Kevad 2015

Märkusi arvuteooria 2. praktikumi kohta:

A. Käesoleval nädalal esitatud ja TEX abil küljendatud lahenduste vormistus oli küllaltki ebaühtlane. Soovitan kõigil võtta seda kui ettevalmistust muude tulevikus kirjutamist vajavate matemaatiliste tekstide (näiteks bakalaureusetöö) jaoks ja proovida oma lahendused võimalikult korrektselt ja heas eesti keeles kirja panna. Eeskujuks võib võtta suvalise matemaatilise teksti, näiteks arvuteooria või matemaatilise analüüsi elektroonilise konspekti, Mati Kilbi algebra või Leiki Loone analüüsi õpiku jne.

Lõpuks, terminoloogiliselt on olemas paarisarvud ja paaritud arvud, aga mitte paaris arvud ja paaritudarvud.

B. Kommentaare ülesannete kaupa:

1. Efektiivne meetod vähima ühiskordse leidmiseks on $[m,n] = \frac{m}{(m,n)} \cdot n$, sest jagatis $\frac{m}{(m,n)}$ esineb on juba Eukleidese algoritmi rakendamisel välja arvutatud. Algteguriteks lahutamine on üldiselt väga ebaefektiivne lähenemine.

2. Siin püüti mõnikord arutleda lineaarkombinatsioonide abil. Tõepoolest, võttes näiteks $1 = (a,b) = ax + by$, $(ac,b) = acs + bt$ ja $(b,c) = bu + cv$ saame, et

$$(ac,b) = ax(ac,b) + by(ac,b) = c \cdot a^2xs + b \cdot (axt + y(ac,b)),$$

mistõttu seoste $(b,c) \mid c$ ja $(b,c) \mid b$ abil $(b,c) \mid (ac,b)$. Samas on selline meetod üldiselt pikem ja kohmakam, kui otse suurima ühisteguri definitsiooni rakendamine.

Aga me EI SAA automaatselt väita, et kuna $(b,c) = bu + cv$ ja $(ac,b) = c \cdot a^2xs + b \cdot (axt + y(ac,b))$ on mõlemad nö. lineaarkombinatsioonid arvudest b ja c, siis nad jagavad teineteist. Näiteks $3 \cdot 5 + 1 \cdot 4 = 19$ ja $3 \cdot 1 + 1 \cdot 2 = 5$ on hoopiski ühistegurita.

3. Selles ülesandes sai väga edukalt kasutada loengukonspekti teoreemi 2.7 (Tšebõšovi teoreem, Bertrand'i postulaat). Tüüpiliselt jäeti tähelepanuta eeldus $n > 6$, mis on vajalik. Lõpuks, paarisarvulist juhtu analüüsides on suurima ühisteguri puudumise jaoks väga mugav rakendada 4. ülesandes kasutatud mõttekäiku.

4. Kõige lihtsam lahendusmeetod: kuna $(a, a+2) \mid a$ ja $(a, a+2) \mid a+2$, siis $(a, a+2) \mid a+2-a = 2$. Märgi täpsusega on arvul 2 vaid kaks tegurit, nimelt 1 ja 2. Järelikult ongi ainsad sobivad ühistegurid 1 ja 2, mis tõepoolest ka tegelikult esinevad, sest näiteks $(2, 2+2) = 2$ ja $(2, 3+2) = 1$.

5. Erilahendi leidmiseks võib kasutada ka muid meetodeid peale Eukleidese algoritmi. Antud juhul oli ilmne, et $2 \cdot 333 + 5 \cdot 0 = 666$. Päris mitmel lahendajal tekkis viga vahemikku $[0, 67]$ või $[267, 333]$ kuuluvate täisarvude loendamisega. Nimelt on neid kokku $67 - 0 + 1 = 333 - 267 + 1 = 67$ tükki, mitte $67 - 0 = 333 - 267 = 66$ tükki.

6. Analoogiline eelmise ülesandega ja toetus loengukonspekti näitele 1.16. Ka siin võis erilahendeid leida ilma Eukleidese algoritmi kasutamata. Esines ka loendamisel põhinevaid lahendusi.

7. Kõige lihtsam on võtta kaks erinevat algarvu p ja q, mis on mõlemad suuremad nii arvust m kui arvust n. Kuna algarve on lõpmata palju, siis sellised p ja q tõepoolest leiduvad. Teoreemi 1.14 põhjal ($(p, q) = 1$) avalduvad võrrandi $px + qy = pm + qn$ lahendid järgmiselt

$$\begin{cases} x = m + qt \\ y = n - pt \end{cases}.$$

Siit on näha, et kui $t > 0$, siis $y < 0$ ja kui $t < 0$, siis $x < 0$, seega ainus naturaalarvuline lahend tekib juhul $t = 0$, ja selleks ongi $x = m$, $y = n$.

