Otázka 08 - Y01DMA

Zadání

Dělitelnost celých čísel. Eukleidův algoritmus pro nalezení největšího společného dělitele a jeho zobecnění. Relace modulo n, zbytkové třídy a operace s nimi. Binární operace na množině, pologrupy, monoidy a grupy. (Y01DMA)

Slovníček pojmů

- **Faktorizace - rozložení čísla na součin menších čísel (vetšinou prvočísel); my zde dále budeme pod pojmem faktorizace uvažovat právě prvočíselný rozklad.**
- **Prvočíselný rozklad - Prvočíselným rozkladem přirozeného čísla x rozumíme rovnost $x=p_1^{n_1}.p_2^{n_2}.\cdots.p_r^{n_r}$, kde $r\geq 1$ je přirozené číslo, $p_1<p_2<\cdots<p_r$ jsou navzájem různá prvočísla a $n_1,n_2,\cdots,n_r$ jsou kladná přirozená čísla.**
- **Princip dobrého uspořádání - Každá neprázdná podmnožina množiny přirozených čísel má nejmenší prvek. Toto tvrzení je ekvivalentní vzhledem k tvrzení: v množině $\mathbb{N}$ neexistuje nekonečná klesající posloupnost $x_0>x_1>x_2\cdots$.**

Dělitelnost celých čísel

Definice relace dělění

Celé číslo a dělí celé číslo b (značíme $a|b$), pokud existuje celé číslo n takové, že $b=n.a$

Základní věta elementární teorie čísel

Pro každé přirozené číslo $x\geqslant 2$ existuje jednoznačný prvočíselný rozklad.

Dělení se zbytkem v oboru celých čísel

a,b jsou libovolná celá čísla, $b\neq 0$, pak existují jednoznačně určená celá čísla q a r taková, že platí:

1. $a=q.b+r$
2. **Číslo r splňuje nerovnost $0\leqslant r<|b|$**

Jednoznačně určené r nazýváme zbytkem po dělení čísla a číslem b.

Eukleidův algoritmus pro nalezení největšího společného dělitele

Definice největšího společného dělitele

Přirozené číslo d je největším společným dělitelem přirozených čísel a a b (označení $d=\gcd(a,b)$), pokud jsou splněny následující podmínky:

1. **Číslo d je společným dělitelem čísel a, b, tj. platí, $d|a$ a současně $d|b$ (v oboru přirozených čísel).**
2. **Číslo d je největším ze všech společných dělitelů čísel a, b, tj. platí následující: je-li c takové přirozené číslo, pro které platí $c|a$ a současně $c|b$, potom $c|d$.**

Pokud $\gcd(a,b)=1$, řekneme, že přirozená čísla a, b jsou *nesoudělná*.

Pokud známe prvočíselný rozklad čísel a a b, tak nalezení největšího společného dělitele těchto čísel je velmi snadné.

1. Příklad - nalezení gcd pomocí prvočíselného rozkladu

$a=1960=2^3.5.7^2$

$b=308=2^2.7.11$

Stačí vzít z obou prvočíselných rozkladů společná prvočísla v maximální společné mocnině. Tedy:

$\gcd(a,b)=2^2.7=28$

2. Příklad - nalezení gcd pomocí prvočíselného rozkladu

$a=427=7.61$

$b=133=7.19$

$\gcd(a,b)=7$

3. Příklad - nalezení gcd pomocí prvočíselného rozkladu

$a=523=523$

$b=21=3.7$

Protože čísla nemají žádné společné prvočísla, je jediným společným dělitelem obou čísel 1. Z toho plyne, že největším společným dělitelem čísel a a b je 1, tj. čísla a a b jsou *nesoudělná*.

$\gcd(a,b)=1$

Největším problémem zde je, že nalezení provočíselného rozkladu je velmi obtížné. Na této skutečnosti je založeno šifrování RSA.

Eukleidův algoritmus

Euklidův algoritmus je způsob, jak najít největšího společného dělitele dvou přirozených čísel bez nutnosti jejich faktorizace.

