Arvuteooria

Näidislahendused

Praktikum 9

1 Lahenduse autorid on toimetusele teada

Kuna arvu 455 esitus algtegurite korrutisena on $455 = 5 \cdot 7 \cdot 13$, siis piisab näidata, et $5 \mid a^{15} - a^3$, $7 \mid a^{15} - a^3$ ja $13 \mid a^{15} - a^3$:

- Kui $5 \mid a$, siis ka $5 \mid a^{15}$ ja $5 \mid a^3$, millest järeldub, et $5 \mid a^{13} - a^3$.

  Kui $5 \nmid a$, siis Fermat' väikese teoreemi põhjal $a^4 \equiv 1 \pmod 5$. Seega $a^3 \equiv 1^3 \cdot a^3 \equiv (a^4)^3 a^3 \equiv a^{12} a^3 \equiv a^{15} \pmod 5$. Niisiis kuna $a^3 \equiv a^{15} \pmod 5$, siis kongruentsuse definitsiooni kohaselt $5 \mid a^{15} - a^3$.

- Kui $7 \mid a$, siis ka $7 \mid a^{15}$ ja $7 \mid a^3$, millest järeldub, et $7 \mid a^{13} - a^3$.

  Kui $7 \nmid a$, siis Fermat' väikese teoreemi põhjal $a^6 \equiv 1 \pmod 7$. Seega $a^3 \equiv 1^2 \cdot a^3 \equiv (a^6)^2 a^3 \equiv a^{12} a^3 \equiv a^{15} \pmod 7$. Niisiis kuna $a^3 \equiv a^{15} \pmod 7$, siis kongruentsuse definitsiooni kohaselt $7 \mid a^{15} - a^3$.

- Kui $13 \mid a$, siis ka $13 \mid a^{15}$ ja $13 \mid a^3$, millest järeldub, et $13 \mid a^{13} - a^3$.

  Kui $13 \nmid a$, siis Fermat' väikese teoreemi põhjal $a^1 2 \equiv 1 \pmod{13}$. Seega $a^3 \equiv 1 \cdot a^3 \equiv a^{12} a^3 \equiv a^{15} \pmod{13}$. Niisiis kuna $a^3 \equiv a^{15} \pmod{13}$, siis kongruentsuse definitsiooni kohaselt $13 \mid a^{15} - a^3$.

2 Laura Karu ja Susan Männik

Kuna arvude a ja b suurim ühistegur on 6, siis need arvud avalduvad kujul $a = 6k$ ja $b = 6l$, kus $(k, l) = 1$. Kui $m := (k, l) > 1$, siis oleks $(a, b) = 6 \cdot m > 6$, kuid see oleks vastuolus eeldusega. Järgmisena arvutame suurima ühisteguri.

$$(a^2, b^3) = ((6k)^2, (6l)^3) = (36k^2, 216l^3) = 36 \cdot (k^2, 6l^3)$$

Nüüd on neli võimalust.

1. Kui $2 \nmid k$ ja $3 \nmid k$ ehk $(k^2, 6l^3) = 1$, siis $(a^2, b^3) = 36$.
2. Kui $2 \mid k$ ja $3 \nmid k$ ehk $(k^2, 6l^3) = 2$, siis $(a^2, b^3) = 72$.
3. Kui $2 \nmid k$ ja $3 \mid k$ ehk $(k^2, 6l^3) = 3$, siis $(a^2, b^3) = 108$.
4. Kui $6 \mid k$ ehk $(k^2, 6l^3) = 6$, siis $(a^2, b^3) = 216$.

3 Erki Külaots ja Marcus Lõo

Kirjutame ülesandes küsitu välja avaldisena.

$$18p + 30q + 48r = 1002$$

, kus $p, q, r \in \mathbb{P}$. Lihtsustame.

$$\begin{aligned} 18p + 30q + 48r &= 1002 \\ 3p + 5q + 8r &= 167 \\ 3(p + r) + 5(q + r) &= 167 \end{aligned}$$

Saime diofantilise võrrandi kujul $3x + 5y = 167$, kus $x = p + r$ ja $y = q + r$. Pakkudes leiame, et $x_0 = -1$ ja $y_0 = 34$ ning kuna $(3, 5) = 1$, siis saame, et

$$\begin{cases} x = -1 + 5k \\ y = 34 - 3k \end{cases}, \text{ kus } k \in \mathbb{Z}$$

Kuna algarvud on positiivsed, siis kirjutame välja kõik naturaalarvulised lahendid.

