RECIPROCIDADE QUADRÁTICA

Carlos Gustavo T. de A. Moreira & Nicolau C. Saldanha, Rio de Janeiro - RJ

♦ Nível Avançado.

A lei de Gauss de reciprocidade quadrática afirma que se p e q são primos há uma relação direta entre p ser quadrado módulo q e q ser quadrado módulo p. Este teorema fornece um rápido algoritmo para determinar se a é quadrado módulo p onde a é um inteiro e p um número primo. Lembramos que a é quadrado módulo n se existe $x \in \mathbb{Z}$ com $x^2 \equiv a \pmod{n}$. Este artigo foi adaptado de [3].

Definição: Seja p um primo e a um inteiro. Definimos o símbolo de Lagrange $\left(\frac{a}{p}\right)$ por

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & \text{se } p \text{ divide } a \\ -1 & \text{se } a \text{ não é quadrado módulo } p \\ 1 & \text{se } p \text{ não divide } a \text{ e } a \text{ é quadrado módulo } p. \end{cases}$$

Proposição: Seja p um primo ímpar e $a \in \mathbb{Z}$ tal que p não divide a.

Então $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}$.

Demonstração: Sabemos que se p não divide a então $a^{p-1} \equiv 1 \pmod{p}$, ou seja, $x^{p-1} - 1$ tem como raízes 1, 2,..., p – 1 em $\mathbb{Z}/p\mathbb{Z}$. Por outro lado, $x^{p-1} - 1 = \left(x^{\frac{p-1}{2}} - 1\right)\left(x^{\frac{p-1}{2}} + 1\right)$. Se existe $b \in \mathbb{Z}$ tal que $a \equiv b^2 \pmod{p}$ então $a^{\frac{p-1}{2}} \equiv b^{p-1} \equiv 1 \pmod{p}$; ou seja, $\left(\frac{a}{p}\right) = 1 \equiv a^{\frac{p-1}{2}} \pmod{p}$.

Como $x^2 \equiv y^2 \pmod{p} \Leftrightarrow x \equiv \pm y \pmod{p}$, há pelo menos $\frac{p-1}{2}$ quadrados em $(\mathbb{Z}/p\mathbb{Z})^*$, logo os quadrados são exatamente as raízes de $x^{\frac{p-1}{2}} - 1$ em $\mathbb{Z}/p\mathbb{Z}$, donde os não quadrados são exatamente as raízes de $x^{\frac{p-1}{2}} + 1$, ou seja, se $\left(\frac{b}{p}\right) = -1$ então $b^{\frac{p-1}{2}} \equiv -1 \pmod{p}$.

Corolário: Se p é primo ímpar então $\left(\frac{-1}{p}\right)=(-1)^{\frac{p-1}{2}}$.

Vamos agora reinterpretar a proposição. Seja $a\in(\mathbb{Z}/p\mathbb{Z})^*$. Para cada $j=1,2,...,\frac{p-1}{2}$ escrevemos $a\cdot j$ como $\varepsilon_j m_j$ com $\varepsilon_j\in\{-1,1\}$ e $m_j\in\left\{1,2,...,\frac{p-1}{2}\right\}$. Se $m_i=m_j$ temos $a\cdot i=a\cdot j$ ou $a\cdot i=-a\cdot j$; a primeira possibilidade implica $i=j$ e a segunda é impossível. Assim, se $i\neq j$ temos $m_i\neq m_j$ donde $\left\{m_1;m_2;...;m_{\frac{p-1}{2}}\right\}=\left\{1,2,...,\frac{p-1}{2}\right\}$. Assim,

$$\left(\frac{a}{p}\right)\equiv a^{\frac{p-1}{2}}=\frac{(a\cdot 1)(a\cdot 2)..\left(a\cdot\frac{p-1}{2}\right)}{1\cdot 2\cdot ....\cdot\frac{p-1}{2}}\equiv$$

$$\equiv\frac{\varepsilon_1\varepsilon_2...\varepsilon_{\frac{p-1}{2}}m_1\cdot m_2\cdot ....\cdot m_{\frac{p-1}{2}}}{1\cdot 2\cdot ....\cdot\frac{p-1}{2}}=\varepsilon_1\varepsilon_2...\varepsilon_{\frac{p-1}{2}}\ (\text{mod } p)$$

donde $\left(\frac{a}{p}\right)=\varepsilon_1\varepsilon_2...\varepsilon_{\frac{p-1}{2}}$, pois ambos pertencem a { − 1, 1}. Assim, $\left(\frac{a}{p}\right)=(-1)^m$, onde m é o número de elementos j de $\left\{1,2,...,\frac{p-1}{2}\right\}$ tais que $\varepsilon_j=-1$. Como primeira conseqüência deste fato temos o seguinte resultado.

