Funciones Aritméticas

Trabajeremos con funciones $f : \mathbb{N} \longrightarrow \mathbb{C}$ pero varios de los resultados seguirán valiendo si el codominio se reemplaza por otro grupo o anillo. Denominaremos $\mathfrak{A}$ al conjunto de tales funciones.

Ejemplos:

i. $\delta(n) = \begin{cases} 1 & n = 1 \\ 0 & n \neq 1 \end{cases}$

ii. $p_k(n) = n^k$ si $k \in \mathbb{R}$

$p_0 = C_1$ (la función constante 1)

$p_1 = 1_{\mathbb{N}}$ la inclusión de $\mathbb{N}$ en $\mathbb{C}$.

iii. $\mu(n) = \begin{cases} 1 & n = 1 \\ (-1)^k & n = p_1 p_2 \dots p_k \text{ con } p_i \neq p_j \text{ si } i \neq j \\ 0 & \text{en otro caso} \end{cases}$

la función de Möbius.

iv. $d(n) = \#\{m \in \mathbb{N} \,/\, m|n\}$

v. $\sigma(n) = \sum_{d|n} d$

vi. $\phi(n) = \#\{m \in \mathbb{N} \,/\, m \leq n \wedge (n;m) = 1\}$

Definición: Decimos que $f : \mathbb{N} \longrightarrow \mathbb{C}$ es multiplicativa si $f(1) = 1$ y $\forall\, n, m \in \mathbb{N}$ coprimos se tiene que $f(mn) = f(m)f(n)$. Denotaremos con $\mathfrak{M}$ al conjunto de funciones multiplicativas.

Observaciones: Todos los ejemplos anteriores corresponden a funciones multiplicativas (los ejemplos iv y v los demostraremos más adelante). La única función constante y multiplicativa es C_1.

Si f es multiplicativa y $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$ entonces $f(n) = f(p_1^{\alpha_1}) f(p_2^{\alpha_2}) \dots f(p_k^{\alpha_k})$. Consecuentemente, dos funciones multiplicativas que coincidan sobre todas las potencias de primos, serán iguales.

Si $f, g \in \mathfrak{M}$ entonces $fg \in \mathfrak{M}$ donde definimos $fg(n) = f(n)g(n)$.

Definición: Sean $f, g \in \mathfrak{A}$ definimos la convolución de Dirichlet (o simplemente convolución) como:

$$f * g(n) = \sum_{d|n} f(d)g(\frac{n}{d}) = \sum_{\substack{1\leq a,b\leq n \\ ab=n}} f(a)g(b)$$

Observación: Se tiene que:

$$\Big(\sum_{n\in\mathbb{N}} \frac{f(n)}{n^s}\Big)\Big(\sum_{n\in\mathbb{N}} \frac{g(n)}{n^s}\Big) = \sum_{n\in\mathbb{N}} \frac{(f*g)(n)}{n^s} \qquad \forall\, s \in U \subseteq \mathbb{C}$$

bajo ciertas condiciones de convergencia de las series y del dominio U.

Propiedades de la Convolución:

i. $f * g = g * f$

ii. $f * (g + h) = f * g + f * h$

iii. $f * \delta = \delta * f = f$

iv. $(f * g) * h = f * (g * h)$

Para la cuarta propiedad, basta observar que :

$$((f * g) * h)(n) = \sum_{\substack{1\leq a,b,c\leq n \\ abc=m}} f(a)g(b)h(c) = (f * (g * h))(n)$$

Proposición: Sean $f, g \in \mathfrak{M}$ entonces $f * g \in \mathfrak{M}$.

Dem:

$(f * g)(1) = f(1)g(1) = 1$ y si $n, m \in \mathbb{N}$ coprimos tenemos:

$$\begin{aligned}(f*g)(m)(f*g)(n) &= \Big(\sum_{d_1|m} f(d_1)g(\frac{m}{d_1})\Big)\Big(\sum_{d_2|n} f(d_2)g(\frac{n}{d_2})\Big) = \\ &= \sum_{\substack{d_1|m \\ d_2|n}} f(d_1)g(\frac{m}{d_1})f(d_2)g(\frac{n}{d_2}) = \sum_{\substack{d_1|m \\ d_2|n}} f(d_1)f(d_2)g(\frac{m}{d_1})g(\frac{n}{d_2}) = \\ &= \sum_{\substack{d_1|m \\ d_2|n}} f(d_1d_2)g(\frac{mn}{d_1d_2}) = \sum_{d|mn} f(d)g(\frac{mn}{d}) = (f*g)(mn)\end{aligned}$$

dado que cualquier $d|mn$ se puede escribir como $d_1 d_2$ con $d_1|m \wedge d_2|n$.$\square$

Proposición: Sea $\mathfrak{A}_u = \{f \in \mathfrak{A} / f(1) \neq 0\}$ entonces $(\mathfrak{A}_u, *)$ es un grupo abeliano y $(\mathfrak{M}, *)$ un sugrupo.

Dem: Ya sabemos que la convolusión es asociativa y conmutativa, y que δ es el neutro, sólo nos falta ver la existencia de un inverso. Veámoslo primero para las multiplicativas.

Dada $f \in \mathfrak{M}$ buscamos $g \in (M)$ tal que $f * g = \delta$. Comenzaremos definiendo $g(1) = 1$, y recursivamente para las potencias de primos, como:

$$g(p^m) = -\sum_{k=0}^{m-1} f(p^{m-k}) g(p^k)$$

de manera que $(f * g)(n) = \delta(n)$ para n potencia de primo.

