Arvuteooria

Kevad 2020

12. praktikumi näidislahendused

1. ülesanne (Hartvig Tooming)

Leiame kõik algjuured mooduli 19 järgi. Kuna $\varphi(19) = 18 = 2 \cdot 3^2$, siis tuleb leida selline jäägiklass $\overline{a} \in U(\mathbb{Z}_{19})$, et $a^9 \not\equiv 1 \pmod{19}$ ja $a^6 \not\equiv 1 \pmod{19}$. Leiame sellise jäägiklassi:

$$2^6 \equiv 2^2 \cdot 2^4 \equiv 4 \cdot 16 \equiv 4 \cdot (-3) \equiv -12 \not\equiv 1 \pmod{19}$$
$$2^9 \equiv 2^3 \cdot 2^6 \equiv 8 \cdot (-12) \equiv 8 \cdot 7 \equiv 56 \equiv -1 \not\equiv 1 \pmod{19}$$

Leiame ka kõik ülejäänud algjuured, mis esituvad kujul $\overline{2}^k$, kus $1 \leq k < 18$ ja $(k,18) = 1$. Sellised astendajad k on 1, 5, 7, 11, 13, 17.

$$2^1 \equiv 2 \pmod{19}$$
$$2^5 \equiv 32 \equiv 13 \pmod{19}$$
$$2^7 \equiv 2^2 \cdot 2^5 \equiv 4 \cdot 13 \equiv 52 \equiv 14 \pmod{19}$$
$$2^{11} \equiv 2^4 \cdot 2^7 \equiv (-3) \cdot 14 \equiv -42 \equiv 15 \pmod{19}$$
$$2^{13} \equiv 2^2 \cdot 2^{11} \equiv 4 \cdot 15 \equiv 60 \equiv 3 \pmod{19}$$
$$2^{17} \equiv 2^4 \cdot 2^{13} \equiv (-3) \cdot 3 \equiv -9 \equiv 10 \pmod{19}.$$

Saime kõik $\varphi\left(\varphi(19)\right) = \varphi\left(2 \cdot 3^2\right) = 3 \cdot (3-1) = 6$ algjuurt $\overline{2}$,$\overline{3}$,$\overline{10}$,$\overline{13}$,$\overline{14}$,$\overline{15}$. Kuna $4 = 2^2$ ning $1 \leq 2 \leq \varphi 19$, siis $\mathrm{ind}_2 4 = 2$. Leiame ka kõik ülejäänud indeksid. Selleks leiame kõigepealt arvu 2 indeksid kõigi teiste algjuureliste baaside järgi (otsime neid jällegi võimalike astendajate 5, 7, 11, 13, 17 seast):

$$\overline{13} = \overline{2}^5 \to 5 \cdot 5 = 25 \equiv 6 \not\equiv 1 \pmod{18}$$
$$\to 5 \cdot 7 = 35 \equiv -1 \not\equiv 1 \pmod{18}$$
$$\to 5 \cdot 11 = 55 \equiv 1 \pmod{18}$$
$$\overline{14} = \overline{2}^7 \to 7 \cdot 7 = 49 \equiv (-5) \not\equiv 1 \pmod{18}$$
$$\to 7 \cdot 11 = 77 \equiv 5 \not\equiv 1 \pmod{18}$$
$$\to 7 \cdot 13 = 91 \equiv 1 \pmod{18}$$
$$\overline{15} = \overline{2}^{11} \to 11 \cdot 5 \equiv 1 \pmod{18}$$
$$\overline{3} = \overline{2}^{13} \to 13 \cdot 7 \equiv 1 \pmod{18}$$
$$\overline{10} = \overline{2}^{17} \to 17 \cdot 17 \equiv 289 \equiv 1 \pmod{18}.$$

Niisiis saame edasi, et

$$\begin{aligned}
\operatorname{ind}_3 4 &\equiv 2 \cdot \operatorname{ind}_3 2 \equiv 2 \cdot 7 \equiv 14 \pmod{18} \\
\operatorname{ind}_{10} 4 &\equiv 2 \cdot \operatorname{ind}_{10} 2 \equiv 2 \cdot 17 \equiv 34 \equiv 16 \pmod{18} \\
\operatorname{ind}_{13} 4 &\equiv 2 \cdot \operatorname{ind}_{13} 2 \equiv 2 \cdot 11 \equiv 22 \equiv 4 \pmod{18} \\
\operatorname{ind}_{14} 4 &\equiv 2 \cdot \operatorname{ind}_{14} 2 \equiv 2 \cdot 13 \equiv 26 \equiv 8 \pmod{18} \\
\operatorname{ind}_{15} 4 &\equiv 2 \cdot \operatorname{ind}_{15} 2 \equiv 2 \cdot 5 \equiv 10 \pmod{18}.
\end{aligned}$$

Lõppkokkuvõttes saame, et $\operatorname{ind}_2 4 = 2$, $\operatorname{ind}_3 4 = 14$, $\operatorname{ind}_{10} 4 = 16$, $\operatorname{ind}_{13} 4 = 4$, $\operatorname{ind}_{14} 4 = 8$ ja $\operatorname{ind}_{15} 4 = 10$.

