Departamento de Matemáticas
Facultad de Ciencias
Universidad Autónoma de Madrid

Cuestiones de la Aritmética y del Análisis Armónico

Adrián Ubis Martínez

Tesis doctoral dirigida por Fernando Chamizo Lorente

Madrid, junio de 2006

A mis padres.
A María.

Prólogo

Esta memoria contiene el estudio de varios problemas matemáticos de carácter diverso estructurados en tres capítulos, y que podríamos encuadrar en las áreas de la Teoría de Números y del Análisis Armónico.

Pero, ¿qué quiere decir que un problema está en una u otra área? Podemos querer expresar que se plantea de manera natural en el seno de una teoría, o bien que los métodos usados en su solución pertenecen a determinado tipo de razonamientos.

Como cualquiera que haya trabajado en matemáticas sabe, estas dos formas de entender la pregunta no siempre coinciden, lo cuál es natural, porque una teoría crece en parte gracias a cuestiones que escapan a ella. La única esperanza de ir más allá es usar todas las herramientas a nuestro alcance. Los problemas que vamos a resolver en este texto son un ejemplo de ello.

En el capítulo 1 tratamos series de Fourier con frecuencias en las k-potencias, que son funciones de comportamiento muy caótico. Su comprensión requerirá trabajar con sumas de Gauss, desigualdades de gran criba y ondículas, cosas que en apariencia nada tienen que ver con la regularidad de una función.

El número de clases de un cuerpo cuadrático (o clases de formas), que es el tema del capítulo dos, es una cantidad fascinante que mide lo lejos que está su anillo de enteros de ser un dominio de factorización única. Sin embargo su comportamiento en media se puede entender, a través de la geometría hiperbólica, como un problema de puntos de retículo y por tanto controlar con instrumentos del análisis armónico, o mediante el uso de funciones L y las consiguientes sumas de caracteres.

Si nos dieran dos conjuntos pequeños de enteros A y C, es fácil decidir si existe un conjunto B de forma que las sumas de los elementos de A y B dan exactamente los de C. Pero en el capítulo tres veremos que profundizar un poco más en este problema requiere técnicas del análisis de Fourier en cuerpos finitos y algunas construcciones geométricas.

La mayoría de los resultados de esta memoria están recogidos en los artículos de investigación [CCU, CU1, CU2, GU, Ubi]. Pero su historia, como ocurre siempre, ha sido más complicada. Recuerdo como si fuera ayer cuando, habiendo ido a Montreal a hacer una estancia breve de investigación con una beca FPU, estaba sentado con Andrew Granville esperando a que me propusiera un problema en el que trabajar durante esos cuatro meses. En vez

de esto, él me preguntó qué problemas me interesaban. Le dije que quería aprender cosas de funciones L, y me contestó que eso era demasiado general. Después le comenté que había estado leyendo algún artículo de B. Green e I. Ruzsa que Javier Cilleruelo me había recomendado, y fue entonces cuando me propuso el bonito problema sobre sumas de conjuntos. Para conjuntos grandes en seguida me di cuenta de que podían adaptarse los métodos de Green y Ruzsa. Para los pequeños, Granville me dijo que probablemente se podría tratar mediante fórmulas de recurrencia. A partir de entonces he estado trabajando esporádicamente en este problema, dando sólo pequeños pasos en su solución.

Cuando empecé a investigar con Fernando Chamizo, me propuso la cuestión de estudiar series de Fourier con frecuencias en polinomios de grado mayor que dos, extendiendo así el trabajo de S. Jaffard. Dijo que la fórmula de Poisson servía para tratar la función cerca de los racionales y después, los irracionales podían entenderse a partir de ese caso más sencillo. Por mi torpeza con las herramientas del análisis de Fourier me costó un tiempo entender bien cómo esto podía llevarse a cabo. Al final conseguimos controlar la función muy cerca de los racionales, pero todavía estábamos lejos de lo hecho en el caso de grado dos por Jaffard. En un principio no entendí completamente su artículo, en parte debido a mi desconocimiento de la transformada de ondículas. Aunque al final he visto que las ondículas no son totalmente necesarias, me han ayudado a entender realmente la dimensión del tema y a dar una solución parcial.

En el problema del número de clases, ha sido muy bonito compartir las inquietudes de Gauss, y entender los métodos de Siegel, Shintani y de Chamizo e Iwaniec y poder aplicarlos al caso de discriminantes positivos. Cuando finalmente logramos obtener una cota para el término de error, la pregunta natural era qué tamaño real cabía esperar para dicho término. Busqué en la literatura y vi que no había resultados para este problema, e intenté comprobar si se podían usar las fórmulas de sumación que habíamos obtenido para resolverlo, sin éxito. Más tarde comprendí que era posible tratar el término de error directamente a través de la fórmula analítica de Dirichlet para el número de clases. Esta segunda opción funcionó, probando una vez más la importancia de adaptarnos al problema que estamos tratando, de usar el lenguaje y los métodos adecuados.

Sólo me resta saldar la deuda contraída con todas las personas que han hecho posible este proyecto, agradeciéndoselo profundamente: en primer lugar a mi director, Fernando Chamizo. Decir que Fernando ha sobrepasado

el límite de lo que puede esperarse de un director de tesis, como persona y como matemático, sería quedarse corto. Él me ha enseñado, con paciencia y dedicación infinitas, todo lo que sé de teoría analítica de números. Ha soportado mis altibajos, apoyándome hasta el último momento (literalmente). Para mí es un ejemplo a seguir. En segundo lugar a Andrew, con el que he aprendido cómo se trabaja en matemáticas, gracias a su entusiasmo y firmeza. Sus ideas han hecho posible el capítulo tres de esta memoria. A Javier Cilleruelo, que me guió al principio y me hizo comprender que la teoría aditiva de números es más complicada y bonita de lo que pensaba. A los compañeros de despacho que me han padecido: Blanca que me ha enseñado tanto, Susi, Connie, Nati, Paloma, Jose, Charro y nuestras charlas de los jueves, Elías. Siento haberme perdido estos últimos dos meses con ellos. También a mis compañeras de comida Mari Luz y mi compatriota numérica Elena, y a los demás doctorandos: Ana que cuida de todos nosotros, Angélica, Liviu,... En general he sentido un gran ambiente en este departamento. A mi familia y amigos, que me han apoyado incondicionalmente; a María por su ayuda programando y por todo los demás; a Hakima y su familia, que me trataron como a un hijo; a Manolo por haberme mostrado el precioso mundo de la teoría de los números; a Paulo por esos cuatro meses de discusión continua; a Jorge por encargarse (brillantemente) de la ingrata labor de lectura de esta tesis, y por tranquilizarme.

Índice general

Capítulo 1

Series de Fourier polinómicas

1.1. Introducción

primer ejemplo publicado de una función continua y no diferenciable en ningún punto fue obtenido por Weierstrass:

$$f(x) = \sum_{n=0}^{\infty} a^n \cos(\pi b^n x),$$

con b un entero impar, $0 < a < 1$ y $ab > 1 + 3\pi/2$. Pero Weierstrass no creía que él fuese el primero en haber encontrado una función de este tipo, pues en 1873 envió una carta a Du Bois-Reymond diciendo que ya en 1861 Riemann había afirmado que la función

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

no era diferenciable en ningún punto.

En 1916 Hardy [Har] dio un gran paso en el estudio de la función de Riemann y comprendió perfectamente la suavidad de la función de Weierstrass. Lo hizo asociando a cualquier serie absolutamente convergente de la forma

$$f(\theta) = \Re \sum_{n=0}^{\infty} a_n e^{in\theta}$$

la función armónica

$$F(r, \theta) = \Re \sum_{n=0}^{\infty} a_n r^n e^{in\theta}.$$

Demostró que la suavidad de f se puede medir a través de la derivada en θ de F. De forma precisa, si para $0 < \delta < 1$ se cumple

$$f(\theta) - f(\theta_0) = o((\theta - \theta_0)^\delta)$$

entonces

$$\frac{\partial F(r, \theta_0)}{\partial \theta_0} = o\big((1-r)^{\delta-1}\big) \qquad r \to 1^-.$$

Esto lo consiguió demostrar escribiendo $F(r, \theta)$ como la integral,

$$F(r,\theta) = \Re \frac{1}{2\pi} \int_0^{2\pi} f(t)\left(\frac{2}{1 - re^{i(\theta - t)}} - 1\right) dt$$

usando el llamado núcleo de Poisson. Éstos fueron los comienzos de los espacios de Hardy. Así, para ver la regularidad de la función de Weierstrass, Hardy tuvo que estudiar el comportamiento de

$$\frac{\partial F(r,\theta)}{\partial \theta}\Big|_{\theta=\theta_0} = -\pi \sum_{n=0}^{\infty} (ab)^n r^{b^n} \operatorname{sen}(b^n \pi \theta)$$

cuando r está cerca de uno. A partir de aquí pudo probar, sin muchas dificultades, que cuando $ab > 1$, $0 < a < 1$ para la función de Weierstrass se cumple

$$f(x) - f(x_0) = \Omega(|x - x_0|^\delta) \qquad \delta = \frac{\log(1/a)}{\log b} < 1$$

para cualquier $x_0 \in \mathbb{R}$, deduciendo en particular su no diferenciabilidad.

En el caso de la función de Riemann, todo se reducía a controlar

$$\pi \sum_{n=1}^{\infty} r^{n^2} \cos(\pi n^2 x)$$

cuando r cerca de 1. Haciendo el cambio $r = e^{-\pi y}$, esto se convierte en

$$\theta(z) = \sum_{n \in \mathbb{Z}} e^{i\pi n^2 z} \qquad z = x + iy$$

cuando $y \to 0^+$. Pero ésta era la función theta de Jacobi, cuyo comportamiento podía estudiarse a la perfección debido a la ecuación funcional

$$\theta(z) = e^{\pi i/4} z^{-1/2} \theta(-1/z).$$

De hecho, combinándola con su periodicidad módulo 2 obtenemos

$$\theta(z) = e^{\pi i m/4}\theta(\gamma(z))q^{-1/2}(z - \frac{a}{q})^{-1/2}, \tag{1.1}$$

donde $\gamma(z) = (rz + s)/(qz - a)$, $r \equiv a \pmod 2$, $s \equiv q \pmod 2$ cumpliendo $ra + sq = -1$ y m es un entero que depende de γ.

Hardy y Littlewood [HL] vieron que para todo x_0 irracional existen infinitas convergentes a_n/q_n tales que podemos tomar $\gamma(z) = (r_n z + s_n)/(q_n z - a_n)$ de forma que $\Im\gamma(x_0 + i|x_0 - a_n/q_n|) > 1/2$. Pero en esta zona θ tiene un comportamiento estable, ya que $|\theta(z) - 1| < 1/2$ si $\Im z \geq 1/2$. Así

$$|\theta(x_0 + i|x_0 - a_n/q_n|)| \asymp q_n^{-1/2}|x_0 - a_n/q_n|^{-1/2},$$

y como $|x_0 - a_n/q_n| < 1/q_n^2$ (ver [CiCo]), tenemos que

$$\theta(x_0 + iy) = \Omega(y^{-1/4}).$$

Así, Hardy dedujo que la función de Riemann cumple

$$f(x) - f(x_0) = \Omega(|x - x_0|^{3/4})$$

para todo irracional.

Pero había una gran diferencia entre ambas funciones. Para la de Weierstrass se puede probar directamente (y así lo hizo Hardy) que

$$f(x) - f(x_0) = O(|x - x_0|^{\delta}) \qquad \delta = \log(1/a)/\log b < 1$$

para todo x_0, demostrando de esta manera que la regularidad es la misma en todo punto. Para la función de Riemann esto no se cumplía, y Hardy lo sabía. Por ejemplo, para ciertos racionales

$$f(x) - f(a/q) = \Omega(|x - a/q|^{1/2}),$$

lo que no ocurría para la mayoría de irracionales. Esto hacía ver que la regularidad de esta función variaba salvajemente de un punto a otro. Pero todavía quedaba por responder la cuestión de Riemann, ¿qué ocurría en los racionales que están en la órbita del 1 (los que pueden ponerse como $\gamma(1)$)? Para ellos (los de la forma a/q con a, q impares) se cumple

$$\theta(a/q + iy) \to 0,$$

lo que hace pensar que la función debe ser bastante regular en esos puntos. Parece que Hardy no se preocupó por esta cuestión, y en general por la regularidad de la función de Riemann, sólo por su irregularidad. Extrañamente, no fue hasta 50 años más tarde cuando en 1970 Joseph Gerver [Ger1, Ger2] cuando era un estudiante probó que en estos racionales, ¡la función sí es diferenciable y la derivada es siempre $-1/2$! Lo hizo agrupando las frecuencias en la fórmula para $f(a/q+h)-f(a/q)$ de acuerdo a los distintos restos módulo q, y estimando los términos principales de las funciones que quedaban. Un año después H. Queffelec [Que] analizó la diferenciabilidad de funciones del tipo

$$f(x)=\sum_{n=1}^{\infty}\frac{\operatorname{sen}(P(n)x)}{P(n)} \qquad P\in\mathbb{Z}[x]$$

pero sólo en algunos racionales. En 1972 A. Smith [Smi] simplificó la prueba de Gerver por medio de la fórmula de sumación de Poisson.

En 1978 E. Neuenschwander [Neu] realizó un estudio histórico sobre el conocimiento que Riemann realmente tenía sobre esta función. De él se desprende que Riemann probablemente conocía la diferencia entre el comportamiento de la función en racionales e irracionales. Después de todo, es natural interpretar el candidato a derivada en a/q

$$\pi\sum_{n=1}^{\infty}\cos(\pi n^2\frac{a}{q})$$

como $\xi(0)$, donde $\xi(s)$ es la extensión meromorfa de

$$\xi(s)=\pi\sum_{n=1}^{\infty}\cos(\pi n^2\frac{a}{q})n^{-s} \qquad \Re s>1.$$

Se puede probar (ver teorema 1.14) que efectivamente en los racionales en los que la derivada existe su valor es $\xi(0)$, y la derivada va a existir precisamente en los racionales en los que $\xi(s)$ no tiene un polo en $s=1$.

En 1991 J. J. Duistermaat [Dui] precisó el comportamiento de f cerca de los racionales, usando su resultado para estudiar la irregularidad en los irracionales y la regularidad en casi todo punto. Comenzó con la expresión

$$f(x)-f(x_0)=\int_C\frac{1}{2}(\theta(z)-1)dz,$$

donde C es una curva suave que va de x_0 a x contenida en el semiplano superior $\mathbb{H}$. A partir de aquí y de (1.1) obtuvo una fórmula que expresa la autosemejanza de la función de Riemann:

$$f(x) = f(\frac{a}{q}) + e^{\frac{i\pi}{4}m} q^{-\frac{1}{2}} (x - \frac{a}{q})^{\frac{1}{2}} - \frac{1}{2}(x - \frac{a}{q}) + e^{\frac{i\pi}{4}m} q^{\frac{3}{2}} (x - \frac{a}{q})^{\frac{3}{2}} f(\gamma(x)) + \psi_{a/q}(x)$$

dónde $\psi_{a/q}(x)$ es diferenciable y $\psi_{a/q}(a/q) = 0$. De aquí pudo deducir cómo se comportaba f cerca de los racionales, y tomando a/q como las convergentes del punto x_0 demostró

$$f(x) - f(x_0) = \Omega(|x - x_0|^{\frac{1}{2} + \frac{1}{2r}}) \tag{1.2}$$

si x_0 satisface $|x_0 - a_n/q_n| = O(q_n^{-r})$ donde a_n/q_n son sus convergentes. Esto último había sido implícitamente obtenido por Hardy y Littlewood en [HL]. Duistermaat también demostró a partir de su fórmula que

$$f(x) - f(x_0) = O(|x - x_0|^{\frac{3}{4}(1 - r(r-2))}), \tag{1.3}$$

para x_0 satisfaciendo $\liminf_n |x_0 - a_n/q_n| q_n^r > 0$. Ésta era la primera vez que alguien mostraba la regularidad de ciertos puntos no racionales. En particular (1.2) y (1.3) prueban que para casi todo punto el exponente Hölder es exactamente $3/4$, pero cuando $r > 1 + 2/\sqrt{3}$ esta cota no da ninguna información, pues sabemos de forma directa que $f \in C^{1/2}(\mathbb{R})$. Luego para ciertos rangos estamos perdiendo información.

En 1986 P. G. Lemarié e Y. Meyer [LM] caracterizaron la pertenencia de funciones $f : \mathbb{R} \to \mathbb{C}$ al espacio

$$C^\beta(\mathbb{R}) = \{f : \exists C > 0, |f(x) - f(y)| \leq C|x - y|^\beta \, \forall x, y \in \mathbb{R}\} \qquad 0 < \beta < 1$$

a través de condiciones de decaimiento de los coeficientes de la función con respecto a una base de ondículas. Tres años más tarde S. Jaffard [Jaf2] usó las mismas técnicas para caracterizar la regularidad local de funciones, es decir su pertenencia al espacio

$$C^\beta(x_0) = \{f : \exists P \in \mathbb{C}[x], f(x) - P(x - x_0) = O(|x - x_0|^\beta)\} \qquad \beta > 0$$

para $x_0 \in \mathbb{R}$. En 1991 M. Holschneider y Ph. Tchamitchian [HT] usaron esta caracterización sobre la función de Riemann, redescubriendo así el comportamiento en los racionales y la irregularidad en los irracionales. Pero no usaron esta caracterización para estudiar la regularidad en el resto de los puntos.

En 1993, F. Chamizo y A. Córdoba [CC1] demostraron que las gráficas de las funciones

$$f_\alpha(x) = \sum_{n=1}^{\infty} \frac{\operatorname{sen}(n^2 x)}{n^\alpha} \qquad 1 < \alpha \leq 2$$

eran conjuntos fractales de dimensión $9/4 - \alpha/2$. Lo hicieron usando la ecuación funcional aproximada de Hardy y Littlewood [HL] y propiedades de sumas de Gauss.

Fue Jaffard [Jaf1] en 1996 quien, habiendo leído el artículo de Duistermaat, consiguió averiguar la regularidad en todo punto de la función de Riemann mediante el uso de ondículas. Para expresar sus resultados y nuestro estudio posterior asociaremos a cada punto x_0 su exponente Hölder

$$\beta_f(x_0) = \sup\{\beta \geq 0 : f \in C^\beta(x_0)\}. \tag{1.4}$$

Jaffard se dio cuenta de que la regularidad de un punto para la función de Riemann depende exclusivamente de lo bien que se puede aproximar ese punto por racionales. Si $(a_n/q_n)_{n\in\mathbb{N}}$ es la sucesión de convergentes de x_0, y definimos r_n mediante la fórmula

$$|x_0 - \frac{a_n}{q_n}| = q_n^{-r_n},$$

entonces Jaffard consideró los espacios

$$E_r = \{x \in \mathbb{R} \setminus \mathbb{Q} : \operatorname{lím\,sup}_n r_n = r\}, \quad 2 \leq r \leq \infty, \tag{1.5}$$

y probó que

$$\beta_f(x_0) = \frac{1}{2} + \frac{1}{2r} \quad \text{si} \quad x_0 \in E_r. \tag{1.6}$$

Como

$$\mathbb{R} \setminus \mathbb{Q} = \bigcup_r E_r$$

esto daba el exponente Hölder para todo punto (conocida ya la regularidad de cada racional). Además, como la dimensión de Hausdorff de E_r es $2/r$ (ver [Fal2]), con esto consiguió el espectro de singularidades de la función f, que en general se define como

$$d_{\mathrm{H}}(\beta) = \dim_{\mathrm{H}}\{x \in \mathbb{R} : \beta_f(x) = \beta\}, \tag{1.7}$$

la función que asocia a β la dimensión Hausdorff de los puntos de exponente Hölder igual a β, siempre que exista algún punto con ese exponente. En el caso de que no existan se define $d_{\mathrm{H}}(\beta) = -\infty$. Para la función de Riemann demostró por tanto que

$$d_{\mathrm{H}}(\beta) = \begin{cases} 4\beta - 2 & \text{si } \frac{1}{2} \leq \beta \leq \frac{3}{4}, \\ 0 & \text{si } \beta = \frac{3}{2} \\ -\infty & \text{en otro caso.} \end{cases}$$

De esta forma vemos que f es una función multifractal (la función d_{H} es positiva en más de un punto) y la irregularidad de cada punto viene medida por lo bien que se aproxima por racionales.

Una vez entendida la función de Riemann, se paso al estudio de funciones más generales. En 1999 Chamizo y Córdoba [CC2] introdujeron las funciones

$$F_{\alpha,k}(x) = \sum_{n=1}^{\infty} \frac{e(n^k x)}{n^\alpha} \qquad k \in \mathbb{N},\ \alpha > 1.$$

Se tiene que $F_{\alpha,k} \in C^{(\alpha-1)/k}(\mathbb{R})$, pero para la mayoría de los puntos no se cumple que su exponente Hölder sea $(\alpha-1)/k$. Para $k > 2$, ya no se tenían las propiedades de la función modular $\theta(z)$ para comprender $F_{\alpha,k}$. A través del núcleo de Poisson, fueron capaces de caracterizar la diferenciabilidad en los racionales: $F_{k,k}$ es diferenciable en a/q, con a y q comprimos, si y sólo si $\tau(a/q) = 0$ donde

$$\tau(\frac{a}{q}) = \sum_{d=1}^{q} e(\frac{ad^k}{q}). \tag{1.8}$$

Estudiando estas sumas, pudieron decidir (excepto para un conjunto pequeño de q) la diferenciabilidad en a/q por medio de propiedades aritméticas de q. También estudiaron la regularidad de la función en otros puntos, usando acotaciones provenientes de la teoría de números para las sumas

$$\sum_{n \leq N} e(n^k x_0).$$

Estas acotaciones dependen de lo bien que se puede aproximar x_0 por racionales. Por ejemplo, obuvieron que si x_0 es un irracional cuadrático entonces

$$\beta(x_0) \geq \frac{\alpha - 1}{k} + 2^{1-k} k^{-1}.$$

Pero muchas otras cotas pueden deducirse de su análisis, como que para todo $\epsilon > 0$ existe un conjunto A_ϵ de dimensión de Hausdorff positiva tal que

$$\beta(x_0) \geq \frac{\alpha - 1}{k} + \epsilon$$

para todo $x_0 \in A_\epsilon$. En el mismo artículo, extendieron sus resultados de 1993 sobre la dimensión de Minkowski, sustituyendo la ecuación funcional aproximada de $F_{\alpha,2}$ por las técnicas de gran criba, nacidas en el seno de la teoría de números y capaces de encontrar cancelación cuando se tiene cierta independencia. Probaron que

$$\dim_{\mathrm{M}} F_{\alpha,k} = 2 + \frac{1}{2k} - \frac{\alpha}{k} \qquad \frac{k+1}{2} \leq \alpha \leq k + \frac{1}{2}. \tag{1.9}$$

En el 2001 F. Chamizo [Cha] vio que la irregularidad de la función de Riemann es una característica general de funciones del tipo

$$\sum_{m=1}^{\infty} m^{-\alpha} a_m e(mx)$$

donde $f(z) = \sum_m a_m e(mz)$ es una forma autormorfa clásica. Probó que el comportamiento general de la función en los racionales depende de si la forma es o no cuspidal (*cusp form*), y expresó la derivada en ellos a través de valores de funciones L asociadas a f. En [MS] S. Miller y W. Schmid extienden parte de estos resultados a distribuciones provenientes de formas automorfas más generales.

Finalmente, en 2003 Gerver [Ger3] volvió de nuevo al problema estudiando ahora la función $F_{\alpha,3}$ cerca de los racionales, y demostrando a través del estudio de las sumas $\tau(a/q)$ (usó un teorema de Patterson y Heath-Brown sobre la equidistribución de $\tau(a/q)$ en el caso cúbico) y de un teorema de aproximación diofántica de Erdős que $F_{\alpha,3}$ no es diferenciable en casi ningún punto para $\alpha < (\sqrt{97} - 1)/4 = 2{,}212\ldots$

En este capítulo vamos a extender parte del conocimiento sobre la función $F_{\alpha,2}$ a las funciones $F_{\alpha,k}$, aunque muchos resultados en realidad son extensibles a cualquier serie de Fourier cuyas frecuencias vengan dadas por un polinomio y cuyos coeficientes decaigan asintóticamente como una potencia negativa. Parte de los resultados expuestos en este capítulo están contenidos en [CU2]. Para simplificar, a partir de ahora denotaremos

$$F(x) = \sum_{n=1}^{\infty} n^{-\alpha} e(n^k x).$$

En la primera sección estudiaremos las sumas $\tau(a/q)$ y otras sumas relacionadas, que necesitaremos controlar para comprender la regularidad de F.

En la segunda veremos de forma precisa el comportamiento de F muy cerca de los racionales, y en particular deduciremos la regularidad de la función en ellos a través del siguiente resultado

Teorema 1.1. *Para a/q fracción irreducible y $h > 0$ se cumple que*

$$F(\frac{a}{q}+h) = F(\frac{a}{q}) + Aq^{-1}\tau(\frac{a}{q})h^{\frac{\alpha-1}{k}} + 2\pi i\zeta_{\frac{a}{q}}(\alpha-k)h + T(h^{-\frac{1}{k}})h^{\frac{\alpha-1/2}{k-1}}$$

con A la constante definida en (1.20), T una función acotada pero oscilante (que depende de a, q, α y k) y $\zeta_{a/q}(s)$ la extensión meromorfa de la función definida en $\Re s > 1$ mediante

$$\sum_{n=1}^{\infty} e(n^k\frac{a}{q})n^{-s}.$$

De los resultados de la primera sección y del teorema 1.1 deduciremos que

Teorema 1.2. *Para todo racional a/q, con a, q coprimos, se cumple que*

$$\beta_F(\frac{a}{q}) = \frac{\alpha-1}{k}$$

si existe $p^\delta \parallel q$ tal que $(k, p-1) = 1$ y $\delta \equiv 1 \pmod k$. En otro caso

$$\beta_F(\frac{a}{q}) = \frac{\alpha-1/2}{k-1}$$

y F es diferenciable en a/q si y sólo si $\alpha > k - 1/2$, con

$$F'(a/q) = 2\pi i\zeta_{a/q}(\alpha-k).$$

La regularidad de la función en los irracionales se puede controlar aproximándolos por racionales y viendo el comportamiento de la función T al variar h y q. Pero la función T a su vez depende de sumas de la forma

$$S_M(\frac{a}{q}) = \sum_{m\le M}\sum_{d=1}^{q} e(\frac{ad^k+md}{q}),$$

que serán nuestro objeto de estudio en la sección tercera. Probaremos que estas sumas están acotadas por $(Mq)^{1/2+\epsilon}$ uniformemente en $M \leq q$ para la mayoría de los a. El resultado preciso (ver proposición 1.22) es

$$\frac{1}{q}\sum_{a=1}^{q} \sup_{M\leq N} |S_M(\frac{a}{q})|^2 \ll (Nq)^{1+\epsilon} \qquad \epsilon > 0, \tag{1.10}$$

una versión discreta del teorema de Kolmogorov-Plessner-Seliverstov (ver [Zyg]) para series de Fourier en L^2.

En la sección cuarta expondremos la caracterización de regularidad local a través de la transformada continua de ondículas y lo usaremos para ver la relación entre la regularidad de las funciones $F_{\alpha,k}$: se cumple que para cada $x_0 \in \mathbb{R}$ la función

$$\beta_{F_{\alpha,k}}(x_0) - \frac{\alpha}{k} \tag{1.11}$$

crece en α. Además, daremos una caracterización de la dimensión de Minkowski para la gráfica de una función continua en términos de su transformada continua de ondículas. Finalmente extenderemos el rango en el que es válida la fórmula (1.9) a

$$\dim_{\mathrm{M}} F = 2 + \frac{1}{2k} - \frac{\alpha}{k} \qquad \frac{k+2}{4} \leq \alpha \leq k + \frac{1}{2}. \tag{1.12}$$

En la última sección usaremos los resultados de secciones anteriores para estudiar la regularidad en los irracionales. Primero obtenemos un resultado uniforme: para cada $r \geq 2$ y todo punto $x \in E_r$ se cumple (para $\alpha < k-1$ en el caso de la cota superior) que

$$\frac{\alpha-1}{k} + 2^{1-k}\,\mathrm{mín}(\frac{1}{k}, \frac{1}{2(r-1)}) \leq \beta_F(x) \leq \frac{\alpha}{k-1}.$$

Después veremos la regularidad de F en casi todo punto de E_r. Se cumple

Teorema 1.3. *Para todo $r \geq 2$:*

i) En casi todo punto x de E_r (con la medida $\mathcal{H}^{2/r}$) tenemos

$$\beta_F(x) \geq \mathrm{mín}\,\big(\frac{\alpha-1/2}{k}, \frac{\alpha-1}{k} + \frac{1}{2r}\big).$$

ii) Si $r \geq k$, existe un subconjunto $E_{r,0}$ en E_r de medida positiva tal que para todo $x \in E_{r,0}$

$$\beta_F(x) \geq \frac{\alpha - 1/2}{k}. \tag{1.13}$$

iii) Si $r \geq k$, existe un subconjunto $E_{r,1}$ en E_r de medida positiva tal que para todo $x \in E_{r,1}$

$$\beta_F(x) = \frac{\alpha - 1}{k} + \frac{1}{2r}. \tag{1.14}$$

Este resultado por una parte es una generalización de lo que se obtiene con el Teorema Fundamental del Cálculo para $r = 2$, y por otra prueba que F es una función multifractal. Pero veremos que la regularidad de un punto, en contraste con el caso $k = 2$, no sólo depende de lo bien que se pueda aproximar por racionales sino sobre todo de por qué tipo de racionales es aproximable. Los racionales de la forma a/q con q un producto de k-potencias de primos representan el caso extremo y nos dan

Teorema 1.4. *Para todo $r \geq 2$, existe $D_r \subset E_r$ tal que*

$$\beta_F(x) = \frac{\alpha - 1}{k} + \frac{1}{kr} \qquad \textit{para todo} \quad x \in D_r$$

con

$$1 + \frac{1}{2k} \leq \dim_{\mathrm{H}} D_r \leq 1 + \frac{1}{k}.$$

Este teorema nos ofrece una cota inferior para el espectro de singularidades

$$d_{\mathrm{H}}(\beta) \geq k(1 + \frac{1}{2k})(\beta - \frac{\alpha - 1}{k}) \qquad \beta \in (\frac{\alpha - 1}{k}, \frac{\alpha - 1/2}{k})$$

Si pudiéramos probar que realmente $\dim_{\mathrm{H}} D_r = (1 + k^{-1})/r$ (se cumple que $\dim_{\mathrm{M}} D_r = (1 + k^{-1})/r$) esta cota se mejoraría hasta

$$d_{\mathrm{H}}(\beta) \geq k(1 + \frac{1}{k})(\beta - \frac{\alpha - 1}{k}) \qquad \beta \in (\frac{\alpha - 1}{k}, \frac{\alpha - 1/2}{k}),$$

que correspondería a lo que esperamos para la función F en ese rango.

Además, en los puntos x en los que hemos probado que $\beta_F(x) > 1$ se cumple

$$F'(x) = \lim_{n \to \infty} \zeta_{a_n/q_n}(\alpha - k),$$

donde el límite se toma sobre las convergentes de x.

1.2. Sumas completas

Veremos que en el estudio de la regularidad de la función F juegan un papel importante las sumas trigonométricas

$$\tau_m(\frac{a}{q}) = \sum_{d=1}^{q} e(\frac{ad^k + md}{q}) \qquad (a,q) = 1,\ m \in \mathbb{Z}$$

El caso especial $\tau_0 = \tau$ es la suma considerada en la introducción. Vamos a comenzar exponiendo algunos resultados conocidos (ver [Vau]) para estas sumas

Lema 1.5. *Sean q_1, q_2 números naturales comprimos. Entonces*

$$\tau_m(\frac{a}{q_1 q_2}) = \tau_m(\frac{aq_2^{k-1}}{q_1})\tau_m(\frac{aq_1^{k-1}}{q_2}).$$

Demostración: Por el algoritmo de Euclides, todo número entero u, con $1 \le u \le q$ se puede escribir de forma única como

$$u = Aq_1 + Bq_2 \qquad 1 \le A \le q_2,\ 1 \le B \le q_1.$$

Así, el lema se sigue de la identidad

$$e(\frac{au^k + mu}{q_1 q_2}) = e(\frac{aq_2^{k-1}B^k + mB}{q_1})e(\frac{aq_1^{k-1}A^k + mA}{q_2}).$$

□

La suma τ se comporta de forma especial cuando q es primo

Lema 1.6. *Sea q primo. Entonces*

$$\tau(\frac{a}{q}) = \sum_{\chi \in G} \overline{\chi}(a)\tau_\chi. \tag{1.15}$$

donde G es el grupo de caracteres módulo q de orden que divida a $(k, q-1)$ y τ_χ la suma de Gauss

$$\tau_\chi = \sum_{d=1}^{q} \chi(d)e(\frac{d}{q}).$$

Como $|\tau_\chi| = q^{1/2}$ para cualquier carácter no principal, entonces

$$|\tau(a/q)| \le kq^{\frac{1}{2}}.$$

Demostración: Se cumple la igualdad

$$|\{1 \le n \le q : n^k = m\}| = \sum_{\chi \in G} \chi(m).$$

Por tanto

$$\tau(\frac{a}{q}) = \sum_m (\sum_{\chi \in G} \chi(m)) e(\frac{am}{q}) = \sum_{\chi \in G} \sum_{m=1}^{q} \chi(m) e(\frac{am}{q}).$$

Teniendo en cuenta la biyección $x \mapsto a^{-1}x$ de $\mathbb{F}_q$ en $\mathbb{F}_q$ obtenemos (1.15). Para demostrar el resto del lema

$$|\tau_\chi|^2 = \sum_{1 \le d,j \le q-1} \chi(d)\overline{\chi(j)} e(\frac{d-j}{q})$$

y haciendo el cambio $d \mapsto jd$,

$$|\tau_\chi|^2 = \sum_{1 \le d \le q-1} \chi(d) \sum_{1 \le j \le q-1} e(\frac{(d-1)j}{q}) = q.$$

□

Cuando q es una potencia suficientemente alta de un primo, la suma $\tau(a/q)$ se comporta de una forma regular. De forma precisa, se cumple el siguiente resultado

Lema 1.7. *Sea $q = p^d$, p primo, $p^\delta \parallel k$ y*

$$d \ge \begin{cases} 2 & si\ \delta = 0 \\ \delta + 2 & si\ \delta > 0,\ p > 2 \\ \delta + 3 & si\ \delta > 0,\ p = 2. \end{cases}$$

Entonces se satisface

$$\tau(a/p^d) = \begin{cases} p^{d-1} & si\ d \le k \\ p^{k-1}\tau(a/p^{d-k}) & si\ d > k. \end{cases}$$

Demostración: Cualquier residuo módulo p^d podemos representarlo de forma única como

$$bp^{d-\delta-1} + c \qquad \text{con} \qquad 1 \le b \le p^{\delta+1}, \qquad 1 \le c \le p^{d-\delta-1}.$$

Además,

$$(bp^{d-\delta-1}+c)^k \equiv c^k + kc^{k-1}bp^{d-\delta-1} \pmod{p^d}$$

si d cumple las condiciones del enunciado. Por tanto

$$\tau(\frac{a}{q}) = \sum_{c=1}^{p^{d-\delta-1}} e(\frac{c^k}{p^d}) \sum_{b=1}^{p^{\delta+1}} e(\frac{k}{p^\delta}\frac{c^{k-1}b}{p}) = p^{\delta+1} \sum_{\lambda=1}^{p^{d-\delta-2}} e(\frac{p^k}{p^d}\lambda^k)$$

lo que demuestra el lema teniendo en cuenta que $\delta + 2 \leq k$. □

Estos resultados nos dan una cota superior óptima para $\tau(a/q)$

Lema 1.8. *Se cumple*

$$\tau(\frac{a}{q}) \ll q^{1-\frac{1}{k}}.$$

para cualquier a coprimo con q.

Demostración: Por el lema 1.5 podemos escribir

$$\tau(\frac{a}{q}) = \tau(\frac{aq_2^{k-1}}{q_1})\tau(\frac{aq_1^{k-1}}{q_2})$$

siendo q_1 el producto de los primos que dividen a q con exponente mayor que 1 y que también dividen a k. Por los lemas 1.6 y 1.7 se cumple

$$\tau(\frac{aq_1^{k-1}}{q_2}) \ll q_2^{1-\frac{1}{k}}$$

y también

$$\tau(\frac{aq_2^{k-1}}{q_1}) \leq k^2 q_1^{1-\frac{1}{k}}.$$

□

Ahora, usando los lemas anteriores, vamos a estudiar para qué valores de a y q se anula la suma $\tau(a/q)$. Esta proposición completa los lemas 4.6 y 4.7 de [CC2]

Proposición 1.9. *$\tau(a/q) = 0$ si y sólo si existe $p^\delta \parallel q$ tal que $(k, p-1) = 1$ y $\delta \equiv 1 \pmod{k}$.*

Demostración: Por el lema 1.5 podemos escribir

$$\tau(\frac{a}{q}) = \prod_{p^d \| q} \tau(\frac{a_p}{p^d})$$

con $(a_p, p) = 1$. Por tanto reducimos la prueba de la proposición al caso $q = p^d$. Además, por el lema 1.7 sólo es necesario considerar el caso $1 \leq d \leq k$, porque siempre $k \geq \delta + 2$.

Si $d = 1$, como $e(a/p)$ es raíz del polinomio irreducible $x^{p-1}+x^{p-2}+\ldots+1$ la única forma de que $\tau(a/p)$ se anule es que el homomorfismo

$$\mathbb{F}_p \to \mathbb{F}_p$$

$$n \mapsto n^k$$

sea automorfismo, y esto ocurre sólo cuando $(k, p-1) = 1$.

Si $1 < d \leq k$ y $\tau(a/p^d) = 0$ para cierto $(a, p) = 1$, aplicando los automorfismos del grupo de Galois de $\mathbb{Q}(e(1/p^d))$, deducimos que

$$\tau(a/p^d) = 0 \qquad \text{para todo } a, (a, p) = 1.$$

Por otra parte

$$\sum_{(a,p)=1} \tau(\frac{a}{p^d}) = \sum_{n=1}^{p^d} \sum_{(a,p)=1} e(\frac{n^k a}{p^d}) = p^{2d-2},$$

contradicción. Luego $\tau(a/p^d) \neq 0$ cuando $1 < d \leq k$ y la proposición queda demostrada. □

Veamos unos casos especiales en los que τ_m se puede evaluar.

