Kvadratické zbytky

Jakub „šnEk“ Opršal

Definice. *Nechť $a \in \mathbb{Z}$ a $n \in \mathbb{N}$. Řekneme, že a je kvadratickým zbytkem modulo n pokud existuje $c \in \mathbb{N}$ takové, že $c^2 \equiv a \pmod{n}$. V opačném případě řekneme, že a je kvadratickým nezbytkem.*

Definice. *Nechť p je liché prvočíslo a $a \in \mathbb{Z}$, pak definujeme Legendreův symbol $\left(\frac{a}{p}\right)$ následovně:*

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & \text{pro } p|a \\ +1 & \text{pokud } a \text{ je kvadratickým zbytkem a } p \nmid a \\ -1 & \text{pokud } a \text{ neni kvadratickym zbytkem} \end{cases}$$

Lemma. (Počet kvadratických zbytků) *Nechť p je liché prvočíslo, pak mezi čísly $1, 2, \ldots, p-1$ je právě $\frac{p-1}{2}$ kvadratických zbytků modulo p a stejně tolik kvadratických nezbytků.*

Věta. (Eulerovo kritérium) *Nechť p je liché prvočíslo a $a \in \mathbb{Z}$, pak platí:*

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

Důkaz. Případ $p|a$ je jednoduchý, zaměříme se tedy na případ $p \nmid a$. Podle malé Fermatovy věty platí:

$$a^{p-1} \equiv 1 \pmod{p}$$
$$\left(a^{\frac{p-1}{2}} + 1\right)\left(a^{\frac{p-1}{2}} - 1\right) \equiv 0 \pmod{p}$$

Tedy $a^{\frac{p-1}{2}} \equiv \pm 1$ (Protože p je prvočíslo.)

Je-li a kvadratický zbytek pak platí, že existuje $c \in \mathbb{Z}$ takové, že $c^2 \equiv a$ tedy $a^{\frac{p-1}{2}} \equiv c^{p-1} \equiv 1$ (opět podle malé Fermatovy věty), tedy pro kvadratický zbytek věta platí. Navíc žádné jiné číslo kromě $\frac{p-1}{2}$ nenulových kvadratických zbytků modulo p nemůže splňovat $a^{\frac{p-1}{2}} - 1 \equiv 0$, protože levá strana této kongruence je mnohočlen stupně $\frac{p-1}{2}$ a proto má tato rovnice nejvýše $\frac{p-1}{2}$ kořenů modulo p. Tedy pro kvadratické nezbytky platí: $a^{\frac{p-1}{2}} \equiv -1$. □

Uvažme dvě reprezentace zbytků po dělení nějakým lichým prvočíslem p a to množiny:

$$M = \{-\tfrac{p-1}{2}, \ldots, -1, 0, 1, \ldots, \tfrac{p-1}{2}\}$$
$$N = \{0, 1, \ldots, p-1\}$$

Dále pro nějaké celé číslo a $(p \nmid a)$ uvažme posloupnosti délky $p-1$:

$$M(a) = \left\langle m_k \in M : k \in \{1,2,\ldots,\tfrac{p-1}{2}\}, ka \equiv m_k \pmod p \right\rangle$$
$$N(a) = \left\langle n_k \in N : k \in \{1,2,\ldots,\tfrac{p-1}{2}\}, ka \equiv n_k \pmod p \right\rangle$$

Označme $m(a)$ počet záporných členů $M(a)$ a obdobně $n(a)$ počet členů $N(a)$ větších než $\frac{p-1}{2}$. Uvědomme si, že záporné členy $M(a)$ dostaneme z členů $N(a)$, které jsou větší než $\frac{p-1}{2}$ tak, že od nich odečteme p, tedy speciálně dostáváme $n(a) = m(a)$.

Zamyslíme-li se hlouběji snadno přijdeme na to, že pokud v posloupnosti $N(a)$ změníme znaménka všech členů na kladná (označme takovou posloupnost $N^+(a)$) dostaneme všechny zbytky od 1 do $\frac{p-1}{2}$, neboť kdybychom uvážili posloupnost

$$M_-(a) = \left\{ < m_{-k} \in M : k \in \{1,2,\ldots,\tfrac{p-1}{2}\}, -ka \equiv m_{-k} \pmod p \right\}$$

Tak tato posloupnost má právě členy opačných znamének, než $M(a)$ a obě posloupnosti dohromady mají za členy všechny nenulové zbytky modulo p.

Věta. (Gaussovo lemma) *Nechť $a \in \mathbb{Z}$ a p je liché prvočíslo, navíc $p \nmid a$, pak platí:*

$$\left(\frac{a}{p}\right) = (-1)^{m(a)} = (-1)^{n(a)}$$

Důkaz. Protože $m(a) = n(a)$ stačí nám dokázat první rovnost. Platí:

$$\left(\frac{p-1}{2}\right)! = \prod_{m \in M^+(a)} \equiv (-1)^{m(a)} \prod_{k=1}^{\frac{p-1}{2}} ka = (-1)^{m(a)} a^{\frac{p-1}{2}} \left(\frac{p-1}{2}\right)!$$

Pokrácením $\left(\frac{p-1}{2}\right)!$ (což je jistě nesoudělné s p) na obou stranách a použitím Eulerova kritéria dostaneme kongruenci $1 \equiv (-1)^{m(a)} \left(\frac{a}{p}\right)$, což lze snadno upravit do požadovaného tvaru vynásobením $(-1)^{m(a)}$. □

Věta. (Zákon kvadratické reciprocity) *Nechť p, q jsou dvě lichá prvočísla, pak platí:*

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

Lemma. (Nutnost čtyř čtverců) *Nechť $k, m \in \mathbb{N} \cup \{0\}$. Číslo $4^m(8k+7)$ nelze zapsat jako součet nejvýše tří čtverců přirozených čísel.*

Věta. (Lagrange) *Každé přirozené číslo lze zapsat jako součet nejvýše čtyř čtverců přirozených čísel.*