

Matematika pro ekonomickou praxi

Jiří Fišer

30. října 2025

Rekapitulace a cíl

- V minulé přednášce jsme se zabývali soustavami n rovnic o n neznámých.
- Již známe:
 - ▶ obecnou (Gaussovou) metodu
 - ▶ **Cramerovo pravidlo** (pro soustavy $n \times n$ s $\det \mathbf{A} \neq 0$)
- Dnes se zaměříme na slíbený druhý přístup pro regulární soustavy:

Řešení pomocí inverzních matic

- **Připomenutí Frobeniovy věty:** Pro regulární matici $\mathbf{A}$ (tj. $h(\mathbf{A}) = n$ neboli $\det \mathbf{A} \neq 0$) má soustava $\mathbf{A}\vec{x} = \vec{b}$ **právě jedno řešení**.

Rekapitulace a cíl

- V minulé přednášce jsme se zabývali soustavami n rovnic o n neznámých.
- Již známe:
 - ▶ obecnou (Gaussovou) metodu
 - ▶ **Cramerovo pravidlo** (pro soustavy $n \times n$ s $\det \mathbf{A} \neq 0$)
- Dnes se zaměříme na slíbený druhý přístup pro regulární soustavy:

Řešení pomocí inverzních matic

- **Připomenutí Frobeniovy věty:** Pro regulární matici $\mathbf{A}$ (tj. $h(\mathbf{A}) = n$ neboli $\det \mathbf{A} \neq 0$) má soustava $\mathbf{A}\vec{x} = \vec{b}$ **právě jedno řešení**.

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 A a 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 **A** a **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 **A**, **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).

Vizuální schéma (tzv. "skalární součin řádku a sloupce")

$$\begin{pmatrix} \cdots & \cdots & \cdots \\ a_{i1} & a_{i2} & \cdots & a_{in} \\ \cdots & \cdots & \cdots \end{pmatrix} \cdot \begin{pmatrix} \cdots & b_{1j} & \cdots \\ \cdots & b_{2j} & \cdots \\ \cdots & \vdots & \cdots \\ \cdots & b_{nj} & \cdots \end{pmatrix} = \begin{pmatrix} \cdots & \cdots & \cdots \\ \cdots & c_{ij} & \cdots \\ \cdots & \cdots & \cdots \end{pmatrix}$$

Vizuální schéma (tzv. "skalární součin řádku a sloupce")

$$\begin{pmatrix} \dots & \dots & \dots \\ a_{i1} & a_{i2} & \dots & a_{in} \\ \dots & \dots & \dots \end{pmatrix} \cdot \begin{pmatrix} \dots & b_{1j} & \dots \\ \dots & b_{2j} & \dots \\ \dots & \vdots & \dots \\ \dots & b_{nj} & \dots \end{pmatrix} = \begin{pmatrix} \dots & \dots & \dots \\ \dots & c_{ij} & \dots \\ \dots & \dots & \dots \end{pmatrix}$$

- Prvek c_{ij} vzniká vynásobením i -tého řádku matice **A** s j -tým sloupcem matice **B**.
- K tomu je potřeba, aby tento i -tý řádek a tento j -tý sloupec měly stejný počet prvků.
- Proto musí platit, že matice **B** má tolik řádků, kolik má matice **A** sloupců.
- Výsledná matice má pak tolik řádků, kolik jich má matice **A**, a tolik sloupců, kolik jich má matice **B**.

Úloha (Násobení matic)

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

Řešení.

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

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

- V předchozím případě nelze vypočítat $B \cdot A$, neboť matice B má jiný počet sloupců (3) než má matice A řádků (2).
- Necht A, B, C jsou matice a E je jednotková matice (vhodného rozměru). Potom každá z rovností

1) $A \cdot E = A,$

2) $E \cdot A = A,$

3) $(A + B) \cdot C = A \cdot C + B \cdot C,$

4) $A(B + C) = A \cdot B + A \cdot C,$

5) $A \cdot (B \cdot C) = (A \cdot B) \cdot C,$

platí, pokud mají příslušné operace smysl.

Historická "historka": Zrod nekomutativity

Zatímco sčítání nebo násobení čísel je komutativní ($a + b = b + a$, $a \cdot b = b \cdot a$), násobení matic obecně **není** ($\mathbf{A} \cdot \mathbf{B} \neq \mathbf{B} \cdot \mathbf{A}$). To byl obrovský myšlenkový posun!

Objevil to irský matematik **William Rowan Hamilton** kolem roku 1843. Zjistil, že aby mohl násobením popsat otáčení v 3D prostoru (hledal tzv. "kvaterniony"), musel se **vzdát komutativity**. Zpočátku byl z toho tak frustrovaný, že si myslel, že se mu nedaří, ale nakonec pochopil, že právě objevil novou, zásadní vlastnost algebry.

