O SÍMBOLO DE JACOBI

FERNANDO FERREIRA

O símbolo de Legendre $\left(\frac{a}{p}\right)$ está apenas definido para p primo ímpar e a inteiro coprimo com p. O símbolo de Jacobi estende esta definição a números naturais ímpares p diferentes de 1. Seja, então, n um número natural ímpar diferente de 1 e $a \perp n$. Considere-se $n = p_1 p_2 \cdots p_k$ a fatorização de n em números primos (não necessariamente distintos). Define-se:

$$\left(\frac{a}{n}\right) := \left(\frac{a}{p_1}\right)\left(\frac{a}{p_2}\right)\cdots\left(\frac{a}{p_k}\right)$$

Os símbolos que aparecem na direita são símbolos de Legendre e, é claro, estão bem definidos. Se bem que estejamos a usar a mesma notação para os símbolos de Legendre e os símbolos de Jacobi não há perigo pois ambos os símbolos coincidem quando n é primo. Não obstante, há que ter cuidado num ponto: Ao contrário do que sucede com os símbolos de Legendre, pode acontecer que um símbolo de Jacobi seja 1, i.e. pode acontecer que $\left(\frac{a}{n}\right) = 1$, mas que a não seja um quadrado módulo n. Por exemplo: $\left(\frac{2}{15}\right) = \left(\frac{2}{3}\right)\left(\frac{2}{5}\right) = (-1)(-1) = 1$ mas $x^2 \equiv 2 \pmod{15}$ não tem solução. Para o símbolo de Jacobi $\left(\frac{a}{n}\right)$, ser igual a 1 não é condição suficiente para que a seja um quadrado módulo n. É, no entanto, condição necessária como se pode facilmente argumentar. A situação será cabalmente discutida e esclarecida na próxima secção.

Para que servem então os símbolos de Jacobi, dado que não caracterizam os resíduos quadráticos? Servem, por exemplo, para calcular *eficientemente* os símbolos de Legendre. Também os usaremos para dar uma demonstração simples duma lei que ficou pendente da secção anterior. Antes de nos abalançarmos nestes assuntos, listemos algumas propriedades dos símbolos de Jacobi. Sai imediatamente da definição que, para n e m números naturais ímpares diferentes de 1 e $a \in \mathbb{Z}$ com $a \perp nm$, se tem

$$\left(\frac{a}{nm}\right) = \left(\frac{a}{n}\right)\left(\frac{a}{m}\right)$$

As três seguintes propriedades são obviamente herdadas das propriedades correspondentes dos símbolos de Legendre. Se n é um número natural ímpar diferente de 1 e $a, b \in \mathbb{Z}$, então

$$a \perp n \text{ e } a \equiv b \pmod{n} \;\Rightarrow\; \left(\frac{a}{n}\right) = \left(\frac{b}{n}\right)$$

Também se tem

$$\left(\frac{a^2}{n}\right) = 1$$

para n natural ímpar diferente de 1 e $a \perp n$, e

$$\left(\frac{ab}{n}\right) = \left(\frac{a}{n}\right)\left(\frac{b}{n}\right)$$

para n natural ímpar diferente de 1 e $ab \perp n$. Igualmente:

$$\left(\frac{-1}{n}\right) = (-1)^{\frac{n-1}{2}}$$

para n natural ímpar diferente de 1. Esta última igualdade é uma simples consequência da propriedade correspondente dos símbolos de Legendre porque, para n e m números naturais ímpares diferentes de 1, os números $\frac{nm-1}{2}$ e $\frac{n-1}{2} + \frac{m-1}{2}$ têm a mesma paridade. Com esta observação

sobre paridades, também é claro que a lei da reciprocidade quadrática se generaliza aos símbolos de Jacobi:

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

para n e m números naturais ímpares, diferentes de 1 e coprimos entre si. Finalmente, vamos estabelecer a lei dos símbolos de Legendre que ficou pendente da secção anterior. Ela é um caso particular da seguinte lei para símbolos de Jacobi:

$$\left(\frac{2}{n}\right) = (-1)^{\frac{n^2-1}{8}}$$

onde n é um número natural ímpar diferente de 1.

Vamos demonstrar esta lei. Em primeiro lugar, para k número ímpar com $k \geqslant 5$, tem-se

$$\left(\frac{k-2}{k}\right) = \left(\frac{k}{k-2}\right) = \left(\frac{k-2(k-2)}{k-2}\right) = \left(\frac{-1}{k-2}\right)\left(\frac{k-4}{k-2}\right)$$

A primeira igualdade justifica-se pela lei da reciprocidade quadrática pois ou $k \equiv 1 \pmod 4$ ou $k-2 \equiv 1 \pmod 4$. A segunda igualdade justifica-se porque k é congruente com $k-2(k-2)$ módulo $k-2$.

