Funciones Aritméticas

Alan Reyes-Figueroa

Teoría de Números (Aula 27) 28.octubre.2021

La teoría de números, como muchas otras ramas de las matemáticas, a menudo trata con secuencias de números reales o complejos. En teoría de números, tales secuencias se llaman funciones aritméticas.

Definición

Una función $f : \mathbb{Z}^+ \to \mathbb{R}$ (ó $f : \mathbb{Z}^+ \to \mathbb{C}$) definida en el conjunto de enteros positivos, se llama una ***función aritmética****.*

Ejemplos:

- el número de divisores positivos $d(n)$ de n,
- la suma de los divisores positivos $\sigma(n)$ de n,
- el número de primos distintos en la factoración de n,
- la función $\varphi(n)$ de Euler, ...

Este capítulo presenta varias funciones aritméticas que desempeñan un papel importante en el estudio de las propiedades de divisibilidad de los enteros y la distribución de primos.

La función μ de Möbius:

Definición

La función de Möbius $\mu : \mathbb{Z}^+ \to \mathbb{Z}$ se define de la siguiente manera: $\mu(1) = 1$, y si $n > 1$, con factoración en primos de la forma $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$, entonces

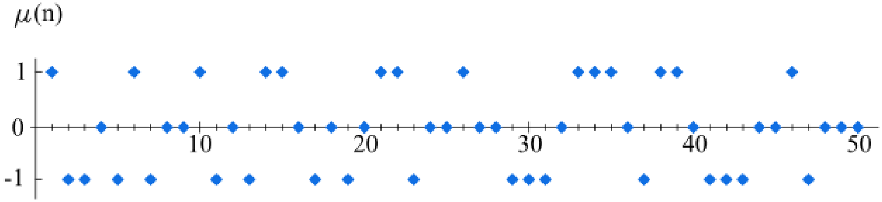
$$\mu(n) = \begin{cases} (-1)^k, & \text{si } \alpha_1 = \alpha_2 = \ldots = \alpha_k = 1; \\ 0, & \text{en cualquier otro caso.} \end{cases}$$

Observe que $\mu(n) = 0$ si, y sólo si, n posee un factor cuadrado > 1. En otras palabras, $\mu(n) = 1$ si, y sólo si $n = 1$, o n es libre de cuadrados.

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

n	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
$\mu(n)$	1	-1	-1	0	-1	1	-1	0	0	1	-1	0	-1	1	1

Funciones Aritméticas



Función μ de Möbius.

La función de Möbius surge en muchos lugares diferentes de la teoría de números. Una de sus propiedades fundamentales es una fórmula notablemente simple para la suma de divisores $\mu(d)$, extendida sobre los divisores positivos de n.

Teorema

Si $n \geq 1$, entonces $\displaystyle\sum_{d|n} \mu(d) = \left\lfloor \frac{1}{n} \right\rfloor = \begin{cases} 1, & n = 1; \\ 0, & n > 1. \end{cases}$

<u>Prueba</u>: La fórmula es claramente verdadera si $n = 1$, pues

$$\sum_{d|1} \mu(d) = \mu(1) = 1 = \left\lfloor \frac{1}{1} \right\rfloor. \qquad (1)$$

Supongamos entonces que $n > 1$ y escribamos $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$, su factoración en primos. En la suma (1), los únicos términos distintos de cero provienen de $d = 1$ y de aquellos divisores de n que son productos de primos distintos. De ahí

$$\begin{aligned} \sum_{d|n} \mu(d) &= \mu(1) + \mu(p_1) + \ldots + \mu(p_k) + \mu(p_1p_2) + \ldots + \mu(p_{k-1}p_k) + \ldots + \mu(p_1p_2\cdots p_k) \\ &= 1 + \binom{k}{1}(-1)^1 + \binom{k}{2}(-1)^2 + \ldots + \binom{k}{k-1}(-1)^{k-1} + \binom{k}{k}(-1)^k \\ &= (1-1)^k = 0. \quad \square \end{aligned}$$

La función φ de Euler:

Definición

Recordemos que la función de Euler o ***totiente*** $\varphi : \mathbb{Z}^+ \to \mathbb{Z}$ *se define de la siguiente manera:*

$$\varphi(n) = \#\{1 \leq k \leq n : \ (k,n) = 1\} = \sum_{k=1,\ (k,n)=1}^{n} 1. \tag{3}$$

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

n	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
$\mu(n)$	1	1	2	2	4	2	6	4	6	4	10	4	12	7	10

Teorema

Si $n \geq 1$, tenemos $\displaystyle\sum_{d|n} \varphi(d) = n.$

<u>Prueba</u>: Sea $S = \{1, 2, ..., n\}$. Distribuimos los enteros de S en conjuntos disjuntos de la siguiente forma. Para cada divisor $d \mid n$, sea $A(d) = \{k : (k, n) = d,\ 1 \leq k \leq n\}$. Esto es $A(d)$ contiene aquellos elementos de S que tienen mdc d con n.

