Kevad 2016

Märkusi arvuteooria 5. praktikumi kohta:

A. Kõigepealt mõned üldised märkused:

- Kirjalikult esitatud lahendustest on märgata, et suure tõenäosusega märgitakse lahendatuks ka mitmed pooliku lahendusega ülesandeid. Sellega tasub ettevaatlik olla.
- Samuti tundub mulle, et praktikumis mitteosalejate lahendamisoskused on nõrgemad, kui kohaletulijatel. See mulje võib olla ekslik, aga ma soovitan siiski vähemalt aeg-ajalt praktikumis käia. Viimase tegevuse plussid:
  - väiksem võimalus kirja pandud punktide kaotamiseks,
  - võidakse esitada efektiivsemaid lahendusi ja mõttekäike,
  - saate natuke esinemiskogemust (sealhulgas auditooriumi ees matemaatilisele sisule keskendumise osas) stressivabamas õhkkonnas, kui suuremad ettekanded (seminarid, kaitsmine, jms).
- Teil võib tekkida arvamus, et teie praegune punktide arv näitab edukat aine omandamist. See arvamus võib osutuda ekslikuks, sest
  - punktide sisse loetakse igasuguseid asju, sealhulgas "tasuta" esimese nädala ülesandeid ja tunnikontrolle, mis kallutavad tulemust alguse suunas,
  - teemad lähevad järjest raskemaks,
  - punktid ei peegelda tingimata teie lahendusoskust (vt. kõige esimene märkus ülalt). Ainest läbisaamiseks on oluline just lahendusoskuse arendamine, mida punktisüsteem motiveerib, aga kahjuks väga täpselt ei peegelda.

  Üks viis oma arengut mõõta on näiteks küsida, kas ma olen võimeline kõiki ülesandeid, mille ma sel nädalal lahendatuks märkisin, seletama nt. Ball State University (Muncie, Indiana) esimese aasta üliõpilasele nii, et ta suudab neid oma õppejõule rahuldavalt esitada.

B. Nüüd neljandast praktikumist üle jäänud ülesandest:

5. Suure vaevaga saime praktikumis lõpuks lahenduse kätte. Arvestades seejures esilekerkinud probleeme, toon siinkohal ära täieliku arutluskäigu:

Meil on vaja uurida, millised arvud on korraga täisruudud ja täiskuubid modulo 63. Üks võimalus seda teha on leida kõigi jäägiklasside ruudud ja kuubid modulo 63 ning võtta nende hulkade ühisosa. See on väga arvutusmahukas (aga niiviisi tõesti tehti!).

Teiseks võime tähele panna, et $63 = 7 \cdot 9$ ja seega kui $a \equiv b^2 \equiv c^3 \pmod{63}$, siis ka $a \equiv b^2 \equiv c^3 \pmod{7}$ ja $a \equiv b^2 \equiv c^3 \pmod{9}$. Kuna $(7, 9) = 1$, siis järelduse 4.3 tõttu kehtib ka vastupidine väide. Seega piisab, kui me leiame kõik jäägiklassid, mis on korraga täisruudud ja täiskuubid modulo 7 ja modulo 9.

Võimalikult väikeste arvudega arvutamiseks võime võtta jäägiklassid modulo 7 esindajatega vahemikust $[-3, 3]$ ja modulo 9 vahemikust $[-4, 5]$. Siit

$$0^2 \equiv 0, (\pm 1)^2 \equiv 1, (\pm 2)^2 \equiv 4, (\pm 3)^2 \equiv 2 \pmod{7},$$

ehk täisruudud modulo 7 on $0, 1, 2$ ja 4. Samamoodi

$$0^3 = 0, (\pm 1)^3 = \pm 1, (\pm 2)^3 = \pm 8 \equiv \pm 1 \text{ ja } (\pm 3)^3 = \pm 27 \equiv \pm 1 \pmod{7},$$

kust täiskuubid modulo 7 on 0, 1 ja 6. Kokkuvõttes oleme saanud, et korraga täisruudud ja täiskuubid on modulo 7 vaid 0 ja 1. Analoogiliselt võime arvutada

$$0^2 = 0, (\pm 1)^2 = 1, (\pm 2)^2 = 4, (\pm 3)^2 \equiv 0, (\pm 4)^2 \equiv 7 \equiv 5^2 \pmod{9}$$

ja

$$0^3 = 0, (\pm 1)^3 = \pm 1, (\pm 2)^3 \equiv \pm 1, (\pm 3)^3 \equiv 0, (\pm 4)^3 \equiv \pm 1, 5^3 \equiv -1 \pmod{9}.$$

Seega on korraga täisruudud ja täiskuubid modulo 9 jällegi ainult 0 ja 1.

