Výpočet hodnot Eulerovy funkce $\varphi(m) = |\mathbb{Z}_m^\times|$

Věta. *Je-li p prvočíslo a $n \in \mathbb{N}$, pak* $\varphi(p^n) = (p-1) \cdot p^{n-1}$. Důkaz.

Věta. *Jsou-li $a, b \in \mathbb{Z}$ nesoudělná celá čísla, pak* $\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)$. Důkaz. Pokračování.

Příklad. Předpoklad o nesoudělnosti je v předchozí větě podstatný, platí třeba $\varphi(2 \cdot 2) = 2 \neq 1 = \varphi(2) \cdot \varphi(2)$.

Důsledek. *Nechť $m \in \mathbb{N}$. Rozložme m na součin mocnin různých prvočísel, tj.*

$$m = p_1^{e_1} \cdot p_2^{e_2} \cdots p_s^{e_s},$$

kde $p_1, p_2, \ldots, p_s$ jsou různá prvočísla, $e_1, e_2, \ldots, e_s \in \mathbb{N}$. Pak platí

$$\varphi(m) = (p_1 - 1) \cdot p_1^{e_1 - 1} \cdot (p_2 - 1) \cdot p_2^{e_2 - 1} \cdots (p_s - 1) \cdot p_s^{e_s - 1},$$

což je možné zapsat také takto:

$$\varphi(m) = m \cdot \prod_{\text{prvočíslo } p \mid m} \left(1 - \tfrac{1}{p}\right).$$

Základní vlastnosti grup, mocnina v pologrupě

Věta. *Nechť $(G, \cdot)$ je pologrupa, $a_1, \ldots, a_n \in G$, přičemž $n > 1$. Pak výsledek součinu prvků $a_1, \ldots, a_n$ (v tomto pořadí) nezáleží na jejich uzávorkování.* Důkaz.

Věta. *Nechť $(G, \cdot)$ je komutativní pologrupa, $a_1, \ldots, a_n \in G$, přičemž $n > 1$. Pak výsledek součinu prvků $a_1, \ldots, a_n$ nezáleží na jejich pořadí.*

Definice. Nechť $(G, \cdot)$ je pologrupa, $a \in G$, $n \in \mathbb{N}$. **Mocninu** a^n prvku a v pologrupě G definujeme jako součin n exemplářů prvku a:

$$a^n = \underbrace{a \cdot \ldots \cdot a}_{n}$$

(podle výše uvedené věty není nutné specifikovat uzávorkování).

Věta. *Nechť $(G, \cdot)$ je pologrupa, $a \in G$, $m, n \in \mathbb{N}$. Pak platí* $a^m \cdot a^n = a^{m+n}$, $\quad (a^m)^n = a^{m \cdot n}$. Důkaz.

Invertibilní prvky

Označení. Nechť $(G, \cdot)$ je grupoid s neutrálním prvkem. Víme, že tento neutrální prvek je v G jediný. Budeme jej označovat symbolem 1 (přestože to nemusí být přirozené číslo 1).

Definice. Nechť $(G, \cdot)$ je pologrupa s neutrálním prvkem 1. Pokud k nějakému $a \in G$ existuje v G prvek inverzní, říkáme, že prvek a je **invertibilní**. Inverzní prvek k prvku a budeme označovat symbolem a^{-1}.

Věta. Nechť $(G, \cdot)$ je pologrupa s neutrálním prvkem 1, $a, a_1, \ldots, a_n$ libovolné invertibilní prvky z G. Pak platí

$$\begin{aligned} 1^{-1} &= 1, \\ (a^{-1})^{-1} &= a, \\ (a_1 \cdot \ldots \cdot a_n)^{-1} &= a_n^{-1} \cdot \ldots \cdot a_1^{-1}. \end{aligned}$$

Množina všech invertibilních prvků pologrupy, mocnina v grupě

Věta. *Nechť $(G, \cdot)$ je pologrupa s neutrálním prvkem 1, H množina všech invertibilních prvků z G. Pak $(H, \cdot)$ je grupa.*

Poznámka. Operace $\cdot$ na množině H je zúžením původní operace na množině G (má stejný předpis, ale je definována na menším definičním oboru $H \times H$ a má menší obor hodnot H).

Poznámka. Předchozí větu jsme už několikrát použili: na pologrupách čtvercových matic $(M_{n,n}(R), \cdot)$, zobrazení $(X^X, \circ)$ a zbytkových tříd $(\mathbb{Z}_m, \cdot)$. Vznikly grupy $\mathcal{GL}_n(R)$, $\mathcal{S}(X)$ a $\mathbb{Z}_m^\times$.

Definice. Nechť $(G, \cdot)$ je grupa s neutrálním prvkem 1, $a \in G$. **Mocninu** a^n prvku a v grupě G definujeme i pro nekladný celočíselný exponent: $a^0 = 1, \quad a^{-n} = (a^n)^{-1}$ pro libovolné $n \in \mathbb{N}$.

Věta. *Nechť $(G, \cdot)$ je grupa, $a \in G$, $m, n \in \mathbb{Z}$. Pak platí* $a^m \cdot a^n = a^{m+n}, \quad (a^m)^n = a^{m \cdot n}$. Část důkazu.

Věta. *Nechť $(G, \cdot)$ je komutativní grupa, $a, b \in G$, $m \in \mathbb{Z}$. Pak platí* $(a \cdot b)^m = a^m \cdot b^m$.

Řád prvku v grupě

Definice. Nechť G je grupa, $a \in G$. Existuje-li přirozené číslo n tak, že $a^n = 1$, pak nejmenší přirozené číslo n s touto vlastností se nazývá **řád prvku** a v grupě G. Příklad. Neexistuje-li žádné přirozené číslo n s touto vlastností, říkáme, že řád prvku a v grupě G je ∞.

Věta. *Nechť G je grupa, $a \in G$. Je-li řád prvku a v grupě G přirozené číslo n, pak pro libovolná $k, l \in \mathbb{Z}$ platí*

$$a^k = a^l \iff k \equiv l \pmod{n}.$$ Důkaz.

Je-li naopak řád prvku a v grupě G roven ∞, pak pro libovolná $k, l \in \mathbb{Z}$ platí

$$a^k = a^l \iff k = l.$$ Důkaz.

Důsledek. *Nechť řád prvku a v grupě G je $n \in \mathbb{N}$. Nechť r je zbytek po dělení čísla $k \in \mathbb{Z}$ číslem n, pak $a^k = a^r$. Prvky $a^0 = 1$, $a^1 = a$, a^2, $\ldots$, a^{n-1} jsou po dvou různé.*

Důsledek. *Řád prvku a v grupě G tedy udává, kolik existuje různých mocnin prvku a. V konečné grupě má každý prvek konečný řád.*

Důsledky věty

Věta. *Nechť G je grupa, $a \in G$. Je-li řád prvku a v grupě G přirozené číslo n, pak pro libovolná $k, l \in \mathbb{Z}$ platí*

$$a^k = a^l \qquad \Longleftrightarrow \qquad k \equiv l \pmod{n}.$$

Důsledek. *Nechť G je grupa, $a \in G$, $k \in \mathbb{N}$. Pak $a^k = 1$, právě když řád prvku a je přirozené číslo, jehož násobkem je číslo k.*

Důsledek. *Nechť G je grupa, $a \in G$, prvek řádu $k \in \mathbb{N}$. Je-li $k = n \cdot m$ pro nějaká $n, m \in \mathbb{N}$, pak řád prvku a^n je m.* Důkaz.