MB141, zkouška 5. 6. 2020

Příklad. 1A. V prostoru $\mathbb{R}_4[x]$ polynomů stupně nejvýše 4 najděte báze a dimenze podprostorů

$$P = \{f \in \mathbb{R}_4[x]; f(1) = f(0),\ f(-1) = f(0)\},$$
$$Q = [x^4 - 3x^2 + 2, x^2 - 1, x^4 + 2x^3 - 3x^2 - 2x + 2]$$

a báze a dimenze jejich průniku a součtu.

Řešení. Koeficienty polynomu $f(x) = a_4x^4 + a_3x^3 + a_2x^2 + a_1x + a_0$ z podprostoru P splňují homogenní soustavu dvou rovnic s maticí

$$\begin{pmatrix} 1 & 1 & 1 & 1 & 0 \\ 1 & -1 & 1 & -1 & 0 \end{pmatrix} \sim \begin{pmatrix} 1 & 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 \end{pmatrix}$$

Proto $(a_4, a_3, a_2, a_1, a_0) = (p, q, -p, -q, r)$, kde $p, q, r \in \mathbb{R}$ jsou parametry. Tedy báze podprostoru P je $x^4 - x^2, x^3 - x, 1$. Polynomy označme f_1, f_2, f_3.

Polynomy generující podprostor Q jsou lineárně nezávislé, tvoří tedy jeho bázi. Označme je g_1, g_2, g_3.

Polynomy z $P \cap Q$ jsou tvaru $p = c_1f_1 + c_2f_2 + c_3f_3 = d_1g_1 + d_2g_2 + d_3g_3$. To vede na homogenní soustavu 5 rovnic o 6 neznámých $c_1, c_2, c_3, d_1, d_2, d_3$, která má matici

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

Řešení této soustavy je $(d_1, d_2, d_3) = (p, 2p + 2q, q)$, kde $p, q \in \mathbb{R}$ jsou parametry. To dává bázi průniku $g_1 + 2g_2 = x^4 - x^2$, $2g_2 + g_3 = x^4 + 2x^3 - x^2 - 2x$ nebo také $x^4 - x^2, x^3 - x$.

Z předchozí soustavy plyne, že $P + Q = [f_1, f_2, f_3, g_1, g_2, g_3] = [f_1, f_2, f_3, g_1]$. Poslední čtyři polynomy tvoří bázi $P + Q$. □

Bodování. Rovnice pro P **2 body**, řešení **2 body**, báze v polynomech **4 body**. Je-li báze jako pětice koeficientů tak **pouze 2 body**.

Dimenze a báze Q **2 body**.

Báze $P \cap Q$. Soustava **3 body**, řešení **3 body**, báze v polynomech **4 body**. Za pětice koeficientů pouze **2 body**.

Báze součtu **5 bodů**.

Je-li u součtu nebo průniku spočtena pouze dimenze podle správné formule, tak **2 body**.

□

Příklad. **1B.** V prostoru $\mathbb{R}_4[x]$ polynomů stupně nejvýše 4 najděte báze a dimenze podprostorů

$$R = \{g \in \mathbb{R}_4[x]; g(1) = g(0),\ g(-1) = 0\},$$
$$S = [x^4 - 3x^2 + 1, 2x^2 - 1, x^4 + x^3 - 3x^2 - x + 1]$$

a báze a dimenze jejich průniku a součtu.

Řešení. Koeficienty polynomu $g(x) = a_4x^4 + a_3x^3 + a_2x^2 + a_1x + a_0$ z podprostoru R splňují homogenní soustavu dvou rovnic s maticí

$$\begin{pmatrix} 1 & 1 & 1 & 1 & 0 \\ 1 & -1 & 1 & -1 & 1 \end{pmatrix} \sim \begin{pmatrix} 1 & 1 & 1 & 1 & 0 \\ 0 & 2 & 0 & 2 & -1 \end{pmatrix}$$

Proto $(a_4, a_3, a_2, a_1, a_0) = (p+q+r, -p, -q, -r, -2p-2r)$, kde $p, q, r \in \mathbb{R}$ jsou parametry. Tedy báze podprostoru R je $x^4 - x^3 - 2, x^4 - x^2, x^4 - x - 2$. Polynomy označme g_1, g_2, g_3.

