Arvuteooria

Kevad 2020

11. praktikumi näidislahendused

1. ülesanne (lahenduse autorid on toimetusele teada)

Kuna 41 on algarv, siis järelduse 7.13 põhjal leidub mooduli 41 järgi

$$\varphi(41-1) = \varphi(40) = \varphi(5) \cdot \varphi(2^3) = 4 \cdot 2^2 = 16$$

$41 - 1 = 40 = 2^3 \cdot 5$, seega järelduse 7.24 põhjal leiame vähima algjuure:

$$\begin{aligned}
2^{\frac{40}{5}} = 2^8 \equiv 10 \quad 2^{\frac{40}{2}} = 2^{20} = 40^2 \equiv 1 \pmod{41} \\
3^8 \equiv 40^2 \equiv 1 \pmod{41} \\
4^8 \equiv 10^2 \equiv 18 \quad 4^{20} \equiv 1^4 = 1 \pmod{41} \\
5^8 \equiv 10^2 \equiv 18 \quad 5^{20} \equiv 9^4 \equiv 40^2 \equiv 1 \pmod{41} \\
6^8 \equiv 25^2 \equiv 10 \quad 6^{20} \equiv 25^5 \equiv 25 \cdot 25^4 \equiv 25 \cdot 10^2 \equiv 25 \cdot 18 \equiv 40 \pmod{41}
\end{aligned}$$

Seega vähim algjuur mooduli 41 järgi on 6. Algjuurteks mooduli 41 järgi on kõik jäägiklassid 6^k, kus $1 \leq k \leq 40$ ja $(k, 40) = 1$. Seega saame

$$\begin{gathered}
6^1 = 6 \quad 6^3 \equiv 11 \quad 6^7 \equiv 29 \quad 6^9 \equiv 19 \quad 6^{11} \equiv 28 \quad 6^{13} \equiv 24 \quad 6^{17} \equiv 26 \quad 6^{19} \equiv 34 \\
6^{21} \equiv 35 \quad 6^{23} \equiv 30 \quad 6^{27} \equiv 12 \quad 6^{29} \equiv 22 \quad 6^{31} \equiv 13 \quad 6^{33} \equiv 17 \quad 6^{37} \equiv 15 \quad 6^{39} \equiv 7
\end{gathered}$$

41 algjuured on: 6, 7, 11, 12, 13, 15, 17, 19, 22, 24, 26, 28, 29, 30, 34, 35.

2. ülesanne (Markus Rene Pae ja Erki Kuus)

a) Kui $n = 105$, siis selle mooduli järgi ei ole algjuuri (teoreemi 7.21) põhjal, sest $105 = 3 \cdot 5 \cdot 7$ ehk pole kujul 2,4, p^k või $2p^k$, kus $p > 2$ on algarv.

b) Kui $n = 106$, siis teoreemi 7.27 põhjal on algjuuri (kehtib, kui leidub algjuuri) $\varphi(\varphi(106)) = = \varphi(52) = 24$ tükki.
Kuna $106 = 2 \cdot 53$, siis vaatleme esmalt algjuuri mooduli 53 järgi. Teame, et 53 on algarv, seega saame rakendada järeldust 7.24. Kuna $53 - 1 = 52 = 13 \cdot 2^2$, ja

$$3^4 \equiv 28, 3^{26} \equiv 52 \pmod{53},$$

siis 3 on üks algjuur mooduli 53 järgi. Nüüd teoreemi 7.19 tõttu on 3 üks algjuur ka mooduli $2 \cdot 53 = 106$ järgi.

c) Kui $n = 107$, siis teoreemi 7.27 põhjal on algjuuri (kehtib, kui leidub algjuuri) $\varphi(\varphi(107)) = = \varphi(106) = 52$ tükki.
Kuna $107 - 1 = 106 = 2 \cdot 53$ ning

$$2^2 \equiv 4, 2^{53} \equiv 106 \pmod{107},$$

siis järelduse 7.24 tõttu on 2 üks algjuur.

