de matrices de orden máximo en $\mathrm{GL}_2(\mathbb{F}_p)$ se beneficia de la reciente prueba [Cha09] de la desigualdad de Burgess en $\mathbb{F}_{p^2}$ y de un procedimiento conjetural de búsqueda determinista en tiempo polinómico [Sho92] para raíces primitivas en $\mathbb{F}_{p^2}$ (lo que significa que se genera en tiempo polinómico un subconjunto que contiene al menos una raíz primitiva).

Dado $N \in \mathbb{Z}^+$ y un intervalo $I = [1, M]$, consideramos la probabilidad $P_N(x)$ de que un entero positivo $n \leq N$ tenga a lo más exponente x para todo primo en I. Por supuesto, si $x \geq |I|$ se tiene trivialmente $P_N(x) = 1$. Por otro lado, el Teorema 5.1.1 implica que si x es ligeramente más pequeño que $|I|$, entonces esta probabilidad disminuye drásticamente. Digamos entonces que el Teorema 5.1.1 puede ser reformulado como

$$P_N(x) \ll \frac{|I|}{N^{1+\epsilon}} \qquad \text{siempre que} \qquad \frac{x}{|I|} < N^{-\epsilon}.$$

En cierto sentido, $N^{-\epsilon}$ establece un umbral para conseguir $O\big(|I|N^{-1-\epsilon}\big)$ respecto a la cota trivial.

En este capítulo se estudia este fenómeno para matrices enteras no singulares de dimensión 2, mostrando que hay un valor de x muy cercano al tamaño del intervalo tal que son pocas las matrices cuyo orden es menor que x. Además, en la última sección se estudian algunas propiedades de elementos con orden grande.

Extendemos la notación previa escribiendo $\exp_p(A)$ para denotar el orden de la matriz A en $\mathrm{GL}_2(\mathbb{F}_p)$ cuando se reduce módulo p si $p \nmid \det(A)$ y $\exp_p(A) = 0$ si $p \mid \det(A)$.

Permitimos intervalos cortos de primos siempre que tengan densidad positiva y sean lo suficientemente grandes. A saber, consideramos intervalos $I = [a, b]$, $0 < a <$

$b-3$, tales que

$$\sum_{p\in I}\log p \gg |I| \qquad \text{y} \qquad \log|I| \gg \log b \tag{5.1}$$

cuando p recorre los primos. El teorema de los números primos implica que este es el caso para $I=[1,x]$ en una forma asintótica más fuerte que se extiende a $I=[x-x^{\alpha},x]$ para $\alpha>7/12$ usando la hipótesis de densidad que se prueba en [Hux72]. En [BHP01] (véase también [Har07]) se usan métodos de criba para probar (5.1) cuando $\alpha\geq 0.525$. Con los conocimientos actuales se tiene $\log|I|\gg\log b$ en todos los casos en los que la densidad es positiva [Mai85].

El análogo natural del intervalo $[0,N]$ en $\mathrm{SL}_2(\mathbb{Z})$ es el conjunto (de cardinalidad comparable a N^2, ver Lema 5.2.8)

$$\mathcal{I}_N=\big\{A\in\mathrm{SL}_2(\mathbb{Z})\ :\ 0\leq a_{ij}\leq N\big\}.$$

Definimos la probabilidad

$$\mathcal{P}_N(x)=\frac{|\mathcal{M}_N(x)|}{|\mathcal{I}_N|}\quad\text{donde}\quad \mathcal{M}_N(x)=\big\{A\in\mathcal{I}_N\ :\ \exp_p(A)\leq x \text{ para } p\in I\big\},$$

siendo nuestro objetivo encontrar una función umbral $\mathfrak{T}=\mathfrak{T}(N,|I|)$ y una función de ganancia $\mathfrak{G}=\mathfrak{G}(N,|I|)$ tales que

$$\mathcal{P}_N(x)\leq\mathfrak{G} \qquad \text{siempre que} \qquad \frac{x}{|I|}\leq\mathfrak{T}. \tag{5.2}$$

Con la misma idea, también consideramos matrices enteras no singulares arbitrarias. Para ello introducimos

$$\mathcal{I}_N^{*}=\big\{A\in\mathrm{M}_{2\times 2}(\mathbb{Z})\ :\ \det(A)\neq 0,\ 0\leq a_{ij}\leq N\big\},$$

y definimos

$$\mathcal{P}_N^{*}(x)=\frac{|\mathcal{M}_N^{*}(x)|}{|\mathcal{I}_N^{*}|}\ \text{ donde }\ \mathcal{M}_N^{*}(x)=\big\{A\in\mathcal{I}_N^{*}\ :\ 0<\exp_p(A)\leq x \text{ para } p\in I\big\}.$$

Una vez más buscamos una función de umbral $\mathfrak{T}=\mathfrak{T}(N,|I|)$ y una función de ganancia $\mathfrak{G}=\mathfrak{G}(N,|I|)$ tal que

$$\mathcal{P}_N^{*}(x)\leq\mathfrak{G} \qquad \text{siempre que} \qquad \frac{x}{|I|}\leq\mathfrak{T}. \tag{5.3}$$

Nuestros resultados demuestran que un umbral logarítmico es suficiente para conseguir una ganancia sustancial.

Teorema 5.1.2. *Sea I un intervalo que satisface* (5.1) *y $N \geq 3$. Entonces existe una constante absoluta $C > 0$ tal que se cumple* (5.2) *con*

$$\mathfrak{S} = \frac{|I|}{N} \log N (\log\log N)^2 \qquad y \qquad \mathfrak{T} = L\big(\log N \log |I|\big)$$

donde $L(t) = Ct^{-1} \log t$.

Teorema 5.1.3. *Con la notación del Teorema 5.1.2, se cumple* (5.3) *con*

$$\mathfrak{S} = \frac{|I|^2 (\log\log N)^2}{N^3 \log\log |I|} \qquad y \qquad \mathfrak{T} = L\big(\log N \log |I| \log\log |I|\big).$$

El significado de estos resultados se aprecia fácilmente cuando se expresa $|I|$ como una potencia de N.

Corolario 5.1.4. *Si $|I| = N^\delta \geq 3$, entonces el número de matrices en $\mathcal{I}_N$ tales que*

$$\exp_p(A) \leq C N^\delta \frac{\log\log N}{\delta (\log N)^2}$$

para todo $p \in I$ es menor que $N^{\delta+1} \log N (\log\log N)^2$.

Corolario 5.1.5. *Si $|I| = N^\delta \geq 3$, entonces el número de matrices en $\mathcal{I}_N^*$ tales que*

$$0 < \exp_p(A) \leq C N^\delta \frac{\log\log N}{\delta (\log N)^2 \log\log N^\delta}$$

para todo $p \in I$ es menor que $N^{2\delta+1} (\log\log N)^2 \big(\log\log N^\delta\big)^{-1}$.

Estos resultados sugieren que es muy poco probable encontrar una matriz con exponente pequeño para muchos primos por lo que, manteniendo la analogía con el caso entero, tenemos muchas posibles elecciones de buenos generadores de vectores pseudoaleatorios.

5.2. Resultados auxiliares

Dado $m \in \mathbb{Z} - \{0\}$ y un primo impar $p \nmid m$, definimos $f(n)$ como el número de posibles formas canónicas de Jordan distintas (sobre $\mathbb{F}_{p^2}$) de todas las matrices diagonalizables en el conjunto

$$\big\{A \in \mathrm{GL}_2(\mathbb{F}_p) \ : \ \det A = m, \ \exp_p(A) = n\big\}.$$

En adelante, escribimos $e = \exp_p(m)$. Como el determinante es multiplicativo, se tiene de forma trivial que $f(n) = 0$ si $e \nmid n$. El siguiente lema se encarga del resto de casos.

Lema 5.2.1. *Para $e \mid n$ escribimos $k = n/e$. Entonces*

$$f(n) = \begin{cases} \phi(k)e & \text{si } n \mid p-1, \\ \dfrac{\phi(n)}{\phi(e)} & \text{si } n \nmid p-1,\ k \mid p+1 \text{ y } e \text{ o } \frac{p+1}{k} \text{ es impar}, \\ 0 & \text{en otro caso.} \end{cases}$$

Demostración. Si la forma canónica de Jordan es del tipo $\left(\begin{smallmatrix} \alpha & 0 \\ 0 & \beta \end{smallmatrix}\right)$ con $\alpha, \beta \in \mathbb{F}_p^*$, entonces podemos tomar $\beta = m\alpha^{-1}$. Claramente $n = \operatorname{mcm}(\exp_p(\alpha), \exp_p(m\alpha^{-1}))$, y además

$$\exp_p(m\alpha^{-1}) \mid \operatorname{mcm}(e, \exp_p(\alpha^{-1})),$$

lo cual es un hecho general de grupos abelianos, por lo tanto $n = \operatorname{mcm}(e, \exp_p(\alpha))$.

Dado $a \mid p-1$, existen $\phi(a)$ elementos en $\mathbb{F}_p^*$ que tienen orden a, y de entre estos hay $F(n,e)$ que dan lugar a matrices de orden n, donde

$$F(n,e) = \sum_{a\,:\,\operatorname{mcm}(a,e)=n} \phi(a).$$

Es fácil ver que $F(p^{r+s}, p^r) = \phi(p^s)p^r$. Como ϕ es multiplicativo, denotando por e_p y n_p la mayor potencia p que divide a e y n respectivamente, se tiene

$$F(n,e) = \prod_p F(n_p, e_p) = \prod_p \phi\Big(\frac{n_p}{e_p}\Big)e_r = \phi\Big(\frac{n}{e}\Big)e,$$

que da la primera parte del resultado.

Ahora, supongamos que la forma canónica de Jordan es del tipo $\left(\begin{smallmatrix} \alpha & 0 \\ 0 & \beta \end{smallmatrix}\right)$ con $\alpha, \beta \in \mathbb{F}_{p^2} \setminus \mathbb{F}_p$ distintos. El endomorfismo de Frobenius genera el grupo de Galois asociado, por lo que $\beta = \alpha^p$. Como m está fijado, podemos elegir un generador $g \in \mathbb{F}_{p^2}^*$ tal que $m = g^{\frac{p^2-1}{e}}$. Por lo tanto, buscamos elementos en $\mathbb{F}_{p^2}$ de la forma $g^{\frac{p^2-1}{n}r}$ con $0 \le r \le n$, $\operatorname{mcd}(r,n) = 1$, que no pertenecen $\mathbb{F}_p$ y que satisfacen $\big(g^{\frac{p^2-1}{n}r}\big)^{p+1} = g^{\frac{p^2-1}{e}}$. La primera condición es equivalente a que $n \nmid p-1$, y la segunda nos lleva a calcular

$$\#\Big\{0 \le r \le ke \ :\ \operatorname{mcd}(r, ke) = 1,\ \frac{p+1}{k}r \equiv 1 \pmod{e}\Big\}. \tag{5.4}$$

Por supuesto, necesariamente $\big(\frac{p+1}{k}, e\big) = 1$, y notando que $\operatorname{mcd}(p+1, p-1) = 2$, esto es equivalente a decir que $\frac{p+1}{k}$ o bien e es impar. Para $\operatorname{mcd}(a,n) = 1$, sea

$$S(a) = \big\{0 \le r \le ke \ :\ \operatorname{mcd}(r,k) = 1 \text{ y } r \equiv a \pmod{e}\big\}.$$

Claramente $|S(a)|$ no depende de la elección a. Sea $\{a = a_1, \ldots, a_{\phi(e)}\}$ un conjunto completo de representantes de $(\mathbb{Z}/e\mathbb{Z})^*$ con $\operatorname{mcd}(a_i, k) = 1$. Entonces (5.4) coincide

con

$$\frac{1}{\phi(e)}\sum_{i=1}^{\phi(e)}|S(a_i)| = \frac{1}{\phi(e)}\#\big\{0 \le r \le ke \ : \ \mathrm{mcd}(r,k)=1,\ (r,e)=1\big\} = \frac{\phi(n)}{\phi(e)},$$

lo que completa la demostración. □

Definimos $g(n)$ como $f(n)$ pero ahora considerando matrices no diagonalizables en el mismo conjunto. De nuevo $g(n)=0$ si $e \nmid n$. Por otro lado, la no anulación de g requiere que m sea residuo cuadrático o, de forma equivalente, $(p-1)/e$ debe ser par porque el polinomio característico tiene una raíz doble. Se tiene

Lema 5.2.2. *Sea $(p-1)/e$ par, entonces*

$$g(n) = \begin{cases} \frac{1-(-1)^e}{2} & \text{si } \ n = ep, \\ \frac{3+(-1)^e}{2} & \text{si } \ n = 2ep, \\ 0 & \text{en otro caso.} \end{cases}$$

Demostración. Dado que la matriz no es diagonalizable, debe ser semejante a una de la forma $\left(\begin{smallmatrix}\alpha & 1\\ 0 & \alpha\end{smallmatrix}\right)$ con $\alpha \in \mathbb{F}_p^*$.

Sea g un generador de $\mathbb{F}_p^*$ tal que $m = g^{\frac{p-1}{e}}$. Como $\alpha^2 = m$, claramente $2 \mid \frac{p-1}{e}$, y por tanto $\alpha = g^{\frac{p-1}{2e}}$ o $g^{\frac{p-1}{2e}+\frac{p-1}{2}}$. En el primer caso, el orden de α es $2e$ y por tanto, el orden de la matriz es $2ep$, mientras que en el segundo caso, el orden de α es $2e$ o e, dependiendo de si e es par o no, en cuyo caso el orden de la matriz es $2ep$ o ep, respectivamente. □

Lema 5.2.3. *Sea p un primo impar, $p \nmid m$ y $x > 0$. Sea*

$$S_{m,p}(x) = \big\{\mathrm{tr}(A) \ : \ A \in \mathrm{GL}_2(\mathbb{F}_p) \text{ con } \det A = m,\ \exp_p(A) \le x\big\},$$

entonces

$$|S_{m,p}(x)| = \frac{1}{2}\sum_{\substack{k\le x/e \\ k\mid(p-1)/e}} \phi(k)e + \frac{1}{2}\sum_{\substack{k\le x/e \\ k\mid p+1}} \frac{\phi(ke)}{\phi(e)} + O(1).$$

Demostración. Primero, nótese que la parte que procede de matrices con un autovalor doble contribuye $O(1)$.

