Kevad 2015

Märkusi arvuteooria 5. praktikumi kohta:

A. Esiteks, mitmetes kirjalikes lahendustes oli näha seda ohtu, et te ei kirjuta tervet oma arutluskäiku välja. Kõige markantsem juht koosnes lihtsalt vastusest. Sellise stiiliga (vahe)eksamil täispunkte ei saa.

B. Seekord sai tervelt kolm ülesannet endale tärni juurde. Ma tõstsin nende ülesannete eest punktide arvu neil, kelle lahenduse kohta mul mingi ettekujutus olemas oli. Edaspidi juhul, kui paistab, et ülesandest on saamas tärnülesanne, saab lisapunkte garanteeritult teenida sel viisil, et esitate oma lahenduse kirjalikult enne selle ülesande tahvlile tegemist. Siis ma võin punkte juurde anda või maha võtta vastavalt sellele, mis lahenduses kirjas on. Selline "käigult esitatud" lahendus ei pea loomulikult olema vormistatud TEX abil.

C. Kommentaare ülesannete kaupa:

1. Vaja oli täita ainult pool tabelit kas all- või ülalpool peadiagonaali. Korrutustabelist on võimalik välja lugeda pööratavaid elemente (millele vastavad read/veerud on arvjada $0, 1, 2, 3, \ldots, 11$ mingid permutatsioonid) ja nende pöördelemente ($\overline{1} \cdot \overline{1} = \overline{1}, \overline{5} \cdot \overline{5} = \overline{1}, \overline{7} \cdot \overline{7} = \overline{1}, \overline{11} \cdot \overline{11} = \overline{1}$) ning nullitegureid (millele vastavates ridades/veergudes on lühemad korduvad tsüklid, mis sisaldavad nulli).

2. Siin piisas teoreemi 4.10 ja fakti $30 = 2 \cdot 3 \cdot 5$ tõttu sellest, kui kontrollida arvude $1, 2, \ldots, 29$ jaguvust 2, 3 ja 5-ga.

3. Praktiliselt keegi ei kasutanud pöördelemendi leidmiseks Eukleidese algoritmi, mis on üldjuhul lihtsam, kui mitmesugused proovimised (kuigi sobivad proovimised võivad tõepoolest erijuhtudel kiiremad olla).

4. Üldine lahendusskeem oli enam-vähem kõigil olemas, aga detailide põhjendamine jäi kahjuks väga piiratuks. Vt. märkust A. osas. Ringi $\mathbb{Z}_3 \times \mathbb{Z}_4$ pööratavaid elemente ja nullitegureid sai leida kahel viisil:

1. otse järeldus 4.9, lause 5.6 ja teoreem 4.10 abil arvutades, või
2. kasutades isomorfismi ringiga $\mathbb{Z}_{12}$ ja vaadates, millele $\mathbb{Z}_{12}$ pööratavad elemendid ja nullitegurid vastavad ringis $\mathbb{Z}_3 \times \mathbb{Z}_4$.

5. Teoreem 4.5 ei saanud antud ülesande puhul kasutada, sest kuigi $(2,6) = 2 \neq 1$ ja see teoreem tegelikult ON tarvilik ja piisav, ei ole me seda ei sellisena sõnastanud ega tõestanud. Seetõttu tuli siin näiteks pööratavaid elemente loendada (nimelt $|U(\mathbb{Z}_{12})| = 4$ ja $|U(\mathbb{Z}_2 \times \mathbb{Z}_6)| = 2$) ja kasutada järeldust 4.9 ning lauset 5.6 näitamaks, et isomorfismi ringide $\mathbb{Z}_{12}$ ja $\mathbb{Z}_2 \times \mathbb{Z}_6$ vahel ei saa olla, sest sel juhul $|U(\mathbb{Z}_{12})| = |U(\mathbb{Z}_2 \times \mathbb{Z}_6)|$.

