

Gymnázium Brno, třída Kapitána Jaroše 14
Školní rok 2008/2009
třída 4.A

ZÁVĚREČNÁ MATURITNÍ PRÁCE

Základní pojmy z algebry a teorie čísel

Autor: Tereza Eliášová

Vedoucí práce: RNDr. Pavel Boucník

Brno, 2009

Prohlášení

Prohlašuji, že jsem předloženou závěrečnou maturitní práci zpracovala samostatně a že jsem použila pouze materiál uvedený v seznamu literatury.

Dne 19. ledna 2009

Tereza Eliášová

Obsah:

I. Teorie množin, výroková logika

§1. Základní pojmy z teorie množin	4
§2. Číselné množiny, zápis čísel, intervaly	8
§3. Výroky a jejich negace	10
§4. Složené výroky, operace s výroky	12
§5. Negace složených výroků. Obměny a obrácení implikací	15
§6. Výrokové formy	18

II. Algebraické výrazy, věty, důkazy, mocniny a odmocniny

§1. Algebraické výrazy a jejich úpravy	21
§2. Rovnice a nerovnice s jednou neznámou, soustavy rovnic a nerovnic, výpočet neznámé ze vzorce	24
§3. Matematické věty	26
§4. Základní typy důkazů	27
§5. Důkaz matematickou indukcí	29
§6. Mocniny s celočíselnými exponenty	31
§7. Mocniny s racionálními exponenty	33

III. Teorie čísel

§1. Základní pojmy teorie čísel	35
§2. Největší společný dělitel	38
§3. Nejmenší společný násobek	42
§4. Prvočísla a čísla složená	45
§5. Rozklad přirozeného čísla na prvočinitele	47
§6. Kritéria dělitelnosti	50
§7. Reálná čísla	53

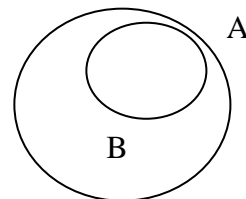
I. Teorie množin, výroková logika

§1. Základní pojmy z teorie množin

- Pozn.:** 1. Množinou nazýváme souhrn objektů, o kterých můžeme rozhodnout, zda do daného souhrnu patří nebo ne. Tyto objekty nazýváme prvky množiny.
2. Konečnou množinou nazýváme množinu s konečným počtem prvků, v opačném případě se množina nazývá nekonečná. Množina, která neobsahuje žádný prvek, se nazývá prázdná. Zapisujeme $A = \emptyset$ nebo $A = \{ \}$.
3. Je-li prvek x prvkem množiny A , zapisujeme $x \in A$.
Není-li jejím prvkem, zapisujeme $x \notin A$.

Zadání množiny: a) výčtem prvků (u konečných množin): $A = \{a, b, c\}$
b) pomocí charakteristické vlastnosti (u nekonečných, někdy i u konečných množin): $S = \{2k, k \in N\}$; k – proměnná, N – obor proměnné

Def.: Podmnožinou množiny A nazýváme množinu B , jestliže pro každý její prvek x platí, že $x \in A$. Zapisujeme $B \subseteq A$.

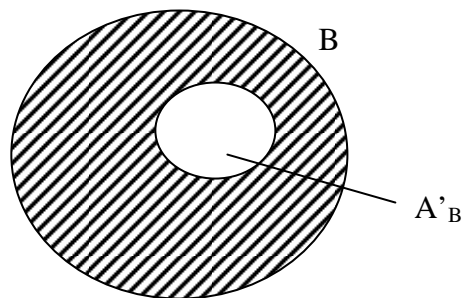


- Pozn.:** 1. \subseteq je znak inkluze.
2. Jestliže $A \neq \emptyset$, pak množina A má alespoň dvě podmnožiny, které nazýváme nevlastní podmnožiny množiny A (= množina prázdná a množina A).
Všechny ostatní (pokud existují) nazýváme vlastní podmnožiny množiny A . Ty někdy označujeme tzv. ostrou inkluzí \subset .

Def.: Řekneme, že množiny A a B se rovnají ($A = B$) právě tehdy, když A je podmnožinou B a zároveň B je podmnožinou A .

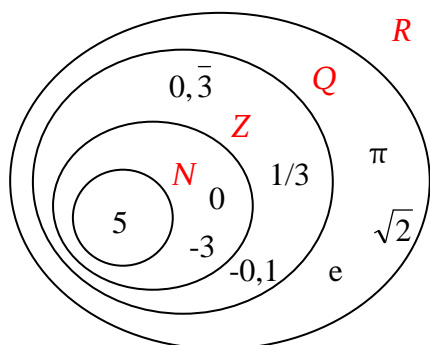
Def.: Necht' $A \subseteq B$ a $B \neq \emptyset$.

Množinu všech prvků B , které nepatří do A , nazýváme doplňk (komplement) množiny A v množině B .
Značíme A'_B nebo jen A' za předpokladu, že víme, ve které množině jej tvoříme.



Pozn.: $(A'_B)'_B = A$, $A'_A = \emptyset$, $\emptyset'_A = A$

Pozn.: Označení číselných množin:



N ... množina všech přirozených čísel

Z ... množina všech celých čísel

Q ... množina všech racionálních čísel

R ... množina všech reálných čísel

N_0 ... množina všech přirozených čísel včetně nuly

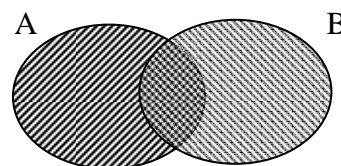
Z^+, Q^+, R^+ ... pouze kladná čísla

Z_0 ... množina všech nekladných celých čísel

Def.: Necht' A, B jsou dvě množiny.

Sjednocení množin A a B nazýváme množinu označenou $A \cup B$, která obsahuje ty prvky, které patří aspoň do jedné z množin A, B .

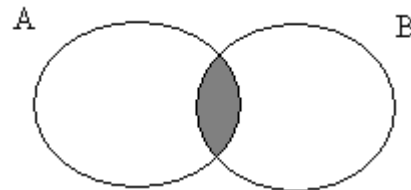
$$A \cup B = \{x \in A \vee x \in B\}$$



Def.: Necht' A, B jsou dvě množiny.

Průnikem množin A a B nazýváme množinu označenou $A \cap B$, která obsahuje ty prvky, které patří zároveň i do množiny A i do množiny B .

$$A \cap B = \{x \in A \wedge x \in B\}$$



Pozn.: Dá se dokázat, že platí:

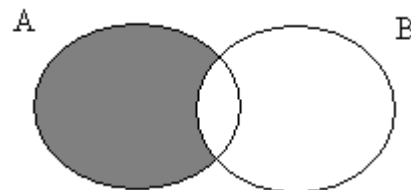
1. $A \cap B = B \cap A$, $A \cup B = B \cup A$ - KOMUTATIVNOST
2. $(A \cap B) \cap C = A \cap (B \cap C)$, $(A \cup B) \cup C = A \cup (B \cup C)$ - ASOCIATIVNOST
3. $A \cup A'_B = B$, $A \cap A'_B = \emptyset$

Def.: Řekneme, že množiny A, B jsou disjunktní, pokud $A \cap B = \emptyset$.

Množiny jsou konjunktní, když $A \cap B \neq \emptyset$.

Def.: Rozdílem množin A, B (v tomto pořadí) nazýváme množinu označenou $A \setminus B$, která obsahuje prvky, které patří do množiny A a nepatří do množiny B .

$$A \setminus B = \{x \in A : x \notin B\}$$



Pozn.: $\forall B'_A$ je navíc podmínka $B \subseteq A$.

Pozn.: 1. Rozdíl množin není komutativní.

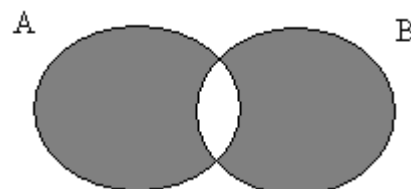
$$2. A \setminus B = B'_{A \cup B}$$

3. Jestliže jsou množiny disjunktní, jejich rozdílem je A .

4. Jestliže $B \subseteq A$, pak $A \setminus B = B'_A$.

Def.: Symetrickým rozdílem množin A, B nazýváme množinu označenou $A \div B$, která obsahuje ty prvky z množin A a B , které patří právě do jedné z nich.

$$A \div B = \{x \in A : x \notin B\} \cup \{x \in B : x \notin A\}$$



Pozn.: Systém všech podmnožin množiny M se nazývá potenční množina množiny. Značí se $P(M)$.

Má-li množina M n prvků, pak má její potenční množina $P(M)$ 2^n prvků.

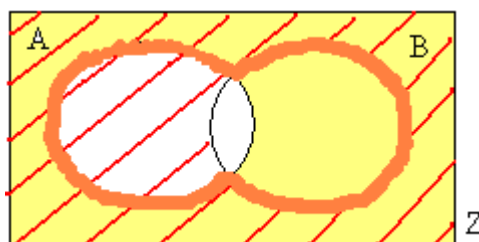
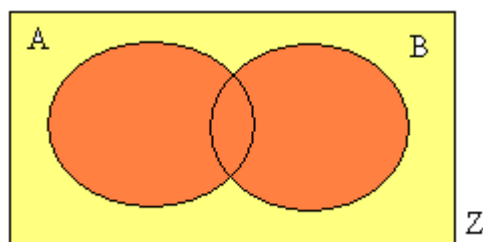
V.1.1. De Morganova pravidla:

Pro každé 2 množiny $A, B \subseteq Z$ platí, že:

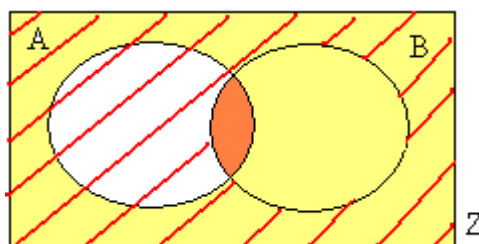
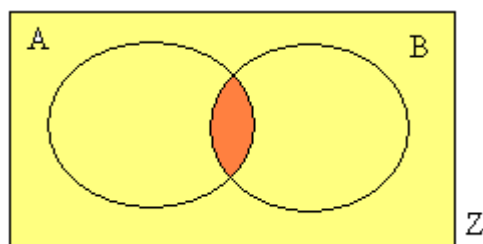
a) $(A \cup B)'_Z = A'_Z \cap B'_Z$

b) $(A \cap B)'_Z = A'_Z \cup B'_Z$

[Dk.: a)



b)



Příklady k §1.:

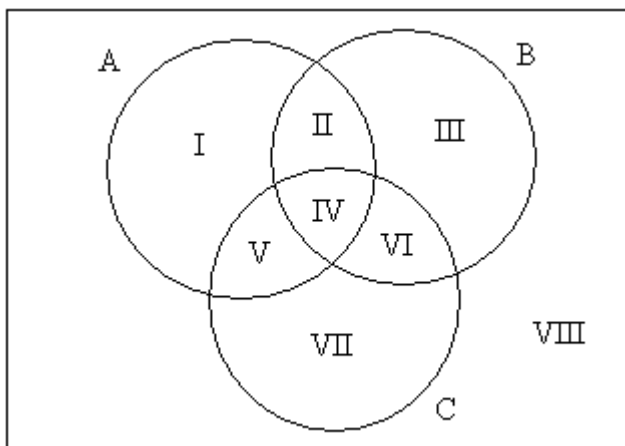
Př.: Určete všechny podmnožiny množin $A = \{x, y\}, B = \{a, b, c\}$:

$A: \emptyset, \{x\}, \{y\}, \{x, y\}$

$B: \emptyset, \{a\}, \{b\}, \{c\}, \{a, b\}, \{a, c\}, \{b, c\}, \{a, b, c\}$

Př.: Nakreslete diagramy pro 3 množiny a symbolicky označte všechny oblasti:

- I. $A \cap B' \cap C'$
- II. $A \cap B \cap C'$
- III. $A' \cap B \cap C'$
- IV. $A \cap B \cap C$
- V. $A \cap B' \cap C$
- VI. $A' \cap B \cap C$
- VII. $A' \cap B' \cap C$
- VIII. $A' \cap B' \cap C'$

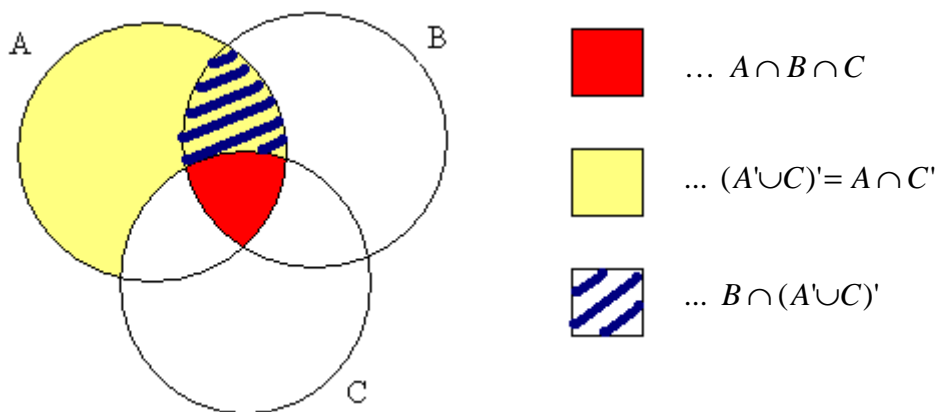


Př.: Určete, čemu se rovná:

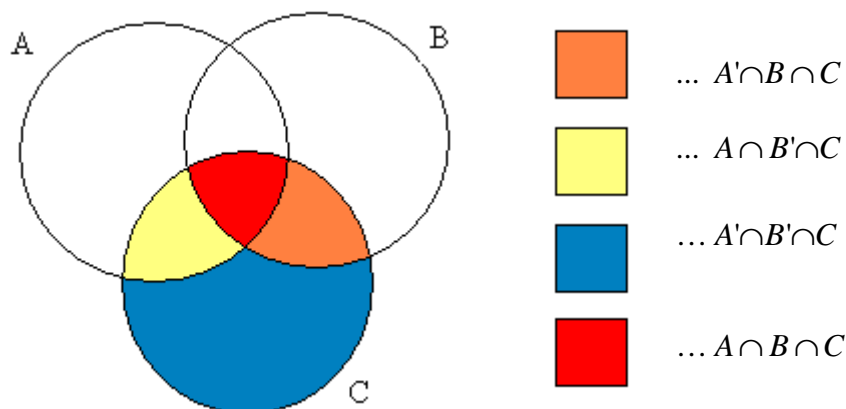
- a) $\langle 4, \infty \rangle'_{\mathbb{R}} = (-\infty, 4)$ b) $(-3, \pi) \cup \langle 1, 4 \rangle = (-3, 4)$
 c) $\langle -3, 1 \rangle \cap \langle 3, 5 \rangle = \emptyset$ d) $(-\infty, 2) \cap \langle 2, \infty \rangle = \emptyset$
 e) $\langle -2, 5 \rangle \cap (0, 7) = (0, 5)$ f) $(-7, -1) \cap \langle -2, 0 \rangle \cap \langle -3, 1 \rangle = \langle -2, -1 \rangle$

Př.: Zjednodušte zápisy množin:

a) $(A \cap B \cap C) \cup [B \cap (A' \cup C)'] = A \cap B$



b) $[(A \cup B')' \cap C] \cup (A \cap B' \cap C) \cup (A' \cap B' \cap C) \cup [(A' \cup B')' \cap C] =$
 $= [A' \cap B \cap C] \cup (A \cap B' \cap C) \cup (A' \cap B' \cap C) \cup [A \cap B \cap C] = C$



Pozn.: Diagramy z předchozích příkladů se nazývají Vennovy diagramy.

§2. Číselné množiny, zápis čísel, intervaly

Pozn.: Číselné množiny: označení v předchozím paragrafu
vztahy mezi číselnými množinami:

1. $N \subseteq Z \subseteq Q \subseteq R$
2. $I = Q'_R \Rightarrow Q \cup I = R$; I – množina všech iracionálních čísel
3. $Q \cap I = \emptyset$

Pozn.: a) Přirozená čísla zapisujeme pomocí číslic 0,1,2,3,4,5,6,7,8,9.
 b) Každé přirozené číslo má číslicový zápis tvořený skupinou číslic, který chápeme takto: $4503 = 4 \cdot 10^3 + 5 \cdot 10^2 + 0 \cdot 10^1 + 3 \cdot 10^0$
 c) V číslicovém zápisu záleží na poloze (pozici) každé číslice, říkáme, že čísla zapisujeme v desítkové poziční soustavě (v dekadickém pozičním systému).
 d) Velká přirozená čísla budeme zapisovat ve tvaru $a \cdot 10^b$, $1 \leq a < 10$, $b \in N_o$
 Např.: $70000 = 7 \cdot 10^4$, $342000 = 3,42 \cdot 10^5$

Def.: Celá čísla jsou čísla, která vyjadřují počty prvků množin, čísla k nim opačná a číslo 0.

Def.: Racionálním číslem a nazýváme číslo tvaru $a = \frac{p}{q}$, kde $p \in Z$, $q \in N$; p, q jsou nesoudělná ($D(p, q) = 1$).

Pozn.: a) V dekadickém pozičním systému je každé racionální číslo vyjádřeno buď ukončeným desetinným rozvojem nebo neukončeným periodickým rozvojem. Iracionální číslo je vyjádřeno neukončeným neperiodickým rozvojem.
 b) Zápis racionálního čísla zlomkem není jednoznačný. Každé racionální číslo může být zapsáno mnoha zlomky (např.: $0, \bar{3} = \frac{1}{3} = \frac{2}{6} = \dots$).
 c) Iracionální čísla často zapisujeme tak, že udáme číslo menší a větší než uvažované číslo.

$$1 < \sqrt{2} < 2$$

 např.: $1,4 < \sqrt{2} < 1,5$

$$1,41 < \sqrt{2} < 1,42$$

Pozn.: Číselnou osou nazýváme přímku s vyznačeným počátkem a určenou délkovou jednotkou.

Def.: Reálnými čísly nazýváme všechna čísla, která jsou velikostmi úseček (při zvolené jednotkové úsečce), čísla k nim opačná a číslo 0.

Pozn.: Každý bod číselné osy je obrazem právě jednoho reálného čísla a naopak každé reálné číslo je na číselné ose reprezentováno právě jedním bodem.

Př.: Zapište zlomkem v základním tvaru čísla: a) $0,\overline{14}$, b) $2,\overline{536}$.

a) $a = 0,\overline{14} \quad / \cdot 100$

$$100a = 14,\overline{14}$$

Rovnice od sebe odečtu:

$$99a = 14$$

$$a = \frac{14}{99}$$

b) $b = 2,\overline{536} \quad / \cdot 10 \quad / \cdot 1000$

$$10b = 25,\overline{36}$$

$$1000b = 2536,\overline{36}$$

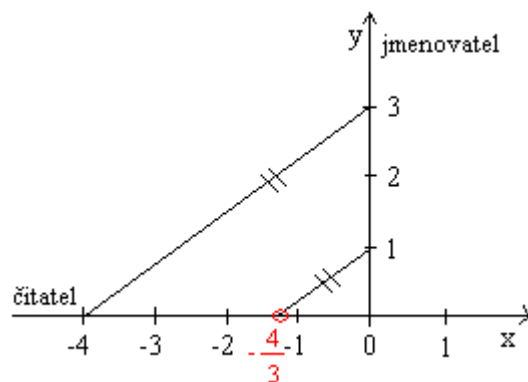
Rovnice od sebe odečtu:

$$990b = 2511$$

$$b = \frac{2511}{990} = \frac{279}{110}$$

Př.: Zakreslete na číselné ose: a) racionální číslo $-\frac{4}{3}$
b) iracionální číslo $\sqrt{3}$

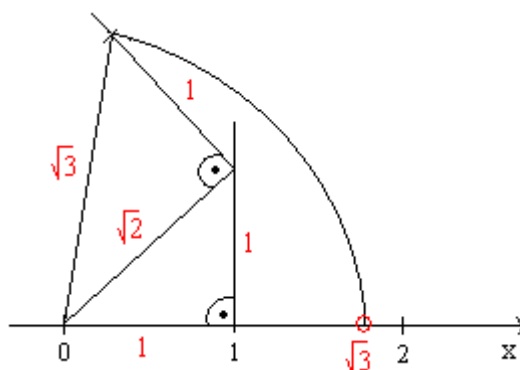
a) $-\frac{4}{3} = \frac{-4}{3} = \frac{-4}{1}$











b)

$$(\sqrt{2})^2 = 1^2 + 1^2$$

$$(\sqrt{3})^2 = (\sqrt{2})^2 + 1^2$$



Def.: Necht' $a, b \in \mathbb{R}, a < b$. Pak následující množiny reálných čísel se nazývají intervaly.

