

Důkazy

- a není del 3, pak $a^2 - 1$ je del 3

prům. d.

$$a = 3k + 1$$

$$a^2 - 1 = (3k + 1)^2 - 1 = 9k^2 + 6k + 1 - 1 = 9k^2 + 6k = 3(3k^2 + 2k)$$

$$a = 3k + 2$$

$$a^2 - 1 = (3k + 2)^2 - 1 = 9k^2 + 12k + 4 - 1 = 9k^2 + 12k + 3 = 3(3k^2 + 4k + 1)$$

$a \Rightarrow b$ přímý d.
 $\neg b \Rightarrow \neg a$ nepřímý d.

- $\sqrt{2}$ není racionální

důkaz sporem

bereme je racionální - lze zapsat jako

$$\sqrt{2} = \frac{a}{b}, \quad a, b \in \mathbb{N}, \quad \text{NSD}(a, b) = 1$$

$$2 = \frac{a^2}{b^2}$$

$$2b^2 = a^2$$

a^2 musí být sudé, pak a je sudé, $a = 2k$
 a je liché, pak a^2 je liché $\rightarrow$ dokazáno

$$(2k + 1)^2 = 4k^2 + 4k + 1$$

$$2b^2 = \cancel{2k^2}$$

$$b^2 = 2k^2 \rightarrow b^2 \text{ je sudé, pak } b \text{ je sudé}$$

a, b sudé, spor s předpokladem proudivnosti

důkaz indukci

$V(n)$, pro všechna $n \geq n_0$

1. $V(n_0)$ platí

2. $V(n)$, pak $V(n+1)$

slabý princip mat. indukce

• $\forall n: \sum_{i=1}^n i = \frac{n(n+1)}{2}; n \in \mathbb{N}$

1. $n=1 \quad 1 = \sum_{i=1}^1 i = \frac{1(1+1)}{2} = 1$

2. předpokládáme, že pro n platí a ~~pak~~ dokazujeme pro $n+1$

$\sum_{i=1}^n i = \frac{n(n+1)}{2}$ pak $\sum_{i=1}^{n+1} i = \frac{(n+1)(n+2)}{2}$

~~nebo~~

$\sum_{i=1}^{n+1} i = \sum_{i=1}^n i + n+1 = \frac{n(n+1)}{2} + n+1 =$

$= \frac{n(n+1) + 2(n+1)}{2} = \frac{n(n+1) + 2(n+1)}{2} = \frac{(n+1)(n+2)}{2}$

• $11^n - 6$ je děl 5 pro $n \geq 1$

$n=1 \quad 11^1 - 6 = 5 : 5 = 1$

1) $5 | (11^n - 6)$, pak $5 | (11^{n+1} - 6)$

$11^n - 6 = 5k$

$11^{n+1} - 6 = 11 \cdot 11^n - 6 =$

$= 11 \cdot (5k + 6) - 6 = 55k + 66 - 6 =$

$= 55k + 60 = 5(11k + 12)$

$\Rightarrow$ ~~neplatí~~

$5 | (11^n - 6)$

nebo $11^{n+1} - 6 = (10+1)11^n - 6 =$

$= 10 \cdot 11^n + 11^n - 6$

$= 5(2 \cdot 11^n + 2)$

silný princip mat. indukce

$V(n)$, pro všechna $n, n \geq n_0$

1. $V(n_0)$ platí

2. $V(k)$, pak $V(m+1)$

$$n_0 \leq k \leq n$$

• $x + \frac{1}{x} \in \mathbb{Z}$, pak pro všechna $n \geq 1$
 $x \in \mathbb{R}$ $x^n + \frac{1}{x^n} \in \mathbb{Z}$

$$a \in \mathbb{Z}$$

$$a = x + \frac{1}{x}$$

$$ax = x^2 + 1$$

$$x^2 - ax + 1 = 0$$

$$D = \sqrt{a^2 - 4}$$

$$x_{1,2} = \frac{a \pm \sqrt{a^2 - 4}}{2}$$

$$x = \pm 1$$

$$x = \frac{3 \pm \sqrt{5}}{2}$$

$$a \neq 0, \pm 1$$

$$n=1 \quad x + \frac{1}{x} \in \mathbb{Z}, \text{ pak } x + \frac{1}{x} \in \mathbb{Z} \quad \checkmark$$

$$n=2 \quad \text{---} \parallel \text{---} \quad x^2 + \frac{1}{x^2} \in \mathbb{Z} \quad \checkmark$$

$$n=3 \quad \text{---} \parallel \text{---} \quad x^3 + \frac{1}{x^3} \in \mathbb{Z} \quad \checkmark$$

$$x + \frac{1}{x} \in \mathbb{Z}$$

$$\left(x + \frac{1}{x}\right)^2 \in \mathbb{Z}$$

$$\underbrace{\left(x + \frac{1}{x}\right)^2}_{\in \mathbb{Z}} = x^2 + 2 + \frac{1}{x^2} = \underbrace{x^2}_{\in \mathbb{Z}} + \underbrace{\frac{1}{x^2}}_{\in \mathbb{Z}} + 2$$

$$(x + \frac{1}{x})^3 = \cancel{x^3 + 3x + \frac{3}{x} + \frac{1}{x^3}} = x^3 + \frac{1}{x^3} + 3(x + \frac{1}{x})$$

$$(a+b)^n = \sum_{i=0}^n \binom{n}{i} a^{n-i} b^i$$

$$(x + \frac{1}{x})^n = \boxed{x^n + \frac{1}{x^n}} + n \overbrace{\left(x^{n-2} + \frac{1}{x^{n-2}}\right)}^{\in \mathbb{Z}} + \underbrace{\binom{n}{2} \left(x^{n-4} + \frac{1}{x^{n-4}}\right)}_{\in \mathbb{Z}} + \dots$$

$$\binom{n}{1} = \binom{n}{n-1}$$

$$x + \frac{1}{x} \in \mathbb{Z}, \text{ pak } x^k + \frac{1}{x^k} \in \mathbb{Z} \text{ pro } 1 \leq k \leq n-1$$

$$x^n + \frac{1}{x^n} \in \mathbb{Z} \quad ?$$

musíme předpokládat, že každé p -tý násobný silný přírůstek mat. ind.

• $x \in \mathbb{N}, x \geq 2$ existuje prvočíselný rozklad

$$x = p_1^{m_1} p_2^{m_2} \dots p_k^{m_k}$$

$$m_i \geq 0$$

$p_i \neq p_j$ prvočísla

1. $2 = 2^1$

2. $y = p_1^{m_1} p_2^{m_2} \dots p_k^{m_k}; 2 \leq y \leq x$

$x+1$ $\begin{cases} \text{je prvočíslo} \\ \text{není prvočíslo} \end{cases}$

$$(x+1)^1$$

$$x+1 = ab$$

$$1 \leq a \leq x+1$$

$$1 \leq b \leq x+1$$

$$a = p_1^{m_1} p_2^{m_2} \dots p_k^{m_k}$$

$$b = q_1^{m_1} q_2^{m_2} \dots q_l^{m_l}$$

odpovídá předpokladu

není hotovo

(2)

$A = \{a, b, c, \dots\}$ log. proměnné

$\neg, \wedge, \vee, \Rightarrow, \Leftrightarrow$

1. $a \in A$ je výroková formule

2. α, β jsou v.f., pak

$(\neg \alpha), (\alpha \vee \beta), (\alpha \wedge \beta), (\alpha \Rightarrow \beta), (\alpha \Leftrightarrow \beta)$ jsou v.f.

3. nic jiného v.f. není

-

$A = \{a, b, c\}$

$(a \Leftrightarrow (b \wedge b))$ není v.f.

$(d) \wedge a$ není

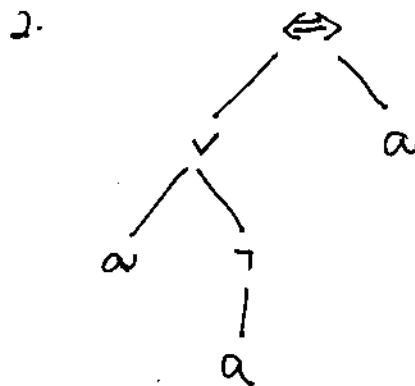
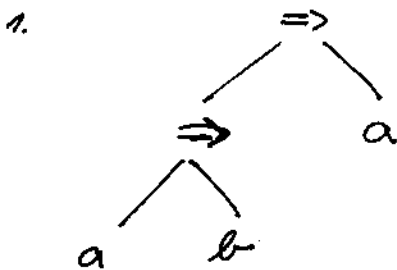
1. $(a \Rightarrow b) \Rightarrow a$ je

2. $((a \vee (\neg a)) \Leftrightarrow a)$ je

můžeme vynechat některé ()

$(a \vee \neg a) \Leftrightarrow a$

↓
Derivační strom



a	b	$a \vee b$	$a \wedge b$	$a \Rightarrow b$	$a \Leftrightarrow b$
0	0	0	0	1	1
0	1	1	0	1	0
1	0	1	0	0	0
1	1	1	1	1	1

a	$\neg a$
0	1
1	0

$$(a \Rightarrow b) \Rightarrow a$$

a	b	$a \Rightarrow b$	$(a \Rightarrow b) \Rightarrow a$
0	0	1	0
0	1	1	0
1	0	0	1
1	1	1	1

$$(a \vee \neg a) \Leftrightarrow a$$

a	$\neg a$	$a \vee \neg a$	$(a \vee \neg a) \Leftrightarrow a$
0	1	1	0
1	0	1	1

$\mathcal{P}(A)$

$$\mu: \mathcal{P}(A) \rightarrow \{0, 1\}$$

ohodnocení

$$\mu_0: A \rightarrow \{0, 1\}$$

φ je pravdivá v μ

$$\mu(\varphi) = 1$$

tautologie
kontradikce
splnitelná

$$\mu(\varphi) = 1 \text{ pro všechna } \mu$$

$$\mu(\varphi) = 0$$

alespoň 1 ohodnocení je pravdivé

taut., kontr., nebo splnitelné?

