Kevad 2015

Arvuteooria 13. praktikumi ülesanded:

Ruutjäägid I.

1. Leida otse, pööratavate elementide ruute järjest välja arvutades, kõik ruutjäägid mooduli 11 järgi.

2. Leida kõik ruutjäägid mooduli 17 järgi Euleri kriteeriumi abil.

3. Leida kõik ruutjäägid mooduli 23 järgi Legendre'i sümboli omaduste abil.

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

a) $x^2 \equiv -1 \pmod{59}$; b) $x^2 \equiv 1 \pmod{61}$;
c) $x^2 \equiv 2 \pmod{59}$; d) $x^2 \equiv -2 \pmod{61}$;
e) $x^2 \equiv -2 \pmod{118}$; f) $x^2 \equiv 2 \pmod{122}$.

5. Tõestada, et kui p on paaritu algarv, siis $\left(\frac{5}{p}\right) = -1$ parajasti siis, kui $p \equiv 2, 3 \pmod{5}$.

6. Olgu p selline algarv, et $p \equiv 3, 5 \pmod{8}$. Tõestada, et $p \mid 2^{\frac{p-1}{2}} + 1$.

7. Tõestada, et kui $p > 5$ on algarv, siis kõigi mitteruutjääkide ruutude summa mooduli p järgi jagub arvuga p.

8. Olgu $p > 5$ algarv. Tõestada, et leiduvad sellised täisarvud k ja l, et k ja $k + 1$ on mõlemad ruutjäägid ning l ja $l + 1$ on mõlemad mitteruutjäägid mooduli p järgi.

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