Introducción a la Teoría Analítica de Números

Pablo De Nápoli

clase 2

1. Propiedades de la función de Euler

Recordamos las fórmulas que probamos la clase anterior:

$$\sum_{d|n} \varphi(d) = n$$

y utilizando la fórmula de inversión de Möbius

$$\varphi(n) = \sum_{d|n} \frac{n}{d}\mu(d) = \sum_{d|n} d\mu\left(\frac{n}{d}\right) \tag{1}$$

Ahora utilizamos esta fórmula para dar otra expresión de $\varphi(n)$:

Teorema 1.1 *Para todo $n \in \mathbb{N}$,*

$$\varphi(n) = n\prod_{p|n}\left(1 - \frac{1}{p}\right)$$

donde el producto se extiende sobre los divisores primos de n.

Prueba: Supongamos que n admite la factorización

$$n = p_1^{e_1}p_2^{e_2}\dots p_k^{e_k}$$

Entonces efectuando la distributiva

$$\prod_{p|n}\left(1 - \frac{1}{p}\right) = 1 - \sum \frac{1}{p_{i_1}} + \sum \frac{1}{p_{i_1}p_{i_2}} - \sum \frac{1}{p_{i_1}p_{i_3}p_{i_3}} + \ldots + (-1)^k \sum \frac{1}{p_{i_1}p_{i_2}\dots p_{i_k}}$$

(donde los p_{i_j} se eligen entre los divisores primos $p_1, p_2, \dots, p_k$ de n).

Teniendo en cuenta la definición de μ, vemos que esta suma es igual a

$$\sum_{d|n} \frac{\mu(d)}{d}$$

Comparando con la fórmula (1), se obtiene el teorema. □

Teorema 1.2 *Sean $m, n \in \mathbb{N}$ y sea $d = (m.m)$ su máximo común divisor entonces:*

$$\varphi(mn) = \varphi(m)\varphi(n)\frac{d}{\varphi(d)}$$

Prueba: Utilizando la fórmula del teorema anterior,

$$\frac{\varphi(nm)}{nm} = \prod_{p|nm}\left(1-\frac{1}{p}\right) = \frac{\prod_{p|n}\left(1-\frac{1}{p}\right)\prod_{p|m}\left(1-\frac{1}{p}\right)}{\prod_{p|d}\left(1-\frac{1}{p}\right)} == \frac{\varphi(n)}{n}\frac{\varphi(m)}{m}\frac{d}{\varphi(d)}$$

□

Corolario 1.1 *Si n y m son coprimos, entonces*

$$\varphi(nm) = \varphi(n)\varphi(m)$$

2. Funciones Multiplicativas

Esta propiedad es de gran importancia, y es compartida por muchas funciones aritméticas, por lo que es conveniente darle un nombre:

Definición 2.1 *Una función aritmética $f : \mathbb{N} \to \mathbb{C}$ se dice* **multiplicativa** *si para $n, m \in \mathbb{N}$ coprimos se verifica que*

$$f(nm) = f(n)f(m)$$

Si se verifica que $f(nm) = f(n)f(m)$ para todos los $n, m \in \mathbb{N}$, decimos que f es **completamente multiplicativa**.

Algunas observaciones:

1. φ es multiplicativa pero no es completamente multiplicativa pues

$$\varphi(4) = 2 \text{ pero } \varphi(2)\varphi(2) = 4$$

2. μ es una función multiplicativa.
3. Una función multiplicativa no idénticamente nula verifica que $f(1) = 0$.
4. Si f es multiplicativa y $m_1, m_2, \ldots m_k$ son coprimos dos a dos, entonces

$$f(m_1 m_2 \ldots m_k) = f(m_1)f(m_2)\ldots f(m_k)$$

5. Una función multiplicativa está determinada por lo que vale en las potencias de los primos: si n admite una factorización en primos

$$n = \prod_{p|n} p^{v_p(n)}$$

y f es multiplicativa

$$f(n) = \prod_{p|n} f\left(p^{v_p(n)}\right)$$

pues las potencias de primos distintos son coprimas dos a dos. Si f es multiplicativa, f queda determinada por su valor en los primos, pues en este caso tenemos