Polynomy generující podprostor S jsou lineárně nezávislé, tvoří tedy jeho bázi. Označme je h_1, h_2, h_3.

Polynomy z $R \cap S$ jsou tvaru $p = c_1g_1 + c_2g_2 + c_3g_3 = d_1h_1 + d_2h_2 + d_3h_3$. To vede na homogenní soustavu 5 rovnic o 6 neznámých $c_1, c_2, c_3, d_1, d_2, d_3$, která má matici

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

Řešení této soustavy je $(d_1, d_2, d_3) = (p - q, p, q)$, kde $p, q \in \mathbb{R}$ jsou parametry. To dává bázi průniku $h_1 + h_2 = x^4 - x^2$, $-h_1 + h_3 = x^3 - x$.

Z předchozí soustavy plyne, že $R + S = [g_1, g_2, g_3, h_1, h_2, h_3] = [g_1, g_2, g_3, h_1]$. Poslední čtyři polynomy tvoří bázi $R + S$. □

Bodování. Rovnice pro R **2 body**, řešení **2 body**, báze v polynomech **4 body**. Je-li báze jako pětice koeficientů tak **pouze 2 body**.

Dimenze a báze S **2 body**.

Báze $R \cap S$. Soustava **3 body**, řešení **3 body**, báze v polynomech **4 body**. Za pětice koeficientů pouze **2 body**.

Báze součtu **5 bodů**.

Je-li u součtu nebo průniku spočtena pouze dimenze podle správné formule, tak **2 body**.

□

Příklad. **1C.** V prostoru $\mathbb{R}_4[x]$ polynomů stupně nejvýše 4 najděte báze a dimenze podprostorů

$$U = \{h \in \mathbb{R}_4[x]; h(-1) = h(0),\ h(1) = 0\},$$
$$V = [x^4 + 2x^3 - x^2 + 1, 2x^3 + 1, x^4 - x^2 + 2x + 1]$$

a báze a dimenze jejich průniku a součtu.

Řešení. Koeficienty polynomu $h(x) = a_4x^4 + a_3x^3 + a_2x^2 + a_1x + a_0$ z podprostoru U splňují homogenní soustavu dvou rovnic s maticí

$$\begin{pmatrix} 1 & -1 & 1 & -1 & 0 \\ 1 & 1 & 1 & 1 & 1 \end{pmatrix} \sim \begin{pmatrix} 1 & -1 & 1 & -1 & 0 \\ 0 & 2 & 0 & 2 & 1 \end{pmatrix}$$

Proto $(a_4, a_3, a_2, a_1, a_0) = (p-q+r, p.q, r, -2p-2r)$, kde $p, q, r \in \mathbb{R}$ jsou parametry. Tedy báze podprostoru U je $x^4 + x^3 - 2, x^4 - x^2, x^4 + x - 2$. Polynomy označme h_1, h_2, h_3.

Polynomy generující podprostor V jsou lineárně nezávislé, tvoří tedy jeho bázi. Označme je g_1, g_2, g_3.

Polynomy z $U \cap V$ jsou tvaru $p = c_1h_1 + c_2h_2 + c_3h_3 = d_1g_1 + d_2g_2 + d_3g_3$. To vede na homogenní soustavu 5 rovnic o 6 neznámých $c_1, c_2, c_3, d_1, d_2, d_3$, která má matici

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

Řešení této soustavy je $(d_1, d_2, d_3) = (p+q, -p, -q)$, kde $p, q \in \mathbb{R}$ jsou parametry. To dává bázi průniku $g_1 - g_2 = x^4 - x^2$, $g_1 - g_3 = 2x^3 - 2x$ nebo také $x^4 - x^2, x^3 - x$.