$$(a \Rightarrow b) \Leftrightarrow (a \vee b)$$

a	b	$a \Rightarrow b$	$a \vee b$	$() \Leftrightarrow ()$
0	0	1	0	0
0	1	1	1	1
1	0	0	1	0
1	1	1	1	1

splnitelná

$$(a \Rightarrow b) \Leftrightarrow (\neg a \vee b)$$

$$a \Rightarrow b \models \neg a \vee b$$

a	b	$a \Rightarrow b$	$\neg a$	$\neg a \vee b$	$() \Leftrightarrow ()$
0	0	1	1	1	1
0	1	1	1	1	1
1	0	0	0	0	1
1	1	1	0	1	1

tautologie

$$\neg(a \vee b) \Leftrightarrow (\neg a \wedge \neg b)$$

a	b	$\neg(a \vee b)$	$(\neg a \wedge \neg b)$	$\Leftrightarrow$
0	0	1	1	1
0	1	0	0	1
1	0	0	0	1
1	1	0	0	1

tautologie

tautologicky ekvivalentní

$$\varphi \models \psi$$

$$\mu(\varphi) = \mu(\psi) \text{ pro všechna } \mu$$

$\varphi \Leftrightarrow \psi$ je tautologie

$$\begin{aligned} a \leftrightarrow b &\equiv \neg a \vee b \\ \neg(a \vee b) &\equiv \neg a \wedge \neg b \\ \neg(a \wedge b) &\equiv \neg a \vee \neg b \end{aligned} \quad \text{De Morgan}$$

$$\begin{aligned} (a \vee b) \vee c &\equiv a \vee (b \vee c) \\ (a \wedge b) \wedge c &\equiv a \wedge (b \wedge c) \\ (a \vee b) \wedge c &\equiv (a \wedge c) \vee (b \wedge c) \\ (a \wedge b) \vee c &\equiv (a \vee c) \wedge (b \vee c) \end{aligned}$$

sjednotění

$$(a \Rightarrow b) \Rightarrow b$$

$$\begin{aligned} (\neg a \vee b) \Rightarrow b &\equiv \{ \neg(\neg a \vee b) \vee b \} \equiv (a \wedge \neg b) \vee b \equiv \\ &\equiv (a \vee b) \wedge (\neg b \vee b) \equiv a \vee b \end{aligned}$$

další spojky

$$\begin{aligned} \text{xor} \quad a \oplus b &\equiv \neg(a \leftrightarrow b) \\ \text{nand} \quad a \downarrow b &\equiv \neg(a \wedge b) \\ \text{nor} \quad a \uparrow b &\equiv \neg(a \vee b) \end{aligned}$$

$$\text{CNF} \quad (a \vee \neg b) \wedge (\neg a \vee c)$$

$$\text{DNF} \quad (a \wedge \neg b) \vee (\neg a \wedge c)$$

obsahují jen $\neg, \wedge, \vee$

úplná forma - obsahuje zároveň všechny proměnné

$$a \Rightarrow (b \wedge c)$$

	a	b	c	$\neg c$	$b \wedge \neg c$	$a \Rightarrow ()$
0	0	0	0	1	0	1
1	0	0	1	0	0	1
2	0	1	0	1	1	1
	0	1	1	0	0	1
	1	0	0	1	0	0
	1	0	1	0	0	0
	1	1	0	1	1	1
	1	1	1	0	0	0

úplně

DNF

$$(a \wedge b \wedge c) \vee (a \wedge b \wedge d) \vee (a \wedge b \wedge e) \vee (a \wedge b \wedge c \wedge d \wedge e)$$

CNF

$$(a \vee b \vee c) \wedge (a \vee b \vee c) \wedge (a \vee b \vee c)$$

$$(7a) \vee (b \wedge 7c) \quad DNF$$

$$(\neg a \vee b) \wedge (\neg a \vee \neg c) \quad \text{CNF}$$

	0	1	2	3
4	5	6	7	8

$$a \Rightarrow (b \vee \neg c)$$

a	b	c	$\neg c$	$b \vee \neg c$	$\Rightarrow$
0	0	0	1	1	1
0	0	1	0	0	1
0	1	0	1	1	1
0	1	1	0	1	1
1	0	0	1	1	1
1	0	1	0	0	0
1	1	0	1	1	1
1	1	1	0	1	1

$$DNF \quad (\neg a \wedge \neg b \wedge \neg c) \vee (\neg a \wedge \neg b \wedge c) \dots$$

$$CNF \quad (\neg a \vee b \vee \neg c)$$

a	b	c
0	0	0
0	0	1
0	1	0
0	1	1
1	0	0
1	0	1
1	1	0
1	1	1

DNF

CNF

$$b \vee \neg a \vee \neg c$$

$$b \vee \neg a \vee \neg c$$

$$\neg a \vee b \vee \neg c$$

opily stejné :)

zjednodušíš

$$(a \wedge b) \oplus (b \vee c)$$

	c	b	a	$a \wedge b$	$b \vee c$	$() \oplus ()$
0	0	0	0	0	0	0
1	0	0	1	0	0	0
2	0	1	0	0	1	1
3	0	1	1	1	1	0
4	1	0	0	0	1	1
5	1	0	1	0	1	1
6	1	1	0	0	1	1
7	1	1	1	1	1	0

a	b	c
0	0	0
0	0	1
0	1	0
0	1	1
1	0	0
1	0	1
1	1	0
1	1	1

$$(c \wedge \neg b) \vee (\neg a \wedge b) \quad DNF$$

$$(c \vee b) \wedge (\neg a \vee \neg b) \quad CNF$$

S je pravdivá v ohodnocení u

$$u(\psi) = 1 \text{ pro vš } \psi \in S$$

je splnitelná?

$$S_1 = \{a \Rightarrow b, a \Rightarrow \neg b, a \wedge b\} \quad X$$

$$S_2 = \{(a \vee b) \Rightarrow c, (a \wedge \neg b) \Rightarrow c, a \Rightarrow c\} \quad \checkmark$$

$$S_1:$$

a	b	$a \Rightarrow b$	$a \Rightarrow \neg b$	$a \wedge b$
0	0	1	1	0
0	1	1	0	0
1	0	0	1	0
1	1	1	0	1

není splnitelná

$$S_2:$$

a	b	c	$(a \vee b)$	$(a \vee b) \Rightarrow c$	$a \wedge \neg b$	$(a \wedge \neg b) \Rightarrow c$	$a \Rightarrow c$
0	0	0	0	1	0	1	1
0	0	1	0	1	0	1	1
0	1	0	1	0	0	1	1
0	1	1	1	1	0	1	1
1	0	0	1	0	1	0	0
1	0	1	1	1	1	1	1
1	1	0	1	0	0	1	0
1	1	1	1	1	0	1	1

splnitelná

$$S_1: u(a \wedge b) = 1$$

$$u(a) = u(b) = 1$$

$$u(a \Rightarrow \neg b) = 0$$

$$S_2: u(c) = 1$$

$S \models \varphi$ pro vs. u : ~~nikdy~~ $u(\varphi)=1, \varphi \in S$, ~~ne~~ $u(\varphi)=1$
 $S \models \varphi$ ex. u $u(\varphi)=0$

1) $\{a \Rightarrow b, \neg b\} \models \neg a$ platí

2) $\{a \vee b; a \Rightarrow c; b \Rightarrow c\} \models c$ platí

3) $\{(a \wedge b) \Rightarrow c, b\} \models c$ neplatí (tedy $\nmodels$)

1)

a	b	$a \Rightarrow b$	$\neg b$	$\neg a$
0	0	1	1	1
0	1	1	0	1
1	0	0	1	0
1	1	1	0	0

ostatní nás
nerajimají

2)

a	b	c	$a \vee b$	$a \Rightarrow c$	$b \Rightarrow c$
0	0	0	0	1	1
0	0	1	0	1	1
0	1	0	1	1	0
0	1	1	1	1	1
1	0	0	1	0	1
1	0	1	1	1	1
1	1	0	1	0	0
1	1	1	1	1	1

předpoklad

$\{1, 1, 1\} \models 0$

jinak

$u(c) = 0$

$u(a \Rightarrow c) = 1$ $u(a) = 0$

$u(b \Rightarrow c) = 1$ $u(b) = 0$

$u(a \vee b) = 0$

~~platí~~ nelze splnit

platí $\models$

3)

a	b	c	$(a \wedge b) \Rightarrow c$
0	0	0	0
0	0	1	0
0	1	0	0
0	1	1	0
1	0	0	0
1	0	1	0
1	1	0	1
1	1	1	1

$\varphi \in S \quad S \models \varphi$ plati

$S \models \varphi$, pro v̄s. S , pak φ je tautologie

$\models \varphi$ - φ je tautologie,
(kons. prārdnē mērošing)

$S \models \varphi$ pro v̄s. φ , pak S je nepelnitelna, npr. $\{a, \neg a\}$

$S \models \varphi$ prātē tehdy, kdyz $S \cup \{\neg \varphi\}$ je nepelnitelna.

