Arvuteooria

Kevad 2020

5. praktikumi näidislahendused

1. ülesanne (Erki Külaots)

Koostame ringi $\mathbb{Z}_{12}$ korrutustabeli

$\mathbb{Z}_{12}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$	$\overline{7}$	$\overline{8}$	$\overline{9}$	$\overline{10}$	$\overline{11}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$	$\overline{7}$	$\overline{8}$	$\overline{9}$	$\overline{10}$	$\overline{11}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{4}$	$\overline{6}$	$\overline{8}$	$\overline{10}$	$\overline{0}$	$\overline{2}$	$\overline{4}$	$\overline{6}$	$\overline{8}$	$\overline{10}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{6}$	$\overline{9}$	$\overline{0}$	$\overline{3}$	$\overline{6}$	$\overline{9}$	$\overline{0}$	$\overline{3}$	$\overline{6}$	$\overline{9}$
$\overline{4}$	$\overline{0}$	$\overline{4}$	$\overline{8}$	$\overline{0}$	$\overline{4}$	$\overline{8}$	$\overline{0}$	$\overline{4}$	$\overline{8}$	$\overline{0}$	$\overline{4}$	$\overline{8}$
$\overline{5}$	$\overline{0}$	$\overline{5}$	$\overline{10}$	$\overline{3}$	$\overline{8}$	$\overline{1}$	$\overline{6}$	$\overline{11}$	$\overline{4}$	$\overline{9}$	$\overline{2}$	$\overline{7}$
$\overline{6}$	$\overline{0}$	$\overline{6}$	$\overline{0}$	$\overline{6}$	$\overline{0}$	$\overline{6}$	$\overline{0}$	$\overline{6}$	$\overline{0}$	$\overline{6}$	$\overline{0}$	$\overline{6}$
$\overline{7}$	$\overline{0}$	$\overline{7}$	$\overline{2}$	$\overline{9}$	$\overline{4}$	$\overline{11}$	$\overline{6}$	$\overline{1}$	$\overline{8}$	$\overline{3}$	$\overline{10}$	$\overline{5}$
$\overline{8}$	$\overline{0}$	$\overline{8}$	$\overline{4}$	$\overline{0}$	$\overline{8}$	$\overline{4}$	$\overline{0}$	$\overline{8}$	$\overline{4}$	$\overline{0}$	$\overline{8}$	$\overline{4}$
$\overline{9}$	$\overline{0}$	$\overline{9}$	$\overline{6}$	$\overline{3}$	$\overline{0}$	$\overline{9}$	$\overline{6}$	$\overline{3}$	$\overline{0}$	$\overline{9}$	$\overline{6}$	$\overline{3}$
$\overline{10}$	$\overline{0}$	$\overline{10}$	$\overline{8}$	$\overline{6}$	$\overline{4}$	$\overline{2}$	$\overline{0}$	$\overline{10}$	$\overline{8}$	$\overline{6}$	$\overline{4}$	$\overline{2}$
$\overline{11}$	$\overline{0}$	$\overline{11}$	$\overline{10}$	$\overline{9}$	$\overline{8}$	$\overline{7}$	$\overline{6}$	$\overline{5}$	$\overline{4}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

2. ülesanne (Rainer Bõkov)

Kõigepealt teeme Euleri funktsiooni($\varphi(n) = |U(\mathbb{Z}_n)|$) ja teoreemi 5.8 abiga selgeks, et pööratavaid elemente ringis $\mathbb{Z}_{36}$ on $\varphi(36) = \varphi(2^2 * 3^2) = 2 \cdot 3 \cdot 1 \cdot 2 = 12$.
Teoreemi 4.10 põhjal on ringi $\mathbb{Z}_{36}$ pööratavate elementide hulk

$$U(\mathbb{Z}_{36}) = \{\overline{a} \in \mathbb{Z}_{36} | (a,36) = 1\} = \{\overline{1},\overline{5},\overline{7},\overline{11},\overline{13},\overline{17},\overline{19},\overline{23},\overline{25},\overline{29},\overline{31},\overline{35}\}.$$

Kuna tingimuseks oli, et $(a,36 = 2^2 \cdot 3^2) = 1$, siis a-ks sobivad sellised arvud, mis ei jagu kahe ega kolmega.

