Kvadratická reciprocita

Nechť p a q jsou lichá prvočísla. Ptáme se, jaký je vztah mezi tím, že p je kvadratické reziduum modulo q, a tím, že je q kvadratické reziduum modulo p. Odpověď dává věta o kvadratické reciprocitě.

Věta.

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

Ekvivalentní formulace:

$$\begin{cases} \left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right), & \text{pokud } p \equiv q \equiv 3 \mod 4 \\ \left(\frac{p}{q}\right) = \left(\frac{q}{p}\right), & \text{jinak.} \end{cases}$$

Důkaz. Uvažujme primitivní p-tou odmocninu z 1 nad tělesem $\mathbb{Z}_q$, označme ji ζ_p.

Důkaz budeme provádět v tělese $\mathbb{Z}_q[\zeta_p]$ a budeme uvažovat okruhový homomorfismus $\varphi : \mathbb{Z}[\omega_p] \to \mathbb{Z}_q[\zeta_p]$ splňující $\varphi(k) = k \mod q$ a $\varphi(\omega_p) = \zeta_p$.

Připomeňme Gaussův kvadratický součet modulo p definovaný jako

$$S = a_1\omega_p + a_2\omega_p^2 + \cdots + a_{p-1}\omega_p^{p-1},$$

kde

$$a_k = \left(\frac{k}{p}\right).$$

Z binomického rozvoje, a protože $a_k = \pm 1$ a q je liché, platí

$$(a_0+a_1\omega_p+a_2\omega_p^2+\cdots+a_{p-1}\omega_p^{p-1})^q = a_0+a_1\omega_p^q+a_2\omega_p^{2q}+\cdots+a_{p-1}\omega_p^{(p-1)q} \mod q.$$

Tedy

$$S^q = \sum_{k=0}^{p-1}\left(\frac{k}{p}\right)\omega_p^{kq} \mod q$$

Použijeme-li zřejmý fakt

$$\left(\frac{k}{p}\right) = \left(\frac{kq^2}{p}\right) = \left(\frac{q}{p}\right)\left(\frac{kq}{p}\right),$$

dostáváme

$$S^q = \left(\frac{q}{p}\right)\sum_{k=0}^{p-1}\left(\frac{kq}{p}\right)\omega_p^{kq} = \left(\frac{q}{p}\right)S \mod q.$$

Poslední rovnost plyne z toho, že $k \mapsto qk$ je permutace $\mathbb{Z}_p$. Protože

Vztah mezi S a $\left(\frac{p}{q}\right)$, získáváme díky tomu, že Gaussův kvadratický součet S splňuje

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

Pak totiž

$$S^{q-1} = (S^2)^{\frac{q-1}{2}} = (-1)^{\frac{(p-1)(q-1)}{4}}\left(\frac{p}{q}\right).$$

Uvedená rovnost platí jistě i modulo q, a tedy

$$\left(\frac{q}{p}\right)\cdot S = (-1)^{\frac{(p-1)(q-1)}{4}}\left(\frac{p}{q}\right)\cdot S \mod q.$$

Označme

$$\delta := (-1)^{\frac{(p-1)(q-1)}{4}} \left(\frac{p}{q}\right)\left(\frac{q}{p}\right)$$

hodnotu, o které chceme ukázat, že je rovna jedné. Víme $\delta = \pm 1$ a

$$(\delta - 1)S = 0 \mod q.$$

Pokud by $\delta = -1$, dostali bychom díky invertibilitě $2 \mod q$ (tj. vynásobením obou stran rovnice číslem $\frac{q+1}{2}$) vztah

$$S = 0 \mod q.$$

Zbývá tedy ukázat, že tato rovnost neplatí. Na tomto místě je vhodné se blíže zamyslet nad tím, co jsme vlastně mínili výrazem $\mod q$. Vzhledem k tomu, že se pohybujeme v okruhu $\mathbb{Z}[\omega_p]$, znamená rovnost $x = y \mod q$, že $x - y$ leží v hlavním ideálu $q \cdot \mathbb{Z}[\omega_p]$. Kdyby S v tomto ideálu leželo, leželo by tam i $|S^2| = p$. Předpokládejme pro spor, že

$$p = c_0 + c_1\omega_p + c_2\omega_p^2 + \cdots + c_{p-1}\omega_p^{p-1},$$

kde $c_i \in q\mathbb{Z}$. To znamená, že ω_p je kořenem polynomu $(c_0 - p) + c_1x + c_2x^2 + \cdots + c_{p-1}\omega_p$, který je tedy soudělný s polynomem $1 + x + x^2 + \cdots + x^{p-1}$, jehož je ω_p také kořenem. Polynom $1 + x + x^2 + \cdots + x^{p-1}$ je ale irreducibilní nad $\mathbb{Q}$, takže musí pro nějaké racionální číslo r platit

$$(c_0 - p) + c_1x + c_2x^2 + \cdots + c_{p-1}\omega_p = r \cdot (1 + x + x^2 + \cdots + x^{p-1}).$$

