FUNÇÕES MULTIPLICATIVAS E A FUNÇÃO DE MÖBIUS*

Carlos Gustavo. T. de A. Moreira, IMPA & Nicolau Saldanha, PUC-Rio

♦ Nível Avançado

Recordamos inicialmente uma propriedade da função φ de Euler, provada em [2] (Lema 2, página 52). Lembremos que, para n inteiro positivo, $\varphi(n) := \#\{\overline{a} \in \mathbb{Z}/n\mathbb{Z} \mid a \text{ é invertível módulo } n\} = \#\{k \in \mathbb{Z} \mid 0 \le k < n \text{ e } \text{mdc}(m,n) = 1\}$.

Teorema 1: Para todo natural n,

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

Prova: Considere as n frações

$$\frac{0}{n}, \frac{1}{n}, ..., \frac{n-1}{n}$$

e simplifique cada uma delas: obtemos assim, para cada $d|n$, $\varphi(d)$ frações com denominador d, donde segue a identidade do enunciado.

Mais formalmente, dado $\overline{a} \in \mathbb{Z}/n\mathbb{Z}$, sejam $d = n/(n, a)$ e $a' = a/(n, a)$.
Claramente $\overline{a'} \in (\mathbb{Z}/d\mathbb{Z})^*$, e definimos assim uma função de $\mathbb{Z}/(n)$ para a união disjunta dos conjuntos $(\mathbb{Z}/d\mathbb{Z})^*$, onde d varia sobre os divisores de n. A inversa desta função leva $\overline{a'} \in (\mathbb{Z}/d\mathbb{Z})^*$ em $\overline{a}$, com $a = na'/d$, donde a função é uma bijeção ❑

O processo de construir g a partir de f como

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

é bastante comum em teoria dos números Um fato interessante sobre este tipo de construção é ligado à noção de funções multiplicativas. Dizemos que $f : \mathbb{N} \to \mathbb{C}$ é multiplicativa se $mdc(m,n) = 1 \Rightarrow f(mn) = f(m)f(n)$. A função φ de Euler, por exemplo, é multiplicativa (ver o corolário da página 47 de [2]). Se f é uma função multiplicativa e $n = p_1^{\alpha_1} p_2^{\alpha_1} ... p_k^{\alpha_k}$ é a fatoração prima de n, então $f(n) = \prod_{i=1}^{k} f(p_i^{\alpha_i})$. Além disso, vale a seguinte

Proposição: Se $f : \mathbb{N} \to \mathbb{C}$ é multiplicativa então $g : \mathbb{N} \to \mathbb{C}$, $g(n) = \sum_{d|n} f(d)$ é multiplicativa.

Prova: Se $mdc(m,n) = 1, g(mn) = \sum_{d|mn} f(d) = \sum_{\substack{d_1|m \\ d_2|n}} f(d_1 d_2) = \sum_{\substack{d_1|m \\ d_2|n}} f(d_1) f(d_2) =$

$$\left(\sum_{d_1|m} f(d_1) \right) \left(\sum_{d_2|n} f(d_2) \right) = g(m)g(n) \text{ ❑}$$

*** Adaptado do livro Primos de Mersenne (e outros primos muito grandes), dos mesmos autores([1]).**

Note que esta proposição fornece uma nova prova do Teorema 1: pela multiplicidade de $\sum_{d|n}\varphi(d)$, basta provar que $\sum_{d|n}\varphi(d)=n$ se n é potência de primo, mas se p é primo, $\sum_{d|p^k}\varphi(d)=\sum_{j=0}^{k}\varphi(p^j)=1+\sum_{j=1}^{k}\varphi(p^j)=1+\sum_{j=1}^{k}(p^j-p^{j-1})=p^k$.

Seria interessante poder inverter em geral identidades do tipo $g(n)=\sum_{d|n}f(d)$ para escrever f a partir de g. O teorema anterior nos mostra que se fazemos $f=\varphi$ na equação acima temos $g(n)=n$; invertendo esta identidade teríamos uma fórmula para φ. Vamos mostrar como fazer este tipo de inversão.

