

Arvuteooria 13. praktikumi ülesanded:

Ruutjäägid I.

1. Leida otse, pööratavate elementide ruute järjest välja arvutades, kõik ruutjäägid mooduli 29 järgi.
2. Leida kõik ruutjäägid mooduli 23 järgi Euleri kriteeriumi abil.
3. Leida kõik ruutjäägid mooduli 47 järgi Legendre'i sümboli omaduste abil.
4. Millised järgmistest kongruentsidest on lahenduvad ja mitu lahendit neil on (kui üldse on):

a) $x^2 \equiv -1 \pmod{97}$;	b) $x^2 \equiv 2 \pmod{107}$;
c) $x^2 \equiv -2 \pmod{2006}$;	d) $x^2 \equiv 8 \pmod{2024}$;
e) $x^2 \equiv -8 \pmod{2025}$;	f) $x^2 \equiv 16 \pmod{2028}$.
5. Olgu $p \in \mathbb{P}$. Leida jääk, mis tekib summa $S = \sum_{\substack{0 < a < p \\ \left(\frac{a}{p}\right)=1}} a$ jagamisel arvuga p .
6. Tõestada, et iga $n \in \mathbb{N}$ korral leidub lõpmata palju algarve $p \in \mathbb{P}$ nii, et $1, 2, \dots, n$ on kõik korraka ruutjäägid mooduli p järgi.
7. 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.
8. Olgu $q \in \mathbb{P}$. Tõestada, et leidub $n \in \mathbb{N}$ nii, et kõik algarvud $2 < p \in \mathbb{P}$, mille korral q on ruutjääk mooduli p järgi, saab jaotada mingite $\frac{\varphi(n)}{2}$ erineva aritmeetilise jada (kõik sammuga n) vahel nii, et iga algarv satub täpselt ühte jadasse ja üheski jadas ei ole teisi algarve peale nende, mille korral q on ruutjääk nende kui mooduli järgi.
- 9*. Olgu $p > 2$ algarv. Leida, mitu ruutjääki a mooduli p järgi, kus $0 < a < p$, on sellised, et $a + 1$ on mitteruutjääk.
- 10**. Tõestada, et arvul $2^{3^n} + 1$ on vähemalt n erinevat algtegurit kujul $8k + 3$.