3. ülesanne (Mikael Raihhelgauz)

Vastandelementide paarid on

$$(\overline{12},\overline{219}),(\overline{13},\overline{218}),(\overline{14},\overline{217}),(\overline{15},\overline{216}),(\overline{16},\overline{215}),(\overline{17},\overline{214}),(\overline{18},\overline{213}).$$

Paneme tähele, et $231 = 3 \cdot 7 \cdot 11$. Leiame pööratavate elementide pöördelemendid.

- Kuna (12,231) = 3, siis $\overline{12}$ ei ole pööratav.
- (13,231) = 1, seega $\overline{13}$ on pööratav. Peame lahendama kongruentsi $13x \equiv 1 \mod 231$. Selleks vaatleme kongruentse

  $$\begin{aligned} 13x &\equiv 1 \mod 3, \\ 13x &\equiv 1 \mod 7, \\ 13x &\equiv 1 \mod 11. \end{aligned}$$

  Igaüks neist on üheselt lahenduv ja lahendid on vastavalt 1, 6 ja 6. Järgnevalt kasutame tähistusi nagu teoreemis 6.6. Märkame, et $m_1 = 77$, $m_2 = 33$ ja $m_3 = 21$. Vastavalt

  $$\overline{k_1} = \overline{77}^{-1} = \overline{2}^{-1} = \overline{2} \text{ (ringis } \mathbb{Z}_3),$$
  $$\overline{k_2} = \overline{33}^{-1} = \overline{5}^{-1} = \overline{3} \text{ (ringis } \mathbb{Z}_7), \overline{k_3} = \overline{21}^{-1} = \overline{10}^{-1} = \overline{10} \text{ (ringis } \mathbb{Z}_{11}).$$

  Niisiis, $x = 1 \cdot 77 \cdot 2 + 6 \cdot 33 \cdot 3 + 6 \cdot 21 \cdot 10 = 2008 \equiv 160 \mod 231$.
- (14,231) = 7, seega $\overline{14}$ pole pööratav.
- (15,231) = 3, seega $\overline{15}$ pole pööratav.
- (16,231) = 1, seega $\overline{16}$ on pööratav. Vaatleme kongruentse

  $$\begin{aligned} 16x &\equiv 1 \mod 3, \\ 16x &\equiv 1 \mod 7, \\ 16x &\equiv 1 \mod 11. \end{aligned}$$

  Lahendid on vastavalt 1, 4 ja 9. Järelikult $x = 1 \cdot 77 \cdot 2 + 4 \cdot 33 \cdot 3 + 9 \cdot 21 \cdot 10 = 2440 \equiv 130 \mod 231$.
- (17,231) = 1, seega $\overline{17}$ on pööratav. Vaatleme kongruentse

  $$\begin{aligned} 17x &\equiv 1 \mod 3, \\ 17x &\equiv 1 \mod 7, \\ 17x &\equiv 1 \mod 11. \end{aligned}$$

  Lahendid on vastavalt 2, 5 ja 2. Niisiis $x = 2 \cdot 77 \cdot 2 + 5 \cdot 33 \cdot 3 + 2 \cdot 21 \cdot 10 = 1223 \equiv 68 \mod 231$.
- (18,231) = 3, seega $\overline{18}$ pole pööratav.

4. ülesanne (Maret Sõmer)