~~$S \models \varphi$ prātē tehdy, kdyz $S \cup \{\neg \varphi\}$ je nepelnitelna.~~

$S \models \varphi \quad \left\{ \begin{array}{l} \text{ex } \varphi \in S, \mu(\varphi) = 0 \\ \mu(\varphi) = 1, \varphi \in S, \text{ pak } \mu(\varphi) = 1, \mu(\neg \varphi) = 0 \end{array} \right.$

$\mu(\varphi) = 1, \varphi \in S, \text{ pak } \mu(\varphi) = 1, \mu(\neg \varphi) = 0$

$S \models \varphi$ plati

? ex. $S_1, S_2 \subseteq S : S_1 \cap S_2 = \emptyset, S_1 \cup S_2 = S$

a) $S_1 \models \varphi$ nebo $S_2 \models \varphi$

b) $S_1 \models \varphi$ a $S_2 \models \varphi$

a) $S_1 = S, S_2 = \emptyset, S \models \varphi$

b) $S = \{a, b\}, \varphi = a$

1) $S_1 = \{a, b\}, S_2 = \emptyset, S_2 \not\models \varphi$

2) $S_1 = \{a\}, S_2 = \{b\}, S_2 \not\models \varphi$

Klausule - disjunktne literāli, napr. $a \vee \neg b \vee c$

ppareiz na množinā klausulī

$$S = \{a \Rightarrow b, (a \vee b) \Rightarrow c\}$$

a	b	c	$a \Rightarrow b$	$(a \vee b) \Rightarrow c$
0	0	0	1	0
0	0	1	1	1
0	1	0	1	0
0	1	1	1	1
1	0	0	0	0
1	0	1	0	1
1	1	0	1	0
1	1	1	1	1

finālā

$$a \Rightarrow b \equiv \neg a \vee b$$

$$(a \vee b) \Rightarrow c \equiv \neg(a \vee b) \vee c \equiv$$

$$(\neg a \wedge \neg b) \vee c \equiv$$

$$(\neg a \vee c) \vee (\neg b \vee c)$$

$$S_2 = \{\neg a \vee b, \neg a \vee c, \neg b \vee c\}$$

CNF ~~$\{a \vee b, \neg a \vee b \vee c\}$~~ $\equiv \{\neg a \vee b \vee c, \neg a \vee b \vee \neg c,$

$$a \vee \neg b \vee c, \neg a \vee \neg b \vee c\} = S_1$$

klausulnā formā

$$S = \{a \vee b, \neg c \vee d, \neg a \vee d, \neg b \vee c, \neg d\}$$

	$a \vee b$	$\neg c \vee d$	$\neg a \vee d$	$\neg b \vee c$	$\neg d$			
a	1		0			b	d	
b				0		1	c	d
c		0					1	
d					0			1
		$\uparrow_1$	$\uparrow_1$	$\uparrow_2$		$\uparrow_1$	$\uparrow_1$	$\uparrow_1$

neizpildnā F - mēķ. spēlētājam
a) jāizvēlas atbilstošā (trīspārē),
b) jāizvēlas atbilstošā (trīspārē),
c) jāizvēlas atbilstošā (trīspārē),
d) jāizvēlas atbilstošā (trīspārē)

beidzotā

$$u(d) = 1$$

$u(c)$ - libovolnā

$$u(b) = 0$$

$$u(a) = 1$$

prārdnā klausule,

S ir neizpildnā

Rozkladní metoda

je splnitelná?

(4)

$$S = \{ p \vee q \vee x, p \vee s \vee t, r \vee y, \neg t, \neg p \vee \neg x, \neg q \vee w, \neg q \vee \neg w \}$$

	$p \vee q \vee x$	$p \vee s \vee t$	$r \vee y$	$\neg t$	$\neg p \vee \neg x$	$\neg q \vee w$	$\neg q \vee \neg w$		
p	1	0			0			$q \vee x \vee s \vee t$	$q \vee x \vee \neg x$
x								1	1
q			1						
s				0					
y						0	0		
t									
w									
	$\uparrow_4$		$\uparrow_3$	$\uparrow_2$		$\uparrow_1$	$\uparrow_5$	$\uparrow_6$	

do ~~jednoho~~ obsazeného sloupce se už další nedává

$$\mu(q) = 0$$

$$\mu(t) = 0$$

$$\mu(y) = 1$$

$$\mu(x) = 1$$

$$\mu(p) = 0$$

$$\mu(s) > \text{lib}$$

$$\mu(w) >$$

je splnitelná

$$S = \{ a \Rightarrow (b \wedge f), (a \wedge b) \Rightarrow c, c \Rightarrow (f \wedge (d \vee f)), a \}$$

$$a \Rightarrow b \equiv \neg a \vee b$$

$$a \Rightarrow (b \wedge f) \equiv \neg a \vee (b \wedge f) \equiv (\neg a \vee b) \wedge (\neg a \vee f)$$

$$(a \wedge b) \Rightarrow c \equiv \neg(a \wedge b) \vee c \equiv \neg a \vee \neg b \vee c$$

$$c \Rightarrow (f \wedge (d \vee f)) \equiv \neg c \vee (f \wedge (d \vee f)) \equiv \neg c \vee ((f \wedge d) \vee f) \equiv \neg c \vee f$$

a

	$\neg a \vee b$	$\neg a \vee f$	$\neg a \vee \neg b \vee c$	$\neg c \vee f$	a
f		1		1	
c			1		
b	1				1
a					

splnitelná

$$\mu(a) = 1$$

$$\mu(b) = 1$$

$$\mu(c) = 1$$

$$\mu(f) = 1$$

$$\mu(d) - \text{lib.}$$

$$(S) \models \{x \Rightarrow y, y \Rightarrow (\neg x \vee \neg x), \neg t \Rightarrow (x \vee \neg x), \neg x \Rightarrow x\} \models \neg$$

$S \models \varphi$ právě tehdy, když $S \cup \{\neg \varphi\}$ je nesplnitelná

$$x \Rightarrow y \equiv \neg x \vee y$$

$$y \Rightarrow (\neg x \vee \neg x) \equiv \neg y \vee \neg x \vee \neg x$$

$$\neg t \Rightarrow (x \vee \neg x) \equiv \neg t \vee x \vee \neg x$$

$$\neg x \Rightarrow x \equiv \neg \neg x \vee x$$

$\neg x$

	$\neg x \vee y$	$\neg y \vee \neg x \vee \neg x$	$\neg t \vee x \vee \neg x$	$\neg \neg x$	$x \vee \neg x$	$\neg x \vee \neg x$	$\neg x \vee \neg x$
t			1	0			
y	1	0					
x					1	0	
$\neg x$				0			

CELOU
sautologii
nemusíme přidat

množina je splnitelná $\rightarrow$ konsekvence neplatí

jazyk pred. logiky

- log. symboly - proměnné
 $\neg, \vee, \wedge, \Rightarrow, \Leftrightarrow$
 $\forall, \exists$

- spec. symboly

P	pred	$\neq \emptyset$
F	fce	
K	kons	

$\rightarrow$ arita - kolika fce, vl. kolika vst

- $(,), ,$

- term 1. prom, kons

2. f - fce arity n , $t_1, \dots, t_n$ - termy
 $f(t_1, \dots, t_n)$ je term

3. nic jiného

atom. formule

P - pred arity n / $t_1, \dots, t_n$ - termy

$P(t_1, \dots, t_n)$ - atom. form.

formule

1. atom. formule

2. φ, ψ - form. $(\neg \varphi), (\varphi \vee \psi), (\varphi \wedge \psi), (\varphi \Rightarrow \psi), (\varphi \Leftrightarrow \psi)$ jsou formule

3. φ - form, x - prom $(\forall x \varphi), (\exists x \varphi)$ jsou formule

4. nic jiného

jeau formule?

P, Q - pred, f, g - fce, a, b - konst
 ita 1 2 2 1

1. $\forall x (Q(f(x, a), b) \Rightarrow P(f(a, b)))$ je form.
2. $(\forall x P(f(x, b))) \Rightarrow (\exists y Q(\underline{f(y)}, \underline{P(y)}))$ není
3. $\forall x (P(x) \Rightarrow (\exists y Q(x, y)))$ je

• Číslo 2 je sudé.

$\mathbb{N}$, konst $a=2$

pred arita 1

S - být sudým číslem

$\rightarrow \underline{S(a)}$

• Následující číslo 2 je číslo liché.

$\mathbb{N}$, konst $a=2$

pred arita 1

L - být lichým číslem

fce arity 1

$f(x) = x+1$

$\underline{L(f(a))}$

• Je-li přiroz č. sudé, jeho následník je liché č.

$\forall x (S(x) \Rightarrow L(f(x)))$

Predikátová logika

5

- Je-li přiroz. č. větší než 0, je jeho následník větší než 1.

$$N, \text{ konst } a=0 \\ b=1$$

$$\text{fce arit. 1 } f(x) = x+1$$

pred arit. 2

$$P(x, y) \dots x > y$$

$$\forall x [P(x, a) \Rightarrow P(f(x), b)]$$

- Čverec lichého čísla je vždy liché číslo.
 N

$$\text{pred. } P \dots \text{ je liché č.}$$

$$\text{fce. } f(x) = x^2$$

$$\forall x (P(x) \Rightarrow P(f(x)))$$

- Existují č. a, b, c taková, že součet čverců a, b je roven čverci c .

$$\text{fce. } f(x) = x^2$$

$$g(x, y) = x + y$$

$$\text{pred } P(x, y) \dots x = y$$

$$\exists a \exists b \exists c (P(g(f(a), f(b)), f(c)))$$

- Součin každých dvou lichých prvočísel je liché číslo.
pred P liché prvočíslo
 L ... liché číslo

for $f(x, y) = x \cdot y$

$$\forall x \forall y [(P(x) \wedge P(y)) \Rightarrow L(f(x, y))]$$

- Každé složené přiroz. č. je dělitelné přiroz. č. větším než 1

D: $\mathbb{N}$

pred. S ... složené číslo

~~prvočíslo~~

D ... číslo dělitelné číslem větším než 1

$$\forall x (S(x) \Rightarrow D(x))$$

_____ nebo

$\mathbb{N}$

$P(x)$... x je složené

$Q(x, y)$... x je dělitelné y

$R(x)$... $x > 1$

$$\forall x \exists y [(P(x) \wedge R(y)) \Rightarrow Q(x, y)]$$

1. $(\forall x P(x)) \wedge (\exists x \neg P(x))$ kontradikce

2. $\forall x ((\exists y Q(x, y)) \vee (\forall z \neg Q(x, z)))$ tautologie

3. $(\exists x P(x)) \Rightarrow (\forall x P(x))$ splnitelná

pravdivá interpretace

$D = \mathbb{N}$

$P(x) : x = 0$ nebo $P(x) : x \in \mathbb{N}$

nepravdivá interpretace

$D = \mathbb{N}$

$P(x) : x$ je sudé

množina sentencí splnitelná - existuje interpretace,
ve které každá sentence α množiny je pravdivá

