La Fórmula de Inversión de Möbius

Alan Reyes-Figueroa
Teoría de Números (Aula 28) 02.noviembre.2021

Funciones Aritméticas

Mostramos ahora que el producto de Dirichlet $*$ posee un elemento neutro.

Definición

Definimos la función aritmética $I : \mathbb{Z}^+ \to \mathbb{Z}$ *como* $I(n) = \left\lfloor \frac{1}{n} \right\rfloor = \begin{cases} 1, & \text{si } n = 1; \\ 0, & \text{si } n > 1. \end{cases}$

Llamamos a I *la función de identidad.*

Propiedad

Para toda función aritmética $f : \mathbb{Z}^+ \to \mathbb{Z}$ *se tiene que* $I * f = f * I = f$.

Prueba: De la definición,

$$(f * I)(n) = \sum_{d|n} f(d)\, I\left(\frac{n}{d}\right) = \sum_{d|n} f(d)\, I\left\lfloor \frac{n}{d} \right\rfloor = f(n) \lfloor 1 \rfloor = f(n),$$

ya que $\lfloor \frac{n}{d} \rfloor = 0$ para $d < n$. $\square$

Teorema

*Si $f : \mathbb{Z}^+ \to \mathbb{Z}$ es una función aritmética con $f(1) \neq 0$, entonces hay una única función aritmética $f^{-1} : \mathbb{Z}^+ \to \mathbb{Z}$, llamada la **inversa de Dirichlet**, tal que $f * f^{-1} = f^{-1} * f = I$. Más aún, f^{-1} viene dada por las **fórmulas de inversión**:*

$$f^{-1}(1) = \frac{1}{f(1)}, \qquad f^{-1}(n) = -\frac{1}{f(1)} \sum_{d|n,\, d<n} f\Big(\frac{n}{d}\Big) f^{-1}(d), \;\; \textit{para } n > 1. \tag{1}$$

Prueba: Dada f, mostramos que la ecuación $(f * f^{-1})(n) = I(n)$ posee solución única.

Para $n = 1$, debemos resolver la ecuación $(f * f^{-1})(1) = I(1) = 1, \implies f(1)f^{-1}(1) = 1$. Como $f(1) \neq 0$, hay una sola posible solución, a saber, $f^{-1}(1) = \frac{1}{f(1)}$.

Suponga ahora que $n > 1$ y que los valores de la función $f^{-1}(k)$ se han determinado de forma única para todo $k < n$. Entonces, debemos resolver ahora la ecuación

$$(f * f^{-1})(n) = I(n) \qquad \Longrightarrow \qquad \sum_{d|n} f\left(\frac{n}{d}\right) f^{-1}(d) = 0.$$

Esto puede reescribirse como

$$f(1)f^{-1}(n) + \sum_{d|n,\, d<n} f\left(\frac{n}{d}\right) f^{-1}(d) = 0.$$

Si los valores $f^{-1}(d)$ se conocen para todos los divisores $d < n$, existe un valor determinado para $f^{-1}(n)$, a saber,

$$f^{-1}(n) = -\frac{1}{f(1)} \sum_{d|n,\, d<n} f\left(\frac{n}{d}\right) f^{-1}(d),$$

ya que $f(1) \neq 0$. Esto establece la existencia y unicidad de f^{-1} por inducción. $\square$

Observaciones:

- Note que $(f*g)(1) = f(1)\,g(1)$, así, si $f(1) \neq 0$ y $g(1) \neq 0$ tendremos que $(f*g)(1) \neq 0$.
- Este hecho, junto con los teoremas que hemos probado anteriormente, nos dice que el conjunto de todas las funciones aritméticas f, con $f(1) \neq 0$ forma un grupo abeliano con respecto al producto de Dirichlet.
- La identidad en este grupo es la función I.
- En consecuencia, vale $(f*g)^{-1} = f^{-1} * g^{-1}$, siempre que $f^{-1}(1) \neq 0$ y $g^{-1}(1) \neq 0$.

Definición

Definimos la función aritmética $\mathbf{1} : \mathbb{Z}^+ \to \mathbb{Z}$ *como la función constante con valor 1:* $\mathbf{1}(n) = 1, \ \forall n \in \mathbb{Z}^+$.