Charakteristická vlastnost prvků intervalu	Symbol intervalu	Znázornění	
$x < a$	$(-\infty, a)$		(1)
$x \leq a$	$(-\infty, a]$		(2)
$a < x < b$	(a, b)		(3)
$a \leq x < b$	$[a, b)$		(4)
$a < x \leq b$	$(a, b]$		(5)
$a \leq x \leq b$	$[a, b]$		(6)
$b < x$	(b, ∞)		(7)
$b \leq x$	$[b, \infty)$		(8)

Interval (6) se nazývá uzavřený, intervaly (1),(3),(7) otevřené, ostatní polouzavřené.

Intervaly (3)-(6) se nazývají omezené (ohraničené), ostatní neomezené (neohraničené).

§3. Výroky a jejich negace

- Pozn.:** a) Výrokem rozumíme každou oznamovací větu, která je buď pravdivá nebo nepravdivá.
 b) Pravdivostní hodnotou výroku rozumíme jednu z jeho kvalit – pravdivost/nepravdivost. (Každý výrok má právě jednu z těchto hodnot.)
 c) Hypotézou (domněnkou) nazýváme výrok, jehož pravdivostní hodnota není známa.

Def.: Negací výroku V nazýváme výrok V' , který má opačnou pravdivostní hodnotu než původní výrok V .

Př.:

Výrok V	Výrok V'
Prší.	Neprší.
Číslo 1 je prvočíslo.	Číslo 1 není prvočíslo.
Mám červený svetr.	Nemám červený svetr.
Kořen této rovnice je kladný.	Kořen této rovnice není kladný.
Kořen této rovnice je záporný není negací výroku V , neboť ještě může nastat možnost „...je roven 0.“	

Pozn.: Vyjadřuje-li výrok V jednu a více možností, které mohou nastat, musí jeho negace V' zahrnout všechny ostatní.

Pozn.: a) Je-li výrok V pravdivý, je výrok V' nepravdivý a naopak.
b) Místo „výrok je pravdivý“ říkáme také „výrok platí“.

Pozn.: V matematice často pracujeme s výroky, které udávají počet objektů – kvantifikované výroky.

Obecný kvantifikovaný výrok: *Pro každé ... platí ...*

\forall - obecný kvantifikátor

Negativní obecný kvantifikovaný výrok: *Pro žádné ... neplatí ...*

Existenční kvantifikovaný výrok: *Existuje alespoň 1 ..., pro které platí ...*

\exists - existenční kvantifikátor

Zesílený existenční kvantifikovaný výrok: *Existuje právě 1 ..., pro které platí ...*

$\exists!$ – zesílený existenční kvantifikátor

Pozn.: Negace kvantifikovaných výroků:

výrok negace	\longleftrightarrow	negace výrok
Každý ... je ...		Alespoň 1 ... není ...
Alespoň 1 ... je ...		Žádný ... není ...
Alespoň n ... je ... ($n > 1$)		Nejvýše $(n-1)$... je ...
Nejvýše n ... je ... ($n \geq 1$)		Alespoň $(n+1)$... je ...

Př.: Negujte následující výroky:

- A: Všichni žáci naší třídy se dobře učí.
A': Aspoň 1 žák naší třídy se neučí dobře.
- B: Aspoň jeden kořen této rovnice není kladný.
B': Každý kořen této rovnice je kladný.
- C: Aspoň 1 číslo z dané množiny je záporné.
C': Žádné číslo z dané množiny není záporné.
- D: Žádný žák naší třídy nenosí brýle.
D': Aspoň 1 žák naší třídy nosí brýle.
- E: V daném čtyřúhelníku jsou alespoň 2 tupé úhly.
E': V daném čtyřúhelníku je nejvýše 1 tupý úhel.
- F: Nejvýše 3 z daných funkcí nejsou lineární.
F': Alespoň 4 z daných funkcí nejsou lineární.
- G: Potkali jsme právě 3 kamarády.
G': Potkali jsme nejvýše 2 nebo alespoň 4 kamarády.
- H: Daná rovnice má právě 1 kořen.
H': Daná rovnice nemá žádný nebo má alespoň 2 kořeny.

Pozn.: Analogie negací výroků a doplňků množin:

Množina A a její doplněk A'	Výrok V a jeho negace V'
-nemají společný prvek v Z	-nezahrnují společný případ
-dohromady zahrnují všechny prvky ze Z	-dohromady zahrnují všechny možné případy
-každý prvek ze Z patří právě do 1 z A a A'	-každý případ je zahrnut právě v 1 z V a V'
$-(A')' = A$	$-(V')' = V$

§4. Složené výroky, operace s výroky

Pozn.: Složeným výrokem rozumíme výrok – souvětí, ve kterém jsou jednotlivé věty spojeny slůvky nebo souslovími, které nazveme logické spojky.

Def.:

Chceme vyjádřit, že	Použijeme spojku	Vytvoříme výrok	Zapisujeme	Název
výrok X neplatí	Není pravda, že ...	Není pravda, že X	X'	<u>Negace</u> výroku X
platí současně oba výroky X, Y	... a ...	X a Y	$X \wedge Y$	<u>Konjunkce</u> výroků X, Y
platí alespoň jeden z výroků X, Y	... nebo ...	X nebo Y	$X \vee Y$	<u>Alternativa</u> výroků X, Y
pokud platí X , pak platí i Y	Jestliže ..., pak	Jestliže X , pak Y	$X \Rightarrow Y$	<u>Implikace</u> výroku Y výrokem X
výroky X, Y mají stejnou pravdivostní hodnotu	... právě tehdy, když ...	X právě tehdy, když Y	$X \Leftrightarrow Y$	<u>Ekvivalence</u> výroků X, Y

Pozn.: a) Spojku „nebo“ chápeme v logice ve významu „alespoň jeden z ...“, tj. nevylučujeme současnou platnost jí spojených výroků.

b) Při implikaci $X \Rightarrow Y$ platnost výroku X není zaručena. Tedy za nepravdivý považujeme pouze případ, kdy výrok X platí a výrok Y neplatí.

Pozn.: Písmena, jež užíváme k označení libovolných výroků, nazýváme výrokové proměnné. Výrazy sestavené z výrokových proměnných, závorek a logických spojek nazýváme výrokové formule.

Pozn.: Je-li výrok X pravdivý, klademe jeho pravdivostní hodnotu 1.
Je-li výrok X nepravdivý, klademe jeho pravdivostní hodnotu 0.

Pozn.: Pravdivostní hodnoty výrokových formulí s jednou logickou spojkou:

X	Y	X'	Y'	$X \wedge Y$	$X \vee Y$	$X \Rightarrow Y$	$X \Leftrightarrow Y$
1	1	0	0	1	1	1	1
1	0	0	1	0	1	0	0
0	1	1	0	0	1	1	0
0	0	1	1	0	0	1	1

Př.: Jestliže svítí lampa, (pak) je vidět na čtení.

- a) Lampa svítí, na čtení je vidět. 1
- b) Lampa svítí, na čtení není vidět. 0
- c) Lampa nesvítí, na čtení je vidět. 1
- d) Lampa nesvítí, na čtení není vidět. 1

Př.: Napište tabulku pravdivostních hodnot výrokové formule $(X \wedge Y) \Rightarrow (X \vee Y)$.

X	Y	$X \wedge Y$	$X \vee Y$	$(X \wedge Y) \Rightarrow (X \vee Y)$
1	1	1	1	1
1	0	0	1	1
0	1	0	1	1
0	0	0	0	1

Pozn.: Výroková formule, která nabývá pravdivostní hodnoty 1 bez ohledu na pravdivostní hodnoty elementárních výroků, se nazývá tautologie.

Př. Dokažte, že výroková formule $[(X \Rightarrow Y) \wedge (Y \Rightarrow X)] \Leftrightarrow (X \Leftrightarrow Y)$ je tautologií.

X	Y	$[(X \Rightarrow Y) \wedge (Y \Rightarrow X)]$	\Leftrightarrow	$(X \Leftrightarrow Y)$
1	1	1	1	1
1	0	0	1	0
0	1	0	1	0
0	0	1	1	1

Pozn.: Formule $X \Leftrightarrow Y$ a $(X \Rightarrow Y) \wedge (Y \Rightarrow X)$ nabývají stejných pravdivostních hodnot, nazýváme je logicky ekvivalentními formulemi. Proto se ekvivalenci někdy též říká oboustranná implikace.

Příklady k §4.:

Př.: Některý z žáků A, B, C rozbil okno. Je zjištěno, že u okna byl v tu chvíli nejvýše jeden z žáků A, B ; žák C byl u okna právě tehdy, když tam nebyl žák A ; když žák B nebyl u okna, nebyl tam ani C . Určete pachatele za předpokladu, že byl právě jeden.

A	B	C	A'	B'	C'	$(A \wedge B)'$	$C \Leftrightarrow A'$	$B' \Rightarrow C'$
1	0	0	0	1	1	1	1	1
0	1	0	1	0	1	1	0	1
0	0	1	1	1	0	1	1	0

Pachatelem byl žák A .

Př.: Na modelu kolejí je možno uvést do pohybu tři vlakové soupravy A, B, C . V daném okamžiku je jejich situace charakterizována formulí $[(A' \vee B') \Rightarrow C] \wedge [(A \vee C) \Rightarrow B']$.

Které soupravy jsou v pohybu?

(X - vlaková souprava X je v pohybu; X' - vlaková souprava X je v klidu)

A	B	C	A'	B'	$(A' \vee B')$	$(A' \vee B') \Rightarrow C$	$(A \vee C)$	$(A \vee C) \Rightarrow B'$	$X \wedge Y$
1	0	0	0	1	1	0	1	1	0
1	0	1	0	1	1	1	1	1	1
1	1	0	0	0	0	1	1	0	0
1	1	1	0	0	0	1	1	0	0
0	1	0	1	0	1	0	0	1	0
0	0	1	1	1	1	1	1	1	1
0	1	1	1	0	1	1	1	0	0
0	0	0	1	1	1	0	0	1	0

V pohybu jsou buď soustavy A a C nebo jen C .

Př.: Dokažte, že výroková formule $[(A \Rightarrow B) \wedge B'] \Rightarrow A'$ je tautologií.

A	B	A'	B'	$A \Rightarrow B$	$(A \Rightarrow B) \wedge B'$	$[(A \Rightarrow B) \wedge B'] \Rightarrow A'$
1	0	0	1	0	0	1
0	1	1	0	1	0	1
1	1	0	0	1	0	1
0	0	1	1	1	1	1

§5. Negace složených výroků. Obměny a obrácení implikací

V.5.1.: Pro každé dva výroky X, Y platí:

- a) Negaci výroku $X \wedge Y$ lze vyjádřit výrokem $X' \vee Y'$.
- b) Negaci výroku $X \vee Y$ lze vyjádřit výrokem $X' \wedge Y'$.
- c) Negaci výroku $X \Rightarrow Y$ lze vyjádřit výrokem $X \wedge Y'$.
- d) Negaci výroku $X \Leftrightarrow Y$ lze vyjádřit výrokem $(X \wedge Y') \vee (X' \wedge Y)$.

[Dk.:

		A							B			
X	Y	X'	Y'	$(X \wedge Y)'$	$X' \vee Y'$	$(X \vee Y)$	$X' \wedge Y'$	$(X \Rightarrow Y)$	$X \wedge Y'$	$(X \Leftrightarrow Y)$	$X' \wedge Y$	$A \vee B$
1	1	0	0	0	0	0	0	0	0	0	0	0
1	0	0	1	1	1	0	0	1	1	1	0	1
0	1	1	0	1	1	0	0	0	0	1	1	1
0	0	1	1	1	1	1	1	0	0	0	0	0

Př.: Negujte následující výroky:

- a) A: Vlakem pojede právě tehdy, když nepojede vhodný autobusový spoj.
A': Vlakem pojede a pojede vhodný autobusový spoj nebo vlakem nepojede a nepojede vhodný autobusový spoj.
- b) B: Bude-li pršet, vezmu si s sebou deštník.
B': Bude pršet a nevezmu si s sebou deštník.
- c) C: Přijedu k vám v sobotu nebo v neděli.
C': Nepřijedu k vám ani v sobotu ani v neděli.
- d) D: Mám žízeň a hlad.
D': Nemám žízeň nebo nemám hlad.

Př.: Napište negace následujících výroků:

- a) A: Každý trolejbus jezdí rychlostí nejvýše 50 km/h.
A': Alespoň jeden trolejbus jezdí rychlostí vyšší než 50 km/h.
- b) B: Bude-li na trhu čerstvé ovoce, nekoupím kompot.
B': Na trhu bude čerstvé ovoce a koupím kompot.
- c) C: Nebude-li na trhu čerstvé ovoce, koupím kompot.
C': Na trhu nebude čerstvé ovoce a nekoupím kompot.
- d) D: Nemám žízeň ani hlad.
D': Mám žízeň nebo hlad.
- e) E: Budu-li obědvat uzené, budu mít pivo.
E': Budu obědvat uzené a nebudu mít pivo.
- f) F: Číslo a je záporné a rovnice má řešení.
F': Číslo a je nezáporné nebo rovnice nemá řešení.
- g) G: Pro každé reálné číslo a platí $a^2 \geq 0$.
G': Existuje reálné číslo a , pro které platí $a^2 < 0$.

Př.: Negujte následující výroky:

- a) A: Přejde-li k nám Věra nebo Zuzana, přijde k nám i Petr.

$$[(V \vee Z) \Rightarrow P]' \Leftrightarrow [(V \vee Z) \wedge P']$$

A': Přejde k nám Věra nebo Zuzana a Petr nepřejde.

- b) B: Přejde-li Věra, pak přijde také Zuzana a Petr.

$$[V \Rightarrow (Z \wedge P)]' \Leftrightarrow [V \wedge (Z \wedge P)'] \Leftrightarrow [V \wedge (Z' \vee P')]$$

B': Věra přijde a alespoň 1 z dvojice Zuzana, Petr nepřejde.

V.5.2.: a) Výrokové formule $X \Rightarrow Y, Y' \Rightarrow X', X' \vee Y$ mají stejnou pravdivostní hodnotu, jsou tedy logicky ekvivalentními formulemi.

- b) Implikace $X \Rightarrow Y, Y \Rightarrow X$ nenabývají vždy týchž pravdivostních hodnot, nejsou tedy logicky ekvivalentními formulemi.

[Dk.:

X	Y	X'	Y'	$X \Rightarrow Y$	$Y' \Rightarrow X'$	$X' \vee Y$	$Y \Rightarrow X$
1	1	0	0	1	1	1	1
1	0	0	1	0	0	0	1
0	1	1	0	1	1	1	0
0	0	1	1	1	1	1	1

Def.: Necht' $X \Rightarrow Y$ je implikace. Pak implikaci $Y \Rightarrow X$ nazýváme obrácením původní implikace a implikaci $Y' \Rightarrow X'$ obměnou původní implikace.

Pozn.: a) Implikaci $X \Rightarrow Y$ můžeme dokázat tak, že místo ní dokážeme její obměnu $Y' \Rightarrow X'$. Hovoříme pak o tzv. nepřímém důkazu.

- b) Je-li dokázána implikace $X \Rightarrow Y$, nelze na základě toho nic říct o pravdivosti obrácené implikace $Y \Rightarrow X$.

Př.: Vytvořte obměny a obrácení daných implikací:

- a) Je-li konstrukce provedena přesně, pak procházejí všechny 3 kružnice jedním bodem.

obměna: Neprocházejí-li všechny 3 kružnice jedním bodem, pak není konstrukce provedena přesně.

obrácení: Procházejí-li všechny 3 kružnice jedním bodem, je konstrukce provedena přesně.

- b) Nejsou-li dané přímky rovnoběžné, pak úloha má alespoň jedno řešení.

obměna: Nemá-li úloha žádné řešení, pak jsou dané přímky rovnoběžné.

obrácení: Má-li úloha alespoň jedno řešení, pak nejsou dané přímky rovnoběžné.

Příklady k §5.:

Na ostrově poctivců a padouchů žijí dvě skupiny obyvatel – **Poctivci**, kteří vždy mluví pravdu a **Padouši**, kteří vždy lžou.

Př.: Cizinec potká tři obyvatele ostrova -A,B,C. Zeptá se obyvatele A: „Jste padouch nebo poctivec?“ A odpoví potichu, takže mu cizinec nerozumí. Zeptá se tedy B: „Co řekl A?“ B odpoví: „A říkal, že je padouch.“ V tom okamžiku C dodá: „Nevěřte B, ten lže!“. Kdo jsou A,B a C?

Nikdo o sobě nikdy nemůže říct, že je padouch, protože kdyby to o sobě řekl poctivec, lhal by, a kdyby to o sobě řekl padouch, mluvil by pravdu. A tedy nemohl říci, že je padouch. Proto **B** musel lhát, když to o A řekl, a tedy je **padouch**. C mluvil pravdu, když říkal, že B lže, a proto je **poctivec**.
O A nelze rozhodnout.

Př.: A řekne: „Já jsem padouch nebo B je poctivec.“ Kdo jsou A a B?

Pokud by A byl padouch, lhal by, tedy by platila negace jeho výroku: „Já jsem poctivec a B je padouch.“ Ta ale neplatí, protože A je padouch. Tato situace tedy nemůže nastat, proto **A** je **poctivec**. Mluví tedy pravdu. První část jeho výroku však není pravdivá, proto musí být pravdivá jeho druhá část (spojka „nebo“), tedy že **B** je **poctivec**.

Př.: A řekne: „Já jsem padouch,ale B je poctivec.“ Kdo jsou A a B?

Pokud by A byl poctivec, lhal by v tom, že je padouch, tedy **A** musí být **padouch**. Lže, platí tedy negace jeho výroku: „Jsem poctivec nebo B je padouch.“ První část výroku neplatí, tedy musí platit alespoň ta druhá – **B** je **padouch**.

Př.: Na ostrov zavítá cizinec a potká tři domorodce A, B a C. A řekne: „Všichni jsme padouši.“, načež B prohlásí: „Právě jeden z nás je poctivec.“ Kdo jsou A,B, a C?

Pokud by A byl poctivec, lhal by, tedy **A** je určitě **padouch**. Musí tedy platit negace jeho výroku: „Alespoň jeden z nás je poctivec.“

Pokud by B byl padouch, musela by platit negace jeho výroku: „Žádný nebo alespoň dva z nás jsou poctivci.“ Ta ale neplatí, protože podle A alespoň jeden z nich poctivcem být musí a alespoň dva být nemohou, protože celkem jsou tři a A a B už jsou padouši. **B** je tedy **poctivec**.

Mluví tedy pravdu – jen jeden z nich je poctivec a to už je sám B, proto **C** musí být **padouch**.

Př.: Uvažme tři obyvatele ostrova A,B,C. A a B pronesou následující výroky:

A: „B je poctivec.“

B: „Pokud A je poctivec, pak je i C poctivcem.“

Kdo jsou A,B,C?

Pokud by A byl padouch, lhal by, tedy i B by byl padouch a musela by platit negace jeho výroku: „A je poctivec a C je padouch.“ Ta ale neplatí, proto **B** je **poctivec**.

A tedy mluví pravdu a je také **poctivcem**.

B mluví pravdu, jeho výrok platí, tedy protože A je poctivec, i **C** je **poctivec**.

§6. Výrokové formy

- Pozn.:** a) Výroková forma je tvrzení obsahující proměnné. Po dosazení konstant za proměnné dostáváme výrok.
 b) Definičním oborem výrokové formy nazýváme množinu D všech takových prvků, po jejichž dosazení přechází výroková forma ve výrok (pro které má výroková forma smysl).
 c) Oborem pravdivosti výrokové formy nazýváme tu podmnožinu P množiny D , pro jejíž prvky přechází výroková forma v pravdivý výrok.

- Pozn.:** a) Výrokovou formu s 1 proměnnou budeme označovat např. $V(x), A(x)$, se 2 proměnnými $V(x, y), A(x, y), \dots$
 Negaci výrokové formy $A(x)$ budeme označovat $A'(x)$.
 b) Obor pravdivosti výrokové formy $A(x)$ označíme P nebo A .
 Obor pravdivosti výrokové formy $A'(x)$ označíme A'_D .

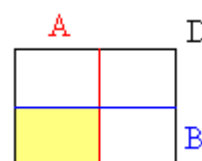
Př.: Určete definiční obor a obor pravdivosti výrokových forem:

- | | | |
|---------------------------------|-------------------|------------------------|
| 1. $V(x) : \frac{1}{x} > 0$ | 2. $V(y) : y = 4$ | 3. $A(a) : a^2 \leq 0$ |
| $D = R \setminus \{0\}$ | $D = R$ | $D = R$ |
| $P = R^+$ | $P = \{4\}$ | $A = \{0\}$ |
| 4. $B(x) : \sqrt{-x^2 - 1} = 3$ | $D = \emptyset$ | $B = \emptyset$ |

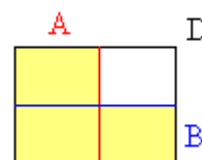
Pozn.: Výrokové formy spojujeme stejnými logickými spojkami jako výroky, užíváme stejné symboly a názvy.

