

# Okruhy ke zkoušce z předmětu Matematické algoritmy pro školní rok 2010/2011

5. ledna 2011

Pro tento semestr pokrývají přednášky předmětu 11MA následující témata:

1. Algoritmizace. Iterační a rekurzivní paradigma. Sériové a paralelní programování. Deterministický a nedeterministický přístup k řešení úloh. Rodzděl a panuj. Dynamické programování. Konečné automaty. Turingův stroj.
2. Vlastnosti čísel. Prvočísla. Mersennova čísla. Fermatova čísla. Faktorizace. Nejvyšší společný dělitel. Nesoudelná čísla. Eukliduv algoritmus.
3. Modulární aritmetika. Kongruence. Modulární dělení. Modulární inverze. Malá Fermatova veta. Eulerova veta. Modulární mocnění.
4. Čínská věta o zbytcích.
5. Šifrování. Symetrické a asymetrické šifry. Výměna klíčů. Princip RSA.
6. Analýza algoritmů. Velká  $\mathcal{O}$  notace. Paměťová a časová složitost algoritmu.
7. Numerická úloha a numerický algoritmus. Reprezentace čísel v pevné a plovoucí řádové čárce. Možné zdroje chyb ve výpočtu. Absolutní a relativní chyba výpočtu. Korektnost úlohy. Podmíněnost úlohy.
8. 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.
9. Numerická integrace. Důvody, princip. Kvadraturní vzorce. Algebraický řád. Newtonovy-Cotesovy vzorce – obdélníkové, lichoběžníkové a Simpsonovo pravidlo. Gaussovy kvadraturní vzorce.

10. Náhodná čísla, pseudonáhodná čísla. Lineární kongruentní generátor. Kvazináhodná čísla. Monte-Carlo metody. Monte-Carlo integrace, klady a zápory, rychlost konvergence.
11. Interpolace a aproximace. Princip, rozdíly. Třídy aproximujících funkcí. Měření chyby aproximace. Lagrangeovský interpolační polynom.