Kevad 2015

Märkusi arvuteooria 12. praktikumi kohta:

A. Kommentaare ülesannete kaupa:

1. Üldiselt lahendati ülesanne kenasti ära, aga mõnes kohas saab arvutusi ratsionaalsemalt teha. Algjuureks olekut tasub kontrollida järelduse 7.21 abil (näiteks $2^{\frac{12}{3}} = 2^4 \equiv 3 \not\equiv 1, 2^{\frac{12}{3}} = 2^4 \cdot 2^2 \equiv 3 \cdot 4 \equiv 12 \not\equiv 1 \pmod{13}$) ja kõiki algjuuri leida järelduse 7.10 põhjal:

$$2, 2^5 = 32 \equiv 6, 2^7 = 2^5 \cdot 2^2 \equiv 6 \cdot 4 \equiv 11, 2^{11} = (2^5)^2 \cdot 2 \equiv 6^2 \cdot 2 \equiv 7 \pmod{13}.$$

Üks korduv probleem kirjalike lahendustega seisnes selles, et mitte ühtegi arvutust ei olnud kirja pandud. Mul ei ole võimalik hinnata, kas ja kuidas te ülesannet lahendanud olete, kui te ainult vastuse üles märgite.

Kontrollvastus: $\operatorname{ind}_2 8 = \operatorname{ind}_6 8 = 3, \operatorname{ind}_7 8 = \operatorname{ind}_{11} 8 = 9$.

2. Seda, et arv 3 on algjuur mooduli 19 järgi, tuleb eraldi kontrollida. Ja uuesti kordus probleem arvutuste mitte välja kirjutamisega.

Siin oli tegelikult kaks lahendusvarianti: arvutada välja kõik arvu 3 astmed kuni tuleb vastu $3^{18} \equiv 1 \pmod{19}$. Iga astme indeksiks ongi siis vastav astendaja, näiteks $3^{11} = 10$, seega $\operatorname{ind}_3 10 = 11$. Teine meetod on võtta mõni juba olemasolev indeksite tabel (tüüpiliselt alusel 2) ja teisendada see valemi

$$\operatorname{ind}_3 x = \operatorname{ind}_3 y \cdot \operatorname{ind}_y x$$

abil otsitavaks tabeliks (y on siin juba olemasoleva tabeli alus, tavaliselt $y = 2$). Teisendamine seisneb lihtsalt terve tabeli arvuga $\operatorname{ind}_3 y$ läbikorrutamises (modulo 19).

3. Lahendusmeetod seisnes jälle samas tähelepanekus, et

$$\operatorname{ind}_3 x = \operatorname{ind}_3 2 \cdot \operatorname{ind}_2 x.$$

Järelikult tuleb alusel 3 oleva indeksite tabeli leidmiseks eelmises ülesandes saadud tabeli kõik lahtrid läbi korrutada arvuga 5 (modulo 19).

Muuseas, kui ülesande sõnastuses on "Leida X, kasutades fakti Y", siis fakt Y tuleb ka ära kasutada. Õige, aga selle sammuta lahendus on väärt heal juhul vaid pooli punkte.

4. Indekseerimisel kasutatavaid indekseid on hea võtta juba mõnest olemasolevast tabelist, näiteks E. Redi arvuteooria õpikust. Kuna antud kongruents on lahenduv, siis ei olnud suurt mõtet teoreemi 7.30 abil kontrollimisel, kas tegu on lahenduva kongruentsiga. Lihtsalt lahendamine annab täpselt sama tulemuse. Küll on aga kontrollimisel abiks sellesama teoreemi väide, et erinevaid lahendeid (modulo 29) on $(28, 8) = 4$ tükki. Nendeks on $x \equiv 3, 7, 22, 26 \pmod{29}$.

Lisamärkus: kui te kirjutate $\operatorname{ind} x$ ilma aluseta, siis peab alus kas olema kontekstist leitav või ei tohi sellest alusest midagi sõltuda.

