Arvuteooria

Näidislahendused

Praktikum 8

1 Laura Karu

Kasutame lahendite leidmiseks Horneri skeemi.

	2	5	2	3	6
0	2	5	2	3	6
1	2	7	9	12	5
2	2	9	7	4	1
3	2	11	9	4	5
4	2	0	2	11	11
5	2	2	12	11	9
6	2	4	0	3	11
7	2	6	5	12	12
8	2	8	1	11	3
9	2	10	1	12	10
10	2	12	5	1	3
11	2	1	0	3	0
12	2	3	12	4	2

Tabelist näeme, et ainus lahend on $x \equiv 11 \pmod{13}$.

2 Aljona Kritševskaja

Tegurdame polünoom

$$f(x) = 2x^4 + 3x^2 + 4x + 2$$

mooduli 7 järgi. Lahendame ülesande Horneri skeemi abil:

	2	0	3	4	2
1	2	2	5	2	4
2	2	4	4	5	5
3	2	6	0	4	0
3	2	5	1	0	
3	2	4	6		
4	2	6	4		
5	2	1	6		
6	2	3	5		
0	2	5	1		

Tabelist saame $2x^4 + 3x^2 + 4x + 2 = (x-3)^2(2x^2 + 5x + 1)$.

3 Johanna Maria Kirss

Ülesande tekstist näeme, et otsime kongruentsi

$$4x^4 + 3x^3 - 3x^2 + x + 1 \equiv 3 \pmod{10}$$

ehk kongruentsi

$$f(x) = 4x^4 + 3x^3 - 3x^2 + x - 2 \equiv 0 \pmod{10}$$

lahendeid. Ilmselt mingi x korral $f(x)$ jagub kümnega parajasti siis, kui ta jagub kahe ja viiega. Seega saame leida veidi vähesema randmevaevaga lihtsalt lahendid süsteemile

$$\begin{cases} 4x^4 + 3x^3 - 3x^2 + x - 2 \equiv x^3 + x^2 + x \equiv 0 \pmod{2} \\ 4x^4 + 3x^3 - 3x^2 + x - 2 \equiv -x^4 - 2x^3 + 2x^2 + x - 2 \equiv 0 \pmod{5}. \end{cases}$$

Siit näeme, et esimese kongruentsi lahendiks on $x \equiv 0 \pmod{2}$ ja teise kongruentsi lahendiks on $x \equiv 4 \pmod{5}$.
On selge, et ainuke arv lõigus $[0, 9]$, mis neid tingimusi rahuldab on 4 ja seega $x \equiv 4 \pmod{10}$. Lahendi võib muidugi ka HJT abil leida.

4 Johanna Maria Kirss

Lahendame kongruentsi

$$f(x) = 2x^4 + 5x^3 + 2x^2 + 3x - 21 \equiv 0 \pmod{81},$$

kusjuures funktsiooni f tuletis on

$$f'(x) = 8x^3 + 15x^2 + 4x + 3.$$

Loome vastava tabeli.

	$f(x)$	2	5	2	3	-21	$f'(x)$	8	15	4	3	
(mod 3)	0	2	2	2	0	0	0	2	0	1	0	
	1	2	1	0	0	0	1	2	2	0	0	
(mod 9)	0	2	5	2	3	-3						$0y + \frac{-3}{3} \equiv 0 \pmod 3$ Vastuolu!
	1	2	7	0	3	0						$0y + \frac{0}{3} \equiv 0 \pmod 3$
(mod 27)	1	2	7	9	12	-9						$0y + \frac{-9}{9} \equiv 0 \pmod 3$ Vastuolu!
	4	2	13	0	3	-9						$0y + \frac{-9}{9} \equiv 0 \pmod 3$ Vastuolu!
	7	2	19	0	3	0						$0y + \frac{0}{9} \equiv 0 \pmod 3$
(mod 81)	7	2	19	54	57	54						$0y + \frac{54}{27} \equiv 0 \pmod 3$ Vastuolu!
	16	2	37	27	30	54						$0y + \frac{54}{27} \equiv 0 \pmod 3$ Vastuolu!
	25	2	55	0	3	54						$0y + \frac{54}{27} \equiv 0 \pmod 3$ Vastuolu!