2. ülesanne (Mikael Raihhelgauz ja Maret Sõmer)

Kõigepealt panen tähele, et vahemikus [0,24] on sellised arvud c, mille korral $(c,25) \neq 1$, parajasti need, mis jaguvad 5-ga, s.t. 0, 5, 10, 15 ja 20. See tähendab, et nende arvude jaoks ei ole indeks mooduli 25 järgi defineeritud.

Arvutan algjuure 3 astmed mooduli 25 järgi:

$3^1 \equiv 3$, $3^2 \equiv 9$, $3^3 \equiv 2$, $3^4 \equiv 6$, $3^5 \equiv 18$, $3^6 \equiv 4$, $3^7 \equiv 12$,
$3^8 \equiv 11$, $3^9 \equiv 8$, $3^{10} \equiv 24$, $3^{11} \equiv 22$, $3^{12} \equiv 16$, $3^{13} \equiv 23$, $3^{14} \equiv 19$
$3^{15} \equiv 7$, $3^{16} \equiv 21$, $3^{17} \equiv 13$, $3^{18} \equiv 14$, $3^{19} \equiv 17$, $3^{20} \equiv 1 \pmod{25}$

Järelikult:

$\operatorname{ind}_3 1 = 20$, $\operatorname{ind}_3 2 = 3$, $\operatorname{ind}_3 3 = 1$, $\operatorname{ind}_3 4 = 6$, $\operatorname{ind}_3 6 = 4$,
$\operatorname{ind}_3 7 = 15$, $\operatorname{ind}_3 8 = 9$, $\operatorname{ind}_3 9 = 2$, $\operatorname{ind}_3 11 = 8$, $\operatorname{ind}_3 12 = 7$,
$\operatorname{ind}_3 13 = 17$, $\operatorname{ind}_3 14 = 18$, $\operatorname{ind}_3 16 = 12$, $\operatorname{ind}_3 17 = 19$, $\operatorname{ind}_3 18 = 5$,
$\operatorname{ind}_3 19 = 14$, $\operatorname{ind}_3 21 = 16$, $\operatorname{ind}_3 22 = 11$, $\operatorname{ind}_3 23 = 13$, $\operatorname{ind}_3 24 = 10$

Seega indeksite tabel alusel 3 mooduli 25 järgi on:

	0	1	2	3	4	5	6	7	8	9
0		20	3	1	6		4	15	9	2
1		8	7	17	18		12	19	5	14
2		16	11	13	10					

kus esimeses reas on indekseeritava arvu üheliste number ning esimeses veerus on indekseeritava arvu kümneliste number.

3. ülesanne (Erki Külaots ja Marcus Lõo)

Leiame kõigepealt $\text{ind}_{13}3$ modulo 25, ehk teisisõnu leiame k kongruentsis $13^k \equiv 3 \pmod{25}$. Paneme tähele eelnevast indeksite tabelist, et $3^{17} \equiv 13 \pmod{25}$. Seega saame lemma 7.31 põhjal, et

$$3^{17k} \equiv 3 \pmod{25} \iff 17k \equiv 1 \pmod{20}.$$

Seega peab olema elemendi $\overline{17}$ pöördelement ringis $U(\mathbb{Z}_{20})$ just k kõrvalklass. Märgime, et kuna (17,20) = 1, siis on $\overline{17}$ pööratav. Kasutame selleks Eukleidese algoritmi

$$\begin{aligned} 20 &= 17 \cdot 1 + 3, \\ 17 &= 3 \cdot 5 + 2, \\ 3 &= 2 \cdot 1 + 1, \\ 2 &= 1 \cdot 2 + 0, \end{aligned}$$

seega tagurpidi liikudes saame, et

$$1 = 3 - 2 = 3 - 17 + 3 \cdot 5 = 3 \cdot 6 - 17 = (20 - 17)6 - 17 = 20 \cdot (6) + 17 \cdot (-7).$$

