Arvuteooria

Kevad 2020

16. praktikumi näidislahendused

1. ülesanne (Erki Külaots ja Marcus Lõo)

Tõestame seda induktsiooni abil.

Alus: $n = 1$. [1,2] = 2 ja [2,2] = 2. Seega [1,2] = [2,2].

Samm: Eeldame, et kehtib $[1,2,3,\ldots,2n] = [n+1,n+2,n+3,\ldots,2n]$.

Näitame, et siis ka $[1,2,3,\ldots,2n,2n+1,2(n+1)] = [n+2,n+3,n+4,\ldots,2n,2n+1,2(n+1)]$

Kuna $[[a,b],c] = [a,[b,c]]$, siis

$$[1,2,3,\ldots,2n,2n+1,2(n+1)] = [n+1,n+2,n+3,\ldots,2n,2n+1,2(n+1)]$$

Teame, et $[n+1,2(n+1)] = 2(n+1)$, siis

$$[n+1,n+2,n+3,\ldots,2n,2n+1,2(n+1)] = [n+2,n+3,\ldots,2n,2n+1,[n+1,2(n+1)]] =$$
$$= [n+2,n+3,\ldots,2n,2n+1,2(n+1)]$$

Mida oligi vaja tõestada.

2. ülesanne (lahenduse autorid on toimetusele teada)

Tõestame väite induktsiooniga:

Baas: $n = 1$, siis kehtib $2^1 \mid (1+1)$ ehk $2 \mid 2$.

Samm: Eeldame, et $2^k \mid (k+1)(k+2)\ldots(k+k)$ ning näitame, et siis ka $2^{k+1} \mid ((k+1)+1)((k+1)+2)\ldots((k+1)+(k+1))$.

Kehtigu $2^k \mid (k+1)(k+2)\ldots(k+k)$ ehk $(k+1)(k+2)\ldots(k+k) = 2^k \cdot m$, kus $m \in \mathbb{Z}$.

$$\begin{aligned}
&((k+1)+1)((k+1)+2)\ldots((k+1)+(k+1)) = \\
&= (k+2)(k+3)\ldots(k+k)(k+k+1)(k+k+2) = \\
&= (k+2)(k+3)\ldots(k+k)(k+k+1)(2k+2) = \\
&= (k+2)(k+3)\ldots(k+k)(k+k+1)2(k+1) = \\
&= (k+1)(k+2)(k+3)\ldots(k+k)(k+k+1)2 = \\
&= 2^k m(k+k+1)2 = \\
&= 2^{k+1} m(k+k+1) =
\end{aligned}$$

seega $2^{k+1} \mid ((k+1)+1)((k+1)+2)\ldots((k+1)+(k+1))$, mida oligi tarvis näidata.

3. ülesanne (Mikael Raihhelgauz ja Maret Sõmer)

$$4x + 6y + 10z = 146, \qquad \div 2 \tag{1}$$
$$2x + 3y = 73 - 5z. \tag{2}$$

Otsime lahendeid, kus $x, y, z \geq 1$. Järelikult $73 - 5z \geq 2 + 3 = 5$ ehk $5z \leq 68$ ja kuna z peab olema täisarv, siis $z \leq 13$.
Kõigepealt leiame (1) erilahendi. Märgime, et (2,3) = 1 ning

$$2 \cdot (-1) + 3 \cdot 1 = 1,$$
$$2 \cdot (-1)(73 - 5z) + 3 \cdot (73 - 5z) = 73 - 5z$$

ehk $x_0 = (-1)(73 - 5z) = 5z - 73$, $y_0 = 73 - 5z$ sobib erilahendiks. Järelikult kõik ülejäänud lahendid avalduvad kujul

$$x = 5z - 73 + 3t, \qquad y = 73 - 5z - 2t.$$

Vaatleme, milliste t väärtuste korral on x ja y positiivsed, s.t millal kehtivad võrratused $5z + 3t \geq 72$ ja $5z - 2t \leq 72$ ehk

$$\frac{73 - 5z}{3} < t < \frac{73 - 5z}{2}.$$

- $z = 1$. Siis $23 \leq t \leq 33$ – 11 lahendit.
- $z = 2$. Siis $22 \leq t \leq 31$ – 10 lahendit.
- $z = 3$. Siis $20 \leq t \leq 28$ – 9 lahendit.
- $z = 4$. Siis $18 \leq t \leq 26$ – 9 lahendit.
- $z = 5$. Siis $17 \leq t \leq 23$ – 7 lahendit.
- $z = 6$. Siis $15 \leq t \leq 21$ – 7 lahendit.
- $z = 7$. Siis $13 \leq t \leq 18$ – 6 lahendit.
- $z = 8$. Siis $12 \leq t \leq 16$ – 5 lahendit.
- $z = 9$. Siis $10 \leq t \leq 13$ – 4 lahendit.
- $z = 10$. Siis $8 \leq t \leq 11$ – 4 lahendit.
- $z = 11$. Siis $7 \leq t \leq 8$ – 2 lahendit.
- $z = 12$. Siis $5 \leq t \leq 6$ – 2 lahendit.
- $z = 13$. Siis $t = 3$ – ainult 1 lahend.