Para el resto de casos aplicamos el Lema 5.2.1, notando que al intercambiar los autovalores, dos formas canónicas de Jordan corresponden a una misma clase de matrices bajo la relación de semejanza y por tanto a un valor de traza. □

Lema 5.2.4. *Para p primo impar, $p \nmid m$ y $x > 0$ tenemos*

$$|S_{m,p}(x)| \ll \varepsilon_m(p) \sum_{\substack{n \le x \\ n \mid p-1}} \phi(n) + \sum_{\substack{n \le x \\ n \mid p+1}} \phi(n),$$

donde

$$\varepsilon_m(x) = \begin{cases} 1 & \text{si } m = \pm 1, \\ \log\log x & \text{en otro caso.} \end{cases}$$

Demostración. El resultado es consecuencia del lema previo. El caso $m = \pm 1$ es trivial. Si $m > 1$, usando la definición de ϕ y [HW08, Theorem 328] se tiene

$$\phi(\frac{n}{e})e \le \phi(n)\frac{e}{\phi(e)} \ll \phi(n)\log\log p.$$

Para la segunda suma, nótese que $\mathrm{mcd}(k, e) \mid 2$ porque $k \mid p + 1$, y por tanto

$$\frac{\phi(ke)}{\phi(e)} \le 2\phi(k)$$

con lo que se llega al resultado fácilmente. □

Para el siguiente lema necesitamos la desigualdad de criba mayor de Gallagher [Gal71].

Teorema 5.2.5 ([Gal71, Th.1]). *Si todas excepto $g(p)$ clases residuales* (mód p) *se eliminan para cada primo p en el conjunto finito $\mathcal{S}$, entonces el número de enteros que permanecen en cualquier intervalo de longitud N es como mucho*

$$\Big(\sum_{p \in \mathcal{S}} \log p - \log N\Big) \Big/ \Big(\sum_{p \in \mathcal{S}} \frac{\log p}{g(p)} - \log N\Big)$$

siempre que el denominado sea positivo.

Lema 5.2.6. *Sea*

$$\mathcal{T}_m(x) = \big\{1 \le t \le 2N \ : \ t \in S_{m,p}(x) \text{ para todo } p \in I\big\},$$

con $S_{m,p}$ definido como en el Lema 5.2.3. Entonces, para $x = |I|M^{-1}\log M$ donde $M > C'\epsilon_m(|I|)\log|I|\log N$ y C' es una constante, se tiene

$$|\mathcal{T}_m(x)| \ll \epsilon_m(|I|)M^{-1}|I|\log|I|.$$

Demostración. La prueba es similar a la del Teorema 5.1.1 (véase [Gal71]). Por la desigualdad de Cauchy-Schwarz se tiene

$$\Big(\sum_{p\in I}\frac{\log p}{|S_{m,p}(x)|}\Big)\Big(\sum_{p\in I}|S_{m,p}(x)|\log p\Big)\geq\Big(\sum_{p\in I}\log p\Big)^2\gg|I|^2.$$

Por otro lado, el teorema de Brun-Titchmarsh [MV73] da la cota

$$\pi(y_0+y_1;q,c)-\pi(y_0;q,c)<\frac{2y_1}{\phi(q)\log(y_1/q)},\quad 1\leq q<y_1$$

que, junto con el Lema 5.2.4, nos permite escribir

$$\begin{aligned}\sum_{p\in I}|S_{m,p}(x)|\log p&\ll\sum_{p\in I}\Big(\varepsilon_m(p)\sum_{\substack{n\leq x\\ n|p-1}}\phi(n)+\sum_{\substack{n\leq x\\ n|p+1}}\phi(n)\Big)\log p\\&\ll|I|\log|I|\varepsilon_m(|I|)\sum_{n\leq x}\Big(\log\frac{|I|}{n}\Big)^{-1}\\&\ll\epsilon_m(|I|)M^{-1}|I|^2\log|I|.\end{aligned}$$

Por lo tanto, se deduce que

$$\sum_{p\in I}\frac{\log p}{|S_{m,p}(x)|}\gg\frac{M}{\epsilon_m(|I|)\log|I|}.$$

Ahora, por el Teorema 5.2.5 se tiene

$$|\mathcal{T}_m(x)|\ll\Big(\sum_{p\in I}\log p\Big)/\Big(\sum_{p\in I}\frac{\log p}{|S_{m,p}(x)|}\Big)\ll\epsilon_m(|I|)M^{-1}|I|\log|I|.$$

Nótese que el tamaño de M asegura que el denominador en el enunciado del Teorema 5.2.5 es positivo y, de hecho, para una constante adecuada C', es mayor que $c\log N$ con $c>0$. □

Lema 5.2.7. *Sea*

$$\mathcal{A}_m=\sup_t\#\big\{A\in\mathcal{I}_N^*\ :\ \det A=m,\ \operatorname{tr}(A)=t\big\},$$

entonces

$$\mathcal{A}_m\ll N(\log N)^2(\log\log N)^2\quad\textit{para todo } m.$$

Demostración. El problema se reduce a contar el número de soluciones de

$$\begin{cases} 0 \leq a_{11}, a_{12}, a_{21}, a_{22} \leq N \\ a_{11} + a_{22} = t \\ a_{11}a_{22} - a_{12}a_{21} = m \end{cases}$$

Escribiendo $h(n) = n(t-n) - m$, tenemos que $h(a_{11}) = a_{12}a_{21}$, entonces el número de soluciones está acotado por

$$\sum_{n \leq N} \sum_{k \mid h(n)} 1 = \sum_{k \leq N} \sum_{\substack{n \leq N \\ h(n) \equiv 0 \ (k)}} 1 \ll \sum_{k \leq N} \rho(k) \frac{N}{k}$$

donde $\rho(k)$ representa el número de soluciones de $h(n) \equiv 0$ (mód k). Como ρ es multiplicativa, se tiene

$$\sum_{k \leq N} \frac{\rho(k)}{k} \leq \prod_{p \leq N} \Big(1 + \frac{\rho(p)}{p} + \frac{\rho(p^2)}{p^2} + \dots\Big).$$

Ahora conviene separar el producto en dos partes. En la primera, se consideran los primos tales que $\rho(p) = 0, 2$ y, por [Mol10, Lemma 6.1], verifican $\rho(p^k) \leq 2$. En la segunda parte, consideramos aquellos primos que cumplen $\rho(p) = 1$, o equivalentemente $p \mid \Delta = t^2 - 4m$, en este caso [Mol10, Lemma6.1] asegura que $\rho(p^k) \leq p^{[k/2]}$ para $k \geq 1$. Por lo tanto, el producto está acotado por

$$\begin{aligned} &\prod_{\substack{p \leq N \\ \rho(p) = 0,2}} \Big(1 + \frac{2}{p} + \frac{2}{p^2} + \dots\Big) \prod_{\substack{p \leq N \\ p \mid \Delta}} \Big(1 + \frac{1}{p} + \frac{p}{p^2} + \dots\Big) \\ &\qquad \ll \prod_{p \leq N} \Big(1 + \frac{2}{p}\Big) \prod_{\substack{p \leq N \\ p \mid \Delta}} \Big(1 + \frac{2}{p}\Big) \ll (\log N)^2 \prod_{\substack{p \leq N \\ p \mid \Delta}} \Big(1 + \frac{2}{p}\Big). \end{aligned}$$

Usando [HW08, Theorem 323], el último producto es menor que $(\log\log N)^2$, por tanto

$$\mathcal{A}_m \ll N(\log N)^2(\log\log N)^2$$

llegando así al resultado deseado. □

Lema 5.2.8. *Se tiene*

$$|\mathcal{I}_N| = \frac{12}{\pi^2} N^2 + O\big(N(\log N)^2\big) \quad y \quad |\mathcal{J}_N| = (N+1)^4 + O\big(N^2(\log N)^3\big).$$

Demostración. Sea N_{cd} el número de matrices en $\mathcal{I}_N$ que tienen (c,d) como fila inferior. Por supuesto c y d deben ser coprimos y es fácil probar que

$$|\mathcal{I}_N| = \sum_{d<c\le N} N_{cd} + \sum_{c<d\le N} N_{cd} + O(N)$$

donde la suma se restringe a valores positivos.

Si $0 < d < c \le N$ entonces las posibles filas superiores de una matriz en N_{cd} son $(x_0 + ct, y_0 + dt)$ con $0 \le t \le (N - x_0)/c$ donde $x_0 d - y_0 c = 1$ y $x_0 = \overline{d}$, definidas como la solución de $dx \equiv 1 \pmod{c}$ con $0 \le x < c$.

El caso $0 < c < d \le N$ es muy similar pero ahora $0 \le t \le (N - y_0)/c$ y $y_0 = d - \overline{c}$ que es solución de $cx \equiv -1 \pmod{d}$ con $0 \le x < d$.

Entonces

$$|\mathcal{I}_N| = \sum_{\substack{d<c\le N\\ \mathrm{mcd}(c,d)=1}} \Big(\big[\frac{N-\overline{d}}{c}\big] + 1 \Big) + \sum_{\substack{c<d\le N\\ \mathrm{mcd}(c,d)=1}} \Big(\big[\frac{N-c+\overline{d}}{c}\big] + 1 \Big) + O(N)$$

donde $[\,\cdot\,]$ denota la parte entera. Intercambiando c y d en la última suma e introduciendo la función $\psi(x) = x - [x] - 1/2$, podemos escribir la fórmula anterior como

$$|\mathcal{I}_N| = \sum_{\substack{d<c\le N\\ \mathrm{mcd}(c,d)=1}} \frac{2N}{c} - \sum_{\substack{d<c\le N\\ \mathrm{mcd}(c,d)=1}} \Big(\psi\big(\frac{N-\overline{d}}{c}\big) + \psi\big(\frac{N+\overline{d}}{c}\big) \Big) + O(N). \tag{5.5}$$

La primera suma da el término principal junto con un término de error admisible sumando por partes en $\sum_{n\le x} \phi(n) = 3x^2/\pi^2 + O(x \log x)$, que es bien conocida [HW08, Th.330]. Queda por demostrar que la segunda suma es $O\big(N(\log N)^2\big)$.

Dado un entero positivo M [Mon94], existen números reales $a_m^{\pm} \ll m^{-1}$ y $a_0^{\pm} \ll M^{-1}$ tales que

$$\sum_{|m|\le M} a_m^- e(mx) \le \psi(x) \le \sum_{|m|\le M} a_m^+ e(mx) \qquad \text{con} \quad e(t) = e^{2\pi i t}.$$

Usando la evaluación de las sumas de Ramanujan y $\phi(ab) \le a\phi(b)$,

$$\Big| \sum_{\substack{d=1\\ \gcd(c,d)=1}}^{c} e\big(m\frac{\overline{d}}{c}\big) \Big| \le \mathrm{mcd}(c,m).$$

Por lo tanto, la segunda suma en (5.5) está acotada por

$$\frac{N^2}{M} + \sum_{c\le N} \sum_{m\le M} \frac{\mathrm{mcd}(c,m)}{m} \le \frac{N^2}{M} + \sum_{d\le M} d \sum_{d|c\le N} \sum_{d|m\le M} \frac{1}{m}.$$

Eligiendo $M = N(\log N)^{-2}$ se consigue el resultado.

La segunda fórmula del enunciado se reduce a demostrar que el número de matrices singulares con elementos $0 \le a, b, c, d \le N$ es $O\big(N^2(\log N)^3\big)$. Es fácil ver que solo hay $O\big(N^2\big)$ de ellas con $abcd = 0$, entonces podemos suponer $a, b, c, d > 0$. Estas matrices singulares están claramente contadas en exceso por

$$\sum_{a\le N}\sum_{d\le N}\sum_{b\mid ad} 1 \le \sum_{m\le N^2}\sum_{d\mid m}\sum_{b\mid m} 1 = \sum_{m\le N^2} \tau^2(m)$$

donde $\tau(m)$ es la función divisor. Usando argumentos elementales [Dav80, p.140] se deduce que la última suma tiene el orden de magnitud esperado. □

5.3. Prueba de los resultados principales

Demostración del Teorema 5.1.2. Recordemos que habíamos definido

$$\mathcal{M}_N(x) = \big\{A \in \mathcal{I}_N \ : \ \exp_p(A) \le x \text{ para todo } p \in I\big\}.$$

Claramente, con la misma notación que en el Lema 5.2.6, se tiene

$$|\mathcal{M}_N(x)| \le \sum_{t\in\mathcal{T}_1(x)} \big|\big\{A \in \mathcal{I}_N \ : \ \mathrm{tr}(A) = t\big\}\big|.$$

Por lo tanto $|\mathcal{M}_N(x)| \le |\mathcal{T}_1(x)|\mathcal{A}_1$, con $\mathcal{A}_1$ como en el Lema 5.2.7, y las cotas dadas en los Lemas 5.2.6, 5.2.7 y 5.2.8 dan, tomando M comparable a $\log N \log|I|$,

$$\mathcal{P}_N(x) \ll C\mathfrak{S} \qquad \text{para } x = |I|\mathfrak{T}.$$

Eligiendo C lo suficientemente pequeño obtenemos el resultado. □

Demostración del Teorema 5.1.3. En este caso, nos interesa en el conjunto

$$\mathcal{M}_N^*(x) = \big\{A \in \mathcal{I}_N^* \ : \ 0 < \exp_p(A) \le x \text{ para todo } p \in I\big\}.$$

Como el determinante es multiplicativo, si $A \in \mathrm{GL}_2(\mathbb{F}_p)$ tiene orden n, entonces el orden de $\det A$, visto como elemento de $\mathbb{F}_p$, divide a n. Por lo tanto

$$|\mathcal{M}_N^*(x)| \le \sum_{m\in\mathcal{Z}} \big|\big\{A \in \mathcal{I}_N^* : \ \det A = m, \ 0 < \exp_p(A) \le x \text{ para todo } p \in I\big\}\big|$$

donde $\mathcal{Z} = \{1 \le m \le N^2 \ : \ 0 < \exp_p(m) \le x \text{ para todo } p \in I\}$.

