4. cvičení z MB141, jaro 2023

Příklad. 1. V šifrovacím systému RSA s veřejným klíčem skládajícím se z modulu $n = 2021$ a exponentu $e = 11$ došlo k prozrazení faktorizace $n = p \cdot q = 43 \cdot 47$. S její pomocí dešifrujte zprávu $c = 21$. Při výpočtu mocniny $c^d \mod 2021$ počítejte zvlášť modulo 43 a modulo 47 a tyto mezivýsledky pak dejte dohromady.

Řešení. $d = 527$, $c^d \equiv 11 \mod 43$, $c^d \equiv 34 \mod 47$, zpráva je 269. □

Příklad. 2. Najděte všechny primitivní kořeny modulo 26.

Řešení. $7, 11, 15, 19$. □

Příklad. 3a. Alice a Bob komunikují šífrou ElGamal. Oba se dohodli na prvočísle $p = 41$ a primitivním kořenu $g = 11$. Alice si zvolila soukromý klíč $x = 10$. Jaký údaj poskytla Bobovi? Bobův tajný klíč je y. Bob poslal Alici zprávu $(g^y = 22, c = 6)$. Pomozte Alici s dešifrováním?

Řešení. Při počítání $\mod 41$ je $g^x \equiv 11^{10} \equiv 9$, $g^{xy} \equiv (g^y)^x \equiv 22^{10} \equiv 32$, inverze k němu je 9, $m \equiv c \cdot 9 \equiv 6 \cdot 9 \equiv 13$. □

Příklad. 3b. V ElGamalově šifrovacím systému si Alice zvolila veřejný klíč sestávající z prvočísla $p = 997$, primitivního kořene $g = 11$ a jeho mocniny g^x (kde exponent $x = 23$ je soukromý). Bob si pro komunikaci s Alicí zvolil soukromý klíč $y = 25$ a poslal jí svůj veřejný klíč g^y. Pomocí společného soukromého klíče g^{xy} pak zašifroval zprávu m a výslednou zprávu $c = 20$ poslal Alici. Jak ji bude Alice dešifrovat?

Řešení. Při počítání $\mod 997$ je $g^x \equiv 11^{23} \equiv 659$, $g^y \equiv 11^{25} \equiv 976$, $g^{xy} \equiv (g^y)^x \equiv 976^{23} \equiv 950$, inverze k němu je -297, $m \equiv c \cdot (-297) \equiv 42$. □

Příklad. 4. Řešte soustavu rovnic s neznámými v $\mathbb{R}$

$$\begin{array}{rcrcrcrcrcr} x_1 & + & 2x_2 & + & x_3 & + & 3x_4 & + & 2x_5 & = & -8 \\ 2x_1 & + & x_2 & + & x_3 & + & x_4 & + & 3x_5 & = & 1 \\ x_1 & & & + & x_3 & - & x_4 & + & 2x_5 & = & 0 \\ x_1 & + & 2x_2 & + & 2x_3 & + & 2x_4 & + & 3x_5 & = & 0 \end{array}$$

Řešte stejnou soustavu v $\mathbb{Z}_{13}$, zbytkových třídách modulo 13.

Řešení. V $\mathbb{R}$ nemá řešení. V $\mathbb{Z}_{13}$ má více řešení. □

Příklad. 5. Řešte soustavu rovnic

$$\begin{array}{rcrcrcrcrcr} x_1 & + & 2x_2 & + & x_3 & - & x_4 & + & x_5 & = & 0 \\ 2x_1 & + & x_2 & + & 2x_3 & - & 2x_4 & + & 2x_5 & = & 0 \\ 2x_1 & & & + & x_3 & - & x_4 & + & 2x_5 & = & -1 \\ x_1 & + & x_2 & + & 2x_3 & - & 2x_4 & + & x_5 & = & 1 \end{array}$$

Řešení. $[-1, 0, 1, 0, 0] + s(0, 0, 1, 1, 0) + t(-1, 0, 0, 0, 1)$
http://www.math.muni.cz/ xfrancirekp/vyuka/seste_cviceni/sedme_cviceni.pdf □

Příklad. 6. Řešte soustavu rovnic

$$\begin{array}{rcrcrcrcr} 2x_1 & - & x_2 & + & x_3 & - & x_4 & = & 1 \\ 2x_1 & - & x_2 & & & - & 3x_4 & = & 2 \\ 3x_1 & & & - & x_3 & + & x_4 & = & -3 \\ 2x_1 & + & 2x_2 & - & 2x_3 & + & 5x_4 & = & -6 \end{array}$$

Příklad. 7. Zjistěte, zda jde matice násobit , a pokud ano, vynásobte je.

$$\begin{pmatrix} 3 & 5 & 6 & 7 \\ -2 & 1 & 0 & 5 \end{pmatrix} \cdot \begin{pmatrix} 2 & 8 \\ -1 & -5 \\ 9 & 11 \end{pmatrix}, \quad \begin{pmatrix} 2 & 8 \\ -1 & -5 \\ 9 & 11 \end{pmatrix} \cdot \begin{pmatrix} 3 & 5 & 6 & 7 \\ -2 & 1 & 0 & 5 \end{pmatrix},$$

$$\begin{pmatrix} 2 & 8 & 3 & 21 & 5 \end{pmatrix} \cdot \begin{pmatrix} 2 \\ -1 \\ 9 \\ -6 \\ 3 \end{pmatrix}, \quad \begin{pmatrix} 2 \\ -1 \\ 9 \\ -6 \\ 3 \end{pmatrix} \cdot \begin{pmatrix} 2 & 8 & 3 & 21 & 5 \end{pmatrix}$$

Příklad. 8. V rovině jsou dány body $A = [-3 + \sqrt{3}, -1 + 2\sqrt{3}]$, $B = [3, -4]$, vektor $\vec{v} = (6, 3)$ a přímka $p: \ y - 2x + 7 = 0$.

a) Určete parametrický a obecný popis přímky procházející body A a B.
b) Určete přímku r, která je rovnoběžná s pčímkou p a prochází bodem A.
c) Určete přímku q určenou bodem B a vektorem $\vec{v}$.
d) Spočítejte průsečík přímek q a r (pokud existuje).
e) Spočítejte obsah trojúhelníka ABC.
f) Rozhodněte, zda bod $O = [0, 0]$ leží uvnitř trojúhelníka ABC.
g) Určete, které strany trojúhelníka ABC jsou vidět z bodu $D = [-1, 4]$.
h) Spočtěte úhel při vrcholu B.

Řešení. http://www.math.muni.cz/ xfrancirekp/vyuka/seste_cviceni/seste_cviceni.pdf □