Kokku on 11+10+9+9+7+7+6+5+4+4+2+2+1=77 positiivset lahendit.

4. ülesanne (lahenduse autorid on toimetusele teada)

Kuna faktoriaal on defineeritud mittenegatiivsete täisarvude korral, siis seega $p \geq 5$.

Kui $p = 5$, siis ilmselt $5 \nmid 6^p(p-4)$ ja $5 \mid 10^{3p}$, seega $p \nmid 6^p(p-4)! + 10^{3p}$.

Olgu $p > 5$, siis $p \nmid 6, 10$, järelikult Fermat' väikese teoreemi kohaselt $6^p \equiv 6 \pmod{p}$ ja $10^p \equiv 10 \pmod{p}$. Wilsoni teoreemi põhjal $(p-1)! \equiv -1 \pmod{p}$. Selle põhjal:

$$
\begin{gathered}
p \mid 6^p(p-4)! + 10^{3p} \\
6^p(p-4)! + 10^{3p} \equiv 0 \pmod{p} \\
6 \cdot (p-4)! + (10^p)^3 \equiv 0 \pmod{p} \\
6 \cdot (p-4)! + (10)^3 \equiv 0 \pmod{p} \\
6 \cdot (p-4)! + 1000 \equiv 0 \pmod{p} \\
6 \cdot (p-4)! \equiv -1000 \pmod{p} \\
6 \cdot (p-4)!(p-3)(p-2)(p-1) \equiv -1000(p-3)(p-2)(p-1) \pmod{p} \\
6 \cdot (p-1)! \equiv -1000 \cdot -3 \cdot -2 \cdot -1 \pmod{p} \\
6 \cdot (-1) \equiv 6000 \pmod{p} \\
-6 \equiv 6000 \pmod{p} \\
6006 \equiv 0 \pmod{p} \\
p \mid 6006
\end{gathered}
$$

Kuna $6006 = 2 \cdot 3 \cdot 7 \cdot 11 \cdot 13$ ja eelneva põhjal $p \neq 2, 3$, siis $p = 7, 11, 13$

5. ülesanne (lahenduse autor on toimetusele teada)

$691488 = 2^5 \cdot 3^2 \cdot 7^4$

$$x^2 \equiv x \pmod{691488}$$
$$x^2 - x \equiv 0 \pmod{691488}$$
$$x(x-1) \equiv 0 \pmod{691488}$$
$$\begin{cases} x(x-1) \equiv 0 \pmod{2^5} \\ x(x-1) \equiv 0 \pmod{3^2} \\ x(x-1) \equiv 0 \pmod{7^4} \end{cases}$$

Paneme tähele, et iga kongruentsi lahendid sellest süsteemist on $x = 0$ ja $x = 1$ vastavas ringis. Rohkem lahendeid vastavas ringis $\mathbb{Z}_{p^k}$ ei ole. Näitame seda. Oletame vastuväiteliselt, et mooduli p^k järgi leidub veel mõni lahend võrrandile $x(x-1) = 0$ ning $x \neq 1, 0$. Siis see tähendab, et x ja $x-1$ on nullitegurid. Kuna ringi $\mathbb{Z}_{p^k}$ kõik elemendid jagunevad nulliks, pööratavateks elementideks ja nulliteguriteks (seejuures on need hulgad lõikumatud), siis x ja $x-1$ on mittepööratavad elemendid ehk $(x, p^k) \neq 1$ ja $(x-1, p^k) \neq 1$ (kuna pööratavad elemendid a on parajasti need, mille korral $(x, a) = 1$). Kuna $(x, p^k) \neq 1$ ja p^k ainus algtegur on p, siis $p \mid x$, analoogiliselt $p \mid x-1$ ning sealt siis $p \mid x-(x-1)$ ehk $p \mid 1$, mis on vastuolu.

