*příjmení:* **MA – závěrečný test – varianta X**

*jméno:* **22.1.2009**

*skupina:*

| | | | | |
|---|---|---|---|---|
| | | | | |

1. Určete, jaká $x$ jsou řešeními soustavy kongruencí

$$3\,x \equiv 2 \pmod 4,$$
$$2\,x \equiv 1 \pmod 3,$$
$$4\,x \equiv 1 \pmod 5.$$

   Nezapomeňte soustavu nejprve transformovat na tvar odpovídající definici Čínské věty o zbytcích. [7 bodů]

2. Polyalfabetická *Hillova šifra* je dána šifrovací transformací $\mathcal{C}(\mathbf{m}) \equiv \mathbf{A}\cdot\mathbf{m} \pmod n$ a dešifrovací transformací $\mathcal{D}(\mathbf{c}) \equiv \mathbf{A}^{-1}\cdot\mathbf{c} \pmod n$, přičemž musí existovat modulární inverze matice $\mathbf{A}^{-1}$ a musí tedy platit, že $\gcd(\det(\mathbf{A}), n) = 1$. V polyalfabetických šifrách zprávy šifrujeme a dešifrujeme po $k$ znacích, proto $\mathbf{A}$ je čtvercová matice $k \times k$ a $\mathbf{m}$ a $\mathbf{c}$ jsou sloupcové vektory délky $k$.

   Přiřadíme-li jednotlivým znakům anglické abecedy ($n = 27$) jejich numerické ekvivalenty podle následující tabulky,

| | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| A | B | C | D | E | F | G | H | I | J | K | L | M | N |
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 |
| O | P | Q | R | S | T | U | V | W | X | Y | Z | ⊔ | |
| 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 | |

   a zvolíme-li $\mathbf{A} = \begin{pmatrix} 3 & 1 \\ 5 & 4 \end{pmatrix}$, obdržíme po zakódování textu šifrovanou zprávu RDEJCH.

   Nalezněte matici $\mathbf{A}^{-1}$ [4 body] a znění původního textu [8 bodů].

   *Nápověda:* Pro inverzi matic $2 \times 2$ v modulární aritmetice modulo $n$ platí klasický vztah $\mathbf{A}^{-1} \equiv \det(\mathbf{A})^{-1} \cdot \begin{pmatrix} * & * \\ * & * \end{pmatrix} \pmod n$. Modulární inverze determinantu nahrazuje dělení, jež znáte z lineární algebry, znak $*$ pak permutaci a případnou změnu znaménka prvků původní matice $\mathbf{A}$.

3. Určete, pro jaká $n$ platí $15|n^8 + 14$ [3 body].

4. Napište algoritmus pro výpočet jednoho kroku, nakreslete vysvětlující obrázek a spočtěte prvních šest kroků *metody půlení intervalu* při vyšetřování kořenů funkce

$$y = f(x) = x^2 + 10\sin x.$$

   Kořen hledáme na intervalu $\langle -2{,}6; -2{,}4\rangle$ [8 bodů]

## Řešení

1. Nejprve je třeba převést násobitele $x$ z levé strany na pravou. Toho dosáhneme například použitím modulární inverze:

$$\begin{aligned}(3 \cdot 3)\, x &\equiv 3 \cdot 2 \pmod{4},\\ (2 \cdot 2)\, x &\equiv 2 \cdot 1 \pmod{3},\\ (4 \cdot 4)\, x &\equiv 4 \cdot 1 \pmod{5},\end{aligned}$$

a po úpravě

$$\begin{aligned}x &\equiv 2 \pmod{4},\\ x &\equiv 2 \pmod{3},\\ x &\equiv 4 \pmod{5}.\end{aligned}$$

► Tuto soustavu řešíme klasickým algoritmem

| $i$ | $a_i$ | $M_i$ | $N_i$ | $n_i$ |
|---|---|---|---|---|
| 1 | 2 | 3 | 15 | 4 |
| 2 | 2 | 2 | 20 | 3 |
| 3 | 4 | 3 | 12 | 5 |

Výsledná třída kongruence je pak dána modulem 60 a hodnotou

$$x = 2 \cdot 3 \cdot 15 + 2 \cdot 2 \cdot 20 + 4 \cdot 3 \cdot 12 = 90 + 80 + 144 = 314.$$

Výsledek je tedy

$$x \equiv 14 \pmod{60} \Leftrightarrow x = 14 + k \cdot 60.$$

► Alternativně

$$\begin{aligned}q_1 = 45 &\equiv 0 \pmod{3 \cdot 5} \quad \wedge \quad q_1 = 45 \equiv 1 \pmod{4},\\ q_2 = 40 &\equiv 0 \pmod{4 \cdot 5} \quad \wedge \quad q_2 = 40 \equiv 1 \pmod{3},\\ q_3 = 36 &\equiv 0 \pmod{4 \cdot 3} \quad \wedge \quad q_3 = 36 \equiv 1 \pmod{5}.\end{aligned}$$

Výsledná třída kongruence je pak dána modulem 60 a hodnotou

$$x = 2 \cdot 45 + 2 \cdot 40 + 4 \cdot 36 = 90 + 80 + 144 = 314.$$

Výsledek je tedy

$$x \equiv 14 \pmod{60} \Leftrightarrow x = 14 + k \cdot 60.$$

Bodování: 1 bod za převod do upravené formy, 3 body za tabulku nebo soustavu kongruencí $q_1$ až $q_3$, 2 body za výpočet do výsledku, 1 bod za to, že výsledek zapíšou v jedné ze dvou akceptovatelných forem znázorněných výše.