Vidíme, že $r = c_0 - p = c_1 = \cdots = c_{p-1}$, což je spor, protože $c_0 - p$ neleží, na rozdíl od c_i, v $q\mathbb{Z}$. □

Algebraické úvahy k předchozímu důkazu. Předchozí důkaz je veden poměrně jednoduchou myšlenkou uvažovat $\mathbb{Z}[\omega_p]$ modulo q. Tato myšlenka ale není tak nevinná, jak se na první pohled zdá, což vede ke krkolomně působícímu závěru celého důkazu.

Ve snaze se komplikacím vyhnout můžeme být v pokušení jednoduše prohlásit, že budeme pracovat v $\mathbb{Z}_q[\omega_p]$. Taková struktura ale nedává dobrý smysl. K okruhu $\mathbb{Z}$ můžeme přidat prvek ω_p jeho nadtělesa $\mathbb{C}$, ale totéž nemůžeme udělat pro okruh (resp. těleso) $\mathbb{Z}_q$, protože ten není v $\mathbb{C}$ obsažen. Analogickým postupem bychom však mohli vytvořit $\mathbb{Z}_q[\zeta_p]$, kde ζ_p je primitivní p-tá odmocnina z jedné v příslušném rozkladovém nadtělese polynomu $x^p - 1$ nad tělesem $\mathbb{Z}_q$. Problém se ale přesune do faktu, že vztah $S^2 = \left(\frac{-1}{p}\right) p$ je dokázaný v $\mathbb{Z}[\omega_p]$ a není jasné, jak ho dokázat pro analogicky definovanou hodnotu v $\mathbb{Z}_q[\zeta_p]$. Možným řešením je přenést tento výsledek ze $\mathbb{Z}[\omega_p]$ do $\mathbb{Z}_q[\zeta_p]$ homomorfismem φ splňujícím $\varphi(\omega_p) = \zeta_p$ a $\varphi(1) = 1$ (a tedy $\varphi(z) = z \mod q$ pro $z \in \mathbb{Z}$). Pak bychom dostali vztah

$$\left(\frac{q}{p}\right) \cdot \varphi(S) = (-1)^{\frac{(p-1)(q-1)}{4}} \left(\frac{p}{q}\right) \cdot \varphi(S),$$

a možnost zkrátit $\varphi(S)$ by snadno plynula z toho, že

$$\varphi(S)^2 = \varphi(S^2) = \varphi(p) = p \mod q \neq 0.$$

To koresponduje se závěrečným krokem našeho původního důkazu, který konstatuje, že p není násobek q.

Úvahy o vlastnostech polynomů, jejichž kořenem je primitivní p-tá odmocnina se ale také zcela neztratily. Přesunuly se do nutnosti ověřit, že uvažovaný homomorfismus φ je dobře definovaný. Můžeme postupovat např. takto. Uvažme homomorfismus $\psi : \mathbb{Z}[x] \to \mathbb{Z}_q[\zeta_p]$ splňující $\psi(1) = 1$ a $\psi(x) = \zeta_p$. Že se jedná o homomorfismus, vidíme z toho, že vznikne složením homomorfismů $\mathbb{Z}[x] \to \mathbb{Z}_q[x]$ modulícího koeficienty a dosazovacího homomorfismu dosazujícího ζ_p za x. Okruh $\mathbb{Z}[\omega_p]$ je isomorfní okruhu $\mathbb{Z}[x]/m$, kde m je minimální polynom ω_p. To je právě polynom $1 + x + x^2 + \cdots + x^{p-1}$. Věta o homorfismu nyní garantuje definici φ, pokud ideál generovaný m leží v jádru ψ. To však platí, protože primitivní p-tá odmocnina je kořenem m nad libovolným tělesem.

K předvedené opatrnosti v definicích vede např. to, že navzdory intuitivnímu očekávání nemusí být $\mathbb{Z}_q[\zeta_p]$ isomorfní $\mathbb{Z}_q[x]/m$. Polynom m totiž může mít nad $\mathbb{Z}_q$ netriviální rozklad, a není tak minimálním polynomem ζ_p. Viz např.

$$\begin{aligned} x^{10} + x^9 + x^8 + x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x + 1 = \\ = \left(x^5 + 2x^3 + x^2 + 2x + 2\right)\left(x^5 + x^4 + 2x^3 + x^2 + 2\right) \mod 3. \end{aligned}$$