Lema 1.10. *Sea p primo, $(a, p) = 1$ con $(p, k) = 1$. Sean $j, d \in \mathbb{Z}$, $j \geq 0$, $1 \leq d \leq k$ y $p^{j(k-1)+d-1} \mid m$. Entonces*

$$\tau_m(\frac{a}{p^{jk+d}}) = p^{j(k-1)+d-1}.$$

Demostración:

$$\tau_m(\frac{a}{p^{jk+d}}) = \sum_{u=1}^{p^{jk+d}} e(\frac{au^k + mu}{p^{jk+d}})$$

Podemos representar todo residuo módulo p^{jk+d} en la forma

$$u = Ap^{jk+d-1} + B \qquad 1 \le A \le p,\ 1 \le B \le p^{jk+d-1}$$

por tanto

$$\begin{aligned}\tau_m(\frac{a}{p^{jk+d}}) &= \sum_B e(\frac{mB}{p^{jk+d}})e(\frac{aB^k}{p^{jk+d}}) \sum_A e(\frac{kB^{k-1}A}{p}) \\ &= p \sum_{C=1}^{p^{jk+d-2}} e(\frac{mC}{p^{jk+d-1}})e(\frac{ap^kC^k}{p^{jk+d}}).\end{aligned}$$

Si $j = 0$ esto es p^{d-1}, y si $j > 0$ es igual a

$$p^{k-1}\tau_{mp^{-k+1}}(\frac{a}{p^{(j-1)k+d}}).$$

Esta igualdad nos permite demostrar el lema inductivamente. □

Para el estudio que realizaremos en la sección tercera de las sumas $\sum_{m\le M} \tau_m$ necesitaremos controlar las siguiente suma doble

Lema 1.11. *Sea $n \in \mathbb{N}$ y*

$$\varrho_n(q) = \sum_{m=1}^{q} |\sum_{a=1}^{q} \tau_n(\frac{a}{q})\overline{\tau_m(\frac{a}{q})}|.$$

Se cumple que ϱ_n es una función multiplicativa. Además, para $q = p^v$ con p primo, $(p,k) = 1$, $v = jk + d$, $1 \le d \le k$ tenemos

$$\varrho_n(p^v) = \begin{cases} 2(k, p-1)(p^{2v} - p^{2v-j-1}) & \text{si } p^{v-j-1} \nmid n \\ 2(k, p-1)(p^{2v} - p^{2v-j-1}) + p^{3v-j-1} & \text{en otro caso.} \end{cases}$$

Demostración: Por el lema 1.5 vemos que

$$\varrho_n(q) = \sum_{m=1}^{q} \prod_{p^v \| q} |\sum_{a=1}^{p^v} \tau_n(\frac{a}{p^v})\overline{\tau_m(\frac{a}{p^v})}| = \prod_{p^v \| q} \big(\sum_{m=1}^{p^v} |\sum_{a=1}^{p^v} \tau_n(\frac{a}{p^v})\overline{\tau_m(\frac{a}{p^v})}|\big),$$

lo que prueba la multiplicatividad de ϱ_n. Por otra parte

$$\varrho_n(q) = q \sum_{m=1}^{q} | \sum_{\substack{1\le c,d\le q \\ c^k \equiv d^k \pmod q}} e(\frac{nc - md}{q})|.$$

Si $q = p^v$ dividimos la suma en dos partes $\varrho_n(p^v) = S_1 + S_2$ con

$$\begin{aligned} S_1 &= p^v \sum_{\Omega^k \equiv 1 \,(\mathrm{mod}\, p^v)} \sum_{m=1}^{p^v} | \sum_{\substack{1 \le c \le p^v \\ (c,p)=1}} e(\frac{(n-\Omega m)c}{p^v})| \\ &= p^v (k, p-1) \sum_{N=1}^{p^v} | \sum_{\substack{1 \le c \le p^v \\ (c,p)=1}} e(\frac{Nc}{p^v})| \\ &= p^v (k, p-1)(\phi(p^v) + (p-1)\frac{\phi(p^{jk+d})}{p-1}) \\ &= 2(k, p-1)\phi(p^v)p^v \end{aligned}$$

y

$$S_2 = p^v \sum_{m=1}^{p^v} | \sum_{\substack{1 \le c,d \le p^{v-1} \\ c^k \equiv d^k \,(\mathrm{mod}\, p^{v-k})}} e(\frac{nc-md}{p^{v-1}})|.$$

Repitiendo el proceso j veces, llegamos a que

$$\tau_n(p^v) = p^v \big[2(k, p-1)\big(\sum_{i=0}^{j} \phi(p^{v-i})\big) + \sum_{m=1}^{p^v} | \sum_{1 \le c,d \le p^{v-j-1}} e(\frac{nc-md}{p^{v-j-1}})|\big]$$

y esto nos da el resultado. □

1.3. Regularidad en los racionales

Vamos a ver que la fórmula de sumación de Poisson nos permite comprender bien $F(x)$ cuando

$$|x - \frac{a}{q}| < q^{-k},$$

y nos ayudará a entender el comportamiento de F en el rango $|x - a/q| < q^{-1-\epsilon}$, $\epsilon > 0$. Al aplicarla aparecerán las sumas τ_m estudiadas en la sección anterior, así como la función zeta definida por

$$\zeta_{a/q}(s) = \sum_{n=1}^{\infty} e(\frac{a}{q}n^k)n^{-s} \tag{1.16}$$

en el semiplano $\Re s > 1$. Separando en residuos módulo q y aplicando la fórmula de Poisson en progresiónes aritméticas podemos escribir

$$\zeta_{a/q}(s) = \frac{\tau}{q}(\int_0^1 \phi(x)x^{-s} + \frac{1}{s-1}) + \sum_{m\neq 0} \frac{\tau_m}{q} \int_0^\infty \phi(x)x^{-s}e(-\frac{m}{q}x)dx \qquad (1.17)$$

donde ϕ es cualquier función en $C_0^\infty((0,\infty])$ que valga 1 en $[1,\infty)$, y las integrales se entienden como integrales oscillatorias (ver [Hör]). Además esta representación es válida para todo $s \in \mathbb{C}$, dándonos la extensión meromorfa de $\zeta_{a/q}(s)$. Vemos que $\zeta_{a/q}$ tiene un polo en $s = 1$ cuando $\tau(a/q) \neq 0$.

Tras aplicar Poisson sobre la función F cerca de a/q, deberemos tratar con la transformada de Fourier de la distribución

$$g(x) = \frac{e(x^k) - 1 - 2\pi i x^k}{x^\alpha} \mathbb{I}_{(0,\infty)}(x).$$

Así pues vamos a comenzar estudiándola

Lema 1.12. *Existe una sucesión $(c_j)_{j=0}^\infty$ de números complejos dependientes de α y k tales que para $\lambda > 1$ y $n \in \mathbb{N}$ se cumple*

$$\widehat{g}(\lambda) = \lambda^{\alpha-1}\sum_{j=2}^n a_j\lambda^{-jk} + i^{1/2}\lambda^{-\frac{1}{2}-\frac{\alpha-1/2}{k-1}}e(-C\lambda^{\frac{k}{k-1}})\sum_{j=0}^n c_j\lambda^{-j\frac{k}{k-1}} + O_n(\lambda^{\alpha-n-1})$$

con $C = (1-1/k)k^{-1/(k-1)}$ y

$$a_j = \Gamma(jk-\alpha+1)(2\pi i)^{\alpha-1+(1-k)j}(j!)^{-1}.$$

Además

$$\widehat{g}(-\lambda) = \lambda^{\alpha-1}\sum_{j=2}^n \overline{a_j}\lambda^{-jk} + O(\lambda^{\alpha-n}).$$

Demostración: Dividimos la integral en dos partes

$$\widehat{g}(\lambda) = I(\psi) + I(\eta),$$

donde $\psi \in C_0^\infty([0,\infty))$, $\psi(x) = 1$ para $0 \leq x \leq 1$, $\eta = 1 - \psi$ y $I(f) = \widehat{gf}(\lambda)$. Desarrollando $u^\alpha g(u)$ en serie de potencias podemos escribir

$$I(\psi) = \sum_{j=2}^n \frac{(2\pi i)^j}{j!} I_{kj-\alpha}(\psi) + \int_0^\infty u^{n+1-\alpha}g_n(u)\psi(u)e(-\lambda u)du,$$

donde $g_n(u)$ es una función entera y

$$I_\beta(\psi) = \int_0^\infty x^\beta \psi(x) e(-\lambda x) dx = (2\pi\lambda)^{-\beta-1} \int_0^\infty x^\beta e^{-ix} dx - I_\beta(\eta).$$

Integrando por partes vemos que $I_\beta(\eta) \ll_{\beta,n} \lambda^{-n}$. Por el teorema de Cauchy y la definición de la función Γ podemos calcular la primera integral, obteniendo

$$I_\beta(\psi) = (2\pi i\lambda)^{-\beta-1}\Gamma(\beta+1) + O(\lambda^{-n}).$$

Finalmente integrando por partes $n+1-[\alpha]$ veces obtenemos

$$\int_0^\infty u^{n+1-\alpha} g_n(u)\psi(u)e(-\lambda u)du \ll \lambda^{\alpha-n-1}.$$

Por otra parte, integrando de nuevo por partes

$$I(\eta) = \int_0^\infty \eta(x)x^{-\alpha}e(x^k - \lambda x)dx + O(\lambda^{-n}).$$

Haciendo el cambio $x \to \lambda^{1/(k-1)}x$ tenemos

$$I(\eta) = \lambda^{-\frac{\alpha-1}{k-1}} \int u(x) e(\lambda^{\frac{k}{k-1}}(x^k - x))dx + O(\lambda^{-n})$$

con $u(x) = \eta(\lambda^{1/(k-1)}x)x^{-\alpha}$. Escribiendo u como suma de tres funciones de $C_0^\infty((0,\infty))$, está claro que podemos sustituir en la integral a u por una función $u_0 \in C_0^\infty((0,\infty))$ con soporte contenido en $(1/2k, 2)$ y $u_0 = u$ en $(1/k, 1)$, y de forma que al hacerlo sólo perdamos $O(\lambda^{-n})$. Ahora, aplicando fase estacionaria (ver Teorema 7.7.5 en [Hör]) conseguimos

$$I(\eta) = \lambda^{-\frac{\alpha-1}{k-1}} \frac{e(-C\lambda^{\frac{k}{k-1}})}{(-ik^2C\lambda^{\frac{k}{k-1}})^{1/2}} \sum_{j\le n} \widetilde{c_j}(\lambda^{\frac{k}{k-1}})^{-j} + O(\lambda^{-n-1})$$

donde $C = (1-1/k)k^{-1/(k-1)}$ y $\widetilde{c_j}$ son números que sólo dependen de α y k. En particular $\widetilde{c_0} = u(k^{-1/(k-1)}) = k^{\alpha/(k-1)}$.

El cálculo de $\widehat{g}(-\lambda)$ es igual, teniendo en cuenta que en este caso $\widehat{g\eta}(-\lambda) \ll \lambda^{-n}$, debido a que la derivada de $x^k - (-\lambda)x$ no se anula en $[0,\infty)$.

□

Al usar este resultado en el siguiente lema necesitaremos saber que cierta suma converge. Esto quedará asegurado por la desigualdad

$$\sum_{m\leq N} e(b(m+\theta)^{\frac{k}{k-1}}) \ll b^{\frac{1}{2}} N^{\frac{1}{2}+\frac{1}{2(k-1)}} \tag{1.18}$$

uniforme en $0 \leq \theta \leq 1$ y $b \geq 1$, que se deduce del lema de van Der Corput (ver [GK]). Ahora veremos dos resultados sobre el comportamiento de $F(a/q + h) - F(a/q)$ para $h > 0$. Podemos conseguir los equivalentes para $h < 0$ por la fórmula

$$F(a/q + h) - F(a/q) = \overline{F(-a/q - h) - F(-a/q)}. \tag{1.19}$$

Proposición 1.13. *Sea $x \in \mathbb{R}$. Para cualquier par de enteros a, q coprimos, tenemos que*

$$F(x) = F(\frac{a}{q}) + 2\pi i \zeta_{\frac{a}{q}}(\alpha - k)h + A\frac{\tau}{q}h^{\frac{\alpha-1}{k}} + h^{\frac{\alpha-1}{k}} \sum_{m\neq 0} \frac{\tau_m}{q}\, \widehat{g}\big(\frac{m}{qh^{1/k}}\big)$$

dónde $h = x - a/q > 0$ y

$$A = \big(\frac{i}{2\pi}\big)^{\frac{1-\alpha}{k}} \frac{1}{k}\Gamma(\frac{1-\alpha}{k}). \tag{1.20}$$

Demostración: Sea $\phi \in C_0^\infty((0,\infty])$ con $\phi = 1$ en $[1,\infty)$. Podemos escribir

$$F(x) - F(\frac{a}{q}) = \lim_{N\to\infty} S_N$$

$$S_N = \sum_{n\in\mathbb{Z}} \phi_N(n) e(\frac{an^k}{q}) \frac{e(n^k h) - 1}{n^\alpha}.$$

con $\phi_N \in C_0^\infty((0,\infty))$, $\phi_N(t) = 1$ para $1 \leq t \leq N$ y $\phi_N(t) = \phi(t)$ si $0 < t < 1$. Aplicando Poisson en progresiones aritméticas

$$S_N = \sum_{m\in\mathbb{Z}} \frac{\tau_m}{q} \int_0^\infty \phi_N(t) t^{-\alpha}(e(ht^k) - 1) e(-\frac{m}{q}t)dt$$

lo que podemos expresar como

$$S_N = D_N + \frac{\tau}{q}\int_0^\infty \phi_N(t)\frac{e(ht^k) - 1}{t^\alpha} + \sum_{m\neq 0} h^{\frac{\alpha-1}{k}} \frac{\tau_m}{q} \int_0^\infty \phi_N(h^{-\frac{1}{k}}t) g(t) e(-\frac{m}{qh^{1/k}}t)dt$$

donde

$$D_N = 2\pi i h \sum_{m\neq 0} \frac{\tau_m}{q} \int \phi_N(t) t^{k-\alpha} e(-\frac{m}{q}t) dt.$$

Gracias al lema 1.12 y a (1.18) podemos hacer tender N a infinito. Por (1.17) obtenemos

$$\lim_N D_N = 2\pi i h \zeta_{\frac{a}{q}}(\alpha - k) - 2\pi i h \frac{\tau}{q}(\frac{1}{\alpha - k - 1} + \int_0^1 \phi(t) t^{k-\alpha} dt).$$

Finalmente haciendo $\phi \to 1$ y teniendo en cuenta que

$$\int_0^\infty t^{-\alpha}(e(t^k) - 1) dt = A$$

hemos terminado. □

El resultado siguiente es una consecuencia directa de los dos resultados anteriores (teniendo en cuenta (1.18))

Teorema 1.14. *Sea $x \in \mathbb{R}$, $a, q \in \mathbb{Z}$ coprimos, $1 < \alpha < k+1$. Si $h = x - a/q$ entonces para $0 < h < q^{-k}$ y $n > \alpha$ se tiene la fórmula*

$$F(x) = F(\frac{a}{q}) + h^{\frac{\alpha-1}{k}} \frac{A\tau}{q} + \sum_{j=1}^{n} (2\pi i h)^j \zeta_{\frac{a}{q}}(\alpha - kj) + (qh)^\beta \sum_{j=0}^{n} c_j T_j(qh^{\frac{1}{k}}) + O((qh^{\frac{1}{k}})^n)$$

con

$$T_j(y) = y^{\frac{jk}{k-1}} \sum_{m=1}^{\infty} \frac{\tau_m}{q^{1/2}} e((my^{-1})^{\frac{k}{k-1}}) m^{-\frac{1}{2}-\beta-j\frac{k}{k-1}}$$

y

$$\beta = (\alpha - 1/2)/(k-1).$$

Este teorema permite controlar la regularidad de la función en los racionales. En particular deducimos

Corolario 1.15. *Sean α, k y a/q como en el teorema anterior. Entonces:*

i) Si $\tau \neq 0$ entonces $F \in C^{\frac{\alpha-1}{k}}(a/q)$ y $F \notin C^\delta(a/q)$ para $\delta > (\alpha - 1)/k$.

ii) Si $\tau = 0$ entonces $F \in C^{\frac{\alpha-1/2}{k-1}}(a/q)$ y $F \notin C^\delta(a/q)$ para $\delta > \frac{\alpha-1/2}{k-1}$.

iii) F es diferenciable en a/q si y sólo si $\tau = 0$ y $\alpha > k - 1/2$. En este caso

$$F'(\frac{a}{q}) = 2\pi i \zeta_{\frac{a}{q}}(\alpha - k).$$

Demostración: Teniendo en cuenta el Teorema 1.14 sólo hay que demostrar que F no es diferenciable en el caso $\alpha = k - 1/2$, $\tau = 0$. Esto se debe a que T_0 oscila. Para probarlo, tomamos $m_0 \neq 0$ tal que $\tau_{m_0} \neq 0$ (siempre es posible porque $\sum_{m=0}^{q} \tau_m = q$). Entonces

$$\int_Y^{2Y} T_0(y^{-1}) e(C(m_0 y)^{\frac{k}{k-1}}) dy = q^{-\frac{1}{2}} \tau_{m_0} m_0^{-\frac{1}{2}-\beta} Y + O(1).$$

Luego $\lim_{y\to\infty} T(y^{-1})$ no existe. □

Vemos que la la regularidad de la función va a depender de que τ se anule o no. Podemos caracterizar totalmente esta propiedad a partir de propiedades de q. Por el corolario anterior y la proposición 1.9 concluimos

Teorema 1.16. *Para todo racional a/q, con a, q coprimos, se cumple que*

$$\beta_F(x_0) = \frac{\alpha - 1}{k}$$

si existe $p^\delta \parallel q$ tal que $(k, p-1) = 1$ y $\delta \equiv 1 \pmod k$. En otro caso

$$\beta_F(x_0) = \frac{\alpha - 1/2}{k - 1}.$$

Como en la proposición 1.13, pero de manera más sencilla, se prueba

Proposición 1.17. *Sea $h = x - a/q > 0$ y $1 < \alpha < k$. Entonces*

$$F(x) = F(\frac{a}{q}) + A\frac{\tau}{q} h^{\frac{\alpha-1}{k}} + q^{-1} h^{\frac{\alpha-1}{k}} \sum_{m\neq 0} \tau_m \widehat{g_0}(\frac{m}{h^{1/k} q})$$

donde $g_0(x) = x^{-\alpha}(e(x^k) - 1)$.

Veamos que cuando h es pequeño con respecto a q^{-1}, realmente el término $Aq^{-1}h^{(\alpha-1)/k}$ es el principal en $F(a/q + h) - F(a/q)$.

Proposición 1.18. *Sea $k/2 < \alpha < k$ y $h > 0$. Entonces para todo $\epsilon > 0$ se tiene*

$$F(x) - F(\frac{a}{q}) = \frac{A\tau}{q} h^{\frac{\alpha-1}{k}} + O(h^{\frac{\alpha}{k}} q^{\frac{1}{2}+\epsilon}).$$

Demostración: Por el lema 1.12 vemos que $\widehat{g}_0(\lambda) \ll \lambda^{-\delta}$ con $\delta > 1$, y por la proposición 1.13 llegamos a

$$F(x) - F(\frac{a}{q}) = \frac{A\tau}{q} h^{\frac{\alpha-1}{k}} + \frac{h^{\frac{\alpha-1}{k}}}{q} O(\sum_{m\neq 0} |\tau_m| \operatorname{mín}(1, (\frac{|m|}{h^{1/k}q})^{-\delta}))$$

Se puede deducir de la hipótesis de Riemann para curvas sobre cuerpos finitos (ver [Vau]) la cota

$$\tau_m \ll (m,q) q^{\frac{1}{2}+\epsilon},$$

para todo $\epsilon > 0$, de donde se sigue la proposición. □

Con esta proposición podríamos hallar la regularidad encontrada por Jaffard para la función F en el caso $k = 2$ (ver (1.6)). No ocurre lo mismo cuando $k \geq 3$. En este caso no es suficiente con acotar la suma $\sum_{m\leq M} \tau_m$ controlando el tamaño de τ_m. En la siguiente sección vamos a ver que en esa suma se produce mucha cancelación, al menos para la mayoría de los racionales a/q.

1.4. Sumas incompletas

Como acabamos de ver, el término $\tau(a/q)$ determina en parte el comportamiento de la función F. Cuando q es primo, esta suma se comporta de manera irregular. Vamos a probar que para la mayoría de residuos a el tamaño de $\tau(a/q)$ esta cerca de $q^{1/2}$ exceptuando el caso $(k, q-1) = 1$, en el que τ se anula.

Proposición 1.19. *Sea $1 \leq N \leq q$, q primo y $l = (k, q-1) > 1$. Entonces se cumple*

$$\sum_{a\leq N} |\tau(\frac{a}{q})|^2 = l(q-1)N + O(l^2 q^{3/2} \log q).$$

Demostración: Comenzamos completando la suma

$$\begin{aligned} \sum_{a\leq N} |\tau(\frac{a}{q})|^2 &= \sum_{a=1}^{q} |\tau(\frac{a}{q})|^2 \sum_{s\leq N} \frac{1}{q} \sum_{r=1}^{q} e(\frac{(a-s)r}{q}) \\ &= \frac{1}{q} \sum_{r=1}^{q} \sum_{s\leq N} e(\frac{-sr}{q}) \sum_{a=1}^{q} e(\frac{ra}{q}) |\tau(\frac{a}{q})|^2. \end{aligned}$$

Usando (1.15) obtenemos

$$\sum_{a=1}^{q} |\tau(\frac{a}{q})|^2 = \sum_{\chi,\psi\in G} \tau_\chi \overline{\tau_\psi} \sum_{a=1}^{q} \overline{\chi(a)}\psi(a) = (q-1)lq$$

y para $r \neq q$

$$\begin{aligned} \sum_{a=1}^{q} e(\frac{ra}{q})|\tau(\frac{a}{q})|^2 &= \sum_{\chi,\psi\in G} \tau_\chi \overline{\tau_\psi} \sum_{a=1}^{q} \overline{\chi(a)}\psi(a)e(\frac{ra}{q}) \\ &= \sum_{\chi,\psi\in G} \chi(r)\overline{\psi(r)}\tau_\chi \overline{\tau_\psi}\tau_{\overline{\chi}\psi} \end{aligned}$$

Luego

$$\begin{aligned} |\sum_{a\leq N} |\tau(\frac{a}{q})|^2 - N(q-1)l| &\leq l^2 q^{1/2} \sum_{r=1}^{q-1} |\sum_{s\leq N} e(\frac{-sr}{q})| \\ &\leq l^2 q^{1/2} \sum_{r=1}^{q-1} |\operatorname{sen}(\pi\frac{r}{q})|^{-1} \end{aligned}$$

y el resultado se sigue de la equivalencia $\operatorname{sen} x \sim x$. □

Como consecuencia directa de esta proposición y del lema 1.6 obtenemos

Proposición 1.20. *Sea I un intervalo cerrado con $|I| < 1$. Dado $\epsilon > 0$ existe $C = C(\epsilon, k)$ tal que para todo primo $q > C|I|^{-2-\epsilon}$ con $(q-1,k) \neq 1$, se cumple*

$$|\{1 \leq a \leq q : \frac{a}{q} \in I, |\tau(\frac{a}{q})| \geq \frac{q^{1/2}}{2}\}| \geq \frac{q}{k}|I|.$$

Hemos comprendido ya (ver 1.17) que las sumas $\sum_m \tau_m f(m/Y)$ tienen mucha importancia para entender la irregularidad de la función. Vamos a ver que en ellas hay mucha cancelación para la mayoría de los residuos a. En la prueba vamos a usar una desigualdad de tipo gran criba, que ha sido utilizada con frecuencia en teoría de números. Es una generalización de la desigualdad de Bessel (ver [Dav2])

Lema 1.21. *Sea u un vector en un espacio euclídeo. Para cualquier conjunto de l vectores $v_1, v_2, \ldots, v_l$ se cumple la desigualdad*

$$\sum_{i=1}^{l} |\langle u, v_i\rangle|^2 \leq \left(\max_{1\leq i\leq l} \sum_{j\leq l} |\langle v_i, v_j\rangle| \right) \|u\|^2.$$

Vamos con el resultado principal de esta sección

Proposición 1.22. *Sea $f : [0, \infty] \to \mathbb{C}$ una función continua con transformada de Mellin integrable y que representa a f a través de la fórmula de inversión en $\Re s = 1/2$. Definimos*

$$S^*_{a/q}(x) = \sup_{Y \in [x,2x]} |\sum_{m=1}^{q} \tau_m(\frac{a}{q}) f(\frac{m}{Y})|$$

se cumple

$$\frac{1}{q} \sum_{a=1}^{q} |S^*_{a/q}(x)|^2 \ll xqk^{\omega(q)} d(q)^2 \log q.$$

Demostración: Escribimos

$$\sum_{m=1}^{q} \tau_m(\frac{a}{q}) f(\frac{m}{Y}) = \sum_{q_0|q} \sum_{\substack{m=1 \\ (m,q)=q_0}}^{q} \tau_m(\frac{a}{q}) f(\frac{m}{Y})$$

y por la desigualdad de Cauchy-Schwarz

$$\sum_{a=1}^{q} |S^*_{a/q}(x)|^2 \leq d(q)^2 \max_{q_0|q} \sum_{a=1}^{q} |S^*_{a/q}(x, q_0)|^2$$

con

$$S^*_{a/q}(x, q_0) = \sup_{Y \in [x,2x]} |\sum_{\substack{m=1 \\ (m,q)=q_0}}^{q} \tau_m(\frac{a}{q}) f(\frac{m}{Y})|.$$

Sea

$$B = \bigcup_{d=1}^{k} \bigcup_{j=0}^{\infty} \{(jk + d, n) \in \mathbb{N}^2 : n \geq jk + d - j - 1\},$$

y A su complementario en $\mathbb{N}^2$. Sea $q_0 = q_A q_B q_C$ y $q = q_0 l_A l_B l_C$, con $q_C l_C \mid k$, $(q_A l_A, q_B l_B) = (q_A l_A, k) = (q_B l_B, k) = 1$, con $q_A l_A = \prod_p p^{v_p}$, $q_A = \prod_p p^{u_p}$ con $(v_p, u_p) \in A$ para todo $p \mid q_A l_A$ y $q_B l_B = \prod_p p^{m_p}$, $q_B = \prod_p p^{n_p}$ con $(m_p, n_p) \in B$ para todo $p \mid q_B l_B$.

Entonces

$$\tau_m(\frac{a}{q}) = \tau_m(\frac{a(q_B l_B)^{k-1}}{\Delta}) \tau_m(\frac{a\Delta^{k-1}}{q_B l_B}) = \tau_m(\frac{a(q_B l_B)^{k-1}}{\Delta}) \eta(q_B l_B)$$

con $\Delta = q_A l_A q_C l_C$ y η la función multiplicativa que cumple $\eta(p^v) = p^{v-j-1}$. De esta forma tenemos que

$$\sum_{a=1}^{q} |S^*_{a/q}(x, q_0)|^2 \leq \eta(q_B l_B)^2 q \Delta^{-1} \|w^*\|^2 \tag{1.21}$$

donde $\|w^*\|^2 = \sum_{a=1}^{\Delta} |w^*(a)|^2$ con $w^*(a) = \sup_{Y \in [x,2x]} |w_Y(a)|$ y

$$w_Y(a) = \sum_{\substack{\lambda=1 \\ (\lambda, qq_0^{-1})=1}}^{qq_0^{-1}} \tau_{\lambda q_0}(\frac{a}{\Delta}) f(\frac{\lambda q_0}{Y}).$$

Podemos escribir

$$\|w^*\| = \langle w^*, g \rangle$$

con g un vector de norma 1. Además, como f es continua para todo a tenemos que $w^*(a) = |w_{Y(a)}(a)|$ para cierto $Y(a)$. Por tanto

$$\|w^*\| = \sum_{a=1}^{\Delta} w_{Y(a)}(a) \overline{g(a)}.$$

Usando la fórmula de inversión

$$f(u) = \frac{1}{2\pi i} \int_{1/2-i\infty}^{1/2+i\infty} u^{-s} \mathcal{M}_f(s) ds$$

podemos escribir

$$w_{Y(a)}(a) = \frac{1}{2\pi i} \int_{1/2-i\infty}^{1/2+i\infty} \mathcal{M}_f(s) \sum_{\substack{\lambda=1 \\ (\lambda, qq_0^{-1})=1}}^{qq_0^{-1}} \frac{Y(a)^s}{(\lambda q_0)^s} \tau_{\lambda q_0}(\frac{a}{\Delta}) ds.$$

Por tanto

$$\|w^*\| = \frac{1}{2\pi i} \int_{1/2-i\infty}^{1/2+i\infty} \mathcal{M}_f(s) \sum_{\substack{\lambda=1 \\ (\lambda, qq_0^{-1})=1}}^{qq_0^{-1}} T_s(\lambda)(\lambda q_0)^{-s} ds, \tag{1.22}$$

con

$$T_s(\lambda) = \sum_{a=1}^{\Delta} Y(a)^s \overline{g(a)} \tau_{\lambda q_0}(\frac{a}{\Delta}).$$

Pero por la desigualdad de Cauchy

$$|\sum_{\substack{\lambda=1 \\ (\lambda, qq_0^{-1})=1}}^{qq_0^{-1}} T_s(\lambda)(\lambda q_0)^{-s}|^2 \leq q_0^{-1} \log q \sum_{\substack{\lambda=1 \\ (\lambda, qq_0^{-1})=1}}^{qq_0^{-1}} |T_s(\lambda)|^2$$

Ahora usamos el lema 1.21 para deducir

$$\sum_{\substack{\lambda=1 \\ (\lambda, qq_0^{-1})=1}}^{qq_0^{-1}} |T_s(\lambda)|^2 \leq x \|g\|^2 \max_{(n,q)=q_0} \sum_{\substack{\lambda=1 \\ (\lambda, qq_0^{-1})=1}}^{qq_0^{-1}} |\sum_{a=1}^{\Delta} \overline{\tau_n(\frac{a}{\Delta})} \tau_{\lambda q_0}(\frac{a}{\Delta})|.$$

Pero

$$\sum_{\substack{\lambda=1 \\ (\lambda, qq_0^{-1})=1}}^{qq_0^{-1}} |\sum_{a=1}^{\Delta} \overline{\tau_n(\frac{a}{\Delta})} \tau_{\lambda q_0}(\frac{a}{\Delta})| \leq l_B \varrho_n(\Delta)$$

luego

$$|\sum_{\substack{\lambda=1 \\ (\lambda, qq_0^{-1})=1}}^{qq_0^{-1}} T_s(\lambda)(\lambda q_0)^{-s}|^2 \leq x q_0^{-1} (\log q) l_B \varrho_n(\Delta). \tag{1.23}$$

Como $(n, q) = q_0$ entonces por el lema 1.11 se cumple

$$\varrho_n(\Delta) = \varrho_n(q_C l_C) \varrho_n(q_A l_A) \leq (q_C l_C)^4 k^{\omega(q_A l_A)} (q_A l_A)^2 \ll k^{\omega(q)} (q_A l_A)^2.$$

Así, sustituyendo en (1.22) concluimos que

$$\|w^*\|^2 \ll x q_0^{-1} (\log q) l_B k^{\omega(q)} (q_A l_A)^2$$

y por (1.21)

$$\sum_{a=1}^{q} |S^*_{a/q}(x, q_0)|^2 \ll \eta(q_B l_B)^2 q \Delta^{-1} (\log q) x q_0^{-1} l_B k^{\omega(q)} (q_A l_A)^2.$$

Siempre se cumple que $\eta(q_B l_B) \leq q_B$, luego

$$\sum_{a=1}^{q} |S^*_{a/q}(x, q_0)|^2 \ll x q_B^2 l_B^2 q_A l_A^2 k^{\omega(q)} (\log q) \leq x q^2 (\log q) k^{\omega(q)}$$

y el resulado queda probado. □

De la misma forma podemos probar

Proposición 1.23. *Sea $D \in \mathbb{Z}, D \geq 1$, $1/2 \leq c < 1$ y $f : [0, \infty] \to \mathbb{C}$ una función continua con transformada de Mellin integrable y que representa a f a través de la fórmula de inversión en $\Re s = c$. Definimos*

$$S^*_{a/q}(x) = \sup_{Y \in [x, 2x]} |\sum_{m=1}^{q} \tau_m(\frac{a}{q}) f(\frac{m + Dq}{Y})|$$

se cumple

$$\frac{1}{q} \sum_{a=1}^{q} |S^*_{a/q}(x)|^2 \ll D^{-2c} x q k^{\omega(q)} d(q)^2.$$

Demostración: Procediendo como en la prueba de la proposición 1.22, pero usando la fórmula de inversión de Mellin en $\Re s = c$ llegamos a la ecuación,

$$\|w^*\| = \frac{1}{2\pi i} \int_{c-i\infty}^{c+i\infty} \mathcal{M}_f(s) \sum_{\substack{\lambda=1 \\ (\lambda, q q_0^{-1})=1}}^{q q_0^{-1}} T_s(\lambda)(\lambda q_0 + Dq)^{-s} ds, \tag{1.24}$$

que sustituye a la ecuación (1.22). Ahora al aplicar Cauchy-Schwarz obtenemos

$$|\sum_{\substack{\lambda=1 \\ (\lambda, q q_0^{-1})=1}}^{q q_0^{-1}} T_s(\lambda)(\lambda q_0 + Dq)^{-s}|^2 \leq q_0^{-1} q (Dq)^{-2c} \sum_{\substack{\lambda=1 \\ (\lambda, q q_0^{-1})=1}}^{q q_0^{-1}} |T_s(\lambda)|^2$$

$$\sum_{\substack{\lambda=1 \\ (\lambda, q q_0^{-1})=1}}^{q q_0^{-1}} |T_s(\lambda)|^2 \leq x^{2c} l_B \varrho_n(\Delta).$$

Como $x \leq q$ deducimos que $q_0^{-1}q(Dq)^{-2c}x^{2c} \leq D^{-2c}q_0^{-1}x$ y por tanto

$$|\sum_{\substack{\lambda=1 \\ (\lambda, qq_0^{-1})=1}}^{qq_0^{-1}} T_s(\lambda)(\lambda q_0 + Dq)^{-s}|^2 \leq D^{-2c}q_0^{-1}xl_B\varrho_n(\Delta),$$

que sustituye a la ecuación (1.23) lo que demuestra el resultado finalizando como en la prueba de la proposición 1.22. □

Corolario 1.24. *Sea $J \in \mathbb{N}$. Sea $f : [0, \infty] \to \mathbb{C}$ continua tal que su transformada de Mellin es integrable y representa a f mediante la fórmula de inversión en $\Re s = c$ para todo $1/2 \leq c < 1$. Definimos*

$$S^*_{a/q}(x) = \sup_{Y \in [x,2x]} |\sum_{m=1}^{Jq} \tau_m(\frac{a}{q}) f(\frac{m}{Y})|$$

se cumple

$$\frac{1}{q}\sum_{a=1}^{q} |S^*_{a/q}(x)|^2 \ll xqk^{\omega(q)}d(q)^2 \log(Jq).$$

Demostración: Por Cauchy-Schwarz

$$|S^*_{a/q}(x)|^2 \leq \sup_{Y \in [x,2x]} (|\sum_{m=1}^{q} \tau_m(\frac{a}{q}) f(\frac{m}{Y})|^2 + (\log J) \max_{1 \leq L \leq J} |\sum_{m=Lq}^{2Lq} \tau_m(\frac{a}{q}) f(\frac{m}{Y})|^2).$$

También

$$|\sum_{m=Lq}^{2Lq} \tau_m(\frac{a}{q}) f(\frac{m}{Y})|^2 \leq L \sum_{D=L}^{2L} |\sum_{m=1}^{q} \tau_m(\frac{a}{q}) f(\frac{m+Dq}{Y})|^2.$$

Así, usando las proposiciones 1.22 y 1.23 deducimos

$$\frac{1}{q}\sum_{a=1}^{q} |S^*_{a/q}(x)|^2 \ll xqk^{\omega(q)}d(q)^2(\log(q) + \log(J)J^{2(1-c)}),$$

y tomando $c = 1 - (\log J)^{-1}$ probamos el corolario. □

Para aplicar el resultado que acabamos de demostrar a las funciones $\widehat{g}$ y $\widehat{g_0}$ de la sección anterior, necesitamos primero ver cómo se comporta su transformada de Mellin

Lema 1.25. *Sea* $0 < c < 1$, $f \in L^1([0,\infty])$, $f(u)u^{-c} \in L^1([0,\infty])$. *Entonces sobre la línea* $\Re s = c$ *se cumple*

$$\mathcal{M}_{\widehat{f}}(s) = (2\pi i)^{-s}\Gamma(s)\mathcal{M}_f(1-s).$$

Demostración: Para todo $L > 0$ tenemos

$$\int_0^L \widehat{f}(x)x^{s-1}dx = \int_0^\infty f(u)\int_0^L e(-xu)x^{s-1}dx = \int_0^\infty f(u)u^{-s}du\int_0^{Lu} e(-x)x^{s-1}dx.$$

Como la integral interior está uniformemente acotada en $L \geq 0$, aplicando el teorema de convergencia dominada tenemos que

$$\int_0^\infty \widehat{f}(x)x^{s-1}dx = \int_0^\infty e(-x)x^{s-1}dx\int_0^\infty f(u)u^{-s}du.$$

Pero deformando el dominio de integración en el plano complejo vemos que

$$\int_0^\infty e(-x)x^{s-1}dx = (2\pi i)^{-s}\Gamma(s).$$

□

Lema 1.26. *Sea* $0 < c < 1$, $f \in L^1([0,\infty])$, $f(u)u^{-c} \in L^1([0,\infty])$. *Entonces podemos escribir*

$$\widehat{f}(x) = \frac{1}{2\pi i}\int_{c-i\infty}^{c+i\infty} \mathcal{M}_{\widehat{f}}(s)x^{-s}ds$$

con $\mathcal{M}_{\widehat{f}}(s) = (2\pi i)^{-s}\Gamma(s)\mathcal{M}_f(1-s)$.

Demostración: Sea $\rho \in C_0^\infty(\mathbb{R})$ con $\int \rho = 1$. Definimos $\rho_M(u) = M\rho(Mu)$. Por la fórmula de inversión para la transformada de Mellin

$$\widehat{f}(x) = \lim_{M\to\infty}\frac{1}{2\pi i}\int_{c-i\infty}^{c+i\infty} \mathcal{M}_{\widehat{f}*\rho_M}(s)x^{-s}ds.$$

Como $f \in L^1$ y $\rho \in C_0^\infty$ se cumple $\widehat{f} * \rho_M(x) = (f\check{\rho}_M)\widehat{\ }(x)$. Aplicando el lema 1.25 tenemos

$$\mathcal{M}_{\widehat{f}*\rho_M}(s) = (2\pi i)^{-s}\Gamma(s)\mathcal{M}_{f\check{\rho}_M}(1-s).$$

Pero $\check{\rho}_M(u) = \widehat{\rho}(-uM^{-1})$ y

$$\int_0^\infty |u^{-c-it} f(u) \widehat{\rho}(-\frac{u}{M})| du \ll \int_0^\infty |f(u)| u^{-c} du < \infty,$$

por lo que aplicando convergencia dominada obtenemos el lema, debido al decaimiento de $\Gamma(s)$. □

El corolario 1.24 nos permite entender el comportamiento de F cerca de la mayoría de los racionales

Proposición 1.27. *Sea $q \in \mathbb{N}$, $0 < H < 1$ y $\delta > 1$. Sea $1 < \alpha_1 < k$ y $k + 1/2 < \alpha_2 < k$. Existe un conjunto $B = B(\delta, q, H)$ contenido en*

$$\{a \in \mathbb{Z} : 1 \leq a \leq q, (a, q) = 1\}$$

con $|B| \ll q\delta^{-2} d(q)^2 k^{\omega(q)} \log(qH^{-1})$, tal que para todo $a \notin B$ y para cualquier $H < h < 2H$ se cumple

$$F_{\alpha_1}(\frac{a}{q} + h) - F_{\alpha_1}(\frac{a}{q}) = A\frac{\tau}{q} h^{\frac{\alpha_1 - 1}{k}} + O(\delta h^{\frac{\alpha_1 - 1/2}{k}}) \tag{1.25}$$

y

$$F_{\alpha_2}(\frac{a}{q} + h) - F_{\alpha_2}(\frac{a}{q}) = A\frac{\tau}{q} h^{\frac{\alpha_2 - 1}{k}} + 2\pi i \zeta_{a/q}(\alpha - k)h + O(\delta h^{\frac{\alpha_2 - 1/2}{k}}). \tag{1.26}$$

Demostración: Sea $J = (H^{-1}q)^{(k-1)/(\alpha_1 - 1)}$, y B el conjunto de los a tales que

$$\sup_{Y \in [H^{1/k}q, 2H^{1/k}q]} |\sum_{1 \leq |m| \leq qJ} \tau_m(\frac{a}{q}) \widehat{g}_0(\frac{m}{Y})| + |\sum_{1 \leq |m| \leq qJ} \tau_m(\frac{a}{q}) \widehat{g}(\frac{m}{Y})| \geq \delta (H^{\frac{1}{k}} q)^{\frac{1}{2}} q^{\frac{1}{2}}.$$

con $g_0(x) = x^{-\alpha_1}(e(x^k) - 1)$ y $g(x) = x^{-\alpha_2}(e(x^k) - 1 - 2\pi i x^k)$. Por el lema 1.26 está claro que podemos aplicar el corolario 1.24 a la funciones $\widehat{g}_0(x)$ y $\widehat{g}_0(-x)$. En el caso de la función g, hacemos la separación

$$g(x) = g(x)\mathbb{I}_{[0,1]}(x) + x^{-\alpha_2}(e(x^k) - 1)\mathbb{I}_{(1,\infty)}(x) - \eta(x),$$

con $\eta(x) = 2\pi i x^{k - \alpha_2} \mathbb{I}_{(1,\infty)}(x)$. Sobre las dos primeras podemos aplicar el lema 1.26. Además, escribiendo

$$\widehat{\eta}(y) = \lim_{N \to \infty} \widehat{\eta_N}(y)$$

con $\eta_N = \eta \mathbb{I}_{[0,N]}$ y usando el lema 1.26 sobre η_N vemos que es posible aplicar el corolario 1.24 sobre $\widehat{g}(x)$ y sobre $\widehat{g}(-x)$. Por tanto

$$|B| \ll q\delta^{-2} d(q)^2 k^{\omega(q)} \log(qH^{-1}).$$

Si $a \notin B$, usando las proposiciones 1.13 y 1.17 y la desigualdad (1.18) se prueba (1.26) y (1.25) respectivamente. □

1.5. Ondículas

Como en el trabajo de Hardy [Har], la integral de Poisson se ha empleado frecuentemente en el estudio de la regularidad global de funciones (ver [Ste]). Ciertas generalizaciones de esta herramienta eran conocidas por A. P. Calderón [Cal] pero no fueron redescubiertas hasta 20 años después, con el nombre de transformada de ondículas, por A. Grossmann y J. Morlet [GM]. Más tarde se usó en la construcción de bases ortonormales formadas por funciones suaves y bien localizadas para el espacio $L^2(\mathbb{R}^n)$ (ver [Mey, HW]).