2. Dešifrovací transformace má tvar $\mathcal{D}(\mathbf{c}) \equiv \mathbf{A}^{-1}\mathbf{c} \pmod{n}$. Pro výpočet modulární inverze $\mathbf{A} = \begin{pmatrix} 3 & 1 \\ 5 & 4 \end{pmatrix}$ vztahem

$$\mathbf{A}^{-1} \equiv (\det \mathbf{A})^{-1} \begin{pmatrix} 4 & -1 \\ -5 & 3 \end{pmatrix} \pmod{n}$$

je třeba invertovat $\det \mathbf{A}$, jenž má v modulární reprezentaci tvar

$$\det \mathbf{A} = 7 \equiv 7 \pmod{27}$$

a platí

$$(\det \mathbf{A})^{-1} \equiv 7^{-1} \pmod{27} \equiv 4 \pmod{27}.$$

Je tedy $\mathbf{A}^{-1} \equiv \begin{pmatrix} 16 & 23 \\ 7 & 12 \end{pmatrix} \pmod{27}$.

Modulární inverzi $a^{-1} \cdot a \equiv 1 \pmod{n}$ je možné provést buď hrubou silou s vyhledáváním $a^{-1} \in \langle 1, n-1 \rangle$ tak, aby $a^{-1} \cdot a = k \cdot n + 1$, případně modulárním mocněním podle Eulerovy věty, jež pro nesoudělná $a$ a $n$ říká $a^{\Phi(n)} \equiv 1 \pmod{n}$ a tedy $a^{\Phi(n)-1} \equiv a^{-1} \pmod{n}$. Pro tuto šifru je $\Phi(27) = \Phi(3^3) = 3^2 \cdot (3-1) = 9 \cdot 2 = 18$.

| šifra | RD | EJ | CH |
|---|---|---|---|
| $c$ | 17 3 | 4 9 | 2 7 |
| $\mathbf{A}^{-1}\mathbf{c}$ | 341 155 | 271 136 | 193 98 |
| $\mathbf{A}^{-1}\mathbf{c} \pmod{27}$ | 17 20 | 1 1 | 4 17 |
| původní text | RU | BB | ER |

Bodování: 2 body za inverzi $\det \mathbf{A}$, 2 body za kompletní $\mathbf{A}^{-1}$, 8 bodů za celý text.

3. Je $n^18 + 14 \equiv 0 \pmod{15}$ a z toho $n^8 \equiv -14 \pmod{15} \equiv 1 \pmod{15}$ a pak Eulerovou větou $a^{\Phi(n)} \equiv 1 \pmod{n}$ pro nesoudělná $a$ a $n$, přičemž $\Phi(15) = (3-1)(5-1) = 8$.
   Bodování: za modulo, za Eulerovu větu, za výsledek.

4. Měli by mít napsáno, že

$$x_t = \frac{x_n + x_{n-1}}{2}$$

plus podmínky, za nichž $x_t$ přepíše levý respektive pravý okraj intervalu.

První šest iterací počínajících intervalem $\langle -2{,}6; -2{,}4 \rangle$ je

| iterace | $a$ | $b$ | $f(a)$ | $f(b)$ | $c$ | $f(c)$ |
|---|---|---|---|---|---|---|
| 1 | $-2{,}60000$ | $-2{,}40000$ | 1,60499 | $-0{,}99463$ | $-2{,}50000$ | 0,26528 |
| 2 | $-2{,}50000$ | $-2{,}40000$ | 0,26528 | $-0{,}99463$ | $-2{,}45000$ | $-0{,}37515$ |
| 3 | $-2{,}50000$ | $-2{,}45000$ | 0,26528 | $-0{,}37515$ | $-2{,}47500$ | $-0{,}05749$ |
| 4 | $-2{,}50000$ | $-2{,}47500$ | 0,26528 | $-0{,}05749$ | $-2{,}48750$ | 0,10326 |
| 5 | $-2{,}48750$ | $-2{,}47500$ | 0,10326 | $-0{,}05749$ | $-2{,}48125$ | 0,02273 |
| 6 | $-2{,}48125$ | $-2{,}47500$ | 0,02273 | $-0{,}05749$ | $-2{,}47813$ | $-0{,}01742$ |

Bodování: 5 bodů za kompletní výpočet, 2 body za popis a 1 za obrázek.