# TECHNICKÁ UNIVERZITA V LIBERCI

## PEDAGOGICKÁ FAKULTA

Katedra: matematiky a didaktiky matematiky

Kombinace oborů: matematika - informatika


# [2×2]-matice ve výuce v 5. až 9. třídě ZŠ

Diplomová práce 95-PF-KMD-006


Autor:

Libor OUŘADA

Podpis: Libor Ouřada

Adresa: Italská 2415

272 01, Kladno

Vedoucí práce: Doc. RNDr. Jaroslav Vild


| Počet | stran | obrázků | tabulek | příloh |
|---|---|---|---|---|
| | 46 | 5 | 3 | 0 |

V Liberci dne 22.5. 1995

Vysoká škola strojní a textilní
PEDAGOGICKÁ FAKULTA
461 17 LIBEREC 1, Hálkova 6 Telefon: 329 Telefax: 21301

Katedra: matematiky a didaktiky matematiky

# ZADÁNÍ DIPLOMOVÉ PRÁCE

(závěrečného projektu)

pro (diplomanta) Libora OUŘADU

adresa: Italská 2415, 272 01 Kladno 2

obor matematika - informatika

Název: [2x2]-matice ve výuce v 5. až 9. třídě ZŠ

Vedoucí práce: Doc. RNDr. Jaroslav Vild

Termín odevzdání: 15.5.1995

Pozn. Podmínky pro zadání práce jsou k nahlédnutí na katedrách. Katedry rovněž formulují podrobnosti zadání. Zásady pro zpracování DP jsou k dispozici ve dvou verzích (stručné, resp. metodické pokyny) na katedrách a na Děkanátě Pedagogické fakulty.

V Liberci dne 27. května 1994

J. Vild
vedoucí katedry

děkan

Převzal (diplomant):
Datum: 26. 5. 1994

Podpis: Ouřadu

**Prohlášení o původnosti práce:**

Prohlašuji, že jsem diplomovou práci vypracoval samostatně a že jsem uvedl veškerou použitou literaturu.

Liberec, 22. 5. 1995

Libor Ouřada

Libor Ouřada

**Poděkování:**

Děkuji vedoucímu práce Doc. RNDr. Jaroslavu Vildovi, bez jehož podnětných připomínek by tato práce nevznikla. Dále děkuji svým spolužákům za jejich dílčí pomoc a v neposlední řadě své přítelkyni za duševní podporu.

**Prohlášení k využívání výsledků DP:**

Jsem si vědom těchto skutečností:

a) diplomová práce je majetkem školy,

b) s diplomovou prací nelze bez svolení školy disponovat,

c) diplová práce může být zapůjčena či objednána (kopie) za účelem využití jejího obsahu.

Beru na vědomí, že po pěti letech si mohu diplomovou práci vyžádat v Univerzitní knihovně TU v Liberci, kde bude uložena.

Libor OUŘADA

Adresa: Italská 2415, 272 01 Kladno

Podpis: Libor Ouřada

[2×2]-matice ve výuce v 5. až 9. třídě ZŠ


## Anotace

Práce je zaměřena na některé možné aplikace matic na základní škole. Zabývá se zejména speciálními případy [2×2]-matic, kde jsou uváděna i některá méně známá fakta. Matice jsou pak uplatňovány v základech teorie maticových her, v geometrii, algebře a v kódování. Práce dále obsahuje experimentální uplatnění algebry [2×2]-matic na druhém stupni základní školy při opakování řetězců aritmetických úkonů.


The [2×2]-matrices in the tuition process in the 5th through 9th forms of elementary school


## Summary

This work is concerned with some applications of the matrices at elementary schools. It is particularly focused on special cases of the [2×2]-matrices, giving some less familiar facts as well. Then, matrices are utilized in the fundamentals of the matrix games, in geometry, algebra and coding. This work also deals with the experimental application of the [2×2]-matrix algebra in the 5th through 9th forms of elementary school in revising the strings of arithmetical operations.


Les [2×2]-matrices à l´enseignement de la 5. - 9. classe dans l´école primaire.


## Annotation

Le diplôme d`études supérieures concerne quelques possibilités d´application matrices dans l´école primaire. Il touche notamment les cas [2×2]-matrices citant aussi les faits moins connus. Les matrices sont puis utilisées dans les fondaments de la théorie des jeux matriciels, de la géométrie, de l´algèbre et dans le codage. Cet oeuvre contient aussi une application expérimentale de l´algèbre dans deuxième degré de l´école primaire pour la répétition des chaînes des procédures arithmétiques.

## OBSAH

-3-

## SEZNAM OZNAČENÍ:

| | |
|---|---|
| $\boldsymbol{N,Z,Q,R}$ | mn. přirozených, celých, rac., reálných čísel |
| $:=$ | " ...je definováno jako... " |
| $M^n := M\times..\times M$ | kartézský součin n exemplářů množiny M |
| $\pi$ | Ludolfovo číslo, $\pi$ = 3,141592... |
| $\mathbf{A,B,C}$ | matice |
| $\mathbf{A}^{-1}$ | matice inverzní k matici A |
| $\mathbf{A}^t$ | matice transponovaná k matici A |
| $\mathbf{E}$ | jednotková matice |
| $\mathbf{O}$ | nulová matice |
| det $\mathbf{A}$ | determinant matice A |
| St $\mathbf{A}$ | stopa matice A |
| $h(\mathbf{A})$ | hodnost matice A |
| $a_{ij}$ | prvek matice A v $i$-tém řádku a $j$-tém sloupci |
| $[r\times s]$-matice | matice s $r$ řádky a $s$ sloupci |
| $\boldsymbol{Z}_N$ | zbytkové třídy mod N |
| $\boldsymbol{Z}_{N,n}$ | $\boldsymbol{Z}_{N,n} := \boldsymbol{Z}_N^n$ |
| $r$-matice | $[r\times r]$-matice, tj. čtvercová matice stupně $r$ |
| $r$-řádek | řádkový vektor $[1\times r]$-matice |
| $s$-sloupec | sloupcový vektor $[s\times 1]$-matice |
| $a_{i*}$ | $i$-tý $s$-řádek $[r\times s]$-matice |
| $b_{*k}$ | $k$-tý $r$-sloupec $[r\times s]$-matice |
| $x$ | vektor $x$ |
| $x^\perp$ | vektor ortogonální k vektoru $x$ |
| $\|x\|$ | velikost vektoru $x$ |
| $\|x-y\|$ | vzdálenost mezi vektory |
| $\langle x,y\rangle$ | skalární součin |
| Id | identické zobrazení |
| $\circ$ | skládání funkcí |
| $\alpha, \beta, ..., \lambda$ | čísla |

-4-

## ÚVOD

Práce zpracovává některé možnosti použití [2×2]-matic ve výuce na základní škole. Poukazuje na některá méně známá fakta z teorie [2×2]-matic. Všímá si speciálních případů [2×2]-matic. Zabývá se jejich uplatněním v algebře, v geometrii (transformace souřadnic), matice jako zobrazení, v teorii maticových her ([2×2]-hry, [2×*m*]-hry, [*n*×2]-hry) a v kódování (hillovská šifra). Práce nabízí jednu z variant zavedení pojmu matice na základní škole.

Práce a obrázky byly vytvořeny v AmiPro 3.0.

-5-

## 1. TERMINOLOGICKÉ A HISTORICKÉ POZNÁMKY

Na začátek něco z historie pojmu, který je ústředním v této práci.

Termín matice [Ale-78:74$_{7-10}$ ] pochází z latinského slova matrix - matka živočicha. Souvisí s faktem, že první matice, jimiž se zabývali James Joseph Sylvestr a Arthur Cayley, generovaly lineární transformace. Vymezení matice dvěma svislými čarami zavedl A. Cayley (1843-1845), kulaté závorky užíval anglický matematik Cuthbert Edmund Cullis (1913). V současnosti se používají přednostně hranaté závorky, které zdůrazňují, že jde o obdélníkové schéma čísel.

V polovině 19. století vznikly matice současně při bádání několika vědců. Počátky teorie matic obsahuje stať Williama Rowana Hamiltona "Linear and vector functions" (Lineární a vektorové funkce, 1853). A. Cayley objevil, že se systémem čísel lze pracovat jako se samotným matematickým objektem, se kterým můžeme provádět algebraické úkony. A. Cayley a J.J. Sylvestr od roku 1843 rozvíjeli ideu maticového počtu. Základy maticového počtu uvedl A. Cayley v "Memoire on theory of matrix" (Pojednání o teorii matic, 1858). J.J. Sylvestr prozkoumal otázky spojené s teorií charakteristické rovnice.

V roce 1867 publikoval Edmond Nicolas Laguerre článek "Sur le calcul des systèmes lineaires" (O počítání s lineárními soustavami), ve které se matice uvádějí téměř v současné podobě. Nakonec Georg Ludwig Frobenius v článku "Über

-6-

lineare Substitutionen und bilinearen Formen" (O lineárních substitucích a bilineárních formách, 1878) dospěl k teorii matic kvadratických forem. Na konci 19. století tyto objevy spojil v jedinou teorii.

Pojem hodnosti matice zavedl J. Sylvester kolem r. 1850. Nedal mu však název, což je při jeho vášni zavádět nové termíny těžko vysvětlitelné. Termín pochází od G. Frobenia (asi r. 1879) z německého Rang (= stupeň, řád). Definici řádu determinantu a název Rang zavedl L. Kronecker r. 1880. Podmínku řešitelnosti soustavy, jejíž hodnost je rovna počtu rovnic, formuloval J. Heger r. 1858.

Pojem hodnosti matice a Frobeniova (či Kroneckerova-Capelliho věta) o řešitelnosti obecné soustavy se objevily nezávisle v pracích několika vědců. Formulace pomocí hodnosti je od A. Capelliho [Šed-84]. První vytištěný důkaz této věty náleží Ch. L. Dodgsonovi (1832-1898), který je znám (pseudonym Lewis Carroll) jako autor "Alenky v kraji divů a za zrcadlem" [Gus-83:213$^{9}_{11}$].

-7-

## 2. OBECNĚ O MATICÍCH

V této části práce si definujeme základní pojmy z teorie matic.

### *A. ZAVEDENÍ POJMU MATICE*

Definice: Pole P je každá neprázdná množina (komplexních) čísel, která má tyto dvě vlastnosti:

1, Obsahuje alespoň jedno číslo $p \neq 0$.

2, S každou dvojicí (stejných nebo různých čísel) $a \in P$, $b \in P$ obsahuje též součet $a + b$, rozdíl $a - b$, součin $ab$, a je-li $b \in 0$, též podíl $a/b$.

V dalším budeme zpravidla pracovat s polem **R** reálných čísel.

Definice: Tabulku $\mathbf{A} = [a_{ij}] = \begin{bmatrix} a_{11}, & a_{12}, & .., & a_{1n} \\ a_{21}, & a_{22}, & .., & a_{2n} \\ .., & .., & .., & .. \\ a_{m1}, & a_{m2}, & .., & a_{mn} \end{bmatrix}$

prvků z pole P nazýváme $[m \times n]$-maticí (nad P). Aritmetický vektor $(a_{i1}, a_{i2}, .., a_{in})$ z $P^n$ nazýváme $i$-tým řádkem matice **A** a aritmetický vektor $(a_{1j}, a_{2j}, .., a_{mj})$ z $P^m$ nazýváme $j$-tým sloupcem matice **A**.