Definimos a função de Möbius $\mu:\mathbb{N}\to\mathbb{Z}$ por

$$\mu(n)=\begin{cases}(-1)^m, & \text{se } n=p_1p_2...p_m, \text{com } p_1, p_2,..., p_m \text{ primos distintos,}\\ 0, & \text{se } n \text{ tem algum fator primo repetido em sua fatoração.}\end{cases}$$

Assim, $\mu(1)=\mu(6)=\mu(10)=1$, $\mu(2)=\mu(3)=\mu(5)=\mu(7)=-1$ e $\mu(4)=\mu(8)=\mu(9)=0$. Note que μ é uma função multiplicativa.

Lema: Para todo inteiro positivo n temos

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

Dem: Como μ é multiplicativa, $h(n)=\sum_{d|n}\mu(d)$ é multiplicativa.

Temos $h(1)=1$ e, para cada p primo e $k\geq 1$ inteiro, $h(p^k)=\sum_{j=0}^{k}\mu(p^j)=1+(-1)=0$,

donde, se $n>1$, $n=p_1^{\alpha_1}...p_k^{\alpha_k}\Rightarrow h(n)=h(p_1^{\alpha_1})h(p_2^{\alpha_2})h(p_k^{\alpha_k})=0$ ❑

Teorema 2: (Fórmula de inversão de Möbius) Se para todo $n > 0$ temos

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

então

$$g(n) = \sum_{d|n} \mu(n/d)\, g(d).$$

Dem: Basta provar que

$$f(n) = \sum_{d|n} \mu(n/d) \left(\sum_{d'|d} f(d') \right).$$

Mas, escrevendo $d'' = n/d$ e $m = n/d'$ temos

$$\sum_{d|n} \mu(n/d) \left(\sum_{d'|d} f(d') \right) = \sum_{m|n} \left(\sum_{d''|m} \mu(d'') \right) f(n/m) = f(n) \quad \square$$

Corolário: Para todo natural n, $\varphi(n) = \sum_{d|n} \mu(n/d)\, d = n \sum_{d|n} \frac{\mu(d)}{d}$.

Teorema 1.22: (Segunda fórmula de inversão de Möbius) Sejam f e g funções reais com domínio $(0, +\infty)$ tais que $f(t) = g(t) = 0$ para todo $t < 1$. Se

$$g(x) = \sum_{k=1}^{\infty} f\left(\frac{x}{k}\right) = \sum_{k=1}^{\lfloor x \rfloor} f\left(\frac{x}{k}\right)$$

para todo x então, para todo x,

$$f(x) = \sum_{k=1}^{\infty} \mu(k)\, g\left(\frac{x}{k}\right) = \sum_{k=1}^{\lfloor x \rfloor} \mu(k)\, g\left(\frac{x}{k}\right).$$

Prova: Basta provar que

$$f(x) = \sum_{k=1}^{\infty} \mu(k) \left(\sum_{r=1}^{\infty} f\left(\frac{x}{kr}\right) \right),$$

mas, tomando $m = kr$ a última soma é igual a

$$\sum_{m=1}^{\infty} \left(\left(\sum_{k|m} \mu(k) \right) f\left(\frac{x}{m}\right) \right),$$

que pelo lema é igual a $f(x)$ $\square$

Apesar de não estar relacionada com o resto da nossa discussão, não podemos deixar de mencionar a seguinte conjectura.

Conjectura (Hipótese de Riemann): Se $\alpha > 1/2$ então

$$\lim_{n\to\infty} \frac{1}{n^{\alpha}} \sum_{m=1}^{n} \mu(m) = 0.$$

Esta é uma das formulações da famosa hipótese de Riemann, um dos problemas em aberto mais importantes da matemática.
Podemos reenunciar esta conjectura assim: seja $f : (0,+\infty) \to \mathbb{R}$ definida por $f(t) = 0$ se $t < 1$ e

$$\sum_{k=1}^{\infty} f(t/k) = 1, \text{ se } t \geq 1.$$

Então, para todo $\alpha > 1/2$,

$$\lim_{n\to\infty} \frac{f(t)}{t^{\alpha}} = 0.$$

De fato, pela segunda fórmula de inversão de Möbius temos

$$f(t) = \sum_{m=1}^{\lfloor t \rfloor} \mu(m).$$

[1] Carlos Gustavo T. de A. Moreira e Nicolau Saldanha, Primos de Mersenne (e outros primos muito grandes), 22º. Colóquio Brasilerio de Matemática IMPA, 1999.

[2] Carlos Gustavo T. de A. Moreira, Divisibilidade, congruências e aritmética módulo *n*, Eureka! Nº. 2, pp. 41-52.