MB141, zkouška 16. 6. 2020

Příklad. **1A.** V $\mathcal{A}_4$ jsou dány tři body body $A = [1, 2, 1, 2]$, $B = [2, 0, 1, 3]$, $C = [0, 1, -2, 4]$ a afinní podprostor $\mathcal{M}$ zadaný rovnicí

$$x_1 + x_2 - x_3 - x_4 = -1.$$

(a) Napište parametrickou rovnici roviny ρ, která je určena body A, B, C. [8 bodů]
(b) Napište obecný (implicitní) popis roviny ρ pomocí soustavy rovnic. [8 bodů]
(c) Spočítejte průnik $\rho \cap \mathcal{M}$. [9 bodů]

Řešení. **(a)** Parametrická rovnice roviny ρ je

$$A + a(B - A) + b(C - A) = [1, 2, 1, 2] + a(1, -2, 0, 1) + b(-1, -1, -3, 2).$$

(b) Nejdříve najdeme homogenní soustavu rovnic pro zaměření roviny ρ. Pro hledané koeficienty c_1, c_2, c_3, c_4 rovnic $c_1x_1 + c_2x_2 + c_3x_3 + c_4x_4 = 0$ musí platit soustava rovnic

$$c_1 - 2c_2 + c_4 = 0, \quad -c_1 - c_2 - 3c_3 + 2c_4 = 0$$

Její řešení je $s(1, 1, 0, 1) + t(2, 1, -1, 0)$. Homogenní rovnice jsou

$$x_1 + x_2 + x_4 = 0, \quad 2x_1 + x_2 - x_3 = 0.$$

Dosazením souřadnic bodu P do levých stran dostaneme soustavu rovnic pro π

$$x_1 + x_2 + x_4 = 5, \quad 2x_1 + x_2 - x_3 = 3.$$

(c) Průnik spočítáme řešením tří rovnic z obecných popisů afinních podprostorů. Matice soustavy je

$$\left(\begin{array}{cccc|c} 1 & 1 & -1 & -1 & -1 \\ 1 & 1 & 0 & 1 & 5 \\ 2 & 1 & -1 & 0 & 3 \end{array}\right) \sim \left(\begin{array}{cccc|c} 1 & 1 & 0 & 1 & 5 \\ 0 & -1 & 1 & 2 & 5 \\ 0 & 0 & 1 & 2 & 6 \end{array}\right)$$

Řešením je přímka $[4, 1, 6, 0] + p(-1, 0, -2, 1)$.

Lze také řešit dosazením parametrického vyjádření roviny ρ do rovnice pro $\mathcal{M}$.

Řešení, které hledá prvně parametrické vyjádření pro $\mathcal{M}$ a průnik hledá z parametrických vyjádření obou afinních podprostorů je nešikovné, zdlouhavé, a proto při něm dojde lehce k chybě. □

Bodování. Parametrické vyjádření roviny ρ za **8 bodů**.

Soustava rovnic pro ρ, správný postup **4 body**, výsledek **4 body**.

Vhodný postup výpočtu průniku **3 body**, řešení soustavy **3 body**, výsledek **3 body**. □

Příklad. **1B.** V $\mathcal{A}_4$ jsou dány tři body body $P = [2, 1, 1, 2]$, $Q = [0, 2, 1, 3]$, $R = [1, 0, -2, 4]$ a afinní podprostor $\mathcal{N}$ zadaný rovnicí

$$x_1 + x_2 - x_3 - x_4 = -1.$$

(a) Napište parametrickou rovnici roviny π, která je určena body P, Q, R. [8 bodů]
(b) Napište obecný (implicitní) popis roviny π pomocí soustavy rovnic. [8 bodů]
(c) Spočítejte průnik $\pi \cap \mathcal{N}$. [9 bodů]