5. Täpselt seesama märkus aluste puudumise kohta. Pöördelemendi leidmine tasub ka alati läbi teha, mitte lihtsalt kirjutada á la $(\overline{19}_{22})^{-1} = \overline{7}_{22}$. Mina ei saa niiviisi aru, kas te ikka oskate pöördelementi leida, ja teie ei saa kontrollida, kas kasutatud meetod on ikka korrektne.

6. Teoreemi 7.30 saab rakendada vaid siis, kui $p \nmid b$, st. vastavalt $b \neq 7, 14$ või $b \neq 11$ või $b \neq 19$. Viimaseid juhte tuleb eraldi vaadelda ja üleüldse on ülevaatlikkuse huvides hea vahevastused iga juhu ($p = 7, 11, 19$) jaoks eraldi välja kirjutada.

Põhimõtteliselt võis lahendada kõik juhud eraldi ja siis leida lahendite ühisosa, aga efektiivsem on seda teha järk-järguliselt (asendada eelmised vastused järgmisesse kongruentsi). Indekseid võib sel juhul leida kas otse või mõnest indeksite tabelist. Kristo Väljakol oli selline, väga ülevaatlik lahendus:

"Ülesande lahendamiseks kasutan teoreemi 7.30. Selle teoreemi eeldus on $(b, n) = 1$, kus $n = 7, 11, 19$. Sellised täisarvud vahemikust $[1, 19]$, mille korral see eeldus ei kehti (7,11,14,19) vaatan pärast eraldi. Uurin, millised arvud sobivad mooduli 7 korral. Sel juhul peab b rahuldama teoreemis 7.30 antud seost.

$$b^{\frac{\varphi(7)}{(4,\varphi(7))}} = b^{\frac{6}{2}} = b^3 \equiv 1 \pmod{7}$$

Lahendan saadud kongruentsi analoogiliselt eelise ülesandega. Esiteks indekseerin kongruentsi.

$$3 \operatorname{ind} b \equiv \operatorname{ind} 1 = 0 \pmod{6}$$

Jagan selle kongruentsi läbi arvuga 3.

$$\operatorname{ind} b \equiv 0 \pmod{2}$$

Valides arve täisarvude lõigust $[1, 6]$ saame, et $\operatorname{ind} b \equiv 0, 2, 4 \pmod{6}$. Nüüd indeksite tabelist tagurpidi vaadates saame, et $b \equiv 1, 2, 4 \pmod{7}$. Nüüd

vaatan nendega kongruentseid arve vahemikust $[1, 19]$.

$$b \equiv 1, 8, 15; 2, 9, 16; 4, 11, 18 \pmod 7$$

Uurin, millised arvud sobivad mooduli 11 korral. Sel juhul peab b rahuldama seost:

$$b^{\frac{\varphi(11)}{(4,\varphi(11))}} = b^{\frac{10}{2}} = b^5 \equiv 1 \pmod{11}$$

Esiteks indekseerin kongruentsi.

$$5 \operatorname{ind} b \equiv \operatorname{ind} 1 = 0 \pmod{10}$$

Jagan selle kongruentsi läbi arvuga 5.

$$\operatorname{ind} b \equiv 0 \pmod 2$$

Valides arve täisarvude lõigust $[1, 10]$ saame, et $\operatorname{ind} b \equiv 0, 2, 4, 6, 8 \pmod{10}$. Nüüd indeksite tabelist tagurpidi vaadates saame, et $b \equiv 1, 4, 5, 9, 3 \pmod{11}$. Nüüd vaatan nendega kongruentseid arve vahemikust $[1, 19]$.

$$b \equiv 1, 12; 3, 14; 4, 15; 5, 16; 9 \pmod{11}$$

Uurin, millised arvud sobivad mooduli 19 korral. Sel juhul peab b rahuldama seost:

$$b^{\frac{\varphi(19)}{(4,\varphi(19))}} = b^{\frac{18}{2}} = b^9 \equiv 1 \pmod{19}$$

Esiteks indekseerin kongruentsi.

