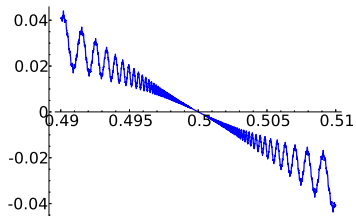


2.3. Sumas oscilatorias

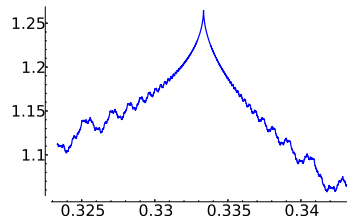
Las sumas oscilatorias que vamos a tratar son sumas trigonométricas, los parientes discretos de las integrales oscilatorias que ya hemos estudiado. Esta naturaleza discreta hace que se manifiesten en ocasiones fenómenos aritméticos que no han aparecido en nuestro análisis de las integrales oscilatorias. Aunque en lo sucesivo nos ocuparemos de sumas finitas, damos aquí una ilustración de este hecho a través de una serie que según K. Weierstrass [Edg04] fue considerada por Riemann como un ejemplo de función continua no derivable en ningún punto. En realidad sí lo es en infinitos puntos, aunque esto no se probó hasta 1970 ¡y lo hizo un estudiante! La serie en cuestión es

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

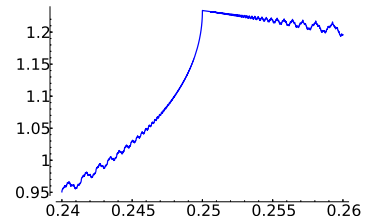
Una mirada cercana alrededor de los puntos $x = 1/2$, $1/3$ y $1/4$ muestra las siguientes curiosas gráficas



$R(x)$ en $[0.490, 0.510]$



$R(x)$ en $[0.323, 0.343]$



$R(x)$ en $[0.240, 0.260]$

Pues bien, para $x = a/b$ fracción irreducible, cualitativamente se obtiene, con un “zoom” suficientemente grande, una de estas tres situaciones. Si $b \equiv 2 \pmod{4}$, al igual que en la primera figura, hay una oscilación que se estrecha tanto que llega a haber tangente en x (por tanto es derivable en ese punto), la pendiente es de hecho siempre $-\pi$. Si $b \equiv 1, 3 \pmod{4}$, entonces siempre hay una tangente vertical (pendiente infinita) como en la segunda figura. En el caso restante, $b \equiv 0 \pmod{4}$, hay siempre una tangente vertical por un lado y no por el otro, como en la tercera figura. Saber por qué lado aparece la tangente vertical, o en el segundo caso, si hay una cúspide o no, requiere considerar propiedades aritméticas más finas de a y b [Dui91] relacionadas con la ley de reciprocidad cuadrática. Finalmente, en los irracionales, no hay patrones claros. Según varía la escala surgen diferentes configuraciones fractales que no se estabilizan y dependen de la aproximación por racionales del punto considerado.

La relación entre sumas oscilatorias y teoría de números actúa en ambos sentidos, a veces se usan métodos aritméticos para estudiar funciones como la anterior y a veces obtenemos resultados aritméticos con técnicas analíticas. Este último esquema es parte de un área muy amplia llamada *teoría analítica de números* de la que veremos algunos ejemplos.

2.3.1. El método de van der Corput

Si una función varía lentamente, todos sabemos por los cursos básicos de cálculo o de manera más precisa por la Proposición 1.2.8 que las sumas se aproximan por integrales. Sin embargo parece increíble que se salve de algún modo esta idea trabajando con sumas oscilatorias en las que cada término presenta una variación apreciable con respecto al anterior. El método introducido por J. van der Corput alrededor de 1920 se basa en llevar a cabo esta aproximación, aparentemente imposible, de una suma oscilatoria por una o varias integrales oscilatorias. Además se combina con un ingenioso argumento elemental debido a H. Weyl que actúa sobre las fases.

La idea de aproximar sumas oscilatorias por integrales oscilatorias es fácil de entender cuando se consideran sumas regularizadas

$$S = \sum_n \varphi(n) e(f(n)) \quad \text{con} \quad \varphi \in C_0^\infty(\mathbb{R}).$$

La fórmula de sumación de Poisson (Teorema 1.2.4) implica

$$S = \sum_n \int_{-\infty}^{\infty} \varphi(x) e(f(x) - nx) dx$$

y en primera instancia tenemos S escrita como suma de infinitas integrales. En el soporte de φ , la derivada de la fase $F(x) = f(x) - nx$ será grande en valor absoluto cuando $|n|$ es grande y un argumento similar al empleado en la Proposición 2.2.1 permite deducir que la contribución es pequeña. En la cantidad finita de integrales que restan, se pueden usar los lemas de van der Corput (Proposición 2.2.4) o incluso alguna variante del principio de fase estacionaria para obtener una nueva suma trigonométrica.

En muchas aplicaciones en teoría de números, las sumas trigonométricas aparecen sin regularizar, a pesar de que en muchas ocasiones esto es más una costumbre que una necesidad teórica real. Ello causa que el argumento antes indicado requiera modificaciones fundamentales.

Proposición 2.3.1. *Sea $f \in C^2([a, b])$, $a, b \in \mathbb{Z}$ con f' monótona, y $\alpha, \beta \in \mathbb{Z}$ tales que $\alpha < f' < \beta$; entonces*

$$\sum_{a \leq n \leq b} e(f(n)) = \sum_{\alpha \leq n \leq \beta} \int_a^b e(f(x) - nx) dx + O(\log(\beta - \alpha + 1)).$$

Demostración. Cambiando $f(n)$ por $f(n) - \alpha n$, lo cual no modifica el valor de la suma, podemos suponer $\alpha = 0$.

Integrando por partes en la Proposición 1.2.6 (cambiando n por $-n$), se tiene

$$(2.29) \quad \sum_{a \leq n \leq b} e(f(n)) = \int_a^b e(f(x)) dx + \sum_{n \neq 0} \frac{1}{n} \int_a^b f'(x) e(g(x)) dx + O(1),$$

con $g(x) = f(x) - nx$.

Si $n > \beta$ o $n < \alpha = 0$, se tiene $g'(x) \neq 0$ en $[a, b]$ y se puede integrar por partes para obtener

$$2\pi \left| \int_a^b f'(x)e(f(x) - nx) dx \right| \leq \left| \frac{f'(a)}{g'(a)} \right| + \left| \frac{f'(b)}{g'(b)} \right| + \int_a^b |(f'/g')'| \leq \frac{2\beta}{|\beta - n|},$$

donde para la última desigualdad se ha usado que f'/g' es monótona (ya que es composición de f' y una función creciente) y por tanto se pueden meter la última integral dentro del valor absoluto, como en la prueba de la Proposición 2.2.4. Nótese que esto asegura la convergencia absoluta de la serie en (2.29). Según lo anterior, la contribución de los términos con $n > \beta$ y $n < 0$ está acotada por

$$\sum_{n=-\infty}^{-1} \frac{\beta}{n(n-\beta)} + \sum_{n=\beta+1}^{\infty} \frac{\beta}{n(n-\beta)} \ll \sum_{|n|>2\beta} \frac{1}{n^2} + \sum_{0 \neq |n| \leq 2\beta} \frac{1}{|n|} \ll \log(\beta + 2),$$

donde se han aproximado sumas por integrales. Sustituyendo en (2.29) se tiene

$$\sum_{a \leq n \leq b} e(f(n)) = \int_a^b e(f(x)) dx + \sum_{0 < n \leq \beta} \frac{1}{n} \int_a^b f'(x)e(g(x)) dx + O(\log(\beta + 2)).$$

Ahora bien,

$$\int_a^b f'(x)e(g(x)) dx - n \int_a^b e(g(x)) dx = \frac{e(g(b)) - e(g(a))}{2\pi i} = O(1)$$

y despejando y sustituyendo $\int f'(x)e(g(x)) dx$ se obtiene el resultado. \square

La condición $\alpha, \beta \in \mathbb{Z}$ se ha introducido en el enunciado para simplificarlo (véase en [IK04] la forma habitual) y tiene como contrapartida que alguna de las integrales pueden ser incorporadas fácilmente en el término de error. Para incidir sobre este punto separamos un caso particular.

