Zkouška z Číselných algoritmů, ukázkový test

(1) Stručně vysvětlete princip Lenstrova ECM-algoritmu a dokažte tvrzení o jeho úspěchu.

(9 bodů)

(2) Popište a stručně vysvětlete algoritmus odmocňování modulo p^n.

(5 bodů)

(3) Popište generátor relací kvadratického síta (včetně popisu samotných relací) a zformulujte některou variantu prosívání

(6 bodů)