Předpokládejme přirozená čísla a a b, pro která platí $a \geq b > 0$. Eukleidův algoritmus pro nalezení největšího společného dělitele je potom popsán takto:

Označme $b = b_0$ a dělením se zbytkem vytvořme posloupnost přirozených čísel $b_1, b_2, \cdots$:

$$a = q_0 . b_0 + b_1$$

$$b_0 = q_1 . b_1 + b_2$$

$$b_1 = q_2 . b_2 + b_3$$

$$\vdots$$

$$b_{n-2} = q_{n-1} . b_{n-1} + b_n$$

Platí, že $b_0 > b_1 > b_2 > b_3 > \cdots$, protože jde o zbytky při dělení. Proto existuje n takové, že $b_n = 0$ (to vyplývá z *principu dobrého uspořádání*; zajišťuje terminaci Eukleidova algoritmu). Když tohoto b_n dosáhneme, tak tvorbu posloupnosti $b_1, b_2, \cdots$ zastavíme. Potom číslo b_{n-1} je *největším společným dělitelem* čísel a a b, tj. $\gcd(a, b) = b_{n-1}$. To vychází z následujícího tvrzení.

Tvrzení

Předpokládejme, že pro přirozená čísla a a b platí $a \geq b > 0$. Vydělme číslo a číslem b se zbytkem. Pro některá q a r tedy platí:

$a = q . b + r$**, kde** $0 \leq r < b$**.**

1. **Je-li $r = 0$, potom b je největším společným dělitelem čísel a, b.**
2. **Je-li $r > 0$, označme jako d jakéhokoli společného dělitele původních čísel a a b. Potom d je společný dělitel čísel b a r. (DŮKAZ na stránce č. 49 v publikaci [1])**

Toto tvrzení nám dokazuje, že b_{n-1} je největším společným dělitelem čísel a a b, což je vidět z posledního řádku naší posloupnosti ($b_{n-2} = q_{n-1} . b_{n-1} + b_n$).

$b_n = 0$**, a tedy** $b_{n-1} = \gcd(a, b)$**.**

1. Příklad - Eukleidův algoritmus

Příklad běhu Euklidova algoritmu pro přirozená čísla $a = 427$, $b = 133$.

$$427 = 3 \cdot 133 + 28$$
$$133 = 4 \cdot 28 + 21$$
$$28 = 1 \cdot 21 + 7$$
$$21 = 3 \cdot 7 + 0$$

Postup

1. **Postupně provádíme dělení se zbytkem v oboru celých čísel.**
2. **Vezmeme číslo** $a=427$ **a vydělíme ho číslem** $b_0=b=133$ **se zbytkem, čímž získáme** $427=3.133+28$**.**
3. **Pokračujeme tím, že číslo** $b_0=b=133$ **vydělíme se zbytkem číslem** $b_1=28$**, čímž získáme** $133=4.28+21$**.**
4. **Dále číslo** b_1 **vydělíme číslem** b_2 **se zbytkem.**
5. **Takto pokračujeme do té doby, než je zbytek roven nule.**
6. **Když je zbytek roven nule, tj.** $b_n=0$**, tak mužeme číslo** $b_{n-1}=7$ **označit za největšího společného dělitele čísel** a **a** b**.**

Výsledek

$\gcd(a,b)=\gcd(427,133)=7$.

2. Příklad - Eukleidův algoritmus

Zadání tohoto příkladu je shodné s předchozím příkladem. Liší se pouze ve formě zápisu jeho řešení.

	427	a
	133	b
3	28	b_1
4	21	b_2
1	7	$b_3 = b_{n-1}$
3	0	$b_4 = b_n$

Písmena po pravé straně obrázku jsou pouze informativní.