Leian ringi $\mathbb{Z}_{40}$ pööratavad elemendid. Kasutan teoreemi 4.10, mis ütleb, et element $\overline{a} \in \mathbb{Z}_n$ pööratav parajasti siis, kui $(a,n) = 1$. Kuna $40 = 2^3 \cdot 5$, siis $(a,40) = 1$ ehk $\overline{a} \in U(\mathbb{Z}_{40})$ parajasti siis, kui $2 \nmid a$ ja $5 \nmid a$. Seega
$U(\mathbb{Z}_{40}) = \{\overline{1}, \overline{3}, \overline{7}, \overline{9}, \overline{11}, \overline{13}, \overline{17}, \overline{19}, \overline{21}, \overline{23}, \overline{27}, \overline{29}, \overline{31}, \overline{33}, \overline{37}, \overline{39}\}$.
Analoogselt leian ka $U(\mathbb{Z}_5)$ ja $U(\mathbb{Z}_8)$.
$U(\mathbb{Z}_5) = \{\overline{1}, \overline{2}, \overline{3}, \overline{4}\}, \qquad U(\mathbb{Z}_8) = \{\overline{1}, \overline{3}, \overline{5}, \overline{7}\}$.
Lause 5.6 ütleb, et mistahes ringide $R_1, ..., R_s$ korral $U(R_1 \times ... \times R_s) = U(R_1) \times ... \times U(R_s)$.
Sellest järeldub, et $U(\mathbb{Z}_5 \times \mathbb{Z}_8) = \{(\overline{1}, \overline{1}), (\overline{1}, \overline{3}), (\overline{1}, \overline{5}), (\overline{1}, \overline{7}), (\overline{2}, \overline{1}), (\overline{2}, \overline{3}), (\overline{2}, \overline{5}), (\overline{2}, \overline{7}), (\overline{3}, \overline{1}),$
$(\overline{3}, \overline{3}), (\overline{3}, \overline{5}), (\overline{3}, \overline{7}), (\overline{4}, \overline{1}), (\overline{4}, \overline{3}), (\overline{4}, \overline{5}), (\overline{4}, \overline{7})\}$.

Lause 4.15 ütleb, et iga jäägiklassiringi $\mathbb{Z}_n$ element on kas $\overline{0}$, nullitegur või pööratav element. See tähendab, et jäägiklassiringi $\mathbb{Z}_{40}$ nullitegurite hulk on $\mathbb{Z}_{40} \setminus \{\{\overline{0}\} \cup U(\mathbb{Z}_{40})\}$ ning ringi $\mathbb{Z}_5 \times \mathbb{Z}_8$ nullitegurite hulk on $\mathbb{Z}_5 \times \mathbb{Z}_8 \setminus \{\{\overline{0}\} \cup U(\mathbb{Z}_5 \times \mathbb{Z}_8)\}$.

$\mathbb{Z}_{40}$ nullitegurid:
$\overline{2}$, kuna $\overline{2} \cdot \overline{20} = \overline{0}$
$\overline{4}$, kuna $\overline{4} \cdot \overline{10} = \overline{0}$
$\overline{5}$, kuna $\overline{5} \cdot \overline{8} = \overline{0}$
$\overline{6}$, kuna $\overline{6} \cdot \overline{20} = \overline{0}$
$\overline{8}$, kuna $\overline{8} \cdot \overline{5} = \overline{0}$
$\overline{10}$, kuna $\overline{10} \cdot \overline{4} = \overline{0}$
$\overline{12}$, kuna $\overline{12} \cdot \overline{10} = \overline{0}$
$\overline{14}$, kuna $\overline{14} \cdot \overline{20} = \overline{0}$
$\overline{15}$, kuna $\overline{15} \cdot \overline{8} = \overline{0}$
$\overline{16}$, kuna $\overline{16} \cdot \overline{5} = \overline{0}$
$\overline{18}$, kuna $\overline{18} \cdot \overline{20} = \overline{0}$
$\overline{20}$, kuna $\overline{20} \cdot \overline{2} = \overline{0}$
$\overline{22}$, kuna $\overline{22} \cdot \overline{20} = \overline{0}$
$\overline{24}$, kuna $\overline{24} \cdot \overline{5} = \overline{0}$
$\overline{25}$, kuna $\overline{25} \cdot \overline{8} = \overline{0}$
$\overline{26}$, kuna $\overline{26} \cdot \overline{20} = \overline{0}$
$\overline{28}$, kuna $\overline{28} \cdot \overline{10} = \overline{0}$
$\overline{30}$, kuna $\overline{30} \cdot \overline{4} = \overline{0}$
$\overline{32}$, kuna $\overline{32} \cdot \overline{5} = \overline{0}$
$\overline{34}$, kuna $\overline{34} \cdot \overline{20} = \overline{0}$
$\overline{35}$, kuna $\overline{35} \cdot \overline{8} = \overline{0}$
$\overline{36}$, kuna $\overline{36} \cdot \overline{10} = \overline{0}$
$\overline{38}$, kuna $\overline{38} \cdot \overline{20} = \overline{0}$