Corolario 2.3.2. *Con la notación de la Proposición 2.3.1, si $|f'| \leq 1/2$ en $[a, b]$, entonces*

$$\sum_{a \leq n \leq b} e(f(n)) = \int_a^b e(f(x)) dx + O(1).$$

Demostración. Basta aplicar la Proposición 2.3.1 con $\alpha = -1$, $\beta = 1$ y estimar las integrales correspondientes a $n = \pm 1$ con el caso $k = 1$ de la Proposición 2.2.4. \square

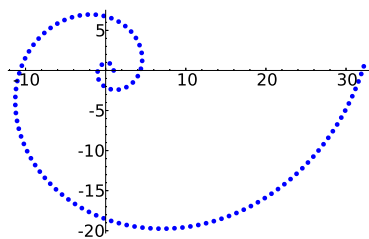
Un ejemplo correspondiente a $f(n) = \frac{3}{2\pi} \log n$ es

$$\sum_{n=1}^N n^{3i} = \frac{N^{1+3i}}{1+3i} + O(1).$$

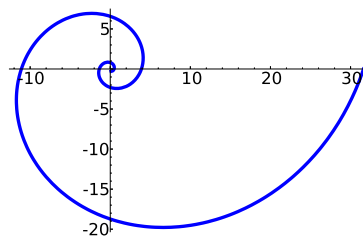
Entonces la gráfica de las sumas parciales de $\sum n^{3i}$ hasta N debe aproximarse por la curva parametrizada

$$c(t) = \left(\frac{t}{10} \cos(3 \log t) + \frac{3t}{10} \sin(3 \log t), -\frac{3t}{10} \cos(3 \log t) + \frac{t}{10} \sin(3 \log t) \right)$$

que es una *espiral equiangular* (reparametrizada en polares, $r = Ce^\theta$).



$\sum_{n \leq k} n^{3i}$ con $1 \leq k \leq 100$



$c(t)$ con $1 \leq t \leq 100$

Una vez que con la Proposición 2.3.1 sabemos aproximar sumas oscilatorias por integrales oscilatorias, estamos en situación de aplicar técnicas como las de la anterior sección. El empeño en no regularizar sólo deja como opciones directas aplicar los lemas de van der Corput (Proposición 2.2.4). El siguiente resultado es el más emblemático en este sentido. Es posible dar una prueba elemental sin pasar por la Proposición 2.3.1 con un uso ingenioso de la sumación por partes, aunque no seguiremos esa línea aquí (véase [GK91]).

Teorema 2.3.3. *Sea $f \in C^2([a, b])$ con $a, b \in \mathbb{Z}$. Si $0 < \lambda \ll |f''| \ll \lambda$ entonces*

$$\sum_{a \leq n \leq b} e(f(n)) \ll (b-a)\lambda^{1/2} + \lambda^{-1/2}.$$

Demostración. El teorema del valor medio aplicado a f' , asegura que en la Proposición 2.3.1 se pueden elegir α y β con $\beta - \alpha \ll \lambda(b-a) + 1$. Según la Proposición 2.2.4 con $k = 2$, cada una de las integrales es $O(\lambda^{-1/2})$, de forma que

$$\sum_{a \leq n \leq b} e(f(n)) \ll (\lambda(b-a) + 1)\lambda^{-1/2} + \log(\lambda(b-a) + 2).$$

Si $\lambda \leq 1$ el primer sumando domina al logaritmo, mientras que para $\lambda > 1$ el teorema es trivial. \square

Si por ejemplo aplicamos el resultados con $[a, b] = [1, N]$ y $f(n) = n^2/N$, se tiene una acotación para las sumas de Gauss del orden correcto según la Proposición 1.2.7, además se deduce que las sumas parciales de las sumas de Gauss también son $O(\sqrt{N})$, lo cual no es intuitivo en absoluto.

La condición $\lambda \ll |f''| \ll \lambda$, es decir, que f'' presente valores comparables en todo el intervalo es típica y muchas forzada tras una subdivisión en intervalos diádicos. La debilidad del resultado aparece cuando λ es muy pequeño o cuando es poco pequeño, concretamente si $\lambda \ll (b-a)^{-2}$ o $\lambda \gg 1$. el primer caso no es tan importante porque indica que f es prácticamente una función lineal. A pesar de que podemos dar fases como $f(n) = n^2$ que se ajustan al segundo caso para las que la única acotación es la trivial, en principio no hay razón para suponer que si $e(f(n))$ oscila realmente, la condición $\lambda \gg 1$ impida la cancelación. Así por ejemplo, esperamos que haya cancelación en $\sum e(n^{5/2})$. La idea para tratar estas sumas que oscilan demasiado como para que el Teorema 2.3.3 sea útil proviene de un trabajo anterior de Weyl de principios del siglo XX. Se basa simplemente en subdividir el intervalo de sumación en subintervalos y calcular su módulo al cuadrado. Con ello se obtendrán incrementos de las fases y la oscilación será menor. Graduando la longitud de los intervalos, el parámetro H en el siguiente resultado, tendremos cierto control sobre la magnitud de la oscilación.

Lema 2.3.4. *Dada una función $f : [a, b] \rightarrow \mathbb{R}$ con $a, b \in \mathbb{Z}$, para cualquier entero positivo $H \leq b - a$ se tiene*

$$\left| \sum_{a \leq n \leq b} e(f(n)) \right|^2 \leq \frac{4(b-a)^2}{H} + \frac{4(b-a)}{H} \sum_{1 \leq r < H} \left| \sum_{a \leq n \leq b-r} e(f(n+r) - f(n)) \right|.$$

Demostración. Para cada $n \in \mathbb{Z}$ consideremos el intervalo $I_n = [1, H] \cap [a-n, b-n]$. El paso inicial, a veces llamado *Weyl shift*, es el artificio aparentemente inútil de repetir la suma H veces

$$|S| = \left| \sum_{a \leq n \leq b} e(f(n)) \right| = \left| \frac{1}{H} \sum_n \sum_{m \in I_n} e(f(m+n)) \right| \leq \frac{1}{H} \sum_{a-H \leq n \leq b-1} \left| \sum_{m \in I_n} e(f(m+n)) \right|.$$

La desigualdad de Cauchy-Schwarz produce los incrementos de f

$$|S|^2 \leq \frac{b-a+H}{H^2} \sum_{a-H \leq n \leq b-1} \sum_{m \in I_n} \sum_{l \in I_n} e(f(m+n) - f(l+n)).$$

Separando el término diagonal $l = m$ y notando que intercambiar l y m sólo conjuga los sumandos; al cambiar el orden de sumación se tiene:

$$|S|^2 \leq \frac{b-a+H}{H^2} \left(H(b-a+H) + 2 \sum_{1 \leq l < m \leq H} \left| \sum_{a-l \leq n \leq b-m} e(f(m+n) - f(l+n)) \right| \right).$$

Ahora basta renombrar $l+n \mapsto n$, $m-l \mapsto r$ y emplear $H \leq b-a$. \square

La estrategia es ahora clara, si una suma oscila demasiado, entonces le aplicamos unas cuantas veces el Lema 2.3.4 para terminar usando el Teorema 2.3.3. Con esta idea se obtiene el siguiente resultado que se reduce a Teorema 2.3.3 cuando $k = 2$.

