Arvuteooria

Näidislahendused

Praktikum 7

1 Johanna Maria Kirss

Kuna $(2019, 2021) = 1$, siis on lineaarkongruentsi lahend ühene.

$$\begin{aligned} 2019x + 7531 &\equiv 2020 \pmod{2021} \\ 2019x &\equiv -5511 \pmod{2021} \\ -2x &\equiv 552 \pmod{2021} \\ 2x &\equiv -552 \pmod{2021} \end{aligned}$$

Nüüd paneme tähele, et kuna $(2, 2021) = 1$, siis leidub kahel mingi pöördelelment 2^{-1} mooduli 2021 järgi. Korrutades sellega kongruentsi pooli, saame:

$$\begin{aligned} 2x &\equiv 2 \cdot (-276) \pmod{2021} \\ x &\equiv -276 \pmod{2021} \\ x &\equiv 1745 \pmod{2021} \end{aligned}$$

2 Markus Rene Pae

Meil on lineaarkongruentside süsteem

$$\begin{cases} 3x \equiv 5 & \pmod{32} \\ 5x \equiv 3 & \pmod{22} \\ 7x \equiv 1 & \pmod{12}. \end{cases}$$

Kuna $22 = 2 \cdot 11$ ja $12 = 4 \cdot 3$, kusjuures $(2, 11) = 1$ ja $(4, 3) = 1$, siis vastavalt loengukonspekti lausele 6.10 on ülesandes püstitatud lineaarkongruentside süsteem samaväärne järgneva kongruentside süsteemiga:

$$\begin{cases} 3x \equiv 5 & \pmod{32} \\ 5x \equiv 3 & \pmod{2} \\ 5x \equiv 3 & \pmod{11} \\ 7x \equiv 1 & \pmod{3} \\ 7x \equiv 1 & \pmod{4}. \end{cases}$$

Selle saame lihtsustada kujule:

$$\begin{cases} x \equiv 23 & (\text{mod } 32) \\ x \equiv 1 & (\text{mod } 2) \\ x \equiv 5 & (\text{mod } 11) \\ x \equiv 1 & (\text{mod } 3) \\ x \equiv 3 & (\text{mod } 4). \end{cases}$$

Nüüd paneme tähele, et sellest et $x \equiv 23 \pmod{32}$ järeldub, et $x \equiv 1 \pmod{2}$ ja $x \equiv 3 \pmod{4}$. Seda sellepärast, et kui $x \equiv 23 \pmod{32}$, siis $x = 32k + 23$ mingi $k \in \mathbb{Z}$ korral ja seega $x \equiv 23 \equiv 1 \pmod{2}$ ja $x \equiv 23 \equiv 3 \pmod{4}$. Seega saame oma võrrandisüsteemi lihtsustada kujule

$$\begin{cases} x \equiv 23 & (\text{mod } 32) \\ x \equiv 5 & (\text{mod } 11) \\ x \equiv 1 & (\text{mod } 3) \end{cases}$$

Selle süsteemi lahendi saame kätte Hiina jäägiteoreemi abil. Selleks tähistame $m_1 = 33$, $m_2 = 96$, $m_3 = 352$ ning leiame, et ringis $\mathbb{Z}_{32}$ $\overline{k_1} = \overline{m_1}^{-1} = \overline{1}^{-1} = \overline{1}$, ringis $\mathbb{Z}_{11}$ $\overline{k_2} = \overline{m_2}^{-1} = \overline{8}^{-1} = \overline{7}$ ja ringis $\mathbb{Z}_3$ $\overline{k_3} = \overline{m_3}^{-1} = \overline{1}^{-1} = \overline{1}$. Lineaarkongruentside süsteemile saame lahendi valemist

$$x = \sum_{j=1}^{3} a_j k_j m_j = 23 \cdot 1 \cdot 33 + 5 \cdot 7 \cdot 96 + 1 \cdot 1 \cdot 352 = 4471$$

Seega $x \equiv 4471 \equiv 247 \pmod{32 \cdot 11 \cdot 3}$ ehk $x \equiv 247 \pmod{1056}$.

