Kodutöö nr. 9

Joosep Näks ja Uku Hannes Arismaa

1. Tõestada Lemma 7.17 pöördväide: kui $n \mid \binom{n}{k}$ iga $1 \leq k < n$ korral, siis n on algarv.

Kui väide kehtiks kordarvuga, siis sellel kordarvul peaks olema mingi algtegur, mille väärtuse k omandab. Sellise k väärtuse korral saame, et $n \mid \frac{n(n-1)...(n-k+1)}{1 \cdot 2 \cdot ... \cdot k}$ ning $k \mid n$. Kuna k järjestikusest arvust ainult ühte jagab k, peab see olema n. Kui k on n algtegurduses astmes a, siis jaguvuse vasakul pool esineb see selles astmes, aga paremal pool täpselt astmes $a-1$, kuna ainult n algtegurdudses see esineda saab ning sealt jagame ühe maha. See on aga vastuolu, kuna jagades mõlemad pooled läbi k^{a-1}, saame et vasakule poole jääb mingi k kordne, aga paremal pool ei tohiks ühtki arvu jagada k, mis on vastuolu.

2. Leida kõik täisarvud a, b, c, mille korral $(a, b, c) = 44$ ja $[a, b, c] = 2024$.

Viin antud arvud standardkujudele: $44 = 2^2 \cdot 11$, $2024 = 2^8 \cdot 11 \cdot 23$. Seega kõigi kolme arvu a, b ja c standardkujud on $2^l \cdot 11 \cdot 23^k$, kus ühel arvul $l = 2$, teisel arvul $l = 3$ ja kolmandal $l \in \{2, 3\}$, samuti ühel arvul $k = 0$, teisel $k = 1$ ja kolmandal $k \in \{0, 1\}$. Seega on võimalikud kõik järgnevad kolmikud ja nende permutatsioonid.

l \ k	(0,0,1)	(0,1,1))	(0,1,0))	(1,0,0))	(1,0,1))	(1,1,0))
(1,1,2)	(44,44,2024)	(44,1012,2024)	(44,1012,88)	(1012,44,88)	(1012,44,2024)	(1012,1012,88)
(1,2,2)	(44,88,2024)	(44,2024,2024)	(44,2024,88)	(1012,88,88)	(1012,88,2024)	(1012,2024,88)

3. Terviseamet ostis spetsiaalselt strateegiliste võtmeisikute vaktsineerimiseks 1936€ eest vaktsiine, 20€ AstraZeneca, 72€ Pfizeri ja 108€ Moderna pudeli eest. Kui palju neid võtmeisikuid maksimaalselt olla võis, kui kõiki pudeleid oli algarv tükki ja konsulteeritud matemaatikud kinnitasid, et piisab suvalisest neid tingimusi rahuldavast pudelikombinatsioonist?

Selleks, et saada maksimaalselt vaktsiine, tuleb osta maksimaalselt AstraZeneca vaktsiine. Kuna 1936 ei jagu 20ga, siis tuleb osta ka natuke teisi vaktsiine. Selleks, et ülejäänud arv jaguks 20ga peab ostma kas 3 pudelit Pfizerit või 2 pudelit Modernat. Siis saaks ülejäänud raha eest osta 86 pudelit AstraZenecat. See pole algarv, seega tuleb osta veel vähemalt [20,72] või [20,108] euro eest vähem AstaZenecat. Kui osta ainult [20,72] jagu vähem, ei ole Astra Zenecat ikka algarv. Vaktsiinide arvult järgmine parim variant on osta [20,108] Modernat. Tuleb välja, et siis on kõik kordajad algarvud, kui esialgse 20 kordsuse saavutamiseks osta Pfizerit, ehk kokku oleks 59 pudelit AstraZenecat, 3 Pfizerit ning 5 Modernat.

