Jakobiho symboly

Legenderův lze rozšířit i pro složené jmenovatele induktivní definicí:

$$\left(\frac{a}{k\cdot\ell}\right) := \left(\frac{a}{k}\right)\cdot\left(\frac{a}{\ell}\right).$$

Na základě konvence budeme i v tomto případě uvažovat jen liché jmenovatele.

Tomuto zobecněnému symbolu říkáme *Jakobiho symbol*. Značí se stejně, protože se jedná jen o rozšíření. Jakobiho symbol ztrácí pro složené jmenovatele některé vlastnosti Legenderova symbolu. Obecně např. neplatí

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

už proto, že hodnota vpravo často pro složená n není rovna ± 1, jak víme z Rabinova-Millerova testu. Jakobiho symbol také obecně není indikátorem kvadratické reziduity. Pokud je a kvadratickým reziduem pro $k\cdot\ell$, je kvadratickým reziduem pro k i pro ℓ. Případ $\left(\frac{a}{n}\right) = -1$ tedy vždy znamená, že a je kvadratické nereziduum modulo n, musí být totiž kvadratickým nereziduem pro alespoň jedno prvočíslo v rozkladu n. Naopak to ale neplatí: pokud je a kvadratické nereziduum modulo k i ℓ, je jistě kvadratickým nereziduem i modulo $k\cdot\ell$, přestože $\left(\frac{a}{k\cdot\ell}\right) = \left(\frac{a}{k}\right)\cdot\left(\frac{a}{\ell}\right) = -1\cdot -1 = 1$.

Některé důležité vlastnosti Legenderova symbolu jsou však zachovány i pro složené jmenovatele. Je to zejména výpočet hodnoty pro -1, pro 2 a také formule pro reciprocitu.

Věta. Nechť $a, b \in \mathbb{Z}$ a nechť $m, n \in \mathbb{Z}$ jsou lichá čísla. Pak platí

(1)
$$\left(\frac{ab}{n}\right) = \left(\frac{a}{n}\right)\cdot\left(\frac{b}{n}\right)$$

(2) Pro $a \equiv b \mod n$ platí
$$\left(\frac{a}{n}\right) = \left(\frac{b}{n}\right)$$

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

(4)
$$\left(\frac{2}{n}\right) = (-1)^{\frac{n^2-1}{8}}$$

(5)
$$\left(\frac{n}{m}\right)\cdot\left(\frac{m}{n}\right) = (-1)^{\frac{(n-1)(m-1)}{4}}$$

Důkaz. První dva body plynou okamžitě z definice a vlastností Legenderova symbolu.

Zbývající dokážeme indukcí podle počtu členů v prvočíselném rozkladu jmenovatele. Použijeme opakovaně vztah

$$(\clubsuit) \qquad (x-1)+(y-1)+(x-1)(y-1) = xy-1.$$

Nechť $n = k \cdot \ell$. Pak podle indukčního předpokladu platí

$$\left(\frac{-1}{n}\right) = \left(\frac{-1}{k}\right)\left(\frac{-1}{\ell}\right) = (-1)^{\frac{k-1}{2}} \cdot (-1)^{\frac{\ell-1}{2}} = (-1)^{\frac{k-1}{2}} \cdot (-1)^{\frac{\ell-1}{2}} \cdot (-1)^{\frac{(k-1)(\ell-1)}{2}}$$
$$= (-1)^{\frac{k\ell-1}{2}} = (-1)^{\frac{n-1}{2}}.$$

Třetí rovnost plyne z toho, že $\frac{(k-1)(\ell-1)}{2}$ je sudé, čtvrtá využívá (♣).

Podobně dostaneme na základě pozorování, že čtverec lichého čísla je vždy roven jedné modulo 8, bod (4):

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

Stejně odvodíme i kvadratickou reciprocitu. Vzhledem k symetrii m a n stačí uvažovat složenost jen jednoho z čísel.

$$\left(\frac{m}{k\ell}\right)\left(\frac{k\ell}{m}\right) = \left(\frac{m}{k}\right)\left(\frac{k}{m}\right)\left(\frac{m}{\ell}\right)\left(\frac{\ell}{m}\right) = (-1)^{\frac{(k-1)(m-1)}{4}} \cdot (-1)^{\frac{(\ell-1)(m-1)}{4}}$$
$$= (-1)^{\frac{(k-1)(m-1)}{4}} \cdot (-1)^{\frac{(\ell-1)(m-1)}{4}} (-1)^{\frac{(k-1)(\ell-1)(m-1)}{4}} =$$
$$= (-1)^{\frac{(k\ell-1)(m-1)}{4}} = (-1)^{\frac{(n-1)(m-1)}{4}}.$$

□

Předchozí věta má velké praktické využití pro výpočet Jakobiho symbolů. Postupným využitím zákona reciprocity totiž můžeme hodnotu Jakobiho symbolu spočítat jen dělením se zbytkem, bez znalosti faktorizace uvažovaných čísel. Ze vzniklých sudých čísel odstraníme dvojky použitím explicitního vzorce (5).