Název předmětu: **Matematika pro informatiky**

(platné pro ak. rok 2019/20)

Zkratka předmětu: **MIE**

Počet kreditů: 5 Forma studia: kombinovaná

Způsob zakončení: zkouška (písemná a ústní část)

Anotace:
Předmět seznamuje se základy dělitelnosti, vybranými partiemi algebry, šifrování a kódování.

Doporučená literatura:
Koucký, M.: Matematika pro informatiky I. + II. Skripta TUL, 2017.

Zápočet

- Student vypracuje zápočtový test – zadání viz níže. Řešení úloh musí být správné a dostatečně podrobně okomentované. Formální stránka zpracování musí odpovídat studentu VŠ, obor informatika.
- Vyřešené úlohy je třeba zaslat elektronickou poštou na univerzitní adresu přednášejícího ve formě jednoho souboru (v některém z formátů - doc, docx, rtf, pdf; velikost max. 4 MB), a to nejpozději do konce zkouškového období ZS ak. roku 2019/20.
- O výsledku zápočtu bude student informován mailem do čtyř 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 ak. roku 2019/20.
- 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).

15. listopadu 2019

doc. RNDr. Miroslav Koucký, CSc.
garant, přednášející

Matematika pro informatiky

Předpokládané znalosti

- Základy maticového počtu (počítání s maticemi nad Z_p, výpočet inverze, Gaussova eliminace).

Obsah samostudia

Úvod do teorie dělitelnosti

- Relace „býti dělitelem“, vlastnosti, věta o dělení se zbytkem (číselná soustava o základu b, převody mezi číselnými soustavami), Eukleidův algoritmus;
- Společný dělitel, NSD, Eukleidův algoritmus, dvojkový NSD algoritmus;
  Bezoutova rovnost: $NSD(a,b) = min\{ax + by > 0 | x, y \in Z\}$; využití rozšířeného Eukleidova alg., řešení diofantické rovnice $ax + by = c$, kde $a, b, c \in Z$; řetězových zlomků; $NSD(a_1, a_2, \dots, a_n)$; nesoudělnost po dvou × sdružená nesoudělnost;
- Společný násobek, NSN, výpočet;
- Prvočísla, základní věta aritmetiky, kanonický rozklad a jeho využití (dělitele, NSD, NSN, počet, součet dělitelů). Eulerova funkce (definice, výpočet, multiplikativnost).

Řetězové zlomky

- konstrukce řet. zlomků rac. čísel pomocí Eukleidova alg.;
- přibližné zlomky $\delta_i = [q_0, q_1, \dots, q_i] = P_i/Q_i$, vlastnosti - rekurentní vztahy pro P_i a Q_i, $\delta_i - \delta_{i-1}$, $NSD(\delta_i, \delta_{i-1})$, tabulka přibližných zlomků.

Kongruence

- definice relace $\equiv_m$, vlastnosti (stejný i nestejný modul);
- Z_m - úplná soustava zbytků, Z_m^* redukovaná soustava zbytků;
- počítání v $Z_m \rightarrow$ sčítání, nulový prvek, opačný prvek; násobení, jednotkový prvek, (ne/vlastní) dělitele nuly, podmínka existence inverzního prvku v Z_m;
- řešení kongruencí 1. stupně a jejich soustav (Čínská věta o zbytku a její zobecnění);
- aritmetika velkých čísel; Eulerova a malá Fermatova věta.

Obsah prezenční části výuky

1. **blok prezenční části výuky (25. 10. 2019 (pá); 16:10-19:30; MIE; G4-mat)**
   Informace o předmětu (podmínky získání zápočtu, průběh zkoušky), předpokládané znalosti, obsah samostudia.
   Úvod do algebry
   - Pojmy kartézský součin, relace (vlastnosti, ekvivalence $\leftrightarrow$ rozklad, uspořádání; příklady), zobrazení, binární operace na množině - uzavřenost, asociativita, komutativita, neutrální prvek - jednoznačnost, symetrický prvek – jednoznačnost (asociativita).

2. <u>blok prezenční části výuky (16. 11. 2019 (so); 8:50-12:10; MIE; G4-mat)</u>

- Grupy, podgrupy, cyklické grupy, vlastnosti, příklady $(Z,+)$, $(Z_n,+)$;
  Permutace (dvouřádkový zápis), násobení, existence jednotkového a inverzního prvku; symetrická grupa $(S_n,\cdot)$; cyklus, permutace ve tvaru součinu disjunktních cyklů.
- Okruhy (ne/vlastní) dělitelé nuly → obory integrity → tělesa (stručně, příklady).
- Obory integrity polynomů nad tělesem. Dělení polynomů se zbytkem, NSD, NSN.
- Ireducibilita obecně a nad R, C. Existenční věta o ired. polynomech pro Z_n. Definice „býti kongruentní modulo polynom“, rozklad T[x]/q[x], tj. modulo polynom q[x], počítání v T[x]/q[x]. Konečná tělesa.
- Příklady počítání s polynomy (věta o dělení se zbytkem; NSD – eukleidův alg. + rozklad na ired. polynomy; počítání modulo $q(x)$);

3. <u>blok prezenční části výuky (13. 12. 2019 (pá); 16:10-19:30; MIE; G4-mat)</u>

<u>Úvod do kryptologie, kódování, komprese</u>

Základní pojmy a myšlenky (kryptografie, kryptoanalýza, steganografie).

