2) $((a,b),c) \overset{?}{=} (a,(b,c))$

pro $a,b \in \mathbb{N}$ značí

(a,b) největšího společného dělitele čísel a,b

$[a,b]$ nejmenší společný násobek

Tato operace nemá neutrální prvek:

Nechť by operace měla neutrální prvek n. Pak obzvlášť $(n,n+1) \leq n$, tedy $(n,n+1) \neq n+1$, spor.

3) monoid

4) nechť A je invertibilní matice.
Pak $-A$ je také invertibilní, ale
$A + (-A) = 0$, což není inv. matice
tedy daná množina není uzavřená
vzhledem ke sčítání matic.

6) $(A - B) - C \neq A - (B - C)$

7) 1

	A	B	C	D	E	F
A	A	B	C	D	E	F
B	B	A	E	F	C	D
C	C					
D	D					
E	E					
F	F					

8) $\mathbb{Z}_6^+ = \mathbb{Z}_6 - \{[0]_6\}$ - není nul. vzhledem k násobení

9) $\mathbb{Z}_7^+ = \mathbb{Z}_7 - \{[0]_7\}$ -

Grupa má 48 prvků.

3) $\sigma^{336} = [(1,9,5)(2,8,4,7,3,6)]^{336} =$

$= \underbrace{(1,9,5)^{336}}_{id} \circ \underbrace{(2,8,4,7,3,6)^{336}}_{id} =$

$= id$

	a	b	c
a	b	a	c
b	a	b	c
c	c	c	c

$* = \cdot$

$a \cdot (c \cdot c) = c \cdot c$

$a \cdot (b \cdot c) = (a \cdot b) \cdot c$

$= a$

$a \cdot (c \cdot b) = c \cdot b \Rightarrow$

$\Rightarrow c \cdot b = c$

asociativita

$b \cdot a = (a \cdot a) \cdot a \overset{\downarrow}{=} a \cdot (a \cdot a) = a \cdot b = a$

$b \cdot b = (a \cdot a) \cdot b \overset{\downarrow}{=} a \cdot (a \cdot b) = a \cdot a = b$

$b \cdot c = (a \cdot a) \cdot c \overset{\downarrow}{=} a \cdot (a \cdot c) = a \cdot c = c$

$c \cdot a = a \cdot c \cdot a = c \cdot a$

$\times \qquad \times$

$ax = x_1$

tzn. $c \cdot a$ je řešením rovnice $ax = x$. Tato rovnice má obecně podle tabulky jediné řešení a tím je prvek c, tzn. $c \cdot a = c$

a, b, c prvky nějaké grupy

$ab = ac$ | vlevo vynásobíme prvkem a^{-1}

$(a^{-1}) \cdot a \cdot b = (a^{-1}) a \cdot c$

$eb = e \cdot c$

$b = c$

$ba = ca \Rightarrow b = c$

	a	b	c
a	a	b	c
b	b	a	c
c	c	b	a

Z tabulky vyplývá, že b a c nemohou být neutrálními prvky. Jsou to neutr. (jednostrojmi)

prvkem musí být prvek a. Doplníme první řádek a první sloupec.

Tabulku lze doplnit tak, aby $*$ byla grupovou operací na množině $\{a, b, c\}$.

Isomorfismus dvou grupoidů $(G, *), (H, \square)$ je bijekce $f: G \to H$ taková, že $f(a * b) = f(a) \square f(b)$ pro libovolná a, b.

	a	b	c
a	.	.	.
b	.	.	.
c	.	.	.

Celkem existuje 3^9 různých tříprvkových grupoidů.

	e	a	b
e	e	a	b
a	a	b	$\boxed{e}$
b	b	$\boxed{e}$	a

BV $\Rightarrow$ pokud $(a, n) = 1$ pak
a má inverzi v $\mathbb{Z}_n$

$$au + v \cdot n = 1$$

$$au = 1 - v \cdot n \Rightarrow$$

$$\Rightarrow au \equiv 1 \pmod{n}$$

Jedno u je inverze k a v $\mathbb{Z}_n$.

(u, v - Bezoutovy koeficienty)

$171 = 13 \cdot 13 + 2 \Rightarrow 2 = 171 - 13 \cdot 13$

$13 = 6 \cdot 2 + \boxed{1} \Rightarrow 1 = 13 - 6 \cdot 2 =$

$2 = 2 \cdot 1$ $= 13 - 6 \cdot (171 - 13 \cdot 13) =$

$= 13 - 6 \cdot 171 + 6 \cdot 13 \cdot 13 = 13 \cdot 79 - 6 \cdot 171$

$13 \cdot (79)$

$u \quad v$

$\Rightarrow$ inverzní číslo 13 v $\mathbb{Z}_{171}$ je 79

Nalezněte inverzi čísla 13 v $\mathbb{Z}_{163}$.

Aplikujeme Euklidův algoritmus:

$163 = 12 \cdot 13 + 7$

$13 = 1 \cdot 7 + 6$

$7 = 1 \cdot 6 + \boxed{1}$ ← poslední nenulový zbytek = největší spol. dělitel

$6 = 6 \cdot 1$

$1 = 7 - 1 \cdot 6 = 7 - (13 - 7) = 2 \cdot 7 - 13 =$

$= 2 \cdot (163 - 12 \cdot 13) - 13 = 2 \cdot 163 - 25 \cdot 13 \Rightarrow$

$\Rightarrow$ inverze k prvku 13 v $\mathbb{Z}_{163}$ je

$[-25]_{163} = [138]_{163}$

(protože $(-25) \cdot 13 = 1 - 2 \cdot 163 \equiv 1 \ (163)$