Kevad 2018

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 29 järgi Euleri kriteeriumi abil.

3. Leida kõik ruutjäägid mooduli 31 järgi Legendre'i sümboli omaduste abil.

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

a) $x^2 \equiv -1 \pmod{41}$; b) $x^2 \equiv -11 \pmod{41}$;
c) $x^2 \equiv 2 \pmod{43}$; d) $x^2 \equiv -12 \pmod{43}$;
e) $x^2 \equiv 2 \pmod{82}$; f) $x^2 \equiv 12 \pmod{86}$.

5. Teha kindlaks, milliste algarvude p korral on p ruutjääk mooduli 11 järgi.

6. Tõestada, et kui a on vähim positiivne mitteruutjääk algarvulise mooduli p järgi, siis $a < \sqrt{p} + 1$.

7. Olgu $p > 5$ algarv. Leida kõigi mitteruutjääkide ruutude summa, arvutatuna mooduli p järgi.

8. Tõestada, et kui täisarv a on ruutjääk kõigi paaritute algarvuliste moodulite järgi, siis a on täisruut.

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 funktsioonina:

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

10**. Tõestada, et arvul $2^{3^n} + 1$ on vähemalt n algtegurit kujul $8k + 3$.