3 Markus Rene Pae

Meil on lineaarkongruentside süsteem

$$\begin{cases} 3x \equiv 7 & (\text{mod } 22) \\ 5x \equiv 5 & (\text{mod } 32) \\ 7x \equiv 1 & (\text{mod } 12). \end{cases}$$

Analoogiliselt eelmise ülesandega, saame selle süsteemi kirja panna kujul:

$$\begin{cases} 3x \equiv 7 & (\text{mod } 2) \\ 3x \equiv 7 & (\text{mod } 11) \\ 5x \equiv 5 & (\text{mod } 32) \\ 7x \equiv 1 & (\text{mod } 3) \\ 7x \equiv 1 & (\text{mod } 4) \end{cases}$$

Seda lihtsustades jõuame kujuni

$$\begin{cases} x \equiv 1 & (\text{mod } 2) \\ x \equiv 6 & (\text{mod } 11) \\ x \equiv 1 & (\text{mod } 32) \\ x \equiv 1 & (\text{mod } 3) \\ x \equiv 3 & (\text{mod } 4) \end{cases}$$

ui kehtib kongruents $x \equiv 1 \pmod{32}$, siis x avaldub kujul $32k+1$, kus $k \in \mathbb{Z}$. Sellisel kujul x puhul kehtib kongruents $x = 32k+1 \equiv 1 \pmod{4}$. See on aga vastuolus süsteemis oleva kongruentsiga $x \equiv 3 \pmod{4}$. Seega see süsteem ei ole lahenduv.

4 Lahenduse autor on toimetusele teada

Olgu $A = 12^{(34^{(56^{78})})}$. Leidmaks millega on võrdne A mooduli 91 järgi leiame kõigepealt millega ta on võrdne moodulite 7 ja 13 järgi. Kuna $91 = 7 \cdot 13$, siis saame moodustada kongruentsid

$$\begin{cases} A \equiv y & \pmod{13} \\ A \equiv z & \pmod{7} \end{cases}$$

Lahendame kõigepealt kongruentsi $A \equiv y \pmod{13}$

Arvus A on korrutatud arvu 12 iseendaga mingi arv kordi ning me teame, et seda on tehtud paarisarv kordi, sest 34 on paarisarv. Seega saame rühmitada arvus A tegurid 12 paarikaupa ning mooduli 13 järgi arvutada kõikide paaride korrutise väärtuse. Kuna $12 \cdot 12 = 144 \equiv 1 \pmod{13}$, siis saame $A \equiv 1 \pmod{13}$.

Nüüd vaatame kongruentsi

$$A = 12^{34^{56^{78}}} \equiv 5^{34^{56^{78}}} \pmod{7}$$

Olgu $B = 5^{34^{56^{78}}}$. Arvus B on arvu 5 korrutatud iseendaga $34^{56^{78}}$ korda. Kasutades Fermat' väikest teoreemi, leiame viimase arvu mooduli $\varphi(7) = 6$ järgi:

$$34^{56^{78}} \equiv 4^{56^{78}} \pmod{6}$$

Kuna $4 \cdot 4 = 16 = 4 \pmod{6}$, siis olenemata saanud, et

$$34^{56^{78}} \equiv 4^{56^{78}} \equiv 4 \pmod{6}$$

Seega

$$5^{34^{56^{78}}} \equiv 5^{6t+4} = 5^4 \equiv 2 \pmod{7}$$

Nüüd jääb rakendada Hiina jäägiteoreemi süsteemile

$$\begin{cases} x \equiv 1 \pmod{13} \\ x \equiv 2 \pmod{7}. \end{cases}$$

Võttes $m_1 = \frac{91}{13} = 7, m_2 = \frac{91}{7} = 13$, siis vahetult leides nende pöördelemendid vastavalt ringides $\mathbb{Z}_{13}$, $\mathbb{Z}_7$ saame, et

$$x = 1 \cdot 7 \cdot 2 + 2 \cdot 13 \cdot 6 = 170 \equiv 79 \pmod{91}.$$

Oleme seega saanud, et $12^{(34^{(56^{78})})} \equiv 79 \pmod{91}$.

5 Johanna Maria Kirss

Kuna $792 = 9 \cdot 11 \cdot 8$, siis selleks, et arv $x13yz57w$ jaguks arvuga 792, tahame leida tingimused, kunas see arv jagub kaheksa, üheksa ja üheteistkümnega.

Et arv jaguks kaheksaga, peab arvu viimasest kolmest numbrist saadud arv jaguma kaheksaga. See on antud juhul $57w$ ning ainuke sellisel kujul kaheksaga jaguv arv on 576.