Řešení. **(a)** Parametrická rovnice roviny π je

$$P + a(Q - P) + b(R - P) = [2, 1, 1, 2] + a(-2, 1, 0, 1) + b(-1, -1, -3, 2).$$

(b) Nejdříve najdeme homogenní soustavu rovnic pro zaměření roviny ρ. Pro hledané koeficienty c_1, c_2, c_3, c_4 rovnic $c_1x_1 + c_2x_2 + c_3x_3 + c_4x_4 = 0$ musí platit soustava rovnic

$$-2c_1 + c_2 + c_4 = 0, \quad -c_1 - c_2 - 3c_3 + 2c_4 = 0$$

Její řešení je $s(1, 1, 0, 1) + t(1, 2, -1, 0)$. Homogenní rovnice jsou

$$x_1 + x_2 + x_4 = 0, \quad x_1 + 2x_2 - x_3 = 0.$$

Dosazením souřadnic bodu P do levých stran dostaneme soustavu rovnic pro ρ

$$x_1 + x_2 + x_4 = 5, \quad x_1 + 2x_2 - x_3 = 3.$$

(c) Průnik spočítáme řešením tří rovnic z obecných popisů afinních podprostorů. Matice soustavy je

$$\left(\begin{array}{cccc|c} 1 & 1 & -1 & -1 & -1 \\ 1 & 1 & 0 & 1 & 5 \\ 1 & 2 & -1 & 0 & 3 \end{array}\right) \sim \left(\begin{array}{cccc|c} 1 & 1 & 0 & 1 & 5 \\ 0 & 1 & 0 & 1 & 4 \\ 0 & 0 & 1 & 2 & 6 \end{array}\right)$$

Řešením je přímka $[1, 4, 6, 0] + p(0, -1, -2, 1)$.

Lze také řešit dosazením parametrického vyjádření roviny π do rovnice pro $\mathcal{N}$.

Řešení, které hledá prvně parametrické vyjádření pro $\mathcal{N}$ a průnik hledá z parametrických vyjádření obou afinních podprostorů je nešikovné, zdlouhavé, a proto při něm dojde lehce k chybě. □

Bodování. Parametrické vyjádření roviny π za **8 bodů**.

Soustava rovnic pro π, správný postup **4 body**, výsledek **4 body**.

Vhodný postup výpočtu průniku **3 body**, řešení soustavy **3 body**, výsledek **3 body**. □

Příklad. **2A.** Zobrazení $\varphi : \mathbb{R}^3 \to \mathbb{R}^3$ je symetrie podle roviny $x_1 + x_2 + 2x_3 = 0$.

(a) Najděte matici A tak, aby ve standardních souřadnicích bylo

$$\varphi \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = A \cdot \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} \quad \text{[18 bodů]}.$$

(b) Je A ortogonální matice? Zdůvodněte svou odpověď. [3 body]

(c) Najděte inverzní matici A^{-1}. [4 body]

Řešení. **(a)** Symetrie podle roviny zobrazuje normálový vektor na opačný vektor a vektory z roviny na sebe. Normálový vektor je $n = (1, 1, 2)$, vektory v rovině jsou např. $u = (1, -1, 0)$ a $v = (0, 2, -1)$. Platí

$$\varphi(n) = -n, \quad \varphi(u) = u, \quad \varphi(v) = v.$$

Odtud již můžeme určit hodnoty zobrazení φ na vektorech e_1, e_2, e_3 standardní báze a tyto hodnoty tvoří sloupce hledané matice. Pro výpočet pišme vektory do řádků

$$\left(\begin{array}{ccc|ccc} & x & & & \varphi(x) & \\ 1 & 1 & 2 & -1 & -1 & -2 \\ 1 & -1 & 0 & 1 & -1 & 0 \\ 0 & 2 & -1 & 0 & 2 & -1 \end{array}\right) \sim \left(\begin{array}{ccc|ccc} & x & & & \varphi(x) & \\ 6 & 0 & 0 & 4 & -2 & -4 \\ 0 & 6 & 0 & -2 & 4 & -4 \\ 0 & 0 & 3 & -2 & -2 & -1 \end{array}\right)$$

Tedy matice

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

(b) Sloupce matice jsou na sebe kolmé a mají jednotkovou velikost. Proto je matice ortogonální.

(c) Protože je A ortogonální je $A^{-1} = A^T = A$. Jiné zdůvodnění spočívá v tom, že se spočítá součin $A \cdot A = E$. □

Bodování. **(a)** Obrazy tří vhodných vektorů **9 bodů**.

Spočítání hodnot na vektorech standardní báze **5 bodů**.

Správný výsledek **4 body**

(b) Zdůvodnění ortogonality **3 body**.

(c) Výpočet inverze **4 body**. □

Příklad. **2B.** Zobrazení $\psi : \mathbb{R}^3 \to \mathbb{R}^3$ je symetrie podle roviny $2x_1 - x_2 + x_3 = 0$.