Vimos en la clase anterior que si $n \geq 1$, entonces $\displaystyle\sum_{d|n} \mu(d) = \left\lfloor \frac{1}{n} \right\rfloor = \begin{cases} 1, & n = 1; \\ 0, & n > 1. \end{cases}$

En la notación del producto de Dirichlet, esto se convierte en

$$\mu * \mathbf{1} = \mathbf{1} * \mu = I. \tag{2}$$

Por lo tanto, μ y $\mathbf{1}$ son inversos en el producto de Dirichlet

$$\mu^{-1} = \mathbf{1}, \qquad \mathbf{1}^{-1} = \mu.$$

Esta simple propiedad de la función de Möbius, junto con la asociatividad de $*$, nos permite dar una demostración simple de la propiedad de inversión.

Teorema (Fórmula de inversión de Möbius)

La ecuación

$$f(n) = \sum_{d|n} g(d), \tag{3}$$

implica

$$g(n) = \sum_{d|n} f(d)\, \mu\left(\frac{n}{d}\right) \tag{4}$$

La Fórmula de Inversión

Prueba: En la notación de Dirichlet, la ecuación (3) establece que

$$f = g * \mathbf{1}.$$

Ahora, multiplicando ambos lados por μ, obtenemos

$$f * \mu = (g * \mathbf{1}) * \mu = g * (\mathbf{1} * \mu) = g * I = g,$$

que es la ecuación (4).

Recíprocamente, la ecuación (4) corresponde a

$$g = f * \mu.$$

Multiplicando ambos lados por **1**, obtenemos

$$g * \mathbf{1} = (f * \mu) * \mathbf{1} = f * (\mu * \mathbf{1}) = f * I = f,$$

que es la ecuación (3). □

La Fórmula de Inversión

La fórmula de inversión de Mobius ya ha sido ilustrada por el par de fórmulas en el aula anterior:

$$n = \sum_{d|n} \varphi(d), \qquad \varphi(n) = \sum_{d|n} d\,\mu\left(\frac{n}{d}\right) = \sum_{d|n} \frac{n}{d}\,\mu(d).$$

Esto es $\mathrm{id} = \varphi * \mathbf{1}$ y $\varphi = \mathrm{id} * \mu$.

La función de VON MANGOLDT $\Lambda(n)$:

Presentamos a continuación la función Λ de von Mangoldt, que juega un papel central en la distribución de primos.

Definición

Para cada entero $n > 1$, definimos

$$\Lambda(n) = \begin{cases} \log p, & \text{si } n = p^k,\ p \text{ primo},\ k \geq 1; \\ 0, & \text{en cualquier otro caso.} \end{cases}$$

Algunos valores de $\Lambda(n)$ son los siguientes:

n	1	2	3	4	5	6	7	8	9	10	11	12
$\Lambda(n)$	0	$\log 2$	$\log 3$	$\log 2$	$\log 5$	0	$\log 7$	$\log 2$	$\log 3$	0	$\log 11$	0

La demostración del siguiente teorema muestra cómo esta función surge naturalmente del teorema fundamental de la aritmética.

Teorema

Si $n \geq 1$ tenemos
$$\log n = \sum_{d|n} \Lambda(d). \tag{5}$$

Prueba: El teorema es cierto si $n = 1$, ya que ambos lados son 0.

Supongamos que $n > 1$ y escribimos $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ su factoración en primos. Tomando logaritmos tenemos,
$$\log n = \sum_{k=1}^{r} \alpha_k \log p_k.$$

Ahora consideramos la suma a la derecha en (5). Los únicos términos distintos de cero en la suma provienen de aquellos divisores d de la forma p_k^m para $m = 1, 2, \ldots, \alpha_k$ y $k = 1, 2, \ldots, r$. De ahí
$$\sum_{d|n} \Lambda(d) = \sum_{k=1}^{r} \sum_{m=1}^{\alpha_k} \Lambda(p_k^m) = \sum_{k=1}^{r} \sum_{m=1}^{\alpha_k} \log p_k = \sum_{k=1}^{r} \alpha_k \log p_k = \log n. \quad \square$$

Ahora usamos la inversión de Mobius para expresar $\Lambda(n)$ en términos del logaritmo.

Teorema

Si $n \geq 1$, tenemos que $\Lambda(n) = \sum_{d|n} \mu(d) \log \frac{n}{d} = -\sum_{d|n} \mu(d) \log d$.

