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

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, část 4.1)
(3) Vyslovte a dokažte Čínskou větu o zbytcích v Eukleidových oborech a zformulujte a vysvětlete Lagrangeův a Garnerův algoritmus. (6.2, 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}, 7.2, část 7.3).
(5) Zformulujte algoritmus na rychlé násobení polynomů a dokažte jeho správnost. Naznačte způsoby nalezení primitivních n-tých odmocnin z jedné. (A_{15}, část Věty 8.2).
(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}, 9.5).
(7) Zaveďte pojmy pseudodělení a posloupnost polynomiálních zbytků. Zformuljte a vysvětlete generický algoritmus na hledání NSD polynomů a generický algoritmus hledání NSD nad celými čísly pomocí posloupnosti polynomiálních zbytků. (A_{19}, A_{20}, 10.4).
(8) Popište soudělnost polynomů pomocí rezultantů a dokažte Sylvesterovo kritérium soudělnosti. (11.2)
(9) Vyslovte a dokažte větu o výpočtu rezultantu polynomů f a g jako polynomiální kombinace polynomů f a g. (11.4)
(10) Zformulujte modulární algoritmus na výpočet NSD polynomů nad celými čísly a dokažte jeho správnost. (A_{21} nebo A_{22}, 12.8, 12.9)
(11) Dokažte tvrzení (a vysvětlete pojmy), že smolných prvočísel i hodnot je jen konečně mnoho. (12.3, 12.4)
(12) Vysvětlete pojmy šťasné a smolné hodnoty a nastiňte postup, jak hledat NSD v okruzích polynomů dvou neurčitých (skripta: sekce 14.2)

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, 4.1)
(5) 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. ($\tilde{A}_8$ 5.1)

(6) Zformulujte Lagrangeův algoritmus na Čínskou větu o zbytcích a odhadněte asymptoticky jeho časovou složitost nad celými čísly a nad polynomy nad tělesem. (A_{11}, 6.3)

(7) Zformulujte Garnerův algoritmus na Čínskou větu o zbytcích a odhadněte asymptoticky jeho časovou složitost nad celými čísly a nad polynomy nad tělesem. (A_{12}, 6.3)

(8) Zformulujte algoritmus Rychlé Fourierovy transformace a odhadněte asymptoticky jeho časovou složitost (v závislosti na stupni polynomu). (A_{13}, část 7.3).

(9) Zformulujte algoritmus na rychlé násobení polynomů a odhadněte asymptoticky jeho časovou složitost. (A_{15}, část 8.2).

(10) 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}, 9,2, část 9.5).

(11) 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}).

(12) Zformulujte algoritmus rychlého dělení se zbytkem a s jeho pomocí spočítejte $\mathbb{Z}_5[x]$ podíl $x^4 + x^3 + 3x^2 + x + 1 \quad : x^2 + 2$. ($A_{16}$).

(13) 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 verzí modulárního algoritmu. (A_{21}, A_{22}).

Konkrétní hodnoty v příkladech na aplikaci algoritmů budou změněny.