Esta transformada ha probado ser conveniente para el estudio de la regularidad de funciones [JM]. Nosotros la vamos a usar para entender la suavidad de la función F, aunque no de forma directa como hace Jaffard en [Jaf1] sino para extender resultados al variar α.

Llamamos ondícula a una función $\varphi : \mathbb{R} \to \mathbb{C}$ diferenciable y que tenga algo de decaimiento

$$|\varphi(t)| + |\varphi'(t)| = O(\frac{1}{1+|t|^{1+\delta}}) \qquad \text{para algún } \delta > 0 \tag{1.27}$$

y de oscilación

$$\int_{-\infty}^{\infty} \varphi(t)dt = 0. \tag{1.28}$$

A partir de ella podemos construir una familia de ondículas

$$\frac{1}{a}\varphi(\frac{t-b}{a}) \qquad a > 0,\, b \in \mathbb{R}$$

que nos van a servir como base para expresar muchas otras funciones. Para ello consideramos la transformada continua de ondículas de una función $f \in L^\infty(\mathbb{R})$ con respecto a φ

$$T(b,a) = \int_{-\infty}^{+\infty} f(t)\overline{\varphi}(\frac{t-b}{a})\frac{dt}{a}. \tag{1.29}$$

Podemos recuperar la función f a partir de su transformada T. Para ello elegimos una función g, tal que $g(t)\log(2+|t|) \in L^1(\mathbb{R})$, $a^{-1}\hat{\varphi}(a)\hat{g}(a) \in L^1(\mathbb{R})$ y

$$\int_0^\infty \overline{\hat{\varphi}}(a)\hat{g}(a)\frac{da}{a} = 1 \quad \text{si} \quad \text{supp}\varphi \cap (0,\infty) \neq \emptyset \tag{1.30}$$

$$\int_0^\infty \overline{\hat{\varphi}}(-a)\hat{g}(-a)\frac{da}{a} = 1 \quad \text{si} \quad \text{supp}\varphi \cap (-\infty,0) \neq \emptyset \tag{1.31}$$

Una función g cumpliendo estos requisitos recibe el nombre de ondícula de reconstrucción para φ. Siempre existe alguna ondícula de reconstrucción, y de hecho podemos tomar $g \in C_0^\infty(\mathbb{R})$ que es lo que haremos a partir de ahora. Se cumple que (ver [HT])

Teorema 1.28. *Sea f una función acotada y débilmente oscilante alrededor de 0, lo que viene expresado por la condición*

$$\lim_{u\to\infty} \frac{1}{2u}\int_{t-u}^{t+u} f(y)dy = 0 \qquad \textit{uniformemente en } t.$$

Entonces para todo t donde f es continua se cumple

$$f(t) = \lim_{\substack{\epsilon\to 0\\ \rho\to\infty}} \int_\epsilon^\rho \frac{da}{a}\int_{-\infty}^{+\infty} T(b,a)\frac{1}{a}g(\frac{t-b}{a})db.$$

Para estudiar la regularidad local hasta exponente $n \in \mathbb{N}$ vamos a exigir que $t^n\varphi(t) \in L^1(\mathbb{R})$ y además que

$$\int_{-\infty}^{\infty} t^m\varphi(t)dt = 0 \qquad m = 0,1,\ldots,n-1 \tag{1.32}$$

los primeros n momentos se anulen (es un "átomo"). De esta forma, la regularidad local de f puede caracterizarse por el decaimiento de su transformada T (ver [HT], [Jaf1]):

Teorema 1.29. *Sea f una función acotada y satisfaciendo*

$$f \in C^\beta(x_0) \qquad \beta \in (0,n)$$

para un punto $x_0 \in \mathbb{R}$. Entonces se cumple

$$T(b,a) \ll a^\beta(1+\frac{|b-x_0|}{a})^\beta,$$

donde T es la transformada de f con respecto a una ondícula satisfaciendo (1.32).

Demostración: Como $f \in C^\beta(x_0)$, existe un polinomio p de grado $n-1$ tal que

$$f(x) - p(x - x_0) \ll |x - x_0|^\beta. \tag{1.33}$$

Por 1.29 y (1.32) tenemos que

$$|T(b,a)| = |\int_{-\infty}^{\infty} (f(x) - p(x-x_0))\overline{\psi}(\frac{x-b}{a})\frac{dx}{a}|,$$

y por (1.33)

$$T(b,a) \ll \int_{-\infty}^{\infty} |x-b|^\beta |\psi(\frac{x-b}{a})|\frac{dx}{a} + |b-x_0|^\beta \int_{-\infty}^{\infty} |\psi(\frac{x-b}{a})|\frac{dx}{a}$$

de donde deducimos el resultado porque $t^n\psi(t) \in L^1$. □

Teorema 1.30. *Sea f acotada, débilmente oscilante y con $f \in C^\gamma(\mathbb{R})$ para algún $\gamma > 0$. Sean $\beta' < \beta$ y $\beta \in (0,n)$, $\beta \notin \mathbb{Z}$ tales que*

$$T(b,a) \ll a^\beta (1 + \frac{|b-x_0|}{a})^{\beta'}, \tag{1.34}$$

con T la transformada de f con respecto a una ondícula satisfaciendo (1.32). Entonces se cumple que

$$f \in C^\beta(x_0).$$

Además, si $\beta > 1$ podemos expresar la derivada de f en x_0 como

$$f'(x_0) = \int_0^{\infty} \frac{da}{a} \int_0^{\infty} T(b,a) g'(\frac{x_0 - b}{a})\frac{db}{a^2}$$

Demostración: Por el teorema 1.28 tenemos

$$f(x) = \int_0^{\infty} \omega(a,x)\frac{da}{a}$$

con

$$\omega(a,x) = \int_{-\infty}^{\infty} T(b,a) g(\frac{x-b}{a})\frac{db}{a}.$$

De la desigualdad (1.34) deducimos

$$\omega(a,x) \ll a^\beta + a^{\beta-\beta'}|x-x_0|^{\beta'} + a^\beta \int_{-\infty}^{\infty} |\frac{b-x}{a}|^{\beta'} |g(\frac{x-b}{a})|\frac{db}{a} \ll a^\beta (1 + \frac{|x-x_0|}{a})^{\beta'}$$

y de la misma forma para todo entero $j \geq 0$ se cumple

$$(\frac{\partial}{\partial x})^j \omega(a,x) = a^{-j} \int_{-\infty}^{\infty} T(b,a) g^{(j)}(\frac{x-b}{a}) \frac{db}{a} \ll a^{\beta-j}(1+\frac{|x-x_0|}{a})^{\beta'}. \quad (1.35)$$

Por tanto, definiendo

$$p(t) = \sum_{j=0}^{m-1} \frac{t^j}{j!} \int_0^{\infty} (\frac{\partial}{\partial x})^j \omega(a,x_0) \frac{da}{a} = \int_0^{\infty} \upsilon(a,t) \frac{da}{a}$$

donde m es el entero que cumple $m-1 < \beta < m$, tenemos que

$$f(x) - p(x-x_0) = \int_0^{\infty} (\omega(a,x) - \upsilon(a,x-x_0)) \frac{da}{a},$$

luego por (1.35) y la fórmula del desarrollo de Taylor vemos que salvo una constante $f(x) - p(x-x_0)$ está acotado por

$$|x-x_0|^{\beta'} \int_0^{|x-x_0|} a^{\beta-\beta'} \frac{da}{a} + \sum_{j=0}^{m-1} |x-x_0|^j \int_0^{|x-x_0|} a^{\beta-j} \frac{da}{a} + |x-x_0|^m \int_{|x-x_0|}^{\infty} a^{\beta-m} \frac{da}{a}$$

luego

$$f(x) - p(x-x_0) \ll |x-x_0|^{\beta}.$$

□

Por tanto tenemos

Teorema 1.31. *Sea f acotada, $f \in C^{\gamma}(\mathbb{R})$ para algún $\gamma > 0$ y $0 < \beta_f(x_0) < n$. Se cumple*

$$\beta_f(x_0) = \sup\{\beta \in \mathbb{R} : T(x_0+b,a) = O((a+|b|)^{\beta})\}.$$

Apliquemos esta caracterización de regularidad a nuestra familia de funciones

$$F(x) = F_{\alpha}(x) = \sum_{n=1}^{\infty} n^{-\alpha} e(n^k x).$$

Para esto vamos a considerar una ondícula adaptada a estas funciones

Lema 1.32. *Sea $r > 0$ y*

$$\varphi_r(t) = \frac{1}{(2\pi)^{r+1}} \frac{\Gamma(1+r)}{(1+it)^{r+1}}.$$

Si T es la transformada de ondículas de la función

$$f(x) = \sum_{m=1}^{\infty} a_m e(mx)$$

con $\sum_{m=1}^{\infty} |a_m| < \infty$, con respecto a la ondícula φ_r entonces

$$T(b,a) = a^r \theta(b+ia)$$

con

$$\theta(z) = \sum_{n=1}^{\infty} a_m m^r e(mz).$$

Demostración:

$$T(b,a) = \sum_{m=1}^{\infty} a_m e(mb) \widehat{\varphi}_r(-ma). \tag{1.36}$$

Consideramos la función

$$G_r(x) = e^{-2\pi x} x^r \mathbb{I}_{[0,\infty]}(x).$$

Deformando el dominio de integración en $\mathbb{C}$ vemos que

$$\widehat{G}_r(u) = \varphi_r(u)$$

luego por la fórmula de inversión para la transformada de Fourier

$$\widehat{\varphi}_r(-x) = G_r(x).$$

Sustituyendo esta fórmula en (1.36) finalizamos la prueba. □

Usando el teorema 1.31 y el lema 1.32 deducimos una relación entre la regularidad de $F_{\alpha,k}$ al variar α

Corolario 1.33. *Sea $x_0 \in \mathbb{R}$, $1 < \alpha$ y $v > 0$. Se cumple que*

$$\beta_{F_{\alpha+v,k}}(x_0) \geq \beta_{F_{\alpha,k}}(x_0) + \frac{v}{k}.$$

Demostración: Sea $T_{\alpha,k}$ la transformada de $F_{\alpha,k}$ con respecto a $\varphi_{d+\alpha/k}$, para cualquier $d > 0$. Se cumple que

$$T_{\alpha,k}(b,a) = a^{\frac{\alpha}{k}+d}\theta_d(b+ia)$$

con $\theta_d(z) = \sum_{n=1}^{\infty} n^{dk} e(n^k z)$. Por tanto

$$T_{\alpha+v,k}(b,a) = a^{\frac{v}{k}} T_{\alpha,k}(b,a).$$

Por el teorema 1.29 deducimos que si $F_{\alpha,k} \in \mathbb{C}^{\beta}(x_0)$ entonces

$$T_{\alpha+v,k}(b,a) \ll a^{\frac{v}{k}+\beta}(1+\frac{|b-x_0|}{a})^{\beta}$$

y por el teorema 1.30 obtenemos el corolario. □

Ya hemos observado que las transformada de ondículas nos sirve para manejar la regularidad de funciones. Veamos ahora que también se puede usar para determinar la dimensión fractal de gráficos de funciones continuas.

Sea E un subconjunto acotado de $\mathbb{R}^2$ y $N_h(E)$ el mínimo número de conjuntos de diámetro menor o igual que h que cubren E. Entonces se define la dimensión fractal o dimensión de Minkowski de E como

$$\dim_{\mathrm{M}}(E) = \lim_{h\to 0} \frac{\log N_h(E)}{\log h^{-1}}$$

cuando existe el límite. En cualquier caso podemos considerar las dimensiones superior $\overline{\dim_{\mathrm{M}}}$ e inferior $\underline{\dim_{\mathrm{M}}}$ dadas por los límites superior en inferior. Sea $f : [0,1] \to \mathbb{C}$ continua. Definiendo $\Gamma_f = \{(x, f(x)) \in \mathbb{R}^2 : 0 \le x \le 1\}$, se cumple que

$$\log N_h(\Gamma_f) \sim \log(h^{-1}(V_h(f)+1))$$

con

$$V_h(\phi) = \sup\{\sum_{j<h^{-1}} |\phi(x_j) - \phi(y_j)| : x_j, y_j \in I_j, \forall j < h^{-1}\}$$

e

$$I_j = [(j-1)h, jh] \qquad j \in \mathbb{N}.$$

Vamos a estudiar como se relaciona $V_h(f)$ con $S_h(T,a)$ donde T es la transformada de ondículas de f y

$$S_h(T,a) = \sup\{\sum_{j<h^{-1}} |T(b_j,a)| : b_j \in I_j \, \forall j < h^{-1}\}.$$

Se cumple que

$$\lim_{h\to 0} hS_h(T,a) = \int_0^1 |T(b,a)|db$$

y como $tS_t(T,a)$ es decreciente en t tenemos que

$$\int_0^1 |T(b,a)|db \le tS_t(T,a) \qquad \text{para todo}\, t>0. \tag{1.37}$$

Lema 1.34. *Sea $f:\mathbb{R}\to\mathbb{C}$ una función periódica de período 1. Si $T(b,a)$ es su transformada con respecto a una ondícula φ que cumpla*

$$\varphi(t) = O(t^{-2-\epsilon}),$$

entonces

$$S_h(T,a) \ll V_h(f)$$

uniformemente en $a<h$.

Demostración: Se cumple

$$T(b,a) = \int_{-\infty}^{+\infty} \frac{1}{a}\overline{\varphi}(\frac{u}{a})(f(b+u)-f(b))\,du$$

luego

$$\sum_{j<h^{-1}} |T(b_j,a)| \le \int_{-\infty}^{+\infty} \frac{1}{a}|\varphi(\frac{u}{a})| \sum_{j<h^{-1}} |f(b_j+u)-f(b_j)|\,du$$

Pero

$$\sum_{j<h^{-1}} |f(b_j+u)-f(b_j)| \ll V_h(f),$$

y por tanto

$$\sum_{j<h^{-1}} |T(b_j,a)| \ll V_h(f).$$

□

Lema 1.35. *Sea f una función periódica de período 1, con $f\in C^\gamma(\mathbb{R})$ para algún $\gamma>0$. Si $T(b,a)$ es su transformada de ondículas, se cumple*

$$V_h(f) \ll (\log h^{-1})\big(\sup_{a<h} S_h(T,a) + \sup_{h<a<1} S_a(T,a)\big).$$

Demostración: Podemos considerar que γ es suficientemente pequeño. Entonces

$$T(b,a) \ll a^{\gamma} \qquad a \to 0.$$

Por lo tanto se cumple por el teorema 1.28

$$\sum_{j\le h^{-1}} |f(x_j)-f(y_j)| \le \int_{\epsilon}^{h} I_1(a)\frac{da}{a} + \int_{h}^{\rho} I_2(a)\frac{da}{a} + O(h^{-1}\epsilon^{\gamma}),$$

con

$$I_1(a) = \int_{-\infty}^{\infty} |g(\frac{u}{a})|\frac{1}{a}\sum_{j<h^{-1}} (|T(x_j-u,a)|+|T(y_j-u,a)|)\,du,$$

$$I_2(a) = \int_{-\infty}^{\infty} |T(b,a)|\frac{1}{a}\sum_{j<h^{-1}} |g(\frac{x_j-b}{a}) - g(\frac{y_j-b}{a})|\,db.$$

Tenemos que $I_1(a) \ll S_h(T,a)$. Por la periodicidad de T y aplicando el teorema del valor medio vemos que

$$I_2(a) \ll \frac{h}{a}\int_0^1 |T(b,a)|\frac{db}{a}\sup\{\sum_{j\in\mathbb{Z}} |g'(\frac{\xi_j}{a})| : h \le |\xi_{j+1}-\xi_j| \le 2h\ \forall j\in\mathbb{Z}\}$$

luego

$$I_2(a) \ll \int_0^1 |T(b,a)|\frac{db}{a}.$$

Considerando (1.37) se sigue

$$\int_0^1 |T(b,a)|\frac{db}{a} \le S_a(T,a), \qquad a<1$$

luego tomando $\epsilon = h^{-1/\gamma}$ obtenemos el lema. □

Como consecuencia de los dos últimos lemas deducimos

Proposición 1.36. *Sea* $f \in C^{\gamma}(\mathbb{R})$, $|\varphi(t)| \ll (1+|t|)^{-2-\epsilon}$ *y*

$$L(h) = \sup_{a\le h} S_h(T,a).$$

Entonces

$$\dim_{\mathrm{M}}(\Gamma_f) = \lim_{h\to 0} \frac{\log\left(h^{-1}(L(h)+1)\right)}{\log h^{-1}}$$

si existe el límite. Además el límite existe si y sólo si existe $\dim_{\mathrm{M}}(\Gamma_f)$.

En [CC2] se calcula la dimensión fractal del gráfico Γ en $[0,1]$ de la función

$$\sum_{n=1}^{\infty} \frac{c_n e(n^k x)}{n^\alpha} \qquad \textit{donde} \qquad 0 < \underline{\lim} c_n \leq \overline{\lim} c_n < \infty$$

en el rango $\alpha > (k+1)/2$. De hecho se prueba que la cota para la dimensión inferior

$$\underline{\dim}_{\mathrm{M}}(\Gamma) \geq 2 + \frac{1}{2k} - \frac{\alpha}{k}$$

se cumple en todo el rango $\alpha > 1$. Aquí vamos a extender el calculo a un rango mayor, aunque escribimos el resultado sólo para el caso $c_n = 1$. En la prueba vamos a usar un resultado (ver [Dav2]) de tipo gran criba diferente del lema 1.21

Lema 1.37. *Sea $S : [0,1] \to \mathbb{R}$ una función con derivada continua. Si $x_1, x_2, \ldots, x_R$ son puntos h-espaciados, se cumple*

$$\sum_{j=1}^{R} |S(x_j)|^2 \leq \frac{1}{h} \int_0^1 |S(x)|^2 dx + (\int_0^1 |S(x)|^2 dx)^{1/2} (\int_0^1 |S'(x)|^2 dx)^{1/2}.$$

En la prueba del resultado para la dimensión fractal usaremos, como se hizo en [CC2] para calcular la dimensión inferior, que

$$(\int_0^1 |\sum_{n \leq N} c_n e(n^k x)|^4 \, dx)^{1/4} \ll N^{\frac{1}{2}+\epsilon}. \tag{1.38}$$

Esta desigualdad se deduce de que $r(n) \ll n^\epsilon$, donde $r(n)$ es el número de representaciones n como suma de dos k-potencias, porque si $n = a^k + b^k$ entonces $a+b$ divide a n cuando k es impar y $a^{k/2} + ib^{k/2}$ divide a n en $\mathbb{Z}[i]$ cuando k es par.

Si tuvieramos el mismo resultado para la norma en L^{2k} conseguiríamos la dimensión fractal en todo el rango $\alpha > 1$. Cotas para diferentes normas pueden darnos cotas superiores para la dimensión fractal (ver [CU1]). Nuestro resultado usando (1.38) es el siguiente

Proposición 1.38. *Para $\alpha > (k+2)/4$ se cumple*

$$\dim_{\mathrm{M}}(\Gamma_F) = \max(1, 2 + \frac{1}{2k} - \frac{\alpha}{k}).$$

Demostración: Tenemos que la transformada de F con respecto a $\varphi_{1+\alpha/k}$ es $T(b,a) = a^{1+\alpha/k}\theta(b+ia)$ con

$$\theta(b+ia) = \sum_{n=1}^{\infty} n^k e(n^k(b+ia)).$$

Dividimos la suma en intervalos diádicos

$$\theta(b+ia) = \sum_{l=0}^{\infty} P_{2^l}(b),$$

con

$$P_M(b) = \sum_{M\leq n<2M} n^k e^{-2\pi n^k a} e(n^k b).$$

Por la desigualdad de Hölder

$$\sum_{j<h^{-1}} |P_M(b_j)| \ll h^{-\frac{3}{4}}(\sum_{j<h^{-1}} |P_M(b_j)|^4)^{1/4}.$$

Usando el lema 1.37 sobre $P_M(x)^2$ y la desigualdad (1.38) vemos que si b_j están h-espaciados se cumple

$$\sum_{j<h^{-1}} |P_M(b_j)|^4 \ll M^{4k+\epsilon}(h^{-1}+M^k)e^{-M^k a}M^2.$$

Por tanto para $a < h$

$$S_h(T,a) \ll a^{\frac{\alpha}{k}} h^{-\frac{3}{4}}(a^{-1-\frac{2}{k}})^{\frac{1}{4}+\epsilon} = h^{-\frac{3}{4}} a^{\frac{\alpha}{k}-\frac{1}{4}-\frac{1}{2k}-\epsilon},$$

y como $\alpha > (k+2)/4$,

$$\sup_{a<h} S_h(T,a) \ll h^{-1-\frac{1}{2k}+\frac{\alpha}{k}-\epsilon}$$

y por el lema 1.35 obtenemos el resultado. □

Esta proposición se podría haber demostrado de la misma forma sin el uso de ondículas. Lo que sí que pueden demostrar las ondículas es una relación entre las dimensión de las gráficas de las funciones $F_{\alpha,k}$

Proposición 1.39. *Sea $\alpha_2 > \alpha_1 > 1$. Entonces*

$$\overline{\dim}\Gamma_{F_{\alpha_2}} \leq \overline{\dim}\Gamma_{F_{\alpha_1}} - \frac{\alpha_2 - \alpha_1}{k}.$$

Demostración: Si T_1 y T_2 son las transformadas de ondículas de F_{α_1} y F_{α_2} con respecto a $\varphi_{1+\alpha_1/k}$ y $\varphi_{1+\alpha_2/k}$ respectivamente, entonces

$$T_2(b,a) = a^{\frac{\alpha_2-\alpha_1}{k}} T_1(b,a)$$

luego

$$S_h(T_2,a) = a^{\frac{\alpha_2-\alpha_1}{k}} S_h(T_1,a)$$

y tomando supremos en $a < h$ deducimos el resultado. □

1.6. Regularidad en los irracionales

Decimos que una función $f : \mathbb{R} \to \mathbb{C}$ es multifractal cuando la función

$$d_{\mathrm{H}}(\beta) = \dim_{\mathrm{H}}\{x \in \mathbb{R} : \beta_f(x) = \beta\}$$

es mayor que cero en más de un punto.

Hasta ahora hemos estudiado la regularidad de la función solamente cerca de los racionales, luego no podemos decir que $F_{\alpha,k}$ sea una función multifractal. En esta sección vamos a ver que como en el caso de $F_{\alpha,2}$, toda $F_{\alpha,k}$ es multifractal y de hecho la regularidad de un punto depende de lo bien que se pueda aproximar por racionales. Pero, a diferencia del caso $k = 2$ también va a depender de por qué tipo de racionales es aproximable.

Vamos a comenzar obteniendo cotas inferiores y superiores para el exponente Hölder de un punto. Para ello recordamos el siguiente resultado de acotación de sumas trigonométricas (ver [Vau])

Lema 1.40. *(Desigualdad de Weyl). Si P es un polinomio de grado k con coeficiente principal A y a/q es una fracción irreducible tal que*

$$|A - \frac{a}{q}| \leq q^{-2}$$

entonces

$$\sum_{n \leq N} e(P(n)) \ll (Nq^{-1/K} + N^{1-1/K} + N^{1-k/K}q^{1/K})N^{\epsilon}$$

para todo $\epsilon > 0$ con $K = 2^{k-1}$.

Esta es la cota superior que obtenemos para la regularidad de un punto x_0, que depende de a qué espacio E_r pertenezca

Proposición 1.41. *Para todo punto x de E_r se cumple*

$$\beta_F(x) \geq \frac{\alpha-1}{k} + 2^{1-k}\,\text{mín}(\frac{1}{k}, \frac{1}{2(r-1)}).$$

Demostración: Por el teorema del valor medio se cumple que

$$F(x+h) - F(x+\frac{h}{2}) \ll h|\sum_{n\leq h^{-1/k}} 2\pi i n^{k-\alpha} e(n^k\xi_1)| + |\sum_{n>h^{-1/k}} n^{-\alpha} e(n^k\xi_2)| \tag{1.39}$$

para ciertos $x+h/2 \leq \xi_1, \xi_2 \leq x+h$. Consideramos las convergentes consecutivas a_n/q_n y a_{n-1}/q_{n-1} de x tales que

$$q_n^{-r_n} = |x - \frac{a_n}{q_n}| \leq |h| \leq |x - \frac{a_{n-1}}{q_{n-1}}| = q_{n-1}^{-r_{n-1}}.$$

Como

$$|\frac{a_n}{q_n} - \frac{a_{n-1}}{q_{n-1}}| = \frac{1}{q_n q_{n-1}}$$

y están en lados opuestos con respecto a x vemos que

$$\frac{1}{2} q_{n-1}^{r_{n-1}-1} \leq q_n \leq q_{n-1}^{r_{n-1}-1}. \tag{1.40}$$

Vamos a considerar dos casos. El primero es cuando h cumple

$$q_n^{-r_n} \leq |h| \leq q_n^{-2}$$

que podemos transformar en

$$h^{-\frac{1}{r_n}} \leq q_n \leq h^{-\frac{1}{2}}.$$

En este caso dividiendo las sumas de (1.39) en intervalos diádicos y sumando por partes podemos aplicar el lema 1.40 con a_n/q_n como aproximante de ξ_j, $j = 1, 2$, y así obtenemos

$$F(x+h) - F(x+\frac{h}{2}) \ll h^{\frac{\alpha-1}{k}}(h^{\frac{1}{kK}} + h^{\frac{1}{r_n K}} + h^{(1-\frac{1}{2})\frac{1}{K}}).$$

El segundo caso es cuando h está más cerca de a_{n-1}/q_{n-1}, es decir

$$q_n^{-2} \leq |h| \leq q_{n-1}^{-r_{n-1}},$$

que por (1.40) podemos transformar en

$$h^{-\frac{1}{2r_{n-1}-2}} \ll q_{n-1} \leq h^{-\frac{1}{r_{n-1}}}.$$

Actuando como en el caso anterior, pero usando como aproximante al racional a_{n-1}/q_{n-1} obtenemos

$$F(x+h) - F(x+\frac{h}{2}) \ll h^{\frac{\alpha-1}{k}}(h^{\frac{1}{kK}} + h^{\frac{1}{(2r_{n-1}-2)K}} + h^{(1-\frac{1}{r_{n-1}})\frac{1}{K}}).$$

Por tanto, tomando el máximo de ambos casos llegamos a

$$F(x+h) - F(x+\frac{h}{2}) \ll h^{\frac{\alpha-1}{k}}(h^{\frac{1}{kK}} + h^{\frac{1}{(2r_{n-1}-2)K}} + h^{\frac{1}{r_nK}} + h^{(1-\frac{1}{r_{n-1}})\frac{1}{K}}).$$

Teniendo en cuenta que $\limsup_n r_n = r$ y que

$$F(x+h) - F(x) = \sum_{j=0}^{\infty} \big(F(x+h2^{-j}) - F(x+h2^{-j-1})\big)$$

concluimos la prueba. □

También podemos ver que la función no puede ser demasiado regular en un punto. Podemos probar

Proposición 1.42. *Sea $\alpha < k-1$. Para todo x tenemos que*

$$\beta_F(x) \leq \frac{\alpha}{k-1}.$$

Demostración: Vamos a probar que

$$F(x+h) - F(x) = \Omega(h^{\frac{\alpha}{k-1}} |\log h|^{-2}).$$

Consideramos el núcleo de Féjer

$$f_M(x) = \sum_{|n|\leq M} (1 - \frac{|n|}{M}) e(nx) = \frac{1}{M}\big(\frac{\operatorname{sen}(\pi M x)}{\operatorname{sen}(\pi x)}\big)^2 \quad \text{con } M = N^{k-1}, N > 1.$$

Nótese que para $n \neq N$ se cumple $|N^k - n^k| \geq N^k - (N-1)^k > M$, luego

$$\int_{-1/2}^{1/2} e(N^k t) f_M(t)(F(x-t) - F(x))dt = N^{-\alpha} e(N^k x).$$

Si $|F(x-t)-F(x)| = O(t^{\alpha/(k-1)}(\log|t|)^{-2})$, entonces la integral anterior sería $O(\int |t|^{\alpha/(k-1)} |\log t|^{-2} |f_M(t)|dt)$. Subdividiendo en intervalos de longitud M^{-1} obtenemos que la integral es $O(M^{-\alpha/(k-1)}(\log M)^{-1})$ pero esto no es posible. □

Las cotas que hemos obtenido están lejos de la realidad, al menos para la mayoría de puntos. Como $F'_{k+1/2+\epsilon,k} \in L^2([0,1])$, por el Teorema fundamental del Cálculo se cumple que $F_{k+1/2+\epsilon,k}$ es derivable en casi todo punto, luego

$$F_{k+1/2+\epsilon,k} \in C^1(x_0)$$

para casi todo punto x_0. Por el corolario 1.33 obtenemos que para $\alpha \geq k+1/2$, en casi todo punto $x \in \mathbb{R}$ se cumple

$$\beta_F(x) \geq \frac{\alpha - 1/2}{k}. \tag{1.41}$$

Vamos a ver que este tipo de resultado se puede generalizar para la función F a todo $\alpha > 1$ y E_r con $r \geq 2$. Para entenderlo, primero vamos a necesitar controlar la medida de Hausdorff de estos conjuntos

Definición 1.43. Sea $E \subset \mathbb{R}$. Para cada $s > 0$ definimos su medida exterior s-dimensional de Hausdorff como

$$\mathcal{H}^s(E) = \sup_{\delta>0} \mathcal{H}^s_\delta(E) = \lim_{\delta \to 0+} \mathcal{H}^s_\delta(E)$$

con

$$\mathcal{H}^s_\delta(E) = \text{ínf}\{\sum_{i=1}^{\infty} |U_i|^s : E \subset \bigcup_i U_i, |U_i| \leq \delta\}.$$

Puede probarse (ver [Fal1]) que todo conjunto de Borel de $\mathbb{R}$ es $\mathcal{H}^s$-medible, y nosotros sólo trataremos con este tipo de conjuntos. Para todo $\gamma > 0$ y $\delta < 1$ se tiene

$$\mathcal{H}^{s+\gamma}_\delta(E) \leq \delta^\gamma \mathcal{H}^s_\delta.$$

Luego $\mathcal{H}^s(E)$ es una función no creciente y como $\mathcal{H}^s(E) = 0$ si $s > 1$, tiene sentido definir la dimensión de Hausdorff de E como

$$\dim_{\mathrm{H}}(E) = \text{ínf}\{s > 0 : \mathcal{H}^s(E) = 0\}.$$

Veamos el resultado básico con el que controlar inferiormente la dimensión de Hausdorff de un conjunto

Lema 1.44. *(Ejemplo 4.6 en [Fal2]) Sea* $[0,1] = G_0 \supset G_1 \supset G_2 \supset \ldots$, *donde cada* G_j *es una unión finita de intervalos (cuya máxima longitud tiende a cero con* j*) de tal forma que cada intervalo de* G_{j-1} *contiene al menos* $m_j \geq 2$ *intervalos de* G_j *y éstos están separados por una distancia de al menos* ε_j, *con* $0 < \varepsilon_j < \varepsilon_{j-1}$. *Entonces si*

$$s_j = \frac{\log(m_1 \ldots m_{j-1})}{-\log(m_j \varepsilon_j)}, \qquad s = \liminf_j s_j$$

$$\dim_{\mathrm{H}}(\bigcap_{j=0}^{\infty} G_j) \geq s$$

Si además $s_j \geq s$ *para todo* j *suficientemente grande, entonces se cumple* $\mathcal{H}^s(\cap G_j) > 0$.

Lema 1.45. *Para todo* $r \geq 2$ *se cumple que* $\dim_{\mathrm{H}} E_r = 2/r$ *y*

$$\mathcal{H}^{2/r}(E_r) > 0.$$

Demostración: Para la dimensión superior, observamos que para cualquier $r' < r$ se cumple

$$E_r \subset \bigcap_{N=1}^{\infty} A_N$$

con

$$A_N = \bigcup_{\substack{n \geq N \\ 1 \leq a \leq n}} [\frac{a}{n} - \frac{1}{(n \log n)^{r'}}, \frac{a}{n} + \frac{1}{(n \log n)^{r'}}].$$

Pero

$$\mathcal{H}^{2/r'}(A_N) \ll (\log N)^{-1}$$

luego $\mathcal{H}^{2/r'}(E_r) = 0$ y por tanto $\dim_{\mathrm{H}} E_r \leq 2/r$.

Para la inferior, consideramos una sucesión $(n_j)_{j\in\mathbb{N}}$ definida por $n_j = n_{j-1}^j$ y formamos los conjuntos

$$G_j = \bigcup_{n_j<p<2n_j} \bigcup_{1\le a<p} I_r(a,p).$$

con

$$I_r(a,p) = [\frac{a}{p} - \frac{e^{(\log p)^{1/2}}}{p^r}, \frac{a}{p} - \frac{1}{p^r}] \cup [\frac{a}{p} + \frac{1}{p^r}, \frac{a}{p} + \frac{e^{(\log p)^{1/2}}}{p^r}]. \tag{1.42}$$

Tenemos que

$$E_r \supset \bigcap_{j=1}^{\infty} G_j$$

pero podemos usar el lema 1.44 con $m_j \asymp n_j^2 (\log n_j)^{-1} \exp((\log n_{j-1})^{1/2})(n_{j-1})^{-r}$ y $\epsilon_j \asymp n_j^{-2}$. Por tanto para j suficientemente grande

$$s_j \ge \frac{2\log n_{j-1} - r\log n_{j-2} - \log\log n_{j-1}}{r\log n_{j-1} - (\log n_{j-1})^{1/2} + \log\log n_j} \ge \frac{2}{r},$$

luego $\mathcal{H}^{2/r}(E_r) > 0$.

□

Podemos ya enunciar el siguiente resultado que trata la regularidad de F sobre casi todo punto de E_r

Teorema 1.46. *Para todo $r \ge 2$, se cumple que*

i) En casi todo punto x de E_r (con la medida $\mathcal{H}^{2/r}$) se tiene

$$\beta_F(x) \ge \text{mín}\,\big(\frac{\alpha - 1/2}{k}, \frac{\alpha - 1}{k} + \frac{1}{2r}\big).$$

Además, si $\alpha > k + 1/2$ y $(\alpha-1)/k + 1/(2r) > 1$ entonces

$$F'(x) = \lim_{n\to\infty} \zeta_{a_n/q_n}(\alpha - k). \tag{1.43}$$

ii) Si $r \ge k$, existe un subconjunto $E_{r,0}$ en E_r de medida positiva tal que para todo $x \in E_{r,0}$

$$\beta_F(x) \ge \frac{\alpha - 1/2}{k}. \tag{1.44}$$

iii) Si $r > k$, existe un subconjunto $E_{r,1}$ en E_r de medida positiva tal que para todo $x \in E_{r,1}$

$$\beta_F(x) = \frac{\alpha - 1}{k} + \frac{1}{2r}. \tag{1.45}$$

Demostración: Comenzamos probando *i*). Sean $1 \leq \alpha_1 < k$ y $k + 1/2 < \alpha_2 < k + 1$ tales que $\alpha_1 \leq \alpha \leq \alpha_2$. Para cada $\epsilon > 0$, tomamos

$$B_\epsilon(q) = \bigcup_{\substack{j \in \mathbb{N} \\ q^{-r-1} \leq 2^{-j} \leq q^{-1}}} B(q^\epsilon, q, 2^{-j})$$

con $B(q^\epsilon, q, 2^{-j})$ el conjunto que aparece en el enunciado de la proposición 1.27. Se cumple que

$$|B_\epsilon(q)| \ll q^{1-\epsilon}. \tag{1.46}$$

Por otra parte, definimos

$$C_\epsilon(q) = \{a \in \mathbb{Z} : 1 \leq a \leq q, (a, q) = 1, |\tau(a/q)| \geq q^{1/2+\epsilon}\}.$$

Por los lemas 1.5, 1.6 y 1.7 tenemos

$$\sum_{q \leq Q} \sum_{\substack{a=1 \\ (a,q)=1}}^{q} |\tau(\frac{a}{q})| \ll Q^{2+1/2+\epsilon/2}. \tag{1.47}$$

Si $(a_n/q_n)_{n \in \mathbb{N}}$ es la sucesión de convergentes de x, entonces definimos

$$M_{r,\epsilon} = \{x \in E_r : |\{a_n/q_n : a_n \in B_\epsilon(q_n) \cup C_\epsilon(q_n)\}| = \infty\}.$$

Para todo $Q_0 \in \mathbb{N}$ se tiene el contenido

$$M_{r,\epsilon} \subset \bigcup_{2^j = Q \geq Q_0} \bigcup_{Q \leq q \leq 2Q} \bigcup_{a \in B_\epsilon(q) \cup C_\epsilon(q)} [\frac{a}{q} - \frac{1}{q^{r-\epsilon/2}}, \frac{a}{q} + \frac{1}{q^{r-\epsilon/2}}].$$

Como la $\mathcal{H}^{2/r}-$medida de cada intervalo es menor o igual que $q^{\epsilon/2-2}$, por (1.46) y (1.47) obtenemos

$$\mathcal{H}^{2/r}(M_{r,\epsilon}) \ll Q_0^{-\epsilon/2}$$

y por tanto $\mathcal{H}^{2/r}(M_{r,\epsilon}) = 0$. Definiendo

$$M_r = \bigcup_{n=1}^{\infty} M_{r,1/n}$$

tenemos que $\mathcal{H}^{2/r}(M_r) = 0$. Si $x \in E_r \setminus M_r$, para todo h suficientemente pequeño podemos encontrar convergentes a_{n-1}/q_{n-1}, a_n/q_n de x tales que

$$2q_n^{-r_n} < |h| \leq 2q_{n-1}^{-r_{n-1}} \leq q_n^{-1}.$$

Así, escribimos

$$F_{\alpha_1,k}(x+h) - F_{\alpha_1,k}(x) = F_{\alpha_1,k}(x+h) - F_{\alpha_1,k}(\frac{a_n}{q_n}) - (F_{\alpha_1,k}(x) - F_{\alpha_1,k}(\frac{a_n}{q_n})).$$

Por (1.25), para cada $\epsilon > 0$ obtenemos

$$F_{\alpha_1,k}(x+h) - F_{\alpha_1,k}(x) \ll \frac{|h|^{\frac{\alpha_1-1}{k}}}{q_n^{\frac{1}{2}-\epsilon}} + q_n^{\epsilon}|h|^{\frac{\alpha_1-1/2}{k}} \ll |h|^{\frac{\alpha_1-1}{k}+\frac{1}{2r_n}-\frac{\epsilon}{r_n}} + |h|^{\frac{\alpha_1-1/2}{k}-\epsilon}.$$

Haciendo tender h a cero se cumple

$$\beta_{F_{\alpha_1,k}}(x) \geq \text{mín}\,(\frac{\alpha_1-1}{k} + \frac{1}{2r}, \frac{\alpha_1-1/2}{k}) - \epsilon.$$

Pero esto se tiene para cada $\epsilon > 0$, luego se cumple para $\epsilon = 0$. Por el corolario 1.33 deducimos

$$\beta_{F_{\alpha^*,k}}(x) \geq \text{mín}\,(\frac{\alpha^*-1}{k} + \frac{1}{2r}, \frac{\alpha^*-1/2}{k}) \tag{1.48}$$

para todo $\alpha^* > \alpha_1$, y en particular para $\alpha^* = \alpha$. Además si $\alpha > k + 1/2$ y tomamos $\alpha_2 = \alpha$ y por (1.26) tenemos para $x \in E_r \setminus M_r$, $h = x - a_n/q_n > 0$ que

$$F(x) - F(\frac{a_n}{q_n}) = 2\pi i \zeta_{a_n/q_n}(\alpha - k)h + O(|h|^{\frac{\alpha-1}{k}+\frac{1}{2r_n}-\frac{\epsilon}{r_n}} + |h|^{\frac{\alpha-1/2}{k}-\epsilon})$$

pero por (1.48) sabemos que cuando $(\alpha-1)/k + 1/(2r) > 1$ se cumple

$$F(x) - F(\frac{a_n}{q_n}) = F'(x)h + O(|h|^{\frac{\alpha-1}{k}+\frac{1}{2r}-\epsilon} + |h|^{\frac{\alpha-1/2}{k}-\epsilon})$$

luego

$$(F'(x) - 2\pi i\zeta_{a_n/q_n}(\alpha - k))h = o(|h|)$$

lo que prueba (1.43).

