

## Zápočtové příklady 2018/19

### (1) Číselné soustavy

- Uvedená čísla seřadte nerostoucím způsobem:

$$(b8ea)_{15}; (1001000100110000)_2; (14b01)_{13}; (1212222102)_3; (216202)_7$$

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

- Nechť  $a = 117\,204\,711$ ,  $b = 15\,923\,349$ ,  $c = 2\,880\,267$ . Pomocí kanonických rozkladů nalezněte: a)  $NSD(a, b, c)$ , b) vypište všechny společné dělitele čísel  $a, b, c$  seřazené vzestupně, c)  $\varphi(NSD(a, c))$
- Nechť  $a = 42\,237$ ,  $b = 305\,045$ ,  $c = 183\,027$ . Využijte Eukleidův algoritmus a určete  $NSD(a, b, c)$ .
- Největšího společného dělitele čísel  $a = 3\,420$ ,  $b = 4\,698$  vyjádřete ve tvaru Bezoutovy rovnosti.

### (3) Řetězové zlomky

- Pro  $\alpha = \frac{5321}{3400}$  sestavte tabulku přibližných zlomků a následně sestavte tabulku přibližných zlomků pro  $\alpha^{-1}$ .

### (4) Řešení diofantické rovnice $ax + by = c$

- Nalezněte všechna celočíselná řešení rovnice  $66x - 21y = -33$ . Dále nalezněte takové celočíselné řešení, pro které platí  $|x - y| = 113$ .

### (5) Řešení kongruencí 1. stupně

- Vyřešte kongruenci  $768x \equiv -1240 \pmod{412}$ . Výsledek zapište v soustavě nejmenších nezáporných zbytků zadaného modulu. Dále nalezněte nejmenší celé číslo větší než záporný trojnásobek modulu, které vyhovuje zadané kongruenci.

### (6) Zobecněná čínská věta o zbytku

- Vyřešte následující soustavu kongruencí  $x \equiv 6 \pmod{12}$ ,  $x \equiv 2 \pmod{14}$ ,  $x \equiv 3 \pmod{15}$ ,  $x \equiv 9 \pmod{21}$ . Výsledek zapište v soustavě nejmenších nezáporných zbytků odpovídajícího modulu.
- Vyřešte následující soustavu kongruencí  $x \equiv 3 \pmod{15}$ ,  $x \equiv 6 \pmod{9}$ ,  $x \equiv 14 \pmod{70}$ ,  $x \equiv 7 \pmod{8}$ . Výsledek zapište v soustavě nejmenších nezáporných zbytků odpovídajícího modulu.

### (7) Počítání s polynomy

- Nechť  $f(x), g(x) \in \mathbb{Z}_7[x]$ , kde  $f(x) = 4x^6 + 6x^5 + 6x^4 + 4x^3 + 4x^2 + 3$  a  $g(x) = 5x^6 + x^5 + 4x^3 + 2x^2 + 3x + 1$ . a) Pomocí Eukleidova algoritmu spočítejte  $NSD(f(x), g(x))$ . Výsledek zapište ve tvaru monického polynomu (tj. polynomu s vedoucím koeficientem rovným 1). b) Polynomy  $f(x)$  a  $g(x)$  rozložte na součin monických ireducibilních polynomů. Při zápisu výsledků vždy používejte soustavu nejmenších nezáporných zbytků.
- Nechť  $f(x), g(x) \in \mathbb{Z}_5[x] / (x^5 + 3x^3 + 2x + 2)$ , kde  $f(x) = 3x^4 + 2x^3 + x + 4$ ,  $g(x) = 4x^3 + 3x^2 + 2x + 1$ . Spočítejte  $g(x) \cdot f(x)$ . Při zápisu výsledků používejte soustavu nejmenších nezáporných zbytků.

### (8) Počítání s permutacemi

- Permutace  $\pi, \rho, \sigma \in S_6$ , kde  $\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 5 & 2 & 4 & 6 & 1 \end{pmatrix}$ ;  $\rho = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 4 & 5 & 6 & 1 & 2 \end{pmatrix}$ ;  $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 6 & 5 & 1 & 4 & 3 \end{pmatrix}$ , zapište ve tvaru součinu disjunktních cyklů.
- Uvažujte permutace  $\pi, \rho, \sigma \in S_7$ , kde  $\pi = (35712)(465)(632)$ ,  $\rho = (6247135)(6157243)$ ,  $\sigma = (2451)(376)$ .
  - a) Zapište  $\pi, \rho$  ve tvaru součinu disjunktních cyklů a  $\sigma$  ve tvaru součinu transpozic.
  - b) Zapište  $\pi, \rho, \sigma$  v tzv. dvouřádkovém tvaru.
- Uvažujte permutace  $\pi, \rho, \sigma \in S_7$ , kde  $\pi = (1524)(437)(13642)$ ,  $\rho = (3761)(24536)(2751)$ ,  $\sigma = (7653214)$ .
  - a) Spočtete  $(\pi \cdot \rho^{-1})^{-1}$ .
  - b) Určete  $x \in S_7$  tak, aby platilo  $(\pi^{-1} \cdot \sigma \cdot x)^{-1} \cdot \pi^{-1} = \sigma \cdot \pi$ . Výsledky uvádějte vždy ve tvaru součinu disjunktních cyklů.

### (9) Hillova šifra (3 x 3)

- Uvažujte Hillovu šifru s šifrovací maticí  $H = \begin{pmatrix} 10 & 19 & 21 \\ 17 & 20 & 23 \\ 25 & 9 & 11 \end{pmatrix}$ . a) Zašifrujte text: turdus. b) Dešifrujte text: "GGQATP".
- Uvažujte Hillovu šifru s šifrovacími maticemi  $H_i$  ( $i = 1, 2, 3$ ). Nalezněte dešifrovací matice  $H_i^{-1} \pmod{26}$ .
  - a)  $H_1 = \begin{pmatrix} 22 & 15 & 21 \\ 13 & 12 & 7 \\ 16 & 6 & 19 \end{pmatrix}$ ;
  - b)  $H_2 = \begin{pmatrix} 12 & 13 & 7 \\ 16 & 6 & 19 \\ 15 & 22 & 21 \end{pmatrix}$ ;
  - c)  $H_3 = \begin{pmatrix} 21 & 13 & 15 \\ 13 & 3 & 16 \\ 7 & 22 & 12 \end{pmatrix}$

### (10) Huffmanova konstrukce (binární varianta)

- Uvažujte zdrojovou abecedu  $S = a \quad b \quad c \quad d \quad e \quad f \quad g \quad h \quad i$ .  
3/40 1/24 1/6 1/30 31/120 1/24 5/24 1/20 1/8  
Nalezněte nejkratší kód dané abecedy a spočtete střední délku kódového slova.

### (11) Aritmetické kódy (metoda DFWLD), dyadické zlomky

- Určete:
  - a) dyadický rozvoj čísla  $21 \frac{37}{128}$ ,
  - b) racionální číslo reprezentované dyadickým rozvojem  $(11010.01101111)_2$ .
- Uvažujte zdrojovou abecedu 

znak	$a_1$	$a_2$	$a_3$	$a_4$	$a_5$	$a_6$
pst.	0,25	0,2	0,2	0,15	0,15	0,05

. Pomocí metody DFWLD zakódujte slovo  $a_3 a_1 a_3 a_2$ .