Proposição: Se p é um primo ímpar então

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

Demonstração: Se $p\equiv 1(\text{mod } 4)$, digamos $p=4k+1$, temos $\frac{p-1}{2}=2k$. Como $1\le 2j\le\frac{p-1}{2}$ para $j\le k$ e $\frac{p-1}{2}<2j\le p-1$ para $k+1\le j\le 2k$, temos

$$\left(\frac{a}{p}\right)=(-1)^k=\begin{cases}1, & \text{se } p\equiv 1\ (\text{mod } 8),\\ -1, & \text{se } p\equiv 5\ (\text{mod } 8).\end{cases}$$

Se $p \equiv 3 (\mathrm{mod}\, 4)$, digamos $p = 4k+3$, temos $\frac{p-1}{2} = 2k+1$. Para $1 \le j \le k$ temos $1 \le 2j \le \frac{p-1}{2}$ e para $k+1 \le j \le 2k+1$ temos $\frac{p-1}{2} < 2j \le p-1$, donde

$$\left(\frac{a}{p}\right) = (-1)^{k+1} = \begin{cases} -1, & \text{se } p \equiv 3 \pmod 8, \\ 1, & \text{se } p \equiv 7 \pmod 8. \end{cases}$$

Teorema: (Lei de reciprocidade quadrática) Sejam p e q primos ímpares.

Então $\left(\frac{p}{q}\right) = (-1)^{(p-1)(q-1)/4} \left(\frac{q}{p}\right)$.

Demonstração: Na notação acima, com $a = q$, para cada $j \in P$, onde

$$P = \{1,2,\ldots,(p-1)/2\},$$

temos que $\varepsilon_j = -1$ se e só se existe $y \in \mathbb{Z}$ tal que $-(p-1)/2 \le qj - py < 0$. Tal y deve pertencer a Q, onde $Q = \{1,2,\ldots,(q-1)/2\}$.

Assim, temos que $\left(\frac{q}{p}\right) = (-1)^m$ onde $m = |X|$ e

$$X = \{(x,y) \in P \times Q \mid -(p-1)/2 \le qx - py < 0\};$$

note que $qx - py$ nunca assume o valor 0. Analogamente, $\left(\frac{p}{q}\right) = (-1)^n$, onde $n = |Y|$

e $Y = \{(x,y) \in P \times Q \mid 0 < qx - py \le (q-1)/2\}$.

Daí segue que $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^k$ onde $k = m + n = |Z|$ onde

$$Z = \{(x,y) \in P \times Q \mid -(p-1)/2 \le qx - py \le (q-1)/2\}$$

pois $qx - py$ nunca assume o valor 0. Temos $k = |C| - |A| - |B|$ onde $C = P \times Q$,

$$A = \{(x,y) \in C \mid qx - py < -(p-1)/2\},$$

$$B = \{(x,y) \in C \mid qx - py \quad (q-1)/2\}$$

Como $|C| = (p-1)(q-1)/4$, basta mostrar que $|A| = |B|$. Mas $f : C \quad C$ definida por $f(x,y) = (((p+1)/2) - x, ((q+1)/2) - y)$ define uma bijeção entre A e B □

Exemplo: Se $n \quad 1$ e $p = 2^{2^n} + 1$ é primo, então 3 não é quadrado módulo p (e logo 3 é raiz primitiva módulo p; ver [1]).

De fato, como $p \equiv 1 (\mathrm{mod}\ 4), \left(\frac{3}{p}\right) = \left(\frac{p}{3}\right)$, mas $2^{2^n} \equiv 1 (\mathrm{mod}\ 3)$, como pode ser facilmente mostrado por indução, donde $p = 2^{2^n} + 1 \equiv 2 (\mathrm{mod}\ 3)$, e $\left(\frac{p}{3}\right) = \left(\frac{2}{3}\right) = -1$.

REFERÊNCIAS:

[1] Carlos Gustavo T. de A. Moreira, *Divisibilidade, Congruências e Aritmética módulo n,* Eureka! Nº. 2, pp. 41-52, 1998.
[2] Guilherme Camarinha Fujiwara, *Inteiros de Gauss e Inteiros de Eisenstein*, *Eureka! Nº.* 14, pp. 23-31, 2002.
[3] Carlos Gustavo T. de A. Moreira e Nicolau C. Saldanha, *Primos de Mersenne (e outros primos muito grandes)*, 22º. Colóquio Brasileiro de Matemática, IMPA, 1999.