(a) Najděte matici B tak, aby ve standardních souřadnicích bylo

$$\psi \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = B \cdot \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} \quad \text{[18 bodů]}.$$

(b) Je B ortogonální matice? Zdůvodněte svou odpověď. [3 body]

(c) Najděte inverzní matici B^{-1}. [4 body]

Řešení. **(a)** Symetrie podle roviny zobrazuje normálový vektor na opačný vektor a vektory z roviny na sebe. Normálový vektor je $n = (2, -1, 1)$, vektory v rovině jsou např. $u = (1, 2, 0)$ a $v = (0, 1, 1)$. Platí

$$\varphi(n) = -n, \quad \varphi(u) = u, \quad \varphi(v) = v.$$

Odtud již můžeme určit hodnoty zobrazení φ na vektorech e_1, e_2, e_3 standardní báze a tyto hodnoty tvoří sloupce hledané matice. Pro výpočet pišme vektory do řádků

$$\left(\begin{array}{ccc|ccc} & x & & & \varphi(x) & \\ 2 & -1 & 1 & -2 & 1 & -1 \\ 1 & 2 & 0 & 1 & 2 & 0 \\ 0 & 1 & 1 & 0 & 1 & 1 \end{array}\right) \sim \left(\begin{array}{ccc|ccc} & x & & & \varphi(x) & \\ 6 & 0 & 0 & -2 & 4 & -4 \\ 0 & 6 & 0 & 4 & 4 & 2 \\ 0 & 0 & 6 & -4 & 2 & 4 \end{array}\right)$$

Tedy matice

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

(b) Sloupce matice jsou na sebe kolmé a mají jednotkovou velikost. Proto je matice ortogonální.

(c) Protože je B ortogonální je $B^{-1} = B^T = B$. Jiné zdůvodnění spočívá v tom, že se spočítá součin $B \cdot B = E$. □

Bodování. **(a)** Obrazy tří vhodných vektorů **9 bodů**.

Spočítání hodnot na vektorech standardní báze **5 bodů**.

Správný výsledek **4 body**

(b) Zdůvodnění ortogonality **3 body**.

(c) Výpočet inverze **4 body**. □

Příklad. **2C.** Zobrazení $\omega : \mathbb{R}^3 \to \mathbb{R}^3$ je symetrie podle roviny $x_1 - 2x_2 + x_3 = 0$.

(a) Najděte matici C tak, aby ve standardních souřadnicích bylo

$$\omega \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = C \cdot \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} \quad \text{[18 bodů]}.$$

(b) Je C ortogonální matice? Zdůvodněte svou odpověď. [3 body]

(c) Najděte inverzní matici C^{-1}. [4 body]

Řešení. **(a)** Symetrie podle roviny zobrazuje normálový vektor na opačný vektor a vektory z roviny na sebe. Normálový vektor je $n = (1, -2, 1)$, vektory v rovině jsou např. $u = (1, 0, -1)$ a $v = (0, 1, 2)$. Platí

$$\varphi(n) = -n, \quad \varphi(u) = u, \quad \varphi(v) = v.$$

Odtud již můžeme určit hodnoty zobrazení φ na vektorech e_1, e_2, e_3 standardní báze a tyto hodnoty tvoří sloupce hledané matice. Pro výpočet pišme vektory do řádků

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

Tedy matice

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

(b) Sloupce matice jsou na sebe kolmé a mají jednotkovou velikost. Proto je matice ortogonální.

(c) Protože je C ortogonální je $C^{-1} = C^T = C$. Jiné zdůvodnění spočívá v tom, že se spočítá součin $C \cdot C = E$. □

Bodování. **(a)** Obrazy tří vhodných vektorů **9 bodů**.

Spočítání hodnot na vektorech standardní báze **5 bodů**.

Správný výsledek **4 body**

(b) Zdůvodnění ortogonality **3 body**.