Pozn.: Necht' $A(x), B(x)$ jsou výrokové formy se společným definičním oborem D . Označme A (resp. B) jejich obory pravdivosti. Pak platí:

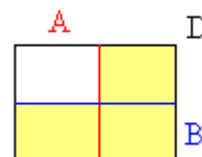
- a) Výroková forma $A(x) \wedge B(x)$ má obor pravdivosti $A \cap B$.



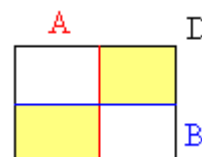
- b) Výroková forma $A(x) \vee B(x)$ má obor pravdivosti $A \cup B$.



- c) Výroková forma $A(x) \Rightarrow B(x)$ má obor pravdivosti $A'_D \cup B$.

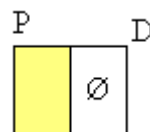


- d) Výroková forma $A(x) \Leftrightarrow B(x)$ má obor pravdivosti $(A \div B)'$.

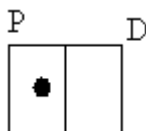


Pozn.: Kvantifikované výrokové formy mají zpravidla tvar $\forall x \in D : V(x)$, $\exists x \in D : V(x)$, kde $V(x)$ je výroková forma s definičním oborem D a oborem pravdivosti P . Množinový význam těchto výrokových forem je tento:

a) $\forall x \in D : V(x) \quad D \subseteq P \wedge P \subseteq D (\text{def.}) \Rightarrow P = D$



b) $\exists x \in D : V(x) \quad P \neq \emptyset$

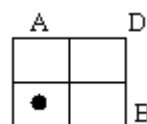


Pozn.: Necht' $A(x)$ ($B(x)$) je výroková forma se společným definičním oborem D a oborem pravdivosti A (B). Pak množinový význam následujících výrokových forem je tento:

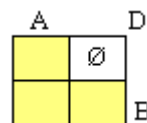
a) $\forall x \in D : A(x) \wedge B(x) \quad P = A \cap B$



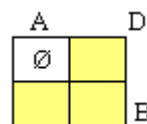
b) $\exists x \in D : A(x) \wedge B(x) \quad A \cap B \neq \emptyset$



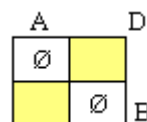
c) $\forall x \in D : A(x) \vee B(x) \quad P = A \cup B$



d) $\forall x \in D : A(x) \Rightarrow B(x) \quad P = A'_D \cup B, A \subseteq B$



e) $\forall x \in D : A(x) \Leftrightarrow B(x) \quad P = (A \cap B) \cup (A'_D \cap B'_D)$
 $A \subseteq B \wedge B \subseteq A \Rightarrow A = B$



Př.: Zapište pomocí symbolů následující výrokové formy:

a) Pro každé reálné číslo b platí: $(b+1)^2 = b^2 + 2b + 1$

$\forall b \in R : (b+1)^2 = b^2 + 2b + 1$

b) Existuje takové reálné číslo m , že platí: $(m+1)^3 = m^3 + 1$

$\exists m \in R : (m+1)^3 = m^3 + 1$

c) Všechna reálná čísla mají nezáporné druhé mocniny.

$\forall x \in R : x^2 \geq 0$

d) Lze nalézt racionální číslo mezi $\frac{1}{98}$ a $\frac{1}{99}$.

$\exists x \in Q : \frac{1}{98} > x > \frac{1}{99}$

e) Některá přirozená čísla jsou větší než 10^{20} .

$$\exists n \in N : n > 10^{20}$$

f) Přirozená čísla jsou sudá nebo lichá.

$$\forall n \in N : (n = 2k) \vee (n = 2k + 1), k \in N$$

Příklady k §6.:

Př.: Jsou dány výrokové formy

$A(n)$: Číslo $3n - 2n^2 - 1$ je přirozené číslo dělitelné pěti

$B(n)$: Číslo $n(n-1) - 5$ je přirozené číslo dělitelné sedmi

Najdi $n \in N$ takové, aby výrok $V(n) = A(n) \vee B(n)$ byl pravdivý.

Výrok $V(n)$ je pravdivý, pokud alespoň jeden z výroků $A(n)$, $B(n)$ je pravdivý.

$A(n)$: $5 \mid 3n - 2n^2 - 1 \Leftrightarrow 3n - 2n^2 - 1 = 5k, k \in N$

$$-2n^2 + 3n - (1 + 5k) = 0$$

$$D = 3^2 - 4 \cdot (-2) \cdot [-(1 + 5k)] = 9 - 8 - 40k = 1 - 40k$$

$$D \geq 0 \Leftrightarrow 1 - 40k \geq 0 \Leftrightarrow k \leq \frac{1}{40}, k \in N - \text{takové } k \text{ neexistuje}$$

Tedy výrok $A(n)$ není pravdivý pro žádné $n \in N$.

$B(n)$: $7 \mid n(n-1) - 5 \Leftrightarrow n(n-1) - 5 = 7l, l \in N$

$$n^2 - n - (5 + 7l) = 0$$

$$D = (-1)^2 - 4 \cdot 1 \cdot [-(5 + 7l)] = 1 + 20 + 28l = 28l + 21$$

$$n_{1,2} = \frac{1 \pm \sqrt{28l + 21}}{2} \Rightarrow n_1 = \frac{1 - \sqrt{28l + 21}}{2} < 0, n_2 = \frac{1 + \sqrt{28l + 21}}{2}$$

Pro $l = 1$ vyjde $n \in N$:

$$n_2 = \frac{1 + \sqrt{28 \cdot 1 + 21}}{2} = \frac{1 + 7}{2} = 4$$

Výrok $B(4)$ je pravdivý $\Rightarrow V(4)$ je pravdivý.

II. Algebraické výrazy, věty, důkazy, mocniny a odmocniny

§1. Algebraické výrazy a jejich úpravy

Pozn.: a) Algebraickým výrazem rozumíme každý zápis, který je správně utvořený podle úmluv o zápisech čísel, proměnných, výsledků operací a hodnot funkcí a závorek.

b) U výrazů obsahujících proměnné musíme uvést obor jednotlivých proměnných.

c) Výrazy budeme označovat symboly $a(x)$, $b(x,y)$,... (v závorce jsou uvedeny všechny proměnné).

Pozn.: Nejběžnějšími výrazy s proměnnou jsou mnohočleny s jednou proměnnou – polynomy – výrazy $a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$, kde x je proměnná, čísla $a_n, a_{n-1}, \dots, a_1, a_0$ koeficienty, číslo n stupeň polynomu (mnohočlenu).

Např.: $7x - 6$, $5x^4 - 3x^2 + 2x - 1$

Pozn.: Dva výrazy s týmiž proměnnými jsou si rovny v dané množině M (společném oboru proměnných), jestliže platí:

1. do obou lze na místa proměnných dosadit symboly všech prvků množiny M
2. oba dávají pro stejné hodnoty proměnných stejné výsledky

Např.: výrazy $a^3 - b^3$, $(a-b)(a^2 + ab + b^2)$ jsou si rovny $\forall a, b \in R$

výrazy $\frac{x}{x}$, 1 si nejsou rovny v množině R , ale jen v množině $R \setminus \{0\}$

Pozn.: a) Úpravy výrazů v dané množině spočívají v tom, že jeden nahradíme druhým, který je mu v této množině roven.

b) Za jednodušší budeme považovat ten výraz, který obsahuje méně znaků operací, funkcí, závorek nebo proměnných.

Pozn.: Základní úpravy:

$$a(b \pm c) = ab \pm ac$$

→
roznásobování

←
vytýkání

$$(a+b)(a-b) = a^2 - b^2$$

roznásobování

rozklad

$$(a \pm b)(a^2 \mp ab + b^2) = a^3 \pm b^3$$

roznásobování

rozklad

$$(a \pm b)^2 = a^2 \pm 2ab + b^2$$

umocňování

úprava na mocninu dvojčlenu

$$(a \pm b)^3 = a^3 \pm 3a^2b + 3ab^2 \pm b^3$$

umocňování

úprava na mocninu dvojčlenu

$$\frac{ac}{bc} = \frac{a}{b}, b \neq 0, c \neq 0$$

krácení

rozšiřování

Pozn.: Se základními úpravami algebraických výrazů jsme se již seznámili.

Nyní se seznámíme s dalšími možnostmi úprav.

A) SUBSTITUTE – nahrazení výrazu, respektive části výrazu $a(x)$, $a(x,y)$ jednou novou proměnnou t

$$\begin{array}{ccc}
 \text{výraz } a(x) & \xrightarrow{\text{substitute}} & \text{výraz } a(t) \\
 & & \downarrow \text{úprava} \\
 \text{upravený výraz } a(x) & \xleftarrow{\text{zp. substitute}} & \text{upravený výraz } a(t)
 \end{array}$$

Př.: Upravte v R výraz $d(x) = (x+16)(x+17)(x+18) - (x+17)^2(x+19)$

$$x+17=t : d(t) = (t-1)t(t+1) - t^2(t+2) = t(t^2-1-t^2-2t) = t(-1-2t) = -t(2t+1)$$

$$d(x) = -(x+17)(2x+34+1) = -(x+17)(2x+35)$$

B) ÚPRAVY DVOJIC VÝRAZŮ - na základě úpravy 1.výrazu upravíme bez řešení 2.výraz

Př.: Upravte výraz V_1 a s využitím tohoto výsledku upravte výrazy V_2 a V_3 :

$$\begin{array}{l}
 V_1 = \left(1 - \frac{2}{a}\right)\left(1 - \frac{2}{a-2}\right) = \frac{a-2}{a} \cdot \frac{a-2-2}{a-2} = \frac{a-4}{a}, (a \neq 0, a \neq 2) \\
 \begin{array}{l} a \rightarrow 2a+1 \\ a \rightarrow 2a \end{array} \quad \begin{array}{l} \curvearrowright \\ \curvearrowright \end{array} \\
 V_2 = \left(1 - \frac{2}{2a+1}\right)\left(1 - \frac{2}{2a-1}\right) = \frac{2a+1-4}{2a+1} = \frac{2a-3}{2a+1}, (a \neq -\frac{1}{2}, a \neq \frac{1}{2}) \\
 V_3 = \left(1 - \frac{1}{a}\right)\left(1 - \frac{1}{a-1}\right) = \frac{2a-4}{2a} = \frac{a-2}{a}, (a \neq 0, a \neq 1)
 \end{array}$$

C) „PRODLUŽOVÁNÍ“ A „ZKRACOVÁNÍ“ VÝRAZŮ - přechod od $V(n)$ k $V(n+1)$ a $V(n-1)$

Pozn.: Předpokládáme, že platí tvrzení, které je vyjádřeno pro každé $i = 1, 2, \dots, n$.

Potřebujeme jej aplikovat na každé $i = 1, 2, \dots, n, n+1$ ($i = 1, 2, \dots, n, n-1$), tzn. přejít od výrazu $V(n)$ k $V(n+1)$ ($V(n-1)$).

Př.: $V(n) : \forall n \in N : \frac{1}{2} \cdot \frac{3}{4} \cdot \frac{5}{6} \cdot \dots \cdot \frac{2n-1}{2n} \leq \frac{1}{\sqrt{3n+1}}$

Zapište tuto nerovnost pro případ, kdy je na levé straně:

a) $n+1$ zlomků: $V(n+1) : \frac{1}{2} \cdot \frac{3}{4} \cdot \frac{5}{6} \cdot \dots \cdot \frac{2n+1}{2n+2} \leq \frac{1}{\sqrt{3n+4}}$

b) $n-1$ zlomků: $V(n-1) : \frac{1}{2} \cdot \frac{3}{4} \cdot \frac{5}{6} \cdot \dots \cdot \frac{2n-3}{2n-2} \leq \frac{1}{\sqrt{3n-2}}$

D) VYČLENĚNÍ VÝRAZU $V(n)$ Z VÝRAZU $V(n+1)$ - vyjádření, jak $V(n+1)$ závisí na $V(n)$

Př.: Ve výrazu $V(n+1)$ vyčleňte daný výraz $V(n)$:

a) $V(n) = n^3 + 2n$

$$\begin{aligned} V(n+1) &= (n+1)^3 + 2n + 2 = n^3 + 3n^2 + 3n + 1 + 2n + 2 = (n^3 + 2n) + 3n^2 + 3n + 3 = \\ &= V(n) + 3(n^2 + n + 1) \end{aligned}$$

b) $V(n) = 16^n - 15n - 1$

$$\begin{aligned} V(n+1) &= 16^{n+1} - 15n - 16 = 16 \cdot 16^n - 15n - 16 = 16 \cdot V(n) + 16 \cdot 15n + 16 - 15n - \\ &- 16 = 16 \cdot V(n) + 225n \end{aligned}$$

c) $V(n) = 2^{4n+1} - 4^n$

$$\begin{aligned} V(n+1) &= 2^{4n+5} - 4^{n+1} = 2^4 \cdot 2^{4n+1} - 4 \cdot 4^n = 16 \cdot V(n) + 16 \cdot 4^n - 4 \cdot 4^n = \\ &= 16 \cdot V(n) + 12 \cdot 4^n \end{aligned}$$

§2. Rovnice a nerovnice s jednou neznámou, soustavy rovnic a nerovnic, výpočet neznámé ze vzorce

Def.: Rovnicí s neznámou $x \in R$ rozumíme každou výrokovou formu tvaru

$L(x) = P(x)$, kde $L(x)$ a $P(x)$ jsou výrazy s proměnnou $x \in R$.

Řešit rovnici znamená stanovit její obor pravdivosti P , tzn. určit všechna taková $c \in R$, po jejichž dosazení ze neznámou přejde rovnice v pravdivý výrok.

Pozn.: Rovnice řešíme pomocí ekvivalentních úprav = úpravy, které nemění obor pravdivosti:

1. úprava výrazů $L(x)$ a $P(x)$ na jedné straně rovnice
2. přičtení nebo odečtení stejného výrazu k oběma stranám rovnice
3. násobení nebo dělení obou stran rovnice stejným číslem různým od nuly (rovnici nenásobíme nebo nedělíme (to nikdy!) výrazem, který obsahuje proměnnou, neboť se může změnit obor pravdivosti P)

Pozn.: Prvky oboru pravdivosti P rovnice nazveme kořeny rovnice a množinu všech kořenů označíme K .

Př.: V R řešte rovnice:

a) $2(3x - 5) = x$	b) $3(x - 2) = x - 2(3 - x)$	c) $(x - 1)x - 1 = (x - 1)^2 + x$
$6x - 10 = x$	$3x - 6 = 3x - 6$	$x^2 - x - 1 = x^2 - 2x + 1 + x$
$5x = 10$	$0x = 0$	$-x - 1 = -x + 1$
$x = 2$	<u>$K = R$</u>	$0x = 2$
<u>$K = \{2\}$</u>		<u>$K = \emptyset$</u>

Def.: Nerovnicí s neznámou $x \in R$ rozumíme každou výrokovou formu zapsanou některým z tvarů $L(x) < P(x)$, $L(x) > P(x)$, $L(x) \leq P(x)$, $L(x) \geq P(x)$, kde $L(x)$ a $P(x)$ jsou výrazy s proměnnou $x \in R$.

Řešit nerovnici znamená stanovit její obor pravdivosti P .

Pozn.: Nerovnice řešíme pomocí ekvivalentních úprav:

1. úprava výrazu $L(x)$ nebo $P(x)$ na jedné straně
2. vzájemná výměna obou stran nerovnice, přitom se znak nerovnosti mění v opačný
3. přičtení nebo odečtení stejného výrazu k oběma stranám rovnice
4. násobení nebo dělení obou stran rovnice stejným číslem různým od nuly (jde-li o číslo záporné, znak nerovnosti se mění v opačný).

Př.: V R řešte nerovnici:

$$\begin{aligned}(x - 3)x &\geq x^2 - 3 \\ x^2 - 3x &\geq x^2 - 3 \\ -3x &\geq -3 \quad / : (-3) \\ \underline{x \leq 1} &\quad \Rightarrow \quad \underline{K = (-\infty, 1]}\end{aligned}$$

Def.: Soustavou rovnic (soustavou nerovnic) s neznámou $x \in R$ rozumíme konjunkci výrokových forem $L_1(x) = P_1(x), L_2(x) = P_2(x), \dots, L_n(x) = P_n(x)$
 $(L_1(x) < P_1(x), L_2(x) < P_2(x), \dots, L_n(x) < P_n(x), L_1(x) \leq P_1(x), \dots, L_n(x) \geq P_n(x))$.
 Řešit soustavu rovnic (soustavu nerovnic) znamená stanovit její obor pravdivosti P , který je roven průniku oborů pravdivosti jednotlivých rovnic (nerovnic).

Př.: V R a Z řešte soustavu nerovnic: $3x - 5(2 - x) \leq 4(2x - 1)$
 $2x - 3(x + 4) < 5x + 6$
 $6x + 2(5 - 3x) \geq x + 7$

$3x - 5(2 - x) \leq 4(2x - 1)$	$2x - 3(x + 4) < 5x + 6$	$6x + 2(5 - 3x) \geq x + 7$
$3x + 5x - 8x \leq -4 + 10$	$2x - 3x - 5x < 6 + 12$	$6x - 6x - x \geq 7 - 10$
$0x \leq 6$	$-6x < 18$	$-x \geq -3$
$\underline{K_1 = R}$	$x > -3$	$x \leq 3$
	$\underline{K_2 = (-3, \infty)}$	$\underline{K_3 = (-\infty, 3]}$

$$\underline{K_R = K_1 \cap K_2 \cap K_3 = (-3, 3)}$$

$$\underline{K_Z = \{-2, -1, 0, 1, 2, 3\}}$$

Pozn.: Nerovnici $A(x) < B(x) < C(x)$ chápeme jako soustavu nerovnic $A(x) < B(x)$.
 $B(x) < C(x)$

Pozn.: a) Rovnici $A(x) \cdot B(x) = 0$ řešíme: buď $A(x) = 0$ nebo $B(x) = 0$
 b) Nerovnici $A(x) \cdot B(x) < 0$ řešíme: $[A(x) > 0 \wedge B(x) < 0] \vee [A(x) < 0 \wedge B(x) > 0]$

Př.: V R řešte nerovnici $x^2 - 5x + 6 \geq 0$:
 $x^2 - 5x + 6 = (x - 2)(x - 3) \geq 0 \Leftrightarrow (x \geq 2 \wedge x \geq 3) \vee (x \leq 2 \wedge x \leq 3)$
 $K_1 = \langle 3, \infty) \quad K_2 = (-\infty, 2]$
 $\underline{K = K_1 \cup K_2 = (-\infty, 2] \cup \langle 3, \infty)}$

Pozn.: Výpočet neznámé ze vzorce provádíme tak, jako bychom řešili rovnici o jedné neznámé, všechny ostatní neznámé považujeme za konstanty.

Př.: a) Ze vzorce pro povrch válce $S = 2\pi r(r + v)$ vyjádřete neznámou v :

$$S = 2\pi r^2 + 2\pi r v \Rightarrow v = \frac{S - 2\pi r^2}{2\pi r} = \frac{S}{2\pi r} - r$$

b) Ze vzorce pro dráhu rovnoměrně zrychleného pohybu $s = \frac{at^2}{2}$

($s_0 = 0m, v_0 = 0ms^{-1}$) vyjádřete neznámou t :

$$s = \frac{at^2}{2} \Rightarrow t^2 = \frac{2s}{a} \Rightarrow t = \underline{\underline{\sqrt{\frac{2s}{a}}}}$$

§3. Matematické věty

Pozn.: Výroky nebo výrokové formy s matematickým obsahem nazýváme matematické věty. Často se týkají prvků jisté množiny D a mívají:

Tvar	Množinový význam
$\forall x \in D : A(x)$	$A = D$
$\exists x \in D : A(x)$	$A \neq \emptyset$
$\forall x \in D : A(x) \Rightarrow B(x)$	$A \subseteq B$
$\forall x \in D : A(x) \Leftrightarrow B(x)$	$A = B$

kde $A(x)$, $B(x)$ jsou výrokové formy s definičním oborem D a oborem pravdivosti A (B).

Def.: Nechť $\forall x \in D : A(x) \Rightarrow B(x)$ je matematická věta. Pak větu $\forall x \in D : B(x) \Rightarrow A(x)$ nazýváme obrácením původní věty, větu $\forall x \in D : B'(x) \Rightarrow A'(x)$ obměnou původní věty a větu $\exists x \in D : A(x) \wedge B'(x)$ negací původní věty.

