Capítulo 2

Nociones de teoría analítica

2.1. Funciones aritméticas y series de Dirichlet

Convolución. Productos de Euler. Inversión de Möbius. Promedios de funciones aritméticas.

En cierto contexto de la teoría de números es tradición renombrar las sucesiones, reales o complejas, y llamarlas *funciones aritméticas*. Es decir, una función aritmética no es más que una función $f : \mathbb{Z}^+ \longrightarrow \mathbb{C}$.

Sobre todo en problemas relacionados con los números primos, es conveniente asociar a cada función aritmética una serie compleja llamada *serie de Dirichlet* dada por

$$D_f(s) = \sum_{n=1}^{\infty} \frac{f(n)}{n^s}.$$

Dependiendo de f, la serie $D_f(s)$ puede converger o no para cierto valor del parámetro s que se supone complejo. De hecho podría no converger nunca. Es fácil ver que la convergencia absoluta en un subconjunto propio siempre ocurre en semiplanos salvo que la convergencia en la frontera está indeterminada. Concretamente, siempre existe $\sigma \in \mathbb{R} \cup \{\pm\infty\}$ tal que la serie converge absolutamente en $\{\Re(s) > \sigma\}$ y no converge absolutamente en $\{\Re(s) < \sigma\}$. En realidad, esto también ocurre con la convergencia usual, aunque es más difícil de probar [43, Cor. 1.2].

Dentro de las funciones aritméticas, tienen especial relevancia las que dependen de la factorización, lo que motiva definir una *función aritmética multiplicativa* como una función aritmética f no idénticamente nula que cumple

$$f(mn) = f(m)f(n) \qquad \text{para} \quad \gcd(m, n) = 1.$$

Se dice que es *completamente multiplicativa* si la igualdad se cumple sin la condición $\gcd(m, n) = 1$. Nótese que las funciones multiplicativas cumplen necesariamente $f(1) = 1$.

Ya sabemos que φ, la función de Euler, es multiplicativa (por el Corolario 1.2.4) y es fácil ver que no lo es completamente. Por ejemplo, se cumple $\varphi(4) = 2$ y $\varphi(2)\varphi(2) = 1$. La fórmula general $\varphi\big(\gcd(m,n)\big)\varphi(mn) = \varphi(m)\varphi(n)\gcd(m,n)$ muestra cómo influyen los factores comunes.

La función aritmética completamente multiplicativa más tonta es la que vale idénticamente 1. Su serie de Dirichlet asociada es la famosa *función ζ de Riemann*

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} \tag{2.1}$$

que converge absolutamente en $\Re(s) > 1$.

Euler estableció la relación de esta serie de Dirichlet con los números primos, notando que, formalmente (sin preocuparse de cuestiones de convergencia), el teorema fundamental de la aritmética implica

$$\sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_{p} \Big(1 + \frac{1}{p^s} + \frac{1}{(p^2)^s} + \frac{1}{(p^3)^s} + \dots\Big)$$

donde p recorre los primos. Sumando la progresión geométrica de cada factor se obtiene el *producto de Euler* por antonomasia:

$$\zeta(s) = \prod_{p} (1 - p^{-s})^{-1}. \tag{2.2}$$

Avanzando algo que desarrollaremos más tarde, B. Riemann fue más allá y logró, en cierto modo, despejar de esta relación los primos en términos de ζ. En una revolucionaria y brevísima memoria mostró que la distribución de los números primos está ligada al estudio de ζ como una función de variable compleja.

Para cualquier función multiplicativa podemos proceder de la misma manera y obtener también un *producto de Euler* (que a veces se califica de *generalizado*). Concretamente

$$D_f(s) = \prod_{p} D_{f,p}(s) \qquad \text{con} \qquad D_{f,p}(s) = 1 + \frac{f(p)}{p^s} + \frac{f(p^2)}{p^{2s}} + \frac{f(p^3)}{p^{3s}} + \dots \tag{2.3}$$

Si f es completamente multiplicativa, sumando la progresión geométrica, $D_{f,p}(s) = \big(1 - f(p)p^{-s}\big)^{-1}$. Por otro lado, la identidad formal anterior, cambiando el 1 de $D_{f,p}(s)$ por $f(1)$, implica que f es multiplicativa.