$$f(n) = \prod_{p|n} f\left(p\right)^{v_p(n)}$$

Observación 2.1 *Dado que la descomposición de un entero n en factores primos es única, podemos definir una función aritmética $v_p : \mathbb{N} \to \mathbb{N}_0$ especificando que $v_p(n)$ es el exponente del primo p en la factorización de n. Esta función se conoce como la* **valuación p-ádica**. *Entonces, la factorización de n es:*

$$n = \prod_{p|n} p^{v_p(n)}$$

Convenimos en que $v_p(n) = 0$ si el primo p no aparece en la factorización de n. Con este convenio podemos escribir:

$$n = \prod_{p} p^{v_p(n)}$$

donde él producto (formalmente infinito) sobre todos los primos es en realidad finito, pues sólo un número finito de factores es diferente de 1.

Alternativamente podemos definir v_p por

$$v_p(n) = \text{máx}\{k \in \mathbb{N}_0 : p^k | n\}$$

Notamos que v_p tiene la siguiente propiedad, análoga a la del logaritmo:

$$v_p(ab) = v_p(a) + v_p(b) \; \forall \; a, b \in \mathbb{N}$$

Teorema 2.1 *Si $f, g : \mathbb{N} \to \mathbb{C}$ son funciones aritméticas multiplicativas, también lo es su convolución de Dirichlet $h = f * g$.*

Prueba: La prueba de este teorema se basa en la siguiente observación: si $m = m_1 m_2$ con m_1 y m_2 coprimos, entonces cada divisor d de m se puede factorizar de manera única como $d = d_1 d_2$ donde $d_1 | m_1$ y $d_2 | m_2$. Para ello, basta tomar:

$$d_1 = \prod_{p|m_1} p^{v_p(d)}, \quad d_2 = \prod_{p|m_2} p^{v_p(d)}$$

Recíprocamente, si $d = d_1 d_2$ con $d_1 | m_1$ y $d_2 | m_2$, entonces $d = d_1 d_2$ es un divisor de m.

Además, en esta situación d_1 y d_2 son coprimos, asi como m_1/d_1 y m_2/d_2 son coprimos. Por lo tanto:

$$h(m) = \sum_{d|m} f(d)g\left(\frac{m}{d}\right) = \sum_{d_1|m_1, d_2|m_2} f(d_1 d_2)g\left(\frac{m_1 m_2}{d_1 d_2}\right)$$

Utilizando que f y g son multiplicativas, esto es igual a:

$$\sum_{d_1|m_1, d_2|m_2} f(d_1)f(d_2)g\left(\frac{m_1}{d_1}\right) g\left(\frac{m_2}{d_2}\right) =$$

$$\left\{\sum_{d_1|m_1} f(d_1)g\left(\frac{m_1}{d_1}\right)\right\}\left\{\sum_{d_2|m_2} f(d_2)g\left(\frac{m_2}{d_2}\right)\right\} = h(m_1)h(m2)$$

□

Ejemplo: Consideramos la función $d(n)$ que cuenta la cantidad de divisores de n. Como

$$d(n) = \sum_{d|n} u(d)$$

donde u es la funcióna aritmética unidad, tenemos que $d = u * u$. En consecuencia, d es multiplicativa. Y como $d(p^k) = k + 1$, vemos que

$$d(n) = \prod_{p|n} (v_p(n) + 1)$$

Dado que d no es completamente multiplicativa (ya que $d(4) = 3$ mientras que $d(2) = 1$), el mismo ejemplo muestra que la convolución de Dirichlet de dos funciones completamente multiplicativas no tiene porqué serlo.

También podemos considerar la función $\sigma(n)$ que devuelve la suma de los divisores de n. Nuevamente $\sigma = u * N$, luego σ es multiplicativa. Como

$$\sigma(p^k) = 1 + p + p^2 + \ldots + p^k = \frac{p^{k+1} - 1}{p - 1}$$

tenemos que

$$\sigma(n) = \prod_{p|n} \frac{p^{v_p(n)+1} - 1}{p - 1}$$

Otro ejemplo: Definimos la función λ de Liouville

$$\lambda(n) = (-1)^{\{\sum_{p|n} v_p(n)\}}$$

Como $v_p(n) = 0$ si p no divide a n en esta suma podríamos sumar sobre todos los primos y escribir