Teorema 2.3.5. *Sea $f \in C^k([a, b])$ para cierto $k \geq 2$ con $a, b \in \mathbb{Z}$. Supongamos que $\lambda \leq |f^{(k)}(x)| \leq h\lambda$ con $h, \lambda \in \mathbb{R}^+$, entonces*

$$\sum_{a \leq n \leq b} e(f(n)) \ll h^{2/K} (b-a) \lambda^{1/(2K-2)} + (b-a)^{1-2/K} \lambda^{-1/(2K-2)} \quad \text{donde } K = 2^{k-1}.$$

Demostración. Suponemos $\lambda > 1$ ya que en otro caso la cota es trivial.

Procedemos por inducción en k . Como ya hemos observado, el caso $k = 2$ es el Teorema 2.3.3. Si suponemos el resultado cierto hasta $k - 1$, se tendrá

$$\sum_{a \leq n \leq b-r} e(f(n+r) - f(n)) \ll h^{2/K'} (b-a) (r\lambda)^{1/(2K'-2)} + (b-a)^{1-2/K'} (r\lambda)^{-1/(2K'-2)}$$

con $K' = K/2$, porque la derivada $k - 1$ -ésima de $f(n+r) - f(n)$ está entre $r\lambda$ y $hr\lambda$, por el teorema del valor medio. Introduciendo esta cota en el Lema 2.3.4 y eligiendo como H la parte entera de $\lambda^{-1/(K-1)}$, después de hacer algunas operaciones se obtiene el resultado. \square

Por ejemplo con $k = 3$ y $k = 4$ se obtiene

$$\sum_{N \leq n \leq 2N} e(n^{5/2}) \ll N^{11/12} \quad \text{y} \quad \sum_{N \leq n \leq 2N} e(n^{5/2}) \ll N^{25/28}$$

mientras que el Teorema 2.3.3 daba la acotación trivial. Valores mayores de k no producen ninguna mejora sobre la última cota.

Es posible rescatar la idea del principio de fase estacionaria para integrales en intervalos acotados. Por dar una idea del tipo de resultados (véase [Ivi03], [IK04] y [Mon94]), mencionaremos por ejemplo que si $f \in C^4([a, b])$ con $0 < \lambda \leq f'' < 1$ tiene un punto estacionario $f'(c) = 0$ con $\min(b-c, c-a) \gg b-a$ y $|f^{(k)}|(b-a)^{k-2} \ll \lambda$ para $k = 3$ y $k = 4$, entonces

$$\int_a^b e(f(x)) dx = \frac{e(f(c) + 1/8)}{\sqrt{f''(c)}} + O(\lambda^{-1}(b-a)^{-1}).$$

Si utilizamos resultados de este tipo en la Proposición 2.3.1 habremos transformado la suma inicial en una nueva suma. Esto es lo que se llama *Proceso B*. Por otra parte, también el Lema 2.3.4 permite pasar de una suma a otra, es lo que se llama *Proceso A*. Combinando ambos procesos para terminar aplicando la estimación trivial, completa el método de van der Corput. De cara a la presentación de esta idea, el método de *pares*

de exponentes [GK91] describe de forma sencilla y elegante cómo actúan estos procesos en una suma oscilatoria bajo ciertas condiciones (bastante estrictas). De hecho existe un algoritmo que permite hallar la mejor manera de combinar ambos procesos para una suma dada. Las mejoras son habitualmente cualitativamente pequeñas con respecto de la cota del Teorema 2.3.5. Por ejemplo, la suma $S = \sum_{n < \sqrt{t}} n^{it}$ es relevante en el estudio de la función ζ (véase [Ivi03]). Si aplicamos para acotarla el Teorema 2.3.5 con $k = 3$, tras dividir en intervalos diádicos se tiene

$$S = \sum_{N=2^j \leq \sqrt{t}} \sum_{\substack{N \leq n < 2N \\ n < \sqrt{t}}} e\left(\frac{t}{2\pi} \log n\right) \ll \sum_{N=2^j \leq \sqrt{t}} \left(N(t/N^3)^{1/6} + N^{1/2}(t/N^3)^{-1/6}\right) \ll t^{5/12}.$$

Por otro lado, la mejor combinación de los procesos A y B reduce el exponente $5/12$ en poco más de 2 milésimas

2.3.2. La gran criba

Si se consideran sumas oscilatorias con cierta amplitud suave, $\sum A(n)e(f(n))$, podemos sumar por partes y trabajar con sumas sin amplitud. Sin embargo, en diversas situaciones, especialmente en teoría de números, las amplitudes son funciones que varían de forma incontrolable, muchas veces con contenido aritmético. La aspiración sería una teoría de sumas oscilatorias con coeficientes arbitrarios $\sum a_n e(f(n))$ pero tal cosa no puede existir porque si los coeficientes al variar entran en “resonancia” con las fases acabarán con la cancelación, el caso extremo es $a_n = e(-f(n))$. En muchos problemas, aparecen familias de sumas con unos mismos coeficientes. Bajo la denominación de *gran criba* se recogen una serie de técnicas que explotan la idea de que si hay cierta “independencia” entre las fases de las diferentes sumas, entonces los coeficientes no pueden entrar en resonancia en todas ellas y aunque alguna suma pueda ser grande, en promedio serán pequeñas.

El nombre de gran criba requiere cierta explicación. Fue introducido en un trabajo de Yu.V. Linnik y seguramente su difusión debe mucho a que apareció en el título de un libro de E. Bombieri. El hecho es que en algunas de las aplicaciones originales (en especial en la de Linnik) la acotación de sumas oscilatorias se usaba para diseñar un método para estimar el tamaño de un conjunto que evitase muchas clases de congruencia (véase el Teorema 2.3.8), lo que se llama en general un *método de criba*, en recuerdo de la criba de Eratóstenes. El nombre ha permanecido pero es poco indicativo y confuso porque se aplica por igual a las acotaciones de sumas trigonométricas y a los propios métodos de criba.

Aquí trataremos el caso más habitual, el de fases lineales, en el que la independencia se expresa como una separación entre las frecuencias. La terminología en uso es bastante intuitiva: Se dice que x_1, x_2, \dots están δ -espaciados en \mathbb{T} , con $0 < \delta < 1$, si al considerarlos

como números reales, cumplen $\delta \leq \|x_\nu - x_\mu\|$ para $\nu \neq \mu$ donde $\|\cdot\|$ indica la distancia al entero más cercano. Esto es como decir que estén a distancia al menos δ unos de otros cuando pensamos \mathbb{T} enrollado como una circunferencia de longitud 1.