El número de elementos de orden menor o igual que x en $\mathbb{F}_p^*$ es $\sum \phi(n)$ donde la suma recorre los $n \le x$ con $n \mid p-1$, que está mayorado por $2|S_{1,p}(x)|$. Entonces,

procediendo como en el Lema 5.2.6 conseguimos una cota para $|\mathcal{Z}|$ similar a la de $|\mathcal{T}_1(x)|$,

$$|\mathcal{Z}| \ll M^{-1}|I|\log|I| \ll \frac{C|I|}{\log N \log\log|I|}$$

con M comparable a $C^{-1}\log N\log|I|\log\log|I|$ que corresponde a $x = |I|\mathfrak{T}$.

Escribiendo

$$\left|\left\{A \in \mathcal{I}_N^* \ : \ \det A = m,\ 0 < \exp_p(A) \le x \text{ para todo } p \in I\right\}\right| \le \sum_{t\in\mathcal{T}_m(x)} \mathcal{A}_m,$$

junto con los Lemas 5.2.6, 5.2.7 y 5.2.8 (véase la demostración del Teorema 5.1.2) se concluye

$$\mathcal{P}_N^*(x) \ll C\mathfrak{S}$$

y de nuevo, basta elegir C suficientemente pequeño. □

5.4. Otras cuestiones acerca de la distribución

Nuestro interés en esta sección consiste en saber si siempre podemos conseguir matrices de orden grande con pequeñas perturbaciones. Para ello, podemos limitarnos al estudio de las trazas y luego traducir los resultados a las matrices a través del siguiente lema.

Lema 5.4.1. *Sea A un elemento de $\mathrm{SL}_2(\mathbb{Z})$. Fijado un generador g de $\mathbb{F}_p^*$ y q un factor primo de $p-1$, se tiene que $\exp_p(A) = q$ si y solo si*

$$\mathrm{tr}(A) = g^{k(p-1)/q} + g^{-k(p-1)/q}$$

para algún $1 \le k < q$.

Demostración. La condición impuesta en el orden de la matriz fuerza a que la forma canónica de Jordan sea diagonal con entradas $\alpha, \alpha^{-1} \in \mathbb{F}_p$. El resultado se prueba escribiendo $\alpha = g^{k(p-1)/q}$ pues $\exp_p(A) = q$. □

Identificando matrices con la misma traza y tomando la distancia (entre clases) como la distancia entre trazas, obtenemos resultados sobre un tipo de discrepancia de matrices.

Teorema 5.4.2. *Sea J un intervalo de longitud mayor que $6p^{3/2}(q-1)^{-1}\log p$, donde q es un primo divisor de $p-1$, entonces existe una matriz $A \in \mathrm{SL}_2(\mathbb{F}_p)$ tal que $\mathrm{tr}(A) \in J$ y $\exp_p(A) = q$.*

R.C. Baker y G. Harman probaron en [BH98] que para infinitos primos p el mayor factor de $p-1$ es mayor que $p^{0.677}$. De hecho, en realidad se prueba para una proporción positiva de primos (véase [Har07, §8.1], especialmente (8.1.7) y las fórmulas cercanas). Usando este resultado, se obtiene el siguiente corolario:

Corolario 5.4.3. *Existen constantes positivas C_1 y C_2 tales que para al menos $C_1 N/\log N$ primos p en el rango $[N, 2N]$, cualquier intervalo de longitud mayor que $C_2 N^{0.823}\log N$ contiene matrices con $\exp_p(A) > N^{0.677}$.*

Ahora, cambiamos nuestro punto de vista. Fijada una matriz de orden grande, pasamos a estudiar la distribución de sus potencias. Nótese que el orden máximo de una matriz diagonalizable en $\mathrm{SL}_2(\mathbb{F}_p)$ es $p-1$, por lo que esperamos que una matriz de este orden sea un buen generador de vectores pseudoaleatorios. El siguiente resultado muestra que las potencias de estas matrices están bien distribuidas.

Teorema 5.4.4. *Sea $A \in \mathrm{SL}_2(\mathbb{Z})$ tal que $\exp_p(A) = p-1$. Entonces*

$$\#\big\{A^k,\ 1 \le k \le N\ :\ \mathrm{tr}(A^k) \in J\big\} = \frac{N|J|}{p} + O\big(p^{1/2}(\log p)^2\big),$$

donde J es un intervalo contenido en $[1,p]$ y $N < p$.

Para cada par de enteros m y n, con $p \nmid m$, definimos la siguiente suma trigonométrica

$$S(N) = \sum_{k=1}^{N} e\Big(\frac{m}{p}(g^k + g^{-k})\Big) e\Big(\frac{nk}{p-1}\Big) \qquad \text{donde} \qquad e(t) = e^{2\pi i t}.$$

Para demostrar los teoremas anteriores, estableceremos primero dos lemas.

Lema 5.4.5. *Se tiene*

$$\text{a)}\ \ |S(p-1)| \le 2p^{1/2} \qquad y \qquad \text{b)}\ \ |S(N)| \le 7p^{1/2}\log p$$

donde $p \nmid m$ y $N < p$.

Demostración. En el primer caso, tras el cambio de variable $x = g^k$ obtenemos

$$S(p-1) = \sum_{x=1}^{p-1} e\Big(\frac{m}{p}(x + \overline{x})\Big)\chi(x)$$

donde χ es cierto carácter de Dirichlet, y $\overline{x}$ denota el inverso de x modulo p. Ahora, el resultado se sigue de la cota de Weil [Li96, Th.10]. Para probar la cota b), empleamos la técnica de completación [IK04]. Sea $\widetilde{S}$ dado por

$$\widetilde{S}\Big(\frac{a}{p}\Big) = \sum_{0<k\le p-1} e\Big(\frac{(m-a)g^k + mg^{-k}}{p}\Big) e\Big(\frac{nk}{p-1}\Big),$$

entonces

$$S(N) = \frac{1}{p} \sum_{a \,(\text{mód } p)} \lambda\Big(\frac{a}{p}\Big) \widetilde{S}\Big(\frac{a}{p}\Big)$$

donde

$$\lambda\Big(\frac{a}{p}\Big) = \sum_{0<y\le N} e\Big(\frac{ay}{p}\Big).$$

Por un lado $\lambda(0) = N$, mientras que por otro, si $0 < |a| \le p/2$, se tiene que $|\lambda(a/p)| \le p|a|^{-1}$. Por lo tanto, usando estas observaciones y la cota a), se concluye

$$|S(N)| \le \frac{N}{p}|\widetilde{S}(0)| + \sum_{0<|a|\le p/2} |a|^{-1}\big|\widetilde{S}\Big(\frac{a}{p}\Big)\big| \le 2p^{1/2} + 4p^{1/2}(1+\log(p/2)) \le 7p^{1/2}\log p.$$

□

Lema 5.4.6. *Escribamos $S(m,n;N)$ en lugar de $S(N)$ para enfatizar la dependencia en los parámetros. Entonces*

$$\sum_{k=1}^{q} e\Big(\frac{m}{p}(g^{k(p-1)/q} + g^{-k(p-1)/q})\Big) = \frac{q}{p-1} \sum_{h=1}^{(p-1)/q} S(m, hq; p-1).$$

Demostración. Por la definición de $S(N)$, la suma de la derecha es

$$\sum_{s=1}^{p-1} e\Big(\frac{m}{p}(g^s + g^{-s})\Big) \sum_{h=1}^{(p-1)/q} e\Big(\frac{hqs}{p-1}\Big)$$

donde la suma interna es igual a $(p-1)/q$ si $(p-1)/q$ divide a s y cero en otro caso. Basta entonces hacer un cambio de variable $s \to k\frac{p-1}{q}$ para llegar al resultado. □

Demostración del Teorema 5.4.2. Podemos asumir que $q - 1 > ep^{1/2}\log p$ pues en otro caso el resultado es trivial.

Sea g un generador de $\mathbb{F}_p^*$. Consideremos $\alpha = g^{(p-1)/q}$ y sean $t_k = (\alpha^k + \alpha^{-k})p^{-1}$ las trazas normalizadas módulo p en $[0,1]$. Entonces

$$\#\big\{k \le q-1 \,:\, t_k \in [a,b]\big\} \ge (b-a)(q-1) - D(q-1)(q-1),$$

donde

$$D(N) = \sup_{0\le a<b\le 1} \Big|\frac{\#\{k \le N \,:\, a \le t_k \le b\}}{N} - (b-a)\Big|$$

es la discrepancia de la sucesión $\{t_k\}$. Por un lado, los Lemas 5.4.6 y 5.4.5 conducen a

$$\Big|\sum_{k=1}^{q-1} e(mt_k)\Big| \le \frac{q}{p-1}\sum_{h=1}^{(p-1)/q} |S(m,hq;p-1)| \le 2p^{1/2}.$$

Por otro lado, la desigualdad de Erdős-Turán [Mon94, Corollary 1.1] implica

$$\begin{aligned} D(q-1) &\le \frac{1}{M+1} + \frac{3}{q-1}\sum_{m=1}^{M}\frac{1}{m}\Big|\sum_{k=1}^{q-1} e(mt_k)\Big| \\ &\le \frac{1}{M+1} + \frac{6p^{1/2}}{q-1}\big(1+\log(M+1)\big), \end{aligned}$$

y eligiendo M como la parte entera de $(q-1)/ep^{1/2}\log p$, se tiene $(q-1)D(q-1) \le 6p^{1/2}\log p$ pues $1/(M+1) \le ep^{1/2}\log p/(q-1)$ y (recordando que $p > 211$)

$$\log(M+1) \le \log\big(\frac{p-1}{ep^{1/2}\log p}+1\big) \le \log\frac{p^{1/2}}{e} = -1+\frac{1}{2}\log p.$$

Se concluye entonces que el intervalo $J = J(p,q)$ satisface

$$|J| > 6p^{3/2}(q-1)^{-1}\log p.$$

□

Demostración del Teorema 5.4.4. En este caso, la matriz es semejante a una de la forma $\left(\begin{smallmatrix} g & 0 \\ 0 & g^{-1}\end{smallmatrix}\right)$ con g un generador de $\mathbb{F}_p^*$, por lo que $\operatorname{tr}(A^k) = g^k + g^{-k}$.

Sean $t_k = (g^k+g^{-k})p^{-1}$ las trazas normalizadas módulo p en $[0,1]$. Por el Lema 5.4.5,

$$\Big|\sum_{k=1}^{N} e\Big(\frac{m}{p}(g^k+g^{-k})\Big)\Big| \le 7p^{1/2}\log p,$$

y usando de nuevo la desigualdad de Erdős-Turán obtenemos

$$D(N) \le \frac{1}{M+1} + \frac{21p^{1/2}\log p}{N}\big(1+\log(M+1)\big).$$

Tomando

$$M = \left\lceil \frac{N}{p^{1/2}(\log p)^2} \right\rceil$$

donde $\lceil x \rceil$ denota el menor entero no inferior a x, se tiene $D(N) \ll N^{-1}p^{1/2}(\log p)^2$ y el resultado se deriva de la definición de discrepancia [KN74]. □

Parte III

Métodos analíticos

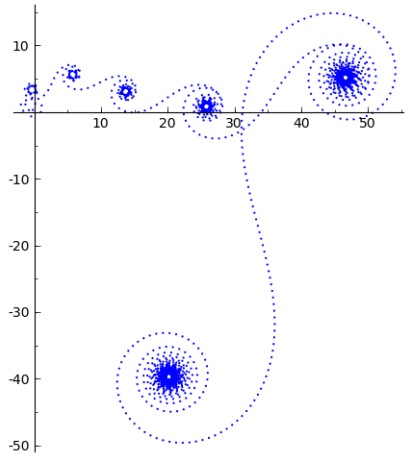
Capítulo 6

El método de van der Corput e ilusiones ópticas

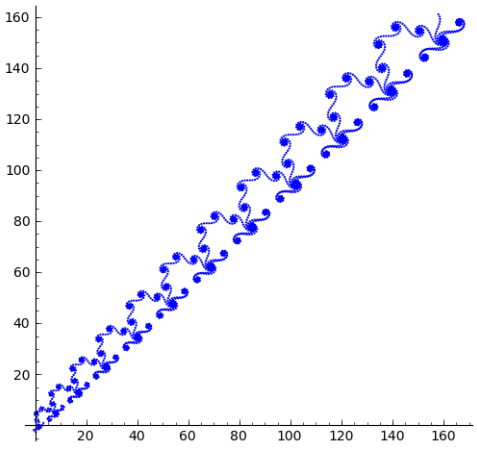
6.1. Introducción

Algunos autores han señalado la naturaleza fractal o simplemente el aspecto estéticamente atractivo de las sumas parciales de algunas sumas trigonométricas simples [DMF81], [Leh76], [Lox83], [Des85], [Mon94], [EMY03], [TMF00, §3] (véase también el reciente trabajo [DGL13] para otro tipo de imágenes, pero aún más impresionantes).

Por mencionar un par de ejemplos que han aparecido en la literatura, consideramos los siguientes dibujos de 5000 puntos a partir de sumas parciales.



$\sum_{n\leq N} e\big((\log n)^4\big)$



$\sum_{n\leq N} e\big(n^{3/2}\big)$

La explicación de estos y otros ejemplos se encuentra en el método de van der Corput [GK91] y parece ser menos conocido fuera del contexto de la teoría analítica

de números, tal vez debido a su naturaleza aritmética. Por ejemplo, en la primera figura, apodada como el monstruo del Lago Ness en [Lox83], vemos 6 concentraciones de puntos porque la derivada de $(\log n)^4$ toma 6 valores semienteros en su rango y en el segundo ejemplo las concentraciones tienen que ver con los residuos cúbicos módulo 27 [Mon94].

