

# O LEI DA RECIPROCIDADE QUADRÁTICA DE GAUSS

FERNANDO FERREIRA

A lei da reciprocidade quadrática foi primeiramente demonstrada por Gauss no final do século XVIII. Ela relaciona os símbolos de Legendre  $\left(\frac{p}{q}\right)$  e  $\left(\frac{q}{p}\right)$ , para  $p$  e  $q$  primos ímpares distintos.

**Lei da reciprocidade quadrática.** *Sejam  $p$  e  $q$  primos ímpares distintos. Se  $p \equiv 1 \pmod{4}$  ou  $q \equiv 1 \pmod{4}$ , então  $q$  é resíduo quadrático módulo  $p$  se, e somente se,  $p$  é resíduo quadrático módulo  $q$ . Se  $p \equiv 3 \pmod{4}$  e  $q \equiv 3 \pmod{4}$ , então  $q$  é resíduo quadrático módulo  $p$  se, e somente se,  $p$  é não resíduo quadrático módulo  $q$ .*

Uma forma alternativa de apresentar esta lei é através da fórmula:

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = \begin{cases} 1 & \text{se } p \equiv 1 \pmod{4} \text{ ou } q \equiv 1 \pmod{4} \\ -1 & \text{se } p \equiv 3 \pmod{4} \text{ e } q \equiv 3 \pmod{4} \end{cases}$$

onde  $p$  e  $q$  são primos ímpares distintos. Equivalentemente:

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

Vamos dar uma demonstração relativamente recente (1991) desta lei devida a George Rousseau. Esta demonstração usa apenas o teorema chinês dos restos, o critério de Euler e o teorema de Wilson (este último resultado não é realmente necessário).

**Demonstração da lei da reciprocidade quadrática.** Sejam dados  $p$  e  $q$  primos ímpares distintos. Como sabemos, a função

$$\begin{aligned} \gamma : (\mathbb{Z}/pq\mathbb{Z})^* &\rightarrow (\mathbb{Z}/p\mathbb{Z})^* \times (\mathbb{Z}/q\mathbb{Z})^* \\ [k]_{pq} &\rightsquigarrow ([k]_p, [k]_q) \end{aligned}$$

é uma bijeção. Sejam  $E := \{[k]_{pq} \in (\mathbb{Z}/pq\mathbb{Z})^* : k \perp pq \text{ e } 0 < k < \frac{pq}{2}\}$  e

$$D := \{([a]_p, [b]_q) \in (\mathbb{Z}/p\mathbb{Z})^* \times (\mathbb{Z}/q\mathbb{Z})^* : 0 < a < p \text{ e } 0 < b < \frac{q}{2}\}$$

Dado  $([a]_p, [b]_q) \in D$ , sabemos que existe um único  $k$  com  $0 < k < pq$  tal que  $\gamma([k]_{pq}) = ([a]_p, [b]_q)$ . Se  $\frac{pq}{2} < k < pq$ , é claro que  $\gamma([pq - k]_{pq}) = \gamma([-k]_{pq}) = ([-a]_p, [-b]_q) = -([a]_p, [b]_q)$ . Desta discussão conclui-se facilmente que, para cada  $([a]_p, [b]_q) \in D$ , existe uma única classe de congruência  $[k]_{pq} \in E$  tal que  $\gamma([k]_{pq})$  é  $([a]_p, [b]_q)$  ou  $-([a]_p, [b]_q)$ . Logo:

$$(*) \quad \prod_{\substack{0 < k < \frac{pq}{2} \\ k \perp pq}} (k, k) = \varepsilon \prod_{\substack{0 < a < p \\ 0 < b < \frac{q}{2}}} (a, b)$$

em que  $\varepsilon$  é 1 ou  $-1$ , e onde o sinal de igualdade deve ser entendido como igualdade modular em  $p$  na primeira componente e igualdade modular em  $q$  na segunda componente. Com este entendimento, e pondo  $r := \frac{p-1}{2}$  e  $s := \frac{q-1}{2}$  tem-se:

$$\prod_{\substack{0 < a < p \\ 0 < b < \frac{q}{2}}} (a, b) = \prod_{0 < a < p} \prod_{0 < b < \frac{q}{2}} (a, b) = \prod_{0 < a < p} (a^s, s!) = ((p-1)!)^s, s!^{p-1} = ((p-1)!)^s, s!^{2r}$$

Ora, módulo  $q$ , tem-se que  $s!^2 = s!s! = s!(-1)(s+1)(-1)(s+2)\cdots(-1)(q-1) = (q-1)!(-1)^s$ , pois  $s+i \equiv -(s+1-i) \pmod{q}$ , para  $1 \leq i \leq s$ . Sai:

$$\prod_{\substack{0 < a < p, \\ 0 < b < \frac{q}{2}}} (a, b) = ((p-1)!)^s, (q-1)!^r (-1)^{rs} = ((-1)^s, (-1)^r (-1)^{rs})$$

pelo teorema de Wilson.