4. Leida kõik algarvud p, mille korral $\dfrac{(2^{p-1}-1)}{p}$ on täisruut.

Kui $p=2$, siis $\dfrac{2^{2-1}-1}{2}=\dfrac{1}{2}$, mis ei ole täisruut.
Kõik teised algarvud on paaritud ehk 2^{p-1} on täisruut, nii et arvu saab lahti kirjutada järgnevalt: $\dfrac{(2^{p-1}-1)}{p}=\dfrac{(2^{\frac{p-1}{2}}-1)(2^{\frac{p-1}{2}}+1)}{p}$. Kui see arv on täisarv, peab Eukleidese lemma tõttu p jagama kas arvu $(2^{\frac{p-1}{2}}-1)$ või arvu $(2^{\frac{p-1}{2}}+1)$. Samuti on näha, et $(2^{\frac{p-1}{2}}-1, 2^{\frac{p-1}{2}}+1)=1$, kuna need arvud on järjestikused paaritud arvud ja nende suurim ühistegur peaks jagama nende vahet, kuid vahe on 2 ehk ainus võimalik tegur oleks 1, see aga ei sobi kuna tegu on paaritute arvudega. Kuna nendel arvudel puudub ühistegur, peavad mõlemad olema ise täisruudud, et nende korrutis oleks täisruut.
Seega juhul kui p jagab esimest nendest arvudest, saame et $2^{\frac{p-1}{2}}-1=px^2$ ja $2^{\frac{p-1}{2}}+1=y^2$. Viimase saab lahti kirjutada kujule $2^{\frac{p-1}{2}}=(y-1)(y+1)$, mis tähendab, et kaks arvu, mille vahe on 2, peavad mõlemad olema 2 astmed. See kehtib vaid $y=1$ ja $y=3$ puhul. Esimesel nendest võimalustest tuleks $p=1$, mis ei ole algarv, ning teisel võimalusel $p=7$, mis on üks võimalik vastus.
Teine juht on see, kui p jagab teist saadud teguritest, sel juhul saame et $2^{\frac{p-1}{2}}-1=x^2$ ja $2^{\frac{p-1}{2}}+1=py^2$. Esimest nendest ümber kirjutades saab $2^{\frac{p-1}{2}}=x^2+1$. Märkan, et jäägiklassiringis $\mathbb{Z}_4$ ei ole ühegi liikme ruut 3 ehk arv x^2+1 ei saa jaguda neljaga. See tähendab et $\dfrac{p-1}{2}<2$. Siit saab, et võimalikud algarvulised p väärtused on 2 ja 3, millest ainult 3 on paaritu.
Seega ainsad p väärtused, mis saaksid anda täisruutu, on 3 ja 7 ning läbi proovides need ka annavad vastavalt täisruudud 1 ja 9, seega need on ainsad sobivad algarvud.

5. Olgu $p\in\mathbb{P}$, $n\in\mathbb{N}$, $(p,n)=1$ ja $n\not\equiv 1 \pmod p$. Leida jäägiklassi $\overline{1+n+n^2+\ldots+n^{p-2}}\in\mathbb{Z}_p$ vähim esindaja.

Geomeetrilise jada summa valemist saame selle jäägiklassi kirjutada kui $\dfrac{\overline{1-n^{p-1}}}{1-n}$ Kuna $n\not\equiv 1$, siis $1-n\not\equiv 0 \pmod p$, seega saame sellega jagamise asendada selle pöördelemendiga k korrutamisega, saame jäägiklassi $\overline{(1-n^{p-1})k}=\overline{k}(\overline{1}-\overline{n^{p-1}})$. Kuna $(p,n)=1$, siis FVT järgi $n^{p-1}\equiv 1 \pmod p$, seega on esialgne jäägiklass $\overline{0}$, mille vähim naturaalarvuline esindaja on p.

6. Olgu $n\in\{1,2,\ldots,9\}$ number. Leida suurim ja vähim n väärtus, mille korral ükski arv, mis on saadud numbrite $1,\ldots,n$ permuteerimisel, ei jagu arvuga 11.