Niisiis saame kokku saame moodustada kokku $2 \cdot 2 \cdot 2 = 8$ kongruentside süsteemi

$$\begin{cases} x \equiv 0 \pmod{2^5} \\ x \equiv 0 \pmod{3^2} \\ x \equiv 0 \pmod{7^4} \end{cases} \quad \begin{cases} x \equiv 0 \pmod{2^5} \\ x \equiv 0 \pmod{3^2} \\ x \equiv 1 \pmod{7^4} \end{cases} \quad \begin{cases} x \equiv 0 \pmod{2^5} \\ x \equiv 1 \pmod{3^2} \\ x \equiv 0 \pmod{7^4} \end{cases}$$
$$\begin{cases} x \equiv 0 \pmod{2^5} \\ x \equiv 1 \pmod{3^2} \\ x \equiv 1 \pmod{7^4} \end{cases} \quad \begin{cases} x \equiv 1 \pmod{2^5} \\ x \equiv 0 \pmod{3^2} \\ x \equiv 0 \pmod{7^4} \end{cases} \quad \begin{cases} x \equiv 1 \pmod{2^5} \\ x \equiv 0 \pmod{3^2} \\ x \equiv 1 \pmod{7^4} \end{cases}$$
$$\begin{cases} x \equiv 1 \pmod{2^5} \\ x \equiv 1 \pmod{3^2} \\ x \equiv 0 \pmod{7^4} \end{cases} \quad \begin{cases} x \equiv 1 \pmod{2^5} \\ x \equiv 1 \pmod{3^2} \\ x \equiv 1 \pmod{7^4} \end{cases}$$

Igal kongruentside süsteemil on Hiina jäägiteoreemi kohaselt ühene lahend mooduli 691488 järgi (seejuures need lahendid ei kattu). Seega kokku on ringi $\mathbb{Z}_{691488}$ 8 elementi, mille korral $x^2 \equiv x \pmod{691488}$.

6. ülesanne (Mikael Raihhelgauz ja Maret Sõmer)

Ülesandes on vaja tõestada, et diofantiline võrrand $x^2 + 5 = y^3$ ei ole lahenduv.

Oletan vastuväiteliselt, et võrrand $x^2 + 5 = y^3$ on lahenduv.

Kirjutan antud võrrandi kujul $x^2 + 4 = y^3 - 1$ ning tegurdan:
$x^2+4 = (y-1)(y^2+y+1)$. Uurin seda võrrandit mooduli 4 järgi. Kuna paarisarvulise $x = 2k$ korral $x^2 = 4k^2 \equiv 0 \pmod 4$ ning paarituarvulise $x = 2k+1$ korral $x^2 = 4k^2 + 4k + 1 \equiv 1 \pmod 4$, siis järelikult $x^2 \equiv 0$ või $x^2 \equiv 1 \pmod 4$ ning kuna $4 \equiv 0 \pmod 4$, siis $x^2+4 \equiv 0$ või $x^2 + 4 \equiv 1 \pmod 4$. Vaatlen y^3 mooduli 4 järgi. Kehtib täpselt üks järgmistest variantidest: $y \equiv 0$, $y \equiv 1$, $y \equiv 2$, $y \equiv 3 \equiv -1 \pmod 4$. Proovides kõik need variandid läbi, leian et $y^3 \equiv 0$, $y^3 \equiv 1$ või $y^3 \equiv -1 \equiv 3 \pmod 4$ ning vastavalt $y^3 - 1 \equiv -1 \equiv 3$, $y^3 - 1 \equiv 0$ või $y^3 - 1 \equiv 2 \pmod 4$. Kuna peab kehtima võrdus $x^2 + 4 = y^3 - 1$, siis peavad $x^2 + 4 \equiv y^3 - 1 \pmod 4$. Võimalustest, millega x^2+4 ja y^3-1 mooduli 4 järgi kongruentsed saavad olla, on neil ühine ainult 0. Seega $x^2 + 4 \equiv 0 \equiv y^3 - 1 \pmod 4$, mis muuhulgas tähendab, et $y^3 \equiv 1$ ehk $y \equiv 1 \pmod 4$.