Nüüd on kõige lihtsam kasutada Hiina jäägiteoreemi kongruentside süsteemide

$$\begin{cases} x \equiv 0 \pmod{7} \\ x \equiv 0 \pmod{9} \end{cases}, \quad \begin{cases} x \equiv 0 \pmod{7} \\ x \equiv 1 \pmod{9} \end{cases},$$

$$\begin{cases} x \equiv 1 \pmod{7} \\ x \equiv 0 \pmod{9} \end{cases}, \quad \begin{cases} x \equiv 1 \pmod{7} \\ x \equiv 1 \pmod{9} \end{cases}$$

lahendamiseks. Kuna me ei ole aga HJT loengus veel käsitlenud, siis toimime järgnevalt. Kirjutame üles kõik arvud vahemikust $[0, 62]$, mis on kongruentsed arvudega 0 ja 1 modulo 9:

$$0, 1, 9, 10, 18, 19, 27, 28, 36, 37, 45, 46, 54, 55.$$

Tõmbame nende seast maha kõik arvud, mis ei ole kongruentsed kas arvuga 0 või 1 modulo 7:

$$0 \equiv 0, 1 \equiv 1, \cancel{9} \equiv 2, \cancel{10} \equiv 3, \cancel{18} \equiv 4, \cancel{19} \equiv 5, \cancel{27} \equiv 6, 28 \equiv 0, 36 \equiv 1 \pmod{7},$$

$$\cancel{37} \equiv 2, \cancel{45} \equiv 3, \cancel{46} \equiv 4, \cancel{54} \equiv 5, \cancel{55} \equiv 6 \pmod 7.$$

Alles jäid $0, 1, 28$ ja 36, nagu tarvis.

Veel üks võimalus lahendust lihtsustada on tähele panna, et tegelikult otsime me kuuendaid astmeid. Nimelt kui $a = b^2 = c^3$, siis me võime tänu aritmeetika põhiteoreemile arvu a algtegurite p_i, $i = 1, \ldots, s$, abil kirjutada

$$p_1^{k_1} \cdot \ldots, \cdot p_s^{k_s} = p_1^{2l_1} \cdot \ldots, \cdot p_s^{2l_s} = p_1^{3m_1} \cdot \ldots, \cdot p_s^{3m_s}.$$

Siis aga $2 \mid k_i$ ja $3 \mid k_i$ ehk fakti $(2, 3) = 1$ ja järelduse 4.3 tõttu $6 \mid k_i$ iga $i = 1, \ldots, s$ korral. Seega $k_i = 6n_i$ ja $a = (p_1^{n_1} \cdot \ldots, \cdot p_s^{n_s})^6$. Võib kas uuesti otse välja arvutada või kasutada Fermat' väikest teoreemi (5.13) näitamaks, et $x^6 \equiv 1 \pmod 7$, kui $(7, x) = 1$, ja $0^7 = 0 \pmod 7$. Modulo 9 tuleb korrata eelnevat tegevust:

$$0^6 = \textcircled{0}, (\pm 1)^6 = \left((\pm 1)^3\right)^2 \equiv (\pm 1)^2 = \textcircled{1}, \left((\pm 2)^3\right)^2 \equiv (\pm 1)^2 = \textcircled{1},$$

$$\left((\pm 3)^3\right)^2 \equiv 0^2 = \textcircled{0}, \left((\pm 4)^3\right)^2 \equiv (\pm 1)^2 = \textcircled{1}, \left(5^3\right)^2 \equiv (-1)^2 = \textcircled{1} \pmod 9.$$

C. Kommentaare ja tüüpvigu ülesannete kaupa:

1. Jäägiklassiringides arvutamisega kellelgi õnneks probleeme ei ole.

2. Õige vastus: $\overline{1}, \overline{3}, \overline{5}, \overline{9}, \overline{11}, \overline{13}, \overline{15}, \overline{17}, \overline{19}, \overline{23}, \overline{25}, \overline{27}$. Lahenduses tuleb kindlasti viidata teoreemile 4.10. Vastust saab kontrollida Euleri φ-funktsiooni abil: $\varphi(28) = 12$, mis on pööratavate elementide arv ringis $\mathbb{Z}_{28}$.