Součtem dvou $[m \times n]$-matic

$$\mathbf{A} = \begin{bmatrix} a_{11}, & a_{12}, & .., & a_{1n} \\ a_{21}, & a_{22}, & .., & a_{2n} \\ .., & .., & .., & .. \\ a_{m1}, & a_{m2}, & .., & a_{mn} \end{bmatrix}, \quad \mathbf{B} = \begin{bmatrix} b_{11}, & b_{12}, & .., & b_{1n} \\ b_{21}, & b_{22}, & .., & b_{2n} \\ .., & .., & .., & .. \\ b_{m1}, & b_{m2}, & .., & b_{mn} \end{bmatrix}$$

-8-

rozumíme matici

$$\mathbf{A} + \mathbf{B} := \begin{bmatrix} a_{11}+b_{11} & a_{12}+b_{12} & .., & a_{1n}+b_{1n} \\ a_{21}+b_{21} & a_{22}+b_{22} & .., & a_{2n}+b_{2n} \\ .., & .., & .., & ... \\ a_{m1}+b_{m1} & a_{m2}+b_{m2} & .., & a_{mn}+b_{mn} \end{bmatrix}.$$

Je-li $r \in P$ libovolný prvek, pak $r$-násobkem matice **A** rozumíme matici $r\mathbf{A} := \begin{bmatrix} ra_{11}, & ra_{12}, & .., & ra_{1n} \\ ra_{21}, & ra_{22}, & .., & ra_{2n} \\ .., & .., & .., & .. \\ ra_{m1}, & ra_{m2}, & .., & ra_{mn} \end{bmatrix}$.

Matice **A** se rovná matici **B**, **A** = **B** , právě když $a_{ij} = b_{ij}$ pro všechna $i = 1,2,..,n$. $[n \times n]$-matice se nazývá čtvercová matice stupně $n$, stručně $n$-matice. O prvcích $a_{11}, a_{22}, .., a_{kk}$ $[m \times n]$-matice **A**, kde $k = \min(m,n)$, říkáme, že leží v (hlavní) diagonále, nebo že tvoří diagonálu matice **A**.

Definice: Buď $[m \times n]$-matice **A**, **A** = $[a_{ij}]$, a $[n \times p]$-matice **B**, **B** = $= [b_{ij}]$. Součinem **AB** těchto matic (v tomto pořadí!) rozumíme $[m \times p]$-matici **C** , kde $c_{ij} = \sum_{k=1}^{n} a_{ik}b_{kj}$.

Součin **AB** $[m \times n]$-matice **A** a $[k \times p]$-matice **B** je definován pouze tehdy, je-li $n = k$. V tomto případě je výsledkem $[m \times p]$-matice **AB**. Je-li definován součin **AB**, nemusí být definován součin **BA**. Je patrno, že oba součiny **AB**, **BA** jsou definovány, právě když **A** je $[m \times n]$-matice a **B** je $[n \times m]$-matice. Součin **AB** je čtvercová matice stupně $m$ , zatímco **BA** je čtvercová matice stupně $n$. Jsou-li **A** i **B** čtvercové matice stupně $n$, jsou oba součiny **AB**, **BA** definovány, avšak obecně

-9-

neplatí rovnost **AB** = **BA**, tj. obecně násobení není komutativní.

## *B. PRAVIDLA PRO POČÍTÁNÍ S MATICEMI*

Buď $[m\times n]$-matice **A**, buďte $[n\times p]$-matice **B**,**C**, buď $[p\times q]$-matice **D** a $r\in P$ libovolný prvek. Pak platí zákony:

Pro sčítání:

1. Komutativní: **A**+**B** = **B**+**A**
2. Asociativní: (**A**+**B**)+**C** = **A**+(**B**+**C**)

Pro skalární násobení matice číslem:

1. Komutativní: $a$**A** = **A**$a$
2. Asociativní: ($ab$)**A** = $a$($b$**A**)
3. Distributivní: $a$(**A**+**B**) = $a$**A**+$a$**B**

Pro násobení matic:

1. Asociativní: (**AB**)**D** = **A**(**BD**)
2. Distributivní: **A**(**B**+**C**) = **AB**+**AC**

(**B**+**C**)**D** = **BD**+**CD**

-10-

# *C. LINKOVÉ INTERPRETACE SOUČINU MATIC*

## 1. OBECNĚ

Součin **AB** $[r\times s]$-matice **A** a $[s\times t]$-matice **B** se obvykle zavádí (v souhlase se skládáním lineárních operátorů reprezentovaných maticemi **A**, **B** a formuluje pomocí skalárních součinů $s$-řádků matice **A** s $s$-sloupci matice **B**.

Existují však další užitečné interpretace součinu matic. Přirozené je vyjít z rozdělení každého z činitelů na linky, tj. na řádky nebo na sloupce. Matice tedy chápeme jako řádek sloupců, či sloupec řádků. Dostáváme tak 4 možnosti:

{řádky **A**, sloupce **A**}. {řádky **B**, sloupce **B**}

1. Řádky **A**. sloupce **B**. je zmíněná tradiční úvodní formulace součinu matic. Chápeme-li matici **A** jako sloupec jejích $s$-řádků $a_{i*}$ a matici **B** jako řádek jejích $s$-sloupců $b_{*k}$, pak

$$\mathbf{C} = \mathbf{AB} = \begin{bmatrix} a_{1*} \\ \cdot \\ \cdot \\ a_{i*} \\ \cdot \\ \cdot \\ a_{r*} \end{bmatrix} \begin{bmatrix} b_{*1}, & .., & b_{*k}, & .., & b_{*t} \end{bmatrix} =$$

-11-

$$= \begin{bmatrix} a_{1*}b_{*1} & a_{1*}b_{*2} & \dots & a_{1*}b_{*t} \\ a_{2*}b_{*1} & a_{2*}b_{*2} & \dots & a_{2*}b_{*t} \\ \cdot & & & \cdot \\ \cdot & & & \cdot \\ \cdot & & & \cdot \\ a_{r*}b_{*1} & a_{r*}b_{*2} & \dots & a_{r*}b_{*t} \end{bmatrix} = \left[ a_{i*}b_{*k} \right]_{\substack{i=1,..,r \\ k=1,..,t}}$$

Další dvě možnosti se uplatňují při teoretických úvahách např. o hodnostech matic. Součin **AB** nyní chápeme jako manipulaci s pravým, resp. s levým činitelem.

2. Řádky **A**. řádky **B**. $i$-tý řádek součinové matice vzniká lineární kombinací řádků (pravé) matice **B**. Koeficienty této lineární kombinace jsou prvky $i$-tého řádku (levé) matice **A**:

$$\mathbf{AB} = \begin{bmatrix} a_{1*} \\ \cdot \\ a_{i*} \\ \cdot \\ a_{r*} \end{bmatrix} \begin{bmatrix} b_{1*} \\ \cdot \\ \cdot \\ b_{j*} \\ \cdot \\ \cdot \\ b_{s*} \end{bmatrix} = \begin{bmatrix} \sum_{j=1}^{s} a_{1j}b_{j*} \\ \cdot \\ \cdot \\ \cdot \\ \sum_{j=1}^{s} a_{rj}b_{j*} \end{bmatrix},$$

předp., že $a_{i*}$ jsou $s$-vektory.

3. Sloupce **A**. sloupce **B**. $i$-tý sloupec součinové matice vzniká lineární kombinací sloupců (levé) matice **A**. Koeficienty této lineární kombinace jsou prvky $i$-tého sloupce (pravé) matice **B**:

$$\mathbf{AB} = \left[ a_{*1}, \dots, a_{*s}, \dots, a_{*s} \right] \left[ b_{*1}, \dots, b_{*k}, \dots, b_{*t} \right] =$$

$$= \left[ \sum_{j=1}^{s} b_{j1}a_{*j}, \dots, \sum_{j=1}^{s} b_{jk}a_{*j}, \dots, \sum_{j=1}^{s} b_{jt}a_{*j} \right]$$

4. Sloupce **A.** řádky **B.** Nyní chápeme matici **A** jako řádek jejích sloupců $a_{*i}$ a matici **B** jako sloupec jejích řádků $b_{k*}$, čímž dostáváme jiné (méně frekventované) vyjádření součinu **AB**:

$$\mathbf{AB} = \left[ a_{*1}, \ldots, a_{*j}, \ldots, a_{*s} \right] \begin{bmatrix} b_{1*} \\ \cdot \\ b_{j*} \\ \cdot \\ b_{s*} \end{bmatrix} = \sum_{j=1}^{s} a_{*j} b_{j*}$$

Tuto formulaci součinu matic můžeme nazvat sloupcově-řádkovou, neboť tentokrát se sloupce levé matice násobí (shodně umístěnými) řádky pravé matice (a tyto maticové mezivýsledky se pak sečtou). Součin matic je takto vyjádřen jako součet součinů sloupců s řádky. Každý z dílčích součinů (sloupec krát řádek) je matice (nejvýš) hodnosti 1. Tím jsme přepsali součin matic jako součet matic hodnosti 1, kde hodnost matice je počet nezávislých vektorů matice.

## 2. KONKRÉTNĚ [2×2]-MATICE

Řádky **A.** sloupce **B.**

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} e & f \\ g & h \end{bmatrix} = \begin{bmatrix} \begin{bmatrix} a & b \end{bmatrix} \begin{bmatrix} e \\ g \end{bmatrix}, & \begin{bmatrix} a & b \end{bmatrix} \begin{bmatrix} f \\ h \end{bmatrix} \\ \begin{bmatrix} c & d \end{bmatrix} \begin{bmatrix} e \\ g \end{bmatrix}, & \begin{bmatrix} c & d \end{bmatrix} \begin{bmatrix} f \\ h \end{bmatrix} \end{bmatrix} =$$

-13-

$$= \begin{bmatrix} ae+bg, & af+bh \\ ce+dg, & cf+dh \end{bmatrix} =: \mathbf{C}$$

Řádky **A.** řádky **B.**

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix}\begin{bmatrix} e & f \\ g & h \end{bmatrix} = \begin{bmatrix} a\begin{bmatrix} e & f \end{bmatrix}+b\begin{bmatrix} g & h \end{bmatrix} \\ c\begin{bmatrix} e & f \end{bmatrix}+d\begin{bmatrix} g & h \end{bmatrix} \end{bmatrix} =$$

$$= \begin{bmatrix} \begin{bmatrix} ae+bg, & af+bh \end{bmatrix} \\ \begin{bmatrix} ce+dg, & cf+dh \end{bmatrix} \end{bmatrix} = \mathbf{C}$$

Sloupce **A.** sloupce **B.**

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix}\begin{bmatrix} e & f \\ g & h \end{bmatrix} = \left[ \begin{bmatrix} a \\ c \end{bmatrix} e + \begin{bmatrix} b \\ d \end{bmatrix} g \, , \, \begin{bmatrix} a \\ c \end{bmatrix} f + \begin{bmatrix} b \\ d \end{bmatrix} h \right] =$$

$$= \left[ \begin{bmatrix} ae+bg \\ ce+dg \end{bmatrix}, \begin{bmatrix} af+bh \\ cf+dh \end{bmatrix} \right] = \mathbf{C}$$

Sloupce **A.** řádky **B.**

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix}\begin{bmatrix} e & f \\ g & h \end{bmatrix} = \begin{bmatrix} a \\ c \end{bmatrix}\begin{bmatrix} e & f \end{bmatrix} + \begin{bmatrix} b \\ d \end{bmatrix}\begin{bmatrix} g & h \end{bmatrix} =$$

$$= \begin{bmatrix} ae, & af \\ ce, & cf \end{bmatrix}+\begin{bmatrix} bg, & bh \\ dg, & dh \end{bmatrix} =$$

$$= \begin{bmatrix} ae+bg, & af+bh \\ ce+dg, & cf+dh \end{bmatrix} = \mathbf{C}$$

## *D. SPECIÁLNÍ VLASTNOSTI [2×2]-MATIC*

[1×1]-matice reprezentují reálná čísla, [2×2]-matice dávají první zajímavý případ maticové algebry. Objevují se zde

zvláštní jevy, a proto tento případ rozebíráme podrobněji [Koe-92:$84_8$-$5_{10}$].

