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

jméno: **26.1.2009**

skupina:

1. Určete, jaká x jsou řešeními soustavy kongruencí

$$2\,x \equiv 6 \pmod 7,$$
$$3\,x \equiv 1 \pmod 4,$$
$$2\,x \equiv 2 \pmod 3.$$

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

2. Tak zvaná *afinní šifra* je definována šifrovací transformací $\mathcal{C}(m) \equiv a \cdot m + b \pmod n$ a dešifrovací transformací $\mathcal{D}(c) \equiv a^{-1} \cdot (c - b) \pmod n$, přičemž musí existovat multiplikativní inverze a^{-1} a musí tedy platit, že $\gcd(a, n) = 1$. Zprávy šifrujeme a dešifrujeme po jednotlivých znacích.

   Přiřadíme-li jednotlivým znakům české abecedy ($n = 42$) jejich numerické ekvivalenty podle následující tabulky,

A	Á	B	C	Č	D	Ď	E	É	Ě	F	G	H	Ch	I	Í	J	K	L	M	N
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
Ň	O	Ó	P	Q	R	Ř	S	Š	T	Ť	U	Ú	Ů	V	W	X	Y	Ý	Z	Ž
21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41

   a zvolíme-li $a = 19$ a $b = 2$, obdržíme po zakódování textu šifrovanou zprávu ŘÉSŤA OQ ĎŤFTÉA, přičemž mezery se zachovávají.

   Jaké bylo znění původního textu? [9 bodů]

3. Obecně ukažte, jakou důležitou vlastnost má číslo, jež je součtem dvou po sobě následujících přirozených čísel [3 body].

4. Napište vzorec pro výpočet x_{n+1}, nakreslete vysvětlující obrázek a spočtěte prvních šest kroků *metody sečen* při vyšetřování kořenů funkce

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

   Kořen hledáme na intervalu $\langle -2{,}6; -2{,}4 \rangle$ [11 bodů]

Řešení

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

$$\begin{aligned}(4 \cdot 2)\, x &\equiv 4 \cdot 6 \pmod 7,\\ (3 \cdot 3)\, x &\equiv 3 \cdot 1 \pmod 4,\\ (2 \cdot 2)\, x &\equiv 2 \cdot 2 \pmod 3,\end{aligned}$$

a po úpravě

$$\begin{aligned}x &\equiv 3 \pmod 7,\\ x &\equiv 3 \pmod 4,\\ x &\equiv 1 \pmod 3.\end{aligned}$$

► Tuto soustavu řešíme klasickým algoritmem

i	a_i	M_i	N_i	n_i
1	3	3	12	7
2	3	1	21	4
3	1	1	28	3

Výsledná třída kongruence je pak dána modulem 84 a hodnotou

$$x = 3 \cdot 3 \cdot 12 + 3 \cdot 1 \cdot 21 + 1 \cdot 1 \cdot 28 = 108 + 63 + 28 = 199.$$

Výsledek je tedy

$$x \equiv 31 \pmod{84} \Leftrightarrow x = 31 + k \cdot 84.$$

► Alternativně

$$\begin{aligned}q_1 = 36 \equiv 0 \pmod{4 \cdot 3} \quad &\wedge \quad q_1 = 36 \equiv 1 \pmod 7,\\ q_2 = 21 \equiv 0 \pmod{7 \cdot 3} \quad &\wedge \quad q_2 = 21 \equiv 1 \pmod 4,\\ q_3 = 28 \equiv 0 \pmod{7 \cdot 4} \quad &\wedge \quad q_3 = 28 \equiv 1 \pmod 3.\end{aligned}$$

Výsledná třída kongruence je pak dána modulem 84 a hodnotou

$$x = 3 \cdot 36 + 3 \cdot 21 + 1 \cdot 28 = 108 + 63 + 28 = 199.$$

Výsledek je tedy

$$x \equiv 31 \pmod{84} \Leftrightarrow x = 31 + k \cdot 84.$$

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. Pro $a = 19$ a $b = 2$ je dešifrovací transformace $\mathcal{D}(c) \equiv 19^{-1}(c - 2) \pmod{42}$ a platí $19^{-1} \equiv 31 \pmod{42}$. Je tedy $\mathcal{D}(c) \equiv 31 \cdot (c - 2) \pmod{42}$.

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 $\Phi(42) = \Phi(2 \cdot 3 \cdot 7) = (2-1) \cdot (3-1) \cdot (13-1) = 12$.

šifra	Ř	É	S	Ť	A		O	Q		Ď	Ť	F	T	É	A
c	27	8	28	31	0		22	25		6	31	10	30	8	0
$(c-2) \pmod{42}$	25	6	26	29	40		20	23		4	29	8	28	6	40
$31 \cdot (c-2) \pmod{42}$	19	18	8	17	22		32	41		40	17	38	28	18	22
původní text	M	L	É	K	O		U	Ž		Z	K	Y	S	L	O

Bodování: 2 body za inverzi a, 7 bodů za dešifrovaný text.

3. Je to liché číslo, protože $n = k + (k+1) = 2k + 1$.
Bodování: Bod za výrok, dva za zápis.

4. Vzorec, který asi bude nejčastější, je

$$x_{n+1} = x_n - \frac{x_n - x_{n-1}}{f(x_n) - f(x_{n-1})} \cdot f(x_n)$$

případně si ti chytřejší pamatují

$$x_{n+1} = x_n + \frac{s_n}{1 - s_n} \cdot (x_n - x_{n-1}), \quad s_n = \frac{f(x_n)}{f(x_n)}.$$

Za použití

$$x_{n+1} = \frac{x_{n-1} f(x_n) - x_n f(x_{n-1})}{f(x_n) - f(x_{n-1})} \cdot f(x_n)$$

dávám jednobodovou penalizaci, protože ten vzorec je pro výpočet nevhodný a říkal jsem jim to.

Prvních 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	−2,47652	−0,03799
2	−2,47652	−2,60000	−0,03799	1,60499	−2,47938	−0,00135
3	−2,47938	−2,47652	−0,00135	−0,03799	−2,47948	0,00000
4	−2,47948	−2,47938	0,00000	−0,00135	−2,47948	−0,00000
5	−2,47948	−2,47948	−0,00000	0,00000	−2,47948	−0,00000
6	−2,47948	−2,47948	−0,00000	−0,00000	−2,47948	−0,00000

Bodování: 8 bodů za kompletní výpočet, 2 body za vzorec a 1 za obrázek.