Proposición 2.3.6 (Desigualdad de gran criba). *Existe una constante absoluta C tal que si $x_1, x_2, \dots \in \mathbb{T}$ están δ -espaciados se cumple*

$$\sum_{\nu} \left| \sum_{n=1}^N a_n e(nx_\nu) \right|^2 \leq C(N + \delta^{-1}) \sum_{n=1}^N |a_n|^2$$

para cualesquiera $a_1, a_2, \dots, a_n \in \mathbb{C}$. De hecho, se puede tomar $C = 1$.

La complicación artificial del enunciado en lo que respecta a la constante, tiene una explicación. Deducir la desigualdad con constante uno, que es óptima, es bastante más duro y no es necesario para muchas aplicaciones, por ello probaremos en primer lugar la Proposición 2.3.6 para una constante indeterminada y después obtendremos el caso $C = 1$ dando por supuesto cierto resultado.

La prueba con la constante indeterminada la obtendremos con un argumento analítico elemental que se debe a P.X. Gallagher. Siguiendo el razonamiento con un poco de cuidado, se podría obtener $C = \pi$ como constante válida.

Demostración de la Proposición 2.3.6 con C indeterminada. Si $I \subset \mathbb{R}$ es un intervalo, para todo $x, y \in I$ se tiene $|f(x)| \leq |f(y)| + \int_I |f'|$, simplemente por la regla de Barrow. Al tomar y de modo que $|f|$ alcance un mínimo, se sigue

$$|f(x)| \leq \frac{1}{|I|} \int_I |f| + \int_I |f'|$$

que puede considerarse como una desigualdad de Sobolev.

Identificando \mathbb{T} con el intervalo $[0, 1)$ y subdividiéndolo en intervalos semiabiertos I_k de longitud $\delta/2$, en cada uno de ellos a lo más hay un x_ν . Ahora elegimos $f = g^2$ con $g(x) = \sum_{n=1}^N a_n e(nx)$ en la desigualdad anterior para $I = I_k$ y sumamos en k .

$$\sum_{\nu} \left| \sum_{n=1}^N a_n e(nx_\nu) \right|^2 \ll \sum_k \left(\delta^{-1} \int_{I_k} |g|^2 + \int_{I_k} |gg'| \right) = \delta^{-1} \int_0^1 |g|^2 + \int_0^1 |gg'|.$$

La desigualdad de Cauchy-Schwarz implica

$$\sum_{\nu} \left| \sum_{n=1}^N a_n e(nx_\nu) \right|^2 \ll \delta^{-1} \int_0^1 |g|^2 + \left(\int_0^1 |g'|^2 \right)^{1/2} \left(\int_0^1 |g|^2 \right)^{1/2}$$

y la identidad de Parseval concluye la prueba. \square

Una forma de obtener $C = 1$ es por medio de una variante de la *desigualdad de Hilbert* obtenida por H.L. Montgomery y R.C Vaughan [MV74]. Otra forma, desarrollada por A. Selberg, se basa en cierta manera en encontrar la mejor mayorante de una función característica que sea una función entera con ciertas propiedades (véase [Mon78] y [Mur08]).

En su forma original la desigualdad de Hilbert establece

$$\left| \sum_{n \neq m} \sum \frac{a_n \bar{a}_m}{n - m} \right| \leq \pi \quad \text{cuando} \quad \sum |a_n|^2 = 1.$$

Aunque la prueba es elemental, es bastante ingeniosa. Una aplicación (no directa) debida a M. Riesz es la acotación del operador conjugado en el disco. Dada una función holomorfa en el disco unidad, si el valor en el borde de su parte real está en $L^p(\mathbb{T})$ para cierto $1 < p < \infty$, entonces el de su parte imaginaria también. La variante de Montgomery y Vaughan es:

Lema 2.3.7. *Si $x_1, x_2, \dots \in \mathbb{T}$ están δ -espaciados, se cumple*

$$\left| \sum_{\nu \neq \mu} \sum \frac{c_\nu \bar{c}_\mu}{\sin(\pi(x_\nu - x_\mu))} \right| \leq \delta^{-1} \quad \text{cuando} \quad \sum |c_\nu|^2 = 1.$$

Para la prueba, véase [MV74] o [IK04].

Demostración de la Proposición 2.3.6 con $C = 1$. Consideremos un vector cuya coordenada ν es $\sum_n \bar{a}_n e(-nx_\nu)$. Sea b_ν el valor de esta coordenada cuando se normaliza el vector, entonces

$$\sum_{\nu} \left| \sum_{n=1}^N a_n e(nx_\nu) \right|^2 = \left(\sum_{\nu} b_\nu \sum_{n=1}^N a_n e(nx_\nu) \right)^2 \leq \sum_{n=1}^N |a_n|^2 \cdot \sum_{n=1}^N \left| \sum_{\nu} b_\nu e(nx_\nu) \right|^2.$$

Desarrollando el cuadrado lo que resta probar es

$$\sum_{\nu \neq \mu} \sum_{n=1}^N b_\nu \bar{b}_\mu e(n(x_\nu - x_\mu)) \leq \delta^{-1}.$$

Para ello utilizamos la identidad

$$\sum_{n=1}^N e(n(x_\nu - x_\mu)) = \frac{e((N+1/2)x_\nu) e(-(N+1/2)x_\mu)}{2i \sin(\pi(x_\nu - x_\mu))} - \frac{e(x_\nu/2) e(-x_\mu/2)}{2i \sin(\pi(x_\nu - x_\mu))}.$$

Por el Lema 2.3.7 con $c_\nu = b_\nu e((N+1/2)x_\nu)$, la primera fracción contribuye a la suma triple con una cantidad acotada en módulo por $(2\delta)^{-1}$ y lo mismo ocurre con la segunda fracción tomando $c_\nu = b_\nu e(x_\nu/2)$. \square

Ahora ya estamos preparados para enunciar la versión combinatoria de la gran criba. Recordamos de la teoría de números elemental que se dice que un entero positivo es *libre de cuadrados* si no es divisible por ningún cuadrado perfecto mayor que 1. La función característica de los números libres de cuadrados es $\mu^2(n)$ donde μ es la *función de Möbius* definida como

$$\mu(n) = \begin{cases} (-1)^k & \text{si } n = p_1 p_2 \cdots p_k \text{ con } p_j \text{ primos distintos} \\ 1 & \text{si } n = 1 \\ 0 & \text{en otro caso} \end{cases}$$

Si no se usa la desigualdad criba con $C = 1$, entonces la conclusión en el siguiente resultado se mantiene reemplazando \leq por \ll .