Järelikult ei leidu ühtki täisarvu, mille korral antud kongruents kehtiks.

5 Johanna Maria Kirss

Tegurdame $51597 = 3^4 \cdot 7^2 \cdot 13$. Seega algne kongruents on samaväärne süsteemiga:

$$\begin{cases} 2x^4 + 5x^3 + 2x^2 + 3x + 6 \equiv 0 \pmod{81} \\ 2x^4 + 5x^3 + 2x^2 + 3x + 6 \equiv 0 \pmod{49} \\ 2x^4 + 5x^3 + 2x^2 + 3x + 6 \equiv 0 \pmod{13} \end{cases}$$

Märkame kõigepealt, et antud funktsioon

$$f(x) = 2x^4 + 5x^3 + 2x^2 + 3x + 6$$

on mooduli 27 järgi ekvivalentne eelmise ülesande polünoomiga

$$2x^4 + 5x^3 + 2x^2 + 3x - 21.$$

Seega on tal mooduli 27 järgi samad lahendid, mis tähendab, et meil jääb vaid otsida lahendeid mooduli 81 järgi:

	$f(x)$	2	5	2	3	6	$f'(x)$	8	15	4	3	
(mod 81)	7	2	19	54	57	0						$0y + \frac{0}{27} \equiv 0 \pmod 3$
	16	2	37	27	30	0						$0y + \frac{0}{27} \equiv 0 \pmod 3$
	25	2	55	0	3	0						$0y + \frac{0}{27} \equiv 0 \pmod 3$

Kuna kõik kongruentsid osutusid samaselt tõesteks, siis lahendid on $x \equiv 7, 16, 25 \pmod{27}$ ehk $x \equiv 7 \pmod 9$.

	$f(x)$	2	5	2	3	6	$f'(x)$	8	15	4	3	
(mod 7)	0	2	5	2	3	6	4	1	5	3	1	
	1	2	0	2	5	4	5	1	-1	-1	-2	
	2	2	2	6	1	1						
	3	2	4	0	3	1						
	4	2	-1	5	2	0						
	5	2	2	1	0							
	-1	2	0	1								
(mod 49)	4	2	13	5	23	0						$1y + \frac{0}{7} \equiv 0 \pmod 7$
	5	2	15	28	-4	-14						$(-2)y + \frac{-14}{7} \equiv 0 \pmod 7$

Näeme, et kongruentsi $f(x) \equiv 0 \pmod{49}$ lahenditeks sobivad kindlasti arvud kujul $x = 4 + 49z$. Uurime avaldist

$$(-2)y + \frac{-14}{7} \equiv (-2)y - 2 \pmod{7} \Leftrightarrow y \equiv -1 \pmod{7}.$$

Saame, et teiseks lahendiks on seega $x = 7(7z - 1) + 5 = 49z - 2$.
Esimesest ülesandest saame, et mooduli 13 järgi on lahendiks $x \equiv 11$.
Nüüd saame kasutada Hiina jäägiteoreemi, sest oleme saanud süsteemid

$$\begin{cases} x \equiv 7 \pmod{9} \\ x \equiv 4 \pmod{49} \\ x \equiv -2 \pmod{13} \end{cases} \quad \text{ja} \quad \begin{cases} x \equiv 7 \pmod{9} \\ x \equiv -2 \pmod{49} \\ x \equiv 11 \pmod{13}. \end{cases}$$