Postup

1. Číslo 427 vydělíme číslem 133 se zbytkem. Zbytek po dělení (28) napíšeme pod dělitele, výsledek (3) napíšeme zleva od zbytku.
2. Takto postupujeme do té doby, než se zbytek rovná nule. Zbytek se rovná 0 na čtvrtém řádku výpočtu. Tedy $b_4 = b_n = 0$.
3. Největší společný dělitel čísel 427 a 133 je tedy $b_3 = b_{n-1} = 7$.

3. Příklad - Eukleidův algoritmus

Úkolem je naleznout největšího společného dělitele čísel $a=99$ a $b=28$.

Postup

Opět použijeme Eukleidův algoritmus na čísla a a b s tím, že dělíme větší číslo menším.

	99	
	28	
3	15	
1	13	
1	2	
6	1	
2	0	

Na průběhu algoritmu je vidět, že největším společným dělitelem čísel a a b je číslo 1. Čísla a a b jsou tedy nesoudělná.

Bezoutova rovnost

Ať a a b jsou přirozená čísla. Potom existují celá čísla α, β tak, že platí rovnost: $\gcd(a,b) = \alpha.a + \beta.b$.

K nalezení čísel α a β slouží *rozšířený Eukleidův algoritmus*.

Příklad

$\gcd(427,133) = 7$ **(viz. výše)**

Rovnosti, které jsme vytvořili v průběhu průchodu euklidovým algoritmem využijeme pro nalezení koeficientů $\alpha, \beta \in \mathbb{Z}$ Bezoutovy rovnice. Tzn. hledáme celá čísla α, β, tak, aby platilo:

$7 = \alpha.427 + \beta.133$

Číslo 7 je zbytkem po dělení (viz předposlední rovnice na obrázku počítání gcd pomocí eukleidova algoritmu), proto můžeme napsat:

$7=1.28-21$,

kde čísla 28 a 21 jsou opět zbytky po dělení (viz 1. a 2. rovnice na obrázku). Postupným využíváním rovnic z eukleidova algoritmu tak dostaneme:

$$7=1.28-21$$

$$7=1.\left(427-3.133\right)-\left(133-4.28\right)$$

$$7=1.\left(427-3.133\right)-\left(133-4.\left(427-3.133\right)\right)$$

$$7=5.427-16.133$$

Hledané koeficienty jsou tedy $\alpha=5,\beta=-16$.

Je patrné, že s narůstajícím počtem rovnic je tento způsob hledání koeficientů Bezoutovy rovnice velice nepřehledný a těžkopadný. Z tohoto důvodu zformulujeme rozšířený Eukleidův algoritmus, kde hledané koeficienty nalezneme jako „vedlejší produkt" při hledání největšího společného dělitele.

Rozšířený Eukleidův algoritmus

Vstup: $a\geqslant b\geqslant 0, a,b\in\mathbb{N}$

Výstup: $\gcd\left(a,b\right)$**, koeficienty** α,β **Bezoutovy rovnice.**

Jednotlivé kroky algoritmu:

1. **Je-li** $b=0$**, položte** $d=a,\alpha=1,\beta=0$ **a skončete**
2. **Položte** $\alpha_2=1,\alpha_1=0,\beta_2=0,\beta_1=1$
3. **Dokud** $b>0$ **dělejte**
   I. **Spočtěte** q,r **tak, že** $a=q.b+r, 0\leqslant r\leqslant b$
   II. **Položte** $\alpha=\alpha_2-q.\alpha_1,\beta=\beta_2-q.\beta_1$
   III. **Položte** $a=b,b=r$
   IV. **Položte** $\alpha_2=\alpha_1,\alpha_1=\alpha,\beta_2=\beta_1,\beta_1=\beta$
4. **Položte** $d=a,\alpha=\alpha_2,\beta=\beta_2$ **a skončete.**

Když si zmíněný postup zformátujeme do tabulky, je rozšířený eukleidův algoritmus velice příjemný a jednoduchý na zapamatování. Způsobů jak zformátovat je víc, osobně doporučuju ten, co je popsaný v [2 [http://marauder.millersville.edu/~bikenaga/absalg/exteuc/exteucex.html]]

1. Příklad - rozšířený Eukleidův algoritmus

$$\gcd\left(427,133\right)=?$$

Tabulka je vytvořena podle návodu [2].