1) $S_1 = \{ \forall x \exists y Q(x, y), \forall x \neg Q(x, x) \}$ splnitelná

2) $S_2 = \{ \forall x (P(x) \vee R(x)), \neg \exists x R(x), \neg P(a) \}$
nesplnitelná

pred Q
P
R
konst A

1) $D = \mathbb{N}$

pred $Q(x, y) : x \neq y$

2) žádný nemá R, proto musí všechny mít P,
ale a ji nemá

model - interpretace, ve které je sentence pravdivá

$$S \models \varphi$$

$$\varphi \models \varphi \quad \varphi \Leftrightarrow \varphi \text{ ist tautologie}$$

$$\neg(\forall x P(x)) \models \exists x \neg P(x)$$

$$\neg(\exists x P(x)) \models \forall x \neg P(x)$$

$$\bullet \quad \exists x \forall y (P(x, y) \Leftrightarrow \neg P(y, y)) \quad \text{kontradikt} \\ (\text{für } x=y \quad P(x, x) \Leftrightarrow \neg P(x, x))$$

$$\bullet \quad (\forall x \exists y (Q(x, y))) \Leftrightarrow (\exists y \forall x Q(x, y))$$

$$\mathbb{D} = \mathbb{N}; \quad Q(x, y) \dots x \neq y \dots \text{wahr}$$

$$Q(x, y) \quad x + y < 0 \dots \text{falsch}$$

$$\bullet \quad (\forall x P(x)) \wedge (\forall x Q(x)) \models \forall x (P(x) \wedge Q(x))$$

(6)

$$A, B \subseteq U$$

$$A \cup B = \{x; x \in A \text{ oder } x \in B\}$$

$$A \cap B = \{x; x \in A \text{ und } x \in B\}$$

$$A \setminus B = \{x; x \in A \text{ und } x \notin B\}$$

$$\bar{A} = U \setminus A$$

$$A \times B = \{(a, b); a \in A, b \in B\}$$

Lib. A, B, C

$B \subseteq C$, pak $A \times B \subseteq A \times C$ - platí

$A \times B \subseteq A \times C$, pak $B \subseteq C$ - neplatí

↓

$$A = \emptyset$$

$$B = \{1\}$$

$$C = \{2\}$$

$$A \times B = \emptyset \times \{1\} = \emptyset$$

binární relace

$$R = A \times B$$

$$(a, b) \in R, a R b$$

~~Ukázka~~

A je množina všech podm. $\{1, 2\}$

R - bytí vlastní podmnož

$$B \subseteq C, B \not\subseteq C$$

$$A = \{\emptyset, \{1\}, \{2\}, \{1, 2\}\}$$

$$R \subseteq A \times A; R = \{(\emptyset, \{1\}), (\emptyset, \{2\}), (\emptyset, \{1, 2\}), (\{1\}, \{1, 2\}), (\{2\}, \{1, 2\})\}$$

$$R, S \subseteq A \times B$$

podrelace $R \subseteq S$

$$R \cup S, R \cap S$$

$$\text{inverzní } R^{-1} \subseteq B \times A$$

$$x R^{-1} y \text{ právě tehdy, když } y R x$$

složená relace

$$R \circ S \quad R \subseteq A \times B$$

$$S \subseteq B \times C$$

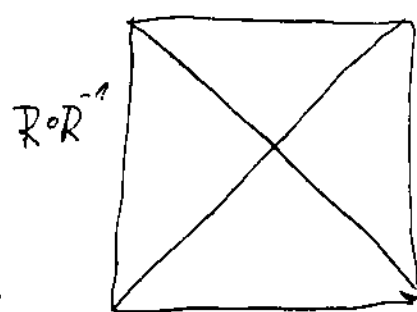
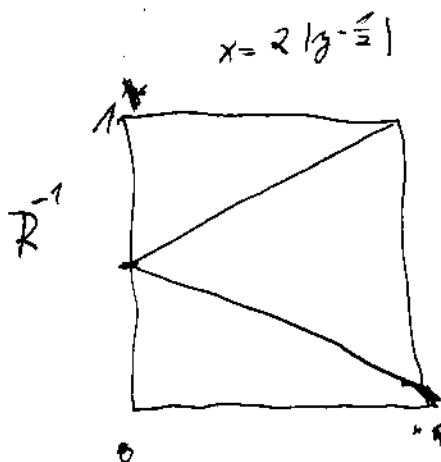
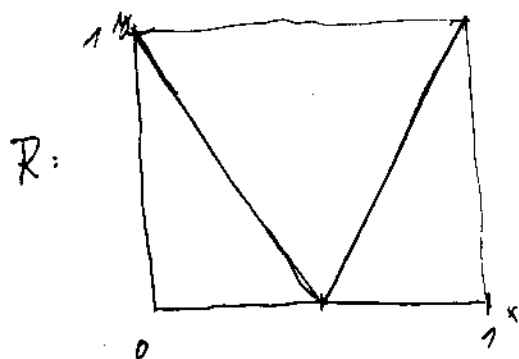
$$R \circ S \subseteq A \times C$$

$$a R \circ S c \text{ právě tehdy, když } \exists b \in B : a R b, b S c$$

$$A = \langle 0, 1 \rangle$$

$$x R y \text{ právě tehdy, když } y = 2|x - \frac{1}{2}|$$

zkoušet do roviny $R, R^{-1}, R \circ R^{-1}$



$$\begin{aligned} x R \circ R^{-1} y \\ x R a \wedge a R^{-1} y \\ a R \wedge \end{aligned}$$

$$\begin{aligned} x - \frac{1}{2} &= y - \frac{1}{2} \\ y - \frac{1}{2} &= -y + \frac{1}{2} \\ y &= \frac{1}{2} \end{aligned}$$

$$R \subseteq A \times B$$

$$S \subseteq B \times C$$

$$(R \circ S)^{-1} = S^{-1} \circ R^{-1}$$

$$R \circ S \subseteq A \times C$$

$$S^{-1} \subseteq C \times B$$

$$(R \circ S)^{-1} \subseteq C \times A$$

$$R^{-1} \subseteq B \times A$$

$$S^{-1} \circ R^{-1} \subseteq C \times A$$

$$c \bullet (R \circ S)^{-1} \bullet a$$

$$a(R \circ S) \bullet c$$

$$\text{ex } b \in B : a R b, b S c$$

$$c S^{-1} b, b R^{-1} a$$

$$c S^{-1} \circ R^{-1} a$$

$$R \subseteq A \times A$$

reflexivni - pro vs. $a \in A$, $a R a$

symetrični - pro vs. $a, b \in A$, ~~je-li~~ $a R b$, pak $b R a$

antisimetrični - pro vs. $a, b \in A$, ~~je-li~~ $a R b$ a $b R a$, pak $a = b$

transitivni - pro vs. $a, b, c \in A$, ~~je-li~~ $a R b$ a $b R c$, pak $a R c$

ekvivalenčni relacije

$$\text{Pr. } * A = \{1, 2, 3, 4, 5, 6\}$$

$$R = \{(1, 2), (3, 4), (5, 6)\}$$

$$S = \{(1, 1), (2, 2), (3, 3), (4, 4), (5, 5), (6, 6)\}$$

	R	S	$\emptyset$	$A \times A$
refl.	x	✓	x	✓
sym.	x	✓	✓	✓
antisym.	✓	✓	✓	x
trans.	✓	✓	✓	✓

$$R_{\text{sym}} = R \cup \{(2,1), (4,3), (6,5)\}$$

je-li relace tranzitivní a symetrická, pak je reflexivní?

je-li aRb , pak

(sym) bRa

(trans?) aRa

není refl.

$$\{(1,2), (2,1), (1,1), (2,2)\}$$

R je refl. a tranzitivní

$$R \circ R = R \quad ?$$

1) pokud $aR \circ Rb$, pak aRb ?

2) pokud aRb , pak $aR \circ Rb$?

1. $aR \circ Rb$ - ex. c : aRc a cRb $\xrightarrow{\text{trans}} aRb$

2. aRb refl bRb , pak $aR \circ Rb$

ekvivalence - refl., sym., tranz.

usporádání - refl., antisym., tranz.

$\hookrightarrow$ $\overline{P} \times$

$R, S, \emptyset, A \times A$
nie ekv. nie ekv.
usp. usp.

$R, S \subseteq A \times A$ ekv.

$R \circ S$ je ekv. ? NE

$a R b$, pak $b R a$

ex $c \in A: a R c, c S b$

(sym) $c R a, b S c \dots b S \circ R a$

$A = \mathbb{Z}$

$m R n \dots m - n$ je del. 3

$m R m \dots m - m = 0$ je del. 3 - reflexivní

$m R n$ pak $m - n$ je del. 3

$m - n = -(n - m)$ $m R n$ - symetrická

$4 R 1, 1 R 4$, ale $1 \not R 4$ není antisym.

$m R n, n R k$

$$m - n = 3a$$

$$n - k = 3b$$

$$(m - n) + (n - k) = m - k = 3(a + b)$$

$m R k$

- transitivní

$$R \subseteq A \times A \quad \text{obr.}, \quad a \in A$$

$R[a]$ tridy ekvivalence proku a

$$R[a] = \{b \in A : aRb\}$$

1. $a \in R[a]$

2. $\bigcup_{a \in A} R[a] = A$

3. $R[a] \cap R[b] \neq \emptyset$, pak $R[a] = R[b]$
(aRc, bRc)

$$A = \mathbb{Z}$$

mRn $m-n$ je del 3

$$R[0] = \{x \in \mathbb{Z} : xR0\}$$

$$\{x \in \mathbb{Z} : x-0 \text{ je del } 3\}$$

$$\{3k : k \in \mathbb{Z}\}$$

$$R[1] = \{3k+1 : k \in \mathbb{Z}\}$$

$$R[2] = \{3k+2 : k \in \mathbb{Z}\}$$

$$A = \mathbb{C}, \quad i^2 = -1$$

$$xRy \iff |x| = |y|$$

je to ekvivalence? $R[3+4i] = ?$

reflexivita: pro vs ~~pro vs~~ $|x| = |x|$ je

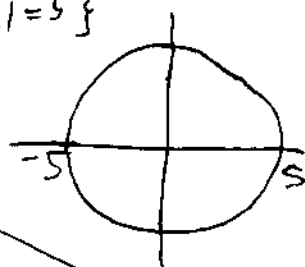
symetr. pro vs ~~pro vs~~ xRy pak yRx je

trans. pro vs. x, y, z pak xRy a yRz , pak xRz je

$$R[3+4i] = \{c \in \mathbb{C} : cR(3+4i)\}$$

$$\{c \in \mathbb{C} : |c| = |3+4i|\}$$

$$\{c \in \mathbb{C} : |c| = 5\}$$



rozklad mn. A

$$M = \{X : \emptyset \neq X \subseteq A\}$$

$$\bigcup_{X \in M} X = A$$

$$X \cap Y \neq \emptyset, \text{ pak } X = Y$$

$a R b$ právě tehdy, když $\exists X \in M : a \in X, b \in X$
 $\Rightarrow$

$$A = \{1, 2, 3, 4\}$$

1) Kolik je relací?