Para tranquilidad de los más exigentes con el rigor, estas identidades formales tienen sentido numérico exigiendo la convergencia absoluta, como indica el siguiente enunciado. La demostración es sencilla, pero la omitiremos aquí [43, Th. 1.9].

Lema 2.1.1. *Si f es multiplicativa y $D_f(s)$ converge absolutamente para cierto s, entonces el producto en* (2.3) *converge a $D_f(s)$.*

Por ejemplo, en cursos de análisis se prueba, habitualmente empleando series de Fourier, $\zeta(2) = \pi^2/6$ (*problema de Basilea*) y $\zeta(4) = \pi^2/90$. De (2.2) se deducen las identidades espectaculares

$$\prod_p (1-p^{-2}) = \frac{6}{\pi^2} \qquad \text{y} \qquad \prod_p (1+p^{-2}) = \prod_p \frac{(1-p^{-2})^{-1}}{(1-p^{-4})^{-1}} = \frac{15}{\pi^2}.$$

Dadas dos funciones aritméticas f y g se define su *convolución* como

$$(f*g)(n) = \sum_{d|n} f(d)g(n/d). \tag{2.4}$$

Aquí se sobreentiende $d \in \mathbb{Z}^+$. Es fácil ver que es conmutativa, es decir, $f*g = g*f$. El nombre no es gratuito, tiene cierto paralelismo con la operación homónima en análisis armónico abstracto.

La convolución se refleja fielmente en las series de Dirichlet. De nuevo, si uno renuncia a entrar en cuestiones de convergencia, todo se reduce a cálculos formales directos.

▶ **Proposición 2.1.2.** *La relación $h = f*g$ entre funciones aritméticas equivale a $D_h(s) = D_f(s)D_g(s)$ con igualdad numérica para todo $s \in \mathbb{C}$ tal que $D_f(s)$ y $D_g(s)$ converjan absolutamente. Además, si f y g son multiplicativas, h también lo es y $D_{h,p}(s) = D_{f,p}(s)D_{g,p}(s)$ con igualdad numérica bajo la convergencia absoluta de $D_{f,p}(s)$ y $D_{g,p}(s)$.*

Demostración. Escribiendo $n = dm$ se tiene que $D_h(s)$ es

$$\sum_{n=1}^{\infty}\sum_{d|n} n^{-s}f(d)g(n/d) = \sum_{d=1}^{\infty}\sum_{m=1}^{\infty} d^{-s}m^{-s}f(d)g(m) = D_f(s)D_g(s).$$

Si $D_f(s)$ y $D_g(s)$ son absolutamente convergentes, es lícita la reordenación de los términos a voluntad (que en las igualdades anteriores se requiere para cambiar el orden de sumación) y con ello se tiene las igualdades numéricas. Nótese que $\sum_{n=1}^{N} \left|h(n)n^{-s}\right| \leq \sum_{n=1}^{N} \left|f(n)n^{-s}\right| \sum_{n=1}^{N} \left|g(n)n^{-s}\right|$.

Veamos ahora una prueba libre de series de Dirichlet, y por tanto de condiciones de convergencia, de que si f y g son multiplicativas h también lo es. El punto fundamental es que si $d \mid mn$ para $\gcd(m,n) = 1$ cada potencia de primo que aparece en la factorización de d debe dividir a m o a n (y no a ambos), ya que en otro caso entraríamos en contradicción con el Lema 1.1.6. Por tanto cada $d|mn$ se descompone de manera única como $d = d_1d_2$ con $d_1 \mid m$ y $d_2 \mid n$ y se tiene

$$h(mn) = \sum_{d|mn} f(d)g\Big(\frac{mn}{d}\Big) = \sum_{d_1|m}\sum_{d_2|n} f(d_1d_2)g\Big(\frac{m}{d_1}\frac{n}{d_2}\Big).$$

El argumento de la suma es $f(d_1)f(d_2)g(m/d_1)g(n/d_2)$, por ser f y g multiplicativas, y se obtiene $h(m)h(n)$.