V.3.1.: a) Matematická věta a její obměna mají stejnou pravdivostní hodnotu.
 b) Matematická věta a její obrácení nemají vždy stejnou pravdivostní hodnotu.
 c) Matematická věta a její negace mají opačnou pravdivostní hodnotu.
 [Dk.: plyne bezprostředně z V.5.2. I.kapitoly a z definice negace]

Pozn.: Matematickou větu $A(x) \Rightarrow B(x)$ můžeme dokázat tak, že místo ní dokážeme její obměnu $B'(x) \Rightarrow A'(x)$. Hovoříme o nepřímém důkazu.

Př.: Vytvořte obměny, obrácení a negace matematických vět:

- a) Kvadrát sudého přirozeného čísla je sudé číslo.
 $\forall n \in N : n = 2k \Rightarrow n^2 = 2l; k, l \in N$
 obměna: $\forall n \in N : n^2 = 2l - 1 \Rightarrow n = 2k - 1; k, l \in N$
 obrácení: $\forall n \in N : n^2 = 2l \Rightarrow n = 2k; k, l \in N$
 negace: $\exists n \in N : n = 2k \wedge n^2 = 2l - 1; k, l \in N$
- b) Součin dvou kladných reálných čísel a, b je kladné číslo.
 $\forall a, b \in R^+ : a > 0 \wedge b > 0 \Rightarrow a \cdot b > 0$
 obměna: $\forall a, b \in R^+ : a \cdot b \leq 0 \Rightarrow a \leq 0 \vee b \leq 0$
 obrácení: $\forall a, b \in R^+ : a \cdot b > 0 \Rightarrow a > 0 \wedge b > 0$
 negace: $\exists a, b \in R^+ : a > 0 \wedge b > 0 \wedge a \cdot b \leq 0$

§4. Základní typy důkazů

Pozn.: Důkazem matematické věty rozumíme úvahu, která ukazuje, že pravdivost matematické věty je logickým důsledkem pravdivosti jiných známých matematických vět nebo axiomů.

1) Přímý důkaz: $A, A \Rightarrow B \dots B$ platí

Jestliže to takto nejde, pak vytvoříme řetězec implikací na sebe navazujících:

$A, A \Rightarrow B_1, B_1 \Rightarrow B_2, \dots, B_{n-1} \Rightarrow B_n, B_n \Rightarrow B \dots B$ platí

Př.: Když n je sudé, je i n^2 sudé, $n \in N$. Dokažte.

$$n \in N, n \text{ je sudé} \Rightarrow \exists k \in N : n = 2k \Rightarrow n^2 = 4k^2 = 2 \cdot (2k^2) = 2m \Rightarrow n^2 \text{ je sudé}$$

2) Nepřímý důkaz: Místo $A \Rightarrow B$ dokazujeme obměnu $B' \Rightarrow A'$.

Př.: Je-li n^2 sudé, je i n sudé, $n \in N$. Dokažte.

obměna: n je liché $\Rightarrow n^2$ je liché, $n \in N$.

$$\begin{aligned} n \text{ je liché} &\Rightarrow \exists k \in N : n = 2k - 1 \Rightarrow n^2 = (2k - 1)^2 = 4k^2 - 4k + 1 = 2 \cdot (2k^2 - 2k) + 1 \Rightarrow \\ &\Rightarrow n^2 = 2m + 1, m \in N_0 \Rightarrow n^2 \text{ je liché} \end{aligned}$$

3) Důkaz sporem: 1. Předpokládáme, že věta V neplatí, tzn. platí její negace V' .

2. Z ní řetězcem implikací odvodíme důsledek Z , který neplatí:

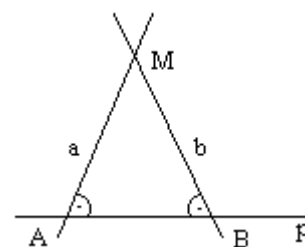
$V' \Rightarrow Z, Z$ neplatí.

3. Tedy věta V' neplatí, tzn. platí V .

Př.: Dokažte, že každým bodem roviny lze vést k dané přímce nejvýše jednu kolmici.

sporem: Existuje bod roviny, jímž lze vést k dané přímce alespoň dvě kolmice.

$\Rightarrow \exists a, b \subseteq \rho : a \perp p$ (p je daná přímka), $b \perp p, a \neq b, M \in a$,
 $M \in b$ (M je daný bod) $\Rightarrow \exists A, B \in p, A \in a \cap p, B \in b \cap p$,
 $A \neq B \Rightarrow \exists \triangle ABM \subseteq \rho : AB \perp AM \wedge BA \perp BM \Rightarrow |\angle MAB| =$
 $= 90^\circ \wedge |\angle MBA| = 90^\circ$ - spor s tím, že součet vnitřních úhlů
v trojúhelníku je 180°



Příklady k §10.:

Př.: $\forall n \in N : n$ -liché $\Rightarrow n^3$ -liché. Dokažte.

$$\begin{aligned} \text{Nechť } n \text{ -liché} &\Rightarrow n = 2k + 1, k \in N_0 \Rightarrow n^3 = (2k + 1)^3 = 8k^3 + 12k^2 + 6k + 1 = \\ &= 2(4k^3 + 6k^2 + 3k) + 1 = 2l + 1, l \in N_0 \Rightarrow n^3 \text{ -liché} \end{aligned}$$

Př.: Dokažte a) nepřímo, b) sporem: $\forall n \in \mathbb{N} : n^3\text{-liché} \Rightarrow n\text{-liché}$.

a) obměna: $\forall n \in \mathbb{N} : n\text{-sudé} \Rightarrow n^3\text{-sudé}$

Nechť $n\text{-sudé} \Rightarrow n = 2k, k \in \mathbb{N} \Rightarrow \underline{n^3} = (2k)^3 = 8k^3 = 2(4k^3) = 2l, l \in \mathbb{N} \Rightarrow n^3\text{-sudé}$

b) sporem: $\exists n \in \mathbb{N} : n^3\text{-liché} \wedge n\text{-sudé}$

Nechť $n\text{-sudé} \Rightarrow n = 2k, k \in \mathbb{N} \Rightarrow \underline{n^3} = (2k)^3 = 8k^3 = 2(4k^3) = 2l, l \in \mathbb{N} \Rightarrow n^3\text{-sudé}$

- spor s předpokladem, že $n^3\text{-liché}$

Př.: Dokažte, že $\sqrt{2}$ je iracionální číslo.

sporem: Nechť $\sqrt{2}$ je racionální číslo $\Rightarrow \exists m, n \in \mathbb{N} : \sqrt{2} = \frac{m}{n}, D(m, n) = 1$

$\sqrt{2} = \frac{m}{n} \Rightarrow 2 = \frac{m^2}{n^2} \Rightarrow \underline{m^2 = 2n^2} \Rightarrow m^2\text{-sudé} \Rightarrow m\text{-sudé}$ (viz důkaz ve 2.př. tohoto

paragrafu) $\Rightarrow \exists p \in \mathbb{N} : \underline{m = 2p} \Rightarrow \underline{m^2 = (2p)^2}$

Z jedenkrát podtržených vztahů plyne: $2n^2 = (2p)^2 \Rightarrow 2n^2 = 4p^2 \Rightarrow n^2 = 2p^2 \Rightarrow$

$\Rightarrow n^2\text{-sudé} \Rightarrow n\text{-sudé}$ (viz výše) $\Rightarrow \exists q \in \mathbb{N} : \underline{n = 2q}$

Z dvakrát podtržených vztahů plyne, že m, n jsou dělitelná dvěma, tedy soudělná, což je spor s předpokladem, že jsou nesoudělná.

Př.: Dokažte, že číslo utvořené z rozdílu třetí mocniny přirozeného čísla n a tohoto čísla je dělitelné šesti:

$n^3 - n = n(n^2 - 1) = (n - 1)n(n + 1)$ - 3 po sobě jdoucí přirozená čísla, z nichž právě jedno je dělitelné třemi a alespoň jedno dělitelné dvěma, tedy celý výraz je dělitelný třemi a zároveň dvěma. Protože 3 a 2 jsou čísla nesoudělná, je celý výraz dělitelný šesti.

Př.: Dokažte, že součet dvou dvouciferných přirozených čísel, které se liší jen pořadím cifer, je dělitelný 11.

1. číslo: $10x + y$

2. číslo: $10y + x$

$10x + y + 10y + x = 11x + 11y = 11(x + y) \Rightarrow 11 \mid V(x, y)$

§5. Důkaz matematickou indukcí

Pozn.: Matematickou indukcí dokazujeme věty typu $\forall n \in N : V(n)$.

V.5.1: Princip matematické indukce:

Nechť $V(n)$ je tvrzení, které máme dokázat pro $\forall n \in N$. Dokážeme-li:

1) $V(1)$ (tzn. pro $n = 1$ výrok platí)

2) $\forall n \in N : V(n) \Rightarrow V(n+1)$,

pak můžeme uzavřít, že tvrzení $V(n)$ platí pro $\forall n \in N$.

Pozn.: a) Důkaz matematickou indukcí se skládá ze dvou částí – tzv. prvního kroku (1)) a indukčního kroku (2)).

b) Předpoklad, že výrok platí pro n ($V(n)$), se nazývá indukční předpoklad.

[Dk. V.5.1.: sporem: Nechť existuje alespoň jedno n , pro které $V(n)$ neplatí. Označme M množinu všech n , pro které $V(n)$ neplatí, $M \neq \emptyset$.

Označme n_0 nejmenší prvek množiny M . Platí: $n_0 > 1$ (pro $n = 1$ $V(1)$ platí podle prvního kroku) $\Rightarrow n_0 - 1 \in N$. Protože n_0 je nejmenší prvek M , tvrzení $V(n_0 - 1)$ platí.

Protože podle 2) platí implikace $V(n_0 - 1) \Rightarrow V(n_0)$, $V(n_0)$ platí – spor.]

Př.!: Dokažte matematickou indukcí: $\forall n \in N : 1 + 2 + 3 + \dots + n = \frac{n(n+1)}{2}$

$$1) n = 1 : L = 1, P = \frac{1(1+1)}{2} = 1 \Rightarrow L = P$$

$$2) \forall n \in N : 1 + 2 + 3 + \dots + n = \frac{n(n+1)}{2} \Rightarrow 1 + 2 + 3 + \dots + n + (n+1) = \frac{(n+1)(n+2)}{2}$$

(to máme dokázat)

$$\frac{1 + 2 + 3 + \dots + n + (n+1)}{2} = \frac{n(n+1)}{2} + n + 1 = (n+1)\left(\frac{n}{2} + 1\right) = \frac{(n+1)(n+2)}{2}$$

$$\forall n \in N : 1 + 2 + 3 + \dots + n = \frac{n(n+1)}{2}$$

Př.: Je dáno schéma

		1					
	1	2	1				
	1	2	3	2	1		
	1	2	3	4	3	2	1

Zkoumejte součty v jednotlivých řádcích, vyslovte hypotézu o součtu v k -tém řádku a ověřte ji.

Hypotéza: v k -tém řádku bude součet $S_k = k^2$

Hypotézu nyní dokážeme matematickou indukcí:

1) $k = 1 : S_1 = 1^2 = 1$ platí

2) $\forall k \in N : S_k = k^2 \Rightarrow S_{k+1} = (k+1)^2$

$\begin{array}{ccccccc} & & & & k-1 & k & k-1 & & \\ & & & & \text{...} & \text{...} & \text{...} & & \\ & & & & k-1 & k & k+1 & k & k-1 & \text{...} \\ & & & & \text{...} & \text{...} & \text{...} & & \text{...} & \end{array}$

$\begin{array}{cc} \text{v } (k+1)\text{-ním přibude} & k+1 \quad k \end{array}$

$$\underline{S_{k+1}} = S_k + (k+1) + k = k^2 + 2k + 1 = \underline{(k+1)^2}$$

Př.: Dokažte: $\forall n \in \mathbb{N} : 1^2 - 2^2 + 3^2 - 4^2 + \dots + (-1)^{n-1} \cdot n^2 = (-1)^{n-1} \cdot \frac{n(n+1)}{2}$

$$1) \ n = 1 : L = 1, P = (-1)^0 \cdot \frac{2}{2} = 1 \Rightarrow L = P$$

$$2) \ \forall n \in \mathbb{N} : 1^2 - 2^2 + 3^2 - 4^2 + \dots + (-1)^{n-1} \cdot n^2 = (-1)^{n-1} \cdot \frac{n(n+1)}{2} \Rightarrow$$

$$\Rightarrow 1^2 - 2^2 + 3^2 - 4^2 + \dots + (-1)^{n-1} \cdot n^2 + (-1)^n \cdot (n+1)^2 = (-1)^n \cdot \frac{(n+1)(n+2)}{2}$$

$$\frac{1^2 - 2^2 + \dots + (-1)^{n-1} \cdot n^2 + (-1)^n \cdot (n+1)^2}{-1} = (-1)^{n-1} \cdot \frac{n(n+1)}{2} + (-1)^n \cdot (n+1)^2 =$$

$$= \frac{(-1)^n}{-1} \cdot \frac{n(n+1)}{2} + (-1)^n \cdot (n+1)^2 = (-1)^n \cdot (n+1) \cdot \left(-\frac{n}{2} + n + 1 \right) =$$

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

§6. Mocniny s celočíselnými exponenty

Pozn.: V dosavadních úvahách byly exponenty mocnin přirozená čísla. Rozšíříme nyní pojem mocniny tak, že exponent bude 0 nebo záporné číslo.

Mocniny $a^0, a^{-1}, a^{-2}, \dots$ definujeme tak, aby zůstaly v platnosti věty o mocninách s přirozenými exponenty, zejména věta:

$$\forall a \in R, \forall n \in N : a^1 = a, a^{n+1} = a^n \cdot a,$$

která vychází z definice mocniny a^n jakou součinu n činitelů rovných a :

$$\forall a \in R, \forall n \in N : a^n \equiv \underbrace{a \cdot a \cdot \dots \cdot a}_n$$

$$a^{n+1} = a^n \cdot a$$

$$a^{-1+1} = a^{-1} \cdot a$$

$$a^{0+1} = a^0 \cdot a$$

$$1 = a^{-1} \cdot a \Rightarrow a^{-1} = \frac{1}{a}$$

$$a = a^0 \cdot a$$

$$a^{-2} = \frac{1}{a^2}$$

$$\bullet \quad a = 0 \Rightarrow a^0 \text{ nedefinujeme}$$

$$a^{-k} = \frac{1}{a^k}$$

$$\bullet \quad a \neq 0 \Rightarrow \underline{a^0 = 1}$$

Def.: $\forall a \in R \setminus \{0\}, \forall k \in Z, k \leq 0 : a^0 \equiv 1$

$$a^k \equiv \frac{1}{a^{-k}}$$

V.6.1: $\forall a, b \in R \setminus \{0\}, \forall r, s \in Z :$ a) $a^{-r} = \frac{1}{a^r}$

$$\text{b) } a^r \cdot a^s = a^{r+s}$$

$$\text{c) } \frac{a^r}{a^s} = a^{r-s}$$

$$\text{d) } (a^r)^s = a^{r \cdot s}$$

$$\text{e) } (a \cdot b)^r = a^r \cdot b^r$$

$$\text{f) } \left(\frac{a}{b} \right)^r = \frac{a^r}{b^r}$$

[Dk.: a) plyne přímo z definice

b) 1. Předpokládáme platnost věty pro $r, s \in N$ (dokáže se přímo z definice mocniny):

$$a^r \cdot a^s = \underbrace{a \cdot a \cdot \dots \cdot a}_r \cdot \underbrace{a \cdot a \cdot \dots \cdot a}_s = \underbrace{a \cdot a \cdot \dots \cdot a}_{r+s} = a^{r+s}$$

$$2. \quad r > 0, s < 0 \Rightarrow -s > 0, r - s > 0$$

$$a^r \cdot a^s = a^r \cdot \frac{1}{a^{-s}} = \frac{a^r}{a^{-s}} = a^{r-(-s)} = a^{r+s}$$

$$3. \quad r < 0, s > 0 \Rightarrow \text{analogicky}$$

$$4. r < 0, s < 0 \Rightarrow -s > 0 \wedge -r > 0$$

$$a^r \cdot a^s = \frac{1}{a^{-r}} \cdot \frac{1}{a^{-s}} = \frac{1}{a^{-r} \cdot a^{-s}} = \frac{1}{a^{-r-s}} = \frac{1}{a^{-(r+s)}} = a^{r+s}$$

$$5. r = 0 \Rightarrow a^r \cdot a^s = a^0 \cdot a^s = 1 \cdot a^s = a^s = a^{0+s} = a^{r+s}$$

$$6. s = 0 \Rightarrow \text{analogicky}$$

c)- f) podobně jako b)]

Př.: Vypočtete a vyjádřete desetinným číslem:

$$\frac{(3 \cdot 10^{-3})^{-2}}{3^{-1} \cdot (10^2)^{-1}} = \frac{3^{-2} \cdot 10^6}{3^{-1} \cdot 10^{-2}} = 3^{-1} \cdot 10^8 = \frac{100000000}{3} = \underline{\underline{33333333,3}}$$

Příklady k §6.:

Př.: Zjednodušte:

$$a) \frac{5^{-3} + 2^{-3}}{5^{-3} \cdot 2^{-3}} = \frac{\frac{1}{5^3} + \frac{1}{2^3}}{\frac{1}{5^3 \cdot 2^3}} = \frac{2^3 + 5^3}{5^3 \cdot 2^3} \cdot \frac{5^3 \cdot 2^3}{1} = 2^3 + 5^3 = \underline{\underline{133}}$$

$$b) \frac{5^{-2}}{\left(\frac{1}{5}\right)^4 \cdot 25^{-6}} = \frac{\frac{1}{5^2}}{\frac{1}{25^2} \cdot \frac{1}{25^6}} = \frac{1}{5^2} \cdot \frac{25^8}{1} = \underline{\underline{25^7}}$$

$$c) (2^{-5} + 5^{-2})(5^2 - 2^5) = \frac{5^2}{2^5} - \frac{2^5}{2^5} + \frac{5^2}{5^2} - \frac{2^5}{5^2} = \frac{5^2}{2^5} - \frac{2^5}{5^2} = \frac{25 - 32}{32 - 25} = \frac{-7}{7} = \underline{\underline{-1}}$$

$$\begin{aligned} d) (x^{-1} - y^{-1})^{-1}(x^4 - y^4) &= \left(\frac{1}{x} - \frac{1}{y}\right)^{-1} (x^2 + y^2)(x^2 - y^2) = \\ &= \left(\frac{y-x}{xy}\right)^{-1} (x^2 + y^2)(x+y)(x-y) = \frac{xy}{y-x} (x^2 + y^2)(x+y)(x-y) = \\ &= \underline{\underline{-xy(x^2 + y^2)(x+y)}} \quad (x \neq 0, y \neq 0, x \neq y) \end{aligned}$$

$$e) (x^3y - xy^3)x^{-1}y^{-1} = x^2y^0 - x^0y^2 = x^2 - y^2 = \underline{\underline{(x+y)(x-y)}} \quad (x, y \neq 0)$$

$$\begin{aligned} f) (x^{-1} + y^{-1})^2 : (x^{-3}y^{-2} + x^{-2}y^{-3}) &= \frac{x^{-2} + 2x^{-1}y^{-1} + y^{-2}}{x^{-3}y^{-2} + x^{-2}y^{-3}} = \frac{x^3y^2 + x^2y^3}{x^2 + 2xy + y^2} = \\ &= \frac{x^2y^2(x+y)}{(x+y)^2} = \underline{\underline{\frac{x^2y^2}{x^2y^2}}} \quad (x, y \neq 0, x \neq -y) \end{aligned}$$

§7. Mocniny s racionálními exponenty

Def.: Necht' $a \in R_0^+$. Druhou odmocninou čísla a nazveme to nezáporné číslo $x \in R_0^+$, pro něž platí: $x^2 = a$ a zapisujeme $\sqrt{a} = x$.

Pozn.: Platí tedy např. $\sqrt{9} = 3$, nikdy $\sqrt{9} = \pm 3$.

Pozn.: Zřejmě platí $\sqrt{a} \cdot \sqrt{a} = a^1$. Chápeme-li tedy \sqrt{a} jako mocninu a^r , musí platit $a^r \cdot a^r = 1 \Rightarrow 2r = 1 \Rightarrow r = \frac{1}{2}$. Druhou odmocninu lze chápat jako mocninu s exponentem $\frac{1}{2}$, kterou definujeme pro nezáporný základ a .