$$\lambda(n) = (-1)^{\{\sum_{p} v_p(n)\}}$$

Afirmamos que λ es completamente multiplicativa, pues:

$$\lambda(nm) = (-1)^{\{\sum_p v_p(nm)\}} = (-1)^{\{\sum_p v_p(n)+v_p(m)\}}$$

$$(-1)^{\{\sum_p v_p(n)\}}(-1)^{\{\sum_p v_p(m)\}} = \lambda(n)\lambda(m)$$

Ahora vamos a calcular la suma

$$q(n) = \sum_{d|n} \lambda(d)$$

Notamos que como λ es multiplicativa y $q = \lambda * u$, q es así mismo multiplicativa.

$$q(p^k) = \lambda(1) + \lambda(p) + \lambda(p^2) + \ldots + \lambda(p^k) = \begin{cases} 1 & \text{si} \quad k \text{ es par} \\ 0 & \text{si} \quad k \text{ es impar} \end{cases}$$

En consecuencia,

$$q(n) = \prod_{p|n} q\left(p^{v_p(n)}\right) = \begin{cases} 1 & \text{si} \quad n \text{ es un cuadrado} \\ 0 & \text{si} \quad n \text{ si no lo es} \end{cases}$$

3. Funciones Generatrices: Series de Dirichlet

Para conectar a las funciones aritméticas con el análisis se emplean *funciones generatrices*. En general, una función generatriz es una función en cuyo desarrollo en serie (o en producto infinito) aparecen como coeficientes los valores de la función aritmética que uno quiere estudiar.

En la teoría aditiva (dedicada a las propiedades de los enteros que se relacionan con la suma), se emplean por lo general series de potencias de la forma

$$\sum_{n=0}^{\infty} a_n z^n$$

Por ejemplo, consideramos la función aritmética $p(n)$ que cuenta el número de particiones de n como suma de enteros menores o iguales que n, sin tener en cuenta el orden.

Por ejemplo, $p(5) = 7$ ya que 5 admite las siguientes particiones:

$$5 = 1+1+1+1+1$$

$$5 = 2+1+1+1$$

$$5 = 3+1+1$$

$$5 = 4+1$$

$$5 = 2+2+1$$

$$5 = 2+3$$

$$5 = 5$$

(Notamos que no partirlo, también cuenta como una partición).

Entonces una identidad debida a Euler, proporciona una función generatriz para $p(n)$[1]:

$$\prod_{n=1}^{\infty} \frac{1}{1-z^n} = 1 + \sum_{n=1}^{\infty} p(n) z^n \text{ si } |z| < 1$$

Por otra parte, en la teoría multiplicativa (en la que nos centraremos en este curso), se utilizan generalmente series de Dirichlet. Una serie de Dirichlet es una serie de la forma

$$F(s) = \sum_{n=1}^{\infty} \frac{f(n)}{n^s} \tag{2}$$

donde $f : \mathbb{N} \to \mathbb{C}$ es una función aritmética.

El ejemplo más sencillo de serie de Dirichlet es la función zeta de Riemann $\zeta(s)$ que introdujimos la clase pasada, que corresponde a la función aritmética unidad u.

A continuación, comenzaremos un estudio sistemático de las propiedades de las series de Dirchlet.

Utilizaremos la notación de Riemann: dado $s \in \mathbb{C}$, escribimos $s = \sigma + it$ (donde σ es la parte real, y t la parte imaginaria). Notamos que:

$$\left| \frac{f(n)}{n^s} \right| = \frac{|f(n)|}{n^\sigma}$$

Observamos que si para un valor $s = s_0$ de s la serie (2) converge absolutamente, también lo hace para cualquier s con $\sigma = \text{Re}(s) > \text{Res}(s_0) = \sigma_0$ en virtud del criterio de comparación.