(c) Výpočet inverze **4 body**. □

Příklad. **3A.** Model růstu nějaké populace určené třemi generacemi je dán Leslieho maticí s parametrem $a \in [0,1]$

$$A = \begin{pmatrix} 0 & \frac{5}{3} & \frac{1}{2} \\ \frac{1}{2} & 0 & 0 \\ 0 & a & 0 \end{pmatrix}.$$

(a) Jaká je úmrtnost 2. generace? [3 body]
(b) Jestliže je poměr prvé, druhé a třetí generace v čase 3 roven $1 : 6 : 2$ a parametr $a = 1/2$, jaký bude poměr těchto generací v čase 4? [3 body]
(c) Pro které hodnoty parametru a populace expanduje, pro které směřuje k vyhynutí a pro které se stabilizuje? [12 bodů]
(d) Určete dlouhodobé rozložení této populace pro parametr a, kdy se populace stabilizuje. [7 bodů]

Řešení. **(a)** Úmrtnost druhé generace je $1 - a$.

(b) Vynásobíme $A \cdot \begin{pmatrix} 1 \\ 6 \\ 2 \end{pmatrix} = \begin{pmatrix} 11 \\ 1/2 \\ 3 \end{pmatrix}$.

(c) Spočítáme charakteristický polynom

$$f(\lambda) = \det(A - \lambda E) = -\lambda^3 + \frac{5}{6}\lambda + \frac{1}{4}a.$$

Stabilita nastane, když 1 je vlastní číslo, tj.

$$f(1) = -1 + \frac{5}{6} + \frac{1}{4}a = 0.$$

Tedy pro $a = \frac{2}{3}$ je populace stabilní,

Pro $a \in (\frac{2}{3}, 1]$ je $f(1) > 0$, proto f má kořen > 1 a A má vlastní číslo > 1. Populace expanduje.

Pro $a \in [0, \frac{2}{3})$ je $f(1) < 0$, proto f má kořen < 1 a A má největší vlastní číslo < 1. Populace vymírá.

(d) Poměr generací je dán vlastním vektorem k vlastnímu číslu 1. Řešíme homogenní soustavu rovnic $(A - E)x = 0$. Vlastní vektor je $(6, 3, 2)^T$.

□

Bodování. **(a)** Úmrtnost **3 body**.

(b) Správný výpočet **3 body**. Bez výpočtu **0 bodů**.

(c) Charakteristický polynom **4 body**.
Kritická hodnota parametru **4 body**. Expanze **2 body**. Vymírání **2 body**

(d) Soustava pro vlastní vektor **3 body**.
Správný výsledek **4 body**.

□

Příklad. **3B.** Model růstu nějaké populace určené třemi generacemi je dán Leslieho maticí s parametrem $b \in [0,1]$

$$B = \begin{pmatrix} \frac{1}{2} & \frac{3}{2} & 1 \\ b & 0 & 0 \\ 0 & \frac{1}{2} & 0 \end{pmatrix}.$$

(a) Jaká je úmrtnost 1. generace? [3 body]
(b) Jestliže je poměr prvé, druhé a třetí generace v čase 4 roven $6:2:1$ a parametr $b = 1/3$, jaký bude poměr těchto generací v čase 5? [3 body]
(c) Pro které hodnoty parametru b populace expanduje, pro které směřuje k vyhynutí a pro které se stabilizuje? [12 bodů]
(d) Určete dlouhodobé rozložení této populace pro parametr b, kdy se populace stabilizuje. [7 bodů]

Řešení. **(a)** Úmrtnost první generace je $1 - b$.

(b) Vynásobíme $B \cdot \begin{pmatrix} 6 \\ 2 \\ 1 \end{pmatrix} = \begin{pmatrix} 7 \\ 2 \\ 1 \end{pmatrix}$.

(c) Spočítáme charakteristický polynom

$$f(\lambda) = \det(A - \lambda E) = \left(\frac{1}{2} - \lambda\right)\lambda^2 + \frac{3}{2}b\lambda + \frac{1}{2}b$$

Stabilita nastane, když 1 je vlastní číslo, tj.

$$f(1) = -\frac{1}{2} + \frac{3}{2}b + \frac{1}{2}b = 0.$$

Tedy pro $b = \frac{1}{4}$ je populace stabilní,

Pro $b \in (\frac{1}{4}, 1]$ je $f(1) > 0$, proto f má kořen > 1 a B má vlastní číslo > 1. Populace expanduje.

Pro $b \in [0, \frac{1}{4})$ je $f(1) < 0$, proto f má kořen < 1 a B má největší vlastní číslo < 1. Populace vymírá.

