Skaitļu teorija

Mājas darbi

Uzmanību! Par programmēšanas uzdevumu vērtēšanu. Programmēšanas uzdevuma vērtējumā nozīmīgu lomu spēlēs ne tikai tas, vai programma izdod pareizu iznākumu, bet arī, vai lietotie algoritmi ir efektīvi, tas ir, to sarežģītībai jābūt polinomiālai no ieejas datu garuma. Ja nav priekšstata par algoritmu sarežģītību, var palīdzēt tas, ka lekcijās tika izstāstīti atbilstoši efektīvi algoritmi, turklāt Shoupa grāmatā gan aprakstīti visi nepieciešamie algoritmi, gan noteikta to sarežģītība. Algoritmu sarežģītība Jūsu risinājumā NAV jāpierāda, pietiek, ka zināms, ka tie IR efektīvi. Ja būs lietots neefektīvs algoritms (piemēram, pilnās pārlases algoritms), vērtējums var būt visai zems, ja tas ļoti būtiski atvieglo risinājumu un parāda, ka neesat apguvuši attiecīgo tēmu, kurā tika izstāstīts efektīvs algoritms (un skaitļu teorijas pielietojumos efektivitāte parasti ir būtiska).

1. mājas darbs

1. Atrast Jūsu studenta apliecības numurā esošā skaitļa un 2024 lielāko kopīgo dalītāju, lietojot Eiklīda algoritmu. Piemēram, ja studenta apliecības numurs ir mk24035, tad jāaprēķina $LKD(24035, 2024)$.

2. Atrast skaitļu $35 + 13i$ un $1 + 15i$ lielāko kopīgo dalītāju gredzenā $\mathbb{Z}[i]$. (Ieteikums: izdomāt, kas derētu kā piemērota λ funkcija, lai varētu ieviest dalīšanu ar atlikumu un lietot Eiklīda algoritmu.)

3. Uzrakstīt programmu, kas dotiem veseliem pozitīviem skaitļiem k, m_1, m_2, …, m_k, a_1, a_2, …, a_k (ieejas dati atrodas failā "ieeja.txt" šajā secībā, katrs skaitlis jaunā rindiņā), kur skaitļi m_i ir savstarpēji pirmskaitļi, atrod un izvada tādu a, ka $0 \leq a < m_1 m_2 \dots m_k$ un $a \equiv a_1 \pmod{m_1}$, $a \equiv a_2 \pmod{m_2}$, …, $a \equiv a_k \pmod{m_k}$.

2. mājas darbs

Jāatrisina tikai viens no 3. un 4. uzdevuma (ja būs risināti abi, ieskaitīts tiks labākais sasniegums).

1. Atrast visas pirmatnējās saknes pēc moduļa 17. Kādiem kāpinātājiem n eksistē tādi a, ka kongruenčvienādojumam $x^n \equiv a \pmod{17}$ nav atrisinājumu?

2. Uzrakstīt programmu, kas dotiem veseliem pozitīviem skaitļiem k, p_1, p_2, …, p_k, e_1, e_2, …, e_k (ieejas dati atrodas failā "ieeja.txt" šajā secībā, katrs skaitlis jaunā rindiņā), tādiem, ka p_1, p_2, …, p_k un $p = p_1^{e_1} p_2^{e_2} \cdot \ldots \cdot p_k^{e_k} + 1$ ir pirmskaitļi, atrod pirmatnēju sakni pēc moduļa p.

3. Dots, ka p ir nepāra pirmskaitlis. Pierādīt: 10 ir pirmatnēja sakne pēc moduļa p tad un tikai tad, ja daļas $1/p$ decimālajā pierakstā (mazākā) perioda garums ir $p - 1$.

4. Pierādīt, ka, ja $p = 4k + 1$ ir pirmskaitlis (kur k ir naturāls skaitlis), tad: g ir pirmatnēja sakne pēc moduļa p tad un tikai tad, ja $-g$ ir pirmatnēja sakne pēc moduļa p.