Esta observación implica que en general una serie de Dirichlet tendrá un semiplano de convergencia absoluta:

Teorema 3.1 *Supongamos que la serie*

$$\sum_{n=1}^{\infty} |f(n)| n^{-\sigma} \tag{3}$$

no converge para todo σ ni diverge para todo σ. Entonces existe un número real σ_a, llamado absisa de convergencia absoluta *de la serie* (2) *tal que*

1. *Si $\sigma = Re(s) > \sigma_a$, entonces la serie* (2) *converge absolutamente.*
2. *Si $\sigma = Re(s) < \sigma_a$, entonces la serie* (2) *no converge absolutamente.*

[1] La idea para demostrar esta identidad es expandir $\frac{1}{1-z^n}$ en serie geométrica, y efectuar la distributiva. Esto se puede justificar rigurosamente considerando el producto de finitos factores, y después pasando al límite. Ver por ejemplo el libro de Apostol (teorema 14.2).

Prueba: Sea

$$A = \left\{ \sigma \in \mathbb{R} : \sum_{n=1}^{\infty} |f(n)| n^{-\sigma} \text{ converge} \right\}$$

Dado que por hipóteis la serie (3) no diverge para todo s, A es no vacío. Como por otra parte, dicha serie no convegerge para todo s, A debe ser acotado inferiormente (por la observación anterior al teorema). Por lo tanto, podemos definir $\sigma_a = \text{ínf}(A)$.

Si $\sigma < \sigma_a$, $\sigma \notin A$, luego la serie (2) no converge absolutamente.

Si $\sigma > \sigma_a$, existirá un σ' tal que $\sigma > \sigma'$ y $\sigma' \in A$ (pues σ no es una cota inferior de A). Por la observación anterior al teorema, resulta que $\sigma \in A$, esto es (2) converge absolutamente. □

Por ejemplo, en el caso de la función zeta de Riemann, tenemos $\sigma_a = 1$.

Podemos completar la definición de σ_a especificando que $\sigma_a = -\infty$ si la serie (3) converge para todo σ, o $\sigma_a = +\infty$ si la serie (3) diverge para todo σ.

Ejemplo: La serie de Dirichlet

$$\sum_{n=1}^{\infty} n^n n^{-s}$$

no converge absolutamente para ningún s. La serie de Dirichlet

$$\sum_{n=1}^{\infty} n^{-n} n^{-s}$$

converge absolutamente para todo s (Esto se ve fácilmente aplicando el criterio de convergencia de Cauchy).

Observación 3.1 *Por el test de Weierstrass, la serie de Dirichlet converge uniformemente en cada semiplano de la forma $\sigma \geq \sigma_a + \varepsilon$ (con $\varepsilon > 0$). Esto implica que en su semiplano de convergencia absoluta $\sigma > \sigma_a$, una serie de Dirichlet define una función analítica de la variable compleja s.*

Necesitaremos un lema que nos permitirá acotar las colas de una serie de Dirichlet absolutamente convergente:

Lema 3.1 *Consideramos una serie de Dirichlet* (2) *absolutamente convergente en un semiplano $Re(s) > \sigma_a$. Entonces si $N \geq 1$ y $\sigma = Re(s) > c > \sigma_a$, tenemos que:*

$$\left| \sum_{n=N}^{\infty} f(n) n^{-s} \right| \leq N^{-(\sigma - c)} \sum_{n=N}^{\infty} |f(n)| n^{-c}$$

Prueba:

$$\left| \sum_{n=N}^{\infty} f(n) n^{-s} \right| \leq \sum_{n=N}^{\infty} |f(n)| n^{-\sigma} = \sum_{n=N}^{\infty} |f(n)| n^{-c} n^{-(\sigma - c)} \leq N^{-(\sigma - c)} \sum_{n=N}^{\infty} |f(n)| n^{-c}$$

□

Teorema 3.2

$$\lim_{\sigma \to +\infty} F(\sigma + it) = f(1) \text{ } \textit{uniformemente en } t \in \mathbb{R}$$

Prueba: Separando el primer término

$$F(s) = f(1) + \sum_{n=2}^{\infty} \frac{f(n)}{n^s}$$

Entonces aplicando el lema:

$$|F(s) - f(1)| \leq 2^{-(\sigma - c)} \sum_{n=N}^{\infty} |f(n)| n^{-c} = 2^{-\sigma} A$$

donde la constante A no depende de σ ni de t. Haciendo que $\sigma \to +\infty$, se deduce la conclusión del teorema. □