$\mathbb{Z}_5 \times \mathbb{Z}_8$ nullitegurid:
$(\overline{0}, \overline{1})$, kuna $(\overline{0}, \overline{1}) \cdot (\overline{1}, \overline{0}) = (\overline{0}, \overline{0})$
$(\overline{0}, \overline{2})$, kuna $(\overline{0}, \overline{2}) \cdot (\overline{1}, \overline{0}) = (\overline{0}, \overline{0})$
$(\overline{0}, \overline{3})$, kuna $(\overline{0}, \overline{3}) \cdot (\overline{1}, \overline{0}) = (\overline{0}, \overline{0})$
$(\overline{0}, \overline{4})$, kuna $(\overline{0}, \overline{4}) \cdot (\overline{1}, \overline{0}) = (\overline{0}, \overline{0})$

$(\overline{0},\overline{5})$, kuna $(\overline{0},\overline{5})\cdot(\overline{1},\overline{0})=(\overline{0},\overline{0})$
$(\overline{0},\overline{6})$, kuna $(\overline{0},\overline{6})\cdot(\overline{1},\overline{0})=(\overline{0},\overline{0})$
$(\overline{0},\overline{7})$, kuna $(\overline{0},\overline{7})\cdot(\overline{1},\overline{0})=(\overline{0},\overline{0})$
$(\overline{1},\overline{0})$, kuna $(\overline{1},\overline{0})\cdot(\overline{0},\overline{1})=(\overline{0},\overline{0})$
$(\overline{1},\overline{2})$, kuna $(\overline{1},\overline{2})\cdot(\overline{0},\overline{4})=(\overline{0},\overline{0})$
$(\overline{1},\overline{4})$, kuna $(\overline{1},\overline{4})\cdot(\overline{0},\overline{2})=(\overline{0},\overline{0})$
$(\overline{1},\overline{6})$, kuna $(\overline{1},\overline{6})\cdot(\overline{0},\overline{4})=(\overline{0},\overline{0})$
$(\overline{2},\overline{0})$, kuna $(\overline{2},\overline{0})\cdot(\overline{0},\overline{1})=(\overline{0},\overline{0})$
$(\overline{2},\overline{2})$, kuna $(\overline{2},\overline{2})\cdot(\overline{0},\overline{4})=(\overline{0},\overline{0})$
$(\overline{2},\overline{4})$, kuna $(\overline{2},\overline{4})\cdot(\overline{0},\overline{2})=(\overline{0},\overline{0})$
$(\overline{2},\overline{6})$, kuna $(\overline{2},\overline{6})\cdot(\overline{0},\overline{4})=(\overline{0},\overline{0})$
$(\overline{3},\overline{0})$, kuna $(\overline{3},\overline{0})\cdot(\overline{0},\overline{1})=(\overline{0},\overline{0})$
$(\overline{3},\overline{2})$, kuna $(\overline{3},\overline{2})\cdot(\overline{0},\overline{4})=(\overline{0},\overline{0})$
$(\overline{3},\overline{4})$, kuna $(\overline{3},\overline{4})\cdot(\overline{0},\overline{2})=(\overline{0},\overline{0})$
$(\overline{3},\overline{6})$, kuna $(\overline{3},\overline{6})\cdot(\overline{0},\overline{4})=(\overline{0},\overline{0})$
$(\overline{4},\overline{0})$, kuna $(\overline{4},\overline{0})\cdot(\overline{0},\overline{1})=(\overline{0},\overline{0})$
$(\overline{4},\overline{2})$, kuna $(\overline{4},\overline{2})\cdot(\overline{0},\overline{4})=(\overline{0},\overline{0})$
$(\overline{4},\overline{4})$, kuna $(\overline{4},\overline{4})\cdot(\overline{0},\overline{2})=(\overline{0},\overline{0})$
$(\overline{4},\overline{6})$, kuna $(\overline{4},\overline{6})\cdot(\overline{0},\overline{4})=(\overline{0},\overline{0})$

Ringid $\mathbb{Z}_{40}$ ja $\mathbb{Z}_5\times\mathbb{Z}_8$ on isomorfsed, kuna 5,8 $\in\mathbb{N}$; (5,8) = 1 ja $40=5\cdot 8$ ning teoreem 4.5 ütleb, et kui arvud n_1,...,$n_s\in\mathbb{N}$ on paarikaupa ühistegurita ja $n=n_1\cdot\ldots\cdot n_s$, siis ringid $\mathbb{Z}_n$ ja $\mathbb{Z}_{n_1}\times\ldots\times\mathbb{Z}_{n_s}$ on isomorfsed.

