Kevad 2015

Märkusi arvuteooria 3. praktikumi kohta:

A. Selle nädala ülesanded valmistasid juba nii mõnelegi kuulajale raskusi. Soovitan ikkagi võimalusel praktikumi kohale tulla, sest seal saavad kõik ülesanded lõpuks täieliku lahenduse.

Kirjalikes lahendustes oli väga mitmetel juhtudel vajalikest tõestuselementidest üle libisetud. Igasugused lihtsamad tulemused võivad teile ilmsed tunduda siis, kui te olete arvuteooria kursusest edukalt läbi saanud ja teate täpselt, millise meetodiga "ilmseid" tulemusi tõestada. Praegu tuleks lähtuda seisukohast, et tõestada on vaja kõiki väiteid, mida ei ole olnud loengus, isegi näiteks selliseid fakte: $(2 \mid a \wedge 3 \mid a) \Rightarrow 6 \mid a$. Mul ei ole võimalust kirjaliku lahenduse korral kontrollida, kas te olete kõigist nüanssidest tõepoolest aru saanud, või panite lihtsalt tõesena tunduva väite kirja ja loodate, et ma jään seda niisama uskuma.

B. Kommentaare ülesannete kaupa:

1. Vastuste loetelu ei ole lahendus, on vaja ka kirjeldada, kuidas need vastused saadi. Ja Eratosthenese sõela korral on väga hea kasutada mingit tabelkujul skeemi, mitte kirjutada leheküljepikkust kirjeldust sellest, kuidas te kusagil arve maha tõmmanud olete. Viimast on nimelt väga raske lugeda.

2. Siin võis kasutada Dirichlet' teoreemi, aga ülesanne oli ikkagi mõeldud lahendamiseks elementaarsete vahenditega. Kirjalikud tõestused jäid üldiselt lünklikeks ja peegeldasid liiga täpselt Eukleidese tõestust (nt. nummerdatakse ära KÕIK algarvud, mitte kõik algarvud kujul $8k + 1$ jmt.).

Korrektne tõestus: oletame vastuväiteliselt, et $p_1, \ldots, p_s$ on kõik algarvud kujul $8k + 1$. Vaatleme arvu

$$a = (2 \cdot p_1 \cdot \ldots \cdot_s)^2 + 1 = 8 \cdot (2 \cdot p_1 \cdot \ldots \cdot p_s) + 1.$$

Kuna $a > p_i$ iga i korral, siis vastuväitelise eelduse kohaselt on a kordarv. Olgu p mingi arvu a algtegur, st $p \mid a$ ja $p \in \mathbb{P}$. Siis $p \mid (2 \cdot p_1 \cdot \ldots \cdot p_s)^2 + 1$ ja ülesande sõnastuses oleva lisaväite kohaselt on p kujul $8k + 1$, ehk $p = p_i$ mingi indeksi i korral. Järelikult $p \mid 16 \cdot p_1 \cdot \ldots \cdot p_s$, mistõttu

$$p \mid a - 16 \cdot p_1 \cdot \ldots \cdot p_s = 1,$$

kust $p = \pm 1$, mis ei saa kehtida, sest p on algarv. Järelikult on meie vastuväiteline eeldus väär ja algarve kujul $8k + 1$ on lõpmata palju.

3. Siin pidi tähele panema, et kuna n on kordarv, siis on tal vähemalt kaks algtegurit. Järelikult vastuseks tuleb, et arvul on on kas 2 või 3 erinevat algtegurit. Lisaks ei ole näiteks kolme algteguriga arvul $8 = 2^3$ kolme ERINEVAT algtegurit (ainus algtegur on 2). Seega selline kolme algteguriga arv, mis rahuldab ülesande tingimusi, on näiteks $385 = 5 \cdot 7 \cdot 11$.

4. Siin oli kaks võimalust: leida n järjestikust kordarvu ja liikuda kas üles- või allapoole kuni esimese algarvuni. Esimesel juhul võis kasutada kas Bertrand'i postulaati või algarvude hulga lõpmatust garanteerimaks, et see protsess lõpeb. Teisel juhul on alumiseks piiriks algarv 2.

5. Siin tehti natuke palju lisatööd sellega, et lahutati $p^4 - q^4$ kaheks liidetavaks $(p + 1)(p - 1)(p^2 + 1)$ ja $(q + 1)(q - 1)(q^2 + 1)$. Lihtsam on võtta kohe

$$p^4 - q^4 = (p - q)(p + q)(p^2 + q^2).$$

Siis üks esimesest kahest tegurist jagub arvudega kolm, sest $p, q > 3$ tõttu annavad p ja q arvuga kolm jagades jäägid kas 1 või 2. Kui mõlemad neist annavad sama jäägi, siis $3 \mid (p - q)$, vastasel korral $3 \mid (p + q)$. Kuna $2 \nmid q$, siis $q = 2k + 1$ ja paarisarvu $p - q$ jaoks kas $4 \mid p - q$ või $p - q = 4l + 2$ ja