En el caso de convergencia absoluta de $D_f(s)$ y $D_g(s)$ también se tendrá dicha convergencia para las series de Dirichlet asociadas a $f_p(n)$ y $g_p(n)$ definidas como $f(n)$ y $g(n)$ si n es una potencia de p y cero en otro caso. Sus series asociadas son $D_{f,p}$ y $D_{g,p}$ y h_p definida de la misma forma es $f_p * g_p$, por tanto $D_{h,p}(s) = D_{f,p}(s)D_{g,p}(s)$ se sigue de la primera parte. □

Llamemos **1** a la función aritmética (multiplicativa) que vale constantemente uno y τ a la *función divisor* que cuenta el número de divisores. Por ejemplo, $\tau(2) = 2$, $\tau(12) = 6$. Es evidente que $\tau = \mathbf{1} * \mathbf{1}$, con ello concluimos que τ es multiplicativa y se obtiene una fórmula en términos de la factorización de $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$,

$$\tau(n) = \tau(p_1^{\alpha_1})\tau(p_2^{\alpha_2}) \cdots \tau(p_k^{\alpha_k}) = (\alpha_1 + 1)(\alpha_2 + 1) \cdots (\alpha_k + 1).$$

Introduzcamos ahora la *función de Möbius* que es la función multiplicativa que verifica $\mu(p) = -1$ y $\mu(p^\alpha) = 0$ para $\alpha > 1$. Si uno prefiere una versión más explícita, se tiene

$$\mu(n) = \begin{cases} 1 & \text{si } n = 1, \\ (-1)^r & \text{si } n = p_1 p_2 \cdots p_r \quad \text{(primos distintos)}, \\ 0 & \text{en otro caso .} \end{cases}$$

Según (2.3) y (2.2)

$$D_\mu(s) = \prod_p (1 - p^{-s}) = \frac{1}{\zeta(s)}. \tag{2.5}$$

La convergencia en $\Re(s) > 1$ está asegurada por el Lema 2.1.1, lo cual, dicho sea de paso, implica que $\zeta(s)$ no se anula en $\Re(s) > 1$. Según la Proposición 2.1.2, multiplicar por ζ está asociado a convolver con **1** que es lo mismo que sumar sobre los divisores. Entonces (2.5) implica $\mu * (\mathbf{1} * f) = f$. De una manera más explícita:

Corolario 2.1.3 (Fórmula de inversión de Möbius)**.** *Dada f función aritmética, sea $F(n) = \sum_{d|n} f(d)$ entonces $f(n) = \sum_{d|n} \mu(d)F(n/d)$.*

Esta relación fue introducida por A. F. Möbius, el mismo que concibió la famosa banda, con un enunciado ligeramente distinto más "analítico".

Tomando $f(n) = 1$ y $f(n) = 0$ para $n > 1$, se sigue la fórmula

$$\sum_{d|n} \mu(d) = \begin{cases} 1 & \text{si } n = 1, \\ 0 & \text{si } n > 1. \end{cases}$$

En contra de lo que parece a primera vista, este humilde detector de unos desempeña en algunos temas un papel destacado y resume la inversión de Möbius, siendo equivalente a ella.

La función de Möbius está ligada a la función φ. Por el Corolario 1.2.5,

$$\frac{\varphi(n)}{n} = \prod_{p|n} \Big(1 - \frac{1}{p}\Big) = \sum_{d|n} \frac{\mu(d)}{d}.$$

Despejando $\varphi(n)$ se obtiene $\varphi = \mu * \mathrm{id}$ con $\mathrm{id}(n) = n$, la función identidad, lo que se traduce en términos de series de Dirichlet en

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

Por otro lado, la fórmula de inversión de Möbius implica $\mathrm{id} = \mathbf{1} * \varphi$. Esto es, $n = \sum_{d|n} \varphi(d)$.

También se podría proceder en el sentido contrario probando de manera combinatoria $n = \sum_{d|n} \varphi(d)$ y deduciendo la fórmula inicial para $\varphi(n)/n$ a partir del Corolario 2.1.3. Tal prueba combinatoria pasa por considerar que todo número $1 \leq m \leq n$ admite una descomposición como $m = d \cdot m/d$ donde d divide a n y m/d es coprimo con n/d, simplemente eligiendo el divisor mayor posible, es decir, $d = \gcd(m, n)$. Dado d, hay $\varphi(n/d)$ posibilidades para m/d, por tanto $n = \sum_{d|n} \varphi(n/d)$ y se puede cambiar $\varphi(n/d)$ por $\varphi(d)$ gracias a la biyección entre divisores $d \leftrightarrow n/d$. En [22, Th. 63] se incluye una prueba basada en que φ es multiplicativa.

