Kevad 2015

Märkusi arvuteooria 11. praktikumi kohta:

A. Kommentaare ülesannete kaupa:

1. Mõned märkused arvutuste optimeerimise kohta: esiteks, algjuureks olekut tasub kontrollida järelduse 7.21 abil, sest siis on vaja välja arvutada suhteliselt vähe astmeid, antud ülesandes $\frac{42}{7} = 6$, $\frac{42}{3} = 14$ ja $\frac{42}{2} = 21$. Ei ole mõttekas välja arvutada kõiki astmeid ühest $\varphi(n)$-ni, ega isegi mitte kõiki $\varphi(n)$ jagajateks olevaid astmeid. Astmete arvutamist on mõistlik teha samm-sammult:

$$3^6 = 9 \cdot 81 \equiv 9 \cdot (-5) = -45 \equiv -2 \equiv 41 \pmod{43},$$

$$3^{14} = (3^6)^2 \cdot 3^2 \equiv (-2)^2 \cdot 9 = 36 \equiv -7 \pmod{43},$$

$$3^{21} = 3^6 \cdot 3^{14} \cdot 3 \equiv (-2) \cdot (-7) \cdot 3 = 42 \equiv -1 \pmod{43}.$$

Viimane tulemus on annab muuseas võimaluse arvutuste õigsust kontrollida, sest algjuure $\frac{\varphi(n)}{2}$ -s aste peab alati olema -1. Kõigi algjuurte leidmiseks ei ole mõistlik kontrollida algjuureks olekut eraldi iga $1 \leq a \leq \varphi(n)$ jaoks, isegi mitte järelduse 7.21 abil. Parem on leida üks (suurte vahetulemuste vältimiseks võimalikult väike) algjuur ja siis kasutada järeldust 7.10. Antud juhul on 3 algjuur ja seega kõik algjuured mooduli 43 järgi on $3, 3^5 \equiv 28, 3^{11} \equiv 30, 3^{13} \equiv 12, 3^{17} \equiv 26, 3^{19} \equiv 19, 3^{23} \equiv 34, 3^{25} \equiv 5, 3^{29} \equiv 18, 3^{31} \equiv 33, 3^{37} \equiv 20, 3^{41} \equiv 29 \pmod{43}$. Siin on samuti arukas teha arvutusi järk-järgult, näiteks

$$3^{23} = 3^{19} \cdot 3^4 \equiv 19 \cdot 81 \equiv 19 \cdot (-5) = -95 \equiv 34 \pmod{43}.$$

Lõpptulemust saab kontrollida järelduse 7.24 abil, nimelt peab kokku olema $\varphi(\varphi(n))$ algjuurt, antud juhul siis $\varphi(\varphi(43)) = \varphi(42) = 12$ algjuurt, mis meil tõepoolest kõik olemas on.

2-3. Jälle, algarvulise mooduli järgi on optimaalne üks algjuur leida järelduse 7.21 abil. Lisaks tasub vaadata 2014. a. arvuteooria 10. praktikumi 2. ülesande tagasisidet, kus on kirjas optimaalne meetod teoreemide 7.11, 7.15

ja 7.16 kasutamise kohta algjuurte leidmiseks. Käesoleva aasta ülesannetes tuleks moodulite osas liikuda skeemide

$$7 \to 7^2, 5 \to 5^2 \to 2 \cdot 5^2, 3 \to 3^2 \to 3^4$$

abil. Näiteks mooduli 50 järgi leiame esmalt algjuure mooduli 5 järgi, milleks sobib näiteks 2, sest $2^{\frac{5-1}{2}} = 4 \not\equiv 1 \pmod 5$. Seejärel testime $2^{5-1} = 16 \not\equiv 1 \pmod{25}$ (kui see nii ei oleks, siis sobiks algjuureks $2 + 5 = 7$). Seega 2 on algjuur ka mooduli 5^2 järgi. Lõpuks võtame paaritu arvudest 2 ja $2+5^2 = 27$, milleks on 27. See ongi algjuur mooduli $2 \cdot 5^2 = 50$ järgi.