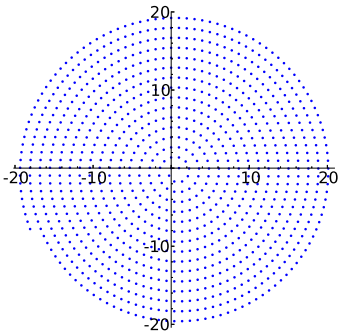
Nosotros consideramos la suma trigonométrica

$$S(N;\alpha) = \sum_{n=1}^{N} e(\alpha\sqrt{n}) \qquad \text{con } \alpha > 0 \text{ fijado.}$$

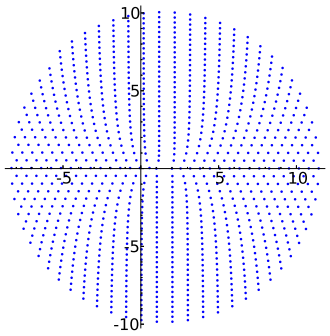
La derivada de $\alpha\sqrt{x}$ decrece a 0 (como en el primer ejemplo). De hecho, para α razonablemente pequeño, después de algunos términos esta derivada es menor que uno, y según las ideas subyacentes del método de van der Corput [GK91] se espera una buena aproximación mediante

$$\int_1^N e\big(\alpha\sqrt{x}\big)\, dx = \frac{\sqrt{N}}{\pi\alpha} e\big(\alpha\sqrt{N} - 1/4\big) + O(1). \tag{6.1}$$

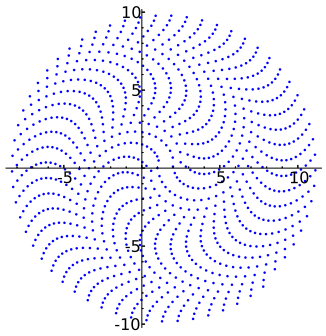
Esto sugiere que al tener en cuenta únicamente el término principal, la sucesión finita $\{S(n;\alpha)\}_{n=1}^{N}$ se debería parecer a una espiral de Arquímedes $\frac{1}{2}(\pi\alpha)^{-2}t(\operatorname{sen} t, -\cos t)$ con $t \in [1, 2\pi\alpha\sqrt{N}]$. La sorpresa es que en los dibujos muy rara vez se observa la estructura de espiral. Por ejemplo, para $N = 1000$ se obtienen las siguientes figuras para los valores indicados de α



$\alpha = 1/2$

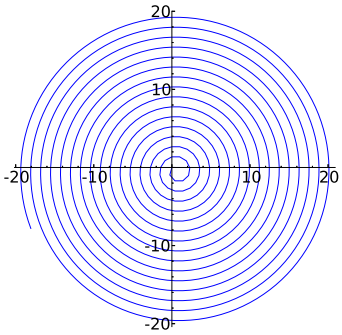


$\alpha = 1$

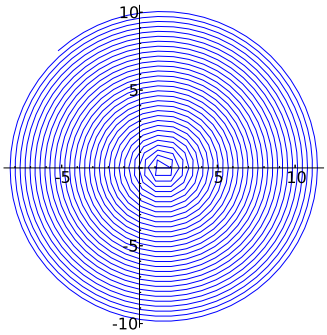


$\alpha = 65/64$

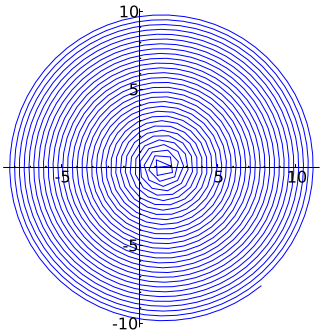
Esto es en cierto sentido una ilusión óptica, puesto que si conectamos puntos consecutivos de la sucesión con líneas (como se hace en los anteriormente mencionados [DMF81], [Leh76], [Lox83], [Des85], [Mon94], [EMY03] y [TMF00, §3]) las espirales de Arquímedes reaparecen y, como predice (6.1), un valor mayor de α da una menor distancia entre giros sucesivos.



$\alpha = 1/2$



$\alpha = 1$



$\alpha = 65/64$

En este capítulo se estudian los patrones que aparecen al dibujar $\{S(n;\alpha)\}_{n=1}^{N}$ para algunos valores de α. Una primera observación es que las espirales de Arquímedes exactas dadas por el término principal de (6.1) son visualmente indistinguibles en la forma de estos dibujos cuando N crece (salvo por una traslación). Esto no es evidente porque el término de error en (6.1) es comparable a la separación entre los puntos. Abordamos este problema en §2. Con una buena aproximación explícita a nuestra disposición, las sumas trigonométricas no juegan ningún papel. La ilusión óptica se produce porque nuestra vista tiende a conectar puntos cercanos. En §3 establecemos una relación de recurrencia de naturaleza aritmética para puntos cercanos. La iteración de esta recurrencia da cada "rama" del patrón. Por último, en §4 se muestra cómo la recurrencia puede ser resuelta para algunos valores de α, dando una explicación completa del patrón.

6.2. Aproximación de la suma trigonométrica

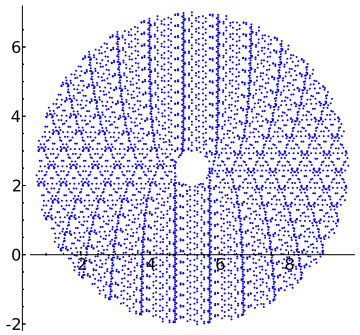
Si nos olvidamos por un momento de los patrones y consideramos las sumas parciales como una nube de puntos, se pueden dar algunas observaciones geométricas que no se pueden explicar con la aproximación (6.1). Estas se vuelven evidentes cuando α no es muy pequeño (por ejemplo, mayor que 3)

1. Existen algunos puntos aleatorios iniciales y concentraciones de puntos antes de entrar en una estructura circular creciente.

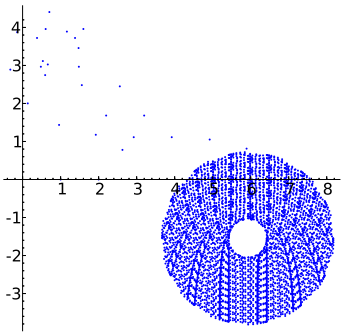
2. Esta estructura circular tiene un agujero en el centro de radio $1/2$

3. El centro de la figura y la distancia al origen es comparable a α.

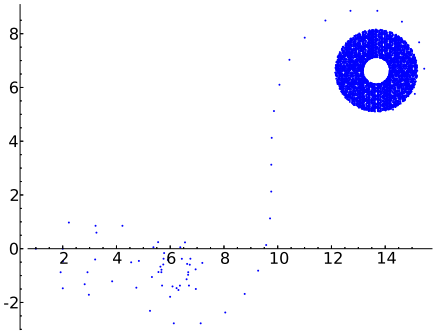
Las siguientes figuras corresponden a 10^4 puntos con los valores indicados de α. La última imagen se corresponde con un primer plano de la concentración de puntos inferior de la figura anterior para valores grandes de N.



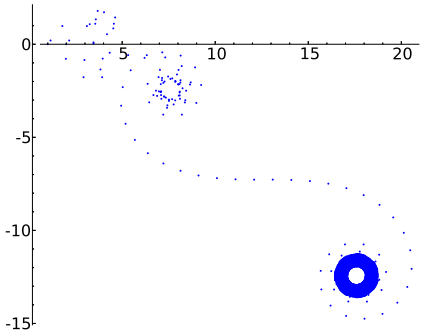
$\alpha = 5$



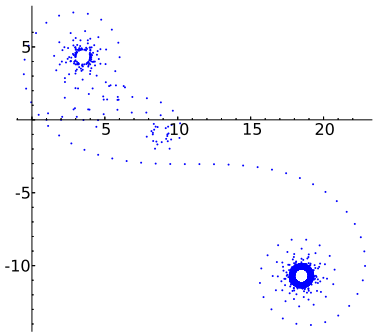
$\alpha = 10$



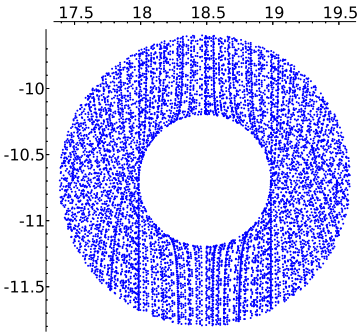
$\alpha = 15$



$\alpha = 20$



$\alpha = 30$



$\alpha = 30$ (close up)

El método de van der Corput se remonta a los trabajos [vdC21] y [vdC22]. Su estrategia es que básicamente las sumas trigonométricas se pueden aproximar por integrales (sumación de Poisson, fórmula de Euler-Maclaurin), integrales que pueden ser estimadas (aproximación de fase estacionaria, lemas de van der Corput).

Si aplicamos ciegamente a $S(N;\alpha)$ la típica aproximación por integrales [Ivi03, §2.2] perdemos $O(1)$ y este tipo de incertidumbre en la posición de un punto puede destruir el patrón. De modo que se deben modificar los argumentos para obtener

términos de error arbitrariamente pequeños. Esto se hace en el Teorema 1 de [Lox83] (nótese el pequeño error de imprenta en su resultado: 1 debería ser 1/2 en el paréntesis) pero debemos trabajar para obtener constantes explícitas eficaces. En una gran parte de su trabajo original [vdC21], van der Corput trató de mantener constantes explícitas.

El significado geométrico del siguiente resultado es que los puntos de $\{S(n;\alpha)\}_n$ están eventualmente bien aproximados por la espiral $\{\mathcal{A}(n;\alpha)\}_n$ salvo por una traslación $S(M;\alpha)-\mathcal{A}(M;\alpha)$ y un término de error arbitrariamente pequeño.

Lema 6.2.1. *Si $\alpha^2 \le M \le N$, entonces*

$$S(N;\alpha)-\mathcal{A}(N;\alpha) = S(M;\alpha)-\mathcal{A}(M;\alpha)+\frac{\alpha\theta}{\sqrt{M}}$$

donde $\mathcal{A}$ es el término principal

$$\mathcal{A}(x;\alpha) = \frac{e\big(\alpha\sqrt{x}-1/4\big)}{\pi\alpha}\Big(\sqrt{x}+i\cosh\log(\pi\alpha)\Big),$$

y $\theta=\theta(N,M,\alpha)$ es un número complejo con $|\theta|\le 1$.

Demostración. A partir del caso más simple de la fórmula de Euler-Maclaurin (véase por ejemplo el Apéndice de [Ivi03]) aplicado a $F(x)=e\big(\alpha\sqrt{x}\big)$,

$$\sum_{M<n\le N} e\big(\alpha\sqrt{n}\big) = \int_M^N e\big(\alpha\sqrt{x}\big)\,dx + \frac{e\big(\alpha\sqrt{N}\big)-e\big(\alpha\sqrt{M}\big)}{2}+E$$

con

$$E = -\sum_{n\neq 0}\frac{\alpha}{2n}\int_M^N x^{-1/2}e\big(nx+\alpha\sqrt{x}\big)\,dx = -\sum_{n\neq 0}\frac{\alpha}{n}\int_{\sqrt{M}}^{\sqrt{N}} e\big(nx^2+\alpha x\big)\,dx.$$

Y al integrar se obtiene

$$\int_M^N e\big(\alpha\sqrt{x}\big)\,dx+\frac{e\big(\alpha\sqrt{N}\big)-e\big(\alpha\sqrt{M}\big)}{2} = \mathcal{A}(N;\alpha)-\mathcal{A}(M;\alpha).$$

Entonces solamente tenemos que lidiar con E.

El lema de van der Corput con constante óptima (ver [Rog05, Lemma 3] y [Cat14]) asegura que si f' es monótona y $|f'|\ge\lambda$, entonces

$$\Big|\int_a^b e\big(f(x)\big)\,dx\Big| \le \frac{1}{\pi\lambda}.$$

En nuestro caso $f(x) = nx^2 + \alpha x$ y se tiene

$$|E| \le \frac{\alpha}{2\pi\sqrt{M}} \sum_{n=1}^{\infty} \Big(\frac{1}{n^2} + \frac{1}{n(n-1/2)} \Big) = \frac{\alpha}{2\pi\sqrt{M}} \Big(\frac{\pi^2}{6} + 4\log 2 \Big) \le \frac{\alpha}{\sqrt{M}},$$

donde se ha usado que para $x \ge \sqrt{M}$, la derivada de $f(x) = nx^2 + \alpha x$ satisface $|f'| \ge 2n\sqrt{M}$ si $n \in \mathbb{Z}^+$ y $|f'| \ge 2\sqrt{M}|n + 1/2|$ si $n \in \mathbb{Z}^-$. □

Con esta aproximación y la teoría de sumas trigonométricas se pueden explicar las propiedades geométricas mencionadas anteriormente.

Fijado M lo suficientemente grande para disminuir la influencia de $\alpha\theta/\sqrt{M}$, se tiene que para $N > M$, $S(N;\alpha)$ se aproxima bien por $\mathcal{A}(N;\alpha)$ más una constante compleja (una traslación). Entonces, asintóticamente tenemos

$$S(x;\alpha) \sim \frac{\sqrt{x}}{\pi\alpha} e\big(\alpha\sqrt{x} - 1/4\big)$$

que cuando x varía describe una espiral de Arquímedes de amplitud $1/\pi\alpha$. Por otro lado, como $\alpha\sqrt{N+1} - \alpha\sqrt{N} \sim \alpha/2\sqrt{N}$, después de la discretización, se tiene un número de puntos por vuelta comparable a la longitud. Esto explica que a la larga se observe una estructura circular creciente. La concentración de puntos que aparecen antes de entrar en la estructura circular provienen de integrales de Fresnel (espiral de Cornu) y son una reminiscencia de la fórmula truncada de sumación de Poisson para funciones convexas

$$\sum_{A \le n \le B} e\big(f(n)\big) = \sum_{f'(A)-1 \le n \le f'(B)-1} \int_A^B e\big(f(x) - nx\big)\, dx + \text{Error},$$

introducida en [vdC22]. Esto se estudia con detalle en [Lox83]. Dirigimos al lector al Teorema 2 de este trabajo en el que se demuestra que para cualquier entero positivo $n \le \alpha^{2/3}$ aparece una espiral de Cornu para N comparable a $(\alpha/2n)^2$. La más visible (la menos afectada por la discretización y el término de error) es la última, que corresponde a tomar $n = 1$ y tiene una amplitud proporcional a α.

