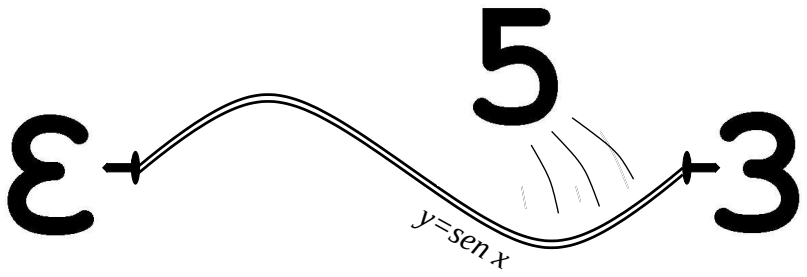
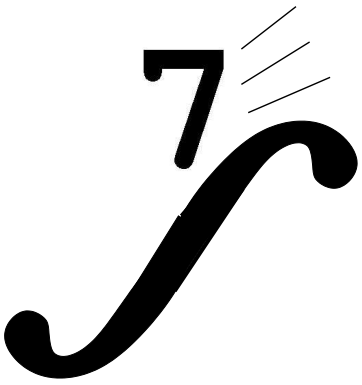
Métodos Analíticos en Teoría de Números





Lorenzo Fernando Tenenblat Colozimah

2002

En estas notas mostraremos algunas de las pinceladas que conforman la teoría analítica de números. Veremos en particular, la teoría multiplicativa que rodea a la demostración del teorema de los números primos, y la estimación de sumas trigonométricas. Además, completaremos los dos últimos capítulos con aplicaciones a diversos problemas aritméticos.

Índice

0. Notación y preliminares

0.1. Hablando del infinito

En la extraña y fructífera alianza que haremos con el Análisis, buscaremos auxilio en sus métodos y también en una partecita de su notación, que comenzamos recordando aquí.

Se indicará mediante $f \sim g$ que las funciones f y g son asintóticamente iguales. Es decir,

$$\lim_{x\to\infty} \frac{f(x)}{g(x)} = 1$$

donde la mayoría de las veces se sobreentenderá que ∞ es en realidad $+\infty$.

Ejemplo. $x^3 - 1 \sim x^3 + x^2 + \cos x$, $\int_2^x \frac{dt}{\log t} \sim x/\log x$ (L'Hopital), $\int_{-\infty}^x e^{-t^2} dt \sim \sqrt{\pi}$.

De acuerdo con la notación "O" de Landau, $f = O(g)$ y $f = o(g)$ significan respectivamente

$$\limsup_{x\to\infty} \left|\frac{f(x)}{g(x)}\right| < \infty \qquad \text{y} \qquad \lim_{x\to\infty} \frac{f(x)}{g(x)} = 0.$$

Como antes, ∞ querrá decir típicamente $+\infty$. Si se indica explícitamente, se puede reemplazar $x \to \infty$ por $x \to a$.

Ejemplo. $\log x = O(x^{0'001})$, $\log x = o(x^{0'001})$, $2\,\mathrm{sen}\, x = O(1)$, $e^x \,\mathrm{sen}\, x = O(x - \pi)$ si $x \to \pi$, $e^{-x} = o(1/x)$, $1/x = o(1)$.

Nótese que $f = O(g)$ implica que a la larga se cumple $|f| \leq C|g|$ para alguna constante C. Esta interpretación da preferencia a la notación de Vinogradov, más manejable e intuitiva, que consiste en escribir simplemente $f \ll g$ en vez de $f = O(g)$, y $f \gg g$ para indicar $g = O(f)$. Conviene de todas formas conservar la notación O porque hay una diferencia en cuanto a uso, y es que tanto $O(g)$ como $o(g)$ se pueden emplear dentro de una expresión con el significado de "cierta función f que satisface $f = O(g)$ o $f = o(g)$". En ello radica el poder de la notación "O" de Landau.

Ejemplo. $1/x \ll 1$, $\mathrm{sen}\, x \ll 2 + \cos x$, $e^x = 1 + x + O(x^2)$ si $x \to 0$, $\int_2^x \frac{dt}{\log t} = (1 + o(1))x/\log x$, $(x^2 + O(x))/(x + o(1)) = x + o(x)$, $\log x \ll x$.

0.2. Aprendiendo a sumar

En Teoría de Números una necesidad fundamental es contar. Esto se traduce a menudo en evaluar o estimar una suma. Por ello merece la pena considerar algunas maneras de calcular y transformar sumas. Casi todas ellas serán versiones discretas o continuas de la maravillosa y ubicua integración por partes.

Lema 0.1 (Sumación por partes)**.** *Se cumple la identidad*

$$\sum_{n=1}^{N} a_n b_n = a_N S_N + \sum_{n=1}^{N-1} (a_n - a_{n+1}) S_n$$

donde $S_n = \sum_{k=1}^{n} b_k$.

DEM.: Basta escribir $b_n = S_n - S_{n-1}$ y agrupar convenientemente los términos. ■

Ejemplo . Dada la serie $\mathcal{S} = \sum (\log(n+100))^{-1} 8^n/n!$, sumando por partes con $a_n = 1/\log(n+100)$ y $b_n = 8^n/n!$ y permitiendo $N \to \infty$, se tiene

$$\mathcal{S} = \sum_{n=1}^{\infty} \Big(\frac{1}{\log(n+100)} - \frac{1}{\log(n+101)} \Big) \sum_{k=1}^{N} \frac{8^k}{k!} \leq \sum_{n=1}^{\infty} \Big(\frac{1}{\log(n+100)} - \frac{1}{\log(n+101)} \Big) e^8$$

que coincide con $e^8/\log 101 = 645'9\ldots$. Para apreciar la precisión de la cota compárese con $\mathcal{S} = 636'5\ldots$.

El procedimiento del ejemplo se puede enunciar en general, lo cual ilustra el uso habitual de la sumación por partes para deshacerse de coeficientes monótonos.

Corolario 0.2. *Si* $(a_n)_{n=1}^{N}$ *es una sucesión real monótona no creciente y positiva, entonces*

$$\Big| \sum_{n=1}^{N} a_n b_n \Big| \leq a_1 \sup_{1 \leq n \leq N} |S_n|.$$

A veces es útil disponer de una variante "continua" de la sumación por partes conteniendo una integral.

Lema 0.3 (Lema de Abel)**.** *Sea* $(c_n)_{n=1}^{\infty}$ *una sucesión arbitraria de números complejos y sea* $C(t) = \sum_{n \leq t} c_n$. *Dado* $x \geq 1$, *para cualquier* $g : [1, \infty) \longrightarrow \mathbb{C}$, $g \in C^1$, *se verifica*

$$\sum_{n \leq x} c_n g(n) = C(x) g(x) - \int_1^x C(t) g'(t)\, dt.$$

DEM.: Basta aplicar sumación por partes con $N = xM$ (o su parte entera, si no es entero), $a_n = g(n/M)$ y b_n definido como $c_{n/M}$ si $M|n$ y $b_n = 0$ en otro caso. Cuando $M \to \infty$ se tiene el resultado deseado. Otra prueba, demasiado avanzada pero muy reveladora, consiste en observar que la derivada de la función escalonada $C(t)$ es $\sum c_n \delta(t-n)$ con δ la delta de Dirac. El lema de Abel se reduce entonces a integrar por partes. ■

Ejemplo . Aplicando el lema de Abel con $c_n = 1$ y $g(t) = 1/t$ se deduce

$$\sum_{n \le x} \frac{1}{n} = \frac{[x]}{x} + \int_1^x \frac{[t]}{t^2}\, dt = \log x + \frac{[x]}{x} + \int_1^x \frac{[t]-t}{t^2}\, dt$$

donde, como es habitual, $[x]$ denota la parte entera de x. Observando que $\int_1^x = \int_1^\infty - \int_x^\infty = \text{cte} + O(1/x)$, se llega al resultado clásico **[Sp]** afirmando que $\sum_{n \le x} n^{-1} = \log x + \gamma + O(1/x)$, donde $\gamma = 0'577\ldots$ es una constante llamada *constante de Euler*.

La siguiente fórmula de sumación es menos elemental pero mucho más poderosa. Recuérdese que la transformada de Fourier de f, $\widehat{f}$, se define como

$$\widehat{f}(\xi) = \int_{-\infty}^{\infty} f(x) e(-\xi x)\, dx$$

donde aquí y en lo sucesivo $e(t)$ denota la exponencial compleja $e^{2\pi i t}$.

Lema 0.4 (Fórmula de sumación de Poisson)**.** *Sea f una función de decaimiento rápido, entonces*

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

Nota: El lema admite una generalización obvia a dimensiones mayores, $f : \mathbb{R}^d \longrightarrow \mathbb{R}$, utilizando la transformada de Fourier en $\mathbb{R}^d$ y sumando en $\vec{n} \in \mathbb{Z}^d$. Además en cualquier dimensión la regularidad se puede relajar mucho por densidad.

DEM.: Sean las funciones regulares periódicas dadas por $F(x) = \sum f(x+n)$ y $G(x) = \sum \widehat{f}(n) e(nx)$. El k-ésimo coeficiente de Fourier de F es $\sum \int_0^1 f(t+n) e(-kt)\, dt = \widehat{f}(n)$ que coincide con el de G. Por tanto $F = G$, en particular $F(0) = G(0)$. ■

Ejemplo . Sea $\theta(t) = \sum_{n=-\infty}^{\infty} e^{-\pi n^2 t}$ con $t > 0$. Aplicando la fórmula de sumación de Poisson con $f(x) = e^{-\pi t x^2}$, se obtiene

$$\sum_{n=-\infty}^{\infty} e^{-\pi n^2 t} = \frac{1}{\sqrt{t}} \sum_{n=-\infty}^{\infty} e^{-\pi n^2/t}, \qquad \text{es decir } \ \theta(t) = t^{-1/2}\theta(1/t).$$

Por ejemplo, la serie $\theta(0'01) = \sum e^{-\pi n^2 0'01}$ es costosa de evaluar con precisión empleando una calculadora de bolsillo, debido a la lenta convergencia inicial. La fórmula anterior permite asegurar $\theta(0'01) \approx 10$, que es cierto con una precisión de más de 100 decimales.

La siguiente fórmula de sumación se suele enunciar introduciendo los números y polinomios de Bernoulli **[Sp]**, **[Gr-Ry]**. Con vistas a simplificar la demostración aquí consideraremos en su lugar una variante a propósito.

Sea $E_1(x) = x - 1/2$ y considérense los polinomios $E_2 = -\int E_1$, $E_3 = -\int E_2$, ... con la constante de integración ajustada para que tengan integral nula en $[0, 1]$. De aquí $E_n(0) = E_n(1)$ si $n > 1$ (de hecho estos números son nulos para $n > 1$ impar). Por ejemplo, $E_2(x) = -x^2/2 + x/2 - 1/12$ y $E_3(x) = x^3/6 - x^2/4 + x/12$.

Lema 0.5 (Fórmula de sumación de Euler-Mac Laurin)**.** *Sea $N, M \in \mathbb{Z}^+$, si $f \in C^M([1, N])$ se verifica*

$$\sum_{n=1}^{N} f(n) = \int_1^N f(t)\,dt + f(1) + \sum_{m=1}^{M} E_m(0)\big(f^{(m-1)}(1) - f^{(m-1)}(N)\big) + \int_1^N E_M(t-[t]) f^{(M)}(t)\,dt.$$

DEM.: La función $E_1(x - [x]) = x - [x] - 1/2$ tiene derivada constante 1 en cada intervalo $(n, n + 1)$, de donde es fácil deducir integrando por partes:

$$\sum_{n=1}^{N} f(n) = \int_1^N f(t)\,dt + \frac{1}{2}\big(f(1) + f(N)\big) + \int_1^N E_1(t - [t]) f'(t)\,dt,$$

que es el caso $M = 1$ ya que $E_1(0) = -1/2$.

Por otro lado, Integrando por partes (nótese que $E_{M+1}(t - [t])$ es C^1 a trozos)

$$\int_1^N E_M(t - [t]) f^{(M)}(t)\,dt = -E_{M+1}(t - [t]) f^{(M)}(t)\Big|_1^N + \int_1^N E_{M+1}(t - [t]) f^{(M+1)}(t)\,dt$$

y el caso general se sigue por inducción. ■

Ejemplo . Sea $f(x) = x^3$. Tomando $M = 4$ en la fórmula de Euler-Mac Laurin se deduce

$$\sum_{n=1}^{N} n^3 = \frac{N^4 - 1}{4} + 1 - \frac{1}{2}(1 - N^3) - \frac{1}{12}(3 - 3N^2) = \frac{N^2(N + 1)^2}{4}.$$

Fórmulas similares se pueden obtener para otras potencias.

0.3. Cosas que deberíamos saber

En lo sucesivo emplearemos algunos resultados básico sdel Análisis Real y Complejo, los cuales mencionaremos rápidamente a continuación para que nadie tenga que sonrojarse preguntándolas.

Si D es un dominio simplemente conexo con frontera regular ∂D, la *fórmula integral de Cauchy* afirma que para $a \in D$ y f holomorfa en un dominio que contiene a D se cumple

$$f^{(n)}(a) = \frac{n!}{2\pi i} \int_{\partial D} \frac{f(z)}{(z-a)^{n+1}}\, dz \qquad \text{con } n = 0, 1, 2, \ldots$$

Si f en lugar de ser holomorfa es meromorfa, en cada punto $z_k \in D$ en el que tiene una singularidad se pueden hallar $c_{1k}, c_{2k}, \ldots, c_{Nk}$ tales que $f(z) - c_{1k}/z - c_{2k}/z^2 - \ldots - c_{Nk}/z^N$ sea holomorfa en un entorno de z_k. Al coeficiente c_{1k} se le llama *residuo de f en z_k*. Repitiendo este procedimiento en todos los puntos singulares y aplicando la fórmula integral de Cauchy, se deduce el *teorema de los residuos*

$$\frac{1}{2\pi i} \int_{\partial D} f(z)\, dz = \sum_k c_{1k}.$$

Pasemos ahora al Análisis Armónico. Si $f : \mathbb{R} \longrightarrow \mathbb{C}$ es una función periódica de periodo uno, se definen sus coeficientes de Fourier y su serie de Fourier como

$$a_n = \int_0^1 f(t) e(-nt)\, dt \qquad \text{y} \qquad \sum_{n=-\infty}^{\infty} a_n e(nx).$$

Para $f \in L^2([0,1])$ la serie de Fourier converge a f en sentido L^2 (y si es suficientemente regular, en sentido usual). Igualando la norma dos de f y de su serie de Fourier se llega a la *identidad de Plancherel*:

$$\int_0^1 |f|^2 = \sum_{n=-\infty}^{\infty} |a_n|^2$$

que por polarización lleva a la *identidad de Parseval*:

$$\int_0^1 \overline{f} g = \sum_{n=-\infty}^{\infty} \overline{a_n} b_n$$

donde a_n y b_n son los coeficientes de Fourier de f y g respectivamente (ambas en L^2).

El análogo en el caso no periódico de los coeficientes de Fourier es la transformada de Fourier, ya introducida anteriormente:

$$\widehat{f}(\xi) = \int_{-\infty}^{\infty} f(t)e(-\xi t)\,dt.$$

Si se entiende la integral de forma adecuada se puede dar sentido a la definición para toda $f \in L^2(\mathbb{R})$ y se tiene el análogo de las fórmulas anteriores:

$$\int_{-\infty}^{\infty} |f|^2 = \int_{-\infty}^{\infty} |\widehat{f}|^2 \qquad \text{y} \qquad \int_{-\infty}^{\infty} \overline{f}g = \int_{-\infty}^{\infty} \overline{\widehat{f}}\,\widehat{g}$$

Para no complicarse la vida con la regularidad uno puede restringirse a las *funciones de decaimiento rápido* (clase de Schwarz), caracterizadas por la propiedad de que ellas y sus derivadas decaen más rápido que cualquier potencia. Sus transformadas de Fourier tienen esta misma propiedad.

Como colofón, definiremos cierta función compleja clásica que generaliza al factorial y que aparecerá sobre todo en el primer capítulo.

Es fácil probar integrando por partes que

$$(n-1)! = \int_0^{\infty} t^{n-1}e^{-t}\,dt.$$

La integral del segundo miembro está bien definida si $n \in \mathbb{R}^+$ e incluso si n es un número complejo en el semiplano derecho. Con esta idea se define para $\operatorname{Re} s > 0$

$$\Gamma(s) = \int_0^{\infty} t^{s-1}e^{-t}\,dt.$$

Esta función hereda del factorial la propiedad $\Gamma(s+1) = s\Gamma(s)$. De esta forma se puede extender la definición a $-1 < \operatorname{Re} s \leq 0$ como $\Gamma(s) = s^{-1}\Gamma(s+1)$. Repitiendo este argumento Γ queda definida como una función meromorfa en $\mathbb{C}$ con polos en $s = 0, -1, -2, -3, \ldots$. Casi todas las propiedades de la función Γ se pueden deducir de la fórmula (véase **[Ci-Co]**) $1/\Gamma(s) = se^{\gamma s}\prod(1 + s/n)e^{-s/n}$ donde n recorre $\mathbb{Z}^+$ y γ es la constante de Euler. En el primer capítulo emplearemos $|\Gamma(s)/\Gamma'(s)| = O(\log|s|)$ siempre que s esté retirado de los polos de Γ.

1. El teorema de los números primos

1.1. Un poco de historia

Hay veces que por una extraña y armónica conjunción de la sencillez, la belleza y la relevancia, una fórmula simple sostiene los cimientos de una compleja teoría. Esto es lo que ocurre en el estudio de la distribución de los primos con la *identidad de Euler*

$$\boxed{\sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_{p} (1 - \frac{1}{p^s})^{-1}}$$

donde $s > 1$ y p recorre los primos. La demostración se reduce al teorema fundamental de la aritmética (descomposición única en primos) después de notar que el segundo miembro es $\prod(1 + p^{-s} + p^{-2s} + p^{-3s} + \ldots)$.

Esta sencilla fórmula es muy importante porque relaciona los números naturales, que conocemos bien, con los número primos, que conforman una sucesión muy caótica. Euler utilizó su identidad para probar la infinitud de los primos notando que el primer miembro diverge cuando $s \to 1^+$. Lo bueno de esta prueba frente a la usual, es que admite cierta cuantificación del crecimiento de los primos. Por ejemplo, si alguien afirmase que a partir de cierto número gigantesco hay siempre a lo más un número primo entre cada par de cuadrados consecutivos, podríamos ver la falsedad de tal afirmación deduciendo de la identidad de Euler

$$\sum_{n=1}^{\infty} \frac{1}{n^s} \leq \text{cte} \prod_{k=1}^{\infty} (1 - \frac{1}{k^2})^{-1}.$$

Lo cual lleva a una contradicción cuando $s \to 1^+$ porque $\prod(1 - k^{-2})^{-1} < \infty$.

Una cuestión básica en el estudio de la distribución de los primos es la densidad que tienen en los naturales. Se puede probar por métodos elementales, pero ingeniosos, que $\pi(x) = o(x)$ donde

$$\pi(x) = \sum_{p \leq x} 1 = |\{p \leq x \,:\, p \text{ es primo}\}|.$$

Así pues la densidad tiende a cero. La pregunta natural es si se puede afinar más. Gauss conjeturó (de manera un poco imprecisa, basándose en resultados numéricos) el *teorema de los números primos*, afirmando que

$$\pi(x) \sim Li(x) \qquad \text{con} \quad Li(x) = \int_2^x \frac{dt}{\log t}.$$

De los trabajos de Chebychev en 1849/50 (véase **[Sm]**) se deduce que $C_1 Li(x) < \pi(x) < C_2 Li(x)$ para ciertas constantes C_1 y C_2. Chebychev controló con precisión suficiente estas constantes (en realidad para $x/\log x$ en lugar de $Li(x)$) para probar el *postulado de Bertrand* (entre un número natural y su doble siempre hay un primo).

La gran obra maestra en la distribución de los primos es la brevísima memoria que escribió Riemann en 1860 (hay una traducción en **[Ed]**). En ella utilizó técnicas de Variable Compleja para despejar $\pi(x)$ a partir de la identidad de Euler en términos de una extensión compleja del primer miembro. Con ello obtuvo una fórmula para $\pi(x)$ cuyo primer término era $Li(x)$.

Por poco exigente que uno sea con el rigor, no se puede decir que Riemann probase el teorema de los números primos porque en su memoria enuncia varias propiedades que no demuestra (véase **[Da]** §3), e incluso no está nada claro que en su fórmula para $\pi(x)$ el término $Li(x)$ domine sobre el resto, ni siquiera está claro que tenga sentido por algunos problemas de convergencia.

A pesar de su insuficiencia, la memoria de Riemann marcó el camino para demostrar el teorema de los números primos y fue la clave para que treinta y seis años después, en 1896, de la Vallée Poussin y Hadamard consiguieran independientemente una demostración completa. Es históricamente poco correcto decir que estas pruebas fueran consecuencia necesaria del desarrollo de la Variable Compleja. Más bien al contrario, parte de la Variable Compleja se desarrolló más rápido gracias a la búsqueda de una prueba del teorema de los números primos.

En 1949 Selberg **[Se]** y Erdős sorprendieron al colectivo matemático encontrando una demostración "elemental" (pero no sencilla) del teorema de los números primos. También hay pruebas que están más cerca del Análisis Real que del Complejo **[Dy-Mc]**, sin embargo, desde Riemann está claro que si uno quiere estudiar el error en el teorema de los números primos, $\pi(x) - Li(x)$, necesariamente debe enfrentarse a los misteriosos ceros de cierta función compleja. El resultado óptimo se obtendría resolviendo la *hipótesis de Riemann*, la cual sigue sin probarse a pesar del empeño dedicado a ello durante más de 140 años.

1.2. Diversas formas del teorema de los números primos

Es fácil comprobar (por L'Hopital) que el *logaritmo integral*, $Li(x)$, satisface $Li(x) \sim x/\log x$, por lo cual el teorema de los números primos aparece en la mayoría de los textos enunciado como $\pi(x) \sim x/\log x$. Sin embargo hay razones teóricas para escribir $Li(x)$ ya que en cierto sentido da la mejor aproximación posible y se sabe positivamente que aproxima mejor que $x/\log x$. El que confíe más en los datos que en la teoría puede

observar la siguiente tabla:

	$\pi(x)/Li(x)$	$\pi(x)/(x/\log x)$
$x = 10^4$	$0'986$	$1'132$
$x = 10^6$	$0'9983$	$1'084$
$x = 10^8$	$0'99987$	$1'061$
$x = 10^{10}$	$0'9999932$	$1'048$

Es evidente que la aproximación de $\pi(x)$ por $x/\log x$ es muy pobre.

La pregunta ingenua de cuál es el n-ésimo primo p_n sugiere encontrar aproximaciones no sólo para $\pi(x)$ sino también para p_n. De todos modos, por razones técnicas el teorema de los números primos no se suele probar usando directamente $\pi(x)$ o p_n sino a través de una función bastante antinatural introducida por Chebychev y definida como

$$\psi(x) = \sum_{n \le x} \Lambda(n) \qquad \text{con} \quad \Lambda(n) = \begin{cases} \log p & \text{si } n = p^k,\ p \text{ primo } k \in \mathbb{Z}^+ \\ 0 & \text{en otro caso} \end{cases}$$

La relación entre estas funciones y las diferentes formas del teorema de los números primos están contenidas en el enunciado y la prueba del siguiente resultado:

Lema 1.1 . *Las siguiente afirmaciones son equivalentes*

a) $\pi(x) \sim Li(x)$, *b)* $\pi(x) \sim x/\log x$, *c)* $p_n \sim n \log n$, *d)* $\psi(x) \sim x$.

DEM.: Ya hemos mencionado que *a)* $\Leftrightarrow$ *b)*. Claramente $\pi(p_n) = n$, así pues *b)* implica $p_n/\log p_n \sim n$ y tomando logaritmos $\log p_n \sim n$. Multiplicando estas relaciones se obtiene *c)*. El recíproco se prueba en las mismas líneas: $p_n \le x < p_{n+1}$, *c)* $\Rightarrow p_n \sim x$.

Es fácil ver que $\pi(x) = \sum_{n \le x} \Lambda(n)/\log n + O(x^{1/2} \log x)$. De hecho con un poco de esfuerzo se puede reducir el error a $O(x^{1/2})$. Del Lema de Abel se deduce por tanto $\pi(x) = \psi(x)/\log x + \int_2^x (\psi(t) - t)/(t \log^2 t)\, dt + O(x^{1/2})$, o equivalentemente

$$\pi(x) = Li(x) + \frac{\psi(x) - x}{\log x} + \int_2^x \frac{\psi(t) - t}{t \log^2 t}\, dt + O(x^{1/2}) \tag{1.1}$$

que inmediatamente prueba *d)* $\Rightarrow$ *a)*. Si se parte de $\psi(x) = \sum_{n \le x} (\pi(n) - \pi(n-1)) \log n + O(x^{1/2} \log^2 x)$, un argumento similar prueba *b)* $\Rightarrow$ *d)*. ■

La fórmula (1.1) muestra la relevancia del logaritmo integral si partimos de buenas estimaciones de $\psi(x) - x$. Concretamente, si $\psi(x) = x + O(E(x))$ para cierta E creciente, entonces $\pi(x) = Li(x) + O(E(x)/\log x)$. Si, como probaremos, $E(x) = o(x/\log x)$ entonces

la fórmula $Li(x) - x/\log x \sim x/\log^2 x$ implica $\pi(x) - x/\log x \sim x/\log^2 x$, lo que explica la pobreza de la aproximación $x/\log x$. Este razonamiento es en cierta manera condicional, porque no está claro que $\psi(x)$ sea la función natural a considerar y $\psi(x) - x$ el error a estimar. La razón última es la estrecha relación entre $\sum n^{-s}$ y $\psi(x)$.

1.3. Un ejemplo de Cálculo I que se complica

En esta sección vamos a comenzar divagando a través de un problema aparentemente de Cálculo I, para después mostrar por analogía algunos pasos fundamentales en la demostración del teorema de los números primos. Puede que sea un mal truco explicar lo fácil por lo difícil, pero también puede que, como dijo un filósofo, el conocimiento se adquiera a través de metáforas.

Cuando miramos las tablas que reparten las academias a los alumnos de Selectividad, vemos que casi todas las series de Taylor que aparecen tienen una un aspecto sencillo. Una excepción viene dada por la función $f(x) = \tan x$ cuya serie de Taylor alrededor de $x = 0$ es

$$x + \frac{1}{3}x^3 + \frac{2}{15}x^5 + \frac{17}{315}x^7 + \frac{62}{2835}x^9 + \dots$$

Cualquiera sabe que los coeficientes impares n-ésimos, c_n, responden a la fórmula $c_n = f^{(2n-1)}(0)/(2n-1)!$ (los pares son trivialmente nulos) y, en principio, hallar los c_n es un problema de Cálculo I, ya que a fin de cuentas sólo implica derivadas en una variable. Los c_n forman una sucesión que aparentemente tiende a cero pero que por lo demás es muy caótica (no parece haber una fórmula computacionalmente sencilla para calcular cada término). Por ello vamos a rebajar el problema de Cálculo I y nos contentaremos con aproximar los c_n en vez de evaluarlos.

La gran dificultad está en que no parece fácil calcular c_n haciendo $2n-1$ derivadas una detrás de otra. Sería conveniente disponer de una fórmula mágica para despejar el coeficiente n-ésimo usando Cálculo Diferencial *menos elevado*. Dicha fórmula mágica (o una de ellas) es la fórmula integral de Cauchy que permite expresar una derivada de cualquier orden como una integral simple. Eso sí, hay que conceder el empleo de números complejos:

$$c_n = \frac{f^{(2n-1)}(0)}{(2n-1)!} = \frac{1}{2\pi i}\int_{C_R} \frac{\tan z}{z^{2n}}\, dz$$

donde $C_R = \{z : |z| = R\}$ con $R < \pi/2$ para trabajar en un dominio en el que $\tan z$ sea holomorfa. Si R es pequeño, el integrando crece en módulo y la integral es difícil de estimar porque requiere el estudio de la cancelación de grandes cantidades oscilatorias. Llevar R más allá de $\pi/2$ es ventajoso porque se reduce el tamaño del integrando. A cambio hay que pagar con los residuos de algunas singularidades. Por ejemplo, si $\pi/2 < R < 3\pi/2$, C_R encierra los polos de $\tan z$ en $z = \pm\pi/2$ con residuo 1 y se tiene

$$c_n = \frac{2}{(\pi/2)^{2n}} + \frac{1}{2\pi i}\int_{C_R} \frac{\tan z}{z^{2n}}\, dz.$$

Es fácil ver que la integral es de orden inferior al término anterior, de modo que esto prueba

$$c_n \sim 2(2/\pi)^{2n}.$$

Si queremos aproximaciones mejores todavía, podemos tomar un R mayor para hacer menor la integral y pagando con nuevos residuos. Si, por ejemplo, $3\pi/2 < R < 5\pi/2$, entonces

$$c_n = \frac{2}{(\pi/2)^{2n}} + \frac{2}{(3\pi/2)^{2n}} + \frac{1}{2\pi i}\int_{C_R} \frac{\tan z}{z^{2n}}\, dz.$$

De modo que $2(2/\pi)^{2n}(1 + 3^{-2n})$ es una aproximación todavía. En una tabla:

	$c_n/A_1(n)$	$c_n/A_2(n)$
$n = 1$	$1'2337006$	$1'1103305$
$n = 2$	$1'0146780$	$1'0023039$
$n = 3$	$1'0014471$	$1'0000752$
$n = 4$	$1'0001552$	$1'0000028$
$n = 5$	$1'0000170$	$1'0000001$

donde $A_1(n) = 2(2/\pi)^{2n}$ y $A_2(n) = 2(2/\pi)^{2n}(1 + 3^{-2n})$.

Utilizando repetidamente esta idea se puede dar una fórmula para c_n con la aproximación que deseemos, y en el límite se obtendrá una fórmula exacta si admitimos series infinitas. A saber:

$$c_n = 2(2/\pi)^{2n}(1 + 3^{-2n} + 5^{-2n} + 7^{-2n} + \ldots).$$

Repasemos los puntos principales en el ejemplo anterior:

Hemos partido de la expresión $\tan x = x + x^3/3 + 2x^5/15 + \ldots$ (válida sólo en cierto rango de valores) y queríamos despejar los coeficientes del segundo miembro que son desconocidos a diferencia del primer miembro que es una función familiar que aparece en

las calculadoras de bolsillo. Para ello hemos considerado $f(z) = \tan z$ como una función de variable compleja y hemos usado una fórmula mágica con una integral compleja para despejar los coeficientes, después hemos transformado el dominio de integración llevándolo a un lugar donde las estimaciones de la integral son sencillas, y finalmente nos hemos percatado de que en el límite podríamos tener una fórmula exacta, aunque no del todo satisfactoria desde el punto de vista computacional por la aparición de sumas infinitas.