Los conjuntos $A(d)$ forman una partición de S. Portanto, si $f(d)$ denota el número de enteros en $A(d)$ que tenemos que $\sum_{d|n} f(d) = n$.

Pero $(k, n) = d$ si y sólo si $(\frac{k}{d}, \frac{n}{d}) = 1$, y $0 < k \leq n$ si y sólo si $0 < \frac{k}{d} \leq \frac{n}{d}$. Por lo tanto, si hacemos $q = \frac{k}{d}$, tenemos una correspondencia uno a uno entre los elementos de $A(d)$ y los números enteros q satisfacen $0 < q \leq \frac{n}{d}$, $(q, \frac{n}{d}) = 1$. La cantidad de tales q es precisamente $\varphi(\frac{d}{n})$.

Esto muestra que $f(d) = \varphi(\frac{n}{d})$, de modo que $\sum_{d|n} \varphi(\frac{n}{d}) = n$. Como hay una correspondencia entre los divisores $d \mid n$ y $\frac{n}{d} \mid n$, esto equivale a

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

Tenemos una relación entre la función φ de Euler y la función μ de Möbius, a través de las siguiente fórmula:

Teorema

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

Prueba: La suma (3) que define $\varphi(n)$ se puede reescribir en la forma

$$\varphi(n) = \sum_{k=1}^{n} \left\lfloor \frac{1}{(k,n)} \right\rfloor,$$

donde ahora k pasa por todos los enteros positivos $\leq n$. Ahora reemplazamos el valor entero, según el teorema anterior, en términos de la función μ, con n reemplazado por (k,n), Así

$$\varphi(n) = \sum_{k=1}^{n} \left\lfloor \frac{1}{(k,n)} \right\rfloor = \sum_{k=1}^{n} \sum_{d|(k,n)} \mu(d) = \sum_{k=1}^{n} \sum_{d|k,\, d|n} \mu(d).$$

Para un divisor fijo d de n, debemos sumar todos los k en el rango $1 \leq k \leq n$, que son múltiplos de d.

Si escribimos $k = qd$, entonces $1 \leq k \leq n \iff 1 \leq q \leq \frac{n}{d}$. Por tanto, la última suma para $\varphi(n)$ se puede escribir como

$$\begin{aligned} \varphi(n) &= \sum_{k=1}^{n} \sum_{d|k,\, d|n} \mu(d) = \sum_{d|n} \sum_{k=1,\, d|k}^{n} \mu(d) = \sum_{d|n} \sum_{q=1}^{n/d} \mu(d) \\ &= \sum_{d|n} \mu(d) \sum_{q=1}^{n/d} 1 \\ &= \sum_{d|n} \mu(d) \frac{n}{d}, \end{aligned}$$

lo que muestra el teorema. $\square$

Tenemos una fórmula para $\varphi(n)$ en forma de producto.

Propiedad

Para $n \geq 1$ tenemos

$$\varphi(n) = n \prod_{p|n} \left(1 - \frac{1}{p}\right). \tag{4}$$

Prueba: Para $n = 1$, el producto es vacío ya que no hay primos que dividan a 1. En este caso se entiende que al producto se le asignará el valor 1.

Supongamos $n > 1$ y sean $p_1, p_2, \ldots, p_r$, los distintos divisores primos de n. El producto se puede escribir como

$$\begin{aligned}
\prod_{p|n} \left(1 - \frac{1}{p}\right) &= \prod_{i=1}^{r} \left(1 - \frac{1}{p_i}\right) \\
&= 1 - \sum \frac{1}{p_i} + \sum \frac{1}{p_i p_j} - \sum \frac{1}{p_i p_j p_k} + \ldots + (-1)^r \frac{1}{p_1 p_2 \ldots p_r}.
\end{aligned}$$

UNIVERSIDAD DEL VALLE DE GUATEMALA

Observe que cada término a la derecha de la ecuación anterior tiene la forma $\pm\frac{1}{d}$, donde d es un divisor de n que es 1 o un producto de primos distintos. El numerador ± 1 es exactamente $\mu(d)$.
Como $\mu(d) = 0$ si d no es libre de cuadrados, en particular si d es divisible por el cuadrado de cualquier p_i, entonces la suma anterior es

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

Así, $\displaystyle\prod_{p|n}\left(1 - \frac{1}{p}\right) = \sum_{d|n} \frac{\mu(d)}{d}$, y en consecuencia

$$\varphi(n) = \sum_{d|n} \mu(d)\frac{n}{d} = n\sum_{d|n} \frac{\mu(d)}{d} = n\prod_{p|n}\left(1 - \frac{1}{p}\right). \quad \square$$

Propiedades

La función φ de Euler satisface las siguientes propiedades:

a) $\varphi(p^\alpha) = p^\alpha - p^{\alpha-1} = p^{\alpha-1}(p-1)$, *para p primo y $\alpha \geq 1$.*

b) $\varphi(mn) = \varphi(m)\,\varphi(n)\,\frac{d}{\varphi(d)}$, *donde $d = (m,n)$.*

c) $\varphi(mn) = \varphi(m)\,\varphi(n)$, *si $(m,n) = 1$.*

d) $a \mid b \implies \varphi(a) \mid \varphi(b)$.