První dva řádky vyplníme následovně:

1. $a=427, q=X\left(tzn.\,žádná\,hodnota\right), \alpha=1, \beta=0$
2. $a=133, q=3\left(kvocient\,celočíselného\,dělení\,427\,div\,133\right), \alpha=0, \beta=1$

Další řádky vyplňujeme následovně (i značí číslo aktuálního řádku):

- $a_i=a_{i-2}\,mod\,a_{i-1}$
- $\alpha_i=\alpha_{i-2}-q_{i-1}.\alpha_{i-1}$

Po vyplnění tabulky máme $a_k=\gcd\left(427,133\right), \alpha=\alpha_k, \beta=\beta_k, k$ značí poslední řádek. Viz následující tabulka:

a	q	α	β
427	X	1	0
133	3	0	1
28	4	1	-3
21	1	-4	13
7	3	5	-16

A jak vidíme, dospěli jsme ke stejnému výsledku jako výše: $\gcd\left(427,133\right)=7, \alpha=5, \beta=-16$

2. Příklad - rozšířený Eukleidův algoritmus

Pro přirozené číslo $x=17$ nalezněte jeho inverzi modulo $m=29$.

	29	1	0
	17	0	1
1	12	1	-1
1	5	-1	2
2	2	3	-5
2	**1**	**-7**	**12**
2	0	17	-29

Postup

Inverzní číslo k přirozenému číslu x je takové číslo x^{-1}, pro které ptatí $1=x.x^{-1}$, a to vše modulo m. Inverzní číslo x^{-1} čísla x modulo m můžeme spočítat, pokud je číslo x nesoudělné s modulem m. A k tomuto zjištění můžeme právě použít Eukleidův algoritmus, viz. obrázek výše.

1. **Modulo m dělíme číslem x se zbytkem a výsledek zapisujeme stejně jako v případě příkladu *2. Příklad - Eukleidův algoritmus*.**
2. **Postupujeme stejně jako u příkladu *2. Příklad - Eukleidův algoritmus* do té doby, dokud**

zbytek po dělení není nulový.

3. Když se zbytek po dělení rovná 0, tak přerušíme provádění algoritmu a číslo řádek nad číslem 0 vezmeme za největšího společného dělitele modula m a čísla x.

Zjistili jsme, že číslo $x=17$ není soudělné s modulem $m=29$, tj. $\gcd(x,m)=1$. Z toho plyne, že existuje v modulu m inverze čísla x. A k jejímu nalezení nám pomůže rozšířený Eukleidův algoritmus. Zápis rozšířeného Eukleidova algoritmu (na obrázku výše) je ekvivalentní zápisu v příkladu *1. Příklad - rozšířený Eukleidův algoritmus*.

Z rozšířeného Eukleidova algoritmu dostáváme tuto Bezoutovu rovnost: $1=-7.29+17.12$. Tuto rovnici můžeme jednoduše upravit do tvaru $17.12-1=7.29$. Pomocí definice kongruence jsme schopni tuto rovnici přepsat do tvaru $17.12\equiv 1\left(mod\ 29\right)$. Z této kongruence vidíme, že součin $17.12=1$ v modulu $m=29$. Námi hledaná inverze čísla $x=17$ je tedy číslo 12, tj. $x^{-1}=12$.

Relace modulo n

Kongruence modulo n

Definice kongruence

Ať $n>1$ je pevné přirozené číslo. Řekneme, že celá čísla a a b jsou kongruentní modulo n (značíme $a\equiv b\left(mod\ n\right)$), pokud existuje celé číslo k takové, že $a-b=k.n$.

Poznámka

Vztah $a\equiv b$ (mod n) platí právě tehdy, když čísla a a b mají stejný zbytek po dělení číslem n.