(d) Poměr generací je dán vlastním vektorem k vlastnímu číslu 1. Řešíme homogenní soustavu rovnic $(B - E)x = 0$. Vlastní vektor je $(8, 2, 1)^T$.

□

Bodování. **(a)** Úmrtnost **3 body**.

(b) Správný výpočet **3 body**. Bez výpočtu **0 bodů**.

(c) Charakteristický polynom **4 body**.
Kritická hodnota parametru **4 body**. Expanze **2 body**. Vymírání **2 body**

(d) Soustava pro vlastní vektor **3 body**.
Správný výsledek **4 body**.

□

Příklad. **3C.** Model růstu nějaké populace určené třemi generacemi je dán Leslieho maticí s parametrem $c \in [0, 1]$

$$C = \begin{pmatrix} \frac{1}{3} & \frac{9}{5} & 1 \\ \frac{1}{3} & 0 & 0 \\ 0 & c & 0 \end{pmatrix}.$$

(a) Jaká je úmrtnost 2. generace? [3 body]
(b) Jestliže je poměr prvé, druhé a třetí generace v čase 2 roven $3 : 5 : 4$ a parametr $c = 1/2$, jaký bude poměr těchto generací v čase 3? [3 body]
(c) Pro které hodnoty parametru c populace expanduje, pro které směřuje k vyhynutí a pro které se stabilizuje? [12 bodů]
(d) Určete dlouhodobé rozložení této populace pro parametr c, kdy se populace stabilizuje. [7 bodů]

Řešení. **(a)** Úmrtnost druhé generace je $1 - c$.

(b) Vynásobíme $C \cdot \begin{pmatrix} 3 \\ 4 \\ 5 \end{pmatrix} = \begin{pmatrix} 14 \\ 1 \\ 5/2 \end{pmatrix}$.

(c) Spočítáme charakteristický polynom

$$f(\lambda) = \det(A - \lambda E) = \left(\frac{1}{3} - \lambda\right)\lambda^2 + \frac{9}{15}\lambda + \frac{1}{3}c.$$

Stabilita nastane, když 1 je vlastní číslo, tj.

$$f(1) = -\frac{2}{3} + \frac{3}{5} + \frac{1}{3}c = 0.$$

Tedy pro $c = \frac{1}{5}$ je populace stabilní,

Pro $c \in (\frac{1}{5}, 1]$ je $f(1) > 0$, proto f má kořen > 1 a C má vlastní číslo > 1. Populace expanduje.

Pro $c \in [0, \frac{1}{5})$ je $f(1) < 0$, proto f má kořen < 1 a C má největší vlastní číslo < 1. Populace vymírá.

(d) Poměr generací je dán vlastním vektorem k vlastnímu číslu 1. Řešíme homogenní soustavu rovnic $(C - E)x = 0$. Vlastní vektor je $(15, 5, 1)^T$.

□

Bodování. **(a)** Úmrtnost **3 body**.

(b) Správný výpočet **3 body**. Bez výpočtu **0 bodů**.

(c) Charakteristický polynom **4 body**.
Kritická hodnota parametru **4 body**. Expanze **2 body**. Vymírání **2 body**

(d) Soustava pro vlastní vektor **3 body**.
Správný výsledek **4 body**.

□

Příklad. **4A.** Julie a Romeo komunikují šifrou Elgamal. Oba se dohodli na prvočísle $p = 19$ a na primitivním kořenu $g = 10$. Julie si za svůj tajný klíč zvolila číslo $a = 11$, Romeo má svůj tajný klíč b.

(a) Ověřte, že 10 je skutečně primitivní kořen modulo 19. [5 bodů]
(b) Jaký údaj poskytla Julie Romeovi? [5 bodů]
(c) Romeo posléze poslal Julii jako zprávu dvojici čísel $(g^b \equiv 7,\ 4)$. Pomozte Julii s dešifrováním zprávy. [15 bodů]

Proveďte celý výpočet bez použití kalkulačky nebo jakéhokoliv softwaru.

Řešení. **(a)** $\varphi(19) = 18 = 2 \cdot 3^2$. Proto $10^{18} \equiv 1 \mod 19$. Počítáme modulo 19

$$10^6 \equiv 100^3 \equiv 5^3 \equiv 6 \cdot 5 \equiv 11,$$
$$10^9 \equiv 10^6 \cdot 100 \cdot 10 \equiv 11 \cdot 5 \cdot 10 \equiv 11 \cdot 12 \equiv 8 \cdot 7 \equiv 18.$$

Tedy 10 je primitivní kořen.