Järelikult on $\overline{17}^{-1} = \overline{-7} = \overline{13} \pmod{20}$.
Seega oleme leidnud otsitava indeksi $\text{ind}_{13}3 = 13$. Kasutame seda indeksit tabeli tegemiseks alusel 13, rakendades teoreemi 7.32 punkti 6 ning eelmise ülesande indeksite tabelit.
(Jätkub järgmisel leheküljel.)

$$\begin{aligned}
\operatorname{ind}_{13} b &\equiv \operatorname{ind}_3 b \cdot \operatorname{ind}_{13} 3 = \operatorname{ind}_3 b \cdot 13 \pmod{20} \\
\operatorname{ind}_{13} 2 &\equiv \operatorname{ind}_3 1 \cdot 13 = 3 \cdot 13 = 39 \equiv 19 \pmod{20} \\
\operatorname{ind}_{13} 3 &\equiv \operatorname{ind}_3 3 \cdot 13 = 1 \cdot 13 = 13 \pmod{20} \\
\operatorname{ind}_{13} 4 &\equiv \operatorname{ind}_3 4 \cdot 13 = 6 \cdot 13 = 78 \equiv 18 \pmod{20} \\
\operatorname{ind}_{13} 6 &\equiv \operatorname{ind}_3 6 \cdot 13 = 4 \cdot 13 = 52 \equiv 12 \pmod{20} \\
\operatorname{ind}_{13} 7 &\equiv \operatorname{ind}_3 7 \cdot 13 = 15 \cdot 13 = 195 \equiv 15 \pmod{20} \\
\operatorname{ind}_{13} 8 &\equiv \operatorname{ind}_3 8 \cdot 13 = 9 \cdot 13 = 117 \equiv 17 \pmod{20} \\
\operatorname{ind}_{13} 9 &\equiv \operatorname{ind}_3 9 \cdot 13 = 2 \cdot 13 = 26 \equiv 6 \pmod{20} \\
\operatorname{ind}_{13} 11 &\equiv \operatorname{ind}_3 11 \cdot 13 = 8 \cdot 13 = 4 \pmod{20} \\
\operatorname{ind}_{13} 12 &\equiv \operatorname{ind}_3 12 \cdot 13 = 7 \cdot 13 = 11 \pmod{20} \\
\operatorname{ind}_{13} 13 &\equiv \operatorname{ind}_3 13 \cdot 13 = 17 \cdot 13 = 1 \pmod{20} \\
\operatorname{ind}_{13} 14 &\equiv \operatorname{ind}_3 14 \cdot 13 = 18 \cdot 13 = 14 \pmod{20} \\
\operatorname{ind}_{13} 16 &\equiv \operatorname{ind}_3 16 \cdot 13 = 12 \cdot 13 = 16 \pmod{20} \\
\operatorname{ind}_{13} 17 &\equiv \operatorname{ind}_3 17 \cdot 13 = 19 \cdot 13 = 7 \pmod{20} \\
\operatorname{ind}_{13} 18 &\equiv \operatorname{ind}_3 18 \cdot 13 = 5 \cdot 13 = 5 \pmod{20} \\
\operatorname{ind}_{13} 19 &\equiv \operatorname{ind}_3 19 \cdot 13 = 14 \cdot 13 = 2 \pmod{20} \\
\operatorname{ind}_{13} 21 &\equiv \operatorname{ind}_3 21 \cdot 13 = 16 \cdot 13 = 8 \pmod{20} \\
\operatorname{ind}_{13} 22 &\equiv \operatorname{ind}_3 22 \cdot 13 = 11 \cdot 13 = 3 \pmod{20} \\
\operatorname{ind}_{13} 23 &\equiv \operatorname{ind}_3 23 \cdot 13 = 13 \cdot 13 = 9 \pmod{20} \\
\operatorname{ind}_{13} 24 &\equiv \operatorname{ind}_3 24 \cdot 13 = 10 \cdot 13 = 10 \pmod{20}.
\end{aligned}$$

Paneme ka tabelisse:

	0	1	2	3	4	6	7	8	9
0		20	19	13	18	12	15	17	6
1		4	11	1	14	16	7	5	2
2		8	3	9	10				

4. ülesanne (lahenduse autorid on toimetusele teada)

Indeksite tabel alusel 3 mooduli 31 järgi on (E.Redi "Arvuteooria", lk 330)

	0	1	2	3	4	5	6	7	8	9
0		0	24	1	18	20	25	28	12	2
1	14	23	19	11	22	21	6	7	26	4
2	8	29	17	27	13	10	5	3	16	9
3	15									

Teoreem 7.36 järgi elemendi b järk rühmas $U(\mathbb{Z}_n)$ on $\frac{\varphi(n)}{(\mathrm{ind}_a b, \varphi(n))}$.

