

Elektrotechnika a informatika - magisterské studium FM TUL

(dvouleté)

Studijní předmět

Název: Diskrétní matematika
Zkratka: DIM
Typ: povinný pro obor IT
Rozsah: 14 týdnů, týdně 2 hodiny přednášek + 2 hodiny seminárních cvičení
Kredity: 5
Způsob ukončení: zkouška

Katedra: katedra aplikované matematiky FP TUL
Přednášející: Doc. RNDr. Miroslav Koucký, CSc.

Stručná anotace předmětu:

Předmět seznamuje studenty s následujícími tématickými okruhy a jejich aplikacemi v oblasti technických disciplín – úvod do teorie dělitelnosti (číselné soustavy, lineární kongruence), základní algebraické struktury s jednou a dvěma binárními operacemi (zejména grupy, okruhy polynomů a konečná tělesa), úvod do teorie šifrování (se symetrickým i asymetrickým klíčem) a kódování (lineární kódy).

Získané kompetence:

Získané znalosti lze uplatnit v další části studia, zejména v předmětech zaměřených na informační technologie.

Témata přednášek:

Úvod do teorie dělitelnosti – relace „býti kongruentní modulo m “ a její vlastnosti. Základní celočíselné funkce – horní, dolní celá část, Eulerova a Möbiova funkce. Lineární kongruence. Čínská věta o zbytku. Řešení kongruencí 1. stupně a jejich soustav.

Základní algebraické struktury s jednou a dvěma binárními operacemi. Základní pojmy (n -ární operace na množině, homomorfismus, izomorfismus). Úvod do teorie grup - základní pojmy (podgrupy, normální podgrupy, konečné grupy, cyklické grupy). Lagrangeova věta. Okruhy polynomů (nad R , C i Z_n), tělesa, konečná tělesa. Základní věta algebry, rozklady polynomů v oboru reálných i komplexních čísel.

Úvod do šifrování - základní pojmy, Kerckhoffův princip. Šifrování se symetrickým klíčem – metody transpoziční, substituční (mono i polyalfabetické, homofonní). Základy kryptoanalýzy. Hillovo šifrování. Šifrování s asymetrickým klíčem (metoda RSA).

Úvod do teorie kódování – základní pojmy (prosté, jednoznačně dekódovatelné, blokové a prefixové kódování). Kódování bez šumu - Kraftova nerovnost, Huffmanova konstrukce nejkratšího kódu. Bezpečnostní kódy – základní pojmy (násobnost chyby, objevování a opravování chyb). Lineární kódy (kontrolní a generující matice, standardní dekódování, syndrom). Hammingovy kódy.

Náplň cvičení:

Počítání v soustavě nejmenších nezáporných zbytků „modulo m “, základní kritéria dělitelnosti. Číselné soustavy. Příklady na řešení kongruencí 1. stupně a jejich soustav. Aplikace - aritmetika velkých čísel, generátory pseudonáhodných čísel.

Příklady základních algebraických struktur - Kleinova čtyřgrupa, kvaterniony, symetrické a alternující grupy. Konstrukce konečných těles a počítání v nich. Hornerovo schéma.

Příklady na jednoduché transpoziční, afinní, Hillovo a Vigenèrovo šifrování. Praktické ukázky kryptoanalýzy.

Příklady na Huffmanovu konstrukci nejkratšího kódu, konstrukci vytvářející a generující matice lineárního a systematické dekódování. Hammingův kód a jeho dekódování.

Literatura:

Adámek J.: Kódování. SNTL, Praha 1989
Bican L.: Algebra. Academia, Praha 2001

Koucký M., Zelinka B.: Diskrétní matematika I. Skriptum TUL, 2003
Koucký M.: Diskrétní matematika II. Skriptum TUL, 2003
Koucký M.: Sbírka příkladů z diskretní matematiky. Skriptum TUL, 2003
Matoušek J., Nešetřil J.: Kapitoly z diskretní matematiky. Matfyzpress, Praha 1996

Prerekvizity: Základní znalosti z oblasti výrokové logiky a booleovských funkcí (v rozsahu bakalářského studia).

Navazující: -

Datum poslední změny: 22. 8. 2005