Para α no demasiado pequeño $\cosh\log(\pi\alpha)$ se aproxima por $\pi\alpha/2$, por lo que cuando x es mucho menor que $\pi^2\alpha^2/4$ se tiene

$$\big|\mathcal{A}(x;\alpha)\big| = \frac{(x + \cosh^2 \log \pi\alpha)^{1/2}}{\pi\alpha} \approx \frac{1}{2}$$

y $\big|\mathcal{A}(x;\alpha)\big| \ge \big|\mathcal{A}(0;\alpha)\big|$, lo que explica el agujero en la estructura circular.

Si queremos que el término de error $\alpha\theta/\sqrt{M}$ sea pequeño debemos tomar M como una constante (grande) por α^2. En esta situación, $\mathcal{A}(M;\alpha) = O(1)$ (suponemos que

α no es pequeño) y la determinación de la traslación viene dada por el tamaño de $S(M;\alpha)$. La última parte de la suma se controla fácilmente aproximando por integrales como se mencionó anteriormente. Si dividimos el resto de la suma en intervalos diádicos, debemos estudiar

$$\sum_{X<n\leq 2X} e(\alpha\sqrt{n}) \qquad \text{con} \quad 2X < \alpha^2.$$

Ahora, por la estimación más simple de van der Corput [GK91, Theorem 2.2], tenemos

$$\Big|\sum_{X<n\leq 2X} e(\alpha\sqrt{n})\Big| \leq C\Big(X\big(\alpha X^{-3/2}\big)^{1/2} + \big(\alpha X^{-3/2}\big)^{-1/2}\Big) \leq 2C\alpha^{1/2}X^{1/4}$$

con una constante absoluta (y efectiva) C. Sumando las contribuciones diádicas correspondientes a $X = M/2^j$, se tiene que $S(M;\alpha)$, y por tanto la traslación, está acotada por $C'\alpha$.

6.3. Modelo matemático de los patrones

A partir del Lema 6.2.1, la sucesión $\{\mathcal{A}(n;\alpha)\}_{n=1}^{\infty}$ a la larga representa con precisión arbitraria el comportamiento de $\{S(n;\alpha)\}_{n=1}^{\infty}$. Aunque la curva parametrizada $\{\mathcal{A}(x;\alpha) \ : \ x \in \mathbb{R}^+\}$ no es exactamente una espiral de Arquímedes, debido a la constante $ic\cosh\log(\pi\alpha)$, tiende a ella. Nótese que

$$\mathcal{A}(x^2/\alpha^2;\alpha) \sim x\frac{e(x-1/4)}{\pi\alpha^2}, \tag{6.2}$$

entonces, la separación entre vueltas sucesivas tiende a ser $1/\pi\alpha^2$. Por otro lado,

$$\big|\mathcal{A}(n+1;\alpha) - \mathcal{A}(n;\alpha)\big| \to 1, \qquad \text{cuando} \quad n \to \infty.$$

Por lo tanto, cuando $\alpha > \pi^{-1}$ la amplitud de la espiral es menor que la distancia entre los valores consecutivos de la discretización. Entonces la ilusión óptica sólo debe aparecer en este caso, lo que concuerda con los experimentos. La explicación de la ilusión óptica es que nuestra vista tiende a conectar los puntos en diferentes turnos porque están más cerca. De esta manera, y teniendo en cuenta (6.2), $\mathcal{A}(n_1;\alpha)$ y $\mathcal{A}(n_2;\alpha)$, con $n_1, n_2 \in \mathbb{Z}^+$ llegan a ser geométricamente consecutivos si

$$\alpha\sqrt{n_1} \approx \alpha\sqrt{n_2} + 1.$$

Dado n_1, la mejor opción es tomar el incremento $n_2 - n_1$ como el número entero más cercano a $2\alpha^{-1}\sqrt{n} + \alpha^{-2}$. Esto conduce a la relación de recurrencia

$$t_{k+1} = t_k + \Big\lfloor \frac{2\alpha\sqrt{t_k}+1}{\alpha^2} + \frac{1}{2} \Big\rfloor. \tag{6.3}$$

Definition 6.3.1. Una *rama* es una sucesión $\{\mathcal{A}(t_k;\alpha)\}_{k=0}^{\infty}$ donde t_k satisface la relación de recurrencia (6.3).

Las curvas que se observan en las figuras de las sumas parciales de $S(N;\alpha)$ corresponden a porciones de ramas. De ahí que las ramas plasman completamente la información acerca de los patrones. Desde el punto de vista matemático, la comprensión de los patrones da medios para resolver la recurrencia (6.3).

6.4. Solución de la recurrencia

Si en (6.3) aproximamos $\lfloor x+1/2\rfloor$ por x, la solución se puede resolver explícitamente como una función cuadrática. Este comportamiento cuadrático se conserva, de alguna manera, cuando $\alpha^2\in\mathbb{Z}^+$.

Nos limitamos al caso en el que α^2 es par. Parece que el caso impar es similar con una simetría adicional, pero no hemos trabajado en los detalles.

Escribimos $n=\alpha^2$ y asumimos que la sucesión definida por (6.3) no es constante. Es fácil ver que esto equivale a imponer $t_0\geq\lfloor(n+12)/16\rfloor$. En resumen, se estudia (6.3) en la siguiente forma

$$t_{k+1}=t_k+\Big\lfloor\frac{2\sqrt{nt_k}+1}{n}+\frac{1}{2}\Big\rfloor\qquad\text{con}\quad t_0\geq\Big\lfloor\frac{n+12}{16}\Big\rfloor\quad\text{y}\quad 2\mid n. \tag{6.4}$$

Para presentar nuestra solución de esta relación de recurrencia, definimos $\delta(x)$ como la función que da el incremento $t_{k+1}-t_k$ en términos de t_k:

$$\delta(x)=\Big\lfloor 2\sqrt{\frac{x}{n}}+\frac{1}{2}+\frac{1}{n}\Big\rfloor$$

e introducimos una sucesión auxiliar $\{a_k\}_{k=0}^{\infty}$

$$a_k=\sum_{0\leq m<k}\Big\lfloor\frac{2m}{n}\Big\rfloor.$$

Es fácil ver que a_k admite una fórmula explícita simple:

$$a_k=kq-\frac{q(q+1)n}{4}\qquad\text{donde}\quad q=\Big\lfloor\frac{2(k-1)}{n}\Big\rfloor.$$

Proposición 6.4.1. *Las sucesiones que verifican* (6.4) *están dadas por*

$$t_k=a_{k+n/2-J}+\delta_0 k+t_0,$$

donde $\delta_0=\delta(t_0)$ *y* J *es el menor entero positivo tal que* $\delta(t_0+J\delta_0)-\delta_0=1$.

Nótese que t_k viene dado por un polinomio cuadrático cuando k se restringe a las clases módulo $n/2$. El resultado explica las estructuras parabólicas que aparecen en al caso $\alpha^2 = \sqrt{n}$. Algunos de los puntos más finos en los patrones podrían requerir algún conocimiento sobre $J = J(t_0)$. Discutiremos más adelante una posible fórmula explícita.

El caso $\alpha = \sqrt{2}$ es un poco especial porque $n/2 = 1$ y la fórmula no requiere división en clases de congruencia por lo que resulta especialmente sencilla:

$$t_k = \frac{k(k+1)}{2} + k\lfloor\sqrt{2t_0}\rfloor + t_0.$$

El caso genérico $\alpha^2 \notin \mathbb{Z}^+$ parece ser una deformación del caso $\alpha^2 \in \mathbb{Z}$ en el sentido que las segundas diferencias finitas de t_k parecen ser cuasi-periódicas. Experimentalmente se obtiene conjuntos de polinomios cuadráticos dando una buena aproximación en un rango más o menos grande, pero no explica toda la sucesión. Por ejemplo, para $\alpha = 1.3$ tenemos un primer período de longitud 11 y que el período 169 se acerca más a la realidad. Hemos verificado que para $\alpha = 65/64$, el periodo (si existe) debe ser superior a 4225. Con los conocimientos actuales, no tenemos una explicación matemática de los patrones en este caso genérico.

Lema 6.4.2. *Para todo $m \in \mathbb{Z}^+$, si $\delta(m) > 0$ entonces*

$$\delta\big(m + \frac{n}{2}\delta(m)\big) = \delta(m) + 1,$$

y si $\delta(m) - \delta\big(m + 1 - \delta(m)\big) = 1$ entonces

$$\delta(m) = \delta\big(m + (\frac{n}{2} - 1)\delta(m)\big).$$

Demostración. Para abreviar, escribiremos $I = \delta(m)$, $c = 1/2 + 1/n$ y f para la parte fraccionaria de $2\sqrt{m/n} + c$. Con esta notación, la primera igualdad se lee

$$\Big\lfloor\sqrt{\frac{4m}{n} + 2I} + c\Big\rfloor = I + 1.$$

Como $\sqrt{4m/n} + c = I + f$, esto es lo mismo que

$$(I + 1 - c)^2 \le (I + f - c)^2 + 2I < (I + 2 - c)^2. \tag{6.5}$$

Usando que $c > 1/2$,

$$(I + 1 - c)^2 - (I + f - c)^2 = (2I + 1 + f - 2c)(1 - f) < (2I + f)(1 - f) \le 2I.$$

Esto demuestra la primera desigualdad en (6.5). La segunda se sigue de la misma manera, usando que $c \leq 1$,

$$(I+2-c)^2 - (I+f-c)^2 = (2I+2+f-2c)(2-f) > 2I.$$

Para la segunda parte del lema, procediendo como en (6.5) podemos escribir $\delta\big(m+1-\delta(m)\big) = \delta(m) - 1$ como

$$(I-c-1)^2 \leq (I+f-c)^2 + \frac{4}{n} - \frac{4I}{n} < (I-c)^2. \tag{6.6}$$

Se tiene

$$(I-c-1)^2 + 2I - \frac{4}{n} = (I-c)^2 - \frac{4}{n} + 2c + 1 \geq (I-c)^2$$

y

$$(I-c)^2 + 2I - \frac{4}{n} = (I-c+1)^2 - \frac{4}{n} + 2c - 1 \leq (I-c+1)^2.$$

Entonces, al sumar $2I - 4/n$ a (6.6) se obtiene

$$(I-c)^2 \leq (I+f-c)^2 + 2I - \frac{4I}{n} < (I-c+1)^2$$

que, como en (6.6), es equivalente a $\delta\big(m + (\frac{n}{2}-1)\delta(m)\big) = \delta(m)$. □

Demostración de la Proposición 6.4.1. Es suficiente probar que

$$\delta(t_k) - \delta_0 = \Big\lfloor \frac{2(k+n/2-J)}{n} \Big\rfloor, \tag{6.7}$$

pues podemos reescribirlo como

$$t_{k+1} - t_k = a_{k+1+n/2-J} - a_{k+n/2-J} + \delta_0$$

y considerar la siguiente suma telescópica para deducir el resultado,

$$t_k - t_0 = \sum_{0 \leq m < k} \big(t_{m+1} - t_m\big) = a_{k+n/2-J} - a_{n/2-J} + \delta_0 k.$$

Tenga en cuenta que $a_{n/2-J} = 0$.

Es claro que (6.7) es válido para $0 \leq k \leq J$ porque en este rango $t_k = t_0 + k\delta_0$, por la definición de J y la recurrencia. Un observación importante es que el lado derecho de (6.7) aumenta en 1 cuando $n/2$ divide a $k-J$, entonces queda por demostrar

$$\delta(t_k) - \delta(t_{k-1}) = 1 \quad \Leftrightarrow \quad k \equiv J \pmod{n/2}, \tag{6.8}$$

que es cierto para $k \le J$ por la fórmula $t_k = t_0 + k\delta_0$. Tomando $m = t_J$ entonces

$$\begin{aligned}\delta(m) - \delta\big(m+1-\delta(m)\big) &= \delta(t_J) - \delta\big(t_J+1-\delta(t_J)\big)\\ &= \delta_0 + 1 - \delta(t_J-\delta_0) = \delta_0 + 1 - \delta(t_{J-1}) = 1.\end{aligned}$$

Por la segunda parte del Lema 6.4.2, se tiene

$$\delta(t_J) = \delta\big(t_J + (\frac{n}{2}-1)\delta(t_J)\big).$$

Nótese que el lado izquierdo también coincide con $\delta\big(t_J + \frac{n}{2}\delta(t_J)\big) - 1$. De ello se deduce que $\delta(t_J) = \delta(t_{J+n/2-1})$ y

$$\delta(t_J) = \delta(t_{J+1}) = \cdots = \delta(t_{J+n/2-1}) \qquad \text{and} \qquad \delta(t_{J+n/2}) = \delta(t_J) + 1.$$

Con esto queda demostrado (6.8) para $k \le J + n/2$. El mismo razonamiento sirve sustituyendo J por $J + n/2$ y, en general, un argumento inductivo, completa la prueba. □

Antes de introducir la fórmula experimental para J, es conveniente enunciar el siguiente lema elemental.

Lema 6.4.3. *Dado $n \in \mathbb{Z}^+$ par, para cada número entero no negativo k, existen $l, r \in \mathbb{Z}$ unívocamente determinados tales que*

$$k = nl^2 + \big(\frac{n}{2}+1\big)l + r \quad \textit{con} \quad l \ge 0 \quad \textit{y} \quad r \in I_l,$$

donde $I_l = \big[1-nl, (2l+1)\frac{n}{2}+1\big]$.