Vamos agora calcular (módulo  $p$ ) a primeira componente de  $\prod_{0 < k < \frac{pq}{2}, k \perp pq} (k, k)$ . Tem-se

$$\prod_{\substack{0 < k < \frac{pq}{2} \\ k \perp pq}} k = \left( \prod_{\substack{0 < k < \frac{pq}{2} \\ p \nmid k}} k \right) \left( \prod_{\substack{0 < k < \frac{pq}{2} \\ q \mid k}} k \right)^{-1}$$

onde o fator inverso permite cancelar os fatores  $k$  que são múltiplos de  $q$  e que aparecem no primeiro produto do lado direito da igualdade. Assim, a primeira componente é

$$\left( \prod_{0 < k < p} k \right) \left( \prod_{p < k < 2p} k \right) \cdots \left( \prod_{(s-1)p < k < sp} k \right) \left( \prod_{sp < k < \frac{pq}{2}} k \right) (q(2q)(3q)\cdots(rq))^{-1}$$

e, módulo  $p$ , fica  $(p-1)!^s \cdot r! \cdot (q^r r!)^{-1}$  porque  $\prod_{sp < k < \frac{pq}{2}} k = r!$  (note-se que  $\frac{pq}{2} = sp + r + \frac{1}{2}$ ). A expressão simplifica para  $(-1)^s \left(\frac{q}{p}\right)$  usando o teorema de Wilson e o critério de Euler. Analogamente, a segunda componente (módulo  $q$ ) de  $\prod_{0 < k < \frac{pq}{2}, k \perp pq} (k, k)$  é  $(-1)^r \left(\frac{p}{q}\right)$ . Por  $(\star)$ , conclui-se

$$(-1)^s \left(\frac{q}{p}\right) = \varepsilon (-1)^s \quad \text{e} \quad (-1)^r \left(\frac{p}{q}\right) = \varepsilon (-1)^r (-1)^{rs}$$

Logo  $\left(\frac{q}{p}\right) = \varepsilon$  e  $\left(\frac{p}{q}\right) = \varepsilon (-1)^{rs}$ , o que demonstra a lei da reciprocidade quadrática.  $\square$

Para estabelecer o teorema da reciprocidade quadrática da secção anterior falta-nos ainda uma lei. A lei será demonstrada na próxima secção:

$$\left(\frac{2}{p}\right) = \begin{cases} 1 & \text{se } p \equiv \pm 1 \pmod{8} \\ -1 & \text{se } p \equiv \pm 3 \pmod{8} \end{cases}$$

onde  $p$  é um primo ímpar. Equivalentemente:

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

Podemos agora demonstrar o teorema da reciprocidade quadrática. 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  $p \equiv q \pmod{4}$ , 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. Seja

$a = 2^l p_1^{r_1} \cdots p_k^{r_k}$  a fatorização de  $a$  em primos distintos. Os primos (ímpares)  $p_1, \dots, p_k$  são todos diferentes de  $p$  e de  $q$  (pois  $p \perp a$  e  $q \perp a$ ). Ora:

$$\left(\frac{a}{p}\right) = \left(\frac{2}{p}\right)^l \left(\frac{p_1}{p}\right)^{r_1} \cdots \left(\frac{p_k}{p}\right)^{r_k} \quad \text{e} \quad \left(\frac{a}{q}\right) = \left(\frac{2}{q}\right)^l \left(\frac{p_1}{q}\right)^{r_1} \cdots \left(\frac{p_k}{q}\right)^{r_k}$$

Para mostrar que  $\left(\frac{a}{p}\right) = \left(\frac{a}{q}\right)$ , basta ver que  $\left(\frac{p_i}{p}\right) = \left(\frac{p_i}{q}\right)$ , para  $1 \leq i \leq k$  e, caso  $l \neq 0$ ,  $\left(\frac{2}{p}\right) = \left(\frac{2}{q}\right)$ . Dado que se tem  $p \equiv q \pmod{4}$  e  $p \equiv q \pmod{p_i}$  vem

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

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 na fatorização de  $a$ , então tem-se mesmo  $p \equiv q \pmod{8}$ . A igualdade desejada sai imediatamente, atendendo à lei do símbolo de Legendre para o número 2.