Z předchozí soustavy plyne, že $U + V = [h_1, h_2, h_3, g_1, g_2, g_3] = [h_1, h_2, h_3, g_1]$. Poslední čtyři polynomy tvoří bázi $U + V$. □

Bodování. Rovnice pro U **2 body**, řešení **2 body**, báze v polynomech **4 body**. Je-li báze jako pětice koeficientů tak **pouze 2 body**.

Dimenze a báze V **2 body**.

Báze $U \cap V$. Soustava **3 body**, řešení **3 body**, báze v polynomech **4 body**. Za pětice koeficientů pouze **2 body**.

Báze součtu **5 bodů**.

Je-li u součtu nebo průniku spočtena pouze dimenze podle správné formule, tak **2 body**.

□

Příklad. **2A.** Ukažte, že matice

$$A = \frac{1}{3}\begin{pmatrix} -2 & -1 & 2 \\ 2 & -2 & 1 \\ 1 & 2 & 2 \end{pmatrix}$$

je ortogonální, a zjistěte, jaké geometrické zobrazení v $\mathcal{E}_3$ popisuje předpis $\varphi(x) = Ax$, kde $x = (x_1, x_2, x_3)^T$ je sloupec standardních souřadnic v $\mathcal{E}_3$.

Řešení. Sloupce matice jsou na sebe kolmé a mají jednotkovou velikost. Proto je matice ortogonální.

Spočítáme determinant matice A. Ten je roven 1, proto musí mít matice vlastní číslo 1 a proto je také dané zobrazení otočení kolem osy procházející počátkem se směrovým vektorem, který je vlastním vektorem k vlastnímu číslu 1.

Spočítáme vlastní vektor k vlastnímu číslu 1. Jsou to násobky vektoru $u = (1, 1, 3)^T$. Je dobré provést kontrolu tím, že se přesvědčíme, že skutečně $Au = u$.

Nyní zjistíme úhel otočení α. Vezmeme nějaký nenulový vektor kolmý k u, např. $v = (1, -1, 0)^T$. Spočítáme

$$Av = \left(-\frac{1}{3}, \frac{4}{3}, -\frac{1}{3}\right)^T.$$

Cosinus úhlu otočení bude

$$\cos\alpha = \frac{\langle v, Av\rangle}{||u|| \cdot ||Av||} = -\frac{5}{6}.$$

Závěr: Dané zobrazení je otočení kolem osy $[0, 0, 0]+a(1, 1, 3)$ o úhel α, kde $\cos\alpha = -\frac{5}{6}$.

□

Bodování. Kontrola ortogonality **3 body**.

Výpočet determinantu **3 body**.

Úvaha, že jde o otočení kolem osy určené vlastním vektorem k 1 **2 body**.

Výpočet vlastního vektoru k 1: soustava **3 body**, výsledek **3 body**.

Volba kolmého vektoru v a jeho zobrazení Av **6 bodů**.

Výpočet cosinu úhlu otočení **3 body**, explicitní popis osy otáčení **2 body**.

□

Příklad. **2B.** Ukažte, že matice

$$B = \frac{1}{3}\begin{pmatrix} -2 & 2 & -1 \\ 2 & 1 & -2 \\ 1 & 2 & 2 \end{pmatrix}$$

je ortogonální, a zjistěte, jaké geometrické zobrazení v $\mathcal{E}_3$ popisuje předpis $\varphi(x) = Bx$, kde $x = (x_1, x_2, x_3)^T$ je sloupec standardních souřadnic v $\mathcal{E}_3$.

Řešení. Sloupce matice jsou na sebe kolmé a mají jednotkovou velikost. Proto je matice ortogonální.

