

Okruhy ke zkoušce z předmětu Matematické algoritmy pro školní rok 2009/2010

19. prosince 2009

Algoritmizace. Iterační a rekurzivní paradigma. Sériové a paralelní programování. Deterministický a nedeterministický přístup k řešení úloh. Rodzdel a panuj. Dynamické programování. Konečné automaty. Turingův stroj.

Vlastnosti čísel. Prvočísla. Mersennova čísla. Fermatova čísla. FaktORIZACE. Nejvyšší společný dělitel. Nesoudělná čísla. Euklidův algoritmus.

Modulární aritmetika. Kongruence. Modulární dělení. Modulární inverze. Malá Fermatova věta. Eulerova věta. Modulární mocnění.

Čínská věta o zbytcích.

Šifrování. Symetrické a asymetrické šifry. Výměna klíčů. Princip RSA.

Kódování. Blokové kódy, prefixové kódy. Minimální vzdálenost. Detekce a opravy chyb. Lineární kódy.

Analýza algoritmů. Velká O notace. Paměťová a časová složitost algoritmu.

Řetězové zlomky. Definice. Pravý řetězový zlomek. Řetězový zlomek jako vedlejší produkt Eukleidova algoritmu. Vyjádření odmocniny řetězovým zlomkem. Řetězový zlomek jako kořen kvadratické rovnice. Převod součtu nekonečné řady na řetězový zlomek. Sblížené zlomky.

Numerická úloha a numerický algoritmus. Reprezentace čísel v pevné a plovoucí řádnové čárce. Možné zdroje chyb ve výpočtu. Absolutní a relativní chyba výpočtu. Korektnost úlohy. Podmíněnost úlohy.

Řešení nelineárních rovnic. Požadavky na existenci řešení. Ohraničující interval (bracket). Podmíněnost řešení. Rychlost konvergence. Metoda půlení intervalu. Metoda prosté iterace a její varianty – metoda tečen, metoda sečen.

Numerická integrace. Důvody, princip. Kvadraturní vzorce. Algebraický řád. Newtonovy-Cotesovy vzorce – obdélníkové, lichoběžníkové a Simpsonovo pravidlo. Gaussovy kvadraturní vzorce.