Příklad

$13\equiv 1\left(mod\ 12\right)$

Tvrzení

Ať $n>1$ je pevné přirozené číslo. Potom platí

1. Kongruence modulo n je reflexivní relace, tj. pro každé celé číslo a platí: $a\equiv a\left(mod\ n\right)$.
2. Kongruence modulo n je symetrická relace, tj. pro všechna celá čísla a,b platí: jestliže platí $a\equiv b\left(mod\ n\right)$, pak platí $b\equiv a\left(mod\ n\right)$.
3. Kongruence modulo n je transitivní relace, tj. pro všechna celá čísla a,b,c platí: jestliže platí $a\equiv b\left(mod\ n\right)$ a zároveň jestliže platí $b\equiv c\left(mod\ n\right)$, pak platí: jestliže platí $a\equiv c\left(mod\ n\right)$.
4. Kongruence modulo n respektuje operaci sčítání, tj. pro všechna celá čísla a,b,a',b'

platí: jestliže platí $a \equiv b \pmod n$ **a zároveň** $a' \equiv b' \pmod n$, **pak platí:** $a + a' \equiv b + b' \pmod n$.

5. **Kongruence modulo** n **respektuje operaci násobení, tj. pro všechna celá čísla** a, b, a', b' **platí: jestliže platí** $a \equiv b \pmod n$ **a zároveň** $a' \equiv b' \pmod n$, **pak platí:** $a.a' \equiv b.b' \pmod n$.

Důsledkem prvních třech podmínek je, že kongruence modulo n je relací ekvivalence. Zbylé dvě podmínky říkají, že zbytky po dělení n **smíme sčítat a násobit.**

Zbytkové třídy a operace s nimi

Definice zbytkové třídy

Ať $n > 1$ **je pevné přirozené číslo. Pro libovolné celé číslo** c **definujeme** $[c]_n$ **jako množinu všech čísel kongruentních s** c **modulo** n**. Přesněji:**

$$[c]_n = \left\{ a \in \mathbb{Z} \mid c \equiv a \pmod n \right\}.$$

Množinu $[c]_n$ **nazýváme třídou kongruence čísla** c **modulo** n **a libovolný prvek množiny** $[c]_n$ **nazýváme representantem třídy** $[c]_n$**. Označme** $\mathbb{Z}_n = \left\{ [a]_n \mid a \in \mathbb{Z} \right\}$

kde jsme vzali pojem trida kongruence?

Jak kde jsme vzali třídu kongruence? Není to tady snad jasně napsané? Třída kongruence je množina $[c]_n$ **viz 4. řádky výše.**

Příklad

Pro $n = 12$ **je například** $[1]_{12} = \left\{ \cdots, -23, -11, 1, 13, 25, \cdots \right\}$.

Z uvedeného příkladu si můžeme všimnout, že modulo 12 jsou čísla -23 a 13 „stejná“. To lze vyjádřit následovně:

$$[-23]_{12} = \left\{ \cdots, -23, -11, 1, 13, 25, \cdots \right\} = [13]_{12}$$

Obecně pro libovolné $n>1$ platí:

$\left[a\right]_n = \left[b\right]_n$ **právě tehdy, když** $a \equiv b \left(mod\, n\right)$ **Množina** $\mathbb{Z}_n$ **má přesně** n **různých prvků.**

Definice operace sčítání a násobení na množině modulo n

Ať $n>1$ **je pevné přirozené číslo. Třídy kongruence** $\left[0\right]_n, \left[1\right]_n, \cdots, \left[n-1\right]_n$ **nazveme standardními tvary prvků** $\mathbb{Z}_n$

Ať $n>1$ **je pevné přirozené číslo. Na množině** $\mathbb{Z}_n$ **definujeme binární operace** $+_n$ **a** $._n$ **následovně:**

$$\left[a\right]_n +_n \left[b\right]_n = \left[a+b\right]_n \quad \left[a\right]_n ._n \left[b\right]_n = \left[a.b\right]_n$$