Nejprve zjednodušíme označení na bezindexové a budeme psát $\mathbf{A} = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$.

Definujeme determinant [2×2]-matice, det **A** := ad - b. S hlediska hodnosti matice jsou možné pouze 3 disjunktní případy:

(1) $\begin{cases} h(\mathbf{A}) = 0 \text{ pro } \det \mathbf{A} = 0 \\ h(\mathbf{A}) = 1 \text{ pro } \det \mathbf{A} = 0, \det \mathbf{A} \neq 0 \\ h(\mathbf{A}) = 2 \text{ pro } \det \mathbf{A} \neq 0 \end{cases}$

Aplikací algebraických doplňků získáme hned vzorec pro inverzní [2×2]-matici $\mathbf{A}^{-1}$.

(2) $\mathbf{A}^{-1} = \frac{1}{\det \mathbf{A}} \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$ pro [2×2]-matici **A**, det **A** ≠ 0.

Inverzní matice k regulární matici se tedy získá prohozením prvků na hlavní diagonále, záměnou prvků na vedlejší diagonále jejich opačnými prvky a násobením inverzní hodnotou determinantu.

Máme též možnost ověřit větu o násobení determinantů pro [2×2]-matice **A**,**B**:

(3) $\det(\mathbf{AB}) = \det \mathbf{A} \times \det \mathbf{B}$

stejně tak jako vzorec známý jako Cayleyho věta

(4) $\mathbf{A}^2 - (\mathrm{St}\ \mathbf{A})\mathbf{A} + (\det \mathbf{A})\mathbf{E} = \mathbf{O}$ pro [2×2]-matici **A**,

kde St **A** je stopa matice **A**.

-15-

Stopa := součet prvků $[n\times n]$-matice ležících na diagonále.

Odtud plyne

$$\mathbf{A}[\mathbf{A} - (\mathrm{St}\ \mathbf{A})\mathbf{E}] = -(\det \mathbf{A})\mathbf{E}$$

a dostaneme nový vzorec pro inverzní matici

$$\mathbf{A}^{-1} = \frac{1}{\det \mathbf{A}} ((\mathrm{St}\ \mathbf{A})\mathbf{E} - \mathbf{A}) \quad pro \quad \det \mathbf{A} \neq 0.$$

Dále platí

$$\mathrm{St}(\mathbf{AB} - \mathbf{BA}) = 0,$$

z čehož plyne

$$(\mathbf{AB} - \mathbf{BA})^2 = \det(\mathbf{AB} - \mathbf{BA})$$

a dále

$$(\mathbf{AB} - \mathbf{BA})^2\mathbf{C} = \mathbf{C}(\mathbf{AB} - \mathbf{BA})^2.$$

Pokud tento vztah rozepíšeme, dostaneme pozoruhodnou identitu (zrcadlová symetrie vzhledem k rovnítku)

$$\mathbf{ABABC} - \mathbf{AB^2AC} - \mathbf{BA^2BC} + \mathbf{BABAC} = \mathbf{CABAB} - \mathbf{CBA^2B} - \mathbf{CAB^2A} + \mathbf{CBABA},$$

což platí pro všechny $[2\times2]$-matice $\mathbf{A}$, $\mathbf{B}$, $\mathbf{C}$.

# 3. APLIKACE [2×2]-MATIC NA 2. STUPNI ZŠ

V této části práce se budeme zabývat možnými aplikacemi [2×2]-matic na 2. stupni základních škol.

## *A. TRANSFORMACE SOUŘADNIC V ROVINĚ (GRUPA O(2))*

V přehledu teorie budeme postupovat podle německé učebnice [Koe-92:$137_3$-$141_4$].

### 1. OTÁČENÍ A OSOVÁ SOUMĚRNOST (ZRCADLENÍ).

Pro $\alpha \in \boldsymbol{R}$ platí

$$(1a)\quad \mathbf{T}(\alpha) := \begin{bmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{bmatrix},$$

$$(1b)\quad \mathbf{S}(\alpha) := \begin{bmatrix} \cos\alpha & \sin\alpha \\ \sin\alpha & -\cos\alpha \end{bmatrix} = \mathbf{T}(\alpha)\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

Pomocí součtové věty pro sinus a kosinus ověříme

$$(2)\quad \mathbf{T}(\alpha)\mathbf{T}(\beta) = \mathbf{T}(\alpha+\beta), \qquad \mathbf{S}(\alpha)\mathbf{S}(\beta) = \mathbf{T}(\alpha-\beta)$$

$$\mathbf{T}(\alpha)\mathbf{S}(\beta) = \mathbf{S}(\alpha+\beta), \qquad \mathbf{S}(\beta)\mathbf{T}(\alpha) = \mathbf{S}(\beta-\alpha)$$

Dále platí

$$(3)\quad \det \mathbf{T}(\alpha) = 1, \qquad \det \mathbf{S}(\alpha) = -1$$

$$(4)\quad [\mathbf{T}(\alpha)]^{-1} = \mathbf{T}(-\alpha) = [\mathbf{T}(\alpha)]^{t}, \quad [\mathbf{S}(\alpha)]^{-1} = \mathbf{S}(\alpha) = [\mathbf{S}(\alpha)]^{t}$$

$$(5)\quad \mathbf{T}(\beta)e(\alpha) = e(\alpha+\beta), \qquad \mathbf{S}(\beta)e(\alpha) = e(\beta-\alpha),$$

$$\text{kde } e(\alpha) := \begin{bmatrix} \cos\alpha \\ \sin\alpha \end{bmatrix}$$

Zobrazení $x \to \mathbf{T}(\beta)x$ tedy popisuje otáčení o úhel $\beta$.

Speciálně $x^{\perp} = \mathbf{T}(\pi/2)^{x}$.

Podle (1b) se $\mathbf{S}(\alpha)$ skládá z otáčení $\mathbf{T}(\alpha)$ a osové souměrnosti vzhledem k $x_1$, takže $x \to \mathbf{S}(\alpha)x$ popisuje osovou souměrnost.

Označíme-li

$O^{+}(2) := \{\mathbf{T}(\alpha); \alpha \in \boldsymbol{R}\} =: SO(2)$,

$O^{-}(2) := \{\mathbf{S}(\alpha); \alpha \in \boldsymbol{R}\}$,

$O(2) := O^{+}(2) \cup O^{-}(2)$,

pak z (2) a (4) vyplývá

Lemma: $O(2)$ je podgrupa z $GL(2;\boldsymbol{R})$ (lineární grupa [2×2]-matic, s reálnými prvky);

$O^{+}(2) = SO(2)$ je komutativní podgrupa z $O(2)$.

## 2. ORTOGONÁLNÍ MATICE

Definice: [2×2]-matice $\mathbf{T}$ se nazývá ortogonální, jestliže platí $\mathbf{T}^{t} \times \mathbf{T} = \mathbf{E}$. Zjevně T bude ortogonální, jestliže platí

(1) $\langle \mathbf{T}x, \mathbf{T}y \rangle = \langle x, y \rangle$ pro $x, y \in \boldsymbol{R}^2$

Věta: [2×2]-matice $\mathbf{T}$ je ortogonální,

právě když náleží do $O(2)$.

Důkaz: $\mathbf{T} \in O(2)$ je podle 1(4) ortogonální. Jestliže $\mathbf{T}$ je ortogonální a píšeme $\mathbf{T} = (a,b)$ jako dvojici sloupcových vektorů, pak platí $|a| = |b| = 1$ a $\langle a,b \rangle = 0$. Sloupec $a$ má

tvar $e(\alpha)$, můžeme dosadit $\mathbf{T} = \begin{bmatrix} \cos\alpha & \pm\sin\alpha \\ \sin\alpha & +\cos\alpha \end{bmatrix}$ a dostaneme $\mathbf{T} =$

$= \mathbf{T}(\alpha)$ nebo $\mathbf{T} = \mathbf{S}(\alpha)$.

Poznámka. Pomocí pojmu determinantu dostaneme

$$(2)\quad O^+(2) = \{\mathbf{T}\in O(2);\ \det \mathbf{T} = 1\} = SO(2)$$

$$O^-(2) = \{\mathbf{T}\in O(2);\ \det \mathbf{T} = -1\}$$

V grupové terminologii je det: $O(2) \to \{\pm 1\}$ epimorfismus grup, a jádro $O^+(2) = SO(2)$ je normální dělitel grupy $O(2)$ indexu 2.

Matice z $O^+(2)$ resp. $O^-(2)$ můžeme rozlišovat také podle stopy. Podle (1) při $\pm\begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \neq \mathbf{T}\in O(2)$ platí,

$\mathbf{T}\in O^+(2) \Leftrightarrow \mathrm{St}\ \mathbf{T} \neq 0$,

$\mathbf{T}\in O^-(2) \Leftrightarrow \mathrm{St}\ \mathbf{T} = 0$,

a kosinus úhlu otáčení $\mathbf{T}$ z $O^+(2)$ je $\frac{1}{2}\ \mathrm{St}\ \mathbf{T}$.

## 3. POHYBY

Každé zobrazení $\boldsymbol{R}^2$

$$(1)\quad x \mapsto f(x) = Tx + a,\ T\in O(2),\ a\in\boldsymbol{R}^2$$

nazýváme pohybem v $\boldsymbol{R}^2$.

Pohyby zachovávají vzdálenost $d(x,y) = |x-y|$ mezi dvěma body a úhel mezi dvěma směry.

Při vyšetřování geometrických problémů můžeme tedy pomocí pohybu zvolit vhodně souřadnicový systém aniž by se změnily vzdálenosti a úhly, které chceme zkoumat. Pohyb (1) nyzýváme vlastní (zachovávající orientaci), je-li T z $O^+(2)$.

