Kevad 2016

Märkusi arvuteooria 16. praktikumi kohta:

A. Kahjuks ei motiveerinud punktisüsteem paljusid kuulajaid kõiki või isegi suuremat osa ülesandeid lahendama. Kuna tegu on täpselt selliste ülesannetega, mis eksamitöös esineda võivad, siis on tegu käestlastud võimalusega varakult eksamiks valmistuma hakata.

B. Kommentaare ja tüüpvigu ülesannete kaupa:

1. Lihtsaim lahendus on tähele panna, et 1001 järjestikust naturaalarvu annavad arvuga 1001 jagades mingis järjekorras jäägid $0, 1, \ldots, 1000$, seega otsitav summa S on

$$S \equiv \sum_{i=0}^{1000} i = \frac{1000}{2}(1000+1) \equiv 0 \pmod{1001}.$$

2. Antud ülesande sai taandada diofantilise võrrandisüsteemi

$$\begin{cases} 4x + 3y + 2x &= 47 \\ x + y + z &= 15 \end{cases}$$

lahendamisele. Lahendamisel tekib diofantiline võrrand

$$2x + y = 17,$$

mille lahendid on (avaldades lisaks z võrrandist $x + y + z = 15$)

$$\begin{cases} x &= 8 + t \\ y &= 1 - 2t \\ z &= 6 + t \end{cases},$$

$t \in \mathbb{Z}$. Arvestades kitsendusi $x, y, z > 0$ ja $y < z$, on kaks võimalikku lahendit:

$$(x, y, z) \in \{(8, 1, 6), (7, 3, 5)\}.$$

Seega hinde B sai kas 7 või 8 üliõpilast.
Võrrandisüsteemi koostamisel võis muutujaid valida ka teistmoodi, näiteks $x, y, y + r$, $r > 0$. Lahendus sellest oluliselt ei muutu.

3. Vastus: jah, näiteks

$$102, 115, 128, 141, 154$$

või

$$18356, 18369, 18382, 18395, 18408.$$

Tegelikult on igas aritmeetilises jadas kuitahes pikki järjestikustest kordarvudest koosnevaid lõike. Miks? Olgu meil aritmeetiline jada

$$(a + bk)_{k=0}^{\infty}.$$

Fikseerime järjestikuste kordarvude arvu n ja n algarvu $p_1, \ldots, p_n$, mis rahuldavad tingimust

$$(p_i, b) = 1.$$

Kuna arvul b on lõplik arv algtegureid ja algarve on lõpmata palju, siis on selline algarvude p_i valik võimalik. Eelneva põhjal on element $\overline{b}$ pööratav kõigis ringides $\mathbb{Z}_{p_i}$, järelikult saame leida täisarvud arvud k_i nii, et

$$k_i \cdot b \equiv 1 \pmod{p_i}.$$

Hiina jäägiteoreemi kohaselt on kongruentside süsteem

$$\begin{cases} x \equiv -a \cdot k_1 \pmod{p_1} \\ x \equiv -(a+b) \cdot k_2 \pmod{p_2} \\ x \equiv -(a+2b) \cdot k_3 \pmod{p_3} \\ \quad \ldots \\ x \equiv -(a+(n-1)b) \cdot k_n \pmod{p_n} \end{cases}$$

lahenduv. Selle mistahes lahend x_0 rahuldab järgmiseid seoseid:

$$\begin{cases} a + x_0 b \equiv 0 \pmod{p_1} \\ a + (x_0+1)b \equiv 0 \pmod{p_2} \\ a + (x_0+2)b \equiv 0 \pmod{p_3} \\ \quad \ldots \\ a + (x_0 + (n-1))b \equiv 0 \pmod{p_3} \end{cases}$$