3. ülesanne (Laura Karu ja Susan Männik)

a) $n = 250$
Teame, et $250 = 2 \cdot 5^3$, seega vastavalt teoreemile 7.21 leidub algjuuri mooduli 250 järgi.
Leiame mitu algjuurt leidub mooduli 250 järgi, kasutades teoreemi 7.27.

$$\varphi(250) = \varphi(2 \cdot 5^3) = 2^{1-1} \cdot 5^{3-1} \cdot (2-1) \cdot (5-1) = 5^2 \cdot 4 = 100$$
$$\varphi(100) = \varphi(2^2 \cdot 5^2) = 2^{2-1} \cdot 5^{2-1} \cdot (2-1) \cdot (5-1) = 2 \cdot 5 \cdot 4 = 40$$

Seega mooduli 250 järgi leidub 40 algjuurt.
Leiame ühe algjuure mooduli 250 järgi. Selleks leiame kõigepealt algjuure mooduli 5 järgi.
On lihtne näha, et 2 on algjuur mooduli 5 järgi, sest $U(\mathbb{Z}_5) = \{\overline{1}, \overline{2}, \overline{3}, \overline{4}\} = \{\overline{2}, \overline{2}^2, \overline{2}^3, \overline{2}^4\}$.
Järeldus 7.15 ütleb, et kui a on algjuur mooduli $p > 2$ järgi, $b \in \{a, a+p\}, b^{p-1} \not\equiv 1 \pmod{p^2}$, siis b on algjuur mooduli p^2 järgi.
Et $2^{5-1} = 2^4 = 16 \not\equiv 1 \pmod{5^2}$, siis on 2 algjuur mooduli 5^2 järgi.
Teoreem 7.18 ütleb, et iga algjuur mooduli p^2 järgi ($p > 2$) on ka algjuur mooduli p^k järgi, $k > 2$.
Seega on 2 ka algjuur mooduli 5^3 järgi.
Vastavalt teoreemile 7.19 on $2 + 125 = 127$ algjuur mooduli 250 järgi.

b) $n = 252$
Teame, et $252 = 2^2 \cdot 63$, seega vastavalt teoreemile 7.21 ei leidu mooduli 252 järgi algjuuri.

c) $n = 254$
Teame, et $254 = 2 \cdot 127$, seega vastavalt teoreemile 7.21 leidub mooduli 254 järgi algjuuri.
Leiame, mitu algjuurt leidub mooduli 254 järgi, kasutades teoreemi 7.27.

$$\varphi(254) = \varphi(2 \cdot 127) = 2^{1-1} \cdot 127^{1-1} \cdot (2-1) \cdot (127-1) = 126$$
$$\varphi(126) = \varphi(2 \cdot 3^2 \cdot 7) = 2^{1-1} \cdot 3^{2-1} \cdot 7^{1-1} \cdot (2-1) \cdot (3-1) \cdot (7-1) = 3 \cdot 2 \cdot 6 = 36$$

Seega leidub 36 algjuurt mooduli 254 järgi.
Leiame ühe algjuure mooduli 254 järgi. Selleks leiame kõigepealt algjuure mooduli 127 järgi.
Kasutades järeldust 7.24 leiame ühe algjuure mooduli 127 järgi.

$$\begin{aligned}
2^{\frac{126}{2}} &= 2^{63} = 2 \cdot 2^{62} = 2 \cdot 4^{31} = 8 \cdot 4^{30} = 8 \cdot 16^{15} \equiv 1 \cdot 16^{14} \equiv 2^7 = 128 \equiv 1 \\
3^{\frac{126}{2}} &= 3^{63} = (3^7)^9 \equiv 28^9 = 28 \cdot 28^8 \equiv 28 \cdot 22^4 \equiv 28 \cdot 103^2 \equiv 90 \cdot 103 \equiv 126 \not\equiv 1 \\
3^{\frac{126}{3}} &= 3^{42} = (3^7)^6 \equiv 28^6 \equiv 22^3 \equiv 22 \cdot 103 \equiv 107 \not\equiv 1 \\
3^{\frac{126}{7}} &= 3^{18} = (3^7)^2 \cdot 3^4 \equiv 28^2 \cdot 81 \equiv 22 \cdot 81 \equiv 4 \not\equiv 1
\end{aligned}$$

Järelikult 3 on algjuur mooduli 127 järgi.
Vastavalt teoreemile 7.19 on 3 algjuur ka mooduli 254 järgi.