Prueba: Invirtiendo (5) mediante la fórmula de inversión de Mobius, obtenemos

$$\begin{aligned} \Lambda(n) &= \sum_{d|n} \mu(d) \log \frac{n}{d} = \sum_{d|n} \mu(d) \log n - \sum_{d|n} \mu(d) \log d \\ &= \log n \sum_{d|n} \mu(d) - \sum_{d|n} \mu(d) \log d = \log n \, I(n) - \sum_{d|n} \mu(d) \log d \\ &= -\sum_{d|n} \mu(d) \log d, \end{aligned}$$

pues $\log n \, I(n) = 0$, para todo $n \geq 1$. $\square$

Funciones Multiplicativas

Ya hemos señalado que el conjunto de todas las funciones aritméticas f con $f(1) \neq 0$ forma un grupo abeliano bajo el producto de Dirichlet. En esta sección discutimos un subgrupo importante de este grupo, el llamado *grupo de funciones multiplicativas*.

Definición

*Una función aritmética f se llama **multiplicativa** si f no es idénticamente cero y si*

$$f(mn) = f(m)f(n), \text{ siempre que } (m,n) = 1.$$

*Una función multiplicativa f se llama **completamente multiplicativa** si además*

$$f(mn) = f(m)f(n), \text{ para todo } m,n \in \mathbb{Z}^+.$$

Ejemplo 1: Sea $f(n) = n^\alpha$, donde $\alpha \in \mathbb{R}$ (o $\alpha \in \mathbb{C}$) es un número real o complejo fijo. Observe que f es completamente multiplicativa, pues

$$f(mn) = (mn)^\alpha = m^\alpha n^\alpha = f(m)f(n).$$

Funciones Multiplicativas

Ejemplo 2: En particular, cuando $\alpha = 1$, obtenemos la función identidad $f(n) = \mathrm{id}(n) = n$. La función id es completamente multiplicativa.

Ejemplo 3: En particular, cuando $\alpha = 0$, obtenemos la función constante 1
$f(n) = \mathbf{1}(n) = 1$.
La función **1** es completamente multiplicativa.

Ejemplo 4: La función identidad $I(n) = \left\lfloor \frac{1}{n} \right\rfloor$, es completamente multiplicativa.

- Si $m = n = 1$, entonces $mn = 1 \implies I(mn) = I(1) = 1 = 1 \cdot 1 = I(m)\, I(n)$.
- Si $m > 1$ ó $n > 1$, resulta $mn > 1 \quad I(mn) = 0 = I(m)\, I(n)$.

Ejemplo 5: Ya mostramos que la función φ de Euler $\varphi(n)$ es multiplicativa. Sin embargo, φ no es completamente multiplicativa. Para ello, basta ver el caso cuando $d = (m, n) > 1$. Por ejemplo $m = 12$, $n = 6$.

$$\varphi(mn) = f(72) = \varphi(2^3 \cdot 3^2) = \varphi(2^3) \cdot \varphi(3^2) = 4 \cdot 6 = 24,$$

mientras que $\varphi(12) \cdot \varphi(6) = \varphi(2^2 \cdot 3) \cdot \varphi(2 \cdot 3) = 2(2) \cdot 2 = 8$.

Funciones Multiplicativas

Ejemplo 6: La función μ de Möbius es multiplicativa, pero no es completamente multiplicativa.

Para ver que es multiplicativa, consideremos el caso en que m y n sn primos relativos. Si alguno de m ó n poseen un factor cuadrado, también mn tiene ese factor cuadrado, de donde $\mu(mn) = 0 = \mu(m)\,\mu(n)$.

Si no, $m = p_1 \cdots p_r$ y $n = q_1 \cdots q_s$, con p_i, q_s todos primos distintos. En ese caso, $mn = p_1 \cdots p_r\, q_1 \cdots q_s$ y

$$\mu(mn) = \mu(p_1 \cdots p_r\, q_1 \cdots q_s) = (-1)^{r+s} = (-1)^r(-1)^s = \mu(m)\,\mu(n).$$

Ejemplo 7: Consideramos el producto y cociente ordinarios de funciones aritméticas

$$(fg)(n) = f(n)g(n), \qquad \Big(\frac{f}{g}\Big)(n) = \frac{f(n)}{g(n)}, \text{ siempre que } g(n) \neq 0.$$

Si f y g son multiplicativas, también lo son fg y $\frac{f}{g}$.