Todas estas ideas se pueden aplicar, con muchísimas complicaciones técnicas, en la demostración del teorema de los números primos. Nuestro problema consiste ahora en despejar los primos, en realidad $\psi(x)$, del segundo miembro de la identidad de Euler. Para ello extenderemos la definición del primer miembro a una función de variable compleja, la *función ζ de Riemann*. Después aplicaremos una fórmula mágica para despejar $\psi(x)$ en términos de dicha función. La parte más delicada viene cuando queremos mover el dominio de integración al lugar donde tenemos buenas estimaciones. El problema es que hay que atravesar cierta región desconocida y sobre todo que está la hipótesis de Riemann, todavía sin probar, que nos permitiría controlar los residuos que aparecen. Hasta que alguien la demuestre, debemos dar un rodeo para evitar nuestro desconocimiento. Incluso sin la hipótesis de Riemann se pueden obtener fórmulas "explícitas" para $\pi(x)$ o $\psi(x)$ si se admiten series infinitas que involucran los residuos desconocidos. Estas fórmulas son de escaso interés computacional, pero en forma truncada y con algunas propiedades de los residuos, son suficiente como para concluir el teorema de los números primos. De alguna forma esto es como decir que en el ejemplo anterior $c_n \sim 2(2/\pi)^{2n}$ porque los términos que faltan para tener la igualdad son de orden inferior.

1.4. La extensión meromorfa y la ecuación funcional

Con el propósito de comenzar a seguir el esquema trazado anteriormente, vamos a definir una función $\zeta = \zeta(s)$, (la *función ζ de Riemann*) que es meromorfa en $\mathbb{C}$ y que coincide con el primer miembro de la identidad de Euler cuando $\operatorname{Re} s > 1$. Por las propiedades básicas de las funciones meromorfas, si tal función existe es única.

En vez de dar construcciones más directas (por ejemplo, no es difícil ver que $\zeta(s) = (1-2^{1-s})^{-1}\sum(-1)^{n+1}n^{-s}$ es la extensión meromorfa en $\operatorname{Re} s > 0$, y con el Lema de Abel se pueden dar extensiones sucesivas [**El**]), seguiremos el razonamiento original de Riemann, obteniendo por el mismo precio la extensión deseada y una relación de simetría entre $\zeta(s)$ y $\zeta(1-s)$ llamada la *ecuación funcional* por antonomasia (en [**Ti**] hay otras pruebas diferentes de la de Riemann, algunas muy breves). Tal ecuación funcional es muy interesante, porque traducirá nuestro buen conocimiento de ζ en $\operatorname{Re} s > 1$ en un conocimiento similar en $\operatorname{Re} s < 0$. A la *terra incognita* que queda entremedias, $0 \le \operatorname{Re} s \le 1$, se le llama *banda crítica*.

La ecuación funcional es tan notable que merece la pena alguna ensoñación para motivar su existencia. Podemos hacerla creíble si pensamos que desde el punto de vista de las distribuciones la transformada de Fourier de $|x|^{-s}$ es $|x|^{s-1}$ con ciertos factores **[Li]**. De modo que si creemos con fe ciega en la fórmula de sumación de Poisson se debería tener $\sum n^{-s} = \text{factores} \sum n^{-(1-s)}$. Claramente esta igualdad no puede entenderse de la forma habitual ya que el término $n = 0$ da problemas y, para el resto de los términos, si la serie de la derecha converge la de la izquierda diverge, y viceversa. Pero cabe esperar que si evitamos el problema en $n = 0$ con algún tipo de "renormalización" todo funcione reemplazando la serie que diverge por la extensión dada por la función ζ. Como curiosidad se puede mencionar que antes de ser "descubierto", Ramanujan envió a un matemático (a través de un tercero) la fórmula $1 + 2 + 3 + 4 + 5 + \ldots = -1/12$ que corresponde a lo que se obtendría con la ecuación funcional. Obviamente el matemático dijo con buen criterio que había que tener mucho cuidado con las series divergentes **[Be]**.

Riemann partió de la definición de la función Gamma en $s/2$, $\Gamma(s/2) = \int_0^\infty t^{s/2-1} e^{-t}\, dt$ para probar tras el cambio de variable $t \mapsto \pi n^2 t$ que si $\operatorname{Re} s > 1$

$$\pi^{-s/2}\Gamma(s/2)\sum_{n=1}^{\infty} n^{-s} = \sum_{n=1}^{\infty} \int_0^\infty t^{s/2-1} e^{-\pi n^2 t}\, dt$$

o equivalentemente

$$\pi^{-s/2}\Gamma(s/2)\sum_{n=1}^{\infty} n^{-s} = \frac{1}{2}\int_0^\infty t^{s/2-1}(\theta(t)-1)\, dt \qquad \text{donde} \qquad \theta(t) = \sum_{n=-\infty}^{\infty} e^{-\pi n^2 t}.$$

Lo que hemos ganado es que se puede aplicar la fórmula de Poisson en sentido clásico a $\theta(t)$ dentro de la integral. Con ello esencialmente t pasará a $1/t$ y por tanto la parte de la integral $\int_0^1$ se transformará en $\int_1^\infty$. Esto es interesante para llevar a cabo la extensión ya que la divergencia de $\int_0^1 t^{s/2-1} t^{-1/2} dt$ para $\operatorname{Re} s < 1$ es la responsable de que no podamos extender el segundo miembro. Con esta idea en mente separamos el rango de integración y utilizamos Poisson en la forma $\theta(t) = t^{-1/2}\theta(1/t)$, con ello el segundo miembro es (para $\operatorname{Re} s > 1$)

$$\frac{1}{2}\int_0^1 + \frac{1}{2}\int_1^\infty = \frac{1}{2}\int_0^1 t^{s/2-1}(t^{-1/2}\theta(1/t) - 1)\, dt + \frac{1}{2}\int_1^\infty t^{s/2-1}(\theta(t)-1)\, dt.$$

Con el cambio $t \mapsto 1/t$ en la primera integral y algunos cambios cosméticos, se llega a que para $\operatorname{Re} s > 1$

$$\pi^{-s/2}\Gamma(s/2)\zeta(s) = \frac{1}{s(s-1)} + \frac{1}{2}\int_1^\infty (t^{s/2-1} + t^{-1/2-s/2})(\theta(t)-1)\, dt \tag{1.2}$$

Ahora la integral tiene sentido para todo $s \in \mathbb{C}$ y como $\Gamma(s/2)$ no se anula, la función ζ así definida (que coincide con $\sum n^{-s}$ en $\operatorname{Re} s > 1$) es meromorfa en $\mathbb{C}$ y holomorfa en $\mathbb{C} - \{0, 1\}$. Usando que $\lim_{s\to 0} s\Gamma(s/2) = 2$ y $\Gamma(1/2) = \pi^{1/2}$, se deduce que ζ es de hecho meromorfa en $\mathbb{C}$ con un único polo en $s = 1$ de residuo 1. Además la invariancia del segundo miembro de (1.2) al cambiar s por $1 - s$ prueba la *ecuación funcional*

$$\boxed{\pi^{-s/2}\Gamma(s/2)\zeta(s) = \pi^{-(1-s)/2}\Gamma((1-s)/2)\zeta(1-s).}$$

A partir de las propiedades básicas de la función Γ se sigue que ζ tiene ceros simples en $s = -2, -4, -6, \ldots$ Estos ceros son los llamados *ceros triviales*. Sabiendo que $\sum n^{-s} \neq 0$ en $\operatorname{Re} s > 1$, es fácil deducir que si hay otros ceros deben estar en la banda crítica $0 \leq \operatorname{Re} s \leq 1$. Se pueden calcular otros valores especiales como $\zeta(-1) = -1/12$ que corresponde a la identidad no rigurosa de Ramanujan. A propósito, nótese que la fórmula obtenida para los coeficientes de Taylor de la tangente implica $\zeta(2n) = c_n\pi^{2n}/(2(2^{2n} - 1))$ para $n \in \mathbb{Z}^+$. No se conocen fórmulas similares para $\zeta(2n + 1)$.

1.5. Fórmulas mágicas y productos infinitos: el poder de la Variable Compleja

Con diversas variantes de la fórmula integral de Cauchy es posible despejar a partir de ζ y por medio de la identidad de Euler funciones como $\pi(x)$ (esto es lo que hizo Riemann) o la función característica de los primos. Sin embargo los resultados obtenidos son un poco aparatosos y técnicamente es mucho más ventajoso tratar con la función $\psi(x)$ que lleva a fórmulas más limpias.

Tomando logaritmos en la identidad de Euler y derivando, es fácil probar (utilícese $(1 - x)^{-1} = 1 + x + x^2 + \ldots$) para $\operatorname{Re} s > 1$

$$-\frac{\zeta'(s)}{\zeta(s)} = \sum_{n=1}^{\infty} \Lambda(n) n^{-s}.$$

(Nótese que la convergencia en $\operatorname{Re} s > 1$ implica, como habíamos mencionado, que $\sum n^{-s} \neq 0$ en dicha región). Si encontrásemos una fórmula mágica que aplicase n^{-s} en 1 si $n \leq x$ y en 0 si $n > x$, obtendríamos $\psi(x)$. Esta fórmula mágica vuelve a ser la fórmula integral de Cauchy pero en un caso un poco especial.

Proposición 1.2 . *Sea $c > 1$ y sea la línea vertical $L = \{\operatorname{Re} s = c\}$, entonces*

$$\frac{1}{2\pi i}\int_L \frac{t^s}{s}\, ds = \begin{cases} 0 & \text{si } 0 < t < 1 \\ 1 & \text{si } t > 1 \end{cases}$$

DEM.: El caso $0 < t < 1$ se obtiene considerando $\lim_{N\to\infty} \int_{\partial R_N} t^s s^{-1} ds$ con R_N el rectángulo $\{-N < \operatorname{Re} s < c\} \cap \{|\operatorname{Im} s| < N\}$. El otro caso es similar pero considerando el simétrico de R_N por L. ■

De modo que con L como antes, si $x > 1$ no es entero

$$\boxed{\psi(x) = \frac{1}{2\pi i} \int_L -\frac{\zeta'(s)}{\zeta(s)} \frac{x^s}{s}\, ds} \tag{1.3}$$

Una vez que tenemos la fórmula mágica nos gustaría llevar la línea de integración lo más lejos posible a la izquierda para aprovechar el decaimiento exponencial de x^s cuando $\operatorname{Re} s \to -\infty$, pero teniendo buen cuidado de esquivar los ceros triviales. El gran problema es que para ello debemos pagar con los residuos correspondientes a los ceros no triviales de ζ, los que están en $0 \le \operatorname{Re} s \le 1$, cuya localización no se conoce. De ahí surgirán casi todas las dificultades.

Para tomar resuello veamos cómo la Variable Compleja es tan poderosa que permite relacionar la función $-\zeta'/\zeta$ con los ceros de ζ. A pesar de nuestro desconocimiento de ambos objetos en la banda crítica, esperamos obtener alguna ganancia de esta relación.

Aplicaremos la teoría de funciones de orden finito de Hadamard [**Ci-Co**], quien la creó especialmente para aplicarla a ζ. Resumimos aquí los puntos principales:

Si P es un polinomio no constante, evidentemente se puede factorizar como $P(z) = A\prod(1 - z/z_n))$ donde z_n son sus raíces y $A = P(0)$. Podríamos sospechar que lo mismo ocurre con otras funciones enteras, por ejemplo que se cumple $\cos z = \prod(1 - z/z_n)$ para $z_n = n\pi + \pi/2$, los ceros de $\cos z$. Hay problemas de convergencia, pero esta fórmula es cierta si entendemos el producto infinito como límite de $\prod_{n\le N}(1 - z/z_n)$. Sin embargo algo falla en general en este esquema porque la función e^z no tiene ceros y no es constante. La teoría de Hadamard dice que todo funciona bien si nos restringimos a funciones que no crezcan demasiado, permitimos que A sea una función exponencial, y escribimos algunos factores artificiales no nulos para conseguir la convergencia absoluta. La teoría es bastante general, pero aquí sólo emplearemos un resultado específico en este sentido:

Teorema 1.3 . *Sea f una función entera no nula tal que para cada $\epsilon > 0$ verifica $|f(z)| = O\big(e^{|z|^{1+\epsilon}}\big)$. Entonces se cumple la igualdad*

$$f(z) = e^{A+Bz} \prod (1 - z/z_n) e^{z/z_n}$$

donde A y B son constantes y z_n son los ceros de f. Además $\sum |z_n|^{-1-\epsilon} < \infty$ y por tanto el producto converge absolutamente.

Es interesante reescribir el primer miembro de la ecuación funcional de una forma

bonita que dé lugar a una función entera. Exactamente se define

$$\xi(s) = \frac{1}{2}s(s-1)\pi^{-s/2}\Gamma(s/2)\zeta(s).$$

Nótese que $\xi(s) = \xi(1-s)$. De (1.2) se puede deducir que $|\xi(s)| = O\big(e^{C|s|\log|s|}\big)$ para cierta constante $C > 0$ cuando $|s| \to \infty$ (por la simetría de ξ basta considerar el caso $\operatorname{Re} s \geq 1/2$). Al aplicar el teorema anterior se tiene

$$\boxed{\xi(s) = e^{A+Bs}\prod(1-s/\rho)e^{s/\rho}}$$

donde el producto es sobre todos los ceros ρ no triviales de ζ, esto es $0 \leq \operatorname{Re} s \leq 1$. Tomando logaritmos y derivando se sigue

$$\boxed{\frac{\zeta'(s)}{\zeta(s)} = C - \frac{1}{s-1} - \frac{1}{2}\frac{\Gamma'(s/2+1)}{\Gamma(s/2+1)} + \sum_{\rho}\big(\frac{1}{s-\rho}+\frac{1}{\rho}\big)} \tag{1.4}$$

donde C es una constante que se puede evaluar exactamente **[Da]** pero que no tiene relevancia para demostrar el teorema de los números primos.

1.6. La fórmula explícita

La integral en (1.3) tiene una particularidad que puede dar lugar a muchos problemas técnicos, y es que está al borde de la no convergencia. Si vamos a llevar L a una zona donde $-\zeta/\zeta$ es muy poco conocida cabe la posibilidad de que nos tengamos que enfrentar a una integral divergente. Por ello es mejor "cortar" desde el principio la línea L dejando sólo el segmento $L_T = L \cap \{|\operatorname{Im} s| \leq T\}$. Como es natural, si T es grande la aproximación es buena. De hecho se cumple

$$\psi(x) = \frac{1}{2\pi i}\int_{L_T} -\frac{\zeta'(s)}{\zeta(s)}\frac{x^s}{s}\,ds + O\big(\frac{x^c}{T(c-1)} + \frac{x}{T}\log^2 x\big) \tag{1.5}$$

para $x > 1$ no entero (la constante "O" depende de la distancia de x al entero más cercano). Dejaremos esto como un detalle a probar más adelante.

Elegiremos desde ahora $c = 1 + 1/\log x$ para que el término de error se reduzca a $O(xT^{-1}\log^2 x)$.

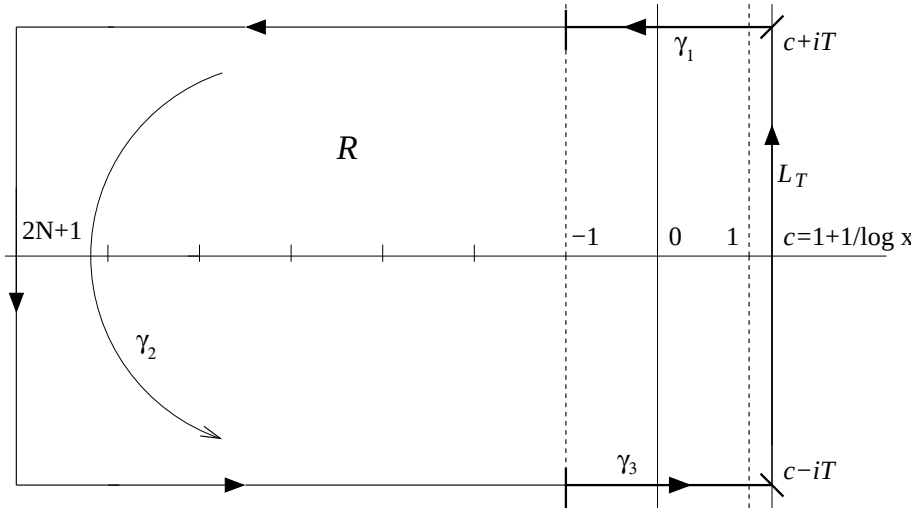
El siguiente paso es aplicar el teorema de los residuos al contorno ∂R donde R es el

rectángulo que tiene a L_T como uno de sus lados y a $-(2N+1)\pm iT$ como vértices opuestos con $N \in \mathbb{Z}^+$ y $N > T \geq 2$.

En la línea quebrada $\partial R \cap \{\operatorname{Re} s \leq -1\}$ se tiene $|\zeta'(s)/\zeta(s)| = O(\log|s|)$. Este segundo detalle no es difícil de probar con la ecuación funcional.

Como no sabemos exactamente dónde están los ceros de ζ en la banda crítica, no hay esperanza de estimar para un T dado ζ'/ζ en el trozo restante de $\partial R - L_T$. Todo lo que vamos a afirmar es que siempre podemos mover T a lo más una unidad, es decir, cambiar T por $T+\delta$, $0 \leq \delta \leq 1$, de manera que $|\zeta'(s)/\zeta(s)| = O(\log^2 T)$ en $\partial R \cap \{-1 \leq \operatorname{Re} s \leq c\}$. Éste es el detalle más sutil.

En un dibujo:



y las acotaciones que hemos dado por supuesto son:

$$\frac{\zeta'(s)}{\zeta(s)} = O(\log|s|) \quad \text{en } \gamma_2, \qquad \frac{\zeta'(s)}{\zeta(s)} = O(\log^2 T) \quad \text{en } \gamma_1 \cup \gamma_3 \quad \text{(quizá moviendo } T\text{)}.$$

Con estas acotaciones y aplicando el teorema de los residuos a (1.5) con $f(s) = -x^s\zeta'(s)/(s\zeta(s))$, se obtiene:

$$\psi(x) = \sum_{s\in R} \operatorname{Res}(f,s) + O\Big(\int_{\gamma_1\cup\gamma_2\cup\gamma_3} |f| + \frac{x}{T}\log^2 x\Big) = \sum_{s\in R} \operatorname{Res}(f,s) + O\Big(\frac{x}{T}\log^2(xT)\Big).$$

La función f tiene polos en $s=1$, en $s=0$, en los ceros triviales $s=-2n$ y en los ceros no triviales $s=\rho$. Los residuos son respectivamente x, $-\zeta'(0)/\zeta(0)$, $x^{-2n}/(2n)$ y

$-x^\rho/\rho$. De modo que para x como antes ($x > 1$ y no entero), se tiene

$$\psi(x) = x - \frac{\zeta'(0)}{\zeta(0)} + \frac{1}{2}\sum_{n\le N}\frac{x^{-2n}}{n} - \sum_{|\rho|<T}\frac{x^\rho}{\rho} + O\big(\frac{x}{T}\log^2(xT)\big). \tag{1.6}$$

Permitiendo $T \to \infty$ se deduce la fórmula inútil pero exacta

$$\psi(x) = x - \frac{\zeta'(0)}{\zeta(0)} - \frac{1}{2}\log(1-x^{-2}) - \sum_\rho \frac{x^\rho}{\rho}$$

donde la suma se debe entender como límite de $\sum_{|\rho|<T}$, no converge absolutamente. Curiosamente se llama *fórmula explícita* a la fórmula anterior.

Mucho más interesante es la fórmula truncada (1.6). Nótese que $\psi(x)$ en los enteros puede "saltar" a lo más $O(\log x)$, así pues añadiendo este término a (1.6) se tiene una fórmula válida uniformemente para x, sin necesidad de imponer que no sea entero. De modo que para $x \ge 2$

$$\psi(x) = x - \sum_{|\rho|<T}\frac{x^\rho}{\rho} + O\big(\frac{x}{T}\log^2(xT) + \log x\big). \tag{1.7}$$

Podemos elegir cualquier $T \ge 2$, pero si lo tomamos pequeño entonces el error es demasiado grande como para probar el teorema de los números primos. Por otra parte, la obligación de tomar T grande lleva al difícil problema de la distribución de los ceros ρ.

Veamos ahora un esbozo de los detalles.

El primero tenía que ver con la aproximación de $\int_L$ por $\int_{L_T}$. Para $0 < t < 1$ se tiene $\int_{L-L_T} t^s/s\,ds = -\int_{L_+} + \int_{L_-}$ donde $L_\pm$ es la semirrecta que une $c \pm iT$ con $+\infty \pm iT$. De donde

$$\int_{L-L_T}\frac{t^s}{s}\,ds = O\big(\frac{t^c}{T|\log t|}\big).$$

Para $t > 1$ se obtiene en su lugar $O(t^c)$ en el segundo miembro. Para comprobarlo basta emplear que $\int_{L-L_T} = -\int_C$ donde C es el arco de circunferencia en $\operatorname{Re} s < c$ centrado en en origen que une $c - iT$ con $c + iT$.

La fórmula mágica (1.3) se puede escribir como

$$\psi(x) = \frac{1}{2\pi i}\int_{L_T} -\frac{\zeta'(s)}{\zeta(s)}\frac{x^s}{s}\,ds + \frac{1}{2\pi i}\sum_n \Lambda(n)\int_{L-L_T}\frac{(x/n)^s}{s}\,ds.$$

Sustituyendo las acotaciones anteriores con $t = x/n$, después de un poco de trabajo se llega a (1.5).

El segundo detalle se puede completar tomando derivadas logarítmicas en la ecuación funcional. Gracias a la simetría la cota trivial $|\zeta'(s)/\zeta(s)| \leq$cte en $\operatorname{Re} s \geq 2$ se transforma en la deseada, $|\zeta'(s)/\zeta(s)| = O(\log|s|)$ en $\operatorname{Re} s \leq -1$, empleando $\Gamma'(s)/\Gamma(s) = O(\log|s|)$.

El último detalle es tan ingenioso que en justicia no merece tal apelativo. Si en (1.4) escribimos $s = 2 + iT$ y tomamos partes reales se tiene

$$1 \gg -\log T + \sum_\rho \operatorname{Re}\big(\frac{1}{2+iT-\rho} + \frac{1}{\rho}\big).$$

Después de calcular la parte real (recuérdese que $0 \leq \operatorname{Re}\rho \leq 1$) se sigue $\log T \gg \sum(1 + (T - \operatorname{Im}\rho)^2)^{-1}$ y de aquí que sólo hay $O(\log T)$ ceros con $T \leq \operatorname{Im}\rho \leq T+1$. Por tanto quizá cambiando T por $T + \delta$, $0 \leq \delta \leq 1$, se puede suponer que hay una distancia $d \gg 1/\log T$ de cada cero de ζ a la horizontal $\operatorname{Im} s = T$.

Si ahora en (1.4) sustituimos $s = \sigma + iT$ con $-1 \leq \sigma \leq 2$ y restamos lo obtenido al sustituir $s = 2 + iT$, se sigue

$$\frac{\zeta'(\sigma+iT)}{\zeta(\sigma+iT)} \ll \log T + \sum_\rho \left|\frac{1}{\sigma+iT-\rho} - \frac{1}{2+iT-\rho}\right|.$$

Los $O(\log T)$ sumandos correspondientes a $|T - \operatorname{Im}\rho| \leq 1$ contribuyen $O(\log^2 T)$ en total por la condición de la distancia. La contribución de los correspondientes a $|T - \operatorname{Im}\rho| > 1$ es menor sin más que emplear la acotación para $\sum(1 + (T - \operatorname{Im}\rho)^2)^{-1}$.

1.7. ¿Qué podemos probar con la hipótesis de Riemann?

Antes de adscribirnos a las ventajas del que nos prometen ser el mejor de los mundos posibles, vamos a comprobar que realmente lo es.

La fórmula

$$-\frac{\zeta'(s)}{\zeta(s)} = \frac{s}{s-1} + s\int_1^\infty (\psi(x) - x)x^{-s-1}dx,$$

que se deduce con el Lema de Abel, prueba directamente que $\psi(x) = x + o(x)$ implica necesariamente $\lim_{\sigma\to 1^+} |\zeta'(\sigma + it)/\zeta(\sigma + it)| < \infty$ para todo $t \neq 0$. Es decir, si hubiera algún cero en $\operatorname{Re} s = 1$, el teorema de los números primos no sería cierto. De la misma forma, la existencia de un solo cero en $\operatorname{Re} s = \sigma_0$ es incompatible con $\psi(x) = x + o(x^{\sigma_0})$, como sugiere (1.7).

Según esto, el error más pequeño en el teorema de los números primos se obtendría si todos los ceros no triviales tuviesen la parte real lo menor posible. Por otro lado, la ecuación funcional implica que si ρ es un cero no trivial entonces $1 - \rho$ también lo es. De forma que para que el supremo de las partes reales de los ceros no triviales sea lo menor posible todas ellas deben ser $1/2$. Quizá fuera este argumento, o simplemente la evidencia numérica [**Ed**] lo que llevo a Riemann a formular su hipótesis, cuyo enunciado es:

Hipótesis de Riemann: *Todos los ceros no triviales de la función ζ están en la línea crítica $Re\, s = 1/2$.*

Que los ceros de una función meromorfa se coloquen todos en fila india es algo tan singular que debería ser fácil de probar si es cierto, o de refutar si hay un contraejemplo. Sin embargo han pasado más de 140 años desde que Riemann hizo su conjetura y no sólo no se ha probado sino que no se ha logrado estrechar ni un ápice la banda crítica en la que viven los ceros. Es decir, no se conoce nigún $\epsilon > 0$ tal que todos los ceros no triviales pertenezcan a una *banda crítica reducida*, $\epsilon < \operatorname{Re} s < 1 - \epsilon$.

De todas maneras no está de más imaginar cuál es la mejor situación y ver al menos las consecuencias más inmediatas. Si se cumpliera la hipótesis de Riemann, tomando $T = x^{1/2}$ en (1.7) se tiene (recuérdese que hay $O(\log N)$ ceros con $N \leq |\rho| \leq N + 1$)

$$\psi(x) = x + O(x^{1/2}\log^2 x).$$

Esto se traduce en

$$\pi(x) = Li(x) + O(x^{1/2}\log x).$$

Se conoce que el factor $\log^2 x$ no se puede suprimir totalmente en la primera fórmula [**El**] ya que los límites superior e inferior de $(\psi(x) - x)/\sqrt{x}$ son $+\infty$ y $-\infty$. De ello se puede deducir que $Li(x)$ es la aproximación óptima de $\pi(x)$ si no admitimos términos oscilatorios.

Aparte de la optimización del término de error, conocer la hipótesis de Riemann de antemano permitiría reducciones importantes en la demostración del teorema de los números primos. Así como la prueba de muchos resultados condicionales de la Teoría de Números que dependen de ella.

1.8. ¿Qué podemos probar sin la hipótesis de Riemann?

Como ya hemos mencionado, no se sabe probar la ausencia de ceros en ninguna bandita del tipo $1-\epsilon < \operatorname{Re} s < 1$. Todo lo que se sabe al respecto **[Iv]**, y con mucho esfuerzo, es que si existiera una sucesión de ceros no triviales $\rho_n = \sigma_n + it_n$ con $\sigma_n \to 1$, entonces $\log|t_n|$ a la larga superaría a cierta potencia negativa de $1-\sigma_n$. El resultado que veremos aquí es el clásico (no el mejor posible) y permite acotar la suma en (1.7) por el término principal multiplicado por un factor que tiende lentamente a cero; lo cual prueba el teorema de los números primos.

En primer lugar nótese que, por un argumento de continuidad en (1.4), intuitivamente si existiera un cero no trivial $\sigma_n + it_n$ muy cerca de $\operatorname{Re} s = 1$ entonces para $\sigma \to 1^+$ se tendría que $-\zeta'(\sigma+it_n)/\zeta(\sigma+it_n)$ tiene parte real muy grande y negativa. En ese caso, $\zeta'(s)/\zeta(s) = \sum \Lambda(n)n^{-s}$ sugiere que $\cos(t_n \log p)$ toma muchas veces valores negativos. Entonces, recíprocamente, $\cos(2t_n \log p)$ debe tomar muchas veces valores positivos y $-\zeta'(\sigma+2it_n)/\zeta(\sigma+2it_n)$ debe tener parte real grande y positiva. Controlando el tamaño de esta última cantidad controlaremos la cercanía del posible cero a la línea $\operatorname{Re} s = 1$. Lo más ingenioso, a la par que simple, es la manera de cuantificar los tamaños relativos al evaluar en $\sigma + it_n$ y en $\sigma + 2it_n$. Se emplea para ello la sencilla desigualdad trigonométrica

$$3 + \cos(2\alpha) \geq -4\cos\alpha \qquad \forall \alpha \in \mathbb{R}.$$

Susituyendo $\alpha = t_n \log p$ y sumando con coeficientes adecuados se tiene, para $\sigma > 1$,

$$-3\frac{\zeta'(\sigma)}{\zeta(\sigma)} - \operatorname{Re}\frac{\zeta'(\sigma+2it_n)}{\zeta(\sigma+2it_n)} \geq 4\operatorname{Re}\frac{\zeta'(\sigma+it_n)}{\zeta(\sigma+it_n)}$$

De (1.4), cuando $\sigma > 1$ está suficientemente cercano a 1 se cumple $-\zeta'(\sigma)/\zeta(\sigma) < (\sigma-1)^{-1} + \text{cte}$, y además las desigualdades

$$-\operatorname{Re}\frac{\zeta'(\sigma+2it_n)}{\zeta(\sigma+2it_n)} < \text{cte}\,\log(|t_n|+2) \quad \text{y} \quad -\operatorname{Re}\frac{\zeta'(\sigma+it_n)}{\zeta(\sigma+it_n)} < \text{cte}\,\log(|t_n|+2) - \frac{1}{\sigma-\sigma_n}.$$

Para probarlas utilícese (1.4), $\Gamma'(s)/\Gamma(s) = O(\log|s|)$ y que $\operatorname{Re}\left((s-\rho)^{-1} + \rho^{-1}\right) > 0$ para $\operatorname{Re} s > 1$. Sustituyendo se obtiene

$$3/(\sigma-1) + \text{cte}\log(|t_n|+2) \geq 4/(\sigma-\sigma_n).$$

Tomando $\sigma = 1 + \epsilon/\log(|t_n|+2)$ con ϵ pequeño se sigue que $\sigma_n \leq 1 - \text{cte}/\log(|t_n|+2)$ para cierta constante positiva. O dicho de otro modo, existe una constante $C > 0$ tal que

la región $s = \sigma + it$ con

$$\sigma > 1 - \frac{C}{\log(|t| + 2)}$$

está libre de ceros.

