

Otázky ke zkoušce z Číselných algoritmů

1. VZTAH RSA A FAKTORIZACE

1. Popište faktorizační algoritmus využívající orákulum na určení soukromého klíče RSA (Alg 1). Dokažte korektnost a odhad pravděpodobnosti úspěchu (1.3, 1.4).

2. POLLARDOVA ρ -METODA

2. Popište a vysvětlete (pomocí souvisejících pojmů a jejich vlastností, není třeba dokazovat) Pollardův-Floydův algoritmus (Alg 4).

3. B-MOCNÁ ČÍSLA

3. Zaveďte pojem B -hladkého a B -mocného čísla a popište jednodušší verzi faktorizačního Pollardova (p-1)-algoritmu (Alg 5A). Jakou má časovou složitost?

4. Napište 2.verzi Pollardova (p-1)-algoritmu (Alg 5B) a dokažte pravděpodobnost úspěchu pro faktorizaci součinu dvou prvočísel (3.6).

5. Napište a stručně vysvětlete (odkazem na platné tvrzení) faktorizační (p+1)-algoritmus (Alg 6).

6. Vysvětlete princip Lenstrova ECM-algoritmu (Alg 7 a 8).

7. Stručně vysvětlete princip Lenstrova ECM-algoritmu (Alg 8) a dokažte tvrzení o jeho úspěchu (3.10).

4. ODMOCŇOVÁNÍ MODULO N

8. Napište a stručně vysvětlete (odkazem na platné pozorování) Tonelli-Shanksův algoritmus pro počítání druhé odmocniny modulo liché prvočísel (Alg 10).

9. Napište algoritmy pro hledání kořenů polynomů stupně dva a obecného polynomu modulo liché prvočísel (Alg 11, 12).

10. Popište a stručně vysvětlete algoritmus odmocňování modulo p^n (Alg 13).

11. Popište útok na RSA pomocí deterministického orákula na hledání druhé odmocniny modulo součin dvou různých prvočísel (Alg 14) a dokažte tvrzení o jeho korektnosti a pravděpodobnosti neúspěchu (4.5).

5. DIXONOVA FAKTORIZACE A CFRAC

12. Zaveďte pojmy báze faktorizace, relace a hladké relace a napište schéma Dixonovy faktorizace. Jak funguje její lineární fáze (formulace 5.2).

13. Zformulujte algoritmus výpočtu řetězového rozvoje odmocniny $\sqrt{N}$ pomocí jediného odhadu $\lfloor \sqrt{N} \rfloor$ (Alg 16) a dokažte jeho korektnost (5.5).

14. Zformulujte algoritmus CFRAC faktorizace pomocí řetězových zlomků (Alg 17) a dokažte jeho korektnost (5.7).

6. KVADRATICKÉ SÍTO.

15. Popište generátor relací kvadratického síta (včetně popisu samotných relací) a zformulujte některou variantu prosívání (Alg 18A, 18B nebo 18D)

7. DISKRÉTNÍ LOGARITMUS

16. Zformulujte a dokažte tvrzení o redukce výpočtu diskrétního logaritmu na výpočet diskrétních logaritmů pro jeho dělitele (7.1). Jak funguje algoritmus Baby-steps, giant-steps (Alg 19)?

17. Popište algoritmus faktorizace pomocí orákula pro řešení zobecněného problému diskrétního logaritmu v grupě Z_N^* (Alg 20) a stručně vysvětlete (odkazem na platná tvrzení, není nutné dokazovat) jeho korektnost a pravděpodobnost úspěchu (formulace 7.3, 7.4).