Vajadusel arvu x_0 suurendades ($x_1 = x_0 + p_1 \cdot \ldots \cdot p_n$ on samuti eelmainitud kongruentside süsteemi lahend, kusjuures kui näiteks $a + x_0 b = p_i$, siis $a + x_1 b > p_i$) saame, et arvud

$$a + x_0 b, a + (x_0 + 1)b, \ldots, a + (x_0 + (n-1))b$$

on kõik kordarvud. Ilmselt on tegu jada $(a + bk)_{k=0}^{\infty}$ järjestikuste liikmetega. Sellisel viisil ongi antud ülesande jaoks leitud arvud

$$18356, 18369, 18382, 18395, 18408,$$

võttes $p_1 = 2, p_2 = 3, p_3 = 5, p_4 = 7$ ja $p_5 = 11$.
Lahendamisel ei saa otse kasutada asjaolu, et iga $n \in \mathbb{N}$ korral leidub n järjestikust kordarvu, sest üldiselt $b > 1$. Samuti ei saa otseselt kasutada teoreemi 2.5, lauset 2.6 või Tao-Greeni tulemust järjestikustest algarvulistest jadadest.

4. Vastus: kas $x = 3$ ja $y = 4$ või $x = 6$ ja $y = 7$.
Ülesannet sai lahendada proovimismeetodil, lahendades kongruentsi

$$10101010100x + 7050703040 + y \equiv 302x + y + 1 \equiv 0 \pmod{909}$$

või kasutades jaguvustunnuseid arvudega 9 ja 101. Viimane meetod on kõige üldisem. Jaguvustunnus arvu 101 jaoks on sarnane jaguvustunnusega arvu 11 jaoks, ainus erinevus on vaheldumisi liitmisel ja lahutamisel ühekohaliste arvude asendamine kahekohalistega, st.

$$101 \mid 100^k a_k + 100^{k-1} a_{k-1} + \ldots + 100a_1 + a_0$$

parajasti siis, kui

$$101 \mid a_k - a_{k-1} + \ldots + (-1)^{k-1} a_1 + (-1)^k a_0.$$

Antud ülesandes peavad siis kehtima

$$9 \mid x + 7 + x + 5 + x + 7 + x + 3 + x + 4 + y \equiv 5x + y - 1 \pmod{9}$$

ja

$$101 \mid -x+70+x-50-x+70+x-30-x+40+y \equiv y-x+100 \pmod{101}.$$

Kuna $y - x + 100 \in [91, 108]$, siis $y - x = 1$ ja meile jääb alles kongruents

$$6x \equiv 0 \pmod{9}.$$

Selle lahendiks on ilmselt $x \equiv 0 \pmod 3$ ehk $x \in \{0, 3, 6, 9\}$. Kuna arv ei alga numbriga 0 ja $y = 9 + 1 = 10$ ei ole kümnendnumber, siis kas $x = 3$ ja $y = 4$ või $x = 6$ ja $y = 7$.

5. Vastus: nullitegurid on $11, 13, 22, 26, 33, 39, 44, 52, 55, 65, 66, 77, 78, 88, 91, 99, 104, 110, 117, 121, 130$ ja 132.
Lahendamisega kellelgi probleeme ei olnud.

6. Vastus: 1800.
Ülesanne oli analoogiline 6. praktikumi 2. ülesandega. Probleemideks olid siin lause 5.10 mittemäletamine, püüe kasutada ühistegureid, mis on ≥ 10 (neid on siin rohkem, kui kümnest väiksemaid ühistegureid, mistõttu arvutusi saab

olema rohkem, aga mõnikord on selline lähenemine tõesti kasulik) ja liigne arvutamine tegurdamise asemel (vt. 6. praktikumi tagasisidet).

7. Vastus: vähemalt 19 kitse.
Ülesande sai taandada kongruentside süsteemi

$$\begin{cases} x & \equiv & 6 \pmod{23} \\ x & \equiv & 43+6+4 \equiv 1 \pmod{13} \\ x & \equiv & 3+13+4+6+43 \equiv 3 \pmod{11} \end{cases}$$

lahendamisele, mida saab teha Hiina jäägiteoreemi abil. Lahendiks tuleb

$$x \equiv 443 \pmod{3289},$$

mistõttu vähim esimese jagamise käigus tekkiv tekkiv kitseosak on

$$\frac{443-6}{23} = 19.$$

Arvatavasti kitsekari ei sisaldanud tuhandeid kitsi, mistõttu 19 on suhteliselt realistlik vastus.