La *región libre de ceros* anterior, en conjunción con que hay $O(\log N)$ ceros con $N \leq |\rho| \leq N + 1$ permite estimar la suma de (1.7) como

$$\sum_{|\rho|<T} \left| \frac{x^\rho}{\rho} \right| \ll \sum_{N<T} \log N \frac{x^{1-C/\log T}}{N} \ll x^{1-C/\log T} \log^2 T.$$

Finalmente tomando $T = e^{\sqrt{\log x}}$ y haciendo limpieza de los términos de orden inferior se concluye

$$\boxed{\psi(x) = x + O\big(xe^{-K\sqrt{\log x}}\big)}$$

para cierta constante positiva K (en **[El]**, $K = 1/15$). Esto está muy lejos de lo que se obtendría con la hipótesis de Riemann pero prueba en particular que $(\psi(x) - x)/x$ tiende a cero más rápido que cualquier potencia negativa de $\log x$. Lo mejor que se ha conseguido hasta la fecha, tras los profundos trabajos de Vinogradov y Korobov **[Iv]**, es reemplazar en el exponente de la fórmula anterior $\sqrt{\log x}$ por $\log^\alpha x$ para cualquier $\alpha < 3/5$.

1.9. Primos en progresiones aritméticas

Por último vamos a considerar la distribución de los primos en una progresión aritmética $\{an + b\}$ con $a, b \in \mathbb{Z}^+$ coprimos entre sí (en otro caso la progresión contiene a lo más un primo). Para cada a fijo se cumple $\mathbb{Z} = \{an + 0\} \cup \{an + 1\} \cup \ldots \cup \{an + (a - 1)\}$ con n recorriendo $\mathbb{Z}$. De estas progresiones, $\{an + b\}$, hay $\phi(a)$ con b coprimo con a. Parece natural suponer que no hay ninguna de ellas privilegiada, de modo que todas contienen la misma proporción de primos. Esto sugiere el *teorema de los números primos en progresiones aritméticas*, que afirma

$$\pi(x; a, b) \sim \frac{1}{\phi(a)} Li(x) \qquad \text{con} \quad \pi(x; a, b) = \sum_{\substack{p \equiv b \pmod a \\ p \leq x}} 1$$

Por ejemplo, si $a = 5$ todos los primos mayores que 5 son de la forma $5n + 1$, $5n + 2$, $5n + 3$ o $5n + 4$. Por tanto cabe esperar que la cuarta parte de los primos sean de la forma $5n + 2$, esto es, $\pi(x; 5, 2) \sim \frac{1}{4} Li(x)$.

Si tratamos de adaptar la demostración del teorema de los números primos usual al caso de progresiones aritméticas, una primera dificultad es que el análogo natural de la identidad de Euler no es cierto. En nuestro caso $\sum(5n+2)^{-s} \neq \prod(1-p^{-s})^{-1}$ con $p \equiv 2 \ (mod\ 5)$; la razón es simplemente que un número de la forma $5n+2$ no tiene siempre factores primos de este mismo tipo. Se hace necesaria una manera de seleccionar progresiones aritméticas que sea coherente con una identidad como la de Euler.

Un ejemplo que nos puede dar alguna luz es tratar de extraer los términos con grado en cierta progresión geométrica a partir de una serie de Taylor conocida, como la de $e^x = 1 + x/1! + x^2/2! + x^3/3! + \ldots$. Seleccionar los de grado par o impar es sencillo y da lugar a las funciones trigonómetricas hiperbólicas:

$$1 + \frac{x^2}{2!} + \frac{x^4}{4!} + \ldots = \frac{1}{2}(e^x + e^{-x}) = \cosh x, \quad \frac{x}{1!} + \frac{x^3}{3!} + \frac{x^5}{5!} + \ldots = \frac{1}{2}(e^x - e^{-x}) = \operatorname{senh} x.$$

Si nos queremos restringir a los múltiplos de cuatro, la expresión es más complicada:

$$1 + \frac{x^4}{4!} + \frac{x^8}{8!} + \ldots = \frac{1}{4}(e^x + e^{ix} + e^{-x} + e^{-ix}) = \frac{\cosh x + \cos x}{2}.$$

Pero nos da la clave para entender que lo necesario para obtener los múltiplos de a es introducir como coeficientes raíces de la unidad teniendo en cuenta que la suma de todas ellas es nula. Así pues (recuérdese la notación $e(t) = e^{2\pi i t}$)

$$1 + \frac{x^a}{a!} + \frac{x^{2a}}{(2a)!} + \frac{x^{3a}}{(3a)!} + \ldots = \frac{1}{a}\sum_{k=0}^{a-1} e^{x\, e(k/a)} \qquad \text{para} \ \ a \in \mathbb{Z}^+.$$

Si quisiéramos, por ejemplo, seleccionar los congruentes con 2 módulo 5, o en general módulo a, bastaría "adelantar" la suma en dos unidades:

$$\frac{x^2}{2!} + \frac{x^{a+2}}{(a+2)!} + \frac{x^{2a+2}}{(2a+2)!} + \frac{x^{3a+2}}{(3a+2)!} + \ldots = \frac{1}{a}\sum_{k=0}^{a-1} e(-2k/a) e^{x\, e(k/a)}.$$

Una vez vistos estos ejemplos volvamos al problema con la identidad de Euler. Para que una función $f : \mathbb{Z}^+ \to \mathbb{C}$ dé lugar a una identidad como la de Euler:

$$\sum_{n=1}^{\infty} \frac{f(n)}{n^s} = \prod_p \Big(1 - \frac{f(p)}{p^s}\Big)^{-1},$$

debe ser completamente multiplicativa (es decir, $f(mn) = f(m)f(n), \ \ \forall n, m \in \mathbb{Z}^+$). Lo

que haremos será elegir f que tome valores entre las raíces de la unidad de manera que nos permita seleccionar progresiones aritméticas como antes. Primeramente nótese que como estamos interesados sólo en el caso en que a y b son coprimos es natural definir $f(n) = 0$ cuando n y a tienen divisores propios comunes porque $n = ak + b$, $\mathrm{mcd}(n, a) > 1 \Rightarrow \mathrm{mcd}(a, b) > 1$. Para el resto de los valores de n queremos que $f(n)$ sea una raíz de la unidad y que, en general, f sea una función multiplicativa y periódica de periodo a. Todos estos requerimientos se pueden completar de forma elegante considerando los *caracteres módulo a*, es decir, los homomorfismos $\chi : \mathbb{Z}_a^* \longrightarrow (\mathbb{C} - \{0\}, \cdot)$ donde $\mathbb{Z}_a^*$ es el grupo (multiplicativo) de unidades del anillo $\mathbb{Z}_a$. No es difícil probar que las únicas funciones con las propiedades anteriores son de la forma

$$f(n) = \begin{cases} 0 & \text{si } \mathrm{mcd}(n, a) > 1 \\ \chi(\overline{n}) & \text{si } \overline{n} \in \mathbb{Z}_a^* \end{cases}$$

donde χ es un carácter módulo a. Nótese que $\chi(\overline{n})$ es una raíz de la unidad para $\overline{n} \in \mathbb{Z}_a^*$ porque

$$(\chi(\overline{n}))^{|\mathbb{Z}_a^*|} = \chi(\overline{n}^{|\mathbb{Z}_a^*|}) = \chi(\overline{1}) = 1.$$

En el grupo $\mathbb{Z}_a^*$ (y en general en todos los abelianos cuando se extiende la definición) los caracteres forman un grupo con la multiplicación isomorfo al de partida. De algún modo conforman un dual del grupo que lo representa fielmente. Por ejemplo $\mathbb{Z}_5^* = \{\overline{1}, \overline{2}, \overline{3}, \overline{4}\}$ es un grupo cíclico de orden cuatro ($\mathbb{Z}_5^* = \{\overline{2}^0, \overline{2}^1, \overline{2}^3, \overline{2}^2\}$) cuyos caracteres son:

	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
χ_0	1	1	1	1
χ_1	1	i	$-i$	-1
χ_2	1	-1	-1	1
χ_3	1	$-i$	i	-1

que de nuevo forman un grupo cíclico de orden cuatro ($\chi_0 = \chi_1^4$ es la identidad, $\chi_1 = \chi_1^1$, $\chi_2 = \chi_1^2$ y $\chi_3 = \chi_1^3$).

No es difícil definir constructivamente los caracteres **[Da]**, **[El]** en términos de raíces primitivas de la unidad en $\mathbb{Z}_{p^k}^*$ con $p^k | a$ pero no será de interés aquí. Con el abuso de notación obvio, se suele denotar igual a los caracteres χ que a las funciones f asociadas. Conviniendo en ello, y después de lo dicho anteriormente las funciones que reemplazan a la función ζ en el contexto de los primos en progresiones aritméticas, son las *funciones L de Dirichlet* definidas como

$$L(s, \chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}.$$

Estas funciones satisfacen para $\operatorname{Re} s > 1$

$$L(s,\chi) = \prod_p \big(1 - \frac{\chi(p)}{p^s}\big)^{-1} \quad \text{y} \quad -\frac{L'(s,\chi)}{L(s,\chi)} = \sum_{n=1}^{\infty} \Lambda(n)\frac{\chi(n)}{n^s}.$$

Variando χ podemos seleccionar los primos en cierta progresión aritmética jugando, como antes, con las raíces de la unidad. Por ejemplo, con los caracteres de la tabla anterior se tiene

$$\sum_{\substack{n\equiv 1 \pmod 5 \\ n\le x}} \frac{\Lambda(n)}{n^s} = -\frac{1}{4}\sum_{j=0}^{4} \frac{L'(s,\chi_j)}{L(s,\chi_j)} \quad \text{y} \quad \sum_{\substack{n\equiv 2 \pmod 5 \\ n\le x}} \frac{\Lambda(n)}{n^s} = -\frac{1}{4}\sum_{j=0}^{4} \overline{\chi}_j(2)\frac{L'(s,\chi_j)}{L(s,\chi_j)}.$$

En general se puede aplicar la "fórmula mágica" como en el teorema de los números primos y probar que

$$\psi(x;a,b) = \sum_{\substack{n\equiv b \pmod a \\ n\le x}} \Lambda(n) = -\frac{1}{\phi(a)}\sum_{\chi} \frac{\overline{\chi}(b)}{2\pi i}\int_{L_T} \frac{L'(s,\chi)}{L(s,\chi)}\frac{x^s}{s}\,ds + \text{Error}$$

donde χ recorre todos los caracteres módulo a (nótese que $\phi(a) = |\mathbb{Z}_a^*|$ es el número de estos caracteres) y Error$= O(x^c/(T(c-1)) + xT^{-1}\log^2 x)$.

Cuando uno llega a este punto ya está cansado y tiende a decir que se procede de forma similar a como se hizo en el teorema de los números primos. Sin embargo esto no es realmente así, hay varias dificultades técnicas y teóricas. Entre las dificultades más notables está la prueba de que $L'(s,\chi)/L(s,\chi)$ sólo tiene un polo en $s = 1$ si χ es constantemente uno (naturalmente, en los coprimos con a); lo cual requiere demostrar que para el resto de los caracteres se cumple $L(1,\chi) \neq 0$. Nótese que si damos esto por supuesto, la prueba de Euler se puede adaptar para deducir el *Teorema de Dirichlet* que afirma que $\{an + b\}$ contiene infinitos primos. Otra dificultad aparece al estudiar la uniformidad en a de las regiones libres de ceros de $L'(s,\chi)/L(s,\chi)$. Este problema viene motivado porque en muchas aplicaciones se necesita que $\pi(x;a,b) \sim \frac{1}{\phi(a)}Li(x)$ siga siendo cierto si a es una función de x que no crece demasiado. Hoy en día sólo se sabe tratar el caso en que a es extremadamente pequeño en comparación con x, debido a que no se conoce la ausencia de ciertos ceros reales de $L(s,\chi)$ llamados *ceros de Siegel* [**Da**], [**El**]. Por otra parte, la generalización de la hipótesis de Riemann a las funciones L, si fuera cierta, implicaría $\pi(x;a,b) \sim \frac{1}{\phi(a)}Li(x)$ para $a = a(x) = O(x^{1/2-\epsilon})$ cualquiera que sea $\epsilon > 0$. Nuestro conocimiento actual con respecto a esta *hipótesis de Riemann generalizada* es todavía mucho más precario que con respecto a la hipótesis original.

2. La estimación de sumas trigonométricas

2.1. Introducción y dos principios principales: incertidumbre y fase estacionaria

Las demoledoras preguntas infantiles "¿por qué?" y "¿para qué?", aunque denostadas habitualmente en Matemáticas, no son superfluas. En nuestro caso, vamos a hacer durante un capítulo una árida teoría de sumas trigonométricas y seguramente nuestra fe flaquearía si sólo nos respondieran que "las sumas trigonométricas son importantes en la Teoría Analítica de Números". Merece la pena, por tanto, gastar unas pocas líneas a modo de motivación antes del capítulo con algunas aplicaciones.

En realidad ya ha aparecido un ejemplo. La función ζ para valores complejos con $\operatorname{Re} s > 1$ da lugar a una serie trigonométrica que puede acotarse con métodos sofisticados. Empleando la relación entre los ceros y el crecimiento de las funciones holomorfas, el resultado permite ensanchar un poco la región libre de ceros. Como este ejemplo es un poco impreciso, fabricaremos otro más tangible, en el que podamos poner las manos.

Supongamos que queremos estimar con precisión el número total de divisores (la suma del número de divisores) de los enteros positivos menores que X, digamos $1 < X \notin \mathbb{Z}^+$. Podemos "contar con los dedos" viendo que el 1 aparece en $1\cdot 1$, $1\cdot 2$, $\dots 1\cdot[X]$, y por tanto $[X]$ veces; el 2 aparece $[X/2]$ veces ($2\cdot 1$, $2\cdot 2$, $\dots 2\cdot[X/2] < [X]$); y en general m aparece $[X/m]$ veces. En definitiva tenemos que estimar la suma $\sum[X/m]$. Ahora guardemos nuestro dedos y escribamos $[X]$ como $-\frac{1}{2} + \frac{1}{2}\sum \Psi(n)$ donde Ψ es la función característica de $[-X, X]$. Por la fórmula de sumación de Poisson, $\sum \Psi(n) = \sum \widehat{\Psi}(n)$. Un cálculo muestra que, aparte del término principal obtenido para $n = 0$, $\widehat{\Psi}(n)$ es un coeficiente por $\operatorname{sen}(2\pi nX)$. Lo mismo podríamos hacer con $[X/m]$ sustituyendo $\Psi(t)$ por $\Psi_m(t) = \Psi(mt)$; y en total tendríamos que estimar una suma de la forma $\sum\sum \operatorname{sen}(2\pi nX/m)$. Por cierto, el mismo resultado se obtendría desarrollando en serie de Fourier la función periódica $t - [t]$ en $t = X/m$.

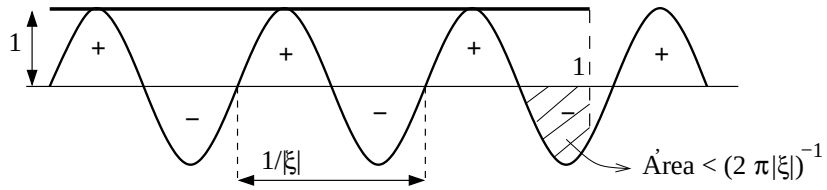
Ahora tenemos que decidir entre enfrentarnos a una suma con partes enteras o a otra con funciones trigonométricas. Siempre se tiende a pensar erróneamente que la propia área es más difícil e interesante que el resto, y que está minusvalorada. Como la primera suma suena a Teoría de Números y la segunda a Análisis Armónico, nos decidimos por la segunda confiando en que avezados analistas hayan desarrollado unas teorías de cancelación de sumas trigonométricas. La historia no es tan sencilla, aunque les robemos sus armas a los analistas, en realidad la teoría siempre ha estado bajo la sombra de la Teoría de Números y parece no haber tenido un gran impacto en el tipo de problemas que trata el Análisis Armónico.

Como hemos visto, la fórmula de sumación de Poisson permite contar por medio de integrales oscilatorias dadas por transformadas de Fourier. Por ello nos detendremos a ver dos ideas intuitivas, el principio de incertidumbre y el de fase estacionaria, que posibiliten controlar dichas integrales.

Para funciones con regularidad suficiente, inegrando por partes se tiene:

$$|\widehat{f}(\xi)| \leq \frac{1}{(2\pi|\xi|)^n}\|f^{(n)}\|_1. \tag{2.1}$$

De modo que si $f \in C^\infty$ y ella y sus derivadas son integrables , $|\widehat{f}(\xi)| = O(|\xi|^{-n})$ para todo n; es decir, en estas condiciones la transformada de Fourier decae más rápido que el inverso de cualquier polinomio. Para funciones con poca regularidad esto no es cierto (aunque por el *Lema de Riemann-Lebesgue* **[Dy-Mc]** $f \in L^1 \Rightarrow \widehat{f}(\xi) \to 0$). Por ejemplo, la transformada de Fourier de la función característica de $[-1,1]$ sólo decae como $1/|\xi|$. Podemos interpretar esto analíticamente viendo que al integrar por partes aparecen términos de frontera, o geométricamente diciendo que debido al corte abrupto, en cada extremo una oscilación de $y(x) = e(\xi x)$ puede quedar sin completar y en el peor caso (media longitud de onda) la masa residual es comparable a $1/|\xi|$.

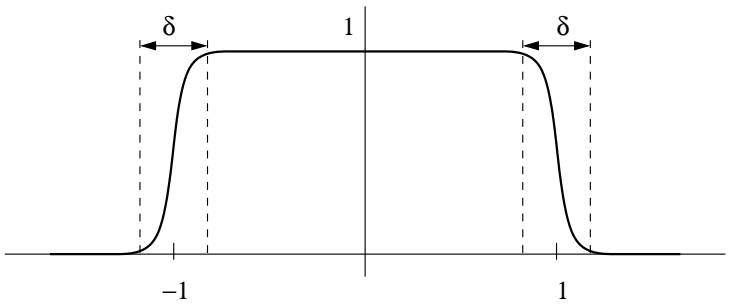


Evidentemente necesitamos $|\xi| \geq 1$ para que $y = y(x)$ llegue a oscilar unas cuantas veces en $[-1,1]$. Insistiendo en este punto, si tomamos la función de masa uno, $f = (2\epsilon)^{-1}\chi_{[-\epsilon,\epsilon]}$, donde $\chi_{[-\epsilon,\epsilon]}$ indica la función característica de $[-\epsilon,\epsilon]$, a las ondas con frecuencia $|\xi|$ mucho menor que ϵ^{-1} no les dará tiempo a oscilar y se tendrá $\widehat{f}(\xi) \approx \widehat{f}(0) = 1$, pero si $|\xi|$ es mucho mayor que ϵ^{-1}, entonces de nuevo tenemos típicamente una oscilación que no se completa y por tanto un decaimiento de orden $|\xi|^{-1}$ (multiplicado por una constante que depende de ϵ).

La idea empleada en los ejemplos anteriores es la base del *Principio de incertidumbre* en una forma tan básica que seguramente pocos lo llamarían así.

Principio de incertidumbre (idea intuitiva): *En un intervalo de longitud δ sólo veremos oscilar las ondas de frecuencia mayor o igual que δ^{-1}.*

Para mostrar cómo aplicar este principio, supongamos que en cierto problema necesitásemos que la transformada de Fourier de algo como $\chi_{[-1,1]}$ decayera a la larga más rápido que $|\xi|^{-1}$, y con tal fin hacemos una regularización C^∞ en una pequeña bandita de anchura δ en cada extremo.



La regularización tiene masa (área) comparable a δ, por tanto sólo puede modificar el valor de la transformada de Fourier a lo más en una cantidad de este orden. Para frecuencias $|\xi|$ mucho menores que δ^{-1}, como $\widehat{\chi}_{[-1,1]}(\xi)$ es típicamente mayor que δ, se tiene $\widehat{f}(\xi) \approx \widehat{\chi}_{[-1,1]}(\xi)$. Por otro lado, cuando $|\xi|$ es bastante mayor que δ^{-1}, las ondas de frecuencia $|\xi|$ oscilan mucho en las banditas de regularización y hay una gran cancelación (si se quiere, utilícese (2.1) estudiando el tamaño típico de las derivadas), de modo que $\widehat{f}(\xi) \approx 0$. En el rango de transición con $|\xi|$ comparable a δ^{-1}, las ondas "verán" la regularización y se tendrá, según crece $|\xi|$, un aumento en la cancelación que se traduce en un decaimiento gradual de $\widehat{f}(\xi)$.

Nótese que en el ejemplo anterior no podemos distinguir la función sin regularizar de la regularizada mediante la transformada de Fourier si no consideramos frecuencias grandes del orden de al menos el inverso del tamaño del intervalo en que se diferencian. Ahí está la *incertidumbre*. Dicho de otro modo, si queremos analizar una función, una señal, una fotografía ... mediante ondas de frecuencias menores o iguales que M, el principio de incertidumbre implica que el resultado será en general "borroso" en los intervalos de longitud mucho menor que M^{-1}. Para estas longitudes no se puede mejorara la precisión, el resultado es incierto.

En los textos de Física no es raro que lo anterior se considere una explicación completa del principio de incertidumbre, pero en Matemáticas estamos malacostumbrados a través de los libros a la difícil tarea de extraer ideas de las fórmulas, y cuando se presenta una idea sin fórmulas nos afecta un escalofrío de inseguridad. Por ello, no está de más mencionar un par de enunciados al respecto. El primero dice que al estrechar una función T veces, conservando la masa, la banda de frecuencias significativas se ensancha T veces.

Principio de incertidumbre (versión "light"): *La transformada de Fourier de* $g(x) = Tf(Tx)$ *es* $\widehat{g}(\xi) = \widehat{f}(\xi/T)$.

Otra versión se emplea en Mecánica Cuántica [**Yn**] y de nuevo dice que no podemos concentrar alrededor del origen simultáneamente la masa de una función y de su transformada de Fourier [**Dy-Mc**].

PRINCIPIO DE INCERTIDUMBRE (desigualdad de Heisenberg): *Cualquiera que sea f de decaimiento rápido, se verifica:*

$$16\pi^2 \int_{-\infty}^{\infty} x^2 |f(x)|^2 dx \cdot \int_{-\infty}^{\infty} \xi^2 |\widehat{f}(\xi)|^2 d\xi \geq 1.$$

Nota: En Mecánica Cuántica, salvo constantes, la posición y el momento se pueden considerar como variables aleatorias con funciones de densidad dadas por $|\Psi|^2$ y $|\widehat{\Psi}|^2$ para cierta *función de onda* Ψ. La relación anterior permite deducir que el producto de las varianzas de posición y momento son mayores que una constante (muy pequeña en las unidades del Sistema Internacional) y por tanto ambos no pueden tener simultáneamente *dispersión* arbitrariamente pequeña. Si la varianza de la posición tiende a cero, la del momento tiende a infinito.

Más adelante será conveniente considerar no sólo transformadas de Fourier sino integrales oscilatorias en general de la forma $\int g(x)e(f(x))\,dx$. Si la función f que representa la *fase* crece muy deprisa, es decir, si $f' >$ cte grande, entonces integrando por partes en $\int (g/f')f'e(f)$ se concluye que la integral es pequeña. Pero este truco no funciona si en algunos puntos f' es pequeño. En ellos la onda $e(f)$ oscila muy poco y típicamente no hay cancelación al integrar contra g. En pocas palabras:

PRINCIPIO DE FASE ESTACIONARIA (idea intuitiva): *La mayor contribución a una integral oscilatoria proviene de los puntos en que la fase es estacionaria.*

Si tenemos alguna información local en los puntos críticos podemos ser más precisos. Por ejemplo, si x_0 es un único punto crítico con $f''(x_0) \neq 0$ entonces cerca de x_0, $f(x) \approx f(x_0) + \frac{1}{2}f''(x_0)(x-x_0)^2$ y $g(x) \approx g(x_0)$; lo que sugiere que $\int g(x)e(f(x))\,dx$ se puede aproximar por

$$g(x_0)e(f(x_0)) \int e(\frac{1}{2}f''(x_0)(x-x_0)^2)\,dx = \frac{1}{2}g(x_0)\frac{e(f(x_0))}{\sqrt{|f''(x_0)|}} \int \frac{e(\pm t/2)}{\sqrt{t}}\,dt$$

(donde el $\pm$ depende del signo de $f''(x_0)$). Esto es, $\int g(x)e(f(x))\,dx$ se aproxima por cte $g(x_0)e(f(x_0))/\sqrt{|f''(x_0)|}$ y cabe esperar, por tanto, un decaimiento como el inverso de la raíz cuadrada de la derivada segunda.

Como ejemplo consideremos la fórmula que se puede comprobar en una tabla de integrales [**Gr-Ry**]: $I = \int e^{-x^2}\cos(\lambda x^2)\,dx = \sqrt{\frac{\pi}{2}}\sqrt{1+\sqrt{1+\lambda^2}}/\sqrt{1+\lambda^2}$. Según ésta, para $\lambda \to \infty$ se tiene $I \sim \frac{1}{2}\sqrt{2\pi/|\lambda|}$ (nótese que el resultado se ajusta al esquema anterior). El principio de fase estacionaria nos dice que este comportamiento depende de lo que ocurre en las cercanías del punto $x = 0$ en el que la fase es estacionaria (derivada nula). De modo que debe mantenerse si se reemplaza e^{-x^2} por cualquier función que se le parezca en un entorno de cero. Así pues, podemos intuir resultados tan complejos como $\int(\log(1+x^6)+1)e^{-x^2}\cos(\lambda x^2)\,dx \sim \frac{1}{2}\sqrt{2\pi/|\lambda|}$ o en general $\int g(x)\cos(\lambda x^2)\,dx \sim \frac{1}{2}g(0)\sqrt{2\pi/|\lambda|}$ si $g(0) \neq 0$.

De nuevo uno puede tranquilizar su espíritu matemático aferrándose a un enunciado preciso pero mucho más rígido que la idea intuitiva [**So**].

Principio de fase estacionaria: *Sea $f, g \in C^\infty$ con g de decaimiento rápido y $f'' > 0$. Si f tiene un punto crítico en $x = c$; cuando $\lambda \to +\infty$ para cada n se cumple*

$$\int_{-\infty}^{\infty} g(x)e(\lambda f(x))\,dx = \frac{e(\lambda f(c)+1/8)}{\sqrt{\lambda f''(c)}}\big(a_0 + \frac{a_1}{\lambda} + \frac{a_2}{\lambda^2} + \ldots + O(\frac{1}{\lambda^n})\big)$$

donde los a_i dependen de los coeficientes de Taylor de f y g en $x = c$. En particular $a_0 = g(c)$.

2.2. La acotación básica de van der Corput

Hay una joyita temprana que destaca en el árido mundo de la acotación de sumas trigonométricas, repleto de quincalla de términos de error evanescentes. Con ella van der Corput nos mostró que simplemente sabiendo que las fases son cóncavas o convexas, ya podemos obtener una acotación. Un resultado tan sencillo debería admitir una explicación sencilla, o al menos con más palabras que fórmulas.

Supongamos que queremos estimar $\sum_{n\in I} e(f(n))$ con I un intervalo de longitud N, donde controlamos el tamaño de la derivada segunda de f, $0 < \lambda_2 \ll |f''| \ll \lambda_2$.

Aplicando la fórmula de sumación de Poisson sin considerar los problemas de convergencia y regularidad (por ejemplo suponiendo que se multiplica por una función C^∞ adaptada a I), se llega a integrales del tipo $\int e(g_n(x))\,dx$ con $g_n(x) = f(x) - nx$. Si n está fuera de un intervalo $[\alpha, \beta]$ que contenga a la imagen de f', entonces $e(g_n(x))$ oscila mucho (g_n' es grande) y hay una gran cancelación (esto no es más que una variante del principio de incertidumbre ya que cerca de x la longitud de onda de $e(g_n(x))$ es aproximadamente $|g_n'(x)|^{-1}$). Por tanto cabe esperar

$$\sum_{n\in I} e(f(n)) \approx \sum_{\alpha\le n\le\beta} \int e(g_n(x))\,dx.$$

Según el principio de fase estacionaria la contribución a $\int e(g_n(x))\,dx$ vendrá sobre todo de los puntos críticos x_n con un decaimiento comparable a $(|f''(x_n)|)^{-1/2} = O(\lambda_2^{-1/2})$. Así pues, si este razonamiento intuitivo es cierto, como el número de sumandos es $O(\beta-\alpha+1)$, se concluye

$$\sum_{n\in I} e(f(n)) \ll (\beta-\alpha+1)\lambda_2^{-1/2} \ll N\lambda_2^{1/2} + \lambda_2^{-1/2},$$

donde se ha empleado el teorema del valor medio en la forma $(\beta-\alpha)/N \ll \lambda_2$.

Resumiendo, esperamos que se cumpla el siguiente resultado:

Teorema 2.1 . *Sea $f \in C^2(I)$ con I un intervalo de longitud N. Si $0 < \lambda_2 \ll |f''| \ll \lambda_2$ entonces*

$$\sum_{n\in I} e(f(n)) \ll N\lambda_2^{1/2} + \lambda_2^{-1/2}.$$

La demostración consiste en dar rigor a los pasos anteriores: la aplicación de la fórmula de sumación de Poisson y del principio de fase estacionaria.

Proposición 2.2 . *Sea $f \in C^2([a,b])$, $a,b \in \mathbb{Z}$ con $f'' \neq 0$, y $\alpha,\beta \in \mathbb{Z}$ tales que $\alpha < f' < \beta$; entonces*

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

Nota: La hipótesis $a,b \in \mathbb{Z}$ es en realidad superflua.

