Kevad 2016

Märkusi arvuteooria 6. praktikumi kohta:

A. Üldisi märkusi:

- viimased kolm ülesannet olid märgatavalt väiksema arvu lahendajatega. Tuletan meelde, et nii vaheeksmil kui eksamil esineb kindlasti üks tõestusülesanne, ja see võib vabalt olla üks eelmainitutest;
- viidata on korrektne niiviisi:
  "**teoreemi 5.8 põhjal**", mitte
  "(teoreem 5.8) põhjal" ja isegi
  "teoreemi (5.8) põhjal" ei ole eriti hea variant.

B. Viienda praktikumi viimasest ülesandest:

8. Selle ülesande lahendamine osutus samuti keeruliseks. Küll püüti läheneda mingi nilpotentsusele sarnase metoodikaga, või prooviti kuidagi midagi järeldada faktist $(m, m-1) = 1$. Viimast asjaolu saab küll kasutada, aga täislahendust sealt oodata ei ole.

Lahenduse visand: idempotendi $\overline{m} \in \mathbb{Z}_{p^k}$ korral

$$p^k \mid m(m-1).$$

Jaguvuse transitiivsuse ja Eukleidese lemma põhjal siis kas

$$p \mid m \quad \text{või} \quad p \mid (m-1).$$

Nüüd kas $d := (p^k, m) = 1$ või $e := (p^k, m-1) = 1$, sest vastasel korral $1 < d \mid p^k$, $1 < e \mid p^k$ ja kuna arvu p^k kõik ühest suuremad tegurid jaguvad algarvuga p, siis $p \mid d \mid m$, $p \mid e \mid m-1$ ning $p \mid m-(m-1) = 1$. See ei ole võimalik, järelikult kas

$$(p^k, m) = 1 \quad \text{või} \quad (p^k, m-1) = 1.$$

Kuna $p^k \mid m(m-1)$, siis Eukleidese lemmast kas $p^k \mid (m-1)$ või $p^k \mid m$, ehk $m \equiv 1 \pmod{p^k}$ või $m \equiv 0 \pmod{p^k}$. Kuna ilmselt $\overline{0}^2 = \overline{0}$ ja $\overline{1}^2 = \overline{1}$, siis on jäägiklassiringi $\mathbb{Z}_{p^k}$ ainsad idepotendid $\overline{0}$ ja $\overline{1}$.

C. Kommentaare ja tüüpvigu ülesannete kaupa:

1. Efektiivsem lahendusmeetod on kasutada Gaussi teoreemi ja leida, et

$$S = 72 - \varphi(72) - \varphi(1) = 72 - 24 - 1 = 47.$$

Samas tegid mitmed lahendajad oma elu raskemaks ja arvutasid kõik φ väärtused välja, mõni isegi otse φ definitsiooni järgi ja mitte teoreemi 5.8 abil.

2. Lahendusidee oli enam-vähem kõigil olemas, aga selle lahtikirjutamisel oli mitmeid kitsaskohti. Kasutatud tulemustele ei viidatud; leiti ka need arvud, mille SÜT on 16 või ei leitud neid, mille SÜT on 1. Arvutusefektiivsusest: ei ole vaja vahetulemusi välja arvutada kujul

$$\varphi(\frac{2016}{7}) = \varphi(\mathbf{288}) = \varphi(2^5 \cdot 3^2) = 2^4 \cdot 2 \cdot 3 = 96.$$

Otsitavas summas $\varphi(2016) + \varphi(\frac{2016}{2}) + \varphi(\frac{2016}{3}) + \ldots$ on peale φ väärtuste leidmist liidetavatel palju ühiseid tegureid, seega ei ole mõtet iga kord φ väärtust lõpuni välja arvutada, tasub hoopis kõigepealt summat tegurdada ja alles lõpus kokku korrutada. Näiteks

$$\begin{aligned}\varphi(\frac{2016}{2}) + \varphi(\frac{2016}{3}) + \varphi(\frac{2016}{4}) &= 2^3 \cdot 2 \cdot 3 \cdot 6 + 2^4 \cdot 2 \cdot 6 + 2^2 \cdot 2 \cdot 3 \cdot 6 \\ &= 2^3 \cdot 6 \cdot (6 + 4 + 3) = 8 \cdot 6 \cdot 13 = 624.\end{aligned}$$

