Kevad 2016

Märkusi arvuteooria 11. praktikumi kohta:

A. Algjuuri on väikeste n väärtuste korral võimalik leida ka indeksite tabeli ja teoreemi 7.33 abil (järgmise praktikumi teema).

B. Kommentaare ja tüüpvigu ülesannete kaupa:

1. Vastus: algjuured mooduli 31 järgi on

$$\{3, 3^7, 3^{11}, 3^{13}, 3^{17}, 3^{19}, 3^{23}, 3^{29}\} \equiv \{3, 11, 12, 13, 17, 21, 22, 24\} \pmod{31}.$$

Esiteks saab kontrollida, et $3^6 \not\equiv 1, 3^{10} \not\equiv 1, 3^{15} \not\equiv 1 \pmod{31}$. Järelduse 7.21 põhjal on siis 3 algjuur ja järelduse 7.10 tõttu avalduvad ülejäänud algjuured eeltoodud kujul. Astendamist ot mõttekas läbi viia selliselt:

$$3^7 = (3^3)^2 \cdot 3 = 27^2 \cdot 3 \equiv (-4)^4 \cdot 3 = 16 \cdot 3 = 48 \equiv 17 \pmod{31};$$

$$3^{13} = (3^3)^4 \cdot 3 \equiv 16^2 \cdot 3 \equiv 16 \cdot 17 \equiv 16 \cdot (-14) = -224 \equiv 24 \pmod{31};$$

$$3^{17} = (3^7)^2 \cdot 3^3 \equiv 17^2 \cdot (-4) \equiv 10 \cdot (-4) = -40 \equiv 22 \pmod{31}.$$

Oma tulemuse kontrolliks võib arvutada, et $\varphi(31) = 8$, ja me oleme tõepoolest leidnud 8 erinevat algjuurt.

2. Vastus: a) 32 algjuurt, millest üks on 5;
b) 12 algjuurt, millest üks on 3;
c) algjuuri ei leidu.

Algjuurte arvuks on $\varphi(\varphi(n))$, KUI algjuuri leidub.
Alamülesandes b) saab kasutada järeldust 7.20 juhul $n = 7^2$, aga efektiivsem on kasutada järeldust 7.21 juhul $n = 7$ ja järeldust 7.12.

3. Vastus: a) 40 algjuurt, millest üks on 127;
b) algjuuri ei leidu;
c) 36 algjuurt, millest üks on 3.

Algjuureks oleku kontrollis järelduse 7.21 abil tuleb kontrollida, kas $a^{\frac{p-1}{q}} \equiv 1 \pmod{p}$, mitte $a^q \equiv 1 \pmod{p}$.

4. Vastus: $x \equiv 2, 4, 8, 15, 16, 23, 27, 29, 30 \pmod{31}$.
Kui uuritavat kongruentsi korrutada teguriga $x - 1$, siis tekib kongruents

$x^{10} \equiv 1 \pmod{31}$. Kuna $10 \not\equiv 0 \pmod{31}$, siis 1 ei ole esialgse kongruentsi lahend ja kõik lahendid on võimalik leida, kui lahendada kongruents

$$x^{10} \equiv 1 \pmod{31}$$

ja jätta lahendite seast välja 1. Viimase kongruentsi lahendamisel võib tundmatu x asendada mingi algjuure astmega a^k ja lahendada tundmatu k suhtes. Ülesande 1. põhjal on 3 algjuur, seega tekib kongruents

$$3^{10k} \equiv 1 \pmod{31}.$$

Tänu lemmale 7.3 on viimane väide samaväärne sellega, et

$$\varphi(31) = 30 \mid 10k$$

ehk $3 \mid k$. Seega

$$k \in \{3, 6, 9, 12, 15, 18, 21, 24, 27, 30\}$$

ja

$$x \in \{1, 2, 4, 8, 15, 16, 23, 27, 29, 30\}.$$

Ülesannet võis muidugi lahendada ka proovimismeetodil näiteks Horneri skeemi abil, sest 30 arvu läbiproovimine ei ole väga töömahukas.
Tüüpvigu: puudujääke oli selle põhjendamisel, miks võib üle minna kongruentsile $x^{10} \equiv 1 \pmod{31}$. Samuti ei põhjendatud seost $30 \mid 10k$ ning mõnikord jäeti 1 vastusena siiski sisse.

5. Kogu ülesanne taandus kongruentsile

$$4^{\frac{p-1}{2}} = 2^{p-1} \equiv 1 \pmod{p}.$$

Eraldi tuleb vaadelda juhtu $p = 2$, sest ainult sel juhul $(4, p) \neq 1$. Üheks veaks oligi fakti $(4, p) = 1$ tõestamata jätmine.

6. See osutus väga raskeks ülesandeks, mida keegi täielikult ära ei lahendanudki. Üks lihtsamaid lahendusi oleks alljärgnev.