Dem.: Supondremos $\alpha = 0$. Esto se puede hacer sin perder generalidad, ya que en otro caso basta cambiar $f(n)$ por $f(n)-\alpha n$, lo que no modifica el valor de la suma.

Partimos de la fórmula

$$\sum_{a\le n\le b} e(f(n)) = \int_a^b e(f(x))\,dx + O(1) + \sum_{n\neq 0} \frac{1}{n}\int_a^b f'(x)e(f(x)-nx)\,dx. \tag{2.2}$$

que se sigue a partir de la fórmula de sumación de Euler-Mc Laurin para $n=1$ desarrollando por Fourier $t-[t]-1/2$ como $\sum_{n\neq 0} e(-nx)/(2\pi in)$. También es posible deducirla de la fórmula de sumación de Poisson integrando por partes.

Si $n > \beta$ o $n < \alpha = 0$, la derivada de $g_n(x) = f(x) - nx$ no se anula, e integrando por partes con $u = f'/g_n'$ y $dv = g_n' e(g_n)\,dx$, se tiene

$$\left| \int_a^b f'(x) e(f(x) - nx)\,dx \right| \leq \left| \frac{f'(a)}{g_n'(a)} \right| + \left| \frac{f'(b)}{g_n'(b)} \right| + \int_a^b \left| (f'/g_n')' \right|.$$

La función f'/g_n' es monótona ($f'' \neq 0$) y por tanto se pueden sacar los valores absolutos fuera de la última integral. En definitiva

$$\left| \int_a^b f'(x) e(f(x) - nx)\,dx \right| \leq \frac{4\beta}{|\beta - n|}.$$

En particular la serie del segundo miembro de (2.2) converge uniformemente. Y la contribución de estos términos con $n > \beta$ y $n < 0$ está acotada por

$$\sum_{n<0} \frac{4\beta}{n(\beta - n)} + \sum_{n>\beta} \frac{4\beta}{n(n - \beta)} \ll \sum_{|n|>2\beta} \frac{1}{n^2} + \sum_{0\neq|n|\leq 2\beta} \frac{1}{|n|} \ll 1 + \log(\beta + 1),$$

donde se han aproximado sumas por integrales (una versión débil del Lema de Abel). Sustituyendo en (2.2) e integrando por partes los términos con $0 = \alpha \leq n \leq \beta$ se obtiene la fórmula buscada salvo un término de frontera que es absorbido por $O(\log(\beta + 1))$. ■

Respecto al principio de fase estacionaria, más adelante veremos un resultado más preciso, pero todo lo que se necesita para demostrar el teorema es la segunda parte del siguiente ingenioso y sencillo lema:

Lema 2.3 (Lemas de van der Corput)**.** *Sea $f \in C^2([a, b])$ con $f''(x) \neq 0$ en $[a, b]$.*

a) Si $|f'| \geq \lambda_1 > 0$, se cumple

$$\left| \int_a^b e(f(x))\,dx \right| \leq \frac{2}{\pi\lambda_1}.$$

b) Si $|f''| \geq \lambda_2 > 0$, se cumple

$$\left| \int_a^b e(f(x))\,dx \right| \leq \frac{4\sqrt{2}}{\sqrt{\pi\lambda_2}}.$$

DEM.: *a)* Integrando por partes tomando $u = 1/f'$ y $dv = f' e(f)\,dx$ (nótese que u es

monótona)

$$\left|\int_a^b e(f(x))\,dx\right| \le \frac{1}{\pi\lambda_1} + \frac{1}{2\pi}\int_a^b |u'| \le \frac{2}{\pi\lambda_1}.$$

b) Sea c tal que f alcance un máximo o un mínimo en $x=c$, en particular, $f'(c)=0$. Quizá extendiendo la definición de f más allá de $[a,b]$ siempre se puede suponer que tal valor existe. Sea $I=[c-\delta,c+\delta]\cap[a,b]$ con $\delta=\sqrt{2}/\sqrt{\pi\lambda_2}$ y $J=[a,b]-I$. Este último conjunto está formado a lo más por dos intervalos, en los que se aplica el apartado *a)*, teniéndose:

$$\left|\int_a^b e(f(x))\,dx\right| \le \frac{2}{\pi|f'(c-\delta)|} + \frac{2}{\pi|f'(c-\delta)|} + \left|\int_I e(f(x))\,dx\right|.$$

Por otra parte $|f'(c\pm\delta)| = |\int_c^{c\pm\delta} f''| \ge \delta\lambda_2$ prueba que el segundo miembro es menor o igual que $2\sqrt{2}/\sqrt{\pi\lambda_2}$. Añadiendo la acotación trivial sobre I, se concluye la demostración. ■

El teorema es la combinación de los dos resultados anteriores.

Dem. (del Teorema 2.1): Por el teorema del valor medio se pueden tomar en la Proposición 2.2 α y β con $\beta-\alpha \ll \lambda_2 N+1$. Según el Lema 2.3 *b)* cada una de las integrales es $O(\lambda_2^{-1/2})$, de forma que

$$\sum_{n\in I} e(f(n)) \ll (\lambda_2 N+1)\lambda_2^{-1/2} + \log(\lambda_2 N+2).$$

Si $\lambda_2 \le 1$ el término logarítmico se puede suprimir; mientras que si $\lambda_2 > 1$ el teorema es trivial. ■

La acotación del Lema 2.3 *b)* se puede transformar en una aproximación, más que en una acotación, a cambio de algunas condiciones sobre f y de una pueba más compleja **[Gr-Ko]** que requiere hacer explícito el principio de fase estacionaria.

Proposición 2.4. *Sea $f\in C^4([a,b])$ con $0<\lambda_2<|f''|$, $|f'''|<\lambda_3$ y $|f^{(iv)}|<\lambda_4$. Si existe $c\in[a+\lambda_2^{-1/2}, b-\lambda_2^{-1/2}]$ con $f'(c)=0$, entonces se cumple*

$$\int_a^b e(f(x))\,dx = \frac{e(f(c)\pm 1/8)}{\sqrt{|f''(c)|}} + O\big(\lambda_2^{-1}(c-a)^{-1} + \lambda_2^{-1}(b-c)^{-1} + (b-a)\lambda_2^{-3}(\lambda_4\lambda_2+\lambda_3^2)\big),$$

donde el signo $\pm$ se elige de manera que coincida con el de f''.

2.3. El truco de Weyl (y van der Corput)

Cuando uno trata de probar algo, parte del oficio radica en reconocer al *enemigo* al que tiene que enfrentarse. Veamos dónde se oculta éste en la acotación básica de van der Corput.

Si aplicamos el Teorema 2.1 cuando λ_2 es comparable a $1/N$ estamos en el caso óptimo, por ejemplo, para las sumas de Gauss se obtiene $|G| = |\sum_{n\leq N} e(n^2/N)| \ll N^{1/2}$ que es el orden correcto según la fórmula exacta dada por Gauss para estas sumas, la cual es tan interesante que mereció un lugar en su famoso diario **[Ga]**. Sin embargo, si $\lambda_2 \gg 1$ o $\lambda_2 \ll N^{-2}$, como ocurre por ejemplo en $\sum_{N\leq n<2N} e(n^3/N)$, sólo se obtiene la cota trivial.

Si λ_2 es muy pequeño, entonces la derivada permanece casi constante. Estas condiciones son óptimas para aplicar la fórmula de sumación de Poisson (en la forma de la Proposición 2.2) y se obtiene una aproximación de la suma por una integral, lo cual es muy ventajoso. Sin embargo, si λ_2 es muy grande la derivada vive en un intervalo demasiado extenso como para que se pueda obtener algo provechoso a partir de la fórmula de sumación de Poisson. Identificando la derivada con la frecuencia, vemos que el *enemigo* está en una variación incontrolada de las frecuencias. Se muestra necesario un método para actuar sobre las frecuencias si queremos superar el Teorema 2.1.

En un famoso trabajo **[We]**, Weyl necesitó en 1916 acotar sumas del tipo $\sum e(P(n))$ donde P es un polinomio con coeficiente principal irracional. Esto es fácil para grado uno (porque se tiene la suma de una progresión geométrica). En el resto de los casos Weyl empleó un truco sencillísimo que consistía en que al hallar el cuadrado del módulo se obtienen incrementos de las fases, y el incremento ("derivada") de un polinomio de grado k es otro de grado $k-1$. Por ejemplo, si $S = \sum_{n\in I} e(\alpha n^2)$

$$|S|^2 = \sum_n \sum_m e(\alpha(m^2-n^2)) \underset{m=n+r}{=} \sum_r \sum_n e(2\alpha nr + r^2\alpha) \leq \sum_r |\sum_n e(2\alpha nr)|.$$

Lo malo de este truco es que es demasiado algebraico. Si lo aplicamos a $\sum e(f(n))$ no funciona si f no es un polinomio o algo demasiado parecido. Si pensamos en desarrollos de Taylor, la mayoría de las funciones con que tratamos habitualmente son algo así como polinomios de grado infinito. Hay además un problema más básico. Excepto para los valores de r pequeños, típicamente tan enemigo es $f(n)$ como $f(n+r)-f(n)$. Si pudiéramos limitar el rango en el que se mueve r, podríamos controlar mejor la oscilación de $e(f(n+r)-f(n))$ que la de $e(f(n))$. Van der Corput materializó esta idea con algo muy similar a subdividir la suma en sumas cortas (véase la siguiente demostración) de modo que al

elevar cada una al cuadrado sólo aparezcan incrementos pequeños. Todo se resume en el siguiente resultado.

Lema 2.5 . *Sean $a, b \in \mathbb{Z}$ y $H \in \mathbb{Z}^+$ tales que $H \leq b - a$. Para cualquier función $f : [a, b] \longrightarrow \mathbb{R}$ se tiene*

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

Dem.: Para cada $n \in \mathbb{Z}$ definimos $I_n = [1, H] \cap [a - n, b - n] \cap \mathbb{Z}$. El truco está en trasladar la suma H veces y agrupar los sumandos de H en H que es lo que mide típicamente I_n:

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

Ahora al aplicar Cauchy-Schwarz se obtienen incrementos de f en un intervalo controlado por H:

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

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:

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

Ahora basta "limpiar" esta desigualdad con los cambios de variable $m - l \mapsto r$, $l + n \mapsto n$ y empleando $b - a \leq H$. ■

2.4. Pares de exponentes. Un bonito envoltorio para un dolor de cabeza

Según se desprende de la sección anterior, la idea para ir más allá de la acotación básica de van der Corput es dominar el crecimiento de las frecuencias con el Lema 2.5 (quizá aplicado repetidas veces) para poder emplear la fórmula de sumación de Poisson en condiciones adecuadas. Si en vez de acotar las integrales resultantes se las aproxima con la

Proposición 2.4, se obtiene una nueva suma trigonométrica, que se puede tratar de nuevo de la misma forma refinando la estimación, y así sucesivamente.

El problema es que si se quiere resumir todo este proceso en un teorema general, escribir las condiciones de regularidad y los resultados que se obtienen es un dolor de cabeza. La solución es considerar una clase de funciones extremadamente restricitiva en la que todas las frecuencias que puedan aparecer estén bajo control, y utilizar un lenguaje adecuado en el que cada paso esté representado por sencillas fórmulas inductivas.

Nótese en primer lugar que el teorema del valor medio sugiere que para funciones "normales" la derivada $k+1$-ésima sea como la k-ésima divida por la longitud del intervalo donde está definida, y el teorema de la función inversa (en una variable) sugiere que las inversas de las derivadas tienen una propiedad similar. Con esta idea en mente, definimos el escenario en el que vamos a trabajar.

Diremos que $f \in \mathcal{F}$ si $|f^{(k)}|/|I| \ll |f^{(k+1)}| \ll |f^{(k)}|/|I|$, $k \in \mathbb{Z}^+$, donde I es el intervalo de definición de f, y si además una desigualdad similar se cumple al cambiar f por la función inversa de $f^{(r)}$, $r \in \mathbb{Z}^+$, e I por su intervalo de definición. Por ejemplo, $f(x) = \lambda/x$ con $I = [N, 2N]$, donde λ es un parámetro, pertenece a $\mathcal{F}$.

Como vimos, el "enemigo" para acotar una suma trigonométrica está en la variación incontrolada de las frecuencias, que en $\mathcal{F}$ depende del tamaño de la derivada primera. Además hay otro enemigo tan patente que es casi vecino, y es que las sumas más largas requerirán acotaciones mayores. Con estos obstáculos identificados, diremos que $(p, q) \in [0, 1] \times [0, 1]$ es un *par de exponentes* si para toda $f \in \mathcal{F}$ definida en un intervalo I de longitud N con $1 < D \ll |f'| \ll D$, se cumple

$$\Big|\sum_{n\in I} e(f(n))\Big| \ll D^p N^q.$$

Obviamente $(0, 1)$ es un par de exponentes.

Una vez que hemos escondido bajo la alfombra todos los posibles problemas de regularidad y hemos dado con el *envoltorio* adecuado, podemos enunciar los dos resultados que constituyen la teoría de pares de exponentes.

Teorema 2.6 (Proceso A). *Si (p, q) es un par de exponentes entonces*

$$(p', q') = \Big(\frac{p}{2p+2}, \frac{p+q+1}{2p+2}\Big)$$

también lo es.

Teorema 2.7 (Proceso B). *Si (p, q) es un par de exponentes entonces*

$$(p', q') = (q - \frac{1}{2}, p + \frac{1}{2})$$

también lo es.

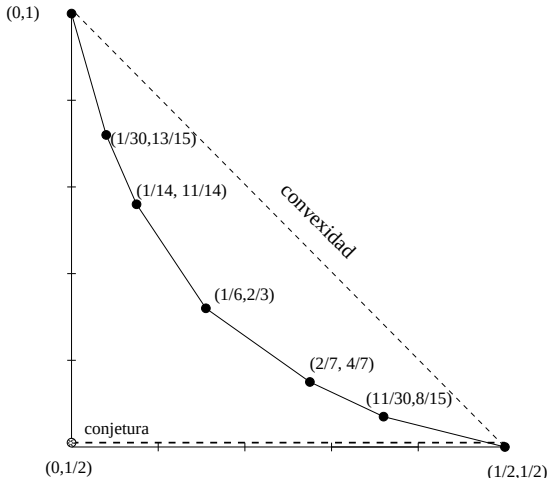
A veces se menciona como *Proceso C* la convexidad, esto es, que si (p_1, q_1) y (p_2, q_2) son pares de exponentes cualquier punto del segmento que los une también lo es (esto no es más que tomar medias geométricas).

Partiendo del par de exponentes trivial $(0, 1)$ podemos obtener infinitos pares de exponentes aplicando repetidas veces las funciones A y B que definen los procesos anteriores. Éstos son los llamados *pares de exponentes de van der Corput* (se sabe que hay pares de exponentes que no pueden ser obtenidos de esta forma). Algunos de ellos son:

$$\begin{array}{ccc} \left(\frac{1}{2}, \frac{1}{2}\right) = B(0,1), & \left(\frac{1}{6}, \frac{2}{3}\right) = AB(0,1), & \left(\frac{1}{14}, \frac{11}{14}\right) = A^2B(0,1), \\ \left(\frac{2}{7}, \frac{4}{7}\right) = BA^2B(0,1), & \left(\frac{11}{30}, \frac{8}{15}\right) = BA^3B(0,1), & \left(\frac{1}{9}, \frac{13}{18}\right) = ABABAB(0,1). \end{array}$$

Por ejemplo, si quisiéramos acotar por ejemplo $S = \sum_{N \leq n \leq 2N} e(N^3/n)$, el Teorema 2.1, que corresponde en cierta forma al par de exponentes $(1/2, 1/2)$, no sirve de nada; mientras que el par $(1/6, 2/3)$ permite concluir $|S| \ll N^{5/6}$ que rebaja en un factor $N^{1/6}$ la acotación trivial.

Geométricamente el Proceso B es una simetría por la recta $y = x + 1/2$ y el Proceso A atrae los pares de exponentes hacia el trivial $(0, 1)$. De esta forma los pares de exponentes de van der Corput se sitúan en una curva que une $(0, 1)$ y $(1/2, 1/2)$, y que supera a la convexidad entre ellos



Con métodos avanzados que mencionaremos más adelante se ha probado que hay pares

de exponentes que mejoran los de van der Corput. Aunque esto es teóricamente muy significativo, lo cierto es que las diferencias numéricas son levísimas (unas milésimas en p y q en el mejor de los casos). Cabe preguntarse si es posible esperar algo mejor. Considerando la norma 2 en λ de $\sum_{N<n\leq 2N} e(\lambda/n)$ es fácil ver que necesariamente siempre $q \geq 1/2$, y tomando $\lambda = (2N)!$, que $p = 0$ sólo se verifica para el par de exponentes trivial. Por otra parte, incluso si la oscilación de $S = \sum_{n\leq N} e(f(n))$ fuera totalmente alocada y $e(f(n))$ no tuviera "nada que ver" con $e(f(n+1))$, el teorema central del límite sugiere para $S/\sqrt{N}$ una distribución normal cuando $N \to \infty$, lo que motiva conjeturar que cualquier exponente por encima de $1/2$ es válido. Es decir, la conjetura es que $(\epsilon, 1/2+\epsilon)$ es par de exponentes para todo $\epsilon > 0$. Con ella se podrían resolver algunos antiguos problemas.

La demostración de ambos procesos consiste en unir las piezas formadas por los resultados anteriores. El proceso A se sigue del Lema 2.5.

DEM.(Proceso A): La función $g(n) = f(n+h) - f(n)$ verifica $hDN^{-1} \ll |g'| \ll hDN^{-1}$. Si suponemos que podemos aplicar el par de exponentes (p, q), por el Lema 2.5 se sigue

$$|S|^2 \ll N^2H^{-1} + NH^{-1}\sum_h (hDN^{-1})^p N^q \ll N^2H^{-1} + H^pD^pN^{1-p+q}. \tag{2.3}$$

Escogiendo $H^{p+1} = D^{-p}N^{1+p-q}$ para que ambos sumandos sean iguales, se obtiene $|S| \ll D^{p'}N^{q'}$.

La demostración es *tramposa* (incompleta) porque cuando h es pequeño puede que la derivada de g' sea pequeña y no se ajuste a los requerimientos de la teoría de pares de exponentes ($1 \ll |g'|$). Para solucionarlo se separan los términos con $h \leq \epsilon N/D$ (para los que $|g'| \ll \epsilon$). Por el Teorema 2.1 la contribución de esos términos a (2.3) es $\ll NH^{-1}\cdot(\epsilon N/D)^{1/2}\cdot D^{-1/2}N$. Si $D > N^{1/2}$ esto es $O(N)$ que claramente no influye en la acotación anterior ($q' > 1/2$). Y si $D \leq N^{1/2}$, el Teorema 2.1 aplicado a la suma original implica $|S| \ll D^{1/2}N^{1/2} \leq D^{p'}(N^{1/2})^{1-p'}N^{1/2}$, y es fácil comprobar que $\frac{1}{2}(1-p') + \frac{1}{2} \leq q'$. ■

El segundo proceso consiste en proceder como en la prueba del Teorema 2.1 pero, en vez de acotar las integrales con el Lema 2.3 *b)*, se aproximan con la Proposición 2.4 para que resulte una nueva suma trigonométrica. Esto es automático salvo por la tediosa tarea de contabilizar la suma de los términos de error, que queda resumida en el siguiente resultado **[Gr-Ko]**, **[Iv]**:

Lema 2.8 . *Sea $f \in C^4([a,b])$, $b-a = N$, con $DN^{-1} \ll |f''| \ll DN^{-1}$, $|f'''| \ll DN^{-2}$ y $|f^{(iv)}| \ll DN^{-3}$. Para cada n en el intervalo J determinado por $f'(a)$ y $f'(b)$ sea c_n tal*

que $g_n(c_n) = 0$ *con* $g_n(x) = f(x) - nx$. *Entonces*

$$\sum_{a\le n\le b} e(f(n)) = \sum_{n\in J} \frac{e(f(c_n) - nc_n \pm 1/8)}{\sqrt{|f''(c_n)|}} + O(D^{-1/2}N^{1/2}) + O(\log(D+2)),$$

donde el signo $\pm$ *se elige para que coincida con el de* f''.

DEM.(Proceso B): Sumando por partes en el lema anterior, se tiene

$$|S| \ll D^{-1/2}N^{1/2}\Big|\sum_{D\ll n\ll D} e(F(n))\Big| + D^{-1/2}N^{1/2} + \log D$$

donde $F(n) = f(c_n) - nc_n$ y $c_n = (f')^{-1}(n)$. Un cálculo con el teorema de la función inversa prueba $F' = -(f')^{-1}$, de modo que $N \ll F' \ll N$. Por hipótesis podemos aplicar el par de exponentes (p, q) a F y se sigue $|S| \ll D^{-1/2}N^{1/2}N^pN^q$. ■

Una crítica bastante razonable que se puede hacer a la teoría de pares de exponentes es que bajo su aparente versatilidad hay que comprobar unas hipótesis que rara vez se dan en la práctica. Sin embargo en muchos casos no es difícil rastrear en la demostración lo que realmente necesitamos relajando enormemente las hipótesis. Por ejemplo, supongamos que queremos emplear el par de exponentes

$$(p, q) = A^jB(0, 1) = \big(\frac{1}{2^{j+2} - 2}, 1 - \frac{j+1}{2^{j+2} - 2}\big).$$

Para aplicar j veces el Proceso A, cada vez hay que controlar una derivada, es decir, requiere $|f^{(k)}|/|I| \ll |f^{(k+1)}| \ll |f^{(k)}|/|I|$ para $k = 1, 2, \ldots, j-1$. La aplicación del Proceso B requiere, en principio, controlar cuatro derivadas más, pero como no vamos a emplear más procesos, bastaría la acotación del Teorema 2.1 (acotar integrales en lugar de estimarlas), lo cual hacen sólo dos derivadas más. Además controlando ambas, podemos suponer que en el Teorema 2.1 el primer término domina al segundo usando en la prueba el apartado *a)* del Lema 2.3 en lugar del *b)*, cuando dé un mejor resultado. Completando este esquema se obtiene:

Proposición 2.9 . *Sea* $f \in C^{j+2}([a, b])$ *con* $b-a = N$, $j \ge 0$. *Si para* $k = 1, 2, \ldots, j+2$ *se cumple* $DN^{1-k} \ll |f^{(k)}| \ll DN^{1-k}$ *con* $D > 1$, *entonces*

$$\Big|\sum_{a\le n\le b} e(f(n))\Big| \ll D^pN^q \qquad con \quad (p, q) = \big(\frac{1}{2^{j+2} - 2}, 1 - \frac{j+1}{2^{j+2} - 2}\big).$$

Para terminar esta sección diremos que en algunas aplicaciones se necesita estimar sumas en más de una dimensión. Por ejemplo del tipo $\sum_{n_1,n_2} e(f(n_1,n_2))$. Siempre se puede congelar una de las variables y acotar sólo la suma en la otra, pero parece que lo natural es que la cancelación aparezca en ambas variables. Es decir, que si la teoría de pares de exponentes nos da D^pN^q para la suma unidimensional, entonces se debería obtener en total $D_1^pN_1^qD_2^pN_2^q$. Todavía hoy esto es una conjetura sólo probada en situaciones tan particulares que restringen la aplicabilidad de una teoría multidimensional de pares de exponentes con hipótesis comparables a las de la unidimensional.

2.5. Gran criba y sumas raras

Hasta ahora nos hemos puesto en un contexto analítico aceptable en el que las fases son funciones suaves con propiedades de regularidad. Sin embargo en las aplicaciones aritméticas esto no es simepre así y nos encontramos con sumas totalmente salvajes como $\sum_{p\leq x} e(f(p))$ donde p recorre los primos. Podemos pasar el problema de las fases a los coeficientes diciendo que la suma anterior es muy parecida a $\sum_{n\leq x} \Lambda(n)e(f(n))/\log n$, pero eso no arregla nada. Evidentemente, no se puede hacer una teoría de sumas trigonométricas con coeficientes generales, porque siempre podríamos elegir los signos de dichos coeficientes para que "conspiren" resonando con $e(f(n))$ y no haya ninguna cancelación. (Tampoco funcionaría ni siquiera pidiendo coeficientes positivos ya que simplemente bastaría provocar las resonancias con los nodos positivos. Sin embargo, como veremos en esta sección, cuando se consideran diversas sumas que comparten los mismos coeficientes y cuyas fases son independientes en cierto sentido, es imposible que haya una conspiración de los coeficientes a gran escala. Esta idea es tan poderosa que incluso sirve para obtener cancelación en $\sum_{p\leq x} e(f(p))$, una vez que se ha escrito, de forma muy ingeniosa, como una suma de varias sumas. Como en tantos otros resultados avanzados, lo fundamental es entender el Álgebra Lineal.

Dada una base ortonormal $\{\vec{u}_1,\vec{u}_2,\dots\vec{u}_d\}$ de $\mathbb{R}^d$, las coordenadas de un vector $\vec{x}$ en esta base son $\vec{x}\cdot\vec{u}_1$, $\vec{x}\cdot\vec{u}_2$,… $\vec{x}\cdot\vec{u}_d$, y por Pitágoras

$$|\vec{x}\cdot\vec{u}_1|^2+|\vec{x}\cdot\vec{u}_2|^2+\ldots+|\vec{x}\cdot\vec{u}_r|^2\leq\|x\|^2 \tag{2.4}$$

para cualquier $r\leq d$, con igualdad si $r=d$. Si uno quiere poner nombres, ésta es la *desigualdad de Bessel*. Evidentemente nada cambia si trabajamos en $\mathbb{C}^d$ en vez de en $\mathbb{R}^d$. Pensemos que $\vec{x}$ es un vector cuyas coordenadas son coeficientes (complejos) arbitrarios a_n con n en cierto intervalo entero, y que cada $\vec{u}_j$ es un vector oscilatorio de coordenadas

$e(f(j,n))$, normalizado para que $\|\vec{u}_j\| = 1$. Con (2.4) podríamos esperar estimar la suma de muchas sumas trigonométricas. Naturalmente esto no es tan fácil porque sería mucha casualidad que estos $\vec{u}_j$ con la f requerida en alguna aplicación práctica fueran ortogonales. El enemigo que hay que evitar aquí es que los $\vec{u}_j$ apunten más o menos en la misma dirección, en ese caso (2.4) es radicalmente falsa. Por otra parte, tampoco parece muy probable que el enemigo asome muchas veces, porque eligiendo unos cuantos vectores al azar, un número menor que la dimensión, hay probabilidad cero de que sean linealmente dependientes. Lo que buscamos es algo intermedio que diga que si los $\vec{u}_j$ son un poco ortogonales, digamos *cuasiortogonales* para quedar bien, entonces (2.4) es más o menos cierto, salvo alguna constante. Desde el punto de vista de las sumas trigonométricas la conclusión que queremos obtener es

cuasiortogonalidad $\Rightarrow$ cancelación

Si definimos la matriz B cuyas columnas son las coordenadas de $\vec{u}_1$, $\vec{u}_2$,... $\vec{u}_r$, entonces (2.4) se escribe de forma más breve como $\|\vec{x}^t B\|^2 \leq \|\vec{x}\|^2$ y aplicando la desigualdad de Cauchy-Schwarz, esto equivale a $|\vec{x}^t B\vec{y}|^2 \leq \|\vec{x}\|^2\|\vec{y}\|^2$, de modo que también se puede entender (2.4) como una desigualdad para ciertas formas bilineales. En el caso de (2.4), la matriz B tiene sus columnas ortonormales (es unitaria, en caso de que sea cuadrada). El siguiente sencillo lema dice en cuánto falla $|\vec{x}^t B\vec{y}|^2 \leq \|\vec{x}\|^2\|\vec{y}\|^2$, y por tanto (2.4), en función de lo lejos que esté B de tener columnas ortonormales.

Lema 2.10 . *Sea $B = (b_{ij})_{i=1,\,j=1}^{s,\,r}$ una matriz de números complejos. Entonces para cada $\vec{x} \in \mathbb{C}^s$ e $\vec{y} \in \mathbb{C}^r$, se cumple*

$$|\vec{x}^t B\vec{y}|^2 \leq \Delta(B)\|\vec{x}\|^2\|\vec{y}\|^2$$

donde

$$\Delta(B) = \max_j \sum_{k=1}^{r} \Big| \sum_{i=1}^{s} b_{ij}\overline{b}_{ik} \Big|.$$

DEM.: Por la desigualdad de Cauchy-Schwarz

$$|\vec{x}^t B\vec{y}|^2 \leq \|\vec{x}\|^2\|B\vec{y}\|^2 = \|\vec{x}\|^2 \sum_i \Big| \sum_j b_{ij}y_j \Big|^2 = \|\vec{x}\|^2 \sum_{j,k} y_j\overline{y}_k \sum_i b_{ij}\overline{b}_{ik}.$$

Por la desigualdad aritmético-geométrica $|y_j\overline{y}_k| \leq (|y_j|^2 + |\overline{y}_k|^2)/2$, se tiene

$$|\vec{x}^t B\vec{y}|^2 \leq \frac{1}{2}\|\vec{x}\|^2 \Big(\sum_j |y_j|^2 \sum_k \Big| \sum_i b_{ij}\overline{b}_{ik} \Big| + \sum_k |y_k|^2 \sum_j \Big| \sum_i b_{ij}\overline{b}_{ik} \Big| \Big).$$

Los dos sumandos dentro del paréntesis son iguales (basta intercambiar el nombre de las variables mudas k y j), y es evidente que el primero de ellos está acotado por $\Delta(B)$. ■

El análogo de (2.4) cuando los $\vec{u}_j$ (las columnas de B) no son ortornormales, es ahora inmediato.

