

Arvuteooria 13. praktikumi ülesanded

1. Too näide kongruentsist $x^m \equiv b \pmod{n}$, $(b, n) = 1$, mis on lahenduv, kuid lahendite arv ei ole $(m, \varphi(n))$.
2. Leia otse, pööratavate elementide ruute järjest välja arvutades, kõik ruutjäägid mooduli 13 järgi.
3. Leia kõik ruutjäägid mooduli 23 järgi Euleri kriteeriumi abil.
4. Leia kõik ruutjäägid mooduli 19 järgi Legendre'i sümboli omaduste abil.
5. Millised järgmistest kongruentsidest on lahenduvad ja mitu lahendit neil on (kui üldse on):

(a) $x^2 \equiv 1 \pmod{59}$;

(d) $x^2 \equiv 2 \pmod{122}$;

(b) $x^2 \equiv -1 \pmod{61}$;

(e) $x^2 \equiv 7 \pmod{59}$;

(c) $x^2 \equiv -2 \pmod{118}$;

(f) $x^2 \equiv 11 \pmod{61}$;

6. Leia vähim kahekohaline positiivne ruutjääk mooduli 31 järgi.
7. Mitu lahendit on kongruentsil $x^2 - 6x + 7 \equiv 0 \pmod{31}$?
8. Olgu $p > 2$ algarv, $a, b, c \in \mathbb{Z}$ ja $(a, p) = 1$. Tõesta, et kongruentsil

$$ax^2 + bx + c \equiv 0 \pmod{p}$$

on täpselt $\left(\frac{D}{p}\right) + 1$ lahendit, kus $D = b^2 - 4ac$.

9. Olgu $p > 2$ algarv kujul $p = 4k + 1$, kus $k \in \mathbb{N}$. Arvuta

$$\sum_{i=0}^{p-1} \left(\frac{i^i}{p}\right).$$

- 10*. 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 $0 < a < \frac{p}{2}$. Leia järgmiste korrutiste väärtused jäägiklassikorpuses Z_p arvu n kaudu: $A = \overline{1} \cdot \overline{3} \cdot \overline{5} \cdot \dots \cdot \overline{p-2}$ ja $B = \overline{2} \cdot \overline{4} \cdot \overline{6} \cdot \dots \cdot \overline{p-1}$.

- 11**. Milliste a, b, c täisarvuliste väärtuste korral on murru

$$\frac{a^2 + b^2 + c^2}{3(ab + bc + ca)}$$

väärtus samuti täisarv?

1. Näited, mis rahuldavad teoreemi 7.30 eeldusi, kindlasti ei sobi.
2. Ruutjääkide peatüki sissejuhatus.
3. Lause 8.7.
4. Laused 8.7 ja 8.8, teoreem 8.11.
5. Märkus peale definitsiooni 8.1. Lause 8.8 ja teoreem 8.11. Alapeatükk 6.5.
6. Legendre'i sümboli omadused: lause 8.8 ja teoreem 8.11.
7. Teisenda kujule $y^2 \equiv b \pmod{31}$ või kasuta ülesanne 8.
8. Teisenda kujule $y^2 \equiv D \pmod{p}$.
9. Lause 8.8.(3) ja järeldus 8.6.