5. ülesanne (Mikael Raihhelgauz)

Kõigepealt leiame ringi $\mathbb{Z}_4$ pööratavad elemendid. Et $4=2^2$ siis nendeks on parajasti kõik paaritud elemendid: $U(\mathbb{Z}_4)=\{\overline{1},\overline{3}\}$. Nüüd leiame $\mathbb{Z}_8$ pööratavad elemendid. Et $8=2^3$, siis nendeks on samuti kõik paaritud jäägiklassid: $U(\mathbb{Z}_8)=\{\overline{1},\overline{3},\overline{5},\overline{7}\}$. Lause 5.6 põhjal seega

$$U(\mathbb{Z}_4\times\mathbb{Z}_8)=\{(1,1),(1,3),(1,5),(1,7),(3,1),(3,3),(3,5),(3,7)\}.$$

Paneme tähele, et rühmas $U(\mathbb{Z}_4\times\mathbb{Z}_8)$ on 8 elementi. Ühtlasi paneme tähele, et $32=2^5$, seega rühm $U(\mathbb{Z}_{32})$ sisaldab kõiki ringi $\mathbb{Z}_{32}$ paarituid elemente, mida on kokku 16. Oletame nüüd, et ringid $\mathbb{Z}_{32}$ ja $\mathbb{Z}_4\times\mathbb{Z}_8$ on isomorfsed. Lause 4.8 põhjal leidub bijektsioon $f:\mathbb{Z}_{32}\to\mathbb{Z}_4\times\mathbb{Z}_8$ nii, et $f(U(\mathbb{Z}_{32}))\subset U(\mathbb{Z}_4\times\mathbb{Z}_8)$. See ei ole aga võimalik, sest f injektiivsuse tõttu on vasakpoolses hulgas 16 elementi. Järelikult ringid ei ole isomorfsed.

Lauri Tart: Siin oleks optimaalne tegelikult viidata järeldusele 4.9, sest isomorfsete rühmade võimsused on alati samad.

6. ülesanne (Lauri Tart)

Sellele ülesandele ei andnud peaaegu keegi **täiesti** õiget lahendust. Rasmus Borni oma oli kõige lähedasem. Toon siinkohal ära lühema sarnase lahenduse.

- Olgu meil aritmeetiline jada $\overline{a} + k\overline{b}$, $k \in \mathbb{N} \cup \{0\}$. Siis

  $$\overline{a} + n\overline{b} = \overline{a} + \overline{nb} = \overline{a} + \overline{0} = \overline{a},$$

  ehk tõesti ülimalt n sammu järel hakkab jada korduma. Olgu m selle jada minimaalne periood. Siis $\overline{a} + m\overline{b} = \overline{a}$ ehk

  $$a + mb \equiv a \,(\mathrm{mod}\ n) \iff n \mid mb.$$

  Tähistame $d = (b,n)$, $n = dn'$ ja $b = db'$, kusjuures $(b',n') = 1$. Eukleidese lemma põhjal

  $$dn' \mid mdb' \iff n' \mid mb' \implies n' \mid m.$$

  Seega $n' \leq m$. Samas

  $$\overline{a} + n'\overline{b} = \overline{a} + \overline{n'db'} = \overline{a} + \overline{nb'} = \overline{a} + \overline{0} = \overline{a}.$$

  Seega ka n' on selle jada periood, mistõttu $m \leq n' \leq m$ ja otsitav vähim periood on

  $$m = n' = \frac{n}{(n,b)}.$$

- Olgu meil nüüd geomeetriline jada $\overline{a} \cdot \overline{q}^k$, $k \in \mathbb{N} \cup \{0\}$ jäägiklassikorpuses $\mathbb{Z}_p$. Kui $\overline{q} = \overline{0}$ või $\overline{a} = \overline{0}$, siis on sõltuvalt konventsioonist tegu kas konstantse jadaga $\overline{0},\overline{0},\overline{0},\ldots$ või $\overline{a},\overline{0},\overline{0},\overline{0}$. Mõlemad on perioodilised vähima võimaliku perioodiga 1. Vaatleme edaspidi juhtu, kus $\overline{q} \neq \overline{0}$ ja $\overline{a} \neq \overline{0}$. Siis $\overline{q} \in \mathbb{Z}_p^*$ ehk teoreemi 4.10 põhjal $(q,p) = 1$. Nüüd Fermat' väikese teoreemi tõttu $q^{p-1} \equiv 1 \pmod{p}$, mistõttu

  $$\overline{a} \cdot \overline{q}^{p-1} = \overline{a} \cdot \overline{q^{p-1}} = \overline{a} \cdot \overline{1} = \overline{a}.$$