Teorema 2.3.8 (La gran criba como método de criba). *Sea \mathcal{Z} un conjunto de enteros $\mathcal{Z} \subset [M + 1, M + N]$, $N, M \in \mathbb{Z}^+$. Supongamos que para cada primo $p \leq Q$, hay $\omega(p)$ clases módulo p que no aparecen en \mathcal{Z} , entonces*

$$|\mathcal{Z}| \leq \frac{N + Q^2}{\sum_{q \leq Q} h(q)} \quad \text{con} \quad h(q) = \mu^2(q) \prod_{p|q} \frac{\omega(p)}{p - \omega(p)}.$$

Demostración. Lo que vamos a probar es

$$(2.30) \quad h(q)|\mathcal{Z}|^2 \leq \sum_{\substack{a=1 \\ (a,q)=1}}^q \left| \sum_{n \in \mathcal{Z}} e\left(\frac{an}{q}\right) \right|^2 \quad \text{para } q \leq Q \text{ libre de cuadrados.}$$

Veamos que esto es suficiente para conseguir nuestro objetivo. Sea $a_n = 1$ si $n + M \in \mathcal{Z}$ y $a_n = 0$ en otro caso, entonces

$$\sum_{q \leq Q} \sum_{\substack{a=1 \\ (a,q)=1}}^q \left| \sum_{n \in \mathcal{Z}} e\left(\frac{an}{q}\right) \right|^2 = \sum_{\nu} \left| \sum_{n=1}^N a_n e((n + M)x_{\nu}) \right|^2 = \sum_{\nu} \left| \sum_{n=1}^N a_n e(nx_{\nu}) \right|^2$$

donde x_{ν} recorre las fracciones irreducibles $0 < a/q < 1$, y estas fracciones están claramente Q^{-2} -espaciadas. Entonces el resultado se sigue de la Proposición 2.3.6 sumando en (2.30).

Ahora deduciremos (2.30) por inducción en el número de factores primos de q . Si $q = 1$, es decir, si no tiene factores primos, el resultado es trivial (interpretando $h(1) = 1$ por el producto vacío). Supongamos ahora que el resultado es cierto para un libre de cuadrados $q \leq Q$ y vamos a deducirlo para qp con $p \nmid q$ un primo $p \leq Q$.

Según las hipótesis, sólo se obtienen $p - \omega(p)$ clases al reducir módulo p los elementos de \mathcal{Z} , sean $b_1, b_2, \dots, b_{p-\omega(p)}$ representantes de estas clases. Por la desigualdad de Cauchy-Schwarz

$$\left| \sum_{n \in \mathcal{Z}} e\left(\frac{bn}{q}\right) \right|^2 = \left| \sum_{j=1}^{p-\omega(p)} \sum_{\substack{n \in \mathcal{Z} \\ n \equiv b_j \pmod{p}}} e\left(\frac{bn}{q}\right) \right|^2 \leq (p - \omega(p)) \sum_{k=1}^p \left| \sum_{\substack{n \in \mathcal{Z} \\ n \equiv k \pmod{p}}} e\left(\frac{bn}{q}\right) \right|^2.$$

Recordando (1.28), al expandir el cuadrado el último término es

$$(p - \omega(p)) \sum_{n \in \mathcal{Z}} \sum_{m \in \mathcal{Z}} \frac{1}{p} \sum_{a=1}^p e\left(\frac{a(n-m)}{p}\right) e\left(\frac{b(n-m)}{q}\right) = \frac{p - \omega(p)}{p} \sum_{a=1}^p \left| \sum_{n \in \mathcal{Z}} e\left(\frac{an}{p}\right) e\left(\frac{bn}{q}\right) \right|^2.$$

Separando la contribución de $a = p$, despejando y sumando en b , se deduce

$$h(p) \sum_{\substack{b=1 \\ (b,q)=1}}^q \left| \sum_{n \in \mathcal{Z}} e\left(\frac{bn}{q}\right) \right|^2 \leq \sum_{\substack{a=1 \\ (a,p)=1}}^p \sum_{\substack{b=1 \\ (b,q)=1}}^q \left| \sum_{n \in \mathcal{Z}} e\left(\frac{an}{p}\right) e\left(\frac{bn}{q}\right) \right|^2 = \sum_{\substack{a=1 \\ (a,pq)=1}}^{pq} \left| \sum_{n \in \mathcal{Z}} e\left(\frac{an}{pq}\right) \right|^2$$

donde la igualdad se debe al teorema chino del resto. Por la hipótesis de inducción, esto implica

$$h(p)h(q)|\mathcal{Z}|^2 \leq \sum_{\substack{a=1 \\ (a,pq)=1}}^{pq} \left| \sum_{n \in \mathcal{Z}} e\left(\frac{an}{pq}\right) \right|^2$$

que es (2.30) para qp . □

En seguida veremos aplicaciones significativas del resultado anterior. Para apreciar su sentido, consideraremos un ejemplo trivial. Supongamos que queremos contar los enteros positivos en $[1, N]$ que no son ni múltiplos de 2 ni de 3. Un razonamiento elemental lleva a que hay $N/6 + O(1)$ de ellos. Con la notación del Teorema 2.3.8, $\omega(2) = \omega(3) = 1$ que implica $h(2) = 1$ y $h(3) = 1/2$, y $Q = 3$ da que el cardinal buscado es a lo más $2N/5 + O(1)$. Esto es más débil que la asintótica elemental pero pensemos que cuando incrementamos la cantidad de primos el argumento elemental se complica y empieza a fallar si esta cantidad depende de N . La “gran” criba es superior cuando se considera una “gran” cantidad de primos.

2.3.3. Algunas aplicaciones aritméticas

Comencemos con un problema con sabor geométrico consistente en contar los puntos de coordenadas enteras bajo la gráfica de una función no negativa. Concretamente, queremos aproximar

$$\mathcal{N}_f(A, B) = \{(n, m) \in \mathbb{Z}^2 : A \leq n \leq B, 0 \leq m \leq f(n)\}.$$

Este problema tiene raíces muy antiguas que llegan hasta Gauss y Dirichlet pero desde el punto de vista moderno, están ligados a I.M. Vinogradov que es probablemente el matemático que más ha contribuido a la estimación de sumas trigonométricas.

No se pierde generalidad suponiendo $A, B \in \mathbb{Z}$. Es fácil intuir que la integral es una buena aproximación, con alguna modificación para tener en cuenta los bordes rectos. Por supuesto, se necesita alguna condición sobre f porque en otro caso los resultados pueden ser muy variados. Por ejemplo, si f es constante $\mathcal{N}_f(A, B)$ da saltos de $B - A + 1$ según esa constante es algo menor o algo mayor que un entero positivo. Algo crucial para evitar esta situación es que la gráfica de f tenga cierta curvatura. Nosotros aquí tendremos en mente el caso de una familia de gráficas que se va expandiendo por una homotecia de razón λ , es decir, $f(x) = \lambda g(x/\lambda)$. Si g tiene una curvatura acotada, esto implica que f'' es comparable a λ^{-1} . Como los extremos del intervalo, A y B , se dilatan de la misma manera la condición natural con este ejemplo en mente es que f'' sea comparable a $(B - A)^{-1}$.

