Sügis 2016

Lõplikud korpused I
2. praktikumi ülesanded
Arvutamine lõplikes korpustes. Jälg ja norm.

1. Leida kõik ülimalt neljanda astme taandumatud polünoomid üle $\mathbb{Z}_3$.

2. Leida ringi $\mathbb{Z}_3[x]/(x^3+x^2+1)$ korrutustabel. Kas see ring on korpus?

3. Leida 27-elemendilise korpuse $\mathbb{F}_{27} = \mathbb{Z}_3[x]/(x^3+x^2-1)$ mingi primitiivne element ja selle elemendi astmete esitused polünoomide kujul (nagu tabelis arvuteooria kursuse loengukonspekti leheküljel 59).

4. Leida avaldise

$$\big([x^2+x+2]+[x+2]^{2016}+[2x+3]\big)\cdot\big([x^{19}-2]+[x^3+2x^2+2]\big)$$

väärtus korpuses $\mathbb{F}_{27} = \mathbb{Z}_3[x]/(x^3+x^2-1)$.

5. Leida elementide $[2]$, $[2x]$ ja $[2x^2]$ minimaalsed polünoomid, kaaselemendid, jäljed ja normid üle $\mathbb{F}_3$ korpuses $\mathbb{F}_{27} = \mathbb{Z}_3[x]/(x^3+x^2-1)$.

6. Tõestada, et iga $p \in \mathbb{P}$ ja $n \in \mathbb{N}$ korral $n \mid \varphi(p^n-1)$.

7. Olgu $\mathbb{F}_q = K \leq L = F_{q^n}$ lõplikud korpused. Tõestada, et iga $k \in K$ korral

$$|\{l \in L \mid \mathrm{Tr}_{L/K}(l) = k\}| = q^{n-1}.$$

8. Tõestada, et kui $\mathbb{F}_q = K \leq L$ on lõplikud korpused, siis iga $l \in L$ jaoks $N_{L/K}(l) = \mathbf{1}$ parajasti siis, kui $l = (l')^{q-1}$ mingi $l' \in L$ korral.

9*. Olgu K lõplik korpus, mille karakteristika ei ole 2. Defineerime sümboli

$$\left(\frac{k}{K}\right) = \begin{cases} 1, & \text{kui } k \in K^2 \setminus \{0\} = \{l^2 \mid 0 \neq l \in K\}, \\ -1, & \text{kui } k \notin K^2, \\ 0, & \text{kui } k = \mathbf{0}. \end{cases}$$

Olgu $K \leq L$ korpuse K lõplik laiend. Leida seos $\left(\frac{k}{K}\right)$ ja $\left(\frac{k}{L}\right)$ vahel.