Kirjutan nüüd algse võrrandi kujul $x^2-(y-1)(y^2+y+1) = -4$. Panen tähele, et $y^2+y+1 = = y(y+1)+1$, mis tähendab, et sõltumata y väärtusest on $y^2 + y + 1$ alati paaritu arv. Olgu p arvu $y^2 + y + 1$ suvaline algtegur p. Eelnevast järeldub, et $p \neq 2$. Vaatan nüüd kongruentsi $x^2 - (y-1)(y^2 + y + 1) \equiv -4 \pmod p$. Kuna p on defineeritud arvu $y^2 + y + 1$ tegurina, siis on eelnev kongruents samaväärne järgmisega: $x^2 \equiv -4$. Kuna on teada, et $p \nmid -4$, siis kongruentsi $x^2 \equiv -4$ (oletatud) lahenduvusest ja ruutjäägi definitsioonist saan, et -4 on ruutjääk mooduli p järgi. Legendre'i sümboli definitsioonist $\left(\frac{-4}{p}\right) = -1$. Lause 8.8 omadusest 2) ning tingimusest $p \nmid 2$ järeldub $\left(\frac{-4}{p}\right) = \left(\frac{-1 \cdot 2^2}{p}\right) = \left(\frac{-1}{p}\right) = -1$, mis omadusest 3) tähendab, et $p \equiv 1 \pmod 4$. Sellega on näidatud, et arvu y^2+y+1 iga algtegur p on mooduli 4 järgi kongruentne arvuga 1. Teades, et kui $a \equiv 1$ ja $b \equiv 1 \pmod 4$, siis ka $ab \equiv 1 \pmod 4$, saan et järelikult $y^2 + y + 1 \equiv 1 \pmod 4$.

Eelnevalt leidsin aga, et $y \equiv 1 \pmod 4$. Sellest järeldub, et $y^2 + y + 1 \equiv 3 \pmod 4$, mis on vastuolus eelnevalt leitud tulemusega $y^2 + y + 1 \equiv 1 \pmod 4$.

Seega tehtud vastuväiteline oletus ei saa kehtida, ehk diofantiline võrrand $x^2 + 5 = y^3$ ei ole lahenduv, m.o.t.t.

7. ülesanne (lahenduse autorid on toimetusele teada)

$n = 1$ sobib kuna $\prod_{d|1} d = 1 = 1^3$.

Olgu $n \geq 2$ Paneme tähele, et naturaalarvu n jagunevad paaridesse, mille korrutis on n. (Kui $d \mid n \Rightarrow n = da \Rightarrow a \mid n$, kusjuures $a = \frac{n}{d}$ ja $da = d \cdot \frac{n}{d} = n$). Seega

$$\prod_{d|n} d = n^{\frac{\tau(n)}{2}}$$

(võrdus jääb ka kehtima juhul ku $\tau(n)$ on paaritu ehk n on täisruut, sel juhul arvul $\sqrt{n}$ "paarilist"ehk korrutisse jääbki $n^{\frac{1}{2}}$)

Et $n^{\frac{\tau(n)}{2}} = n^3$, siis $\tau(n) = 6$

Kuna $\tau(n) = (k_1 + 1)(k_2 + 1)\dots(k_s + 1)$, kus $k_1 \dots k_s$ on arvu n standardkujus algtegurite astendajad (kusjuures $k_i \geq 1$).

Selleks, $\tau(n) = (k_1 + 1)(k_2 + 1)\dots(k_s + 1) = 6$, peab 6 esituma korrutisena $6 = 2 \cdot 3$ ehk $s = 2$ ja $k_1 = 1, k_2 = 2$ või vastupidi.

Kokkvõttes peab n olema kujul $n = p^2q$, kus p, q on erinevad algarvud või $n = 1$.

Lauri Tart: Siit on puudu lahendid kujul $n = p^5$, $p \in \mathbb{P}$, mis saadakse teisest teguriteks lahutusest $6 = 6 \cdot 1$.

8. ülesanne (Mikael Raihhelgauz ja Maret Sõmer)

Ülesandes on vaja lahendada kongruents $3x^4 + 3x^3 + 4x^2 + x + 64 \equiv 0 \pmod{875}$.
Tähistan $f(x) = 3x^4 + 3x^3 + 4x^2 + x + 64$. Seega $f'(x) = 12x^3 + 9x^2 + 8x + 1$.

Kõigepealt panen tähele, et arvu 875 standardkuju on $875 = 5^3 \cdot 7$. Seega on lause 6.10 põhjal kongruentsi $3x^4 + 3x^3 + 4x^2 + x + 64 \equiv 0 \pmod{875}$ lahendamine samaväärne kongruentside süsteemi

$$\begin{cases} 3x^4 + 3x^3 + 4x^2 + x + 64 \equiv 0 \pmod{5^3} \\ 3x^4 + 3x^3 + 4x^2 + x + 64 \equiv 0 \pmod{7} \end{cases}$$

lahendamisega.

- Lahendan kongruentsi $3x^4 + 3x^3 + 4x^2 + x + 64 \equiv 0 \pmod{5^3}$.

  Selleks lahendan esialgu kongruentsi $3x^4 + 3x^3 + 4x^2 + x + 64 \equiv 0 \pmod 5$. Proovimise teel leian, et ainus lahend on $x_0 \equiv 1 \pmod 5$.