  Siit on näha, et jada on perioodiline maksimaalse võimaliku perioodiga $p-1$. Olgu m elemendi $\overline{q}$ järk multiplikatiivses rühmas $\mathbb{Z}_p^*$, st vähim selline naturaalarv, mille korral $q^m \equiv 1 \pmod{p}$. Selline arv alati eksisteerib (vt 7. peatüki algust) ja on Lagrange'i teoreemi kohaselt rühma $\mathbb{Z}_p^*$ järgu $p-1$ jagaja. Siis

  $$\overline{a} \cdot \overline{q}^m = \overline{a} \cdot \overline{q^m} = \overline{a} \cdot \overline{1} = \overline{a}.$$

  Seega on m samuti antud jada periood. Kui jada minimaalne periood $k_0 \in \mathbb{N}$ (see ei saa olla 0!) oleks väiksem kui q, siis $\overline{a} \cdot \overline{q}^{k_0} = \overline{a}$. Kuna korpuse $\mathbb{Z}_p^*$ element $\overline{a}$ ei ole $\overline{0}$, siis on ta pööratav ja eelmine võrdus omandab kuju

  $$\overline{q}^{k_0} = \overline{1} \iff q^{k_0} \equiv 1 \,(\mathrm{mod}\ p).$$

  Kuna $k_0 \geq 1$, siis arvu m definitsiooni kohaselt $m \leq k_0$. Samas k_0 oli vähim periood, kust $k_0 \leq m$ ja kokku $k_0 = m$. Järelikult on antud geomeetrilise jada vähim periood elemendi $\overline{q}$ järk multiplikatiivses rühmas Z_p^*, ja muuseas alati arvu $p-1$ jagaja.

Märkus: saab näidata, et ka mitte-algarvulise mooduli korral on geomeetriline jada teatud lisatingimustel perioodiline minimaalse perioodiga, mis on arvu $\varphi(n)$ jagaja.

7. ülesanne (Aljona Kritševskaja)

Leiame ringi $\mathbb{Z}_n$ kõigi pööratavate elementide korrutise. Selleks grupeerime need elemendid. Osad elemendid grupeerime nii, et võtame kokku elemendi ja selle pöördelemendi $(a \cdot a^{-1})$, siis nende korrutis on 1. Ehk need grupid ei mõjuta ringi $\mathbb{Z}_n$ kõigi pööratavate elementide korrutist.

Probleem siin tekib selles, et mõned elemendid on iseenda pöördelemendid. Neid uurime eraldi.

Vaatame hulka $S := \{a \in U(\mathbb{Z}_n) \colon a^2 = 1\}$. Seega ringi $\mathbb{Z}_n$ kõigi pööratavate elementide korrutis sõltub vaid hulga S kõigi elementide korrutisest.

Nüüd grupeerime ka hulga S elemente. Neid grupeerime nii, et korrutame elemendi ja teme vastandelemendi $(a \cdot (-a))$, siis nende korrutis on $a \cdot (-a) = -(a^2) = -1$. Seega saame, et hulga S elementide korrutis on $(-1)^k$, kus k on saadud paaride arv.

Lauri Tart: Siin oleks pidanud ka näitama, et $-a \in S$.

Uurime veel eraldi olukorda, et kui element on iseenda vastandelement. Olgu $a \in S$ selline, et $a = -a$. Element a on mingi jäägiklass, seega võtame mingi suvalise esindaja sellest $k = -k$. Liidame mõlemale poolele k, siis saame $2k = 0$. See tähendab, et $n \mid 2k$. Kuid me teame, et k ja n on ühistegurita, siis nüüd võtame kaks viimast tulemust kokku ja saame, et $n \mid 2$. See tähendab, et ainuke võimalus on $n = 2$. Vaatame selle juhtu eraldi läbi. $U(\mathbb{Z}_2) = 1$, seega pööratavate elementide korrutis on 1. Kui $n \nmid 2$, siis peaks $n \mid k$, kuid siis k ei oleks pööratav.

