Arvuteooria 6. praktikum
Kevad 2003

1. Tõestada, et mistahes lõpliku korpuse, välja arvatud $\mathbb{F}_2$, korral on kõigi tema elementide summa 0.

2. Vaatleme polünoomi $p(x) = x^2 + 1 \in \mathbb{F}_3[x]$. Tõestada, et p on taandumatu üle $\mathbb{F}_3$. Leida korpuse $\mathbb{F}_9 = \mathbb{F}_3[x]/ < x^2 + 1 >$ korrutustabel.

3. Leida eelmises näites konstrueeritud korpuse $\mathbb{F}_9$ mingi primitiivne element ja selle elemendi astmete esitused polünoomide kujul (nagu tabelis loengukonspekti leheküljel 34).

4. Leida avaldise

$$\left([2x^2 + 1] + [x + 2]^{2003} - [2x + 2]\right)\left([2x^3 + 1] + [x^5 + x^3 + 2x]\right)$$

väärtus korpuses $\mathbb{F}_9 = \mathbb{F}_3[x]/ < x^2 + 1 >$.

5. Leida kõik 3. astme ühejuured korpuses $\mathbb{F}_{19}$. Kas nende hulgas on primitiivseid ühejuuri? Kui jah, siis leida üks neist. Kui palju on korpuses $\mathbb{F}_{19}$ elemente, mis omavad 3. astme juurt?

6. Tõestada, et lõpliku korpuse $\mathbb{F}_{p^n}$ igal elemendil on selles korpuses täpselt üks p. astme juur.

7^{**}. Olgu a ja b korpuse $\mathbb{F}_{2^n}$ elemendid, kusjuures n on paaritu arv. Tõestada, et võrdusest $a^2 + ab + b^2 = 0$ järeldub, et $a = b = 0$.