  Järgmisena lahendan kongruentsi $3x^4 + 3x^3 + 4x^2 + x + 64 \equiv 0 \pmod{5^2}$.
  Leian Horneri skeemi abil iga $x_0 \in \{1\}$ korral $f(x_0)$ ja $f'(x_0)$ väärtused.
  (Arvestan, et arvutused $f(x_0)$ leidmiseks võib teha mooduli $5^2 = 25$ järgi ning arvutused $f'(x_0)$ leidmiseks võib teha mooduli 5 järgi.)

x_0					$f(x_0)$				$f'(x_0)$
	3	3	4	1	64	12	9	8	1
1	3	6	10	11	0	2	1	4	0

  Seega tuleb lahendada kongruents:
  $0y + \frac{0}{5} \equiv 0 \pmod 5$, ehk $0 \equiv 0 \pmod 5$, mis tähendab, et $x_0 = 1$ korral võib y olla suvaline täisarv.
  Seega kongruentsi $3x^4 + 3x^3 + 4x^2 + x + 64 \equiv 0 \pmod{5^2}$ lahendid on:
  $x_1 \equiv 1 + 5 \cdot 0 \equiv 1 \pmod{5^2}$, $x_1 \equiv 1 + 5 \cdot 1 \equiv 6 \pmod{5^2}$, $x_1 \equiv 1 + 5 \cdot 2 \equiv 11 \pmod{5^2}$,
  $x_1 \equiv 1 + 5 \cdot 3 \equiv 16 \pmod{5^2}$, $x_1 \equiv 1 + 5 \cdot 4 \equiv 21 \pmod{5^2}$.

  Järgmisena lahendan kongruentsi $3x^4 + 3x^3 + 4x^2 + x + 64 \equiv 0 \pmod{5^3}$.
  Leian Horneri skeemi abil iga $x_1 \in \{1,6,11,16,21\}$ korral $f(x_1)$ ja $f'(x_1)$ väärtused.
  (Arvestan, et arvutused $f(x_1)$ leidmiseks võib teha mooduli $5^3 = 125$ järgi ning arvutused $f'(x_0)$ leidmiseks võib teha mooduli 5 järgi.)

x_1					$f(x_1)$				$f'(x_1)$
	3	3	4	1	64	12	9	8	1
1	3	6	10	11	75	2	1	4	0
6	3	21	5	31	0	2	1	4	0
11	3	36	25	26	100	2	1	4	0
16	3	51	70	-4	0	2	1	4	0
21	3	66	15	66	75	2	1	4	0

  Seega tuleb:
  $x_1 \in \{1,21\}$ korral lahendada kongruents $0y + \frac{75}{25} \equiv 0$, ehk $3 \equiv 0 \pmod 5$,
  $x_1 \in \{6,16\}$ korral lahendada kongruents $0y + \frac{0}{25} \equiv 0$, ehk $0 \equiv 0 \pmod 5$,
  $x_1 = 11$ korral lahendada kongruents $0y + \frac{100}{25} \equiv 0$, ehk $4 \equiv 0 \pmod 5$.
  See tähendab, et $x_1 \in \{6,16\}$ korral sobib lahendiks y iga täisarv, ning
  $x_1 \in \{1,11,21\}$ korral lahendid puuduvad.
  Seega kongruentsi kongruentsi $3x^4 + 3x^3 + 4x^2 + x + 64 \equiv 0 \pmod{5^3}$ lahendid on:
  $x_1 \equiv 6 + 25 \cdot 0 \equiv 6 \pmod{5^3}$, $x_1 \equiv 6 + 25 \cdot 1 \equiv 31 \pmod{5^3}$,
  $x_1 \equiv 6 + 25 \cdot 2 \equiv 56 \pmod{5^3}$, $x_1 \equiv 6 + 25 \cdot 3 \equiv 81 \equiv -44 \pmod{5^3}$,
  $x_1 \equiv 6 + 25 \cdot 4 \equiv 106 \equiv -19 \pmod{5^3}$, $x_1 \equiv 16 + 25 \cdot 0 \equiv 16 \pmod{5^3}$,
  $x_1 \equiv 16 + 25 \cdot 1 \equiv 41 \pmod{5^3}$, $x_1 \equiv 16 + 25 \cdot 2 \equiv 66 \equiv -59 \pmod{5^3}$,
  $x_1 \equiv 16 + 25 \cdot 3 \equiv 91 \equiv -34 \pmod{5^3}$, $x_1 \equiv 16 + 25 \cdot 4 \equiv 116 \equiv -9 \pmod{5^3}$,
  ehk $x \in \{-59, -44, -34, -19, -9, 6, 16, 31, 41, 56\}$.