8. Vastus: $x \equiv 9, 28, 63, 73, 79, 89, 124, 143, 153, 159 \pmod{160}$.
Lahendamismetoodika on sama, mis 8. praktikumi 5. ülesandel (vt. 8. praktikumi tagasisidet). Vahevastused:

$$x \equiv 0, 1, 3 \pmod 4, \quad x \equiv 1, 3, 4, 5, 7 \pmod 8,$$

$$x \equiv 1, 7, 9, 12, 15 \pmod{16}, \quad x \equiv 9, 15, 25, 28, 31 \pmod{32},$$

$$x \equiv 3, 4 \pmod 5.$$

Ainus suurem viga, mida tehti, oli $f'(x_i)$ väljaarvutamine kõigi vahetulemuste jaoks, näiteks $f'(15) = 3258$. Praktikas on vaja ainult $f'(x_i) \pmod 2$, seega piisab, kui leida $f'(0) \pmod 2$ ja $f'(1) \pmod 2$ ning $x_i \pmod 2$. Samuti tasub alati, kus võimalik, arvutada mooduli järgi. Arvutusvahendite abil väikeste arvudega arvutades ei ole erilist vahet, suurte arvudega või eksamil käsitsi tehes aga on küll.

9. Vastus: a) algjuuri ei leidu;
b) 8 algjuurt, millest üks on 27, 3 või 33;
c) algjuuri ei leidu;
d) 54 algjuurt, millest üks on 2.
Suuremaid vigu: valiku 2 või $2 + 5 = 7$ (modulo 25) korral järelduse 7.12 lõpuni mitte kasutamine ja modulo 25 arvu 2 algjuureks oleku kontrollimine

järelduse 7.20 abil. Otseselt vale see ei ole, märgatavalt lisatööd tekitab küll. Teiseks, järelduse 7.12 tõttu tuleb kontrollida, kas

$$2^{5-1} \not\equiv 1 \pmod{25},$$

MITTE

$$2^5 \not\equiv 1 \pmod{25}.$$

10. Vastus:

	0	1	2	3	4	5	6	7	8	9
0		36/1	1/36	26/18	2/18	23/36	27/4	32/9	3/12	16/9
1	24/3	30/6	28/9	11/36	33/12	13/36	4/9	7/36	17/36	35/36
2	25/36	22/18	31/36	15/12	29/36	10/18	12/3	6/6	34/18	21/12
3	14/18	9/4	5/36	20/9	8/9	19/36	18/2			

,

kus esimene arv näitab elemendi indeksit alusel 2 ja teine järku rühmas $\mathbb{Z}_{37}$. Lahendamine käis otse teoreemi 7.33 põhjal, kusjuures eelnevalt tuli kas leida või koostada indeksite tabel.
Vigadest: konspekti definitsiooni kohaselt on indeks positiivne, seega arvu 1 indeks on 36, mitte 0.

11. Vastus: neli lahendit ($795, 7483, 9073$ ja 15761).
Antud kongruents on samaväärne kongruentside süsteemiga

$$\begin{cases} x^2 \equiv 2897 \equiv 1 \pmod{4} \\ x^2 \equiv 2897 \pmod{4139} \end{cases}.$$

Kuna 4139 on algarv ja $\left(\frac{2897}{4139}\right) = 1$, siis on viimasel kongruentsil kaks lahendit. Esimesel kongruentsil on ilmselt kaks lahendit $1, 3 \pmod 4$, seega kokku peab olema $2 \cdot 2 = 4$ lahendit.
Probleeme: lahendite arvude korrutamine alapeatükis 6.5 kirjeldatud meetodil ei ole kõigil ikka veel meeles.

12. Vastus: $2701 = 37 \cdot 73$ on kordarv.
Arv 5 on Fermat' tunnistaja:

$$5^{2700} \equiv 2554 \not\equiv 1 \pmod{2701}.$$

Tegu ei ole Carmichaeli arvuga, sest $(5, 2701) = 1$. Kuna $2^{2700} \equiv 1 \equiv 3^{2700} \pmod{2701}$, siis on tegu nn. *pseudoalgarvuga* alustel 2 ja 3.