Üheksaga jagumises peab arvu ristsumma jaguma üheksaga, ning üheteistkümne puhul kehtib sama reegel vahetuvate märkidega ristsumma puhul:

$$9|x + 1 + 3 + y + z + 5 + 7 + 6 = x + y + z + 22,$$

$$11|6 - 7 + 5 - z + y - 3 + 1 - x = -x + y - z + 2.$$

Uurime kõigepealt jaguvust üheteistkümnega. Näeme, et saab kehtida $-x+y-z+2 = 11$ vaid siis, kui $x = z = 0$ ja $y = 9$. Selline väärtustus aga ei tagaks üheksaga jaguvust, sest $0 + 9 + 0 + 22 = 31$. Igal muul väärtustusel on summa $-x+y-z+2$ ilmselt üheteistkümnest väiksem. Seega vaatam kahte juhtu, kui

$$-x + y - z + 2 = 0.$$

ja kui

$$-x + y - z + 2 = -11$$

. Vaatama kõigepealt juhtu $-x + y - z + 2 = 0$.
Siit on kohe näha, et $y = x+z-2$. Asendame selle üheksaga jaguvuse tingimusse ning saame, et peab kehtima

$$9|x + x + z - 2 + z + 22 = 2x + 2z + 20.$$

Summa $2x+2z+20$ võimalikud väärtused jäävad 20 ja 56 vahele. Sellesse lõiku kuuluvad üheksaga jaguvad arvud on 27, 36, 45 ja 54, millest ainult 36 ja 54 sobivad antud summa paarisarvulisusega. Seega saame kaks võimalikku seost:

$$2x + 2z + 20 = 36 \Leftrightarrow x + z = 8$$

ja

$$2x + 2z + 20 = 54 \Leftrightarrow x + z = 17.$$

Näeme, et teine saadud tulemus on vastuoluline, sest $y = 17 - 2 = 15$ ei oleks siis enam number. Jääb alles vaid esimene seos, mille puhul siis $y = 8 - 2 = 6$. Olemegi saanud väärtustuse igale muutujale nii, et arv $x13yz57w$ jaguks arvuga 792. Muutujatel y ja w on kindel väärtus - mõlemal 6 - ning x ja z võivad omandada mistahes väärtusi nii, et nende summa oleks 8. Sobivad arvud $x13yz57w$ on järelikult

$$01368576, 11367576, 21366576, 31365576, 41364576, 51363576, 61362576, 71361576, 81360576.$$

Vaatame nüüd juhtu $-x + y - z + 2 = -11$. Siis $y = -13 + x + z$ ja asendades selle 9-ga jagumise tingimusse saame et peab kehtima

$$9 \mid 2x + 2z + 9$$

ehk $9 \mid 2(x+z)$. Seega $x+z=9$ või $x+z=0$ või $x+z=18$. Esimesed kaks juhtu ei sobi, sest siis vastavalt $y=-4$ või $y=-13$. Viimsel juhul $y=5$ ja me saame lahendiks

$$91359576$$

6 Vigane ülesanne

Algne ülesanne oli raske ja ei ole kindel, kas see sellisel kujul on üldse elementaarselt lahendatav. Seetõttu lahendame natuke muudetud ülesande:

Tõestada, et iga naturaalarvu n jaoks leiduvad n järjestikust naturaalarvu $x_1, x_2, .., x_i, ..., x_n$ selliselt, et igal arvul x_i on vähemalt i algtegurit. Fikseerime vabalt $n \in \mathbb{N}$. Lahendame ülesande HJT kasutades. Olgu meil $m = \frac{n(n-1)}{2}$ erinevat algarvu $p_1, p_2, ..., p_m$, siis moodustame süsteemi

$$\begin{cases} x_1 \equiv 0 & (\text{mod } p_1) \\ x_2 \equiv 0 & (\text{mod } p_2 \cdot p_3) \\ x_3 \equiv 0 & (\text{mod } p_4 \cdot p_5 \cdot p_6) \\ & ... \\ x_n \equiv 0 & (\text{mod } p_{m-n+1} \cdot ... \cdot p_m). \end{cases}$$

Kasutades teadmist, et $x_2 = x_1 + 1$ ehk üldisemalt $x_i = x_1 + (i-1)$ saame selle ümber kirjutada kujule

$$\begin{cases} x_1 \equiv 0 & (\text{mod } p_1) \\ x_1 \equiv -1 & (\text{mod } p_2 \cdot p_3) \\ x_1 \equiv -2 & (\text{mod } p_4 \cdot p_5 \cdot p_6) \\ & ... \\ x_1 \equiv -(n-1) & (\text{mod } p_{m-n+1} \cdot ... \cdot p_m). \end{cases}$$

Nüüd kuna kõik algarvud $p_1, ..., p_m$ on omavahel ühistegurita, siis leidub sellel süsteemil Hiina jäägiteoreemi järgi lahend. See lahend rahuldabki meie ülesande tingimusi.

