MB141, 19. 6. 2023, zkouška, skupina Y

Příklad. **1A.** [2 body] Rozhodněte, zda soustava lineárních rovnic

$$\begin{array}{rrrrl} x & +4y & -2z & +3w & = 0 \\ 2x & +7y & -z & +4w & = -3 \\ -x & -2y & -4z & +w & = 6 \end{array}$$

má řešení. Případné řešení nehledejte, ale odpověď náležitě zdůvodněte.

Řešení. Soustavu přepíšeme do maticového schématu a upravíme na schodový tvar:

$$\left(\begin{array}{cccc|c} 1 & 3 & -2 & 3 & 0 \\ 2 & 6 & -1 & 4 & -2 \\ -1 & -1 & -4 & 2 & 4 \end{array}\right) \sim \cdots \sim \left(\begin{array}{cccc|c} 1 & 4 & -2 & 3 & 0 \\ 0 & -1 & 3 & -2 & -2 \\ 0 & 0 & 0 & -1 & 0 \end{array}\right)$$

Hodnost (počet nenulových řádků) základní i rozšířené matice je stejný (3), soustava tedy má řešení. □

Příklad. **1B.** [2 body] Najděte matici M zobrazení $f : \mathbb{R}^3 \to \mathbb{R}^3$ (ve standardní bázi), které je kolmou projekcí (promítáním) na rovinu $\rho : y = 0$.

Řešení. Normálovým vektorem roviny ρ je $n = (0, 1, 0)$. Ten se při projekci anuluje: $f(n) = 0$. V rovině ρ leží mimo jiné další dva vektory standardní báze $u = (1, 0, 0)$ a $v = (0, 0, 1)$ a ty projekce ponechává na místě: $f(u) = u, f(v) = v$. Protože známe obrazy všech vektorů standardní báze, jejich prostým poskládáním do sloupců dostáváme ihned matici M:

$$M = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

□

Příklad. **1C.** [2 body] Určete vzdálenost bodu $A = [11, 5, 3]$ od roviny $\rho : B + su + tv, B = [2, 2, 3], u = (0, 1, -2), v = (1, -3, 2)$ v prostoru $\mathbb{R}^3$.

Řešení. Vzdálenost se realizuje kolmicí na rovinu ρ, tj. ve směru jejího normálového vektoru n. Ten je řešením soustavy rovnic $\langle n, u\rangle = 0, \langle n, v\rangle = 0$, tedy např. $n = (4, 2, 1)$. Úlohu lze dopočítat mnoha způsoby, např. tak, že do směru vektoru n promítneme vektor $A - B = (9, 3, 0)$. Je-li P pata kolmice z B, platí $A - B = (A - P) + (P - B)$, přičemž $A - P = kn$ a $P - B \perp n$. Po aplikaci skalárního součinu s n dostaneme $\langle A - B, n\rangle = k\langle n, n\rangle$, odkud $42 = 21k$ a $k = 2$. Hledaná vzdálenost je tedy $\|kn\| = 2 \cdot \sqrt{4^2 + 2^2 + 1} = 2 \cdot \sqrt{21}$. □

Příklad. **2A.** [2 body] Najděte inverzi prvku $x = 35$ modulo 96.

Řešení. Modul lze rozložit $96 = 2^5 \cdot 3$. Platí $35 \equiv 3 \pmod{32}$ a zřejmě $3 \cdot 11 \equiv 1 \pmod{32}$. Dále $35 \equiv -1 \pmod{3}$ a $-1 \cdot (-1) = 1$. Platí tak $x^{-1} = 32a + 11$ a $32a + 11 \equiv -1 \pmod{3}$, odkud $a \equiv 0 \pmod{3}$, a celkem tedy $x^{-1} \equiv 11 \pmod{96}$.

Alternativní postup: Inverzi určíme jako koeficient a v Bezoutově rovnosti $35a + 96b = 1$ s využitím Eukleidova algoritmu. □

Příklad. **2B.** [5 bodů] Nechť $n = 29$ je modul a $g = 8$.

a) Dokažte, že g je primitivní kořen.

b) Bob zná Alicin veřejný klíč $g^a = 27$, zvolí si $b = 9$ a chce poslat zprávu $M = 13$ protokolem ElGamal. Určete jeho veřejný klíč g^b a zašifrovanou zprávu $g^{ab}M$.