Para probar *ii*), definimos

$$E_{r,0} = (E_r \setminus M_r) \cap \{x : (q_n)_{n\in\mathbb{N}} \subset P_0\},$$

donde $P_0 = \{p \in \mathbb{N} : p \text{ primo }, (p, k-1) = 1\}$. De la misma forma que en el lema 1.45 se prueba $\mathcal{H}^{2/r}(E_{r,0}) > 0$. Teniendo en cuenta que $\tau(a/p) = 0$ si $p \in P_0$, igual que antes se tiene que

$$\beta_{F_{\alpha^*,k}}(x) \geq \frac{\alpha^* - 1/2}{k}$$

para todo $\alpha^* > \alpha_1$.

Por último, para probar *iii*), definimos

$$E_{r,1} = (E_r \setminus M_r) \cap \{x : |(q_n)_{n\in\mathbb{N}} \cap P_1| = \infty, |\tau(a_n/q_n)| \geq q_n^{1/2}/2\}$$

con $P_1 = \{p \in \mathbb{N} : p \text{ primo }, (p, k-1) \neq 1\}$. Usando la proposición 1.20 podemos probar $\mathcal{H}^{2/r}(E_{r,1}) > 0$ siguiendo la demostración del lema 1.45. Si $x \in E_{r,1}$ y $h_n = x - a_n/q_n > 0$ tenemos

$$F_{\alpha_2,k}(x) - F_{\alpha_2,k}(\frac{a_n}{q_n}) = A\tau(\frac{a_n}{q_n})h_n^{\frac{\alpha_2-1}{k}} + 2\pi i\zeta_{a_n/q_n}(\alpha_2 - k)h_n + O(|h_n|^{\frac{\alpha_2-1/2}{k}-\epsilon})$$

pero además para todo $h \in (h_n/2, 2h_n)$ se cumple

$$F_{\alpha_2,k}(\frac{a_n}{q_n}+h)-F_{\alpha_2,k}(\frac{a_n}{q_n}) = A\tau(\frac{a_n}{q_n})h^{\frac{\alpha_2-1}{k}}+2\pi i\zeta_{a_n/q_n}(\alpha_2-k)h+O(|h_n|^{\frac{\alpha_2-1/2}{k}-\epsilon})$$

luego si $r > k$ existe $h_n^* \in (h_n/2, 2h_n)$ tal que

$$|F_{\alpha_2,k}(x) - F_{\alpha_2,k}(\frac{a_n}{q_n} + h_n^*)| \gg q_n^{-\frac{1}{2}}h_n^{\frac{\alpha_2-1}{k}} \gg h_n^{\frac{\alpha_2-1}{k}+\frac{1}{2r_n}},$$

tomando ϵ suficientemente pequeño. Por el corolario 1.33 se tiene

$$\beta_{F_{\alpha^*,k}}(x) = \frac{\alpha^* - 1}{k} + \frac{1}{2r}$$

para todo $\alpha^* \in [\alpha_1, \alpha_2]$, y en particular para $\alpha^* = \alpha$. □

En E_r hay puntos que tienen una irregularidad mucho mayor que la media. Para controlar cual es la cantidad de estos puntos necesitamos el siguiente lema

Lema 1.47. *Sea I un intervalo contenido en $[0,1]$ y $N \in \mathbb{N}$, con $|I| \geq N^{-1}$. Existe un entero n con $N \leq n \leq 2N$, una constante $c > 0$ y un subconjunto $B = B_n$ de*

$$\{a/p^k \in I : (a,p) = 1, 1 \leq a \leq p^k, n \leq p \leq n + n^{1/2}\}$$

con $|B| \geq cn^{k+1/2}(\log n)^{-1}$ tal que todo par de elementos de B están distanciados al menos n^{-k-1}.

Demostración: Por el teorema del número primo podemos encontrar n con $N \leq n \leq 2N$ tal que en el intervalo $[n, n + n^{1/2}]$ haya al menos $n^{1/2}/(4 \log n)$ primos. Si $p, p + d$ son dos primos cualesquiera en $[n, n + n^{1/2}]$, y

$$\frac{a}{p^k} - \frac{b}{(p+d)^k} = \theta \quad |\theta| \leq n^{-k-1},$$

entonces

$$\frac{a+j}{p^k} - \frac{b+j}{(p+d)^k} = \theta + \frac{kjd}{p(p+d)^k} + O(jd^2 n^{-k-2}),$$

luego

$$|\frac{a+j}{p^k} - \frac{b+j}{(p+d)^k}| \geq n^{-k-1}$$

para $1 \leq j \leq c_1 n/d$, c_1 cierta constante. Esto implica que

$$|\{1 \leq a \leq p^k : \exists\, b \in \mathbb{N}, |\frac{a}{p^k} - \frac{b}{(p+d)^k}| < n^{-k-1}\}| \ll |I| d n^{k-1}.$$

Esto implica la existencia de B cumpliendo el enunciado del lema. □

El resultado que obtenemos es

Teorema 1.48. *Para todo $r > 2$, existe $D_r \subset E_r$ tal que*

$$\beta_F(x) = \frac{\alpha - 1}{k} + \frac{1}{kr} \tag{1.49}$$

y con

$$1 + \frac{1}{2k} \leq \dim_{\mathrm{H}} D_r \leq 1 + \frac{1}{k}.$$

Demostración: Sean $1 \leq \alpha_1 < k$ y $k + 1/2 < \alpha_2 < k + 1$ tales que $\alpha_1 \leq \alpha \leq \alpha_2$, y sea

$$B(q) = \bigcup_{\substack{j\in\mathbb{N} \\ q^{-r-1}\leq 2^{-j}\leq q^{-1}}} B((\log q)^4, q, 2^{-j})$$

con $B((\log q)^4, q, 2^{-j})$ el conjunto del enunciado de la proposición 1.27. Como en la demostración del teorema 1.46, teniendo en cuenta que $\tau(a/p^k) = p^{k-1}$ para todo $p > k$ y que $(\alpha - 1)/k + 1/(kr) < (\alpha - 1/2)/k$, se prueba que los puntos de

$$D_r = \{x \in E_r : q_n = p_n^k, p_n \text{ primo }, |\{a_n/q_n : a_n \in B(q_n)\}| < \infty\}$$

tienen la regularidad dada por (1.49). La cota superior para la dimensión de D_r se prueba como en el lema 1.45. Para la inferior, observamos que

$$D_r \supset \bigcap_{n=1}^{\infty} \bigcup_{p\geq n} \bigcup_{\substack{1\leq a\leq p^k \\ a\notin B(p^k)}} I_r(a, p^k)$$

con $I_r(a, p^k)$ definido como en (1.42). Por tanto tenemos que $D_r^* \subset D_r$ con

$$D_r^* = \bigcap_{n=1}^{\infty} \bigcup_{n\leq p\leq n+n^{1/2}} \bigcup_{\substack{1\leq a\leq p^k \\ a\notin B(p^k)}} I_r(a, p^k)$$

Pero $D_r^* = L_r \setminus \Delta$ con

$$L_r = \bigcap_{n=1}^{\infty} \bigcup_{n\leq p\leq n+n^{1/2}} \bigcup_{1\leq a\leq p^k} I_r(a, p^k)$$

y

$$\Delta = \bigcap_{n=1}^{\infty} \bigcup_{n\leq p\leq n+n^{1/2}} \bigcup_{\substack{1\leq a\leq p^k \\ a\in B(p^k)}} I_r(a, p^k)$$

De forma sencilla podemos ver que la $\mathcal{H}^{(1+1/(2k))/r}(\Delta) = 0$. Para ver la dimensión inferior de L_r, usando el lema 1.47 consideramos el conjunto B_n descrito en su enunciado y construimos

$$G_j = \bigcap_{n=1}^{\infty} \bigcup_{a/p^k\in B_{n_j}} I_r(a, p^k)$$

con $n_j = n_{j-1}^j$. Por el lema 1.44 tenemos que

$$s_j \geq \frac{1 + 1/2k}{r}$$

para j suficientemente grande y por tanto $\mathcal{H}^{(1+1/2k)/r}(L_r) > 0$. □

Nota 1.49. De la misma forma que en los últimos dos resultados, podríamos probar para cada $1/k < v < 1/2$ y $r > k$ existe un subconjunto de E_r de dimensión de Hausdorff positiva cuyos puntos tienen exponente Hölder igual a $(\alpha - 1)/k + v/r$.

Sabemos que el subconjunto de E_r aproximado por fracciones del tipo a/p^k tiene dimensión de Minkowski igual a $(1 + 1/k)/r$. Pensamos que esto también se cumple para la dimensión de Hausdorff, lo que podría probarse obteniendo el equivalente al lema 1.47 con p variando entre n y $2n$. Este resultado se deduce a su vez de la desigualdad

$$|\{(a, b, p, q) \in \mathbb{Z}^4 : |ap^k - bq^k| \leq N^\epsilon, |a|+|b|+|p|+|q| \leq N, (p, q) = 1\}| \ll N^{2-\epsilon}$$

para algún $\epsilon > 0$. Por otra parte, es natural suponer que para una función f continua e integrable se cumple

$$\sum_{m \neq 0} \tau_m(\frac{a}{q}) f(\frac{m}{Y}) \ll Y^{\frac{1}{2}} q^{\frac{1}{2}+\epsilon}$$

para cualquier racional a/q. Esto probaría entonces que

$$d_{\mathrm{H}}(\beta) = (k + 1)(\beta - \frac{\alpha - 1}{k}) \qquad \beta \in [\frac{\alpha - 1}{k}, \frac{\alpha - 1/2}{k}).$$

Finalmente, si pensamos que casi todo punto tiene exponente Hölder igual a $(\alpha - 1/2)/k$, podemos conjeturar que el espectro de singularidades de F tiene la forma

$$d_{\mathrm{H}}(\beta) = \begin{cases} 0 & \text{si } \beta = (\alpha - 1/2)/(k - 1) \\ 1 & \text{si } \beta = (\alpha - 1/2)/k \\ (k + 1)(\beta - (\alpha - 1)/k) & \text{si } (\alpha - 1)/k \leq \beta < (\alpha - 1/2)/k \\ -\infty & \text{en otro caso.} \end{cases}$$

Capítulo 2

Medida promedio de clases de formas cuadráticas

2.1. Introducción

Para cada $n \in \mathbb{Z}$ definimos

$$P_n = \{ax^2+bxy+cy^2 : a,b,c \in \mathbb{Z}, (a,b,c) = 1, b^2-4ac = n, n < 0 \Rightarrow a > 0\}, \tag{2.1}$$

el espacio de formas cuadráticas binarias primitivas de discriminante n. El grupo $SL(2,\mathbb{Z})$ actua de forma natural sobre este espacio y el conjunto $SL(2,\mathbb{Z})\backslash P_n$, que como vio Gauss tiene una estructura natural de grupo abeliano, juega un papel fundamental para comprender el comportamiento de las formas y la representación de éstas de números naturales. En particular, es de singular importancia el estudio de su cardinal

$$h(n) = |SL(2,\mathbb{Z})\backslash P_n|,$$

el número de clases de formas de discriminante n.

En Art. 302 y Art. 304 de *Disquisitiones Arithmeticae* [Gau], Gauss consideró el promedio del número de clases cuando varía el discriminante (con la definición actual en realidad sólo para discriminantes múltiplos de 4) . En el primero de dichos artículos, trató el caso de discriminantes negativos y vio que el número de clases crecía de forma regular como la raíz cuadrada del discriminante. De forma precisa, afirmó haber obtenido "mediante una

investigación teórica" una fórmula promedio que podemos escribir como

$$\sum_{n\leq N} h(-4n) = \frac{4\pi}{21\zeta(3)}N^{3/2} - \frac{2}{\pi^2}N + E_2^-(N), \quad \text{con } E_2^-(N) = o(N). \quad (2.2)$$

Es probable que Gauss probase esta afirmación usando la interpretación del número de clases en términos de puntos de retículo (Art. 172, Art. 174 [Gau]): $h(-n)$ es igual al número de puntos en el conjunto

$$\{(a,b,c) \in \mathbb{Z}^3 : b^2 - 4ac = -n, (a,b,c) = 1, -a < b \leq a < c \text{ o } 0 \leq b \leq a = c\} \quad (2.3)$$

En Art. 304 investigó el caso de discriminantes positivos. Gauss vio que el número de clases se comportaba de una forma muy irregular, pero se dio cuenta que al multiplicarlo por el logaritmo de la unidad fundamental se recuperaba la regularidad, creciendo de nuevo como la raíz del discriminante. Gauss escribió: "[. . .] el valor promedio de este producto es aproximadamente expresado por una fórmula del tipo $m\sqrt{D}-n$. Sin embargo, todavía no hemos sido capaces de determinar los valores de las constantes m, n teóricamente. Si se puede sacar alguna conclusión de la comparación de algunos cientos de determinantes, m parece estar muy cerca de 7/3". El valor correcto de m fue dado por Gauss en una de sus notas escritas a mano (ver [Gau] p. 462), donde dice que la demostración "ilustra brillantemente muchas partes de la Aritmética superior y del Análisis". El valor que da para m es $2\pi^2/(7\zeta(3))$, el cual está muy cerca del anteriormente conjeturado por él $(2\pi^2/(7\zeta(3))-7/3 \approx 0{,}01)$. Podemos escribir esta afirmación en notación moderna como

$$\sum_{n\leq N} h(4n)\log\epsilon_{4n} \sim \frac{4\pi^2}{21\zeta(3)}N^{3/2} \quad (2.4)$$

donde $\epsilon_n = (t + u\sqrt{n})/2$, con (t,u) la solución más pequeña de la ecuación de Pell $t^2 - nu^2 = 4$, si n no es un cuadrado. Si lo es, definimos $\epsilon_n = 1$. Más tarde se comprendió el porqué de este comportamiento, a través de la fórmula de Dirichlet (ver [Lan]) para el número de clases:

$$h(d)\log\epsilon_d = d^{\frac{1}{2}}L(1,\chi_d) \qquad \text{para } d > 0 \quad (2.5)$$

y

$$h(d)w_d^{-1} = (2\pi)^{-1}|d|^{\frac{1}{2}}L(1,\chi_d) \qquad \text{para } d < 0, \quad (2.6)$$

con $\chi_d(n) = (d/n)$ el símbolo de Kronecker-Jacobi-Legendre, y

$$w_d = \begin{cases} 2 & \text{si } d < -4 \\ 4 & \text{si } d = -4 \\ 6 & \text{si } d = -3 \end{cases} \tag{2.7}$$

el número de elementos de $SL(2,\mathbb{Z})$ que dejan fija una forma de discriminante $d < 0$.

En 1863 Lipschitz [Lip] y más tarde Mertens [Mer] obtuvieron

$$\sum_{n \le N} h(-4n) = \frac{4\pi}{21\zeta(3)} N^{3/2} + O(N \log N) \tag{2.8}$$

usando (2.3) y contando puntos de retículo de forma trivial, lo que probaba parcialmente lo afirmado por Gauss. Pero la conjetura de Gauss para discriminantes negativos hubo de esperar a 1917, cuando I. M. Vinogradov [Vin1] demostró $E_2^-(N) \ll N^{5/6}(\log N)^{2/3}$ a través de una estimación más precisa de puntos de retículo. Un año más tarde [Vin2] mejoró este resultado hasta $E_2^-(N) \ll N^{3/4}(\log N)^2$ introduciendo en el problema el análisis de Fourier mediante la fórmula

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

La afirmación de Gauss para discriminantes positivos (2.4) fue también demostrada por Vinogradov [Vin3] en 1919. Usó la fórmula de Dirichlet (2.5), y para acotar el término de error tuvo que controlar sumas incompletas de caracteres, empleando la importante desigualdad

$$\sum_{n \le x} \chi_d(n) \ll d^{\frac{1}{2}} \log d, \tag{2.9}$$

que fue obtenida al mismo tiempo e independientemente por G. Pólya [Pól]. Con ella, Vinogradov dedujo

$$\sum_{n \le N} h(4n) \log \epsilon_{4n} = \frac{4\pi^2}{21\zeta(3)} N^{3/2} + O(N \log N). \tag{2.10}$$

También comprobó que se podía usar (2.6) para obtener (2.8), lo que no superaba lo obtenido por él anteriormente. Años más tarde Vinogradov [Vin4,

Vin5, Vin6] y J.-R. Chen [Che1, Che2] demostraron, acotando ciertas sumas trigonométricas a través del método de Van der Corput, que el término de error $o(N)$ en la fórmula (2.2) era en realidad $O(N^{2/3+\epsilon})$.

En 1944 C. L. Siegel [Sie] redescubrió el uso de los caracteres para este problema, probando (2.8) y (2.10). Todo hace suponer que no tenía conocimiento de los artículos de I. M. Vinogradov, y de hecho en su trabajo uso el artículo de Pólya para acotar sumas cortas de caracteres. Pero lo importante para nuestro trabajo es que Siegel también probó (2.10) de otra forma. En el caso en que el discriminante es negativo, se puede identificar una forma $ax^2 + bxy + cy^2$ con el único punto del plano hiperbólico $\mathfrak{H}$ solución de la ecuación $az^2 + bz + c = 0$. Además, la acción de $SL(2, \mathbb{Z})$ sobre las formas se transforma en la acción habitual de $SL(2, \mathbb{Z})$ sobre $\mathfrak{H}$. Así, la condición de que la forma (a, b, c) esté en el conjunto (2.3) equivale a que z esté en el dominio fundamental (o en parte la mitad izquierda de su frontera)

$$\mathcal{F} = \{x + iy : x^2 + y^2 > 1, |x| < \frac{1}{2}\}. \tag{2.11}$$

Cuando el discriminante es positivo, $az^2 + bz + c = 0$ tiene dos raíces reales $\rho_- < \rho_+$. Lo que hizo Siegel fue considerar $\mathfrak{H}$ provisto con la métrica hiperbólica $ds^2 = y^{-2}(dx^2 + dy^2)$, y asociar a la forma $ax^2 + bxy + cy^2$ la geodésica g_{abc} que pasa por los puntos ρ_- y ρ_+ con un sentido dado por la desigualdad $a(\rho_- - \rho_+) > 0$. Además asoció a esta forma una cantidad

$$\mu(a, b, c) = \ell(g_{abc} \cap \mathcal{F}),$$

la longitud hiperbólica del arco intersección de g_{abc} con el dominio fundamental.

Si A es un arco determinado por los puntos z_1 y z_2 en la geodésica que va de ρ_- a ρ_+, entonces es fácil calcular la expresión

$$\ell(A) = \int_{\lambda_1}^{\lambda_2} \frac{d\lambda}{\lambda} = \log \frac{\lambda_2}{\lambda_1}, \tag{2.12}$$

donde λ_j es la tangente del argumento de $z_j - \rho_-$.

De esta manera, tomando un representante g_{abc} de una clase, tenemos que los elementos de $SL(2, \mathbb{Z})$ que dejan fijo a g_{abc} actúan sobre los puntos de la geodésica. Como este grupo está generado por el elemento

$$\begin{pmatrix} (t - bu)/2 & -cu \\ au & (t + bu)/2 \end{pmatrix} \qquad \text{con } \epsilon_n = (t + u\sqrt{n})/2$$

podemos tomar como "dominio" fundamental un arco J, que por (2.12) tendrá longitud hiperbólica igual a $\log \epsilon_n^2$.

Por una parte, para cada punto $z_0 \in J$ existe un único $f \in PSL(2,\mathbb{Z})$ tal que $f(z_0) \in \mathcal{F}$, y por tanto $A_{z_0} = f(J) \cap \mathcal{F}$ es un arco distinto de vacío. Por otra, para cada geodésica que interseque con $\mathcal{F}$ existe un único elemento de $PSL(2,\mathbb{Z})$ que la lleva a un arco contenido en J. De esta manera, hay un número finito de arcos disjuntos dos a dos y cuya unión es J que son las únicas imágenes por un elemento de $SL(2,\mathbb{Z})$ de arcos de geodésicas contenidos en $\mathcal{F}$. Sumando sobre todas las clases de discriminante $n > 0$ obtenemos

$$h(n) \log \epsilon_n^2 = \sum_{\substack{(a,b,c)\in\mathbb{Z}^3 \\ (a,b,c)=1 \\ b^2-4ac=n}} \mu(a,b,c). \tag{2.13}$$

Teniendo en cuenta que $\mu(\lambda a, \lambda b, \lambda c) = \mu(a,b,c)$ para todo $\lambda \in \mathbb{R}$ no nulo, esta fórmula permitió a Siegel controlar $\sum_{n\leq x} h(n) \log \epsilon_n$ a través de la integral

$$\int\limits_{0<b^2-4ac<1} \mu(a,b,c)\, da\, db\, dc.$$

La fórmula (2.13) es un equivalente de la expresión (2.3) para discriminantes positivos.

Además, Siegel generalizó este procedimiento a formas cuadráticas en más variables. Para $n \in \mathbb{N}$ con $n \geq 2$, consideramos la acción del grupo $GL(n,\mathbb{R})$ sobre el conjunto $V^{(n)}$ de matrices simétricas reales de dimensión n (es decir, de formas cuadráticas con n variables) dada por $(g,x) \mapsto gxg^t$. Sea $GL(n,\mathbb{R})_x$ el grupo de isotropía de $x \in V_{\mathbb{Q}}^{(n)} = V^{(n)} \cap M_n(\mathbb{Q})$ con respecto a esta acción. Entonces, podemos considerar en los subgrupos $G_x = GL(n,\mathbb{R})_x \cap SL(n,\mathbb{R})$ y $\Gamma_x = G_x \cap SL(n,\mathbb{Z})$ las medidas de Haar naturales (en el primer grupo la inducida por la acción que acabamos de describir y en el segundo la medida de contar), que inducen en el espacio homogéneo $H_x = G_x/\Gamma_x$ una medida invariante (ver [Wei]). Sea m_x tal medida, entonces definimos

$$\nu(x) = m(H_x)$$

cuando H_x es compacto. H_x es siempre compacto excepto cuando $n = 2$ y x es una forma que descompone en producto de dos formas de grado 1 (es decir, cuando el discriminante es un cuadrado). En este último caso Γ_x es finito y $m(H_x) = \infty$ por lo que definimos $\nu(x) = 0$.

Se puede comprobar que $\nu(x)$ no varía cuando x se mantiene en la misma clase con respecto a $SL(n,\mathbb{Z})$. En el caso $n=2$ tenemos que $\nu(x)=2w_d^{-1}$ si el discriminante es negativo y $\nu(x)=\log\epsilon_d^2$ si es positivo. Para $n>2$, $\nu(x)$ en general va a variar para distintas clases con el mismo determinante, pero se puede obtener (como hizo Siegel) la fórmula promedio

$$\sum_{\substack{x\in SL(n,\mathbb{Z})\backslash L_i \\ |\det x|<N}} \nu(x) = \frac{1}{n+1}\big(\prod_{k=2}^{n}\zeta(k)\big)N^{\frac{n+1}{2}} + O(N^{\frac{n}{2}}), \tag{2.14}$$

donde L_i es el retículo de formas con coeficientes enteros de signatura $0 \leq i \leq n$. La forma de conseguirlo es similar a la usada para llegar a (2.13), relacionando una forma cualquiera con formas definidas positivas y seleccionando las que intersequen con el dominio fundamental de Minkowski (ver [Sie]).

Esta nueva interpretación del número de clases para discriminantes positivos abría la puerta al uso del análisis de Fourier. Esto fue materializado de una forma muy precisa por T. Shintani [Shi]. M. Sato y T. Shintani [SS] desarrollaron en la decada de los 70 el concepto de espacio vectorial prehomogéneo, asociando una función zeta a este tipo de espacio y obteniendo ecuaciones funcionales. En el caso de formas cuadráticas, para $n \geq 3$ Shintani asoció a cada retículo L en $V_{\mathbb{Q}}^{(n)}$ invariante por el grupo $SL(n,\mathbb{Z})$ la función zeta

$$\xi_i^{(n)}(s,L) = \sum_{x\in SL(n,\mathbb{Z})\backslash L_i} \nu(x)|\det x|^{-s}, \tag{2.15}$$

con $L_i = L\cap V_i^{(n)}$ y $V_i^{(n)}$ el conjunto de matrices simétricas de dimensión n y signatura i, que converge para $\Re s > (n+1)/2$ por (2.14). Usando el análisis de Fourier sobre el espacio homogeneo $V_i^{(n)} = GL(n,\mathbb{R})/GL(n,\mathbb{R})_x$ probó que $\xi_i^{(n)}$ es una función meromorfa con posibles polos en $s=(n+1-j)/2$ $(0\leq j\leq n-1)$, y que satisface la ecuación funcional

$$\xi_i^{(n)}(\frac{n+1}{2}-s,L) = v(L)^{-1}\sum_{j=0}^{n} u_{j,i}(s)\xi_j^{(n)}(s,L^*) \tag{2.16}$$

donde $u_{ij}(s)$ son productos de funciones Γ y exponenciales, $v(L)$ es el volumen de un paralelogramo fundamental de L, y L^* es el retículo dual de L

$$L^* = \{x\in V^{(n)} : \mathrm{tr}(xy)\in\mathbb{Z}\,\forall y\in L\}.$$

El caso $n = 2$ es anómalo debido a que $m(H_x) = \infty$ para las formas descomponibles. Esto hace necesario un cambio de definición para la función $\xi_1^{(2)}$. En el caso que L sea el retículo

$$L = \{\begin{pmatrix} a & b/2 \\ b/2 & c \end{pmatrix} : a, b, c \in \mathbb{Z}\},$$

se cumple que L^* es el conjunto de matrices simétricas con coeficientes en $\mathbb{Z}$. En este caso Shintani definió

$$\xi_1^{(2)}(s, L) = \sum_{x \in SL(2,\mathbb{Z})\backslash L_1} \nu(x) |\det x|^{-s} + 4^{s-1} B(s) \tag{2.17}$$

con $B(s) = \zeta(2s-1)(\zeta'(2s)\zeta(2s)^{-1} - \zeta'(2s-1)\zeta(2s-1)^{-1})$ y

$$\xi_1^{(2)}(s, L^*) = \sum_{x \in SL(2,\mathbb{Z})\backslash L_1^*} \nu(x) |\det x|^{-s} + \frac{B(s)}{2} + \frac{\log 2}{4} \frac{\zeta(2s-1)}{1 - 2^{-2s}}. \tag{2.18}$$

Obtuvo que esta función es meromorfa con polos en $s = 1$ y $s = 3/2$ y se cumplen las ecuaciones funcionales

$$\xi_i^{(2)}(s)(\frac{3}{2} - s) = \sum_{j=0}^{2} u_{j,i}(s) \xi_j^{(2)}(s, L^*) + \chi_i(s) \tag{2.19}$$

para cierta función meromorfa $\chi_i(s)$ que especificaremos más tarde. Usando una modificación de un lema de Landau supo extraer de los polos de la función los términos principales de la suma de sus coeficientes y así probó

$$\sum_{n \leq N} h(4n) \log \epsilon_{4n} = \frac{4\pi^2}{21\zeta(3)} N^{\frac{3}{2}} - \frac{4}{\pi^2} N(\log N + C') + E_2^+(N) \tag{2.20}$$

con $C' = -1 + (8/3)\log 2 + \log(2\pi) - \zeta'(2)\zeta(2)^{-1}$ y $E_2^+(N) \ll N^{\frac{3}{4}}$, lo que por una parte mostraba el fallo en la intuición de Gauss para el segundo término, y por otro que el error obtenido por Vinogradov y Siegel no se podía mejorar. De la misma manera obtuvo una formula similar para el promedio de $h(n) \log \epsilon_n$.

La cota dada por Chen y Vinogradov para E_2^- permaneció intacta hasta que F. Chamizo y H. Iwaniec [CI1, CI2] tuvieron la gran idea de mezclar los dos métodos usados hasta entonces, el análisis de Fourier y las sumas

de caracteres. Lo que hicieron fue primero expresar la suma en términos de sumas

$$\sum_{n\leq M} N_-(n) \tag{2.21}$$

donde

$$N_-(n) = 2\sum_{k^2|n} h(-n/k^2)w^{-1}_{-n/k^2}, \tag{2.22}$$

que es lo que aparecía como coeficiente en una de la funciones zeta de Shintani. Así, dividieron la suma (2.21) como

$$\sum_{n\leq M} N_-(n) = \sum_{n\leq M+\Delta} N_-(n)g(n) - \sum_{M\leq n\leq M+\Delta} N_-(n)g(n)$$

con $\Delta \ll M^{1/2}$ y $g \in C_0^\infty((0,\infty))$ con $g = 1$ en $[1, M]$ y soporte contenido en $(0, M + \Delta)$. Desde el trabajo de Voronoi era conocido que a partir de cierto tipo de ecuaciones funcionales para funciones zeta, se pueden deducir fórmulas de sumación. Con ello, partiendo de (2.19), trataron la primera suma. La segunda, la transformaron en una suma doble de caracteres gracias a (2.6). La diferencia de los caracteres con respecto a las exponenciales es que al multiplicarlos se multiplica el argumento (mientras que en las exponenciales se suma). Esto permite, a través de la desigualdad de Cauchy, "alargar" las sumas. Para obtener el mejor resultado usaron una estimación muy precisa para sumas dobles de caracteres reales [HB1, HB2] de Heath-Brown consiguiendo

$$|E_1^-(N)| + |E_2^-(N)| \ll N^{\frac{21}{32}+\epsilon} \qquad \text{para todo } \epsilon > 0, \tag{2.23}$$

donde $E_1^-(N)$ es el término de error que equivale a $E_2^-(N)$ cuando promediamos sobre todos los discriminantes.

En este capítulo estudiaremos el caso de discriminantes positivos, exponiendo los resultados obtenidos en [CU1] y [Ubi]. Para acotar E_1^+ y E_2^+ seguiremos la forma de proceder de Chamizo e Iwaniec a través de la interpretación (2.13) para el número de clases de Siegel. También estudiaremos el comportamiento de los términos de error en promedio.

En la primera sección usamos las ecuaciones funcionales de Shintani para obtener fórmulas de sumación, a través de la transformada de Mellin.

En la segunda, veremos como la interpretación de Siegel del número de clases para discriminantes positivos en términos de longitudes de arcos de geodésicas nos permite controlar la sumas exponenciales que aparecen en las fórmulas de sumación.

En la tercera usando las secciones anteriores y el resultado para sumas de caracteres [HB2] obtendremos

Teorema 2.1. *Para todo $\alpha > 21/32$ se cumple que $E_1^+(N) \ll N^\alpha$, donde*

$$\sum_{n\leq N} h(n)\log\epsilon_n = \frac{\pi^2}{18\zeta(3)}N^{3/2} - \frac{3}{\pi^2}(C+\log N)N + E_1^+(N)$$

y $C = \log(2\pi) - \zeta'(2)/\zeta(2) - 1$.

De igual modo llegaremos a

Teorema 2.2. *Para todo $\alpha > 21/32$ se cumple que $E_2^+(N) \ll N^\alpha$, donde*

$$\sum_{n\leq N} h(4n)\log\epsilon_{4n} = \frac{4\pi^2}{21\zeta(3)}N^{3/2} - \frac{4}{\pi^2}(C'+\log N)N + E_2^+(N)$$

y $C' = \log(2\pi) + 8(\log 2)/3 - \zeta'(2)/\zeta(2) - 1$.

En general, este procedimiento se podría aplicar al estudio del promedio de $h(n)\log\epsilon_n$ y $h(-n)$ sobre cualquier progresión aritmética. Esto podría permitirnos probar de otra manera la fórmula obtenida en [GH] para el promedio sobre discriminanes fundamentales, es decir, sobre los cuerpos cuadráticos.

En la última sección estudiaremos el comportamiento de los términos de error. Se conoce [Cho, GS] que

$$L(1,\chi_d) \geq e^\gamma(\log\log|d| - 10) \tag{2.24}$$

para infinitos discriminantes d. Por (2.5) y (2.6) deducimos que $E_1^+(n) = \Omega(\sqrt{d}\log\log d)$ y lo mismo para el resto de términos de error. Por otra parte, de las fórmulas de sumación obtenidas en [CI2] (y de las que obtendremos en la primera sección) se deduce una expresión en términos de sumas de exponenciales para el término de error en el promedio de $N_-(n)$ (y de $N_+(n)$). Esto ha sido utilizado [Küh] (cf. [Tsa]) para estudiar la norma dos de estos términos de error, deduciendo que son $\Omega_\pm((n\log n)^{1/2})$. Para usar este método en el estudio de $E_j^+(N)$ primero se debe usar la fórmula de inversión de Möbius, para pasar de $N_+(n)$ a $h(n)\log\epsilon_n$. Pero si ahora queremos hallar la norma 2 de esta expresión, parece difícil controlar los términos no diagonales que surgen. Lo que se puede hacer (ver [Pet]) es, introduciendo valores absolutos, dar la acotación

$$(\sum_{N\leq x}|E_j^+(N)|^2)^{\frac{1}{2}} \ll x^{\frac{1}{2}}(\log x)^{\frac{3}{2}}. \tag{2.25}$$

En vez de seguir este camino, nosotros usaremos la fórmula de Dirichlet (2.5) y trabajando con sumas de caracteres obtendremos

Teorema 2.3. *Para todo* $K \ll x^{\frac{1}{4}-\epsilon}$ *se cumple*

$$\sum_{N\leq x} |E_2^+(N+K) - E_2^+(N)|^2 = (\frac{3P}{4\pi})^2 x^2 \log K + O(x^2 (\log K)^{\frac{2}{3}}),$$

con

$$P = \prod_{p\neq 2} (1 - \frac{1}{p^2(p+1)}).$$

Este resultado nos permite deducir que

$$E_2^+(N) = \Omega((N\log N)^{\frac{1}{2}}),$$

pero además que E_2^+ es una función oscilante, porque sabemos que el promedio $\sum_{n<x} E_2^+(N)$ es pequeño. Podemos probar lo mismo para $E_j^{\pm}(N)$.

Es natural preguntarse si tenemos una fórmula para el promedio del número de clases en el caso de discriminantes positivos. En este caso se comporta de una forma muy irregular, sobre todo influenciada a través de la ecuación (2.5) por la distribución caótica de la solución fundamental de la ecuación de Pell. Ni siquiera es conocida la existencia de infinitos cuerpos cuadráticos con número de clases 1, que corresponden a dominios de factorización única, la llamada conjetura de Gauss-Hasse. En 1984 C. Hooley [Hoo] obtuvo

$$\sum_{\substack{n\leq x \\ \epsilon_n \leq n^{1/2+\alpha}}} 1 \sim \frac{4\alpha^2}{\pi^2} x^{\frac{1}{2}} (\log x)^2 \tag{2.26}$$

en el rango $0 \leq \alpha \leq 1/2$, de donde se deduce

$$\sum_{\substack{n\leq x \\ \epsilon_n \leq n^{1/2+\alpha}}} h(n) \sim \frac{4}{\pi^2}(2\alpha - \log(1+2\alpha)) x \log x.$$

Además, por argumentos heurísticos sobre la distribución de ϵ_n llegó a la conjetura

$$\sum_{n\leq x} h(n) \sim \frac{25}{12\pi^2} x (\log x)^2.$$

Por otra parte, P. Sarnak [Sar] ha obtenido como consecuencia de la fórmula de la traza de Selberg una fórmula para el promedio en relación al tamaño del discriminante

$$\sum_{\epsilon_n \leq x} h(n) = \mathrm{Li}(x^2) + O(x^{\frac{3}{2}}(\log x)^2).$$

2.2. Fórmulas de sumación

Voronoi [Vor1, Vor2] usó la ecuación funcional de $\zeta(s)^2 = \sum_{n=1}^{\infty} d(n)n^{-s}$, donde $\zeta(s)$ es la función zeta de Riemann, para obtener una fórmula para el promedio de la función divisor. A partir de ese momento, se ha entendido [CR] que en ciertos contextos una ecuación funcional para una serie de Dirichlet equivale a una fórmula de sumación para sus coeficientes. Las funciones zeta de Shintani van a tener como coeficientes los números $N_+(n)$ y $N_-(n)$, dónde $N_-(n)$ se define como en (2.22) y

$$N_+(n) = \sum_{k^2|n} h(n/k^2) \log \epsilon_{n/k^2}.$$

De esta forma, a partir de la ecuación funcional obtendremos fórmulas de sumación para estos coeficientes. Con ellas podemos recuperar los promedios para $h(-n)$ y $h(n)\log\epsilon_n$ por la siguiente fórmula de inversión de Möbius

Lema 2.4. *Para $n \geq 1$*

$$h(n)\log\epsilon_n = \sum_{k^2|n} \mu(k) N_+(n/k^2)$$

y

$$h(4n)\log\epsilon_{4n} = \sum_{\substack{k^2|n \\ 2\nmid k}} \mu(k)\big(N_+(4n/k^2) - N_+(n/k^2)\big).$$

Demostración: La primera fórmula es directa. Para la segunda vemos que

$$\begin{aligned} h(4n)\log\epsilon_{4n} &= \sum_{k^2|4n} \mu(k) N_+(4n/k^2) = \sum_{2\nmid k} + \sum_{2|k} \\ &= \sum_{\substack{k^2|n \\ 2\nmid k}} \mu(k) N_+(4n/k^2) + \sum_{k^2|n} \mu(2k) N_+(n/k^2) \end{aligned}$$

y el resultado se obtiene porque $\mu(2k) = -\mu(k)$ para k impar y $\mu(2k) = 0$ para k par. □

Para facilitar la exposición, vamos a cambiar la notación con respecto a Shintani. En el semiplano $\Re s > 2$ definimos

$$\xi_2^-(s) = \sum_{n=1}^{\infty} \frac{N_-(4n)}{\sqrt{4n}}(\sqrt{4n})^{-s} \qquad \xi_1^-(s) = \sum_{n=1}^{\infty} \frac{N_-(n)}{\sqrt{n}}(\sqrt{n})^{-s}$$

$$\xi_1^+(s) = \sum_{n=1}^{\infty} \frac{N_+(n)}{\sqrt{n}}(\sqrt{n})^{-s} + \zeta(s)\left(\frac{\zeta'(s+1)}{\zeta(s+1)} - \frac{\zeta'(s)}{\zeta(s)}\right)$$

$$\xi_2^+(s) = \sum_{n=1}^{\infty} \frac{N_+(4n)}{\sqrt{4n}}(\sqrt{4n})^{-s} + 2^{-s}\zeta(s)\left(\frac{\zeta'(s+1)}{\zeta(s+1)} - \frac{\zeta'(s)}{\zeta(s)}\right) + \frac{\zeta(s)\log 2}{2^{s+1}-1}.$$

La relación con las funciones zeta de Shintani es

$$\begin{aligned}
\xi_1^{(2)}(s, L^*) &= \zeta(2)^{-1}\xi_2^+(2s-1) + c_1 2^{1-2s}\zeta(2s-1) \\
\xi_1^{(2)}(s, L) &= \zeta(2)^{-1}\xi_1^+(2s-1) + c_1\zeta(2s-1) \\
\xi_2^{(2)}(s, L^*) &= \zeta(2)^{-1}\pi\xi_2^-(2s-1) \\
\xi_2^{(2)}(s, L) &= \zeta(2)^{-1}\pi\xi_1^-(2s-1),
\end{aligned}$$

donde c_1 es el residuo de $\zeta^2(s)/\zeta(2s)$ en $s = 1$. Entonces, escribiendo

$$\vec{z}_2(s) = \begin{pmatrix} \xi_2^+(s) \\ \xi_2^-(s) \end{pmatrix} \qquad \text{y} \qquad \vec{z}_1(s) = \begin{pmatrix} \xi_1^+(s) \\ \xi_1^-(s) \end{pmatrix}$$

podemos poner las ecuaciones funcionales de Shintani (Teorema 2 de [Shi]) en la forma

Teorema 2.5. *Cada una de las componentes de los vectores*

$$\vec{z}_2(s) - \frac{1}{s-2}\begin{pmatrix} \pi^2/12 \\ \pi/12 \end{pmatrix} + \frac{1}{(s-1)^2}\begin{pmatrix} 1/2 \\ 0 \end{pmatrix} + \frac{1}{s-1}\begin{pmatrix} \log(2\pi)/2 \\ 1/4 \end{pmatrix}$$

y

$$\vec{z}_1(s) - \frac{1}{s-2}\begin{pmatrix} \pi^2/6 \\ \pi/6 \end{pmatrix} + \frac{1}{(s-1)^2}\begin{pmatrix} 1 \\ 0 \end{pmatrix} + \frac{1}{s-1}\begin{pmatrix} \log(2\pi) \\ 1/2 \end{pmatrix}$$

tiene extensión entera de orden 1 al plano complejo. Además, se cumple

$$\vec{z}_1(1-s) = (2\pi)^{-s}\Gamma(s)(\mathcal{A}(s)\vec{z}_2(s) - \cos(\pi s/2)\zeta(s)\vec{B}(s)).$$

donde

$$\mathcal{A}(s) = 2^{s+1}\begin{pmatrix}\cos(\pi s/2) & \pi \\ 0 & -\operatorname{sen}(\pi s/2)\end{pmatrix}\ ,\ \ \vec{B}(s) = \begin{pmatrix}\psi(s/2) - \psi((s+1)/2) \\ \sec(\pi s/2)\end{pmatrix}$$

con $\psi(s) = \Gamma'(s)/\Gamma(s)$.