6. Muutus ühetärniülesandeks. Ülesanne osutus samaväärseks sellega, et 1 ja -1 on kongruentsi $x^2 - 1 \equiv 0 \pmod{p^k}$ ainsad lahendid. Viimane väide kehtib aga seetõttu, et siis $p \mid p^k \mid (x-1)(x+1)$, kust Eukleidese lemma põhjal $p \mid x-1$ või $p \mid x+1$. Kui korraga $p \mid x-1$ ja $p \mid x+1$, siis $p \mid x+1-(x-1) = 2$ ja $p = 2$, mis on vastuolus ülesande eeldustega. Seega täpselt üks arvudest $x-1$ ja $x+1$ jagub arvuga p. Kuna p on algarv ja $p^k \mid (x-1)(x+1)$, siis ka p^k jagab täpselt ühte arvudest $x-1$ ja $x+1$. Esimesel juhul $\overline{x} = \overline{1}$, teisel juhul $\overline{x} = -\overline{1}$. Kuna ilmselt $\overline{1}^2 = (-\overline{1})^2 = 1$, siis tõepoolest on kongruentsi $x^2 - 1 \equiv 0 \pmod{p^k}$ ainsateks lahenditeks 1 ja -1.

7. Ka sellest ülesandest sai ühetärniülesanne. Kuna $\overline{ym} = \overline{0}$ parajasti siis, kui $ym = nk$ mingi $k \in \mathbb{Z}$ korral, siis $y \cdot (m,n) \cdot \frac{m}{(m,n)} = (m,n) \cdot \frac{n}{(m,n)} \cdot k$, kust $\left(\frac{m}{(m,n)}, \frac{n}{(m,n)}\right) = 1$ ja Eukleidese lemma tõttu $\frac{n}{(m,n)} \mid y$. Teisipidi, kui $\frac{n}{(m,n)} \mid y$, siis $ym = nl \equiv 0 \pmod{n}$. Seega on vaja vaid loendada, mitu arvu $0 \leq y \leq n-1$ on sellised, et $\frac{n}{(m,n)} \mid y$. Neid on (m,n) tükki: $0 \cdot \frac{n}{(m,n)}, 1 \cdot \frac{n}{(m,n)}, 2 \cdot \frac{n}{(m,n)}, \ldots ((m,n)-1) \cdot \frac{n}{(m,n)}$.

8. Viimane lisatud tärniga ülesanne. Seda saab lahendada mitmel viisil: Fermat' väikese teoreemiga, Lagrange'i teoreemi ja alamrühmade indeksite abil (nagu Rasmus praktikumis tegi), ruutjääkide abil. Visandan siin esimese, kõige lihtsama variandi. Esiteks $\overline{0} = \overline{0}^3$. Teiseks, kui $\overline{a} \neq \overline{0}$, siis $p \nmid a$ ja FVT tõttu $a^{p-1} \equiv 1 \pmod{p}$ ning $a^p \equiv a \pmod{p}$. Võttes $p = 2 + 3k$ saame nüüd, et

$$a = 1 \cdot a \equiv a^{p-1} \cdot a^p = a^{2p-1} = a^{6k+3} = (a^{2k+1})^3 =: b^3 \pmod{p}.$$

Seega iga jäägiklassikorpuse $\mathbb{Z}_p$ element avaldub mingi elemendi kuubina. Järelikult

$$\mathbb{Z}_p \subseteq \{\overline{b}^3 \mid \overline{b} \in \mathbb{Z}_p\} \subseteq \mathbb{Z}_p,$$

kust $|\{\overline{b}^3 \mid \overline{b} \in \mathbb{Z}_p\}| = |\mathbb{Z}_p| = p$. Kui nüüd $\overline{a} = \overline{b}^3 = \overline{c}^3$, kus $\overline{b} \neq \overline{c}$, siis $p = |\{\overline{b}^3 \mid \overline{b} \in \mathbb{Z}_p\}| < |\{\overline{b} \mid \overline{b} \in \mathbb{Z}_p\}| = p$, vastuolu. Järelikult on kõik kuubid

erinevad ja $\overline{a}$ esitus kuubina $\overline{b}^3$ on ühene.