Teorema 2.3.9. *Sea $f \in C^2([A, B])$ no negativa con $A < B$ enteros. Supongamos que $1 \ll (B - A)f'' \ll 1$, entonces*

$$\mathcal{N}_f(A, B) = \int_A^B f(x) dx + \frac{1}{2}(B - A + f(A) + f(B)) + O((B - A)^{2/3}).$$

Demostración. Partimos de la identidad

$$\mathcal{N}_f(A, B) = \frac{1}{2}(B - A + 1) + \sum_{n=A}^B f(n) - \sum_{n=A}^B \{f(n)\} \quad \text{donde } \{x\} = x - [x] - \frac{1}{2}.$$

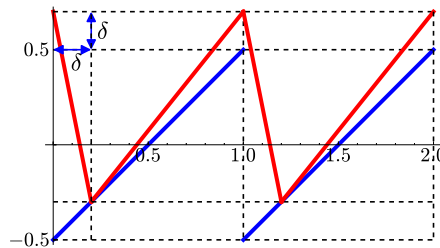
Por la fórmula de sumación de Euler-Maclaurin, Proposición 1.2.8, con $K = 2$, aplicada a la primera suma, se deduce

$$\mathcal{N}_f(A, B) = \int_A^B f(x) dx + \frac{1}{2}(B - A + f(A) + f(B)) - \sum_{n=A}^B \{f(n)\} + O(1).$$

Entonces todo lo que hay que ver es que la suma restante es $O((B - A)^{2/3})$. Sustituyendo $\{x\}$ por su serie de Fourier, se obtiene una suma trigonométrica pero la convergencia es un problema y es conveniente regularizar antes de aplicar ningún método.

Sea ϕ la función 1-periódica que conecta con segmentos $(0, 1/2 + \delta)$, $(\delta, -1/2 + \delta)$ y $(1, 1/2 + \delta)$ para cierto $0 < \delta \leq 1/2$.

$$\phi(x) = \begin{cases} -\frac{x}{\delta} + \frac{1}{2} + \delta & \text{si } 0 \leq x \leq \delta \\ \frac{x-1}{1-\delta} + \frac{1}{2} + \delta & \text{si } \delta \leq x \leq 1 \end{cases}$$



La fórmula para ϕ en realidad no es importante, lo único que emplearemos es que $\int_0^1 \phi = \delta$ y que ϕ' es $-\delta^{-1}$ para $0 < x < \delta$ y $(1 - \delta)^{-1}$ para $\delta < x < 1 - \delta$, lo cual se deduce del dibujo. Con ello, integrando por partes, se tiene que los coeficientes de Fourier son

$$a_0 = \delta \quad \text{y} \quad a_n = \frac{1}{2\pi i n} \int_0^1 \phi'(x) e(-nx) dx = \frac{1 - e(-n\delta)}{4\pi^2 n^2 \delta (1 - \delta)} \quad \text{si } n \neq 0.$$

Está claro que $-\phi(-x) \leq \{x\} \leq \phi(x)$, por tanto para cierta elección del signo \pm independiente de las variables de sumación,

$$\sum_{n=A}^B \{f(n)\} \ll (B - A)\delta + \left| \sum_{m \neq 0} \frac{1 - e(-m\delta)}{m^2 \delta} \sum_{n=A}^B e(\pm m f(n)) \right|.$$

Por el Teorema 2.3.3 con $\lambda = m(B - A)^{-1}$, se tiene

$$\sum_{n=A}^B \{f(n)\} \ll (B - A)\delta + (B - A)^{1/2} \delta^{-1} \sum_{m=1}^{\infty} \frac{|1 - e(-m\delta)|}{m^{3/2}}.$$

Si empleamos $|1 - e(-m\delta)| \ll m\delta$ para $\delta|m| < 1$ (Taylor) y $|1 - e(-m\delta)| \leq 2$ en el resto, deducimos que la suma es $O(\delta^{1/2})$. Escogiendo $\delta = \frac{1}{2}(B - A)^{-1/3}$ se termina la prueba. \square

En teoría de números es muy común estimar sumas o promedios de funciones aritméticas. Si nos fijamos en $r_2(n)$, el número de representaciones como suma de dos cuadrados, entonces la suma se relaciona con el número de puntos de coordenadas enteras en un círculo.

$$\sum_{n \leq R^2} r_2(n) = \mathcal{N}(R) \quad \text{con} \quad \mathcal{N}(R) = \#\{(n, m) \in \mathbb{Z}^2 : n^2 + m^2 \leq R^2\}.$$

Razonando geoméricamente, es fácil ver que $\mathcal{N}(R)$ es como el área del círculo salvo un error $O(R)$. Con el Teorema 2.3.9, considerando la parte del círculo en $[0, R/\sqrt{2}] \times \mathbb{R}^+$ y usando las simetrías, se refina este resultado hasta

$$(2.31) \quad \mathcal{N}(R) = \pi R^2 + O(R^{2/3}).$$

Un antiguo problema llamado el *problema del círculo de Gauss* consiste en determinar el exponente óptimo en el término de error. La conjetura (*conjetura de Hardy*) es que $2/3$ se puede sustituir por cualquier $\sigma > 1/2$ y se conoce que el exponente $1/2$ no es válido.

Utilizando métodos más precisos que los empleados en el Teorema 2.3.9 vamos a mejorar (2.31).

Teorema 2.3.10. *Sea $\mathcal{N}(R)$ el número de puntos de \mathbb{Z}^2 en el interior de un círculo de radio R , entonces*

$$\mathcal{N}(R) = \pi R^2 + O(R^{27/41}).$$

Nótese que pasar de $2/3$ a $27/41$, cuantitativamente es una mejora de menos del 2%. El menor exponente conocido hasta la fecha supone una mejora de menos del 6% sobre $2/3$, lo cual es descorazonador, habida cuenta que entre ambos resultados han pasado prácticamente 100 años de estudio de sumas trigonométricas.

Los cálculos hechos para la difracción de Fraunhofer de una abertura circular prueban que si χ_R es la función característica de un círculo de radio R se tiene

$$(2.32) \quad \widehat{\chi}_R(n, m) = R \frac{J_1(2\pi R \sqrt{n^2 + m^2})}{\sqrt{n^2 + m^2}} \quad \text{para } n^2 + m^2 \neq 0.$$

Si aplicamos “a ciegas” la versión en dos variables de la fórmula de sumación de Poisson (Teorema 1.2.4) entonces obtenemos la *serie de Hardy*

$$(2.33) \quad \mathcal{N}(R) = \pi R^2 + R \sum_{n^2 + m^2 \neq 0} \frac{J_1(2\pi R \sqrt{n^2 + m^2})}{\sqrt{n^2 + m^2}},$$

la cual fue establecida por Hardy para $R > 0$ no entero, entendiendo la suma como límite sobre $n^2 + m^2 \leq M$.

La idea para demostrar el teorema anterior es sustituir J_1 por su fórmula asintótica (2.20) y utilizar el Teorema 2.3.5 con $k = 5$ para estimar la suma en n o en m . El problema para seguir esta idea es que (2.33) no converge absolutamente, de hecho la prueba de esta igualdad es bastante complicada y la lenta convergencia hace que sea poco útil. El problema proviene de que $\widehat{\chi}_R$ decae demasiado despacio y la solución pasa por regularizarla, así el esquema funciona como se ha explicado si se cambia (2.33) por la fórmula del Lema 2.3.13, que es más fea pero converge absolutamente. Antes de enunciar este resultado, separamos la estimación de la suma trigonométrica fundamental y un cálculo explícito de una transformada de Fourier que nos servirá para regularizar.