Spočítáme determinant matice B. Ten je roven -1, proto musí mít matice vlastní číslo -1 a proto je také dané zobrazení složení otočení kolem osy procházející počátkem se směrovým vektorem, který je vlastním vektorem k vlastnímu číslu -1, se symetrií podle roviny procházející počátkem a kolmé na osu otáčení.

Spočítáme vlastní vektor k vlastnímu číslu -1. Jsou to násobky vektoru $u = (2, -1, 0)^T$. Je dobré provést kontrolu tím, že se přesvědčíme, že skutečně $Bu = -u$.

Nyní zjistíme úhel otočení β. Vezmeme nějaký nenulový vektor kolmý k u, např. $v = (0, 0, 1)^T$. Spočítáme

$$Bv = \left(-\frac{1}{3}, -\frac{2}{3}, \frac{2}{3}\right)^T.$$

Cosinus úhlu otočení bude

$$\cos\alpha = \frac{\langle v, Bv\rangle}{||u|| \cdot ||Bv||} = \frac{2}{3}.$$

Závěr: Dané zobrazení je složení symetrie podle roviny

$$2x_1 - x_2 = 0$$

s otočením kolem osy $[0, 0, 0] + a(2, -1, 0)$ o úhel β, kde $\cos\beta = \frac{2}{3}$.

□

Bodování. Kontrola ortogonality **3 body**.

Výpočet determinantu **3 body**.

Výpočet vlastního vektoru k -1: soustava **3 body**, výsledek **3 body**.

Volba kolmého vektoru v a jeho zobrazení Av **6 bodů**.

Výpočet cosinu úhlu otočení **3 body**, explicitní popis osy otáčení **2 body** a roviny symetrie **2 body**. Pokud není explicitně uvedeno, že jde o složení otočení a symetrie poslední 4 body nedávat .

□

Příklad. **2C.** Ukažte, že matice

$$C = \frac{1}{3}\begin{pmatrix} -2 & -1 & 2 \\ 1 & 2 & 2 \\ 2 & -2 & 1 \end{pmatrix}$$

je ortogonální, a zjistěte, jaké geometrické zobrazení v $\mathcal{E}_3$ popisuje předpis $\varphi(x) = Cx$, kde $x = (x_1, x_2, x_3)^T$ je sloupec standardních souřadnic v $\mathcal{E}_3$.

Řešení. Sloupce matice jsou na sebe kolmé a mají jednotkovou velikost. Proto je matice ortogonální.

Spočítáme determinant matice C. Ten je roven -1, proto musí mít matice vlastní číslo -1 a proto je také dané zobrazení složení otočení kolem osy procházející počátkem se směrovým vektorem, který je vlastním vektorem k vlastnímu číslu -1, se symetrií podle roviny procházející počátkem a kolmé na osu otáčení.

Spočítáme vlastní vektor k vlastnímu číslu -1. Jsou to násobky vektoru $u = (2, 0, -1)^T$. Je dobré provést kontrolu tím, že se přesvědčíme, že skutečně $Cu = -u$.

Nyní zjistíme úhel otočení γ. Vezmeme nějaký nenulový vektor kolmý k u, např. $v = (0, 1, 0)^T$. Spočítáme

$$Cv = \left(-\frac{1}{3}, \frac{2}{3}, -\frac{2}{3}\right)^T.$$

Cosinus úhlu otočení bude

$$\cos\alpha = \frac{\langle v, Cv\rangle}{||u|| \cdot ||Cv||} = \frac{2}{3}.$$

Závěr: Dané zobrazení je složení symetrie podle roviny

$$2x_1 - x_3 = 0$$

s otočením kolem osy $[0, 0, 0] + c(2, 0, -1)$ o úhel γ, kde $\cos\gamma = \frac{2}{3}$.

□

Bodování. Kontrola ortogonality **3 body**.

Výpočet determinantu **3 body**.

Výpočet vlastního vektoru k -1: soustava **3 body**, výsledek **3 body**.

Volba kolmého vektoru v a jeho zobrazení Av **6 bodů**.