(b) Julie poskytla údaj

$$g^a \equiv 10^{11} \equiv 10^9 \cdot 100 \equiv (-1) \cdot 5 \equiv 14, \mod 19.$$

(c) Romeo zašifroval zprávu M jako dvojici $(g^b, M(g^a)^b) = (7, 4)$. Proto dešifrujeme takto

$$M \equiv M(g^a)^b \cdot \left(g^b)^a\right)^{-1} \equiv 4 \cdot \left(7^{11}\right)^{-1} \equiv 4 \cdot (11)^{-1} \equiv 4 \cdot 7 \equiv 9 \mod 19.$$

Výpočet

$$7^{11} \equiv 49^5 \cdot 7 \equiv 11^5 \cdot 7 \equiv (-8)^5 \cdot 7 \equiv -64^2 \cdot 56 \equiv -7^2(-1) \equiv 11 \mod 19.$$

Inverze k $11 \mod 19$ se najde jako číslo a takové, že $11a + 19b = 1$ pro nějaké b. Jednoduše $(a, b) = (7, -4)$. Inverze je tedy 7.

□

Bodování. **(a)** Za $\varphi(19)$ a jeho rozklad **1 bod**. Za každou mocninu **2 body**.

(b) Ví, co má počítat **3 body**. Mocnina **2 body**.

(c) Správný vzorec **7 bodů**.
Mocnina **3 body**.
Inverze **3 body**.
Správný výsledek **2 body**. □

Příklad. **4B.** Desdemona a Othelo komunikují šifrou Elgamal. Oba se dohodli na prvočísle $p = 23$ a na primitivním kořenu $g = 10$. Desdemona si za svůj tajný klíč zvolila číslo $a = 9$, Othelo má svůj tajný klíč b.

(a) Ověřte, že 10 je skutečně primitivní kořen modulo 23. [5 bodů]
(b) Jaký údaj poskytla Desdemona Othelovi? [5 bodů]
(c) Othelo posléze poslal Desdemoně jako zprávu dvojici čísel $(g^b \equiv 2,\ 19)$. Pomozte Desdemoně s dešifrováním zprávy. [15 bodů]

Proveďte celý výpočet bez použití kalkulačky nebo jakéhokoliv softwaru.

Řešení. **(a)** $\varphi(23) = 22 = 2 \cdot 11$. Proto $10^{22} \equiv 1 \mod 23$. Počítáme modulo 23

$$10^2 \equiv 100 \equiv 8,$$
$$10^{11} \equiv 100^5 \cdot 10 \equiv 8^5 \cdot 10 \equiv 64^2 \cdot 80 \equiv 5^2 \cdot 11 \equiv 22.$$

Tedy 10 je primitivní kořen.

(b) Desdemona poskytla údaj

$$g^a \equiv 10^9 \equiv 100^4 \cdot 10 \equiv 8^4 \cdot 10 \equiv 5^2 \cdot 10 \equiv 20, \mod 23.$$

(c) Othelo zašifroval zprávu M jako dvojici $(g^b, M(g^a)^b) = (2, 19)$. Proto dešifrujeme takto

$$M \equiv M(g^a)^b \cdot \left(g^b)^a\right)^{-1} \equiv 19 \cdot \left(2^9\right)^{-1} \equiv 19 \cdot (6)^{-1} \equiv 19 \cdot 4 \equiv 7 \mod 23.$$

Výpočet

$$2^9 \equiv 16^2 \cdot 2 \equiv 7^2 \cdot 2 \equiv 3 \cdot 2 \equiv 6 \mod 23.$$

Inverze k $6 \mod 19$ se najde jako číslo a takové, že $6a + 23b = 1$ pro nějaké b. Jednoduše $(a, b) = (4, -1)$. Inverze je tedy 4.

□

Bodování. **(a)** Za $\varphi(19)$ a jeho rozklad **1 bod**. Za každou mocninu **2 body**.

(b) Ví, co má počítat **3 body**. Mocnina **2 body**.

(c) Správný vzorec **7 bodů**.
Mocnina **3 body**.
Inverze **3 body**.
Správný výsledek **2 body**. □