3. Vastandelementidega oli kõik korras. Pöördelemente leiti üldiselt proovimise teel (liites järjest arvu 176), aga parem on kasutada Eukleidese algoritmi. Näiteks $(7, 176) = 1 = 176 - 25 \cdot 7$, kust

$$\overline{1} = \overline{176} - \overline{25} \cdot \overline{7} = 0 + \overline{-25} \cdot \overline{7} = \overline{151} \cdot \overline{7}.$$

Kuna jäägiklassiringid on kommutatiivsed ja pöördelement on ühene, siis $\overline{7}^{-1} = \overline{151}$. Samamoodi

$$\overline{1} = \overline{2} \cdot \overline{176} - \overline{39} \cdot \overline{9} = \overline{176 - 39} \cdot \overline{9}$$

ja $\overline{9}^{-1} = \overline{137}$.

Mõnikord ilmusid pöördelemendi kandidaadid lahendustesse ilma mingi seletuseta (mis on lahenduse seisukohalt aktsepteeritav, aga ei aita teil meelde jätta meetodit nende leidmiseks). Samuti oli puudus põhjendustest, miks $\overline{8}, \overline{9}$ ja $\overline{11}$ ei ole pööratavad.

4. Siin on optimaalne koostada isomorfismi tabel:

$\mathbb{Z}_{20}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$	$\overline{7}$	$\overline{8}$	$\overline{9}$
$\mathbb{Z}_5 \times \mathbb{Z}_4$	$(\overline{0},\overline{0})$	$(\overline{1},\overline{1})$	$(\overline{2},\overline{2})$	$(\overline{3},\overline{3})$	$(\overline{4},\overline{0})$	$(\overline{0},\overline{1})$	$(\overline{1},\overline{2})$	$(\overline{2},\overline{3})$	$(\overline{3},\overline{0})$	$(\overline{4},\overline{1})$
$\mathbb{Z}_{20}$	$\overline{10}$	$\overline{11}$	$\overline{12}$	$\overline{13}$	$\overline{14}$	$\overline{15}$	$\overline{16}$	$\overline{17}$	$\overline{18}$	$\overline{19}$
$\mathbb{Z}_5 \times \mathbb{Z}_4$	$(\overline{0},\overline{2})$	$(\overline{1},\overline{3})$	$(\overline{2},\overline{0})$	$(\overline{3},\overline{1})$	$(\overline{4},\overline{2})$	$(\overline{0},\overline{3})$	$(\overline{1},\overline{0})$	$(\overline{2},\overline{1})$	$(\overline{3},\overline{2})$	$(\overline{4},\overline{3})$

Tänu teoreemile 4.5, järeldusele 4.9 ja lausele 5.6 võime pööratavad elemendid leida $\mathbb{Z}_5$-s ja $\mathbb{Z}_4$-s: esimene on korpus, seega pööratavad on $\overline{1},\overline{2},\overline{3},\overline{4}$; teises on teoreem 4.10 tõttu pööratavad $\overline{1}$ ja $\overline{3}$. Seega pööratavad elemendid on parajasti need, mille esimene komponent ei ole $\overline{0}$ ja teine komponent on kas $\overline{1}$ või $\overline{3}$. Sellisel teel leitud elementidele ja nendele vastavatele $\mathbb{Z}_{20}$ elementidele on tabelis ring ümber tõmmatud. Lause 4.15 tõttu on kõik muud elemendid peale $\overline{0}$ (vastavalt $(\overline{0},\overline{0})$) nullitegurid.

Kuigi antud ülesandes ei ole ajavõit suur, siis näiteks $\mathbb{Z}_3 \times \mathbb{Z}_5 \times \mathbb{Z}_8 \cong \mathbb{Z}_{120}$ korral on juba selgelt optimaalsem teha arvutusi maksimaalselt modulo 8. Ja jälle annab Euleri φ-funktsioon võimaluse kontrolliks: $\varphi(20) = 8$, mis on täpselt leitud pööratavate elementide arv.

