Kevad 2015

Märkusi arvuteooria 8. praktikumi kohta:

A. Kommentaare ülesannete kaupa:

1. Üldiselt hästi tehtud. Kaks nõuannet oma tegevuse optimeerimiseks: kasutada absoluutväärtuselt vähimaid jääke (antud juhul $0, \pm1, \pm2, \pm3$) ja lahendi leidmisel jätkata Horneri skeemis jagamist saadud jagatispolünoomiga, st. võttes kordajad edaspidi sellest reast, mille viimane liige tuli null:

	5	4	3	2	5
0	5	4	3	2	5
1	5	2	5	0	5
−1	5	−1	4	−2	0
2	5	2	1	0	
−2	5	−1	3		
3	5	3	3		
−3	5	1	−2		

See võte töötab kahjuks kindlalt vaid siis, kui mooduliks on algarv (siin 7).

2. Selles ülesandes oli komistuskohaks tõsiasi, et esines üks kahekordne juur 1. Eelmise ülesande kommentaarid on ka siin asjakohased, lisaks tasub polünoomi tegurdamisel ühe ja sama lineaarpolünoomiga nii kaua läbi jagada, kuni enam ei jagu (nii saab juure koos kordsusega kätte):

	4	2	3	2	4
0	4	2	3	2	4
1	4	1	4	6	0
1	4	0	4	0	
1	4	4	1		
−1	4	−4	3		
2	4	3	0		
2	4	1			
−2	4	0			

Lisaks jääb kõige viimasest jagamisest alles tegur 4, seega
$f(x) \equiv 4(x-1)^2(x-2)(x+2)$, mitte $f(x) \equiv (x-1)^2(x-2)(x+2)$.

3. Siin võis peale süsteemide

$$\begin{cases} x & \equiv & 1 & \pmod 2 \\ x & \equiv & 0,1,3,4 & \pmod 5 \end{cases}$$

saamist kasutada Hiina jäägiteoreemi, aga tegelikult on lihtsam otse vaadata, et teised kongruentsid annavad võimalikeks lahenditeks $x \equiv 0,5,1,6,3,8,4,9 \pmod{10}$ ja esimene kongruents ütleb, et sobivad vaid paaritud arvud, seega $x \equiv 1,3,5,9 \pmod{10}$.

4. ja 5. Horneri skeem oli siin väga kasulik nii arvutuste lihtsustamiseks kui ülevaatlikkuse säilitamiseks. Muuseas sai viiendas ülesandes kasutada 3. ülesande lahendeid moodulite 2 ja 5 järgi, sest

$$3x^4 + 6x^3 + 2x^2 + 4x + 5 \equiv 3x^4 - 4x^3 + 2x^2 + 4x - 5 \pmod{10}.$$

Kontrollvastused: 4. ülesandes mooduli 125 järgi

$$x \equiv 3,7,18,22,28,32,43,47,53,57,68,72,78,82,93,97,103,107,118,122;$$

5. ülesandes mooduli 450 järgi

$$x \equiv 1,23,73,95,101,145,149,173,199,245,251,299,323,395,401,449.$$

6. Segadust tekitas see, et $**$ võis olla suvaline kahekohaline arv, mitte tingimata samade üheliste ja kümneliste numbritega arv. Muuseas sai lahendamisel kasutada fakti, et juhul, kui $p > 2$ on algarv, siis $x^2 \equiv 1 \pmod p$ omab tänu lausele 2.9 täpselt kahte lahendit $x \equiv \pm 1 \pmod p$ (juhul $p = 2$ langevad need lahendid kokku). Seega $(YX)^2 \equiv 1 \pmod{10}$ annab meile, et $YX \equiv \pm 1 \pmod 5$ ja $YX \equiv 1 \pmod 2$, kust HJT või otsese analüüsi abil $YX \equiv 1,9 \pmod{10}$. Järelikult piisab leida kõik arvudega 1 või 9 lõppevad kahekohalised arvud, mille ruut langeb vahemikku $[2001, 2991]$. Nendeks on 49 ja 51; $49^2 = 2401$ ja $51^2 = 2601$.

7. Suhteliselt väheste poolt lahendatud ülesanne. Näidislahendus: kongruentsil $ax \equiv b \pmod{15}$ on lause 6.2 põhjal täpselt üks lahend, kui $(a, 15) = 1$ ja üks või rohkem lahendit, kui $(a, 15) \mid b$. Esimene juht realiseerub, kui $a \in \{1,2,4,7,8,11,13,14\}$, seega 8 juhul 14 võimalikust. Teine juht koosneb kolmest alamvariandist: $(a, 15) = 1$, nagu esimesel juhulgi; $(a, 15) = 3 \mid b$, mis saab toimuda vaid $a \in \{3,6,9,12\}$ ja $b \in \{3,6,9,12,15\}$ korral, ning $(a, 15) = 5$, milleks on vaja, et $a \in \{5,10\}$ ja $b \in \{5,10,15\}$. Arvestades, et

a valikuks on 14 ja b valikuks 15 teineteisest sõltumatut võimalust, on otsitav tõenäosus

$$\frac{8}{14} + \frac{4}{14} \cdot \frac{5}{15} + \frac{2}{14} \cdot \frac{3}{15} = \frac{73}{105}.$$

8. Muutus *-ülesandeks, sest oli vaid kaks lahendajat. Lahendamiseks on mitmeid meetodeid, ühte esitati praktikumis ja teine oli kirjas vihjete failis.