<p>V.7.1: $\forall a, b \in R_0^+; \forall n \in N$: a) $(\sqrt{a})^2 = a$</p> <p style="text-align: center;">$\sqrt{a^2} = a$</p> <p>b) $\sqrt{a} \cdot \sqrt{b} = \sqrt{a \cdot b}$</p> <p>c) $b \neq 0$: $\frac{\sqrt{a}}{\sqrt{b}} = \sqrt{\frac{a}{b}}$</p> <p>d) $a \cdot \sqrt{b} = \sqrt{a^2 b}$</p> <p>e) $\sqrt{a^{2n}} = a^n$</p> <p>f) $\sqrt{a^{-2n}} = a^{-n}$</p>	<p>$(a^{\frac{1}{2}})^2 = a$</p> <p>$(a^2)^{\frac{1}{2}} = a$</p> <p>$a^{\frac{1}{2}} \cdot b^{\frac{1}{2}} = (a \cdot b)^{\frac{1}{2}}$</p> <p>$\frac{a^{\frac{1}{2}}}{b^{\frac{1}{2}}} = \left(\frac{a}{b}\right)^{\frac{1}{2}}$</p> <p>$a \cdot b^{\frac{1}{2}} = (a^2 b)^{\frac{1}{2}}$</p> <p>$(a^{2n})^{\frac{1}{2}} = a^n$</p> <p>$(a^{-2n})^{\frac{1}{2}} = a^{-n}$</p>
----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

[Dk.: b) Označme $\sqrt{a} = x, \sqrt{b} = y \Rightarrow a = x^2, b = y^2 \Rightarrow ab = x^2 y^2 = (xy)^2 \Rightarrow \sqrt{ab} = \sqrt{(xy)^2} = xy = \sqrt{a} \cdot \sqrt{b}$
ostatní obdobně]

Př.: Odstraňte odmocniny ze jmenovatele:

a) $\frac{1}{2\sqrt{x}} = \frac{1}{2\sqrt{x}} \cdot \frac{\sqrt{x}}{\sqrt{x}} = \frac{\sqrt{x}}{2x}, x > 0$

b) $\frac{1}{\sqrt{6}-\sqrt{5}} = \frac{1}{\sqrt{6}-\sqrt{5}} \cdot \frac{\sqrt{6}+\sqrt{5}}{\sqrt{6}+\sqrt{5}} = \frac{\sqrt{6}+\sqrt{5}}{6-5} = \underline{\underline{\sqrt{6}+\sqrt{5}}}$

c) $\frac{x-4y}{\sqrt{x}-2\sqrt{y}} = \frac{x-4y}{\sqrt{x}-2\sqrt{y}} \cdot \frac{\sqrt{x}+2\sqrt{y}}{\sqrt{x}+2\sqrt{y}} = \frac{x\sqrt{x}-4y\sqrt{x}-8y\sqrt{y}+2x\sqrt{y}}{x-4y} =$
 $= \frac{\sqrt{x}(x-4y)+2\sqrt{y}(x-4y)}{x-4y} = \underline{\underline{\sqrt{x}+2\sqrt{y}}}, x \geq 0, y \geq 0, x \neq 4y$

Pozn.: Odstraňování odmocniny ze jmenovatele se nazývá usměrňování zlomků.

Def.: Necht' $a \in R_0^+, n \in N, n \geq 2$. n -tou odmocninou čísla a nazveme to nezáporné číslo $x \in R_0^+$, pro něž platí: $x^n = a$ a zapisujeme $\sqrt[n]{a} = x$.

Pozn.: a) n -tou odmocninu lze chápat jako mocninu s racionálním exponentem:

$$\sqrt[n]{a} = a^{\frac{1}{n}}, a \in R_0^+$$

b) Význam mocniny $a^{\frac{m}{n}}, \frac{m}{n} \in Q$: $a^{\frac{m}{n}} = (\sqrt[n]{a})^m = \sqrt[n]{a^m}$. Tuto mocninu definujeme jen pro $a \in R^+$.

V.7.2: $\forall a, b \in R^+; \forall r, s \in Q$: a) $a^r \cdot a^s = a^{r+s}$

$$b) \frac{a^r}{a^s} = a^{r-s}$$

$$c) (a^r)^s = a^{r \cdot s}$$

$$d) (a \cdot b)^r = a^r \cdot b^r$$

$$e) \left(\frac{a}{b}\right)^r = \frac{a^r}{b^r}$$

Pozn.: Rozšíření oboru exponentu si vyžádalo zúžení oboru základu mocniny.

- exponent přirozený – základ libovolný
- exponent celočíselný – základ $\neq 0$
- exponent racionální – základ obecně kladný (exponent kladný racionální – základ nezáporný)

Př.: Zjednodušte:

$$a) \left(\frac{125}{8}\right)^{-\frac{2}{3}} = \left(\frac{8}{125}\right)^{\frac{2}{3}} = \left[\left(\frac{2}{5}\right)^3\right]^{\frac{2}{3}} = \left(\frac{2}{5}\right)^2 = \frac{4}{25}$$

$$b) \sqrt[5]{\left(\frac{\sqrt{x} : x}{\sqrt[3]{x}}\right)^{-3}} = \left(\frac{x^{\frac{1}{2}} \cdot x^{-1}}{x^{\frac{1}{3}}}\right)^{-\frac{3}{5}} = \left(x^{-\frac{5}{6}}\right)^{-\frac{3}{5}} = x^{\frac{1}{2}} = \underline{\underline{\sqrt{x}}}, x > 0$$

$$\begin{aligned} c) & \left(\frac{x\sqrt{x} + y\sqrt{y}}{\sqrt{x} + \sqrt{y}} - \sqrt{xy}\right) : (x - y) + \frac{2\sqrt{y}}{\sqrt{x} + \sqrt{y}} = \frac{x\sqrt{x} + y\sqrt{y} - \sqrt{xy}(\sqrt{x} + \sqrt{y})}{\sqrt{x} + \sqrt{y}} \cdot \frac{1}{x - y} + \\ & + \frac{2\sqrt{y}}{\sqrt{x} + \sqrt{y}} = \frac{x\sqrt{x} + y\sqrt{y} - x\sqrt{y} - y\sqrt{x}}{\sqrt{x} + \sqrt{y}} \cdot \frac{1}{x - y} + \frac{2\sqrt{y}}{\sqrt{x} + \sqrt{y}} = \\ & = \frac{x(\sqrt{x} - \sqrt{y}) + y(\sqrt{y} - \sqrt{x})}{(\sqrt{x} + \sqrt{y})(x - y)} + \frac{2\sqrt{y}}{\sqrt{x} + \sqrt{y}} = \frac{(\sqrt{x} - \sqrt{y})(x - y)}{(\sqrt{x} + \sqrt{y})(x - y)} + \frac{2\sqrt{y}}{\sqrt{x} + \sqrt{y}} = \\ & = \frac{\sqrt{x} - \sqrt{y} + 2\sqrt{y}}{\sqrt{x} + \sqrt{y}} = \frac{\sqrt{x} + \sqrt{y}}{\sqrt{x} + \sqrt{y}} = \underline{\underline{1}} \quad (x, y \geq 0, x \neq y) \end{aligned}$$

III. Teorie čísel

§1. Základní pojmy teorie čísel

Def.: Necht' $a, b \in \mathbb{Z}$. Říkáme, že číslo a dělí číslo b (a je dělitelem b , b je dělitelné a , b je násobek a), jestliže $\exists c \in \mathbb{Z} : b = a \cdot c$; zapisujeme $a \mid b$.
 $a \mid b \Leftrightarrow \exists c \in \mathbb{Z} : b = a \cdot c$
 V opačném případě (tzn. když žádné takové $c \in \mathbb{Z}$ neexistuje) říkáme, že číslo a nedělí číslo b a píšeme $a \nmid b$.

Pozn.: Přímo z definice plyne: $\forall c \in \mathbb{Z} : c \mid 0$ (protože $0 = c \cdot 0$). Naopak číslo 0 je dělitelem pouze 0 a žádného jiného celého čísla.

Def.: Necht' $a \in \mathbb{Z}$. Absolutní hodnotu čísla a označujeme $|a|$ a definujeme takto:

1. $a > 0 \Rightarrow |a| = a$
2. $a = 0 \Rightarrow |a| = 0$
3. $a < 0 \Rightarrow |a| = -a$

Pozn.: $\forall a \in \mathbb{Z} : |a| \geq 0$

V.1.1: $\forall a, b, c \in \mathbb{Z} :$ a) $a \mid a, 1 \mid a$

$$\text{b) } a \mid b \wedge b \mid a \Rightarrow |a| = |b|$$

$$\text{c) } a \mid b \wedge b \mid c \Rightarrow a \mid c$$

[Dk.: a) $\forall a \in \mathbb{Z} : a = a \cdot 1 \Rightarrow a \mid a \wedge 1 \mid a$

b) Necht' $a \mid b \wedge b \mid a \Rightarrow \exists c, d \in \mathbb{Z} : b = a \cdot c, a = b \cdot d \Rightarrow b = a \cdot c = b \cdot d \cdot c \Rightarrow d \cdot c = 1 \Rightarrow$
 $\Rightarrow c = d = 1 \vee c = d = -1 \Rightarrow a = b \vee a = -b \Rightarrow |a| = |b|$

c) Necht' $a \mid b \wedge b \mid c \Rightarrow \exists e, f \in \mathbb{Z} : b = a \cdot e \wedge c = b \cdot f \Rightarrow c = b \cdot f = a \cdot e \cdot f =$
 $= a \cdot m, m \in \mathbb{Z} \Rightarrow c = a \cdot m \Rightarrow a \mid c]$

Pozn.: Jsou-li speciálně $a, b \in \mathbb{N} : a \mid b \wedge b \mid a \Rightarrow a = b$.

V.1.2: $\forall a, b \in \mathbb{Z} : b \neq 0 \wedge a \mid b \Rightarrow |a| \leq |b|$

[Dk.: Necht' $a \mid b \Rightarrow \exists c \in \mathbb{Z} : b = a \cdot c \Rightarrow |b| = |a \cdot c| = |a| \cdot |c|$
 $b \neq 0 \Rightarrow |b| \neq 0 \Rightarrow |a| \neq 0 \wedge |c| \neq 0 \Rightarrow |c| \geq 1 \Rightarrow |a| \leq |b|]$

V.1.3: Necht' $\forall a, b, c \in \mathbb{Z} \wedge a \mid b$. Pak platí:

- 1) $a \mid (b + c) \Leftrightarrow a \mid c$
- 2) $a \mid (b - c) \Leftrightarrow a \mid c$

[Dk.: 1) „ \Rightarrow “: Necht' $a \mid b \wedge a \mid (b+c) \Rightarrow \exists e, f \in \mathbb{Z} : b = a \cdot e \wedge b+c = a \cdot f \Rightarrow$
 $\Rightarrow c = a \cdot f - b = a \cdot f - a \cdot e = a(f-e) = a \cdot m, m \in \mathbb{Z} \Rightarrow a \mid c$
 „ \Leftarrow “: Necht' $a \mid b \wedge a \mid c \Rightarrow \exists e, f \in \mathbb{Z} : b = a \cdot e \wedge c = a \cdot f \Rightarrow b+c = a \cdot e + a \cdot f =$
 $= a(e+f) = a \cdot n, n \in \mathbb{Z} \Rightarrow a \mid (b+c)$
 2) analogicky]

V.1.4: Věta o dělení se zbytkem:

Necht' $a \in \mathbb{Z}, b \in \mathbb{N}$. Pak $\exists ! q \in \mathbb{Z}, r \in \mathbb{N}_0 : a = b \cdot q + r, 0 \leq r < b$.

[Dk.: a) existence: Mezi všemi násobky čísla b vybereme takový násobek $q \cdot b$, že platí:
 $q \cdot b \leq a < (q+1)b$ (číslo $q \cdot b$ je nejbližší menší, číslo $(q+1) \cdot b$ nejbližší větší
 násobek čísla b vzhledem k a). Označme $r = a - bq \Rightarrow a = bq + r, 0 \leq r < b$.
 b) jednoznačnost: sporem: Necht' $a = bq + r, 0 \leq r < b \wedge a = bq' + r', 0 \leq r' < b$. Pak platí:
 $bq - bq' = r' - r \Rightarrow b(q - q') = r' - r \Rightarrow b \mid (r' - r)$. Necht' např. $r' \geq r \Rightarrow$ protože
 $0 \leq r' - r < b \wedge b \mid (r' - r)$, platí $r' - r = 0 \Rightarrow r = r' \Rightarrow q = q'$]

Def.: Necht' čísla q, r vyhovují požadavkům V.1.4. Pak q se nazývá neúplný podíl a r zbytek po dělení čísla a číslem b .

Př.: Vyjádřete ve tvaru podle V.1.4., určete q, r .

- a) $a = 60, b = 8$: $60 = 8 \cdot 7 + 4$ $q = 7, r = 4$
 b) $a = -60, b = 8$: $-60 = 8 \cdot (-8) + 4$ $q = -8, r = 4$
 c) $a = -56, b = 11$: $-56 = 11 \cdot (-6) + 10$ $q = -6, r = 10$

Pozn.: $b \mid a \Leftrightarrow r = 0$

Důkazy o dělitelnosti:

Př.!: Dokažte: $\forall a \in \mathbb{Z} : 3 \mid (a^3 - a)$.

Jde o příklad malé Fermatovy věty pro $p = 3$ - obecně:

$\forall a \in \mathbb{Z}, \forall p \in \mathbb{N}, p$ - prvočíslo: $p \mid (a^p - a)$

I. způsob – obecný postup: Označme $V(a) = a^3 - a$

- $a = 3k, k \in \mathbb{Z} \Rightarrow V(a) = (3k)^3 - 3k = 27k^3 - 3k = 3(9k^3 - k) \Rightarrow 3 \mid V(a)$
 - $a = 3k+1, k \in \mathbb{Z} \Rightarrow V(a) = (3k+1)^3 - (3k+1) = 27k^3 + 27k^2 + 9k + 1 - 3k - 1 =$
 $= 3(9k^3 + 9k^2 + 2k) \Rightarrow 3 \mid V(a)$
 - $a = 3k+2, k \in \mathbb{Z} \Rightarrow V(a) = (3k+2)^3 - (3k+2) = 3 \cdot 9k^3 + 3 \cdot 18k^2 + 3 \cdot 12k + 8 - 3k - 2 =$
 $= 3(9k^3 + 18k^2 + 11k + 2) \Rightarrow 3 \mid V(a)$
- Tedy $\forall a \in \mathbb{Z} : 3 \mid (a^3 - a)$.

II. způsob – úvahou přes rozklad:

$a^3 - a = a(a^2 - 1) = (a-1)a(a+1)$ - 3 po sobě jdoucí přirozená čísla, z nichž právě jedno je dělitelné třemi, tedy celý výraz je dělitelný třemi.

Př.: Dokažte: $\forall n \in N : 8 \mid ((2n+1)^2 - 1)$

$(2n+1)^2 - 1 = 4n^2 + 4n + 1 - 1 = 4n(n+1) - 2$ po sobě jdoucí čísla, tudíž právě jedno z nich je dělitelné 2 $\Rightarrow 4n(n+1) = 4 \cdot 2k, k \in N = 8k \Rightarrow 8 \mid ((2n+1)^2 - 1)$

Př.: Dokažte: $\forall n \in N : 6 \mid (n^3 + 11n)$.

- $n = 3k, k \in N \Rightarrow V(n) = (3k)^3 + 11(3k) = 27k^3 + 33k = 3(9k^3 + 11k) \Rightarrow 3 \mid V(n)$
- $n = 3k + 1, k \in N \Rightarrow V(n) = (3k+1)^3 + 11(3k+1) = 27k^3 + 27k^2 + 9k + 1 + 33k + 11 = 3(9k^3 + 9k^2 + 14k + 4) \Rightarrow 3 \mid V(n)$
- $n = 3k - 1, k \in N \Rightarrow V(n) = (3k-1)^3 + 11(3k-1) = 27k^3 - 27k^2 + 9k - 1 + 33k - 11 = 3(9k^3 - 9k^2 + 14k - 4) \Rightarrow 3 \mid V(n)$
- $n = 2k, k \in N \Rightarrow V(n) = (2k)^3 + 11(2k) = 8k^3 + 22k = 2(4k^3 + 11k) \Rightarrow 2 \mid V(n)$
- $n = 2k + 1, k \in N \Rightarrow V(n) = (2k+1)^3 + 11(2k+1) = 8k^3 + 12k^2 + 6k + 1 + 22k + 11 = 2(4k^3 + 6k^2 + 14k + 6) \Rightarrow 2 \mid V(n)$

$3 \mid V(n) \wedge 2 \mid V(n) \Rightarrow 6 \mid V(n)$, neboť čísla 2 a 3 jsou nesoudělná

Př.: Dokažte: $\forall n \in N : 7 \mid (2^{3n} - 1)$

MI: 1) $n = 1: 7 \mid (2^3 - 1) \Rightarrow 7 \mid 7$ - platí

2) $\forall n \in N : 7 \mid (2^{3n} - 1) \Rightarrow \underline{7 \mid (2^{3(n+1)} - 1)}$

$$V(n+1) = 2^{3n+3} - 1 = 8 \cdot V(n) + 8 - 1 = 8 \cdot V(n) + 7$$

z indukčního předpokladu $7 \mid V(n) \wedge 7 \mid 7 \Rightarrow 7 \mid V(n+1)$

Př.: Dokažte: $\forall n \in N : 24 \mid (25^n + 23)$

MI: 1) $n = 1: 24 \mid (25 + 23) \Rightarrow 24 \mid 48$ - platí

2) $\forall n \in N : 24 \mid (25^n + 23) \Rightarrow \underline{24 \mid (25^{n+1} + 23)}$

$$V(n+1) = 25^{n+1} + 23 = 25 \cdot V(n) - 25 \cdot 23 + 23 = 25 \cdot V(n) - 24 \cdot 23$$

z indukčního předpokladu $24 \mid V(n) \wedge 24 \mid 24 \cdot 23 \Rightarrow 24 \mid V(n+1)$

§2. Největší společný dělitel

Pozn.: a) V tomto paragrafu se omezíme na vyšetřování dělitelnosti v N , i když mnohé výsledky lze jednoduše zobecnit do Z .
 b) S pojmem dělitel jsme se seznámili v §1.
 c) Každému přirozenému číslu n lze přiřadit neprázdnou množinu všech jeho dělitelů, kterou označíme $D(n)$.

Př.: Určete všechny dělitele čísel 48 a 64.

$$D(48) = \{1, 2, 3, 4, 6, 8, 12, 16, 24, 48\}$$

$$D(64) = \{1, 2, 4, 8, 16, 32, 64\}$$

Def.: Necht' $a, b \in N$.

Číslo $c \in N$ nazýváme společným dělitelem čísel a, b , jestliže $c \mid a \wedge c \mid b$.

Číslo $d \in N$ nazýváme největším společným dělitelem čísel a, b , který označujeme $d = D(a, b)$ (někdy jen (a, b)), jestliže platí:

$$1) d \mid a \wedge d \mid b$$

$$2) \forall c \in N : c \mid a \wedge c \mid b \Rightarrow c \mid d$$

Pozn.: Největší společný dělitel 2 přirozených čísel a, b je ten společný dělitel d , který má tuto vlastnost:

Každý jiný společný dělitel čísel a, b je dělitelem čísla d .

V.2.1: Ke každým dvěma přirozeným číslům $a, b \in N$ existuje právě jeden největší společný dělitel.

[Dk.!: konstruktivní – Euklidův algoritmus:

$$a) a = b \Rightarrow (a, b) = a$$

b) $a \neq b \wedge a > b$: Proved'me nyní postupně posloupnost dělení se zbytkem:

$$a = b \cdot q_1 + r_1, \quad 0 < r_1 < b$$

$$b = r_1 \cdot q_2 + r_2, \quad 0 < r_2 < r_1$$

$$r_1 = r_2 \cdot q_3 + r_3, \quad 0 < r_3 < r_2$$

$$\vdots$$

$$r_{n-2} = r_{n-1} \cdot q_n + r_n, \quad 0 < r_n < r_{n-1}$$

$$r_{n-1} = r_n \cdot q_{n+1}, \quad r_{n+1} = 0$$

Toto dělení ukončíme, až dostaneme nulový zbytek. Vzhledem k nerovnostem platí: $b > r_1 > r_2 > \dots > r_{n-1} > r_n > r_{n+1} = 0$, takže tento nulový zbytek existuje.