Corolario 2.11. *Con la notación anterior*

$$\|\vec{x}^t B\|^2 \leq \Delta(B)\|\vec{x}\|^2.$$

DEM.: Basta tomar $\vec{y}^t = \vec{x}^t B$. ■

Hagamos un pequeño receso para probar lo que se llama (por razones históricas) lema de gran criba, el cual está relacionado con la acotación de una suma de sumas trigonométricas, que consideramos primero en una forma suavizada

$$S = \sum_{j=1}^{r} \Big| \sum_n a_n g(n/N) e(nx_j) \Big|^2$$

donde $g \in C_0^\infty$ y los a_n son coeficientes arbitrarios. Evidentemente si los x_j son muy parecidos (módulo 1) no hay esperanza de obtener una cota no trivial porque los único que hacemos es repetir la misma suma. Supongamos, por tanto, que los x_j están δ-*espaciados módulo* 1, es decir, que $|||x_j - x_k||| \geq \delta$ para $j \neq k$; donde $||| \cdot |||$ indica la distancia al entero más cercano. Según el corolario anterior, eligiendo $\vec{x}$ de coordenadas a_n y $b_{nj} = g(n/N)e(nx_j)$, se tiene $S \leq \Delta(B) \sum |a_n|^2$. Aplicando la fórmula de sumación de Poisson e integrando por partes dos veces, o usando la acotación trivial si fuera mejor, se tiene

$$\Big| \sum_n g^2(n/N) e(n(x_j - x_k)) \Big| \ll \min(N, N^{-1}|||x_j - x_k|||^{-2})$$

donde la constante "$\ll$" sólo depende de g. De aquí es fácil deducir

$$\Delta(B) \ll N + \sum_l \min(N, N^{-1}(l\delta)^{-2}) \ll N + \delta^{-1}.$$

De modo que $S \ll (N + \delta^{-1}) \sum |a_n|^2$. Nótese que siempre podemos hacer desaparecer la función regularizante $g(n/N)$ en S eligiéndola de manera que sea uno en cierto intervalo y escogiendo los a_n nulos fuera de él. De modo que hemos probado (véase una prueba más directa en **[Da]**):

Lema 2.12 (gran criba)**.** *Sean x_1, x_2,... x_r números reales con $|||x_j - x_k||| \geq \delta$ para*

$j \neq k$. Existe una constante absoluta C tal que cualquiera que sean $a_n \in \mathbb{C}$ se cumple

$$\sum_{j=1}^{r} \Big| \sum_{n \leq N} a_n e(n x_j) \Big|^2 \leq C(N + \delta^{-1}) \sum |a_n|^2.$$

Nota: Se puede probar que $C = 1$ es una constante válida (y óptima).

Para comprobar la precisión de este resultado, obsérvese que si obligamos a que los coeficientes conspiren tomando $a_n = e(-n x_{j_0})$ para hacer la suma interior con $j = j_0$ tan grande como $N \sum |a_n|^2$, el lema anterior nos dice que, siempre que δ no sea muy pequeño, las otras sumas se vuelve mágicamente pequeñas. Obérvese también que si los x_j están equidistribuidos en $[0, 1]$ con $x_{j+1} - x_j = \delta$, para $\delta \to 0$ se obtiene la desigualdad de Bessel para series de Fourier.

Después de este desvío veamos cómo se pueden estimar sumas sobre primos. Nos centraremos en

$$S = \sum_{n \leq N} \Lambda(n) e(f(n)),$$

que salvo un término de error pequeño se relaciona fácilmente con $\sum_{p \leq N} e(f(p))$ sumando por partes, como se hizo con $\psi(x)$ y $\pi(x)$.

La idea original de Vinogradov para tratar esta última suma **[El]** fue elegir $\mathcal{P}$ como el producto de los primos menores que $N^{1/2}$ y escribir

$$\sum_{N^{1/2} < p \leq N} e(f(p)) = \sum_{i | \mathcal{P},\, i \leq N} \mu(i) \sum_{j \leq N/i} e(f(ij))$$

(donde μ es la función de Möbius). Lo cual no es más que la criba de Eratóstenes (esto explica en parte de dónde vino el nombre de "gran criba"). Con ello tenemos una suma de sumas y según la idea anterior, todo lo que hay que hacer es controlar $\sum_k |\sum_i e(f(ij) - f(ik))|$, lo cual es factible. El problema técnico que aparece es que si i es próximo a N, la suma es muy corta y no se puede medir la cancelación (para $r = 1$ el Lema 2.10 es trivial). Sin embargo este caso no debería ser tan malo porque es de esperar que entonces la cancelación aparezca al sumar en i clasificando los valores dependiendo del signo de $\mu(i)$. Reordenar la suma como hizo Vinogradov para que apareciesen siempre sumas largas, lleva a complicaciones muy tediosas. En 1977 Vaughan consiguió dosificar y ocultar el aburrimiento pasándolo todo a una identidad, que por otra parte es trivial si uno tapa el enunciado y mira su demostración.

Identidad de Vaughan. *Para $N_1, N_2 \in \mathbb{Z}^+$ con $N_1 N_2 \leq N$, y cualquier función g, se cumple*

$$\sum_{n \leq N} \Lambda(n) g(n) = S_1 + S_2 + S_3 + S_4$$

donde

$$S_1 = \sum_{i \leq N_1} \Lambda(i) g(i), \qquad S_2 = - \sum_{i \leq N_1 N_2} \Big(\sum_{\substack{l \leq N_1,\ m \leq N_2 \\ lm = i}} \mu(m) \Lambda(l) \Big) \sum_{k \leq N/i} g(ik),$$

$$S_3 \sum_{i \leq N_2} \mu(i) \sum_{k \leq N/i} g(ik) \log k, \qquad S_4 = - \sum_{N_1 < i < N/N_2} \Lambda(i) \sum_{N_2 < j \leq N/i} \Big(\sum_{l \mid j,\ l \leq N_2} \mu(l) \Big) g(ij).$$

La identidad puede ser apabullante, pero la prueba consiste simplemente en partir de la siguiente trivialidad

$$-\frac{\zeta'(s)}{\zeta(s)} = F(s) - \zeta(s) F(s) G(s) - \zeta'(s) G(s) + \big(- \frac{\zeta'(s)}{\zeta(s)} - F(s) \big) (1 - \zeta(s) G(s))$$

con $F(s) = \sum_{n \leq N_1} \Lambda(n) n^{-s}$ y $G(s) = \sum_{n \leq N_2} \mu(n) n^{-s}$. Comparando los coeficientes de n^{-s} en cada miembro y multiplicándolos por $g(n)$ y sumando, después de cansarse un rato, se obtiene el resultado deseado.

Con esta maquinaria ya estamos pertrechados para pasar sumas trigonométricas sobre primos a sumas sobre enteros que se pueden tratar con las técnicas de van der Corput. Enunciaremos el resultado general y dejaremos la aplicación en algún caso concreto para un capítulo posterior.

Proposición 2.13 . *Sea $g(n) = e(f(n))$ si $1 \leq n \leq N$ y cero en otro caso. Para cualquier $N_1, N_2 \in \mathbb{Z}^+$ con $N_1 N_2 \leq N$, se cumple*

$$\sum_{n \leq N} \Lambda(n) e(f(n)) \ll N_1 + \log N \sum_{i \leq N_1 N_2} \Big| \sum_{k \leq N/i} g(ik) \Big|$$

$$+ N^{1/2} \log^3 N \max_{N_1 < I \leq N/N_2} \max_{N_2 \leq j \leq N/I} \Big(\sum_{N_2 < k \leq N/I} \Big| \sum_{I < i \leq 2I} g(ij)\, \overline{g}(ik) \Big| \Big)^{1/2}.$$

Dem.: Estimando trivialmente S_1 se obtiene el primer término del segundo miembro,

N_1. Usando que $|\mu(m)| \leq 1$ y que $\sum_{l|n} \Lambda(l) = \log n$ **[Ci-Co]**, de S_2 se obtiene el segundo término, y S_3 se acota de la misma forma. Antes de tratar S_4, se divide en intervalos diádicos el rango de i, esto es, se considera $I < i \leq 2I$ con I una potencia de dos, $N_1 < I < N/N_2$. Entonces, teniendo en cuenta que hay $O(\log N)$ intervalos diádicos,

$$|S_4| \ll \log N \max_{N_1 < I \leq N/N_2} \Big| \sum_{I < i \leq 2I} \sum_{N_2 < j \leq N/i} \Lambda(i) a_j g(ij) \Big|$$

con $|a_j| \leq d(j)$ el número de divisores de j. Aplicando el Lema 2.10 y las acotaciones elementales (pero no del todo inmediatas **[Da]**) $\sum_{i \leq x} \Lambda^2(i) \ll x \log x$ y $\sum_{j \leq x} d^2(j) \ll x \log^3 x$, se concluye la prueba. ■

2.6. Introducción a otros métodos

Esta sección en parte prolonga la anterior porque mencionaremos con cierto detalle dos métodos que emplean las ideas de la gran criba.

El primero es el *método de Vinogradov* (que históricamente precedió a la gran criba) y que fue desarrollado en múltiples variantes por I.M. Vinogradov. Desde el punto de vista de los pares de exponentes permite crear algunos muy próximos al trivial $(0, 1)$ que mejoran los de van der Corput (véanse las notas al capítulo 6 de **[Ti]**), lo cual es útil para tratar series que están al borde de la convergencia, como ocurre con $\zeta(1 + it)$. No es extraño, por consiguiente, que el método de Vinogradov dé lugar a las mejores regiones libres de ceros conocidas. Sin embargo es más fácil exponer las ideas básicas cuando se aplica a sumas trigonométricas $\sum e(f(n))$ con f un polinomio. Si los coeficientes de f son enteros no hay cancelación, y lo mismo ocurre, por la periodicidad, si son racionales de denominador pequeño. De modo que las acotaciones dependerán de propiedades de aproximación diofántica de los coeficientes (normalmente sólo se consideran las del principal).

Digamos que $f(n) = \alpha_k n^k + \alpha_{k-1} n^{k-1} + \ldots + \alpha_1 n + \alpha_0$. Siguiendo la idea de Weyl y van der Corput al comienzo de la demostración del Lema 2.5, para estimar $\sum e(f(n))$ podemos emplear

$$\frac{1}{H} \sum_n \Big| \sum_{m \leq H} e(f(m+n)) \Big| = \frac{1}{H} \sum_n \Big| \sum_{m \leq H} e(\alpha_k m^k + A_{k-1}(n) m^{k-1} + \ldots + A_2(n) m^2 + A_1(n) m) \Big|$$

donde A_i son funciones de n que dependen de los α_j, por ejemplo, $A_{k-1}(n) = nk\alpha_k + \alpha_{k-1}$. Si α_k no es racional con denominador pequeño cabe esperar cierto espaciamiento entre los valores de $A_{k-1}(n)$, lo que sugiere utilizar alguna variante de la gran criba. Sin embargo esto no puede dar buen resultado porque m^{k-1} crece demasiado deprisa en comparación

con m, para $k > 2$,lo que correspondería, en algún sentido, a tener que tomar en el Lema 2.12 todos los a_n nulos salvo una proporción despreciable. Para ser más concretos con un ejemplo, si quisiéramos aplicar el lema de gran criba por ejemplo a una suma del tipo

$$S = \sum_{j=1}^{r} \Big| \sum_{m \le M} c_m e(m^2 x_j) \Big|^2 \qquad \text{con } c_m \in \{-1, 1\},$$

habría que tomar $N = M^2$ y $a_n = c_{\sqrt{n}}$ si n es un cuadrado, $n \le N$, y $a_n = 0$ en otro caso. El resultado sería entonces $S \ll (M^2 + \delta^{-1})M$ que es trivial para $r \le M$. Para ir más allá, apliquemos la desigualdad de Cauchy-Schwarz y desarrollemos el cuadrado, obteniendo

$$S^2 \le r \sum_{j=1}^{r} \Big| \sum_{n \le 2M^2} b_n e(n x_j) \Big|^2 \qquad \text{con } |b_n| = O(n^\epsilon) \ \ \forall \epsilon > 0;$$

ya que $|\{(a, b) \in \mathbb{Z}^2 : n = a^2 + b^2)\}| = O(n^\epsilon)$. La gran criba implica ahora $S \ll r^{1/2}(M^2 + \delta^{-1})^{1/2} M^{1+\epsilon}$, que mejora la acotación anterior si r no es muy grande.

Análogamente, la idea inicial del método de Vinogradov es aplicar la desigualdad de Hölder para completar los huecos entre diferentes potencias. Para $l \in \mathbb{Z}^+$

$$\sum_{n} \Big| \sum_{m \le H} e(f(m+n)) \Big|^{2l} = \sum_{n} \sum_{m_1, \ldots, m_k} \Big| a(m_1, \ldots, m_k) e(\alpha_k m_k + \ldots + A_1(n) m_1) \Big|^2$$

donde $a(m_1, \ldots, m_k)$ es el número de soluciones enteras $1 \le x_1, x_2, \ldots, x_l \le H$ de

$$x_1^k + x_2^k + \ldots + x_l^k = m_k, \quad x_1^{k-1} + x_2^{k-1} + \ldots + x_l^{k-1} = m_{k-1}, \quad x_1 + x_2 + \ldots + x_l = m_1.$$

Si se hace crecer l, se van cubriendo muchos de los posibles valores de los m_i y la aplicación de la gran criba (en varias dimensiones) será ventajosa. Por otra parte el control en media de los $a(m_1, \ldots, m_k)$ conlleva estudiar las diversas sumas de potencias i-ésimas que pueden dar los mismos m_i, es decir el número $\mathcal{J}(H)$ de soluciones del sistema

$$\begin{aligned} x_1^k + x_2^k + \ldots + x_l^k &= x_{l+1}^k + x_{l+2}^k + \ldots + x_{2l}^k \\ x_1^{k-1} + x_2^{k-1} + \ldots + x_l^{k-1} &= x_{l+1}^{k-1} + x_{l+2}^{k-1} + \ldots + x_{2l}^{k-1} \\ \ldots \quad \ldots \qquad & \qquad \ldots \quad \ldots \\ x_1 + x_2 + \ldots + x_l &= x_{l+1} + x_{l+2} + \ldots + x_{2l} \end{aligned}$$

con $1 \le x_1, \ldots, x_{2l} \le H$. Esto es un problema aritmético complicadísimo en los rangos relevantes, pero Vinogradov fue capaz de acotar convenientemente $\mathcal{J}(H)$ con lo que se ha

dado en llamar el *teorema del valor medio de Vinogradov*. El nombre, un poco confuso, proviene de que $\mathcal{J}(H)$ se puede expresar como el "promedio":

$$\mathcal{J}(H) = \int_0^1 \dots \int_0^1 \Big| \sum_{m \leq H} e(a_k m^k + a_{k-1} m^{k-1} + \dots + a_1 m) \Big|^{2l} da_1 \dots da_k.$$

La prueba de dicho teorema es muy compleja **[Va]**, **[Iv]**, **[El]**. Esencialmente se basa en estudiar el sistema módulo p para relacionar de alguna manera diferentes soluciones y poder llevar a cabo un esquema inductivo.

Para terminar analizaremos brevemente un método basado en un trabajo de 1986 de Bombieri e Iwaniec que permite crear nuevos pares de exponentes. En particular, con sus técnicas se puede probar que $(9/56 + \epsilon, 37/56 + \epsilon)$ es un par de exponentes para todo ϵ, además no es de van der Corput en general porque para éstos $p + q > 0'829$ **[Gr-Ko]**. Las ideas del método han sido aplicadas fructíferamente por Huxley **[Hu]** a problemas de puntos del retículo dando lugar a lo que se denomina el método discreto de Hardy y Littlewood. Aquí seguiremos las líneas del artículo original en el que las sumas de Gauss desempeñan un papel importante (lo que no ocurre en el método discreto de Hardy y Littlewood).

El punto de partida es como antes el paso

$$\sum_{N < n \leq 2N} e(f(n)) \quad \longrightarrow \quad \frac{1}{H} \sum_n \Big| \sum_{m \leq H} e(f(m+n)) \Big|.$$

Para funciones con f''' que no sea pequeña el par de exponentes $(9/56 + \epsilon, 37/56 + \epsilon)$ no sirve de nada (por ejemplo, si $|f'''| \approx DN^{-2} > N^{-2/3}$, el par de exponentes de van der Corput $(1/9, 13/18)$, sería mejor). Esto motiva entender f como una perturbación de un polinomio de segundo grado y pasar a estudiar

$$\sum_n \Big| \sum_m e(f'(n)m + \frac{1}{2} f''(n) m^2) g(m) \Big|$$

donde g es una función adaptada a un intervalo de longitud comparable a H multiplicada por otra que oscila menos que el polinomio cuadrático (en el artículo original $g(m)$ es, salvo una función de corte, $e(\mu n^3)$ con μ pequeño). Ahora, para cada n, se aproxima $\frac{1}{2} f''(n)$ por una fracción irreducible a/c y se halla b tal que b/c aproxime a $f'(n)$. En rangos

apropiados esto se puede hacer con precisión según conocidos teoremas de aproximación diofántica [**Ha-Wr**], [**Ci-Co**]. De esta forma se pasa a

$$\sum_{a,c} \big| \sum_{m} e\big(\frac{am^2+bm}{c}\big) g(m) \big|.$$

Si se divide la suma interior en clases de congruencia módulo c y se aplica la fórmula de sumación de Poisson en la forma $\sum_{m \equiv d \ (c)} f(m) = c^{-1} \sum_m e(dm/c) \widehat{f}(m/c)$, se llega a

$$\sum_{a,c} \frac{1}{c} \big| \sum_{m} G(a, b+m; c) \widehat{g}(m/c) \big| \quad \text{donde} \ \ G(a,k;c) = \sum_{l=1}^{c} e\big(\frac{al^2+kl}{c}\big).$$

La suma G es una *suma de Gauss*. Se conoce que, salvo en unos casos especiales en que aparece un factor constante extra, $|G| = \sqrt{c}$ pero el signo de $G(a, b+m; c)$ varía con m de una manera demasiado aritmética. Concretamente, para c impar (en el caso par hay fórmulas similares)

$$G(a, b+m; c) = e\big(-\frac{\overline{a}}{c}(b+m)^2\big) G(a, 0; c)$$

donde $\overline{a}$ es el inverso de a módulo c. Olvidarse de los signos tomando valores absolutos implica no ir más allá del método de van der Corput (aplicar Poisson), pero conservarlos conlleva enfrentarse a sumas intratables del tipo

$$\sum_{a,c} \frac{1}{\sqrt{c}} \big| \sum_{m} e\big(-\frac{\overline{a}}{c}(b+m)^2\big) \widehat{g}(m/c) \big|.$$

La idea fundamental de la gran criba sugiere que controlando el espaciamiento de $\overline{a}/c$ en los rangos significativos, lo cual es un problema aritmético, se puede asegurar cierta cuasiortogonalidad que implica cancelación. Realizar esta idea es mucho más complicado, porque hay que utilizar un lema de gran criba más poderoso (Lemma 7.5 [**Gr-Ko**]) que permita aprovechar el espaciamiento cuando m varía ($\widehat{g}$ también oscila), y para hacer este espaciamiento más homogéneo se aplica la desigualdad de Hölder como en el método de Vinogradov, necesitándose una especie de versión en miniatura del teorema del valor medio.

3. Algunas aplicaciones

3.1. Problemas de puntos del retículo

¿Cuántos puntos de coordenadas enteras quedan bajo una gráfica? ¿Cuántos caen dentro de un círculo grande? ¿Cuál es el promedio de la función que cuenta el número de divisores? Lo que tienen en común estos problemas es que requieren contar puntos en algún subconjunto del retículo $\mathbb{Z}^2$. Cuando estos subconjuntos están limitados por fronteras "suaves" las sumas trigonométricas se muestran como un arma fundamental, siempre que trabajemos con el derroche típico del Análisis, que va perdiendo un ϵ en cada paso. Así que no tendremos respuestas exactas a las cuestiones anteriores, pero sí cotas para los términos de error.

Ya mencionamos en el capítulo anterior cómo obligar a que aparezca un suma trigonométrica cuando contamos: si queremos contar los enteros que hay en $[-X, X]$, el resultado es $\sum \Psi(n)$ donde Ψ es la función característica de $[-X, X]$. Al aplicar la fórmula de sumación de Poisson ya tenemos una serie trigonométrica. El caso de dos dimensiones se reduce a éste cortando en rodajas unidimensionales. La dificultad que aparece en este esquema es la lentitud de la convergencia o la ausencia de ella debido a que Ψ es muy poco regular. Una vez que lo hayamos resuelto, podremos aplicar nuestros métodos favoritos del pasado capítulo.

La máquina de hacer regularizaciones

Se define la convolución de dos funciones f y g como

$$(f * g)(x) = \int_{-\infty}^{\infty} f(x-t)g(t)\,dt.$$

Si $g \in C_0^\infty$, inmediatamente $f * g$ es C^∞ para cualquier f integrable. Por otra parte, si g es la delta de Dirac (una "función" infinitamente concentrada alrededor del origen con integral uno) entonces $f * g$ es lo mismo que f. La idea es que si tomamos una función $g \in C_0^\infty$ que se parezca mucho a la delta de Dirac, tendremos una función C^∞ que se parece mucho a f. Se puede forzar el parecido de cualquier función de C_0^∞ a la delta de Dirac encogiendo la x y estirando la y. Concretamente, si $\eta \in C_0^\infty$ con $\int \eta = 1$, entonces la máquina de hacer regularizaciones será:

$$f \mapsto f * g \qquad \text{con } \; g(x) = \delta^{-1}\eta(\delta^{-1}x) \text{ y } \delta > 0 \text{ pequeño.}$$

De alguna forma el efecto de esto es que promediamos f en cada intervalo de tamaño proporcional a δ y entonces consideramos que $f * g$ y f son iguales si nuestra miopía no nos permite distinguir letras de tamaño δ.

La pregunta natural es qué ventaja reporta hacer las regularizaciones de esta forma tan rara. El truco está en que si vamos a aplicar la fórmula de sumación de Poisson, más vale que sepamos manejar las transformadas de Fourier que aparezcan, y esto es automático usando convoluciones gracias a la sencilla propiedad:

$$\widehat{f * g} = \widehat{f} \cdot \widehat{g}. \tag{3.1}$$

Curiosamente este truco, que es ampliamente usado en Análisis Armónico, apenas tiene arraigo entre los investigadores en Teoría Analítica de Números, pero la comodidad no sabe de tradiciones.

Con este armamento vamos a hacer dos regularizaciones de la función que nos interesa. Dibujándolas es fácil percatarse de que en una se suavizan el escalón hacia afuera y en otra hacia adentro.

Proposición 3.1 . *Sea Ψ la función característica de $[-X, X]$. Dado $0 < \delta \leq X$, existen dos funciones $\Psi^-, \Psi^+ \in C_0^\infty$ con $\int \Psi^- = 2X - 2\delta$, $\int \Psi^+ = 2X + 2\delta$; tales que*

$$\Psi^-(x) \leq \Psi(x) \leq \Psi^+(x) \quad \forall x \in \mathbb{R},$$

y

$$\widehat{\Psi}^-(\xi) = \phi(\delta\xi)\frac{\operatorname{sen}(2\pi(X-\delta)\xi)}{\pi\xi}, \qquad \widehat{\Psi}^+(\xi) = \phi(\delta\xi)\frac{\operatorname{sen}(2\pi(X+\delta)\xi)}{\pi\xi} \qquad \text{para } \xi \neq 0$$

donde $-1 \leq \phi \leq 1$ es una función de decaimiento rápido.

Dem.: Sea $\eta \in C_0^\infty$ una función par, no negativa con $\int \eta = 1$ y $\operatorname{sop} \eta = [-1/2, 1/2]$. Esto implica que $\widehat{\eta}$ es real de decaimiento rápido y $-1 \leq \widehat{\eta} \leq 1$. Tomando Ψ^- como la convolución de la función característica de $[-(X-\delta), X-\delta]$ con $\delta^{-1}\eta(\delta^{-1}x)$, es fácil comprobar que $\Psi^-(x) = 0$ si $|x| \geq X$ y $\Psi^-(x) \leq 1$ en general; lo que prueba $\Psi^-(x) \leq \Psi(x)$ mientras que $\int \Psi^- = 2X - 2\delta$ se sigue por integración directa. Por otra parte, teniendo en cuenta (3.1) y que la transformada de Fourier de la función característica de $[-y, y]$ es $(\pi\xi)^{-1}\operatorname{sen}(2\pi y\xi)$, se obtiene la fórmula para $\widehat{\Psi}^-(\xi)$.

Para $\widehat{\Psi}^+$ se procede exactamente igual pero ahora partiendo de la función característica de $[-(X+\delta), X+\delta]$. ■

Puntos bajo gráficas

Supongamos una función f no negativa definida en $[a, b]$ con $a, b \in \mathbb{Z}$. Nos preguntamos acerca del número de puntos de coordenadas enteras que están entre la gráfica de f y el eje X, es decir:

$$\mathcal{N} = \#\{(m, n) \in \mathbb{Z}^2 \,:\, a \leq n \leq b,\ 0 \leq n \leq f(m)\}.$$

Para ello vamos a pedir cierta condición de convexidad sobre la función f. Esto es natural, ya que una función muy plana o con un crecimiento incontrolado, podría atrapar demasiados puntos arruinando el término de error.

Teorema 3.2. *Con la notación anterior, si $f \in C^2$ y $0 < \lambda_2 \ll |f''| \ll \lambda_2 < 1$ entonces*

$$\mathcal{N} = \frac{b-a}{2} + \frac{f(a)+f(b)}{2} + \int_a^b f(x)\,dx + O((b-a)\lambda_2^{1/3} + \lambda_2^{-1/2}).$$

Nota: Esto se puede interpretar diciendo que si los puntos de las fronteras rectas cuentan sólo la mitad, el número de puntos limitados por la gráfica de f se aproxima por el área (la integral).

Dem.: Quizá cambiando f por $f+1$ (lo que lleva a un resultado equivalente) siempre se puede suponer $f \geq 1$. Fijado m, el número $\mathcal{N}_m$ de valores de n con $0 \leq n \leq f(m)$ se puede escribir como $\frac{1}{2} + \frac{1}{2}\sum \Psi(n)$ donde Ψ es la función característica de $[-X, X]$ con $X = f(m)$. Por la proposición anterior y la fórmula de sumación de Poisson, para $0 < \delta \leq 1$

$$-\delta + \sum_{n\neq 0} \phi(\delta n) \frac{\operatorname{sen}(2\pi(f(m)-\delta)n)}{2\pi n} \leq \mathcal{N}_m - f(m) - \frac{1}{2} \leq \delta + \sum_{n\neq 0} \phi(\delta n) \frac{\operatorname{sen}(2\pi(f(m)+\delta)n)}{2\pi n}.$$

Sumando en m y aplicando el teorema de los valores intermedios, existe $\delta' \in [-\delta, \delta]$ tal que

$$\mathcal{N} - \sum_{a\leq m\leq b} \big(f(m) + \frac{1}{2}\big) \ll (b-a)\delta + \left| \sum_{n\neq 0} \frac{\phi(\delta n)}{2\pi n} \sum_{a\leq m\leq b} \operatorname{sen}(2\pi(f(m)+\delta')n) \right|. \tag{3.2}$$

Como ϕ es de decaimiento rápido, $|\phi(\delta n)| \ll (1+\delta|n|)^{-1}$, y por la acotación de van der Corput, $\sum e(f(m)n) \ll (b-a)(\lambda_2|n|)^{1/2} + (\lambda_2|n|)^{-1/2}$. Por tanto el sumatorio entre valores absolutos está acotado por

$$\sum_{n=1}^{\infty} \frac{(b-a)\lambda_2^{1/2} n^{1/2} + \lambda_2^{-1/2} n^{-1/2}}{n(1+\delta n)} \ll \sum_{1\leq n\leq \delta^{-1}} \big((b-a)\lambda_2^{1/2} n^{-1/2} + \lambda_2^{-1/2} n^{-3/2}\big)$$
$$+ \delta^{-1} \sum_{n>\delta^{-1}} \big((b-a)\lambda_2^{1/2} n^{-3/2} + \lambda_2^{-1/2} n^{-5/2}\big).$$

Acotando las sumas de potencias ($p < 1 \Rightarrow \sum_{n\leq M} n^{-p} \ll M^{1-p}$; $p > 1 \Rightarrow \sum_{n>M} n^{-p} \ll M^{1-p}$), se obtiene un término que es de orden $(b-a)\lambda_2^{1/2}\delta^{-1/2} + \lambda_2^{-1/2}$.

Por otra parte, la fórmula de sumación de Euler-Mac Laurin implica

$$\sum_{a\le m\le b}\big(f(m)+\frac{1}{2}\big)=\frac{b-a+f(a)+f(b)}{2}+\int_a^b f(x)\,dx+O\big(1+\int_a^b|f''|\big).$$

Sustituyendo estas estimaciones en (3.2) se obtiene el teorema con un término de error del orden de

$$(b-a)\delta+(b-a)\lambda_2^{1/2}\delta^{-1/2}+\lambda_2^{-1/2}+1+(b-a)\lambda_2.$$

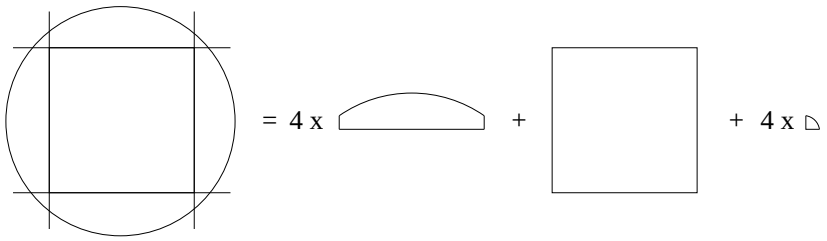
Y escogiendo $\delta=\lambda_2^{1/3}$ esta expresión es $O\big((b-a)\lambda_2^{1/3}+\lambda_2^{-1/2}\big)$. ■

Ya habíamos mencionado que la acotación básica de van der Corput es fácil de mejorar si λ_2 es muy pequeño. Es este contexto, si la gráfica de f se parece mucho a una recta, una cuenta directa puede dar mejor resultado que las sumas trigonométricas para determinar el número de puntos de coordenadas enteras.

Los problemas del círculo y del divisor

Después de haber contado puntos bajo gráficas, le toca el turno a las otras dos preguntas que nos hicimos al comenzar, las cuales dan lugar a los problemas del círculo y del divisor.

Sea $r(n)$ el número de representaciones de n como suma de dos cuadrados de números enteros, $r(n)=\#\{(a,b)\in\mathbb{Z}^2\,:\,a^2+b^2=n\}$. Es fácil comprobar que la suma de $r(n)$ de $n=0$ a N coincide con el número de puntos del retículo en el círculo centrado en el origen de radio $R=\sqrt{N}$. Sea M la parte entera de $R/\sqrt{2}$. Cortando el susodicho círculo por los lados del cuadrado $[-M,M]\times[-M,M]$ se obtienen típicamente nueve regiones.