Výpočet cosinu úhlu otočení **3 body**, explicitní popis osy otáčení **2 body** a roviny symetrie **2 body**. Pokud není explicitně uvedeno, že jde o složení otočení a symetrie poslední 4 body nedávat .

□

Příklad. **3A.** Profesor má 3 oblíbené otázky, z kterých se u každého zkouškového termínu jedna objeví. Profesor nikdy nepoužije stejné otázky po sobě. Když naposledy použil otázku 1, hodí mincí a v případě, že padne líc, zadá otázku 2. Když použil otázku 2, hází 2 mincemi a přejde k otázce 3, pokud je líc na obou mincích. Pokud naposledy zadal otázku 3, tak si hodí 3 mincemi a přejde k otázce 1, když na všech třech padl líc.

Modelujte zadávání otázek pomocí Markovova procesu. Určete jeho matici a zdůvodněte, že je primitivní. Pomocí maticového násobení zjistěte, jaká je pravděpodobnost, že u třetího termínu zadá otázku 2, jestliže u prvního zadal otázku 1. Za předpokladu, že tímto způsobem zadává otázky hodně dlouho, zjistěte, kterou otázku zadává nejčastěji - výsledek vyjádřete v procentech a vysvětlete, jak jste k němu dospěli.

Řešení. Matice Markovovova procesu je

$$M = \begin{pmatrix} 0 & 3/4 & 1/8 \\ 1/2 & 0 & 7/8 \\ 1/2 & 1/4 & 0 \end{pmatrix}$$

Spočteme-li $M^2 = M \cdot M$, dostaneme matici se všemi vstupy kladnými. Proto je M primitivní matice.

Pravděpodobnost, že profesor zadá u třetího termínu 2. otázku, když u prvního zadal 1. otázku je dána druhou složkou součinu

$$M \cdot M \cdot \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}$$

a ta je $7/16$.

Při dlouhodobém zadávání se pravděpodobnosti zadání jednotlivých otázek blíží pravděpodobnostnímu vektoru, který je vlastním vektorem matice M k vlastnímu číslu 1. Řešíme proto homogenní soustavu

$$(M - E)x = 0.$$

Její matici upravíme na schodovitý tvar

$$\begin{pmatrix} -1 & 3/4 & 1/8 \\ 1/2 & -1 & 7/8 \\ 1/2 & 1/4 & -1 \end{pmatrix} \sim \begin{pmatrix} 4 & -8 & 7 \\ 0 & -2 & 3 \\ 0 & 0 & 0 \end{pmatrix}.$$

Vlastní vektory jsou $a(5, 6, 4)$. Pravděpodobnostní vektor je

$$(1/3, 2/5, 4/15).$$

V dlouhodobém horizontu pokládá profesor nejčastěji otázku 2, a to s pravděpodobností $2/5$, tj. 40%.

□

Bodování. Správná matice **6 bodů**. (2 za každý sloupec) Zdůvodnění primitivnosti **2 body**.

Výpočet $7/16$ **2 body**.

Soustava pro vlastní vektor a její úprava na schodovitý tvar **5 bodů**. Správné řešení ve formě pravděpodobnostního vektoru **5 bodů**.

Správné určení otázky **2 body**, správná procenta **3 body**. □

Příklad. **3B.** Profesor trpí syndromem vyhoření a u zkoušek už zadává jenom jeden ze tří testů A, B, C. Nikdy však nepoužije po sobě stejné testy. Když naposledy zadal test A, hodí si kostkou a v případě, že padne číslo dělitelné 3, zadá test B. Když použil test B, hází dvěma mincemi a přejde k testu C, pokud na obou padne líc. Když naposledy zadal test C, tak hází opět kostkou a přejde k testu A, pokud na kostce padne prvočíslo.