- Elemendi 1 järk rühmas $U(\mathbb{Z}_{31})$ on 1.
- Elemendi 2 järk rühmas $U(\mathbb{Z}_{31})$ on $\frac{30}{(\mathrm{ind}_3 2,30)} = \frac{30}{(24,30)} = \frac{30}{6} = 5$.
- Elemendi 3 järk rühmas $U(\mathbb{Z}_{31})$ on $\frac{30}{(\mathrm{ind}_3 3,30)} = \frac{30}{(1,30)} = \frac{30}{1} = 30$.
- Elemendi 4 järk rühmas $U(\mathbb{Z}_{31})$ on $\frac{30}{(\mathrm{ind}_3 4,30)} = \frac{30}{(18,30)} = \frac{30}{6} = 5$.
- Elemendi 5 järk rühmas $U(\mathbb{Z}_{31})$ on $\frac{30}{(\mathrm{ind}_3 5,30)} = \frac{30}{(20,30)} = \frac{30}{10} = 3$.
- Elemendi 6 järk rühmas $U(\mathbb{Z}_{31})$ on $\frac{30}{(\mathrm{ind}_3 6,30)} = \frac{30}{(25,30)} = \frac{30}{5} = 6$.
- Elemendi 7 järk rühmas $U(\mathbb{Z}_{31})$ on $\frac{30}{(\mathrm{ind}_3 7,30)} = \frac{30}{(28,30)} = \frac{30}{2} = 15$.
- Elemendi 8 järk rühmas $U(\mathbb{Z}_{31})$ on $\frac{30}{(\mathrm{ind}_3 8,30)} = \frac{30}{(12,30)} = \frac{30}{6} = 5$.
- Elemendi 9 järk rühmas $U(\mathbb{Z}_{31})$ on $\frac{30}{(\mathrm{ind}_3 9,30)} = \frac{30}{(2,30)} = \frac{30}{2} = 15$.
- Elemendi 10 järk rühmas $U(\mathbb{Z}_{31})$ on $\frac{30}{(\mathrm{ind}_3 10,30)} = \frac{30}{(14,30)} = \frac{30}{2} = 15$.
- Elemendi 11 järk rühmas $U(\mathbb{Z}_{31})$ on $\frac{30}{(\mathrm{ind}_3 11,30)} = \frac{30}{(23,30)} = \frac{30}{1} = 30$.
- Elemendi 12 järk rühmas $U(\mathbb{Z}_{31})$ on $\frac{30}{(\mathrm{ind}_3 12,30)} = \frac{30}{(19,30)} = \frac{30}{1} = 30$.
- Elemendi 13 järk rühmas $U(\mathbb{Z}_{31})$ on $\frac{30}{(\mathrm{ind}_3 13,30)} = \frac{30}{(11,30)} = \frac{30}{1} = 30$.
- Elemendi 14 järk rühmas $U(\mathbb{Z}_{31})$ on $\frac{30}{(\mathrm{ind}_3 14,30)} = \frac{30}{(22,30)} = \frac{30}{2} = 15$.
- Elemendi 15 järk rühmas $U(\mathbb{Z}_{31})$ on $\frac{30}{(\mathrm{ind}_3 15,30)} = \frac{30}{(21,30)} = \frac{30}{3} = 10$.
- Elemendi 16 järk rühmas $U(\mathbb{Z}_{31})$ on $\frac{30}{(\mathrm{ind}_3 16,30)} = \frac{30}{(6,30)} = \frac{30}{6} = 5$.
- Elemendi 17 järk rühmas $U(\mathbb{Z}_{31})$ on $\frac{30}{(\mathrm{ind}_3 17,30)} = \frac{30}{(7,30)} = \frac{30}{1} = 30$.
- Elemendi 18 järk rühmas $U(\mathbb{Z}_{31})$ on $\frac{30}{(\mathrm{ind}_3 18,30)} = \frac{30}{(26,30)} = \frac{30}{2} = 15$.
- Elemendi 19 järk rühmas $U(\mathbb{Z}_{31})$ on $\frac{30}{(\mathrm{ind}_3 19,30)} = \frac{30}{(4,30)} = \frac{30}{2} = 15$.
- Elemendi 20 järk rühmas $U(\mathbb{Z}_{31})$ on $\frac{30}{(\mathrm{ind}_3 20,30)} = \frac{30}{(8,30)} = \frac{30}{2} = 15$.

