Kodutöö nr. 5

Joosep Näks ja Uku Hannes Arismaa

1. Koostada ringi $\mathbb{Z}_{15}$ korrutustabel ilma **kõiki** korrutisi välja arvutamata.

Kuna ringis $\mathbb{Z}_{15}$ on korrutamine kommutatiivne ning kahe elemendi vastandelementide korrutis on sama, mis elmenetide oma, ning elemendi korrutised vastand elemendiga, on samad, mis elemendi endaga, ainult vastandmärgilised, saame välja kirjutada järgmise osa (jäägiklasside korrutus-) tabelist.

	1	2	3	4	5	6	7
1	1	2	3	4	5	6	7
2		4	6	-7	-5	-3	-1
3			-6	-3	0	3	6
4				1	5	-6	-2
5					-5	0	5
6						6	-3
7							4

Täis tabeli saab antud tabeli peegeldamisel parema ääre suhtes kõiki elemente -1ga korrutades ning seejärel saadud kumbagi diagonaali mööda peegeldades.

2. Leida kõik ringi $\mathbb{Z}_{28}$ pööratavad elemendid.

Teoreem 4.10 põhjal on $\mathbb{Z}_{28}$ ringi pööratavate elementide hulk $\{\overline{a} \in \mathbb{Z}_{28} \mid (a, 28) = 1\}$. Seega on pööratavad elemendid kõik elemendid, mis ei oma arvuga 28 ühistegureid. 28 algtegurid on 2 ja 7 ehk ainsad elemendid, mis omavad arvuga 28 ühistegureid on 2 ja 7 kordsed arvud, kui need välja jätta, jäävad alles elemendid $\{\overline{1}, \overline{3}, \overline{5}, \overline{9}, \overline{11}, \overline{13}, \overline{15}, \overline{17}, \overline{19}, \overline{23}, \overline{25}, \overline{27}\}$, mis ongi kõik pööratavad elemendid.

3. Leida elementide $\overline{12}$, $\overline{13}$, $\overline{14}$, $\overline{15}$, $\overline{20}$, $\overline{21}$ ja $\overline{22}$ vastandelemendid ning (kui need on olemas) pöördelemendid ringis $\mathbb{Z}_{336}$.

Vastandelemndid on $\overline{-12}$, $\overline{-13}$, $\overline{-14}$, $\overline{-15}$, $\overline{-20}$, $\overline{-21}$, $\overline{-22}$. Kuna 12, 14, 15, 0, 21 ja 22 omavad 336ga ühest suuremat ühiskordset, siis neil pöördelemente pole. $\overline{13}$ pöördelemendi leiame Eukleidese algoritmiga.

336	1	0
13	0	1
11	1	-25
2	-1	26
1	6	-155

Seega saime, et $\overline{13}$ pöördelement on $\overline{-155}$.

4. Leida **mõlema** ringi $\mathbb{Z}_{24}$ ja $\mathbb{Z}_8 \times \mathbb{Z}_3$ jaoks kõik pööratavad elemendid ning kõik nullitegurid koos vastavate nulli tegurdustega (st. nulliteguri a jaoks tuleb leida b nii, et $ab = 0$). Kas ringid $\mathbb{Z}_{24}$ ja $\mathbb{Z}_8 \times \mathbb{Z}_3$ on isomorfsed? Miks?

Teoreem 4.10 põhjal on $\mathbb{Z}_{24}$ ringi pööratavate elementide hulk $\{\overline{a} \in \mathbb{Z}_{24} \mid (a, 24) = 1\}$. Seega on pööratavad elemendid kõik elemendid, mis ei oma arvuga 24 ühiseid tegureid. 24 algtegurid on 2 ja 3 ehk ainsad elemendid, mis omavad arvuga 24 ühiseid tegureid on 2 ja 3 kordsed arvud, kui need välja jätta, jäävad alles $\{\overline{1}, \overline{5}, \overline{7}, \overline{11}, \overline{13}, \overline{17}, \overline{19}, \overline{23}\}$, mis ongi kõik pööratavad elemendid.
Kuna $(8, 3) = 1$ ja $8 \cdot 3 = 24$, on teoreemi 4.5 eeldused täidetud ehk $\mathbb{Z}_{24}$ ja $\mathbb{Z}_8 \times \mathbb{Z}_3$ on isomorfsed.
Nende isomorfsuse tõttu on ka nende pööratavad elemendid samad, ehk $\mathbb{Z}_8 \times \mathbb{Z}_3$ pööratavad elemendid on $\{(\overline{1}, \overline{1}), (\overline{5}, \overline{2}), (\overline{7}, \overline{1}), (\overline{3}, \overline{2}), (\overline{5}, \overline{1}), (\overline{1}, \overline{2}), (\overline{3}, \overline{1}), (\overline{7}, \overline{2})\}$.

5. Leida ringi $\mathbb{Z}_6 \times \mathbb{Z}_4$ kõik pööratavad elemendid. Kas ringid $\mathbb{Z}_{24}$ ja $\mathbb{Z}_6 \times \mathbb{Z}_4$ on isomorfsed? Põhjendada vastust.