$$9 \operatorname{ind} b \equiv \operatorname{ind} 1 = 0 \pmod{18}$$

Jagan selle kongruentsi läbi arvuga 9.

$$\operatorname{ind} b \equiv 0 \pmod 2$$

Valides arve täisarvude lõigust $[1, 18]$ saame, et $\operatorname{ind} b \equiv 0, 2, 4, 6, 8, 10, 12, 14, 16 \pmod{18}$. Nüüd indeksite tabelist tagurpidi vaadates saame, et $b \equiv 1, 4, 16, 7, 9, 17, 11, 6, 5 \pmod{19}$.
Kirjutan kõik saadud arvud korraga välja, et oleks lihtsam vastust näha.

$$b \equiv 1, 2, 4, 8, 9, 11, 15, 16, 18 \pmod 7$$
$$b \equiv 1, 3, 4, 5, 9, 12, 14, 15, 16 \pmod{11}$$
$$b \equiv 1, 4, 5, 6, 7, 9, 11, 16, 17 \pmod{19}$$

Nagu näha, on kõikide moodulitega korraga sobivad arvud:

$$1, 4, 9, 16.$$

Näen, et lisaks neile neljale arvule, sobib arvuks b ka 11, kuna tema korral on teoreemi 7.30 järgi lahenduvad kongruentsid $x^4 \equiv b$ moodulite 7 ja 19 korral ning mooduli 11 korral on ilmseks lahendiks $x \equiv 0$. (Ülejäänud teoreemi eeldustele mittevastavate arvudega lahenduvust ei teki.)
Teisisõnu

$$b \in \{1, 4, 9, 11, 16\}.$$

Kõige parem on aga otse indekseerida. Illimar Gross tegi seda väga lühidalt: "Teoreemi 7.29 omaduse 6 järgi saame

$$\begin{aligned} 4 \cdot \operatorname{ind} x &\equiv \operatorname{ind} b \pmod 6 \\ 4 \cdot \operatorname{ind} x &\equiv \operatorname{ind} b \pmod{10} \\ 4 \cdot \operatorname{ind} x &\equiv \operatorname{ind} b \pmod{18} \end{aligned}$$

Nendel kongruentsidel on lahendid olemas parajasti siis kui ind$b$ jagub 2-ga. Seega tuleb leida indeksite tabelitest $p = 7$, $p = 11$, $p = 19$ arvud, mille indeksite väärtused on korraga kõigi moodulite tabelites paarisarvud.

Nendeks on arvud $4, 9, 11, 16$."
Kahega jaguvuse kriteerium tuleb siin lausest 6.2. Muuseas on antud lahenduses näha mitmes töös korduv viga, kus arv 1 on millegipärast lahendite seast välja jäetud.

7. Algjuurte kasutamisel on vaja kontrollida, et $-\overline{1} = \overline{p-1}$ on pööratav, st. $(p, p-1) = 1$.

8. Potentseerides ja arvuga $p-1$ läbi korrutades taandub ülesanne väitele

$$1 \cdot 2 \cdot \ldots \cdot (p-2) \cdot (p-1) \equiv 1 \cdot (p-1) \equiv -1 \pmod p.$$

See on 10. praktikumis juba (pooleldi, aga siin ülesandes vajalik pool) tõestatud Wilsoni teoreem. Oli ka alternatiivseid lahendusi, mille kõigi ühisosa oli fakt $a^{\frac{p-1}{2}} \equiv -1 \pmod p$, kui $p > 2$ on algarv ja a algjuur mooduli p järgi. Selle tõestus on kirjas loengukonspektis ja me oleme seda juba kaks praktikumi järjest tõestanud, aga ikka leidub lahendajaid, kelle jaoks ei ole see kuigi selge. Kui te ei saa lahendusest aru, siis küsige kohe, mitte ärge leiutage kaks praktikumi hiljem imeseletusi. Te ei peagi kõigest kohe aru saama, aga lõpuks küll. Lektori ja/või praktikumijuhendaja põhiline kasutegur seisnebki selles, et tema käest saab segaseid kohti üle küsida.