TEORÍA ELEMENTAL DE NÚMEROS

DAVID M. BURTON, TRADUCIDO POR PAUL A. LOOMIS

6.2 La Fórmula de Inversión de Möbius

Introducimos otra función naturalmente definida sobre los enteros positivos, la función μ de Möbius.

Definición 6.3. Para un entero positivo n, definimos μ con las reglas

$$\mu(n) = \begin{cases} 1 & \text{si } n = 1 \\ 0 & \text{si } p^2 | n \text{ por algún primo } p \\ (-1)^r & \text{si } n = p_1 p_2 \cdots p_r \text{, en donde } p_i \text{ son primos distintos} \end{cases}$$

Dicho de otra manera, la Definición 6.3 afirma que $\mu(n) = 0$ si n no es un entero libre de cuadrados, mientras $\mu(n) = (-1)^r$ si n es libre de cuadrados con r factores primos. Por ejemplo: $\mu(30) = \mu(2 \cdot 3 \cdot 5) = (-1)^3 = -1$. Los primeros valores de μ son

$$\mu(1) = 1 \quad \mu(2) = -1 \quad \mu(3) = -1 \quad \mu(4) = 0 \quad \mu(5) = -1 \quad \mu(6) = 1 \ldots$$

Si p es un número primo, es claro que $\mu(p) = -1$; además, $\mu(p^k) = 0$ para $k \geq 2$.

Como el lector puede adivinado ya, la function μ de Möbius es multiplicativa. Este es el contenido del Teorema 6.5.

Theorem 6.5. La función μ es una función multiplicativa.

Demostración. Queremos demostrar que $\mu(mn) = \mu(m)\mu(n)$ siempre que m y n son coprimos. Si o $p^2|m$ o $p^2|n$, p un primo, entonces $p^2|mn$; entonces $\mu(mn) = 0 = \mu(m)\mu(n)$, y la fórmula es trivialmente cierta. Por lo tanto, podemos suponer que m y n ambos son enteros libres de cuadrados. Digamos $m = p_1 p_2 \cdots p_r$, $n = q_1 q_2 \cdots q_s$, con todos los primos p_i y q_j distintos. Entonces

$$\begin{aligned} \mu(mn) = \mu(p_1 p_2 \cdots p_r q_1 q_2 \cdots q_s) &= (-1)^{r+s} \\ &= (-1)^r (-1)^s = \mu(m)\mu(n) \end{aligned}$$

lo que completa la demostración.

Veamos que pasa si se evalua $\mu(d)$ para todos los divisores positivos d de un entero n y suma los resultados. En el caso $n = 1$, la respuesta es fácil; aquí,

$$\sum_{d|1} \mu(d) = \mu(1) = 1$$

Supongamos que $n > 1$ y pongamos

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

Para preparar el terreno, primero calculamos $F(n)$ para las potencias de un primo, digamos $n = p^k$. Los divisores positivos de p^k son solo los $k+1$ enteros $1, p, p^2, \ldots, p^k$, de modo que

$$\begin{aligned} F(p^k) = \sum_{d|p^k} \mu(d) =& \mu(1) + \mu(p) + \mu(p^2) + \cdots + \mu(p^k) \\ =& \mu(1) + \mu(p) = 1 + (-1) = 0 \end{aligned}$$

Como se sabe que μ es una función multiplicativa, una apelación al Teorema 6.4 es legítimo; este resultado garantiza que F también es multiplicativa. Por lo tanto, si la factorización canónica de n es $n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$, entonces $F(n)$ es el producto de los valores asignados a F para las potencias de primos en esta representación:

$$F(n) = F(p_1^{k_1}) F(p_2^{k_2}) \cdots F(p_r^{k_r}) = 0$$

Registramos este resultado com el Teorema 6.6.

Teorema 6.6. Para cada entero positivo $n \geq 1$,

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

en donde d pasa por los divisores positivos de n.

Para una ilustración de este último teorema, consideramos $n = 10$. Los divisores positivos de 10 son $1, 2, 5, 10$ y la suma deseada es

$$\begin{aligned} \sum_{d|10} \mu(d) =& \mu(1) + \mu(2) + \mu(5) + \mu(10) \\ =& 1 + (-1) + (-1) + 1 = 0 \end{aligned}$$

El significado completo de la función μ de Möbius debería hacerse evidente con el próximo teorema.

Teorema 6.7. Fórmula de Inversión de Möbius. Sean F y f dos funciones número-teóricas relacionadas por la fórmula

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

Entonces

$$f(n) = \sum_{d|n} \mu(d) F\left(\frac{n}{d}\right) = \sum_{d|n} \mu\left(\frac{n}{d}\right) F(d)$$

Demostración. Se ve que las dos sumas mencionadas en la conclusión del teorema son iguales al reemplazar el índice d por $d' = n/d$; mientras d pasa por todos los divisores positivos de n, también lo hace d'.

