Arvuteooria 13. praktikumi ülesanded:
Ruutjäägid I.

1. Leida otse, pööratavate elementide ruute järjest välja arvutades, kõik ruutjäägid mooduli 13 järgi.

2. Leida kõik ruutjäägid mooduli 11 järgi Euleri kriteeriumi abil.

3. Leida kõik ruutjäägid mooduli 19 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) $x^2 \equiv -1 \pmod{59}$;
c) $x^2 \equiv 2 \pmod{61}$; d) $x^2 \equiv -2 \pmod{59}$;
e) $x^2 \equiv -2 \pmod{122}$; f) $x^2 \equiv -2 \pmod{118}$.

5. Tõestada, et $\left(\frac{-2}{p}\right) = -1$ parajasti siis, kui $p \equiv 5 \pmod 8$ või $p \equiv 7 \pmod 8$.

6. Teha kindlaks (analoogiliselt eelmise ülesandega), milliste algarvude $p > 5$ korral on 5 ruutjääk mooduli p järgi.

7. Tõestada, et kui algarvul p on kuju $p = 4k + 3$ ja $a \in \mathbb{Z} \setminus p\mathbb{Z}$, siis üks arvudest a ja $-a$ on ruutjääk ja teine mitteruutjääk mooduli p järgi.

8. Olgu $p > 2$ algarv ja a algjuur mooduli p järgi. Tõestada, et kõigi mittekongruentsete ruutjääkide korrutis mooduli p järgi on kongruentne arvuga $a^{\frac{p^2-1}{4}} \pmod p$.

9*. Olgu $p > 3$ algarv. Leida kõigi mittekongruentsete ruutjääkide summa mooduli p järgi.