Element saab olla pööratav parajasti siis, kui $\mathbb{Z}_6$ ja $\mathbb{Z}_4$ osad on mõlemad pööratavad, vastasel juhul ei saa ühte nendest vastava ringi ühikelemendiks muuta. $\mathbb{Z}_6$ pööratavad elemendid on $\overline{1}$, $\overline{5}$, jäägiklassis $\mathbb{Z}_4$ $\overline{1}$ ja $\overline{3}$. Seega on $\mathbb{Z}_6 \times \mathbb{Z}_4$ pööratavd elemendid ($\overline{1}$, $\overline{1}$),($\overline{1}$, $\overline{3}$),($\overline{5}$, $\overline{1}$),($\overline{5}$, $\overline{3}$). Need pole isomorfsed, kuna isomorfism peab ühikelemendi ühikelemendiks teisendama ning ühikelemendile iseennast 12 korda liites saame jääägiklassis $\mathbb{Z}_{24}$ $\overline{13}$ ning $\mathbb{Z}_6 \times \mathbb{Z}_4$s ($\overline{1}$,$\overline{1}$), mis on juba oli esialgne ühikelement, seega pole teisendus injektiivne, seega pole ka isomorfism.

6. Tõestada, et ringi $\mathbb{Z}_n$ ei ole võimalik isegi osaliselt järjestada nii, et tekkiv järjestus oleks liitmisega kooskõlas (va triviaalne järjestus ehk võrdusseos).

Võtan kaks arvu $\overline{a}$ ja $\overline{b}$ nii et $\overline{a} < \overline{b}$ ja $\overline{a} \neq \overline{b}$. Kui võrratuses mõlemale poolele liita $\overline{b-a}$, saab et $\overline{b} < \overline{2b-a}$. Kui seda sama suurust mõlemale poole liita $n-1$ korda ning kõik võrratused transitiivsusega üksteise otsa panna, saab $\overline{a} < \overline{b} < \overline{2b-a} < .. < \overline{b+(n-1)(b-a)} = \overline{b-b+a+n(b-a)} = \overline{a}$ ehk $\overline{a} < \overline{a}$, mis on vastuolu. Seega ei saa jäägiklassi võimalik järjestada.

7. Jäägiklassiringi $\mathbb{Z}_n$ elementi $\overline{m}$ nimetatakse *idempotentseks* või *idempotendiks*, kui $\overline{m}^2 = \overline{m}$. Leida ringi $\mathbb{Z}_n$ idempotentide arv.

Vaadates isomorfset ringi, mis koosneb $\mathbb{Z}_{p^k}$de otsekorrutisest, kus p^k on n algtegurduses olev algarvu aste, saame, et element on idempotentne esialgses ringis parajasti siis, kui temale vastava otsekorrutise iga liige on vastavas jäägiklassiringis ka idempotentne. Vastasel juhul vähemalt ühe jäägiklassiringi element muutuks ruutu võttes ning seega ka kogu arv, kuna muidu poleks see otsekorrutis algse jäägiklassiringiga isomorfne.

Igas otsekorrutise osas saab see olla kas vastava jäägiklassiringi null- või ühikelement. Vastasel juhul mingi $\mathbb{Z}_{p^k}$ korral leidub mingi muu idempotentne element, mille puhul kehtib, et $\overline{m}^2 = \overline{m}$, kust ringi omadusi kasutades saame $(\overline{m} - \overline{1})\overline{m} = \overline{0}$. See aga tähendaks, et korrutis peab jaguma p^kga. Seega peab seda tegema ka kas m või $m-1$ (kuni kumbki 0 pole), kuna iga jagaja puhul (peale 1) annavad need erineva jäägi, annavad need ka erineva jäägi $p$ga jagades, seega saab ainult üks jaguda p ning seega p^kga, mis on aga võimatu, sest valides esindajad $0 \leq m < p^k$ on kõik m liiga väiksed, et jaguda p^kga.

Seega saab idempotentsele elemendile vastava otsekorrutise iga liiga olla kas $\overline{0}$ või $\overline{1}$, seega iga algtegurduses esineva algarvu kohta lisandub uus liige ning võimaluste arv kahekordistub. Seega, kui nl on x unikaalset algtegurit, siis on $\mathbb{Z}_n$s 2^x idempotentset elementi.

8. Leida ringi $\mathbb{Z}_n$ kõigi **mitte**pööratavate elementide summa.

Märkan, et element $\overline{-1}$ on alati pööratav, kuna teda iseendaga korrutades saab $\overline{1}$. Samuti kui mingi element $\overline{a} \in \mathbb{Z}_n$ on pööratav, siis on ka tema vastandelement pööratav, sest $\overline{a}^{-1} \cdot \overline{-1}^{-1} = (\overline{a} \cdot \overline{-1})^{-1} = \overline{-a}^{-1}$. See aga tähendab, et kui element on mittepööratav, siis tema vastandelement on ka mittepööratav, ning kuna elemendi ja tema vastandelemendi summa on 0, on seega kõigi endast erineva vastandelemendiga mittepööratavate elementide summa 0. Erandiks on paarisarvulised n väärtused, kus on element $\frac{n}{2}$, mis on ise enda vastandelement. See element on ka alati pööratav kui $n > 2$, kuna teoreemi 4.10 järgi on mittepööratavad elemendid elemendid, mis omavad arvuga n suurimat ühistegurit, mis erineb ühest, ning kuna $2 \cdot \frac{n}{2} = n$, siis $\frac{n}{2} \mid n$ ehk $(\frac{n}{2}, n) = \frac{n}{2}$ ja see on 1 vaid juhul kui $n = 2$.
Seega on $n = 2$ ja paarituarvuliste n väärtuste puhul summaks 0 ning paarisarvuliste n väärtuste puhul on summaks $\frac{n}{2}$.