Realizando el cálculo requerido, obtenemos

$$\begin{aligned} \sum_{d|n} \mu(d) F\left(\frac{n}{d}\right) &= \sum_{d|n} \left(\mu(d) \sum_{c|(n/d)} f(c)\right) \\ &= \sum_{d|n} \left(\sum_{c|(n/d)} \mu(d) f(c)\right) \end{aligned} \tag{1}$$

Es facil verificar que $d|n$ y $c|(n/d)$ si y solo si $d|(n/c)$. Debido a esto, la última expresión en la Eq. (1) se convierte en

$$\begin{aligned} \sum_{d|n} \left(\sum_{c|(n/d)} \mu(d) f(c)\right) &= \sum_{c|n} \left(\sum_{d|(n/c)} f(c) \mu(d)\right) \\ &= \sum_{c|n} \left(f(c) \sum_{d|(n/c)} \mu(d)\right) \end{aligned} \tag{2}$$

En conformidad con el Teorema 6.6, la suma $\sum_{d|(n/c)} \mu(d)$ debe desaparecer excepto cuando $n/c = 1$; el resultado es que la mano derecha de la Eq. (2) simplifica a

$$\begin{aligned} \sum_{c|n} \left(f(c) \sum_{d|(n/c)} \mu(d)\right) &= \sum_{c=n} f(c) \cdot 1 \\ &= f(n) \end{aligned}$$

dándonos el resultado indicado.

Usemos $n = 10$ otra vez para ilustrar como se invierte la suma doble en la Eq. (2). En este caso, encontramos que

$$\begin{aligned}\sum_{d|10}\left(\sum_{c|(10/d)}\right) =&\mu(1)[f(1)+f(2)+f(5)+f(10)]\\ &+\mu(2)[f(1)+f(5)]+\mu(5)[f(1)+f(2)]\\ &+\mu(10)f(1)\\ =&f(1)[\mu(1)+\mu(2)+\mu(5)+\mu(10)]\\ &+f(2)[\mu(1)+\mu(5)]+f(5)[\mu(1)+\mu(2)]\\ &+f(10)\mu(1)\\ =&\sum_{c|10}\left(\sum_{d|(10/c)} f(c)\mu(d)\right)\end{aligned}$$

Para ver como funciona la fórmula de inversión de Möbius en un caso particular, recordamos al lector que se puede describir las funciones τ y σ como "funciones sumas":

$$\tau(n) = \sum_{d|n} 1 \qquad \text{y} \qquad \sigma(n) = \sum_{d|n} d$$

El Teorema 6.7 nos dice que se puede invertir estas fórmulas para dar

$$1 = \sum_{d|n} \mu\left(\frac{n}{d}\right)\tau(d) \qquad \text{y} \qquad n = \sum_{d|n} \mu\left(\frac{n}{d}\right)\sigma(d)$$

cuales son validos para cada $n \geq 1$.

El Teorema 6.4 asegura que si f es una función multiplicativa, entonces también es $F(n) = \sum_{d|n} f(d)$. Cambiando la situación, se podría preguntar si la naturaleza multiplicativa de F obliga lo de f. Sorprendentemente, esto es exactamente lo que sucede.

Teorema 6.8. Si F es una función multiplicativa y

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

entonces f también es multiplicativa.

Demostración. Sean m y n enteros positivos coprimos. Recordamos que se puede escribir cualquier divisor d de mn únicamente como $d = d_1 d_2$, en donde $d_1|m$ y

$d_2|n$, y $\text{mcd}(d_1, d_2) = 1$. Entonces, usando la fórmula de inversión,

$$\begin{aligned} f(mn) &= \sum_{d|mn} \mu(d) F\left(\frac{mn}{d}\right) \\ &= \sum_{d_1|m, d_2|n} \mu(d_1 d_2) F\left(\frac{mn}{d_1 d_2}\right) \\ &= \sum_{d_1|m, d_2|n} \mu(d_1)\mu(d_2) F(\left(\frac{m}{d_1}\right) F(\left(\frac{n}{d_2}\right) \\ &= \sum_{d_1|m} \mu(d_1) F\left(\frac{m}{d_1}\right) \sum_{d_2|n} \mu(d_2) F\left(\frac{n}{d_2}\right) \\ &= f(m) f(n) \end{aligned}$$

cual es la afirmación del teorema. No hace falta decir que el carácter multiplicativo de μ y F es crucial para el cálculo anterior.