Para n um número natural ímpar diferente de 1, tem-se

$$\left(\frac{2}{n}\right) = \left(\frac{2-n}{n}\right) = \left(\frac{-1}{n}\right)\left(\frac{n-2}{n}\right)$$

Utilizando a igualdade dos ks acima um número suficiente de vezes ficamos com

$$\left(\frac{n-2}{n}\right) = \left(\frac{-1}{n-2}\right)\left(\frac{n-4}{n-2}\right) = \left(\frac{-1}{n-2}\right)\left(\frac{-1}{n-4}\right)\left(\frac{n-6}{n-4}\right) = \cdots$$

$$= \left(\frac{-1}{n-2}\right)\left(\frac{-1}{n-4}\right)\cdots\left(\frac{-1}{5}\right)\left(\frac{-1}{3}\right)\left(\frac{1}{3}\right)$$

Ora, $\left(\frac{1}{3}\right) = 1$ e, para m número natural ímpar diferente de 1, tem-se $\left(\frac{-1}{m}\right) = (-1)^{\frac{m-1}{2}}$. Logo

$$\left(\frac{2}{n}\right) = \left(\frac{-1}{n}\right)\left(\frac{-1}{n-2}\right)\left(\frac{-1}{n-4}\right)\cdots\left(\frac{-1}{5}\right)\left(\frac{-1}{3}\right) = (-1)^{\frac{n-1}{2}+\frac{n-3}{2}+\frac{n-5}{2}+\cdots+\frac{5-1}{2}+\frac{3-1}{2}}$$

$$= (-1)^{1+2+\cdots+\frac{n-5}{2}+\frac{n-3}{2}+\frac{n-1}{2}} = (-1)^{\frac{n^2-1}{8}}$$

como se queria.

O uso do símbolo de Jacobi permite calcular eficientemente os símbolos de Legendre. Vamos dar um exemplo com o cálculo do símbolo de Legendre $\left(\frac{-1872}{7411}\right)$. (O número 7411 é, de facto, um número primo.) Tem-se:

$$\begin{aligned}
\left(\frac{-1872}{7411}\right) &= \left(\frac{-1}{7411}\right)\left(\frac{1872}{7411}\right) = -\left(\frac{1872}{7411}\right) \\
&= -\left(\frac{16\times 117}{7411}\right) = -\left(\frac{16}{7411}\right)\left(\frac{117}{7411}\right) = -\left(\frac{117}{7411}\right) \\
&= -\left(\frac{7411}{117}\right) \\
&= -\left(\frac{40}{117}\right) \\
&= -\left(\frac{8\times 5}{117}\right) = -\left(\frac{2\times 2^2}{117}\right)\left(\frac{5}{177}\right) = -\left(\frac{2}{117}\right)\left(\frac{5}{117}\right) = \left(\frac{5}{117}\right) \\
&= \left(\frac{117}{5}\right) \\
&= \left(\frac{2}{5}\right) = -1
\end{aligned}$$

No primeiro passo reduzimos o cálculo a um símbolo de Jacobi com entradas positivas utilizando para isso a fórmula que permite calcular símbolos de Jacobi cuja entrada superior é -1. Na segunda linha retirámos todas as potências de 2 da entrada superior do símbolo de Jacobi e, na linha seguinte, usámos a lei de reciprocidade quadrática para inverter as entradas do símbolo de Jacobi. Na quarta linha reduzimos a entrada superior módulo a entrada inferior: com efeito, $7411 \equiv 40 \pmod{117}$. Estes três últimos movimentos (retirar as potências de 2, usar a lei da reciprocidade quadrática e reduzir a entrada superior módulo a inferior) são depois repetidos sucessivamente até se chegar ao resultado final. Devido ao terceiro destes movimentos (reduzir a entrada superior módulo a inferior) o número de passos do algoritmo é linear na entrada maior (como acontece com o algoritmo de Euclides para calcular o máximo divisor comum). Assim, como em cada movimento o cálculo a efetuar é eficiente, o algoritmo que acabámos de ilustrar é, no seu todo, eficiente. A análise que esboçámos mostra que este algoritmo trabalha em tempo cúbico.

Note-se que se não tivéssemos símbolos de Jacobi, não poderíamos obter o símbolo da terceira linha, pois 117 não é um número primo. Sem o símbolo de Jacobi, para calcular $\left(\frac{117}{7411}\right)$ teríamos que fatorizar 117 de modo a obter $\left(\frac{117}{7411}\right) = \left(\frac{9}{7411}\right)\left(\frac{13}{7411}\right)$. Dado que não se conhece um modo eficiente de fatorizar números, este processo não dá origem a um cálculo eficiente.