El número de puntos del retículo en el círculo se puede escribir como la suma de los que hay en estas regiones contando los de las fronteras rectas (que son comunes a dos regiones) sólo por la mitad. La región superior está acotada por la gráfica de la función $f(x)=\sqrt{R^2-x^2}$ que cumple $R^{-1}\ll|f''(x)|\ll R^{-1}$ en $[-M,M]$. Así que con esta manera de contar, según el teorema anterior el número de puntos diferirá del área en

$O(R(R^{-1})^{1/3} + (R^{-1})^{-1/2}) = O(R^{2/3})$. Lo mismo se aplica, por simetría, a las otras tres regiones congruentes con la superior. Por otro lado, en el cuadrado $[-M, M] \times [-M, M]$ la diferencia entre los puntos así contados y el área es exactamente uno; y trivialmente la contribución de las "esquinas" es $O(1)$. Con ello hemos probado el siguiente resultado para el llamado *problema del círculo*, que consiste en estudiar el error al aproximar por el área el número de puntos en el interior de un círculo grande.

Proposición 3.3 . *Para* $R > 1$

$$\#\{(m,n) \in \mathbb{Z}^2 \,:\, m^2 + n^2 \leq R^2\} = \pi R^2 + O(R^{2/3}),$$

o equivalentemente

$$\sum_{n \leq N} r(n) = \pi N + O(N^{1/3}).$$

Sea $d(n)$ el número de divisores (positivos) de n. El *problema del divisor* consiste en estimar $\sum_{n \leq N} d(n)$. Lo cual lleva directamente a contar puntos bajo la gráfica de $f(x) = N/x$ ya que

$$\sum_{n \leq N} d(n) = \#\{(m,n) \,:\, 1 \leq m \leq N,\ 1 \leq n \leq N/m\} \tag{3.3}$$

La función f'' presenta unas variaciones tan grandes que el resultado que teníamos al respecto es de escasa utilidad, siendo necesario hurgar un poco en la demostración aprovechando la simetría de la gráfica de f y empleando una alternativa a la fórmula de sumación de Euler-Mac Laurin.

Proposición 3.4 . *Para* $N > 1$

$$\sum_{n \leq N} d(n) = N \log N + (2\gamma - 1)N + O(E(N))$$

donde

$$E(N) = 1 + N^{1/2}\delta + \sum_{n=1}^{\infty} \frac{1}{n(1+n\delta)} \Big| \sum_{m \leq N^{1/2}} e\big(\frac{Nn}{m}\big) \Big|$$

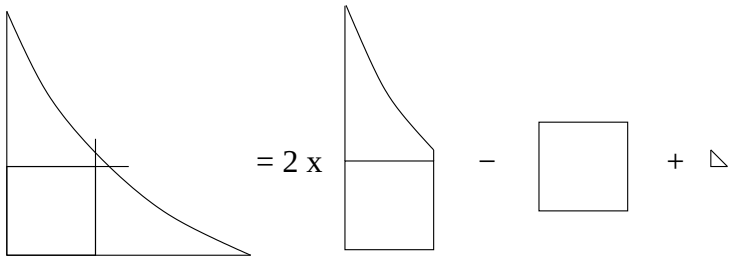
y $0 < \delta \leq 1$ *es una función arbitraria de* N.

Nota: Recuérdese que $\gamma = 0'577\ldots$ es la constante de Euler dada por $\lim_{n\to\infty}(1 + \frac{1}{2} + \ldots + \frac{1}{n} - \log n)$ o por $1 - \int_1^\infty t^{-2}\mathrm{Frac}(t)\,dt$, donde $\mathrm{Frac}(t)$ indica la parte fraccionaria de t.

Dem.: Sea M la parte entera de $N^{1/2}$. Por la simetría de $f(x) = N/x$ a través de $y = x$, es fácil ver que (3.3) implica

$$\sum_{n \leq N} d(n) = 2\#\{(m,n) \,:\, 1 \leq m \leq M,\ 0 \leq n \leq N/m\} - M^2 - 2M + O(1).$$

Donde $-M^2$ viene de los puntos del cuadrado $[1,M]\times[1,M]$, que se cuentan dos veces, y $-2M$ por haber reemplazado en (3.3), $1\le n\le N/m$ por $0\le n\le N/m$.



Aplicando (3.2) con $f(x)=N/x$ y $[a,b]=[1,M]$, se llega al resultado deseado siempre que se cumpla

$$2\sum_{m\le M}\big(\frac{N}{m}+\frac{1}{2}\big)-M^2-2M=N\log N+(2\gamma-1)N+O(1). \tag{3.4}$$

El lema de Abel se puede utilizar, como se hizo en los preliminares pero extrayendo un término más, para deducir

$$\sum_{m\le M}\frac{1}{m}=\log M+\gamma+\frac{1}{2M}+O(M^{-2}).$$

Por Taylor, $\log M=\frac12\log N+\log(1+(M-N^{1/2})N^{-1/2})=\frac12\log N+MN^{-1/2}-1+O(N^{-1})$. Sustituyendo estas igualdades en el primer miembro de (3.4) se sigue que es igual al segundo salvo un sumando de la forma $2MN^{1/2}-N+NM^{-1}-M^2-M$. Basta escribir $M=N^{1/2}+O(1)$ para llegar a que su contribución es $O(1)$. ■

Las fases $f(m)=Nn/m$ son adecuadas para la aplicación de la teoría de pares de exponentes, permitiendo una versátil acotación del término de error.

Teorema 3.5 . *Sea (p,q) un par de exponentes $0<p\le q\le 1$. Entonces se verifica*

$$\sum_{n\le N}d(n)=N\log N+(2\gamma-1)N+O\big(N^{(p+q)/(2p+2)}\big).$$

DEM.: El par de exponentes (p,q) implica

$$\Big|\sum_{N^{1/2}/2<m\le N^{1/2}}e\big(\frac{Nn}{m}\big)\Big|\ll n^pN^{q/2}.$$

Es fácil ver que la contribución de sumas similares en los intervalos $(N^{1/2}/4,N^{1/2}/2]$,

$(N^{1/2}/8, N^{1/2}/4]$, etc. es absorbida por la acotación anterior. Por tanto

$$E(N) \ll N^{1/2}\delta + \sum_{n\leq\delta^{-1}} n^{p-1}N^{q/2} + \sum_{n>\delta^{-1}} \delta^{-1}n^{p-2}N^{q/2} \ll N^{1/2}\delta + \delta^{-p}N^{q/2}.$$

Escogiendo $\delta = N^{(q-1)/(2p+2)}$ se deduce el resultado. ■

Se puede probar **[Ci-Co]**

$$r(n) = 4(d_1(n) - d_3(n))$$

donde $d_1(n)$ y $d_3(n)$ son respectivamente el número de divisores de la forma $4n+1$ y $4n+3$. Con ello es posible obtener una expresión similar a $E(N)$ para el error al aproximar $\sum_{n\leq N} r(n)$ por πN (en **[Gr-Ko]** parece haber algunas erratas en la relación exacta entre ambos problemas). Y el mismo exponente $(p+q)/(2p+2)$ del término de error se tiene en este caso.

Con el par de exponentes $(1/2, 1/2)$ el error es $O(N^{1/3})$, como ya se obtuvo para el problema del círculo. El par $(11/30, 16/30)$ permite ir un poco más allá pasando de $1/3 = 0'3333\ldots$ (a veces llamado *exponente trivial*) a $27/82 = 0'3292\ldots$. Incluso existe un algoritmo **[Gr-Ko]** para aproximar con precisión arbitraria el ínfimo de $(p+q)/(2p+2)$ con (p,q) par de exponentes de van der Corput. El resultado es desalentador, ya que dicho ínfimo es $0'3290\ldots$, extremadamente cerca de $1/3$. Esta barrera fue sobrepasada primero con métodos bidimensionales (gracias a Titchmarsh, Hua, Kolesnik y otros), y más recientemente con el llamado método discreto de Hardy y Littlewood **[Hu]**. El último exponente anunciado (todavía no publicado) es $131/416 = 0'3149\ldots$ debido a Huxley.

Por otro lado se sabe desde 1916 que el error no es $O(N^{1/4})$, y la Conjetura de Hardy es que éste es el exponente ínfimo. Es decir, que para todo $\theta > 1/4$ el error es $O(N^\theta)$, lo cual está avalado por diferentes resultados en media **[Ha]**. Además sería consecuencia del hipotético par de exponentes $(\epsilon, 1/2+\epsilon)$.

3.2. Partes fraccionarias de polinomios

Tomemos un número $x \in \mathbb{R}$. ¿Qué ocurre con las partes fraccionarias de nx? Si x es una fracción, cuando n supere al denominador la misma lista de números se repetirá de nuevo. Las sucesiones periódicas son un poco aburridas, así que probamos con x irracional. Por ejemplo para $x = \sqrt{2}$ se obtiene la sucesión:

$$0'41421\ldots,\ 0'82842\ldots,\ 0'24264\ldots,\ 0'65685\ldots,\ 0'07106\ldots,\ 0'48528\ldots,\ 0'89949\ldots$$

Ahora el resultado es caótico. Para no quedarnos sin estudiar nada, vamos a tratar de preguntarnos hasta qué punto es caótica la sucesión anterior u otras dadas por polinomios

más complicados como $\sqrt{2}\,n^3 + 7n^2 + \pi n + 1$. La respuesta será que cuando el coeficiente principal de un polinomio no constante es irracional (en realidad basta que lo sea cualquiera excepto el término independiente), al evaluarlo en los naturales su parte fraccionaria visita por igual todos los rincones de $[0, 1)$. También estudiaremos brevemente un problema más delicado relativo a la posibilidad de visitar rinconcitos minúsculos alrededor del cero o el uno, es decir, de obtener números casi enteros.

Sucesiones equidistribuidas

Si dibujamos con un ordenador los valores $\mathrm{Frac}(n\sqrt{2})$ para $n = 1, 2, 3, \ldots$ veremos una nube de puntos que rellena uniformemente el intervalo $[0, 1]$. Pero, ¿qué queremos decir exactamente con "uniformemente"? Para ser exactos nada mejor que una definición matemática.

DEFINICIÓN: *Se dice que una sucesión* $\{a_n\}_{n=1}^{\infty} \subset [0, 1]$ *está equidistribuida en* $[0, 1]$ *si para cualquier intervalo* $[a, b] \subset [0, 1]$ *se cumple*

$$\lim_{N\to\infty} \frac{\#\{n \leq N \,:\, a_n \in [a, b]\}}{N} = b - a.$$

Esto es lo mismo que decir que, en algún sentido, la probabilidad de que un término de la sucesión esté en $[a, b]$ coincide con la masa de probabilidad de este intervalo al utilizar la distribución uniforme en $[0, 1]$.

Ahora comprobamos que el problema que nos hemos propuesto no es trivial a partir de la definición. De hecho, parece muy difícil, porque no sabemos cuánto va a dar $n\sqrt{2}$ cuando n es grande (ni cuando es pequeño, porque $\sqrt{2}$ tiene infinitos decimales y la calculadora sólo emplea un número finito).

Lo que asegura el siguiente resultado es que tener una sucesión equidistribuida es lo mismo que tener un método de Montecarlo para aproximar integrales. (Para funciones "normales" los métodos típicos del Cálculo Numérico: Newton-Côtes, cuadraturas de Gauss, Romberg, etc. son mucho más efectivos). Con $\mathbb{T}$ (el toro unidad unidimensional) representaremos el intervalo $[0, 1]$ con los extremos identificados. Por tanto las funciones continuas en $\mathbb{T}$ son las funciones continuas en $[0, 1]$ con $f(0) = f(1)$.

Lema 3.6 . *La sucesión* $\{a_n\}_{n=1}^{\infty} \subset [0, 1]$ *está equidistribuida en* $[0, 1]$ *si y sólo si*

$$\lim_{N\to\infty} \frac{1}{N} \sum_{n\leq N} f(a_n) = \int_0^1 f(x)\,dx$$

para toda función continua $f : \mathbb{T} \longrightarrow \mathbb{R}$.

DEM.: $\Rightarrow$) Toda función continua es límite uniforme de funciones escalonadas y cada una de ellas es combinación lineal de funciones características de intervalos con interior disjunto. Por tanto basta considerar el caso en que f es la función característica de un intervalo $[a,b] \subset [0,1]$, y en este caso el límite del enunciado es idéntico a la definición de equidistribución.

$\Leftarrow$) Si Ψ es la función característica de $[a,b] \subset [0,1]$, sean Ψ^- y Ψ^+ funciones continuas en $\mathbb{T}$ con $\Psi^- \leq \Psi \leq \Psi^+$, y tales que $\int \Psi^+$ y $\int \Psi^-$ se diferencien de $b-a$ en menos de ϵ (compárese con las homónimas de la sección anterior, basta hacer las convoluciones en $\mathbb{T}$). Entonces

$$\frac{1}{N}\sum_{n\leq N} \Psi^-(a_n) \leq \frac{\#\{n \leq N \,:\, a_n \in [a,b]\}}{N} \leq \frac{1}{N}\sum_{n\leq N} \Psi^+(a_n).$$

Tomando límites cuando $N \to \infty$ y haciendo ϵ arbitrariamente pequeño, se llega a que a_n está equidistribuida. ■

Y por fin llegamos a un criterio eficiente en el caso que nos ocupa.

Proposición 3.7 (Criterio de Weyl)**.** *Una sucesión $\{a_n\}_{n=1}^{\infty} \subset [0,1]$ está equidistribuida en $[0,1]$ si y sólo si para cada entero $m \neq 0$, $\sum_{n\leq N} e(ma_n) = o(N)$.*

DEM.: $\Rightarrow$) Nótese que $\int_0^1 \cos(2\pi mx)\,dx = \int_0^1 \operatorname{sen}(2\pi mx)\,dx = 0$ para $m \neq 0$. Por el lema anterior, esto implica $N^{-1}\sum_{n\leq N} e(ma_n) \to 0$.

$\Leftarrow$) Por el teorema de Fejér **[Dy-Mc]** cualquier función continua en $\mathbb{T}$ se puede aproximar uniformemente por sumas finitas de la forma $S(x) = \sum_{|m|\leq M} \lambda_m e(mx)$. Y por tanto basta comprobar la condición del lema anterior para las partes real e imaginaria de $e(mx)$. (Nótese que $N^{-1}\sum_{n\leq N} \lambda_0 = \int S$). ■

Funciones polinómicas y equidistribución

El criterio de Weyl es suficiente para resolver nuestro problema tipo acerca de la distribución de $\operatorname{Frac}(n\sqrt{2})$. Y como no hemos hecho consideraciones especiales a $\sqrt{2}$, el resultado es general.

Proposición 3.8 . *Si $\alpha \notin \mathbb{Q}$, la sucesión $\operatorname{Frac}(n\alpha)$ con $n \in \mathbb{N}$ está equidistribuida en $[0,1]$.*

DEM.: Empleando la suma de una progresión geométrica, para cada $m \neq 0$

$$\left|\sum_{n\leq N} e(mn\alpha)\right| = \left|\frac{e((N+1)m\alpha) - e(m\alpha)}{e(m\alpha)-1}\right| \leq \frac{2}{|e(m\alpha)-1|} = \frac{1}{|\operatorname{sen}(\pi m\alpha)|}.$$

Fijados m y α este último valor es una constante, y se aplica el Criterio de Weyl. ■

Con esto tenemos resuelto el caso de grado uno. Lo que hizo Weyl **[We]** en el de grado k es elevar al cuadrado para que aparecieran incrementos (derivadas) de las fases y poder llevar a cabo un ingenioso argumento inductivo. Para evitar algunos detalles emplearemos la versión de van der Corput del truco de Weyl que permite hacer general dicho razonamiento inductivo.

Teorema 3.9 (Criterio de van der Corput)**.** *Sea* $\{a_n\}_{n=1}^{\infty} \subset [0,1]$. *Si para cada* $r \in \mathbb{Z}^+$ *la sucesión dada por* $b_n = \mathrm{Frac}(a_{n+r} - a_n)$ *está equidistribuida en* $[0,1]$ *entonces* a_n *también lo está.*

Nota: Se sabe que $\mathbb{Z}^+$ puede reemplazarse por conjuntos más pequeños **[Mo]**.

Dem.: Fijados m y H, por el Lema 2.5 con $f(n) = ma_n$, para $N > H$

$$\left|\sum_{n\leq N} e(ma_n)\right|^2 \leq 4\frac{N^2}{H} + 4N \max_{r\leq H}\left|\sum_{n\leq N-r} e(mb_n)\right|.$$

Dividiendo entre N^2 y empleando que $\sum_{n\leq N-r} e(mb_n) = o(N)$ (por el Criterio de Weyl), se concluye

$$\limsup_{N\to\infty}\left|\frac{1}{N}\sum_{n\leq N} e(ma_n)\right|^2 \leq \frac{4}{H}.$$

Como H es arbitrario, el límite debe existir y ser nulo, lo que implica la equidistribución de acuerdo con el Criterio de Weyl. ■

Corolario 3.10. *Sea un polinomio* $P(x) = a_0x^k + a_1x^{k-1} + \ldots + a_{k-1}x + a_k \in \mathbb{R}[x]$ *con* $a_0 \notin \mathbb{Q}$, *entonces la sucesión* $\mathrm{Frac}(P(n))$ *con* $n \in \mathbb{N}$ *está equidistribuida en* $[0,1]$.

Dem.: Se procede por inducción en el grado. Ya hemos visto el caso $k = 1$. Por otra parte, si P es de grado k entonces $P(n+r) - P(n)$ es de grado $k-1$ (en n) y basta aplicar el teorema anterior y la hipótesis de inducción. ■

Aproximación diofántica

Ya sabemos que $\mathrm{Frac}(\pi n)$ está equidistribuida, por tanto habrá muchos valores de n para los que πn esté cerca de un entero, pero ¿cuánto de cerca? Si lo estuviera mucho tendríamos una buena aproximación $\pi \approx m/n$. ¿Y si nos empeñamos en que el denominador sea un cuadrado? No queremos conceder a π ningún privilegio, que bastantes tiene ya, sino que buscamos resultados generales.

El caso lineal está basado en una bella aplicación del principio del palomar.

Lema 3.11 (Dirichlet)**.** *Sea $\alpha \in \mathbb{R}$. Para cada $N \in \mathbb{Z}^+$ existen $a, q \in \mathbb{Z}$ con $1 \leq q \leq N$ tales que $|q\alpha - a| < 1/N$.*

Nota: La condición $N \in \mathbb{Z}^+$ es superflua **[Va]**, pudiéndose reemplazar por $N \in [1, \infty)$.

DEM.: Considérense Frac(α), Frac(2α), Frac(3α),... Frac($N\alpha$). Evidentemente son N números que pertenecen a

$$[0, \frac{1}{N}) \cup [\frac{1}{N}, \frac{2}{N}) \cup \ldots \cup [\frac{N-1}{N}, 1) = [0, 1).$$

Si cada uno de estos números perteneciera a exactamente uno de los N subintervalos, alguno de ellos, digamos Frac($q\alpha$), pertenecería al primero, entonces $|q\alpha - a| < 1/N$ donde a es la parte entera de $q\alpha$.

En otro caso, si Frac($q_1\alpha$) y Frac($q_2\alpha$), $q_1 < q_2$, están en un mismo subintervalo, se verifica $|qx - a| < 1/N$ con $q = q_2 - q_1$ y a es igual a la diferencia de las correspondientes partes enteras. ■

Proposición 3.12 . *Dado $\alpha \notin \mathbb{Q}$ sea $\delta(n)$ la distancia de $n\alpha$ al entero más cercano, entonces se verifica $n\delta(n) < 1$ para infinitos $n \in \mathbb{Z}^+$.*

DEM.: Sean a y q como en el lema anterior, entonces $|q\alpha - a| < N^{-1} \leq q^{-1}$ implica $q\delta(q) \leq 1$. Sea N' tal que $(N')^{-1} < |q\alpha - a|$. Aplicando el lema anterior con N' en lugar de N se tiene $q'\delta(q') \leq 1$ con $|q'\alpha - a'| < |q\alpha - a|$, y por tanto $q \neq q'$. Este proceso se puede repetir indefinidamente. ■

En el difícil caso de polinomios de grado superior, sólo se tienen resultados parciales lejanos del caso lineal. Estudiaremos aquí el caso cuadrático.

Proposición 3.13 . *Dado $\alpha \notin \mathbb{Q}$ sea $\Delta(n)$ la distancia de $n^2\alpha$ al entero más cercano, entonces para cada $\sigma < 1/2$ se verifica $n^\sigma \Delta(n) < 1$ para infinitos $n \in \mathbb{N}$.*

DEM.: Sea $M = N^\sigma$ con $N\delta(N) < 1$, digamos que $|\alpha - a/N| < N^{-2}$ con a/N irreducible. Por el resultado anterior M puede tomar valores arbitrariamente grandes (suponemos $\sigma > 0$). Sea la función

$$F(x) = M \sum_{m=-\infty}^{\infty} \eta(M(x+m))$$

con $\eta \in C_0^\infty$ no negativa y sop $\eta = [-1, 1]$. La "gracia" de la función F es que $F(n^2\alpha) \neq 0$ si y sólo si $\Delta(n) < M^{-1} = N^{-\sigma}$. De modo que basta probar

$$\sum_{n \leq N} F(n^2\alpha) \neq 0. \tag{3.5}$$

Desarrollando por Fourier (véase la demostración de la fórmula de sumación de Poisson)

$$F(x) = \int \eta(t)\, dt + \sum_{m \neq 0} \widehat{\eta}(m/M) e(mx).$$

Sea $M' = N^{\sigma'}$ con $\sigma < \sigma' < 1/2$. Como $\widehat{\eta}$ es de decaimiento rápido, la contribución de los términos con $|m| > M'$ es $o(1)$. Además, una vez fijada η, $\int \eta$ es una constante positiva y $\widehat{\eta}$ está acotada. Por tanto (3.5) se deduce si establecemos

$$\sum_{m \leq M'} \Big| \sum_{n \leq N} e(mn^2\alpha) \Big| = o(N). \tag{3.6}$$

Llamemos S a esta suma doble. Por la desigualdad de Cauchy-Schwarz, expandiendo el cuadrado (lo que equivale a aplicar el Lema 2.5 con $H = b - a$)

$$|S|^2 \ll M' \sum_{m \leq M'} \left(N + \sum_{r \leq N} \Big| \sum_{n \leq N'} e(2mnr\alpha) \Big| \right) \qquad \text{para algún } N' \leq N.$$

Como ya habíamos visto, la suma interior es la de una progresión geométrica, y se tiene

$$|S|^2 \ll (M')^2 N + M' \sum_{m \leq M'} \sum_{r \leq N} \min(N, |\operatorname{sen}(2\pi mr\alpha)|^{-1}).$$

El número de formas de expresar un número como mr con $m \leq M'$ y $r \leq N$ es de orden menor que cualquier potencia positiva de N **[Ha-Wr]**, por tanto

$$|S|^2 \ll (M')^2 N + N^{1/2} \sum_{l \leq M'N} \min(N, |\operatorname{sen}(2\pi l\alpha)|^{-1}). \tag{3.7}$$

Por hipótesis, $\alpha = a/N + \epsilon/N^2$ con $|\epsilon| \leq 1$. La contribución a la suma en cada intervalo de longitud N es

$$\begin{aligned} \sum_{L < l \leq L+N} \min(N, |\operatorname{sen}(2\pi l\alpha)|^{-1}) &= \sum_{n \leq N} \min\left(N, \left|\operatorname{sen}(L_0 + 2\pi \frac{an}{N} + 2\pi \frac{\epsilon n}{N^2})\right|^{-1}\right) \\ &\ll N + \frac{N}{2} + \frac{N}{3} + \ldots + \frac{N}{N-1} \ll N \log N \end{aligned}$$

donde se ha escrito $L_0 = 2\pi L\alpha$ y $l = L + n$ en la primera igualdad. La desigualdad posterior se debe a que an/N recorre módulo uno los números 0, $1/N$, $2/N$, $\ldots$ $(N-1)/N$

cuando $1 \leq n \leq N$ (ya que $n \mapsto an$ es biyectiva en $\mathbb{Z}_N$); mientras que $\epsilon n/N^2$ vale como máximo $1/N$.

Sustituyendo en (3.7) y extrayendo raíces cuadradas se tiene

$$|S| \ll M' N^{1/2} + N^{1/4} (M')^{1/2} N^{1/2} \log^{1/2} N.$$

Recordando que $M' = N^{\sigma'}$ con $\sigma' < 1/2$, se deduce finalmente (3.6). ■

La conjetura es que en el caso cuadrático, por analogía con el lineal, se puede tomar $\sigma < 1$ en vez de $\sigma < 1/2$ **[Mo]**; lo cual sería cierto bajo otras conjeturas acerca de sumas trigonométricas. Sin embargo durante más de cuarenta años, no se consiguió ir más allá de $1/2$, hasta que en 1995 Zaharescu **[Za]** probó que $\sigma < 2/3$ es válido, y que fijado $\sigma < 4/7$, para N mayor que cierta constante siempre existe algún $n \leq N$ tal que $n^\sigma \Delta(n) \leq 1$.

3.3. Volviendo al teorema de los números primos

La función $\zeta(s)$ viene representada para $\operatorname{Re} s > 1$ por una serie trigonométrica ya que $s = \sigma + it \;\Rightarrow\; n^{-s} = n^{-\sigma} e(-\frac{t}{2\pi} \log n)$. Como ya habíamos mencionado, los métodos de sumas trigonométricas permiten conseguir mejores estimaciones que las obtenidas en el primer capítulo y ensanchar la región libre de ceros un poco, con la consiguiente mejora del error en el teorema de los números primos.

De nuevo la variable compleja

Si revisamos cómo habíamos obtenido la región libre de ceros $\sigma > 1 - C/\log(|t| + 2)$, veremos que el logaritmo en el denominador proviene directamente del que aparecía al acotar $\operatorname{Re}(\zeta'/\zeta)$. Cambiando este logaritmo por una función genérica se tiene el siguiente resultado:

Lema 3.14 . *Sea $E = E(t)$ una función positiva con $\lim_{t\to\infty} E(t) = +\infty$ tal que*

$$-Re\,\frac{\zeta'(\sigma + i\gamma)}{\zeta(\sigma + i\gamma)} \leq E(\gamma) - \frac{1}{\sigma - \beta} \qquad y \qquad -\operatorname{Re}\frac{\zeta'(\sigma + 2i\gamma)}{\zeta(\sigma + 2i\gamma)} \leq E(\gamma)$$

para cualquier cero $\rho = \beta + i\gamma$ no trivial de ζ y todo $\sigma \geq 1 + 0'1/E(\gamma)$. Entonces para cierta constante $C > 0$, la región formada por los $s = \sigma + it$ tales que

$$\sigma > 1 - \frac{C}{E(t)},$$

está libre de ceros. de ζ.

Un inconveniente llamativo es que aunque acotáramos muy bien ζ empleando sumas trigonométricas, no parece claro que se concluya nada acerca de ζ'/ζ. Como tantas otras veces, la Variable Compleja, siempre solícita, viene al rescate.

Lema 3.15. *Sea f una función holomorfa en $|z-z_0|<\delta$ sin ceros en el círculo $|z-z_0|\le\delta/2$. Si $f(z_0)=1$ y $|f(z)|\le M$ para algún $M>2$, entonces se cumple $|f'(z)/f(z)|\ll\delta^{-1}\log M$ en el círculo $|z-z_0|<\delta/4$.*

No demostraremos aquí este resultado de verdad (véase **[Iv]**, **[Ti]**), sino que daremos una prueba mentirosa pero ilustrativa. Es un ejercicio encontrar el error: $g(z)=\log z$ es holomorfa en $|z-z_0|\le\delta/2\Rightarrow$ (Cauchy) $|g'(z)|\ll\int_C|g(\eta)|z-\eta|^{-2}|d\eta|$ con $C=\{\eta:|\eta-z|=\delta/4\}$ y $|z-z_0|<\delta/4\Rightarrow|f'(z)/f(z)|\ll\delta^{-1}\sup|g(z)|$, y $|f(z)|\le M\Rightarrow|g(z)|\le\log M$.

En definitiva, saber bien cómo crece la función ζ se traduce en ensanchar la región libre de ceros.

Proposición 3.16. *Si existe $r>1$ tal que $\zeta(\sigma+it)=O(\log^r t)$ para $\sigma>1-(\log\log t)^2/\log t$, $t>3$; entonces la región $\sigma>1-C(\log\log t)/\log t$ está libre de ceros para cierta constante positiva C y todo $t>3$.*

Nota: La condición $t>3$ no es relevante, simplemente se pide para que $\log\log t>0$. Evidentemente una región libre de ceros para $t>0$ se extiende simétricamente para $t<0$ ya que $\overline{\zeta(\sigma+it)}=\zeta(\sigma-it)$. Y como el número de ceros con $0\le t\le3$ es finito, uno puede hacer válida la región anterior para todo t quizá modificando la constante y escribiendo $\sigma>1-C(\log\log(|t|+3))/\log(|t|+2)$.

Dem.: Sea $\beta+i\gamma$ un cero de ζ con $\gamma>3$ y $\sigma=1+\log^{-r}\gamma$. Tómese en el lema anterior $z_0=\sigma+i\gamma$, $\delta=(\log\log\gamma)^2/\log\gamma$ y

$$f(z)=-\frac{\zeta(z)}{\zeta(z_0)}\prod_j\frac{z_0-\rho_j}{z-\rho_j}$$

donde ρ_j son los posibles ceros de ζ en el círculo $|z-z_0|\le\delta/2$ (repetidos con sus multiplicidad, si no existen el producto no aparece). Es posible elegir $M=O(\log^{2r}\gamma)$ ya que el producto permanece acotado en la frontera $|z-z_0|=\delta$ (principio del máximo) y

$$|\zeta(z_0)|^{-1}\ll\prod(1+p^{-\sigma})\ll\zeta(\sigma)\ll(\sigma-1)^{-1}=\log^r\gamma.$$

En definitiva, el lema implica

$$\left|-\frac{\zeta'(\sigma+i\gamma)}{\zeta(\sigma+i\gamma)}+\sum\frac{1}{\sigma+i\gamma-\rho_j}\right|\le\text{cte}\,\frac{\log\gamma}{\log\log\gamma}.$$

La parte real de $(\sigma+i\gamma-\rho_j)^{-1}$ es positiva porque $\sigma>1$, por consiguiente

$$-\text{Re}\,\frac{\zeta'(\sigma+i\gamma)}{\zeta(\sigma+i\gamma)}\le\text{cte}\,\frac{\log\gamma}{\log\log\gamma}-\text{Re}\sum\frac{1}{\sigma+i\gamma-\rho_j}\le\text{cte}\,\frac{\log\gamma}{\log\log\gamma}-\frac{1}{\sigma-\beta}.$$

Nótese que si $\beta + i\gamma$ no estuviera entre los ρ_j entonces $|\beta + i\gamma - z_0| > \delta/2 \Rightarrow (\sigma - \beta)^{-1} = O(\delta^{-1})$, y el término $(\sigma - \beta)^{-1}$ se puede conservar en la desigualdad anterior sin más que cambiar la constante que multiplica a $\log\gamma/\log\log\gamma$.

