Matematika pro ekonomickou praxi

Jiří Fišer

30. října 2025

- V dnešní přednášce se vrátíme k soustavám lineárních rovnic.
- Již známe:
  - obecnou (Gaussovu) metodu jejich řešení
  - a pro „čtvercové“ soustavy Cramerovo pravidlo, kdy jsou jednotlivé složky řešení vyjádřeny jako podíly dvou determinantů,
- Dnes u „čtvercových“ zůstaneme: soustavy n rovnic o n neznámých

$$\begin{array}{rcl} a_{11}x_1 + \cdots + a_{1n}x_n & = & b_1, \\ \vdots & \vdots & \vdots \\ a_{n1}x_1 + \cdots + a_{nn}x_n & = & b_n \\ \hline \end{array}$$

se (čtvercovou) maticí soustavy

$$\begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{pmatrix}$$

o plné hodnosti n.

- Z Frobeniovy věty víme, že v tomto případě, kdy

$$h(\mathbf{A}) = h(\mathbf{A}_R) = n,$$

máme zajištěnu existenci právě jednoho řešení

$$(x_1, \ldots, x_n).$$

- Ukážeme si dva přístupy, jak toto řešení získat:

  1) pomocí Cramerova pravidla, kdy jsou jednotlivé složky řešení vyjádřeny jako podíly dvou determinantů,
  2) pomocí inverzních matic.

Základní operace s maticemi

- **Součin čísla α a matice $\mathbf{A}$:**

$$\alpha\mathbf{A} = (\alpha a_{ij})$$

(každý prvek matice $\mathbf{A}$ vynásobíme číslem α, výsledkem je opět matice typu (m, n)).

Násobení matice číslem

$$2\begin{pmatrix} 1 & -1 \\ 0 & 1 \\ 3 & -2 \end{pmatrix} = \begin{pmatrix} 2\cdot 1 & 2\cdot(-1) \\ 2\cdot 0 & 2\cdot 1 \\ 2\cdot 3 & 2\cdot(-2) \end{pmatrix} = \begin{pmatrix} 2 & -2 \\ 0 & 2 \\ 6 & -4 \end{pmatrix},$$

- **Součet matic** $\mathbf{A}$ a $\mathbf{B}$ typu (m, n):

$$\mathbf{A} + \mathbf{B} = (a_{ij} + b_{ij})$$

(sčítáme podle pozic po prvcích (jako u součtu vektorů), výsledkem je opět matice typu (m, n), matice $\mathbf{A}$ a $\mathbf{B}$ musí být stejného typu).

Sčítání matic

$$\begin{pmatrix} 6 & 2 & 7 \\ 1 & 4 & -2 \end{pmatrix} + \begin{pmatrix} 2 & 5 & -1 \\ 3 & -8 & 0 \end{pmatrix} = \begin{pmatrix} 6+2 & 2+5 & 7-1 \\ 1+3 & 4-8 & -2+0 \end{pmatrix} = \begin{pmatrix} 8 & 7 & 6 \\ 4 & -4 & -2 \end{pmatrix}$$

- Pro matice $\mathbf{A}$, $\mathbf{B}$, které jsou typu (m, n), nulovou matici $\mathbf{O}_{mn}$ a $\alpha, \beta \in \mathbb{R}$ platí
  1) $\mathbf{A} + \mathbf{B} = \mathbf{B} + \mathbf{A}$,
  2) $\mathbf{A} + \mathbf{O}_{mn} = \mathbf{A}$,
  3) $\alpha(\beta\mathbf{A}) = (\alpha\beta)\mathbf{A}$.