4. ülesanne I (Johanna Maria Kirss ja Rainer Bõkov)

Oletame vastuväiteliselt, et a ei ole algjuur mooduli p järgi. Siis leidub mingi aste $l < p-1$ nii, et $a^l \equiv 1 \pmod{p}$. Teame, et a^k on algjuur mooduli p järgi ehk $(a^k)^l \not\equiv 1 \pmod{p}$, sest $l < p-1$. See aga tähendab, et $(a^k)^l = (a^l)^k \equiv 1^k \not\equiv 1 \pmod{p}$. Oleme saanud vastuolu.

4. ülesanne II (Urmas Luhaäär ja Kristjan Kallikivi)

Vaatame rühma $U(\mathbb{Z}_p)$ tsüklilist alamrühma $\langle a \rangle$. Ilmselt $U(\mathbb{Z}_p) = \langle a^k \rangle \subset \langle a \rangle$. Kuna teistpidi sisalduvus kehtib ilmselt, siis $U(\mathbb{Z}_p) = \langle a \rangle$, mis tähendabki seda, et a on algjuur.

5. ülesanne (Erki Külaots ja Marcus Lõo)

Kui $x = 1$, siis $1+1+1+1+1+1+1+1 = 8 \not\equiv 0 \pmod{41}$. Seega $x \neq 1$.

Kasutame geomeetrilise rea summa valemit. (Teame, et $x \neq 1$)

$$1 + x + x^2 + x^3 + x^4 + x^5 + x^6 + x^7 = \frac{x^8 - 1}{x - 1} \equiv 0 \pmod{41}$$

Kuna $\frac{x^8-1}{x-1} \equiv 0 \pmod{41}$, siis kindlasti $x^8 - 1 \equiv 0 \pmod{41}$ ehk $x^8 \equiv 1 \pmod{41}$. Et see kehtiks, siis elemendi a järk rühmas $U(\mathbb{Z}_{41})$ peab jagama arvu 8. Kasutades ülesannet nr 1. ellimineerime suure osa x-i võimalikest väärtustest, sest ülesandes üks leidsime kõik elemendid, mille järk oli $\varphi(41) = 40$ ja $40 \nmid 8$.

Seega ellimineerime võimalike lahendite hulgast elemendid

$$\{6,7,11,12,13,15,17,19,-19,-17,-15,-13,-12,-11,-7,-6\}$$

Alles jäid $\{-1, \pm 2, \pm 3, \pm 4, \pm 5, \pm 9, \pm 10, \pm 14, \pm 16, \pm 18, \pm 20\}$

Katsetame neid lihtsalt läbi.

$$x = -1$$
$$(-1)^8 \equiv 1 \pmod{41}$$

$$x = \pm 2$$
$$(\pm 2)^8 = 256 \equiv 10 \pmod{41}$$

$$x = \pm 3$$
$$(\pm 3)^8 = 81^2 \equiv (-1)^2 \equiv 1 \pmod{41}$$

$$x = \pm 4$$
$$(\pm 4)^8 = 256^2 \equiv (10)^2 \equiv 100 \equiv 18 \pmod{41}$$

$$x = \pm 5$$
$$(\pm 5)^8 = 625^2 \equiv (10)^2 \equiv 100 \equiv 18 \pmod{41}$$

$$x = \pm 9$$
$$(\pm 3^2)^8 = (3^8)^2 \equiv (1)^2 \equiv 1 \pmod{41}$$

$$x = \pm 10$$
$$(\pm 10)^8 = 5^8 \cdot 2^8 \equiv 18 \cdot 10 \equiv 180 \equiv 16 \pmod{41}$$

$$x = \pm 14$$
$$(\pm 14)^8 = 196^4 \equiv 32^4 \equiv 1024^2 \equiv (-1)^2 \equiv 1 \pmod{41}$$

$$x = \pm 16$$
$$(\pm 16)^8 = 18^2 \equiv 324 \equiv 37 \pmod{41}$$

$$x = \pm 18$$
$$(\pm 18)^8 = 9^8 \cdot 2^8 \equiv 1 \cdot 10 \equiv 10 \pmod{41}$$

$$x = \pm 20$$
$$(\pm 20)^8 = 4^8 \cdot 5^8 \equiv 18 \cdot 18 = 324 \equiv 37 \pmod{41}$$

Seega lahendid on $\{-14, -9, -3, -1,3,9,14\}$.

v. Kongruentsi $1+x+x^2+x^3+x^4+x^5+x^6+x^7 \equiv 0 \pmod{41}$ lahendid on $\{-1,\pm 3,\pm 9,\pm 14\}$.

