Artigos

Matemática Universitária N. 8, Dezembro de 1988, 37 - 42.

O Símbolo de Legendre

Derek Hacon
Departamento de Matemática PUC/RJ
Rua Marquês de São Vicente 225, Gávea
22.453 Rio de Janeiro, RJ

Uma questão básica de aritmética é decidir, para dois inteiros l e m, se ou não l é um quadrado módulo m, ou seja se existe um inteiro k tal que $l \equiv k^2$ módulo m. O símbolo (de Legendre-Jacobi) fornece uma resposta rápida a esta pergunta. O símbolo $(\frac{l}{m})$ é igual a ± 1 e é definido só para inteiros l e m tais que l e m são coprimos e m é ímpar e positivo. Se m for primo então $(\frac{l}{m}) = +1$ se e sómente se l é um quadrado módulo m. Por exemplo, $(\frac{1}{5}) = +1 = \frac{4}{5}$ e $(\frac{2}{5}) = -1 = (\frac{3}{5})$ mas $(\frac{0}{5})$ não é definido.

As propriedades básicas do símbolo são:

I: $(\frac{l}{m}) = (\frac{l'}{m})$ se $l \equiv l'$ módulo m.

II: $(\frac{l \cdot l'}{m}) = (\frac{l}{m})(\frac{l'}{m})$.

III: $(\frac{l}{m})(\frac{m}{l}) = -1 \Leftrightarrow l \equiv 3 \equiv m$ módulo 4.

Estas e outras propriedades do símbolo são demonstrados em quase todo livro sobre a teoria elementar dos números. Aqui abordaremos o símbolo de um ponto de vista axiomático. Mostraremos primeiro como os axiomas I,II,III determinam $(\frac{l}{m})$ completamente, no sentido que $(\frac{l}{m})$ pode ser calculado a partir dos axiomas. Em seguida mostraremos que existe uma fórmula explícita para $(\frac{l}{m})$

que satisfaz os axiomas, de maneira que os axiomas são consistentes. Finalmente, usando esta fórmula, verificaremos o critério, citado acima, para l ser um quadrado módulo um primo m. A fórmula que usaremos é baseada no teorema de Zolotareff, do século passado, que diz que o símbolo é o sinal de uma certa permutação.

Vejamos agora como calcular $(\frac{l}{m})$ a partir dos axiomas. Considere $(\frac{185}{257})$, por exemplo. Temos $(\frac{185}{257}) = (\frac{257}{185})$ (axioma III) $= (\frac{72}{185})$ (axioma I) $= (\frac{2}{185})^3(\frac{3}{185})^2$ (axioma II) $= (\frac{2}{185})$, pois $(\frac{l}{m})$ é sempre ± 1.

Os valores de $(\frac{2}{m})$ e de $(\frac{-1}{m})$ podem ser calculados a partir dos axiomas. Pelo axioma III temos

$$(\frac{m+4}{m}) = (-1)^{\frac{m-1}{2}} \cdot (\frac{m}{m+4})$$

$$\text{e } (\frac{m+2}{m}) = (\frac{m}{m+2})$$

O leitor poderá deduzir, usando só axiomas I e II que

$$(\frac{-1}{m}) = (-1)^{\frac{m-1}{2}}$$

$$\text{e } (\frac{2}{m}) = (\frac{-1}{m+2}) \cdot (\frac{2}{m+2})$$

Mas $(\frac{2}{7}) = (\frac{9}{7}) = +1$. Então

$$+1 = -(\frac{2}{3}) = -(\frac{2}{5}) = (\frac{2}{7}) = (\frac{2}{9}) = -(\frac{2}{11}) = -(\frac{2}{13}) = \ldots$$

Em particular, $(\frac{2}{185}) = (\frac{2}{9}) = +1$. Como 257 é primo, concluimos que existe k tal que $185 \equiv k^2$ módulo 257.

Conhecendo o valor de $(\frac{2}{m})$ é fácil se convencer que qualquer $(\frac{l}{m})$ pode ser calculado a partir dos axiomas.