- **Násobení matic:** Nechť $\mathbf{A} = (a_{ij})$ je matice typu (m, n) a $\mathbf{B} = (b_{ij})$ je typu (n, p).
  Potom matici $\mathbf{C} = (c_{ij})$ typu (m, p), pro kterou platí

  $$c_{ij} = a_{i1}b_{1j} + a_{i2}b_{2j} + \cdots + a_{in}b_{nj},$$

  označujeme $\mathbf{A} \cdot \mathbf{B}$ a nazýváme součinem matice $\mathbf{A}$ a matice $\mathbf{B}$ (v tomto pořadí).
  - Prvek c_{ij} vzniká vynásobením i-tého řádku matice $\mathbf{A}$ s j-tým sloupcem matice $\mathbf{B}$.
  - K tomu je potřeba, aby tento i-tý řádek a tento j-tý sloupec měly stejný počet prvků.
  - Proto musí platit, že matice $\mathbf{B}$ má tolik řádků, kolik má matice $\mathbf{A}$ sloupců.
  - Výsledná matice má pak tolik řádků, kolik jich má matice $\mathbf{A}$, a tolik sloupců, kolik jich má matice $\mathbf{B}$.

Úloha (Násobení matic)

Vypočtěte $\mathbf{A} \cdot \mathbf{B}$ pro matice $\mathbf{A} = \begin{pmatrix} 2 & 3 \\ 1 & -1 \end{pmatrix}$ a $\mathbf{B} = \begin{pmatrix} 1 & 0 & -1 \\ 3 & -1 & 2 \end{pmatrix}$.

Řešení.

Matice $\mathbf{A}$ má dva sloupce a matice $\mathbf{B}$ dva řádky, součin $\mathbf{A} \cdot \mathbf{B}$ tedy existuje. Výsledná matice bude mít dva řádky (=počet řádků matice $\mathbf{A}$) a tři sloupce (=počet sloupců matice $\mathbf{B}$).

$$\begin{aligned} \mathbf{A} \cdot \mathbf{B} &= \begin{pmatrix} 2 & 3 \\ 1 & -1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 & -1 \\ 3 & -1 & 2 \end{pmatrix} \\ &= \begin{pmatrix} 2 \cdot 1 + 3 \cdot 3 & 2 \cdot 0 + 3 \cdot (-1) & 2 \cdot (-1) + 3 \cdot 2 \\ 1 \cdot 1 + (-1) \cdot 3 & 1 \cdot 0 + (-1) \cdot (-1) & 1 \cdot (-1) + (-1) \cdot 2 \end{pmatrix} \\ &= \begin{pmatrix} 11 & -3 & 4 \\ -2 & 1 & -3 \end{pmatrix}. \end{aligned}$$

- V předchozím případě nelze vypočítat $\mathbf{B} \cdot \mathbf{A}$, neboť matice $\mathbf{B}$ má jiný počet sloupců (3) než má matice $\mathbf{A}$ řádků (2).

- Nechť $\mathbf{A}, \mathbf{B}, \mathbf{C}$ jsou matice a $\mathbf{E}$ je jednotková matice (vhodného rozměru). Potom každá z rovností

  1) $\mathbf{A} \cdot \mathbf{E} = \mathbf{A}$,
  2) $\mathbf{E} \cdot \mathbf{A} = \mathbf{A}$,
  3) $(\mathbf{A} + \mathbf{B}) \cdot \mathbf{C} = \mathbf{A} \cdot \mathbf{C} + \mathbf{B} \cdot \mathbf{C}$,
  4) $\mathbf{A}(\mathbf{B} + \mathbf{C}) = \mathbf{A} \cdot \mathbf{B} + \mathbf{A} \cdot \mathbf{C}$,
  5) $\mathbf{A} \cdot (\mathbf{B} \cdot \mathbf{C}) = (\mathbf{A} \cdot \mathbf{B}) \cdot \mathbf{C}$,

  platí, pokud mají příslušné operace smysl.

Inverzní matice

- Nechť $\mathbf{A}$ a $\mathbf{B}$ jsou čtvercové matice typu (n,n). Jestliže platí

$$\mathbf{A}\mathbf{B} = \mathbf{B}\mathbf{A} = \mathbf{E}_n,$$

potom $\mathbf{B}$ nazýváme **inverzní maticí** k matici $\mathbf{A}$ a značíme ji $\mathbf{A}^{-1}$.