Řešení. a) Stačí zkontrolovat, že g^m nenabývá hodnoty 1 pro maximální dělitele m čísla $\phi(n)$. Protože platí $\phi(29) = 28 = 2^2 \cdot 7$, jsou těmito „kritickými“ exponenty $2^2 = 4$ a $2 \cdot 7 = 14$. Dostáváme $8^4 = 64^2 \equiv 6^2 \equiv 7 \not\equiv 1 \pmod{29}$ a $8^{14} \equiv 6^7 \equiv 6 \cdot 7^3 \equiv 6 \cdot 7 \cdot (-9) = -117 \equiv -1 \not\equiv 1 \pmod{29}$.

b) S využitím výpočtů z části (a) dostáváme: $g^b = 8^9 = 8 \cdot (8^4)^2 \equiv 8 \cdot 7^2 \equiv 8 \cdot (-9) \equiv 15 \pmod{29}$, $g^{ab} = 27^9 \equiv (-2)^9 = (-8)^3 \equiv -8 \cdot 6 \equiv 10 \pmod{29}$ a $10 \cdot 13 \equiv 14 \pmod{29}$. □

Příklad. **3A.** [2 body] Určete vlastní čísla matice

$$A = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 2 \end{pmatrix}.$$

Řešení. Hledáme kořeny charakteristického polynomu, tj. determinantu

$$|A - \lambda E| = \begin{vmatrix} -\lambda & 1 & 0 \\ 1 & -\lambda & 0 \\ 0 & 0 & 2-\lambda \end{vmatrix}.$$

Determinant lze rozvinout např. podle třetího řádku, a následně snadno dopočítat: $|A - \lambda E| = (2-\lambda)(\lambda^2 - 1) = (2-\lambda)(\lambda - 1)(\lambda + 1)$. Kořeny tedy jsou $2, 1, -1$. □

Příklad. **3B.** [5 bodů] Starý dub prochází každý rok některou ze tří růstových fází: buď to sílí v kořenech, nebo ve větvích, nebo plodí žaludy. Po roce, ve kterém dub neplodí, s pravděpodobností $1/2$ následuje rok, ve kterém dub sílí ve větvích, a s pravděpodobností $1/4$ následuje rok, ve kterém dub sílí v kořenech. Po roce, ve kterém dub plodí, následuje s pravděpodobností $3/4$ rok, ve kterém dub sílí ve kořenech, a dub určitě zvovu neplodí.

a) Určete matici Markovova procesu M v pořadí stavů „kořeny“, „větve“, „žaludy“.

b) Určete pravděpodobnost, že v daném roce dub plodí.

Řešení. a) Pro „nežaludové“ roky dopočítáme doplňkovou pravděpodobnost $1/4$ pro situaci, že dub bude v následujícím roce plodit. Podobně určíme, že po „žaludovém“ roce následuje s pravděpodobností $1/4$ „kořenový“ rok. Poskládáním pravděpodobnostních rozdělení do sloupců dostaneme matici

$$M = \begin{pmatrix} 1/4 & 1/4 & 3/4 \\ 1/2 & 1/2 & 1/4 \\ 1/4 & 1/4 & 0 \end{pmatrix}.$$

b) Nejprve určíme stacionární vektor v jako vlastní vektor matice M pro vlastní číslo 1, tj. řešení homogenní soustavy $(M - E)v = 0$. Řešením je např. vektor $v = (7, 9, 4)$, po normalizaci dostáváme pravděpodobnostní vektor $\frac{1}{20}v$. Pravděpodobnost žaludového roku je tedy $\frac{4}{20} = \frac{1}{5}$.

Alternativní postup: Bylo možné využít i faktu, že nežaludové roky vedou ke stejnému vývoji, sloučit je do jednoho stavu a počítat pouze dvoustavový proces. □