3. Vastused olid üldjuhul õiged, põhjendused aga mittetäielikud. Kõige suuremaks probleemiks oli selle kindlakstegemine, et kõik võimalused on tõepoolest läbi vaadatud. Seega visandan siia täieliku lahenduse:

Ilmselt $n > 1$, seega avaldades $n = p_1^{k_1} \cdot \ldots \cdot p_s^{k_s}$ peab kehtima

$$24 = (p_1^{k_1 - 1})(p_1 - 1) \cdot \ldots \cdot (p_s^{k_s - 1})(p_s - 1).$$

Järelikult on kõik arvu n algtegurid ühe võrra suuremad mingist arvu 24 jagajast. Kuna viimased on $1, 2, 3, 4, 6, 12$ ja 24, siis sobivad algteguriteks $2, 3, 5, 7$ ja 13 (4 ja 25 ei ole algarvud). Koostame järgmise tabeli, kus on kirjas võimalikud n algtegurite astmetele p^k vastavad väärtused $p^{k-1}(p-1)$ (pidades silmas piirangut $p^{k-1}(p-1) \mid 24$):

k=	1	2	3	4
2	1	2	4	8
3	2	6		
5	4			
7	6			
13	12			

Nüüd on meil lihtsalt vaja valida igast reast ülimalt üks arv nii, et nende korrutis oleks 24. Kuna $3 \mid 24$, siis üks teguritest peab alati jaguma kolmega,

ehk olema kas 6 või 12. Korraga 6 ja 12 teguritena esineda ei saa, sest $6 \cdot 12 = 72 > 24$. Valides esimesena 12, on sobivad võimalused $12 \cdot 2$ ja $12 \cdot 2 \cdot 1$, mis vastavad n väärtustele $13 \cdot 3 = 39$, $13 \cdot 2^2 = 52$ ja $13 \cdot 3 \cdot 2 = 78$. Kui mitte valida 12 ja valida 6, tekivad korrutised $6 \cdot 4$, $6 \cdot 4 \cdot 1$, $6 \cdot 2 \cdot 2$ ($6 \cdot 2 \cdot 2 \cdot 1$ ei ole võimalik), mis vastavad n väärtustele $7 \cdot 5 = 35$, $7 \cdot 2^3 = 56$, $3^2 \cdot 5 = 45$, $3^2 \cdot 2^3 = 72$, $7 \cdot 5 \cdot 2 = 70$, $3^2 \cdot 5 \cdot 2 = 90$, $7 \cdot 3 \cdot 2^2 = 84$. Seega $\varphi(n) = 24$ parajasti siis, kui

$$n \in \{35, 39, 45, 52, 56, 70, 72, 78, 84, 90\}.$$

4. Üldiselt hästi tehtud ülesanne. Viidata tasub Fermat' **väikesele** teoreemile, sest on olemas mitmeid Fermat' nime kandvaid teoreeme (nt. Fermat' suur teoreem, analüüsi algkursuse Fermat' teoreem, jne.). Ja põhjendus "analoogiliselt" siin väga hästi ei tööta, sest lahenduse jaoks on oluline, et $\varphi(7) \mid 60$, $\varphi(11) \mid 60$ ja $\varphi(13) \mid 60$. "Analoogiliselt" näiteks 17 korral ei töötaks.