Demostración. Definimos $P(l,r) = nl^2 + \big(\frac{n}{2}+1\big)l + r$. Incrementando ambas variables en los rangos indicados, un cálculo demuestra que

$$P(l+1, 1-n(l+1)) = P\big(l, (2l+1)\frac{n}{2}+1\big) + 1.$$

Esto implica que los intervalos $P(l, I_l)$ son disjuntos y consecutivos cuando l varía. □

Desde el punto de vista computacional, l y r son fáciles de determinar como solución de la ecuación $nx^2 + \big(\frac{n}{2}+1\big)x = k$ con $x \ge 0$, entonces $l = \lfloor x \rfloor$ o $l = \lfloor x \rfloor + 1$ y $r = k - nl^2 - \big(\frac{n}{2}+1\big)l$.

Conjetura 6.4.4. *Con la notación y la hipótesis de la Proposición 6.4.1 y asumiendo que $n/2 \not\equiv 2, 3, 4, 5 \pmod 8$, sea r el entero correspondiente a $k = t_0 - [(n+12)/16]$ en*

la representación del Lema 6.4.3, entonces J es el entero $0 < J \leq n/2$ determinado por

$$J \equiv -1 - \lfloor \frac{r-1}{2l+1} \rfloor \pmod{n/2} \qquad \textit{if } r \geq 0,$$

y por

$$J \equiv \lfloor \frac{-r-1}{2l} \rfloor \pmod{n/2} \qquad \textit{if } r < 0.$$

Un análisis experimental muestra que la conjetura también se aplica al caso $n/2 \equiv 2, 3, 4, 5 \pmod 8$ con muy pocas excepciones.

En el momento de terminar esta memoria, tenemos indicios claros acerca de la demostración de este resultado y su extensión al resto de casos. Además, parte de nuestro análisis se puede traducir a α^2 impar, de hecho, hemos resuelto algunos casos particulares.

Capítulo 7

Puntos del retículo en el toro sólido

7.1. Introducción

Consideremos un cuerpo compacto fijado $\mathbb{B} \subset \mathbb{R}^3$. El estudio de

$$\#\big\{\vec{n} \in \mathbb{Z}^3 \ : \ R^{-1}\vec{n} \in \mathbb{B}\big\}, \qquad R > 1,$$

es un problema básico en la teoría de puntos del retículo. Bajo condiciones muy generales de regularidad, esta cantidad se aproxima bien por $|\mathbb{B}|R^3$ donde $|\mathbb{B}|$ denota el volumen de $\mathbb{B}$. Asumiendo regularidad y convexidad, en el sentido de curvatura gaussiana positiva, el error en esta aproximación, la llamada *discrepancia de puntos del retículo*, es asintóticamente más pequeña que el área de la frontera, es decir, $O\big(R^\gamma\big)$ para algún $\gamma < 2$. Muchos autores han dedicado sus esfuerzos a dar una respuesta parcial a la pregunta natural de determinar el ínfimo de los valores válidos de γ, resultados que en general, dependen de técnicas sutiles con sumas trigonométricas. La cuestión sigue abierta incluso para cuerpos simples como la esfera (véase el survey [IKKN06] y los nuevos resultados en [Guo12]).

El caso no convexo también ha sido de interés, apareciendo en numerosos trabajos de la última década (véase por ejemplo [Pet02] [Krä02b] [Krä02a] [Now08a] [Now08b] [Guo13]). Una diferencia notable es que a veces el término principal tiene que ser complementado con un término principal secundario que proviene, de alguna manera, de los puntos de curvatura nula. Nótese, por ejemplo, que si $\mathbb{B}$ es el cubo $[-1,1]^3$ con esquinas y bordes suavizados entonces $\#\big\{\vec{n} \in \mathbb{Z}^3 \ : \ R^{-1}\vec{n} \in \mathbb{B}\big\}$ cuenta con más de R^2 puntos en la frontera cuando $R \in \mathbb{Z}^+$.

Un ejemplo particularmente atractivo, considerado en [Now08a], es el *toro sólido*

$$\mathbb{T} = \Big\{(x,y,z) \in \mathbb{R}^3 \ : \ \big(\rho' - \sqrt{x^2+y^2}\big)^2 + z^2 \leq \rho^2\Big\} \tag{7.1}$$

donde $0 < \rho < \rho'$ son constantes fijadas. Su volumen es $2\pi^2\rho^2\rho'$ pero el término principal natural que aproxima el número de puntos del retículo en el toro R-escalado

es

$$\mathcal{M}(R) = 2\pi^2\rho^2\rho' R^3 + 4\pi\rho\rho' R^2 \sum_{n=1}^{\infty} \frac{J_1(2\pi R\rho n)}{n} \tag{7.2}$$

donde J_1 es la función de Bessel. Si bien es cierto que este segundo termino principal tiene un carácter oscilatorio, es esencialmente una sencilla función ρ^{-1} periódica, por ejemplo si $R\rho \in \mathbb{Z}^+$ entonces (7.2) puede leerse como $CR^3 + C'R^{3/2}$ para ciertas constantes C y C' salvo un error despreciable.

Nuestro resultado principal acota la discrepancia de puntos del retículo cuando $\mathcal{M}(R)$ se toma como el término principal.

Teorema 7.1.1. *Con la notación de* (7.1) *y* (7.2)*, consideramos*

$$\mathcal{N}(R) = \#\big\{\vec{n} \in \mathbb{Z}^3 \ : \ R^{-1}\vec{n} \in \mathbb{T}\big\}, \qquad y \qquad \mathcal{E}(R) = \mathcal{N}(R) - \mathcal{M}(R).$$

Entonces se tiene que

$$\mathcal{E}(R) = O\big(R^{4/3+\epsilon}\big) \qquad \textit{para todo} \quad \epsilon > 0.$$

El resultado previamente conocido, debido a W.G. Nowak [Now08a], sustituye el exponente 4/3 por 11/8. Nowak escribe $\mathcal{M}(R)$ como una serie dependiendo de funciones elementales, que es equivalente a nuestro resultado tras sustituir la fórmula asintótica de J_1.

El exponente 4/3 es mejor que el resultado más conocido para cuerpos convexos generales de rotación. Esto es notable porque, en principio, el caso no convexo es más difícil desde un punto de vista analítico. El exponente viene de un término diagonal y parece poco probable una mejora en el contexto de los enfoques clásicos basados en sumas trigonométricas. Si se pudiera contar con precisión (más allá de los límites del análisis armónico) puntos cercanos a la frontera en la teoría de escalado, entonces uno podría usar los argumentos de [CI95] (mejorado en [HB99]) o [CCU09] para ir más allá de 4/3. Los armónicos multiplicativos (caracteres de Dirichlet) y los armónicos automorfos empleados en estos documentos, aparentemente, no se pueden utilizar en el toro.

En lo que sigue, asumiremos $\rho' = 1$. Por supuesto, esto se puede hacer sin perdida de generalidad pues estamos considerando dominios homotéticos. En este capítulo denotamos por ϵ una cantidad positiva arbitrariamente pequeña, no necesariamente la misma cada vez. Las constantes que intervienen en O y $\ll$ (notaciones que consideramos equivalentes) pueden depender de ϵ y de ρ.

7.2. Aplicación de la fórmula de sumación de Poisson

Sea χ la función característica de $\mathbb{T}$,

$$\chi(\vec{x}) = 1 \quad \text{si } \vec{x} \in \mathbb{T} \qquad \text{y} \qquad \chi(\vec{x}) = 0 \quad \text{si } \vec{x} \in \mathbb{R}^3 - \mathbb{T}.$$

Una aplicación formal de la fórmula de sumación de Poisson daría

$$\mathcal{N}(R) = \sum_{\vec{n}\in\mathbb{Z}^3} \chi\big(R^{-1}\vec{n}\big) = R^3 \sum_{\vec{n}\in\mathbb{Z}^3} \widehat{\chi}(R\vec{n}),$$

y se puede comprobar que $\mathcal{M}(R)$ proviene de los términos con $n_1 = n_2 = 0$ (Lema 7.2.2, nótese que $\widehat{\chi}(\vec{0}) = |\mathbb{T}| = 2\pi^2\rho^2$). En principio esto permitiría expresar directamente $\mathcal{E}(R)$ como una suma oscilatoria. Por desgracia, la hipótesis para aplicar la fórmula de sumación de Poisson no se cumple y la convergencia de la última suma no está asegurada. Una herramienta analítica estándar para evitar este problema es introducir una función de suave en χ. Se procede como en la Proposición 2.1 de [Cha98]. En aras de la completitud incluimos aquí una prueba.

Proposición 7.2.1. *Dados $R > 2$ y $\delta = R^{-c}$ con $0 < c < 1$ una constante fijada, existe $R - 2\delta^{1-\epsilon} < R' < R + 2\delta^{1-\epsilon}$ tal que*

$$\mathcal{N}(R) = 2\pi\rho^2 R^3 + R'^3 \sum \eta\big(\delta\|\vec{n}\|\big)\widehat{\chi}(R'\vec{n}) + O\big(R^{2+\epsilon}\delta\big),$$

donde la suma se lleva a cabo sobre $\vec{n} \in \mathbb{Z}^3 - \{\vec{0}\}$.

Demostración. Sea la función $\eta \in C_0^\infty(-1,1)$ con $\eta(0) = 1$ y tal que la transformada de Fourier de $\eta(\|\vec{x}\|)$ es positiva y sea $\widehat{\eta}_\delta$ la transformada de Fourier de$\eta(\delta\|\cdot\|)$. Entonces, para $k \geq 1$ se tiene

$$\int_{\|\vec{t}\|\leq\delta^{1-\epsilon}} \widehat{\eta}_\delta(\vec{t})\, d\vec{t} = 1 + O(\delta^k) \quad \text{y} \quad \int_{\|\vec{t}\|\geq\delta^{1-\epsilon}} \widehat{\eta}_\delta(\vec{t})\, d\vec{t} = O(\delta^k).$$

Además, consideramos la convolución

$$(\widehat{\eta}_\delta * \chi_R)(\vec{x}) = \int_{\mathbb{R}^3} \widehat{\eta}_\delta(\vec{t})\chi_R(\vec{x} - \vec{t})\, d\vec{t},$$

donde $\chi_R(\vec{x}) = \chi(R^{-1}\vec{x})$. Si $R_1 = R - 2\delta^{1-\epsilon}$ y $R_2 = R + 2\delta^{1-\epsilon}$ tenemos que

$$(\widehat{\eta}_\delta * \chi_{R_1})(\vec{x}) \leq \chi_R(\vec{x}) + O(\delta^k) \qquad \text{y} \qquad (\widehat{\eta}_\delta * \chi_{R_2})(\vec{x}) \geq \chi_R(\vec{x}) + O(\delta^k).$$

Por lo tanto, debe existir un R' con $|R' - R| < 2\delta^{1-\epsilon}$, tal que

$$\sum_{\vec{n}\in\mathbb{Z}^3} (\widehat{\eta}_\delta * \chi_{R'})(\vec{n}) = \mathcal{N}(R) + O\big(R^3\delta^k\big).$$

Aplicando la fórmula de sumación de Poisson al primer término se llega a

$$\mathcal{N}(R) = R'^3\eta(0)\widehat{\chi}(0) + R'^3 \sum_{\vec{0}\neq\vec{n}\in\mathbb{Z}^3} \eta\big(\delta\|\vec{n}\|\big)\widehat{\chi}(R'\vec{n}) + O\big(R^3\delta^k\big).$$

Como $R'^3 = R^3 + O(R^2\delta^{1-\epsilon})$, tomando k suficientemente grande se obtiene el resultado. □

Para interpretar la suma como una suma trigonométrica es importante estudiar la oscilación de $\widehat{\chi}$. Como paso previo, damos una fórmula integral para esta función.

Lema 7.2.2. *La transformada de Fourier de χ es una función radial en las dos primeras variables y verifica $\widehat{\chi}(\xi_1,\xi_2,\xi_3) = \Psi(\xi_1^2+\xi_2^2,\xi_3)$ para $\xi_1^2+\xi_2^2\neq 0$, donde*

$$\Psi(t,u) = \frac{\rho}{\sqrt{t}}\int_0^{2\pi} (1+\rho\operatorname{sen}\theta)\operatorname{sen}\theta J_1\big(2\pi(1+\rho\operatorname{sen}\theta)\sqrt{t}\big)e(\rho u\cos\theta)\,d\theta.$$

Demostración. Es bien conocido que la transformada de Fourier de una función radial es radial, separando las dos primeras variables, $\widehat{\chi}(\xi_1,\xi_2,\xi_3) = \Phi(\xi_1^2+\xi_2^2,\xi_3)$ donde $\Phi(t,u) = \widehat{\chi}(\sqrt{t},0,u)$. Con un cambio a coordenadas cilíndricas y la representación integral (2.11), se tiene

$$\Phi(t,u) = \iiint_{\mathbb{T}} e(-x\sqrt{t}-zu)\,dxdydz = \iint_D 2\pi r J_0(2\pi r\sqrt{t})e(-zu)\,drdz,$$

donde D es el disco $D = \big\{(r,z)\in\mathbb{R}^2 \,:\, (1-r)^2+z^2\leq\rho^2\big\}$.

El integrando es la derivada respecto de la variable r de la función $f(r,z) = rt^{-1/2}J_1(2\pi r\sqrt{t})e(-zu)$, porque $\big(zJ_1(z)\big)' = zJ_0(z)$. Entonces el teorema de Green aplicado al campo $\vec{F} = \big(0,f\big)$ da el resultado esperado con la parametrización de la frontera $r = 1+\rho\operatorname{sen}\theta$, $z = -\rho\cos\theta$ □

Después de la aplicación de la fórmula de sumación de Poisson, el término de volumen $2\pi\rho^2R^3$ aparece de forma evidente. El término principal secundario proviene de la parte de la suma con $\vec{n}$ en el eje z.