Regulární a singulární matice

- Nechť $\mathbf{A}$ je čtvercová matice typu (n, n).
  - Jestliže $\boxed{h(\mathbf{A}) = n}$, pak $\mathbf{A}$ nazýváme **regulární** maticí.
  - Jestliže $\boxed{h(\mathbf{A}) < n}$, pak $\mathbf{A}$ nazýváme **singulární** maticí.

- Nechť je dána čtvercová matice $\mathbf{A}$ typu (n, n).
  Potom jsou následující podmínky ekvivalentní:
  1) $\mathbf{A}$ je regulární ($h(\mathbf{A}) = n$),
  2) $\det \mathbf{A} \neq 0$,
  3) k matici $\mathbf{A}$ existuje inverzní matice $\mathbf{A}^{-1}$,
  4) matici $\mathbf{A}$ lze převést pomocí konečně mnoha ekvivalentních úprav na jednotkovou matici $\mathbf{E}_n$.

$$\mathbf{A}\cdot\mathbf{A}^{-1}=\begin{pmatrix}1 & 2 & -1\\ 2 & 0 & 1\\ 1 & -2 & 1\end{pmatrix}\begin{pmatrix}\frac{1}{2} & 0 & \frac{1}{2}\\ -\frac{1}{4} & \frac{1}{2} & -\frac{3}{4}\\ -1 & 1 & -1\end{pmatrix}=\cdots=\begin{pmatrix}1 & 0 & 0\\ 0 & 1 & 0\\ 0 & 0 & 1\end{pmatrix}.$$

$$\mathbf{A}^{-1}\cdot\mathbf{A}=\begin{pmatrix}\frac{1}{2} & 0 & \frac{1}{2}\\ -\frac{1}{4} & \frac{1}{2} & -\frac{3}{4}\\ -1 & 1 & -1\end{pmatrix}\begin{pmatrix}1 & 2 & -1\\ 2 & 0 & 1\\ 1 & -2 & 1\end{pmatrix}=\cdots=\begin{pmatrix}1 & 0 & 0\\ 0 & 1 & 0\\ 0 & 0 & 1\end{pmatrix}.$$

Je-li $\mathbf{A}^{-1}$ inverzní k $\mathbf{A}$, potom je i $\mathbf{A}$ inverzní k $\mathbf{A}^{-1}$, tj.

$$\mathbf{A}\mathbf{A}^{-1}=\mathbf{A}^{-1}\mathbf{A}=\mathbf{E}_n.$$

Výpočet inverzní matice pomocí ekvivalentních úprav

- Zapíšeme danou (regulární) matici $\mathbf{A}$ ve dvojici s $\mathbf{E}_n$:

$$(\mathbf{A}|\mathbf{E}_n) = \left(\begin{array}{cccc|cccc} a_{11} & a_{12} & \dots & a_{1n} & 1 & 0 & \dots & 0 \\ a_{21} & a_{22} & \dots & a_{2n} & 0 & 1 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \dots & a_{nn} & 0 & 0 & \dots & 1 \end{array}\right).$$

- Nyní pomocí ekvivalentních úprav (kromě přehazování sloupců) převedeme $\mathbf{A}$ na jednotkovou matici $\mathbf{E}_n$, přičemž stejné úpravy budeme vždy aplikovat i na pravou část matice (za svislou čarou).
- V okamžiku, kdy se vlevo objeví $\mathbf{E}_n$, vpravo získáme $\mathbf{A}^{-1}$:

$$(\mathbf{A}|\mathbf{E}_n) = \left(\begin{array}{cccc|cccc} a_{11} & a_{12} & \dots & a_{1n} & 1 & 0 & \dots & 0 \\ a_{21} & a_{22} & \dots & a_{2n} & 0 & 1 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \dots & a_{nn} & 0 & 0 & \dots & 1 \end{array}\right) \sim \dots \sim \left(\mathbf{E}_n|\mathbf{A}^{-1}\right)$$