Lema 2.3.11. *Supongamos $N \leq a < b \leq 2N$ y $R^{-1/2} N^{33/16} \leq m \leq a$, entonces*

$$\sum_{a \leq n \leq b} e(R\sqrt{n^2 + m^2}) \ll m^{1/15} R^{1/30} N^{4/5}.$$

Demostración. Un cálculo prueba que la derivada quinta de $f(n) = R\sqrt{n^2 + m^2}$ satisface $\lambda \ll f^{(5)} \ll \lambda$ donde $\lambda = Rm^2 N^{-6}$. El Teorema 2.3.5 con $k = 5$ implica en esta situación

$$\sum_{a \leq n \leq b} e(R\sqrt{n^2 + m^2}) \ll m^{1/15} R^{1/30} N^{4/5} + m^{-1/15} R^{-1/30} N^{43/40}$$

y la condición $m \geq R^{-1/2} N^{33/16}$ asegura que el segundo sumando es superfluo. \square

Lema 2.3.12. Para $\delta > 0$ sea la función $f : \mathbb{R}^2 \rightarrow \mathbb{R}$ definida por $\frac{3}{2\pi}\delta^{-3}(\delta^2 - x^2 - y^2)^{1/2}$ si $x^2 + y^2 \leq \delta^2$ y 0 en el resto, y sea $F(t) = 3t^{-3}(\sin t - t \cos t)$ para $t > 0$. Entonces

$$\int_{-\infty}^{\infty} \int_{-\infty}^{\infty} f(x, y)e(-x\xi - y\eta) dx dy = F(2\pi\delta\sqrt{\xi^2 + \eta^2}).$$

En particular, la integral de f es $\lim_{t \rightarrow 0^+} F(t) = 1$.

Demostración. Como ya se vio en el caso de J_1 , geoméricamente parece claro que la integral debe ser una función radial de (ξ, η) . Se deja al lector curioso el interesante (y nada inmediato) ejercicio de probarlo analíticamente. Teniendo esto en cuenta, hay que demostrar

$$\int_{-\infty}^{\infty} \int_{-\infty}^{\infty} f(x, y)e(-x\delta^{-1}R) dx dy = F(2\pi R) \quad \text{para } R > 0.$$

Con el cambio $(x, y) \mapsto (\delta x, \delta y)$, la integral es

$$\frac{3}{2\pi} \int_{-1}^1 e(-Rx) \int_{-\sqrt{1-x^2}}^{\sqrt{1-x^2}} \sqrt{1-x^2-y^2} dy dx = \frac{3}{2\pi} \int_{-1}^1 e(-Rx) \frac{\pi}{2}(1-x^2) dx,$$

donde se ha empleado la integral que da el área del semicírculo. La igualdad se sigue ahora integrando por partes dos veces de la manera habitual. \square

Ahora vamos por fin con la versión regularizada de (2.33). Bajo la filosofía del principio de incertidumbre, consideramos una serie que imita a (2.33) para frecuencias menores que δ^{-1} pagando el precio de ver borroso en una corona de anchura δ del círculo de radio R . Su área es la que crea el término de error $O(R\delta)$. Cuando menor sea δ , menor será este error pero la serie tendrá más términos significativos.

Lema 2.3.13. Dado $R > 2$, para cualquier $R^{-1/2} < \delta < 1$ existe $r \in [R - 2\delta, R + 2\delta]$ tal que

$$\mathcal{N}(R) = \pi R^2 + \frac{r^{1/2}}{\pi} \sum_{n^2+m^2 \neq 0} \frac{\text{sen}(2\pi r\sqrt{n^2+m^2} - \pi/4)}{(n^2+m^2)^{3/4}} F(2\pi\delta\sqrt{n^2+m^2}) + O(R\delta).$$

Demostración. Como f en el Lema 2.3.12 tiene soporte en el círculo centrado de diámetro 2δ y su integral es 1, se cumple $\chi_{R-2\delta} * f \leq \chi_R \leq \chi_{R+2\delta} * f$, donde se ha usado la notación de (2.32) para la función característica del círculo y el asterisco significa la convolución en \mathbb{R}^2 (como en \mathbb{R} pero en ambas variables). Por la continuidad de $\chi_{R\pm 2\delta} * f$, el teorema de los valores intermedios asegura

$$\mathcal{N}(R) = \sum_{n,m \in \mathbb{Z}} \chi_R(n, m) = \sum_{n,m \in \mathbb{Z}} (\chi_r * f)(n, m) \quad \text{para algún } r \in [R - 2\delta, R + 2\delta].$$

Usando la fórmula de sumación de Poisson (Teorema 1.2.4) y la propiedad de la convolución (1.12) en sus versiones bidimensionales,

$$\mathcal{N}(R) = \sum_{n,m \in \mathbb{Z}} \widehat{\chi}_r(n,m) \widehat{f}(n,m) = \pi R^2 + O(R\delta) + \sum_{n^2+m^2 \neq 0} \widehat{\chi}_r(n,m) F(2\pi\delta\sqrt{n^2+m^2}).$$

Ahora basta recordar (2.32) y (2.20). El término de error es absorbido por $O(R\delta)$. \square

Demostración del Teorema 2.3.10. Vamos a elegir $\delta = R^{-14/41}$ en el Lema 2.3.13, con ello lo que buscamos es

$$\sum_{n^2+m^2 \neq 0} \frac{e(2\pi r\sqrt{n^2+m^2})}{(n^2+m^2)^{3/4}} F(2\pi\delta\sqrt{n^2+m^2}) \ll R^{13/82}.$$

Por la simetría, podemos restringir la suma a $0 < n < m$, ya que $m = 0$ o $n = m$ claramente sólo contribuyen $O(1)$. Sea $\mathfrak{N} = \{2^j m : j \geq 0\}$, entonces lo que hay que probar es

$$(2.34) \quad \sum_{m=1}^{\infty} \sum_{N \in \mathfrak{N}} S_N \ll R^{13/82} \quad \text{con} \quad S_N = \sum_{N < n \leq 2N} \frac{e(2\pi r\sqrt{n^2+m^2})}{(n^2+m^2)^{3/4}} F(2\pi\delta\sqrt{n^2+m^2}).$$

Se deja como ejercicio comprobar que podemos restringir la suma a los N que satisfacen $m < R^{-1/2} N^{33/16}$, ya que para el resto la estimación trivial es suficiente.

La función $F(t)/t^{3/2}$ es decreciente para $0 < t < 4$, de donde para $N \leq \delta^{-1}/6$ se puede sumar por partes con el Lema 1.2.1 y después aplicar el Lema 2.3.11 obteniendo, para algún $N' \leq 2N$,

$$S_N \ll N^{-3/2} \sum_{N < n \leq N'} e(2\pi r\sqrt{n^2+m^2}) \ll m^{1/15} R^{1/30} N^{-7/10}.$$

Si $N > \delta^{-1}/6$, escribiendo $\sin t = (e^{it} - e^{-it})/2i$ y $\cos t = (e^{it} + e^{-it})/2$ en $F(t)$, podemos agrupar estas funciones oscilatorias con la exponencial compleja en S_N reemplazando r por $r' = r \pm \delta$. Entonces, notando $F(t) \ll t^{-2}$, la sumación por partes da en este caso

$$S_N \ll N^{-3/2} (\delta N)^{-2} \sum_{N < n \leq N'} e(2\pi r'\sqrt{n^2+m^2}) \ll m^{1/15} R^{1/30} N^{-27/10} \delta^{-2}.$$

Al sumar sobre la progresión geométrica $N \in \mathfrak{N}$, el resultado será comparable al primer término en cada caso, por tanto la contribución de toda la suma en (2.34) es

$$\sum_{m \ll \delta^{-1}} m^{1/15} R^{1/30} m^{-7/10} + \sum_{m \gg \delta^{-1}} m^{1/15} R^{1/30} m^{-27/10} \delta^{-2} \ll R^{1/30} \delta^{-11/30},$$

lo cual prueba (2.34) para el valor escogido de δ . \square

Pasemos ahora a ver algunas aplicaciones de la gran criba. Comenzamos estimando la cantidad de primos en un intervalo.