4. Siin oli võimalik kasutada teoreemi 7.30, aga ülesannet võis lahendada ka lemma 7.3 abil. Viimast võimalust eriti ei kasutatud, seega visandan siinkohal sel viisil saadud lahenduse. Ei ole raske kontrollida, et 2 on algjuur mooduli 13 järgi. Ilmselt $x \not\equiv 0 \pmod{13}$, seega 13 algarvulisuse tõttu on $\overline{x}$ pööratav ja $x \equiv 2^k$ mingi $1 \leq k \leq 12$ jaoks. Siis

$$2^{15k} \equiv 2^3 \pmod{13}, \quad \text{ehk} \quad 2^{15k-3} \equiv 1 \pmod{13}$$

kust lemma 7.3 tõttu saame, et $\varphi(13) = 12 \mid 15k - 3$. Viimane samm on tegelikult formaliseeritud lemmas 7.28 ja see on põhimõtteliselt indekseerimine. Järelikult $4 \mid 5k - 1$, ning vahemikust $[1, 12]$ rahuldavad seda seost vaid $k = 1, 5, 9$. Seetõttu on lahenditeks $2, 2^5 \equiv 6, 2^9 \equiv 5 \pmod{13}$. Teise kongruentsiga sama protseduuri läbi viies on tulemuseks, et $12 \mid 16k - 3$ ehk $16k \equiv 3 \pmod{12}$, mis ei ole lause 6.2 tõttu lahenduv, sest $(16, 12) = 4 \not| 3$.

Mitmed lahendajad kasutasid mingil kujul indeksarvutust, aga kahjuks ei suutnud keegi seda päris veatult teha. Positiivsema poole pealt, nii mõnigi lahendaja lihtsustas esialgsed kongruentsid Fermat' väikese teoreemi abil kujule $x^3 \equiv 8 \pmod{13}$ ja $x^4 \equiv 8 \pmod{13}$. Hästi tehtud!

5. Paar lahendajat kasutasid siin Horneri skeemi ja viisid läbi tohutud arvutused, et proovimismeetodil lahendeid leida. Otseselt vale see just ei ole, ebaratsionaalne aga küll. Parem on tähele panna, et

$$(x - 1)(x^7 + \ldots + x + 1) = x^8 - 1 \equiv 0 \pmod{41}.$$

Kuna 41 on algarv ja seega $\mathbb{Z}_{41}$ on korpus, kus ei ole nullitegureid, siis kas $x \equiv 1 \pmod{41}$ või $x^8 \equiv 1 \pmod{41}$. Viimase kongruentsi saame lahendada algjuurte abil samamoodi, nagu eelmises ülesandes. Vastuseks tuleb $x \equiv 1, 3, 9, 14, 27, 32, 38, 40 \pmod{41}$. Kuna me aga vahesammuna korrutasime läbi teguriga $x-1$, mis võib olla 0, siis tasub lahendit $x \equiv 1 \pmod{41}$ eraldi kontrollida. Ja tõepoolest on tegu võõrlahendiga, sest

$$1 + 1 + 1^2 + 1^3 + 1^4 + 1^5 + 1^6 + 1^7 = 8 \not\equiv 0 \pmod{41}.$$

6. Millegipärast osutus *-ülesandeks. Siin tasub tähele panna, et $\overline{x}$ peab olema pööratav $\mathbb{Z}_{p^2}$-s, sest muidu $p \mid x$ ja x^{p-1} sisaldab $p > 2$ tõttu vähemalt tegurit p^2. Seega $x \equiv a^k \pmod{p^2}$,

$$x^{p-1} \equiv a^{k(p-1)} \pmod{p^2},$$

ja lemma 7.3 tõttu $\varphi(p^2) = p(p-1) \mid k(p-1)$. Järelikult $p \mid k$ ja $\overline{x}$ peab olema üks ülesandes toodud jäägiklassidest. Teiselt poolt on lihtne välja arvutada, et kõik need jäägiklassid on tõepoolest lahenditeks.

Siin oli tegemist piisava ja tarviliku tingimusega ja nii mõnelgi lahendajal jäi punkt saamata, sest nad viisid korrektselt läbi ainult kas piisavuse või tarvilikkuse osa.

7. Osutus, et ei olnudki väga lihtne tähele panna, et

$$a^{p-2} \cdot a = a^{p-1} \equiv 1 \pmod{p}$$

ja $(p-2, p-1) = 1$. Järeldus 7.10 annab siis kohe, et a^{p-2} on samuti algjuur.

8. Pool sellest ülesandest sisaldus 10. praktikumi 8. ülesandes, nimelt fakt, et antud eeldustel $a^{\frac{p-1}{2}} \equiv -1 \pmod{p}$. Nüüd jäi järgi vaid näha, et $\frac{p-1}{2} = 2k+1$ on paaritu ja seega $(-a)^{\frac{p-1}{2}} \equiv -(a^{\frac{p-1}{2}}) \equiv 1 \pmod{p}$. Siis aga ei saa $-a$ olla algjuur, sest elemendi $\overline{-a}$ järk rühmas $U(\mathbb{Z}_p)$ on eelneva põhjal maksimaalselt $\frac{p-1}{2}$, aga algjuure järk peaks olema $\varphi(p) = p - 1$.