Lauri Tart: Kui teada järgmise, st 12. praktikumi materjali, siis on lihtsam ja kiirem indekseerida ja kasutada nt. E. Redi "Arvuteooria" õpikus toodud tabelit mooduli 41 ja algjuure 6 jaoks. Indekseerides

$$x^8 \equiv 1 \,(\mathrm{mod}\ 41) \Longleftrightarrow \mathrm{ind}_6(x^8) \equiv \mathrm{ind}_6 1 \,(\mathrm{mod}\ \varphi(41)) \Longleftrightarrow 8\mathrm{ind}_6 x = 0 \pmod{40}.$$

Jagame kongruentsi mõlemaid pooli arvuga 8 ja saame, et $\mathrm{ind}_6 x = 0 \pmod 5$ ehk

$$\mathrm{ind}_6 x \in \{5,10,15,20,25,30,35,40\}.$$

Tabeli põhjal vastavad neile indeksitele täpselt juba leitud väärtused

$$x \equiv 27, 32, 3, 40, 14, 9, 38, 1 \pmod{40}.$$

6. ülesanne (lahenduse autorid on toimetusele teada)

Kõigepealt tõestame mõned abitulemused
Lemma 1. *Kui a on algjuur mooduli $p \in \mathbb{P}$, $p \geq 3$, siis $a^{\frac{p-1}{2}} \equiv -1 \pmod{p}$*

Tõestus. Fermat väikese teoreemi põhjal $a^{p-1} \equiv 1$.

Kuna $(a^{\frac{p-1}{2}})^2 = a^{p-1}$, siis $a^{\frac{p-1}{2}} \equiv -1 \pmod{p}$ või $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$. (Polünoomil $x^2 \equiv 1$ on nulliteguriteta ringis ülimalt 2 juurt, kuna $1^2 = (-1)^2 = 1$, siis on need ainsad juured).

Kuna a on algjuur ehk $p-1$ on vähim naturaalarv, mille korral $a^{p-1} \equiv 1 \pmod{1}$, siis ei saa kehtida, et $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$.

Järelikult peab $a^{\frac{p-1}{2}} \equiv -1 \pmod{p}$ □

Lauri Tart: Järgnevat lemmat ei ole tegelikult kursuse lõpus enam vaja eraldi tõestada, sest see on loengukonspekti lause 8.8 osa 3.
Lemma 2. *$p \equiv 1 \pmod{4}$, kus $p \geq 3$ parajasti siis, kui leidub $a \in \mathbb{Z}$ nii et $a^2 \equiv -1 \pmod{p}$*

Tõestus. Piisavus Eelmise lemma põhjal kui a on algjuur mooduli p järgi, siis $a^{\frac{p-1}{2}} \equiv -1 \pmod{p}$, samuti on teada, et algarvulise mooduli järgi leidub algjuuri ehk olgu a algjuur. Kuna $p \equiv 1 \pmod{4}$ siis $\frac{p-1}{4} \in \mathbb{Z}$ ja $(a^{\frac{p-1}{4}})^2 \equiv a^{\frac{p-1}{2}} \equiv -1 \pmod{p}$, mida oligi tarvis näidata.

Tarvilikkus Olgu a selline, et $a^2 \equiv -1 \pmod{p}$

Oletame vastuväiteliselt, et $p \not\equiv 1 \pmod{4}$. Kuna p peab olema paaritu, siis $p \equiv 3 \pmod{4}$ ehk $p = 4k+3$.

Kuna $a^4 \equiv (-1)^2 \equiv 1$, siis elemendi a järk on 4 (1 ei sobi, kuna siis $a^2 = 1$ ning 3 ei sobi kuna, siis $1 = a^3 = a^2a = -a \Rightarrow a = -1 \Rightarrow a^2 = 1 \neq -1$.)