Kiirel läbivaatlusel on näha, et $n=1$ ja $n=2$ puhul ei jagu ükski permutatsioon arvuga 11 kuna kõik võimalikud permutatsioonid on 1, 12 ja 21.
Arvuga 11 jaguvuse kontrollimiseks saab liita arvu numbrid kokku vahelduvate märkidega ning kontrollida kas tulemus jagub arvuga 11. Kuna kontrollime jaguvust kõigi permutatsioonide hulgas piisab, kui saame jagada arvu numbrid kahte hulka, kus hulkade summad on võrdsed või erinevad 11 kordse arvu võrra ning kus hulkade võimsuste vahe on ülimalt 1. Nii on lihtne näha et 3, 4, 7 ja 8 puhul saab jagada numbrid kahte võrdse summaga hulka:

n	3	4	7	8
I	1+2=3	2+3=5	3+5+6=14	1+4+5+8=18
II	3	1+4=5	1+7+2+4=14	2+1+6+7=18

Teiste n väärtuste puhul ei saa summaks 0 saada, kuna kõigi numbrite $1,..,n$ summa on paaritu arv ehk seda ei saa kaheks võrdseks summaks jagada. Seega tuleb teistel summade vaheks saada 11 või mõni kõrgem 11 kordne arv, kusjuures 22 ei ole samuti võimalik kuna kui arvude vahe on paaritu, ei saa ka nende summa paaris olla. Arvu 5 puhul suurim võimalik vahe mida saab tekitada on $5+4+3-2-1=9<11$ ehk ükski $n=5$ permutatsioon ei saa jaguda arvuga 11. Samuti $n=6$ puhul on suurim vahe $6+5+4-3-2-1=9<11$ ehk samuti pole jaguvus võimalik. Viimaks $n=9$ puhul saab moodustada summad $1+2+5+9=17$ ja $3+4+6+7+8=28$, mille vahe on 11, ehk leidub permutatsioone, mis jaguvad arvuga 11.
Seega vähim n väärtus, mille korral ükski permutatsioon ei jagu arvuga 11 on $n=1$ ja suurim on $n=6$.

7. Lahendada *diofantiline* võrrand $x^{13} + 12x + 13y^6 = 1$.

Vaatame võrrandit mooduli 13 järgi. Saame $x^{13} - x \equiv 1 \pmod{13}$. Valem ei kehti, kui $x = 0$ igal teisel juhul teame FVTst, et $x^{12} \equiv x \pmod{13}$, seega iga teise x väärtuse korral saame $0 \equiv 1 \pmod{13}$, mis on vastuolu, seega ei leidu x väärtust, mis sobiks lahendisse, seega ei leidu lahendit.

8. Leida, mitu pööratavat elementi on ringides $\mathbb{Z}_{2028}$ ja $\mathbb{Z}_{39} \times \mathbb{Z}_{52}$. Kas ringid $\mathbb{Z}_{2028}$ ja $\mathbb{Z}_{39} \times \mathbb{Z}_{52}$ on isomorfsed? Miks?

Ringi $\mathbb{Z}_{2028}$ pööratavate elementide leidmiseks leian elementide koguse, millel on arvuga 2028 ühistegur suurem kui üks. Tegurdades saan et $2028 = 2^2 \cdot 3 \cdot 13^2$, seega omavad ühistegurit arvuga 2028 arvud, mis on 2, 3 või 13 kordsed. Selliseid elemente on $\mathbb{Z}_{2028}$ ringis $\frac{2028}{2} + \frac{2028}{3} + \frac{2028}{13} - \frac{2028}{2 \cdot 3} - \frac{2028}{3 \cdot 13} - \frac{2028}{13 \cdot 2} + \frac{2028}{2 \cdot 3 \cdot 13} = 1014 + 676 + 156 - 338 - 52 - 78 + 26 = 1404$. Seega on pööratavaid elemente ehk elemente, mille suurim ühistegur arvuga 2028 on 1, kokku $2028 - 1404 = 624$ tükki.
Ringi $\mathbb{Z}_{39} \times \mathbb{Z}_{52}$ pööratavate elementide leidmiseks leian kõigepealt eraldi $\mathbb{Z}_{39}$ ja $\mathbb{Z}_{52}$ pööratavad elemendid. Tegurdades saan $39 = 3 \cdot 13$ ja $52 = 2^3 \cdot 13$. Seega on $\mathbb{Z}_{39}$ pööratavaid elemente $39 - \left(\frac{39}{3} + \frac{39}{13} - \frac{39}{3 \cdot 13}\right) = 24$ ja $\mathbb{Z}_{52}$ pööratavaid elemente on $52 - \left(\frac{52}{2} + \frac{52}{13} - \frac{52}{2 \cdot 13}\right) = 24$. Seega on ringis $\mathbb{Z}_{39} \times \mathbb{Z}_{52}$ on $24 \cdot 24 = 576$ pööratavat elementi.
Ringid $\mathbb{Z}_{2028}$ ja $\mathbb{Z}_{39} \times \mathbb{Z}_{52}$ ei ole isomorfsed, sest neis on erinev kogus pööratavaid elemente.

