Arvuteooria 11. praktikumi ülesanded:
Lõplikud korpused I.

1. Tõestada, et kui K on lõplik korpus, siis mistahes elementide $k, l \in K$ ja täisarvude m, n korral $(mn)(kl) = (mk)(nl)$.

2. Tõestada, et polünoom $p(x) = x^2 + 1 \in \mathbb{Z}_7[x]$ on taandumatu üle $\mathbb{Z}_7$.

3. Tuua näide: a) kolmanda astme taandumatust polünoomist üle korpuse $\mathbb{Z}_5$,
   b) neljanda astme taanduvast polünoomist üle korpuse $\mathbb{Z}_5$.

4. Leida kõik ülimalt teise astme taandumatud polünoomid üle korpuse $\mathbb{Z}_3$.

5. Leida 9-elemendilise korpuse

$$\mathbb{F}_9 = \mathbb{Z}_3[x]/\langle x^2 - x + 2\rangle$$

korrutustabel.

6. Leida 9-elemendilise korpuse $\mathbb{F}_9 = \mathbb{Z}_3[x]/\langle x^2 - 2\rangle$ mingi primitiivne element ja selle elemendi astmete esitused polünoomide kujul (nagu tabelis loengukonspekti leheküljel 37).

7. Leida avaldise

$$\left([2x^3 + 2] + [x - 2]^{2013} - [x + 1]\right)\left([x^{33} + 1] + [x^5 + 2x^3 + x]\right)$$

väärtus korpuses $\mathbb{F}_9 = \mathbb{Z}_3[x]/\langle x^2 - 2\rangle$.

8. Tõestada, et iga lõpliku korpuse (välja arvatud $\mathbb{Z}_2$) kõigi elementide summa on 0.

9*. Tõestada, et iga lõpliku korpuse K elemendi k jaoks leiduvad $m, n \in K$ nii, et

$$k = m^2 + n^2.$$