Teorema 2.3.14. *Sea $\pi(N)$ el cardinal de los primos menores o iguales que N . Para todo $N, M \in \mathbb{Z}^+$ se cumple*

$$\pi(M + N) - \pi(M) \leq (2 + o(1)) \frac{N}{\log N}$$

donde $o(1)$ tiende a cero cuando $N \rightarrow \infty$.

El teorema de los números primos afirma que en el caso $M = O(1)$ se puede cambiar la igualdad con la constante 1 en lugar de 2. M.N. Huxley probó que esta igualdad también es correcta si $M = O(N^\sigma)$ para algún $\sigma < 12/7$.

Corolario 2.3.15. *Se tiene $\pi(N) = O(N/\log N)$.*

Demostración. Consideremos

$$\mathcal{Z} = \{M \leq n \leq M + N : n \not\equiv 0 \pmod{p} \quad \forall p \leq Q\}.$$

Es obvio que \mathcal{Z} contiene todos los primos que son mayores que Q , mientras que hay menos de Q que son menores que Q , por tanto

$$\pi(M + N) - \pi(M) \leq Z + Q.$$

Como se excluye una clase por cada primo, $h(p) = 1/(p-1) = p^{-1} + p^{-2} + p^{-3} + \dots$, con la notación del Teorema 2.3.8. Por tanto, para q libre de cuadrados, $h(q)$ es la suma de los inversos de todos los números con los mismos factores primos que q . Así pues

$$\sum_{q \leq Q} h(q) \geq \sum_{q \leq Q} \frac{1}{q} = \log Q + O(1).$$

Elegiendo por ejemplo $Q = \sqrt{N}/\log N$ en el Teorema 2.3.8 se obtiene el resultado. \square

Siguiendo esta idea de primos en intervalos, una conjetura muy antigua es si hay infinitos *primos gemelos*, esto es, primos cuya diferencia es 2. La gran criba permite dar una cota que es del orden de magnitud esperado y obtener lo que se llama el *teorema de Brun* que afirma que la serie de los inversos de los primos gemelos converge. V. Brun fue el pionero de los métodos de criba y su prueba es muy anterior a la introducción de la gran criba.

Teorema 2.3.16. Sea \mathcal{G} el conjunto de los $n \in \mathbb{Z}^+$ tales que n y $n + 2$ son primos (gemelos) y sea $\pi_2(N)$ el cardinal de $\mathcal{G} \cap [1, N]$. Existen dos constantes positivas C_1 y C_2 tales que

$$\pi_2(N) \leq C_1 \frac{N}{(\log N)^2} \quad y \quad \sum_{p \in \mathcal{G}} \frac{1}{p} = C_2.$$

En la demostración apelaremos al siguiente lema. Con técnicas bien conocidas de teoría analítica de números [IK04, §1] se deduce una fórmula asintótica.

Lema 2.3.17. Sea $d(n)$ la función que cuenta el número de divisores (positivos) de n , entonces

$$\sum_{n \leq N} \mu^2(n) d(n) \gg N \log N.$$

Demostración. Vamos a emplear que

$$(2.35) \quad \sum_{n \leq N} \mu^2(n) d(n) \geq \sum_{n \leq N} d(n) - \sum_{p \leq \sqrt{N}} \sum_{n \leq N/p^2} d(p^2 n).$$

Se tiene

$$\sum_{n \leq N} d(n) = \sum_{kl \leq N} 1 = \sum_{k \leq N} \left(\frac{N}{k} + O(1) \right) = N \log N + O(N).$$

Un razonamiento similar sirve para tratar $\sum_{n \leq N/p^2} d(p^2 n)$ imponiendo que k o l sean divisibles por p^2 o cada una de ellas por p . En los casos $p = 2, 3$ se obtiene

$$\sum_{n \leq N/4} d(n) = \frac{1}{2} N \log N + O(N). \quad y \quad \sum_{n \leq N/4} d(n) = \frac{2}{9} N \log N + O(N).$$

Para el resto de los primos usaremos simplemente que $d(p^2 n) \leq 3d(n)$, porque cada divisor de $p^2 n$ dividido por 1, p o p^2 da un divisor de n . Entonces, deducimos a partir de (2.35)

$$\sum_{n \leq N} \mu^2(n) d(n) \geq \left(1 - \frac{1}{2} - \frac{2}{9} - 3 \sum_{p \geq 5} p^{-2} \right) N \log N + O(N).$$

Todo lo que resta comprobar es que $\sum_{p \geq 5} p^{-2} \leq 5/54 = 0.09259\dots$. Para ello usamos que $p^{-2} \leq \log(1 + p^{-2}) + \frac{1}{2} p^{-4}$ y por tanto

$$\sum_{p \geq 5} p^{-2} \leq \log \prod_{p \geq 5} \frac{1 - p^{-4}}{1 - p^{-2}} + \frac{1}{2} \sum_{n \geq 5} n^{-4} = \log \frac{\zeta(2)}{\zeta(4)} - \log \frac{5}{4} - \log \frac{10}{9} + \frac{1}{2} \left(\zeta(4) - \sum_{n=1}^4 n^{-4} \right),$$

donde se ha empleado la fórmula producto de Euler (1.33). Con (1.19) podemos evaluar $\zeta(2)$ y $\zeta(4)$ y comprobar que la última expresión es algo menor que 0.092. \square

Demostración del Teorema 2.3.16. Sea

$$\mathcal{Z} = \{n \in [1, N] : n \not\equiv 0, -2 \pmod{p} \quad \forall p \leq \sqrt{N}\}.$$

Entonces, con la notación del Teorema 2.3.8, $h(2) = 1/2$ y para cada $2 < p \leq \sqrt{N}$ se tiene $h(p) = 2/(p-2)$. Entonces para $q \leq \sqrt{N}$

$$h(q) \geq \frac{1}{2} \mu^2(q) \prod_{p|q} \frac{2}{p} = \frac{\mu^2(q)d(q)}{2q}.$$

Sumando por partes en el Lema 2.3.17, se tiene

$$\sum_{q \leq \sqrt{N}} h(q) \gg (\log N)^2.$$

Evidentemente $\pi_2(N) \leq Z + \sqrt{N}$ y el Teorema 2.3.8 con $Q = [\sqrt{N}]$ prueba la primera parte del enunciado.

La segunda parte se deduce de la primera mediante sumación por partes. Concretamente, escogiendo en el Lema 1.2.2 $g(n) = 1/n$ y $c_n = 1$ si $n \in \mathcal{G}$ y $c_n = 0$ en otro caso. De esta forma $C(N) = \pi_2(N)$. \square