<u>Základy šifrování</u>

- Abeceda *A*, prostor otevřených textů *M*, šifrových textů *C*; prostor klíčů *K*; Kerckhoffův princip; šifrovací systém = prostor klíčů + $\{E_e\}$ ... šifrovací transformace + $\{D_d\}$ ... dešifrovací transformace; metody: symetrický klíč (transpozice, substituce: monoalefabetické → homofonní → polyalfabetické) x asymetrický klíč (RSA).
- Transpoziční metody: jednoduchá transpozice s periodou *d*.
- Substituční metody: jednoduchá substituce/s klíčovým slovem; afinní; Hillova; Vigenerova;
- blokové šifrování, operace $\oplus$ … xor, + … nebo, $\cdot$ … a; Vernam, Feistel (DES, NDS);

4. <u>blok prezenční části výuky (18. 01. 2020 (so); 8:50-12:10; MIE; G4-mat)</u>

<u>Úvod do kódování</u> - základy bezeztrátové komprese, základy

- Zdrojová, kódová abeceda, kódování, kód. Jednoznačně dekódovatelné kódování; prefixový a blokový kód;
- Kraftova nerovnost, McMillanova věta. Nejkratší kód, střední délka kódového slova.
- Huffmanova konstrukce nejkratšího kódu - binární i obecná varianta.
- Aritmetické kódy, metoda DFWLD; dyadické zlomky

Zápočtové příklady 2019/20

(1) Číselné soustavy

- Uvedená čísla seřaďte neklesajícím způsobem:
  $(\text{b8ea})_{15}$; $(1001000100110000)_2$; $(14\text{b}01)_{13}$; $(1212222102)_3$; $(216202)_7$

(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) $\varphi\big(NSD(a,c)\big)$
- 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

- Nechť $\alpha = {}^{5321}/_{3400}$. Sestavte tabulku přibližných zlomků pro α^{-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 $768x \equiv -1240\ (mod\ 412)$. 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 $x \equiv 6\ (12), x \equiv 2\ (14), x \equiv 3\ (15), x \equiv 9\ (21)$. Výsledek zapište v soustavě nejmenších nezáporných zbytků odpovídajícího modulu.
- Vyřešte následující soustavu kongruencí $x \equiv 3\ (15), x \equiv 6\ (9), x \equiv 14\ (70), x \equiv 7\ (8)$. Výsledek zapište v soustavě nejmenších nezáporných zbytků odpovídajícího modulu.

(7) Počítání s polynomy

- Nechť $f(x), g(x) \in Z_7[x]$, 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 spočtěte $NSD\big(f(x), g(x)\big)$. 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 $f(x), g(x) \in {}^{Z_5[x]}/_{(x^5 + 3x^3 + 2x + 2)}$, kde $f(x) = 3x^4 + 2x^3 + x + 4, g(x) = 4x^3 + 3x^2 + 2x + 1$. Spočtěte $g(x) \cdot f(x)$. 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 π, ρ ve tvaru součinu disjunktních cyklů a σ ve tvaru součinu transpozic.
  b) Zapište π, ρ, σ v tzv. dvouřádkovém tvaru.
- Uvažujte permutace $\pi, \rho, \sigma \in S_7$, kde $\pi = (1524)(437)(13642), \rho = (3761)(24536)(2751), \sigma = (7653214)$. a) Spočtěte $(\pi \cdot \rho^{-1})^{-1}$. 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} $(mod\ 26)$.
  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 $S = \begin{matrix} a & b & c & d & e & f & g & h & i \\ 3/40 & 1/24 & 1/6 & 1/30 & 31/120 & 1/24 & 5/24 & 1/20 & 1/8 \end{matrix}$.
  Nalezněte nejkratší kód dané abecedy a spočtěte 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 $\begin{matrix} znak \\ pst. \end{matrix} \left| \begin{matrix} a_1 & a_2 & a_3 & a_4 & a_5 & a_6 \\ 0{,}25 & 0{,}2 & 0{,}2 & 0{,}15 & 0{,}15 & 0{,}05 \end{matrix} \right.$. Pomocí metody DFWLD zakódujte slovo $a_3 a_1 a_3 a_2$.