- Lahendan kongruentsi $3x^4 + 3x^3 + 4x^2 + x + 64 \equiv 0 \pmod 7$.
  Leian lahendeid Horneri skeemiga.

x					$f(x)$
	3	3	4	1	64
0	3	3	4	1	1
1	3	6	3	4	5
2	3	2	1	3	0
3	3	5	5	2	0
4	3	1	1	5	0
5	3	4	3	2	4
6	3	0	4	4	4

  Seega lahendid on $x \equiv 2$, $x \equiv 3$, $x \equiv 4 \pmod 7$.

Kuna kongruentside süsteemi esimesel kongruentsil (mod 125) on 10 lahendit ja teisel kongruetnsil (mod 7) on 3 lahendit, siis kokku on kongruentside süsteemil $10 \cdot 3 = 30$ lahendit. Iga lahendi saamiseks tuleb Hiina jäägiteoreemi abil lahendada üks lineaarkongruentside süsteem:

$$\begin{cases} x \equiv a_1 \pmod{125} \\ x \equiv a_2 \pmod 7 \end{cases}$$

kus $a_1 \in \{-59, -44, -34, -19, -9, 6, 16, 31, 41, 56\}$ ja $a_2 \in \{2,3,4\}$.

Tähistan $m_1 = 7$, $m_2 = 125$.
Ringis $\mathbb{Z}_{125}$ on $\overline{k_1} = \overline{m_1}^{-1} = \overline{7}^{-1} = \overline{18}$.
Ringis $\mathbb{Z}_7$ on $\overline{k_2} = \overline{m_2}^{-1} = \overline{125}^{-1} = \overline{6}^{-1} = \overline{6}$.

Hiina jäägiteoreemi kohaselt kui $x \equiv a_1 \pmod{125}$ ja $x \equiv a_2 \pmod 7$, siis
$x \equiv a_1 \cdot k_1 \cdot m_1 + a_2 \cdot k_2 \cdot m_2 \pmod{125 \cdot 7}$ ehk $x \equiv a_1 \cdot 18 \cdot 7 + a_2 \cdot 6 \cdot 125 \pmod{875}$.
Teen läbi esimese näite.

1. $a_1 = -59$, $a_2 = 2$.
   $$\begin{cases} x \equiv -59 \pmod{125} \\ x \equiv 2 \pmod 7 \end{cases}$$
   $x = -59 \cdot 18 \cdot 7 + 2 \cdot 6 \cdot 125 = -5934 \equiv 191 \pmod{875}$

Analoogselt arvutades saan kätte ka kõik ülejäänud lahendid, ning leian, et kongruentsi $3x^4 + 3x^3 + 4x^2 + x + 64 \equiv 0 \pmod{875}$ lahendid on:
$x \in \{16, 31, 66, 81, 116, 156, 191, 206, 241, 256, 291, 331, 366, 381, 416, 431, 466, 506, 541, 556, 591, 606, 641, 681, 716, 731, 766, 781, 816, 856\} \pmod{875}$

9. ülesanne (Erki Külaots ja Marcus Lõo)

Tegurdame arvud $509 = 509$, $512 = 2^9$, $515 = 5 \cdot 103$ ja $686 = 2 \cdot 7^3$. Näeme, et 515 ja 512 ei sobi, sest 515 jagub kahe erineva paaritu algarvuga ja 512 jagub 4-ga, aga pole 4.

Leiame, mitu algjuurt on arvul 509. $\varphi(\varphi(509)) = \varphi(508) = \varphi(2^2 \cdot 127) = 126 \cdot 2 = 252$. Uurime, kas 2 on algjuur, selleks kasutame järeldust 7.24.

$$2^{\frac{508}{2}} = 2^{254} = -1 \pmod{509}$$
$$2^{\frac{508}{127}} = 2^4 = 16 \pmod{509}$$

Seega 2 on algjuur moodulis 509.

Leiame, mitu algjuurt on arvul 686. $\varphi(\varphi(686)) = \varphi(2 \cdot 3 \cdot 7^2) = 2 \cdot 6 \cdot 7 = 84$. Uurime, kas 2 on algjuur mooduli 7 järgi.

$$2^3 = 8 \equiv 1 \pmod{7}$$

Seega 2 pole, uurime arvu 3.

$$3^2 \equiv 2, 3^3 \equiv 6, 3^4 \equiv 4, 3^5 \equiv 5, 3^6 \equiv 1$$

Seega 3 on moodulis 7 algjuur. Kasutades järeldust 7.15 uurime, kas 3 või $7 + 3 = 10$ on algjuur mooduli 49 järgi.

$$3^6 \equiv 43 \pmod{49}$$

Seega 3 on algjuur moodulis 7^2 ja teoreemi 7.18 põhjal ta on ka algjuur mooduli 7^3 järgi. Kuna ta on paaritu, siis teoreemi 7.19 järgi on ta ka algjuur moodulis 686.

v. Arvul 509 on 252 algjuurt, nt 2. Arvul 686 on 84 algjuurt, nt 3. Arvudel 512 ja 515 pole ühtegi algjuurt.

10. ülesanne (Mikael Raihhelgauz ja Maret Sõmer)

Olgu $f(x) = 1 - x + x^2 - x^3 + x^4 - \ldots + x^{2030}$. Kui leidub x_0 nii, et $f(x_0) \equiv 0 \mod 162$, siis $f(x_0) \equiv 0 \mod 2$, kuna $2|162$. Kui $x_0 \equiv 0 \mod 2$, siis

$$f(x_0) \equiv 1 - 0 + 0^2 - 0^3 + 0^4 - \ldots + 0^{2030} \equiv 1 \mod 2.$$

Kui $x_0 \equiv 1 \mod 2$, siis

$$f(x_0) \equiv 1 - 1 + 1^2 - 1^3 + 1^4 - \ldots + 1^{2030} \equiv 1 + \sum_{n=0}^{1014} -1^{2n+1} + \sum_{n=1}^{1015} 1^{2n} \equiv$$
$$\equiv 1 - 1015 + 1015 \equiv 1 \mod 2.$$

Järelikult kongruentsil $f(x) \equiv 0 \mod 162$ puuduvad lahendid.

11. ülesanne (Mikael Raihhelgauz ja Maret Sõmer)

Kuna a on ruutjääk mooduli pq järgi, siis $x^2 \equiv a \mod pq$ on lahenduv (ühtlasi eeldame, et 'ruutjäägi' mõistet kasutatakse def 8.1 kitsamas tähenduses, sest juhul, kui $a \equiv 0$ on lubatud, siis lause igal ei kehti). HJT põhjal selle lahendid ühtivad süsteemi

$$\begin{cases} x^2 \equiv a \mod p, \\ x^2 \equiv a \mod q, \end{cases} \tag{3}$$

lahenditega. Kuna p, q on algarvud, siis $\mathbb{Z}_p$ ja $\mathbb{Z}_q$ on nullitegureita. Lause 2.9 põhjal on kummalgi kongruentsil ülimalt kaks lahendit.
Oletame vastuväiteliselt, et kongruentsi $x^2 \equiv a \mod p$ lahendid a_1 ja a_2 langevad kokku, s.t $a_1 \equiv a_2 \mod p$. Märgime, et juhul, kui $a_1^2 \equiv a \mod p$, siis ka $(-a_1)^2 \equiv a \mod p$. Kuna eelduse põhjal on kongruentsil ainult üks lahend, siis

$$a_1 \equiv -a_1 \mod p \Rightarrow 2a_1 \equiv 0 \mod p \Rightarrow a_1 \equiv 0 \mod p.$$

Järelikult $a \equiv 0 \mod p$. Siis aga $\left(\frac{a}{pq}\right) = \left(\frac{a}{p}\right)\left(\frac{a}{q}\right) = 0 \cdot \left(\frac{a}{q}\right) = 0$ ehk a pole ruutjääk. Niisiis, kongruentsi $x \equiv a \mod p$ lahendid a_1, a_2 on erinevad. Sama mõttekäik kehtib ka kongruentsi $x \equiv a \mod q$ lahendite a_3, a_4 kohta.
Nüüd on selge, et

$$\begin{cases} x \equiv a_1 \mod p \\ x \equiv a_3 \mod q \end{cases} \qquad \begin{cases} x \equiv a_1 \mod p \\ x \equiv a_4 \mod q \end{cases}$$

$$\begin{cases} x \equiv a_2 \mod p \\ x \equiv a_3 \mod q \end{cases} \qquad \begin{cases} x \equiv a_2 \mod p \\ x \equiv a_4 \mod q \end{cases}$$

on süsteemi (3) lahendid. Järelikult igaüks neist määrab HJT põhjal ühe $x^2 \equiv a \mod pq$ lahendi.
Kui $p = q$, siis lause üldjuhul ei kehti. Näiteks 1 on ruutjääk mod 9 järgi, aga võrrandi $x^2 \equiv 1 \mod 9$ ainsad lahendid on 1 ja 8.