Hiina jäägiteoreemi abil saame esimesest süsteemist

$$x \equiv 4561 \pmod{5733}$$

ja teisest

$$x \equiv 5731 \pmod{5733}.$$

6 Lahenduse autor on toimetusele teada

Paneme tähele, et arvude LEHV ja 1KSTREHV viimased kolm kümnendnumbrit on võrdsed, seega lahendame kongruentsi, kus EHV $= x$:

$$x^2 \equiv x \pmod{1000}$$

Kuna $1000 = 2^3 \cdot 5^3$, siis peame lahendama kongruentside süsteemi

$$\begin{cases} x^2 \equiv x \pmod{8} \\ x^2 \equiv x \pmod{125} \end{cases}$$

$$\begin{cases} x^2 - x \equiv 0 \pmod{8} \\ x^2 - x \equiv 0 \pmod{125} \end{cases}$$

$$\begin{cases} x(x-1) \equiv 0 \pmod{8} \\ x(x-1) \equiv 0 \pmod{125} \end{cases}$$

Mõlema kongruentsi lahendid on ainult 0 ja 1 vastavates jäägiklassides. Kui oletada, et on veel mõni lahend, siis peavad x ja $x - 1$ olema mõlemad nullitegurid vastavas jäägiklassiringis. Samas aga on ringis $\mathbb{Z}_8$ nullitegurid ainult 2-ga jaguvad (ja ringid $\mathbb{Z}_{125}$ ainult 5-ga jaguvad) arvud, mistõttu ei saa need nullitegurid olla järjestikused arvud (sel juhul saaksime, et $2 \mid 1$ või $5 \mid 1$ ehk vastuolu).

Saame Hiina jäägiteoreemi abil lahedada 4 kongruentside süsteemi.

$$\begin{cases} a \equiv 0 \pmod 8 \\ a \equiv 0 \pmod{125} \end{cases} \Rightarrow a \equiv 0 \pmod{1000}$$

$$\begin{cases} a \equiv 1 \pmod 8 \\ a \equiv 1 \pmod{125} \end{cases} \Rightarrow a \equiv 1 \pmod{1000}$$

$$\begin{cases} a \equiv 0 \pmod 8 \\ a \equiv 1 \pmod{125} \end{cases} \Rightarrow a \equiv 376 \pmod{1000}$$

$$\begin{cases} a \equiv 1 \pmod 8 \\ a \equiv 0 \pmod{125} \end{cases} \Rightarrow a \equiv 625 \pmod{1000}$$

Seega EHV $= 000, 001, 376, 625$. Neist $000, 001$ saame välistada, kuna sel juhul $0 = \mathrm{E} = \mathrm{H}$.

Kuna igale tähele vastab üks number, siis $10000000 \leq \overline{1\mathrm{KSTREHV}} \leq 19999999$, millest saame, et $3163 \leq \mathrm{LEHV} = \sqrt{\overline{1\mathrm{KSTREHV}}} \leq 4472$ ehk $L = 3, 4$.

Niisiis jääb üle kontrollida kokku 4 varianti:

- LEHV $= 3376$ – ei sobi, kuna sel juhul $3 = \mathrm{L} = \mathrm{E}$.
- LEHV $= 4376$ – siis LEHV$\times$LEHV $= 4376 \cdot 4376 = 19149376 = 1\mathrm{KSTREHV}$, mis ei sobi, kuna sel juhul $4 = \mathrm{L} = \mathrm{T}$.
- LEHV $= 3625$ – siis LEHV$\times$LEHV $= 3625 \cdot 3625 = 13140625 = 1\mathrm{KSTREHV}$, mis ei sobi, kuna sel juhul $3 = \mathrm{L} = \mathrm{K}$.
- LEHV $= 4625$ – siis LEHV$\times$LEHV $= 4625 \cdot 4625 = 21390625 = 1\mathrm{KSTREHV}$, mis ei sobi, kuna siin $2 = 1$.

Järelikult sellel mõistatusel pole lahendeid.