2) Kolik je ekvivalencí?

$$1) R \subseteq A \times A$$

Potenciální množ.

$$\mathcal{P}(A) = \{B : B \subseteq A\}$$

$$|A| = m \quad |\mathcal{P}(A)| = 2^m$$

$$\mathcal{P}(\emptyset) = \{\emptyset\}$$

$$\mathcal{P}(\{1\}) = \{\emptyset, \{1\}\}$$

$$A = \{1, \dots, n\} \quad |\mathcal{P}(A)| = 2^n$$

$$B = \{1, \dots, n, n+1\}$$

pro lib. $S \subseteq A$, pak $S, S \cup \{n+1\} \in \mathcal{P}(B)$

$$|\mathcal{P}(S)| = 2 \cdot 2^n = 2^{n+1}$$

$$|A| = 4$$

$$|A \times A| = 16 \quad |\mathcal{P}(A \times A)| = 2^{16}$$

2)

$$R_1 = \{(1,1), (2,2), (3,3), (4,4)\}$$

$$R_2 = A \times A$$

$$R_3 = R_1 \cup \{(1,2), (2,1)\}$$

$$R_1[1] = \{1\} \dots \textcircled{1} \{1\} \cup \{2\} \cup \{3\} \cup \{4\}$$

$$R_2[1] = \{1,2,3,4\} = A \dots \textcircled{1} \{1,2,3,4\}$$

$$\textcircled{6} \{1,2\} \cup \{3\} \cup \{4\}$$

$$\textcircled{4} \{1,2,3\} \cup \{4\}$$

12 ekvivalenci

Uspořádaní $R \subseteq A \times A$

$a \in A$ je největší (supremum)
pro vs. $b \in A$ je bRa

$a \in A$ je maximální
neex. $b \in A, a \neq b : aRb$

$$A = \{1, 2, 3, 4, 5, 6, 7, p\}$$

$$xRy \dots x \text{ dělí } y \quad (x|y)$$

je uspořádaní? nejprvek? max prvek?

reflexivní: pro vs. $a \in A, aRa$ $\neq x|x$

antisym: pro vs. $a, b \in A, aRb \wedge bRa$, pak $a=b$

trans: $(a, b, c \in A, \text{if } aRb \wedge bRc, \text{ pak } aRc)$

$$xRx \quad xRy$$

$$x = xm \quad y = xm \quad y = x(mm)$$

největší - neex.

$$\begin{aligned} x|y \quad y|x \quad x=y \\ y=xm \quad x=ym \\ y=(mm)y \end{aligned}$$

$a \in A$ je největší

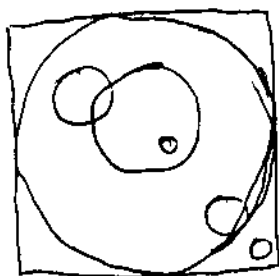
$\forall b \in A, b/a$: není

$a \in A$ je max

$\exists b \in A, b \neq a : a/b$

max: 5, 6, 7, 8

množ všech kruhů ve čtverci



$\subseteq$

nejo. neex.

max

dostávají se k hraně

$$A = \langle 0, 1 \rangle$$

$$x \leq y \iff (y+1)^2 \leq x+y$$

1) ? $0 \leq 0$

2) ? $1 \leq 1$

platí iff $\exists a \in A : 0 \leq a, a \leq 0$

$$(0+1)^2 \leq 0+a$$

$$a^2 + 2a + 1 \leq a$$

$$a^2 + a + 1 \leq 0$$

X

$$(0+1)^2 \leq (a+0)$$

$$1 \leq a$$

X

neex

$$1 \leq a$$

$$\begin{bmatrix} a \leq 1 \\ a \leq 1 \end{bmatrix}$$

$$(1+1)^2 \leq 1+a$$

$$2 \leq 1+a$$

$$1 \leq a$$

neex

DMC

$$a|b \quad a, b \in \mathbb{N} \quad \text{ex } m \in \mathbb{N} : b = m \cdot a$$

$$\mathbb{Z}$$

$\mathbb{N}$ refl., antisym., trans.

$$\text{gcd}(a, b) = d \quad (1) \ d|a \text{ a souč. } d|b$$

$$(2) \text{ je-li } c|a, c|b, \text{ pak } c|d$$

$$\text{gcd}(a, \text{gcd}(b, c)) = \text{gcd}(\text{gcd}(a, b), c)$$

$$d_3 \stackrel{?}{=} d_4$$

$$(1) \ d_1|b, d_1|c$$

$$(1) \ d_3|a, d_3|d_1$$

$$(\text{trans}) \ d_3|d_1, d_1|b, \text{ pak } d_3|b$$

$$d_3|c$$

$$d_3|a, d_3|b, d_3|c$$

$$(2) \ d_3|d_2$$

$$(2) \ d_3|d_4$$

$$d_4|d_3$$

$$(\text{antisym}) \ d_3 = d_4$$

$$a, b \in \mathbb{Z}, b \neq 0, \text{ ex. } q, r \in \mathbb{Z} : a = qb + r, 0 \leq r < |b|$$

Euklidischer alg.

$$d = \text{gcd}(a, b)$$

$$\alpha, \beta \quad d = \alpha a + \beta b$$

$$a = 1960, b = 308$$

$$d, \alpha, \beta$$

rozkladem	$2 \cdot 2 \cdot 2 \cdot 5 \cdot 7 \cdot 7$	$2 \cdot 2 \cdot 7 \cdot 11$	$d = 2^2 \cdot 7 = 28$
	980	154	
	490	77	
	245		
	49		

$$b_0 = b$$

$$a = q_0 b_0 + b_1 \quad \begin{array}{l} 0 \leq b_1 < b \\ a \leq b_0 < b_1 \end{array}$$

$$b_{i-1} = q_i b_i + b_{i+1}$$

$$b_{m-1} = q_m b_m + \boxed{b_m}$$

$$b_{m+1} = q_{m+1} b_m + 0$$

$$\text{gcd}(a, b) = b_m$$

$$(1) \quad 1960 = q_0 \cdot 308 + b_1 = 6 \cdot 308 + \underline{112}$$

$$(2) \quad 308 = q_1 \cdot 112 + b_2 = 2 \cdot 112 + \underline{84}$$

$$(3) \quad 112 = q_2 \cdot 84 + b_3 = 1 \cdot 84 + \underline{28}$$

$$84 = q_3 \cdot 28 + b_4 = 3 \cdot 28 + 0$$

$$\text{gcd}(a, b) = 28$$

$$? \quad 28 = \alpha \cdot 1960 + \beta \cdot 308$$

$$(3) \quad 28 = \underline{112} - \underline{84} \stackrel{(2)}{=} \underline{112} - (308 - 2 \cdot \underline{112}) =$$

$$= -308 + 3 \cdot \underline{112} = -308 + 3 \cdot (1960 - 6 \cdot 308) =$$

$$= \underline{-19 \cdot 308 + 3 \cdot 1960}$$

$$\alpha = 3, \beta = -19$$

α	β	γ	δ	ϵ	ζ	η	θ	ι	κ
1295	42						0	0	1
1295	42	30	35	1	-30	0	1	1	-30
42	35	1	7	-1	31	1	-1	-30	37
35	7	5	0	16	-185	-1	36	31	-185
7	0					α		β	

Diophantická rovnice

$$ax + by = c \quad a, b, c \in \mathbb{Z}$$

$$x, y \in \mathbb{Z} ?$$

Řeš x, y existuje tehdy, když $d | c$, $d = \gcd(a, b)$

$$26x + 7y = 1$$

$$(x, y) = (x_p, y_p) + (x_h, y_h)$$

part.

homog.

$$26x + 7y = 0$$

$$26x = -7y, \quad \frac{26}{y} = -\frac{7}{x} = t, \quad (7, -26)t = (x_h, y_h), \quad t \in \mathbb{Z}$$

a	b	q	r	α	β	α_2	α_1	β_2	β_1
26	7					1	0	0	1
26	7	3	5	1	-3	0	1	1	-3
7	5	1	2	-1	4	1	-1	-3	4
5	2	2	1	3	-11	-1	3	4	-11
2	~~7~~	2	0	~~-7~~	26	3	~~-7~~	-11	~~26~~
1	0					r		s	

$$(x, y) = (3, -11) + (7, -26)t, \quad t \in \mathbb{Z}$$

$$26x + 7y = 2$$

negativně dáme správo gcd,
part. řešení pak vynásobíme

$$26x + 7y = 1$$

$$26(2x) + 7(2y) = 2$$

$$(x, y) = (6, -22) + (7, -26)t, \quad t \in \mathbb{Z}$$

10

$$1) \quad bc|ac, c \neq 0, \text{ pak } b|a, \quad a, b, c \in \mathbb{Z}$$

$$2) \quad a|bc, \gcd(a, b) = 1, \text{ pak } a|c$$

$$\text{def } x|y \quad \text{ex } n \in \mathbb{Z}, y = nx$$

$$1) \quad \text{ex } n \in \mathbb{Z} \quad ac = n \cdot bc, \text{ pak } a = nb$$

$$2) \quad \left. \begin{array}{l} \text{ex } n \in \mathbb{Z} \quad bc = na \\ \text{ex } \alpha, \beta \in \mathbb{Z} \quad 1 = \alpha a + \beta b \end{array} \right\} \quad \text{? ex } m \in \mathbb{Z} : c = ma$$

$$c = \alpha ac + \beta bc = \alpha ac + \beta na = (\alpha c + \beta n)a$$

$$a \equiv b \pmod{m} \quad \dots \quad m|(a-b)$$

$$\mathbb{Z}_m = \{[0]_m, [1]_m, \dots, [m-1]_m\}$$

$$a, b, a', b' \in \mathbb{Z} \quad \begin{array}{l} a \equiv b \pmod{m} \\ a' \equiv b' \pmod{m} \end{array} \quad \text{pak} \quad \begin{array}{l} a+a' \equiv b+b' \pmod{m} \\ a \cdot a' \equiv b \cdot b' \pmod{m} \end{array}$$