9. Lahendada diofantiline võrrand $\varphi(5x) = \varphi(6x)$.

$r = \varphi(x)$ Kui $5 \mid x$, siis $\varphi(5x) = 5r$, vastasel juhul $\varphi(5x) = 4r$. Kui $6 \mid x$, siis $\varphi(6x) = 6r$, kui ainult $3 \mid x$, siis $\varphi(6x) = 3r$, kui ainult $2 \mid x$, siis $\varphi(6x) = 4r$ ning kui kumbki ei jaga, siis $\varphi(6x) = 2r$. Nendest variantidest kattuvad ainult $4r$, seega peab olema, et $2 \mid x$ ning $5 \nmid x$ ning $3 \nmid x$.

10. Leida kõik naturaalarvud n, mille korral $\frac{n}{\tau(n)}$ on algarv.

On näha, et töötavad kõik arvud kujul $2^3 \cdot p$, kus $p > 2$ on algarv, kuna $\tau(2^3 \cdot p) = 8$ ehk $\frac{2^3 \cdot p}{\tau(2^3 \cdot p)} = p$. Samuti töötavad kõik arvud kujul $2^2 \cdot 3 \cdot p$, kus $p > 3$ on algarv, kuna $\frac{2^2 \cdot 3 \cdot p}{\tau(2^2 \cdot 3 \cdot p)} = p$. Samuti saab väikeste arvude läbivaatlusel, et sobivad 8, 9, 12, 18 ja 24. Väidan, et rohkem sobivaid arve pole.

Kui $n = p_1^{k_1}...p_s^{k_s}$, saame üldisust kitsendamata $\frac{n}{\tau(n)} = p_1$, kust saame $p_1^{k_1}...p_s^{k_s} = p_1(k_1+1)\cdot...\cdot(k_s+1)$, kust p_1 taandamisel saame $p_1^{k_1-1}...p_s^{k_s} = (k_1+1)\cdot...\cdot(k_s+1)$. Kui alustame p_1^1, siis saame vasakule poole 1 ning paremale 2. Kui me suurendame p_1 astendajat, siis parem pool suureneb p_1 korda ehk vähemalt 2 korda, parem pool suureneb vähem. Kui korrutada p_1^x läbi uue algarvuga p_s, saame vasaku poole p_s kordse kasbvu ning parema poole kahekordistumise. Seega saab parem pool kasvada kiiremini va siis, kui $p_s = 2$, mis saab juhtuda maksimaalselt ühe korra. Seega nii n moodustades alustades p_1-st saame uurida, mis hetkel parem pool on suurem kui vasak. Sellest hetkest alates tingimus enam kehtida ei saa, kuna parem pool on ja jääb liiga suureks. Kui esialgset p_1 korrutada 5 või suurema algarvuga, siis saame, et vasak pool on 5 ning parem 4, seega sellisel kujul arvud ei sobi. Samuti ei sobi, et p_1 on suuremas astmes kui 1 ning 5 või suurem. p_1^1 puhul $1 = 2$, seega peame vasakut poolt veel suurendama.

Kui $p_1 = 2$, siis vasakul pool on 1 ja paremal 2.
Korrutades n läbi 2ga saame vasakule 2 ning paremale 3.
Korrutades uuesti 2ga, leiame vastuse $n = 8$.
Korrutades aga 3ga saame sobiva vastuse $n = 12$.
Korrutades n läbi kolmega saame vasakule 3 ning paremale 6.
Veelkord 3ga korrutades saame sobiva vastuse $n = 18$.

Kui $p_1 = 3$, siis vasakul pool on 1 ja paremal 2. Siit analoogselt minnes satuma paljude eelnevalt leitud n peale. Ainus uus tulemus on enne varju jäänud $n = 9$.