Antes de dar a fórmula para o símbolo, lembramos que o sinal de uma permutação σ dos números $\{1, 2, \ldots, n\}$ pode ser definido pela fórmula

$$\varepsilon(\sigma) = \prod_{j<k} \frac{\sigma(j) - \sigma(k)}{j - k}$$

Se, em vez da ordem usual $1 < 2 < \ldots < n$ usamos uma outra ordem (por exemplo $n < n-1 < \ldots < 1$) para definir ε, o resultado será o mesmo. Por exemplo, usando 3 2 1 em vez de 1 2 3, podemos passar de 1 2 3 para 3 2 1 por uma seqüência de trocas de elementos vizinhos $1\,2\,3 \to 2\,1\,2 \to 2\,3\,1 \to 3\,2\,1$. Escrevendo ε_{ijk} para o ε definido usando a ordem ijk, temos, por exemplo,

$$\begin{aligned} \varepsilon_{213}(\sigma) &= \tfrac{\sigma(2)-\sigma(1)}{2-1} \cdot \tfrac{\sigma(2)-\sigma(3)}{2-3} \cdot \tfrac{\sigma(1)-\sigma(3)}{1-3} \\ &= \tfrac{\sigma(2)-\sigma(1)}{2-1} \cdot \tfrac{\sigma(2)-\sigma(3)}{2-3} \cdot \tfrac{\sigma(3)-\sigma(1)}{3-1} \\ &= \varepsilon_{231}(\sigma) \end{aligned}$$

Assim $\varepsilon_{321}(\sigma) = \varepsilon_{231}(\sigma) = \varepsilon_{213}(\sigma) = \varepsilon_{123}(\sigma)$. A propriedade básica do sinal é a multiplicatividade

$$\varepsilon(\sigma \circ \rho) = \varepsilon(\sigma) \cdot \varepsilon(\rho)$$

onde $\sigma \circ \rho$ leva j em $\sigma(\rho(j))$.Temos

$$\begin{aligned} \varepsilon(\sigma \circ \rho) &= \prod_{j<k} \frac{\sigma(\rho(j)) - \sigma(\rho(k))}{j-k} \\ &= \prod_{j<k} \frac{\sigma(\rho(j)) - \sigma(\rho(k))}{\rho(j) - \rho(k)} \prod_{j<k} \frac{\rho(j) - \rho(k)}{j-k} \end{aligned}$$

Mas,no primeiro fator podemos usar a ordem $\rho(1), \rho(2), \ldots, \rho(n)$ em vez da ordem $1, 2, \ldots, n$. Escrevendo $u = \rho(j)$ e $v = \rho(k)$, obtemos

$$\prod_{u<v} \frac{\sigma(u) - \sigma(v)}{u-v},$$

que mostra que $\varepsilon(\sigma \circ \rho) = \varepsilon(\sigma) \cdot \varepsilon(\rho)$.

Se em vez de $\{1, 2, \ldots, n\}$ consideramos um conjunto finito K num corpo e uma permutação σ dos elementos de K, o sinal

$$\varepsilon(\sigma) = \prod_{x<y} \frac{\sigma(x) - \sigma(y)}{x-y}$$

é bem definido, não depende da ordem escolhida para K e é multiplicativo.

Seja R_m o conjunto das m-esimas raizes complexas de 1 ou seja $\{\zeta^0, \zeta^1, \ldots, \zeta^{m-1}\}$ onde $\zeta = e^{2\pi i/m}$ (ζ^0 sendo 1). Considere a permutação de R_m que leva X em X^l. É uma permutação pois, l e m sendo coprimo, existe l^* tal que $ll^* \equiv 1$ módulo m. Se $X^l = Y^l$ então $X = X^{ll^*} = Y^{ll^*} = Y$.

Define $(\frac{l}{m})$ a ser o sinal desta permutação , ou seja:

$$(\frac{l}{m}) = \prod_{X<Y} \frac{X^l - Y^l}{X - Y}$$

Por definição axioma I é satisfeito e axioma II segue do fato que $X^{ll'} = (X^l)^{l'}$.

Para verificar axioma III (a lei da Reciprocidade Quadratica) sejam l e m inteiros positivos, ímpares, coprimos. Usaremos a seguinte fórmula

$$(\frac{l}{m}) = \prod_{X<Y} \prod_{\alpha<\beta} (\alpha X - \beta Y)(\beta X - \alpha Y)$$

onde X, Y pertencem a R_m e α, β a R_l. Neste produto tem $l \cdot \frac{l-1}{2} \cdot m \cdot \frac{m-1}{2}$ termos da forma $(\alpha X - \beta Y)(\beta X - \alpha Y)$. Para verificar a fórmula precisaremos da observação que $(\frac{l}{m}) = (\frac{l}{m})^l$, pois $(\frac{l}{m}) = \pm 1$ e l é ímpar e do fato que o polinômio homogéneo $\{\frac{x^l - y^l}{x-y}\}^l$ de grau $l(l-1)$ é igual a $\prod_{\alpha \neq \beta} (\alpha x - \beta y)$. Deixamos a prova desta fatoração ao leitor notando que $\prod_{\alpha} \alpha = +1$, pois l é ímpar.