e) $\varphi(n)$ *es par para $n \geq 3$. Además, si n tiene r factores primos impares distintos, entonces $2^r \mid \varphi(n)$.*

<u>Prueba</u>: La parte (a) sigue inmediatamente tomando $n = p^\alpha$ en la eq. (4). Para probar la parte (b), escribimos

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

Funciones Aritméticas

Observe ahora que cada divisor primo de mn es un divisor primo de m ó de n, y los números primos que dividen tanto m como n también dividen a (m,n). De ahí que

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

y se obtiene (b). La parte (c) es un caso especial de (b).

A continuación, deducimos (d) de (b). Como $a \mid b$, tenemos $b = ac$, con $c \in \mathbb{Z}$, y $1 \leq c \leq b$. Si $c = b$, entonces $a = 1$ y la parte (d) se satisface de forma automática. Por lo tanto, asumimos $c < b$. De (b) tenemos

$$\varphi(b) = \varphi(ac) = \varphi(a)\,\varphi(c)\,\frac{d}{\varphi(d)} = d\,\varphi(a)\,\frac{\varphi(c)}{\varphi(d)}, \tag{5}$$

con $d = (a,c)$. Ahora, el resultado sigue por inducción sobre b.

- Para $b = 1$ el resultado se sostiene automáticamente.
- Suponga que (d) se cumple para todos los enteros $k < b$. Entonces también se cumple para c así que $\varphi(d) \mid \varphi(c)$, ya que $d \mid c$. Por tanto, el miembro derecho de (5)

- es un múltiplo de $\varphi(a)$, lo que significa $\varphi(a) \mid \varphi(b)$. Esto prueba (d).

Ahora probamos (e). Si $n = 2^\alpha$, $\alpha \geq 2$, el inciso (a) muestra que $\varphi(n)$ es par. Si n tiene al menos un factor primo impar, escribimos

$$\varphi(n) = n \prod_{p|n} \frac{p-1}{p} = \frac{n}{\prod_{p|n} p} \prod_{p|n} (p-1) = c(n) \prod_{p|n} (p-1),$$

donde $c(n)$ es un entero. El producto que multiplica $c(n)$ es par, de modo que $\varphi(n)$ es par. Además, cada primo impar p aporta un factor 2 a este producto, por lo que $2^r \mid \varphi(n)$, si n tiene r factores primos impares distintos. $\square$

Anteriormente probamos que

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

La suma de la derecha es de un tipo que ocurre con frecuencia en teoría de números. Estas sumas tienen la forma

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

donde f y g son funciones aritméticas.
Más tarde encontraremos que las sumas de este tipo surgen naturalmente en la teoría de las series de DIRICHLET.

Definición

Si f y g son dos funciones aritméticas, definimos su ***producto de Dirichlet*** *(o* ***convolución de Dirichlet****) como la función aritmética h dada por*

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

Notación: $h = f * g$.

Ejemplo: Si $\mathrm{id} : \mathbb{Z}^+ \to \mathbb{Z}$ denota la función identidad $\mathrm{id}(n) = n$, ya vimos que $\varphi = \mu * \mathrm{id}$.

El siguiente teorema describe las propiedades algebraicas del producto de Dirichlet.

Propiedades

Para cualesquiera funciones aritméticas f, g, h, el producto de Dirichlet satisface:

- *(conmutatividad)* $f * g = g * f$,
- *(asociatividad)* $f * (g * h) = (f * g) * h$.

Prueba: 1. Observemos que, a partir de la definición del producto, y la relación de divisores en pares complementos $d \mid n$ y $\frac{n}{d} \mid n$, tenemos

$$(f * g)(n) = \sum_{d|n} f(d)\, g\left(\frac{n}{d}\right) = \sum_{a \cdot b = n} f(a)\, g(b) = \sum_{d|n} f\left(\frac{n}{d}\right) g(d) = (g * f)(n).$$

Funciones Aritméticas

2. Para probar la asociatividad, hagamos $A = g * h$ y consideramos la convolución $f * A = f * (g * h)$.
Tenemos

$$\begin{aligned}
[f * (g * h)](n) &= (f * A)(n) = \sum_{a \cdot d = n} f(a)\, A(d) \\
&= \sum_{a \cdot d = n} f(a)\, (g * h)(d) = \sum_{a \cdot d = n} f(a) \sum_{b \cdot c = d} g(b)\, h(c) \\
&= \sum_{a \cdot b \cdot c = n} f(a)\, g(b)\, h(c) \\
&= \sum_{a \cdot b = e} \sum_{e \cdot c = n} f(a)\, g(b)\, h(c) = \sum_{e \cdot c = n} (f * g)(e)\, h(c) \\
&= [(f * g) * h](n).
\end{aligned}$$

Lo que muestra que $*$ es asociativa. $\square$