Ukážeme, že poslední nenulový zbytek, tzn. číslo r_n , je největším společným dělitelem čísel a, b :

$$1) \text{ Ukážeme, že } r_n \mid a \wedge r_n \mid b : \text{ platí: } r_n \mid r_n \wedge r_n \mid r_{n-1} \Rightarrow r_n \mid r_{n-2}$$

$$r_n \mid r_{n-1} \wedge r_n \mid r_{n-2} \Rightarrow r_n \mid r_{n-3}$$

$$\vdots$$

$$r_n \mid r_2 \wedge r_n \mid r_1 \Rightarrow r_n \mid b$$

$$r_n \mid r_1 \wedge r_n \mid b \Rightarrow r_n \mid a$$

2) Necht' $c \in N : c \mid a \wedge c \mid b$. Ukážeme, že $c \mid r_n$.

$$a = bq_1 + r_1 \Rightarrow c \mid r_1 \wedge c \mid b \Rightarrow c \mid r_2 \wedge c \mid r_1 \Rightarrow \dots \Rightarrow c \mid r_{n-1} \wedge c \mid r_{n-2} \Rightarrow c \mid r_n]$$

Př.: Vypočítejte $D(525,231)$; $D(9694,4181)$.

$$525 = 2 \cdot 231 + 63$$

$$9694 = 2 \cdot 4181 + 1332$$

$$231 = 3 \cdot 63 + 42$$

$$4181 = 3 \cdot 1332 + 185$$

$$63 = 1 \cdot 42 + 21$$

$$1332 = 7 \cdot 185 + 37$$

$$42 = 2 \cdot 21$$

$$185 = 5 \cdot 37$$

$$\underline{\underline{D(525,231) = 21}}$$

$$\underline{\underline{D(9694,4181) = 37}}$$

V.2.2: Necht' $a, b, c \in N \wedge D(a, b) = d$. Potom $D(a, b, c) = D(d, c)$.

[Dk.: Označme $d_1 = D(a, b, c)$, $d_2 = D(d, c)$.

$$a) \ d_1 = D(a, b, c) \Rightarrow d_1 \mid a \wedge d_1 \mid b \wedge d_1 \mid c \Rightarrow d_1 \mid D(a, b) \Rightarrow d_1 \mid d \Rightarrow d_1 \mid D(d, c) \Rightarrow d_1 \mid d_2$$

$$b) \ d_2 = D(d, c) \Rightarrow d_2 \mid d \wedge d_2 \mid c \Rightarrow d_2 \mid D(a, b) \Rightarrow d_2 \mid a \wedge d_2 \mid b \Rightarrow d_2 \mid D(a, b, c) \Rightarrow d_2 \mid d_1 \\ d_1 \mid d_2 \wedge d_2 \mid d_1 \Rightarrow d_1 = d_2]$$

Př.: Určete $D(432, 720, 1080)$.

$$720 = 432 \cdot 1 + 288$$

$$1080 = 144 \cdot 7 + 72$$

$$432 = 288 \cdot 1 + 144$$

$$144 = 2 \cdot 72$$

$$288 = 144 \cdot 2$$

$$\underline{\underline{D(432, 720) = 144}}$$

$$\underline{\underline{D(144, 1080) = D(432, 720, 1080) = 72}}$$

Def.: Necht' $a, b \in N$. Říkáme, že čísla a, b jsou nesoudělná, jestliže platí $D(a, b) = 1$.
Je-li $D(a, b) > 1$, říkáme, že čísla a, b jsou soudělná.

Pozn.: Uvedenou definici lze rozšířit na konečnou množinu přirozených čísel.

V.2.3: $\forall a, b \in N : a \mid b \Leftrightarrow D(a, b) = a$

[Dk.: Označme $d = D(a, b)$.

$$1) \text{ „} \Rightarrow \text{“: } a \mid b \Rightarrow d = D(a, b) \Rightarrow d \mid a \wedge d \mid b.$$

$$\text{Platí } a \mid a \wedge a \mid b \Rightarrow a \mid D(a, b) \Rightarrow a \mid d \Rightarrow a = d$$

$$2) \text{ „} \Leftarrow \text{“: } a = d = D(a, b) \Rightarrow d \mid a \wedge d \mid b \Rightarrow a \mid b]$$

V.2.4: $\forall a, b, n \in N : D(an, bn) = n \cdot D(a, b)$

[Dk.: Označme $d_1 = D(a, b)$, $d_2 = D(an, bn)$. Ukážeme, že $d_2 = nd_1$:

$$a) \ d_1 = D(a, b) \Rightarrow d_1 \mid a \wedge d_1 \mid b \Rightarrow nd_1 \mid na \wedge nd_1 \mid nb \Rightarrow nd_1 \mid D(na, nb) \Rightarrow nd_1 \mid d_2$$

$$b) \text{ Platí: } n \mid na \wedge n \mid nb \Rightarrow n \mid D(na, nb) \Rightarrow n \mid d_2 \Rightarrow \exists c \in N : d_2 = n \cdot c$$

$$d_2 = D(nA, nB) \Rightarrow d_2 \mid na \wedge d_2 \mid nb \Rightarrow nc \mid na \wedge nc \mid nb \Rightarrow c \mid a \wedge c \mid b \Rightarrow c \mid D(a, b) \Rightarrow$$

$$\Rightarrow c \mid d_1 \Rightarrow nc \mid nd_1 \Rightarrow d_2 \mid nd_1$$

$$nd_1 \mid d_2 \wedge d_2 \mid nd_1 \Rightarrow d_2 = nd_1]$$

V.2.5: Fundamentální věta aritmetiky:

Nechť $a_1, a_2, b \in N, b > 1$. Pak platí: $b \mid a_1 a_2 \wedge D(a_1, b) = 1 \Rightarrow b \mid a_2$.

[Dk.: $b \mid a_1 a_2 \Rightarrow D(a_1 a_2, b) = b$. Ukážeme, že $D(a_1 a_2, b) = b = D(a_2, b) \Rightarrow b \mid a_2$.

Označme $d_1 = D(a_1 a_2, b), d_2 = D(a_2, b)$. Ukážeme, že $d_1 = d_2$:

$$\begin{aligned} \text{a) } d_1 = D(a_1 a_2, b) &\Rightarrow \underline{d_1 \mid a_1 a_2} \wedge \underline{d_1 \mid b} \Rightarrow \underline{d_1 \mid a_2 b} \Rightarrow d_1 \mid D(a_1 a_2, a_2 b) \Rightarrow d_1 \mid a_2 \underbrace{D(a_1, b)}_1 \Rightarrow \\ &\Rightarrow \underline{d_1 \mid a_2} \Rightarrow d_1 \mid D(a_2, b) \Rightarrow d_1 \mid d_2 \end{aligned}$$

$$\begin{aligned} \text{b) } d_2 = D(a_2, b) &\Rightarrow d_2 \mid a_2 \wedge \underline{d_2 \mid b} \Rightarrow \underline{d_2 \mid a_1 a_2} \Rightarrow d_2 \mid D(a_1 a_2, b) \Rightarrow d_2 \mid d_1 \\ &d_1 \mid d_2 \wedge d_2 \mid d_1 \Rightarrow d_1 = d_2 \end{aligned}$$

V.2.6: $\forall a, b \in N, a \geq b$: a) $D(a, b) = D(a + b, b)$

$$\text{b) } D(a, b) = D(a - b, b)$$

[Dk.: a) Označme $d_1 = D(a, b), d_2 = D(a + b, b)$

$$,,\Rightarrow": d_1 = D(a, b) \Rightarrow d_1 \mid a \wedge d_1 \mid b \Rightarrow d_1 \mid (a + b) \wedge d_1 \mid b \Rightarrow d_1 \mid D(a + b, b) \Rightarrow d_1 \mid d_2$$

$$\begin{aligned} ,, \Leftarrow ": d_2 = D(a + b, b) &\Rightarrow d_2 \mid (a + b) \wedge d_2 \mid b \Rightarrow d_2 \mid (a + b - b) \Rightarrow d_2 \mid a \wedge d_2 \mid b \Rightarrow \\ &\Rightarrow d_2 \mid D(a, b) \Rightarrow d_2 \mid d_1 \\ &d_1 \mid d_2 \wedge d_2 \mid d_1 \Rightarrow d_1 = d_2 \end{aligned}$$

b) analogicky]

Př.: Dokažte $\forall c, d \in N : D(8c + 5d, 5c + 3d) = D(c, d)$

$$\begin{aligned} D(8c + 5d, 5c + 3d) &= D(8c + 5d - 5c - 3d, 5c + 3d) = D(3c + 2d, 5c + 3d) = \\ &= D(3c + 2d, 2c + d) = D(c + d, 2c + d) = D(c + d, c) = D(c, d) \end{aligned}$$

Def.: Necht' $M = \{a_1, a_2, \dots, a_n\}$ je konečná množina přirozených čísel. Říkáme, že čísla a_1, a_2, \dots, a_n jsou po dvou nesoudělná, jestliže platí:

$$D(a_1, a_2) = D(a_1, a_3) = \dots = D(a_1, a_n) = D(a_2, a_3) = D(a_2, a_4) = \dots = D(a_{n-1}, a_n) = 1$$

Pozn.: a) Podmínku k definici lze symbolicky zapsat takto:

$$D(a_i, a_j) = 1, \forall i, j \in \{1, 2, \dots, n\}, i \neq j$$

b) Jsou-li čísla a_1, a_2, \dots, a_n po dvou nesoudělná, pak jsou nesoudělná, tedy

$$D(a_1, a_2, \dots, a_n) = 1, \text{ přičemž obrácení věty neplatí.}$$

$$\text{Např.: } D(5, 7, 35) = 1, \text{ ale } D(5, 7) = 1, D(35, 7) = 7, D(35, 5) = 5$$

c) Pro $n = 2$ definice po dvou nesoudělných a nesoudělných čísel splývají.

V.2.7: $\forall a, b \in N : d = D(a, b) \Rightarrow \exists q_1, q_2 \in N : a = dq_1 \wedge b = dq_2 \wedge D(q_1, q_2) = 1$

[Dk.: sporem: Necht' $D(q_1, q_2) = d' > 1 \Rightarrow \exists r_1, r_2 \in N : q_1 = d'r_1 \wedge q_2 = d'r_2 \Rightarrow$

$$\Rightarrow a = d \cdot d' \cdot r_1 \Rightarrow (d \cdot d') \mid a$$

$$\underbrace{b = d \cdot d' \cdot r_2}_{(d \cdot d') \mid b}$$

$$\Rightarrow (d \cdot d') \mid D(a, b) \Rightarrow (d \cdot d') \mid d - \text{spor } (d' = 1) \Rightarrow D(q_1, q_2) = 1]$$

Příklady k §2.:

Př.: Najděte všechny dvojice přirozených čísel, jejichž součin je 864 a jejichž největší společný dělitel je 6.

Hledaná čísla označme a, b a předpokládejme, že $a < b$.

$$D(a, b) = 6 \Rightarrow a = 6p, b = 6q; D(p, q) = 1, p < q$$

$$ab = 36pq$$

$$36pq = 864 \Rightarrow pq = 24$$

Nyní číslo 24 rozložíme všemi možnými způsoby na součin dvou činitelů a vybereme ty rozklady, v nichž jsou činitelé nesoudělná čísla:

$$24 = \underline{1 \cdot 24} = \underline{2 \cdot 12} = \underline{3 \cdot 8} = \underline{4 \cdot 6}$$

- $p = 1, q = 24 \Rightarrow \underline{a} = 6 \cdot 1 = \underline{6}, \underline{b} = 6 \cdot 24 = \underline{144}$
- $p = 3, q = 8 \Rightarrow \underline{a} = 6 \cdot 3 = \underline{18}, \underline{b} = 6 \cdot 8 = \underline{48}$

Existují dvě dvojice hledaných čísel: $[6, 144]$, $[18, 48]$.

Př.: Najděte všechny dvojice přirozených čísel, jejichž součet je 432 a jejichž největší společný dělitel je 36.

Hledaná čísla označme a, b a předpokládejme, že $a < b$.

$$D(a, b) = 36 \Rightarrow a = 36p, b = 36q; D(p, q) = 1, p < q$$

$$a + b = 36(p + q)$$

$$36(p + q) = 432 \Rightarrow p + q = 12$$

Nyní číslo 12 rozložíme všemi možnými způsoby na součet dvou sčítanců a vybereme ty rozklady, v nichž jsou sčítanci nesoudělná čísla:

$$12 = \underline{1+11} = \underline{2+10} = \underline{3+9} = \underline{4+8} = \underline{5+7} = \underline{6+6}$$

- $p = 1, q = 11 \Rightarrow \underline{a} = 36 \cdot 1 = \underline{36}, \underline{b} = 36 \cdot 11 = \underline{396}$
- $p = 5, q = 7 \Rightarrow \underline{a} = 36 \cdot 5 = \underline{180}, \underline{b} = 36 \cdot 7 = \underline{252}$

Existují dvě dvojice hledaných čísel: $[36, 396]$, $[180, 252]$.

§3. Nejmenší společný násobek

Pozn.: a) V tomto paragrafu se také omezíme na množinu N .
b) S pojmem násobek jsme se seznámili v §1.

Def.: Necht' $a, b \in N$.

Číslo $m \in N$ nazýváme společným násobkem čísel a, b , jestliže $a \mid m \wedge b \mid m$.

Číslo $n \in N$ nazýváme nejmenším společným násobkem čísel a, b , který označujeme $n = n(a, b)$, jestliže platí:

- 1) $a \mid n \wedge b \mid n$
- 2) $\forall m \in N : a \mid m \wedge b \mid m \Rightarrow n \mid m$

Pozn.: a) Ke každé dvojici přirozených čísel $a, b \in N$ existuje nekonečně mnoho společných násobků, ale právě jeden mezi nimi je nejmenší společný násobek.
b) Analogicky lze definovat společný a nejmenší společný násobek množiny čísel, která je podmnožinou N (libovolné konečné množiny přirozených čísel).

V.3.1: $\forall a, b, k \in N : n(ka, kb) = k \cdot n(a, b)$

[Dk.: Označme $m_1 = n(a, b), m_2 = n(ka, kb)$. Ukážeme, že $m_2 = k \cdot m_1$.

a) $m_1 = n(a, b) \Rightarrow a \mid m_1 \wedge b \mid m_1 \Rightarrow ka \mid km_1 \wedge kb \mid km_1 \Rightarrow km_1$ je společným násobkem čísel ka a $kb \Rightarrow m_2 \mid km_1$

b) Platí: $k \mid ka \wedge k \mid kb \Rightarrow k \mid n(ka, kb) \Rightarrow k \mid m_2 \Rightarrow \exists c \in N : m_2 = kc$
 $m_2 = n(ka, kb) \Rightarrow ka \mid m_2 \wedge kb \mid m_2 \Rightarrow \overline{ka} \mid \overline{kc} \wedge \overline{kb} \mid \overline{kc} \Rightarrow \overline{a} \mid \overline{c} \wedge \overline{b} \mid \overline{c} \Rightarrow c$ je
 společný násobek čísel a a $b \Rightarrow m_1 \mid c \Rightarrow km_1 \mid kc \Rightarrow km_1 \mid m_2$
 $m_2 \mid km_1 \wedge km_1 \mid m_2 \xrightarrow{\dots} m_2 = km_1$]

Pozn.: Z předchozí věty je patrné, že při výpočtu nejmenšího společného násobku lze společného činitele obou čísel vytknout.

V.3.2: Necht' $\forall a, b, c \in N$ platí: $n(a, b) = m$. Potom $n(a, b, c) = n(m, c)$.

[Dk.: Označme $m_1 = n(a, b, c), m_2 = n(m, c)$.

a) $m_1 = n(a, b, c) \Rightarrow a \mid m_1 \wedge b \mid m_1 \wedge c \mid m_1 \Rightarrow \underline{m} \mid m_1 \Rightarrow m_2 \mid m_1$

b) $m_2 = n(m, c) \Rightarrow m \mid m_2 \wedge c \mid m_2 \Rightarrow \underline{a} \mid \underline{m_2} \wedge \underline{b} \mid \underline{m_2} \Rightarrow m_1 \mid m_2$
 $m_2 \mid m_1 \wedge m_1 \mid m_2 \Rightarrow m_1 = m_2$]

V.3.3: $\forall a, b \in N : \underline{a \cdot b} = \underline{D(a, b) \cdot n(a, b)}$

[Dk.: Označme $d = D(a, b), m = n(a, b)$. Ukážeme, že $\underline{a \cdot b} = \underline{d \cdot m}$:

$d = D(a, b) \Rightarrow \exists! q_1, q_2 \in N : a = d \cdot q_1, b = d \cdot q_2, D(q_1, q_2) = 1$.

$\underline{a \cdot b} = \underline{dq_1 \cdot dq_2} = \underline{d \cdot dq_1 q_2}$. Ukážeme, že $\underline{dq_1 q_2} = n$ je nejmenší společný násobek

čísel a a b ($= m$):

- 1) $a = dq_1, n = dq_1 q_2 \Rightarrow a \mid n; b = dq_2, n = dq_1 q_2 \Rightarrow b \mid n \Rightarrow n$ je společný násobek čísel a a b .

$$2) a \mid n \wedge b \mid n \Rightarrow m \mid n \Rightarrow \exists c \in N : n = m \cdot c$$

$$\begin{aligned} \underline{a \cdot b} &= d \cdot dq_1 q_2 = d \cdot n = \underline{d \cdot mc} \Rightarrow a = \frac{med}{b} = k_1 cd, k_1 \in N \wedge b = \frac{med}{a} = k_2 cd, k_2 \in N \Rightarrow \\ &\Rightarrow cd \mid a \wedge cd \mid b \Rightarrow cd \mid D(a, b) \Rightarrow cd \mid d \Rightarrow c = 1 \Rightarrow n = m] \Rightarrow n \text{ je nejmenší spol.} \\ &\text{násobek} \end{aligned}$$

Př.: Určete $n(396, 444)$.

$$444 = 396 \cdot 1 + 48 \quad D(396, 444) = 12$$

$$396 = 48 \cdot 8 + 12 \quad n(396, 444) = \frac{396 \cdot 444}{D(396, 444)} = \frac{175824}{12} = 14652$$

$$48 = 12 \cdot 4$$

Důsledek V.3.3.: $\forall a, b \in N : D(a, b) = 1 \Rightarrow a \cdot b = n(a, b)$

[Dk.: V.3.3.: $D(a, b) \cdot n(a, b) = a \cdot b$

$$D(a, b) = 1 : n(a, b) = a \cdot b]$$

Př.: Největší společný dělitel čísel a, b je 15, jejich nejmenší společný násobek je 900. Určete čísla a, b .

$$D(a, b) = d = 15, n(a, b) = m = 900$$

$$D(a, b) = d \Rightarrow a = dq_1, b = dq_2; q_1, q_2 \in N; D(q_1, q_2) = 1$$

$$m = n(a, b) = dq_1 q_2$$

$$900 = 15q_1 q_2 \Rightarrow q_1 q_2 = \frac{900}{15} = 60$$

$$60 = \underline{1 \cdot 60} = 2 \cdot 30 = 3 \cdot 20 = 4 \cdot 15 = 5 \cdot 12 = \underline{6 \cdot 10}$$

(Vyškrtneme čísla soudělná.)

Existují 4 dvojice hledaných čísel:

15,900; 45,300; 60,225; 75,180.

q_1	q_2	d	a	b
1	60	15	15	900
2	30	15	30	450
3	20	15	45	300
4	15	15	60	225
5	12	15	75	180
6	10	15	90	150

Pozn.: Důsledek V.3.3. lze zobecnit i pro více čísel a_1, a_2, \dots, a_n :

$n(a_1, a_2, \dots, a_n)$, která jsou po dvou nesoudělná, je roven jejich součinu

$$n(a_1, a_2, \dots, a_n) = a_1 \cdot a_2 \cdot \dots \cdot a_k.$$

V.3.4: $\forall a, b \in N : a \mid b \Leftrightarrow n(a, b) = b$

[Dk.: Platí $a \mid b \Leftrightarrow D(a, b) = a$; $\underline{a \cdot b} = D(a, b) \cdot n(a, b) = \underline{a \cdot n(a, b)} \Leftrightarrow n(a, b) = b]$

V.3.5: $\forall a, b_1, b_2 \in N : b_1 \mid a \wedge b_2 \mid a \Rightarrow n(b_1, b_2) \mid a$

[Dk.: $b_1 \mid a \wedge b_2 \mid a \Rightarrow a$ je společným násobkem čísel $b_1, b_2 \Rightarrow n(b_1, b_2) \mid a]$

Důsledek V.3.5.: $\forall a, b_1, b_2 \in N : b_1 \mid a \wedge b_2 \mid a \wedge D(b_1, b_2) = 1 \Rightarrow b_1 b_2 \mid a$

[Dk.: $D(b_1, b_2) = 1 \Rightarrow n(b_1, b_2) = b_1 b_2$ a tvrzení plyne z V.3.5.]