Si f y g son completamente multiplicativas, también lo son fg y $\frac{f}{g}$.

Funciones Multiplicativas

Mostramos ahora algunas propiedades de las funciones multiplicativas.

Propiedad

Si f es multiplicativa, entonces $f(1) = 1$.

<u>Prueba</u>: Como $(n, 1) = 1$, tenemos que $f(n) = f(1 \cdot n) = f(1)f(n)$, $\forall n \in \mathbb{Z}^+$. Dado que f no es idénticamente cero tenemos $f(n) \neq 0$ para algún n, de modo que cancelando, $f(1) = 1$. $\square$

Proposición

Dada $f : \mathbb{Z}^+ \to \mathbb{Z}$, con $f(1) = 1$. Entonces:

a) *f es multiplicativa si, y sólo si, $f(p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}) = f(p_1^{\alpha_1})f(p_2^{\alpha_2}) \cdots f(p_r^{\alpha_r})$, para todo primo p_k y todo $\alpha_k \geq 1$.*

b) *Si f es multiplicativa, entonces f es completamente multiplicativa si, y sólo si, $f(p^\alpha) = f(p)^\alpha$, para todo oprimo p y todo $\alpha \geq 1$.* $\square$

Funciones multiplicativas y el producto de Dirichlet:

Teorema

Si f y g son funciones multiplicativas, también lo es su producto $f * g$.

Prueba: Sea $h = f * g$, y tome m, n enteros primos relativos. Luego,

$$h(mn) = \sum_{c|mn} f(c)\, g\left(\frac{mn}{c}\right).$$

Ahora, cada divisor c de mn puede expresarse en la forma $c = ab$, donde $a \mid m$ y $b \mid n$. Además, $(a, b) = 1$, $(\frac{m}{a}, \frac{n}{b}) = 1$, y hay una correspondencia uno a uno entre el conjunto de productos ab y los divisores c de mn. De ahí,

$$\begin{aligned} h(mn) &= \sum_{a|m,\, b|n} f(ab)\, g\left(\frac{mn}{ab}\right) = \sum_{a|m,\, b|n} f(a) f(b)\, g\left(\frac{m}{a}\right) g\left(\frac{n}{b}\right) \\ &= \left[\sum_{a|m} f(a)\, g\left(\frac{m}{a}\right)\right] \left[\sum_{b|n} f(b)\, g\left(\frac{n}{b}\right)\right] = h(m)\, h(n). \quad \square \end{aligned}$$

Funciones Multiplicativas

Obs! El producto de Dirichlet de dos funciones completamente multiplicativas no necesariamente es completamente multiplicativo.

Una leve modificación de la prueba anterior nos permite probar:

Teorema

Si tanto g como $f * g$ son multiplicativas, entonces f también es multiplicativa.

Prueba: Supondremos que f no es multiplicativa y deduciremos que $f * g$ tampoco es multiplicativa. Sea $h = f * g$. Dado que f no es multiplicativa, existen enteros positivos m, n, con $(m, n) = 1$ tales que $f(mn) \neq f(m)f(n)$.

Elegimos uno de esos pares m y n de modo que el producto mn sea el menor posible.

- Si $mn = 1$, entonces $f(1) \neq f(1)f(1)$ entonces $f(1) \neq 1$. Dado que $h(1) = f(1)g(1) = f(1) \neq 1$, esto muestra que h no es multiplicativa.
- Si $mn > 1$, entonces tenemos $f(ab) = f(a)f(b)$ para todos los enteros positivos a, b, con $(a, b) = 1$ y $ab < mn$. Ahora argumentamos como en la prueba anterior,

UNIVERSIDAD DEL VALLE DE GUATEMALA

excepto que en la suma que define $h(mn)$ separamos el término correspondientes a $a = m, b = n$:

$$\begin{aligned}
h(mn) &= \sum_{a|m,\, b|n} f(ab)\, g\Big(\frac{mn}{ab}\Big) = f(mn) + \sum_{a|m,\, b|n,\, ab<mn} f(ab)\, g\Big(\frac{mn}{ab}\Big) \\
&= f(mn) + \sum_{a|m,\, b|n,\, ab<mn} f(a) f(b)\, g\Big(\frac{m}{a}\Big)\, g\Big(\frac{n}{b}\Big) \\
&= f(mn) - f(m) f(n) + \Big[\sum_{a|m} f(a)\, g\Big(\frac{m}{a}\Big)\Big] \Big[\sum_{b|n} f(b)\, g\Big(\frac{n}{b}\Big)\Big] \\
&= f(mn) - f(m) f(n) + h(m)\, h(n).
\end{aligned}$$