5. Samuti ilusasti lahendatud ülesanne. Probleeme: jäägiklassiringidega ümbernurga opereerimine (nn. "varblaste laskmine kahuriga"), peaaegu kõik jätsid mainimata, et $(25, 2016) = 1$. Ilma selleta lahendus aga ei tööta. Tegelikult kehtib üldiselt, et kui $(m, n) = 1$, siis

$$m^{\varphi(n)} + n^{\varphi(m)} \equiv 1 \pmod{mn}.$$

6. Osutus suhteliselt keerukaks. Peamised vead: $\sigma(n)$ valemi vale kuju $\prod \frac{p_i^{k_1+1}}{p_i - 1}$, algarvulise juhu vaatlemata jätmine. Üks suhteliselt lihtne lahendus on alljärgnev:

Kuna $\mu(n) = 0$, siis leidub algarv p nii, et $p^2 \mid n$. Olgugi $n = p^k \cdot t$, kus $(p, t) = 1$ ja $k \geq 2$. Paneme tähele, et $k - 1 \geq 1$, seega

$$p \mid p^{k-1}(p-1) \cdot \varphi(t) = \varphi(n),$$

kust $p \mid \varphi(n) \cdot \sigma(n)$. Oletame nüüd vastuväiteliselt, et $n \mid \varphi(n) \cdot \sigma(n) + 1$. Siis $p \mid \varphi(n) \cdot \sigma(n) + 1$ ja seega

$$p \mid \varphi(n) \cdot \sigma(n) + 1 - \varphi(n) \cdot \sigma(n) = 1,$$

vastuolu. Järelikult arv $\varphi(n) \cdot \sigma(n) + 1$ ei jagu arvuga n, mida oligi tarvis tõestada.

Juhul, kui p on algarv, kehtib

$$\frac{\varphi(p) \cdot \sigma(p) + 1}{p} = \frac{(p-1)\frac{p^2-1}{p-1} + 1}{p} = \frac{p^2}{p} = p.$$

7. Siin oli väga vajalik tähelepanek, et

$$\sigma(n) \geq n.$$

Kui seda ei maininud, siis jäi alati sisse oht, et kusagil suuremate x väärrtuste korral tekivad lisalahendid. Muidu tuli aga lihtsalt kõik σ väärtused kuni arvuni 24 välja arvutada ja panna tähele, et lahendid puuduvad, kui $n = 2$, lahendeid on täpselt 1 juba siis, kui $n = 1$, kaks lahendit on, kui $n = 12$ ($x \in \{6, 11\}$), ja kolm lahendit tekib juhul, kui $n = 24$ ($x \in \{14, 15, 24\}$).

8. Jäi jälle järgmiseks korraks, aga selle faili avalikustamise ajaks on järgmine kord juba ära olnud. Ülesanne ise oli suhteliselt raske ja lahendused tihti poolikud, seega lisan ka siia täieliku tõestuse.

Kuna algarvu p jagajad on vaid 1 ja p, siis

$$\sum_{d|p} \mu(d) \cdot \varphi(d) = \mu(1) \cdot \varphi(1) + \mu(p) \cdot \varphi(p) = 1 - (p-1) = 2 - p. \qquad (1)$$

Paneme tähele, et ühistegurita arvude m ja n korral

$$\mu(mn) = \mu(m) \cdot \mu(n). \qquad (2)$$

Tõepoolest, kui $\mu(m) = 0$ või $\mu(n) = 0$, siis ilmselt ka $\mu(mn) = 0$. Kui kas $m = 1$ või $n = 1$, siis on väide samuti ilmne. Olgu nüüd m ja n mõlemad ruuduvabad ja ühest suuremad. Siis $m = p_1 \cdot \ldots \cdot p_s$ ja $n = q_1 \cdot \ldots \cdot q_t$, kusjuures ühiseid algtegureid neil eelduse kohaselt ei ole. Järelikult

$$\mu(mn) = \mu(p_1 \cdot \ldots \cdot p_s \cdot q_1 \cdot \ldots \cdot q_t) = (-1)^{s+t} = (-1)^s \cdot (-1)^t = \mu(m) \cdot \mu(n).$$