8. Väga efektiivne lahendus, mille pakkus välja Rasmus Erlemann, on järgmine. Tähistame $m = \frac{ac}{e}$ ja $n = \frac{bd}{e}$. Eelduste kohaselt $m + n = \frac{ac+bd}{e} \in \mathbb{Z}$ ja $m \cdot n = \frac{ab}{e} \cdot \frac{bd}{e} \in \mathbb{Z}$. Täisarvuliste kordajatega polünoomide ratsionaalarvuliste lahendeid kirjeldava teoreemi kohaselt peavad polünoomi

$$(x - m)(x - n) = x^2 - (m + n) + mn$$

taandatud kujul ratsionaalarvulised lahendid $\frac{a}{b}$, $(a, b) = 1$m rahuldama tingimusi $a \mid mn$ ja $b \mid 1$ (kus mn on vabaliime kordaja ja 1 pealiikme kordaja). Kuid sellel polünoomil on ilmselt kaks lahendit, nimelt $m = \frac{ac}{e}$ ja $n = \frac{bd}{e}$, kust kas $e \mid 1$, ehk $e = \pm 1$, või me saame e-ga taandada ja $e \mid ac$ ning $e \mid bd$.

Teine meetod on vaadelda ilmselt kehtivat võrdust

$$(ab + cd)^2 + (ac - bd)^2 = (ab - cd)^2 + (ac + bd)^2.$$

Kuna $e \mid ab$ ja $e \mid cd$, siis $e^2 \mid (ab \pm cd)^2$ ning järelikult (sest ka $e^2 \mid (ac+bd)^2$)

$$e^2 \mid (ab - cd)^2 + (ac + bd)^2 - (ab + cd)^2 = (ac - bd)^2.$$

Tõestame, et ka $e \mid ac-bd$. Selleks tähistame $d = (e, ac-bd)$, $m = \frac{e}{d} \in \mathbb{Z}$ ja $n = \frac{ac-bd}{d} \in \mathbb{Z}$. Järeldusest 1.8 saame, et $(m, n) = 1$. Jaguvuse definitsiooni põhjal leidub $k \in \mathbb{Z}$ selliselt, et $e^2k = (ac - bd)^2$ ehk

$$m^2d^2k = n^2d^2.$$

Kui $e = ac - bd = 0$, siis ilmselt $e \mid ac - bd$. Kui $e \neq 0$ või $ac - bd \neq 0$, siis $d \neq 0$ ja d^2-ga taandades saame, et $m^2k = n^2$, kust $m \mid n^2$. Kuna $(m, n) = 1$, siis Eukleidese lemma abil $m \mid n$. Aga sel juhul lause 1.5 osa 1. põhjal $1 = (m, n) = m$ ja $e = d = (e, ac - bd) \mid ac - bd$.

Nüüd

$$e \mid (ac - bd) + (ac + bd) = 2ac \quad \text{ja} \quad e \mid (ac - bd) - (ac + bd) = 2bd.$$

Leiame arvude a, b, c, d, e standardkujus esinevad kahe astmed: $a = 2^\alpha \cdot a', b = 2^\beta \cdot b', c = 2^\gamma \cdot c', d = 2^\delta \cdot d', e = 2^\varepsilon \cdot e'$, $(2, a') = (2, b') = (2, c') = (2, d') = (2, e') = 1$. Lause 1.20 osa 1. ning seoste $e \mid 2ac$ ja $e \mid 2bd$ tõttu $\varepsilon \leq \alpha+\gamma+1$ ja $\varepsilon \leq \beta + \delta + 1$. Jälle lause 1.20 põhjal on ainus võimalus, et $e \nmid ac$ või $e \nmid bd$ see, et

$$\varepsilon = \max(\alpha + \gamma + 1, \beta + \delta + 1) = 1 + \max(\alpha + \gamma, \beta + \delta)$$

(sest kui e ei jaga väiksemat maksimaalset kahe astet sisaldavad arvudest ac ja bd, siis ei jaga ta ammugi suuremat maksimaalset kahe astet sisaldavat arvu). Ülesande eelduste põhjal $e^2 \mid abcd$ ehk

$$2\varepsilon \leq \alpha + \beta + \delta + \gamma.$$

Seega võimalus, et $e \nmid ac$ või $e \nmid bd$ langeb ära, kuna siis

$$2\varepsilon = 2(1+\max(\alpha+\gamma, \beta+\delta)) > \max(\alpha+\gamma, \beta+\delta)+\max(\alpha+\gamma, \beta+\delta) \geq (\alpha+\gamma)+(\beta+\delta).$$

Seega tõepoolest alati $e \mid ac$ ja $e \mid bd$.