Pro operace $+_n$ **a** $._n$ **na množině** $\mathbb{Z}_n$ **platí následující vlastnosti pro pevné přirozené číslo** $n>1$ **:**

- **Operace** $+_n$ **je komutativní, asociativní, má neutrální prvek** $\left[0\right]_n$ **a každý prvek** $\left[a\right]_n$ **v** $\mathbb{Z}_n$ **má inversi** $\left[-a\right]_n$ **vzhledem k** $+_n$**. Pro libovolné prvky** $\left[a\right]_n, \left[b\right]_n, \left[c\right]_n \in \mathbb{Z}_n$ **platí:**

$$\left[a\right]_n +_n \left[b\right]_n = \left[b\right]_n +_n \left[a\right]_n$$

$$\left(\left[a\right]_n +_n \left[b\right]_n\right) +_n \left[c\right]_n = \left[a\right]_n +_n \left(\left[b\right]_n +_n \left[c\right]_n\right)$$

$$\left[a\right]_n +_n \left[0\right]_n = \left[a\right]_n$$

$$\left[a\right]_n +_n \left[-a\right]_n = \left[0\right]_n$$

- **Operace** $._n$ **je komutativní, asociativní a má neutrální prvek** $\left[1\right]_n$**. Pro libovolné**

prvky $[a]_n, [b]_n, [c]_n \in \mathbb{Z}_n$ **platí:**

$$[a]_n \cdot_n [b]_n = [b]_n \cdot_n [a]_n$$

$$\left([a]_n \cdot_n [b]_n\right) \cdot_n [c]_n = [a]_n \cdot_n \left([b]_n \cdot_n [c]_n\right)$$

$$[a]_n \cdot_n [1]_n = [a]_n$$

*** Operace** $+_n, \cdot_n$ **jsou svázány distributivním zákonem. Pro libovolné prvky** $[a]_n, [b]_n, [c]_n \in \mathbb{Z}_n$ **platí:**

$$[a]_n \cdot_n \left([b]_n +_n [c]_n\right) = \left([a]_n \cdot_n [b]_n\right) +_n \left([a]_n \cdot_n [c]_n\right)$$

Binární operace

Binární operace **je matematická operace, která pracuje se dvěma vstupními hodnotami (operandy).**

Definice

Binární operací $\circ$ **na množině** A **nazveme zobrazení** $\circ: A \times A \to B$

Binární operaci $\circ$ **s operandy** $x, y \in A$ **a výsledkem** $z \in B$ **značíme** $z = x \circ y$

Grupoid

Grupoid **je základní algebraická struktura s jednou operací. Je to množina** A**, na které je definována jedna binární operace** $\bullet$**. Množina** A **je vzhledem k operaci** $\bullet$ **uzavřená, tj. výsledkem operace provedené na libovolných prvcích množiny** A **je prvek množiny** A**.**

Definice

Binární operace **na množine X je zobrazení** $\bullet: X \times X \to X$ **. Dvojici (X,**$\bullet$**) budeme říkat grupoid.**

Príklady

Príklad 1

Na prázdné množine $X=\emptyset$ existuje jediná binární operace, totiž prázdné zobrazení $\emptyset:\emptyset\times\emptyset\to\emptyset$. Proto je príklad grupoidu. $<\emptyset,\emptyset>$

Príklad 2

Na množine $X=a,b,c$ definujeme binární operaci • takto: $x\bullet y=x$ pro všechna $x,y\in X$.

Protože X je konecná množina, mužeme operaci • popsat následující tabulkou:

•	a	b	c
a	a	a	a
b	b	b	b
c	c	c	c

Je-li x v i-tém rádku a y v j-tém sloupci tabulky, pak v položce (i,j) je zapsán výsledek $x\bullet y$. Dvojice $<X,\bullet>$ je grupoid.