Inverzní matice

- Necht A a B jsou čtvercové matice typu (n, n) . Jestliže platí

$$AB = BA = E_n,$$

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

Regulární a singulární matice

- Nechť A je čtvercová matice typu (n, n) .

▶ Jestliže $h(A) = n$, pak A nazýváme **regulární** maticí.

▶ Jestliže $h(A) < n$, pak A nazýváme **singulární** maticí.

- Nechť je dána čtvercová matice A typu (n, n) . Potom jsou následující podmínky **ekvivalentní**:

- 1) A je regulární ($h(A) = n$),
- 2) $\det A \neq 0$, (Víme z minulé přednášky!)
- 3) k matici A existuje inverzní matice A^{-1} ,
- 4) matici A lze převést pomocí konečně mnoha ekvivalentních úprav na jednotkovou matici E_n .

Nyní je potřeba vypočítat $\det \mathbf{A}$ a tím také zjistit, zda $\mathbf{A}$ je regulární ($\det \mathbf{A} \neq 0$):

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

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

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

- Zapišeme 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 $\mathbf{A}^{-1}$:

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

Výpočet inverzní matice – Příklad (G eliminace)

- Určete inverzní matici $\mathbf{A}^{-1}$ k matici $\mathbf{A} = \begin{pmatrix} 1 & 2 & -1 \\ 2 & 0 & 1 \\ 1 & -2 & 1 \end{pmatrix}$.

- Zapišeme 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 řádkových úprav (Gaussova eliminace)
 - ▶ převedeme $\mathbf{A}$ (vlevo) na jednotkovou matici $\mathbf{E}_n$,
 - ▶ stejné úpravy aplikujeme na $\mathbf{E}_n$ (vpravo).

Výpočet inverzní matice pomocí ekvivalentních úprav

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

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

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

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

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

$$\begin{aligned}\mathbf{A}\vec{x} &= \vec{b}, \\ \mathbf{A}^{-1} \cdot (\mathbf{A}\vec{x}) &= \mathbf{A}^{-1} \cdot \vec{b}, \\ (\mathbf{A}^{-1}\mathbf{A})\vec{x} &= \mathbf{A}^{-1}\vec{b}, \quad (\text{asociativita}) \\ \mathbf{E}_n\vec{x} &= \mathbf{A}^{-1}\vec{b}, \\ \vec{x} &= \mathbf{A}^{-1}\vec{b},\end{aligned}$$

což dává další možnost určování řešení soustavy.

Úloha (Řešení soustavy lin. rovnic pomocí inverzní matice)

Pomocí inverzní matice vyřešte soustavu rovnic

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

Máme

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

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

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

(Pozn.: Jde o stejnou soustavu jako v minulé přednášce, kde jsme ji řešili Cramerovým pravidlem. Řešení je, jak se dalo čekat, stejné.)

Teoretický úvod (Aplikace: Šifrování)

- **Šifrování pomocí matic** spočívá v převodu zprávy na číselné hodnoty a v maticovém násobení.
- Klíčové pojmy:
 - ▶ **Šifrovací matice** A – matice (klíč), kterou násobíme vektor zprávy.
 - ▶ **Inverzní matice** A^{-1} – umožňuje dešifrování zprávy. Musí existovat, což znamená, že A musí být **regulární** ($\det A \neq 0$).
- Historie:
 - ▶ **Hillova šifra** (vynalezl Lester S. Hill, 1929) byla první **polygrafická** šifra, která zpracovávala více písmen najednou (jako bloky).
 - ▶ Tím byla mnohem odolnější proti *frekvenční analýze*, která snadno "zlomila" jednoduché záměny (např. Cézarovu šifru), kde stačilo spočítat nejčastější písmeno.
 - ▶ **Historka:** Ironií je, že Hillova šifra byla na svou dobu tak pokročilá, že ji armáda USA zpočátku odmítla. Byla považována za *příliš složitou* na "polní" použití. K jejímu prolomení je totiž potřeba znalost právě lineární algebry – Gaussovy eliminace a inverzních matic!