Para algunas funciones aritméticas la expresión como una convolución permite aproximar su promedio gracias al siguiente resultado elemental:

Lema 2.1.4. *Si $h = f * g$ entonces*

$$\sum_{n=1}^{N} h(n) = \sum_{k=1}^{N} f(k) \sum_{1 \leq \ell \leq N/k} g(\ell).$$

Se ha supuesto implícitamente que $N \in \mathbb{Z}^+$, pero nada impide tomar $N \in \mathbb{R}_{\geq 1}$ escribiendo en los límites de las sumas $1 \leq n \leq N$ y $1 \leq k \leq N$.

Demostración. Tomando $k = d$ y $\ell = n/d$ en (2.4), basta notar que $1 \leq n \leq N$ equivale a $1 \leq k\ell \leq N$. □

Un poco más elaborada, aunque todavía elemental, es la siguiente versión dependiente de un parámetro ajustable t. Formalmente para $t > N$ obtenemos el resultado anterior. Jugar con t tiene sentido si conocemos bien los promedios de f y g.

Lema 2.1.5 (Método de la hipérbola)**.** *Si $h = f * g$, para t real en $[1, N]$ se cumple*

$$\sum_{n=1}^{N} h(n) = \sum_{k\le t} f(k) \sum_{\ell\le N/k} g(\ell) + \sum_{\ell\le N/t} g(\ell) \sum_{k\le N/\ell} f(k) - \sum_{k\le t} f(k) \sum_{\ell N/t} g(\ell)$$

donde k y ℓ toman valores enteros positivos.

Demostración. Procediendo como en la demostración anterior, hay que sumar $f(k)g(\ell)$ sobre los puntos $(k, \ell) \in (\mathbb{Z}^+)^2$ con $1 \le k\ell \le N$. Gráficamente estamos considerando los puntos de coordenadas enteras positivas en la región bajo la hipérbola $xy = N$ en el primer cuadrante. Esta región se descompone en la parte dentro de la banda vertical $x \in (0, t]$, donde $y \le N/x$, y en la parte dentro de la banda horizontal $y \in (0, N/t]$, con $x \le N/y$. Esto da lugar a los límites de los dos primeros sumatorios. Los del último se deben a que estas dos bandas tienen como intersección el rectángulo $(0, t] \times (0, N/t]$ y por tanto hemos sumado en esos puntos dos veces. □

Antes de ver ejemplos, introduzcamos un poco de notación habitual en las fórmulas asintóticas. Escribiremos $f \sim g$ y $f = O(g)$ para indicar, respectivamente,

$$\lim \frac{f}{g} = 1 \qquad \text{y} \qquad \limsup \frac{|f|}{|g|} < \infty.$$

Muchas veces se combina $O(g)$ con las operaciones elementales, especialmente con la suma. Así $h + O(g)$ significa $h + f$ para cierta función no explícita que cumple $f = O(g)$. En esta sección utilizaremos estas notaciones cuando la variable tiende a infinito, pero también se aplican a funciones reales o complejas en otros valores, que normalmente se sobreentienden. Por ejemplo, uno podría escribir $e^x = 1 + x + O(x^2)$ para indicar que el error de Taylor es una función acotada por $K|x|^2$, sin especificar K, en un entorno de 0, de modo que el límite superior se toma con $x \to 0$. También se cumple $\operatorname{sen} x \sim x$, entendiendo que estamos en las cercanías de cero. Cuando hay duda se indica explícitamente a qué tiende la variable.

En un primer ejemplo examinemos un promedio relacionado con la función φ. Si n recorre los primos, $\varphi(n) \sim n$ y, por otra parte, el Corolario 1.2.5 implica que si n tiene factores primos pequeños, $\varphi(n)$ es bastante menor que n. No está muy claro cuál de estas dos tendencias predomina. Para ello, estudiemos la suma de $h(n) = \varphi(n)/n$. Sabíamos que

$$h = f * g \qquad \text{con} \quad f(n) = \frac{\mu(n)}{n} \quad \text{y} \quad g = \mathbf{1}.$$