7 Urmas Luhaäär

Olgu n kujul $n = 3^k n'$, kus $k \in \mathbb{N} \cup \{0\}$. Siis sellest, et $27a^3 + 25b^2 - 1 \equiv 0 \pmod{n}$, saame et

$$\begin{cases} 27a^3 + 25b^2 - 1 \equiv 0 & (\text{mod } 3^k) \\ 27a^3 + 25b^2 - 1 \equiv 0 & (\text{mod } n'). \end{cases}$$

Võtame $a \equiv 0 \pmod{3^k}$, siis $25b^2 - 1 = (5b-1)(5b+1) \equiv 0 \pmod{3^k}$. Võtame $5b \equiv 1 \pmod{3^k}$. Kuna $(3,5) = 1$, siis võime võtta $b \equiv 5^{-1} \pmod{3^k}$.

Nüüd on meil veel kongruents $27a^3 + 25b^2 - 1 \equiv 0 \pmod{n'}$. Võtame $b \equiv 0 \pmod{n}$, siis jääb meile alles kongruents

$$27a^3 - 1 = (3a-1)(9a^2+3a+1) \equiv 0 \pmod{n'}$$

Kuna $(3, n') = 1$, siis saame võtta $a = 3^{-1} \pmod{n'}$. Saame võrrandisüsteemid

$$\begin{cases} a \equiv 0 & \pmod{3^k} \\ a \equiv 3^{-1} & \pmod{n'}. \end{cases}$$

$$\begin{cases} b \equiv 5^{-1} & \pmod{3^k} \\ b \equiv 0 & \pmod{n'}. \end{cases}$$

mis on HJT kohaselt üheselt lahenduvad.

8 Urmas Luhaäär

Olgu $p \in \mathbb{P}$ ja $p \not| 2$. Vaatame juhte, kus $n = 2^t p^k$, $t > 1$ ja $n = qp^k$, kus $q \neq 2^t$ ja $q \neq 1$.
1) Olgu $n = 2^t p^k$ ja $x^2 \equiv 1 \pmod{n}$, siis see on samaväärne kongruentsiga $(x-1)(x+1) \equiv 0 \pmod{n}$. Saame selle kirjutada kujul

$$\begin{cases} (x-1)(x+1) \equiv 0 & \pmod{2^t} \\ (x-1)(x+1) \equiv 0 & \pmod{p^k}. \end{cases}$$

Kuna $t > 1$, siis $1 \not\equiv -1 \pmod{2^t}$ ja mõlemal kongruentsil on vähemalt 2 erinevat lahendit. Saame nüüd moodustada võrrandisüsteemid

$$\begin{cases} x \equiv 1 & \pmod{2^t} \\ x \equiv 1 & \pmod{p^k}, \end{cases} \quad \begin{cases} x \equiv 1 & \pmod{2^t} \\ x \equiv -1 & \pmod{p^k}, \end{cases}$$

$$\begin{cases} x \equiv -1 & \pmod{2^t} \\ x \equiv 1 & \pmod{p^k}, \end{cases} \quad \begin{cases} x \equiv 1 & \pmod{2^t} \\ x \equiv -1 & \pmod{p^k}. \end{cases}$$

HJT ütleb, et kõik need süsteemid on üheselt lahenduvad. Igav süsteemi lahend on erinev ja neid on kokku 4.
2) Olgu n kujul $n = p_1^{k_1} \cdot ... \cdot p_m^{k_m}$, kus $m \geq 2$. Saame süsteemi

$$\begin{cases} (x-1)(x+1) \equiv 0 & \pmod{p_1^{k_1}} \\ (x-1)(x+1) \equiv 0 & \pmod{p_2^{k_2}} \\ & ... \\ (x-1)(x+1) \equiv 0 & \pmod{p_m^{k_m}}, \end{cases}$$

Nüüd saame nagu ennegi, teha süsteemid, kus me võtame iga kongruentsi jaoks x-i kongruentseks 1 või -1-ga. Me saame teha 2^m erinevat süsteemi ja igal neist on erinev lahend. Seega on meie algsel kongruentsil kokku 2^m erinevat lahendit ja kuna $m \geq 2$, siis on lahendeid vähemalt 4.