$$p + q = 4l + 2 + 2(2k + 1) = 4(l + k + 1).$$

Järelikult jagub arvudest $p - q$ ja $p + q$ üks kahega ja teine neljaga. Kui $a \mid c$ ja $b \mid c$ ning $(a, b) = 1$, siis $c = au = bv$, $u, v \in \mathbb{Z}$ ja Eukleidese lemma tõttu $a \mid v$, kust $c = b(aw)$, $w \in \mathbb{Z}$, ehk $ab \mid c$. Seega $2 \cdot 4 \cdot 3 \mid (p - q)(p + q)$ ja ilmselt on $p^2 + q^2$ paarisarv, mistõttu ka

$$48 = 2^4 \cdot 3 \mid (p - q)(p + q)(p^2 + q^2) = p^4 - q^4.$$

6. Üks koht, kus võidi eksida, on arvamus, et kui $ab = cd$, siis $a = c$ ja $b = d$ või $a = d$ ja $b = c$. Isegi siis, kui $c, d \in \mathbb{P}$, ei pruugi see kehtida, näiteks $1 \cdot 15 = 3 \cdot 5$, aga $1 \neq 3$.

7. See osutus üheks raskemaks ülesandeks, millele praktikumis kulus konkurentsitult kõige rohkem aega. Korrektne lahendus:

Oletame, et

$$n = x^2 \cdot 2 = y^3 \cdot 3 = z^5 \cdot 5$$

mingite $x, y, z \in \mathbb{N}$ korral. Siis $2 \mid n$, $3 \mid n$ ja $5 \mid n$, millest

$$n = 2^k \cdot 3^l \cdot 5^m \cdot n',$$

kus $(2, n') = (3, n') = (5, n') = 1$ ja $k, l, m \geq 0$. Kuna meil on vaja leida vähim võimalik n väärtus, siis võime võtta $n' = 1$ ja vaadata, kas me sel juhul suudame sellise n leida. Kui ei suuda, alles siis on vaja n' väärtust suurendada. Olgugi $n = 2^k \cdot 3^l \cdot 5^m$. Aritmeetika põhiteoreemi kohaselt siis ka $x = 2_1^k \cdot 3_1^l \cdot 5_1^m$, $y = 2_2^k \cdot 3_2^l \cdot 5_2^m$ ja $z = 2_3^k \cdot 3_3^l \cdot 5_3^m$, kus $k_1, k_2, k_3, l_1, l_2, l_3, m_1, m_2, m_3 \geq 0$, sest arvude x, y ja z kõik algtegurid peavad olema n algtegurid, milleks on $2, 3$ ja 5. Me võime oma eeldused uuesti lahti kirjutada kujul

$$\begin{aligned}
2^{k-1} \cdot 3^l \cdot 5^m &= (2^k \cdot 3^l \cdot 5^m)/2 = (2_1^k \cdot 3_1^l \cdot 5_1^m)^2 = 2^{2k_1} \cdot 3^{2l_1} \cdot 5^{2m_1}, \\
2^k \cdot 3^{l-1} \cdot 5^m &= (2^k \cdot 3^l \cdot 5^m)/3 = (2_2^k \cdot 3_2^l \cdot 5_2^m)^3 = 2^{3k_2} \cdot 3^{3l_2} \cdot 5^{3m_2}, \\
2^k \cdot 3^l \cdot 5^{m-1} &= (2^k \cdot 3^l \cdot 5^m)/5 = (2_3^k \cdot 3_3^l \cdot 5_3^m)^5 = 2^{5k_3} \cdot 3^{5l_3} \cdot 5^{5m_3}.
\end{aligned}$$

Jälle aritmeetika põhiteoreemi kohaselt

$$\begin{cases} k - 1 = 2k_1 \\ l = 2l_1 \\ m = 2m_1 \end{cases}, \quad \begin{cases} k = 3k_2 \\ l - 1 = 3l_2 \\ m = 3m_2 \end{cases}, \quad \begin{cases} k = 5k_3 \\ l = 5l_3 \\ m - 1 = 5m_3 \end{cases}.$$

Meil on tarvis leida kõigi nende võrrandite jaoks minimaalne lahend (k, l, m). Paneme tähele, et $3 \mid k$, $5 \mid k$, $2 \mid l$, $5 \mid l$, $2 \mid m$, $3 \mid m$, seega $15 \mid k$, $10 \mid l$ ja $6 \mid m$. Võttes vähimad selliseid tingimusi rahuldavad arvud $k = 15$, $l = 10$ ja $m = 6$ näeme, et need tõepoolest rahuldavad ka lisatingimusi $2 \mid k - 1 = 14$, $3 \mid l - 1 = 9$ ja $5 \mid m - 1 = 5$. Seega minimaalne lahend on $(15, 10, 6)$ ja vähim arv n, mis rahuldab ülesande tingimusi, on

$$n = 2^{15} \cdot 3^{10} \cdot 5^6 = 30\,233\,088\,000\,000.$$

8. See ülesanne oli enam-vähem ilusasti lahendatud ja mingeid erilisi vigu lahendamisel ei tehtud.