Věta: Jestliže $f$: $\boldsymbol{R}^2 \to \boldsymbol{R}^2$, $f \neq \mathrm{Id}$, je vlastní pohyb, který není posunutím, potom má $f$ pevný bod.

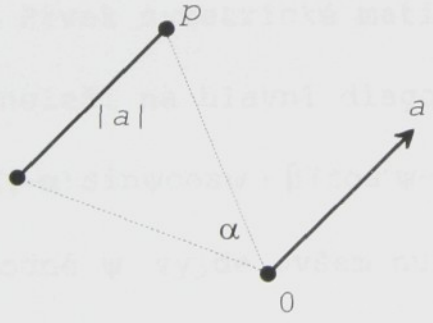
Důkaz: Zobrazení $f$ má formu (1) s $\mathbf{T} \in O^+(2)$, $\mathbf{T} \neq \mathbf{E}$. Je $\det(\mathbf{E}-\mathbf{T}) \neq 0$, takže $\mathbf{E}-\mathbf{T}$ je invertabilní. Je tedy $p := (\mathbf{E}-\mathbf{T})^{-1}a$ pevný bod zobrazení $f$.

Jestliže $p$ je pevným bodem $f$ a definujeme-li posunutí $g$ vztahem $g(x) := x+p$, dostaneme pro $h := g^{-1} \circ f \circ g$ ihned

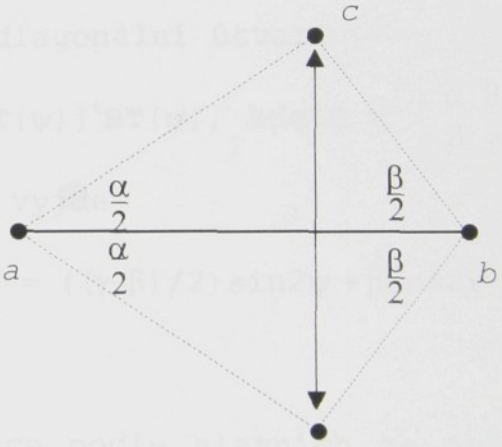
$$h(x) = (\mathbf{T}(x+p)+a) - p = \mathbf{T}x.$$

Odtud plyne na první pohled překvapivý důsledek, že vlastní pohyb v $\boldsymbol{R}^2$, který není posunutím, popisuje vždy otáčení v $\boldsymbol{R}^2$ okolo vhodného bodu v $\boldsymbol{R}^2$.

Na obr. 1 jsou šipky s koncovými body $a$ a $p$ rovnoběžné.




obr. 1




obr. 2

Je-li dán pohyb otáčením o úhel $\alpha$ a posunutím o $a \neq 0$, můžeme geometricky konstruovat pevný bod $p$ pomocí rovnoramen-

-20-

ného trojúhelníku se základnou $|a|$ a vrcholovým úhlem $\alpha$ (obr. 2).

Jsou-li dána dvě taková otáčení, pak jejich složením vznikne opět otáčení, pokud se to nezvrhne v posunutí. Pevný bod odtud můžeme lehce geometricky určit. Pokud se jedná o otáčení $f$ (resp. $g$) a úhlech $\alpha$ (resp. $\beta$) s pevným bodem $a$ (resp. $b$), dostaneme pevný bod složeného zobrazení $fog$ jako vrchol $c$ trojúhelníku nad úsečkou $ab$ s úhly při základně $\frac{\alpha}{2}$ a $\frac{\beta}{2}$ .

## 4. TRANSFORMACE PODLE HLAVNÍCH OS PRO [2×2]-MATICE

Matici $\mathbf{A}$ nazýváme symetrickou, platí-li $\mathbf{A} = \mathbf{A}^t$.

Věta: Ke každé reálné symetrické [2×2]-matici $\mathbf{S}$ existuje otáčení $\mathbf{T}$ z $O^+(2)$, tak že $\mathbf{T}^t\mathbf{S}\mathbf{T}$ má diagonální útvar.

Důkaz: Prvek symetrické matice $[\mathbf{T}(\psi)]^t\mathbf{S}\mathbf{T}(\psi)$, kde $\mathbf{S} = \begin{bmatrix} \alpha & \beta \\ \beta & \gamma \end{bmatrix}$, který neleží na hlavní diagonále, vyjde

$$(\gamma-\alpha)\sin\psi\cos\psi + \beta(\cos^2\psi-\sin^2\psi) = ((\gamma-\beta)/2)\sin 2\psi + \beta\cos 2\psi.$$

Pro vhodné $\psi$ vyjde ovšem nula.

Poznámka: Při problému transformace podle hlavních os nejde o explicitní určení matice $\mathbf{T}$, ale o přímé vypočtení diagonální matice $\mathbf{T}^t\mathbf{S}\mathbf{T} = \begin{bmatrix} \lambda & 0 \\ 0 & \mu \end{bmatrix}$ z $\mathbf{S}$. Vzhledem k

$$\det(\xi\mathbf{E}-\mathbf{S}) = \det(\mathbf{T}^t(\xi\mathbf{E}-\mathbf{S})\mathbf{T}) = \det(\xi\mathbf{E}-\mathbf{T}^t\mathbf{S}\mathbf{T}) = (\xi-\lambda)(\xi-\mu)$$

jsou $\lambda$ a $\mu$ právě nulové prvky $\xi$ kvadratického polynomu $\det(\xi\mathbf{E}-\mathbf{S})$.

-21-

## 5. PEVNÉ PŘÍMKY

Přímku $\boldsymbol{R}u$, $u \neq 0$, procházející počátkem, nazýváme pevnou přímkou matice $\mathbf{T} \in O(2)$ ( = invariantní při $\mathbf{T}$), jestliže se prostřednictvím $\mathbf{T}$ zobrazuje sama na sebe, tj. existuje-li $\lambda \in \boldsymbol{R}$, že $\mathbf{T}u = \lambda u$. Můžeme se omezit na případy $\mathbf{T} = \mathbf{T}(\alpha)$ nebo $\mathbf{T} = \mathbf{S}(\alpha)$. Protože $\mathbf{T}(\alpha)$ popisuje podle 1(5) otáčení o úhel $\alpha$, platí pro $u \neq 0$

$$\mathbf{T}(\alpha)u = \lambda u \iff \mathbf{T}(\alpha) = \pm\mathbf{E}, \quad \lambda = \pm 1,$$

takže $\alpha = \nu\pi$ pro $\nu \in \boldsymbol{Z}$. V případě osové souměrnosti $S(\alpha)$ ukazuje 1(5), že platí

$$\mathbf{S}(\alpha)e(\tfrac{\alpha}{2}) = e(\tfrac{\alpha}{2}) \text{ a } \mathbf{S}(\alpha)e(\tfrac{\alpha+\pi}{2}) = -e(\tfrac{\alpha+\pi}{2}).$$

Má tedy každá osová souměrnost dvě ortogonální pevné přímky, z nichž jedna je pevná po bodech.

## 6. DVĚ ORIENTACE ROVINY

V rovině $\boldsymbol{R}^2$ může být orientace dána tím, že označíme jeden z možných směrů otáčení okolo počátku jako kladný. V matematice a fyzice se jako kladný označuje směr, který jde proti směru pohybu hodinových ručiček. Častá představa, že se přitom musíme dívat "z $\boldsymbol{R}^3$ na $\boldsymbol{R}^2$" se nepotvrzuje.

Říkáme, že dvojice $a,b$ dvou vektorů $\boldsymbol{R}^2$ je

- kladně orientovaná, je-li $\det(a,b) > 0$
- záporně orientovaná, je-li $\det(a,b) < 0$

-22-

Na příkladu kanonické báze vidíme, že pak vzniká $b = e_2$ z $a = e_1$ otáčením o $\frac{\pi}{2}$ v kladném směru otáčení.

Je-li dvojice $(a,b)$ kladně orientovaná, pak pro ortogonální matici $\mathbf{T}$ dvojice $(\mathbf{T}a, \mathbf{T}b)$ je

$$\begin{cases} \text{kladně orientovaná,} & \text{je-li } \mathbf{T} \text{ otáčení,} \\ \text{záporně orientovaná,} & \text{je-li } \mathbf{T} \text{ zrcadlení.} \end{cases}$$

Vzhledem ke vztahu $\det(a, a^{\perp}) = |a^2|$ jsou $a$ a $a^{\perp}$ vždy kladně orientované, jestliže $a \neq \mathbf{0}$.

Příklad: Početně a na obrázku (obr. 3) sledujeme 5 transformací působících na asymetrický domeček s levým oknem. Všechny transformace budeme provádět zároveň s posunutím o vektor $a = (2,1)$.

1, Otočení o úhel $\alpha = 60°$:

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} \cos 60° & -\sin 60° \\ \sin 60° & \cos 60° \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} + \begin{bmatrix} 2 \\ 1 \end{bmatrix}.$$

2, Otočení o úhel $\alpha = -60°$:

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} \cos(-60°) & -\sin(-60°) \\ \sin(-60°) & \cos(-60°) \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} + \begin{bmatrix} 2 \\ 1 \end{bmatrix}$$

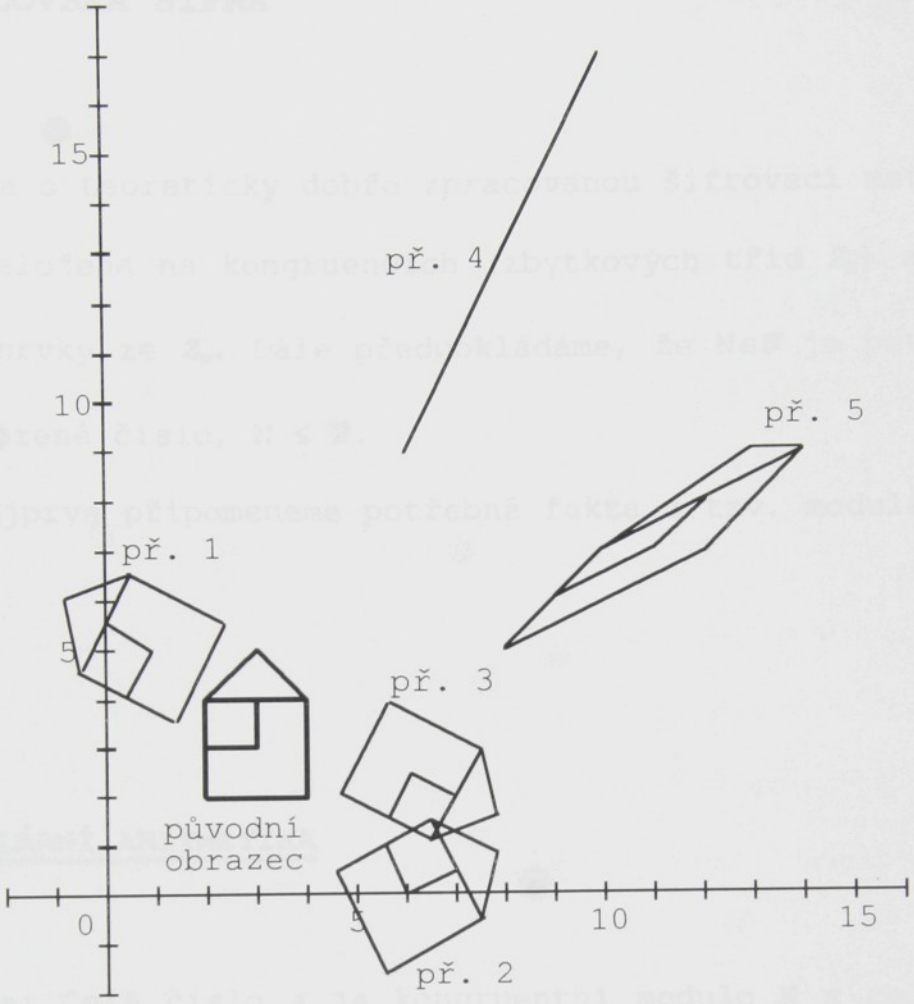
3, Zrcadlení a otočení o úhel $\alpha = 60°$:

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} \cos 60° & \sin 60° \\ \sin 60° & -\cos 60° \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} + \begin{bmatrix} 2 \\ 1 \end{bmatrix}$$

4, $h(\mathbf{A}) = 1$, $\begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 2 & 2 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} + \begin{bmatrix} 2 \\ 1 \end{bmatrix}$

5, $h(\mathbf{A}) = 2$, $\begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} + \begin{bmatrix} 2 \\ 1 \end{bmatrix}$

-23-




obr. 3

-24-

## *B. HILLOVSKÁ ŠIFRA*

Jde o teoreticky dobře zpracovanou šifrovací metodu, která je založena na kongruencích (zbytkových tříd $\boldsymbol{Z}_N$) a na maticích s prvky ze $\boldsymbol{Z}_N$. Dále předpokládáme, že $N \in \boldsymbol{N}$ je pevně zvolené přirozené číslo, $N \leq 2$.

Nejprve připomeneme potřebná fakta z tzv. modulární aritmetiky.

### 1. MODULÁRNÍ ARITMETIKA

Definice: Celé číslo $a$ je kongruentní modulo N s celým číslem $b$, je-li rozdíl $a-b$ je (beze zbytku) dělitelný číslem N. Symbolicky to zapisujeme

$$a \equiv b \pmod{N}.$$

V opačném případě říkáme, že čísla $a,b$ jsou nekongruentní modulo N:

$$a \not\equiv b \pmod{N}$$

Číslo N se nazývá modul kongruence. V případě, že modul N je v našich úvahách neměnný, zjednodušeně říkáme, že čísla $a$, $b$ jsou kongruentní.

-25-

Vztah $a \equiv b \pmod N$ platí, právě když čísla $a$, $b$ dávají po dělení číslem N shodný zbytek.

*a, VLASTNOSTI KONGRUENCE*

Kongruence je binární relace na $\mathbb{Z}_N$, pro niž platí tyto vztahy [GP-92:32-33$_{17}$]:

$a \equiv a \pmod N$ pro každé $a \in \mathbb{Z}$;

je-li $a \equiv b \pmod N$, pak $b \equiv a \pmod N$;

je-li $a \equiv b \pmod N$ a $b \equiv c \pmod N$, pak $a \equiv c \pmod N$

Kongruence je tedy reflexivní, symetrická a tranzitivní relace. Takové relace nazýváme ekvivalencemi. Zadávají rozklady základní množiny, v našem případě množiny $\mathbb{Z}$. Při modulu N platí

$$\mathbb{Z} = (N\mathbb{Z}) \cup (N\mathbb{Z}+1) \cup (N\mathbb{Z}+2) \cup (N\mathbb{Z}+N-1).$$

Výhodné je reprezentovat rozkladové třídy v $\mathbb{Z}$ vhodným úplným systémem zbytků - nejčastěji čísly blízkými k nule:

$$\mathbb{Z}_N = \{0, 1, \ldots, N-1\}$$

*b, KONGRUENCE A ARITMETICKÉ OPERACE*

Kongruence je (jako ekvivalence) zobecněním rovnosti a má obdobné vlastnosti a vztahy k aritmetickým operacím (sčítání, odčítání, násobení, spec. umocňování na přirozený exponent).

-26-

Je-li $a \equiv b \pmod N$ a zároveň

$c \equiv d \pmod N$, pak

$a \omega c \equiv b \omega d \pmod N$, kde $\omega \in \{+, -, \times\}$.

Speciálně $a^k = b^k \pmod N$, pro $k \in \boldsymbol{N}$.

Je-li $ac \equiv bc \pmod N$ a čísla $c$, N jsou nesoudělná,

pak $a \equiv b \pmod N$

Odtud plyne, že počítání v $\boldsymbol{Z}_N$ lze provádět v $\boldsymbol{Z}$ a na závěr redukovat výsledek do množiny $\{0, 1, \ldots, N-1\}$.

## 2. MATICE NAD $Z_N$

Dále pracujeme s $[n \times n]$-maticemi s prvky ze $\boldsymbol{Z}_N$, tj. maticemi tvaru

$$(1) \quad \begin{bmatrix} a_{1,1}, & a_{1,2}, & .., & a_{1,n} \\ a_{2,1}, & a_{2,2}, & .., & a_{2,n} \\ .., & .., & .., & .. \\ a_{n,1}, & a_{n,2}, & .., & a_{n,n} \end{bmatrix}, \text{ kde } a_{i,j} \in \boldsymbol{Z}_N, \ 1 \le i, j \le n.$$

Říkáme, že $[n \times n]$-matice **A** je regulární nad $\boldsymbol{Z}_N$, jestliže existuje $[n \times n]$-matice **B** s prvky ze $\boldsymbol{Z}_N$, taková, že jejich maticový součin **A**×**B** nad $\boldsymbol{Z}_N$ se rovná jednotkové matici $\mathbf{E}_N$. Matici **B** nazýváme inverzní maticí k matici **A** a označujeme je $\mathbf{A}^{-1}$. Dále platí, že regulární matice je taková matice, jejíž determinant má v $\boldsymbol{Z}_N$ vzhledem k násobení inverzní prvek. Víme, že prvek $x \in \boldsymbol{Z}_N$ má v $\boldsymbol{Z}_N$ vzhledem na násobení inverzní prvek,

právě když $x$ je nesoudělný s modulem N, tj. když největší společný dělitel čísel $x$, N je roven 1, nsd($x$,N) = 1.

Příklad: Determinant matice $\begin{bmatrix} 3 & 7 & 9 \\ 11 & 10 & 2 \\ 5 & 4 & 13 \end{bmatrix}$ se rovná -844.

Jelikož -844 je nesoudělné s 5, tak je tato matice regulární nad $\mathbb{Z}_5$. Není však regulární nad $\mathbb{Z}_{211}$, neboť nsd(-844,211) = 211.

Je-li $\mathbf{A} = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$, kde $a, b, c, d \in \mathbb{Z}_N$,

regulární [2×2]-matice s determinantem $\delta$, nsd($\delta$,N),

pak k ní inverzní matice $\mathbf{A}^{-1}$ má tvar

$$\mathbf{A}^{-1} = \begin{bmatrix} d\delta' & -b\delta' \\ -c\delta' & a\delta' \end{bmatrix}, \text{ kde } a, b, c, d \in \mathbb{Z}_N,$$

kde $\delta'$ je prvek inverzní k $\delta$ v $\mathbb{Z}_N$, pro který platí $\delta \times \delta' \equiv 1 \pmod{N}$.

V dalším se budeme zejména zabývat tzv. involutorními maticemi. Involutornost znamená, že příslušná matice **A** má tu vlastnost, že její součin se sebou nad $\mathbb{Z}_N$ se rovná jednotkové matici, tj. že

$$\mathbf{A}^2 := \mathbf{A} \times \mathbf{A} \equiv \mathbf{E} \pmod{N}.$$

Protože det **E** ≡ 1 a det(**AB**) = det **A** × det **B**, je $(\det \mathbf{A})^2 \equiv 1 \pmod{N}$. V každém $\mathbb{Z}_N$ existují jen dva takové prvky, a to 1 a N-1. Protože N-1 ≡ -1 (mod N), můžeme říci, že:

$$\mathbf{A}^2 \equiv \mathbf{E} \Rightarrow \det \mathbf{A} \equiv \pm 1 \pmod{N}.$$

Toto je však jen nutná podmínka pro involutorní matice. Existují totiž matice, které nejsou involutorní, ale je-

jichž determinant je roven 1 nebo -1 (mod N). Například pro každé N > 10 je takovou maticí $\begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix}$.

## 3. ŠIFROVÁNÍ A DEŠIFROVÁNÍ

Hillovu myšlenku budeme nejprve prezentovat všeobecně, a potom ji budeme aplikovat na telegrafickou abecedu [GP-92:122-126]. V úvodním kódování se převádějí abecední znaky do množiny $Z_N = \{0,1,2,\ldots,N-1\}$, kde N je počet znaků dané abecedy (základní). Textem nad abecedou $Z_N$ budeme rozumět uspořádanou $d$-tici $x = (x_1, x_2, \ldots, x_d)$, kde $x \in Z_N$ pro $1 \leq i \leq d$. Počet $d$ znaků textu nazýváme délkou textu.

Množinu všech uspořádaných $n$-tic nad $Z_N$ budeme považovat

$Z_{N,n} := Z_N^n = Z_N \times Z_N \times \ldots \times Z_N$ ($n$ exemplářů množiny $Z_N$).

Kryptografické transformace hillovského kryptografického systému jsou dány prostřednictvím regulárních $[n \times n]$-matic (1).

V případě potřeby (tj. tehdy, když délka $d$ původního textu není dělitelná číslem $n$) se původní text doplní potřebným počtem znaků podle dohody (např. přidáváním posledního znaku).

Každé dílčí $n$-tici $(x_1, x_2, .., x_n)$ znaků $x_i \in Z_N$ původního textu přiřadíme novou $n$-tici $(y_1, y_2, .., y_n)$ znaků $y_i \in$

-29-

$\mathbb{Z}_n$ zašifrovaného textu, která je dána vztahem (násobení $[n\times n]$-matice $n$-sloupcem)

$$\begin{bmatrix} y_1 \\ y_2 \\ .. \\ y_n \end{bmatrix} = \begin{bmatrix} a_{1,1}, & a_{1,2}, & .., & a_{1,n} \\ a_{2,1}, & a_{2,2}, & .., & a_{2,n} \\ .., & .., & .., & .. \\ a_{n,1}, & a_{n,2}, & .., & a_{n,n} \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ .. \\ x_n \end{bmatrix},$$

tj. souřadnicově.

$$y_i \equiv \sum_{j=1}^{n} a_{i,j} \times x_j \pmod{N}, \quad \text{pro} \quad 1 \leq i \leq n.$$

Jde ovšem o zobrazení $\mathbb{Z}_N^n$ do $\mathbb{Z}_N^n$. Obvykle pracujeme s malým $n$. Pro $n = 2$ dostáváme ovšem $[2\times2]$-matice.

Dále nás zajímá nejčastější případ N = 26 (telegrafická abeceda s 26 znaky). Matice nad $\mathbb{Z}_{26}$ je regulární, právě když je její determinant liché číslo a není dělitelný číslem 13.

