Kevad 2016

Märkusi arvuteooria 8. praktikumi kohta:

A. Antud praktikumi ülesanded on terve kursuse arvutuslikult keerulisemate hulgast. Seepärast on lahendajate vähesus mõneti murettekitav.

B. Kommentaare ja tüüpvigu ülesannete kaupa:

1. Vastus: $x \equiv 2, 3 \pmod 5$.
Proovimismeetodi käsitsi läbiviimiseks on optimaalne kasutada Horneri skeemi ja arvutada igal sammul modulo 5.
Samuti on otstarbekas jagamisel arvestada vahetulemusi ning arvutada absoluutväärtustuselt vähimate jääkidega (antud juhul $0, \pm 1, \pm 2$). Näide all vasakul:

	6	4	2	4	6
0	6	4	2	4	1
1	6	0	2	1	2
−1	6	−2	4	0	1
(2)	6	1	4	2	(0)
2	6	3	0	2	
(-2)	6	−1	1	(0)	
−2	1	−3	2		

	5	−2	6	7	−2
0	5	−2	6	7	−2
(1)	5	3	2	2	(0)
1	5	1	3	5	
−1	5	−2	4	−2	
2	5	6	0	2	
−2	5	0	2	−2	
3	5	4	0	2	
(-3)	5	2	3	(0)	
(-3)	5	1	(0)		
(-3)	[5]	(0)			

2. Vastus: $f(x) \equiv \boxed{5} \cdot (x+3)^3 \cdot (x+6) \pmod 7$.
Kordsete juurte eraldamisel on järk-järguline jagamine ja juurekandidaatide korduv läbiproovimine eriti olulised, sest tegurdamisel tuleb leida juure kordsus. Kordsust ei saa "juurde teha", nagu praktikumis arvati. Samuti ei tasu ära unustada jagatist (jagamise viimane samm, selles ülesandes 5). Näide ülal paremal.

3. Vastus: $x \equiv 2, 3 \pmod 5$.
Ülesanne taandus kongruentsi

$$5x^4 + 7x^3 + 6x^2 + 2x - 4 \equiv 0 \pmod{10}$$

lahendamisele. Viimast võib teha nii otse modulo 10 kui Hiina jäägiteoreemi abil, lahendades modulo 2 ja modulo 5.

4. Vastus: $x \equiv 6, 22, 13, 14, 30 \pmod{32}$.
Olulistest arvutustest ülevaate omamiseks tasub neid hoida umbes sellises tabelis:

	$f(x)$	5	3	4	-4	$f'(x)$	15	6	0	
(mod 2)	0	1	1	0	0	0	1	0	$\boxed{0}$	
	1	1	0	0	0	1	1	1	$\boxed{1}$	
(mod 4)	0	1	1	0	$\textcircled{0}$					$\boxed{0}y + \frac{\textcircled{0}}{2} \equiv 0 \pmod 2$
	1	1	0	0	$\textcircled{0}$					$\boxed{1}y + \frac{\textcircled{0}}{2} \equiv 0 \pmod 2$
(mod 8)	0	5	3	4	$\textcircled{4}$					$\boxed{0}z + \frac{\textcircled{4}}{4} \equiv 0 \pmod 2$
	1	5	0	0	$\textcircled{4}$					$\boxed{1}z + \frac{\textcircled{4}}{4} \equiv 0 \pmod 2$
	2	5	5	2	$\textcircled{0}$					$\boxed{0}z + \frac{\textcircled{0}}{4} \equiv 0 \pmod 2$
(mod 16)	2	5	13	10	$\textcircled{0}$					$\boxed{0}u + \frac{\textcircled{0}}{8} \equiv 0 \pmod 2$
	5	5	12	-4	$\textcircled{8}$					$\boxed{1}u + \frac{\textcircled{8}}{8} \equiv 0 \pmod 2$
	6	5	1	6	$\textcircled{0}$					$\boxed{0}u + \frac{\textcircled{0}}{8} \equiv 0 \pmod 2$
(mod 32)	2	5	13	26	$\textcircled{16}$					$\boxed{0}v + \frac{\textcircled{16}}{16} \equiv 0 \pmod 2$
	6	5	1	6	$\textcircled{0}$					$\boxed{0}v + \frac{\textcircled{0}}{16} \equiv 0 \pmod 2$
	10	5	21	18	$\textcircled{16}$					$\boxed{0}v + \frac{\textcircled{16}}{16} \equiv 0 \pmod 2$
	13	5	4	20	$\textcircled{0}$					$\boxed{1}v + \frac{\textcircled{0}}{16} \equiv 0 \pmod 2$
	14	5	9	-2	$\textcircled{0}$					$\boxed{0}v + \frac{\textcircled{0}}{16} \equiv 0 \pmod 2$

5. Vastus: $x \equiv 7, 123, 223, 447 \pmod{540}$.
Kuna $540 = 3^3 \cdot 2^2 \cdot 5$, siis tuleb lahendada eraldi modulo $27, 4$ ja 5. Modulo 4 tasub tegelikult kasutada proovimismeetodit, sest järk-järguline lahendamine mooduli väiksuse tõttu erilist võitu ei anna. Muuseas saab lahendamisel kasutada ülesande 3 vastust, sest

$$5x^4 - 3x^3 - 4x^2 + 2x + 6 \equiv 5x^4 + 7x^3 + 6x^2 + 2x - 4 \pmod{10}.$$

Kontrolli mõttes annan siin ka vahevastused:

$x \equiv 0, 1 (\text{mod } 3), x \equiv 6, 7 (\text{mod } 9), x \equiv 7, 15 (\text{mod } 27), x \equiv 3 (\text{mod } 4), x \equiv 2, 3 (\text{mod } 5).$