Proposición 7.2.3. *Con la notación de la Proposición 7.2.1*

$$\mathcal{E}(R) = R'^3 {\sum}' \eta\big(\delta\|\vec{n}\|\big)\widehat{\chi}(R'\vec{n}) + O\big(R^{2+\epsilon}\delta\big)$$

donde la suma recorre los $\vec{n}\in\mathbb{Z}^3$ tales que $n_1^2+n_2^2\neq 0$.

Demostración. La función de Bessel para valores pequeños satisface $J_1(z)\sim z/2$, por lo que el Lema 7.2.2 y la continuidad de $\widehat{\chi}$ nos permite escribir la suma de la Proposición 7.2.1 restringida a los términos con $n_1 = n_2 = 0$ como

$$2\pi\rho^2R'^3\sum_{n=1}^{\infty}\eta\big(\delta n\big)\int_0^{2\pi}\operatorname{sen}^2\theta\cos(2\pi\rho R'n\cos\theta)\,d\theta,$$

donde la integral es igual a $(\rho R'n)^{-1}J_1(2\pi\rho R'n)$. Combinando $|R'-R| \ll \delta^{1-\epsilon}$ con la fórmula asintótica, esta vez para valores grandes,

$$J_1(2\pi z) = \frac{1}{\pi\sqrt{z}}\cos\big(2\pi z - \frac{3\pi}{4}\big) + O\big(z^{-3/2}\big), \tag{7.3}$$

el error cometido al tomar R en lugar de R', proviene de las sumas

$$R^{3/2}\sum_{n>\delta^{-1+\epsilon}} n^{-3/2} \qquad \text{y} \qquad R^{3/2}\sum_{n<\delta^{-1}} \frac{|\eta\big(\delta n\big)e\big(R'n\big) - e\big(Rn\big)|}{n^{3/2}}$$

Usando que $\eta(x) = 1+O(x)$ y $|e\big(R'n\big)-e\big(Rn\big)| \ll \delta n$, ambas sumas son $\ll R^{3/2+\epsilon}\delta^{1/2}$ lo que completa la prueba □

7.3. Preparación de la suma trigonométrica

El argumento básico es la aplicación del principio de fase estacionaria a la representación integral de la transformada de Fourier dada en el Lema 7.2.2. Para facilitar la referencia, incluimos aquí la versión que utilizamos.

Lema 7.3.1 (Principio de fase estacionaria). *Sean $A \in C^\infty$ y $F \in C^\infty$ funciones 1-periódicas, tal que F tiene un único punto crítico $x = x_0$ en $(0,1)$ y $F''(x_0) > 0$. Entonces*

$$\int_0^1 A(x)e\big(\lambda F(x)\big)\,dx = \frac{e\big(\lambda F(x_0)+1/8\big)}{\sqrt{\lambda F''(x_0)}}A(x_0) + O\big(\lambda^{-3/2}\big) \quad \textit{cuando } \lambda \to +\infty$$

Con este resultado podemos expresar la suma que aparece en la Proposición 7.2.3 como una suma trigonométrica.

Proposición 7.3.2. *Para $t \geq 1$ y $u \geq 1$*

$$\Psi(t,u) = \frac{C\rho^{1/2}}{\ell^{1/2}t^{1/4}}\Big(T(t,u) + O\big(\ell^{-1}\big)\Big) + O\big(t^{-5/4}\big)$$

donde C es una constante absoluta, $\ell = (t+u^2)^{1/2}$ y

$$T(t,u) = (\ell+\rho\sqrt{t})^{1/2}\cos\big(2\pi(\rho\ell+\sqrt{t})\big) - (\ell-\rho\sqrt{t})^{1/2}\operatorname{sen}\big(2\pi(\rho\ell-\sqrt{t})\big).$$

Demostración. A partir de la fórmula asintótica (7.3), $\Psi(t,u)$ puede ser reescrito como

$$\frac{\rho}{\pi t^{3/4}}\int_0^{2\pi} A(\theta)\cos\big(2\pi\sqrt{t}(1+\rho\operatorname{sen}\theta) - \frac{3\pi}{4}\big)e(\rho u\cos\theta)\,d\theta + O(t^{-5/4})$$

donde $A(\theta) = (1+\rho\operatorname{sen}\theta)^{1/2}\operatorname{sen}\theta$. La integral anterior es la parte real de

$$\frac{e(\sqrt{t}-3/8)}{2}\int_0^{2\pi} A(\theta)\Big(e\big(\rho(\sqrt{t}\operatorname{sen}\theta+u\cos\theta)\big)+e\big(\rho(\sqrt{t}\operatorname{sen}\theta-u\cos\theta)\big)\Big)d\theta.$$

Escribiendo $\ell=(t+u^2)^{1/2}$, sea $0<\theta_{tu}<\pi/2$ tal que $\tan\theta_{tu}=\sqrt{t}/u$, de modo que $\sqrt{t}\operatorname{sen}\theta\pm u\cos\theta=\pm\ell\cos(\theta\mp\theta_{tu})$. Por lo tanto, tras un cambio lineal de variables y notando que $A(\theta+\pi-\theta_{tu})=A(\theta_{tu}-\theta)$ se tiene

$$\Psi(t,u)=\frac{\rho}{\pi t^{3/4}}\Re\left(e\big(\sqrt{t}-3/8\big)\int_0^{\pi}A(\theta_{tu}-\theta)e(\rho\ell\cos\theta)\,d\theta\right)+O(t^{-5/4}).$$

Nótese que la contribución principal en la integral resultante proviene de los puntos $\theta=0$ y $\theta=\pi$ en los que la fase $\cos\theta$ es estacionaria. Por el Lema 7.3.1, la integral es igual a

$$\rho^{-1/2}\ell^{-1/2}\Big(e(\rho\ell-1/8)A(\theta_{tu})+e(-\rho\ell+1/8)A(\theta_{tu}-\pi)+O(\ell^{-1})\Big).$$

Finalmente, usando que

$$A(\theta_{tu})=(\ell+\rho\sqrt{t})^{1/2}t^{1/2}\ell^{-3/2}\quad\text{y}\quad A(\theta_{tu}-\pi)=-(\ell-\rho\sqrt{t})^{1/2}t^{1/2}\ell^{-3/2}$$

se llega al resultado. □

7.4. Estimación de la suma trigonométrica

Tras la sumación parcial, la estimación relevante del teorema principal se plasma en el siguiente resultado.

Proposición 7.4.1. *Para todo $M\le R^{4/3}$, $N\le R^{2/3}$ y cualquier elección del signo $\pm$, se tiene*

$$\sup_{\substack{u<M\\ v<N}}\sum_{\substack{M\le m<M+u\\ N\le n<N+v}} r(m)e\big(R(\rho\sqrt{m+n^2}\pm\sqrt{m})\big)=O\big(R^{1/3+\epsilon}M^{1/4}L^{3/4}\big)$$

donde $L=M+N^2$.

El paso crucial en la prueba de la Proposición 7.4.1 es una variación de los argumentos de [CC12] que son una generalización de [CI95] y dan una cota para

$$S=\sum_{M\le m<2M}\Big|\sum_{N\le n<2N}e(\theta n)e\big(R\rho\sqrt{m+n^2}\big)\Big|\qquad\text{donde }\theta\in\mathbb{R}.$$

Lema 7.4.2. *Con la notación anterior, existe cierto $D \leq N^{2-\epsilon}$ tal que si $RD \ll L^{3/2}$ se tiene*

$$S \ll MN^{1/2} + R^{-1+\epsilon}L^{3/2}M,$$

mientras que si $RD \gg L^{3/2}$,

$$S \ll MN^{1/2} + R^{1/4+\epsilon}N^{7/6}L^{-1/24}M^{1/2} + R^{\epsilon}NL^{1/4}M^{1/2}.$$

Demostración. Siguiendo los pasos del Lema 3.1 de [CI95], por la desigualdad de Cauchy se tiene

$$S^2 \ll M \sum_{n_1,n_2} \Big| \sum_{m \asymp M} e\Big(R\rho\big(\sqrt{m+n_1^2} - \sqrt{m+n_2^2}\big)\Big)\Big|,$$

donde $|n_1 - n_2| < N^{1-\epsilon}$. Por tanto, para un $D \leq N^{2-\epsilon}$ adecuado y $\omega \in \mathbb{R}$, se obtiene

$$S^2 \ll M^2N + MR^{\epsilon} \sum_{y \asymp D} \Big| \sum_{x \asymp L} e(\omega x) e\big(R\rho(\sqrt{x} - \sqrt{x+y})\big)\Big|.$$

Este ω se introduce para completar la suma [IK04, §12.1] de modo que el rango de x no depende de y.

Por un lado, si $RD \ll L^{3/2}$ entonces $f(x,y) = \sqrt{x} - \sqrt{x+y}$ es monótona en x y su derivada parcial satisface $\partial_1 f \asymp RDL^{-3/2}$. Por lo tanto, por el test de la derivada primera (véase Teorema 2.1 de [GK91]) la suma interna es $\ll R^{-1}D^{-1}L^{3/2}$.

Si $RD \gg L^{3/2}$, usamos el proceso B del método de van der Corput (Lema 3.6 de [GK91]) para transformar la suma. Esto se hace en el Lema 3.1 de [CI95]. En este caso, se deduce (véase el Lema 3.3 de [CC12]),

$$S^2 \ll M^2N + R^{-1/2+\epsilon}D^{-1/2}L^{5/4}M\big|T_{DL}\big|,$$

donde T_{DL} es la suma trigonométrica

$$T_{DL} = \sum_{y \asymp D} \Big| \sum_{x \asymp RDL^{-3/2}} e\big(g(x,y)\big)\Big|,$$

con $g(x,y) = f(\alpha(x,y),y) - x\alpha(x,y)$ donde $\alpha = \alpha(x,y)$ se define implícitamente como $\partial_1 f(\alpha(x,y),y) = x$.

Por último, la Proposición 3.6 de [CC12] con $p = q = 1/2$ da

$$T_{DL} \ll RD^{5/3}L^{-4/3} + R^{1/2+\epsilon}D^{3/2}L^{-3/4},$$

con lo que se consigue el resultado. □

Proposición 7.4.1. Usando la técnica de completación de sumas, se tiene

$$\sup_{\substack{u<M \\ v<N}} \sum_{\substack{M \leq m < M+u \\ N \leq n < N+v}} r(m) e\big(R(\rho\sqrt{m+n^2} \pm \sqrt{m})\big) \ll R^{\epsilon}S$$

El resultado se sigue del Lema 7.4.2 dividiendo en dos casos, $N^2 < M$ y $N^2 \geq M$, que dan lugar a $L \asymp M$ y $L \asymp N^2$, respectivamente. □

7.5. Final de la Prueba

Para demostrar el teorema principal es suficiente combinar los resultados de las secciones anteriores.

Demostración del Teorema 7.1.1. Por la Proposición 7.2.3 y el Lema 7.2.2, tomando $\delta = R^{-2/3}$ el resultado se deduce al probar

$$R^2 \sum_{n=-\infty}^{\infty} \sum_{m=1}^{\infty} r(m)\eta\big(R^{-2/3}\sqrt{m+n^2}\big)\Psi(R^2 m, Rn) = O\big(R^{1/3+\epsilon}\big).$$

La contribución de $n = 0$ es absorbida por el término de error, y la simetría en n permite considerar la primera suma restringida a $n \geq 1$. Ahora, la Proposición 7.3.2 muestra que lo anterior es equivalente a probar

$$\sum_{\substack{m<R^{4/3} \\ n<R^{2/3}}} h(m,n)r(m)e\big(R(\rho\sqrt{m+n^2} \pm \sqrt{m})\big) = O\big(R^{1/3+\epsilon}\big) \tag{7.4}$$

donde

$$h(m,n) = \frac{\big(\sqrt{m+n^2} \pm \sqrt{m}\big)^{1/2}}{m^{1/4}(m+n^2)}.$$

Nótese que los términos $O\big(\ell^{-1}\big)$ y $O\big(t^{-5/4}\big)$ de la proposición son de nuevo absorbidos por el término de error.

Consideramos la suma anterior restringida a intervalos diádicos de la forma $M \leq m < 2M$, $N \leq n < 2N$. En estos rangos h satisface

$$h(m,n) \ll M^{-1/4}L^{-3/4}, \qquad \partial_1 h(m,n) \ll M^{-5/4}L^{-3/4}$$
$$\partial_2 h(m,n) \ll M^{-1/4}N^{-1}L^{-3/4}, \qquad \partial_1\partial_2 h(m,n) \ll M^{-5/4}N^{-1}L^{-3/4}$$

con $L = M + N^2$. Usando sumación por partes (ver Lema α de [Tit34]), la parte izquierda de (7.4) está acotada por

$$R^{\epsilon}M^{-1/4}L^{-3/4} \sup_{\substack{u<M \\ v<N}} \sum_{\substack{M\leq m<M+u \\ N\leq n<N+v}} r(m)e\big(R(\rho\sqrt{m+n^2} \pm \sqrt{m})\big)$$

y la Proposición 7.4.1 conduce a (7.4). □

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.

[BH98] R. C. Baker and G. Harman. Shifted primes without large prime factors. *Acta Arith.*, 83(4):331–361, 1998.

[BHC61] A. Borel and Harish-Chandra. Arithmetic subgroups of algebraic groups. *Bulletin of the American Mathematical Society*, 67(6):579–583, 11 1961.

[BHP01] R. C. Baker, G. Harman, and J. Pintz. The difference between consecutive primes. II. *Proc. London Math. Soc. (3)*, 83(3):532–562, 2001.

[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.

[Bru78] R. W. Bruggeman. Fourier coefficients of cusp forms. *Invent. Math.*, 45(1):1–18, 1978.

[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.

[Cat14] C. Catalá. An elementary proof of a Van der Corput's lemma. To appear in *The American Mathematical Monthly*, 2014.

