Kevad 2014

Märkusi arvuteooria 11. praktikumi kohta:

A. Kuna ülesanded olid rasked ja teooria keeruline, siis me tegime 5., 6. ja 7. ülesande näidisvariandid $\mathbb{F}_9$ jaoks praktikumis läbi ja ülesanded 5., 6. ja 7. jäävad 12. praktikumi lisaülesanneteks.

B. Vihje 12. praktikumi ülesannete jaoks: suurem osa neist on tehtavad loengukonspekti teoreemi 8.18 ja järelduse 8.20 põhjal. Kaheksas ülesanne on raskem ja nõuab veidi leidlikkust, aga on sisuliselt järgu mõiste peale.

C. Kommentaare ülesannete kaupa:

1. Seda ülesannet sai tõestada kahel viisil: loengukonspekti omaduste abil:

$$k(n(lm)) = (1k)(n(lm)) = (1n)(k(lm)) = n(k(lm)) = n((kl)m),$$

või eelistatult otse täisarvu ja korpuse elemendi korrutise definitsiooni abil: kui $n \in \mathbb{N}$, siis distributiivsuse tõttu

$$k(n(lm)) = k(\underbrace{lm}_{\text{n}}) = \underbrace{k(lm)}_{\text{n}} = n(k(lm)) = n((kl)m).$$

Kui n=0, siis

$$k(n(lm)) = k(0(lm)) = k\mathbf{0} = \mathbf{0} = 0((kl)m) = n((kl)m).$$

Kui $n < 0$, siis $-n > 0$ ja osa $n > 0$ ning omaduse $k(-l) = -(kl)$ põhjal

$$\begin{aligned} k(n(lm)) &= k((-(-n))(lm)) = k(-((-n)(lm))) = -(k((-n)(lm))) \\ &= -((-n)((kl)m)) = -(-(n((kl)m))) = n((kl)m). \end{aligned}$$

2-4. Ülimalt kolmanda astme polünoomi korral kehtivad järgmised omadused:
1) konstantsed polünoomid ei ole taanduvad ega taandumatud;
2) lineaarpolünoomid on alati taandumatud;
3) teise ja kolmanda astme polünoomid on taandumatud parajasti siis, kui nad ei oma ühtegi juurt, sest taanduvuseks tuleb need tegurdada väiksema astme mittekonstantsete (st. 2. ja 1. astme) polünoomide korrutisena, ja kuna (üle korpuse!) korrutamisel polünoomide astmed liituvad, siis peab vähemalt

üks tegur olema 1. astme polünoom (kas $2 = 1 + 1$ teise astme korral, või $3 = 2+1 = 1+2$ kolmanda astme korral). Aga lineaarteguri $ax+b$ olemasolu annab meile juure $-a^{-1}b$ ($a \neq 0$!).

8. Ülesanne tuli viia üle tärnülesandeks. Aga lahendusidee on sama, mis jäägiklassikorpuse $\mathbb{Z}_p$ korral: igal ühikelemendist ja ühikelemendi vastandelemendist erineval pööratava elemendil on temast erinev pöördelement (vastasel juhul $a = a^{-1}$, $a^2 = 1$ ja 2. astme polünoomil $x^2 - 1$ on 3 juurt, $\mathbf{1}$, $-\mathbf{1}$ ja a, mis on vastuolus lausega 2.9.) Seega kõigi pööratavate, st. nullist erinevate elementide korrutises on hulk paare $aa^{-1} = \mathbf{1}$, ning veel tegurid $\mathbf{1}$ ja $-\mathbf{1}$ (juhul $\operatorname{char} K = 2$ $-\mathbf{1} = \mathbf{1}$ ja on vaid tegur $\mathbf{1}$). Järelikult terve korrutis on võrdne elemendiga $\mathbf{1}(-\mathbf{1}) = -\mathbf{1}$.