Mõned levinud vead: arvati, et on ainult üks nullitegur: $(\overline{0},\overline{2})$ (tegelikult on neid 11 tükki); nulli tegurdamisel ei olnud mingit süsteemi märgata (kirjutati läbisegi üles kõik korrutised, mis võrdusid nulliga).

5. Siin ülesandes EI SAA rakendada teoreemi 4.5, sest viimane on sõnastatud ainult piisavana. Mida saab teha, on võrrelda näiteks $\mathbb{Z}_{20}$ ja $\mathbb{Z}_{10} \times \mathbb{Z}_2$ pööratavate elementide arve. Kui need ringid oleksid isomorfsed, siis järelduse 4.9 ja lause 5.6 põhjal peaks neis olema sama palju pööratavaid elemente, aga esimeses on neid 8 ja teises 4. Pööratavate elementide asemel võib kasutada ka nullitegureid, aga see on veidi keerulisem.

6. Lahendajaid oli suhteliselt vähe, mistõtttu visandan siia lahenduse. Esiteks $\overline{m}^2 = \overline{0}$ parajasti siis, kui $n \mid m^2$ (miks?). Aritmeetika põhiteoreemi tõttu

$$m^2 = p_1^{2l_1} \cdot \ldots \cdot p_s^{2l_s} \cdot t,$$

kus $(t, p_i) = 1$ iga $i = 1, \ldots, s$ korral. Kuna $n \mid m^2$, siis lause 1.20 tõttu $2l_i \geq k_i$ ehk $l_i \geq \left\lceil \frac{k_i}{2} \right\rceil$ iga $i = 1, \ldots, s$ korral. Järelikult võttes

$$d := p_1^{\left\lceil \frac{k_i}{2} \right\rceil} \cdot \ldots \cdot p_s^{\left\lceil \frac{k_i}{2} \right\rceil},$$

kehtib $d \mid m$. Selliseid arve $m \in [0, n-1] \cap \mathbb{Z}$, mis omavad tegurit d, on

kokku $\frac{n}{d}$ tükki: $0, d, 2d, \ldots, (\frac{n}{d} - 1) \cdot d$. Seetõttu on otsitav jäägiklasside arv

$$\frac{n}{d} = p_1^{\left\lfloor \frac{k_i}{2} \right\rfloor} \cdot \ldots \cdot p_s^{\left\lfloor \frac{k_i}{2} \right\rfloor}.$$

Üks silma torganud viga oli arvamus, et $m = p_1^{l_1} \cdot \ldots \cdot p_s^{l_s}$. See ei pruugi kehtida, näiteks $30^2 \equiv 0 \pmod{36}$, aga $30 = 2 \cdot 3 \cdot 5$ ja tal on algtegur 5, mis ei ole 36 algtegur.

7. Ülesande sõnastuses oli viga, sest elementi 0 ei loeta nulliteguriks. Vastasel korral oleks ülesande vastus: "kõik jäägiklassiringid, sest need sisaldavad nullelementi." Õige vastus on, et nilpotenseid elemente sisaldavad parajasti need jäägiklassiringid, mille moodulil on vähemalt üks algtegur, mille astendaja mooduli lahutuses algteguriteks on ühest suurem. Teisisõnu, järgmise loengu terminoloogias on vastuseks parajasti need jäägiklassiringid $\mathbb{Z}_n$, mille korral $\mu(n) = 0$.

Levinud vead: uuesti arvati, et nilpotentse elemendi kandidaat peab olema kujul $m = p_1^{l_1} \cdot \ldots \cdot p_s^{l_s}$, kus p_i on mooduli n algtegurid. See on arvamus väär täpselt samal põhjusel, mis viimases ülesandes. Leiti küll, et iga n algtegur peab esinema nilpotentse elemendi m algtegurina, aga arvu n kuju kohta sealt enam järeldusi ei tehtud. Ei toodud otseselt välja, et kui $n = p_1^{k_1} \cdot \ldots \cdot p_s^{k_s}$, siis tingimuse $k \cdot l_i > k_i$ kehtimiseks peab kehtima ka $l_i > 0$.

8. Jäi järgmiseks korraks.