Lagrange'i teoreemi põhjal saame, et $4 \mid p-1$ ehk $4 \mid 4k+3-1$ ehk $4 \mid 4k+2$, mis on vastuolu. □

Kuna q on kahest suurem algarv, siis q on paaritu ehk $q = 2k+1$, seega $p = 2q+1 = 2(2k+1)+1 = 4k+3$ ehk $p \equiv 3 \pmod{4}$.

Olgu $1 < a < p-1$ ja $b := p - a^2$. Selleks, et b on algjuur mooduli p järgi, piisab järelduse 7.24 põhjal näidata, et $p-1$ kõigi algtegurite r korral $b^{\frac{p-1}{r}} \not\equiv 1 \pmod{p}$.

Kuna $p - 1 = 2q + 1 - 1 = 2q$, siis tuleb kontrollida arvu $p-1$ algtegureid 2 ja q:

- $b^{\frac{p-1}{q}} \equiv b^{\frac{2q}{q}} \equiv b^2 \equiv (p-a^2)^2 \not\equiv 1 \pmod{p}$.

  Oletades vastuväiteliselt, et $(p-a^2)^2 \equiv 1 \pmod{p}$, siis $p-a^2 \equiv 1 \pmod{p}$ või $p-a^2 \equiv -1 \pmod{p}$ (Polünoomil $x^2 \equiv 1$ on nulliteguriteta ringis ülimalt 2 juurt, kuna $1^2 = (-1)^2 = = 1$, siis on need ainsad juured).

  Kui $p-a^2 \equiv 1 \pmod{p} => a^2 \equiv -1 \pmod{p}$, mis on vastuolus enne tõestatud lemmaga, kuna sel juhul peaks olema $p \equiv 1 \pmod{4}$.

  Kui $p-a^2 \equiv -1 \pmod{p} => a^2 \equiv 1 \pmod{p} => a \equiv \pm 1 \pmod{p}$, see on aga vastuolus eeldusega, et $1 < a < p-1$.

- $b^{\frac{p-1}{2}} \equiv b^{\frac{2q}{2}} \equiv b^q \equiv (p-a^2)^q \not\equiv 1 \pmod{p}$.

  Oletades vastuväiteliselt, et $(p-a^2)^q \equiv 1 \pmod{p}$

  Binoomvalemi kohaselt $(p-a^2)^q = p^q + zp^{q-1}(-a^2) + \cdots + yp(-a^2)^{q-1} + (-a^2)^q$ vms, seega $(p-a^2) \equiv (-a^2)^q \equiv (-1)^q \cdot a^{2q} \equiv -a^{2q} \equiv -a^{p-1} \equiv -1 \pmod{p}$ (kuna q oli paaritu algarv, siis $(-1)^q = -1$).

Niisiis $b = p - a^2$ on algjuur mooduli p järgi.

7. ülesanne (Urmas Luhaäär ja Kristjan Kallikivi)

Kuna p on algarv, siis leidub mod$p$ algjuur a. Ilmselt $1 < a < p$. Kuna sel juhul $(a, p) = 1$, siis $\overline{a} \in U(\mathbb{Z}_p)$ ja seega leidub $\overline{a}^{-1} \in U(\mathbb{Z}_p)$. Võtame $\overline{a}^{-1}$ suvalise esindaja ja jagame teda jäägiga arvuga p. Saame sellise arvu b, mille puhul $1 < b < p (b \neq 0$, sest muidu ta poleks pööratav) ja $ab \equiv 1 \pmod{p}$.

Näitame, et b on algjuur mod$p$. Vaatame $U(\mathbb{Z}_p)$ alamrühma, $\left\langle \overline{b} \right\rangle$. Ka selles rühmas $\overline{a}^{-1} = \overline{b} \iff \overline{b}^{-1} = \overline{a}$. Seega $\overline{a} \in \langle b \rangle$. Lõpuks

$$U(\mathbb{Z}_p) = \langle a \rangle \subset \langle b \rangle \implies U(\mathbb{Z}_p) = \langle b \rangle,$$

ehk b on algjuur.

Peame näitama, et kas a või b on algjuur $\bmod p^2$, sest sellest järeldub algjuureks olek kõikide suuremate astmete jaoks.