Modelujte zadávání testů pomocí Markovova procesu. Určete jeho matici a zdůvodněte, že je primitivní. Pomocí maticového násobení zjistěte, jaká je pravděpodobnost, že u třetího termínu zadá test B, jestliže u prvního zadal test C. Za předpokladu, že tímto způsobem zadává testy hodně dlouho, zjistěte, který test zadává nejčastěji a s jakou pravděpodobností. Vysvětlete, jak jste k výsledku dospěli.

Řešení. Matice Markovovova procesu je

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

Spočteme-li $M^2 = M \cdot M$, dostaneme matici se všemi vstupy kladnými. Proto je M primitivní matice.

Pravděpodobnost, že profesor zadá u třetího termínu test B, když u prvního zadal test C je dána druhou složkou součinu

$$M \cdot M \cdot \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}$$

a ta je $1/6$.

Při dlouhodobém zadávání se pravděpodobnosti zadání jednotlivých testů blíží pravděpodobnostnímu vektoru, který je vlastním vektorem matice M k vlastnímu číslu 1. Řešíme proto homogenní soustavu

$$(M - E)x = 0.$$

Její matici upravíme na schodovitý tvar

$$\begin{pmatrix} -1 & 3/4 & 1/2 \\ 1/3 & -1 & 1/2 \\ 2/3 & 1/4 & -1 \end{pmatrix} \sim \begin{pmatrix} 2 & -6 & 3 \\ 0 & -9 & 8 \\ 0 & 0 & 0 \end{pmatrix}.$$

Vlastní vektory jsou $a(21, 16, 18)$. Pravděpodobnostní vektor je

$$(21/55, 16/55, 18/55).$$

V dlouhodobém horizontu zadává profesor nejčastěji test A, a to s pravděpodobností $21/55$.

□

Bodování. Správná matice **6 bodů**. (2 za každý sloupec) Zdůvodnění primitivnosti **2 body**.

Výpočet $1/6$ **2 body**.

Soustava pro vlastní vektor a její úprava na schodovitý tvar **5 bodů**. Správné řešení ve formě pravděpodobnostního vektoru **5 bodů**.

Správné určení otázky **2 body**, správná procenta **3 body**. □

Příklad. **3C.** Profesor se po koronavirové epidemii rozhodl, že bude na studenty hodný, a u zkoušek jim zadává jenom jeden ze tří testů X, Y, Z. Nikdy však nepoužije po sobě stejné testy. Když naposledy zadal test X, hodí si kostkou a když padne sudé (párne) číslo, zadá test Y. Když použil test Y, hází mincí a přejde k testu Z, pokud padne líc. Pokud naposledy zadal test Z, tak hází dvěma mincemi a přejde k testu X, když na obou padne líc.

Modelujte zadávání testů pomocí Markovova procesu. Určete jeho matici a zdůvodněte, že je primitivní. Pomocí maticového násobení zjistěte, jaká je pravděpodobnost, že u třetího termínu zadá test X, jestliže u prvního zadal test Z. Za předpokladu, že tímto způsobem zadává testy hodně dlouho, zjistěte, který test zadává nejčastěji a s jakou pravděpodobností. Vysvětlete, jak jste k výsledku dospěli.

Řešení. Matice Markovovova procesu je

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

Spočteme-li $M^2 = M \cdot M$, dostaneme matici se všemi vstupy kladnými. Proto je M primitivní matice.

Pravděpodobnost, že profesor zadá u třetího termínu test X, když u prvního zadal test Z je dána první složkou součinu

$$M \cdot M \cdot \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}$$

a ta je $3/8$.

Při dlouhodobém zadávání se pravděpodobnosti zadání jednotlivých testů blíží pravděpodobnostnímu vektoru, který je vlastním vektorem matice M k vlastnímu číslu 1. Řešíme proto homogenní soustavu

$$(M - E)x = 0.$$

Její matici upravíme na schodovitý tvar

$$\begin{pmatrix} -1 & 1/2 & 1/4 \\ 1/2 & -1 & 3/4 \\ 1/2 & 1/2 & -1 \end{pmatrix} \sim \begin{pmatrix} 2 & -4 & 3 \\ 0 & -6 & 7 \\ 0 & 0 & 0 \end{pmatrix}.$$

Vlastní vektory jsou $a(5, 7, 6)$. Pravděpodobnostní vektor je

$$(5/18, 7/18, 6/18).$$

V dlouhodobém horizontu zadává profesor nejčastěji test Y, a to s pravděpodobností $7/18$.