6. Vastus: $\ddot{U}KS \in \{149, 151\}$.
Siin võis kümnendkujuga otse manipuleerida, aga üks lihtne võimalus lahendada on võtta $x := \ddot{U}KS$ ja lahendada kongruents

$$x^2 = 100u + 1 \equiv 1 \pmod{100},$$

kus $u = \underline{2 * *}$. Analoogiliselt 8. ülesandega võib tähele panna, et kui

$$x^2 - 1 = (x+1)(x-1) \equiv 0 \pmod{p^2},$$

kus $p \in \mathbb{P}$, siis Eukleidese lemma ja $(x+1, x-1) = 1$ tõttu (juhul $x > 0$, mis praegu kehtib) jagab p täpselt ühte arvudest $(x+1)$ ja $(x-1)$. Kuna p on algarv, siis jagab ka p^2 sedasama arvu, ehk

$$x \equiv \pm 1 \pmod{p^2}.$$

Moodul on $100 = 2^2 \cdot 5^2$, järelikult tekib meil kongruentside süsteem

$$\begin{cases} x^2 \equiv 1 & \pmod{2^2} \\ x^2 \equiv 1 & \pmod{5^2} \end{cases},$$

mis on eelneva arutelu põhjal samaväärne nelja kongruentside süsteemiga

$$\begin{cases} x \equiv \pm 1 & \pmod{2^2} \\ x \equiv \pm 1 & \pmod{5^2} \end{cases}.$$

Kaks lahendit on ilmsed (1 ja -1), ülejäänud kaks (49 ja 51) on leitavad Hiina jäägiteoreemi abil. Ülesande lahend $x = \ddot{U}KS$ peab kuuluma vahemikku

$$[\sqrt{20001}, \sqrt{29901}] \subseteq [142, 172],$$

seega sobivad ainult $100 + 49$ ja $100 + 51$.

7. Selle ülesande lahendas ära ainult üks üliõpilane. Seetõttu toon ära täieliku lahenduse:
Kui polünoom $f(x)$ ei ole nullpolünoom modulo p, siis lause 2.9 põhjal on tal maksimaalselt $p-2$ juurt korpuses $\mathbb{Z}_p$, sest selle polünoomi aste on $p-2$ (kõrgema astme liikmed x^{p-1} koonduvad). Fermat' väikese teoreemi kohaselt

$$a^{p-1} \equiv 1 \pmod{p},$$

kui $a = 1, 2, \ldots, p-1$. Seega

$$f(a) = (a-1)\cdot\ldots\cdot(a-a)\cdot\ldots\cdot(a-(p-1)) - a^{p-1} + 1 \equiv 0 + 0 = 0 \pmod{p}$$

iga $a = 1, 2, \ldots, p-1$ korral. Viimaseid väärtusi on kokku $p-1$ tükki ja nad on kõik erinevad modulo p, seega $f(x)$ peab olema nullpolünoom modulo p. See aga tähendabki, et kõik selle polünoomi kordajad on kongruentsed nulliga

modulo p, ehk p jagab kõiki neid kordajaid.
Lisaks võib tähele panna, et Wilsoni teoreemi kohaselt tegelikult ka

$$f(0) = (p-1)! + 1 \equiv -1 + 1 = 0 \pmod{p}.$$

8. Kehtigu $p \in \mathbb{P}$, $a, \in \mathbb{Z}$, $(a, p) = 1$. Lahendamiseks sobib induktsioon k järgi. Baas $k = 1$ on juba ülesande eelduseks. Näitame, et kui kongruents

$$x^2 \equiv a \pmod{p^k}$$

on lahenduv, siis on seda ka kongruents

$$x^2 \equiv a \pmod{p^{k+1}}.$$

Olgu

$$a \equiv b^2 \pmod{p^k},$$

st.

$$b^2 = a + l \cdot p^k,$$

$l \in \mathbb{Z}$. Otsime lahendit modulo p^{k+1} kujul

$$b + t \cdot p^k$$

(lahend modulo p^{k+1} peab olema ka lahend modulo p^k ja olemasolevale lahendile b modulo p^k vastavad just sellised võimalikud lahendid modulo p^{k+1}).
Asendame:

$$a = (b + t \cdot p^k)^2 = b^2 + 2btp^k + (t \cdot p^k)^2 \equiv a + l \cdot p^k + 2btp^k \pmod{p^{k+1}}.$$

Seega taandub lahendi otsimine kongruentsi

$$l \cdot p^k + 2btp^k \equiv 0 \pmod{p^{k+1}}$$

lahendamisele t suhtes. Jagame läbi teguriga p^k ja saame uue kongruentsi

$$2bt \equiv -l \pmod{p}.$$

Nüüd tasub vaid tähele panna, et $(2, p) = 1 = (b, p)$, sest p on paaritu ja kui $p \mid b$, siis ka $p \mid a$, mis on vastuolus ülesande eeldustega. Teoreem 4.10 tõttu leiduvad arvudel 2 ja b pöördelemendid modulo p, kust

$$t \equiv -l \cdot 2^{-1} \cdot b^{-1} \pmod{p}.$$

Seega on eelnev kongruents lahenduv t suhtes ja lahendile t_0 vastab kongruentsi $x^2 \equiv a \pmod{p^{k+1}}$ lahend

$$x = b + t_0 \cdot p^k.$$

Eeltoodud lahenduses saab mõned sammud vahele jätta, kui lugeda teadaolevaks loengukonspekti alajaotuses 6.4 sisalduv materjal.
Fakt $(b, p) = 1$ on lahenduse seisukohalt väga oluline ja see vajab kindlasti ülekontrollimist.