Výpočet inverzní matice pomocí ekvivalentních úprav

- Určete inverzní matici $\mathbf{A}^{-1}$ k matici $\mathbf{A} = \begin{pmatrix} 1 & 2 & -1 \\ 2 & 0 & 1 \\ 1 & -2 & 1 \end{pmatrix}$.
- Zapíšeme matici $(\mathbf{A}, \mathbf{E}_3) = \left(\begin{array}{ccc|ccc} 1 & 2 & -1 & 1 & 0 & 0 \\ 2 & 0 & 1 & 0 & 1 & 0 \\ 1 & -2 & 1 & 0 & 0 & 1 \end{array}\right)$
- Pomocí ekvivalentních úprav (kromě přehazování sloupců)
  - převedeme $\mathbf{A}$ na jednotkovou matici $\mathbf{E}_n$,
  - přičemž stejné úpravy budeme vždy aplikovat i na pravou část matice (za svislou čarou).

Výpočet inverzní matice pomocí ekvivalentních úprav

$$(\mathbf{A},\mathbf{E}_3)=\left(\begin{array}{ccc|ccc} 1 & 2 & -1 & 1 & 0 & 0\\ 2 & 0 & 1 & 0 & 1 & 0\\ 1 & -2 & 1 & 0 & 0 & 1\end{array}\right)\sim\left(\begin{array}{ccc|ccc} 1 & 2 & -1 & 1 & 0 & 0\\ 0 & -4 & 3 & -2 & 1 & 0\\ 0 & -4 & 2 & -1 & 0 & 1\end{array}\right)\sim$$

$$\sim\left(\begin{array}{ccc|ccc} 1 & 2 & -1 & 1 & 0 & 0\\ 0 & -4 & 3 & -2 & 1 & 0\\ 0 & 0 & -1 & 1 & -1 & 1\end{array}\right)\sim\left(\begin{array}{ccc|ccc} 1 & 2 & 0 & 0 & 1 & -1\\ 0 & -4 & 0 & 1 & -2 & 3\\ 0 & 0 & -1 & 1 & -1 & 1\end{array}\right)\sim$$

$$\sim\left(\begin{array}{ccc|ccc} 1 & 2 & 0 & 0 & 1 & -1\\ 0 & 1 & 0 & -\frac{1}{4} & \frac{1}{2} & -\frac{3}{4}\\ 0 & 0 & 1 & -1 & 1 & -1\end{array}\right)\sim\left(\begin{array}{ccc|ccc} 1 & 0 & 0 & \frac{1}{2} & 0 & \frac{1}{2}\\ 0 & 1 & 0 & -\frac{1}{4} & \frac{1}{2} & -\frac{3}{4}\\ 0 & 0 & 1 & -1 & 1 & -1\end{array}\right)=\left(\mathbf{E}_3|\mathbf{A}^{-1}\right)$$

Tedy

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

Provedeme zkoušku:

$$
\begin{aligned}
\mathbf{A} \cdot \mathbf{A}^{-1} &= \begin{pmatrix} 1 & 2 & -1 \\ 2 & 0 & 1 \\ 1 & -2 & 1 \end{pmatrix} \frac{1}{4} \begin{pmatrix} 2 & 0 & 2 \\ -1 & 2 & -3 \\ -4 & 4 & -4 \end{pmatrix} \\
&= \frac{1}{4} \begin{pmatrix} 1 & 2 & -1 \\ 2 & 0 & 1 \\ 1 & -2 & 1 \end{pmatrix} \begin{pmatrix} 2 & 0 & 2 \\ -1 & 2 & -3 \\ -4 & 4 & -4 \end{pmatrix} \\
&= \frac{1}{4} \begin{pmatrix} 4 & 0 & 0 \\ 0 & 4 & 0 \\ 0 & 0 & 4 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = \mathbf{E}_3 .
\end{aligned}
$$

Řešení soustav LR pomocí inverzních matic

Nechť je dána soustava n rovnic o n neznámých

$$
\begin{array}{rcl}
a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n & = & b_1, \\
a_{21}x_1 + a_{22}x_2 + \cdots + a_{2n}x_n & = & b_2, \\
\vdots & \vdots & \vdots \\
a_{n1}x_1 + a_{n2}x_2 + \cdots + a_{nn}x_n & = & b_n. \\
\hline
\end{array}
$$

$$
\mathbf{A} = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{pmatrix}, \qquad \vec{x} = \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix}, \qquad \vec{b} = \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{pmatrix}.
$$

Soustavu lze nyní zapsat pomocí maticové rovnice

$$\mathbf{A}\vec{x} = \vec{b}.$$

Řešení soustav LR pomocí inverzních matic

Jestliže $\mathbf{A}$ je regulární matice, pak podle Frobeniovy věty existuje právě jedno řešení soustavy.
Vynásobíme-li rovnici $\mathbf{A}\vec{x} = \vec{b}$ maticí $\mathbf{A}^{-1}$ zleva, dostaneme

$$\begin{aligned} \mathbf{A}\vec{x} &= \vec{b}, \\ \mathbf{A}^{-1}\mathbf{A}\vec{x} &= \mathbf{A}^{-1}\vec{b}, \\ \mathbf{E}_n\vec{x} &= \mathbf{A}^{-1}\vec{b}, \\ \vec{x} &= \mathbf{A}^{-1}\vec{b}, \end{aligned}$$

což dává další možnost určování řešení soustavy.

Úloha (Řešení soustavy lin. rovnic pomocí inverzní matice)

Pomocí inverzní matice vyřešte soustavu rovnic

$$\begin{aligned} x_1 + 2x_2 - x_3 &= -3, \\ 2x_1 + x_3 &= 7, \\ x_1 - 2x_2 + x_3 &= 7. \end{aligned}$$

Máme

$$\mathbf{A} = \begin{pmatrix} 1 & 2 & -1 \\ 2 & 0 & 1 \\ 1 & -2 & 1 \end{pmatrix}, \qquad \vec{x} = \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix}, \qquad \vec{b} = \begin{pmatrix} -3 \\ 7 \\ 7 \end{pmatrix}.$$

Dále z předchozích příkladů známe inverzní matici

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

Podle vzorce máme

$$\begin{aligned}\vec{x} &= \mathbf{A}^{-1}\vec{b} = \begin{pmatrix} \frac{1}{2} & 0 & \frac{1}{2} \\ -\frac{1}{4} & \frac{1}{2} & -\frac{3}{4} \\ -1 & 1 & -1 \end{pmatrix} \begin{pmatrix} -3 \\ 7 \\ 7 \end{pmatrix} \\ &= \frac{1}{4} \begin{pmatrix} 2 & 0 & 2 \\ -1 & 2 & -3 \\ -4 & 4 & -4 \end{pmatrix} \begin{pmatrix} -3 \\ 7 \\ 7 \end{pmatrix} = \begin{pmatrix} 2 \\ -1 \\ 3 \end{pmatrix}.\end{aligned}$$

Tedy

$$\vec{x} = \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = \begin{pmatrix} 2 \\ -1 \\ 3 \end{pmatrix}.$$

Teoretický úvod

- Šifrování pomocí matic spočívá v převodu zprávy na číselné hodnoty a v maticovém násobení.
- Klíčové pojmy:
  - **Šifrovací matice** – matice, kterou násobíme vektor zprávy.
  - **Inverzní matice** – umožňuje dešifrování zprávy, musí existovat, což znamená, že šifrovací matice je regulární (má nenulový determinant).
- Historie:
  - Hillova šifra (1929) využívala maticové násobení k šifrování textu, což umožnilo zakódování zprávy jako vektorového řetězce.
  - Dnes jsou podobné metody používány v moderní kryptografii, ačkoliv základní maticové šifry jsou již považovány za kryptograficky slabé.

Úvod do šifrování zprávy

Zadání

Zašifrujte zprávu „Matice jsou užitečné“ pomocí matice

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

- Pro šifrování je nutné, aby měla šifrovací matice nenulový determinant, tedy aby byla regulární.
- Vzhledem k tomu, že jde o matici 3×3, použijeme Sarrusovo pravidlo pro výpočet determinantu:

$$\det(\mathbf{A}) = 2\cdot3\cdot2+4\cdot0\cdot1+2\cdot1\cdot2-(1\cdot3\cdot2+2\cdot0\cdot2+2\cdot1\cdot4) = 2 \neq 0.$$

Matice je tedy regulární a lze ji použít k šifrování.