Järelikult saime, et ringi $\mathbb{Z}_n$ kõigi pööratavate elementide korrutis on kas 1 või -1.

8. ülesanne (Erki Külaots)

Olgu n ja $0 < m \leq n$ ning kirjutame nad aritmeetika põhiteoreemia abil lahti ehk

$$n = p_1^{l_1} \cdot \ldots \cdot p_s^{l_s},\ p_1 \ldots p_s \in \mathbb{P}, l_1 \ldots l_s \in \mathbb{N}_0$$

$$n = p_1^{r_1} \cdot \ldots \cdot p_s^{r_s},\ p_1 \ldots p_s \in \mathbb{P}, r_1 \ldots r_s \in \mathbb{N}_0$$

Kongruentsi definitsioonist saame, et kui $\overline{m}^k \equiv \overline{0} \pmod{n}$, siis $n \mid m^k$ ja seega peab kehtima, et

$$\forall i \in \{1,2,\ldots,s\} : l_i \leq k \cdot r_i$$

Kui $r_i \neq 0$ ja $l_i \neq 0$, siis kuna $k \in \mathbb{N}$, siis saame alati leida k nii, et iga i korral $l_i \leq k \cdot r_i$. Võtame lihtsalt maksimaalse k nii, et $k = \max \left\lceil \frac{l_i}{r_i} \right\rceil$, siis iga i korral $k \geq \max \left\lceil \frac{l_i}{r_i} \right\rceil \geq \frac{l_i}{r_i} \Rightarrow l_i \leq k \cdot r_i$

Kui $l_i = 0$, siis kindlasti $l_i \leq r_i$

Kui $r_i = 0$ ja $l_i \neq 0$, siis ühegi k korral ei kehti $l_i \leq k \cdot r_i$, sest $k \cdot 0 = 0$ ja $l_i > 0$

Seega ainukesed nilpotentsed elemendid on sellised, et kui $l_i \neq 0$, siis $r_i \neq 0$ ning siit näeme, et meid huvitavad ainult need algarvud, mille astendajad on nullist suuremad, seega kirjutame arvu n välja standardkujul:

$$n = p_1^{l_1} \cdot \ldots \cdot p_s^{l_s},\ p_1 \ldots p_s \in \mathbb{P}, l_1 \ldots l_s \in \mathbb{N}$$

Nüüd $l_1 \ldots l_s \geq 1$, seega kõik need algarvud peavad jagama ka m-i ning

$$m = p_1 \cdot \ldots \cdot p_s \cdot j, j \in \mathbb{N}$$

Et $n \geq m$, siis $p_1^{l_1} \cdot \ldots \cdot p_s^{l_s} \geq p_1 \cdot \ldots \cdot p_s \cdot j$, mis tähendab $p_1^{l_1-1} \cdot \ldots \cdot p_s^{l_s-1} \geq j$. Kuna j on naturaalarv, siis jäägiklassis $\mathbb{Z}_n$ on täpselt j nilpotentseid elemente. Kusjuures, kui $l_i = 1$ iga i korral, siis $j = 1$ ning jäägiklassi ringi ainus nilpotent on $\overline{n} = \overline{0}$, mis on trivaalne lahend. Seega põhimõtteliselt igas jäägiklassiringis asub mõni nilpotentne element, kuid see pole huvitav, seega kui seda mitte lugeda, siis et leiduks nilpotentne element, siis peab leiduma mõni i, mille korral $l_i > 1$.

v. Olenevalt küsimusest, siis kas iga jäägiklassiring sisaldab nilpotentseid elemente või ainult need mille korral n-i jagab mõne algarvu ruut. Selles jäägiklassis on vastavalt sellele, kas $\overline{0}$ lugeda nilpotendiks või mitte, vastavalt $p_1^{l_1-1} \cdot \ldots \cdot p_s^{l_s-1}$ nilpotentset elementi või $p_1^{l_1-1} \cdot \ldots \cdot p_s^{l_s-1} - 1$, kus n-i standardkuju on $n = p_1^{l_1} \cdot \ldots \cdot p_s^{l_s}$

Lauri Tart: Tavaliselt nullelementi nilpotendiks ei loeta, seega õige on teine vastus.