Por el Lema 2.1.4,

$$\sum_{n=1}^{N} \frac{\varphi(n)}{n} = \sum_{k=1}^{N} \frac{\mu(k)}{k} \left\lfloor \frac{N}{k} \right\rfloor = \sum_{k=1}^{N} \frac{\mu(k)}{k} \Big(\frac{N}{k} + O(1) \Big) = N \sum_{k=1}^{N} \frac{\mu(k)}{k^2} + O(\log N)$$

porque, aproximando por la integral, $1+1/2+\cdots+1/N \sim \log N$. De hecho, es bien conocido que la diferencia entre estas dos cantidades tiende a una constante $C = 0{,}57721\ldots$ llamada *constante de Euler-Mascheroni*. Esto es,

$$C = \lim_{N\to\infty}\Big(\sum_{k=1}^{N}\frac{1}{k} - \log N\Big), \quad \text{incluso} \quad \sum_{k=1}^{N}\frac{1}{k} = \log N + C + O(N^{-1}). \tag{2.6}$$

De nuevo, aproximando por la integral, $\sum_{k>N} k^{-2} = O(N^{-1})$ y se tiene

$$\sum_{n=1}^{N}\frac{\varphi(n)}{n} = N\sum_{k=1}^{\infty}\frac{\mu(k)}{k^2} + O(1) + O(\log N) = ND_\mu(2) + O(\log N).$$

Sabemos que $D_\mu = 1/\zeta$ y $\zeta(2) = \pi^2/6$, por tanto $D_\mu(2) = 6/\pi^2$. Así pues hemos probado

$$\sum_{n=1}^{N}\frac{\varphi(n)}{n} \sim \frac{6}{\pi^2}N.$$

Es decir, el promedio de $\varphi(n)/n$ es $6/\pi^2$, lo cual es, ciertamente, poco intuitivo.

El error $O(\log N)$ tiene orden de magnitud mucho menor que N, por tanto cabe esperar que la aproximación sea razonable numéricamente en lo que respecta al error relativo, como ilustra la siguiente tabla:

	$N = 10$	$N = 100$	$N = 1000$
$\dfrac{\pi^2}{6N}\displaystyle\sum_{n=1}^{N}\frac{\varphi(n)}{n} - 1$	0,023775631	0,000657508	0,000375392

Apliquemos ahora el Lema 2.1.4 a $\tau = \mathbf{1} * \mathbf{1}$ para obtener

$$\sum_{n=1}^{N}\tau(n) = \sum_{k=1}^{N}\Big\lfloor\frac{N}{k}\Big\rfloor = \sum_{k=1}^{N}\Big(\frac{N}{k} + O(1)\Big) = N\sum_{k=1}^{N}\frac{1}{k} + O(N).$$

Por (2.6) el sumatorio es $\log N + O(1)$ y concluimos

$$\sum_{n=1}^{N}\tau(n) = N\log N + O(N) \qquad \text{y} \qquad \sum_{n=1}^{N}\tau(n) \sim N\log N.$$

Aquí el término principal $N\log N$ es de orden solo ligeramente superior al error estimado, con lo cual no hay garantías de que la aproximación sea numéricamente buena, de hecho el error relativo no es pequeño para valores muy grandes de N.

El Lema 2.1.5 permite una aproximación más precisa gracias a que τ es convolución de funciones sencillas. Dejando t libre, se obtiene

$$\sum_{n=1}^{N}\tau(n)=\sum_{k\le t}\frac{N}{k}+O(t)+\sum_{\ell\le N/t}\frac{N}{\ell}+O\Big(\frac{N}{t}\Big)-\big(t+O(1)\big)\Big(\frac{N}{t}+O(1)\Big).$$

Para minimizar la suma de los errores $O(t)$ y $O(N/t)$ la mejor elección es $t=\sqrt{N}$. Teniendo en cuenta (2.6), se obtiene

$$\sum_{n=1}^{N}\tau(n)=2N\big(\log\sqrt{N}+C+O(N^{-1/2})\big)-N+O(\sqrt{N}).$$

En definitiva,

$$\sum_{n=1}^{N}\tau(n)=N\log N+(2C-1)N+O(\sqrt{N}).$$

Una antigua conjetura en teoría de números afirma que $\sqrt{N}$ puede reemplazarse por N^{α} para cualquier $\alpha>1/4$ por cercano que esté a $1/4$. Este es el llamado *problema del divisor*. Cómo llegar a $\sqrt[3]{N}$ es conocido desde los primeros años del siglo XX mientras que mejorarlo ligeramente requiere técnicas bastante avanzadas.