□

Bodování. Správná matice **6 bodů**. (2 za každý sloupec) Zdůvodnění primitivnosti **2 body**.

Výpočet $3/8$ **2 body**.

Soustava pro vlastní vektor a její úprava na schodovitý tvar **5 bodů**. Správné řešení ve formě pravděpodobnostního vektoru **5 bodů**.

Správné určení otázky **2 body**, správná procenta **3 body**. □

Příklad. **4A.** V Rabinově kryptosystému je soukromým klíčem dvojice prvočísel $p = 7$, $q = 23$. Veřejným klíčem je $n = 161$. Dešifrujte zprávu $M = 116$. Proveďte celý výpočet bez použití kalkulačky nebo jakéhokoliv softwaru.

Stručně popište postup, kterým byste mohli provést kontrolu správnosti svého výpočtu.

Řešení. Dešifrovaná zpráva Z splňuje $Z^2 \equiv M \mod n$. Takové jsou 4 a jsou ve tvaru

$$Z \equiv \pm apQ \pm bqP \mod n,$$

kde a, b, P, Q jsou celá čísla splňující

(1) $ap + bq = 1$,
(2) $P \equiv M^{\frac{p+1}{4}} \mod p$,
(3) $Q \equiv M^{\frac{q+1}{4}} \mod q$.

Pomocí algoritmu spočítáme $a = 10$, $b = -3$. Dále počítáme modulo 7

$$116^2 \equiv 4^2 \equiv 16 \equiv 2 \mod 7.$$

Tedy $P = 2$.

Počítáním modulo 23

$$116^6 \equiv 1^6 \equiv 1 \mod 23.$$

Tedy $Q = 1$. Proto

$$Z \equiv \pm 10 \cdot 7 \cdot 1 \pm 3 \cdot 23 \cdot 2 = \pm 70 \pm 138.$$

Dešifrovaná zpráva je jedna z následujících: $47,\ 68,\ 93,\ 114$.

O správnosti výpočtu se můžeme přesvědčit tím, že ověříme platnost kongruencí

$$Z^2 \equiv 116 \equiv 4 \mod 7,$$
$$Z^2 \equiv 116 \equiv 1 \mod 23.$$

□

Bodování. Správný vzorec pro Z ... **6 bodů**.
Výpočet čísel a, b ... **3 body**.
Výpočet $P \equiv M^{\frac{p+1}{4}} \mod p$ ... **4 body**.
Výpočet $Q \equiv M^{\frac{q+1}{4}} \mod q$ ... **4 body**.
Správné hodnoty Z ... **4 body**.
Správná odpověď na otázku o ověření ... **4 body**. Samotné ověření není potřeba provádět.

□

Příklad. **4B.** V Rabinově kryptosystému je soukromým klíčem dvojice prvočísel $p = 7$, $q = 31$. Veřejným klíčem je $n = 217$. Dešifrujte zprávu $M = 78$. Proveďte celý výpočet bez použití kalkulačky nebo jakéhokoliv softwaru.

Stručně popište postup, kterým byste mohli provést kontrolu správnosti svého výpočtu.

Řešení. Dešifrovaná zpráva Z splňuje $Z^2 \equiv M \mod n$. Takové jsou 4 a jsou ve tvaru

$$Z \equiv \pm apQ \pm bqP \mod n,$$

kde a, b, P, Q jsou celá čísla splňující

(1) $ap + bq = 1$,
(2) $P \equiv M^{\frac{p+1}{4}} \mod p$,
(3) $Q \equiv M^{\frac{q+1}{4}} \mod q$.

