MB141, 21. 5. 2024, zkouška

1.1 Najděte všechna řešení komplexní rovnice $x^2 = 2i$.
[≥ 1 správných, 1 bod]

☐ $x = \sqrt{2} + i\sqrt{2}$
☐ $x = 1 + i$
☐ $x = 1 - i$
☐ $x = \sqrt{2} - i\sqrt{2}$
☐ $x = -1 + i$
☐ $x = -1 - i$

1.2 Nechť A je reálná čtvercová matice řádu n a $\det A$ její determinant. Vyberte všechna pravdivá tvrzení.
[≥ 1 správných, 1 bod]

☐ Pokud má A nulový řádek, pak $\det A = 0$.
☐ Pokud $\det A = 0$, pak A má nulový řádek.
☐ Pokud $\det A = 0$, pak k A existuje inverzní matice.
☐ Pokud $\det A = 0$, pak lze A řádkovými úpravami převést na matici s nulovým řádkem.
☐ Pokud má A některý prvek na hlavní diagonále nulový, pak $\det A = 0$.
☐ Matice A má stejný determinant jako matice k ní transponovaná.

1.3 [3 body] Najděte inverzní matici k matici

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

2.1 Vektor u patří do podprostoru generovaného vektory v, w. Vyberte pravdivá tvrzení.
[≥ 1 správných, 1 bod]

☐ Vektory u, v, w jsou lineárně nezávislé.
☐ Matice sestavená z vektorů u, v, w má hodnost nejvýše dva.
☐ Vektory u, v, w tvoří bázi nějakého podprostoru.
☐ Vektor u je lineární kombinací vektorů v, w.
☐ Nulový vektor je nenulovou lineární kombinací vektorů u, v, w.
☐ Matice sestavená z vektorů u, v má menší hodnost než matice sestavená z vektorů u, v, w.

2.2 Uvažujme lineární zobrazení, jenž je zrcadlením prostoru $\mathbb{R}^3$ podle roviny. Určete trojici jeho vlastních čísel.
[1 správná, 1 bod]

☐ $0, 1, 1$.
☐ $-1, 1, 1$.
☐ $-1, -1, 1$.
☐ $0, 0, 1$.
☐ $-1, 0, 1$.
☐ $-1, -1, -1$.

2.3 [3 body] Určete vzdálenost bodu $A = [1, 2, -1]$ od přímky $p : 2x - y + 2z = 7$ v $\mathbb{R}^3$.

3.1 Zaškrtněte všechny primitivní kořeny v modulu 5.
[$\geq$ 1 správných, 1 bod]

☐ 0
☐ 1
☐ 2
☐ 3
☐ 4

3.2 Nechť $n = pq$ je modul, e veřejný klíč pro šifrování metodou RSA, d jeho inverze v modulu n a M zpráva, kterou chceme zašifrovat. Určete, které z čísel lze bezpečně zveřejnit.
[$\geq$ 1 správných, 1 bod]

☐ n
☐ p
☐ $\phi(n)$
☐ Me
☐ d
☐ Med

3.3 [3 body] Určete zbytek po dělení čísla 7^{7^7} číslem 11.

4.1 [1 správná, 1 bod] Leslieho populační model je dán maticí

$$L = \begin{pmatrix} 0 & p & 2 \\ 2/3 & 0 & 0 \\ 0 & 2/3 & 0 \end{pmatrix}.$$

Vyberte hodnotu parametru p, pro kterou je populace stabilní.

☐ 1 ☐ $1/2$ ☐ $1/3$
☐ $1/6$ ☐ 3 ☐ 6

4.2 [$\geq$ 1 správných, 1 bod] Rozhodněte, které z matic jsou primitivní.