Zajímavým případem hillovských šifer je existence tzv. involutorní kryptografické transformace. Rozumíme tím transformace, které splývají se svými inverzními transformacemi. Jinými slovy: při involutorní kryptografické transformaci se stejné transformace používá při zašifrování původního textu a i při dešifrování zašifrovaného textu.

Zůstaňme u problému involutorních $[2\times2]$-matic, protože matice tohoto typu jsou nejjednodušími případy netriviálního použití hillovských šifer. Pro nás jsou nejzajímavější 2 případy:

$$\begin{cases} \text{telegrafní abeceda bez mezery, tj. } N = 26 \\ \text{telegrafní abeceda s mezerou, tj. } N = 27 \end{cases}$$

Při $N = 26$ existuje pouze 7 involutorních matic s determinantem $1 \pmod N$:

$$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 13 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 13 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 14 & 13 \\ 13 & 14 \end{bmatrix}, \begin{bmatrix} 25 & 0 \\ 0 & 25 \end{bmatrix},$$

$$\begin{bmatrix} 25 & 0 \\ 13 & 25 \end{bmatrix}, \begin{bmatrix} 25 & 13 \\ 0 & 25 \end{bmatrix}.$$

Pro $N = 27$ existují jenom dvě takové matice:

$$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 26 & 0 \\ 0 & 26 \end{bmatrix}.$$

Proto jsou z kryptografického hlediska pro $N = 26$ nebo $N = 27$ zajímavější involutorní matice s determinantem $\delta \equiv -1 \pmod N$. Těch je pro $N = 26$ celkově 365 a pro $N = 27$ celkově 478.

Involutorní [2×2]-matice

$$\mathbf{A} = \begin{bmatrix} a & b \\ c & d \end{bmatrix}, \quad \text{kde } a, b, c, d \in \mathbf{Z}_N, \ \delta \equiv -1 \pmod N$$

můžeme jednoduše určit pomocí již známého výrazu pro inverzi [2×2]-matice

$$\mathbf{A}^{-1} = \begin{bmatrix} d\delta' & -b\delta' \\ -c\delta' & a\delta' \end{bmatrix}.$$

Z požadované rovnosti $\mathbf{A} \equiv \mathbf{A}^{-1} \pmod N$, rozepsané prvkově

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \equiv \begin{bmatrix} d\delta' & -b\delta' \\ -c\delta' & a\delta' \end{bmatrix}$$

dostaneme za předpokladu $\delta \equiv -1 \pmod N$, že matice $\mathbf{A}$ je involutorní, právě když

$$a \equiv -d \pmod{N},$$

$$d \equiv -a \pmod{N}.$$

To znamená, že matice **A** nad $Z_N$ s determinantem $\delta \equiv -1 \pmod{N}$ je involutorní, právě když pro její prvky $a,d$ na hlavní úhlopříčce platí

$$a + d \equiv 0 \pmod{N}.$$

Proto nám pro nalezení konkrétní involutorní matice, jejíž determinatnt $\delta$ je kongruentní s -1 modulo N, stačí určit čísla $a, b, c, d$ tak, že současně splňují kongruence

$$a + d \equiv 0 \pmod{N},$$

$$ad - bc \equiv -1 \pmod{N}.$$

Jedno takové řešení pro N = 26 je $\begin{bmatrix} 3 & 2 \\ 9 & 23 \end{bmatrix}$,

kde $\delta = \delta' = 69 - 18 \equiv -1 \pmod{26}$.

Příklad: Zašifrujme a dešifrujme text STUDENT hillovslou involutorní šifrou modulo 26 (telegrafní abeceda bez mezery) pomocí matice

$$\mathbf{A} = \begin{bmatrix} 3 & 2 \\ 9 & 23 \end{bmatrix}.$$

Text má lichý počet znaků, přidáme poslední znak textu. Nyní budeme šifrovat tento text

| S | T | U | D | E | N | T | T |
|---|---|---|---|---|---|---|---|
| 18 | 19 | 20 | 3 | 4 | 13 | 19 | 19 |

Znaky převádíme na čísla podle tab. 1

Tab. 1

| | | | |
|---|---|---|---|
| A ↔ 0 | G ↔ 6 | M ↔ 12 | S ↔ 18 | Y ↔ 24 |
| B ↔ 1 | H ↔ 7 | N ↔ 13 | T ↔ 19 | Z ↔ 25 |
| C ↔ 2 | I ↔ 8 | O ↔ 14 | U ↔ 20 | |
| D ↔ 3 | J ↔ 9 | P ↔ 15 | V ↔ 21 | |
| E ↔ 4 | K ↔ 10 | Q ↔ 16 | W ↔ 22 | |
| F ↔ 5 | L ↔ 11 | R ↔ 17 | X ↔ 23 | |

Šifrování provedeme jen pro úvodní dvojici písmen:

$$\begin{bmatrix} 3 & 2 \\ 9 & 23 \end{bmatrix}\begin{bmatrix} S \\ T \end{bmatrix} = \begin{bmatrix} 3 & 2 \\ 9 & 23 \end{bmatrix}\begin{bmatrix} 18 \\ 19 \end{bmatrix} = \begin{matrix} 92 \\ 599 \end{matrix} \equiv \begin{bmatrix} 14 \\ 1 \end{bmatrix} = \begin{bmatrix} O \\ B \end{bmatrix} \mod(26)$$

Celkem text STUDENTT se zašifruje na text OBOPMXRK.

Jde o involutorní hillovslou šifru, takže dešifrování se provede stejnou maticí:

$$\begin{bmatrix} 3 & 2 \\ 9 & 23 \end{bmatrix}\begin{bmatrix} O \\ B \end{bmatrix} = \begin{bmatrix} 3 & 2 \\ 9 & 23 \end{bmatrix}\begin{bmatrix} 14 \\ 1 \end{bmatrix} = \begin{bmatrix} 44 \\ 149 \end{bmatrix} \equiv \begin{bmatrix} 18 \\ 19 \end{bmatrix} = \begin{bmatrix} S \\ T \end{bmatrix} \mod(26)$$

Celkem text OBOPMXRK se dešifruje na text STUDENTT.

Vlastní využití hillovské šifry na základní škole.

Šifrování je jedna z věcí, která budí v člověku pocit tajemna. Pokud se dětem ve třídě řekne, že se budou zabývat šifrováním, tak podle mého názoru je snadné udržet si po dlouhou dobu výuky jejich pozornost. Hillovská šifra je vhodná na procvičování násobení matic. Její výhoda je v jednoduchém násobení [2×2]-matice s [2×1]-maticí.

-33-

## *C. TEORIE MATICOVÝCH HER*

V této kapitole se budeme zabývat využitím matic v teorii her, kdy jeden z hráčů má dvě strategie (rozhodnutí, volby) a druhý dvě a více strategií [Wil-66:42-105].

Maticová hra je dána tzv. výplatní $[r \times s]$-maticí $\mathbf{A} = [a_{ik}]$ s reálnými prvky $a_{ik}$. Hru hrají dva hráči, z nichž

řádkový hráč (Radek) volí čísla řádků, $i = 1,..,r$

sloupcový hráč (Simona) volí čísla sloupců, $k = 1,..,s$

Při každé partii vybere Radek konkrétní $i$-tý řádek a nezávisle Simona konkrétní $k$-tý sloupec. Výplata mezi hráči je dána prvkem $a_{ik}$ výplatní matice:

je-li $a_{ik}$ kladné číslo,

Radek bere $a_{ik}$ (Kč)

Simona ztrácí $a_{ik}$ (Kč)

je-li $a_{ik}$ záporné číslo,

Radek ztrácí $a_{ik}$ (Kč)

Simona bere $a_{ik}$ (Kč).

Hra pak sestává ze série takových partií. Cílem každého z (inteligentních) hráčů je dopadnout při dané výplatní matici co nejlépe (tj. co nejvíce vyhrát či co nejméně tratit). K tomu volí (pokud existuje) každý hráč svoji tzv. optimální strategii.

-34-

Teorie maticových $[r \times s]$-her je dobře známa [Vor-74:7-32; Maň-74:47-2[23]]. Stěžejním pojmem je u tohoto typu her sedlový bod funkce $f$ dvou proměnných, $f: \boldsymbol{R}^2 \rightarrow \boldsymbol{R}$.

Definice: Funkce $f(x,y)$ má sedlový bod v bodě $[a,b]$, platí-li

$$f(x,b) \leq f(a,b) \leq f(a,y)$$

pro $x \in (a-h, a+h)$, $y \in (a-k, a+k)$.

Příklad: $f(x,y) := y^2 - x^2$ má sedlový bod v $[0,0]$, neboť

$$-x^2 \leq 0 \leq y^2 \quad \text{pro} \quad x, y \in \boldsymbol{R}$$

$$g(x,y) := x^2 - y^2$$

nemá podle naší definice sedlový bod.

Další pojmy, které potřebujeme znát, jsou maxmin $a_{ik}$ a minmax $a_{ik}$, které se vypočítávají z výplatní matice **A**. Slovem maxmin označujeme největší, tj. maximální minimum řádků, minmax je nejmenší, tj. minimální maximum sloupců.

$$\left.\begin{array}{l} \left[\begin{array}{cccc} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \cdots & \cdots & a_{ik} & \cdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{array}\right] \rightarrow \begin{array}{l} \min a_{1k} \\ \min a_{2k} \\ \\ \min a_{mk} \end{array} \end{array}\right\} \text{maxmin } a_{ik}$$

$$\underbrace{\max a_{i1} \quad \max a_{i2} \quad \max a_{in}}_{\text{minmax } a_{ik}}$$

-35-

## 1. [2×2]-HRY

Prvním zajímavým případem maticových her dvou hráčů, kdy každý hráč má osud ve svých rukách (v rámci pravidel), jsou [2×2]-hry. Zde má řádkový i sloupcový hráč k dispozici dvě volby (čisté strategie): 1. nebo 2. řádek, resp. sloupec. Taková hra je dána [2×2]-maticí $\mathbf{A} = [a_{ik}]$.

$$\begin{array}{c} \\ x \\ 1-x \end{array} \begin{array}{c} \begin{array}{cc} y & 1-y \end{array} \\ \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix} \end{array} \text{, kde}$$

- vektor X = [x,1-y] je smíšenou strategií řádkového hráče
- vektor Y = [x,1-y] je smíšenou strategií sloupc. hráče

V [Vor-74:32[15]-5] je zkoumána výplatní funkce

$$H(X,Y) := XAY^T = \begin{bmatrix} x, & 1-x \end{bmatrix} \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix} \begin{bmatrix} y \\ 1-y \end{bmatrix} =$$

$$= xy(a_{11}-a_{12}-a_{21}+a_{22}) + x(a_{12}-a_{22}) + y(a_{21}-a_{22}) + a_{22}$$

s parciálními derivacemi

$$H_x = y(a_{11}-a_{12}-a_{21}+a_{22}) + a_{12} - a_{22},$$

$$H_y = x(a_{11}-a_{12}-a_{21}+a_{22}) + a_{21} - a_{22}.$$

Následovně se odvozuje postup pro [2×2]-hry:

0) Vyčíslí se čísla maxmin $a_{ik}$ a minmax $a_{ik}$.

