Kevad 2014

Arvuteooria 11. praktikumi ülesanded:

Lõplikud korpused I.

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

2. Tõestada, et polünoom $p(x) = x^2 - x + 1 \in \mathbb{Z}_5[x]$ on taandumatu üle $\mathbb{Z}_5$.

3. Tuua näide: a) kolmanda astme taandumatust polünoomist üle korpuse $\mathbb{Z}_7$,
b) viienda astme taanduvast polünoomist üle korpuse $\mathbb{Z}_3$.

4. Leida kõik ülimalt kolmanda astme taandumatud polünoomid üle $\mathbb{Z}_2$.

5. Leida 25-elemendilise korpuse

$$\mathbb{F}_{25} = \mathbb{Z}_5[x]/\langle x^2 + 2\rangle$$

korrutustabel.

6. Leida 25-elemendilise korpuse $\mathbb{F}_{25} = \mathbb{Z}_5[x]/\langle x^2 - x + 1\rangle$ mingi primitiivne element ja selle elemendi astmete esitused polünoomide kujul (nagu tabelis loengukonspekti leheküljel 37).

7. Leida avaldise

$$\big([2x^2 + 3] + [x + 2]^{2014} - [x + 1]\big)\,\big([x^{17} + 1] + [x^3 + 2x^2 + x]\big)$$

väärtus korpuses $\mathbb{F}_{25} = \mathbb{Z}_5[x]/\langle x^2 - x + 1\rangle$.

8. Tõestada, et iga lõpliku korpuse kõigi nullist erinevate elementide korrutis on -1.

9*. Tõestada, et polünoom $x^4 + 1$ ei ole taandumatu mitte üheski lõplikus korpuses K.