Para estimar $-\mathrm{Re}(\zeta'(\sigma + 2i\gamma)/\zeta(\sigma + 2i\gamma))$ se hace lo mismo pero desechando todos los términos del sumatorio.

Escogiendo en el primer lema $E(t) = K \log t/\log\log t$ para $t > 3$ con K suficientemente grande se deduce la región libre de ceros. ■

Una serie que no converge pero es útil

Según vamos resolviendo problemas aparecen otros nuevos. Hemos establecido una relación entre la acotación de ζ y la situación de los ceros, pero ahora el resultado requiere que esta acotación sea válida incluso un poco más a la izquierda de la recta $\mathrm{Re}\, s = 1$, donde ζ no puede representarse por la serie trigonométrica $\sum n^{-s}$. La solución es realmente sorprendente. Resulta que aunque la serie $\sum n^{-s}$ no converge en la banda crítca, cierta suma parcial de ella aproxima a $\zeta(s)$ con la precisión que deseemos.

Lema 3.17 . *Sea $s = \sigma + it$ con $\sigma \geq 1/2$ y sea $x \geq t/\pi > 0$; entonces*

$$\zeta(s) = \sum_{n \leq x} n^{-s} + \frac{x^{1-s}}{s-1} + O(x^{-\sigma}).$$

DEM.: Aplicando la fórmula de sumación de Euler-Mac Laurin con $f(n) = (x + M - 1)^{-s}$ y $N = \infty$, se tiene para $\mathrm{Re}\, s > 1$

$$\sum_{n=M}^{\infty} n^{-s} = \frac{M^{1-s}}{s-1} + \frac{1}{2}M^{-s} - s\int_M^{\infty} (x - [x] - \frac{1}{2})x^{-s-1}dx.$$

Por tanto

$$\zeta(s) = \sum_{n \leq M} n^{-s} + \frac{M^{1-s}}{s-1} - s\int_M^{\infty} (x - [x] - \frac{1}{2})x^{-s-1}dx - \frac{1}{2}M^{-s}. \tag{3.8}$$

Esta igualdad se extiende a $\mathrm{Re}\, s > 0$ porque en esta región ambos miembros definen funciones meromorfas.

Tomando en la Proposición 2.2 $f(n) = -\frac{t}{2\pi}\log n$ y $\alpha = -1$, $\beta = 0$, y aplicando el Lema 2.3 a) a la integral correspondiente a $n = -1$, se tiene para cualquier $y > x$

$$\sum_{x < n \leq y} n^{-it} = \frac{y^{1-it} - x^{1-it}}{1 - it} + O(1).$$

Con esto y el Lema de Abel se concluye

$$\sum_{x<n\leq M} n^{-s} = \frac{M^{1-s} - x^{1-s}}{1-s} + O(x^{-\sigma});$$

que sumado a (3.8) y estimando la integral trivialmente, conduce a

$$\zeta(s) = \sum_{n\leq x} n^{-s} + \frac{x^{1-s}}{s-1} + O(x^{-\sigma} + (t+1)M^{-\sigma}).$$

Como M es tan grande como deseemos, el último término se puede suprimir. ■

El término de error mejorado

Después de haber esquivado todos los escollos, ya podemos dar el golpe de gracia con nuestros métodos de sumas trigonométricas y todo lo que deseamos caerá como fichas de domino impulsadas por los resultados auxiliares anteriores.

Proposición 3.18 . *Sea $\delta = (2^{j+2} - 2)^{-1}$ con $j \in \mathbb{Z}^+$. Para todo $\sigma \geq 1 - (j+2)\delta$ y $t \geq 2$, se verifica*

$$\zeta(\sigma + it) = O(t^{\delta} \log t).$$

Además la constante "O" no depende de j.

DEM.: Tomemos $x = t/\pi$ en el resultado anterior y descompongamos en *intervalos diádicos* $[1, x] = \bigcup I_r \cap [1, x]$ con $I_r = [2^r, 2^{r+1})$. Evidentemente hay $O(\log t)$ intervalos I_r, y sumando por partes (Corolario 0.2),

$$|\zeta(\sigma + it)| \ll \log t \sup_r \Big|\sum_{n\in I_r} n^{-s}\Big| \ll \frac{\log t}{N^{\sigma}} \Big|\sum_{N/2\leq n\leq M} n^{-it}\Big|,$$

para ciertos N y M con $N/2 \leq M < N \leq x$.

Por la Proposición 2.9 cono $D = t/N$,

$$|\zeta(\sigma + it)| \ll \frac{\log t}{N^{\sigma}} \left(\frac{t}{N}\right)^{\delta} N^{1-(j+1)\delta} \ll t^{\delta} \log t.$$

Para comprobar la uniformidad de esta acotación en j, hay que examinar las entrañas de la prueba de la Proposición 2.9. Esto es demasiado tedioso para hacerlo aquí. Sin entrar en detalles, nótese que la aplicación repetida del Proceso A a través del Lema 2.5, da lugar esquemáticamente a acotaciones del tipo $|S_0|^2 \leq C|S_1|$, $|S_1|^2 \leq C|S_2|, \ldots, |S_{j-1}|^2 \leq C|S_j|$;

entonces $|S_0| \leq C^{1/2+1/4+\cdots}|S_j|^{2^{-j}}$ y la constante no degenera cuando j crece porque $1/2 + 1/4 + \ldots$ converge. Nótese también que las constantes "$\ll$" en las acotaciones de $|f^{(k)}|$ son del orden de $(k-1)!$, pero $((k-1)!)^{2^{-k}}$ permanece acotado y tiende rápidamente a uno, lo que permite un factor de este tipo en cada S_j. ■

De todo lo anterior se deduce por fin la nueva región libre de ceros buscada.

Corolario 3.19. *Para cierta constante $C > 0$ la región $\sigma > 1 - C(\log\log t)/\log t$, $t > 3$, está libre de ceros.*

DEM.: Sea j la parte entera de $2 + \log(\log t/\log\log t)/\log 2$ con t suficientemente grande. Entonces con la notación del resultado anterior, $(j+2)\delta \geq (\log\log t)^2/\log t$ y $\delta = O(\log\log t)$, de modo que se satisfacen las hipótesis de la primera proposición. ■

Si reemplazamos esta región por la que habíamos empleado anteriormente en la prueba del teorema de los números primos, se obtiene un término de error más pequeño.

Corolario 3.20. *Para cierta constante positiva K se cumple*

$$\psi(x) = x + O\big(xe^{-K\sqrt{\log x\ \log\log x}}\big).$$

En 1958 Korobov y Vinogradov probaron $\psi(x) = x + O\big(xe^{-K\log^{3/5} x\,(\log\log x)^{-1/5}}\big)$ a partir de una compleja variante del método de Vinogradov **[Iv]**, **[Ka]** que conduce a una región libre de ceros de la forma $\sigma > 1 - C/(\log^{2/3} t(\log\log t)^{1/3})$, $t > 3$. Este resultado ha permanecido imbatible hasta la fecha.

En todas las aplicaciones aquí discutidas del método de sumas trigonométricas, vemos que hay que trabajar muy duro para conseguir pequeñas mejoras que no parecen dirigirse a los objetivos. Éste es un fenómeno general que ha desatado a veces críticas hacia la Teoría Analítica de Números como una disciplina en que gran parte de los esfuerzos se dedican a disminuir infinitesimalmente exponentes que distan mucho de lo que se desea conseguir. La excusa natural es que los valores numéricos y las reducciones obtenidas no son relevantes frente a los poderosos métodos que se crean para llevarlas a cabo. Como contrarréplica también es justo mencionar que muchas de las mejoras se basan en complejísimos ajustes técnicos más que en ideas completamente nuevas.

4. El método del círculo

4.1. A vueltas con el círculo

El método del círculo es una poderosa técnica analítica que permite tratar muchos problemas aditivos en Teoría de Números. Apareció por primera vez en un artículo de Hardy y Ramanujan en 1918, y fue desarrollado por Hardy y Littlewood en los años subsiguientes. También es notable la contribución de H.D. Kloosterman a través de la introducción de una variante del método que empleó en el estudio de las formas cuadráticas cuaternarias.

El contexto general donde se aplica el método del círculo es en el tipo de problemas aditivos en los que se desea dar una aproximación asintótica del número de representaciones, $r_k(N)$, de un número grande N como suma de k elementos de un conjunto $\mathcal{B}$ de números no negativos. Es decir, se busca una fórmula asintótica para

$$r_k(N) = \#\{(b_1, b_2, \ldots, b_k) \in \mathcal{B}^k \,:\, N = b_1 + b_2 + \ldots + b_k\}.$$

Como $\mathcal{B} \subset \mathbb{Z}^+ \cup \{0\}$, la función $F(z) = \sum_{b\in\mathcal{B}} z^b$ es holomorfa en el disco unidad y elevando a la potencia k se obtiene la función generatriz de $r_k(N)$, también holomorfa,

$$F^k(z) = \sum_{n=0}^{\infty} r_k(n) z^n.$$

Ahora se puede rescatar el coeficiente que nos interesa simplemente con la fórmula integral de Cauchy:

$$r_k(N) = \frac{1}{2\pi i} \int_{\mathcal{C}} F^k(z) \frac{dz}{z^{N+1}} \tag{4.1}$$

donde $\mathcal{C}$ es cualquier circunferencia de radio r, $0 < r < 1$.

La idea es obtener información sobre $r_k(N)$ a partir de las singularidades del integrando, en la línea de lo visto en el primer capítulo. El problema aquí es que la única singularidad encerrada por $\mathcal{C}$ es el polo $z = 0$ que no podemos aprovechar porque hallar su residuo es tanto como calcular $r_k(N)$ y volvemos al problema inicial. Por otra parte, típicamente la circunferencia unidad es la frontera natural de F de modo que en general no tiene sentido extender $\mathcal{C}$ más allá en busca de nuevas singularidades que poder aprovechar, tratando de imitar el ejemplo de Cálculo I del primer capítulo.

El truco está en tomar r, el radio de $\mathcal{C}$, muy cercano a 1 para sentir la influencia de las "principales singularidades" de F en la circunferencia unidad, pero también r debe estar

suficientemente separado de 1 como para que no haya "interferencias" entre las influencias de diferentes singularidades. El tamaño de r está en realidad relacionado con el de N, siendo la elección natural tomar $1-r$ comparable a $1/N$. En este caso r^n es muy pequeño justamente cuando n es mucho mayor que N, de modo que en la definición de $F(z)$ los términos con b mucho mayor que N son despreciables, lo que concuerda con el hecho de que $N = b_1 + b_2 + \ldots + b_k \Rightarrow b_i \leq N$. Es decir, como los $b \in \mathcal{B}$ grandes en comparación con N no afectan a la definición de $r_k(N)$, tampoco deben ser relevantes en el comportamiento asintótico de F.

En ciertos arcos de $\mathcal{C}$, llamados *arcos mayores*, podremos dar una buena fórmula aproximada para F debido a la gran influencia de singularidades cercanas en el círculo unidad, mientras que en el resto; en los llamados *arcos menores*, nos tendremos que contentar con una acotación. La idea es que juntando las aproximaciones de F en los arcos mayores podremos obtener un término principal para $r_k(N)$, y las acotaciones de F en los arcos menores darán lugar a un término de error.

Por ejemplo, supongamos $\mathcal{B} = \mathbb{Z}^+ \cup \{0\}$, entonces $r_3(N)$ es el número de representaciones de N como suma de tres enteros no negativos. En este caso es ridículo aplicar el método del círculo para estudiar el comportamiento asintótico de $r_3(N)$, ya que es fácil deducir combinatoriamente la fórmula explícita exacta $r_3(N) = (N+1)(N+2)/2$. Sin embargo vamos a indicar cómo se haría para mostrar los conceptos básicos sobre un ejemplo manejable. Si $\mathcal{B} = \mathbb{Z}^+ \cup \{0\}$, se tiene $F(z) = 1 + z + z^2 + \ldots = 1/(1-z)$ y (4.1) da lugar a la fórmula

$$r_3(N) = \frac{1}{2\pi i} \int_{\mathcal{C}} \frac{dz}{(1-z)^3 z^{N+1}}$$

con $\mathcal{C}$, digamos, la circunferencia de radio $r = 1 - 1/N$. De nuevo apreciamos lo tonto que es el ejemplo, porque F se extiende analíticamente fuera del disco unidad y una aplicación del teorema de los residuos en $\{z : |z| > r\}$ conduce a la fórmula explícita exacta para $r_3(N)$. Como F tiene su única singularidad en $z = 1$, sólo hay que considerar un arco mayor $\mathcal{M} = \{z \in \mathcal{C} : |\arg z| < \delta\}$ formado por los puntos de $\mathcal{C}$ cercanos a $z = 1$. Su complementario conformará el único arco menor $\mathbf{m} = \mathcal{C} - \mathcal{M}$. Por Taylor, $1 - re^{i\theta} = 1 - r - ir\theta + O(\theta^2)$, de modo que $|F(re^{i\theta})| \ll \theta^{-1}$ cuando $1/N < |\theta| < \pi$. En particular, para $\delta^{-1} = o(N)$

$$\frac{1}{2\pi i} \int_{\mathbf{m}} F^3(z) \frac{dz}{z^{N+1}} \ll \int_{\delta}^{\pi} \theta^{-3}\, d\theta = o(N^2).$$

Supongamos que $N^{1/2} = O(\delta^{-1})$, digamos por ejemplo $\delta = N^{-\kappa}$ con $1/2 < \kappa < 1$, entonces

para $re^{i\theta} \in \mathcal{M}$ se cumple $1 - re^{i\theta} \sim 1 - r - i\theta$. Tomando inversos, cuando $N \to \infty$ en $\mathcal{M}$ se tiene

$$F(z) \sim \frac{N}{1 + (N\arg z)^2} - i\frac{N^2 \arg z}{1 + (N\arg z)^2}.$$

La expresión de la derecha se comporta como una constante por N para $|\arg z| < 1/N$ y se hace menor cuando $|\arg z|$ crece, lo que sugiere que

$$\frac{1}{2\pi i}\int_{\mathcal{M}} F^3(z)\frac{dz}{z^{N+1}} \sim CN^3 \cdot \frac{1}{N} = CN^2.$$

Esto se puede probar rigurosamente con $C = 1/2$, aunque no lo haremos aquí. La contribución de los arcos mayores y menores lleva finalmente a $r_3(N) \sim \frac{1}{2}N^2$.

Trabajar con series infinitas puede conllevar algunas dificultades técnicas que se evitan con una formulación ligeramente distinta del método del círculo, que cronológicamente es posterior. Está basada en la sencilla observación, antes comentada, de que $N = b_1 + b_2 + \ldots + b_k \Rightarrow b_i \leq N$. Por tanto en (4.1), se puede reemplazar F por F_N, la suma parcial de la serie que define F correspondiente a los $b \leq N$. Como F_N es un polinomio, no hay problemas para escoger $r = 1$, lo que con el cambio $z = e(x)$ transforma (4.1) en la sencilla igualdad:

$$r_k(N) = \int_0^1 S^k(x)\, e(-Nx)\, dx \qquad \text{con} \quad S(x) = \sum_{b \leq N,\ b \in \mathcal{B}} e(bx).$$

Los arcos mayores serán ahora subintervalos de $[-1/2, 1/2]$ en los que tengamos una buena aproximación para $S(x)$ que se traduzca en otra para la integral correspondiente sobre ellos; mientras que en el resto, los arcos menores, confiamos en que acotaciones de la suma trigonométrica $S(x)$ sean suficientes para acumular los resultados en un témino de error.

4.2. Sumas raras que se pueden calcular

En esta sección evaluaremos algunas sumas relacionadas con las siguientes expresiones:

$$c_q(M) = \sum_{\substack{n=1 \\ (n,q)=1}}^{q} e(Mn/q), \qquad G_q(a,l) = \sum_{n=1}^{q} e((an^2 + ln)/q).$$

En honor a los matemáticos que las introdujeron, se llaman *sumas de Ramanujan* a las primeras, y *suma de Gauss* (generalizadas) a las segundas.

Lema 4.1 . *La función $c_q(M)$ es multiplicativa en q, es decir, si q_1 y q_2 son coprimos, entonces $c_{q_1q_2}(M) = c_{q_1}(M) \cdot c_{q_2}(M)$.*

DEM.: Operando:

$$c_{q_1}(M) \cdot c_{q_2}(M) = \sum_{\substack{n=1 \\ (n,q_1)=1}}^{q_1} \sum_{\substack{m=1 \\ (n,q_2)=1}}^{q_2} e\big(M\frac{nq_2+mq_1}{q_1q_2}\big).$$

Por el teorema chino del resto, $k \equiv nq_2 \pmod{q_1}$, $k \equiv mq_1 \pmod{q_2}$ tiene solución única módulo q_1q_2, y evidentemente k es coprimo con q_1q_2 cuando n y m son coprimos con q_1 y q_2 respectivamente. Además cualquier k coprimo con q_1q_2 es solución de una de estas ecuaciones, porque si q_2' es el inverso de q_2 módulo q_1 y q_1' el de q_1 módulo q_2, se tiene $k \equiv (kq_2')q_2 \pmod{q_1}$, $k \equiv (kq_1')q_1 \pmod{q_2}$. Por tanto

$$c_{q_1}(M) \cdot c_{q_2}(M) = \sum_{\substack{k=1 \\ (k,q_1q_2)=1}}^{q_1q_2} e\big(m\frac{k}{q_1q_2}\big)$$

y ésta es la definición de $c_{q_1q_2}(M)$. ■

Proposición 4.2 . *Si M y q son coprimos entonces $c_q(M) = \mu(q)$. Y si $M/q = M'/q'$ con M' y q' coprimos entonces $c_q(M) = \mu(q')\phi(q)/\phi(q')$.*

DEM.: Por la multiplicidad basta considerar el caso $q = p^r$ con p primo. Si $r = 1$ y $p \not| M$ entonces $c_q(M)$ es la suma de las raíces q-ésimas de la unidad excepto la raíz 1, por tanto $c_q(M) = 0 - 1 = \mu(q)$. Si $r > 1$ y $p \not| M$

$$c_q(M) = \sum_{n=1}^{q} e(Mn/q) - \sum_{m=1}^{q/p} e(pMm/q)$$

y ambas sumas son nulas por ser sumas de todas las raíces de la unidad.

Si $p|M$ y $M/q = M'/q'$ con $p \not| M'$,

$$c_q(M) = \sum_{\substack{n=1 \\ (n,q)=1}}^{q} e(Mn/q) = \sum_{\substack{n=1 \\ (n,q)=1}}^{q} e(M'n/q') = \frac{\phi(q)}{\phi(q')} \sum_{\substack{n=1 \\ (n,q')=1}}^{q'} e(M'n/q').$$

La última igualdad se sigue porque $e(M'n/q')$ tiene periodo q', como función de n y por tanto podemos agrupar los $\phi(q)$ sumandos del sumatorio anterior de $\phi(q')$ en $\phi(q')$ términos. ■

Proposición 4.3 . *Para a y q coprimos $|G_q(a,l)| \leq (2q)^{1/2}$. Y además $(G_q(a,0))^k = (2q)^{k/2}\delta_q$ para k múltiplo de 8, donde*

$$\delta_q = \begin{cases} 2^{-k/2} & \text{si } 2 \not| q \\ 1 & \text{si } 4|q \\ 0 & \text{si } 4|q-2 \end{cases}$$

DEM.: Tomando módulos

$$|G_q(a,l)|^2 = \sum_{n=1}^{q}\sum_{m=1}^{q} e\left(a\frac{(n-m)(n+m)}{q} + l\frac{n-m}{q}\right).$$

Si q es impar, el cambio $u = n-m$, $v = n+m$ es lícito en $\mathbb{Z}_q \times \mathbb{Z}_q$ (la función inversa es $n = (u+v)/2$, $m = (v-u)/2$) y se llega a

$$|G_q(a,l)|^2 = \sum_{u=1}^{q}\left(\sum_{v=1}^{q} e\big(au\frac{v}{q}\big)\right)e\big(\frac{lu}{q}\big).$$

La suma entre paréntesis es no nula sólo si $q|au$ y esto implica $u = q$, por tanto $|G_q(a,l)|^2 = q$. En el caso con q par, el cambio es 2 a 1 (su núcleo es $\{(0,0),(q/2,q/2)\}$) siendo su imagen los u y v con la misma paridad. Por tanto

$$|G_q(a,l)|^2 = 2\sum_{\substack{u=1\\ 2\not| u}}^{q}\left(\sum_{\substack{v=1\\ 2\not| v}}^{q} e\big(au\frac{v}{q}\big)\right)e\big(\frac{lu}{q}\big) + 2\sum_{\substack{u=1\\ 2| u}}^{q}\left(\sum_{\substack{v=1\\ 2| v}}^{q} e\big(au\frac{v}{q}\big)\right)e\big(\frac{lu}{q}\big).$$

El primer sumatorio entre paréntesis es siempre nulo por ser la suma de todas las raíces impares q-ésimas de la unidad. Escribiendo en el segundo $v = 2v'$, se tiene que sólo puede ser no nulo si $u = q/2$ o $u = q$, en cuyo caso vale $q/2$, y el doble sumatorio está acotado, en módulo, por $q/2 + q/2 = q$.

Para evaluar $(G_q(a,0))^k$ utilizaremos el resultado debido a Gauss:

$$G_q(1,0) = \frac{1+i^{-q}}{1+i^{-1}}\sqrt{q}$$

que puede obtenerse como una indirecta y compleja consecuencia de la fórmula de sumación de Poisson ([**Da**] §2, [**Dy-Mc**]). De aquí se deduce que $G_q(1,0)$ es siempre una raíz de $x^k - (2q)^{k/2}\delta_q$. Consideremos el automorfismo del grupo de Galois $\mathrm{Gal}(\mathbb{Q}(\xi)/\mathbb{Q})$ con $\xi = e(1/q)$, definido por $\sigma : \xi \mapsto \xi^a$. Aplicando σ, $G_q(1,0)$ se transforma en $G_q(a,0)$, y como los automorfismos permutan las raíces de los polinomios sobre el cuerpo base, se deduce que $\big(G_q(a,0)\big)^k - (2q)^{k/2}\delta_q = 0$. ■

Lema 4.4 . *Si δ_q es como en el resultado anterior, se cumple*

$$\sum_{q=1}^{\infty} \frac{\delta_q}{q^{k/2}}\, c_q(-N) = \frac{1}{(2^{k/2}-1)\zeta(k/2)} \sum_{d|N} (-1)^{N+N/d} d^{1-k/2}.$$

Dem.: Consideremos la función aritmética $g(q) = 2^{k/2} c_q(-N)\delta_q q^{-k/2}$. Por las propiedades de c_q y la definición de δ_q, esta función es multiplicativa y por tanto

$$\sum_{q=1}^{\infty} \frac{\delta_q}{q^{k/2}}\, c_q(-N) = 2^{-k/2} \prod_p (1 + g(p) + g(p^2) + g(p^3) + \ldots)$$

donde p recorre los primos. Llamemos F_p a cada uno de estos factores. Si p^l es la máxima potencia de p que divide a N, por las propiedades de c_q, para $p \neq 2$ se cumple

$$F_p = 1 + p^{-k/2}(p-1) + (p^2)^{-k/2}(p^2-p) + \ldots + (p^l)^{-k/2}(p^l - p^{l-1}) - (p^{l+1})^{-k/2} p^l$$

$$= (1 - p^{-k/2}) \left(1 + p^{1-k/2} + p^{2(1-k/2)} + \ldots + p^{l(1-k/2)}\right).$$

Y razonamientos similares conducen para $p = 2$ y N par, a

$$F_2 = 1 + 2^{1-k/2} + 2^{2(1-k/2)} + \ldots + 2^{l(1-k/2)} - 2 \cdot 2^{l(1-k/2)},$$

mientras que trivialmente $F_2 = 1$ para N impar.

Así pues

$$\sum_{q=1}^{\infty} \frac{\delta_q}{q^{k/2}}\, c_q(-N) = C\left(\sum_{d|N} d^{1-k/2} - 2 \sum_{d|N,\ 2\not| d} (2^l d)^{1-k/2} \right) \quad \text{con } C = 2^{-k/2} \prod_{p\neq 2} (1 - p^{-k/2})$$

donde $l > 1$ es la máxima potencia de 2 que divide a N y el segundo sumatorio se omite si N es impar. Es decir, la suma buscada es, salvo la constante C, la suma de los divisores

de N restando dos veces aquellos divisores que contienen una potencia máxima de 2 mayor que 1. Notando que $N+N/d$ es impar si y sólo si d es par y contiene esta máxima potencia de 2, se sigue

$$\sum_{q=1}^{\infty} \frac{\delta_q}{q^{k/2}}\, c_q(-N) = C \sum_{d|N} (-1)^{N+N/d} d^{1-k/2}.$$

Finalmente $C^{-1} = (2^{k/2}-1)\zeta(k/2)$ es consecuencia directa de la identidad de Euler para la función ζ. ■

Lema 4.5 . *Sean $N > 1$ y $k > 2$ enteros, entonces*

$$\sum_{q=1}^{\infty} \left(\frac{\mu(q)}{\phi(q)}\right)^k c_q(-N) = \prod_{p\not|N} \left(1 + \frac{(-1)^{k+1}}{(p-1)^k}\right) \prod_{p|N} \left(1 + \frac{(-1)^k}{(p-1)^{k-1}}\right).$$

DEM.: La evaluación de esta suma es muy similar a la del resultado anterior, pero técnicamente es más sencilla. La función multiplicativa a considerar ahora es $g(q) = c_q(-N)(\mu(q)/\phi(q))^k$. Como $g(p^r) = 0$ si $r > 1$, se tiene

$$\sum_{q=1}^{\infty} \left(\frac{\mu(q)}{\phi(q)}\right)^k c_q(-N) = \prod_{p} (1 + g(p)) = \prod_{p} \left(1 + \frac{(-1)^k c_p(-N)}{(p-1)^k}\right).$$

Y según las propiedades de las sumas de Ramanujan, si $p \not| N$, $c_p(-N) = \mu(p) = -1$, y si $p|N$, $c_p(-N) = p-1$. ■

4.3. Sumas de cuadrados

En esta sección vamos a aplicar el método del círculo en su versión clásica para estudiar el número de representaciones como suma de k cuadrados, esto es,

$$r_k(N) = \#\{(n_1, n_2, \ldots, n_k) \in \mathbb{Z}^k \,:\, n_1^2 + n_2 + \ldots + n_k^2 = N\}.$$

Nos vamos a restringir al caso en que k es múltiplo de 8 con el fin de simplificar algunos detalles técnicos y llegar a una fórmula final más sencilla; sin embargo esta condición no es esencial **[Va]**, **[Gr]**.

De acuerdo con (4.1)

$$r_k(N) = \frac{1}{2\pi i} \int_{\mathcal{C}} F^k(z) \frac{dz}{z^{N+1}} \qquad \text{con} \quad F(z) = \sum_{n=-\infty}^{\infty} z^{n^2} = 1 + 2\sum_{n=1}^{\infty} z^{n^2}.$$

Por razones de comodidad vamos a desplegar la circunferencia en un segmento a través del cambio $z \mapsto e(z)$, que da lugar a

$$r_k(N) = \int_L f(z) e(-Nz)\, dz \qquad \text{con} \quad f(z) = \Big(\sum_{n=-\infty}^{\infty} e(n^2 z) \Big)^k \tag{4.2}$$

y L el segmento horizontal $L = \{0 \le \operatorname{Re} z \le 1,\ \operatorname{Im} z = y\}$ donde $r = e^{-2\pi y}$. Escogeremos $y = 1/N$, lo que corresponde aproximadamente a $1 - r = 2\pi/N$.

Antes de efectuar la división en arcos mayores y menores, probaremos una aproximación de $f(z)$ en L que servirá en todos ellos. Por el resultado de Dirichlet que vimos en el capítulo anterior, $\mathbb{T}$ (el toro unidad unidimensional correspondiente al intervalo $[0,1]$ con los extremos identificados) queda cubierto por intervalos de la forma:

$$I_{a/q} = \big\{ x \,:\, |x - \frac{a}{q}| < \frac{1}{q\sqrt{N}} \big\}$$

con a/q fracciones irreducibles $0 \le a < q \le \sqrt{N}$.