1) Rovnají-li se, hra má sedlový bod a existují čisté strategie obou hráčů, které procházejí sedlovým bodem. Ten udává též hodnotu hry.

2) Liší-li se, pak existují optimální smíšené strategie,

$x^*$ - řádkového hráče (Radek) a

-36-

$y^*$ - sloupcového hráče (Simona),

které jsou dány vztahy:

$$x^* = \frac{a_{22}-a_{21}}{a_{11}-a_{12}-a_{21}+a_{22}}, \text{ odtud } 1-x^* = \frac{a_{11}-a_{12}}{a_{11}-a_{12}-a_{21}+a_{22}},$$

$$y^* = \frac{a_{22}-a_{12}}{a_{11}-a_{12}-a_{21}+a_{22}}, \text{ odtud } 1-y^* = \frac{a_{11}-a_{21}}{a_{11}-a_{12}-a_{21}+a_{22}}$$

a hodnota hry s maticí **A** je

$$v(\mathbf{A}) = H(x^*,y^*) = \frac{a_{11}a_{22}-a_{12}a_{21}}{a_{11}-a_{12}-a_{21}+a_{22}}.$$

Čísla $x^*$ a $y^*$ nám udávají v jakém poměru $[x^*:(1-x^*)$, resp. $y^*:(1-y^*)]$ máme používat jednotlivé strategie.

Příklad: Radek má obchodní stánek u stadionu s nanuky a horkými kaštany. Všiml si, že může prodat asi 500 sáčků s horkými kaštany, když prší a asi 100, když svítí slunce. V slunečné dni může prodat okolo 1000 nanuků. Sáček s horkými kaštany nakupuje za 5 Kč a prodává za 10 Kč. Nanuky nakupuje za 2 Kč a prodává za 5 Kč. Do obchodu chce investovat 2500 Kč. Vše co neprodá je ztráta. Uspořádal si údaje o ziscích do tabulky.

| | | prodej při počasí | |
|---|---|---|---|
| | | déšť | slunce |
| nákup pro počasí | deštivé | 2500 | -1500 |
| | slunečné | -1500 | 3500 |

-37-

0) maxmin $a_{ik}$ = -1500, minmax $a_{ik}$ = 2500

1) maxmin $a_{ik} \neq$ minmax $a_{ik} \Rightarrow$ hra nemá sedlový bod

2) vypočteme Radkovu optimální smíšenou strategii a hodnotu hry

$$x^* = \frac{3500+1500}{2500+1500+1500+3500} = \frac{5}{9}$$

$$1-x^* = \frac{4}{9}$$

$$H(x^*,y^*) = \frac{2500\times3500-1500\times1500}{2500+1500+1500+3500} \approx 720 \text{ (Kč)}$$

Radek zjistil, že má nakupovat pro deštivé a slunečné počasí v poměru četností 5:4. Než hrát s poměrem četností, rozhodl se investovat 5/9 svého kapitálu do zboží pro deštivé dny a 4/9 do zboží pro slunečné dny a mít tak stálý zisk okolo 722 Kč.

## 2. [2×M]-HRY

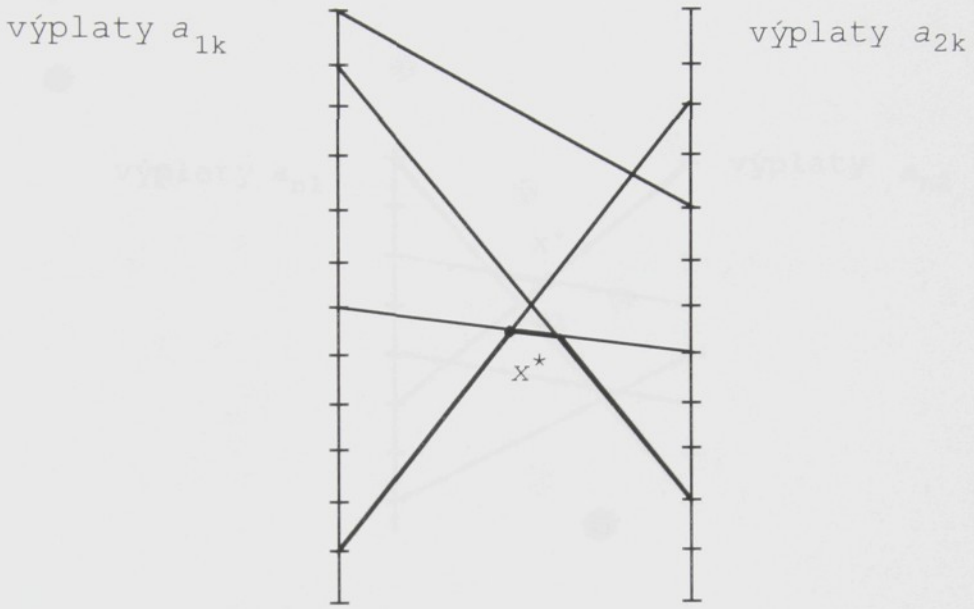
Tento druh her budeme řešit obdobně jako [2×2]-hry. Nejprve vypočítáme minmax a maxmin, rovnají-li se (hra má sedlový bod) a my jsme u konce s řešením příkladu. V případě, že hra nemá sedlový bod, vyloučíme u sloupcového hráče jeho nejlepší strategie. Tento proces nazýváme dominování, tj. snažíme se převést [2×m]-hru do podoby [2×2]-hry.

U tohoto typu her je zajímavější grafické řešení.

Hra je daná výplatní maticí $\mathbf{A} = \begin{bmatrix} a_{11} & a_{12} & \dots & a_{2m} \\ a_{21} & a_{22} & \dots & a_{2m} \end{bmatrix}$.

-38-

Na dvě rovnoběžné osy vyneseme výplaty sloupcového hráče $a_{1k}$, $a_{2k}$ a tyto body spojíme přímkou. Na dolní lomené čáře (na obr. 4 označeno silnější čarou) najdeme nejvyšší bod - $x^*$. Přímky, které se protínají v tomto bodě, nám určují strategie sloupcového hráče pro jeho optimální smíšenou strategii.



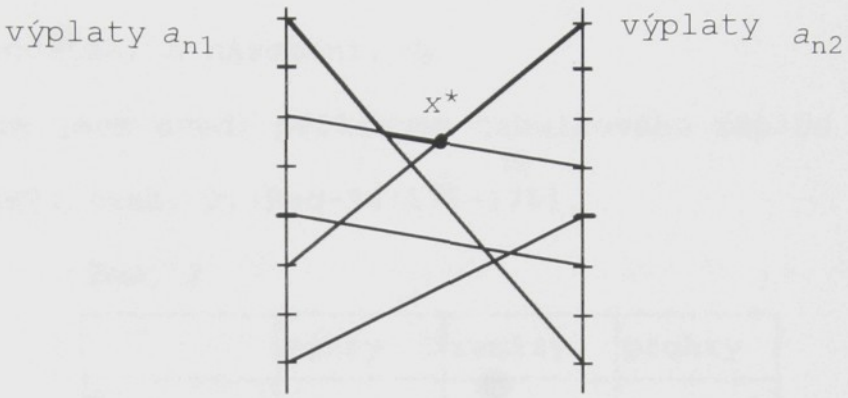

obr. 4

## 3. [N×2]-HRY

Řešíme-li $[n\times 2]$-hru s maticí $\mathbf{A} = \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \\ .. & .. \\ a_{n1} & a_{n2} \end{bmatrix}$, postupujeme při grafickém zpracování příkladu stejně jako u $[2\times m]$-her. S

-39-

tím rozdílem, že u řádkového hráče vyloučíme jeho nejhorší strategie (dominování). Na obrázku obtáhneme horní lomenou čáru (na obr. 5 označeno silnější čarou) a vyznačíme na ní nejnižší bod - $x^*$. Přímky, které se v tomto bodě protínají, určují optimální strategie řádkového hráče.




obr. 5

Vlastní využití teorie maticových her.

Seznámení s problematikou her je nejjednodušší možností, jak seznámit žáky s vlastní podobou matice. Při řešení příkladů nemusíme používat žádné složité matematické operace, naopak pracujeme pouze s prvky výplatní matice.

-40-

# 4. EXPERIMENTÁLNÍ VÝUKA POČÍTÁNÍ S [2×2]-MATICEMI

Výuku jsem prováděl dne 27.2. 1995 v šesté a sedmé třídě 1. základní školy Kladno, a to vždy s jednou polovinou třídy. Při výkladu jsem bral na vědomí, že šestá třída je průměrově slabší a sedmá třída má rozšířenou výuku matematiky. Cílem hodiny bylo seznámení žáků s [2×2]-maticemi a s operacemi sčítání, odčítání a násobení.

Matice jsem uvedl příkladem tabulkového zápisu výsledků v ledním hokeji (tab. 2)[Rad-94:177-178].

Tab. 2

| | výhry | remízy | prohry |
|---|---|---|---|
| ČR | 4 | 2 | 0 |
| RUSKO | 3 | 2 | 1 |
| KANADA | 2 | 1 | 3 |
| ŠVÉDSKO | 1 | 1 | 4 |

Tabulku jsem přepsal do maticového tvaru

$$\begin{bmatrix} 4 & 2 & 0 \\ 3 & 2 & 1 \\ 2 & 1 & 3 \\ 1 & 1 & 4 \end{bmatrix}$$

Po uvedení dalších matic různých rozměrů ([3×3], [4×5], [2×3]) jsem vysvětlil, že je rozdíl mezi čtvercovou a obdélníkovou maticí. Co je sloupec matice, řádek matice, na kterém místě se nachází dané číslo v matici. Na konec jsem žáky seznámil s [2×2]-maticemi. Poté opět následovalo několik

-41-

příkladů. Příklady byly voleny tak, aby se v nich vyskytovala kladná i záporná čísla. Řekl jsem, že [2×2]-matice se mohou použít v šifrování, v algebře (řešení lineárních soustav rovnic), geometrii (transformace souřadnic). Po úvodu do teorie matic jsem na tabuli napsal definici matice - matice je obdélníkové nebo čtvercové uspořádání čísel do řádků a sloupců. Dále jsem na tabuli napsal obecný tvar matic, které budeme používat.

$$\mathbf{A} = \begin{bmatrix} a & b \\ c & d \end{bmatrix}, \quad \mathbf{B} = \begin{bmatrix} e & f \\ g & h \end{bmatrix}$$

Seznámil jsem žáky s:

- vynásobením matice konstantou $r$ (reálné číslo), tzn. že se násobí každé číslo matice stejným číslem

$$r\mathbf{A} = \begin{bmatrix} ra & rb \\ rc & rd \end{bmatrix}$$

- sčítáním matic **A+B**, platí **A+B** = **B+A**, sčítají se čísla na stejných pozicích v maticích **A** a **B**

$$\mathbf{A+B} = \begin{bmatrix} a & b \\ c & d \end{bmatrix} + \begin{bmatrix} e & f \\ g & h \end{bmatrix} = \begin{bmatrix} a+e & b+f \\ c+g & d+h \end{bmatrix}$$