$\mathbb{Z}_4$

$\oplus$	$[0]_m$	$[1]_m$	$[2]_m$	$[3]_m$
$[0]_m$	$[0]_m$	$[1]_m$	$[2]_m$	$[3]_m$
$[1]_m$	$[1]_m$	$[2]_m$	$[3]_m$	$[0]_m$
$[2]_m$	$[2]_m$	$[3]_m$	$[0]_m$	$[1]_m$
$[3]_m$	$[3]_m$	$[0]_m$	$[1]_m$	$[2]_m$

$\odot$	$[0]_m$	$[1]_m$	$[2]_m$	$[3]_m$
$[0]_m$	$[0]_m$	$[0]_m$	$[0]_m$	$[0]_m$
$[1]_m$	$[0]_m$	$[1]_m$	$[2]_m$	$[3]_m$
$[2]_m$	$[0]_m$	$[2]_m$	$[0]_m$	$[2]_m$
$[3]_m$	$[0]_m$	$[3]_m$	$[2]_m$	$[1]_m$

$$[a]_m \text{ je inverzni k } [a]_m \text{ pokud } [a]_m [b]_m = [1]_m$$

$$[b]_m = [a]_m^{-1}$$

$$[1]_m^{-1} = [1]_m, \quad [2]_m^{-1} \text{ neex}, \quad [3]_m^{-1} = [3]_m$$

$$[11]_m^{-1} \text{ in } \mathbb{Z}_m?$$

$$\text{ex. } \alpha, \beta \in \mathbb{Z} : 11\alpha + 19\beta = 1$$

$$11\alpha \equiv 1 \pmod{19}$$

$$[11]_{19} \cdot [\alpha]_{19} = [1]_{19}$$

a	b	2	4	α	β	α_2	α_1	β_2	β_1
19	11					1	0	0	1
19	11	1	8	1	-1	0	1	1	-1
11	8	1	3	-1	2	1	-1	-1	2
8	3	2	2	3	-5	-1	3	2	-5
3	2	1	1	-4	7	3	-4	-5	7
2	1	1	1	7	-12	-4	7	7	-12
1	1	1	0	-11	19	7	-11	-12	19
1	0					β		α	

$$[11]_{19}^{-1} = [7]_{19}$$

$$77 = 4 \cdot 19 + 1$$

2

Malá Fermatova věta

p je prvočíslo

pro lib $a \in \mathbb{Z}$, $\gcd(a, p) = 1$

platí $a^{p-1} \equiv 1 \pmod{p}$

$$p = 19, \quad a = 11$$

$$11^{18} \equiv 1 \pmod{19}$$

$$11^2 = 121 = 6 \cdot 19 + 7$$

$$11 \cdot a \equiv 1 \pmod{19}$$

$$\begin{aligned} a = 11^{17} &= (11^2)^8 \cdot 11 \stackrel{7^2 \cdot 11 \equiv}{=} (7^2)^4 \cdot 11 \equiv 11^4 \cdot 11 \equiv \cancel{11^5} \\ &= (11^2)^2 \cdot 11 \equiv 7^2 \cdot 11 \equiv 11 \cdot 11 \equiv 7 \pmod{19} \end{aligned}$$

test dělitelnosti

$$4, 8, 11, 7, 13$$

$$A = a_n a_{n-1} \dots a_2 a_1 a_0 = \sum_{i=0}^n a_i \cdot 10^i$$

$$4 \mid A \quad (100 \equiv 0 \pmod{4}) \quad \text{právě tehdy, když } 4 \mid a_1 a_0$$

$$8 \mid A \quad (1000 \equiv 0 \pmod{8}) \quad 8 \mid a_2 a_1 a_0$$

$$11 \mid A \quad 10^0 \equiv 1 \pmod{11}$$

$$10^1 \equiv -1 \pmod{11}$$

$$10^2 \equiv 1 \pmod{11}$$

$$10^k \equiv (-1)^k \pmod{11}$$

$$11 \mid (a_0 - a_1 + a_2 - a_3 \dots)$$

$$7 \cdot 11 \cdot 13 = 1001$$

~~11~~

$$7 \mid A \quad (\text{nebo } 13 \mid A)$$

$$7 \mid (a_2 a_1 a_0 - a_5 a_4 a_3 + a_8 a_7 a_6 - \dots)$$

$$13 \mid \dots$$

$$A = 673 \ 524 \ 120$$

$$[A]_7, [A]_{11}, [A]_{13} \quad ?$$

$$15 \cdot 11 \cdot 13$$

$$[3]_7 \quad [5]_{11} \quad [9]_{13}$$

$$269$$

$$2 \cdot 11 \mid 0 - 2 + 1 + 4 + 2 - 5 + 3 - 7 + 6 = -8 \equiv 5 \pmod{11}$$

$$2 \cdot 7, 13 \mid 120 - 524 + 673 = 269 \equiv 3 \pmod{7}$$

$$= 3 \cdot 7 + 3$$

$$= 2 \cdot 13 + 9$$

$$= 24 \cdot 11 + 5$$

Eulerova věta

$$\gcd(a, m) = 1$$

$$\text{platí } a^{\varphi(m)} \equiv 1 \pmod{m}$$

Eulerova funkce $\varphi(m), m \in \mathbb{N}$

pčet čísel $\in \{0, 1, \dots, m-1\}$ nesoud s m

p - prvočíslo

$$\varphi(p) = p - 1$$

$$\varphi(p^k) = p^k - p^{k-1}$$

$$\gcd(m, n) = 1$$

$$\varphi(m \cdot n) = \varphi(m) \cdot \varphi(n)$$

$$\varphi(p_1^{k_1} p_2^{k_2} \dots p_s^{k_s}) = p_1^{k_1-1} (p_1 - 1) \cdot p_2^{k_2-1} (p_2 - 1) \dots$$

$$\varphi(13) = 12$$

$$\varphi(27) = \varphi(3^3) = 18$$

$$\varphi(152) = \varphi(2 \cdot 2 \cdot 7 \cdot 13) = 1 \cdot 1 \cdot 6 \cdot 12 = 72$$

$$\varphi(1960) = \varphi(2^3 \cdot 5 \cdot 7^2) = 4 \cdot 1 \cdot 1 \cdot 4 \cdot 7 \cdot 6 = 16 \cdot 42 = \underline{672}$$

$$8^{103} \text{ del. } 13 \text{ ?}$$

$$\text{pro lib } a \in \mathbb{N} : \gcd(a, 13) = 1$$

$$\text{ip } a^{12} \equiv 1 \pmod{13}$$

$$\varphi(13) = 12$$

$$8^{12} \equiv 1 \pmod{13}$$

$$103 = 8 \cdot 12 + 7$$

$$8^{103} = (8^{12})^8 \cdot 8^7 \equiv 8^7 = 2^{21} \equiv 2^9 = 2^4 \cdot 2^4 \cdot 2 \equiv 3 \cdot 3 \cdot 2 \equiv 5 \pmod{13}$$

$$121^{121} \text{ del } 18$$

$$\gcd(18, 121) = 1$$

$$\varphi(18) = \varphi(2 \cdot 3^2) = \varphi(2) \cdot \varphi(3^2) = 6$$

$$121^6 \equiv 1 \pmod{18}$$

$$121^{121} = (121^6)^{20} \cdot 121 \equiv 121 \equiv 13 \pmod{18}$$

$$\begin{array}{lcl} a \equiv b \pmod{m} & & a+c \equiv b+d \pmod{m} \\ c \equiv d \pmod{m} & \text{pak} & ac \equiv bd \pmod{m} \end{array}$$

$a \equiv b \pmod{m}$ právě tehdy, když ex. $k \in \mathbb{Z}$, $a-b = k \cdot m$

$$\begin{array}{lcl} \text{ex. } k, l \in \mathbb{Z}: a-b = km & & a-b+c-d = km+lm \\ c-d = lm & \text{pak} & (a+c)-(b+d) = (k+l) \cdot m \end{array}$$

Je-li $a \equiv b \pmod{m}$, pak $ac \equiv bc \pmod{m}$

$$a-b = km \quad ac-bc = kcm$$

$$c \equiv d \pmod{m}, \text{ pak } bc \equiv bd \pmod{m}$$

$$(\text{brance}) \quad ac \equiv bd \pmod{m}$$

1. $ac \equiv bc \pmod{m}$, pak $a \equiv b \pmod{m}$?

2. $ac \equiv bc \pmod{mc}$: pak $a \equiv b \pmod{m}$? ✓

② $ac-bc = kmc \quad a-b = km$

① $m | ac-bc = (a-b)c$ $m | a-b$
 $\text{gcd}(m, c) = 1$ pak

$$ax \equiv b \pmod{m}, \quad x = ?$$

$$a \neq 0 \quad \text{gcd}(a, m) = 1$$

$$a^{\varphi(m)} \equiv 1 \pmod{m}$$

$$x \equiv a^{\varphi(m)-1} \cdot b \pmod{m}$$

$$\text{gcd}(a, m) = d > 1$$

potenciál $d \nmid b$ pak x neex.

