Zkoušený dostane dvě otázky z následujícího seznamu:

Otázka 1:

1. Zformulujte Eukleidův algoritmus na výpočet NSD v celých číslech a dokažte, že funguje.

1. Vyslovte a dokažte tvrzení o odhadu časové složitosti rekurentního algoritmu.

1. Vyslovte a dokažte Čínskou větu o zbytcích v Eukleidových oborech a zformulujte a dokažte správnost Lagrangeova a Garnerova algoritmu.

1. Zformulujte algoritmus Rychlé Fourierovy transformace a dokažte jeho správnost. Jak lze hledat primitivním n-té odmocniny z jedné?

1. Zformulujte algoritmus na rychlé dělení polynomů a dokažte jeho správnost.

1. Vysvětlete pojmy pseudodělení a posloupnost polynomiálních zbytků. Popište a dokažte korektnost generického algoritmu na hledání NSD polynomů nad celými čísly pomocí posloupnosti polynomiálních zbytků.

1. Zformulujte modulární algoritmus na výpočet NSD polynomů nad celými čísly a dokažte jeho správnost.

1. Vysvětlete pojmy šťasné a smolné hodnoty a nastiňte postup, jak hledat NSD v okruzích polynomů dvou neurčitých.

1. Popište soudělnost polynomů pomocí rezultantů a dokažte Sylvesterovo kritérium soudělnosti.

1. Vyslovte a dokažte větu o výpočtu rezultantu polynomů f a g jako polynomiální kombinace polynomů f a g.

1. Dokažte tvrzení (a vysvětlete pojmy), že smolných prvočísel i hodnot je jen konečně mnoho.

Otázka 2:

2. Zformulujte algoritmy školských operací s celými čísly (včetně převodu mezi bázemi a binárního mocnění) a odhadněte asymptoticky jejich časovou složitost.

2. Zformulujte Eukleidův algoritmus v celých číslech a odhadněte asymptoticky jeho časovou složitost.

2. Zformulujte Karacubův algoritmus na násobení celých čísel a odhadněte asymptoticky jeho časovou složitost. Nastiňte algoritmus asymptoticky rychlejší (Toom-k).

2. 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?

2. 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.

2. Zformulujte algoritmy operací v konečných tělesech (sčítání, násobení, invertování) a odhadněte asymptoticky jejich časovou složitost v závislosti na velikosti tělesa.

2. Zformulujte Lagrangeův algoritmus na Čínskou větu o zbytcích a odhadněte asymptoticky jeho časovou složitost nad celými čísly a nad polynomy nad tělesem (v závislosti na stupni polynomu).

2. Zformulujte Garnerův algoritmus na Čínskou větu o zbytcích a odhadněte asymptoticky jeho časovou složitost nad celými čísly a nad polynomy nad tělesem (v závislosti na stupni polynomu).

2. Zformulujte algoritmus Rychlé Fourierovy transformace a odhadněte asymptoticky jeho časovou složitost (v závislosti na stupni polynomu).

2. Zformulujte algoritmus modulárního násobení polynomů a odhadněte asymptoticky jeho časovou složitost.

2. 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.

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

2. Spočítejte NSD celočíselných polynomů

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

efektivní i neefektivní verzí modulárního algoritmu.