Matematika pro informatiky

(akademický rok 2016/17)

Předmět je zakončen zkouškou, které musí předcházet získání zápočtu. Podmínky pro získání zápočtu i zkoušky jsou uvedeny níže.

Zápočet

- Student vypracuje zápočtový test – zadání viz níže. Řešení úloh musí být správné a dostatečně podrobně komentované. Formální stránka zpracování musí odpovídat studentu VŠ, obor informatika.
- Vyřešené úlohy je třeba zaslat elektronickou poštou na univerzitní adresu přednášejícího ve formě souboru (v některém z formátů - doc, docx, rtf, pdf), a to nejpozději tři pracovní dny před koncem ZS akademického roku 2016/17.
- O výsledku zápočtu bude student informován mailem nejpozději do tří pracovních dnů od doručení řešení zápočtových úloh.

Zkouška

- Student s platným zápočtem se hlásí na zkoušku prostřednictvím systému stag. Zkušební termíny budou uveřejněny ve stagu nejpozději v zápočtovém týdnu ZS 2016/17.
- Zkouška má písemnou a ústní část. K ústní části postoupí pouze student, který uspěl v písemné části (tj. získá alespoň 70 % bodů z celkového možného počtu).

10. října 2016

doc. RNDr. Miroslav Koucký, CSc.
přednášející

Zápočtové příklady 2016/17

(1) Převody mezi číselnými soustavami

- Proveďte následující převody mezi uvedenými číselnými soustavami

  $(120301)_4 = (\quad)_8$ $(120350)_7 = (\quad)_{13}$ $(32010)_9 = (\quad)_5$

  $(FGH0I)_{19} = (\quad)_{12}$ $(3F0A)_{16} = (\quad)_4$ $(607010)_{10} = (\quad)_5$

(2) Kanonický rozklad, NSD, NSN, počet dělitelů

- Uvažujte $a = 270\,030\,618, b = 479\,000\,925, c = 418\,906\,566$. Pomocí kanonických rozkladů nalezněte: a) $NSD(a,b,c)$, b) počet všech společných dělitelů čísel a, b, c.
- Uvažujte $a = 26\,087\,600, b = 5\,005\,000, c = 5\,236\,000$. Použijte Eukleidův algoritmus a určete $NSD(a,b,c)$.

(3) Řešení diofantické rovnice $ax + by = c$

- Nalezněte všechna celočíselná řešení rovnice $236x + 292y = 44$.

(4) Řešení kongruencí 1. stupně

- Vyřešte kongruenci $508x + 124 \equiv 0\ (mod\ 668)$. Výsledek zapište v soustavě nejmenších nezáporných zbytků zadaného modulu.

(5) Zobecněná čínská věta o zbytku

- Vyřešte následující soustavu kongruencí $4x \equiv 3\ (15), 8x \equiv 3\ (9), 3x \equiv 1\ (10), 5x \equiv 7\ (8)$. Výsledek zapište v soustavě nejmenších nezáporných zbytků odpovídajícího modulu.

(6) Počítání s polynomy v $Z_5[x]$, $Z_7[x]/q[x]$

- Nechť $f(x), g(x) \in Z_5[x]$, kde $f(x) = 2x^6 + 2x^5 + 2x^4 + x^3 + 2x + 1$ a $g(x) = 3x^5 + x^3 + 3x^2 + x + 2$. a) Pomocí Eukleidova algoritmu spočtěte $NSD\big(f(x), g(x)\big)$. b) Polynomy $f(x)$ a $g(x)$ rozložte na součin ireducibilních polynomů. Při zápisu výsledků vždy používejte soustavu nejmenších nezáporných zbytků.
- Nechť $f(x), g(x) \in Z_7[x]/(5x^4 + 3x^2 + x + 2)$, kde $f(x) = 4x^3 + 2x + 5$ a $g(x) = 3x^2 + 6x + 2$. Spočtěte $g(x) \cdot f^2(x)$. Při zápisu výsledků používejte soustavu nejmenších nezáporných zbytků.

