Název předmětu: **Matematika pro informatiky**

(platné pro ak. rok 2018/19)

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. 2 MB), a to nejpozději do konce zkouškového období ZS ak. roku 2018/19.
- 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 2018/19.
- 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).

22. října 2018

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 (13. 10. 2018; 314; 8:50-14:05)

Informace o předmětu (podmínky získání zápočtu, průběh zkoušky), předpokládané znalosti, obsah samostudia.

Úvod do algebry

- Pojmy kartézský součin, zobrazení, binární operace na množině - uzavřenost, asociativita, komutativi-ta, neutrální prvek - jednoznačnost, symetrický prvek – jednoznačnost (asociativita).
- 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.

2. <u>blok prezenční části výuky (9. 11. 2018; F21; 8:50-13:15)</u>

- 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 (7. 12. 2018; F21; 8:50-13:15)</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, · … a; Vernam, Feistel (DES, NDS);

4. <u>blok prezenční části výuky (22. 12. 2017; G4_MAT; 8:50-12:10)</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