Ilmselt tuleb ülesannet kitsendada juhule $m, n > 1$, sest mooduli 1 järgi ei leidu algjuuri. Paneme tähele, et arv a on algjuur mooduli N järgi parajasti siis, kui iga täisarvu b, kus $(b, N) = 1$, korral leidub $i \in \mathbb{N}$ nii, et

$$b \equiv a^i \pmod{N}.$$

Edaspidises tähistame sümboliga p ainult algarve.

Olgu esiteks a algjuur mooduli p^k, $k \in \mathbb{N}$ järgi. Siis iga täisarvu b, $(b, p^k) = 1$ jaoks leidub $i \in \mathbb{N}$ nii, et $b \equiv a^i \pmod{p^k}$. Kuna p on algarv, siis iga

$1 \leq l < k$ korral $(b, p^l) = 1$ parajasti siis, kui $(b, p^k) = 1$. Järelikult kui $(b, p^l) = 1$, siis $b \equiv a^i \pmod{p^k}$ ja seega ka $b \equiv a^i \pmod{p^l}$. Sellega oleme näidanud, et a on algjuur ka iga mooduli p^l, $l < k$ korral.

Teiseks, olgu a algjuur mooduli $2p^k$, $k \in \mathbb{N}$ järgi. Eelnevaga analoogiliselt on võimalik näidata, et a on algjuur ka iga mooduli $2p^l$, $l < k$ järgi. Viimaks näitame, et a on algjuur mooduli p^k (ja tõestuse esimese osa tõttu ka kõigi moodulite p^l, $l < k$) järgi. Selleks võtame arvu b nii, et $(b, p^k) = 1$. Siis kas $(b, 2) = 1$ või $(b, 2) = 2$. Esimesel juhul $(b, 2p^k) = 1$ ja järelikult $b \equiv a^i \pmod{2p^k}$, kust ka $b \equiv a^i \pmod{p^k}$, mida oligi vaja näidata. Teisel juhul $(b + p^k, 2) = 1$, mistõttu $(b + p^k, 2p^k) = 1$ ja $b + p^k \equiv a^i \pmod{2p^k}$, millest $b \equiv b + p^k \equiv a^i \pmod{p^k}$. Mõlemal juhul oleme avaldanud suvalise pööratava elemendi b arvu a astmena, ehk a on algjuur modulo p^k.

Lõpuks jääb üle vaid tähele panna, et algjuurte leidumiseks on tarvilik, et moodul mn oleks kujul $2, 4, p^k$ või $2p^k$. Kuna arvu 2 ei saa kirjutada kahe ühest suurema täisarvu korrutisena, siis esimene juht meid ei huvita. Teisel juhul on algjuureks mooduli 4 järgi 3, mis on seda ka mooduli 2 järgi ($3 \equiv 1 \pmod 2$). Kolmandal juhul on jagajad m ja n kujul p^l, $l < k$, mille kohta me oleme tõestanud, et algjuureks olek kandub neile üle. Viimasel juhul on tegurid m ja n kas kujul p^l, $l \leq k$, või $2p^l$, $l < k$. Mõlema juhu jaoks oleme eelnevalt näidanud, et algjuured kanduvad sellistele teguritele üle.

7. Muutus lahendajate vähesuse tõttu *-ülesandeks. Siin tuleb näidata, et $\overline{x}$ on pööratav (ilmselt $\overline{x}^{-1} = \overline{x}$) ja seetõttu asendatav algjuure astmega a^k. Tekib kongruents

$$a^{2k} \equiv 1 \pmod{n},$$

mis on lemma 7.3 tõttu samaväärne kongruentsiga

$$2k \equiv 0 \pmod{\varphi(n)}.$$

Kuna $n > 2$ korral on $\varphi(n)$ paarisarv, siis lause 6.2 põhjal on sellel kongruentsil, ja järelikult ka esialgsel kongruentsil, $(2, \varphi(n)) = 2$ lahendit. Kui $n = 2$, siis ainus lahend on 1.
Vigadest: elemendi $\overline{x}$ pööratvus jäeti enamasti tõestamata.

8. Ka sellele ülesandele lisandus tärn. Lahendamisel sai tähele panna, et antud eeldustel

$$a(a - 1) \equiv 1 \pmod{p}$$

ja näidata, et algjuure pöördelement on samuti algjuur. Olgu b algjuure a pöördelement modulo p ja olgu m tema järk rühmas $U(\mathbb{Z}_p)$. Siis $b^m \equiv 1 \pmod p$ ja

$$1 = 1^m \equiv (ab)^m = a^m \cdot b^m \equiv a^m \pmod{p}.$$

Lemma 7.3 tõttu $\varphi(p) \mid m$ ja Lagrange'i teoreemist $m \mid \varphi(p)$. Seega elemendi $\overline{b}$ järk on samuti $\varphi(p)$ ja b on samuti algjuur.