7 Luhaäär ja salapärane kaasautor

Paneme kõigepealt tähele, et juhul $x \equiv 0 \pmod p$ ei ole kongruents rahuldatud. Näitame et kongruents ei ole rahuldatud ka kui $x \equiv 1 \pmod p$:

$$\begin{aligned} &(p-2)x^{p-3} + (p-3)x^{p-4} + \ldots + 3x^2 + 2x + 1 \\ &\quad \equiv (p-2)1^{p-3} + (p-3)1^{p-4} + \ldots + 3 \cdot 1^2 + 2 \cdot 1 + 1 \\ &\quad \equiv (p-2) + (p-3) + \ldots + 3 + 2 + 1 \\ &\quad \equiv 1 + ((p-2)+2) + ((p-3)+3) + \ldots \\ &\quad \equiv 1 + p + p + \cdots \equiv 1 \not\equiv 0 \pmod p \end{aligned}$$

Oletame nüüd et $x \not\equiv 1 \pmod{p}$ ja $x \not\equiv 0 \pmod{p}$, siis:

$$(p-2)x^{p-3} + (p-3)x^{p-4} + \ldots + 3x^2 + 2x + 1 \equiv 0 \pmod{p}.$$
$$(x^{p-2} + x^{p-3} \ldots x + 1)' \equiv 0 \pmod{p}$$
$$\left(\frac{x^{p-1}-1}{x-1}\right)' \equiv 0 \pmod{p}.$$

Kasutame jagatise tuletise valemit ja saame:

$$\frac{(p-1)(x^{p-2})(x-1) - (x^{p-1}-1)}{(x-1)^2} \equiv \frac{-1(x^{p-2})(x-1) - (x^{p-1}-1)}{(x-1)^2} \equiv 0 \pmod{p}.$$

Kuna $x \not\equiv 0$ saame Fermat väikest teoreemi kasutades, et $x^{p-1} \equiv 1 \pmod{p}$ ja seega

$$\frac{-(x^{p-2})(x-1) - (x^{p-1}-1)}{(x-1)^2} \equiv \frac{-x^{p-2}}{x-1} \equiv 0 \pmod{p}$$

Kongruentsi kehtimiseks, peab $x^{p-2} \equiv 0 \pmod{p}$. See on võimalik ainult juhul kui $x \equiv 0 \pmod{p}$, kuid me eelnevalt oletasime, et $x \not\equiv 0 \pmod{p}$. Seega sellel kongruentsil lahendid puuduvad.

8 Lahenduse autor on toimetusele teada

$$x^3 \equiv x \pmod{p^k}$$
$$x^3 - x \equiv 0 \pmod{p^k}$$
$$x(x^2-1) \equiv 0 \pmod{p^k}$$
$$x(x-1)(x+1) \equiv 0 \pmod{p^k}$$

Seega selle võrrandi lahendid on kindlasti 0, 1 ja -1. Kui oletada, et leidub mõni lahend $x \neq -1, 0, 1$, siis vähemalt kaks teguritest x, $x-1$ ja $x+1$ peavad olema nullitegurid. Ringis $\mathbb{Z}_{p^k}$ on nullitegurid parajasti need mis jaguvad p-ga.

Kui $p \geq 3$, siis järjestikustest arvudest x, $x-1$ ja $x+1$ saab arvuga p jaguda ülimalt üks, seega sellise mooduli järgi rohkem lahendeid ei ole.

Kui $p = 2$, siis on võimalik, et $x-1$ ja $x+1$ on nullitegurid ehk $2 \mid x-1$ ja $2 \mid x+1$. Kuna mõlemad korraga ei saa jaguda 2^n-ga, kus $n \geq 2$, siis üks tegur peab olema 2^{k-1}. Sellest saame lahendid $x - 1 = 2^{k-1}$ ja $x + 1 = 2^{k-1}$. Seega sobivad lahenditeks veel $x = 2^{k-1} + 1$ ja $x = 2^{k-1} - 1$.