- odčítání matic **A-B**, odečítají se čísla na stejných pozicích v maticích **A** a **B**

$$\mathbf{A-B} = \begin{bmatrix} a & b \\ c & d \end{bmatrix} - \begin{bmatrix} e & f \\ g & h \end{bmatrix} = \begin{bmatrix} a-e & b-f \\ c-g & d-h \end{bmatrix}$$

- násobení matic **AB**

Násobení jsem definoval pro každou polovinu třídy jiným způsobem

1, Řádky **A** . sloupce **B**

-42-

$$\mathbf{AB} = \begin{bmatrix} a & b \\ c & d \end{bmatrix}\begin{bmatrix} e & f \\ g & h \end{bmatrix} = \begin{bmatrix} \begin{bmatrix} a & b \end{bmatrix}\begin{bmatrix} e \\ g \end{bmatrix}, & \begin{bmatrix} a & b \end{bmatrix}\begin{bmatrix} f \\ h \end{bmatrix} \\ \begin{bmatrix} c & d \end{bmatrix}\begin{bmatrix} e \\ g \end{bmatrix}, & \begin{bmatrix} c & d \end{bmatrix}\begin{bmatrix} f \\ h \end{bmatrix} \end{bmatrix} =$$

$$= \begin{bmatrix} ae+bg, & af+bh \\ ce+dg, & cf+dh \end{bmatrix}$$

2, Sloupce **A** . řádky **B**

$$\mathbf{AB} = \begin{bmatrix} a & b \\ c & d \end{bmatrix}\begin{bmatrix} e & f \\ g & h \end{bmatrix} = \begin{bmatrix} a \\ c \end{bmatrix}\begin{bmatrix} e & f \end{bmatrix} + \begin{bmatrix} b \\ d \end{bmatrix}\begin{bmatrix} g & h \end{bmatrix} =$$

$$= \begin{bmatrix} ae, & af \\ ce, & cf \end{bmatrix} + \begin{bmatrix} bg, & bh \\ dg, & dh \end{bmatrix} = \begin{bmatrix} ae+bg, & af+bh \\ ce+dg, & cf+dh \end{bmatrix}$$

- **AB** = **BA** neplatí (obecně)

Příklad: $\begin{bmatrix} 2 & 1 \\ 4 & 3 \end{bmatrix}\begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix} \neq \begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix}\begin{bmatrix} 2 & 1 \\ 4 & 3 \end{bmatrix}$

Vypočítal jsem typové příklady na tabuli s každou polovinou třídy pro ně definovaným způsobem.

1a, $\begin{bmatrix} 2 & 3 \\ 1 & 2 \end{bmatrix}\begin{bmatrix} 5 & 7 \\ 8 & 2 \end{bmatrix} = \begin{bmatrix} 10+24 & 14+6 \\ 5+16 & 7+4 \end{bmatrix} = \begin{bmatrix} 34 & 20 \\ 21 & 11 \end{bmatrix}$

1b, $\begin{bmatrix} 2 & 3 \\ 1 & 2 \end{bmatrix}\begin{bmatrix} 5 & 7 \\ 8 & 2 \end{bmatrix} = \begin{bmatrix} 10 & 14 \\ 5 & 7 \end{bmatrix} + \begin{bmatrix} 24 & 6 \\ 16 & 4 \end{bmatrix} = \begin{bmatrix} 34 & 20 \\ 21 & 11 \end{bmatrix}$

2a, $\begin{bmatrix} 1 & 4 \\ 7 & 9 \end{bmatrix}\begin{bmatrix} 12 & 13 \\ 16 & 18 \end{bmatrix} = \begin{bmatrix} 12+64 & 13+72 \\ 84+144 & 91+162 \end{bmatrix} = \begin{bmatrix} 76 & 85 \\ 228 & 253 \end{bmatrix}$

2b, $\begin{bmatrix} 1 & 4 \\ 7 & 9 \end{bmatrix}\begin{bmatrix} 12 & 13 \\ 16 & 18 \end{bmatrix} = \begin{bmatrix} 12 & 13 \\ 84 & 91 \end{bmatrix} + \begin{bmatrix} 64 & 72 \\ 144 & 162 \end{bmatrix} = \begin{bmatrix} 76 & 85 \\ 228 & 253 \end{bmatrix}$

Uvedl jsem, že dělení matic se v matematice nezavádí.

Nakonec jsem žákům zadal čtyři příklady k samostatné práci. Příklady byly pro obě třídy stejné. První příklad byl

-43-

zaměřen na sčítání matic, ostatní potom na násobení. Na práci měli žáci deset minut. Cílem bylo zjistit, která metoda násobení je pro žáky snazší. Předpokládal jsem, že to bude druhá metoda (sloupce × řádky), která odděluje násobení a sčítání.

1, $\begin{bmatrix} 38 & 26 \\ 29 & 19 \end{bmatrix} + \begin{bmatrix} 49 & 47 \\ -51 & 66 \end{bmatrix} = \begin{bmatrix} 87 & 73 \\ -22 & 85 \end{bmatrix}$

2, $\begin{bmatrix} 3 & 7 \\ 5 & 3 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 4 & 0 \end{bmatrix} = \begin{bmatrix} 31 & 0 \\ 17 & 0 \end{bmatrix}$

3, $\begin{bmatrix} 6 & 8 \\ 0 & 2 \end{bmatrix} \begin{bmatrix} 7 & 0 \\ 2 & 2 \end{bmatrix} = \begin{bmatrix} 58 & 16 \\ 4 & 4 \end{bmatrix}$

4, $\begin{bmatrix} 5 & 8 \\ 1 & 9 \end{bmatrix} \begin{bmatrix} 7 & 1 \\ 4 & 1 \end{bmatrix} = \begin{bmatrix} 67 & 13 \\ 43 & 10 \end{bmatrix}$

Následující tabulka ukazuje, kolik příkladů bylo vypočteno správně (tab. 3).

Tab. 3

| | 6. třída | | | | 7 třída | | | |
|---|---|---|---|---|---|---|---|---|
| | Řád. × Sl. | | Sl. × Řád. | | Řád. × Sl. | | Sl. × Řád. | |
| počet žáků | 13 | | 13 | | 10 | | 12 | |
| 1. příklad | 12 | 92% | 13 | 100% | 9 | 90% | 12 | 100% |
| 2. příklad | 4 | 30% | 8 | 61% | 6 | 60% | 10 | 83% |
| 3. příklad | 4 | 30% | 7 | 53% | 8 | 80% | 10 | 83% |
| 4. příklad | 4 | 30% | 7 | 53% | 7 | 70% | 9 | 75% |
| | dobře | v % | dobře | v % | dobře | v % | dobře | v % |

-44-

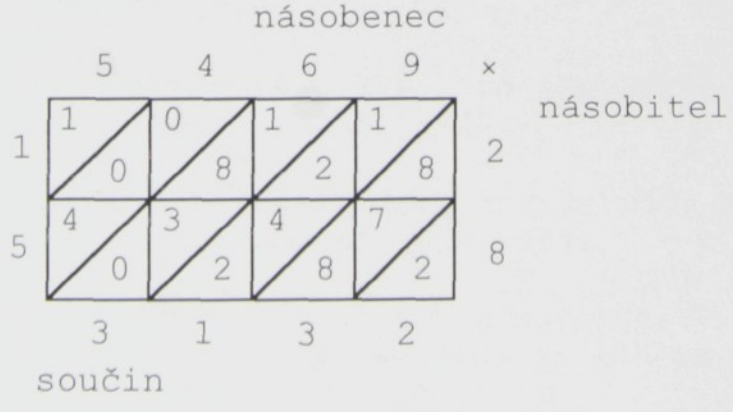
Výsledky v tabulce ukazují, že předpoklad byl správný. Celkově se potvrzuje, že při řetězci aritmetických operací je pro zvýšení rychlosti a zmenšení chybovosti radno (pokud možno) oddělit násobení od sčítání. K tomuto faktu přihlížejí učitelé odjakživa.

Známá je např. Napierova proužková metoda násobení čísel, [Scd-92:$62_{12}$-$3^{8}$; Bal-59:$52_{6}$-$60^{12}$], která odděluje násobení, sčítání a následné přenosy mezi řády. U této metody se mezivýsledky soustřeďují do tabulky. Cifry součinu jsou součtem cifer v šikmých pruzích (s případnými přenosy mezi řády).

Příklad: a, Postup, který se učí na základní škole 5469×28

$$\begin{array}{r} 5469 \\ \underline{\phantom{0}28} \\ 43752 \\ \underline{+10938\phantom{0}} \\ 153132 \end{array}$$

b, Užití Napierovy proužkové metody



-45-

## ZÁVĚR

Tak jako většina mých spolužáků jsem si myslel, že matice se dají využít v největší míře při řešení soustav lineárních rovnic. Tato práce ukazuje, že teorie matic je mnohem zajímavější než by se na první pohled mohlo zdát.

Podle mého názoru by bylo zajímavé zavést teorii matic do učiva pro základní třídy, zejména do vyšších ročníků. Počítání s maticemi nabízí zejména uplatnění v procvičování matematických operací - násobení a sčítání.

-46-

## SEZNAM LITERATURY:

[Ale] Aleksandrova, N.V.: Matematičeskie terminy. Moskva 1978.

[Bal] Balada, F.: Z dějin elementární matematiky. Praha, SPN 1959.

[Bic] Bican, L.: Lineární algebra. Praha, SNTL 1979.

[Bor] Borůvka, O.: Základy teorie matic. Praha, Academia 1971.

[GP] Grošek, O. - Porubský, Š.: Šifrovanie, algoritmy, metódy, prax. Praha, Grada 1992.

[Gus] Gusak, G. M.: Sistemy algebraičeskich uravněnij. Minsk, Vyšejšaja škola 1983.

[HH] Havel, V. - Holenda, J.: Lineární algebra. Praha, SNTL 1984.

[Koe] Koecher, M.: Lineare Algebra und analytische Geometrie. 3. vyd. Springer-Verlag 1992.

[Maň] Maňas, M.: Teorie her a optimální rozhodování. Praha, SNTL 1974.

[NV] Nekvinda, M. - Vild, J.: Náměty pro samostatné referáty z matematiky. Liberec 1995.

[Scd] Scheid, H.: Elemente der Arithmetik und Algebra. 2. vyd. Mannheim, Wissenschaftsverlag 1992.

[Slo] Slouka, R.: Algebra pro 5. - 9. ročník ZŠ a víceletá gymnázia. FIN s.r.o. 1994.

[Šed] Šedivý, J. aj.: Světonázorové problémy matematiky II. Praha, UK MFF 1984.

[Vil] Vild, J.: Metodické pokyny pro diplomové a závěrečné práce na PF TUL. Liberec 1995.

[Vor] Vorob´ev, N.N.: Teoria igr. Lekcii dlja ekonomistov-kibernetikov. Leningrad, ILU 1974.

[VŘ] Vild, J. - Říhová, H.: Rank-2 matrices. In: Proceedings of mathematics in Liberec 1994. Liberec, TU 1995. s. 23-30.

[Wil] Williams, J.D.: Dokonalý stratég aneb slabikář teorie her. 1. vyd. Praha, Orbis 1966.