Pomocí algoritmu spočítáme $a = 9$, $b = -2$. Dále počítáme modulo 7

$$78^2 \equiv 1^2 \equiv 1 \mod 7.$$

Tedy $P = 1$.

Počítáním modulo 31

$$78^8 \equiv 16^8 \equiv 2^{32} \equiv 2^{30} \cdot 4 \equiv 4 \mod 31$$

neboť podle malé Fermatovy věty je $2^{30} \equiv 1 \mod 31$. Tedy $Q = 4$. Proto

$$Z \equiv \pm 9 \cdot 7 \cdot 4 \pm 2 \cdot 31 \cdot 1 = \pm 252 \pm 62.$$

Dešifrovaná zpráva je jedna z následujících: $27,\ 97,\ 120,\ 190$.

O správnosti výpočtu se můžeme přesvědčit tím, že ověříme platnost kongruencí

$$Z^2 \equiv 78 \equiv 1 \mod 7,$$
$$Z^2 \equiv 78 \equiv 16 \mod 31.$$

□

Bodování. Správný vzorec pro Z ... **6 bodů**.

Výpočet čísel a, b ... **3 body**.

Výpočet $P \equiv M^{\frac{p+1}{4}} \mod p$ ... **2 body**.

Výpočet $Q \equiv M^{\frac{q+1}{4}} \mod q$ ... **6 bodů**.

Správné hodnoty Z ... **4 body**.

Správná odpověď na otázku o ověření ... **4 body**. Samotné ověření není potřeba provádět.

□

Příklad. **4C.** V Rabinově kryptosystému je soukromým klíčem dvojice prvočísel $p = 11$, $q = 19$. Veřejným klíčem je $n = 209$. Dešifrujte zprávu $M = 111$. Proveďte celý výpočet bez použití kalkulačky nebo jakéhokoliv softwaru.

Stručně popište postup, kterým byste mohli provést kontrolu správnosti svého výpočtu.

Řešení. Dešifrovaná zpráva Z splňuje $Z^2 \equiv M \mod n$. Takové jsou 4 a jsou ve tvaru

$$Z \equiv \pm apQ \pm bqP \mod n,$$

kde a, b, P, Q jsou celá čísla splňující

(1) $ap + bq = 1$,
(2) $P \equiv M^{\frac{p+1}{4}} \mod p$,
(3) $Q \equiv M^{\frac{q+1}{4}} \mod q$.

Pomocí algoritmu spočítáme $a = 7$, $b = -4$. Dále počítáme modulo 11

$$111^3 \equiv 1^3 \equiv 1 \mod 11.$$

Tedy $P = 1$.

Počítáním modulo 19

$$111^5 \equiv 16^5 \equiv -3^5 \equiv -9 \cdot 9 \cdot 3 \equiv -5 \cdot 3 \equiv 4 \mod 19.$$

Tedy $Q = 4$. Proto

$$Z \equiv \pm 7 \cdot 11 \cdot 4 \pm 4 \cdot 19 \cdot 1 = \pm 308 \pm 76.$$

Dešifrovaná zpráva je jedna z následujících: $23,\ 34,\ 175,\ 186$.

O správnosti výpočtu se můžeme přesvědčit tím, že ověříme platnost kongruencí

$$Z^2 \equiv 78 \equiv 1 \mod 7,$$
$$Z^2 \equiv 78 \equiv 16 \mod 31.$$

□

Bodování. Správný vzorec pro Z ... **6 bodů**.

Výpočet čísel a, b ... **3 body**.

Výpočet $P \equiv M^{\frac{p+1}{4}} \mod p$ ... **3 body**.

Výpočet $Q \equiv M^{\frac{q+1}{4}} \mod q$ ... **5 bodů**.

Správné hodnoty Z ... **4 body**.

Správná odpověď na otázku o ověření ... **4 body**. Samotné ověření není potřeba provádět.

□