$d \mid b$ ex d různých řes.

$$1) \quad 3x \equiv -2 \pmod{7}$$

$$\gcd(3, 7) = 1 \quad \cdot \quad \varphi(7) = 6$$

$$x \equiv 3^5 \cdot (-2) \pmod{7}$$

$$x \equiv 4 \pmod{7}$$

$$-2 \cdot 3^5 = -2 \cdot 3 \cdot 9 \cdot 9 \equiv -2 \cdot 3 \cdot 2 \cdot 2 = -3 \cdot 8 \equiv -3 \equiv 4 \pmod{7}$$

$$3 \cdot 4 \equiv -2 \pmod{7}$$

$$2) \quad 2x \equiv 5 \pmod{4}$$

$$\gcd(2, 4) = 2, \quad 2 \nmid 5$$

$$3) \quad 3x \equiv 9 \pmod{15}$$

$$\gcd(3, 15) = 3, \quad 3 \mid 9 \quad \text{ex } 3 \text{ res.}$$

$$x \equiv 3 \pmod{5}$$

$$x = 3 + 5k, \quad k \in \mathbb{Z}$$

$$x_1 \equiv 3 \pmod{15}$$

$$x_2 \equiv 8 \pmod{15}$$

$$x_3 \equiv 13 \pmod{15}$$

$$\begin{aligned}x + 2y - z + 2t &= 3 \\4x + z + t &= 2 \\4x + 4y + z + 2t &= 2\end{aligned}$$

$$10 \mathbb{Z}_5 \text{ a } 10 \mathbb{Z}_7$$

$$\left(\begin{array}{cccc|c} 1 & 2 & -1 & 2 & 3 \\ 4 & 0 & 1 & 1 & 2 \\ 4 & 4 & 1 & 2 & 2 \end{array} \right) \xrightarrow[\sim]{\substack{+ \text{pr} \\ + \text{pr}}} \left(\begin{array}{cccc|c} 1 & 2 & -1 & 2 & 3 \\ 0 & 2 & 0 & 3 & 0 \\ 0 & 1 & 0 & 4 & 0 \end{array} \right) \sim$$

$$\sim \xrightarrow[\sim]{\substack{2. \text{dr} \\ +3}} \left(\begin{array}{cccc|c} 1 & 2 & -1 & 2 & 3 \\ 0 & 2 & 0 & 3 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{array} \right)$$

$$z = \text{lib}$$

$$x = \text{lib}$$

$$y = \frac{3}{2}t$$

$$y = t$$

$$\begin{aligned}x &= 3 - 2t + z - 2t \\ &= 3 - 4t + z\end{aligned}$$

$$2^{-1} = 3 \text{ in } \mathbb{Z}_5$$

$$2 \cdot 3 = 6 = 1 \text{ in } \mathbb{Z}_5$$

$$\frac{3}{2} \text{ mod } 5 = 4 \text{ in } \mathbb{Z}_5$$

$$(x, y, z, t) = (3 - 4t + z, t, z, t)$$

$$\mathbb{Z}_7: \left(\begin{array}{cccc|c} 1 & 2 & -1 & 2 & 3 \\ 4 & 0 & 1 & 1 & 2 \\ 4 & 4 & 1 & 2 & 2 \end{array} \right) \xrightarrow[\sim]{\substack{3.I+II \\ 3.I+III}} \left(\begin{array}{cccc|c} 1 & 2 & -1 & 2 & 3 \\ 0 & 6 & -2 & 0 & 4 \\ 0 & 3 & -2 & 1 & 4 \end{array} \right) \sim$$

$$\xrightarrow[\sim]{\substack{-2.I+II \\ -2.I+III}} \left(\begin{array}{cccc|c} 1 & 2 & -1 & 2 & 3 \\ 0 & 6 & -2 & 0 & 4 \\ 0 & 0 & 2 & -2 & -4 \end{array} \right) \xrightarrow[\sim]{\substack{\cdot 6 \\ 3}} \left(\begin{array}{cccc|c} 1 & 2 & 4 & 2 & 3 \\ 0 & 1 & 2 & 0 & 3 \\ 0 & 0 & 1 & 6 & 5 \end{array} \right)$$

$$z = 5 + t$$

$$y = 3 - 10 - 2t = -7 - 2t$$

$$x = 3 - 2t - 30 - 6t - 10t = -37 - 18t$$

$$(1, 0, 5, 0) + (3, 5, 1, 1)t, \quad t \in \mathbb{Z}_2$$

$$A = \begin{pmatrix} 1 & 2 & 3 \\ 0 & 5 & 3 \\ 2 & 1 & 1 \end{pmatrix} \in \mathbb{Z}_6$$

$$\det A = 5$$

$$\gcd(5, 6) = 1$$

$$5^{-1} = 5 \in \mathbb{Z}_6$$

$$A^{-1} = 5 \cdot \begin{pmatrix} \begin{vmatrix} 5 & 3 \\ 2 & 1 \end{vmatrix} & -\begin{vmatrix} 0 & 3 \\ 2 & 1 \end{vmatrix} & \begin{vmatrix} 0 & 5 \\ 2 & 3 \end{vmatrix} \\ -\begin{vmatrix} 2 & 3 \\ 2 & 1 \end{vmatrix} & \begin{vmatrix} 1 & 3 \\ 2 & 1 \end{vmatrix} & -\begin{vmatrix} 1 & 2 \\ 2 & 2 \end{vmatrix} \\ \begin{vmatrix} 1 & 2 \\ 5 & 3 \end{vmatrix} & -\begin{vmatrix} 1 & 3 \\ 0 & 3 \end{vmatrix} & \begin{vmatrix} 1 & 2 \\ 0 & 5 \end{vmatrix} \end{pmatrix}^T$$

$$= \begin{pmatrix} 1 & 2 & 3 \\ 0 & 5 & 4 \\ 4 & 4 & 1 \end{pmatrix}$$

adjung. mat.

$$A = \begin{pmatrix} 1 & 2 & 3 \\ 0 & 5 & 3 \\ 2 & 2 & 1 \end{pmatrix} \in \mathbb{Z}_6$$

a^{-1} ex. v $\mathbb{Z}_m$ právě tehdy,

když $\gcd(a, m) = 1$

$$\gcd(\det A, m) = 1$$

$$|A| = 5 \neq 0$$

$$\begin{pmatrix} + & - & + \\ - & + & - \\ + & - & + \end{pmatrix}$$

$$\gcd(|A|, 6) = 1$$

$$A^{-1} = \frac{1}{5} \begin{pmatrix} 5 & 0 & 2 \\ 4 & 1 & 2 \\ 3 & 3 & 5 \end{pmatrix}^T = \frac{1}{5} \begin{pmatrix} 5 & 4 & 3 \\ 0 & 1 & 3 \\ 2 & 2 & 5 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 0 & 5 & 3 \\ 4 & 4 & 1 \end{pmatrix}$$

$$5 \cdot 5 = 1$$

$$5 \equiv -1 \in \mathbb{Z}_6$$

$$A = \begin{pmatrix} 4 & 4 & 1 \\ 2 & 4 & 0 \\ 3 & 4 & 0 \end{pmatrix} \text{ in } \mathbb{Z}_{15}$$

$$\det A = 8 - 12 = -4 = 11$$

$$\gcd(11, 15) = 1$$

$$11^2 = 121 \equiv 1 \pmod{15}$$

$$A^{-1} = 11 \cdot \begin{pmatrix} 0 & 0 & 11 \\ 4 & 12 & 11 \\ 11 & 2 & 108 \end{pmatrix}^T = \begin{pmatrix} 0 & 14 & 1 \\ 0 & 12 & 7 \\ 1 & 1 & 13 \end{pmatrix}$$

$$A = \begin{pmatrix} 4 & 1 \\ 1 & 5 \end{pmatrix} \text{ in } \mathbb{Z}_{27}$$

$$B = A^6$$

$$B^{-1} \text{ ex?}, \det B^{-1} \text{ ex?}$$

✓

$$\det B^{-1} = 1$$

$$(\det A)^6 = \det A^6$$

$$(\det B)^{-1} = \det B^{-1}$$

$$\gcd(\det B, 27) = 1$$

$$\det B = 19^6 = (-8)^6 = ((-8)^2)^3 = 10^3 = 1$$

podgrupoidy $\langle F, \circ \rangle$

$\emptyset, \{f_1\}, \{f_2\}, \{f_3\}, \{f_1, f_2\}, \{f_1, f_3\}, \{f_1, f_4\},$
 $\{f_2, f_3\}, \{f_1, f_2, f_3\}, \{f_1, f_2, f_3, f_4\}$

$\langle A, * \rangle$

$*$ je asociativní $(x * y) * z = x * (y * z)$ pro lib. $x, y, z \in A$

$*$ je komutativní $x * y = y * x$ pro lib. $x, y \in A$

prvek e je neutrální $e * x = x * e = x$ pro lib. $x \in A$

~~1BBAA~~

$$1 \cdot x = x \cdot 1 = x$$

$$0 + x = x + 0 = x$$

e_L levý neutrální $e_L * x = x$ pro lib. $x \in R$

e_R pravý $x * e_R = x$

$\bar{x}$ je inverzní k x pokud platí $\bar{x} * x = x * \bar{x} = e$

$f, g, h \in F, x \in \{0, 1\}$

asoc.

$$(f \circ g) \circ h(x) = (f \circ g)(h(x)) = f(g(h(x)))$$

$$(f \circ (g \circ h))(x) = f((g \circ h)(x)) = f(g(h(x)))$$

operace $\circ$ je asociativní

komut.

není komutativní

neutrální prvek $e = f_1$

$$f_1 \circ g = g \circ f_1 = g$$

$$f^{-1} = f_1 \quad f_2, f_3 \text{ není}, \quad f_4^{-1} = f_4$$

operace $*$

$$x, y, z \in T$$

$$(x * y) * z = x * z = x$$

$$x * (y * z) = x * y = x$$

je asociativní
není komutativní

(12)

$(A, *)$ grupoid

grupa

1) operace $*$ je asociativní $(a * b) * c = a * (b * c)$

2) ex. neutrální prvky e : $e * a = a = a * e$

3) pro lib. $a \in A$ ex. inverzní $a^{-1} * a = a * a^{-1} = e$

okruh

~~$(A, \cdot, +)$~~ $(A, +)$ komutativní grupa $a + b = b + a$

$\langle A \rangle$

$(A, \cdot)$ asoc, neutrální prvky

distributivita $a(b + c) = ab + ac$

$$(b + c)a = ba + ca$$

$$\text{př. } \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Z}_m$$

teleso

$$0 \neq 1$$

pro lib. $a \in A, a \neq 0$ ex a^{-1} . $a \cdot a^{-1} = a^{-1} \cdot a = 1$

$$\text{př. } \mathbb{Z}_p, \mathbb{Q}, \mathbb{R}, \mathbb{C}$$

p prvočíslo

(13)

$$X(n+k) + c_1 X(n+k-1) + \dots + c_m X(n) = F(n) \quad \begin{array}{l} c_i \in \mathbb{R} \\ c_m \neq 0 \\ k \geq 1, k \in \mathbb{N} \end{array}$$