Eeldame vastuväiteliselt, et ei a ega b ei ole alguur modp^2. Siis

$$a^m \equiv 1 \pmod{p^2},$$

kus $m < \varphi(p^2) = p(p-1)$. Siis ka

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

kust saame, et $p-1|m$. Kuna kõik multiplikatiivsed järgud $\bmod p^2$ peavad jagama arvu $p(p-1)$, siis ainsa võimalusena $m = p-1$, ehk

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

Sarnaselt saame ka, et

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

Korrutame need kongruentsid kokku:

$$(ab)^{p-1} \equiv 1 \pmod{p^2} \iff p|(ab)^{p-1} - 1 = (ab-1)((ab)^{p-2} + \cdots + ab + 1).$$

Märkame, et

$$(ab)^{p-2} + \cdots + ab + 1 \equiv 1 + \cdots + 1 \equiv p - 1 \equiv -1 \not\equiv 0 \pmod{p}.$$

Kuna p on algarv, siis

$$((ab)^{p-2} + \cdots + ab + 1, p) = 1.$$

Nüüd saame rakendada Eukeidese lemmat, ehk $p^2|ab-1$. See on aga vastuolus sellega, et $1 < a < p$ ja $1 < b < p$, sest

$$p^2 > ab > ab - 1.$$

8. ülesanne (Mikael Raihhelgauz ja Maret Sõmer)

Ainuke algjuur mooduli 2 järgi on 1 ja ainuke algjuur mooduli 3 järgi on 2. Vaatleme nüüd algarve $p > 3$. Olgu a mingi algjuur mooduli p järgi. Järelduse 7.13 põhjal moodustavad arvud kujul a^k, kus $1 \leq k < p-1$ parajasti kõigi algjuurte hulga. Niisiis, nende korrutis esitub kujul

$$a^1 a^{k_2} \dots a^{\varphi(p-1)} = a^s,$$

kus $s = \sum_{(k_i, p-1)=1} k_i$. Märgime, et $(k_i, p-1) = 1$ parajasti siis, kui $(p-1-k_i, p-1) = 1$.

Tõepoolest, eeldame, et $(k_i, p-1) = 1$ ning oletame vastuväiteliselt, et leidub $d > 1$ nii, et $d|p-1-k_i$ ja $d|p-1$. Siis leiduvad n, m nii, et $p-1 = dm$ ja $p-1-k_i = dn$. Sellisel juhul aga $k_i = p-1-dn = dm-dn = d(m-n)$ ehk $d|k$. Vastuolu!
Nüüd eeldame, et $(p-1-k_i, p-1) = 1$. Oletame vastuväiteliselt, et leidub $d > 1$ nii, et $d|p-1$ ja $d|k_i$. On ilmne, et sel juhul ka $d|p-1-k_i$. Vastuolu! Niisiis, eelneva põhjal

$$\{1, k_2, \dots, k_{\varphi(p-1)}\} = \{p-1-1, p-1-k_2, \dots, p-1-k_{\varphi(p-1)}\}.$$

Järelikult ka

$$\begin{aligned} s &= \sum_{(k_i,p-1)=1} k_i = \sum_{(p-1-k_1,p-1)=1} p-1-k_i, \\ 2s &= \sum_{(k_i,p-1)=1} k_i + \sum_{(p-1-k_1,p-1)} p-1-k_i = \\ &= \sum_{i=1}^{\varphi(p-1)} k_i + (p-1-k_i) = \varphi(p-1)\cdot(p-1), \\ s &= \frac{\varphi(p-1)}{2}(p-1). \end{aligned}$$

Lemma 7.10 põhjal $\varphi(p-1)$ on paarisarv iga $p > 3$ korral. Järelikult $\frac{\varphi(p-1)}{2}$ on täisarv. Meenutame, et Fermat' väikese teoreemi põhjal $a^{p-1} \equiv 1 \mod p$ iga $a \in U(\mathbb{Z}_p)$ korral. Kokkuvõttes

$$a^s = \left(a^{p-1}\right)^{\frac{\varphi(p-1)}{2}} \equiv 1^{\frac{\varphi(p-1)}{2}} \equiv 1 \mod p.$$