Kui $p_1 > 3$, siis vasakul pool on 1 ja paremal 2.
korrutades 2ga saame vasakule 2 ning paremale 4.
Korrutades uuesti kahega, saame vasakule 4 ning paremale 6.
3. korda kahega korrutades saame üldkujul lahendi $n = 8p_1$
Korrutades 3ga saame üldkujul lahendi $n = 12p_1$

Nüüd kuna siin lisamise järjekord pole oluline, pole kõiki vahepeal 3 lisamisi mõtet läbi mängida.
Kohe 3ga korrutades saame vasakule 3 ning paremale 4.
Veelkord kolmega korrutades saame vasakule 9 ning paremale 6.

Kuna eelenevalt näitasime, et suuremate algarvudega n korrutamine ajab vasaku poole lõhki ning oleme väiksemate algarvudega proovides kõik kriitilised punktid leidnud, saame väita, et rohekem lahendeid ei ole ning kõik algselt leitud n on olemas.

11. Lahendada kongruentside süsteem

$$\begin{cases} 3x^2 \equiv 12 & (\text{mod } 16) \\ 4x^4 \equiv 4 & (\text{mod } 125). \end{cases}$$

Esimeses võrrandis korrutan mõlemad pooled läbi arvuga -5, saan uue võrrandi $x^2 \equiv 4 \pmod{16}$. Vaadates kõigepealt võrrandit mooduli 2 järgi on ilmne et $x^2 \equiv 0 \pmod 2$ ainus lahend on 0 ehk lõplikud lahendid on 2 kordsed. Proovin läbi paarisarvud, ning saan et lahenditeks on 2, 6, 10 ja 14.

Teises võrrandis vaatlen kõigepealt korrutan mõlemad pooled 4 pöördarvuga läbi et saada võrrand $x^4 \equiv 1 \pmod{125}$. Vaatan võrrandit mooduli 5 järgi. On näha et $x \equiv 0 \pmod 5$ ei sobi lahendiks, muude väärtuste puhul kehtib võrrand FVT tõttu. Vaatlen neid lahendeid nüüd mooduli 25 järgi. Märgin $f(x) = x^4 - 1$ ja $f'(x) = 4x^3$

Vaatleme juhtu $x \equiv 1 \pmod 5$. Saan $f'(1) = 4 \equiv -1 \pmod 5$ ja $f(1) = 0$, ning $\frac{0}{5} = 0$. Seega $x \equiv 1 + 5y$ leidmiseks leian $-y + 0 \equiv 0 \pmod 5$ lahedi, milleks on 0, ehk olen leidnud lahendi $x \equiv 1 \pmod{25}$. Vaatan seda ka kolmandas astmes mooduli järgi. Selleks on vaja samuti $-b + 0 \equiv 0 \pmod 5$ lahendit, milleks on 0. Seega on üheks lõplikuks lahendiks $x \equiv 1 \pmod{125}$.

Vaatleme juhtu $x \equiv 2 \pmod 5$. Saan $f'(2) = 32 \equiv 2 \pmod 5$ ja $f(2) = 15$, ning $\frac{15}{5} = 3$. Seega $x \equiv 2 + 5y$ leidmiseks leian $2y + 3 \equiv 0 \pmod 5$ lahedi, milleks on 1, ehk olen leidnud lahendi $x \equiv 7 \pmod{25}$. Vaatan seda ka kolmandas astmes mooduli järgi. Selle jaoks $f'(7) \equiv 2 \pmod 5$ ja $f(7) = 2400$, $\frac{2400}{25} = 96 \equiv 1 \pmod 5$. Koostan võrrandi $2b + 1 \equiv 0 \pmod 5$, mille lahendiks on 2. Seega on üheks lõplikuks lahendiks $x \equiv 57 \pmod{125}$.

Vaatleme juhtu $x \equiv 3 \pmod 5$. Saan $f'(3) = 108 \equiv 3 \pmod 5$ ja $f(3) = 80$, ning $\frac{80}{5} = 16 \equiv 1 \pmod 5$. Seega $x \equiv 3 + 5y$ leidmiseks leian $3y + 1 \equiv 0 \pmod 5$ lahedi, milleks on -2, ehk olen leidnud lahendi $x \equiv -7 \pmod{25}$. Vaatan seda ka kolmandas astmes mooduli järgi. Selle jaoks $f'(-7) \equiv 3 \pmod 5$ ja $f(-7) = 2400$, $\frac{2400}{25} = 96 \equiv 1 \pmod 5$. Koostan võrrandi $3b + 1 \equiv 0 \pmod 5$, mille lahendiks on 3. Seega on üheks lõplikuks lahendiks $x \equiv 68 \equiv -57 \pmod{125}$.