$(p+r, q+r) \in \{(4, 31), (9, 28), (14, 25), (19, 22), (24, 19), (29, 16), (34, 13), (39, 10), (44, 7), (49, 4), (54, 1)\}$

Kuna $3p + 5q + 8r = 167$, 167 on paaritu, $8r$ on paaris ja 3 ja 5 on paaritud, siis kas p või q on paaris. Ja ainuke paarisarvuline algarv on 2. Järelikult kui analüüsida neid lahendeid, siis peaks alustama sellest, et eeldada, kas $p = 2$ või

$q = 2$. Analüüsime lahendeid.

$p+r$	$q+r$	p	q	r	Märkus
4	31	2	29	2	$2, 29 \in \mathbb{P}$
		-25	2	29	$-25 \notin \mathbb{P}$
9	28	2	21	7	$21 \notin \mathbb{P}$
		-17	2	26	$26 \notin \mathbb{P}$
14	25	2	13	12	$12 \notin \mathbb{P}$
		-9	2	23	$-9 \notin \mathbb{P}$
19	22	2	5	17	$2, 5, 17 \in \mathbb{P}$
		-1	2	20	$20 \notin \mathbb{P}$
24	19	2	-3	22	$22 \notin \mathbb{P}$
		7	2	17	$2, 7, 17 \in \mathbb{P}$
29	16	2	-11	27	$27 \notin \mathbb{P}$
		15	2	14	$14 \notin \mathbb{P}$
34	13	2	-19	32	$32 \notin \mathbb{P}$
		23	2	11	$2, 11, 23 \in \mathbb{P}$
39	10	2	-27	37	$-27 \notin \mathbb{P}$
		31	2	8	$8 \notin \mathbb{P}$
44	7	2	-35	42	$42 \notin \mathbb{P}$
		39	2	5	$39 \notin \mathbb{P}$
49	4	2	-43	47	$-43 \notin \mathbb{P}$
		47	2	2	$2, 47 \in \mathbb{P}$
54	1	2	-51	52	$52 \notin \mathbb{P}$
		55	2	-1	$-1 \notin \mathbb{P}$

Seega saame lahendid

$$(p, q, r) \in \{(2, 29, 2), (2, 5, 17), (7, 2, 17), (23, 2, 11), (47, 2, 2)\}$$

4 Maret Sõmer ja Mikael Raihhelgauz

Olgu p algarv, mis esitub kujul $p = a^3 - b^3$, kus a ja b on mingid naturaalarvud. Paneme tähele, et $a^3 - b^3 = (a - b)(a^2 + ab + b^2)$. Selge, et $a^2 + ab + b^2 \geq 3$. Järelikult $a - b = 1$, vastasel juhul oleks p kordarv. Niisiis, $b = a + 1$ ja

$$\begin{aligned} p &= a^2 + a(a+1) + (a+1)^2 = a^2 + a^2 + a + a^2 + 2a + 1 \\ &= 3a^2 + 3a + 1 = 3a(a+1) + 1. \end{aligned}$$

ja sobivad kõik algarvud, mis on sellisel kujul

5 Lahenduse autorid on toimetusele teada

Ilmselt $x, y, z \neq 0$.

$$\frac{x}{y} + \frac{y}{z} + \frac{z}{x} = n$$
$$x^2z + y^2x + z^2y = nxyz$$

Kuna $z^2y = nxyz - x^2z + y^2x = x(nyz + xz + y^2)$, siis $x \mid z^2y$.

Teiselt poolt kuna $(y, x) = 1$ ja $(z, x) = 1$, siis ka $(z^2y, x) = 1$ (Kui oletada vastuväiteliselt, et $k := (z^2y, x) > 1$, siis k-l algtegur p korral $p \mid z^2y$ ja $p \mid x$, mistõttu $p \mid z$ või $p \mid y$ ning samas ka $p \mid x$, mis on vastuolus sellega, et $(z, x) = (y, x) = 1$.

Kuna $x \mid x$ ja $x \mid z^2y$ ning $(z^2y, x) = 1$, siis suurima ühisteguri definitsiooni kohaselt $x \mid 1$, mis tähendab, et $x = \pm 1$.

Sümmeetria põhjal saame analoogiliselt ka, et $y = \pm 1$ ja $z = \pm 1$.

Niisiis $(x, y, z) = (\pm 1, \pm 1, \pm 1)$, seega kõik liidetavad $\frac{x}{y}$, $\frac{y}{z}$ ja $\frac{z}{x}$ on samuti ± 1. Järelikult selleks, et summa $\frac{x}{y} + \frac{y}{z} + \frac{z}{x} = n$ oleks naturaalarv, peab vähemalt kaks liidetavat olema võrdsed 1-ga ehk vastavas murrus on lugeja ja nimetaja võrdsed. Kuna igas kahes murrus on vähemalt üks ühine tundmatu, siis peab $x = y = z$. Ehk võimalikud variandid on $(x, y, z) = (-1, -1, -1)$ ja $(x, y, z) = (1, 1, 1)$, Mõlemal juhul $n = 3$.

Niisiis on kokkuvõttes on võrrand lahenduv, parajasti siis, kui $n = 3$ ning sel juhul on lahenditeks $(x, y, z) = (1, 1, 1)$ ja $(x, y, z) = (-1, -1, -1)$.

6 Markus Rene Pae ja Erki Kuus

Olgu meil uurimise all seitsmekohalised arvud $\underline{abcdefg}$. Arvu ristsumma on 59 ehk $a + b + c + d + e + f + g = 59$. Ühtlasi peab see arv jaguma 11-ga ehk paaritutel kohtadel olevate numbrite summa ja paarisarvulistel kohtadel olevate numbrite summa vahe peab jaguma 11-ga:

$$(a + c + e + g) - (b + d + f) = 11k, k \in \mathbb{Z}.$$

Kuna arvu ristsumma on 59, siis summa $a + c + e + g$ minimaalne väärtus saab olla $59 - 3 \cdot 9 = 32$ ning maksimaalne väärtus on 36 (eeldusel, et kõik neli numbrit on 9-ga võrdsed). Analoogiliselt $b+d+f$ minimaalne väärtus saab olla $59 - 4 \cdot 9 = 23$ ning maksimaalne väärtus on 27. Uurime viit võimalikku juhtu, mis sellest tuleneb:

- Kui $a+c+e+g = 36$ ja $b+d+f = 23$, siis $(a+c+e+g)-(b+d+f) = 13$, mis ei jagu 11-ga. See tähendab vastuolu ülesande püstitusega.
- Kui $a+c+e+g = 35$ ja $b+d+f = 24$, siis $(a+c+e+g)-(b+d+f) = 11$, jagub 11-ga.

- Kui $a+c+e+g = 34$ ja $b+d+f = 25$, siis $(a+c+e+g)-(b+d+f) = 9$, mis ei jagu 11-ga. See tähendab vastuolu ülesande püstitusega.
- Kui $a+c+e+g = 33$ ja $b+d+f = 26$, siis $(a+c+e+g)-(b+d+f) = 7$, mis ei jagu 11-ga. See tähendab vastuolu ülesande püstitusega.
- Kui $a+c+e+g = 32$ ja $b+d+f = 27$, siis $(a+c+e+g)-(b+d+f) = 5$, mis ei jagu 11-ga. See tähendab vastuolu ülesande püstitusega.

Seega tasub otsida arve, mille puhul $a+c+e+g = 35$ ja $b+d+f = 24$. Esimesest tingimusest järeldub, et a, c, e, f seas on 3 üheksat ning 1 kaheksa. Teisest tingimusest saab eraldada kolm juhtu:
a) b, d, f seas on 3 kaheksat;
b) b, d, f seas on 1 üheksa, 1 kaheksa ning 1 seitse;
c) b, d, f seas on 2 üheksat ning 1 kuus.

Kui a, c, e, f seas on 3 üheksat ning 1 kaheksa, siis eksisteerib neli erinevat kombinatsiooni, mis seda rahuldab.
a) Kui b, d, f seas on 3 kaheksat, siis leidub vaid üks kombinatsioon, kuidas neid kaheksaid jaotada (st $b = 8, d = 8, f = 8$).
b) Kui b, d, f seas on 1 üheksa, 1 kaheksa ning 1 seitse, siis leidub 3! (ehk 6) erinevat kombinatsiooni, kuidas neid numbreid jaotada.
c) Kui b, d, f seas on 2 üheksat ning 1 kuus, siis leidub kolm erinevat kombinatsiooni numbrite jaotamiseks: 1) $b = d = 9$ ja $f = 6$; 2) $b = f = 9$ ja $d = 6$; 3) $d = f = 9$ ja $b = 6$.
Seega selliseid seitsmekohalisi arve, mis jaguvad 11-ga ja mille ristsumma on 59, leidub $4 \cdot (1+6+3) = 40$ tükki.

7 Johanna Maria Kirss ja Rainer Bõkov

Uurime ülesannet mooduli 4 järgi. Täisarvu ruudu jagamisel arvuga 4 tekkiv jääk saab olla vaid 0 või 1. Tabeli kujul:

a	a^2	a^3
0	0	0
1	1	1
2	0	0
3	1	3

Kui $x \equiv 3 \pmod 4$, siis $x^3 - x^2 + 8 \equiv 2 \pmod 4$, kuna $3 - 1 + 8 = 10 \equiv 2 \pmod 4$. Seega $y^2 \equiv 2$, mis ei sobi.
Kui x on paarisarv, s.t $x = 2a$, siis meil on $y^2 = x^3 - x^2 + 8 = 8a^3 - 4a^3 + 8$, siit järeldub, et $2 \mid y^2$, kust omakorda $2 \mid y$. Olgu $y = 2b$, siis $8a^3 - 4a^2 + 8 = 4b^2$ ja pärast lihtsustamist

$$2a^3 - a^2 + 2 = b^2.$$

Kui a on paarisarv, siis tabeli põhjal $b^2 \equiv 2 \pmod 4$, kui a on paaritu, siis tabelit kasutades $b^2 \equiv 3 \pmod 4$. Mõlemad korrad on võimatud.
Viimaseks juhuks on $x \equiv 1 \pmod 4$. Viime algse avaldise kujule

$$(x+2)(x^2-2x+4) = x^2+y^2. \tag{1}$$

Kuna $x+2 \equiv 3 \pmod 4$, siis peab leiduma algarv $p \equiv 3 \pmod 4$ (algarvud kujul $4k+3$, mida on teoreemi 2.4 põhjal lõpmata palju) nii, et $p \mid x+2$. Siis võrrandist (1) saame $p \mid x^2+y^2$ ehk teisisõnu $x^2 \equiv -y^2 \pmod p$. Kui kehtiks, et $p \mid x$, siis sellest et $p \mid x+2$ saaksime, et $x \mid 2$, mis on vastuolu. Seega $p \nmid x$ ja järelikult ka $p \nmid y$. Lisaks on meil

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

Fermat' väikese teoreemi kohaselt $x^{p-1} \equiv y^{p-1} \equiv 1 \pmod p$. Seega võrrandist (2) saame $(-1)^{\frac{p-1}{2}} \equiv 1 \pmod p$. Kuna $p \equiv 3 \pmod 4$, siis $\frac{p-1}{2}$ on paaritu arv ja seega $(-1)^{\frac{p-1}{2}} = -1 \pmod p$. Kuna $p \geq 3$, siis $-1 \not\equiv 1 \pmod p$, mis on vastuolu sellega, et $(-1)^{\frac{p-1}{2}} \equiv 1 \pmod p$.
Seega sellel võrrandil ei ole ühtegi täisarvulist lahendit.

8 Aljona Kritševskaja

Leiame, mitu pööratavat elementi on ringides $\mathbb{Z}_{2024}$ ja $\mathbb{Z}_{44} \times \mathbb{Z}_{46}$.

Teame, et

$$\varphi(n) = |U(\mathbb{Z}_n)|.$$

Seega on vaja leida $\varphi(2024)$ ja $\varphi(44) \cdot \varphi(46)$.

$$\varphi(2024) = \varphi(2^3 \cdot 11 \cdot 23) = 4 \cdot 10 \cdot 22 = 880$$
$$\varphi(44) \cdot \varphi(46) = \varphi(2^2 \cdot 11) \cdot \varphi(2 \cdot 23) = 2 \cdot 10 \cdot 1 \cdot 22 = 440$$

Nendel ringidel on erinev arv pööratavaid elemente, seega $\mathbb{Z}_{2024}$ ja $\mathbb{Z}_{44} \times \mathbb{Z}_{46}$ ei ole isomorfsed.

9 Lahenduse autorid on toimetusele teada

Kuna $\varphi(1) = 1$, siis $n > 1$. Seega olgu $n = p_1^{k_1} \dots p_s^{k_s}$ standardkuju

$$24 = \varphi(n) = p_1^{k_1-1} \dots (p_1-1)\dot{(}p_s-1)$$

Seega iga arvu n algteguri p_i korral $p_i - 1 \mid 24$.

Kuna 24 positiivsed tegurid on 1, 2, 3, 4, 6, 8, 12, 24, siis n algteguriteks saavad olla 2, 3, 5, 7 ja 13.

Niisiis $n = 2^{k_1} \cdot 3^{k_2} \cdot 5^{k_3} \cdot 7^{k_4} \cdot 13^{k_5}$, kus $k_i \in \mathbb{N} \cup \{0\}$.

Kui arvu n algtegurite hulgas on

Paneme tähele, et kui $k_1 \geq 1$, siis vastavalt $2^{k_1-1} \mid 24$, järelikult $k_1 \leq 4$ (kuna $2^3 \mid 24$, aga $2^4 \nmid 24$). Analoogiliselt saame $k_2 \leq 2$, $k_3 \leq 1$, $k_4 \leq 1$ ja $k_5 \leq 1$.

Vaatame eri juhte, millised on n algtegurite astmed (kõrgem kui 1, saab olla ainult 2 ja 3 aste eelneva põhjal):

- Kui n kõigi algtegururite aste on üks ehk $n = p_1 p_2 \dots p_s$ ja $\phi(n) = (p_1 - 1)(p_2 - 1)\dots(p_s - 1)$, seejuures ($p_i \in \{2, 3, 5, 7, 13\}$ ehk $p_i - 1 \in \{1, 2, 4, 6, 12)$. Seega on võimalused 24 esitamiseks nende arvude korrutisena on:
  - $24 = 12 \cdot 2 = (13 - 1)(3 - 1) \Rightarrow n = 13 \cdot 3 = 39$
  - $24 = 12 \cdot 2 \cdot 1 = (13 - 1)(3 - 1)(2 - 1) \Rightarrow n = 13 \cdot 3 \cdot 2 = 78$
  - $24 = 4 \cdot 6 = (5 - 1)(7 - 1) \Rightarrow n = 5 \cdot 7 = 35$
  - $24 = 4 \cdot 6 \cdot 1 = (5 - 1)(7 - 1)(2 - 1) \Rightarrow n = 5 \cdot 7 \cdot 2 = 70$
- Kui ainult algteguri 2 aste on vähemalt 2, siis $n = 2^k p_1 p_2 \dots p_s$, kus p_i on paarikaupa erinevad paaritud algarvud ja $k \geq 2$. Seega $24 = \varphi(n) = \varphi(2^k p_1 p_2 \dots p_s) = 2^{k-1}(2 - 1)(p_1 - 1)\dots(p_s - 1)$. Seejuures $p_i - 1 \in \{2, 4, 6, 12\}$, seega 24 avaldamiseks vastaval kujul on võimalused:
  - $24 = 2 \cdot 12 = 2^{2-1} \cdot (2 - 1)(13 - 1) \Rightarrow n = 2^2 \cdot 13 = 52$
  - $24 = 2 \cdot 2 \cdot 6 = 2^{2-1}(2 - 1)(3 - 1)(7 - 1) \Rightarrow n = 2^2 \cdot 3 \cdot 7 = 84$
  - $24 = 2^2 \cdot 6 = 2^{3-1}(2 - 1)(7 - 1) \Rightarrow n = 2^3 \cdot 7 = 56$
- Kui ainult algteguri 3 aste on vähemalt 2, siis $n = 3^k p_1 p_2 \dots p_s$, kus p_i on paarikaupa erinevad 3-st erinevad algarvud ja $k \geq 2$. Seega $24 = \varphi(n) = \varphi(3^k p_1 p_2 \dots p_s) = 3^{k-1}(3-1)(p_1-1)\dots(p_s-1) = 3^{k-1} \cdot 2 \cdot (p_1 - 1)\dots(p_s - 1)$. Seejuures $p_i - 1 \in \{1, 4, 6, 12\}$, seega 24 avaldamiseks vastaval kujul on võimalused:
  - $24 = 3 \cdot 2 \cdot 4 = 3^{2-1} \cdot 2 \cdot (5 - 1) \Rightarrow n = 3^2 \cdot 5 = 45$
  - $24 = 3 \cdot 2 \cdot 4 \cdot 1 = 3^{2-1} \cdot 2 \cdot (5 - 1)(2 - 1) \Rightarrow n = 3^2 \cdot 5 \cdot 2 = 90$
- Kui n mõlema algteguri 2 ja 3 astmed on vähemalt kaks, siis $n = 2^k 3^l p_1 \dots p_s$, kus p_i on paarikaupa erinevad 3-st suuremad algarvud ja $k, l \geq 2$. Seega $24 = \varphi(n) = \varphi(2^k 3^l p_1 p_2 \dots p_s) = 2^{k-1}3^{l-1}(3 - 1)(2 - 1)(p_1 - 1)\dots(p_s - 1) = 2^{k-1}3^{l-1} \cdot 2 \cdot (p_1 - 1)\dots(p_s - 1)$. Seejuures $p_i - 1 \in \{4, 6, 12\}$.

  Kuna $k, l \geq 2$, siis $2^{k-1}3^{l-1} \cdot 2 \geq 2 \cdot 3 \cdot 2 = 12$, millest järeldub et $(p_1 - 1)\dots(p_s - 1) \leq 2$, misõttu $s = 0$, kuna $p_i \geq 5$. Niisiis $24 = 2^{k-1}3^{l-1} \cdot 2$, järelikult $k = 3$ ja $l = 2$ ehk $n = 2^3 \cdot 3^2 = 72$

Niisiis võimalikud n väärtused on $n = 35, 39, 45, 52, 56, 70, 72, 78, 84, 90$.

10 Lahenduse autorid on toimetusele teada

Olgu $p = 2^n - 1$ algarv.
Vaatame arvu $x = 2^{n-1}p$ jagajaid:

$$1, 2, \ldots, 2^{n-1}, p, 2p, \ldots, 2^{n-1}p$$

Järelikult saame, et:

$$\begin{aligned}\sigma(x) &= 1 + 2 + \ldots + 2^{n-1} + p + 2p + \ldots + 2^{n-1}p \\ &= (1 + 2 + \ldots + 2^{n-1})(1 + p) = (2^n - 1)2^n = 2x\end{aligned}$$

Olemegi tõestanud, et x ehk arvud kujul $(2^{n-1})(2^n - 1)$, kus $n \in \mathbb{N}$ ja $2^n - 1$ on algarv, on täiuslikud.

11 Lahenduse autorid on toimetusele teada

- $7x^2 \equiv 8 \pmod{40}$

  Kuna ringis $\mathbb{Z}_{40}$ on $7^{-1} = 23$, siis see kongruents on samaväärne kongruentsiga $x^2 \equiv 23 \cdot 8 \equiv 184 \equiv 24 \pmod{40}$. Viimane kongruents on aga samaväärne süsteemiga:

  $$\begin{cases} x^2 \equiv 24 \pmod 8 \\ x^2 \equiv 24 \pmod 5 \end{cases} <=> \begin{cases} x^2 \equiv 0 \pmod 8 \\ x^2 \equiv 4 \pmod 5 \end{cases}$$

  Kongruentsi $x^2 \equiv 0 \pmod 8$ lahendiks on $x \equiv 0, 4 \pmod 8$ ehk $x \equiv 0 \pmod 4$.

  Kongruentsi $x^2 \equiv 4 \pmod 5$ lahendiks on $x \equiv 2, 3 \pmod 5$.

  Saame kaks kongruentside süsteemi:

  $$\begin{cases} x \equiv 0 \pmod 4 \\ x \equiv 2 \pmod 5 \end{cases}, \quad \begin{cases} x \equiv 0 \pmod 4 \\ x \equiv 3 \pmod 5 \end{cases}$$

  Nende lahendideks on, et $x \equiv 8, 12 \pmod{20}$

- $x^3 \equiv 7 \pmod{11}$

  Vaatame kõik võimalikud jäägiklassid mooduli 11 järgi läbi

x	x^3
0	0
1	1
2	8
3	5
4	9
5	4
6	7
7	2
8	6
9	3
10	10

Näeme, et ainsaks lahendiks on $x \equiv 6 \pmod{11}$

Niisiis $x \equiv 16,4 \pmod{20}$ ja $x \equiv 6 \pmod{11}$ ehk saame kaks kongruentside süsteemi:

$$\begin{cases} x \equiv 8 \pmod{20} \\ x \equiv 6 \pmod{11} \end{cases}, \quad \begin{cases} x \equiv 12 \pmod{20} \\ x \equiv 6 \pmod{11} \end{cases}$$

Hiina jäägiteoreemi kohaselt on neil kõigil ühene lahend mooduli $20 \cdot 11 = 220$ järgi.

Olgu $m_1 = 11$, $m_2 = 20$. Siis ringis $\mathbb{Z}_{20}$ $k_1 = m_1^{-1} = 11^{-1} = 11$ ja ringis $\mathbb{Z}_{11}$ $k_2 = m_2^{-1} = 20^{-1} = 9^{-1} = 5$.

Seega nende süsteemide lahendid on

1. $x_1 \equiv 8k_1m_1 + 6k_2m_2 \equiv 8 \cdot 11 \cdot 11 + 6 \cdot 5 \cdot 20 \equiv 1568 \equiv 28 \pmod{220}$
2. $x_2 \equiv 12k_1m_1 + 6k_2m_2 \equiv 12 \cdot 11 \cdot 11 + 6 \cdot 5 \cdot 20 \equiv 2052 \equiv 72 \pmod{220}$

Seega selle kongruentside süsteemi lahenditeks on, et $x \equiv 28, 72 \pmod{220}$

12 Johanna Maria Kirss ja Rainer Bõkov

On antud polünoom

$$f(x) = 4x^4 + 2x^2 + x + 20, \quad f'(x) = 16x^3 + 4x + 1.$$

Kõigepealt märkame, et $459 = 3^3 \cdot 17$. See tähendab, et saame kõigepealt leida lahendid moodulite 3^3 ja 17 järgi eraldi ja siis neid ühildada. Alustame moodulist $3^3 = 27$.

	$f(x)$	4	0	2	1	20	$f'(x)$	16	0	4	1	
(mod 3)	0	1	0	2	1	2						
	1	1	1	0	1	0	1	1	1	2	0	
	2	1	2	0	1	1						
(mod 9)	1	4	4	-3	-2	0						$0y + \frac{0}{3} \equiv 0 \pmod{3}$
(mod 27)	1	4	4	6	7	0						$0y + \frac{0}{9} \equiv 0 (\text{mod } 3)$
	4	4	16	12	-5	0						$0y + \frac{0}{9} \equiv 0 \pmod{3}$
	7	4	1	9	10	9						$0y + \frac{9}{9} \equiv 0 \pmod{3}$ Vastuolu!

Mooduli 27 järgi sobivad järelikult lahenditeks kõik arvud, mis annavad üheksaga jagades jäägi üks või neli. Seega saame tulemuse kirja panna kujul $x \equiv 1, 4 \pmod 9$

Mooduli 17 järgi kasutame proovimismeetodit.

	4	0	2	1	20
0	4	0	2	1	3
1	4	4	6	7	-7
2	4	8	1	3	-8
3	4	-5	4	-4	8
4	4	-1	-2	-7	-8
5	4	3	0	1	8
6	4	7	-7	-7	-5
7	4	-6	-6	-7	5
8	4	-2	3	8	-1
-8	4	2	3	-6	0
-8	4	4	5	5	
-7	4	8	-2	8	
-6	4	-5	-1	0	
-6	4	5	3		
-5	4	-8	5		
-4	4	-4	-2		
-3	4	0	-1		
-2	4	4	8		
-1	4	8	8		

Saime, et siin on lahenditeks 9 ja 11 mooduli 17 järgi.

Otsime nüüd välja kõik sobivad lahendid mooduli 459 järgi. Selleks loome süsteemid

$$\begin{cases} x \equiv a \pmod 9 \\ x \equiv b \pmod{17}, \end{cases}$$

kus $a \in \{1, 4\}$ ning $b \in \{9, 11\}$. Lahendades selle süsteemi Hiina jäägiteoreemiga, saame süsteemi ja seega ka ülesande lahenditeks: $28, 94, 130, 145$.