Veamos en qué fórmulas de sumación se transforman estas ecuaciones funcionales. Definiendo α_n y β_n como los coeficientes de las series de Dirichlet

$$\zeta(s)\left(\frac{\zeta'(s+1)}{\zeta(s+1)} - \frac{\zeta'(s)}{\zeta(s)}\right)$$

y

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

respectivamente, podemos expresar nuestro resultado como

Proposición 2.6. *Sea* $g \in C_0^\infty\big((0,\infty)\big)$. *Entonces*

$$\begin{aligned}\sum_{n=1}^{\infty}\frac{N_+(n)}{\sqrt{n}}g(\sqrt{n}) = \frac{\pi^2}{6}\int_0^\infty tg(t)\,dt - \int_0^\infty g(t)\log(2\pi t)\,dt - \sum_{n=1}^{\infty} g(n)\log n \\ + \sum_{d=1}^{\infty}\frac{\Lambda(d)}{d}\sum_{n=1}^{\infty} g(dn) + 2\sum_{n=1}^{\infty}\frac{N_+(4n)}{\sqrt{4n}}\widetilde{g}(\sqrt{4n}) + 2\sum_{n=1}^{\infty}\beta_n\widetilde{g}(n) \\ +2\pi\sum_{n=1}^{\infty}\frac{N_-(4n)}{\sqrt{4n}}\int_0^\infty g(t)e^{-\pi\sqrt{4n}t}\,dt + 2\int_0^1\frac{1}{t(1+t)}\sum_{n=1}^{\infty}\widetilde{g}(2n/t)\,dt\end{aligned}$$

donde $\widetilde{g}$ *es la transformada de Fourier coseno* $\int g(t)\cos(\pi x t)\,dt$.

Demostración: La fórmula de sumación del enunciado es equivalente a

$$\begin{aligned}\sum_{n=1}^{\infty} b_{1n}^+ g(\sqrt{n}) &= \frac{\pi^2}{6}\int_0^\infty tg(t)\,dt - \int_0^\infty g(t)\log(2\pi t)\,dt + 2\sum_{n=1}^{\infty} b_{2n}^+\widetilde{g}(\sqrt{n}) \\ &+ 2\pi\sum_{n=1}^{\infty} b_{2n}^-\int_0^\infty g(t)e^{-\pi\sqrt{n}t}\,dt + 2\int_0^1\frac{1}{t(1+t)}\sum_{n=1}^{\infty}\widetilde{g}(2n/t)\,dt\end{aligned}$$

donde b_{in}^+ y b_{in}^- se definen mediante las expresiones $\xi_i^+(s) = \sum b_{in}^+(\sqrt{n})^{-s}$ y $\xi_i^-(s) = \sum b_{in}^-(\sqrt{n})^{-s}$.

Por la fórmula de inversión para la transformada de Mellin se cumple

$$\sum_{n=1}^{\infty} b_{1n}^+ g(\sqrt{n}) = \frac{1}{2\pi i} \int_{\sigma-i\infty}^{\sigma+i\infty} \mathcal{M}_g(s)\xi_1^+(s)ds$$

con $2 < \sigma < 3$ y $\mathcal{M}_g(s)$ la transformada de Mellin de g. Por el Teorema 2.5 se tiene

$$\xi_1^+(1-s) = \pi^{-s}\Gamma(s)\big(2\pi\xi_2^-(s) + 2\cos(\frac{\pi}{2}s)\xi_2^+(s) - 2^{-s}\cos(\frac{\pi}{2}s)B_1(s)\zeta(s)\big) \tag{2.27}$$

donde B_1 es la primera coordenada de $\vec{B}$. Esta ecuación asegura (por convexidad) que $\xi_1^+(s)$ crece como un polinomio sobre líneas verticales, luego por el decaimiento de $\mathcal{M}_g(s)$ podemos mover la línea de integración a $-2 < \sigma' < -1$. Así, por el teorema de los residuos y teniendo en cuenta los polos de las funciones involucradas (ver Teorema 2.5) deducimos que

$$\begin{aligned}\sum_{n=1}^{\infty} b_{1n}^+ g(\sqrt{n}) &= \frac{1}{2\pi i} \int_{\sigma'-i\infty}^{\sigma'+i\infty} \mathcal{M}_g(s)\xi_1^+(s)\, ds + \frac{\pi^2}{6}\mathcal{M}_g(2) \\ &\quad -\mathcal{M}_g'(1) - \log(2\pi)\mathcal{M}_g(1).\end{aligned}$$

Además, por (2.27)

$$\frac{1}{2\pi i} \int_{\sigma'-i\infty}^{\sigma'+i\infty} \mathcal{M}_g(s)\xi_1^+(s)ds = I_1 + I_2 + I_3$$

donde

$$\begin{aligned} I_1 &= 2\pi\frac{1}{2\pi i} \int_{\sigma-i\infty}^{\sigma+i\infty} \mathcal{M}_g(1-s)\pi^{-s}\Gamma(s)\xi_2^-(s)\, ds \\ I_2 &= 2\frac{1}{2\pi i} \int_{\sigma-i\infty}^{\sigma+i\infty} \mathcal{M}_g(1-s)\pi^{-s}\Gamma(s)\cos(\frac{\pi}{2}s)\xi_2^+(s)\, ds \\ I_3 &= -\frac{1}{2\pi i} \int_{\sigma-i\infty}^{\sigma+i\infty} \mathcal{M}_g(1-s)(2\pi)^{-s}\Gamma(s)\cos(\frac{\pi}{2}s)B_1(s)\zeta(s)ds \end{aligned}$$

Usando la expansión en serie de Dirichlet de $\xi_2^+(s)$ y moviendo la línea de integración a $0 < \sigma'' < 1$ obtenemos

$$I_2 = 2\sum_{n=1}^{\infty} b_{2n}^+ \frac{1}{2\pi i} \int_{\sigma''-i\infty}^{\sigma''+i\infty} \mathcal{M}_g(1-s)(\pi\sqrt{n})^{-s}\Gamma(s)\cos(\frac{\pi}{2}s)\, ds.$$

En esta zona tenemos la representación $\Gamma(s)\cos(\pi s/2) = \int_0^\infty t^{s-1}\cos t \ dt$, [GR] 17.43.3, luego

$$I_2 = 2\sum_{n=1}^{\infty} b_{2n}^+ \int_0^\infty \frac{1}{2\pi i}\int_{\sigma''-i\infty}^{\sigma''+i\infty} \mathcal{M}_g(1-s)t^{s-1}\, ds\cos(\pi\sqrt{n}t)\, dt$$

y por la fórmula de inversión para la transformada de Mellin se sigue

$$I_2 = 2\sum_{n=1}^{\infty} b_{2n}^+ \widetilde{g}(\sqrt{n}).$$

Igualmente obtenemos

$$I_1 = 2\pi\sum_{n=1}^{\infty} b_{2n}^- \int_0^\infty g(t)e^{-\pi t\sqrt{n}}\, dt.$$

Por otra parte, por la fórmula

$$B_1(s) = -2\int_0^1 \frac{x^s}{1+x}\frac{dx}{x}$$

en $\Re s > 0$ (ver [GR] 8.371.1), podemos escribir

$$I_3 = 2\int_0^1 \frac{1}{2\pi i}\int_{\sigma-i\infty}^{\sigma+i\infty} \mathcal{M}_g(1-s)(2\pi x^{-1})^{-s}\Gamma(s)\cos(\frac{\pi}{2}s)\zeta(s)\, ds\ \frac{1}{1+x}\frac{dx}{x},$$

y expandiendo ζ como serie de Dirichlet llegamos a

$$I_3 = 2\int_0^1 \sum_{n=1}^{\infty} \widetilde{g}(2nx^{-1})\frac{1}{1+x}\frac{dx}{x},$$

procediendo como en el caso de I_2. □

La fórmula de sumación dual es la siguiente

Proposición 2.7. *Sea $g \in C_0^\infty\big((0,\infty)\big)$. Entonces*

$$\begin{aligned}\sum_{n=1}^{\infty}\frac{N_+(4n)}{\sqrt{4n}}g(\sqrt{4n}) &= \frac{\pi^2}{12}\int_0^\infty tg(t)\, dt - \frac{1}{2}\int_0^\infty g(t)\log(2\pi t)\, dt - \sum_{n=1}^{\infty} g(2n)\log n \\ &+ \sum_{d=1}^{\infty}\frac{\Lambda(d)}{d}\sum_{n=1}^{\infty} g(2dn) - \log 2\sum_{k=1}^{\infty}2^{-k}\sum_{n=1}^{\infty} g(2^k n) + \sum_{n=1}^{\infty}\frac{N_+(n)}{\sqrt{n}}\widetilde{g}(\sqrt{n}) \\ &+ \sum_{n=1}^{\infty}\alpha_n\widetilde{g}(n) + \pi\sum_{n=1}^{\infty}\frac{N_-(n)}{\sqrt{n}}\int_0^\infty g(t)e^{-\pi\sqrt{n}t}\, dt - \int_0^1 \frac{1}{t(1+t)}\sum_{n=1}^{\infty}\widetilde{g}(n/t)\, dt\end{aligned}$$

Demostración: Procedemos como en la prueba de la proposición anterior, pero partiendo de la ecuación funcional

$$\xi_2^+(1-s) = \pi^{-s}\Gamma(s)\big(\pi\xi_1^-(s) + \cos(\frac{\pi}{2}s)\xi_1^+(s) - \frac{1}{2}\cos(\frac{\pi}{2}s)B_1(s)\zeta(s)\big),$$

que deducimos del Teorema 2.5 por la ecuación

$$B_1(1-s) + B_1(s) = -2\pi\csc(\pi s).$$

□

2.3. Sumas exponenciales

Hemos visto que en las fórmulas de sumación de las proposiciones 2.6 y 2.7 aparecen unos términos principales, y otros oscilatorios que van a depender de sumas del tipo

$$\sum N_+(n)e(R\sqrt{n}) \qquad \text{y} \qquad \sum N_+(4n)e(R\sqrt{n})$$

con R un cierto parámetro. Para poder tratar esta suma vamos a escribir $N_+(n)$ como una suma sobre puntos de retículo. Para ello usamos la cantidad definida en la introducción

$$\mu(a,b,c) = \ell(g_{abc} \cap \mathcal{F})$$

donde g_{abc} es la geodésica definida por la ecuación $a(x^2+y^2)+bx+c=0$, $y>0$. Sumando (2.13) para todo $k^2 \mid n$ y teniendo en cuenta que $\mu(\lambda a, \lambda b, \lambda c) = \mu(a,b,c)$ obtenemos

Lema 2.8. *Sea $n \in \mathbb{Z}^+$ distinto de un cuadrado. Entonces*

$$N_+(n) = \sum_{\substack{b^2-4ac=n \\ a>0}} \mu(a,b,c).$$

Es fácil ver que en esta suma sólo hay un número finito de términos distintos de cero. Éstos pueden describirse de forma explícita

Lema 2.9. *Sea $ax^2+bxy+cy^2$, $a>0$, con discriminante n no cuadrado. Entonces $\mu(a,b,c) \neq 0$ si y sólo si $a+c < |b|/2$. Además, si $\mu(a,b,c) \neq 0$ entonces $a \leq \sqrt{n/3}$, $|b| \leq 2\sqrt{n/3}$ y $a|c| \leq n/4$.*

Demostración: La primera parte del lema se deduce de que la geodésica g_{abc} tiene intersección no vacía con el dominio fundamental $\mathcal{F}$ si y sólo si alguno de los puntos $(\pm 1 + i\sqrt{3})/2$ está por debajo de la semicircunferencia g_{abc}. La desigualdades se obtienen a partir de la igualdad

$$\frac{1}{4}(4a - |b|)^2 + \frac{3}{4}b^2 = n + 4a(a + c - \frac{1}{2}|b|).$$

□

Nuestro objetivo es acotar $\sum N_+(n)e(R\sqrt{n})$ como en [CI1]. Esto va a ser posible porque, aunque $\mu(a, b, c)$ en algunos rangos puede tener derivadas muy grande, dividiendo el dominio de valores (a, b, c) en tres partes, de acuerdo con la situación geométrica de la geodésica g_{abc}, la función $\mu(a, b, c)$ va a ser el logaritmo de una función algebraica en cada una de ellas.

Proposición 2.10. *Para $R > 1/2$ y $1 \leq M < M' \leq 2M$ se cumple*

$$\sum_{M \leq n < M'} N_+(n)e(R\sqrt{n}) \ll M^{5/4+\epsilon} + (RM)^\epsilon L$$

con

$$L = \text{mín}\left(R^{3/8}M^{15/16} + R^{1/8}M^{17/16}, R^{7/24}M^{49/48} + R^{5/24}M^{53/48}\right),$$

y un resultado similar se tiene cuando $N_+(n)$ es sustituido por $N_+(4n)$.

Demostración: Por los lemas 2.8 y 2.9 podemos escribir

$$\sum_{M \leq n < M'} N_+(n)e(R\sqrt{n}) = \sum_{\substack{a+c<|b|/2 \\ b^2-4ac \neq \square}} \mu(a, b, c)E(b^2 - 4ac) \tag{2.28}$$

donde

$$E(n) = \begin{cases} e(R\sqrt{n}) & \text{si } M \leq n < M' \\ 0 & \text{en otro caso} \end{cases}$$

Consideramos el conjunto

$$\mathcal{M} = \mathcal{M}_1 \cup \mathcal{M}_2 \cup \mathcal{M}_3$$

donde los conjuntos disjuntos $\mathcal{M}_j$ se definen

$$\begin{aligned} \mathcal{M}_1 &= \{(a, b, c) \in \mathbb{Z}^3 \ : \ |a + c| < -b/2, \ a > 0, \ c \neq 0\} \\ \mathcal{M}_2 &= \{(a, b, c) \in \mathbb{Z}^3 \ : \ a + c \leq b/2 \leq -a - c, \ a > 0, \ c \neq 0\} \\ \mathcal{M}_3 &= \{(a, b, c) \in \mathbb{Z}^3 \ : \ |a + c| < b/2, \ a > 0, \ c \neq 0\}. \end{aligned}$$

Los vértices $1/2 + i\sqrt{3}/2$ y $-1/2 + i\sqrt{3}/2$ de $\mathcal{F}$ pertenecen al semicírculo determinado por g_{abc} si y sólo si $(a,b,c) \in \mathcal{M}_2$; de la misma forma, sólo el primer vértice o el segundo pertenecen al semicírculo si y sólo si $(a,b,c) \in \mathcal{M}_1$ o $(a,b,c) \in \mathcal{M}_3$, respectivamente. Por tanto, en $\mathcal{M}$ están cubiertas todas la posibilidades geométricas para las que $\mu(a,b,c) \neq 0$.

Por (2.12), en cada $\mathcal{M}_i$ la función $\mu = \mu(a,b,c)$ es el logaritmo de una función algebraica, y además $\mu(a,b,c) = O(\log M)$ para $M \leq b^2 - 4ac < 2M$.

Nótese que $\mu(a,b,c)$ está bien definida como $\ell(g_{abc} \cap \mathcal{F})$ también cuando $b^2 - 4ac$ es un cuadrado. Por otra parte, el número de elementos del conjunto

$$\{(a,b,c) \ : \ b^2 - 4ac = h^2, \ M \leq h^2 < 2M, \ a + c < |b|/2, \ a > 0, \ c \neq 0\}$$

es $O(M^{1+\epsilon})$. Luego de (2.28) deducimos

$$\begin{aligned} \sum_{M \leq n < M'} N_+(n) e(R\sqrt{n}) &\ll M^{1+\epsilon} + \sum_{(a,b,c) \in \mathcal{M}} \mu(a,b,c) E(b^2 - 4ac) \\ &\ll M^{1+\epsilon} + \sum_{(a,b,c) \in \mathcal{M}_i} \mu(a,b,c) E(b^2 - 4ac) \end{aligned}$$

para algún $i \in \{1,2,3\}$.

Fijemos a, c y consideremos $\mu(a,b,c)$ como una función de b. Como e^{μ} es una función algebraica en $\mathcal{M}_i$, tiene un número uniformemente acotado de máximos y mínimos. Así, dados a, c podemos escribir $\{b \ : \ (a,b,c) \in \mathcal{M}_i\}$ como una unión finita de intervalos I_j en los que $\mu(a,\cdot,c)$ es monótona. La cota $\mu(a,b,c) \ll \log M$ y sumación por partes dan

$$\sum_{(a,b,c) \in \mathcal{M}_i} \mu(a,b,c) E(b^2 - 4ac) \ll M^{\epsilon} \sum_{a,c} \left| \sum_{b \in I_j'} E(b^2 - 4ac) \right|,$$

donde el intervalo $I_j' \subset I_j$ depende de a, c y será vacío si $(a,b,c) \notin \mathcal{M}_i$ para todo b. El lema 2.9 asegura que $a|c| \leq M/2$ y $|b| \leq 2\sqrt{M}$, luego por el lema 7.3 de [GK] aplicado sobre $[-2\sqrt{M}, 2\sqrt{M}]$ y haciendo el cambio $n = 4a|c|$ deducimos que

$$\sum_{a,c} \left| \sum_{b \in I_j'} E(b^2 - 4ac) \right| \ll M^{\epsilon} \sum_{n \leq 2M} \left| \sum_{|b| \leq 2\sqrt{M}} e(\theta b) E(b^2 - n) \right| \tag{2.29}$$

para algún $\theta \in \mathbb{R}$.

Ahora seguimos los argumentos expuestos en el lemma 4.1 de [CI2]. Dividimos el rango de b en M^ϵ intervalos de longitud $O(M^{1/2-\epsilon})$. Si J es uno de esos intervalos, por la desigualdad de Cauchy obtenemos

$$\Big(\sum_{n\le 2M}\Big|\sum_{b\in J} e(\theta b)E(b^2-n)\Big|\Big)^2 \ll M\Big(M^{3/2}+\sum_{|b_1|<|b_2|}\big|\sum_n E(b_1^2-n)\overline{E(b_2^2-n)}\big|\Big).$$

Escribiendo $u=b_1^2-n$, la última suma doble es

$$\sum_{|b_1|<|b_2|}\Big|\sum_{M\le u\le M'+b_1^2-b_2^2} e\big(R(\sqrt{u}-\sqrt{u+b_2^2-b_1^2})\big)\Big| \ll$$

$$\ll M^\epsilon \sum_{v\asymp D}\Big|\sum_{u\asymp M} e(R(\sqrt{u}-\sqrt{u+v}))\Big|$$

para algún $D=o(M)$, donde hemos empleado que el número de representaciones de v como $b_2^2-b_1^2$ es $O(M^\epsilon)$ y $b_2^2-b_1^2=o(M)$ porque $|J|=o(M^{1/2})$.

De todo lo anterior obtenemos finalmente

$$\sum_{M\le n<M'} N_+(n)e(R\sqrt{n}) \ll M^{5/4+\epsilon}+M^{1/2+\epsilon}\Big(\sum_{v\asymp D}\Big|\sum_{u\asymp M} e(R(\sqrt{u}-\sqrt{u+v}))\Big|\Big)^{\frac{1}{2}}$$

Esta suma fue acotada en el lemma 3.1 de [CI1], dando el resultado buscado.

La prueba en el caso de $N_+(4n)$ es similar, teniendo en cuenta que $4|b^2-4ac$ equivale a $2|b$ y $2\sum_{2|b} f(b)=\sum_b f(b)+\sum_b e(b/2)f(b)$, luego la fase $b/2$ puede acumularse a θb en (2.29). □

2.4. Acotación del término de error

Ahora vamos a proceder como en [CI2] y [CI1]. Escribiremos la suma como

$$\sum_{n\le N} N_+(n) = \sum_{\sqrt{n}\le N^{1/2}+\Delta} \frac{N_+(n)}{\sqrt{n}} g(\sqrt{n}) - \sum_{N^{1/2}\le\sqrt{n}\le N^{1/2}+\Delta} \frac{N_+(n)}{\sqrt{n}} g(\sqrt{n}), \tag{2.30}$$

con $\Delta > 0$, y $g : [0, \infty] \longrightarrow \mathbb{R}$ la función definida por

$$g(x) = \begin{cases} \int_0^x \eta(u)\, du & \text{si } x \leq 1 \\ x & \text{si } 1 \leq x \leq N^{1/2} \\ N^{1/2}\Delta^{-1}(N^{1/2} + \Delta - x) & \text{si } N^{1/2} \leq x \leq N^{1/2} + \Delta \\ 0 & \text{si } x \geq N^{1/2} + \Delta, \end{cases}$$

$\eta \in C_0^\infty\big((1/2, 1)\big)$ con $\int_0^1 \eta = 1$. Nótese que $g \in C_0\big((0, \infty)\big)$ y es diferenciable a trozos.

Proposición 2.11. *Si $N^{-1/2} < \Delta \leq N^{-1/4} < 1$, tenemos que*

$$\begin{aligned} \sum_{n=1}^{\infty} \frac{N_+(n)}{\sqrt{n}} g(\sqrt{n}) &= \frac{\pi^2}{18} N^{\frac{3}{2}} + \frac{\pi^2 N\Delta}{12} - \frac{N}{2}\log N + \big(1 - \frac{\zeta'(2)}{\zeta(2)} - \log(2\pi)\big)\frac{N}{2} \\ &+ O(N^{\frac{21}{32}+\epsilon} + N^{\frac{1}{2}+\epsilon}\Delta^{-\frac{1}{2}} + N^{\frac{11}{16}+\epsilon}\Delta^{\frac{1}{8}}) \end{aligned}$$

y

$$\begin{aligned} \sum_{n=1}^{\infty} \frac{N_+(4n)}{\sqrt{4n}} g(\sqrt{4n}) &= \frac{\pi^2}{36} N^{\frac{3}{2}} + \frac{\pi^2 N\Delta}{24} + \big(1 - \frac{\zeta'(2)}{\zeta(2)} + \frac{\log 2}{3} - \log(2\pi)\big)\frac{N}{4} \\ &- \frac{N}{4}\log N + O(N^{\frac{21}{32}+\epsilon} + N^{\frac{1}{2}+\epsilon}\Delta^{-\frac{1}{2}} + N^{\frac{11}{16}+\epsilon}\Delta^{\frac{1}{8}}) \end{aligned}$$

Nota 2.12. Sólo usando esta proposición podemos mejorar el resultado de Shintani, porque tomando $\Delta = N^{-1/3}$ vemos que el término de error en la suma suavizada es $O(N^{2/3+\epsilon})$, y substrayendo el mismo resultado cambiando $N^{1/2}$ por $N^{1/2} - \Delta$ vemos que la contribución de los términos con $N^{1/2} \leq \sqrt{n} \leq N^{1/2} + \Delta$ es absorbida por esta cota.

Demostración: Nos restringiremos primero a la prueba de la primera fórmula y después indicaremos los cambios necesarios para probar la segunda.

Para $x > 0$ tenemos que

$$\widetilde{g}(x) = \frac{\cos(\pi N^{\frac{1}{2}}x) - \cos(\pi x) - \phi(x)}{\pi^2 x^2} + \frac{2N^{\frac{1}{2}}}{\pi^2 x^2 \Delta}\operatorname{sen}(\frac{\pi}{2}\Delta x)\operatorname{sen}\big(\frac{\pi}{2}(2N^{\frac{1}{2}} + \Delta)x\big) \tag{2.31}$$

donde $\phi(x) = \pi x \int \eta(t) \operatorname{sen}(\pi x t)\, dt$. Se cumple que $\phi(x) = O(x^{-\alpha})$ para todo $\alpha > 0$.

Sea $\tau \in C_0^\infty((-1/2, 1/2))$ par, con $\int \tau = 1$, y $\tau_m(x) = m\tau(mx)$ para todo $m \in \mathbb{N}$. Definiendo $g_m = g * \tau_m$, se cumple que $g_m \in C_0^\infty((0,\infty))$ y $\widetilde{g_m}(x) = \widetilde{g}(x)\widehat{\tau}(x/2m)$ convergen uniformemente a g y $\widetilde{g}$. Además, por la proposición 2.10 vemos que la suma $\sum N_+(n)\widetilde{g}(\sqrt{n})/\sqrt{n}$ converge, y por el lema de Abel $\sum_n N_+(n)\widetilde{g_m}(\sqrt{n})/\sqrt{n}$ converge uniformemente en m. Esto justifica la aplicación de la proposición 2.6 para la función g.

En el rango considerado para Δ tenemos que

$$\frac{\pi^2}{6} \int_0^\infty t g(t)\, dt = \frac{\pi^2}{18} N^{3/2} + \frac{\pi^2 N \Delta}{12} + O(1).$$

Por otra parte

$$\int_0^\infty g(t) \log(2\pi t)\, dt = \frac{N}{4} \log N + \big(2\log(2\pi) - 1\big)\frac{N}{4} + O(N^{1/2+\epsilon})$$

y por sumación parcial

$$\sum_{n=1}^\infty g(n)\log n - \sum_{d=1}^\infty \frac{\Lambda(d)}{d} \sum_{n=1}^\infty g(dn) = \frac{N}{4}\log N - \frac{N}{4} + \frac{\zeta'(2)}{2\zeta(2)} N + O(N^{1/2+\epsilon}).$$

Las sumas con términos β_n, $N_-(4n)$ y $\widetilde{g}(2n/t)$ son despreciables. Sus contribuciones son $O(N^{1/2+\epsilon})$, lo que se prueba usando las cotas $\widetilde{g}(x) \ll x^{-2} + N^{1/2} \operatorname{mín}(x^{-1}, \Delta^{-1}x^{-2})$, $\beta_n \ll \log n$ y $N_-(4n) = O(n^{1/2+\epsilon})$.

Por (2.31), la suma $\sum N_+(4n)\widetilde{g}(\sqrt{4n})/\sqrt{n}$, puede escribirse, salvo por una constante, como

$$\sum_{n=1}^\infty \frac{N_+(4n)}{n^{3/2}} \big(\cos(2\pi\sqrt{Nn}) - \cos(2\pi\sqrt{n}) - \phi(\sqrt{4n})\big) +$$

$$2\frac{N^{\frac{1}{2}}}{\Delta} \left(\sum_{n<N^{1/2}} + \sum_{N^{\frac{1}{2}} \le n < \Delta^{-2}} + \sum_{n \ge \Delta^{-2}} \right) \frac{N_+(4n)}{n^{3/2}} \operatorname{sen}(\pi\Delta\sqrt{n}) \operatorname{sen}\big(\pi(2N^{\frac{1}{2}} + \Delta)\sqrt{n}\big)$$

$$= S_0 + S_1 + S_2 + S_3.$$

El decaimiento de ϕ y la proposición 2.10 prueban que $S_0 \ll \log N$. Para S_1, nótese que $\sqrt{n}\Delta \ll 1$ y que podemos extraer el factor $n^{-3/2} \operatorname{sen}(\pi\sqrt{n}\Delta)$

sumando por partes. Usando la proposición 2.10 con el segundo valor del mínimo da

$$S_1 \ll (N^{5/8} + N^{7/48}N^{49/96} + N^{5/48}N^{53/96})N^{\epsilon} \ll N^{21/32+\epsilon}.$$

Para acotar S_2 hacemos lo mismo pero usando el primer valor del mínimo, concluyendo

$$\begin{aligned} S_2 &\ll N^{21/32+\epsilon} + N^{1/2+\epsilon}\Delta^2\big(\Delta^{-5/2} + N^{3/16}\Delta^{-15/8} + N^{1/16}\Delta^{-17/8}\big) \\ &\ll N^{21/32+\epsilon} + N^{1/2+\epsilon}\Delta^{-1/2} + N^{11/16+\epsilon}\Delta^{1/8}. \end{aligned}$$

Finalmente, para S_3 usamos directamente la proposición 2.10 como en S_2 consiguiendo la misma cota.

De todas estas acotaciones deducimos

$$\sum_{n=1}^{\infty} \frac{N_+(4n)}{n^{3/2}} \widetilde{g}(\sqrt{4n}) \ll N^{21/32+\epsilon} + N^{1/2+\epsilon}\Delta^{-1/2} + N^{11/16+\epsilon}\Delta^{1/8}$$

lo que prueba la primera fórmula.

Para la segunda, tenemos en cuenta que

$$\sum_{n=1}^{\infty} g(2n)\log n = \frac{N}{8}\log N - \frac{N}{8} - \frac{N}{4}\log 2 + O(N^{1/2+\epsilon})$$

y que los dos siguientes términos en la proposición 2.7 contribuyen

$$\frac{N}{4}\sum_{d=1}^{\infty}\frac{\Lambda(d)}{d^2} - \log 2 \sum_{k=1}^{\infty} 2^{-2k-1}N + O(N^{1/2+\epsilon}).$$

Introduciendo estos cálculos, la prueba es similar. □

Ahora vamos a estimar la suma corta a través de sumas de caracteres

Proposición 2.13. *Sean g, N y Δ como en la proposición anterior. Entonces*

$$\sum_{N^{1/2}<\sqrt{n}<N^{1/2}+\Delta} \frac{N_+(n)}{\sqrt{n}} g(\sqrt{n}) = \frac{\pi^2 N\Delta}{12} + O(E)$$

y

$$\sum_{N^{1/2}<\sqrt{4n}<N^{1/2}+\Delta} \frac{N_+(4n)}{\sqrt{4n}} g(\sqrt{4n}) = \frac{\pi^2 N\Delta}{24} + O(E)$$

donde $E = N^{11/12+\epsilon}\Delta^{5/6} + N^{7/12+\epsilon}\Delta^{-1/6} + N^{19/30+\epsilon}$.

Demostración: Tenemos que $h(n)\log\epsilon_n \neq 0$ si y sólo si $n \in \mathcal{R}$, donde $\mathcal{R} = \{n \in \mathbb{Z}^+ : n \equiv 0, 1 \pmod 4), n \neq \square\}$. Además en este caso se cumple la fórmula de Dirichlet (2.5), luego podemos escribir el lado izquierdo de la primera identidad en la proposición como

$$\sum_{\sqrt{N}<d\sqrt{a}<\sqrt{N}+\Delta} h(a)\log\epsilon_a \frac{g(d\sqrt{a})}{d\sqrt{a}} = \sum_{d<\sqrt{N}+\Delta} \sum_{\substack{N<ad^2<(\sqrt{N}+\Delta)^2 \\ a\in\mathcal{R}}} \frac{g(d\sqrt{a})}{d} L(1,\chi_a)$$

y por la fórmula de sumación de Abel esto es

$$\frac{N^{1/2}}{2\Delta} \sum_{d<N^{1/2}+\Delta} \frac{1}{d} \int_0^{2\Delta N^{1/2}+\Delta^2} \frac{C(Nd^{-2}, xd^{-2})}{(N+x)^{1/2}} dx, \tag{2.32}$$

donde

$$C(x,K) = \sum_{\substack{x<n<x+K \\ n\in\mathcal{R}}} L(1,\chi_n).$$

Pero en [HB2] tenemos la estimación

$$C(x,K) = \frac{\zeta(2)}{\zeta(3)}\frac{K}{2} + x^{\epsilon}O(K^{5/6} + x^{2/15} + x^{1/6}\,\text{mín}(1, K^{-1/4}))$$

para todo $0 < K \ll x^{1/2}$. Sustituyendo esto en (2.32) se sigue la primera identidad. Para la segunda procedemos de manera similar. □

Eligiendo $\Delta = N^{-5/16}$, como consecuencia de las dos proposiciones anteriores y de la descomposición (2.30) obtenemos

Corolario 2.14. *Para $N > 1$*

$$\sum_{n\leq N} N_+(n) = \frac{\pi^2}{18}N^{\frac{3}{2}} - \frac{N}{2}\log N + (1 - \frac{\zeta'(2)}{\zeta(2)} - \log(2\pi))\frac{N}{2} + O(N^{\frac{21}{32}+\epsilon})$$

y

$$\sum_{n\leq N} N_+(4n) = \frac{2\pi^2}{9}N^{\frac{3}{2}} - N\log N + \big(1 - \frac{\zeta'(2)}{\zeta(2)} - \frac{5\log 2}{3} - \log(2\pi)\big)N + O(N^{\frac{21}{32}+\epsilon}).$$

Ahora, por inversión de Möbius concluimos las pruebas de los resultados en promedio para el número de clases

Demostración del teorema 2.1: Por el lema 2.4 obtenemos la expresión

$$\sum_{n\leq N} h(n)\log\epsilon_n = \sum_{k\leq\sqrt{N}} \mu(k) \sum_{n\leq N/k^2} N_+(n),$$

y por tanto el resultado se sigue del corolario 2.14. Nótese que $\sum k^{-2}\log k = -\zeta'(2)$. □

Demostración del teorema 2.2: Igualmente, por la segunda parte del lema 2.4,

$$\sum_{n\leq N} h(4n)\log\epsilon_{4n} = \sum_{\substack{k\leq\sqrt{N}\\ 2\nmid k}} \mu(k)\Big(\sum_{n\leq N/k^2} N_+(4n) - \sum_{n\leq N/k^2} N_+(n)\Big),$$

y de nuevo el resultado es consecuencia del corolario 2.14, viendo que en este caso

$$\sum_{2\nmid k}\frac{\mu(k)}{k^3} = \frac{8}{7\zeta(3)}, \quad \sum_{2\nmid k}\frac{\mu(k)}{k^2} = \frac{8}{\pi^2} \quad \text{y} \quad \sum_{2\nmid k}\mu(k)\frac{\log k}{k^2} = \big(\frac{\log 2}{3} + \frac{\zeta'(2)}{\zeta(2)}\big)\frac{8}{\pi^2},$$

(para la última igualdad, calcúlese la derivada de $\big((2^{-s}-1)\zeta(s)\big)^{-1}$ en $s=2$). □

2.5. Estudio del término oscilatorio

En la sección anterior hemos probado que

$$E_2^+(x) \ll x^{\frac{21}{32}}.$$

pero se cree que en realidad $E_2^+(x) \ll x^{1/2+\epsilon}$ para cualquier $\epsilon > 0$. En esta sección vamos a estudiar el término E_2^+ en media.

Vamos a calcular la norma 2 de la función $E_2^+(N+K) - E_2^+(N)$ en un intervalo $R \leq N \leq 2R$. Para ello vamos a aprovechar que esta función se puede escribir como sumas cortas de caracteres lo que será bueno a la hora de controlar la integral, pero además estas sumas se pueden expresar en términos

de exponenciales lo que nos va a permitir llevar a cabo la integración. En esta representación serán relevantes las sumas de Gauss

$$\tau_b(m) = \sum_{a(\mathrm{mod}\ m)} (\frac{a}{m}) e(\frac{ba}{m}).$$

La influencia de K quedará codificada en la función

$$f(y) = \frac{e(-Ky) - 1}{e(-y) - 1}.$$

En el siguiente lema vamos a ver como se consigue dicha expresión

Lema 2.15. *Sea $R > 1$, $R < N < 2R$ y $K < R^{1/2}(\log R)^{-1}$. Para todo $K < M < R$ se cumple la expresión*

$$\frac{E_2^+(N+K) - E_2^+(N)}{(4N)^{\frac{1}{2}}} = B_M(N) + \sum_{\substack{N \le n \le N+K \\ M \le m \le R}} \frac{\chi_{4n}(m)}{m} - C(N)\log R + O(1),$$

con

$$B_M(N) = \sum_{m<M, m\neq\square}{}^{*} \frac{1}{m^2} \sum_{b(mod\ m)} \tau_b(m) f(\frac{b}{m}) e(\frac{-b}{m}N)$$

(donde el asterisco restringe la sumación a los impares) y $C(N)$ la función que vale 1 si hay algún entero en el intervalo $[N^{1/2}, (N+K)^{1/2}]$ y cero si no lo hay.

Demostración: Comenzamos deduciendo del teorema 2.2 la fórmula

$$\frac{E_2^+(N+K) - E_2^+(N)}{(4N)^{\frac{1}{2}}} = \sum_{\substack{N < n \le N+K \\ 4n \neq \square}} L(1, \chi_{4n}) - \frac{\pi^2}{7\zeta(3)} K + O(1) \qquad (2.33)$$

para todo $1 < K < N^{1/2}(\log N)^{-1}$. Por la desigualdad de Pólya-Vinogradov, para $4n \neq \square$ podemos escribir

$$L(1, \chi_{4n}) = \sum_{m<R} \frac{\chi_{4n}(m)}{m} + O(R^{-\frac{1}{2}} \log R). \qquad (2.34)$$

Haciendo un cálculo vemos que

$$\sum_{N<n\le N+K} \sum_{m<R, m=\square} \chi_{4n}(m) m^{-1} = \frac{\pi^2}{7\zeta(3)} K + O(1)$$

luego

$$(4N)^{-\frac{1}{2}}(E_2^+(N+K)-E_2^+(N))=\sum_{\substack{N<n\leq N+K\\ 4n\neq\square}}\sum_{\substack{m<R\\ m\neq\square}}\frac{\chi_{4n}(m)}{m}+O(1).$$

Podemos escribir

$$\sum_{\substack{N<n\leq N+K\\ 4n\neq\square}}\sum_{\substack{m<R\\ m\neq\square}}\frac{\chi_{4n}(m)}{m}=\sum_{\substack{m<R\\ m\neq\square}}\frac{1}{m}\sum_{N<n\leq N+K}\chi_{4n}(m)-C(N)\log R+O(1).$$

Para m par tenemos $(4n/m)=0$, y para $m\neq\square$ impar $(4\cdot/m)=(\cdot/m)$ es un carácter no principal módulo m. En el último caso tenemos

$$\sum_{x<n\leq x+K}\big(\frac{4n}{m}\big)=\frac{1}{m}\sum_{a(\mathrm{mod}\ m)}\big(\frac{a}{m}\big)\sum_{x<n\leq x+K}\sum_{b(\mathrm{mod}\ m)}e\big(\frac{b(a-n)}{m}\big)=$$

$$\frac{1}{m}\sum_{b(\mathrm{mod}\ m)}\tau_b(m)\sum_{x<n\leq x+k}e\big(\frac{-bn}{m}\big)=\frac{1}{m}\sum_{b(\mathrm{mod}\ m)}\tau_b(m)f\big(\frac{b}{m}\big)e\big(\frac{-b}{m}x\big)$$

lo que prueba el lema. □

Al hacer la media cuadrática de $E_2^+(N+K)-E_2^+(N)$, el término prinicipal va a venir de los términos diagonales que aparecen al expandir $B_M(N)$, es decir de la suma

$$S=\sum_{\substack{m_1,m_2<M\\ m_1,m_2\neq\square}}{}^{*}\frac{1}{m_1^2m_2^2}\sum_{b_1m_2=b_2m_1}\tau_{b_1}(m_1)\overline{\tau_{b_2}(m_2)}f(\frac{b_1}{m_1})\overline{f(\frac{b_2}{m_2})}.\tag{2.35}$$

Vamos a ver que es posible controlar el comportamiento de S con precisión

Proposición 2.16. *Sea $2\leq K\leq M\leq R$. Entonces se cumple que*

$$S=3(P/4\pi)^2\log K+O((\log K)^{2/3})$$

con $P=\prod_{p\neq 2}(1-1/(p^3+p^2))$.

Demostración: El punto de partida es la fórmula para las sumas de Gauss

$$\tau_{\lambda s}(cs^2)=\varepsilon_c c^{1/2}s\sum_{d|(\lambda,s)}d\big(\frac{\lambda sd^{-2}}{c}\big)\mu\big(\frac{s}{d}\big)\tag{2.36}$$

para cualquier c impar libre de cuadrados [IK], con $\varepsilon_c = 1$ si $c \equiv 1 \pmod 4$ y $\varepsilon_c = i$ si $c \equiv -1 \pmod 4$. Vemos que $\tau_b(cs^2) = 0$ si $s \nmid b$ y podemos reescribir S como

$$\sum_{\substack{c_1 s_1^2 d_1^2 < M \\ c_2 s_2^2 d_2^2 < M \\ c_1 \neq 1, c_2 \neq 1}}{}^{*} \frac{\mu^2(c_1)\varepsilon_{c_1}\mu^2(c_2)\overline{\varepsilon_{c_2}}}{(d_1 d_2)^2 (c_1 s_1^2 c_2 s_2^2)^{\frac{3}{2}}} \sum_{\substack{\lambda_1 < c_1 s_1 \\ \lambda_2 < c_2 s_2 \\ \lambda_1 c_2 s_2 = \lambda_2 c_1 s_1}} \Big| f\Big(\frac{\lambda_1}{c_1 s_1}\Big)\Big|^2 \Big(\frac{\lambda_1 s_1}{c_1}\Big)\Big(\frac{\lambda_2 s_2}{c_2}\Big)\mu(s_1)\mu(s_2).$$

Con estas restricciones podemos considerar la suma sólo sobre los términos cumpliendo

$$c_1(c_2, s_1) = c_2(c_1, s_2), \quad s_1/(s_1, c_2) \mid \lambda_1, \ s_2/(s_2, c_1) \mid \lambda_2.$$

Por tanto, escribiendo

$$c_1 = cj_1, s_2 = q_2 j_1, c_2 = cj_2, s_1 = q_1 j_2, (c, q_1 q_2) = 1,$$

$$\lambda_1 = \lambda q_1, \lambda_2 = \lambda q_2,$$

se sigue que S es igual a

$$\sum_{\substack{cj_1 q_1^2 j_2^2 d_1^2 < M \\ cj_2 q_2^2 j_1^2 d_2^2 < M \\ (q_1 q_2, j_1 j_2) = 1 \\ (c, q_1 q_2) = 1}}{}^{*} \frac{\mu(q_1)\mu(q_2)\mu(j_1 j_2)\mu^2(c)}{(d_1 d_2)^2 (j_1 j_2)^{\frac{9}{2}} (q_1 q_2)^3} \Big(\frac{j_1 j_2}{c}\Big) \frac{\varepsilon_{cj_1}\overline{\varepsilon_{cj_2}}}{c^3} \sum_{\substack{\lambda < cj_1 j_2 \\ c \neq 1}} \Big| f\Big(\frac{\lambda}{cj_1 j_2}\Big)\Big|^2 \Big(\frac{\lambda j_1}{j_2}\Big)\Big(\frac{\lambda j_2}{j_1}\Big).$$

Acotando trivialmente, tenemos que la cantidad que aportan los términos cumpliendo $\lambda(cj_1 j_2)^{-1} < 1/K$ es $O(1)$, notando que

$$|f(u)|^2 = \frac{1 - \cos(2\pi K u)}{2\pi^2 u^2} + O(1).$$

Además, podemos completar las sumas obteniendo

$$S = \frac{1}{2\pi^2} \sum_{\substack{(q_1 q_2, j_1 j_2) = 1 \\ j_1 j_2 \equiv 1 (4)}}{}^{*} \frac{\mu(q_1)\mu(q_2)\mu(j_1 j_2)}{(d_1 d_2)^2 (j_1 j_2)^{\frac{5}{2}} (q_1 q_2)^3} \sum_{\lambda=1}^{\infty} \Big(\frac{\lambda j_1}{j_2}\Big)\Big(\frac{\lambda j_2}{j_1}\Big) \frac{\Delta(\lambda, j_1 j_2, q_1 q_2)}{\lambda^2} + O(1) \tag{2.37}$$

con

$$\Delta(\lambda, j, q) = \sum_{\substack{c < K/j \\ (c,q) = 1}}{}^{*} \frac{1 - \cos(2\pi K\lambda/(cj))}{c} \Big(\frac{j}{c}\Big)\mu^2(c).$$

Para $j > 1$, se cumple (aplicando la fórmula $\mu^2(c) = \sum_{d^2|c} \mu(d)$ y Polya-Vinogradov) que

$$\sum_{\substack{c<K/j \\ (c,q)=1}}^{*} \frac{1}{c}\big(\frac{j}{c}\big)\mu^2(c) \ll (qj)^{1/2}\log(qj).$$

Por otra parte, para cualquier j podemos escribir

$$\sum_{\substack{c<K/j \\ (c,q)=1}}^{*} e(\frac{K\lambda j^{-1}}{c})\big(\frac{j}{c}\big)\frac{\mu^2(c)}{c} = \sum_{\substack{d^2<K/j \\ (d,2q)=1}} \frac{\mu(d)}{d^2}\big(\frac{j}{d^2}\big) \sum_{\substack{c<Kj^{-1}d^{-2} \\ (c,2q)=1}} \big(\frac{j}{c}\big)e(\frac{K\lambda j^{-1}d^{-2}}{c})\frac{1}{c}$$

y esto es más pequeño que

$$2jq\sum_{d=1}^{\infty}\frac{1}{d^2}\max_{1\le a\le 2jq}\Big|\sum_{0\le n<(Kj^{-1}d^{-2}-a)/(2jq)} e(\frac{K\lambda j^{-2}q^{-1}d^{-2}}{n+a/(2jq)})\frac{1}{2jqn+a}\Big|.$$

Luego vemos que es necesario acotar sumas del tipo

$$S(N,N_1) = \sum_{N<n<N_1} e(g(n))$$

para $N_1 < 2N < 2\tilde{K}$ y $g(n) = \tilde{K}/(n+\alpha)$, $0 < \alpha \le 1$. En el rango $\tilde{K}/N \ge N^4$ podemos aplicar el método de Vinogradov [IK] obteniendo que

$$S(N,N_1) \ll N\exp(-2^{-18}(\log N)^3(\log(\tilde{K}/N))^{-2}).$$

Además, en el rango $\tilde{K}^{1/5} \le N \le \tilde{K}^{1/2}$ deducimos por el método de pares de exponentes (ver [IK])

$$S(N,N_1) \ll (\tilde{K}N^{-6})^{1/62}N,$$

y en $\tilde{K}^{1/2} \le N \le \tilde{K}$

$$S(N,N_1) \ll (N\tilde{K}^{-1})^{1/2}N.$$

Luego

$$\sum_{\substack{c<Kj^{-1} \\ (c,q)=1}}^{*} e(\frac{K\lambda j^{-1}}{c})\big(\frac{j}{c}\big)\frac{\mu^2(c)}{c} \ll jq + (\log \lambda K)^{2/3},$$

y entoces para $j \neq 1$

$$\Delta(\lambda, j, q) \ll jq + (\log \lambda K)^{2/3} \tag{2.38}$$

y

$$\Delta(\lambda, 1, q) = \sum_{\substack{c<K \\ (c,2q)=1}} \mu^2(c)c^{-1} + O(q + (\log \lambda K)^{2/3}). \tag{2.39}$$

Es posible estimar esta suma

$$\begin{aligned}
\sum_{\substack{c<K \\ (c,2q)=1}} \mu^2(c)c^{-1} &= \sum_{\substack{d^2<K \\ (d,2q)=1}} \frac{\mu(d)}{d^2} \sum_{\substack{c<Kd^{-2} \\ (c,2q)=1}} \frac{1}{c} \\
&= \sum_{\substack{d^2<K \\ (d,2q)=1}} \frac{\mu(d)}{d^2} (\frac{\varphi(2q)}{2q} \log \frac{K}{d^2} + O((\log q)^2)) \\
&= \frac{\varphi(2q)}{2q} \log K \sum_{\substack{d=1 \\ (d,2q)=1}}^{\infty} \mu(d)d^{-2} + O((\log q)^2) \\
&= \frac{1}{\zeta(2)} \frac{\varphi(2q)}{2q \prod_{p|2q}(1-p^{-2})} \log K + O((\log q)^2) \\
&= \frac{1}{\zeta(2)} \frac{2}{3} \eta(q) \log K + O((\log q)^2)
\end{aligned} \tag{2.40}$$

con $\eta(q) = \prod_{p|q}(1+p^{-1})^{-1}$. Por (2.37), (2.38), (2.39) y (2.40) tenemos

$$S = \frac{1}{18\zeta(2)^2} T \log K + O((\log K)^{2/3}), \tag{2.41}$$

con

$$T = \sum\nolimits^{*} \frac{\mu(q_1)\mu(q_2)}{(d_1 d_2)^2 (q_1 q_2)^3} \eta(q_1 q_2) \sum_{\lambda=1}^{\infty} \frac{1}{\lambda^2} = (1-2^{-2})^2 \zeta(2)^2 (\sum_{q}^{*} \frac{\mu(q)\eta(q)}{q^3})^2 \zeta(2)$$

Usando el producto de Euler para esta suma la proposición queda demostrada. □

Vamos a usar este resultado para probar

Proposición 2.17. *Sea $R > 1$. Uniformemente en $1 < L < R$ y $K < R^{\frac{1}{4}-\epsilon}$ se cumple que*

$$\sum_{R\leq N\leq R+L} \frac{(E_2^+(N+K)-E_2^+(N))^2}{4N} = 3(P/4\pi)^2 L\log K + O(R(\log K)^{2/3})$$

con

$$P = \prod_{p\neq 2}\big(1-\frac{1}{p^3+p^2}\big).$$

Demostración: Tenemos que

$$\sum_{R\leq N\leq 2R} C(N)^2 \ll KR^{1/2} \ll R. \tag{2.42}$$

También, por la desigualdad de Cauchy

$$\sum_{R\leq N\leq 2R} |\sum_{\substack{N\leq n\leq N+K\\ M\leq m\leq R}} \frac{\chi_{4n}(m)}{m}|^2 \ll K^2 \sum_{n\leq 3R} |\sum_{M\leq m\leq R} \frac{\chi_{4n}(m)}{m}|^2.$$

Escribiendo $n = cs^2$ con $\mu(c)\neq 0$ tenemos

$$\sum_{n\leq 3R} |\sum_{M\leq m\leq R} \frac{\chi_{4n}(m)}{m}|^2 = \sum_{s^2\leq 3R} \sum_{\substack{c<3Rs^{-2}\\ \mu(c)\neq 0}} |\sum_{\substack{M<m<R\\ (m,2s)=1}} \frac{\chi_c(m)}{m}|^2.$$

Pero usando el corolario 3 de [HB1] en intervalos diádicos vemos que esta suma es

$$\ll R^{\epsilon}\sum_{s^2\leq 3R}(RM^{-1}s^{-2}+1) \ll R^{\frac{1}{2}+\epsilon}(1+R^{\frac{1}{2}}M^{-1}).$$

Por tanto, tomando $M = R^{\frac{1}{2}-\epsilon}$ se cumple

$$\sum_{R\leq N\leq 2R} |\sum_{\substack{N\leq n\leq N+K\\ M\leq m\leq R}} \frac{\chi_{4n}(m)}{m}|^2 \ll K^2 R^{\frac{1}{2}+2\epsilon} \ll R. \tag{2.43}$$

Luego por (2.42), (2.43), el lema 2.15 y la desigualdad de Cauchy vemos que probar la proposición equivale a obtener la fórmula

$$\sum_{R<N<R+L} |B_M(N)|^2 = 3(P/4\pi)^2 L\log K + O(R(\log K)^{2/3}). \tag{2.44}$$

Expandiendo el cuadrado vemos que

$$B_M(N)^2 = \sum_{\substack{m_1,m_2<M\\ m_1,m_2\neq\square}}{}^{*} \sum_{\substack{b_1 (\mathrm{mod}\ m_1)\\ b_2 (\mathrm{mod}\ m_2)}} \frac{\tau_{b_1}(m_1)}{m_1^2}\overline{\frac{\tau_{b_2}(m_2)}{m_2^2}} f(\frac{b_1}{m_1})\overline{f(\frac{b_2}{m_2})} e\big((\frac{b_2}{m_2}-\frac{b_1}{m_1})N\big).$$

Usando la fórmula

$$\sum_{R<N\leq R+L} e(N\theta) = \frac{e((R+L)\theta)}{2\pi\theta} - \frac{e(R\theta)}{2\pi\theta} + O(1) \qquad |\theta|<1/2$$

obtenemos

$$\sum_{R<N<R+L} |B_M(N)|^2 = LS + O(D(\log R)^2) + O(M^2)$$

donde

$$D = \max_{M_1,M_2\leq M} |\sum_{\substack{M_1<m_1<2M_1\\ M_2<m_2<2M_2}}{}^{*} \sum_{\substack{b_1 (\mathrm{mod}\ m_1)\\ b_2 (\mathrm{mod}\ m_2)\\ b_1m_2\neq b_2m_1}} \frac{a_{b_2,m_2}\overline{a_{b_1,m_1}}}{b_2/m_2 - b_1/m_1}|,$$

con $a_{b,m} = m^{-2}f(b/m)\tau_b(m)e(Zb/m)$ para algún $Z\in\mathbb{R}$. Para $M_j\leq m_j\leq 2M_j$ se cumple

$$|\frac{b_2}{m_2}-\frac{b_1}{m_1}| \geq \frac{1}{M_1M_2},$$

luego por la desigualdad de Hilbert generalizada (ver [IK])

$$D \ll \max_{M_1\leq M} M_1^2 \sum_{\substack{M_1<m<2M_1\\ b\ (\mathrm{mod}\ m)}}{}^{*} |a_{b,m}|^2 \ll \max_{M_1\leq M} M_1^{-2} \sum_{\substack{M_1<m<2M_1\\ 1\leq|b|\leq m/2}} |\tau_b(m)|^2 |f(\frac{b}{m})|^2.$$

De (2.36) deducimos que $|\tau_{\lambda s}(cs^2)| \ll c^{\frac{1}{2}}s(\lambda,s)\log\log(s)$, luego para todo $U\leq M_1$ se cumple

$$\sum_{M_1<m<2M_1}{}^{*} \sum_{U<b<2U} |\tau_m(b)|^2 \ll (UM_1^2 + M_1^2\log M_1)\log\log M_1,$$

y como $|f(t)|\ll \min(K,|t|^{-1})$ para $|t|\leq 1/2$ se tiene

$$\sum_{\substack{M_1<m<2M_1\\ 1\leq|b|\leq m/2}}{}^{*} |\tau_b(m)|^2 |f(\frac{b}{m})|^2 \ll (KM_1^3 + K^2M_1^2\log M_1)\log\log M_1$$

luego $D \ll KM \log\log M \ll R$ y por tanto

$$\sum_{R<N<R+L} |B_M(N)|^2 = LS + O(R), \tag{2.45}$$

y teniendo en cuenta la proposición 2.16 queda probada la fórmula (2.44). □

Finalmente llegamos al resultado que buscábamos

Teorema 2.18. *Sea $x > 1$, $K \leq x^{1/4-\epsilon}$. Entonces se cumple*

$$\sum_{N\leq x} (E_2^+(N+K) - E_2^+(N))^2 = (\frac{3Px}{4\pi})^2 \log K + O(x^2(\log K)^{\frac{2}{3}}).$$

Demostración: Por el lema de Abel

$$\sum_{R\leq N\leq 2R} (E_2^+(N+K) - E_2^+(N))^2 = 8RT(R) - 4\int_R^{2R} T(u)du$$

con $T(u) = \sum_{R\leq N\leq u}(4N)^{-1}(E_2^+(N+K) - E_2^+(N))^2$. Para $R > x(\log x)^{-3}$, por la proposición 2.17 tenemos que

$$\sum_{R\leq N\leq 2R} (E_2^+(N+K) - E_2^+(N))^2 = 2(\frac{3P}{4\pi})^2 R^2 + O(R^2(\log K)^{3/2}).$$

Sumando los resultados para $R = x/2^j$, $j \in \mathbb{N}$, con $R > x(\log x)^{-3}$ y usando (2.25) para $R < x(\log x)^{-3}$ deducimos el teorema. □

Capítulo 3

Número de conjuntos suma

3.1. Introducción.

Para cualesquiera A, B subconjuntos de un grupo G definimos su conjunto suma como

$$A + B = \{a + b \in G : a \in A, b \in B\}.$$

Diversas propiedades de estos conjuntos han sido estudiadas, comenzando con el trabajo de Cauchy [Cau], que demostró la desigualdad

$$|A + B| \geq \text{mín}(|A| + |B| - 1, |G|), \tag{3.1}$$

cuando $G = \mathbb{Z}/p\mathbb{Z}$, p primo. Este resultado fue redescubierto un siglo después por H. Davenport [Dav1]. Más tarde, Vosper [Vos] probó que los casos en los que se da la igualdad son muy particulares: si $|A|, |B| \geq 2$, entonces A y B son progresiones aritméticas con la misma diferencia o bien B es una traslación del complementario de A en $\mathbb{Z}/p\mathbb{Z}$.

En el caso $G = \mathbb{Z}$ ocurre algo similar. Se tiene que $|A+B| \geq |A|+|B|-1$ y, cuando son conjuntos de más de un elemento, la igualdad sólo se da en el caso de que A y B sean progresiones aritméticas con la misma diferencia. Finalmente Kemperman [Kem], usando métodos de Kneser y van der Corput, generalizó este tipo de resultado a cualquier grupo abeliano.

En vez de ser tan restrictivos, podemos preguntarnos qué ocurre si permitivos que

$$|A + A| \leq C|A| \tag{3.2}$$

con C una constante positiva. Si $|A + A| \leq 3|A| - 4$ en el caso $G = \mathbb{Z}$ y $|A + A| \leq (12/5)|A| - 3$ con $|A| \leq p/35$ cuando $G = \mathbb{Z}/p\mathbb{Z}$, Freiman (ver

[Nat]) ha probado que A está contenido en una progresión aritmética de longitud inferior a $2|A| - 2$ y $(7/5)|A| - 1$ respectivamente. Sin embargo, cuando la constante C es mayor hay ejemplos de conjuntos A que no estan bien cubiertos por una progresión aritmética. Freiman entendió la situación, y para resolverla consideró conjuntos del tipo

$$P = \{y_0 + \sum_{j=1}^{d} y_j a_j : 0 \leq a_j \leq m_j - 1\}$$

que llamamos progresiones aritméticas de dimensión d. Si las sumas del conjunto son todas distintas, decimos que P es propia, cumpliéndose en este caso que $|P+P| \leq 2^d|P|$. De esta forma probó [Fre] que básicamente estos son los únicos subconjuntos de $\mathbb{Z}$ con suma pequeña, esto es que si $A \subset \mathbb{Z}$ satisface la condición (3.2) entonces A está contenido en una progresión aritmética de dimensión d y tamaño $K|A|$, donde d y K sólo dependen de la constante C. Este resultado ha sido usado por T. Gowers [Gow1, Gow2] para probar que para todo $k \geq 3$, cualquier subconjunto de $\{1, 2 \ldots, N\}$ de tamaño mayor que $N(\log\log N)^{-2^{-2^{k+9}}}$ contiene alguna progresión aritmética no trivial de longitud k, mejorando substancialmente el resultado de Szemerédi [Sze].

I. Ruzsa [Ruz1] generalizó el teorema de Freiman al caso $|A+B| < C|A|$ con $|A| = |B|$ para grupos abelianos libres de torsión, y más tarde [Ruz2] ha probado un resultado del mismo tipo para G grupo abeliano de torsión finita: sea $A \subset G$, tal que existe $B \subset G$ del mismo tamaño que A con

$$|A + B| \leq C|A|,$$

entonces A está contenido en un subgrupo H con $|H| \leq K|A|$, donde K sólo depende de C y del orden máximo de los elementos del grupo G.

También se sabe que si A y B son conjuntos grandes de $\mathbb{Z}/p\mathbb{Z}$, su suma tiene mucha estructura. En particular se ha probado que contiene progresiones aritméticas de tamaño grande. El mejor resultado es de B. Green [Gre1]: si $|A| = \alpha p$ y $|B| = \beta p$ con $\alpha, \beta > 0$, entonces $A + B$ contiene una progresión aritmética de tamaño mayor que

$$e^{K\sqrt{\log p}},$$

donde $K > 0$ sólo depende de α y β.

En otra dirección, recientemente Green y Ruzsa [GrRu] han estudiado el cardinal de $\mathrm{SS}(G)$, el conjuto de conjuntos suma de la forma $A + A$ en un

grupo abeliano finito G. Han obtenido que

$$|\mathrm{SS}(\mathbb{Z}/p\mathbb{Z})| = (2^{\frac{1}{3}})^{p+o(p)},$$

extendiendo más tarde este resultado a otros grupos.

En este capítulo vamos a tratar un problema relacionado, exponiendo los resultados obtenidos en [GU]. Nos va a interesar controlar el número de conjuntos que son suma de conjuntos grandes, es decir vamos a querer conocer el tamaño del conjunto

$$T(k, G) = \{A + B : |A|, |B| \geq k\}.$$

En la primera sección veremos que para el caso $G = \mathbb{Z}/p\mathbb{Z}$ con p primo podemos probar que

Teorema 3.1. *Sea* $p(\log p)^{-1/10} < k < p/8$. *Entonces*

$$|T(k, \mathbb{Z}/p\mathbb{Z})| = (\sqrt{2})^{p+o(p)}.$$

Para demostrarlo usaremos el método de Green y Ruzsa de conjuntos granulares. Básicamente, lo que ocurre es que como A y B son grandes, tenemos que la función característica de $A + B$ se puede aproximar bien por la convolución de las funciones características de A y B en la mayoría de los casos. Esto nos permite tratar el problema mediante análisis armónico en $\mathbb{Z}/p\mathbb{Z}$.

Cuando A es pequeño, la estructura de los conjuntos $B + A$ cambia fuertemente ante cualquier pequeña variación del conjunto A. Esto motiva la siguiente definición: sea G un grupo y A un subconjunto de G. Llamaremos A-conjuntos a los subconjuntos de G que pueden representarse como

$$B + A$$

para algún $B \subset G$. Si G es finito, estamos interesados en controlar el tamaño del conjunto

$$S(A, G) = \{B + A : B \subset G\}.$$

En el caso de que G sea abeliano y finitamente generado, $G = H \times \mathbb{Z}^d$ con H finito, querremos conocer el tamaño de

$$S_N(A, G) = \{B + A : B \subset H \times I_N^d\}$$

cuando N tiende a infinito, con

$$I_N = \{n \in \mathbb{Z} : 1 \leq n \leq N\}.$$

Este tamaño está controlado por la constante (ver lema 3.12)

$$c(A, G) = \lim_{N\to\infty} |S_N(A, G)|^{\frac{1}{N^d|H|}}.$$

En la sección segunda veremos que en el caso $G = \mathbb{Z}$, si A es finito y $\ell(A) = \max_{a,a'\in A} |a - a'|$, se tiene que

$$c(A, \mathbb{Z}) = \rho_A, \tag{3.3}$$

donde ρ_A es el radio espectral de una matriz cuadrada M_A de dimensión $2^{2\ell(A)+1}$ que podemos expresar de forma explícita en términos de A. Esta caracterización, junto con la propiedad

$$c(\lambda A, \mathbb{Z}) = c(A, \mathbb{Z}) \qquad \text{para todo } \lambda \in \mathbb{Z}^\times,$$

donde $\lambda A = \{\lambda a : a \in A\}$, nos va a permitir demostrar que

Teorema 3.2. *Para todo $a, b \in \mathbb{Z}$ distintos, se cumple que*

$$c(\{a, b\}, \mathbb{Z}) = \rho$$

donde $\rho = 1{,}75488\ldots$ es la raiz positiva de la ecuación

$$x^3 - 2x^2 + x - 1 = 0.$$

También podremos calcular la constante $c(A, \mathbb{Z})$ para conjuntos A con $\ell(A)$ pequeña y para conjuntos especiales como $A_k = \{0, 1 \ldots, k - 1\}$.

El caso $|A| = 3$ lo podemos controlar geométricamente, estableciendo la siguiente relación con el caso bidimensional

Teorema 3.3. *Sean $a, b \in \mathbb{Z}$ con $|a| < |b|$ y $(a, b) = 1$. Entonces*

$$c(U_2, \mathbb{Z}^2)^{1-1/b} \leq c(\{0, a, b\}, \mathbb{Z}) \leq c(U_2, \mathbb{Z}^2)^{1+1/b}.$$

con $U_2 = \{(0, 0), (1, 0), (0, 1)\}$. En particular para todo $a \in \mathbb{Z}$ se cumple

$$\lim_{n\to\infty} c(\{0, a, n\}, \mathbb{Z}) = c(U_2, \mathbb{Z}^2).$$

También probaremos que

$$c(U_2, \mathbb{Z}^2) < c(U_1, \mathbb{Z})$$

con $U_1 = \{0, 1\}$. Por el teorema 3.3 deducimos que

Teorema 3.4. *Existe $b^* \in \mathbb{N}$ tal que para todo $b > b^*$ y $a \in \mathbb{N}$, $(a, b) = 1$ se cumple que*

$$c(\{0, a, b\}, \mathbb{Z}) < c(\{0, 1\}, \mathbb{Z}).$$

Definiendo

$$c(k, G) = \sup\{c(A, G) : A \in G, |A| = k\},$$

por el teorema 3.4 vemos que para probar $c(3, \mathbb{Z}) < c(2, \mathbb{Z}) = c(\{0, 1\}, \mathbb{Z})$ sólo resta controlar $c(\{0, a, b\}, \mathbb{Z})$ para un número finito de conjuntos $\{0, a, b\}$. Pero parece que los casos que quedan son demasiado grandes para tratarlos computacionalmente a través de (3.3). Se necesita alguna idea nueva.

Parece razonable pensar que la sucesión $(c(k, \mathbb{Z}))_{k\in\mathbb{N}}$ es siempre decreciente, pero no sabemos probarlo para ningún valor de k mayor que uno. Considerando el conjunto $A = \{1, 2, 4, 6, \ldots, 2k\}$, vemos que

$$c(k, \mathbb{Z}) \geq \sqrt{2} \qquad \text{para todo } k \in \mathbb{N}.$$

Probaremos que esta desigualdad es en realidad estricta. La pregunta natural, en parte motivada por el teorema 3.1, es si esta sucesión decrece hacia $\sqrt{2}$. El teorema 3.1 nos permite demostrar el siguiente resultado parcial

Teorema 3.5. *Sea $\lambda > 0$ y*

$$c_\lambda(k, \mathbb{Z}) = \sup\{c(A, \mathbb{Z}) : |A| = k, \ell(A) \leq \lambda|A|\}.$$

Entonces

$$\lim_{k\to\infty} c_{\lambda(k)}(k, \mathbb{Z}) = \sqrt{2}.$$

para cualquier sucesión $(\lambda(k))_{k\in\mathbb{N}}$, con $2 \leq \lambda(k) \leq (\log k)^{\frac{1}{10}}$.

En la sección tercera estudiaremos $|S(A, \mathbb{Z}/p\mathbb{Z})|$. Para cada $A \in \mathbb{Z}/p\mathbb{Z}$, con $|A| \geq 2$, tenemos los contenidos

$$B + x \subset B + \{x, y\} \subset B + A,$$

(donde $B + x$ denota $B + \{x\}$) para cualesquiera $x, y \in A$. A partir de ellos, por argumentos combinatorios probaremos que

Teorema 3.6. *Para todo $A \subset \mathbb{Z}/p\mathbb{Z}$ de cardinal mayor o igual que dos tenemos que*

$$|S(A, \mathbb{Z}/p\mathbb{Z})| \ll 1{,}9814^p.$$

Por supuesto, pensamos que esta cota no es adecuada, sino que debiéramos tener

$$|S(A, \mathbb{Z}/p\mathbb{Z})| \ll \eta^p \qquad \text{con } \eta < c(\{0,1\}, \mathbb{Z})$$

para todo A con $|A| \geq 3$. En cualquier caso, esto nos permite probar que

$$c(k, \mathbb{Z}) \leq 1{,}9814 \qquad \text{para todo } k \geq 3,$$

y por el teorema 3.1 se puede demostrar que

$$c(2, \mathbb{Z})^{p+o(p)} \ll |T(2, \mathbb{Z}/p\mathbb{Z})| \ll 1{,}9814^{p+o(p)},$$

donde $c(2, \mathbb{Z}) = \rho$ con $\rho = 1{,}7548\ldots$ definida en el teorema 3.2.

3.2. Sumas de conjuntos grandes

En esta sección queremos contar los conjuntos de la forma $A + B$, siendo A y B subconjuntos de $\mathbb{Z}/p\mathbb{Z}$ de tamaño casi comparable a p. Esta cuestión está relacionada con contar los conjuntos de la forma $A + A$ con $A \subset \mathbb{Z}/p\mathbb{Z}$, problema resuelto exitosamente por Green y Ruzsa en [GrRu]. Después de eso B. Green usó el mismo método y otras herramientas para probar en [Gre2] la conjetura de Cameron y Erdős sobre el número de conjuntos libres de suma en $\{1, 2, \ldots, N\}$. Nosotros usaremos su método para probar el teorema 3.1.

Comenzamos dando algo de notación. Sean $f, g : \mathbb{Z}/p\mathbb{Z} \to \mathbb{C}$ y $n \in \mathbb{Z}/p\mathbb{Z}$, definimos la convolución en $\mathbb{Z}/p\mathbb{Z}$ como

$$f * g(n) = \sum_{m \in \mathbb{Z}/p\mathbb{Z}} f(m) g(n - m).$$

También definimos los coeficientes de Fourier

$$\widehat{f}(n) = \sum_{m \in \mathbb{Z}/p\mathbb{Z}} f(m) e(-nm/p).$$

Sea $C \subset \mathbb{Z}/p\mathbb{Z}$, escribimos $C(n)$ para la función indicatriz del conjunto C. Con estas definiciones, y siendo $D \subset \mathbb{Z}/p\mathbb{Z}$, tenemos que

$$C * D(n) = |\{(x, y) \in C \times D : x + y = n\}|.$$

En la prueba usaremos fundamentalmente la igualdad de Plancherel

$$\sum_n |f(n)|^2 = p^{-1} \sum_x |\widehat{f}(x)|^2 \tag{3.4}$$

y también la relación entre la convolución y los coeficientes de Fourier

$$\widehat{f * g}(x) = \widehat{f}(x)\widehat{g}(x). \tag{3.5}$$

Ahora, sea m un número natural fijo. Para cada $d \in (\mathbb{Z}/p\mathbb{Z})^\times$ vamos a dividir $\mathbb{Z}/p\mathbb{Z}$ en m progresiones aritméticas con diferencia común d definidas como

$$J_i(d) = \{\lambda d : \frac{ip}{m} \leq \lambda < \frac{(i+1)p}{m}\},$$

con $0 \leq i \leq m-1$. La longitud de $J_i(d)$ es L o $L-1$, donde $L = \lceil p/m \rceil$. Decimos que $B \subset \mathbb{Z}/p\mathbb{Z}$ es un conjunto m-granular si existen $d \in (\mathbb{Z}/p\mathbb{Z})^\times$ e $I \subset \{0, 1, \ldots, m-1\}$ tales que

$$B = \bigcup_{i \in I} J_i(d).$$

Finalmente, sea C un subconjunto de $\mathbb{Z}/p\mathbb{Z}$ y $\epsilon_1 > 0$, y sea

$$T(d) = \{i \in \{0, 1, \ldots, m-1\} : |C \cap J_i(d)| \geq \epsilon_1 |J_i(d)|\}.$$

Entonces, definimos la $(m, d)-$granularización C' de C (con respecto al parámetro ϵ_1) como

$$C' = C'(d) = \bigcup_{i \in T(d)} J_i(d).$$

Se cumple

$$|C \setminus C'| = \sum_{i \notin T(d)} |C \cap J_i(d)| < \epsilon_1 \sum_{i \notin T(d)} |J_i(d)| \leq \epsilon_1 p, \tag{3.6}$$

teniendo en cuenta que los conjuntos $J_i(d)$ son disjuntos.

El resultado fundamental que se obtiene por el método de Green y Ruzsa es el siguiente

Lema 3.7. *Sea C un subconjunto de $\mathbb{Z}/p\mathbb{Z}$. Existe $d \in (\mathbb{Z}/p\mathbb{Z})^\times$ tal que se cumple*

$$\max_{x\in\mathbb{Z}/p\mathbb{Z}} h_d(x)|\widehat{C}(x)| \leq \frac{(\log((2/3)^{1/2}\pi L))^{1/2}}{(\log p)^{1/2}}|C|^{1/2}p^{1/2}$$

donde

$$h_d(x) = \frac{2}{2L-1}\sum_{j=1}^{L-1}\big(1-\cos\big(\frac{2\pi j dx}{p}\big)\big).$$

Llamaremos "buena longitud para C" a cualquier d satisfaciendo estas condiciones.

Demostración: Sea $\epsilon > 0$. Supongamos que queremos probar que se cumple la desigualdad

$$h_d(x)|\widehat{C}(x)| \leq \epsilon|C| \tag{3.7}$$

para todo $x \in \mathbb{Z}/p\mathbb{Z}$. Por supuesto, se cumple para $x = 0$ o $|\widehat{C}(x)| \leq \epsilon|C|$ (porque $0 \leq h_d(x) \leq 1$). Sea R el conjunto de x restantes, esto es

$$R = \{x \in \mathbb{Z}/p\mathbb{Z} : x \neq 0, |\widehat{C}(x)| > \epsilon|C|\}.$$

Nos queda demostrar que (3.7) se cumple para todo $x \in R$. Escribiendo $\|t\|$ para la distancia de t al entero más cercano, se cumple la desigualdad $1-\cos 2\pi t \leq 2\pi^2\|t\|^2$. Por tanto

$$h_d(x) \leq \frac{4\pi^2}{2L-1}\sum_{j=1}^{L-1}\|\frac{jdx}{p}\|^2 \leq \frac{4\pi^2}{2L-1}\|\frac{dx}{p}\|^2\sum_{j=1}^{L-1}j^2 \leq \frac{2\pi^2L^2}{3}\|\frac{dx}{p}\|^2.$$

Luego, para que se cumpla (3.7) es suficiente que

$$\|\frac{dx_i}{p}\| \leq b_i \tag{3.8}$$

para todo $1 \leq i \leq k$, donde $R = \{x_1, x_2, \ldots, x_k\}$ y

$$b_i = \frac{\sqrt{3}}{\sqrt{2}\pi L}(\frac{\epsilon|C|}{|\widehat{C}(x_i)|})^{1/2}.$$

Pero esto equivale a la siguiente condición: Sean $M = \prod_{i=1}^k[-b_ip, b_ip] \subset \mathbb{R}^k$ y $\Lambda \subset \mathbb{R}^k$ el retículo generado por los vectores $\vec{x}, p\vec{e_1}, p\vec{e_2}, \ldots, p\vec{e_k}$, con $\vec{e_i}$ los

vectores de la base estándar de $\mathbb{R}^k$ y $\vec{x} = (x_1, x_2, \ldots, x_k)$. Existe un elemento $y \in \Lambda, y \neq \vec{0}$ tal que y está también en M.

Por el primer teorema de Minkowski esta última condición se sigue de la ecuación $|M| \geq 2^k|\Lambda|$. Como $|M| = 2^k p^k \prod b_i$ y como podemos comprobar que $|\Lambda| \leq p^{k-1}$, obtenemos que (3.8) se sigue de

$$\prod_{i=1}^{k} b_i \geq \frac{1}{p},$$

o puesto de otra forma

$$w(k) \leq p \tag{3.9}$$

con

$$w(k) = (\frac{2^{1/2}\pi L}{3^{1/2}\epsilon^{1/2}|C|^{1/2}})^k (\prod_{x \in R} |\widehat{C}(x)|)^{1/2}.$$

Ahora podemos usar la desigualdad aritmética-geométrica para decir que se cumple

$$(\prod_{x \in R} |\widehat{C}(x)|)^{1/k} \leq (\frac{1}{k} \sum_{x \in R} |\widehat{C}(x)|^2)^{1/2}.$$

Además, por (3.4)

$$\sum_{x \in R} |\widehat{C}(x)|^2 \leq p|C|, \tag{3.10}$$

y por tanto $w(k) \leq w_1(k)$, con

$$w_1(k) = ((2/3)^2 \pi^4 L^4 \frac{p}{k\epsilon^2|C|})^{k/4}.$$

De (3.10) también obtenemos que $k < p\epsilon^{-2}|C|^{-1}$ y como $w_1(k)$ es una función creciente en este rango tenemos que

$$w_1(p\epsilon^{-2}|C|^{-1}) \leq p \tag{3.11}$$

implica (3.7). Pero (3.11) se cumple con

$$\epsilon \geq (\frac{\log((2/3)^{1/2}\pi L)p}{\log p|C|})^{1/2},$$

luego deducimos el enunciado del lema. □

El siguiente resultado equivale a la proposición 3 en [GrRu], y será fundamental en la prueba del teorema.