Příklady k §3.:

Př.: Najděte všechny dvojice přirozených čísel, jejichž nejmenší společný násobek je o 7 větší než jejich největší společný dělitel.

$$a = dq_1, b = dq_2; d = D(a, b); n(a, b) = dq_1q_2; D(q_1, q_2) = 1$$

$$7 = dq_1q_2 - d = d(q_1q_2 - 1) = 7 \cdot 1 = 1 \cdot 7$$

- $d = 7 \wedge (q_1q_2 - 1) = 1 \Rightarrow d = 7 \wedge q_1q_2 = 2 = 1 \cdot 2 \Rightarrow \underline{a} = 7 \cdot 1 = \underline{7}, \underline{b} = 7 \cdot 2 = \underline{14}$
- $d = 1 \wedge (q_1q_2 - 1) = 7 \Rightarrow d = 1 \wedge q_1q_2 = 8 = \underline{1} \cdot \underline{8} = 2 \cdot 4 \Rightarrow \underline{a} = 1 \cdot 1 = \underline{1}, \underline{b} = 1 \cdot 8 = \underline{8}$

Existují dvě dvojice hledaných čísel: $[7, 14], [1, 8]$.

Př.: Najděte všechny dvojice přirozených čísel a, b , platí-li $a + b = 100, n(a, b) = 210$.

$$a = dq_1, b = dq_2; d = D(a, b); n(a, b) = dq_1q_2; D(q_1, q_2) = 1$$

$$d(q_1 + q_2) = 100, dq_1q_2 = 210$$

$$D(d(q_1 + q_2), dq_1q_2) = d \Leftrightarrow D(q_1 + q_2, q_1q_2) = 1$$

$$D(d(q_1 + q_2), dq_1q_2) = d = D(100, 210) = 10 \Rightarrow q_1 + q_2 = 10, q_1q_2 = 21 = 1 \cdot 21 = 3 \cdot 7$$

Dvojice 1, 21 nevyhovuje 1. rovnici soustavy, ale dvojice 3, 7 ano ($3 + 7 = 10$).

$$\text{Tedy } q_1 = 3 \wedge q_2 = 7 \Rightarrow \underline{a} = 10 \cdot 3 = \underline{30}, \underline{b} = 10 \cdot 7 = \underline{70}$$

Existuje jedna dvojice hledaných čísel: $[30, 70]$.

Př.: Najděte všechna přirozená čísla a , pro která $D(76, a) = 19$ a zároveň $n(40, a) = 760$.

$$76 = 2 \cdot 2 \cdot 19$$

$D(76, a) = 19$, což je prvočíslo

$$D(76, a) = 19 \Leftrightarrow a = 19p, \quad p \dots \text{součin prvočísel, } 2 \nmid p$$

$$40 = 8 \cdot 5 = 2 \cdot 2 \cdot 2 \cdot 5$$

$$n(40, a) = 760 = 10 \cdot 76 = 10 \cdot 4 \cdot 19 = 2 \cdot 2 \cdot 2 \cdot 5 \cdot 19$$

$$n(40, a) = 760 \Leftrightarrow a = 19q, \text{ kde } q \mid 2 \cdot 2 \cdot 2 \cdot 5$$

Protože p není dělitelné 2, mohou nastat pouze dva případy:

$$a = 19p = 19q \Rightarrow p = q \Rightarrow p \in \{1, 5\}$$

$$a = 19 \cdot 1 = 19 \vee a = 19 \cdot 5 = 95 \Rightarrow \underline{\underline{a \in \{19, 95\}}}$$

Př.: Najděte prvočíslo p tak, aby pro vhodná přirozená čísla a, b platilo:

$$D(a, b) = 77; n(a, b) = 105p; ab = 735p^2$$

Řešíme podle vzorce $a \cdot b = D(a, b) \cdot n(a, b)$:

$$735p^2 = 77 \cdot 105p$$

$$p^2 = 11p \Rightarrow \underline{\underline{p = 11}}$$

§4. Prvočísla a čísla složená

Pozn.: Podle V.1.1. má každé přirozené číslo $n, n > 1$ alespoň dva dělitele - $1 | n, n | n$.

Tyto dělitele nazýváme triviálními (samozřejmými) děliteli; ostatní dělitele čísla n (pokud existují) nazveme netriviálními (nesamozřejmými) děliteli.

Def.: Necht' $n \in N, n > 1$. Má-li číslo n pouze triviální dělitele, nazýváme jej prvočíslem; má-li alespoň jednoho netriviálního, nazýváme jej číslem složeným.

Pozn.: a) Číslo 1 není ani prvočíslo, ani číslo složené.

b) Množinu N lze vyjádřit $N = \{1\} \cup N_p \cup N_s$, kde N_p je množina všech prvočísel (je nekonečná) a N_s je množina všech složených čísel (je nekonečná). Všechny tyto tři množiny jsou po dvou disjunktní.

V.4.1: Necht' $p \in N$ je prvočíslo, $n \in N$ libovolné číslo. Pak platí: $p \nmid n \Leftrightarrow D(p, n) = 1$.

[Dk.: 1. „ \Rightarrow “: nepřímá: $D(p, n) > 1 \Rightarrow p | n$

Necht' $D(p, n) = d \Rightarrow d | n \wedge d | p \Rightarrow d = 1 \vee d = p$. Platí $d > 1 \Rightarrow d = p$.

Platí $d | n \Rightarrow p | n$.

2. „ \Leftarrow “: nepřímá: $p | n \Rightarrow D(p, n) > 1$

$p | n \Rightarrow D(p, n) = p, p$ je prvočíslo $\Rightarrow p > 1 \Rightarrow D(p, n) > 1]$

V.4.2: Necht' $p \in N$ je prvočíslo, $a, b \in N$. Pak platí: $p | a \cdot b \wedge p \nmid a \Rightarrow p | b$

[Dk.: $p \nmid a \Rightarrow D(p, a) = 1$ a tvrzení plyne z fundamentální věty aritmetiky (V.2.5.)]

Pozn.: a) Předpoklad, že p je prvočíslo, je v předchozí větě podstatný a bez něj věta neplatí.

Např.: $6 | 12 = 3 \cdot 4, 6 \nmid 3 \Rightarrow 6 | 4$ - neplatí

b) Logickým důsledkem předchozí věty je tvrzení: $p | ab \Rightarrow p | a \vee p | b$, kterého se někdy užívá k definici prvočísla.

V.4.3: Každé přirozené číslo $n, n > 1$ má alespoň jednoho prvočíselného dělitele p .

[Dk.: Označme M množinu všech dělitelů čísla n větších než 1. Platí: $M \neq \emptyset$ ($n \in M$), tedy existuje její nejmenší prvek a ukážeme, že je to prvočíslo – p – sporem:

Necht' p je složené číslo $\Rightarrow \exists a, b \in N : p = ab, 1 < a < p, 1 < b < p \Rightarrow a | p \wedge p | n \Rightarrow$

(V.1.1.c)) $\Rightarrow a | n \Rightarrow a \in M, a < p$ - spor s tím, že p je nejmenší ze všech dělitelů čísla $n \Rightarrow p$ je prvočíslo]

V.4.4: Každé složené číslo n má alespoň jednoho prvočíselného dělitele $p : p \leq \sqrt{n}$

[Dk.: Necht' n je složené číslo $\Rightarrow \exists a, b \in N : n = ab, 1 < a < n, 1 < b < n$.

Necht' např. $a \leq b \Rightarrow a^2 \leq ab = n \Rightarrow a \leq \sqrt{n}$. Podle V.4.3. má a alespoň 1

prvočíselného dělitele $p, p | a, 1 < p \leq a \Rightarrow p \leq a \leq \sqrt{n} \Rightarrow p \leq \sqrt{n}$.

Platí: $p | a \wedge a | n \Rightarrow p | n]$

Pozn.: Předchozí větu lze ekvivalentně zformulovat takto: Jestliže číslo n má tu vlastnost, že není dělitelné žádným prvočíslem $p : p \leq \sqrt{n}$, pak číslo n je prvočíslo ($n > 1$).
(Jde o obměnu předchozí věty.)

V.4.5: Prvočísel je nekonečně mnoho.

[Dk.: Euklides – sporem:

Předpokládejme, že je prvočísel konečně mnoho, tzn. $N_p = \{p_1, p_2, \dots, p_k\}$. Uvažujme o čísle $p = p_1 \cdot p_2 \cdot \dots \cdot p_k + 1$. Platí: $\forall i \in \{1, 2, \dots, k\} : p \neq p_i \Rightarrow p$ je složené číslo a nepatří do $N_p \Rightarrow \exists a \in N_p : a \mid p \Rightarrow a = p_i \Rightarrow p_i \mid p_1 p_2 \dots p_k \wedge p_i \mid p$ (protože $a \mid p$) $\Rightarrow p_i \mid 1$ - spor]

Př.: Dokažte, že $\forall a, b \in N : D(a, b) = 1 \Rightarrow D(ab, a + b) = 1$

sporem: Necht' $\exists a, b \in N : D(a, b) = 1 \wedge D(ab, a + b) = d > 1 \Rightarrow d \mid ab \wedge d \mid (a + b)$,
 $d > 1 \Rightarrow \exists$ prvočíslo p tak, že $p \mid d \wedge d \mid ab \Rightarrow p \mid ab \Rightarrow p \mid a \vee p \mid b$.

Necht' $\underline{p \mid a} \wedge p \mid d \wedge d \mid (a + b) \Rightarrow \underline{p \mid (a + b)} \Rightarrow p \mid b \Rightarrow p \mid D(a, b) \Rightarrow p \mid 1$ - spor

§5. Rozklad přirozeného čísla na prvočinitele

Pozn.: $\forall n \in N, n > 1$ existuje podle V.4.3. alespoň jedno prvočíslo $p_1 : p_1 \mid n \Rightarrow n = p_1 n_1$.

Je-li $n_1 = 1$, je $n = p_1$. Necht' $n_1 > 1 \Rightarrow \exists p_2$ - prvočíslo: $p_2 \mid n_1 \Rightarrow n = p_2 n_2$. Je-li $n_2 = 1$, je $n_1 = p_2 \wedge n = p_1 p_2$. Je-li $n_2 > 1$, opakujeme tento postup.

Protože $n > n_1 > n_2 > \dots > n_k$, tento postup lze po konečném počtu kroků ukončit.

Tedy $n = p_1 p_2 \dots p_k$, kde $p_i (i = 1, 2, \dots, k)$ jsou prvočísla (ne nutně jsou navzájem všechna různá).

Lze tedy psát $n = p_1^{m_1} \cdot p_2^{m_2} \cdot \dots \cdot p_r^{m_r}$, kde p_i jsou prvočísla a $m_i \in N$ jsou exponenty, s nimiž se prvočísla p_i vyskytují v rozkladu čísla n na součin prvočísel. Dále ukážeme, že toto vyjádření je až na pořadí činitelů jednoznačné.

V.5.1: Necht' p_1, p_2 jsou prvočísla. Pak platí: $p_1 \neq p_2 \Rightarrow p_1 \nmid p_2 \wedge p_2 \nmid p_1$

[Dk.: Necht' $p_1 \neq p_2$ jsou prvočísla. $\Rightarrow D(p_1, p_2) = 1 \Rightarrow p_1 \nmid p_2 \wedge p_2 \nmid p_1$ podle V.4.1.]

V.5.2: Necht' p_1, p_2 jsou prvočísla. Pak platí: $p_1 \neq p_2 \Rightarrow p_1 \nmid p_2^2$

[Dk.: sporem: Necht' $p_1 \neq p_2 \wedge p_1 \mid p_2^2 \Rightarrow p_1 \mid p_2 \cdot p_2 \Rightarrow p_1 \mid p_2$ - spor s V.5.1.]

Důsledek V.5.1. a V.5.2.:

1. Necht' p_1, p_2 jsou prvočísla, $n \in N$. Pak platí: $p_1 \neq p_2 \Rightarrow p_1 \nmid p_2^n$

2. Necht' p_1, p_2 jsou prvočísla, $n_1, n_2 \in N$. Pak platí: $p_1 \neq p_2 \Rightarrow D(p_1^{n_1}, p_2^{n_2}) = 1$

[Dk.: zobecněním úvah z důkazů vět V.5.1. a V.5.2.]

V.5.3: Základní věta aritmetiky:

Věta o existenci a jednoznačnosti rozkladu přirozeného čísla na součin prvočinitelů:

Každé přirozené číslo $n, n > 1$ lze zapsat ve tvaru $n = p_1^{m_1} \cdot p_2^{m_2} \cdot \dots \cdot p_r^{m_r}$,

kde $p_i, i \in \{1, 2, \dots, r\}$ jsou navzájem různá prvočísla, $m_i \in N_0$. Toto vyjádření je jednoznačné až na pořadí činitelů.

[Dk.: 1. existence: plyne z poznámky v úvodu paragrafu

2. jednoznačnost: Necht' $n = p_1^{m_1} \cdot p_2^{m_2} \cdot \dots \cdot p_r^{m_r} = q_1^{l_1} \cdot q_2^{l_2} \cdot \dots \cdot q_s^{l_s}$.

Platí: $p_1 \mid q_1^{l_1} \cdot q_2^{l_2} \cdot \dots \cdot q_s^{l_s}$. Necht' např. $p_1 \mid q_1^{l_1} \Rightarrow p_1 = q_1$.

Analogicky $p_2 = q_2, \dots, p_r = q_s \Rightarrow r = s$.

Ukážeme, že jsou si rovny i exponenty ($m_1 = l_1, m_2 = l_2, \dots, m_r = l_r$):

Platí: $p_1^{m_1} \mid q_1^{l_1} \cdot q_2^{l_2} \cdot \dots \cdot q_s^{l_s} \Rightarrow p_1^{m_1} \mid q_1^{l_1} \Rightarrow \underline{m_1 \leq l_1}$. Analogicky platí $q_1^{l_1} \mid p_1^{m_1} \Rightarrow \underline{l_1 \leq m_1} \Rightarrow m_1 = l_1$. Analogicky $m_2 = l_2, \dots, m_r = l_r$.]

Př.: Nalezněte prvočíselné rozklady těchto čísel:

a) $180 = 5 \cdot 36 = 5 \cdot 2 \cdot 18 = 5 \cdot 2 \cdot 2 \cdot 3 \cdot 3 = 2^2 \cdot 3^2 \cdot 5$

b) $644 = 2^2 \cdot 161 = 2^2 \cdot 7 \cdot 23$

c) $8448 = 2^3 \cdot 1056 = 2^3 \cdot 2^3 \cdot 132 = 2^6 \cdot 2^2 \cdot 33 = 2^8 \cdot 3 \cdot 11$

Def.: Necht' $x_1, x_2 \in R$. Pak definujeme:

- a) $\min(x_1, x_2) = x_1 \Leftrightarrow x_1 \leq x_2$
 $\min(x_1, x_2) = x_2 \Leftrightarrow x_2 \leq x_1$
 b) $\max(x_1, x_2) = x_1 \Leftrightarrow x_1 \geq x_2$
 $\max(x_1, x_2) = x_2 \Leftrightarrow x_2 \geq x_1$

Pozn.: Rozklad přirozeného čísla na prvočinitele lze vhodně užít při hledání největšího společného dělitele a nejmenšího společného násobku dvou (ale i více) čísel.

Př.: Určete $D(a, b)$ a $n(a, b)$ následujících čísel:

$$\begin{array}{ll} \text{a) } 12 = 2^2 \cdot 3 & \text{b) } 980 = 2^2 \cdot 245 = 2^2 \cdot 5 \cdot 49 = 2^2 \cdot 5 \cdot 7^2 \\ 28 = 2^2 \cdot 7 & 1386 = 2 \cdot 693 = 2 \cdot 3^2 \cdot 77 = 2 \cdot 3^2 \cdot 7 \cdot 11 \\ \underline{42 = 2 \cdot 3 \cdot 7} & D(980, 1386) = 2 \cdot 7 = 14 \\ D(12, 28, 42) = 2 & n(980, 1386) = 2^2 \cdot 3^2 \cdot 5 \cdot 7^2 \cdot 11 = 97020 \\ n(12, 28, 42) = 2^2 \cdot 3 \cdot 7 = 84 & \end{array}$$

V.5.4: Necht' $a, b \in N, a > 1, b > 1$. Necht' $a = p_1^{m_1} \cdot p_2^{m_2} \cdot \dots \cdot p_r^{m_r}$,
 $b = p_1^{l_1} \cdot p_2^{l_2} \cdot \dots \cdot p_r^{l_r}$, kde $p_i (i = 1, 2, \dots, r)$

jsou různá prvočísla; $m_i, l_i \in N_0$. Pak platí:

- a) $D(a, b) = p_1^{x_1} \cdot p_2^{x_2} \cdot \dots \cdot p_r^{x_r}$, kde $x_i = \min(m_i, l_i)$
 b) $n(a, b) = p_1^{y_1} \cdot p_2^{y_2} \cdot \dots \cdot p_r^{y_r}$, kde $y_i = \max(m_i, l_i)$

V.5.5: Věta o iracionálnosti odmocnin:

Necht' $n \in N$. Pak platí:

n není druhou mocninou přirozeného čísla $\Rightarrow \sqrt{n} \notin I$.

[Dk.: nepřímou: dokážeme $\sqrt{n} \in Q \Rightarrow \exists m \in N : n = m^2$:

Necht' $\sqrt{n} \in Q \Rightarrow \exists a, b \in N : \sqrt{n} = \frac{a}{b}, D(a, b) = 1 \Rightarrow n = \frac{a^2}{b^2} \Rightarrow \underline{a^2 = n \cdot b^2}$

$$a = p_1^{r_1} \cdot p_2^{r_2} \cdot \dots \cdot p_k^{r_k}$$

$$b = p_1^{s_1} \cdot p_2^{s_2} \cdot \dots \cdot p_k^{s_k}$$

$$n = p_1^{t_1} \cdot p_2^{t_2} \cdot \dots \cdot p_k^{t_k}, \text{ kde } r_i, s_i, t_i \in N_0, i \in \{1, 2, \dots, k\}$$

$$p_1^{2r_1} \cdot p_2^{2r_2} \cdot \dots \cdot p_k^{2r_k} = p_1^{t_1} \cdot p_2^{t_2} \cdot \dots \cdot p_k^{t_k} \cdot p_1^{2s_1} \cdot p_2^{2s_2} \cdot \dots \cdot p_k^{2s_k}$$

$$p_1^{2r_1} \cdot p_2^{2r_2} \cdot \dots \cdot p_k^{2r_k} = p_1^{t_1+2s_1} \cdot p_2^{t_2+2s_2} \cdot \dots \cdot p_k^{t_k+2s_k}$$

$$2r_1 = t_1 + 2s_1 \Rightarrow t_1 = 2l_1$$

$$2r_2 = t_2 + 2s_2 \Rightarrow t_2 = 2l_2$$

$$\vdots \quad \quad \quad \vdots$$

$$2r_k = t_k + 2s_k \Rightarrow t_k = 2l_k, \text{ kde } l_i \in N$$

$$\underline{n = p_1^{2l_1} \cdot p_2^{2l_2} \cdot \dots \cdot p_k^{2l_k} = (p_1^{l_1} \cdot p_2^{l_2} \cdot \dots \cdot p_k^{l_k})^2 = m^2, m \in N}$$

Př.: Najděte takové nejmenší přirozené číslo a , že jeho 1224-násobek je druhou mocninou přirozeného čísla.

$$\underline{n^2} = 1224 \cdot a = 2^2 \cdot 306 \cdot a = 2^3 \cdot 153 \cdot a = \underline{2^3 \cdot 3^2 \cdot 17 \cdot a}$$

$$a = 2^{4-3} \cdot 3^{2-2} \cdot 17^{2-1} = 2 \cdot 17 = 34$$

$$(\text{potom } n^2 = 2^4 \cdot 3^2 \cdot 17^2 = (2^2 \cdot 3 \cdot 17)^2 = 204^2)$$

Př.: Najděte nejmenší dvojici přirozených čísel x, y , aby platilo $28x^4 = 75y^3$.

$$2^2 \cdot 7 \cdot x^4 = 3 \cdot 5^2 \cdot y^3, \quad x = 2^{a_1} \cdot 3^{a_2} \cdot 5^{a_3} \cdot 7^{a_4}, \quad y = 2^{b_1} \cdot 3^{b_2} \cdot 5^{b_3} \cdot 7^{b_4}$$

Dosazení za x a y :

$$2^{2+4a_1} \cdot 7^{1+4a_4} \cdot 3^{4a_2} \cdot 5^{4a_3} = 3^{1+3b_2} \cdot 5^{2+3b_3} \cdot 2^{3b_1} \cdot 7^{3b_4}$$

$$2 + 4a_1 = 3b_1 \quad \wedge \quad 4a_2 = 1 + 3b_2 \quad \wedge \quad 4a_3 = 2 + 3b_3 \quad \wedge \quad 1 + 4a_4 = 3b_4$$

$$a_1 = \frac{3b_1 - 2}{4} \quad a_2 = \frac{3b_2 + 1}{4} \quad a_3 = \frac{3b_3 + 2}{4} \quad a_4 = \frac{3b_4 - 1}{4}$$

$$\underline{b_1 = 2, a_1 = 1} \quad \underline{b_2 = 1, a_2 = 1} \quad \underline{b_3 = 2, a_3 = 2} \quad \underline{b_4 = 3, a_4 = 2}$$

(neboť $a_i, b_i \in N$ - nejmenší, $i \in \{1, 2, 3, 4\}$)

$$\underline{x} = 2^1 \cdot 3^1 \cdot 5^2 \cdot 7^2 = \underline{\underline{7350}} \quad \underline{y} = 2^2 \cdot 3^1 \cdot 5^2 \cdot 7^3 = \underline{\underline{102900}}$$

Př.: V autobusu je 45 sedadel, v osobním vagonu 120 sedadel. Výprava fotbalových fanoušků se přesouvala vlakem a vlakového nádraží potom přistavenými autobusy. Kolik bylo ve výpravě osob, když byla obsazena všechna sedadla ve vlaku i v autobusech a nikdo nemusel stát? Kolik nejméně vagonů měl vlak?