Přiřazení číselných hodnot písmenům

- Každému písmenu abecedy přiřadíme číselnou hodnotu. Diakritiku ignorujeme a písmeno *ch* vynecháme.
- Znak „␣“ představuje mezeru v textu.
- Používáme následující schéma:

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

Číselné vyjádření zprávy (bez diakritiky) je:

$$13 \quad 1 \quad 20 \quad 9 \quad 3 \quad 5 \quad 0 \quad 10 \quad 19 \quad 15 \quad 21 \quad 0 \quad 21 \quad 26 \quad 9 \quad 20 \quad 5 \quad 3 \quad 14 \quad 5$$

Vytvoření matice pro šifrování

- Přepíšeme číselnou reprezentaci zprávy do matice $\mathbf{Z}$ tak, aby součin s maticí $\mathbf{A}$ existoval.
- Protože je $\mathbf{A}$ matice 3×3, musí mít matice $\mathbf{Z}$ tři řádky.
- Zprávu přepíšeme po sloupcích a doplníme nulou:

$$\mathbf{Z} = \begin{pmatrix} 13 & 9 & 0 & 15 & 21 & 20 & 14 \\ 1 & 3 & 10 & 21 & 26 & 5 & 5 \\ 20 & 5 & 19 & 0 & 9 & 3 & 0 \end{pmatrix}$$

Zašifrování zprávy pomocí maticového násobení

- Vynásobíme šifrovací matici $\mathbf{A}$ s maticí $\mathbf{Z}$:

$$\mathbf{A}\cdot\mathbf{Z}=\begin{pmatrix}2&1&1\\4&3&2\\2&0&2\end{pmatrix}\cdot\begin{pmatrix}13&9&0&15&21&20&14\\1&3&10&21&26&5&5\\20&5&19&0&9&3&0\end{pmatrix}$$

- Výsledkem je:

$$\begin{pmatrix}47&26&29&51&77&48&33\\95&55&68&123&180&101&71\\66&28&38&30&60&46&28\end{pmatrix}$$

Přepisem po sloupcích získáme zašifrovanou zprávu jako řetězec čísel.

Odšifrování zprávy pomocí matice

Úkol

Odšifrujte zprávu

$$41 \quad 55 \quad 70 \quad 95 \quad 41 \quad 55 \quad 78 \quad 107 \quad 35 \quad 47 \quad 20 \quad 30 \quad 15 \quad 20 \quad 69 \quad 98 \quad 41 \quad 61 \quad 44 \quad 59$$

zašifrovanou maticí

$$\mathbf{A} = \begin{pmatrix} 3 & 2 \\ 4 & 3 \end{pmatrix}$$

- Matice $\mathbf{A}$ má determinant $1 \neq 0$, takže je regulární a má inverzní matici $\mathbf{A}^{-1}$.

Výpočet inverzní matice a dešifrování

- Inverzní matice je:

$$\mathbf{A}^{-1} = \begin{pmatrix} 3 & -2 \\ -4 & 3 \end{pmatrix}$$

- Násobíme tuto matici zleva na matici zašifrované zprávy:

$$\begin{pmatrix} 3 & -2 \\ -4 & 3 \end{pmatrix} \cdot \begin{pmatrix} 41 & 70 & 41 & 78 & 35 & 20 & 15 & 69 & 41 & 44 \\ 55 & 95 & 55 & 107 & 47 & 30 & 20 & 98 & 61 & 59 \end{pmatrix}$$

Výsledkem je matice s číselnými hodnotami, které pak převedeme na písmena.

Převod čísel zpět na text

- Přepisem hodnot na písmena podle původního schématu získáme dešifrovanou zprávu:

$$M\ A\ T\ E\ M\ A\ T\ I\ K\ A\ \_\ J\ E\ \_\ K\ R\ A\ S\ N\ A$$