Como $f(mn) \neq f(m) f(n)$, esto muestra que $h(mn) \neq h(m)\, h(n)$, así que h no es multiplicativa. $\square$

Funciones Multiplicativas

Corolario

Si f es multiplicativa, entonces también lo es f^{-1}, su inversa de Dirichlet.

Prueba: Se sigue inmediatamente del teorema anterior, ya que tanto f como $f * f^{-1} = I$ son multiplicativas. $\square$

Nota: Los teoremas y corolarios anteriores muestran que el conjunto de funciones multiplicativas forma un subgrupo del grupo de todas las funciones aritméticas f con $f(1) \neq 0$.

Calculamos ahora la inversa de una función completamente multiplicativa.

Teorema

Sea f multiplicativa. Entonces, f es completamente multiplicativo si, y sólo si,

$$f^{-1}(n) = \mu(n) f(n), \quad \textit{para todo } n \geq 1.$$

Funciones Multiplicativas

Prueba: Sea $g(n) = \mu(n) f(n)$.
($\Rightarrow$) Si es completamente multiplicativa, tenemos

$$(g * f)(n) = \sum_{d|n} \mu(d) f(d) f\left(\frac{n}{d}\right) = f(n) \sum_{d|n} \mu(d) = f(n)\, I(n) = I(n),$$

ya que $f(1) = 1$ e $I(n) = 0$ para $n > 1$. Por tanto, $g = f^{-1}$.

($\Leftarrow$) Suponga ahora que $f^{-1}(n) = \mu(n) f(n)$. Para mostrar que f es completamente multiplicativa basta ver que $f(p^k) = f(p)^k$, para p primo y $k \geq 1$. Pero, $f^{-1}(n) = \mu(n) f(n)$ implica que

$$\sum_{d|n} \mu(d) f(d), f\left(\frac{n}{d}\right) = \sum_{d|n} \mu(d) f\left(\frac{n}{d}\right) = 0, \quad \text{para todo } n > 1.$$

Tomando $n = p^k$, tenemos $\mu(1) f(1) f(p^k) + \mu(p) f(p) f(p^{k-1}) = 0$, de donde resulta $f(p^k) = f(p) f(p^{k-1})$. Un argumento inductivo implica que $f(p^k) = f(p)^k$, $\forall k \geq 1$, y entonces f es completamente multiplicativa. $\square$

Funciones Multiplicativas

Ejemplo: La inversa de la función φ de Euler.

Como $\varphi = \mu * \mathrm{id}$, tenemos que $\varphi^{-1} = \mathrm{id}^{-1} * \mu^{-1}$. Pero id es completamente multiplicativa, entonces $\mathrm{id}^{-1} = \mu\,\mathrm{id}$. Así $\varphi^{-1} = \mu^{-1} * \mathrm{id}^{-1} = \mu^{-1} * \mu\,\mathrm{id} = \mathbf{1} * \mu\,\mathrm{id}$. Portanto,

$$\varphi^{-1}(n) = (\mathbf{1} * \mu\,\mathrm{id})(n) = \sum_{d|n} (\mu\,\mathrm{id})(d)\,\mathbf{1}(\tfrac{n}{d}) = \sum_{d|n} d\,\mu(d).$$

Teorema

Si f es multiplicativa, entonces $\displaystyle\sum_{d|n} \mu(d) f(d) = \prod_{p|n} (1 - f(p))$.

Prueba: Sea $g(n) = \sum_{d|n} \mu(d) f(d)$. Entonces, g es multiplicativa, así que para determinar $g(n)$ es suficiente calcular $g(p^k)$ (las potencias en su factoración en primos). Pero $g(p^k) = \sum_{d|p^k} \mu(d) f(d) = \mu(1) f(1) + \mu(p) f(p) = 1 - f(p)$. Luego,

$$g(n) = \prod_{p|n} g(p^k) = \prod_{d|n} (1 - f(p)). \quad \square$$