12. ülesanne (Mikael Raihhelgauz ja Maret Sõmer)

Lauri Tart: Ülesande tekst oli osaliselt vigane, kuna kodeerimine ja dekodeerimine olid ära vahetatud. Rangelt võttes oleks siit pidanud vastuseks tulema mõttetu arvujada, milles ei oleks isegi kõiki tähtede tagasiasendamisi teha saanud.

Ülesandes antud avalik võti on (89942987, 677), ehk $n = 89942987$, $e = 677$. Leian salajase astendaja d.
Kõigepealt panen tähele, et mooduli n standardkuju on $n = 89942987 = 9283 \cdot 9689$, mis tähendab, et $\varphi(89942987) = 9282 \cdot 9688 = 89924016$.
Seega ringis $\mathbb{Z}_{89924016}$ $\overline{d} = \overline{e}^{-1} = \overline{677}^{-1} = \overline{11157485}$, ehk salajane astendaja $d = 11157485$.

Ülesandes antud kodeeritud sõnumi c dekodeerimiseks (algse sõnumi s leidmiseks) on nüüd vaja leida $c^d \equiv s^{de} \equiv s \pmod{n}$.

Kõigepealt jagan kodeeritud sõnumi
$c = 19103293485244600190575259093791$ kaheksanumbrilisteks blokkideks:
19103293, 48524460, 01905752, 59093791.
Nüüd on vaja iga blokk tõsta astmesse d mooduli n järgi. Selleks astendan igat blokki kõigepealt algtegurite 9283 ja 9689 järgi eraldi, ning seejärel kasutan Hiina jäägiteoreemi mooduli n järgi tulemuse leidmiseks.
Hiina jäägiteoreemi kasutamiseks tähistan $m_1 = 9689$, $m_2 = 9283$ ning leian, et ringis $\mathbb{Z}_{9283}$ $\overline{k_1} = \overline{m_1}^{-1} = \overline{9689}^{-1} = \overline{406}^{-1} = 5739$ ning $\mathbb{Z}_{9689}$: $\overline{k_2} = \overline{m_2}^{-1} = \overline{9283}^{-1} = 3699$.
Siis Hiina jäägiteoreemi kohaselt, kui $x \equiv a_1 \pmod{9283}$ ja $x \equiv a_2 \pmod{9689}$, siis $x \equiv a_1 \cdot k_1 \cdot m_1 + a_2 \cdot k_2 \cdot m_2 \pmod{9283 \cdot 9689}$ ehk
$x \equiv a_1 \cdot 5739 \cdot 9689 + a_2 \cdot 3699 \cdot 9283 \pmod{n}$

$19103293^{11157485} \equiv 6251 \pmod{9283}$
$19103293^{11157485} \equiv 5798 \pmod{9689}$
$19103293^{11157485} \equiv 6251 \cdot 5739 \cdot 9689 + 5798 \cdot 3699 \cdot 9283 \equiv 05111901 \pmod{n}$

$48524460^{11157485} \equiv 5314 \pmod{9283}$
$48524460^{11157485} \equiv 8565 \pmod{9689}$
$48524460^{11157485} \equiv 5314 \cdot 5739 \cdot 9689 + 8565 \cdot 3699 \cdot 9283 \equiv 13001514 \pmod{n}$

$01905752^{11157485} \equiv 229 \pmod{9283}$
$01905752^{11157485} \equiv 4640 \pmod{9689}$
$01905752^{11157485} \equiv 229 \cdot 5739 \cdot 9689 + 4640 \cdot 3699 \cdot 9283 \equiv 00120908 \pmod{n}$

$59093791^{11157485} \equiv 5673 \pmod{9283}$
$59093791^{11157485} \equiv 6758 \pmod{9689}$
$59093791^{11157485} \equiv 5673 \cdot 5739 \cdot 9689 + 6758 \cdot 3699 \cdot 9283 \equiv 20140500 \pmod{n}$
Seega dekodeeritud tekst on 05111901130015140012090820140500. Loengukonspektis toodud kodeerimise skeemi kohaselt vastavad sellele numbrijadale järgmised tähed:
$05 \mapsto E$, $11 \mapsto K$, $19 \mapsto S$, $01 \mapsto A$, $13 \mapsto M$, $00 \mapsto$ " ", $15 \mapsto O$, $14 \mapsto N$,
$00 \mapsto$ " ", $12 \mapsto L$, $09 \mapsto I$, $08 \mapsto H$, $20 \mapsto T$, $14 \mapsto N$, $05 \mapsto E$, $00 \mapsto$ " ".

Järelikult dekodeeritud tekst on "EKSAM ON LIHTNE ".