Kevad 2014

Arvuteooria 13. praktikumi ülesanded:

Ruutjäägid I.

1. Leida otse, pööratavate elementide ruute järjest välja arvutades, kõik ruutjäägid mooduli 19 järgi.

2. Leida kõik ruutjäägid mooduli 13 järgi Euleri kriteeriumi abil.

3. Leida kõik ruutjäägid mooduli 17 järgi Legendre'i sümboli omaduste abil.

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

a) $x^2 \equiv -1 \pmod{71}$; b) $x^2 \equiv 1 \pmod{73}$;
c) $x^2 \equiv 2 \pmod{71}$; d) $x^2 \equiv -2 \pmod{73}$;
e) $x^2 \equiv -2 \pmod{142}$; f) $x^2 \equiv -2 \pmod{146}$.

5. Tõestada, et kui p on paaritu algarv, siis $\left(\frac{p}{7}\right) = 1$ parajasti siis, kui $p \equiv 1, 2, 4 \pmod{7}$.

6. Tõestada, et kolme mitteruutjäägi korrutis on mitteruutjääk.

7. Olgu $p > 2$ algarv. Tõestada, et ükski ruutjääk mooduli p järgi ei ole algjuur mooduli p järgi.

8. Tõestada, et kui $p > 3$ on algarv, siis kõigi ruutjääkide summa mooduli p järgi jagub arvuga p.

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:

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