Název předmětu: **Matematika pro informatiky**

Zkratka předmětu: **MIE**

Počet kreditů: 5 Forma studia: kombinovaná

Forma zkoušky: kombinovaná (písemná a ústní část)

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

Doporučená literatura:
Adámek, J.: Kódování. SNTL, Praha, 1989.
Bečvář, J.: Úvod do algebry. Skripta MFF UK, SPN, Praha 1984..
Koucký, M.: Sbírka příkladů z diskrétní matematiky. Skripta TUL, 2003.
Koucký, M.: Diskrétní matematika II. Skripta TUL, Liberec, 2003.
Koucký, M., Zelinka, B.: Diskrétní matematika I. Skripta TUL, Liberec, 2003.

Garant a přednášející: doc. RNDr. Miroslav Koucký, CSc.

## Matematika pro informatiky

### Předpokládané znalosti

- Základy maticového počtu (matice nad $Z_p$, transpozice, součin, výpočet inverze).

### 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 (dělitelé, 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) dělitelé 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 (14. 10. 2016; G4_MAT; 8:50-12:10)**

Přehled značení

Úvod do algebry

- Pojmy kartézský součin, zobrazení, binární operace na množině - uzavřenost, asociativita, komutativita, neutrální prvek - jednoznačnost, symetrický prvek – jednoznačnost (asociativita).
- Grupy, podgrupy, cyklické grupy, vlastnosti, příklady $(Z, +)$, $(Z_n, +)$;

**2. <u>blok prezenční části výuky (4. 11. 2016; G4_MAT; 8:50-12:10)</u>**

dodělat - 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 tvarunsoučinu 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.

**3. <u>blok prezenční části výuky (9. 12. 2016; G4_MAT; 8:50-12:10)</u>**

**4. <u>blok prezenční části výuky (6. 1. 2017; G4_MAT; 8:50-12:10)</u>**

| | | | | | |
|---|---|---|---|---|---|
| 4. 11. | 8.50–12.10 | MIE | G4-MAT | | doc. Koucký |
| 4. 11. | 12.30–14.00 | OPS-P | A10 | | ing. Kosková |
| 11. 11. | 12.30–15.50 | ULA | A11 | | dr. Kalousek |
| 18. 11. | 12.30–14.00 | OPS-P | A10 | | ing. Kosková |
| 25. 11. | 8.50–12.10 | ULA | A11 | | dr. Kalousek |
| 25. 11. | 12.30–14.00 | OPS-P | A10 | | ing. Kosková |
| 9. 12. | 8.50–12.10 | MIE | G4-MAT | | doc. Koucký |
| 10. 12. | 8.50–12.10 | ULA | A11 | | dr. Kalousek |
| 6. 1. | 8.50–12.10 | MIE | G4-MAT | | doc. Koucký |
| 7. 1. | 8.50–12.10 | ULA | A11 | | dr. Kalousek |

---

**1. <u>blok prezenční části výuky (30. 4. 2016, 9:00 - 15:00, G305)</u>**

Přehled značení

<u>Úvod do algebry</u>

- Pojmy kartézský součin, zobrazení, binární operace na množině - uzavřenost, asociativita, komutativita, 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 tvarunsoučinu disjunktních cyklů.
- Okruhy (ne/vlastní) dělitelé nuly → obory integrity → tělesa (stručně, příklady).

**2. <u>blok prezenční části výuky (13. 5. 2016, 12:00 - 18:00, G4-MAT)</u>**
- 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.

<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);
- Poznámky: hash; digitální podpis; digitální certifikát, certifikační autorita. Diffie-Helmann výměna šifrovacích klíčů;

<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

Bezpečnostní (detekční/opravné) kódy - pouze binární
- Binární blokové kódy, pojmy Hammingova vzdálenost, váha. Chyba, objevování/opravování *t*-násobných chyb, minimální vzdálenost kódu; informační a kontrolní znaky, systematický kód, ekvivalentní kódy, (*n*,*k*)-kód, resp. (*n*,*k*,*d*)-kód. Příklady - opakovací kód, kód celkové kontroly parity, koktavý kód, kód 2 z 5.
- Binární lineární (*n*,*k*)-kód, generující matice, kontrolní matice, vzájemný vztah.
- Syndrom a jeho využití, standardní dekódování.
- Binární Hammingův kód řádu *r*, kontrolní matice, dekódování.

Udělené zápočty

- Jindřich Maruška (uznán z loňska)
- Dlouhý
- Kateřina Sinkevičová, P14000571; 6.9.2016
- 