Úloha 209.

Pokyny pro vypracování

Domácí úlohu je nutno odevzdat do 7.5.2010 do 12:00. Úlohy odevzdané později nebudou uznány. Úlohy odevzdejte elektronicky ve formátu *pdf* nebo na nelinkovaném/nečtverečkovaném papíru formátu A4 jako vysázený dokument (tj. ne psané rukou). Na první straně řešení musí být zadání a výsledky, na dalších stranách postup řešení.

Úlohy odevzdané po termínu nebo v jiném elektronickém formátu či na jiném než původně bílém nepotištěném papíře formátu A4 nebudou přijaty. Odevzdáním do termínu se považuje buďto úspěšné odeslání e-mailu včetně přílohy do určeného termínu nebo osobní předání vytištěného textu cvičícímu do určeného termínu.

Úlohu vypracujte pečlivě, každá numerická chyba je podstatná. Pro snížení chyb vzniklých chybným opsáním je na stránkách cvičícího textový soubor *uloha_209.txt* se zadáním úlohy, kde *209* je číslo úlohy.

Přijímáme pouze správně vypracované úlohy.

- První úloha má jednoduchý test správnosti
- U druhé úlohy také existuje jednoduchý test správnosti.
- Řešením třetí úlohy je smysluplný text v nějakém jazyce, který nepoužívá nabodeníčka (háčky, čárky, ...). Neuvádějte výsledný text do uvozovek. Uvozovky a jakékoliv jiné speciální znaky pište pouze, jsou-li součástí řešení.

První příklad je aplikací čínské věty o zbytcích.

Druhý příklad, tzv. Hillova šifra, vezme zdrojový text, převede ho na posloupnost číselných vektorů a každý člen této posloupnosti zleva vynásobí šifrovacím klíčem. Chceme-li zašifrovat v $\mathbf{Z}_{30}$ zprávu "AHOJ" Hillovou šifrou s klíčem

$$\begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix},$$

nejprve převedeme "AHOJ" na posloupnost vektorů (použité kódování viz. příklad 2)

$$\begin{pmatrix} 1 \\ 8 \end{pmatrix} \qquad \begin{pmatrix} 15 \\ 10 \end{pmatrix},$$

a poté zleva vynásobíme šifrovacím klíčem

$$\begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} \cdot \begin{pmatrix} 1 \\ 8 \end{pmatrix} = \begin{pmatrix} 9 \\ 17 \end{pmatrix} \qquad \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} \cdot \begin{pmatrix} 15 \\ 10 \end{pmatrix} = \begin{pmatrix} 25 \\ 5 \end{pmatrix}$$

Třetí příklad se velikostí generovaných prvočísel přibližuje velikosti používané v kryptografických aplikacích současnosti. Jednou ze slabin v příkladě použitého RSA protokolu je blízkost vygenerovaných prvočísel. Z důvodu velikosti použitých čísel je použit nestandardní zápis čísel. Číslo nekončí koncem řádku, či uzavírací závorkou, ale konec čísla je určen černým puntíkem. Například zpráva

$$\begin{pmatrix} 1234 & \\ 12 & \bullet \\ 17 & \\ 8568 & \\ 608 & \\ 1 & \bullet \\ 314159 & \bullet \end{pmatrix}$$

sestává ze tří částí: první 123412, druhá 1785686081 a nakonec třetí 314159. Ještě si ukážeme převod číselné zprávy na textovou. Spočítáme zbytkovou třídu čísla 1785686081 po dělení 256 a dostaneme $65 \equiv 1785686081 \bmod 256$. Na pozici 65 se v ASCII tabulce nachází písmeno 'A'. Číslo 1785686081 celočíselně dělíme 256 a celou proceduru si zopakujeme: $6975336 = 1785686081/256$, spočítáme zbytkovou třídu $104 \equiv 6975336 \bmod 256$. Na této pozici leží písmeno 'h'. Dále pokračujeme obdobně až do nuly. Výsledné dekódované slovo je 'Ahoj'.

Úloha 209.

▸ **Příklad 209.1**
Nalezněte páté nejmenší nezáporné řešení soustavy:

$$\begin{array}{rcrcr} x & \equiv & 57 & \mathrm{mod} & 61 \\ x & \equiv & 2 & \mathrm{mod} & 49 \\ x & \equiv & 39 & \mathrm{mod} & 41 \\ x & \equiv & 8 & \mathrm{mod} & 39 \\ x & \equiv & 24 & \mathrm{mod} & 38 \end{array}$$

Nalezené řešení uvažujte jako 10-ti místné a výsledek rozdělte na posloupnost dvouciferných čísel. Tato čísla označte po řadě $c_0, ..., c_4$. Např. jestliže je počet rovnic 5 a jejich řešení je $x = 1234567890$, potom $c_0 = 12$, $c_1 = 34$, $c_2 = 56$, $c_3 = 78$, $c_4 = 90$, Jestliže $x = 123$ (stále předpokládáme 5 rovnic), potom za x vezmeme číslo $x = 0000000123$ a dostáváme posloupnost $c_0 = 00$, $c_1 = 00$, $c_2 = 00$, $c_3 = 01$, $c_4 = 23$.

▸ **Příklad 209.2**
Pracujte v $\mathbf{Z}_{38}$ a dešifrujte zprávu

$$(4, 3, 9, 5, 5)$$

víte-li, že byla použita Hillova šifra s šifrovacím klíčem

$$\begin{pmatrix} 23 & 37 & c_0 & 20 & 37 \\ c_1 & 3 & 22 & 14 & 24 \\ 30 & 22 & 16 & 37 & c_2 \\ 23 & c_3 & 4 & 3 & 15 \\ 5 & 20 & 35 & c_4 & 19 \end{pmatrix}$$

kde $c_0, ..., c_4$ jsou hodnoty získané z předešlé úlohy. Dešifrovanou zprávu převeďte na text za použití kódování:

$$\begin{array}{ccc} A \mapsto 01 & B \mapsto 02 & C \mapsto 03 \\ & \vdots & \\ \ldots & Z \mapsto 26 & \end{array}$$

Dále dešifrujte zprávu

$$(10, 3, 1, 20, 5)$$

Zpráva byla zašifrována stejnou metodou jako v předchozím případě. Výslednou zprávu nepřevádějte na text, ale označte její hodnoty po řadě $r_0, ..., r_4$. Tyto hodnoty použijete v následující úloze.

▸ **Příklad 209.3**
Dešifrujte zprávu

$$\begin{pmatrix} 59895979813927177746967515458370703674904862688299943711385748532385 79 \\ 28752301236475950575265078980196524004879305850245232315418973577778 51 \\ 27690495625505941643996955084412437156328790378739038694065 9 \bullet \end{pmatrix}$$

víte-li, že byla použita RSA šifra s šifrovacím klíčem

$$(n, e) = \begin{pmatrix} 846035240390623252r_0 2425975695866504839851604689421431 09r_1 71031367804 \\ 23971170401758927r_2 1786449137069965032760728665279410752065231741248450 1 \\ 7202947767074944r_3 963507478095108r_4 4542956436928486362802195508 9 \bullet \\ 1632791988377000748475174684437977532367097307016210424846049528041115 \\ 257776462404103021141134828851 \bullet \end{pmatrix}$$

kde $r_0, ..., r_4$ jsou hodnoty získané z předešlé úlohy. Dešifrovanou zprávu převeďte na text. Bylo použito ASCII kódování.