[CC12] F. Chamizo and E. Cristóbal. The sphere problem and the L-functions. *Acta Math. Hungar.*, 135(1-2):97–115, 2012.

[CCU09] F. Chamizo, E. Cristóbal, and A. Ubis. Lattice points in rational ellipsoids. *J. Math. Anal. Appl.*, 350(1):283–289, 2009.

[CH53] R. Courant and D. Hilbert. *Methods of mathematical physics. Vol. I.* Interscience Publishers, Inc., New York, N.Y., 1953.

[Cha96] F. Chamizo. The large sieve in Riemann surfaces. *Acta Arith.*, 77(4):303–313, 1996.

[Cha98] F. Chamizo. Lattice points in bodies of revolution. *Acta Arith.*, 85(3):265–277, 1998.

[Cha99] F. Chamizo. Correlated sums of $r(n)$. *J. Math. Soc. Japan*, 51(1):237–252, 1999.

[Cha09] M.-C. Chang. Burgess inequality in $\mathbb{F}_{p^2}$. *Geom. Funct. Anal.*, 19(4):1001–1016, 2009.

[Cha11] F. Chamizo. Ocho lecciones de teoría de números. 2011.

[CI95] F. Chamizo and H. Iwaniec. On the sphere problem. *Rev. Mat. Iberoamericana*, 11(2):417–429, 1995.

[Clo11] B. Cloitre. 10 conjectures in additive number theory. ArXiv:1101.4274, 2011.

[CPS90] J. W. Cogdell and I. Piatetski-Shapiro. *The arithmetic and spectral analysis of Poincaré series*, volume 13 of *Perspectives in Mathematics*. Academic Press Inc., Boston, MA, 1990.

[CR10] F. Chamizo and D. Raboso. Modular forms and quasi-integers (Spanish). *Gac. R. Soc. Mat. Esp.*, 13(3):539–555, 2010.

[Dav80] H. Davenport. *Multiplicative number theory*, volume 74 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1980. Revised by Hugh L. Montgomery.

[Des85] J.-M. Deshouillers. Geometric aspect of Weyl sums. In *Elementary and analytic theory of numbers (Warsaw, 1982)*, volume 17 of *Banach Center Publ.*, pages 75–82. PWN, Warsaw, 1985.

[DGL13] W. Duke, S. R. Garcia, and B. Lutz. 10 conjectures in additive number theory. arXiv:1212.6825, 2013.

[DI83] J.-M. Deshouillers and H. Iwaniec. Kloosterman sums and Fourier coefficients of cusp forms. *Invent. Math.*, 70(2):219–288, 1982/83.

[DMF81] F. M. Dekking and M. Mendès France. Uniform distribution modulo one: a geometrical viewpoint. *J. Reine Angew. Math.*, 329:143–153, 1981.

[EHGL89] J. Eichenauer-Herrmann, H. Grothe, and J. Lehn. On the period length of pseudorandom vector sequences generated by matrix generators. *Math. Comp.*, 52(185):145–148, 1989.

[EMY03] R. Evans, M. Minei, and B. Yee. Incomplete higher-order Gauss sums. *J. Math. Anal. Appl.*, 281(2):454–476, 2003.

[FI10] J. Friedlander and H. Iwaniec. *Opera de cribro*, volume 57 of *American Mathematical Society Colloquium Publications*. American Mathematical Society, Providence, RI, 2010.

[FL] D. W. Farmer and S. Lemurell. Maass forms and their L-functions. *Preprint* `http://www.math.chalmers.se/~sj/forskning.html`.

[Gal71] P. X. Gallagher. A larger sieve. *Acta Arith.*, 18:77–81, 1971.

[GBGL08] T. Gowers, J. Barrow-Green, and I. Leader, editors. *The Princeton companion to mathematics*. Princeton University Press, Princeton, NJ, 2008.

[GK91] S. W. Graham and G. Kolesnik. *van der Corput's method of exponential sums*, volume 126 of *London Mathematical Society Lecture Note Series*. Cambridge University Press, Cambridge, 1991.

[Gol06] D. Goldfeld. *Automorphic forms and L-functions for the group* $\mathrm{GL}(n, \mathbb{R})$, volume 99 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, 2006. With an appendix by Kevin A. Broughan.

[GR07] I. S. Gradshteyn and I. M. Ryzhik. *Table of integrals, series, and products*. Elsevier/Academic Press, Amsterdam, seventh edition, 2007.

[Guo12] J. Guo. On lattice points in large convex bodies. *Acta Arith.*, 151(1):83–108, 2012.

[Guo13] J. Guo. Lattice points in rotated convex domains. arXiv:1303.4137, 2013.

[Har07] G. Harman. *Prime-detecting sieves*, volume 33 of *London Mathematical Society Monographs Series*. Princeton University Press, Princeton, NJ, 2007.

[HB99] D. R. Heath-Brown. Lattice points in the sphere. In *Number theory in progress, Vol. 2 (Zakopane-Kościelisko, 1997)*, pages 883–892. de Gruyter, Berlin, 1999.

[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.

[Hux72] M. N. Huxley. On the difference between consecutive primes. *Invent. Math.*, 15:164–170, 1972.

[Hux03] M. N. Huxley. Exponential sums and lattice points. III. *Proc. London Math. Soc. (3)*, 87(3):591–609, 2003.

[HW08] G. H. Hardy and E. M. Wright. *An introduction to the theory of numbers.* Oxford University Press, Oxford, sixth edition, 2008. Revised by D. R. Heath-Brown and J. H. Silverman, With a foreword by Andrew Wiles.

[IK04] H. Iwaniec and E. Kowalski. *Analytic number theory*, volume 53 of *American Mathematical Society Colloquium Publications.* American Mathematical Society, Providence, RI, 2004.

[IKKN06] A. Ivić, E. Krätzel, M. Kühleitner, and W. G. Nowak. Lattice points in large regions and related arithmetic functions: recent developments in a very classic topic. In *Elementare und analytische Zahlentheorie*, Schr. Wiss. Ges. Johann Wolfgang Goethe Univ. Frankfurt am Main, 20, pages 89–128. Franz Steiner Verlag Stuttgart, Stuttgart, 2006.

[Ivi03] A. Ivić. *The Riemann zeta-function.* Dover Publications Inc., Mineola, NY, 2003. Theory and applications, Reprint of the 1985 original [Wiley, New York; MR0792089 (87d:11062)].

[Iwa02] H. Iwaniec. *Spectral methods of automorphic forms*, volume 53 of *Graduate Studies in Mathematics.* American Mathematical Society, Providence, RI, second edition, 2002.

[KN74] L. Kuipers and H. Niederreiter. *Uniform distribution of sequences.* Wiley-Interscience [John Wiley & Sons], New York, 1974. Pure and Applied Mathematics.

[KR01] P. Kurlberg and Z. Rudnick. On quantum ergodicity for linear maps of the torus. *Comm. Math. Phys.*, 222(1):201–227, 2001.

[Krä02a] E. Krätzel. Lattice points in some special three-dimensional convex bodies with points of Gaussian curvature zero at the boundary. *Comment. Math. Univ. Carolin.*, 43(4):755–771, 2002.

[Krä02b] E. Krätzel. Lattice points in three-dimensional convex bodies with points of Gaussian curvature zero at the boundary. *Monatsh. Math.*, 137(3):197–211, 2002.

[KRR07] P. Kurlberg, L. Rosenzweig, and Z. Rudnick. Matrix elements for the quantum cat map: fluctuations in short windows. *Nonlinearity*, 20(10):2289–2304, 2007.

[Kub73] T. Kubota. *Elementary theory of Eisenstein series.* Kodansha Ltd., Tokyo, 1973.

[Kur03] P. Kurlberg. On the order of unimodular matrices modulo integers. *Acta Arith.*, 110(2):141–151, 2003.

[Kuz80] N. V. Kuznecov. The Petersson conjecture for cusp forms of weight zero and the Linnik conjecture. Sums of Kloosterman sums. *Mat. Sb. (N.S.)*, 111(153)(3):334–383, 479, 1980.

[L'E94] P. L'Ecuyer. Uniform random number generation. *Ann. Oper. Res.*, 53:77–120, 1994. Simulation and modeling.

[Leh76] D. H. Lehmer. Incomplete Gauss sums. *Mathematika*, 23(2):125–135, 1976.

[Li96] W. C. Winnie Li. *Number Theory with Applications.* Number 7 in Series on University Mathematics. World Scientific Publishing Co., River Edge, NJ, 1996.

[Lox83] J. H. Loxton. The graphs of exponential sums. *Mathematika*, 30(2):153–163 (1984), 1983.

[Maa49] H. Maass. Über eine neue Art von nichtanalytischen automorphen Funktionen und die Bestimmung Dirichletscher Reihen durch Funktionalgleichungen. *Math. Ann.*, 121:141–183, 1949.

[Mai85] H. Maier. Primes in short intervals. *Michigan Math. J.*, 32(2):221–225, 1985.

[Miy06] T. Miyake. *Modular forms.* Springer Monographs in Mathematics. Springer-Verlag, Berlin, english edition, 2006. Translated from the 1976 Japanese original by Yoshitaka Maeda.

[Mol10] R. A. Mollin. *Advanced number theory with applications*. Discrete Mathematics and its Applications (Boca Raton). CRC Press, Boca Raton, FL, 2010.

[Mon94] H. L. Montgomery. *Ten lectures on the interface between analytic number theory and harmonic analysis*, volume 84 of *CBMS Regional Conference Series in Mathematics*. Published for the Conference Board of the Mathematical Sciences, Washington, DC, 1994.

[Mot96] Y. Motohashi. On Kuznetsov's trace formulae. In *Analytic number theory, Vol. 2 (Allerton Park, IL, 1995)*, volume 139 of *Progr. Math.*, pages 641–667. Birkhäuser Boston, Boston, MA, 1996.

[Mot97] Y. Motohashi. *Spectral theory of the Riemann zeta-function*, volume 127 of *Cambridge Tracts in Mathematics*. Cambridge University Press, Cambridge, 1997.

[MV73] H. L. Montgomery and R. C. Vaughan. The large sieve. *Mathematika*, 20:119–134, 1973.

[Nie90] H. Niederreiter. Statistical independence properties of pseudorandom vectors produced by matrix generators. *J. Comput. Appl. Math.*, 31(1):139–151, 1990. Random numbers and simulation (Lambrecht, 1988).

[Now08a] W. G. Nowak. The lattice point discrepancy of a torus in $\mathbb{R}^3$. *Acta Math. Hungar.*, 120(1-2):179–192, 2008.

[Now08b] W. G. Nowak. On the lattice discrepancy of bodies of rotation with boundary points of curvature zero. *Arch. Math. (Basel)*, 90(2):181–192, 2008.

[ORW99] A. Odlyzko, M. Rubinstein, and M. Wolf. Jumping champions. *Experiment. Math.*, 8(2):107–118, 1999.

[Pet02] M. Peter. Lattice points in convex bodies with planar points on the boundary. *Monatsh. Math.*, 135(1):37–57, 2002.

[Rab13] D. Raboso. When the modular world becomes non-holomorphic. To appear in *Contemporary Mathematics*, 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.

[Rog05] K. M. Rogers. Sharp van der Corput estimates and minimal divided differences. *Proc. Amer. Math. Soc.*, 133(12):3543–3550, 2005.

[Ros00] H. Roskam. A quadratic analogue of Artin's conjecture on primitive roots. *J. Number Theory*, 81(1):93–109, 2000.

[Row08] E. S. Rowland. A natural prime-generating recurrence. *J. Integer Seq.*, 11(2):Article 08.2.8, 13, 2008.

[Sar82] P. Sarnak. Class numbers of indefinite binary quadratic forms. *J. Number Theory*, 15(2):229–247, 1982.

[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.

[Sel63] A. Selberg. Discontinuous groups and harmonic analysis. In *Proc. Internat. Congr. Mathematicians (Stockholm, 1962)*, pages 177–189. Inst. Mittag-Leffler, Djursholm, 1963.

[Shi71] G. Shimura. *Introduction to the arithmetic theory of automorphic functions*. Publications of the Mathematical Society of Japan, No. 11. Iwanami Shoten, Publishers, Tokyo, 1971. Kanô Memorial Lectures, No. 1.

[Sho92] V. Shoup. Searching for primitive roots in finite fields. *Math. Comp.*, 58(197):369–380, 1992.

[SS58] A. Schinzel and W. Sierpiński. Sur certaines hypothèses concernant les nombres premiers. *Acta Arith. 4 (1958), 185–208; erratum*, 5:259, 1958.

[Ste69] P. J. Stephens. An average result for Artin's conjecture. *Mathematika*, 16:178–188, 1969.

[Tit34] E. C. Titchmarsh. On epstein's zeta-function. *Proceedings of the London Mathematical Society*, s2-36(1):485–500, 1934.

[TMF00] G. Tenenbaum and M. Mendès France. *The prime numbers and their distribution*, volume 6 of *Student Mathematical Library*. American Mathematical Society, Providence, RI, 2000. Translated from the 1997 French original by Philip G. Spain.

[vdC21] J. G. van der Corput. Zahlentheoretische Abschätzungen. *Math. Ann.*, 84(1-2):53–79, 1921.

[vdC22] J. G. van der Corput. Verschärfung der Abschätzung beim Teilerproblem. *Math. Ann.*, 87(1-2):39–65, 1922.

[Ven90] A. B. Venkov. *Spectral theory of automorphic functions and its applications*, volume 51 of *Mathematics and its Applications (Soviet Series)*. Kluwer Academic Publishers Group, Dordrecht, 1990. Translated from the Russian by N. B. Lebedinskaya.

[Wat44] G. N. Watson. *A Treatise on the Theory of Bessel Functions*. Cambridge University Press, Cambridge, England, 1944.

[Wey16] H. Weyl. Über die Gleichverteilung von Zahlen mod. Eins. *Math. Ann.*, 77(3):313–352, 1916.

Índice alfabético