$$= 0$$

$$\lambda^k + c_1 \lambda^{k-1} + \dots + c_m = 0$$

$$X(n+2) - 3X(n+1) + 2X(n) = 0$$

$$X(1) = 3, \quad X(2) = 7$$

$$\lambda^2 - 3\lambda + 2 = 0, \quad \lambda_1 = 1$$

$$\lambda_2 = 2$$

$$X(n) = \alpha \cdot 1^n + \beta \cdot 2^n$$

$$X(1) = \alpha \cdot 1 + \beta \cdot 2 = 3$$

$$X(2) = \alpha \cdot 1 + \beta \cdot 4 = 7$$

$$2\beta = 4 \quad \beta = 2$$

$$\alpha = -1$$

$$X(n) = -1 + 2 \cdot 2^n$$

$$- \quad X(n+2) - 2X(n+1) + X(n) = 0$$

$$X(1) = 2, \quad X(2) = 3$$

$$\lambda^2 - 2\lambda + 1 = 0$$

$$\lambda_{1,2} = 1$$

$$X(n) = \alpha \cdot 1^n + n\beta \cdot 1^n$$

$$2 = \alpha + \beta$$

$$3 = \alpha + 2\beta$$

$$\beta = 1$$

$$\alpha = 1$$

$$X(n) = 1 + n$$

$$X(n+3) - 3X(n+2) + 4X(n) = 0$$

$$X(1) = 2, \quad X(2) = 6, \quad X(3) = 22$$

$$\lambda^3 - 3\lambda^2 + 4 = 0$$

$$(\lambda + 1)(\lambda - 2)^2 = 0$$

$$\lambda_{1,2} = 2$$

$$\lambda_3 = -1$$

$$X(n) = \alpha \cdot 2^n + n\beta 2^n + \gamma(-1)^n$$

$$2 = 2\alpha + 2\beta - \gamma$$

$$\alpha = -\frac{1}{3}$$

$$6 = 4\alpha + 8\beta + \gamma$$

$$\beta = 1$$

$$22 = 8\alpha + 26\beta - \gamma$$

$$\gamma = -\frac{2}{3}$$

$$\begin{pmatrix} 2 & 2 & -1 & 2 \\ 6 & 4 & 1 & 6 \\ 8 & 26 & -1 & 22 \end{pmatrix} \sim \begin{pmatrix} 2 & 2 & -1 & 2 \\ 0 & 4 & 3 & 2 \\ 0 & 0 & -3 & 10 \end{pmatrix}$$

$$F(n) = A^n P(n)$$

polynom in n

$$X(n+2) + 3X(n+1) + 2X(n) = 3^n(2n+5)$$

$$\lambda^2 + 3\lambda + 2 = (\lambda + 1)(\lambda + 2) = 0$$

$$X(n) = 3^n(an+b) = \underline{3^n(n-2)}$$

$$3^{n+2}(a(n+2)+b) - 3 \cdot 3^{n+1}(a(n+1)+b) +$$

$$2 \cdot 3^n(a(n+1)+b) = 3^n(2n+5) - 9(a(n+1)+b) +$$

$$- 9(a(n+1)+b) + 2(a(n+1)+b) = 2n+5$$

$$n^1: 9a - 9a + 2a = 2 \quad a = 1$$

$$n^0: 18a + 9b - 9a - 9b + 2b = 5 \quad 2b = -4, \quad b = -2$$

$$X(n+2) - 3X(n+1) + 2X(n) = 2^n(8n+2)$$

$$X_p(n) = \underline{n} \cdot 2^n (an+b)$$

$$(n+2) \cdot 2^{n+2}(a(n+2)+b) - 3(n+1)2^{n+1}(a(n+1)+b) + 2n2^n(a(n+1)+b) =$$

$$2(n+2)(an+2a+b) - 3(n+1)(an+a+b) + 2n(an+b) = 4n+1$$

$$n^2: 0 = 2a - 3a + a \rightarrow 0 = 0$$

$$n^1: 4 = 4a + 2b + 4a - 3a - 3a - 3b + b$$

$$4 = 2a \Rightarrow a = 2$$

$$X_p(n) = n2^n(2n-9)$$

$$n^0:$$

$$\dots b = -9$$

$$X(n+2) - 3X(n+1) + 2X(n) = \boxed{3} + \boxed{5^n}$$

$$X_1(n) = n^1 \cdot 1^n a = a \cdot n$$

$$X_2(n) = b \cdot 5^n$$

$$X_p(n) = X_1(n) + X_2(n)$$

$$a(n+2) - 3(a(n+1)) + 2an = 3$$

$$n^1: a - 3a + 2a = 0 = 0$$

$$n^0: 2a - 3a = 3$$

$$\underline{a = -3}$$

$$b \cdot 5^{n+2} - 3b \cdot 5^{n+1} + 2b \cdot 5^n = 5^n \quad | : 5^n$$

$$b \cdot 5^2 - 15b + 2b = 1$$

$$n^0: 25b - 15b + 2b = 1$$

$$\underline{b = \frac{1}{12}}$$

$$\underline{X_p(n) = -3n + \frac{1}{12} 5^n}$$

$(A, *)$ grupoid, $*$ $A \times A \rightarrow A$

pologrupa: je-li $*$ asociativní operace

pologr $(A, *)$ je monoid, jestliže operace $*$ má
neutrální prvek

$$e * a = a = a * e, a \in A$$

monoid $(A, *, e)$ je grupa, jestliže má každý prvek
 $a \in A$ inverzi

asoc. $(a * b) * c = a * (b * c)$

komut. $a * b = b * a$

$(\mathbb{Z}, -)$ není pologrupa

$$\frac{(m-n) - k}{m-n+k} \neq m - (n-k)$$

$(\mathbb{N} \setminus \{0\}, +)$ není monoid
 $(\mathbb{T}, *)$

$(\mathbb{T}, *)$, $(\mathbb{F}, \circ)$

$$x * y = x$$

$$\mathbb{T} = \{1, 2, 3\}$$

$(\mathbb{N}, +)$, $(\mathbb{F}, \circ)$

$$(\mathbb{N}, *), a * b = \max(a, b)$$

$$\max(e, a) = a, e = 0$$

homomorfismus

izomorfismus
bijekce

$(A, *)$, $(B, *)$ grupoidy, $f: A \rightarrow B$

$$a, b \in A \quad a * b \mapsto f(a) \circ f(b)$$

homom. plogrup
monoidu
grup

$$f(a * b) = f(a) \circ f(b), \quad f(e_A) = e_B$$

$$f(\bar{a}_A) = \overline{f(a)}_B$$

$$(\mathbb{Z}_6, +) \rightarrow (\mathbb{Z}_4, +)$$

$$\{0, 1, 2, 3, 4, 5\} \rightarrow \{0, 1, 2, 3\}$$

$$0 \mapsto 0$$

$$1 \mapsto 1$$

$$2 \mapsto 2$$

$$3 \mapsto 3$$

$$4 \mapsto 0$$

$$5 \mapsto 1$$

$$f(2) = f(1+1) = f(1) + f(1) = 2 \cdot f(1)$$

$$f(m) = m \cdot f(1) = \underbrace{f(1) + f(1) + \dots + f(1)}_{m \text{ krát } f(1)} \\ m \in \mathbb{Z}_6 \quad n \in \mathbb{Z}_4$$

najít izomorfismus $(\mathbb{Z}_4, +) \rightarrow (\mathbb{Z}_4, +)$

$$\begin{array}{ccc|c|c} 0 & \mapsto & 0 & 0 & 0 \\ 1 & \mapsto & 1 & 2 & 3 \\ 2 & \mapsto & 2 & 0 & 2 \\ 3 & \mapsto & 3 & 2 & 1 \end{array}$$

není izomorf

bijekce: $f: A \rightarrow B$ je prostě $\left\{ \begin{array}{l} a \neq b, \text{ pak } f(a) \neq f(b) \\ \text{neboť} \quad f(a) = f(b), \text{ pak } a = b \end{array} \right.$

na B : pro lib $x \in B$ $\exists a \in A: f(a) = x$

není prostě

neníobrazení

okruh $(A, +, \cdot)$

1) $(A, +)$ je komut. grupa

$$(a+b)+c = a+(b+c) \text{ pro } \forall a, b, c \in A$$

$$\text{ex. } 0 \in A : 0+a = a = a+0 \text{ pro } \forall a \in A$$

$$\text{pro } \forall a \in A \text{ ex. } -a \in A : a+(-a) = (-a)+a = 0$$

$$a+b = b+a \text{ pro } \forall a, b \in A$$

2) $(A, \cdot)$ je monoid

$$(a \cdot b) \cdot c = a \cdot (b \cdot c) \text{ pro } \forall a, b, c \in A$$

$$\text{ex. } 1 \in A : 1 \cdot a = a = a \cdot 1 \text{ pro } \forall a \in A$$

$$3) a(b+c) = ab+ac$$

$$(a+b)c = ac+bc \text{ pro lib. } a, b, c \in A$$

$$\text{Pr. } (\mathbb{Z}, +, \cdot) \quad , \quad (\text{Mat}_{n \times n}(\mathbb{R}), +, \cdot)$$

$\mathbb{Q}, \mathbb{R}$

teleso - komutativní okruh

$$a \cdot b = b \cdot a \text{ pro lib. } a, b \in A$$

$$- \text{ pro } \forall a \in A, a \neq 0, \text{ ex. } a^{-1} : a^{-1} \cdot a = a \cdot a^{-1} = 1$$

$$- 0 \neq 1$$

$(\mathbb{Z}_2, +, \cdot)$ nejmenší teleso

$(\mathbb{R}, +, \cdot)$ je teleso

$\mathbb{Q}$

$$\text{Def } \bar{\mathbb{R}}, \quad a \oplus b = a + b + 1 \\ a * b = a + b + ab \quad (\bar{\mathbb{R}}, \oplus, *) \text{ je těleso?}$$

$$\hat{e}_0, \hat{a}, \hat{e}_1, \hat{a}'$$

$$e_0 \oplus a = a \oplus e_0 = a \quad \text{pro vs. } a \in \bar{\mathbb{R}}$$

$$e_0 + a + 1 = a \quad \underline{e_0 = -1}$$

$$a \oplus \bar{a} = \bar{a} + a = -1$$

$$a + \bar{a} + 1 = -1 \quad \underline{\bar{a} = -2 - a}$$

$$e_1 * a = a * e_1 = a$$

$$e_1 + a + e_1, a = a$$

$$e_1(1+a) = 0$$

$$\underline{e_1 = 0}$$

$$a' * a = a^* * a = 0, \quad a \neq e_0$$

$$a + a' + aa' = 0$$

$$\underline{a' = \frac{-a}{1+a}}$$