Proposición 4.6 . *Si* $\operatorname{Re} z \in I_{a/q}$ *y* $\operatorname{Im} z = N^{-1}$, *se cumple*

$$f(z) = (qz - a)^{-k/2} \big(\delta_q + O(e^{-\Delta}) \big)$$

donde $\Delta = \frac{1}{2} \min(Nq^{-2}, N^{-1}(qx-a)^{-2})$ *y* δ_q *es como en la sección anterior, esto es,* $\delta_q = 1$ *si* $4|q$ *y* $\delta_q = 2^{-k/2-1}(1 - (-1)^q)$ *en otro caso.*

DEM.: Descomponiendo en clases de restos módulo q

$$\sum_{n=-\infty}^{\infty} e(n^2 z) = \sum_{m=0}^{q-1} e(am^2/q) \sum_{n \equiv m \,(\mathrm{mod}\, q)} e(n^2 (z - a/q)).$$

Para cada m se puede aplicar la fórmula de sumación de Poisson al último sumatorio:

$$\sum_{n \equiv m \,(\mathrm{mod}\, q)} e(n^2 (z - a/q)) = \frac{1}{q\sqrt{2i(z - a/q)}} \sum_{n=-\infty}^{\infty} e\big(\frac{n^2}{4q(a - qz)} \big)\, e(nm/q).$$

Al sustituir, separando la contribución de $n = 0$, se llega a

$$\sum_{n=-\infty}^{\infty} e(n^2 z) = \frac{1}{q\sqrt{-2i(z - a/q)}} \Big(G_q(a,0) + \sum_{n \neq 0} G_q(a,n)\, e\big(\frac{n^2}{4q(a - qz)} \big) \Big).$$

Sabemos que $|G_q(a,m)| = O(q^{1/2})$ y evidentemente $|e(w)| = O(e^{-\operatorname{Im} w})$. Así pues, notando que $\operatorname{Im}\big(q^{-1}(a-qz)^{-1}\big) = (N(qx-a)^2 + N^{-1}q^2)^{-1}$ y comparando la suma de la serie con una progresión geométrica, se sigue

$$\sum_{n=-\infty}^{\infty} e(n^2 z) = \frac{1}{q\sqrt{-2i(z-a/q)}}\big(G_q(a,0) + O(q^{1/2}e^{-\Delta})\big).$$

Elevando a k cada uno de los miembros y usando $G_q(a,0) = O(q^{1/2})$, se obtiene finalmente el resultado, ya que según la Proposición 4.3, $\delta_q = (2q)^{-k/2}G_q^k(a,0)$. ■

En principio podríamos tomar como arcos mayores los $I_{a/q}$, y como recubren todo $[0,1]$ no habría necesidad de arcos menores. Esta situación es típica de los problemas que provienen de las llamadas formas modulares (véanse los capítulos 11 y 12 de **[Gr]**). Sin embargo, para ser coherentes con la terminología, los $x \in I_{a/q}$ con $4|q-2$ deberían pertenecer a un arco menor ya que en ese caso el término principal en la proposición anterior se anula. Otro problema es que los intervalos $I_{a/q}$ no son estrictamente disjuntos. Una manera de resolver este problema es reemplazarlos por la subdivisión de Farey **[Ci-Co]**, **[Gr]**, pero aquí procederemos de una manera más simple pidiendo $0 \le a < q \le \sqrt{N}/2$ lo que asegura que los $I_{a/q}$ son disjuntos. En definitiva, la elección de los arcos mayores y menores es respectivamente

$$\mathcal{M} = \bigcup_{\substack{0\le a<q\le\sqrt{N}/2\\(a,q)=1\ \ 4\not|q-2}} I_{a/q} \qquad \text{y} \qquad \mathbf{m} = \mathbb{T} - \mathcal{M}.$$

Proposición 4.7 . *Si* $z = x + i/N$

$$\int_{\mathbf{m}} f(z)\, e(-Nz)\, dx = O(N^{k/4}).$$

Dem.: Si $x \in \mathbf{m}$, $x \in I_{a/q}$ con $4|q-2$ o $\sqrt{N}/2 < q \le \sqrt{N}$. En cualquiera de los dos casos el término principal en la proposición anterior es absorbido por el error. Por consiguiente

$$\int_{\mathbf{m}} f(z)\, e(-Nz)\, dx \ll \sum_{0\le a<q\le\sqrt{N}} \int_{I_{a/q}} |qz-a|^{-k/2} e^{-\Delta}\, dx.$$

Es fácil comprobar que $|qz-a|^{-1} \ll N^{1/2}\Delta^{1/2}$. Por otra parte la función $h(t) = t^{k/4}e^{-t}$

está acotada en $[0,\infty)$, así pues $|qz-a|^{-k/2}e^{-\Delta} \ll N^{k/4}$. Y se tiene

$$\int_{\mathbf{m}} f(z)\, e(-Nz)\, dx \ll \sum_{q\le\sqrt{N}} \sum_{0\le a<q} N^{k/4}|I_{a/q}| \ll \sum_{q\le\sqrt{N}} \sum_{0\le a<q} N^{k/4}N^{-1/2}q^{-1}$$

que claramente es $O(N^{k/4})$. ■

Proposición 4.8 . *Con la notación anterior se cumple la fórmula*

$$\int_{\mathcal{M}} f(z)\, e(-Nz)\, dx = \frac{(2\pi)^{k/2}N^{k/2-1}}{(k/2-1)!} \sum_{q\le\sqrt{N}/2} \frac{\delta_q}{q^{k/2}}\, c_q(-N) + O(N^{k/4}).$$

Dem.: La contribución del término de error de $f(z)$, esto es, $O(|qz-a|^{-k/2}e^{-\Delta})$, ha sido ya estudiada en los arcos menores, y da lugar a un término $O(N^{k/4})$. Por tanto

$$\int_{\mathcal{M}} f(z)\, e(-Nz)\, dx = \sum_{q\le\sqrt{N}/2} \sum_{\substack{a=0\\(a,q)=1}}^{q-1} \delta_q \int_{I_{a/q}} (qz-a)^{-k/2}\, dx + O(N^{k/4}). \tag{4.3}$$

Con el cambio de variable $u = N(x-a/q)$ y recordando que $z = x + i/N$,

$$\int_{I_{a/q}} (qz-a)^{-k/2}\, dx = N^{k/2-1}q^{-k/2}e(-aN/q) \int_{-\sqrt{N}/q}^{\sqrt{N}/q} (u+i)^{-k/2}e(-u-i)\, du.$$

Por el teorema de los residuos aplicado en el semiplano inferior

$$\int_{-\infty}^{\infty} (u+i)^{-k/2}e(-u-i)\, du = \frac{(-2\pi i)^{k/2}}{(k/2-1)!}.$$

Integrando por partes, la contribución a la integral de $|u| > \sqrt{N}/q$ es $O(q^{k/2}N^{-k/4})$. Por tanto

$$\int_{I_{a/q}} (qz-a)^{-k/2}\, dx = \frac{(2\pi)^{k/2}N^{k/2-1}}{q^{k/2}(k/2-1)!}\, e(-aN/q) + O(N^{k/4-1}).$$

Sustituyendo en (4.3), se concluye la prueba. ■

Con esto ya podemos probar el teorema que buscábamos:

Teorema 4.9. *Para cada k múltiplo de 8 se cumple la fórmula*

$$r_k(N) = C_k N^{k/2-1} \sum_{d|N} (-1)^{N+N/d} d^{1-k/2} + O(N^{k/4})$$

donde $C_k = (2\pi)^{k/2}/(\zeta(k/2)(2^{k/2}-1)(k/2-1)!)$.

DEM.: Por los resultados anteriores y (4.2)

$$r_k(N) = \frac{(2\pi)^{k/2} N^{k/2-1}}{(k/2-1)!} S + O(N^{k/4}) \qquad \text{con} \quad S = \sum_{q \le \sqrt{N}/2} \frac{\delta_q}{q^{k/2}} \, c_q(-N).$$

Los términos $q > \sqrt{N}/2$ se pueden añadir a la suma conservando el término de error porque

$$\sum_{q > \sqrt{N}/2} \frac{\delta_q}{q^{k/2}} \, c_q(-N) = O\Big(\sum_{q > \sqrt{N}/2} \frac{1}{q^{k/2}} \cdot q \Big) = O(N^{1-k/4}).$$

Y basta aplicar el Lema 4.4 a la suma S completada con estos términos. ■

4.4. Sumas de primos

En esta sección utilizaremos el método del círculo para deducir el comportamiento asintótico del número de representaciones como suma de primos. Es decir, fijado k estudiaremos:

$$r_k(N) = \#\{(p_1, p_2, \ldots, p_k) \in (\mathbb{Z}^+)^k \, : \, N = p_1 + p_2 + \ldots + p_k \text{ con } p_i \text{ primo}\}.$$

El método tendrá éxito para $k > 2$, lo cual nos deja con la miel en los labios a las puertas de poder alcanzar la celebérrima conjetura de Goldbach. Ésta proviene de una carta que envió C. Goldbach a Euler en 1742, y aunque la conjetura original es ligeramente diferente (entre otras cosas porque él consideraba el uno como primo), en términos actuales se podría formular diciendo que todo número par mayor que dos es suma de dos números primos, y todo número impar mayor que cinco es suma de tres primos; siendo la primera afirmación la conjetura de Goldbach por antonomasia. El método del círculo confirma la segunda aserción para números suficientemente grandes (teorema de Vinogradov), donde "grande" significa hoy por hoy "grandísimo", porque el número finito de casos restantes (actualmente del orden de 10^{43000}) está todavía enormemente lejos de las capacidades de las computadoras. De hecho es un problema profundo, relacionado con los ceros de Siegel, dar una cota explícita del número de casos que faltan por comprobar.

Antes de comenzar haremos dos precisiones de tipo técnico. La primera es que al igual que en el primer capítulo era más sencillo aproximar bien $\psi(x)$ que $\pi(x)$ (la función identidad es más simple que el logaritmo integral), aquí será conveniente estudiar

$$r_k^*(N) = \sum_{n_1+n_2+\ldots+n_k=N} \Lambda(n_1)\Lambda(n_2)\cdots\Lambda(n_k)$$

en lugar de $r_k(N)$. Más adelante veremos la relación entre la asintótica de ambas cantidades.

La segunda observación es que como sólo hay un número primo par, el dos, es natural intuir que cuando las paridades de N y k no coinciden $r_k(N)$ será como k veces $r_{k-1}(N-2)$. Por ejemplo, si supiésemos que todo número par mayor que cuatro es suma de tres primos, es fácil ver que habríamos probado la conjetura de Goldbach, en realidad estamos representando un par como suma de dos primos sin más que restar el dos que necesariamente debe haber. De este modo se muestra natural considerar sólo el caso en que N y k tienen la misma paridad, porque el otro es consecuencia de él.

Aplicaremos el método del círculo en su versión "finita", escribiendo

$$r_k^*(N) = \int_0^1 S^k(x)e(-Nx)\,dx \qquad \text{con} \qquad S(x) = \sum_{n\le N} \Lambda(n)e(nx).$$

Al final del segundo capítulo vimos cómo acotar sumas trigonométricas del tipo de $S(x)$, lo cual servirá para dar cuenta de los arcos menores. Por otra parte, los arcos mayores llevan necesariamente al estudio de la distribución de los primos en progresiones aritméticas. Por ejemplo, es fácil ver que

$$S(1/3) = \big[(\log N)/\log 3\big]\log 3 + e(1/3)\psi(N;3,1) + e(2/3)\psi(N;3,2),$$

y en general $S(a/q)$ depende de $\psi(N;q,b)$ con $1 \le b < a$, donde se ha usado la notación introducida en la sección 1.9. Sólo hay que sumar por partes (esencialmente aplicar el lema de Abel) para pasar de a/q a valores de x muy cercanos a a/q. El gran problema está en que se sabe muy poco de la dependencia en q del error en el teorema de los números primos en progresiones aritméticas. A este respecto, definiendo $\psi(x,\chi) = \sum_{n\le x}\Lambda(n)\chi(n)$, se conoce ([**Da**] §22) que si $\chi \neq \chi_0$, el carácter módulo q que vale uno en todos los coprimos con q, para cualquier A se cumple

$$\psi(x,\chi) = O\left(\frac{x}{\log^A x}\right) \tag{4.4}$$

uniformemente en q. De donde para a y q coprimos, empleando la ortogonalidad de los caracteres ($\sum_\chi \overline{\chi}(a)\chi(n) \neq 0 \Leftrightarrow q|n-a$ con a y q coprimos), se tiene

$$\psi(x;q,a) = \frac{1}{\phi(q)} \sum_{\substack{n\leq N \\ (n,q)=1}} \Lambda(n) + \frac{1}{\phi(q)} \sum_{\chi\neq\chi_0} \overline{\chi}(a)\psi(x,\chi) = \frac{x}{\phi(q)} + O\bigg(\frac{x}{\log^A x}\bigg).$$

Nótese sin embargo que a pesar de la uniformidad, esta versión del teorema de los números primos en progresiones aritméticas se vuelve trivial si q crece ligeramente más rápido que una potencia de logaritmo (se cumple $\phi(q) \gg q/\log q$). Esto y la pobreza del término de error, se traducirá en que sólo podemos aproximar $S(a/q+\delta)$ para q y $N|\delta|$ menores que una potencia de logaritmo. En definitiva, elegiremos los arcos mayores como

$$\mathcal{M} = \sum_{\substack{q\leq \log^B N \\ (a,q)=1,\ 0<a\leq q}} I_{a/q} \qquad \text{con} \qquad I_{a/q} = \{x \,:\, |x-a/q| < (\log^B N)/N\}$$

donde B es un número positivo. Es evidente que para N mayor que cierta constante, los $I_{a/q}$ son disjuntos.

Todo lo que necesitamos saber en los arcos mayores está recogido en el siguiente resultado:

Teorema 4.10 . *Si $x \in I_{a/q}$ con a y q coprimos y $q \leq \log^B N$, entonces*

$$S(x) = \frac{\mu(q)}{\phi(q)} \sum_{n\leq N} e((x-a/q)n) + O\bigg(\frac{N}{\log^{2B} N}\bigg).$$

Dem.: Por razones técnicas será útil descartar los sumandos de $S(x)$ correspondientes a $(n,q) \neq 1$. Es fácil ver que su contribución es pequeña, cumpliéndose

$$S(x) = \sum_{\substack{n\leq N \\ (n,q)=1}} \Lambda(n)e(nx) + O(\log^2 N)$$

ya que q tiene $O(\log q)$ factores primos contando multiplicidades, y cada potencia de p aparece $O(\log N/\log p)$ veces hasta N.

Escribamos, para abreviar, $\delta = x - a/q$. Factorizando $e(nx) = e(an/q)e(n\delta)$ y empleando la ortogonalidad de los caracteres, se sigue

$$S(x) = \frac{1}{\phi(q)} \sum_{r=1}^{q} \sum_{\chi} \overline{\chi}(r) \sum_{n\leq N} \chi(n)\Lambda(n)e(ar/q)e(n\delta) + O(\log^2 N),$$

y agrupando términos

$$S(x) = \frac{1}{\phi(q)} \sum_{\chi} \tau(\overline{\chi}, a)\psi_\delta(N, \chi) + O(\log^2 N), \tag{4.5}$$

donde

$$\tau(\overline{\chi}, a) = \sum_{r=1}^{q} \overline{\chi}(r)e(ar/q) \qquad \text{y} \qquad \psi_\delta(N, \chi) = \sum_{n \le N} \chi(n)\Lambda(n)e(n\delta).$$

Por el lema de Abel y (4.4) con $A = 4B$, para $\chi \neq \chi_0$ (el carácter que vale idénticamente uno en $\mathbb{Z}_q^*$),

$$\psi_\delta(N, \chi) = e(N\delta)\psi(N, \chi) - 2\pi i\delta \int_1^N e(\delta t)\psi(t, \chi)\, dt \ll (1 + |\delta|N)\frac{N}{\log^{4B} N}.$$

Además aplicando como antes las propiedades de los caracteres, se tiene que

$$\sum_{\chi} |\tau(\overline{\chi}, a)|^2 = \sum_{r,s=1}^{q} \sum_{\chi} \overline{\chi}(r)\chi(s)e(a(r-s)/q) \le q\phi(q).$$

Así pues, por la desigualdad de Cauchy-Schwarz, la contribución a (4.5) de $\chi \neq \chi_0$ es $O\big((1 + |\delta|N)q^{1/2}N/\log^{4B} N\big)$.

Por otra parte, si $\chi = \chi_0$,

$$\psi_\delta(N, \chi_0) = \sum_{n \le N} e(n\delta) + \sum_{n \le N} (\Lambda(n) - 1)e(n\delta),$$

y una nueva aplicación del lema de Abel y de (4.4) al segundo sumatorio, prueba que éste es $O(N/\log^{4B} N)$. Como $\tau(\overline{\chi_0}, a)$ coincide con la suma de Ramanujan $c_q(a) = \mu(q)$, se deduce finalmente de (4.5)

$$S(x) = \frac{\mu(q)}{\phi(q)} \sum_{n \le N} e(n\delta) + O\left((1 + |\delta|N)q^{1/2}\frac{N}{\log^{4B} N}\right).$$

Sustituyendo $\delta = x - a/q$ y recordando los rangos de δ y q (de la definición de los arcos mayores), se llega al resultado deseado. ■

Los arcos menores son el complementario de los mayores, $\mathbf{m} = \mathbb{T} - \mathcal{M}$. Como hemos mencionado, la cota que emplearemos en ellos proviene de técnicas de sumas trigonométricas introducidas en el segundo capítulo.

Teorema 4.11 . *Se cumple la acotación*

$$\max_{x\in\mathbf{m}} |S(x)| \ll \frac{N}{\log^{B/2-4} N}.$$

DEM.: Aplicando la Proposición 2.13 con $N_1 = N_2 = N^{2/5}$ y $f(n) = nx$, se tiene

$$S(x) \ll N^{2/5} + M_1 \log N + M_2^{1/2} N^{1/2} \log^3 N \tag{4.6}$$

donde M_1 y M_2 son, respectivamente, los máximos valores posibles de las sumas

$$\sum_{i\le N^{4/5}} \Big| \sum_{k\le N/i} e(ikx)\Big| \qquad \text{y} \qquad \sum_{N^{2/5}<k\le N/I} \Big| \sum_{I<i\le 2I} e(i(j-k)x)\Big|$$

con $N^{2/5} < I \le N^{3/5}$ y $N^{2/5} \le j \le N/I$. Operando las sumas geométricas interiores, se deduce

$$M_1 \ll \sum_{i\le N^{4/5}} \min(N/i, |\operatorname{sen}(2\pi i x)|^{-1}), \qquad M_2 \ll N^{3/5} + \sum_{k'\le N^{3/5}} \min(N/k', |\operatorname{sen}(2\pi k' x)|^{-1})$$

donde se ha escrito $k' = |j-k|$, separando el caso $k' = 0$, y se ha empleado $I \le N/k'$.

Por el Lema 3.11, existe una fracción irreducible a/q con $1 \le q \le N/\log^B N$ tal que $|x - a/q| < (\log^B N)/N$. Además debe ser $q > \log^B N$ porque en otro caso $x \in I_{a/q}$ y estamos bajo la hipótesis de que $x \in \mathbf{m}$. En resumen, se puede escribir $x = a/q + \delta$ con $qN|\delta| \le \log^B N$ y $\log^B N < q \le N/\log^B N$. Por tanto para $i \le N^{4/5}$ se tiene $|ix - ia/q| = i|\delta| = o(1/q)$, de manera que $\operatorname{sen}(2\pi i x)$ y $\operatorname{sen}(2\pi i a/q)$ son comparables (su cociente está acotado) siempre que $2i/q \notin \mathbb{Z}$. Bajo esta hipótesis, según varía i, $|\operatorname{sen}(2\pi i a/q)|^{-1}$ tomará $O(1 + N^{4/5}/q)$ veces periódicamente valores acotados por $q/1$, $q/2$, $q/3$,... q/q (ya que $|\operatorname{sen} t|^{-1} \ll |t|^{-1}$ en $[-\pi/2, \pi/2]$). La contribución a M_1 de los términos con $2i/q \in \mathbb{Z}$ es claramente $Nq^{-1}\log N$, con lo cual

$$M_1 \ll Nq^{-1}\log N + (1 + N^{4/5}q^{-1})(q/1 + q/2 + \ldots + q/q) \ll N/\log^{B-1} N.$$

Este razonamiento evidentemente también se aplica a M_2 obteniéndose la misma cota. Sustituyendo en (4.6), el teorema queda probado. ■

Una vez completado nuestro análisis de los arcos mayores y menores sólo hay que unir las piezas para deducir una fórmula asintótica.

Teorema 4.12 . *Dado $A > 0$ y un entero $k > 2$, se cumple*

$$r_k^*(N) = \mathcal{P}_N \frac{N^{k-1}}{(k-1)!} + O\Big(\frac{N^{k-1}}{\log^A N}\Big) \quad con \quad \mathcal{P}_N = \prod_{p\nmid N}\Big(1+\frac{(-1)^{k+1}}{(p-1)^k}\Big)\prod_{p\mid N}\Big(1+\frac{(-1)^k}{(p-1)^{k-1}}\Big).$$

Además $\mathcal{P}_N$ permanece entre dos constantes absolutas positivas si N y k tienen la misma paridad.

DEM.: Veamos la contribución de cada uno de los $I_{a/q}$ pertenecientes a los arcos mayores. Según el Teorema 4.10

$$\int_{I_{a/q}} S^k(x)e(-Nx)\,dx = \int_{I_{a/q}} \Big(\frac{\mu(q)}{\phi(q)}\sum_{n\le N} e((x-a/q)n)\Big)^k e(-Nx)\,dx + O\Big(\frac{N^{k-1}}{\log^B N}\Big).$$

Como $\sum e(nt) \ll |t|^{-1}$ en $[-1/2, 1/2]$, se puede completar la segunda integral a este intervalo perdiendo a lo más $O\big(((\log^B N)/N)^{-k+1}\big)$ que es absorbido por el término de error.

Un sencillo argumento combinatorio para contar el número de representaciones de un entero positivo como suma de otros, prueba

$$\int_{-1/2}^{1/2}\Big(\sum_{n\le N} e((x-a/q)n)\Big)^k e(-Nx)\,dx = e(-Na/q)\int_{-1/2}^{1/2}\Big(\sum_{n\le N} e(nt)\Big)^k e(-Nt)\,dt$$

$$= e(-Na/q)\binom{N-1}{k-1} = e(-Na/q)\frac{N^{k-1}}{(k-1)!} + O(N^{k-2}).$$

Así pues, sumando la contribución de todos los $I_{a/q}$, se tiene

$$\int_{\mathcal{M}} S^k(x)e(-Nx)\,dx = \sum_{q\le \log^B N}\Big(\frac{\mu(q)}{\phi(q)}\Big)^k c_q(-N)\Big(\frac{N^{k-1}}{(k-1)!} + O\Big(\frac{N^{k-1}}{\log^B N}\Big)\Big).$$

Notando que $\phi(q) \gg q/\log q$ (de hecho se tiene algo mejor, Th. 328 [**Ha-Wr**]), se puede completar la sumación hasta infinito con un término de error despreciable, y el Lema 4.5 prueba

$$\int_{\mathcal{M}} S^k(x)e(-Nx)\,dx = \mathcal{P}_N\frac{N^{k-1}}{(k-1)!} + O\Big(\frac{N^k}{\log^B N}\Big).$$

Por otra parte, por el Teorema 4.11 se tiene

$$\int_{\mathbf{m}} S^k(x)e(-Nx)\,dx \ll \left(\frac{N}{\log^{B/2-4} N}\right)^{k-2} \int_{-1/2}^{1/2} |S(x)|^2 dx.$$

Por la identidad de Parseval, la última integral es

$$\sum_{n\leq N} (\Lambda(n))^2 \leq \log N \sum_{n\leq N} \Lambda(n) \ll N \log N.$$

Combinando la contribución de los arcos mayores y menores, y eligiendo adecuadamente B, se deduce la fórmula del enunciado.

Si N y k tienen la misma paridad, entonces todos los factores de $\mathcal{P}_N$ son estrictamente positivos (sólo hay que examinar el caso $p = 2$), y demostrar que $\mathcal{P}_N$ está entre dos constantes absolutas positivas equivale a ver que $|\log \mathcal{P}_N|$ está uniformemente acotado, lo cual se sigue de

$$|\log \mathcal{P}_N| \leq \sum_p \frac{2}{(p-1)^{k-1}},$$

donde se ha usado la desigualdad $|\log(1+x)| \leq 2|x|$ válida en $[-1/2, 1]$. ■

Como hemos mencionado al principio, hemos trabajado con $r_k^*(N)$ únicamente para simplificar los argumentos. Una vez que hemos probado lo que queríamos, podemos volver a nuestra función favorita $r_k(N)$.

Corolario 4.13. *Dado un entero $k > 2$, para $N \equiv k \pmod 2$ se verifica la fórmula asintótica*

$$r_k(N) \sim \mathcal{P}_N \frac{N^{k-1}}{(k-1)! \log^k N}.$$

En particular, todo número impar suficientemente grande es suma de tres primos (teorema de Vinogradov).

DEM.: Es fácil deducir del teorema de los números primos que hay $O(N^{1/2})$ potencias de primos de exponente mayor que uno en $[1, N]$. Por consiguiente

$$r_k^*(N) = \sum_{p_1+p_2+\ldots+p_k=N} (\log p_1)(\log p_2)\cdots(\log p_k) + O(N^{k-3/2}\log^k N),$$

ya que, por ejemplo, hay $O(N^{(k-2)+1/2})$ posibilidades paa $(p_1, p_2, \ldots, p_{k-1})$ si sabemos que p_{k-1} es una potencia de primo como antes. Es evidente que el sumatorio está mayorado por $r_k(N)\log^k N$. Por otra parte, la contribución de los sumandos con algún $p_i \leq N^{1-\epsilon}$, $0 < \epsilon < 1$, es $O(N^{(k-2)+1-\epsilon}\log^k N)$, de forma que el sumatorio vale

$$\sum_{\substack{p_1+p_2+\ldots+p_k=N \\ p_1,p_2,\ldots,p_k \geq N^{1-\epsilon}}} (\log p_1)(\log p_2)\cdots(\log p_k) + O(N^{k-1-\epsilon}\log^k N)$$

$$\geq (1-\epsilon)^k(\log^k N) \sum_{\substack{p_1+p_2+\ldots+p_k=N \\ p_1,p_2,\ldots,p_k \geq N^{1-\epsilon}}} 1 + O(N^{k-1-\epsilon}\log^k N).$$

De la misma forma, podemos añadir los términos con $p_i \leq N^{1-\epsilon}$ al último sumatorio con una pérdida comparable al término de error.

Uniendo estos resultados,

$$(1-\epsilon)^k r_k(N)\log^k N + O(N^{k-1-\epsilon}\log^k N) \leq r_k^*(N) \leq r_k(N)\log^k N + O(N^{k-3/2}\log^k N).$$

Diviendo entre $\mathcal{P}_N N^{k-1}/(k-1)!$ y aplicando el teorema anterior, se deduce que los límites superior e inferior de $(k-1)!r_k(N)(\log^k N)/(\mathcal{P}_N N^{k-1})$ están acotados entre 1 y $(1-\epsilon)^{-k}$, y basta tomar $\epsilon \to 0$. ■

Si creemos en la preponderancia de la contribución de los arcos mayores, el corolario anterior debería ser cierto también para $k = 2$, lo cual probaría la conjetura de Goldbach para números pares mayores que cierta constante. Sin embargo hay serias dificultades teóricas que hacen poco creíble un acercamiento definitivo a la conjetura con el método del círculo. Si queremos conservar el esquema de la prueba con unos arcos menores que tienen la mayor parte de la medida, la cota del Teorema 4.11 debería ser de orden menor que $N^{1/2}$ para que $|S(x)|^2$ no interfiriese con el término principal $\mathcal{P}_N N^{2-1}/(2-1)! \gg N$. Esto choca frontalmente con la filosofía de las sumas trigonométricas (véase el segundo capítulo) que muestra la raíz cuadrada de los términos como un límite natural de la cancelación.

En el lado positivo, el método del círculo sí permite probar (véase **[Va]**) que la fórmula asintótica conjeturada para $r_2(N)$ es cierta quizá omitiendo un subconjunto de los pares muy fino, de densidad nula. Además J.-R. Chen demostró utilizando técnicas de criba que el número de representaciones de un número par como suma de dos primos o como suma de un primo y un producto de dos primos es comparable a $N/\log^2 N$. Aquí también aparecen dificultades teóricas aparentemente irreparables que impiden descontar las representaciones correspondientes al segundo caso.

Referencias

[**Be**] B.C. Berndt, R.A. Rankin. Ramanujan: letters and commentary. History of mathematics 9. American Mathematical Society, 1995.

[**Ci-Co**] F.J. Cilleruelo, A. Córdoba. La teoría de los números. Biblioteca Mondadori 27. Mondadori 1992.

[**Da**] H. Davenport. Multiplicative number theory (2nd ed.). Graduate texts in Mathematics 74. Springer, 1980.

[**Dy-Mc**] H. Dym, H.P. McKean. Fourier series and integrals. Academic Press, 1972.

[**Ed**] H.M. Edwards. Riemann's zeta function. Pure and applied Mathematics 58. Academic Press, 1974.

[**El**] W.J. Ellison, M.M. France. Les nombres premiers. Actualits scientifiques et industrielles 1366. Hermann, cop. 1975.

[**Ga**] C.F. Gauss. Mathematisches Tagebuch, 1796-1814. Akademische Verlagsgesellschaft Geest & Portig K.-G., 1976.

[**Gr**] E. Grosswald. Representations of integers as sums of squares Springer-Verlag, 1985

[**Gr-Ko**] S.W. Graham, G. Kolesnik. Van der Corput's method of exponential sums. London Mathematical Society lecture note series 126. Cambridge University Press, 1991.

[**Gr-Ry**] I.S. Gradshteyn, I.M. Ryzhik. Table of integrals, series and products. Academic Press, 1994.

[**Ha**] G.H. Hardy. The average of the functions $P(x)$ and $\Delta(x)$. Proc. London Math. Soc. (2) 15, 192-213 (1916).

[**Ha-Wr**] G.H. Hardy, E.M. Wright. An introduction to the theory of numbers. Clarendon Press, 1979.

[**Hu**] M.N. Huxley. Area, Lattice Points, and Exponential Sums. Clarendon Press. Oxford 1996.

[**Iv**] A. Ivić. The Riemann zeta-function: the theory of the Riemann zeta-function with applications. Wiley 1985.

[**Ka**] A.A. Karatsuba. Fundamentos de la teoría analítica de los números. Editorial Mir, 1979.

[**Li**] M.J. Lighthill. Fourier Analysis and Generalised Functions. Cambridge University Press, 1970.

[**Mo**] H.L. Montgomery. Ten lectures on the interface between analytic number theory and harmonic analysis. Regional conference series in mathematics 84. American Mathematical Society, 1994.

[**Se**] A. Selberg. Collected papers. Springer-verlag, 1989.

[**Sm**] D.E. Smith. A source book in Mathematics. Dover Publications, 1959.

[**So**] C.D. Sogge. Fourier integrals in classical analysis. Cambridge tracts in Mathematics 105. Cambridge University Press, 1993.

[**Sp**] M. Spivak. Calculus. Reverté, D.L. 1981.

[**Ti**] E.C. Titchmarsh. The theory of the Riemann zeta-function (2nd ed.). Clarendon, 1986.

[**Va**] R.C. Vaughan. The Hardy-Littlewood method. Cambridge tracts in Mathematics 80. Cambridge University Press, 1981.

[**We**] H. Weyl. Über die Gleichverteilung von Zahlen mod. Eins. Math. Ann. 77, 313-352 (1916).

[**Yn**] F.J. Ynduráin. Mecánica cuántica. Alianza Universidad Textos. Alianza, 1988.

[**Za**] A. Zaharescu. Small values of $n^2\alpha \pmod 1$. Invent. Math. 121, 379–388 (1995).