Príklad 3

Ať x je množina všech zobrazení z $\{0,1\}$ do $\{0,1\}$. Množina X má ctyri prvky: $f1:\ 0\to0,\ 1\to1$

$f2:\ 0\to0,\ 1\to0$ $f3:\ 0\to1,\ 1\to1$ $f4:\ 0\to1,\ 1\to0$

Skládání funkcí $\circ$ je binární operace na množine X, a proto je $(X,\circ)$ grupoid. Príslušná tabulka je:

$\circ$	$f1$	$f2$	$f3$	$f4$
$f1$	$f1$	$f2$	$f3$	$f4$
$f2$	$f2$	$f2$	$f2$	$f2$
$f3$	$f3$	$f3$	$f3$	$f3$
$f4$	$f4$	$f3$	$f2$	$f1$

Príklad 4

Ověřte, zda množina přirozených čísel $\mathbb{N}_0$ spolu s operací sčítání $+$, tedy dvojice $<\mathbb{N}_0,+>$ je grupoid. Aby byla dvojice $<\mathbb{N}_0,+>$ grupoid, musí pro $\forall a,b\in\mathbb{N}_0$, platit že $(a+b)\in\mathbb{N}_0$, tj. operace musí být uzavřená na množině $\mathbb{N}_0$. Z definice přirozených čísel nám vyplývá, že součet dvou přirozených čísel je opět přirozené číslo, proto je dvojice $<\mathbb{N}_0,+>$ grupoid.

Vlastnosti

- **Operace • je asociativní, pokud pro všechna $x,y,z\in X$ platí rovnost $x\bullet(y\bullet z)=(x\bullet y)\bullet z$.**
- **Operace • je komutativní, pokud pro všechna $x,y\in X$ platí rovnost $x\bullet y=y\bullet x$.**
- **Prvek el je levý neutrální prvek operace •, pokud pro všechna $x\in X$ platí rovnost**

$el \bullet x = x$.

- Prvek er je pravý neutrální prvek operace •, pokud pro všechna $x \in X$ platí rovnost $x \bullet er = x$.
- Prvek e je neutrální prvek operace •, pokud je pravým i levým neutrálním prvkem, tj. když pro všechna $x \in X$ platí rovnost $e \bullet x = x \bullet e = x$.

Pologrupa, monoid, grupa

Ať $<X, \bullet>$ je grupoid.

1. $<X, \bullet>$ je *pologrupa*, je-li • asociativní operace.
2. Pologrupě $<X, \bullet>$ říkáme *monoid*, jestliže operace • má neutrální prvek.
3. Monoidu $<X, \bullet>$ s neutrálním prvkem e říkáme *grupa*, jestliže má každý prvek x inversi vzhledem k •, tj. jestliže platí: pro každé x existuje právě jedno x^{-1} takové, že platí $x^{-1} \bullet x = e = x \bullet x^{-1}$.

Každá grupa je monoid, každý monoid je pologrupa a každá pologrupa je grupoid. Po dané strukture totiž požadujeme postupně víc a víc. Žádnou z těchto implikací však nelze obrátit.

Příklad 1

Ověřte, zda množina přirozených čísel $\mathbb{N}_0$ spolu s operací sčítání $+$, tedy dvojice $<\mathbb{N}_0, +>$ je pologrupa.

Jak bylo dokázáno výše dvojice $<\mathbb{N}_0, +>$ je grupoid. Z definice operace sčítání nám vyplývá, že tato operace je na množině $\mathbb{N}_0$ asociativní, tj. platí $\left(a+b\right)+c = a+\left(b+c\right); \forall a, b, c \in \mathbb{N}_0$

Příklad 2

Ověřte, zda množina přirozených čísel $\mathbb{N}_0$ spolu s operací umocňování $mocnina$, tedy dvojice $<\mathbb{N}_0, mocnina>$ je pologrupa.

Aby byla dvojice $<\mathbb{N}_0, mocnina>$ grupoid, musí pro $\forall a, b \in \mathbb{N}_0$, platit že $\left(a^b\right) \in \mathbb{N}_0$, tj. operace musí být uzavřená na množině $\mathbb{N}_0$. To platí z definice $mocnina$ na $\mathbb{N}_0$.