- Elemendi 21 järk rühmas $U(\mathbb{Z}_{31})$ on $\frac{30}{(\text{ind}_3 21,30)} = \frac{30}{(29,30)} = \frac{30}{1} = 30$.
- Elemendi 22 järk rühmas $U(\mathbb{Z}_{31})$ on $\frac{30}{(\text{ind}_3 22,30)} = \frac{30}{(17,30)} = \frac{30}{1} = 30$.
- Elemendi 23 järk rühmas $U(\mathbb{Z}_{31})$ on $\frac{30}{(\text{ind}_3 23,30)} = \frac{30}{(27,30)} = \frac{30}{3} = 10$.
- Elemendi 24 järk rühmas $U(\mathbb{Z}_{31})$ on $\frac{30}{(\text{ind}_3 24,30)} = \frac{30}{(13,30)} = \frac{30}{1} = 30$.
- Elemendi 25 järk rühmas $U(\mathbb{Z}_{31})$ on $\frac{30}{(\text{ind}_3 25,30)} = \frac{30}{(10,30)} = \frac{30}{10} = 3$.
- Elemendi 26 järk rühmas $U(\mathbb{Z}_{31})$ on $\frac{30}{(\text{ind}_3 26,30)} = \frac{30}{(5,30)} = \frac{30}{5} = 6$.
- Elemendi 27 järk rühmas $U(\mathbb{Z}_{31})$ on $\frac{30}{(\text{ind}_3 27,30)} = \frac{30}{(3,30)} = \frac{30}{3} = 10$.
- Elemendi 28 järk rühmas $U(\mathbb{Z}_{31})$ on $\frac{30}{(\text{ind}_3 28,30)} = \frac{30}{(16,30)} = \frac{30}{2} = 15$.
- Elemendi 29 järk rühmas $U(\mathbb{Z}_{31})$ on $\frac{30}{(\text{ind}_3 29,30)} = \frac{30}{(9,30)} = \frac{30}{3} = 10$.
- Elemendi 30 järk rühmas $U(\mathbb{Z}_{31})$ on $\frac{30}{(\text{ind}_3 30,30)} = \frac{30}{(15,30)} = \frac{30}{15} = 2$.

Teoreemi 7.36 kohaselt on arv b algjuur mooduli n järgi parajasti siis, kui $(\text{ind}_a b, \varphi(n)) = 1$. Seega on eelneva põhjal algjuured mooduli 31 järgi 3, 11, 12, 13, 17, 21, 22, 24.

5. ülesanne (Mikael Raihhelgauz ja Maret Sõmer)

Ülesandes on vaja lahendada kongruents $2019 \cdot x^{2020} \equiv 2022 \pmod{31}$.

Lause 3.5 põhjal kehtib kongruents $2019 \cdot x^{2020} \equiv 2022 \pmod{31}$ parajasti siis, kui kehtib võrdus $\overline{2019} \cdot x^{2020} = \overline{2022}$ ringis $\mathbb{Z}_{31}$. Panen tähele, et selles ringis on $\overline{2019}^{-1} = \overline{4}^{-1} = \overline{8}$, kuna $\overline{4} \cdot \overline{8} = \overline{32} = \overline{1}$. Seega on võrdus $\overline{2019} \cdot x^{2020} = \overline{2022}$ samaväärne võrdusega $x^{2020} = \overline{2022} \cdot \overline{8}$ ehk $x^{2020} = \overline{25}$. Järelikult piisab esialgse kongruentsi lahendamiseks lahendada kongruents $x^{2020} \equiv 25 \pmod{31}$.

Kuna $\varphi(31) = 30$, ja $25^{30/(2020,30)} = 25^{30/10} = 25^3 \equiv 1 \pmod{31}$, siis on teoreemi 7.33 põhjal kongruents $x^{2020} \equiv 25 \pmod{31}$ lahenduv, ning sellel on (2020,30) = 10 erinevat lahendit. Leian need lahendid.