Temos então

$$\begin{aligned}(\frac{l}{m}) = (\frac{l}{m})^l &= \prod_{X<Y} \{\frac{X^l - Y^l}{X - Y}\}^l \\ &= \prod_{X<Y} \prod_{\alpha \neq \beta} (\alpha X - \beta Y) \\ &= \prod_{X<Y} \prod_{\alpha<\beta} (\alpha X - \beta Y)(\beta X - \alpha Y)\end{aligned}$$

Usando esta fórmula é fácil verificar axioma III, pois, trocando l por m, α por X, β por Y temos

$$\prod_{\alpha<\beta} \prod_{X<Y} (X\alpha - Y\beta)(X\beta - Y\alpha)$$

Então$(\frac{l}{m}) = (-1)^s \cdot (\frac{m}{l})$ onde $s = l \cdot \frac{l-1}{2} \cdot m \cdot \frac{m-1}{2}$. Como lm é ímpar, $s \equiv \frac{l-1}{2} \cdot \frac{m-1}{2}$ módulo 2 e o axioma III é verificado.

Passamos agora a verificar o critério para l ser um quadrado módulo um primo (ímpar) m. Precisaremos do critério de Euler que diz que l é um quadrado módulo $m \Leftrightarrow l^{\frac{m-1}{2}} \equiv +1$ módulo m. Este critério é um caso particular do

Lema Seja F um corpo finito de q elementos e seja $q - 1 = ab$. Então, para todo $x \neq 0$ em F, existe um y tal que $x = y^b \Leftrightarrow x^a = 1$.

Demonstração $F - \{0\}$ é um grupo (multiplicativo) de $q - 1$ elementos. Então $x^a = 1$ se $x = y^b$. Reciprocamente, a equação $x^a = 1$ tem, no máximo, a soluções diferentes no corpo F e, dado x, a equação $y^b = x$ tem, no máximo, b soluções em F. Então, em $F - \{0\}$, tem, no mínimo, $a = \frac{q-1}{b}$ elementos diferentes da forma y^b. Cada um destes elementos é uma solução da equação $x^a = 1$. Então cada solução da equação $x^a = 1$ é da forma y^b.

O critério de Euler corresponde ao caso $F = \mathbb{Z}_m$ e $b = 2$. Dado este critério, precisa só mostrar que $(\frac{l}{m}) = l^{\frac{m-1}{2}}$ em $\mathbb{Z}_m$. O conjunto R_m pode ser identificado com $\mathbb{Z}_m$ pela correspondencia $j \leftrightarrow \zeta^j$. Assim a permutação $X \to X^l$ corresponde à permutação $j \to lj$ em $\mathbb{Z}_m$. O sinal desta permutação é $\prod_{j<k} \frac{lj - lk}{j - k}$ em $\mathbb{Z}_m$, ou seja $l^{m\frac{m-1}{2}}$. Mas, em $\mathbb{Z}_m$, $l^{\frac{m-1}{2}}$ é ± 1 e m é ímpar. Então este sinal é $l^{\frac{m-1}{2}}$ e o critério para l ser um quadrado módulo m é verificado.

A definição usual do símbolo começa por definir $(\frac{l}{m})$ quando m é um primo ímpar (o símbolo de Legendre). Para um produto $m = p_1^{n_1} \cdots p_k^{n_k}$, onde os p_i são primos ímpares, define-se o símbolo $(\frac{l}{m})$ pela fórmula

$$(\frac{l}{m}) = \prod_i (\frac{l}{p_i})^{n_i}.$$

Com esta definição a fórmula $(\frac{l}{mn}) = (\frac{l}{m})(\frac{l}{n})$ é imediata. É um exercício interessante verificar esta fórmula a partir dos axiomas, usando axioma III na forma

$$(\frac{l}{m})(\frac{m}{l}) = (-1)^{\frac{l-1}{2}\cdot\frac{m-1}{2}}$$

e a fórmula $(\frac{2}{m}) = (-1)^{\frac{m^2-1}{8}}$.