Protože $\left(2^2\right)^3 = 64 \neq 256 = 2^{\left(2^3\right)}$ operace $mocnina$ není na množině $\mathbb{N}_0$ pologrupa.

Příklad 3

Ověřte, zda množina celých čísel $\mathbb{Z}$ spolu s operací sčítání $+$, tedy dvojice $<\mathbb{Z}, +>$ je monoid.

$<\mathbb{Z}, +>$ je grupoid, protože z definice sčítání vyplývá, že tato operace je na množině $\mathbb{Z}$

uzavřená ($\forall a,b \in \mathbb{Z}; a+b \in \mathbb{Z}$).

$<\mathbb{Z},+>$ je pologrupa, protože z definice sčítání vyplývá, že tato operace je na množině $\mathbb{Z}$ asociativní ($\forall a,b,c \in \mathbb{Z}; a+\left(b+c\right)=\left(a+b\right)+c$).

$<\mathbb{Z},+>$ je monoid, protože operace $+$ má na množině $\mathbb{Z}$ neutrální prvek $e=0$ ($x+0=x=0+x$).

Příklad 4

Ověřte, zda množina přirozených čísel $\mathbb{N}$ spolu s operací sčítání $+$, tedy dvojice $<\mathbb{N},+>$ je monoid.

$<\mathbb{N},+>$ je grupoid, protože z definice vyplývá, že operace $+$ je na množině $\mathbb{N}$ uzavřená.

$<\mathbb{N},+>$ je pologrupa, protože z definice vyplývá, že operace $+$ je na množině $\mathbb{N}$ asociativní.

$<\mathbb{N},+>$ není monoid, protože operace $+$ nemá na množině $\mathbb{N}$ neutrální prvek.

Příklad 5

Ověřte, zda množina celých čísel $\mathbb{Z}$ spolu s operací sčítání $+$, tedy dvojice $<\mathbb{Z},+>$ je grupa.

$<\mathbb{Z},+>$ je grupoid, protože z definice vyplývá, že operace $+$ je na množině $\mathbb{Z}$ uzavřená.

$<\mathbb{Z},+>$ je pologrupa, protože z definice vyplývá, že operace $+$ je na množině $\mathbb{Z}$ asociativní.

$<\mathbb{Z},+>$ je monoid, protože operace $+$ má na množině $\mathbb{Z}$ neutrální prvek $e=0$.

Množina $\mathbb{Z}$ a operace $+$ je grupa, protože to je monoid a protože $\forall x \in \mathbb{Z} \exists -x$ pro který platí $x+\left(-x\right)=0=-x+x$

Příklad 6

Ověřte, zda množina přirozených čísel $\mathbb{N}\setminus 0$ spolu s operací násobení $\times$, tedy dvojice $<\mathbb{N}\setminus 0,\times>$ je grupa.

$<\mathbb{N}\setminus 0,\times>$ je grupoid, protože z definice vyplývá, že operace $\times$ je na množině $\mathbb{N}\setminus 0$ uzavřená.

$<\mathbb{N}\setminus 0,\times>$ je pologrupa, protože z definice vyplývá, že operace $\times$ je na množině $\mathbb{N}\setminus 0$ asociativní.

$<\mathbb{N}\setminus 0,\times>$ je monoid, protože operace $\times$ má na množině $\mathbb{N}\setminus 0$ neutrální prvek $e=1$.

Monoid $<\mathbb{N}\setminus 0,\times>$ není grupa, protože zde neexistuje inverzní prvek.

Zdroje

- **[1] Velebil, J.: //Diskrétní matematika, Text k přednášce//, Praha 2007 [ftp://math.feld.cvut.cz/pub/velebil/y01dma/dma-notes.pdf]**

- **[2] Rozšířený Eukleidův algoritmus [http://marauder.millersville.edu/~bikenaga/absalg/exteuc/exteucex.html]**

spolecne/spol8.txt · Poslední úprava: 2010/06/06 16:03 autor: Zajouch