☐ $\begin{pmatrix} 1 & 2 \\ 0 & 3 \end{pmatrix}$ ☐ $\begin{pmatrix} 1 & 2 \\ 3 & 0 \end{pmatrix}$

☐ $\begin{pmatrix} 0 & 1 \\ 2 & 3 \end{pmatrix}$ ☐ $\begin{pmatrix} 1 & 0 \\ 2 & 3 \end{pmatrix}$

4.3 [3 body] Uvažujme markovský proces na stavech A, B, C. Systém přechází z A do B s pravděpodoností $1/2$ a do stavu C s pravděpodoností $1/4$. Ze stavu B přechází vždy do stavu A. Ze stavu C přechází s pravděpodoností $1/4$ do stavu A a s pravděpodobností $1/4$ do stavu B.

a) [1 bod] Určete zbývající pravděpodobnosti přechodů a sestavte matici procesu M.

b) [2 body] Určete, s jakou pravděpodobností se po dostatečně dlouhé době systém nachází ve stavu C.

ŘEŠENÍ

1.1 $1+i, -1-i$ (lze řešit i pouhým vyzkoušením)
1.2 1., 4., 6. možnost
1.3 Úlohu řešíme eliminací schématu $(A|E) \sim \ldots \sim (E|A^{-1})$, výsledkem je matice

$$\begin{pmatrix} -1/2 & -1/2 & 1/2 \\ 1/2 & 1/2 & 1/2 \\ -1/2 & 1/2 & 1/2 \end{pmatrix}.$$

2.1 2., 4., 5. možnost
2.2 $-1, 1, 1$
2.3 Rovina p má normálový vektor $n = (2, -1, 2)$, v jehož směru se vzdálenost realizuje. Hledáme tedy bod B, který leží v p a současně je tvaru $A + tn$. Dosazením do rovnice roviny spočítáme $t = 1$, a tedy vzdálenost je rovna velikosti n, tj. $\|n\| = \sqrt{4+1+4} = 3$.
3.1 $\phi(5) = 4$ má jediného maximálního dělitele 2, stačí tedy určit ta x, pro něž $x^2 \not\equiv 1$ a samozřejmě jsou s 5 nesoudělná. Tomu vyhovují jen 2 a 3. **3.2** n, Me, odstatní čísla zprávu snadno vyzradí — Med je přímo M, d dešifruje Me, z $\phi(n)$ zjistíme d a z p zjistíme $\phi(n)$.
3.3 Podle malé Fermatovy věty $7^{10} \equiv 1 \pmod{11}$. Zjednodušíme tedy nejprve 7^7 v modulu 10. Ten můžeme rozložit $10 = 2 \cdot 5$ a spočítat samostatně $7^7 \equiv 1 \pmod 2$ a $7^7 \equiv 2^{4+3} \equiv 2^3 = 8 \equiv 3 \pmod 5$ dalším užitím malé Fermatovy věty. Podle čínské zbytkové věty celkem máme $7^7 \equiv 3 \pmod{10}$, což dosadíme do původní úlohy. Dostáváme $7^{7^7} \equiv 7^3 = 343 \equiv 2 \pmod{11}$.
4.1 Pro správné p musí mít matice L vlastní číslo 1, neboli v $L - E$ jsou závislé řádky. To nastává pro $p = 1/6$.
4.2 2. a 3. matice, ve zbylých po umocnění zůstává nula na stejné pozici.
4.3 Pravděpodobnosti neznámých přechodů zjistíme doplněním známých do jedničky, např $A \to A$ bude $1 - \frac{1}{2} - \frac{1}{4} = \frac{1}{4}$. Přechod $B \to A$ je jistý jev, má tedy pravděpodobnost 1 a zbylé přechody z B musí být 0. Matice je pak

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

Dále potřebujeme najít vlastní vektor v pro vlastní číslo 1, tj. řešit homogenní soustavu $(M - E)v = 0$. Tím je např. vektor $v = (8, 5, 4)$. Jeho normalizací dostaneme pravděpodobnostní vektor $\frac{1}{17}v = \left(\frac{8}{17}, \frac{5}{17}, \frac{4}{17}\right)$, tedy hledaná pravděpodobnost pro stav C je $\frac{4}{17}$.