Definimos $g(p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}) = g(p_1^{\alpha_1}) g(p_2^{\alpha_2}) \dots g(p_k^{\alpha_k})$. Está claro que $g \in \mathfrak{M}$. Como $f * g$ coincide con δ sobre las potencias de primos, y ambas son multiplicativas, deberán ser iguales.

Si $f \in \mathfrak{A}_u$ cualquiera definimos $g(1) = \frac{1}{f(1)}$ y para $n > 1$ recursivamente como:

$$g(n) = \frac{-1}{f(1)} \sum_{\substack{d|n \\ 1 \leq d < n}} f(\frac{n}{d}) g(d)$$

y se tiene que $f * g = \delta$.$\square$

Ejemplos:

i. μ es el inverso de C_1 , dado que ambas son multiplicativas, por lo que también lo será $\mu * C_1$, pero

$$(\mu * C_1)(p^m) = \sum_{k=0}^{m} \mu(p^k) = \begin{cases} 1 & m = 0 \\ 0 & m > 0 \end{cases}$$

es decir, coincide con δ en las potencias de primos, entonces $(\mu * C_1) = \delta$.

ii. Veamos que $\phi * C_1 = 1_{\mathbb{N}}$

$$(\phi * C_1)(p^m) = \sum_{k=0}^{m} \phi(p^k) = 1 + \sum_{k=1}^{m} p^k - p^{k-1} = p^m = 1_{\mathbb{N}}(p^m)$$

como ambas funciones coinciden en las potencias de primos y son multiplicativas, tienen que ser iguales.

Luego $\phi = \phi * \delta = \phi * (C_1 * \mu) = (\phi * C_1) * \mu = 1_{\mathbb{N}} * \mu$ es decir

$$\phi(n) = \sum_{d|n} \mu(d)\frac{n}{d} = (1_{\mathbb{N}} * \mu)(n)$$

(observar que esta fórmula puede deducirse del principio de inclusión-exclusión)

iii. Consideremos $\sigma_m = C_1 * p_m$. Entonces $\sigma = \sigma_1$ y $d = \sigma_0$ resultan multiplicativas. Más aún:

$$d(p_1^{\alpha_1}p_2^{\alpha_2}\dots p_k^{\alpha_k}) = d(p_1^{\alpha_1})d(p_2^{\alpha_2})\dots d(p_k^{\alpha_k}) = (\alpha_1+1)(\alpha_2+1)\dots(\alpha_k+1)$$

y si $m \neq 0$

$$\begin{aligned}\sigma_m(p_1^{\alpha_1}p_2^{\alpha_2}\dots p_k^{\alpha_k}) &= \sigma_m(p_1^{\alpha_1})\sigma_m(p_2^{\alpha_2})\dots\sigma_m(p_k^{\alpha_k}) = \\ &= (\sum_{i=0}^{\alpha_1}(p_1^m)^i)(\sum_{i=0}^{\alpha_2}(p_2^m)^i)\dots(\sum_{i=0}^{\alpha_k}(p_k^m)^i) = \\ &= \frac{p_1^{(\alpha_1+1)m}-1}{p_1^m-1}\,\frac{p_2^{(\alpha_2+1)m}-1}{p_2^m-1}\cdots\frac{p_k^{(\alpha_k+1)m}-1}{p_k^m-1}\end{aligned}$$

Proposición (fórmula de inversión de Möbius): Sea $f \in \mathfrak{A}$ y $F(n) = \sum_{d|n} f(n)$, entonces:

$$f(n) = \sum_{d|n} F(d)\mu(n/d)$$

Dem: Como $F = f * C_1$ tenemos que:

$$\sum_{d|n} F(d)\mu(n/d) = F * \mu = (f * C_1) * \mu = f * (C_1 * \mu) = f * \delta = f.$$

□

Corolario: Sea K un cuerpo finito de q elementos. Entonces, la cantidad de polinomios $P \in K[X]$ mónicos irreducibles de grado n es $\frac{1}{n}\sum_{d|n}\mu(\frac{n}{d})q^d$

Dem: Sean $S_n = \{P \in K[X]$ mónicos irreducibles de grado n$\}$ y $T_n = \cup_{d|n} S_d$. Sea $E \subseteq \overline{K}$ el único cuerpo de q^n elementos dentro de $\overline{K}$una

clausura algebraica de K. Sabemos que E resulta ser el conjunto de raíces (y el cuerpo de descomposición sobre K) de $X^{q^n} - X$ y que éste es un polinomio separable, por lo que resulta ser el producto de los minimales de algunas de sus raíces. Éstos serán todos polinomios mónicos irreducibles cuyos grados dividen a n. Por otro lado, si P es un polinomio mónico irreducible cuyo grado es d divisor de n, su cuerpo de descomposición estará contenido en E, por lo que tendrá que dividir a $X^{q^n} - X$, de donde concluímos:

$$X^{q^n} - X = \prod_{P \in T_n} P$$

Tomando grados tenemos: $q^n = \sum_{P \in T_n} gr(P)$

Llamando $f(n) = \#S_n$ obtenemos:

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

y por la fórmula de inversión de Möbius tenemos que:

$$f(n)n = \sum_{d|n} \mu(\frac{n}{d})q^d \qquad \Longrightarrow \qquad f(n) = \frac{1}{n}\sum_{d|n} \mu(\frac{n}{d})q^d. \qquad \square$$