Počet fanoušků musí být zároveň dělitelný 45 i 120. Počet členů výpravy proto musí být společným násobkem čísel 45 a 120.

$$45 = 5 \cdot 9 = 3 \cdot 3 \cdot 5$$

$$120 = 12 \cdot 10 = 3 \cdot 4 \cdot 2 \cdot 5 = 2 \cdot 2 \cdot 2 \cdot 3 \cdot 5$$

$$\text{Tedy } n(45, 120) = 2 \cdot 2 \cdot 2 \cdot 3 \cdot 3 \cdot 5 = 360$$

Počet členů výpravy byl tedy některý násobek čísla 360.

$$360 \div 120 = 3$$

Vlak měl nejméně 3 vagony.

§6. Kritéria dělitelnosti

Pozn.: Kritériem dělitelnosti čísla $n \in N$ číslem $d \in N, d > 1$ rozumíme větu tvaru
 $\forall n, d \in N : d \mid n \Leftrightarrow d \mid f(n)$, kde $f(n)$ je číslo přiřazené číslu n určitým předpisem,
 zpravidla tak, že $f(n) < n$ a o dělitelnosti $f(n)$ číslem d lze snadno rozhodnout.

Pozn.: $\forall a, b \in N :$

$$(a+b)^1 = a+b$$

$$(a+b)^2 = a^2 + 2ab + b^2 = a^2 + b(2a+b) = b^2 + a(2b+a)$$

$$(a+b)^3 = a^3 + 3a^2b + 3ab^2 + b^3 = a^3 + b(\underbrace{3a^2 + 3ab + b^2}_k) = b^3 + a(\underbrace{3b^2 + 3ab + a^2}_l)$$

V.6.1: $\forall a, b, n \in N : \exists k, al \in N : (a+b)^n = a^n + bk = b^n + al$

[Dk.: plyne z binomické věty]

Př.: Dokažte: $3 \mid \underbrace{(41^{97})}_A - \underbrace{(26^{79})}_B$

$$A = 41^{97} = (42-1)^{97} = (-1+42)^{97} = (-1)^{97} + 42k = -1 + 42k, k \in N$$

$$B = 26^{79} = (27-1)^{79} = (-1+27)^{79} = (-1)^{79} + 27l = -1 + 27l, l \in N$$

$$A - B = -1 + 42k - (-1 + 27l) = -1 + 1 + 42k - 27l = 3(14k - 9l) \Rightarrow$$

$$\Rightarrow 3 \mid (41^{97} - 26^{79})$$

Pozn.: $a^1 + b^1 = a + b$

$$a^3 + b^3 = (a+b)(a^2 - ab + b^2)$$

$$a^1 - b^1 = a - b$$

$$a^2 - b^2 = (a-b)(a+b)$$

$$a^3 - b^3 = (a-b)(a^2 + ab + b^2)$$

$$a^4 - b^4 = (a-b)(a^3 + a^2b + ab^2 + b^3)$$

V.6.2: $\forall a, b \in Z : 1) \forall n \in N : (a-b) \mid (a^n - b^n)$

$$2) \forall n \in N, n \text{ liché} : (a+b) \mid (a^n + b^n)$$

[Dk.: 1) $a^n - b^n = (a-b)(a^{n-1} + a^{n-2}b + a^{n-3}b^2 + \dots + ab^{n-2} + b^{n-1})$

$$2) a^n + b^n = (a+b)(a^{n-1} - a^{n-2}b + a^{n-3}b^2 - \dots - ab^{n-2} + b^{n-1})]$$

Př.: Dokažte: $\forall n \in N : 7 \mid (2^{5n} - 5^{2n})$

$$2^{5n} - 5^{2n} = 32^n - 25^n = (32-25) \underbrace{(32^{n-1} + 32^{n-2} \cdot 25 + \dots + 25^{n-1})}_k = 7k, k \in N \Rightarrow$$

$$\Rightarrow 7 \mid (2^{5n} - 5^{2n})$$

Př.: Dokažte: $\forall n \in N : 17 \mid (5^{2n} + 2^{3n+4})$

$$5^{2n} + 2^{3n+4} = 25^n + 16 \cdot 8^n = 25^n - 8^n + 17 \cdot 8^n = (25-8)k + 17l = 17k + 17l = 17 \underbrace{(k+l)}_m =$$

$$= 17m, m \in N \Rightarrow 17 \mid (5^{2n} + 2^{3n+4})$$

Pozn.: Necht' $n \in N$, v jehož dekadickém zápisu je $k+1$ číslic. Potom se dá n vyjádřit:

$$\underline{n = a_k \cdot 10^k + a_{k-1} \cdot 10^{k-1} + \dots + a_1 \cdot 10 + a_0 = \sum_{i=0}^k a_i \cdot 10^i},$$

kde $a_k \neq 0, a_i \in \{0, 1, \dots, 9\}, i \in \{1, 2, \dots, k\}$.

Např.: $3532 = 3 \cdot 10^3 + 5 \cdot 10^2 + 3 \cdot 10 + 2$

V.6.3: Necht' $n \in N, n = a_k \cdot 10^k + a_{k-1} \cdot 10^{k-1} + \dots + a_1 \cdot 10 + a_0$. Pak platí:

- a) $2 \mid n \Leftrightarrow 2 \mid a_0$
- b) $4 \mid n \Leftrightarrow 4 \mid (a_1 \cdot 10 + a_0)$
- c) $5 \mid n \Leftrightarrow 5 \mid a_0$
- d) $8 \mid n \Leftrightarrow 8 \mid (a_2 \cdot 10^2 + a_1 \cdot 10 + a_0)$
- e) $10 \mid n \Leftrightarrow a_0 = 0$
- f) $25 \mid n \Leftrightarrow 25 \mid (a_1 \cdot 10 + a_0)$

[Dk.: $n = a_k \cdot 10^k + a_{k-1} \cdot 10^{k-1} + \dots + a_1 \cdot 10 + a_0 = 10 \underbrace{(a_k \cdot 10^{k-1} + a_{k-1} \cdot 10^{k-2} + \dots + a_1)}_l + a_0 =$
 $= 10l + a_0, l \in N$

- c) 1. „ \Rightarrow “: $5 \mid n \wedge 5 \mid 10l \Rightarrow 5 \mid a_0$
 2. „ \Leftarrow “: $5 \mid a_0 \wedge 5 \mid 10l \Rightarrow 5 \mid n$]

Def.: Necht' $n \in N, n = a_k \cdot 10^k + a_{k-1} \cdot 10^{k-1} + \dots + a_1 \cdot 10 + a_0$. Pak ciferným součtem čísla n nazveme číslo $S(n) = a_k + a_{k-1} + \dots + a_1 + a_0$.

V.6.4: Necht' $n \in N, n = a_k \cdot 10^k + a_{k-1} \cdot 10^{k-1} + \dots + a_1 \cdot 10 + a_0, S(n)$ je ciferný součet čísla n .

Pak platí: a) $3 \mid n \Leftrightarrow 3 \mid S(n)$

b) $9 \mid n \Leftrightarrow 9 \mid S(n)$

[Dk.: b) $10^k = (9+1)^k = 9l + 1^k = 9l + 1, l \in N$

$$n = a_k \cdot (9l_k + 1) + a_{k-1} \cdot (9l_{k-1} + 1) + \dots + a_1 \cdot (9l_1 + 1) + a_0$$

$$n = 9 \underbrace{(a_k l_k + a_{k-1} l_{k-1} + \dots + a_1 l_1)}_m + \underbrace{(a_k + a_{k-1} + \dots + a_0)}_{S(n)} = 9m + S(n), m \in N$$

- 1. „ \Rightarrow “: $9 \mid n \wedge 9 \mid 9m \Rightarrow 9 \mid S(n)$
- 2. „ \Leftarrow “: $9 \mid S(n) \wedge 9 \mid 9m \Rightarrow 9 \mid n$]

V.6.5: Necht' $n \in N, n = a_k \cdot 10^k + a_{k-1} \cdot 10^{k-1} + \dots + a_1 \cdot 10 + a_0$. Pak platí:

$$11 \mid n \Leftrightarrow 11 \mid (a_0 - a_1 + a_2 - a_3 + \dots + (-1)^k a_k)$$

[Dk.: $a_0 = a_0$

$$a_1 \cdot 10^1 = a_1 \cdot (11 - 1) = 11a_1 - a_1 = 11b_1 - a_1$$

$$a_2 \cdot 10^2 = a_2 \cdot (99 + 1) = 99a_2 + a_2 = 11b_2 + a_2$$

$$a_3 \cdot 10^3 = a_3 \cdot (1001 - 1) = 1001a_3 - a_3 = 11b_3 - a_2$$

\vdots

$$a_{2i-1} \cdot 10^{2i-1} = 11b_{2i-1} - a_{2i-2}$$

$$a_{2i} \cdot 10^{2i} = 11b_{2i} + a_{2i}$$

$$n = 11(\underbrace{b_1 + b_2 + b_3 + \dots + b_k}_m) + (\underbrace{a_0 - a_1 + a_2 - a_3 + \dots - a_{2i-1} + a_{2i} - \dots + (-1)^k a_k}_{S \pm(n)}) =$$

$$= 11m + S \pm(n), \quad m \in N$$

$$1. \text{ „} \Rightarrow \text{“: } 11 | n \wedge 11 | 11m \Rightarrow 11 | S \pm(n)$$

$$2. \text{ „} \Leftarrow \text{“: } 11 | S \pm(n) \wedge 11 | 11m \Rightarrow 11 | n \quad]$$

Př.: Rozhodněte, zda jsou daná čísla dělitelná 11:

a) 8628341 $S \pm(n) = 14 - 18 = -4$ není

b) 18436572 $S \pm(n) = 18 - 18 = 0$ je

V.6.6: Necht' $n \in N, n = 10k + a_0, k \in N$. Pak platí:

a) $7 | n \Leftrightarrow 7 | (k + 5a_0)$

b) $13 | n \Leftrightarrow 13 | (k + 4a_0)$

[Dk.: $n = 10k + a_0$

a) $b = k + 5a_0$

$$\underline{10b} = 10k + 50a_0 = 10k + a_0 + 49a_0 = \underline{n + 49a_0}$$

1. „ \Rightarrow “: $7 | n \wedge 7 | 49a_0 \Rightarrow 7 | 10b \Rightarrow 7 | b$, neboť $D(7,10)=1$

2. „ \Leftarrow “: $7 | b \Rightarrow 7 | 10b \wedge 7 | 49a_0 \Rightarrow 7 | n$

b) $b = k + 4a_0$

$$\underline{10b} = 10k + 40a_0 = 10k + a_0 + 39a_0 = \underline{n + 39a_0}$$

1. „ \Rightarrow “: $13 | n \wedge 13 | 39a_0 \Rightarrow 13 | 10b \Rightarrow 13 | b$, neboť $D(13,10)=1$

2. „ \Leftarrow “: $13 | b \Rightarrow 13 | 10b \wedge 13 | 39a_0 \Rightarrow 13 | n \quad]$

Př.: Rozhodněte, zda jsou daná čísla dělitelná 7:

a) 10248 $1024 + 5.8 = 1064$

$$106 + 5.4 = 126$$

$$12 + 5.6 = 42$$

je

b) 1698 $169 + 5.8 = 209$

$$20 + 5.9 = 65$$

není

Př.: Určete, zda číslo 281 je prvočíslo nebo číslo složené

Podle V.4.4. vyzkoušíme dělitelnost prvočísly menšími než $\sqrt{281} \doteq 16,8$:

$2 \nmid 281$, neboť $2 \nmid 1$

$3 \nmid 281$, neboť $3 \nmid (2 + 8 + 1)$

$5 \nmid 281$, neboť $5 \nmid 1$

$7 \nmid 281$, neboť $7 \nmid (28 + 5.1)$

$11 \nmid 281$, neboť $3 \nmid (2 - 8 + 1)$

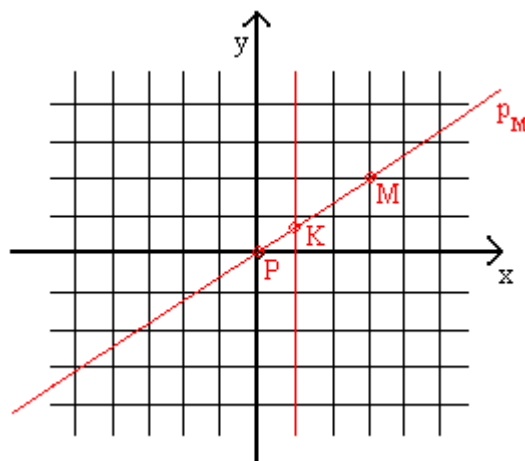
$13 \nmid 281$, neboť $13 \nmid (28 + 4.1)$

Číslo 281 nemá žádného prvočíselného dělitele menšího než jeho odmocnina, tedy číslo 281 je prvočíslo.

§7. Reálná čísla

Pozn.: Ukážeme méně obvyklý způsob vytvoření obrazů množin Q a I :

Zvolme v rovině systém souřadnic a vyznačme v něm body s celočíselnými souřadnicemi – tzv. mřížové body.



Libovolná přímka $p_M \Leftrightarrow PM$, která prochází počátkem P , protne přímku $x=1$ v bodě K (p_M je různá od x, y): $K[1, k]$

Přímka p_M má rovnici $y=kx, k \in R$.

Bod K budeme považovat za obraz reálného čísla k .

V.7.1: Necht' $M[q, p], q \neq 0$ je mřížový bod. Pak přímka p_M vytváří na přímce $x=1$ obraz racionálního čísla $\frac{p}{q}$.

[Dk.: Rovnice přímky $p_M: y=kx, k \in R$. Platí $M \in p_M \Rightarrow p=kq \Rightarrow k=\frac{p}{q} \Rightarrow k \in Q$]

V.7.2: a) Číslo $k \in Q \Leftrightarrow$ přímka $y=kx$ prochází alespoň jedním mřížovým bodem $M \neq P$.
b) Číslo $k \in I \Leftrightarrow$ přímka $y=kx$ neprochází žádným mřížovým bodem

[Dk.: a) „ \Rightarrow “: $k \in Q \Rightarrow \exists p, q; p \in Z, q \in N: k = \frac{p}{q}$

$$y=kx \Rightarrow y = \frac{p}{q}x \Rightarrow \text{bod } M \text{ o souřadnicích } [q, p] \text{ na této přímce leží,}$$

$$\text{protože } p = \frac{p}{q} \cdot q \text{ platí}$$

„ \Leftarrow “: Necht' p_M prochází mřížovým bodem $M[m, n]; m, n \in Z, m \neq 0$.

$$\text{Pak rovnice přímky } p_M \text{ je } y=kx, M \in p_M \Rightarrow n=km \Rightarrow k = \frac{n}{m} \Rightarrow k \in Q$$

b) „ \Rightarrow “: obměna a) „ \Leftarrow “

„ \Leftarrow “: obměna a) „ \Rightarrow “]

Pozn.: Nyní se budeme zabývat číslicovými zápisy racionálních a iracionálních čísel v dekadické soustavě.

Př.: Určete podíl $\frac{430}{132}$.

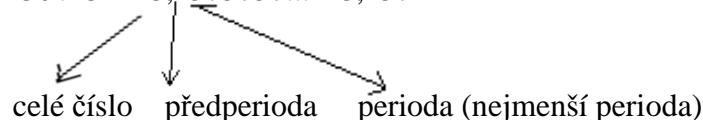
$$430:132 = 3,2575757\ldots = 3,25\overline{7}$$

Pozn.: Při výpočtu podílu $\frac{p}{q}$, $p \in \mathbb{Z}, q \in \mathbb{N}$ se mohou objevit jen takové zbytky z , že

$0 \leq z < q$. Těchto čísel je konečně mnoho (nejvýše q), a z toho plyne, že po nejvýše q krocích výpočtu se objeví stejný zbytek. Tedy v desetinném rozvoji se začnou opakovat číslice a vytvoří skupinu číslic, která se nazývá perioda.

Číslice nebo skupina číslic za desetinnou čárkou před touto periodou (která se neopakuje), se nazývá předperioda.

např.: $430 : 132 = 3,2575757\ldots = 3,2\overline{57}$



V.7.3: Každé racionální číslo $\frac{p}{q}$, $p \in \mathbb{Z}, q \in \mathbb{N}$ má periodický desetinný rozvoj, v němž má (nejmenší) perioda nejvýše q číslic.

[Dk.: plyne z předchozí poznámky]

Př.: Určete racionální číslo s desetinným rozvojem $1,28\overline{7} = r$.

$$\begin{aligned} 1000r &= 1287,\overline{7} \\ -(100r &= 128,\overline{7}) \\ \hline 900r &= 1159 \Rightarrow r = \underline{\underline{\frac{1159}{900}}} \end{aligned}$$

Pozn.: $0,\overline{9} = 0,9999\ldots$

$$10r = 9,\overline{9}$$

$$-r = -0,\overline{9}$$

$$9r = 9 \Rightarrow r = 1$$

Tedy $0,\overline{9} = 1 = 1,\overline{0}$

Periodický rozvoj, který má nejmenší periodu 9, můžeme vždy nahradit periodickým rozvojem s periodou 0, který představuje desetinné číslo s konečným počtem míst.

Proto v dalších úvahách budeme čísla s periodou 9 vylučovat.

V.7.4: Každé iracionální číslo má nekonečný neperiodický desetinný rozvoj.

např.: $\pi = 3,1415926535\ldots$

V.7.5: Každé reálné číslo má nekonečný desetinný rozvoj.

Pokud vyloučíme rozvoje s periodou 9, má každé reálné číslo právě jeden nekonečný desetinný rozvoj.

[Dk.: plyne z V.7.3., V.7.4. a předchozích poznámek]

Pozn.: Protože reálné číslo má nekonečný desetinný rozvoj, lze pro $\forall a \in \mathbb{R}^+, \forall r \in \mathbb{R}$ určit číslo a^r , tedy mocninu s reálným exponentem.

Pro počítání s takovými mocninami platí stejné věty jako pro mocniny s racionálními exponenty.

Př.: Vypočtete pro $a \in R^+$:

$$(a^{\sqrt{5}-\sqrt{2}})^{\sqrt{5}+\sqrt{2}} = a^{5-2} = a^3$$

Seznam použité literatury:

A. Literatura

- *Dr. Jaroslav Šedivý: ZÁKLADNÍ POZNATKY Z ALGEBRY A TEORIE ČÍSEL* – pro I.ročník gymnázií se zaměřením na matematiku, Praha, SPN 1986
- *RNDr. Pavel Boucník, RNDr. Jiří Herman, Ph.D., RNDr. Peter Krupka, Ph.D., doc. RNDr. Jaromír Šimša, CSc.: ODMATURUJ Z MATEMATIKY 3*, sbírka řešených příkladů, Brno, Didaktis 2004

B. Přednášky

- *RNDr. Pavel Boucník* – přednášky v matematické třídě pro I. ročník gymnázií
- *Mgr. Aleš Kobza, Ph.D.* - cvičení v matematické třídě pro I. ročník gymnázií

Resumé:

Úkolem mé závěrečné maturitní práce bylo obsáhnout a systematizovat učivo 1. ročníku z matematiky.

Převedla jsem do elektronické podoby přednášky z vlastních hodin matematiky a doplnila je o příklady ze cvičení a dalších učebnic.

Tato práce bude užitečná pro zefektivnění a usnadnění další výuky.

Tereza Eliášová