Ejemplo:

$$\lim_{\sigma \to +\infty} \zeta(\sigma + it) = 1 \text{ uniformemente en } t \in \mathbb{R}$$

El siguiente *teorema de unicidad* nos dice que toda la información sobre la función aritmética f está contenida en su serie de Dirichlet asociada $F(s)$:

Teorema 3.3 *Sean*

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

$$G(s) = \sum_{n=1}^{\infty} \frac{g(n)}{n^s}$$

dos series de Dirichlet absolutamente convergentes en un semiplano $\sigma > \sigma_a = \text{máx}(\sigma_a(F), \sigma_a(G))$. *Si existe una sucesión* s_k *con* $\sigma_k = Re(sk) \to +\infty$ *tal que* $F(s_k) = G(s_k)$, *entonces* $f(n) = g(n)$ *para todo* $n \in \mathbb{N}$.

Prueba: Definamos $h(n) = f(n) - g(n)$, $H(s) = F(s) - G(s)$; de modo que

$$H(s) = \sum_{n=1}^{\infty} \frac{h(n)}{n^s}$$

Sabemos que $H(s_k) = 0$ y queremos ver que $h(n) = 0$ para todo $n \in \mathbb{N}$. Si suponemos que esto no ocurre, habrá un mínimo N tal que $h(N) \neq 0$. Separando el primer término no nulo, podremos escribir:

$$H(s) = \frac{h(N)}{N^s} + \sum_{n=1}^{\infty} \frac{h(n)}{n^s}$$

Evaluando en $s = s_k$ y despejando:

$$h(N) = -N^{s_k} \sum_{n=N+1}^{\infty} \frac{h(n)}{n^{s_k}}$$

Aplicando el lema 3.1, deducimos que:

$$|h(N)| \leq N^{\sigma_k}(N+1)^{-(\sigma_k - c)} \sum_{n=N+1}^{\infty} |h(n)|n^{-c} = \left(\frac{N}{N+1}\right)^{\sigma_k} A$$

donde la constante A es independiente de k. Haciendo que $k \to +\infty$, como $\sigma_k \to +\infty$; tenemos que

$$\left(\frac{N}{N+1}\right)^{\sigma_k} \to 0$$

y en consecuencia deducimos $h(N) = 0$. Esto contradice la elección de N.

Esta contradicción provino de suponer que h no era idénticamente nula, luego $h(n) = 0$ para todo $n \in \mathbb{N}$, como afirmamos. □

Corolario 3.1 *Supongamos que la serie de Dirichlet* (2) *no diverge para todo s, y que la función aritmética f no es identicamente nula. Entonces existe un semiplano $Re(s) > \sigma_0$ donde la función $F(s)$ definida por dicha serie no se anula.*

Prueba: Razonando por reducción al absurdo, si tal semiplano no existiera tendríamos una sucesión s_k con $\mathrm{Re}(s_k) \to +\infty$ tal que $F(s_k) = 0$. Pero hemos visto en la demostración del teorema anterior que ello no es posible. □

Teorema 3.4 *Sean*

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

$$G(s) = \sum_{n=1}^{\infty} \frac{g(n)}{n^s}$$

dos series de Dirichlet absolutamente convergentes en un semiplano $\sigma > \sigma_a = \max(\sigma_a(F), \sigma_a(G))$. Entonces $H(s) = F(s)G(s)$ admite el desarrollo en serie de Dirichlet

$$H(s) = \sum_{n=1}^{\infty} \frac{h(n)}{n^s}$$

donde $h = f * g$, válido si $\sigma > \sigma_a$.

Prueba: Como las series de $F(s)$ y $G(s)$ convergen absolutamente si $\sigma > \sigma_a$, en dicho semiplano podemos multiplicarlas efectuando la distributiva, y asociar los términos en la serie resultante del modo que más nos convenga. Agrupando los términos con $nm = k$ tenemos que

$$H(s) = \sum_{n=1}^{\infty}\sum_{m=1}^{\infty} \frac{f(n)g(m)}{n^s m^s} = \sum_{k=1}^{\infty} \frac{1}{k^s} \left\{ \sum_{nm=k} f(n)g(m) \right\} = \sum_{k=1}^{\infty} \frac{h(k)}{k^s}$$

□