Olgu jälle $(m, n) = 1$ ning $m = p_1^{k_1} \cdot \ldots \cdot p_s^{k_s}$ ja $n = q_1^{l_1} \cdot \ldots \cdot q_t^{l_t}$. Arutledes samamoodi, nagu teoreemi 5.17 tõestuses (jätame välja kõik jagajad d, mille korral $\mu(d) = 0$) saame, et

$$\begin{aligned}
\sum_{d|mn} \mu(d) \cdot \varphi(d) &= \sum_{d|p_1 \cdot \ldots \cdot p_s \cdot q_1 \cdot \ldots \cdot q_t} \mu(d) \cdot \varphi(d) \\
&= \mu(1) \cdot \varphi(1) + \mu(p_1) \cdot \varphi(p_1) + \ldots + \mu(q_t) \cdot \varphi(q_t) + \mu(p_1 p_2) \cdot \varphi(p_1 p_2) + \ldots \\
&+ \mu(p_1 q_1) \cdot \varphi(p_1 q_1) + \ldots + \mu(q_{t-1} q_t) \cdot \varphi(q_{t-1} q_t) + \ldots \\
&+ \mu(p_1 \cdot \ldots \cdot p_s \cdot q_1 \cdot \ldots \cdot q_t) \cdot \varphi(p_1 \cdot \ldots \cdot p_s \cdot q_1 \cdot \ldots \cdot q_t).
\end{aligned}$$

Teoreemi 5.7 ja seose (2) tõttu

$$\sum_{d|mn} \mu(d)\cdot\varphi(d) =$$
$$= \mu(1)\cdot\varphi(1) + \mu(p_1)\cdot\varphi(p_1) + \ldots + \mu(q_t)\cdot\varphi(q_t) + \mu(p_1p_2)\cdot\varphi(p_1p_2) + \ldots$$
$$+ \mu(p_1)\cdot\mu(q_1)\cdot\varphi(p_1)\cdot\varphi(q_1) + \ldots + \mu(q_{t-1}q_t)\cdot\varphi(q_{t-1}q_t) + \ldots$$
$$+ \mu(p_1\cdot\ldots\cdot p_s)\cdot\mu(q_1\cdot\ldots\cdot q_t)\cdot\varphi(p_1\cdot\ldots\cdot p_s)\cdot\varphi(q_1\cdot\ldots\cdot q_t)$$
$$= [1 + \mu(p_1)\cdot\varphi(p_1) + \ldots + \mu(p_1\cdot\ldots\cdot p_s)\cdot\varphi(p_1\cdot\ldots\cdot p_s))]\cdot$$
$$\cdot [1 + \mu(q_1)\cdot\varphi(q_1) + \ldots + \mu(q_1\cdot\ldots\cdot q_t)\cdot\varphi(q_1\cdot\ldots\cdot q_t))]$$
$$= \left(\sum_{d|p_1\cdot\ldots\cdot p_s} \mu(d)\cdot\varphi(d)\right)\cdot\left(\sum_{d|q_1\cdot\ldots\cdot q_t} \mu(d)\cdot\varphi(d)\right)$$
$$= \left(\sum_{d|m} \mu(d)\cdot\varphi(d)\right)\cdot\left(\sum_{d|n} \mu(d)\cdot\varphi(d)\right).$$

Olgu nüüd $n > 1$ esitatud standardkujul $n = p_1^{k_1}\cdot\ldots\cdot p_s^{k_s}$. Kuna algtegurid p_i on paarikaupa ühistegurita, saab rakendada eelnevat arutelu ja leida võrduse (1) abil, et tõepoolest

$$\sum_{d|n} \mu(d)\cdot\varphi(d) = \prod_{i=1}^{s}\sum_{d|p_i^{k_i}} \mu(d)\cdot\varphi(d) = \prod_{i=1}^{s}\sum_{d|p_i} \mu(d)\cdot\varphi(d) = \prod_{i=1}^{s}(2-p_i).$$