Para $n \geq 1$, definimos la suma

$$M(n) = \sum_{k=1}^{n} \mu(k)$$

Entonces $M(n)$ es la diferencia entre el número de enteros positivos libres de cuadrados $k \leq n$ con un número par de factores primos y esos con un número impar de divisores positivos. Por ejemplo, $M(9) = 2 - 4 = -2$. En 1897, Franz Mertens (1840-1927) publicó un artículo con una table de 50 páginas de valores de $M(n)$ para $n = 1, 2, \ldots, 10000$. Sobre la base de evidencia tabular, Mertens concluyó que la desigualdad

$$|M(n)| < \sqrt{n} \qquad n > 1$$

es “muy probable”. (En el ejemplo anterior, $|M(9)| = 2 < \sqrt{9}$.) Esta conclusión más tarde se conoció como la conjetura de Mertens. Una busqueda por computadora realizado en 1963 verificó la conjetura para todo n hasta 10 mil millones. Pero en 1984, Andrew Odlyzko y Herman te Riele demostraron que la conjetura de Mertens es falsa. Su demostración, que involucró el uso de una computadora, fue indirecto y no produzcó un valor específico de n para que $|M(n)| \geq \sqrt{n}$; solo demostró que tal número n debe existir en alguna parte. Después, ha sido demostrado que hay un contraejemplo a la conjetura de Mertens para por lo menos un $n \leq (3.21)10^{64}$.

PROBLEMAS 6.2

1. (a) Para cada entero positivo n, demostrar que

$$\mu(n)\mu(n+1)\mu(n+2)\mu(n+3) = 0$$

(b) Para cualquier entero $n \geq 3$, demostrar que $\sum_{k=1}^{n} \mu(k!) = 1$.

2. La *función Mangoldt* Λ se define por

$$\Lambda(n) = \begin{cases} \log p & \text{si } n = p^k, \text{en donde } p \text{ es un primo y } k \geq 1 \\ 0 & \text{en otro caso} \end{cases}$$

Demostrar que $\Lambda(n) = \sum_{d|n} \mu(n/d) \log d = -\sum_{d|n} \mu(d) \log(d)$.
[Consejo: Primero demostrar que $\sum_{d|n} \Lambda(d) = \log n$ y luego aplicar la fórmula de inversión de Möbius.]

3. Sea $n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$ la factorización en primos del entero $n > 1$. Si f es una función multiplicativa que no es idénticamente cero, demostrar que

$$\sum_{d|n} \mu(d) f(d) = (1 - f(p_1))(1 - f(p_2) \cdots (1 - f(p_r))$$

[Consejo: Por el Teorema 6.4, la función F definida por $F(n) = \sum_{d|n} \mu(d) f(d)$ es multiplicativa; entonces $F(n)$ es el producto de los valores $F(p_i^{k_i})$].

4. Si el entero $n > 1$ tiene la factorización en primos $n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$, usar el Problema 3 para establecer lo siguiente:
(a) $\sum_{d|n} \mu(d)\tau(d) = (-1)^r$.
(b) $\sum_{d|n} \mu(d)\sigma(d) = (-1)^r p_1 p_2 \cdots p_r$.
(c) $\sum_{d|n} \mu(d)/d = (1 - 1/p_1)(1 - 1/p_2) \cdots (1 - 1/p_r)$.
(d) $\sum_{d|n} d\mu(d) = (1 - p_1)(1 - p_2) \cdots (1 - p_r)$

5. Sea $S(n)$ denotar el número de divisores libres de cuadrados de n. Establecer que

$$S(n) = \sum_{d|n} |\mu(d)| = 2^{\omega(n)}$$

en donde $\omega(n)$ es el número de divisores primos distintos de n.

6. Hallar fórmulas para $\sum_{d|n} \mu^2(d)/\tau(d)$ y $\sum_{d|n} \mu^2(d)/\sigma(d)$ en términos de la factorización en primos de n.

7. La *función λ de Liouville* se define por $\lambda(1) = 1$ y $\lambda(n) = (-1)^{k_1+k_2+\cdots+k_r}$, si la factorización en primos de $n > 1$ es $n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$. Por ejemplo,

$$\lambda(360) = \lambda(2^3 \cdot 3^2 \cdot 5) = (-1)^{3+2+1} = (-1)^6 = 1$$

(a) Demostrar que λ es una función multiplicativa.

(b) Dado un entero positivo n, verificar que

$$\sum_{d|n} \lambda(d) = \begin{cases} 1 & \text{si } n = m^2 \text{ por algún entero } m \\ 0 & \text{en otro caso} \end{cases}$$

8. Por un entero $n \geq 1$, verificar las siguientes fórmulas:
(a) $\sum_{d|n} \mu(d)\lambda(d) = 2^{\omega(n)}$.
(b) $\sum_{d|n} \lambda(n/d)2^{\omega(d)} = 1$.