Kõigepealt märgin, et eelmisest ülesandest on teada, et 3 on algjuur mooduli 31 järgi, ning 4. ülesande lahenduses on ka selle indeksite tabel. Indekseerides (lause 7.30) saan kongruentsist $x^{2020} \equiv 25 \pmod{31}$ esimesega samaväärse kongruentsi $\mathrm{ind}_3 x^{2020} \equiv \mathrm{ind}_3 25 \pmod{30}$, mis teoreemis 7.32 toodud 4. omaduse põhjal on samaväärne kongruentsiga $2020 \cdot \mathrm{ind}_3 x \equiv \mathrm{ind}_3 25 \pmod{30}$. Eelmises ülesandes toodud indeksite tabeli põhjal $\mathrm{ind}_3 25 = 10$, seega $2020 \cdot \mathrm{ind}_3 x \equiv 10 \pmod{30}$.
Lause 3.10 põhjal $10 \cdot 202 \cdot \mathrm{ind}_3 x \equiv 10 \cdot 1 \pmod{10 \cdot 3}$ parajasti siis, kui $202 \cdot \mathrm{ind}_3 x \equiv 1 \pmod{3}$. Kuna $202 \equiv 1 \pmod{3}$, siis olen jõudnud kongruentsini $\mathrm{ind}_3 x \equiv 1 \pmod{3}$.
Teoreemi 7.32 1. omadus ütleb, et $1 \leq \mathrm{ind}_a b \leq \varphi(n)$ ehk $1 \leq \mathrm{ind}_3 x \leq 30$. Järelikult on $\mathrm{ind}_3 x = 1, 4, 7, 10, 13, 16, 19, 22, 25, 28$, kuna need on ainsad arvud vahemikus [1,30], mis on mooduli 3 järgi kongruentsed arvuga 1. Eelmises ülesandes toodud indeksite tabelit n-ö tagurpidi kasutades leian, et
$x = 3, 19, 17, 25, 24, 28, 12, 14, 6, 7$.

Kontroll.
$3^{2020} = 3^{30 \cdot 67+10} = (3^{30})^{67} \cdot 3^{10} \equiv 1^{67} \cdot 3^{10} \equiv (3^5)^2 \equiv (-5)^2 \equiv 25 \pmod{31}$
$6^{2020} = 6^{30 \cdot 67+10} = (6^{30})^{67} \cdot 6^{10} \equiv 1^{67} \cdot 6^{10} \equiv (6^5)^2 \equiv (-5)^2 \equiv 25 \pmod{31}$
$7^{2020} = 7^{30 \cdot 67+10} = (7^{30})^{67} \cdot 7^{10} \equiv 1^{67} \cdot 7^{10} \equiv (7^5)^2 \equiv (5)^2 \equiv 25 \pmod{31}$
$12^{2020} = 12^{30 \cdot 67+10} = (12^{30})^{67} \cdot 12^{10} \equiv 12^{10} \equiv (12^5)^2 \equiv (-5)^2 \equiv 25 \pmod{31}$
$14^{2020} = 14^{30 \cdot 67+10} = (14^{30})^{67} \cdot 14^{10} \equiv 1^{67} \cdot 14^{10} \equiv (14^5)^2 \equiv (5)^2 \equiv 25 \pmod{31}$
$17^{2020} = 17^{30 \cdot 67+10} = (17^{30})^{67} \cdot 17^{10} \equiv 17^{10} \equiv (17^5)^2 \equiv (-5)^2 \equiv 25 \pmod{31}$
$19^{2020} = 19^{30 \cdot 67+10} = (19^{30})^{67} \cdot 19^{10} \equiv 1^{67} \cdot 19^{10} \equiv (19^5)^2 \equiv (5)^2 \equiv 25 \pmod{31}$
$24^{2020} = 24^{30 \cdot 67+10} = (24^{30})^{67} \cdot 24^{10} \equiv 24^{10} \equiv (24^5)^2 \equiv (-5)^2 \equiv 25 \pmod{31}$
$25^{2020} = 25^{30 \cdot 67+10} = (25^{30})^{67} \cdot 25^{10} \equiv 1^{67} \cdot 25^{10} \equiv (25^5)^2 \equiv (5)^2 \equiv 25 \pmod{31}$
$28^{2020} = 28^{30 \cdot 67+10} = (28^{30})^{67} \cdot 28^{10} \equiv 1^{67} \cdot 28^{10} \equiv (28^5)^2 \equiv (5)^2 \equiv 25 \pmod{31}$

See tähendab, et iga lahendi x = 3,6,7,12,14,17,19,24,25,28 korral $x^{2020} \equiv$
$\equiv 25 \equiv -6 \pmod{31}$. Seega $2019 \cdot x^{2020} \equiv 4 \cdot (-6) \equiv -24 \equiv 7 \equiv 2022 \pmod{31}$.

