Kevad 2014

Märkusi arvuteooria 12. praktikumi kohta:

A. Ülesanded 4. ja 8. jäävad 13. praktikumi lisaülesanneteks.

B. Kommentaare ülesannete kaupa:

1. Ühejuuri saab leida loengukonspekti teoreemi 8.18 1) abil. Selleks on vaja leida üks primitiivne element ($\mathbb{Z}_{29}$ korral on selleks algjuur mooduli 29 järgi, näiteks 2), kasutades järeldust 7.20 (või 7.21, kui tegu on jäägiklassikorpusega). Siis 8. astme ühejuured on kujul 2^k, kus $28 \mid 8k$ ehk $7|k$ ehk $k = 7, 14, 21, 28$. Järelikult 8. astme ühejuured on $2^7 \equiv 12, 2^{14} \equiv 28, 2^{21} \equiv 17, 2^{24} \equiv 1 \pmod{29}$. Sellest EI PIISA, kui lihtsalt kirjutada, et $a^7, a^{14}, a^{21}, a^{28}$ ilma primitiivset elementi a leidmata.

2. n. astme juurt omavate elementide arvu saab leida teoreemi 8.18 4) abil: selleks on $\frac{q-1}{(n,q-1)}$, kus q on korpuse elementide arv, antud juhul 29. Ülesande a) osas on seega vaja $\frac{28}{(28,7)} = 4$ elementi. Kõik need elemendid saab leida, kui järjest välja arvutada kõik 7-dad astmed, antud juhul $1^7 = 1, 2^7 \equiv 12 \equiv 3^7, 4^7 \equiv 28, 27^7 \equiv (-2)^7 \equiv -12 \equiv 17$ jne., ja lõpetada, kui 4 erinevat astet on käes (1, 12, 17, 28 ongi otsitavad). Aga kindlam ja rohkem informatsiooni andev viis on kasutada loengukonspekti näidet 8.24.

Üks oluline märkus, millele ma ise loengus unustasin tähelepanu juhtida on see, et elemendil $\mathbf{0}$ on alati olemas mistahes astme juur: $\mathbf{0}^n = \mathbf{0}$. Seepärast ma nulli väljajätmist veaks ei lugenud, aga edaspidiseks tasub see fakt meelde jätta.

Viimaks, see ülesanne oli osaliselt lihtsamini lahendatav, kui kaks korda järjest näidet 8.24 rakendada. Nimelt, kui me a) osast teame kõigi 7. astme ühejuurte rühma $H_7 = \{\overline{1}, \overline{7}, \overline{16}, \overline{20}, \overline{23}, \overline{24}, \overline{25}\}$, siis me teame ka kõiki 8. astme juurt omavaid elemente: kui $a = b^8$, siis $a^7 = (b^8)^7 = b^{56} = (b^{28})^2 = \mathbf{1}^2 = \mathbf{1}$. Seega b) osas otsitavad elemendid on tegelikult (osa) 7. astme ühejuurtest, aga kuna neid peab olema $\frac{28}{(28,8)} = 7$ tükki ja $|H_7| = 7$, siis on vastuseks terve H_7 ning me ei pea enam hakkama 8. astme ühejuuri ja kõrvalklasse leidma.

3. Nagu 1. ülesandes, saab lahendamiseks kasutada teoreemi 8.18 osa 1) ja järeldust 7.20. Siin võib alternatiivina kasutada ka korrutustabelit (mille me leidsime eelmise praktikumi 5. ülesandes), aga parem meetod on korrata 11. praktikumi 6. ülesannet ja leida primitiivne element (näiteks $[x+1]$) ning vastav tabel polünoomesituste jaoks.

Juhin tähelepanu sellele, et n. astme ühejuurte rühm on alati tsükliline ja primitiivse elemendi olemasolu on tegelikult samaväärne sellega, et $|H_n| = n$. Kui $|H_n|$ on algarv, siis muuseas on kõik ühest erinevad n. astme ühejuured primitiivsed, sest nende järk peab olema algarvu $|H_n|$ jagaja ja ei saa olla 1.

5. Otsitavad korpused on $\mathbb{F}_2, \mathbb{F}_4, \mathbb{F}_5, \mathbb{F}_9, \mathbb{F}_{13}, \mathbb{F}_{16}, \mathbb{F}_{17}, \mathbb{F}_{19}, \mathbb{F}_{25}, \mathbb{F}_{29}, \mathbb{F}_{32}$. Välistada tuleb need elementide arvud, mis ei ole algarvu astmed (teoreem 8.5) ja need, mis annavad neljaga jagades jäägi 3 (järeldus 8.20 ning märkus 8.21).

6. Osutus *-ülesandeks. Midagi keerulist siin küll ei olnud. Teoreem 8.18 4) põhjal $(|K| - 1, 256) = 1$, mistõttu $|K| - 1$ on paaritu ja $|K| = 2^k$ mingi $k \in \mathbb{N}$ korral. Aga siis $\operatorname{char} K = 2$.

7. Osutus samuti *-ülesandeks. Aga lahendus on lihtne, kui panna kokku teoreem 8.18 ja lause 7.23: ülesande eeldustel on H_n n-elemendiline tsükliline rühm, mille moodustajaid (ehk primitiivseid n. astme ühejuuri) on kokku $\varphi(n)$ tükki.