Proposición 3.8. *Sean A, B dos subconjuntos de $\mathbb{Z}/p\mathbb{Z}$, y sea $\epsilon_1, \epsilon_2 > 0$, $m \in \mathbb{N}$. Si d es una buena longitud para A entonces las (m,d)-granularizaciones A' y B' (con respecto a ϵ_1) cumplen que $A+B$ contiene todos los x para los que $A' * B'(x) \geq \epsilon_2 p$, con a lo sumo*

$$\frac{324\log((2/3)^{1/2}\pi L)}{\epsilon_1^4\epsilon_2^2\log p}\frac{|A||B|}{p}$$

excepciones.

Demostración: Sea C un subconjunto de $\mathbb{Z}/p\mathbb{Z}$. Definimos la función $f_{C,d} : \mathbb{Z}/p\mathbb{Z} \to \mathbb{R}$ como

$$f_{C,d}(n) = \frac{1}{|dP|}(C * dP)(n) = \frac{1}{|dP|}|C \cap (dP + n)|,$$

donde $P = \{-(L-1), \ldots, -2, -1, 0, 1, 2, \ldots, (L-1)\}$. Nótese que $\widehat{f_{C,d}}(x) = \widehat{C}(x)g_d(x)$, con $g_d(x) = (|dP|)^{-1}\widehat{dP}(x)$. Aplicando la identidad de Plancherel (3.4) dos veces

$$\begin{aligned}
\sum_n |(A*B)(n) - (f_{A,d} * f_{B,d})(n)|^2 &= p^{-1}\sum_x |\widehat{A}(x)\widehat{B}(x) - \widehat{f_{A,d}}(x)\widehat{f_{B,d}}(x)|^2 \\
&= p^{-1}\sum_x |\widehat{B}(x)|^2|\widehat{A}(x)|^2(1-g_d(x)^2)^2 \\
&\leq (\max_x |\widehat{A}(x)||1-g_d(x)^2|)^2 \sum_x \frac{|\widehat{B}(x)|^2}{p} \\
&\leq |B|(\max_x |\widehat{A}(x)||1-g(x)^2|)^2.
\end{aligned}$$

Como $|1-g_d(x)^2| = |(1+g_d(x))(1-g_d(x))| \leq 2|1-g_d(x)|$, usando el lema 3.7 para el conjunto A (porque $1-g_d(x) = h_d(x)$) obtenemos

$$\sum_n |(A*B)(n) - (f_{A,d} * f_{B,d})(n)|^2 \leq 4\frac{\log((2/3)^{1/2}\pi L)}{\log p}|A||B|p. \qquad (3.12)$$

Además, si $n \in A'$ existe una progresión aritmética de diferencia d y longitud L conteniendo a n y al menos $\epsilon_1(L-1)$ puntos de A. A su vez, esta progresión está contenida en $dP+n$. Luego $f_{A,d}(n)$ es como mínimo $\epsilon_1(L-1)/(2L-1) \geq \epsilon_1/3$, y por tanto $f_{A,d}(n) \geq \epsilon_1 A'(n)/3$ para todo $n \in \mathbb{Z}/p\mathbb{Z}$. Por razones

similares se sigue que $f_{B,d}(n) \geq \epsilon_1 B'(n)/3$. Así, obtenemos para todo n las desigualdad $(f_{A,d} * f_{B,d})(n) \geq \epsilon_1^2 (A' * B')(n)/9$.

Ahora consideremos el conjunto $M = \{x \in \mathbb{Z}/p\mathbb{Z}; (A' * B')(x) \geq \epsilon_2 p, x \notin A + B\}$. Se cumple que

$$|(A * B)(n) - (f_A * f_B)(n)|^2 \geq \frac{\epsilon_1^4 \epsilon_2^2 p^2}{3^4} \qquad \text{para todo } n \in M.$$

Sustituyendo en (3.12) obtenemos

$$|M| \leq \frac{4\log((2/3)^{1/2}\pi L)(\log p)^{-1}|A||B|p}{\epsilon_1^4 \epsilon_2^2 p^2/3^4} = \frac{324\log((2/3)^{1/2}\pi L)}{\epsilon_1^4 \epsilon_2^2 \log p}\frac{|A||B|}{p}.$$

□

A grandes rasgos esta proposición dice que, bajo ciertas condiciones, podemos dividir el conjunto de pares (A, B) en unas pocas partes de forma que en cada una de ellas las sumas $A + B$ son muy similares. Ésta es la manera en la que vemos el solapamiento que se produce al sumar conjuntos.

Ahora necesitamos una generalización debida a Pollard [Pol] del teorema de Cauchy-Davenport (desigualdad (3.1))

Proposición 3.9. *Sean $C, D \subset \mathbb{Z}/p\mathbb{Z}$, y para cada $i \in \mathbb{Z}$ sea $R_i = R_i(C, D) = \{n \in \mathbb{Z}/p\mathbb{Z} : (C * D)(n) \geq i\}$. Entonces para todo $r \leq \min(|C|, |D|)$ tenemos que*

$$|R_1| + |R_2| + \ldots + |R_r| \geq r(\min(p, |C| + |D|) - r).$$

Vamos a usarlo para controlar el tamaño del conjunto de elementos que son representables en al menos k maneras distintas como sumas de elementos de C y D:

Proposición 3.10. *Sean C, D subconjuntos de $\mathbb{Z}/p\mathbb{Z}$. Sea k un entero positivo. Entonces, si los tamaños de C y D son más grandes que $\sqrt{kp}$, se cumple*

$$|R_k| \geq \min(|C| + |D|, p) - 2\sqrt{kp}.$$

Demostración: Tenemos que $|R_j| \leq |R_k|$ para $j \geq k$. Por tanto, si $r \geq k$ tenemos

$$r(\min(|C| + |D|, p) - r) \leq |R_1| + \ldots + |R_r| \leq (k-1)p + |R_k|r.$$

de donde

$$|R_k| \geq \text{mín}(|C| + |D|, p) - r - (k-1)p/r.$$

Ahora, tomando $r = [\sqrt{kp}\,]$ en la proposición 3.9 (esto es posible porque $[\sqrt{kp}\,] \leq \text{mín}(|C|, |D|)$) obtenemos el resultado. □

Ya estamos preparados para demostrar el resultado principal

Teorema 3.11. *Sea p un primo. Para todo $\gamma(p) < k < p/8$ tenemos que*

$$|T(k, \mathbb{Z}/p\mathbb{Z})| = 2^{\frac{p}{2}+O(\gamma(p))}$$

donde $p(\log\log p)^{2/3}(\log p)^{-1/9} \ll \gamma(p) \ll p(\log\log p)^{2/3}(\log p)^{-1/9}$.

Demostración: Sean N, M dos conjuntos m-granulares. Definimos

$$\mathcal{F}(N,M) = \{A + B : A, B \subset \mathbb{Z}/p\mathbb{Z}, |A|, |B| \geq \gamma(p) \text{ y existe}$$

d buena longitud para A tal que $N = A'(d), M = B'(d)$(con respecto a ϵ_1)$\}$.

Entonces

$$|\{B + A; B, A \subset \mathbb{Z}/p\mathbb{Z}, |A|, |B| > \gamma(p)\}| \leq \sum_{\substack{N,M\text{conjuntos} \\ m-\text{granulares}}} |\mathcal{F}(N,M)|.$$

Pero

$$|\{(N,M) : N, M \text{ subconjuntos } m\text{-granulares de } \mathbb{Z}/p\mathbb{Z}\}| \leq (p2^m)^2. \quad (3.13)$$

Ahora vamos a acotar $|\mathcal{F}(N,M)|$ para cualquier par de conjuntos m-granulares N, M. Por (3.6) tenemos que si $A + B$ está en $\mathcal{F}(N,M)$ entonces A es un subconjunto de N unión un conjunto de a lo sumo $\epsilon_1 p$ puntos, y B es un subconjunto de M unión un conjunto de a lo sumo $\epsilon_1 p$ puntos. Así

$$|\mathcal{F}(N,M)| \leq \text{n}^\text{o} \text{ posibilidades para } (A,B) \leq 2^{|M|+|N|} \exp(C_1 \log(1/\epsilon_1)\epsilon_1 p) \quad (3.14)$$

para alguna constante $C_1 > 0$. Además, la proposición 3.8 nos dice que si $A + B$ está en $\mathcal{F}(N,M)$ entonces $A + B$ contiene al conjunto $R_{\epsilon_2 p}(N,M)$ menos un conjunto de a lo más $\epsilon_3 p$ puntos (con $\epsilon_3 = 324\log((2/3)^{1/2}\pi L)$ $(\log p)^{-1}\epsilon_1^{-4}\epsilon_2^{-2}$), o equivalentemente el complementario de $A + B$ esta contenido en la unión del complementario de $R_{\epsilon_2 p}(N,M)$ con un conjunto de menos de $\epsilon_3 p$ puntos.

Sean ϵ_1, ϵ_2 con $\epsilon_1 + \epsilon_2^{1/2} \leq \gamma(p)$. Como los tamaños de A y B son mayores que $\gamma(p)$ y $|N| \geq |A| - \epsilon_1 p$, $|M| \geq |B| - \epsilon_1 p$, tenemos que mín$(|N|, |M|) \geq \gamma(p) - \epsilon_1 p \geq \epsilon_2^{1/2} p$. Luego podemos aplicar el teorema 3.9 a los conjuntos N y M, obteniendo

$$|R_{\epsilon_2 p}(N, M)| \geq \text{mín}(|N| + |M|, p) - 2\epsilon_2^{1/2} p.$$

Por lo tanto

$$|\mathcal{F}(N, M)| = |\{(A+B)^c; A + B \in \mathcal{F}(N, M)\}| \leq 2^{p-(|N|+|M|-2\epsilon_2^{\frac{1}{2}} p)} e^{C_2 \log(\frac{1}{\epsilon_3})\epsilon_3 p} \tag{3.15}$$

De las acotaciones (3.14) y (3.15) deducimos

$$|\mathcal{F}(N, M)| \leq 2^{p/2} \exp(C_3 p(\epsilon_2^{\frac{1}{2}} + \log(1/\epsilon_1)\epsilon_1 + \log(1/\epsilon_3)\epsilon_3)),$$

luego por (3.13) tomando $1/L = \epsilon_2^{1/2} = \epsilon_1 \log(1/\epsilon_1)$, $\epsilon_1 = (\log p)^{-\frac{1}{9}} (\log\log p)^{-\frac{1}{3}}$ obtenemos la cota superior del teorema.

La cota inferior es trivial. Sean A, B subconjuntos cualesquiera de $\mathbb{Z}/p\mathbb{Z}$, con $|A|, |B| > p/8$, y sea $y = 0, x = \frac{p-1}{2}$. Si $A \subset [1, [\frac{p-1}{4}]]$ y $B \subset [[\frac{p-1}{4}] + 1, \frac{p-1}{2}]$, entonces

$$(A \cup x) + (B \cup y) = ((A + B) \cup \{x + y\}) \cup (A + y) \cup (B + x),$$

donde las uniones son disjuntas, y por tanto

$$|\{B + A; B, A \subset \mathbb{Z}/p\mathbb{Z}, |A|, |B| > p/8\}| \gg \binom{[p/4]}{[p/8]}^2 = 2^{\frac{p}{2} + O(\gamma(p))}.$$

□

3.3. A-conjuntos

En esta sección vamos a estudiar los A-conjuntos de G un grupo abeliano finitamente generado, centrándonos en el caso $G = \mathbb{Z}$ y en particular en $|A| \leq 3$. Primero vemos la existencia de la constante $c(A, G)$ asociada a los A-conjuntos

Lema 3.12. *Sea $G = H \times \mathbb{Z}^d$, H finito y A subconjunto de G. Existe el límite*

$$c(A, G) = \lim_{N \to \infty} |S_N(A, G)|^{\frac{1}{N^d |H|}},$$

y se tiene que $1 \leq c(A, G) \leq 2$.

Demostración: Para todo $j, N \in \mathbb{N}$ podemos escribir

$$\begin{aligned} S_{jN}(A,G) &= \{\bigcup_{h\in H}(B_h \times \{h\}) + A : B_h \subset I_{jN}^d \, \forall h \in H\} \\ &= \{\bigcup_{u\in I_j^d}(\bigcup_{h\in H}(B_{h,u} \times \{h\}) + A) : B_{h,u} \subset I_N^d + (u-w)N\} \end{aligned}$$

con $w = (1, 1, \ldots, 1) \in \mathbb{Z}^d$, de donde deducimos que

$$|S_{jN}(A,G)| \leq |S_N(A,G)|^{j^d}. \tag{3.16}$$

Sea $M \geq N$, con $M = aN + b$ y $0 \leq b \leq N-1$. Por (3.16) tenemos que

$$|S_M(A,G)|^{M^{-d}} \leq |S_{(a+1)N}(A,G)|^{M^{-d}} \leq |S_N(A,G)|^{N^{-d}(1+N/M)^d}$$

y por tanto para todo $N \in \mathbb{N}$ se cumple

$$\limsup_{M\to\infty} S_M(A,G)^{M^{-d}} \leq S_N(A,G)^{N^{-d}}.$$

Finalmente llegamos a la desigualdad

$$\limsup_{M\to\infty} S_M(A,G)^{M^{-d}} \leq \liminf_{M\to\infty} S_M(A,G)^{M^{-d}},$$

la cuál implica la existencia del límite que define a $c(A,G)$. La cota $c(A,G) \leq 2$ es trivial teniendo en cuenta que $|S_N(A,G)| \leq |\mathcal{P}(H \times I_N^d)|$. □

La constante $c(A,G)$ posee ciertas propiedades

Lema 3.13. *Para todo $A' \subset G$ finito se cumple*

$$c(A + A', G) \leq c(A,G)$$

y para cualquier $x \in G$, se tiene que

$$c(A + x, G) = c(A,G).$$

Demostración: Sea $G = \mathbb{Z}^d \times H$, con H finito. Existe $r \in \mathbb{N}$ tal que $A' \subset I_r^d$. Así, se tiene que $S_N(A + A', G) \subset S_{N+r}(A,G)$ para todo $N \in \mathbb{N}$, lo que prueba $c(A + A', G) = c(A,G)$. Para probar que $c(A + x, G) = c(A,G)$, tenemos en cuenta que la aplicación $C \mapsto C + x$ define una biyección de $S_N(A,G)$ en $S_N(A + x, G)$. □

Además, tenemos el siguiente resultado fundamental

Lema 3.14. *Sea λ automorfismo de $G = \mathbb{Z}^d \times H$. Se cumple que*

$$c(\lambda A, G) = c(A, G).$$

Demostración:

$$S_N(A, G) = \{B + \lambda A : B \subset I_N^d \times H\},$$

luego

$$|S_N(A, G)| = |\{B + A : B \subset \lambda^{-1} I_N^d \times H\}|.$$

Para cada $N \in \mathbb{N}$, existen $R_N \in \mathbb{N}$ y $(v_k)_{1 \leq k \leq R_N}$, $v_k \in \mathbb{Z}^d$ tales que

$$\lambda^{-1} I_{N^2}^d \subset \bigcup_{k=1}^{R_N} (I_N^d + N v_k),$$

y con $R_N |I_N^d| \sim |\lambda^{-1} I_{N^2}^d| = |I_{N^2}^d|$. Por tanto

$$|S_{N^2}(\lambda A, G)| \leq |S_N(A, G)|^{R_N}$$

y haciendo tender N a infinito se tiene

$$c(\lambda A, G) \leq c(A, G).$$

Considerando esta desigualdad para el automormismo λ^{-1} se obtiene la igualdad del enunciado. □

Nota 3.15. Este resultado permite extender la definición de la constante asociada a los A-conjuntos a todo grupo abeliano finitamente generado: Si λ es un isomorfismo de G en $\mathbb{Z}^d \times H$ y $A \subset G$ definimos $c(A, G) = c(\lambda A, \mathbb{Z}^d \times H)$ (el lema anterior nos dice que la definición no depende de λ). Además la constante se conserva por isomorfismo de grupos.

Lema 3.16. *Sea λ un monomorfismo de G. Se cumple que*

$$c(\lambda A, G) = c(A, G).$$

Demostración: Sea $G = \mathbb{Z}^d \times H$, H grupo finito. Por el lema anterior, es suficiente demostrar que $c(fA, G) = c(A, G)$ donde

$$f((a_1, \ldots, a_d, h)) = (\lambda a_1, \ldots, a_d, h), \qquad \lambda \in \mathbb{N}.$$

La imagen de G por f es el subgrupo $(\lambda\mathbb{Z})\times\mathbb{Z}^{d-1}\times H$, lo que nos permite escribir G como la unión disjunta

$$G=\bigcup_{j=1}^{\lambda} g_j+\lambda\mathbb{Z}\times\mathbb{Z}^{d-1}\times H.$$

donde g_j son representantes del grupo G/fG. Por tanto

$$S_{\lambda N}(fA,G)=\{\bigcup_{j=1}^{\lambda}(g_j+f(B_j+A)):B_j\subset I_N\times I_{\lambda N}^{d-1}\times H\,\forall j\in I_\lambda\}$$

y

$$|S_{\lambda N}(fA,G)|=|\{B+A:B\subset I_N\times I_{\lambda N}^{d-1}\times H\}|^{\lambda}. \tag{3.17}$$

Luego $|S_{\lambda N}(fA,G)|\leq|S_N(A,G)|^{\lambda^d}$ lo que prueba que $c(fA,G)\leq c(A,G)$. Por otra parte, escribiendo $w=(1,0,\ldots,0)\in G$, tenemos

$$S_{\lambda N}(A,G)=\{\bigcup_{j=1}^{\lambda}B_j+A+jNw:B_j\subset I_N\times I_{\lambda N}^{d-1}\times H\}$$

y usando (3.17) vemos que $|S_{\lambda N}(A,G)|\leq|S_{\lambda N}(fA,G)|$, lo que prueba el lema. □

Sea C un A-conjunto de un grupo G. Siempre podemos construir el conjunto

$$B_0=\bigcup_{B\subset G,\,B+A=C}B.$$

Se cumple que $C=B_0+A$, y podemos expresar explícitamente B_0 como el conjunto $i_A(C)=\cap_{a\in A}(C-a)$. Por tanto, vemos que ser A-conjunto equivale a satisfacer la condición

$$C=i_A(C)+A.$$

De esta manera, para un grupo abeliano $G=\mathbb{Z}^d\times H$, H finito, y para cualquier subconjunto A finito de G definimos

$$U_A(N,G)=\{C\subset I_N^d\times H:C=i_A(C)+A\}.$$

Si $0\in A$, entonces existe $r\in\mathbb{N}$ tal que para todo $N>r$ se cumple que si $B\subset I_N^d\times H$ entonces $B+A\subset I_{N+r}^d\times H$, y además $i_A(C)\subset C$ para todo C. Por tanto se cumple que

$$S_{N-r}(A,G)\subset U_A(N,G)\subset S_N(A,G).$$

De estos razonamientos deducimos que

Lema 3.17. *Sea $A \subset G$ finito. Entonces*

$$c(A,G) = \lim_{N\to\infty} |U_A(N,G)|^{1/N^d|H|}.$$

Nota 3.18. La igualdad $C = i_A(C) + A$ equivale a satisfacer

$$C \subset \bigcup_{x\in A} \bigcap_{y\in A, y\neq x} C + x - y,$$

o también

$$c \in C \Rightarrow \exists x_c \in A \text{ tal que } c + A \subset x_c + C.$$

En el caso $G = \mathbb{Z}$ esta reformulación nos va a permitir calcular $c(A,\mathbb{Z})$ a través de una recurrencia. Sea d el natural más pequeño tal que $A \subset \{0,1,\ldots,d\}$ (por traslación podemos suponer que 0 es el elemento más pequeño de A). Definimos $\Gamma_d = \{-d,\ldots,d\}$ y

$$\mathcal{E}_A = \{D \subset \Gamma_d : 0 \in D \Rightarrow \exists x \in A \text{ tal que } A \subset D + x\}.$$

Para todo $D \subset \Gamma_d$ definimos

$$v(D) = (D-1) \cap \Gamma_d$$

y

$$u(D) = v(D) \cup \{d\}.$$

Consideramos la biyección entre los conjuntos Γ_d y $I_{2^{2d+1}} - 1$ definida por $C \mapsto \sum_{j\in\Gamma_d} 2^{j+d}u_j$ donde $u_j = 1$ si $j \in C$ y $u_j = 0$ si $j \notin C$. Esta biyección induce una relación de orden en Γ_d.

Así, definimos $M_A = (m_{D,C})$ como la matriz cuadrada indexada en $\mathcal{P}(\Gamma_d)\times \mathcal{P}(\Gamma_d)$, con la relación de orden que acabamos de describir, y

$$m_{D,u(D)} = m_{D,v(D)} = 1 \qquad \text{si } D \in \mathcal{E}_A$$

y $m_{D,C} = 0$ en otro caso. Como la matriz es no negativa, por la teoría de Perron-Frobenius (ver [MeyC]) podemos decir que su radio espectral ρ_A es un autovalor real de M_A y se cumple que

$$\lim_{N\in\mathbb{N}} (\left\|M_A^N\right\|_1)^{1/N} = \rho_A.$$

Pero tenemos el siguiente resultado

Lema 3.19. *Sea $U_A(N) = U_A(N, \mathbb{Z})$. Para todo $N \in \mathbb{N}$, $N > 4d$ se cumple*

$$2^{-8d} \left\| M_A^N \right\|_1 \leq |U_A(N)| \leq \left\| M_A^N \right\|_1 .$$

Demostración: Podemos escribir

$$\begin{aligned} U_A(N) &= \{C \subset I_N : j \in C \Rightarrow \exists x_j \in A \text{ tal que } j + A \subset x_j + C\} \\ &= \{C \subset I_N : (C - j) \cap \Gamma_d \in \mathcal{E}_A \, \forall j \in I_N \}. \end{aligned}$$

Así, consideramos el conjunto

$$\Delta_N = \{(D_j)_{j \in I_N} \in \mathcal{P}(\Gamma_d)^N : m_{D_j, D_{j+1}} = 1 \, \forall j \in I_{N-1}\}.$$

La aplicación

$$f : U_A(N) \longrightarrow \Delta_N$$

definida por $C \mapsto ((C - j) \cap \Gamma_d)_{j \in I_N}$ es una inyección, luego $|U_A(N)| \leq |\Delta_N|$.

Por otra parte, la aplicación

$$g : \Delta_N \longrightarrow U_A(N)$$

definida por

$$(D_j)_{j \in I_N} \mapsto I_d \cup (I_d + N - d) \bigcup_{j=2d+1}^{N-2d} (D_j + j)$$

cumple que $|g^{-1}(C)| \leq 2^{8d}$ para cualquier $C \in U_A(N)$ (porque $g((D_j)_j) = g((D'_j)_j)$ implica que $D_j = D'_j$ para todo $2d + 1 \leq j \leq N - 2d$). Por tanto $2^{8d}|U_A(N)| \geq |\Delta_N|$.

La prueba se concluye observando que

$$|\Delta_N| = \sum_{\substack{(D_1, \ldots, D_N) \\ D_j \in \mathcal{P}(\Gamma_d)}} m_{D_1, D_2} \ldots m_{D_{N-1}, D_N} = \left\| M_A^N \right\|_1 .$$

□

Como consecuencia de este lema deducimos que para $A \subset \mathbb{Z}$ finito

$$c(A, \mathbb{Z}) = \rho_A.$$

Cuando $A = \{0, 1\}$, tenemos que

$$\mathcal{E}_A = \{D \subset \{-1, 0, 1\} : 0 \in D \Rightarrow 0 \in (D-1) \cup (D+1)\} = \mathcal{P}(\Gamma_1) \setminus \{\{0\}\}$$

y

$$M_A = \begin{pmatrix} 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \end{pmatrix}.$$

Calculando el polinomio característico de esta matriz vemos que ρ_A es la raíz real de la ecuación

$$x^3 - 2x^2 + x - 1 = 0.$$

Por tanto

Proposición 3.20. *Se cumple que*

$$c(2, \mathbb{Z}) = c(\{0, 1\}, \mathbb{Z}) = \rho$$

con $\rho = 1{,}75488\ldots$ *la raíz real de la ecuación*

$$x^3 - 2x^2 + x - 1 = 0.$$

De la misma forma podemos calcular (usando el ordenador cuando la matriz es grande) el polinomio mínimo $p_A(t)$ de ρ_A sobre $\mathbb{Z}$ para diferentes conjuntos A de longitud pequeña:

$$A = \{0, 1, 2\} \quad \rho_A = 1{,}6180\ldots \quad p_A(t) = -1 - t + t^2$$

$$A = \{0, 1, 2, 3\} \quad \rho_A = 1{,}5000\ldots \quad p_A(t) = -1 + t^3 - 2t^4 + t^5$$

$$A = \{0, 1, 3\} \quad \rho_A = 1{,}6822\ldots \quad p_A(t) = 1 - 2t^4 + t^5 - t^6 + t^7 - t^8 + t^9 - 2t^{10} + t^{11}$$

$$A = \{0, 1, 2, 3, 4\} \quad \rho_A = 1{,}4655\ldots \quad p_A(t) = -1 - t^2 + t^3$$

$$A = \{0, 1, 2, 4\} \quad \rho_A = 1{,}5750\ldots$$
$$p_A(t) = 1 - 2t^5 + t^6 - t^7 + t^8 - t^9 + t^{11} - 2t^{12} + t^{13}$$

$$A = \{0, 1, 4\} \quad \rho_A = 1{,}6863\ldots$$
$$p_A(t) = 1 + 3t^5 + 2t^8 - t^9 - t^{10} + 2t^{11} - 6t^{12} + t^{13} + t^{16} - t^{18} + t^{19} - 2t^{20} + t^{21}$$

$$A = \{0, 1, 5\} \quad \rho_A = 1{,}6825\ldots$$
$$p_A(t) = -1 - 2t^3 - t^4 - t^6 - 3t^7 + t^8 + 2t^9 - 4t^{10} - 2t^{11} + t^{12} - 6t^{13} + 8t^{14} + t^{15} - 9t^{16}$$
$$+13t^{17} - 4t^{18} - 2t^{19} - 3t^{20} + 13t^{21} + 11t^{22} - 3t^{23} + 20t^{24} + 12t^{25} - 5t^{26} - 2t^{27} + 10t^{28}$$
$$-t^{29} - 10t^{30} - t^{31} + t^{32} - 11t^{33} + t^{34} - t^{35} + 4t^{36} - 2t^{37} + t^{38} + t^{39} - 2t^{40} + t^{42} - 2t^{43} + t^{44}$$

$$A = \{0, 2, 5\} \quad \rho_A = 1{,}6827\ldots \quad p_A(t) = 1 + t + 3t^2 + 3t^3 + 3t^4 + 4t^5 + t^6 + 2t^7 +$$
$$2t^8 - t^9 + 2t^{10} - 2t^{11} + 9t^{12} - t^{13} + 7t^{14} + 12t^{15} - 11t^{16} + 17t^{17} - 12t^{18} + 6t^{19} - 12t^{20} +$$
$$12t^{21} - 20t^{22} + 12t^{23} - 6t^{24} + 2t^{25} - 2t^{26} + 3t^{27} - 2t^{28} + t^{29} - t^{30} + t^{31} - 2t^{32} + t^{33}$$

Para conjuntos A con una estructura sencilla podemos calcular $c(A, \mathbb{Z}) = \rho_A$. Por ejemplo, tenemos que

Proposición 3.21. *Sea $k \in \mathbb{N}$, $k \geq 2$ y $A_k = \{0, 1, \ldots, k-1\}$. Tenemos que*

$$p_{A_k}(t) \mid t^{k+1} - 2t^k + t^{k-1} - 1$$

y por tanto

$$\rho_{A_k} = 1 + \frac{2\log(k-1)}{k-1}(1 + o(1)).$$

Demostración: Podemos probarlo hallando la matriz M_{A_k}, pero como

$$U_{A_k}(N) = \{C \subset I_N : x \in C \Rightarrow \exists j \in A_k, x - j + A_k \subset C\}$$

vemos de forma directa que $U_{A_k}(N)$ se puede poner para $N \geq k+2$ como la unión disjunta

$$U_{A_k}(N) = \Delta_1 \cup \Delta_2 \cup \Delta_3,$$

donde

$$\Delta_1 = \{C_1 \cup \{N\} : C_1 \in U_{A_k}(N-1)\},$$
$$\Delta_2 = \{C_2 \cup (N-k+1+A_k) : C_2 \in U_{A_k}(N-k-1)\},$$
$$\Delta_3 = \{C_3 \cup \{N\} : C_3 \in U_{A_k}(N-1), N-1 \in C_3\},$$

por lo que se cumple la recurrencia

$$|U_{A_k}(N)| = |U_{A_k}(N-1)| + |U_{A_k}(N-k-1)| + (|U_{A_k}(N-1)| - |U_{A_k}(N-2)|),$$

de donde deducimos el resultado para $p_{A_k}(t)$. De esto se sigue la afirmación sobre ρ_{A_k}, teniendo en cuenta que $\rho_{A_k}^{k-1}(\rho_{A_k} - 1)^2 = 1$. □

Pero no sabemos controlar ρ_A en el caso general. Tomando

$$A_k = \{1, 2, 4, 6, \ldots, 2k\}$$

vemos (tomando $B \subset 2\mathbb{Z}$) que para todo $k \in \mathbb{N}$ se tiene

$$c(k, \mathbb{Z}) \geq \sqrt{2}.$$

Podemos probar un resultado algo más fuerte

Proposición 3.22. *Se cumple que*

$$c(k, \mathbb{Z}) \geq 2^{\frac{1}{2}+3^{-k}}.$$

Demostración: Sea A subconjunto finito de $\mathbb{Z}$ y $A' = \{1\} \cup 3A$. Escribiendo

$$B = 3B_0 \cup (3B_1 + 1) \cup (3B_2 + 2)$$

vemos que

$$B + A' = [3(B_0 + A \cup B_2 + 1)] \cup [3(B_1 + A \cup B_0) + 1] \cup [3(B_2 + A \cup B_1) + 2]$$

y tomando $B_2 = \emptyset$ probamos que

$$c(A', \mathbb{Z}) \geq 2^{\frac{1}{3}} c(A, \mathbb{Z})^{\frac{1}{3}}.$$

Comenzando con $A_0 = \{0\}$ y definiendo $A_{j+1} = \{1\} \cup 3A_j$, por la desigualdad que acabamos de demostrar se prueba que

$$c(A_k, \mathbb{Z}) \geq 2^{\frac{1}{2}+3^{-k}}.$$

□

Teniendo en cuenta el teorema 3.11 parece razonable pensar que

$$\lim_{k\to\infty} c(k, \mathbb{Z}) = \sqrt{2}.$$

Como consecuencia de este teorema podemos probar un resultado parcial. Definiendo $\ell(A) = \sup_{a,a'\in A} |a - a'|$ tenemos

Proposición 3.23. *Sea A, con $|A| = k$ y $\ell(A) = d \leq (1/2)k(\log k)^{1/10}$. Entonces*

$$c(A, \mathbb{Z}) \leq 2^{\frac{1}{2}+2dk^{-1}(\log k)^{-1/10}+o(1)}.$$

Demostración: Sea p un primo en el intervalo $[k(\log k)^{10}, 2k(\log k)^{10}]$. Tenemos que $|A| = k \asymp p(\log p)^{-1/10}$, luego aplicando el teorema 3.11 obtenemos

$$|S_{p-d}(A, \mathbb{Z})| \leq |S(A, \mathbb{Z}/p\mathbb{Z})| \leq 2^{\frac{p}{2}+o(p)}.$$

Además, de (3.16) se deduce que $c(A, \mathbb{Z})^{p-d} \leq |S_{p-d}(A, \mathbb{Z})|$ y por tanto

$$c(A, \mathbb{Z}) \leq 2^{\frac{1}{2}+\frac{d}{k(\log k)^{1/10}-d}+o(1)} \leq 2^{\frac{1}{2}+2dk^{-1}(\log k)^{-1/10}+o(1)}.$$

□

Corolario 3.24. *Sea $\lambda > 0$ y*

$$c_\lambda(k, \mathbb{Z}) = \sup\{c(A, \mathbb{Z}) : |A| = k, \ell(A) \leq \lambda|A|\}.$$

Entonces

$$\lim_{k\to\infty} c_\lambda(k, \mathbb{Z}) = \sqrt{2}.$$

En el resto de la sección vamos a tratar el caso $k = 3$. Para ello comenzamos generalizando el concepto de conjunto suma.

Sea H un grupo abeliano finito, $l \in \mathbb{N}$ y $G = \mathbb{Z}^d \times H$. Sea $f : G \to \mathcal{P}(G)$ una función tal que $f(\cdot, h)$ es constante para todo $h \in H$. A partir de f construimos la función $\tilde{f} : \mathcal{P}(G) \to \mathcal{P}(G)$ definida por $\tilde{f}(B) = \bigcup_{b\in B}(b+f(b))$. Para cualquier $s \in \mathbb{Z}$, $0 \leq s \leq d$ y $D \subset G$, $D = \mathbb{Z}^s \times J$ y $J \subset \mathbb{Z}^{d-s} \times H$ un conjunto finito definimos (la existencia del límite se prueba como en el lema 3.12)

$$c(f, D, G) = \lim_{x\to\infty} |\{\tilde{f}(B) : B \subset I_N^s \times J\}|^{1/|I_N^s \times J|}.$$

Cuando f es constantemente igual a A tenemos que $\tilde{f}(B) = B + A$ y escribimos $c(f, D, G) = c(A, D, G)$; además abreviamos $c(f, G, G)$ como $c(f, G)$. Con estas notaciones tenemos el resultado siguiente:

Teorema 3.25. *Sean $a, b \in \mathbb{Z}$, $0 < a < b$ con $(a, b) = 1$. Se cumple que*

$$c(U_2, \mathbb{Z} \times I_{b-1}, \mathbb{Z}^2)^{1-1/b} \leq c(\{0, a, b\}, \mathbb{Z}) \leq c(U_2, \mathbb{Z} \times I_b, \mathbb{Z}^2),$$

con $U_2 = \{(0, 0), (1, 0), (0, 1)\}$.

Demostración: Considerando la biyección

$$w : \mathbb{Z} \to \mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$$

definida por $w(m) = ([m/b], m + b\mathbb{Z})$ (el cociente y el resto al dividir por b), deducimos que

$$c(\{0, a, b\}, \mathbb{Z}) = c(f, \mathbb{Z} \times \mathbb{Z}/b\mathbb{Z})$$

con

$$f(m, \lambda) = \begin{cases} \{(0, 0), (1, 0), (0, a)\} & \text{if } 0 \leq \lambda \leq b - a - 1 \\ \{(0, 0), (1, 0), (1, a)\} & \text{if } b - a \leq \lambda \leq b - 1. \end{cases}$$

Además, por el automorfismo $a^{-1} : \mathbb{Z}/b\mathbb{Z} \to \mathbb{Z}/b\mathbb{Z}$ se sigue que

$$c(f, \mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}) = c(g, \mathbb{Z} \times \mathbb{Z}/b\mathbb{Z})$$

con

$$g(m, \lambda) = \begin{cases} \{(0, 0), (1, 0), (0, 1)\} & \text{if } 0 \leq a\lambda \leq b - a - 1 \\ \{(0, 0), (1, 0), (1, 1)\} & \text{if } b - a \leq a\lambda \leq b - 1. \end{cases}$$

Es directo que

$$c(g', \mathbb{Z} \times I_{b-1}, \mathbb{Z}^2)^{1-1/b} \leq c(g, \mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}) \leq c(g', \mathbb{Z} \times I_b, \mathbb{Z}^2),$$

donde g' es la función inducida por g en el grupo $\mathbb{Z}^2$. Finalmente, las biyecciones $d_j : \mathbb{Z}^2 \to \mathbb{Z}^2$ definidas por $d_j(n,m) = (n,m)$ para $m \leq j$ y $d_j(n,m) = (n+1,m)$ para $m > j$ nos llevan a probar que

$$c(g', \mathbb{Z} \times I_b, \mathbb{Z}^2) = c(U_2, \mathbb{Z} \times I_b, \mathbb{Z}^2).$$

□

Corolario 3.26. *Con las hipótesis del teorema 3.25 se cumple que*

$$c(U_2, \mathbb{Z}^2)^{1-1/b} \leq c(\{0, a, b\}, \mathbb{Z}) \leq c(U_2, \mathbb{Z}^2)^{1+1/b}$$

y en particular

$$\lim_{b \to \infty} c(\{0, a, b\}, \mathbb{Z}) = c(U_2, \mathbb{Z}^2).$$

Demostración: Esto es una consecuencia del teorema 3.25 y de las desigualdades

$$c(U_2, \mathbb{Z}^2) \leq c(U_2, \mathbb{Z} \times I_b, \mathbb{Z}^2) \leq c(U_2, \mathbb{Z}^2)^{1+1/b}.$$

□

Nota 3.27. Si supiésemos que $c(U_2, \mathbb{Z} \times I_b, \mathbb{Z}^2)$ decrece cuando b aumenta, podríamos probar usando el teorema 3.25 que

$$c(3, \mathbb{Z}) < c(\{0, 1\}, \mathbb{Z}),$$

pero con el uso de un ordenador para obtener varios polinomios característicos asociados a las constantes $c(U_2, \mathbb{Z} \times I_b, \mathbb{Z}^2)$.

Nota 3.28. Hasta ahora no hemos sido capaces de encontrar el valor $c(U_2, \mathbb{Z}^2)$. No sabemos incluso como resolver un problema más sencillo: calcular el número de subconjuntos de I_n^2 (para n grande) no teniendo puntos a distancia uno. El único problema relacionado que conocemos es calcular el número de maneras de rellenar I_n^2 con fichas de domino, que está resuelto en la sección 4 de [Lov].