6. ülesanne (Mikael Raihhelgauz ja Maret Sõmer)

Tähistame $d = (8, \varphi(11)) = (8{,}10) = 2$. Teoreemi 7.33 põhjal kongruents $x^8 \equiv a \mod 11$ on lahenduv, kui

$$a^{\frac{\varphi(11)}{2}} = a^5 \equiv 1 \mod 11.$$

On ilmne, et 1 sobib. Leiame lahendid proovimise teel:

$$2^5 = 32 \equiv 10 \mod 11, \quad \mathbf{3^5} \equiv 9 \cdot 5 \equiv 1 \mod 11,$$
$$\mathbf{4^5} = (2^5)^2 \equiv 10^2 \equiv 1 \mod 11, \quad \mathbf{5^5} = 3 \cdot 3 \cdot 5 \equiv 1 \mod 11.$$

Oleme leidnud neli lahendit. Kokku peab antud kongruentsil olema 5 lahendit. Paneme tähele, et $9^5 = (3^5)^2 \equiv 1 \mod 11$. Vahemikust [1,25] sobivad seega $\{1, 3, 4, 5, 9, 12, 14, 15, 16, 20, 23, 25\}$. Tähistame $d = (8, \varphi(13)) = (8{,}12) = 4$. Kongruents $x^8 \equiv a \mod 13$ on lahenduv, kui

$$a^{\frac{\varphi(13)}{4}} = a^3 \equiv 1 \mod 13.$$

Selge, et 1 on üks sobiv lahend. Proovime ka teisi arve:

$$2^3 \equiv 8 \mod 13, \quad \mathbf{3^3} \equiv 1 \mod 13.$$

Paneme tähele, et $9^3 = (3^3)^2 \equiv 1 \mod 13$. Et kongruentsil saab olla vaid 3 lahendit, siis kõik lahendid on leitud. Niisiis, sobivad a väärtused on $\{1, 3, 9, 14, 16, 22\}$. Tähistame $d =$

$= (8, \varphi(25)) = (8{,}20) = 4$. Kongruents $x^8 \equiv a \mod 25$ on lahenduv, kui

$$a^{\frac{\varphi(25)}{4}} = a^5 \equiv 1 \mod 25.$$

Eelnevalt oleme kitsendanud sobivate a väärtuste hulka. Sobivad ainult väärtused $\{1, 3, 9, 14, 16, 22\} \cap \{1, 3, 4, 5, 9, 12, 14, 15, 16, 20, 23, 25\} = \{1, 3, 9, 14, 16\}$. Kontrollime, millised neist sobivad ülaltoodud kongruentsi lahenditeks:

$$3^5 \equiv 2 \cdot 9 \equiv 18 \mod 25, \quad 9^5 \equiv 6 \cdot 6 \cdot 9 \equiv 11 \cdot 9 \equiv 24 \mod 25,$$
$$14^5 \equiv 21 \cdot 21 \cdot 14 \equiv 16 \cdot 14 \equiv 24 \mod 25, \quad 16^5 \equiv 6 \cdot 6 \cdot 16 \equiv 11 \cdot 16 \equiv 1 \mod 25.$$

Näeme, et sobivad a väärtused on 1 ja 16.

Lauri Tart: Vähem arvutamist nõudev lahendus: ei ole raske kontrollida, et arv 2 on algjuur kõigi moodulite 11, 13 ja 25 järgi, kasvõi E. Redi "Arvuteooria" õpiku tabelite põhjal. Kõik vaadeldavad moodulid on ühistegurita, seega näiteks juhul $a \equiv 0 \pmod{11}$ peaks kehtima $a \in \{11{,}22\}$ ja $0 \equiv a^8 \equiv (11)^8 \pmod{13}$ või samamoodi $0 \equiv 22^8 \pmod{13}$. See ilmselt nii ei ole. Seega mooduli 11 järgi on lahendid pööratavad ja esitatavad kujul $x \equiv 2^k \pmod{11}$. Järelikult lemma 7.6 annab meile, et

$$(2^k)^5 \equiv 1 \pmod{11} \iff \varphi(11) = 10 \mid 5k \iff 2 \mid k.$$

Seega lahendid mooduli 11 järgi on täpselt needsamad, mida me eelpool juba nägime:

$$\overline{2}^0 = \overline{1}, \overline{2}^2 = \overline{4}, \overline{2}^4 = \overline{16} = \overline{5}, \overline{2}^6 = \overline{64} = \overline{9} \text{ ja } \overline{2}^8 = \overline{9} \cdot \overline{4} = \overline{36} = \overline{3}.$$

Samamoodi saab lahendeid leida teiste moodulite järgi, näiteks mooduli 25 järgi on need $\overline{2}^4, \overline{2}^8, \overline{2}^{12}, \overline{2}^{16}, \overline{2}^{20}$ ehk $\overline{1}, \overline{6}, \overline{11}, \overline{16}, \overline{21}$. Arvutades Mikaeli ja Mareti lahendusega analoogiliselt välja kõik sobivad $1 \leq a \leq 25$ väärtused 11, 13 ja 25 jaoks ning võttes nende kolme hulga ühisosa, saamegi sama vastuse, st $a = 1$ või $a = 16$.

