Kevad 2016

Arvuteooria 13. praktikumi ülesanded:

Ruutjäägid I.

1. Leida otse, pööratavate elementide ruute järjest välja arvutades, kõik ruutjäägid mooduli 17 järgi.

2. Leida kõik ruutjäägid mooduli 19 järgi Euleri kriteeriumi abil.

3. Leida kõik ruutjäägid mooduli 29 järgi Legendre'i sümboli omaduste abil.

4. Millised järgmistest kongruentsidest on lahenduvad ja mitu lahendit neil on (kui üldse on):

a) $x^2 \equiv 1 \pmod{61}$; b) $x^2 \equiv -1 \pmod{67}$;
c) $x^2 \equiv 2 \pmod{61}$; d) $x^2 \equiv -2 \pmod{67}$;
e) $x^2 \equiv 2 \pmod{122}$; f) $x^2 \equiv -2 \pmod{134}$.

5. Teha kindlaks, milliste algarvude p korral on $-p$ ruutjääk mooduli 7 järgi.

6. Tõestada, et ruutjääk ei ole kunagi algjuur.

7. Tõestada, et kui $p \equiv 1 \pmod{4}$ on algarv, siis

$$\sum_{a=1}^{(p-1)/2} \left(\frac{a}{p}\right) = 0.$$

8. Tõestada, et diofantiline võrrand $x^2 - 2y^2 = p$ ei ole lahenduv ühegi algarvu $p \equiv 3, 5 \pmod{8}$ korral.

9*. Olgu p algarv kujul $4k+3$, $k \in \{0\} \cup \mathbb{N}$, ja olgu n kõigi selliste ruutjääkide a arv mooduli p järgi, mille korral $0 < a < \frac{p}{2}$. Leida järgmiste korrutiste väärtused jäägiklassikorpuses $\mathbb{Z}_p$ arvu n kaudu:

$$A = \overline{1} \cdot \overline{3} \cdot \overline{5} \cdot \ldots \cdot \overline{p-2} \qquad \text{ja} \qquad B = \overline{2} \cdot \overline{4} \cdot \overline{6} \cdot \ldots \cdot \overline{p-1}.$$

10**. Milliste a, b, c täisarvuliste väärtuste korral on murru

$$\frac{a^2 + b^2 + c^2}{3(ab + bc + ca)}$$

väärtus samuti täisarv?

Ajapäevik: 13. nädal

Aeg	Tegevus	Kommentaarid