Teorema 3.29. *Se cumple que*

$$c(\{(0,0), (1,0), (0,1)\}, \mathbb{Z}^2) < c(\{0, 1\}, \mathbb{Z}).$$

Demostración: Tenemos que $c(\{0,1\},\mathbb{Z}) = c(\{(0,0),(1,0)\},\mathbb{Z}^2)$. A partir de cualquier conjunto $D = B + \{(0,0),(1,0),(0,1)\}$ con $B \subset \mathbb{N}^2$ finito, vamos a construir un conjunto $D' = B' + \{(0,0),(1,0)\}$ con $B' \subset \mathbb{Z}^2$ finito. Para ello seguiremos el siguiente procedimiento:

Sea $M \in \mathbb{N}$ tal que $D \subset I_M^2$, entonces nos colocamos en el punto (M,M). De ahí pasamos al punto $(M-1,M)$, después al $(M-2,M)$ y así hasta llegar a $(1,M)$. Entonces pasamos al punto $(M,M-1)$ y después al punto $(M-1,M-1)$. En general pasamos del punto (a_0,b_0) al punto (a_0-1,b_0) excepto cuando $a_0 = 1$, que pasamos a (M,b_0-1). Así hasta llegar al punto $(1,1)$. Siguiendo este recorrido, dejaremos intacto el conjunto D sobre el que nos movemos excepto cuando estemos sobre un punto $x_0 \in D$ tal que $x_0+(1,0)$ y $x_0+(-1,0)$ no pertenezcan a D. En este caso, cambiaremos el conjunto D localmente. Comenzamos definiendo algunas abreviaturas para acortar la exposición: $\mathtt{O} \equiv x_0+(-4,0) \in D$, $\mathtt{R} \equiv x_0+(-3,0) \in D$, $\mathtt{S} \equiv x_0+(-3,-1) \in D$, $\mathtt{U} \equiv x_0+(-2,0) \in D$, $\mathtt{V} \equiv x_0+(-2,-1) \in D$, $\mathtt{W} \equiv x_0+(-2,-2) \in D$, $\mathtt{X} \equiv x_0+(-1,0) \in D$, $\mathtt{Y} \equiv x_0+(-1,-1) \in D$, $\mathtt{Z} \equiv x_0+(-1,-2) \in D$, $\mathtt{A} \equiv x_0 \in D$, $\mathtt{B} \equiv x_0+(0,-1) \in D$, $\mathtt{C} \equiv x_0+(0,-2) \in D$, $\mathtt{D} \equiv x_0+(1,0) \in D$, $\mathtt{E} \equiv x_0+(1,-1) \in D$, $\mathtt{F} \equiv x_0+(1,-2) \in D$, $\mathtt{G} \equiv x_0+(2,0) \in D$, $\mathtt{H} \equiv x_0+(2,-1) \in D$, $\mathtt{I} \equiv x_0+(2,-2) \in D$, $\mathtt{J} \equiv x_0+(3,0) \in D$, $\mathtt{L} \equiv x_0+(3,-2) \in D$, $\mathtt{N} \equiv x_0+(4,-1) \in D$, $\tilde{\mathtt{N}} \equiv x_0+(4,-2) \in D$, $\mathtt{Q} \equiv x_0+(5,-2) \in D$. De la misma forma definimos los equivalentes con letras minúsculas significando lo mismo pero con relación de no pertenencia; por ejemplo $\mathtt{h} \equiv x_0+(2,-1) \notin D$. Por conveniencia también abreviamos $\Delta \equiv \mathtt{xABCdEFI}$, $\vartheta \equiv \mathtt{rUVxYABcdE}$, $\gamma \equiv \vartheta\mathtt{WZ}$, $\lambda \equiv \mathtt{XAbdEH}$, $\tau \equiv \mathtt{xaBDEGh}$, $\sigma \equiv \mathtt{vxYABDE}$. Así, modificamos el conjunto D localmente de acuerdo a las siguientes reglas (cuando se produzcan coincidencias entre varias reglas se elegirá la que tenga un número mayor):

1) $\mathtt{xABdE} \mapsto \mathtt{xaBdE}$.
2) $\Delta\mathtt{H} \mapsto \lambda\mathtt{cfi}$.
3) $\Delta\mathtt{GHJKL\tilde{N}q} \mapsto \mathtt{xabcdEfGHiJKl\tilde{n}q}$.
4) $\Delta\mathtt{GHJKL\tilde{N}Q} \mapsto \mathtt{xabcdEfGHiJKl\tilde{N}Q}$.
5) $\Delta\mathtt{HL\tilde{n}} \mapsto \lambda\mathtt{cfIL\tilde{n}}$.
6) $\Delta\mathtt{wZHL} \mapsto \lambda\mathtt{wZCfIL}$.
7) $\Delta\mathtt{wZHl} \mapsto \lambda\mathtt{wZCfil}$.
8) $\Delta\mathtt{gh} \mapsto \tau\mathtt{cfi}$.
9) $\Delta\mathtt{ghL\tilde{n}} \mapsto \lambda\mathtt{cfgIL\tilde{N}}$.
10) $\Delta\mathtt{GhJ} \mapsto \tau\mathtt{CFiJ}$.
11) $\Delta\mathtt{GhJL\tilde{n}} \mapsto \mathtt{xabcdEfGHIJL\tilde{n}}$.
12) $\Delta\mathtt{wZhL} \mapsto \lambda\mathtt{WZCfIL}$.
13) $\Delta\mathtt{wZhl} \mapsto \lambda\mathtt{WZCfil}$.
14) $\Delta\mathtt{vY} \mapsto \sigma\mathtt{cFI}$.
15) $\Delta\mathtt{vwYZ} \mapsto \sigma\mathtt{wzCFI}$.
16) $\vartheta\mathtt{Sw} \mapsto \mathtt{rSUVwXyaBcdE}$.
17) $\gamma \mapsto \mathtt{ruVWXYZAbcde}$.
18) $\gamma\mathtt{oHk} \mapsto \mathtt{ORuVWxYZAbcDehk}$.
19) $\gamma\mathtt{OHk} \mapsto \mathtt{ORuVWXYZAbcdehk}$.

De esta forma, al llegar al punto $(1,1)$ habremos transformado D en el conjunto D' del principio de la prueba. De hecho, para cualquier $N \in \mathbb{N}$ esta transformación define una inyección de $S_N(\{(0,0),(1,0),(0,1)\},\mathbb{Z}^2)$ en $S_{N+10}(\{(0,0),(1,0)\},\mathbb{Z}^2)$, lo que demuestra que $c(\{(0,0),(1,0),(0,1)\},\mathbb{Z}^2) \leq c(\{0,1\},\mathbb{Z})$.

Además, definiendo $A = \{(x,y) \in \mathbb{Z}^2 : \text{máx}(|x|,|y|) \leq 10\}$ se puede ver que para todo conjunto D' imagen por la aplicación y para todo $x_0 \in \mathbb{Z}^2$ se tiene que $D' \cap (x_0 + A) \neq \{x_0 - (1,0), x_0, x_0 + (1,0)\}$. Veamos que ésto prueba la desigualdad estricta entre las constantes:

Por lo que acabamos de demostrar, tenemos que

$$c(U_2,\mathbb{Z}^2)^{N^2+o(N^2)} \leq |\{C \subset I_N^2 : C \text{ es } V\text{-conjunto}, (C - x_0) \cap A \neq A^* \forall x_0 \in \mathbb{Z}^2\}|$$

con $A^* = \{(-1,0),(0,0),(1,0)\}$ y $V = \{(0,0),(1,0)\}$. Luego

$$c(U_2,\mathbb{Z}^2)^{(21N)^2+o(N^2)} \leq |\Omega_{21N}|^N$$

con

$$\Omega_N = \{D \subset I_N \times I_{21} : D \text{ es } V\text{-conjunto}, \, (D - (a,11)) \cap A \neq A^* \, \forall a \in \mathbb{Z}\}.$$

Por otra parte

$$c(V,\mathbb{Z}^2)^{(21N)^2+o(N^2)} = |\{D \subset I_{21N} \times I_{21} : D \text{ es } V\text{-conjunto }\}|^N.$$

Se tiene que $|\Omega_{jN}| \leq |\Omega_{N+1}|^j$ para todo $j \in \mathbb{N}$, lo que prueba la existencia de

$$c_0 = \lim_{N \to \infty} |\Omega_N|^{1/N}$$

y la desigualdad $|\Omega_N| \geq c_0^{N-1}$. Concluimos que

$$|\{D \subset I_{21N} \times I_{21} : D \text{ es } V\text{-conjunto }\}| \geq \sum_{k=0}^{N} \binom{N}{k} c_0^{21N-21k-1} = c_0^{-1}(c_0^{21}+1)^N$$

de donde

$$c(V,\mathbb{Z}^2)^{21^2} \geq c(U_2,\mathbb{Z}^2)^{21^2} + 1.$$

□

Corolario 3.30. *Existe $b_0 \in \mathbb{N}$ tal que para todo $b \geq b_0$ y $(a,b) = 1$ se cumple*

$$c(\{0,a,b\},\mathbb{Z}) < c(\{0,1\},\mathbb{Z}).$$

Nota 3.31. La inyección del teorema 3.29 nos hace pensar que es posible hacer algo similar para los restantes conjuntos $\{0,a,b\}$.

3.4. A-conjuntos módulo p

En esta sección estudiaremos el número de A conjuntos de $\mathbb{Z}/p\mathbb{Z}$, con p primo, donde A es un conjunto de cardinal mayor o igual que dos, probando el teorema 3.6.

Sean $a, b, c \in \mathbb{Z}$, cumpliendo $0 \leq b/2 \leq c \leq b \leq a \leq p$. Definimos los siguientes conjuntos:

$$G(b,c) = \{B \subset \mathbb{Z}/p\mathbb{Z} : |B| = c, |B + \{0,1\}| = b\}.$$

$$F(b,a) = \{E : B + \{0,1\} \subset E, B \subset \mathbb{Z}/p\mathbb{Z}, |E| = a, |B + \{0,1\}| = b\}.$$

Para probar el teorema 3.6 vamos a estudiar el comportamiento de estos conjuntos cuando a, b y c varían

Lema 3.32. *Sea $0 < \alpha/2 < \lambda < \alpha < 1$, con $\alpha p, \lambda p$ enteros. Entonces*

i) Se cumple que

$$|G(\alpha p, \lambda p)| \ll p g(\alpha, \lambda)^p,$$

donde

$$g(\alpha,\lambda) = \frac{\lambda^\lambda}{(\alpha-\lambda)^{(\alpha-\lambda)}(2\lambda-\alpha)^{(2\lambda-\alpha)}} \frac{(1-\lambda)^{1-\lambda}}{(\alpha-\lambda)^{(\alpha-\lambda)}(1-\alpha)^{(1-\alpha)}}.$$

ii) Sea $g_1(\alpha) = \max_{\alpha/2 \leq \lambda \leq \alpha} g(\alpha,\lambda)$. Entonces g_1 es creciente $\forall \alpha$, $0 \leq \alpha < 3/4$.

Demostración: Observamos que

$$G(\alpha p, \lambda p) = \{B \subset \mathbb{Z}/p\mathbb{Z} : |B| = \lambda p, B \text{ es la unión de } (\alpha-\lambda)p \text{ intervalos}\},$$

donde intervalo significa una sucesión $\{a, a+1, a+2, \ldots, a+k-1\} \subset B$ (con $k \geq 1$) tal que $a-1 \notin B$ y $a+k \notin B$. Entonces, podemos escribir $B = \cup_{r=1}^{(\alpha-\lambda)p} I^{(r)}$ con $I^{(r)}$ un intervalo. Luego podemos identificar, salvo traslación, un conjunto B con un elemento $(i_1, j_1, i_2, j_2, \ldots, i_{(\alpha-\lambda)p}, j_{(\alpha-\lambda)p})$ de $\mathbb{N}^{2(\alpha-\lambda)p}$ satisfaciendo las condiciones $i_r, j_r \geq 1$,

$$i_1 + i_2 + \ldots + i_{(\alpha-\lambda)p} = \alpha p$$

y

$$j_1 + j_2 + \ldots + j_{(\alpha-\lambda)p} = (1-\alpha)p.$$

(i_r es el tamaño de $I^{(r)}$ y j_r es el número de elementos de $\mathbb{Z}/p\mathbb{Z}$ entre $I^{(r)}$ e $I^{(r+1)}$). Por tanto, el número de elementos en $G(\alpha p, \lambda p)$ está acotado por

$$p\binom{\lambda p - 1}{(\alpha - \lambda)p - 1}\binom{(1-\lambda)p - 1}{(\alpha - \lambda)p - 1},$$

(el factor p viene de las posibles traslaciones). Usando la fórmula de Stirling obtenemos i).

Para ii), derivando g con respecto a λ, obtenemos que g es creciente en λ si y sólo si se cumple que $r(\lambda) > 0$, donde

$$r(\lambda) = \lambda(\alpha - \lambda)^2 - (2\lambda - \alpha)^2(1 - \lambda).$$

Pero $r(\alpha/2) > 0$, $r(\alpha) < 0$ y hay sólo una raíz (que llamaremos $\lambda_{max}(\alpha)$) de la ecuación $r(\lambda) = 0$ en el intervalo $\alpha/2 < \lambda < \alpha$. Está claro que $g(\alpha, \lambda_{max}(\alpha)) = g_1(\alpha)$. Luego si g es creciente en α para $\lambda = \lambda_{max}(\alpha)$ entonces g_1 es también creciente debido a las ecuaciones

$$g_1(\alpha) = g(\alpha, \lambda_{max}(\alpha)) \leq g(\alpha + \Delta, \lambda_{max}(\alpha)) \leq g_1(\alpha + \Delta)$$

(para $\Delta > 0$ suficientemente pequeño). Calculando $\partial g/\partial \alpha$ nos damos cuenta que g es creciente en α para todo α que cumpla la ecuación

$$\alpha - \lambda < \lambda(1 - \lambda), \tag{3.18}$$

que bajo nuestras condiciones equivale a

$$\lambda > \lambda_0(\alpha) \tag{3.19}$$

con $\lambda_0(\alpha) = 1 - \sqrt{1 - \alpha}$. Así, si $\lambda_{max}(\alpha) > \lambda_0(\alpha)$ entonces g_1 es creciente para este α. Pero esto ocurre si y sólo si $r(\lambda_0(\alpha)) > 0$. Como $\lambda_0(\alpha)$ satisface la ecuación (3.18), tenemos

$$r(\lambda_0(\alpha)) = \lambda_0(\alpha)^3(1 - \lambda_0(\alpha))(1 - 2\lambda_0(\alpha)),$$

y entonces

$$r(\lambda_0(\alpha)) > 0 \Leftrightarrow \lambda_0(\alpha) = 1 - \sqrt{1 - \alpha} < 1/2 \Leftrightarrow \alpha < 3/4.$$

□

Lema 3.33. *Sea $0 < \alpha < \delta < 1$, p primo y $\alpha p, \delta p \in \mathbb{N}$. Se cumple*

$$|F(\alpha p, \delta p)| \ll p^3(\max_{\substack{0\le\alpha_0\le 1\\ 0\le\alpha_1\le\delta-\alpha}} f(\delta,\alpha_0,\alpha_1))^p$$

donde $f(\delta,\alpha_0,\alpha_1)$ es la función

$$\frac{(1-\delta)^{(1-\delta)}(2\delta-1+\alpha_0)^{2\delta-1+\alpha_0}}{\alpha_0^{\alpha_0}\alpha_1^{\alpha_1}(1-\delta-\alpha_0-\alpha_1)^{2(1-\delta-\alpha_0-\alpha_1)}(3\delta-2+\alpha_1+2\alpha_0)^{3\delta-2+\alpha_1+2\alpha_0}}.$$

Demostración: Sea n_i el número de intervalos de longitud i en E $\forall i \ge 1$, y n_0 el número de elementos $s \in \mathbb{Z}/p\mathbb{Z}$ tales que $s \notin E$ y $s-1 \notin E$. Entonces se cumple que $\sum_i in_i = \delta p$ y $\sum_i (i+1)n_i = p$. Además, como $B+\{0,1\} \subset E$ y $B+\{0,1\}$ no tiene elementos aislados, se cumple que $2n_2+3n_3+\ldots \ge \alpha p$. Por tanto $\sum n_i = (1-\delta)p$ y $n_1 \le (\delta-\alpha)p$. Así, el número de conjuntos E con las condiciones del lema será, salvo traslación, menor o igual que

$$((1-\delta)p)! \times \text{ coeficiente de } x^{(1-\delta)p}y^{\delta p} \text{ en } \sum_{n_0=0}^{\infty}\frac{x^{n_0}}{n_0!}\sum_{n_1=0}^{(\delta-\alpha)p}\frac{(xy)^{n_1}}{n_1!}\sum_{n_2=0}^{\infty}\frac{(xy^2)^{n_2}}{n_2!}\ldots$$

$$= \sum_{n_1=0}^{(\delta-\alpha)p}\sum_{n_0=0}^{\infty}\frac{((1-\delta)p)!}{n_0!n_1!} \times \text{ coeficiente de } x^{(1-\delta)p-n_0-n_1}y^{\delta p-n_1}$$

$$\text{en } \exp(xy^2+xy^3+\ldots),$$

y expandiendo $\exp(\frac{xy^2}{1-y})$ esto es igual a

$$\sum_{n_1=0}^{(\delta-\alpha)p}\sum_{n_0=0}\frac{((1-\delta)p)!}{n_0!n_1!((1-\delta)p-n_1-n_0)!} \times \text{ coeficiente de } y^{(3\delta-2)p+n_1+2n_0}$$

$$\text{en } (1-y)^{-((1-\delta)p-n_0-n_1)} =$$

$$= \sum_{n_1=0}^{(\delta-\alpha)p}\sum_{n_0=0}\binom{(1-\delta)p}{n_0,n_1,(1-\delta)p-n_1-n_0}\binom{(2\delta-1)p+n_0}{(1-\delta)p-n_1-n_0}.$$

Usando la fórmula de Stirling para $n_0 = \alpha_0 p$ y $n_1 = \alpha_1 p$, y añadiendo el factor p debido a las traslaciones, obtenemos el resultado. □

Teorema 3.34. *Sea A un subconjunto de $\mathbb{Z}/p\mathbb{Z}$, $|A| \geq 2$. Entonces*

$$|S(A, \mathbb{Z}/p\mathbb{Z})| \ll 1{,}9184^p$$

Demostración: Tomemos dos elementos en $A \subset \mathbb{Z}/p\mathbb{Z}$, x e y. Se cumple que

$$S(A, \mathbb{Z}/p\mathbb{Z}) \subset \bigcup_{0 \leq b/2 \leq c \leq b \leq a \leq p} D_A(a, b, c)$$

donde

$$D_A(a, b, c) = \{B + A : B \subset \mathbb{Z}/p\mathbb{Z}, |B + A| = a, |B + \{x, y\}| = b, |B| = c\}.$$

Entonces

$$|S(A, \mathbb{Z}/p\mathbb{Z})| \leq (p+1)^3 \max_{0 \leq c \leq b \leq a \leq p} |D_A(a, b, c)|. \tag{3.20}$$

Como para todo $d \in (\mathbb{Z}/p\mathbb{Z})^\times$ las aplicaciones $M \mapsto dM$ y $M \mapsto M + d$ son biyecciones de $\mathcal{P}(\mathbb{Z}/p\mathbb{Z})$, tenemos que $|D_A(a, b, c)| = |\overline{D}_{A'}(a, b, c)|$, donde $A' = (y - x)^{-1}A$ y $\overline{D}_{A'}(a, b, c) = \{B + A' : B \subset \mathbb{Z}/p\mathbb{Z}, |B + A'| = a, |B + \{0, 1\}| = b, |B| = c\}$. Además, se tiene que $\overline{D}_{A'}(a, b, c) \subset F(b, a)$ y $|\overline{D}_{A'}(a, b, c)| \leq |G(b, c)|$. Por tanto,

$$|D_A(a, b, c)| \leq \min(|F(b, a)|, |G(b, c)|),$$

y finalmente por los lemas 3.32*i*) y 3.33 y la ecuación (3.20), tomando $a = \delta p, b = \alpha p, c = \lambda p$, obtenemos

$$\begin{aligned} |S(A, \mathbb{Z}/p\mathbb{Z})| &\ll p^6 (\max_{0<\lambda<\alpha<\delta<1} (\min(\max_{0 \leq \alpha_0 \leq 1, 0 \leq \alpha_1 \leq \delta - \alpha} f(\delta, \alpha_0, \alpha_1), g(\alpha, \lambda))))^p \\ &\ll p^6 (\max_{0<\alpha<1} \min(f_1(\alpha), g_1(\alpha)))^p \end{aligned}$$

con

$$f_1(\alpha) = \max_{\substack{(\delta, \alpha_0, \alpha_1) \\ \delta - \alpha_1 \geq \alpha}} f(\delta, \alpha_0, \alpha_1)$$

y $g_1(\alpha)$ definido como en el lema 3.32. Notamos que $f_1(\alpha)$ es decreciente, y por el lema 3.32ii) $g_1(\alpha)$ es creciente si $0 \leq \alpha < 3/4$.

Sea $\widetilde{\alpha}$ un número real con $0 \leq \widetilde{\alpha} < 3/4$. Si $\alpha < \widetilde{\alpha}$, entonces $g_1(\alpha) < g_1(\widetilde{\alpha})$. Si $\alpha > \widetilde{\alpha}$, entonces $f_1(\alpha) < f_1(\widetilde{\alpha})$. Por tanto,

$$\min(f_1(\alpha), g_1(\alpha)) \leq \max(f_1(\widetilde{\alpha}), g_1(\widetilde{\alpha}))$$

para todo α, y entonces

$$|S(A,\mathbb{Z}/p\mathbb{Z})| \ll p^6(\max(f_1(\widetilde{\alpha}),g_1(\widetilde{\alpha})))^p$$

para cualquier $\widetilde{\alpha}$, $0 \le \widetilde{\alpha} \le 3/4$. Elegimos $\widetilde{\alpha} = 0{,}57402$. Usando los multiplicadores de Lagrange vemos que el máximo de la función $f(\delta,\alpha_0,\alpha_1)$ en la región $\delta - \alpha_1 \ge \widetilde{\alpha}$ se da para δ raíz de la ecuación

$$-1-15\widetilde{\alpha}-49\widetilde{\alpha}^2-51\widetilde{\alpha}^3-9\widetilde{\alpha}^4+23\delta+201\widetilde{\alpha}\delta+415\widetilde{\alpha}^2\delta+233\widetilde{\alpha}^3\delta+24\widetilde{\alpha}^4\delta-178\delta^2$$
$$-955\widetilde{\alpha}\delta^2-1158\widetilde{\alpha}^2\delta^2-347\widetilde{\alpha}^3\delta^2-16\widetilde{\alpha}^4\delta^2+635\delta^3+2023\widetilde{\alpha}\delta^3+1333\widetilde{\alpha}^2\delta^3+169\widetilde{\alpha}^3\delta^3$$
$$-1130\delta^4-1965\widetilde{\alpha}\delta^4-547\widetilde{\alpha}^2\delta^4+975\delta^5+715\widetilde{\alpha}\delta^5-325\delta^6=0$$

y en $\alpha_0 = \sqrt{(1-\delta)(\delta-\widetilde{\alpha})}$, $\alpha_1 = \delta - \widetilde{\alpha}$. Como sabemos por la prueba del lema 3.32*ii*), el máximo de $g(\widetilde{\alpha},\lambda)$ en la región $0 \le \lambda \le \widetilde{\alpha}$ se da para λ raíz de la ecuación $r(\lambda) = 0$. Finalmente obtenemos $\delta \approx 0{,}634563$, $\lambda \approx 0{,}36603$ y

$$|S(A,\mathbb{Z}/p\mathbb{Z})| \ll 1{,}9184^p.$$

□

Corolario 3.35. *Se cumple*

$$c(2,\mathbb{Z})^{p+o(p)} \le |T(2,\mathbb{Z}/p\mathbb{Z})| \ll 1{,}9184^{p+o(p)}$$

con $c(2,\mathbb{Z}) = 1{,}75488\ldots$ *la raíz positiva de la ecuación* $x^3-2x^2+x-1=0$.

Demostración: La cota inferior es trivial, teniendo en cuenta la proposición 3.20. Para la superior, por el teorema 3.11 sabemos que

$$|T(\gamma(p),\mathbb{Z}/p\mathbb{Z})| = 2^{p/2+o(p)}.$$

Luego sólo queda estudiar el caso $3 \le |A| \le \gamma(p)$. Aquí tenemos que

$$|\{B+A : A,B \subset \mathbb{Z}/p\mathbb{Z}, 3 \le |A| \le \gamma(p)\}| \le p\binom{p}{\gamma(p)} \max_{3\le|A|\le\gamma(p)} |S(A,\mathbb{Z}/p\mathbb{Z})|.$$

Como

$$p\binom{p}{\gamma(p)} = \exp(o(p)),$$

por el teorema 3.34 obtenemos el resultado. □

Nota 3.36. Pensamos que $|T(2,\mathbb{Z}/p\mathbb{Z})| = |\cup_{|A|=2} S(A,\mathbb{Z}/p\mathbb{Z})| + O(\alpha^p)$ para algún $\alpha < c(2,\mathbb{Z})$, esto es que la cota inferior es la correcta, pero no sabemos como probarlo. Esto es debido en parte al hecho de que cuando $|A| \ge 3$, realmente en la prueba sólo usamos que $|A| \ge 2$. Para conseguirlo habría que encontrar la manera de usar la suposición $|A| \ge 3$ adecuadamente.

Notación

$f \ll g \quad := \quad f = O(|g|).$

$f \sim g \quad := \quad \lim \dfrac{f}{g} = 1.$

$f \asymp g \quad := \quad g \ll f \ll g.$

$f = O(g) \quad := \quad \limsup \dfrac{|f|}{g} < \infty.$

$f = o(g) \quad := \quad \limsup \dfrac{f}{g} = 0.$

$f = \Omega(g) \quad := \quad \limsup \dfrac{|f|}{g} > 0.$

$\mathbb{I}_A \quad :=$ Función característica del conjunto A.

$|A| \quad :=$ Cardinal del conjunto A si es finito, y medida de Lebesgue de A si es infinito.

$(a_1, a_2, \ldots, a_k) \quad :=$ Máximo común divisor de $a_1, a_2, \ldots, a_k$.

$d(n) \quad :=$ Número de divisores de n.

$\omega(n) \quad :=$ Número de factores primos de n.

$\chi \quad :=$ Carácter de Dirichlet.

$\left(\dfrac{d}{n}\right)$:= Símbolo de Legendre-Jacobi-Kronecker.

$\widehat{f}$:= Transformada de Fourier, $\widehat{f}(\xi) = \int_{-\infty}^{\infty} f(x)\, e^{-2\pi i \xi x}\, dx$.

$\mathcal{M}_f$:= Transformada de Mellin, $\mathcal{M}_f(s) = \int_0^{\infty} f(x)\, x^{s-1}\, dx$.

$e(x)$:= $e^{2\pi i x}$.

$C_0^{\infty}(M)$:= Funciones derivables de cualquier orden con soporte compacto en M.

$p^k || n$:= $p^k | n$ y $p^{k+1} \nmid n$.

$\dim_{\mathrm{H}} A$:= Dimensión de Hausdorff de A.

$\dim_{\mathrm{M}} A$:= Dimensión de Minkowski de A.

$\mathcal{H}^s(A)$:= Medida exterior s-dimensional de Hausdorff de A.

$\mathrm{GL}(n, A)$:= Grupo de matrices no singulares $n \times n$ con coeficientes en A.

$\mathrm{SL}(n, A)$:= Grupo de matrices $n \times n$ con determinante 1 y coeficientes en A.

$L(s, \chi)$:= Función L de Dirichlet asociada al carácter χ.

$\{x\}$:= Parte fraccionaria de x.

$\|x\|$:= Distancia al entero más cercano si $x \in \mathbb{R}$, y norma euclídea si es un vector.

$\mathrm{Li}(x)$:= Logaritmo integral, $\mathrm{Li}(x) = \int_2^x \dfrac{dt}{\log t}$.

$\mu(n)$:= Función μ de Möbius, $\mu(1) = 1$, $\mu(n) = 0$ si n no es libre de cuadrados y $\mu(n) = (-1)^k$ si n es producto de k factores primos distintos.

$\Lambda(n)$:= Símbolo de von Magoldt, $\Lambda(n) = \log p$ si $n = p^k$ con p primo, y $\Lambda(n) = 0$ si $n \neq p^k$.

$\zeta(s)$:= Función ζ de Riemann.

$A^\times$:= Unidades del anillo A.

Bibliografía

[Cal] A.-P. Calderón. Intermediate spaces and interpolation, the complex method. *Studia Math.*, 24 113–190, 1964.

[Cau] A. Cauchy. Recherches sur les nombres. *J. École Polytech*, 9 99–116, 1813.

[Cha] F. Chamizo. Automorphic forms and differentiability properties. *Trans. Amer. Math. Soc.*, 356 1909–1935, 2004.

[CC1] F. Chamizo, A. Córdoba. The fractal dimension of a family of Riemann's graphs. *C. R. Acad. Sci. Paris Sér. I Math.*, 317 455–460, 1993. (Erratum: *C. R. Acad. Sci. Paris Sér. I Math.* 320 649–650, 1995).

[CC2] F. Chamizo, A. Córdoba. Differentiability and dimension of some fractal Fourier series. *Adv. Math.*, 142 335–354, 1999.

[CCU] F. Chamizo, E. Cristóbal, A. Ubis. Visible points in the sphere. *Preprint.*

[CI1] F. Chamizo, H. Iwaniec. On the sphere problem. *Rev. Mat. Iberoamericana*, 11 417–429, 1995.

[CI2] F. Chamizo, H. Iwaniec. On the Gauss mean-value formula for class number. *Nagoya Math. J.*, 151 199–208, 1998.

[CU1] F. Chamizo, A. Ubis. An average formula for the class number. *Acta Arith.*, 122 75–90, 2006.

[CU2] F. Chamizo, A. Ubis. Some fourier series with gaps. To appear in *J. Anal. Math.*

[CR] K. Chandrasekharan, R. Narasimhan. Functional equations with multiple gamma factors and the average order of arithmetical functions. *Ann. of Math. (2)*, 76 93–136 1962.

[Che1] J.-R. Chen. Improvement of asymptotic formulas for the number of lattice points in a region of three dimensions. *Sci. Sinica*, 12 151–161, 1963.

[Che2] J.-R. Chen. Improvement on the asymptotic formulas for the number of lattice points in a region of the three dimensions. II. *Sci. Sinica*, 12 751–764, 1963.

[Cho] S. Chowla. On the k-analogue of a result in the theory of the Riemann zeta function. *Math. Z.*, 38 483–487, 1934.

[CiCo] J. Cilleruelo y A. Córdoba. *La teoría de los números*, Mondadori, Madrid, 1992.

[Dav1] H. Davenport. On the addition of residue classes. *J. London Math. Soc. 10, 30-32*, 1935.

[Dav2] H. Davenport. *Multiplicative number theory*, volume 74 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, third edition, 2000.

[Dui] J. J. Duistermaat. Self-similarity of "Riemann's nondifferentiable function". *Nieuw Arch. Wisk. (4)*, 9 303–337, 1991.

[Fal1] K. J. Falconer. *The geometry of fractal sets*, volume 85 of *Cambridge Tracts in Mathematics*. Cambridge University Press, Cambridge, 1986.

[Fal2] K. J. Falconer. *Fractal geometry*. John Wiley & Sons Inc., Hoboken, NJ, second edition, 2003. Mathematical foundations and applications.

[Fre] G. A. Freĭman. *Foundations of a structural theory of set addition*. American Mathematical Society, Providence, R. I., 1973. Translations of Mathematical Monographs, Vol 37.

[Gau] C. F. Gauss. *Disquisitiones arithmeticae*. Springer-Verlag, New York, 1986.

[Ger1] J. Gerver. The differentiability of the Riemann function at certain rational multiples of π. *Amer. J. Math.*, 92 33–55, 1970.

[Ger2] J. Gerver. More on the differentiability of the Riemann function. *Amer. J. Math.*, 93 33–41, 1971.

[Ger3] J. Gerver. On cubic lacunary fourier series. *Trans. Amer. Math. Soc.*, 355 4297–4347, 2003.

[GH] D. Goldfeld, J. Hoffstein. Eisenstein series of $\frac{1}{2}$-integral weight and the mean value of real Dirichlet L-series. *Invent. Math.*, 80 185–208, 1985.

[Gow1] W. T. Gowers. A new proof of Szemerédi's theorem for arithmetic progressions of length four. *Geom. Funct. Anal.*, 8 529–551, 1998.

[Gow2] W. T. Gowers. A new proof of Szemerédi's theorem. *Geom. Funct. Anal.*, 11 465–588, 2001. (Erratum: *Geom. Funct. Anal.*, 11 869, 2001).

[GR] I. S. Gradshteyn, I. M. Ryzhik. *Table of integrals, series, and products*. Academic Press Inc., Boston, MA, 1994.

[GK] S. W. Graham, G. Kolesnik. *van der Corput's method of exponential sums*, volume 126 of *London Mathematical Society Lecture Note Series*. Cambridge University Press, Cambridge, 1991.

[GS] A. Granville, K. Soundararajan. The distribution of values of $L(1, \chi_d)$. *Geom. Funct. Anal.*, 13 992–1028, 2003. (Errata: *Geom. Funct. Anal.*, 14 245–246, 2004).

[GU] A. Granville, A. Ubis. Counting sumsets. *Preprint*.

[Gre1] B. Green. Arithmetic progressions in sumsets. *Geom. Funct. Anal.*, 12(3) 584–597, 2002.

[Gre2] B. Green. The Cameron-Erdős conjecture. *Bull. London Math. Soc.*, 36 769–778, 2004.

[GrRu] B. Green, I. Z. Ruzsa. Counting sumsets and sum-free sets modulo a prime. *Studia Sci. Math. Hungar.*, 41 285–293, 2004.

[GM] A. Grossmann, J. Morlet. Decomposition of Hardy functions into square integrable wavelets of constant shape. *SIAM J. Math. Anal.*, 15 723–736, 1984.

[Har] G. H. Hardy. Weierstrass's non-differentiable function. *Trans. Amer. Math. Soc.*, 17 301–325, 1916.

[HL] G. H. Hardy, J. E. Littlewood. Some problems of diophantine approximation. I. The fractional part of $n^k\Theta$. II. The trigonometrical series associated with the elliptic ϑ-functions. 1914.

[HB1] D. R. Heath-Brown. A mean value estimate for real character sums. *Acta Arith.*, 72 235–275, 1995.

[HB2] 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.

[HW] E. Hernández, G. Weiss. *A first course on wavelets. Studies in Advanced Mathematics*. CRC Press, Boca Raton, FL, 1996.

[HT] M. Holschneider, Ph. Tchamitchian. Pointwise analysis of Riemann's "nondifferentiable" function. *Invent. Math.*, 105 157–175, 1991.

[Hoo] C. Hooley. On the Pellian equation and the class number of indefinite binary quadratic forms. *J. Reine Angew. Math.*, 353 98–131, 1984.

[Hör] L. Hörmander. *The analysis of linear partial differential operators. I*, volume 256 of *Grundlehren der Mathematischen Wissenschaften*. Springer-Verlag, Berlin, 1983. Distribution theory and Fourier analysis.

[IK] H. Iwaniec, Emmanuel Kowalski. *Analytic number theory*, volume 53 of *American Mathematical Society Colloquium Publications*. American Mathematical Society, Providence, RI, 2004.

[Jaf1] S. Jaffard. The spectrum of singularities of riemann's function. *Rev. Mat. Iberoamericana*, 12 441–460, 1996.

[Jaf2] S. Jaffard. Exposants de Hölder en des points donnés et coefficients d'ondelettes. *C. R. Acad. Sci. Paris Sér. I Math.*, 308 79–81, 1989.

[JM] S. Jaffard, Y. Meyer. Wavelet methods for pointwise regularity and local oscillations of functions. *Mem. Am. Math. Soc.*, 587 110 p., 1996.

[Kem] J. H. B. Kemperman. On small sumsets in an abelian group. *Acta Math.*, 103 63–88, 1960.

[Küh] M. Kühleitner. On the class number of binary quadratic forms: an omega estimate for the error term. *Math. Pannon.*, 13 63–78, 2002.

[Lan] E. Landau. *Elementary number theory*. Chelsea Publishing Co., New York, N.Y., 1958.

[LM] P. G. Lemarié, Y. Meyer. Ondelettes et bases hilbertiennes. *Rev. Mat. Iberoamericana*, 2 1–18, 1986.

[Lip] R. Lipschitz. Über die asymptotischen gesetze von gewissen gattungen zahlentheoretischer functionen. *Monatsber. Königl. Akad. Wiss. Berlin*, pages 174–185, 1865.

[Lov] L. Lovász. *Combinatorial problems and exercises*. North-Holland Publishing Co., Amsterdam, second edition, 1993.

[Mer] F. Mertens. Ueber einige asymptotische Gesetze der Zahlentheorie. 1873.

[MeyC] C. Meyer. *Matrix analysis and applied linear algebra*. Society for Industrial and Applied Mathematics (SIAM), Philadelphia, PA, 2000.

[Mey] Y. Meyer. *Wavelets and operators*, volume 37 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, 1992.

[MS] S. D. Miller, W. Schmid. The highly oscillatory behavior of automorphic distributions for S$L(2)$. *Lett. Math. Phys.*, 69 265–286, 2004.

[Nat] M. B. Nathanson. *Additive number theory*, volume 165 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1996. Inverse problems and the geometry of sumsets.

[Neu] E. Neuenschwander. Riemann's example of a continuous, 'nondifferentiable' function. *Math. Intelligencer*, 1 40–44, 1978/79.

[Pet] M. Peter. Mean values of Dirichlet L-series. *Math. Ann.*, 318 67–84, 2000.

[Pol] J. M. Pollard. A generalisation of the theorem of Cauchy and Davenport. *J. London Math. Soc. (2)*, 8 460–462, 1974.

[Pól] G. Pólya. Über die Verteilung der quadratischen Reste und Nichtreste. *Gött. Nach.* , 21–29, 1918.

[Que] H. Queffelec. Dérivabilité de certaines sommes de séries de Fourier lacunaires. *C. R. Acad. Sci. Paris Sér. A-B*, 273 A291–A293, 1971.

[Ruz1] I. Z. Ruzsa. Generalized arithmetical progressions and sumsets. *Acta Math. Hungar.*, 65 379–388, 1994.

[Ruz2] I. Z. Ruzsa. An analog of Freiman's theorem in groups. *Astérisque*, (258):xv, 323–326, 1999. Structure theory of set addition.

[Sar] P. Sarnak. Class numbers of indefinite binary quadratic forms. *J. Number Theory*, 15 229–247, 1982.

[SS] M. Sato, T. Shintani. On zeta functions associated with prehomogeneous vector spaces. *Ann. of Math. (2)*, 100 131–170, 1974.

[Shi] T. Shintani. On zeta-functions associated with the vector space of quadratic forms. *J. Fac. Sci. Univ. Tokyo Sect. I A Math.*, 22 25–65, 1975.

[Sie] C. L. Siegel. The average measure of quadratic forms with given determinant and signature. *Ann. of Math. (2)*, 45 667–685, 1944.

[Smi] A. Smith. The differentiability of Riemann's functions. *Proc. Amer. Math. Soc.*, 34 463–468, 1972.

[Ste] E. M. Stein. *Singular integrals and differentiability properties of functions*. Princeton Mathematical Series, No. 30. Princeton University Press, Princeton, N.J., 1970.

[Sze] E. Szemerédi. On sets of integers containing no four elements in arithmetic progression. *Acta Math. Acad. Sci. Hungar.*, 20 89–104, 1969.

[Tsa] K.-M. Tsang. Counting lattice points in the sphere. *Bull. London Math. Soc.*, 32 679–688, 2000.

[Ubi] A. Ubis. The error term in the average of class number. *Preprint.*

[Vau] R.C. Vaughan. *The Hardy-Littlewood method. 2nd ed.* Cambridge Tracts in Mathematics. 125. Cambridge: Cambridge University Press. vii, 232 p. , 1997.

[Vin1] I. M. Vinogradov. Eine neue Methode, die asymptotischen Ausdrücke der arithmetischen Funktionen zu finden. *Petrograd, Bull. Ac. Sc. (6) 11, 1347-1378* , 1917.

[Vin2] I. M. Vinogradov. Über den mittleren Wert der Klassenanzahl der binären quadratischen Formen von negativer Determinante. *Charikov, Comm. Soc. Math. (2) 16, 10-38* , 1918.

[Vin3] I. M. Vinogradov. 1. Über eine asymptotische Formel aus der Theorie der binären quadratischen Formen. 2. Sur la distribution des résidus et des nonrésidus des puissances. 3. Über die Verteilung der quadratischen Reste und Nichtreste. *1. Permi, Journ. Soc. Phys. et Math. de l'Univ. des Permi 1, 18-28 (1918 (1919)). 2. Ibid. 94-98 (1919). 3. Ibid. 2, 1-14* , 1919.

[Vin4] I. M. Vinogradov. Improvement of the remainder term of some asymptotic formulas. *Izvestiya Akad. Nauk SSSR. Ser. Mat.*, 13 97–110, 1949.

[Vin5] I. M. Vinogradov. Improvement of asymptotic formulas for the number of lattice points in a region of three dimensions. *Izv. Akad. Nauk SSSR. Ser. Mat.*, 19 3–10, 1955.

[Vin6] I. M. Vinogradov. On the number of integer points in a three-dimensional domain. *Izv. Akad. Nauk SSSR Ser. Mat.*, 27 3–8, 1963.

[Vor1] G. Voronoi. Sur un problème du calcul des fonctions asymptotiques. *J. für Math.*, 126 241-282, 1903.

[Vor2] G. Voronoi. Sur une fonction transcendante et ses applications à la sommation de quelques séries. *Ann. de l'Éc. Norm.*, 21 207–267, 459–533, 1904.

[Vos] A. G. Vosper. The critical pairs of subsets of a group of prime order. *J. London Math. Soc.*, 31 200–205, 1956.

[Wei] A. Weil. *L'intègration dans les groupes topologiques et ses applications*. Hermann, Paris, deuxième édition, 1965.

[Zyg] A. Zygmund. *Trigonometric series. Vol. I and II.* Cambridge University Press. XIV, 1977.