7. ülesanne (Mikael Raihhelgauz ja Maret Sõmer)

Et a on algjuur mooduli p järgi, siis $U(\mathbb{Z}_p) = \{\overline{1}, \overline{2}, \ldots, \overline{p-1}\} = \{\overline{a}, \overline{a}^2, \overline{a}^3, \ldots, \overline{a}^{p-1}\}$. Ehk iga $1 \leq g \leq p-1$ korral leidub parajasti üks arv $1 \leq k \leq p-1$, et $g = a^k \mod p$. Järelikult

$$\mathrm{ind}_a(1) \cdot \mathrm{ind}_a(2) \cdot \ldots \cdot \mathrm{ind}_a(p-1) = 1 \cdot 2 \cdot \ldots \cdot (p-1).$$

Algjuure definitsiooni kohaselt $\mathrm{ind}_a(1) = p-1$. Järelikult

$$\mathrm{ind}_a(2) \cdot \ldots \cdot \mathrm{ind}_a(p-1) = \frac{1 \cdot 2 \cdot \ldots \cdot (p-1)}{p-1}.$$

Märkame, et $(p-1)^2 = p^2 - 2p + 1 = p(p-2) + 1 \equiv 1 \mod p$. Niisiis, $\overline{1}$ ja $\overline{p-1}$ on iseenda pöördelemendid rühmas $U(\mathbb{Z}_p)$, kusjuures $p-1$ järk on 2. Ükski teine element selles rühmas ei ole iseenda pöördelement. Kui veel mõni element g oleks iseenda pöördelemet, siis tähendaks see, et $\mathrm{ord}(g) = 2$, mis on vastuolus lemmaga 7.8. Seega ülejäänud elemendid jagunevad lõikumatuteks pöördelementide paarideks. Niisiis, $2 \cdot \ldots \cdot (p-2) \equiv 1 \mod p$. Järelikult

$$\frac{1 \cdot 2 \cdot \ldots \cdot (p-1)}{p-1} \equiv \frac{p-1}{p-1} \equiv 1 \mod p.$$

Kokkuvõttes iga algarvu p korral

$$\mathrm{ind}_a(2) \cdot \ldots \cdot \mathrm{ind}_a(p-1) \equiv 1 \mod p.$$

8. ülesanne (Johanna Maria Kirss ja Rainer Bõkov)

Näitame kõigepealt, et arv $\frac{p-1}{2}$ on algjuur parajasti siis, kui -2 järk on k. Euleri teoreemist lähtuvalt piisab näidata, et iga arvu $p-1$ jagaja d korral $\left(\frac{p-1}{2}\right)^d \not\equiv 1 \pmod p \Leftrightarrow (-2)^d \not\equiv 1 \pmod p$. Fikseerime seega mingi $d|p-1$ ja näitame:

$$\begin{aligned}\left(\frac{p-1}{2}\right)^d \not\equiv 1 \pmod p &\Leftrightarrow (p-1)^d \not\equiv 2^d \pmod p \\ &\Leftrightarrow (-1)^d \not\equiv 2^d \pmod p \\ &\Leftrightarrow 1 \not\equiv (-2)^d \pmod p.\end{aligned}$$

Olgu näiteks $\frac{p-1}{2}$ on paaritu. Siis $2(-1)^{\frac{p-1}{2}} = (-2)^{\frac{p-1}{2}}$. Saame võtta $d = \frac{p-1}{2}$ ja eelnevalt tõestatu põhjal väide kehtib.

Olgu nüüd aga $\frac{p-1}{2}$ paaris ehk $p \equiv 1 \pmod 4$. Teame, et -2 on algjuur. Kümnendas praktikumis oleme tõestanud, et need kaks asjaolu tingivad, et ka 2 on algjuur ja $2 = 2(-1)^{\frac{p-1}{2}}$. Seega oleme näidanud vajaliku tulemuse.