Kvadratická rezidua

Definice. Legenderův symbol:

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & a \text{ je čtverec modulo } p \\ -1 & a \text{ není čtverec modulo } p \\ 0 & a \equiv 0 \mod p \end{cases}$$

Pro $p = 2$ je situace zřejmá, Legenderův symbol se z praktických důvodů (např. proto, aby následující tvrzení dávalo smysl) definuje jen pro lichá prvočísla.

Tvrzení.

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

Důkaz. Pracujeme v $\mathbb{Z}_p^*$, což je cyklická grupa izomorfní $\mathbb{Z}_{p-1}$. Nechť je α primitivní prvek $\mathbb{Z}_p^*$. Platí, že $\alpha^{\frac{p-1}{2}}$ je rovno -1, je to totiž jediná involuce grupy $\mathbb{Z}_p^*$. Je-li $a = \alpha^r$, máme

$$a^{\frac{p-1}{2}} = (\alpha^{\frac{p-1}{2}})^r = (-1)^r.$$

Nyní si stačí uvědomit, že $a = \alpha^r$ je kvadratické reziduum, právě když je r sudé. □

Pozorování. Z předchozího tvrzení plyne, že

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

a také, že -1 je čtverec modulo p, právě když je $p - 1$ dělitelné 4.

Kdy je čtvercem dvojka?

Tvrzení. Dvojka je čtvercem modulo p, právě když je $p \equiv \pm 1 \mod 8$.

Důkaz. Použijeme Gaussova celá čísla modulo p, neboli $\mathbb{Z}_p[i]$. Zde platí

$$(1+i)^p \equiv 1 + i^p.$$

Navíc použijeme

$$(1+i)^2 = 2i, \qquad i^4 = 1, \qquad i^{\frac{p-1}{2}} = (-1)^{\frac{p-1}{4}} = -i(-1)^{\frac{p+1}{4}}.$$

(1) Nechť nejprve $p = 4k + 1$. Pak $i^p = i$ a

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

Tedy po zkrácení $(1 + i)$ máme

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

Pro $p = 8\ell + 1$ tedy dvojka je čtvercem, pro $p = 8\ell + 5$ nikoli.

(2) Nechť nyní $p = 4k - 1$. Pak $i^p = -i$ a podobně jako výše dostáváme

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

Opět můžeme krátit, neboť $(1 - i) = -i(1 + i)$ a máme

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

Pro $p = 8\ell - 1$ tedy dvojka je čtvercem, pro $p = 8\ell - 5$ nikoli.

□