(7) Jednoduchá transpozice, afinní šifra

- Uvažujte šifrování, které probíhá následovně - nejprve je otevřený text zašifrován jednoduchou transpozicí s klíčem $\rho \cdot \tau$, následně afinní šifrou s klíčem $(a, b) = (7,6)$ a na závěr opět jednoduchou transpozicí s klíčem $\rho^{-1} \cdot \tau^{-1}$, kde $\rho = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 6 & 5 & 1 & 4 & 3 \end{pmatrix}$ a $\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 4 & 5 & 6 & 1 & 2 \end{pmatrix}$. a) Zašifrujte text "fastus", b) dešifrujte text "QCTMBQ".

(8) Vigenerova šífra

- Použijte Vigenerův čtverec a klíčové slovo "crus". Zašifrujte text "velamentum" a dešifrujte text "UZHYWCUJKJ".

(9) Hillova šifra (3 x 3)

- Dešifrujte text "RWZPCZ", který vzniknul zašifrováním pomocí Hillovy matice $(H^{-1} \cdot G)$, kde $H = \begin{pmatrix} 13 & 12 & 21 \\ 22 & 15 & 7 \\ 21 & 3 & 1 \end{pmatrix}$ a $G = \begin{pmatrix} 13 & 2 & 6 \\ 2 & 1 & 6 \\ 1 & 1 & 1 \end{pmatrix}$.

(10) Dvoustupňový Feistel

- Uvažujte dvoustupňovou Feistel šifru s šifrovacími funkcemi

$$f_1(x_1, x_2, x_3, x_4) = (x_1 \oplus 1, x_2 + x_3, x_1 \cdot x_3, x_2 \oplus x_4),$$
$$f_2(x_1, x_2, x_3, x_4) = (\overline{x_1}, \overline{x_2 \cdot x_3}, x_1 + x_3, x_1 \oplus x_4),$$

kde $\oplus$ je exkluzivní disjunkce, $\cdot$ je konjunkce, $+$ je disjunkce a $\overline{\ }$ je negace. Zašifrujte text "ex" reprezentovaný ASCII kódem.

(11) Huffmanova konstrukce (binární varianta)

- Uvažujte zdrojovou abecedu

$$S = \begin{matrix} s_1 & s_2 & s_3 & s_4 & s_5 & s_6 & s_7 & s_8 & s_9 & s_{10} \\ 9/33 & 6/33 & 5/33 & 3/33 & 3/33 & 2/33 & 2/33 & 1/33 & 1/33 & 1/33 \end{matrix}.$$

  Nalezněte nejkratší kód dané abecedy a spočtěte střední délku kódového slova.

- Uvažujte zdrojovou abecedu

$$S = \begin{matrix} s_1 & s_2 & s_3 & s_4 & s_5 & s_6 \\ 0{,}17 & 0{,}09 & 0{,}50 & 0{,}05 & 0{,}13 & 0{,}06 \end{matrix}.$$

  Nalezněte nejkratší kód dané abecedy a spočtěte střední délku kódového slova.

(12) Aritmetické kódy (metoda DFWLD), dyadické zlomky

- Určete: a) dyadický rozvoj čísla $\frac{7}{8}$,
  b) racionální číslo reprezentované dyadickým rozvojem $101.011\overline{01}$, kde pruh označuje periodické opakování.

- Uvažujte zdrojovou abecedu $\begin{matrix} znak \\ pst. \end{matrix} \Big| \begin{matrix} a_1 & a_2 & a_3 & a_4 & a_5 & a_6 \\ 0{,}3 & 0{,}2 & 0{,}2 & 0{,}15 & 0{,}1 & 0{,}05 \end{matrix}$. Pomocí metody DFWLD zakódujte slovo $a_2 a_1 a_2 a_3$.