O critério de Euler e o cálculo eficiente do símbolo de Jacobi pelo processo descrito acima estão na base do *teste probabilístico de primalidade de Solovay-Strassen*. Se n é um número natural ímpar (diferente de 1) e a é tal que $1 \leqslant a \leqslant n-1$, com $a \perp n$, podemos calcular eficientemente $a^{\frac{n-1}{2}} \pmod{n}$ (pelo método da repetição do quadrado) e o símbolo de Jacobi $\left(\frac{a}{n}\right)$ (pelo processo acima). Se estes números são diferentes então, pelo critério de Euler, temos a garantia de que n não é primo. Porém, se forem o mesmo número, n tanto pode ser primo como não ser. Neste último caso, diz-se que n é um *pseudoprimo de Euler de base a*.

Sabe-se que se n é um número ímpar (diferente de 1) composto, então no máximo 50% de todos os números (bases) a com $1 \leqslant a \leqslant n-1$ e $a \perp n$, se tem $a^{\frac{n-1}{2}} \equiv \left(\frac{a}{n}\right) \pmod{n}$. Este facto torna o teste muito fiável. Tal como o teste de Miller-Rabin, o teste de Solovay-Strassen é um teste probabilístico que (consoante os resultados) leva à conclusão de que n é composto ou de que é, com alta probabilidade, um número primo.

Podemos agora demonstrar o teorema da reciprocidade quadrática de há duas secções atrás. Seja a um inteiro (não nulo) e p e q são primos ímpares tais $p \perp a$ e $q \perp a$. Suponhamos que $p \equiv q \pmod{4|a|}$. Queremos ver que $\left(\frac{a}{p}\right) = \left(\frac{a}{q}\right)$.

Assuma-se, nas condições anteriores, que $4a|(p-q)$. Podemos restringir-nos ao caso em que a é positivo. Com efeito, se $a < 0$, tem-se $\left(\frac{a}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{|a|}{p}\right) = (-1)^{\frac{p-1}{2}}\left(\frac{|a|}{p}\right)$ e, analogamente, $\left(\frac{a}{q}\right) = (-1)^{\frac{q-1}{2}}\left(\frac{|a|}{q}\right)$. Como $p \equiv q \,(\mathrm{mod}\ 4)$, os números naturais $\frac{p-1}{2}$ e $\frac{q-1}{2}$ têm a mesma paridade e, portanto, ficamos reduzidos a mostrar que $\left(\frac{|a|}{p}\right) = \left(\frac{|a|}{q}\right)$.

Supomos, pois, que a é positivo. Tome-se $a = 2^s b$, where s é um inteiro não negativo e b é um número natural ímpar. Ora:

$$\left(\frac{a}{p}\right) = \left(\frac{2}{p}\right)^s \left(\frac{b}{p}\right) \quad \text{e} \quad \left(\frac{a}{q}\right) = \left(\frac{2}{q}\right)^s \left(\frac{b}{q}\right)$$

Para mostrar que $\left(\frac{a}{p}\right) = \left(\frac{a}{q}\right)$, basta ver que $\left(\frac{b}{p}\right) = \left(\frac{b}{q}\right)$ e, caso $s \neq 0$, que $\left(\frac{2}{p}\right) = \left(\frac{2}{q}\right)$.

Dado que se tem $p \equiv q \,(\mathrm{mod}\ 4)$ e $p \equiv q \,(\mathrm{mod}\ b)$ vem

$$\left(\frac{b}{p}\right) = \left(\frac{p}{b}\right)(-1)^{\frac{p-1}{2}\frac{b-1}{2}} = \left(\frac{q}{b}\right)(-1)^{\frac{p-1}{2}\frac{b-1}{2}} = \left(\frac{q}{b}\right)(-1)^{\frac{q-1}{2}\frac{b-1}{2}} = \left(\frac{b}{q}\right)$$

onde se usa a lei da reciprocidade quadrática (duas vezes, ao início e no final), a propriedade (i) dos símbolos de Legendre e o facto dos números naturais $\frac{p-1}{2}$ e $\frac{q-1}{2}$ terem a mesma paridade.

Resta ver o caso do primo 2. Se 2 aparece efetivamente na fatorização de a ($s \neq 0$), então tem-se mesmo $p \equiv q \,(\mathrm{mod}\ 8)$. A igualdade desejada sai imediatamente, atendendo à lei do símbolo de Legendre para o número 2.