Vaatleme juhtu $x \equiv 4 \pmod 5$. Saan $f'(4) = 256 \equiv 1 \pmod 5$ ja $f(4) = 255$, ning $\frac{255}{5} = 51 \equiv 1 \pmod 5$. Seega $x \equiv 4 + 5y$ leidmiseks leian $y + 1 \equiv 0 \pmod 5$ lahedi, milleks on -1, ehk olen leidnud lahendi $x \equiv -1 \pmod{25}$. Vaatan seda ka kolmandas astmes mooduli järgi. Selle jaoks $f'(-1) \equiv 1 \pmod 5$ ja $f(-1) = 0$, $\frac{0}{25} = 0$. Koostan võrrandi $b + 0 \equiv 0 \pmod 5$, mille lahendiks on 0. Seega on üheks lõplikuks lahendiks $x \equiv -1 \pmod{125}$.

Seega on nüüd olemas mooduli 16 järgi lahendid 2, 6, 10 ja 14 ning mooduli 125 järgi lahendid 1, 57, -57 ja -1. HJT annab et lahendid on kujul $x = a \cdot 125 \cdot 5 + b \cdot 16 \cdot 86 = 625a + 1376b$. Selle abil saan lõplikud lahendid mooduli $16 \cdot 125 = 2000$ järgi:

b \ a	2	6	10	14
1	626	1126	1626	126
57	1682	182	682	1182
-57	818	1318	1818	318
-1	1874	374	874	1374

12. Lahendada kongruents

$$2x^4 + 6x^3 + 4x^2 - 5x + 12 \equiv 0 \pmod{4459}.$$

Tegurdades saan $4459 = 7^3 \cdot 13$, lahendan kongruentsi eraldi moodulite 7^3 ja 13 järgi.
Moodul 13 järgi Horneri skeem:

	$\overline{2}$	$\overline{6}$	$\overline{4}$	$\overline{-5}$	$\overline{-1}$
$\overline{0}$	$\overline{2}$	$\overline{6}$	$\overline{4}$	$\overline{-5}$	$\overline{-1}$
$\overline{1}$	$\overline{2}$	$\overline{8}$	$\overline{-1}$	$\overline{-6}$	$\overline{-7}$
$\overline{2}$	$\overline{2}$	$\overline{-3}$	$\overline{-2}$	$\overline{4}$	$\overline{7}$
$\overline{3}$	$\overline{2}$	$\overline{-1}$	$\overline{1}$	$\overline{-2}$	$\overline{-7}$
$\overline{4}$	$\overline{2}$	$\overline{1}$	$\overline{-5}$	$\overline{1}$	$\overline{3}$
$\overline{5}$	$\overline{2}$	$\overline{3}$	$\overline{6}$	$\overline{-1}$	$\overline{-6}$
$\overline{6}$	$\overline{2}$	$\overline{5}$	$\overline{-5}$	$\overline{4}$	$\overline{-3}$
$\overline{-6}$	$\overline{2}$	$\overline{-6}$	$\overline{1}$	$\overline{2}$	$\overline{0}$
$\overline{-5}$	$\overline{2}$	$\overline{-4}$	$\overline{-2}$	$\overline{5}$	$\overline{0}$
$\overline{-4}$	$\overline{2}$	$\overline{-2}$	$\overline{-1}$	$\overline{-1}$	$\overline{3}$
$\overline{-3}$	$\overline{2}$	$\overline{0}$	$\overline{4}$	$\overline{-4}$	$\overline{-2}$
$\overline{-2}$	$\overline{2}$	$\overline{2}$	$\overline{0}$	$\overline{-5}$	$\overline{9}$
$\overline{-1}$	$\overline{2}$	$\overline{4}$	$\overline{0}$	$\overline{-5}$	$\overline{4}$

Ehk 13 järgi on lahendid -6 ja -5. