

Arvuteooria 14. praktikumi ülesanded:

Ruutjäägid II.

1. Leida Jacobi sümboli $\left(\frac{7312}{3127}\right)$ väärtus.
2. Leida Gaussi ruutvastavusseaduse abil kõik algarvud p , mille järgi -5 on ruutjääk.
3. Teha kindlaks, kas järgmine ruutkongruents on lahenduv:
a) $x^2 \equiv 123 \pmod{197}$, b) $3x^2 + 6x + 7 \equiv 0 \pmod{97}$.
4. Milliste paaritute naturaalarvude n korral on Jacobi sümboli $\left(\frac{-2}{n}\right)$ väärtus -1 ?
5. Olgu a täisarv ja $n > 1$ naturaalarv, kusjuures $n \equiv 1 \pmod{8}$. Tõestada, et kui $\left(\frac{a}{n}\right) = -1$, siis kongruents $x^2 + 2a \equiv 0 \pmod{n}$ ei ole lahenduv. Kas kehtib ka vastupidine väide?
6. Tõestada, et arvu $n^2 - 2$ paarituarvulised jagajad on kujul $8k \pm 1$.
7. Olgu a algjuur algarvulise mooduli $p > 2$ järgi. Tõestada, et kõik arvud a^{2k+1} , $k \in \mathbb{N} \cup \{0\}$, on mitteruutjäägid mooduli p järgi.
8. Tõestada, et leidub lõpmata palju algarve kujul $8k + 3$. (Vihje: algarvu $p > 2$ korral $\left(\frac{-2}{p}\right) = 1$ parajasti siis, kui $p \equiv 1$ või $p \equiv 3 \pmod{8}$.)
- 9*. Olgu $p > 2$ algarv, n naturaalarv ja $(p, n) = 1$. Leida $\sum_{i=1}^p \left(\frac{i^2+n}{p}\right)$.