Kevad 2016

Märkusi arvuteooria 12. praktikumi kohta:

A. Üks üldine märkus: kirjutatakse $e \in \{a, b, c, \ldots\}$, mitte $e = \{a, b, c, \ldots\}$. Viimane võrdus tähendab juba sootuks midagi muud.

B. Kommentaare ja tüüpvigu ülesannete kaupa:

1. Vastus: $\mathrm{ind}_2 8 = 3, \mathrm{ind}_8 8 = 1, \mathrm{ind}_6 8 = 7, \mathrm{ind}_7 8 = 9$. Kõigepealt on vaja leida algjuured $2, 6, 7, 8$, mida saab teha järelduste 7.10 ja 7.21 abil. Indekseid on siin lihtne leida otse astendades, aga võib kasutada ka seoseid

$$\mathrm{ind}_x 8 \equiv \mathrm{ind}_x 2 \cdot \mathrm{ind}_2 8 \pmod{10} \quad \text{ja} \quad \mathrm{ind}_x 2 \cdot \mathrm{ind}_2 x \equiv 1 \pmod{10}.$$

2. Vastus:

	0	1	2	3	4	5	6	7	8	9
0		16	6	13	12	1	3	15	2	10
1	7	11	9	4	5	14	8			

Ülaltoodud tabeli võib leida otse astendades, aga saab kasutada ka indeksite tabelit alusel 3 (näiteks E. Redi õpikust) ja fakti $\mathrm{ind}_5 3 = 13$.
Siin oli vaja üle kontrollida, et 5 tõepoolest on algjuur. Seda ei ole mõtet teha järjest astendades, selleks on meil järeldus 7.21.

3. Vastus:

	0	1	2	3	4	5	6	7	8	9
0		16	10	3	4	15	13	1	14	6
1	9	5	7	12	11	2	8			

Jälle pidi kontrollima, et 7 on algjuur.
Kui ülesandes on öeldud, et tuleb midagi kasutada, siis ilma seda kasutamata ei ole lahendus korrektne.
Meie definitsiooni järgi ei ole indeks kunagi 0, selle asemel on $\varphi(n)$.

4. Vastus: $x \equiv 22 \pmod{31}$. Antud ülesandes oli näha, miks suuremate n väärtuste korral oleks hea omada ka nn. antiindeksite tabelit (indeksi järgi jäägiklassi leidmine vastupidiselt jäägiklassi indeksi leidmisele).
Kui juba kongruentsi lahendada vaja on, ei ole suurt mõtet teoreemi 7.30 abil lahenduvust kontrollida, sest mittelahenduvus tuleb lahendamise käigus

niikuinii välja.
Pöördelemendi leidmiseks on efektiivne Eukleidese algoritm, ei tasu kasutada valemit $a^{-1} \equiv a^{\varphi(n)-1} \pmod{n}$.
Kongruentsi $x^n \equiv a \pmod{n}$ korral ei pruugi x olla algjuur (leidus lahendajaid, kes arvasid, et x seda alati on).

5. Vastus: $x \equiv 4 \pmod{14}$ või $x \equiv 4, 18 \pmod{28}$. Indeksite korral on kongruentsid modulo $\varphi(29) = 28$, mitte modulo 29.

6. Vastus: kui $p = 7$, siis $a \in \{1, 2, 4\}$;
kui $p = 11$, siis $a \in \{1, 3, 4, 5, 9\}$;
kui $p = 13$, siis $a \in \{1, 3, 9\}$.
Lahenduvuse kontrolli sai teoreemi 7.30 abil taandada kongruentside $x^3 \equiv 1 \pmod{7}$, $x^5 \equiv 1 \pmod{11}$, $x^3 \equiv 1 \pmod{13}$ lahendamisele. Viimast võis mooduli väiksuse tõttu teha nii otse läbi proovides kui indekseerimise teel.

7. Lahendada sai kas otse teoreemi 7.31 abil või indekseerides ja rakendades lauset 6.2. Mõlemad annavad, et kui lahendeid leidub, siis on neid $(3, p-1) = 3$ tükki.

8. Kogu ülesanne taandub tähelepanekule, et tõestamist vajav fakt on tegelikult teguriga $p - 1$ taandatud Wilsoni teoreemi väide

$$(p-1)! \equiv -1 \pmod{p}.$$