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:

$$\det(\mathbf{A}) = 2 \cdot 3 \cdot 2 + 4 \cdot 0 \cdot 1 + 2 \cdot 1 \cdot 2 - (1 \cdot 3 \cdot 2 + 2 \cdot 0 \cdot 2 + 2 \cdot 1 \cdot 4) = 2 \neq 0.$$

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 = <i>E</i>	10 = <i>J</i>	15 = <i>O</i>	20 = <i>T</i>	25 = <i>Y</i>
1 = <i>A</i>	6 = <i>F</i>	11 = <i>K</i>	16 = <i>P</i>	21 = <i>U</i>	26 = <i>Z</i>
2 = <i>B</i>	7 = <i>G</i>	12 = <i>L</i>	17 = <i>Q</i>	22 = <i>V</i>	
3 = <i>C</i>	8 = <i>H</i>	13 = <i>M</i>	18 = <i>R</i>	23 = <i>W</i>	
4 = <i>D</i>	9 = <i>I</i>	14 = <i>N</i>	19 = <i>S</i>	24 = <i>X</i>	

Číselné vyjádření zprávy (bez diakritiky) je:

13 1 20 9 3 5 0 10 19 15 21 0 21 26 9 20 5 3 14 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 **A** s maticí **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

Představte si, že jste kryptoanalytik a zachytili jste zprávu. Váš tým zjistil, že jde o Hillovu šifru 2×2 .

Odšifrujte zprávu

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

zašifrovanou maticí

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

- Matice $\mathbf{A}$ má determinant $3 \cdot 3 - 2 \cdot 4 = 9 - 8 = 1 \neq 0$, takže je regulární a má inverzní matici $\mathbf{A}^{-1}$.

Výpočet inverzní matice a dešifrování

- Inverzní matice (pro matici 2×2 lze snadno spočítat):

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

(Ověření: $\begin{pmatrix} 3 & 2 \\ 4 & 3 \end{pmatrix} \cdot \begin{pmatrix} 3 & -2 \\ -4 & 3 \end{pmatrix} = \begin{pmatrix} 9-8 & -6+6 \\ 12-12 & -8+9 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$)

- Násobíme tuto matici zleva na matici zašifrované zprávy $\mathbf{Z}_{\text{šifr}}$:

$$\mathbf{A}^{-1} \cdot \mathbf{Z}_{\text{šifr}} = \begin{pmatrix} 3 & -2 \\ -4 & 3 \end{pmatrix} \cdot \begin{pmatrix} 41 & 70 & 41 & 78 & 35 & 20 & 15 & 69 & 41 & 44 \\ 55 & 95 & 55 & 107 & 47 & 30 & 20 & 98 & 61 & 59 \end{pmatrix}$$

- Výsledkem je matice původní zprávy $\mathbf{Z}$:

$$\mathbf{Z} = \begin{pmatrix} 13 & 20 & 13 & 20 & 11 & 0 & 5 & 15 & 0 & 14 \\ 1 & 0 & 9 & 0 & 18 & 0 & 10 & 18 & 26 & 5 \end{pmatrix}$$

(kterou pak převedeme na písmena).

Výpočet inverzní matice a dešifrování

- Inverzní matice (pro matici 2×2 lze snadno spočítat):

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

(Ověření: $\begin{pmatrix} 3 & 2 \\ 4 & 3 \end{pmatrix} \cdot \begin{pmatrix} 3 & -2 \\ -4 & 3 \end{pmatrix} = \begin{pmatrix} 9-8 & -6+6 \\ 12-12 & -8+9 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$)

- Násobíme tuto matici zleva na matici zašifrované zprávy $\mathbf{Z}_{\text{šifr}}$:

$$\mathbf{A}^{-1} \cdot \mathbf{Z}_{\text{šifr}} = \begin{pmatrix} 3 & -2 \\ -4 & 3 \end{pmatrix} \cdot \begin{pmatrix} 41 & 70 & 41 & 78 & 35 & 20 & 15 & 69 & 41 & 44 \\ 55 & 95 & 55 & 107 & 47 & 30 & 20 & 98 & 61 & 59 \end{pmatrix}$$

- Výsledkem je matice původní zprávy $\mathbf{Z}$:

$$\mathbf{Z} = \begin{pmatrix} 13 & 20 & 13 & 20 & 11 & 0 & 5 & 15 & 0 & 14 \\ 1 & 0 & 9 & 0 & 18 & 0 & 10 & 18 & 26 & 5 \end{pmatrix}$$

(kterou pak převedeme na písmena).

Převod čísel zpět na text

- Přečteme matici **Z** po sloupcích a převedeme hodnoty na písmena podle původního schématu:

$$\begin{pmatrix} \textcolor{red}{13} & 20 & 13 & 20 & 11 & 0 & 5 & 11 & 1 & 14 \\ \textcolor{red}{1} & 5 & 1 & 9 & 1 & 10 & 0 & 18 & 19 & 1 \end{pmatrix}$$

- $13 \rightarrow M, 1 \rightarrow A, \dots$

M A T E M A T I K A — J E — K R A S N A