

Zkoušený dostane dvě otázky z následujícího seznamu (odkaz je na číslo z přednášky):

Otázka 1:

- (1) Vyslovte a dokažte tvrzení o odhadu časové složitosti rekurentního algoritmu. (1.2)
- (2) Zformulujte Eukleidův algoritmus a binární Eukleidův algoritmus (Steinův) na výpočet NSD v celých číslech a dokažte, že fungují. (A_8 , A_9 , 3.1, 3.6)
- (3) Vyslovte a dokažte Čínskou větu o zbytcích v OHI a zformulujte a vysvětlete Lagrangeův a Garnerův algoritmus. (5.2, A_{11} , A_{12}).
- (4) Zformulujte algoritmus Rychlé Fourierovy transformace a dokažte jeho správnost. Jak lze hledat primitivním n -té odmocniny z jedné? (A_{13} , 6.2, část 6.3).
- (5) Zformulujte algoritmus na rychlé násobení polynomů a dokažte jeho správnost. Naznačte způsoby nalezení primitivních n -tých odmocnin z jedné. (A_{15} , část Věty 6.4).
- (6) Zformulujte algoritmus na rychlé hledání prvních n členů inverzu mocninné řady a na rychlé dělení polynomů a dokažte jeho správnost. (A_{16} , A_{17} , 7.5).
- (7) Zaveďte pojmy pseudodělení a posloupnost polynomiálních zbytků. Zformulujte a vysvětlete generický algoritmus na hledání NSD polynomů a generický algoritmus hledání NSD nad celými čísly pomocí posloupnosti polynomiálních zbytků. (A_{19} , A_{20} , 8.4).
- (8) Popište soudělnost polynomů pomocí resultantů a dokažte Sylvesterovo kritérium soudělnosti. (9.2)
- (9) Vyslovte a dokažte větu o výpočtu resultantu polynomů f a g pomocí jejich kořenů. (9.5)
- (10) Zformulujte modulární algoritmus na výpočet NSD polynomů nad celými čísly a dokažte jeho správnost. (A_{21} nebo A_{22} , 10.8, 10.9)
- (11) Dokažte tvrzení (a vysvětlete pojmy), že smolných prvočísel i hodnot je jen konečně mnoho. (10.4, 10.5)
- (12) Vysvětlete pojmy šťastné a smolné hodnoty a nastiňte postup, jak hledat NSD v okruzích polynomů dvou neurčitých (kapitola 11)

Otázka 2:

- (1) Zformulujte algoritmy školských operací s celými čísly (včetně převodu mezi bázemi a binárního mocnění) a odhadněte asymptoticky jejich časovou složitost. (A_1 , A_2 , A_3 , A_4 , A_7)
- (2) Zformulujte Karacubův algoritmus a nastiňte algoritmus Toom-3 na násobení celých čísel a odhadněte asymptoticky jejich časovou složitost. (A_6 , \tilde{A}_6 2.4, 2.5).
- (3) Zformulujte Eukleidův algoritmus v celých číslech a odhadněte asymptoticky jeho časovou složitost. (A_8 , 3.5).
- (4) Zformulujte binární Eukleidův algoritmus (Steinův) na výpočet NSD v celých číslech a odhadněte asymptoticky jeho časovou složitost. (A_9 , 3.6)
- (5) Zformulujte algoritmy školských operací s polynomy $R[x]$ (sčítání, násobení, dělení se zbytkem) a odhadněte asymptoticky jejich časovou složitost v závislosti na stupni polynomu. Jakou roli hraje pro časovou složitost velikost oboru R ? (\tilde{A}_1 , \tilde{A}_2 , \tilde{A}_{10})

- (6) Zformulujte Eukleidův algoritmus pro hledání NSD v oboru polynomů nad tělesem a odhadněte asymptoticky jeho časovou složitost v závislosti na stupni polynomu a velikosti tělesa. (\tilde{A}_8 4.1)
- (7) Zformulujte Lagrangeův algoritmus na Čínskou větu o zbytcích a odhadněte asymptoticky jeho časovou složitost nad celými čísly a nad polynomy nad tělesem. (A_{11} , část 5.3)
- (8) Zformulujte Garnerův algoritmus na Čínskou větu o zbytcích a odhadněte asymptoticky jeho časovou složitost nad celými čísly a nad polynomy nad tělesem. (A_{12} , část 5.3)
- (9) Zformulujte algoritmus Rychlé Fourierovy transformace a odhadněte asymptoticky jeho časovou složitost (v závislosti na stupni polynomu). (A_{13} , část 6.3).
- (10) Zformulujte algoritmus na rychlé násobení polynomů a odhadněte asymptoticky jeho časovou složitost. (A_{15} , část 6.4).
- (11) Zformulujte algoritmus na rychlé hledání prvních n členů inverzu mocninné řady a na rychlé dělení polynomů a odhadněte asymptoticky jejich časovou složitost. (A_{16} , A_{17} , 7.2, část 7.5).
- (12) Buď $(5, 0, 3, 8)$ modulární reprezentace polynomu f stupně ≤ 3 nad tělesem \mathbb{Z}_{17} pomocí DFT_4 . Zformulujte algoritmus Rychlé Fourierovy transformace a s jeho pomocí najděte polynom f . (A_{13}).
- (13) Zformulujte algoritmus rychlého dělení se zbytkem a s jeho pomocí spočítejte $\mathbb{Z}_5[x]$ podíl $x^4 + x^3 + 3x^2 + x + 1 : x^2 + 2$. (A_{16}).
- (14) Spočítejte NSD celočíselných polynomů

$$x^5 - x^4 - 3x^2 - 3x + 2 \text{ a } x^4 - 2x^3 - 3x^2 + 4x + 4$$

efektivní i neefektivní verzi modulárního algoritmu. (A_{21} , A_{22}).

Konkrétní hodnoty v příkladech na aplikaci algoritmů budou změněny.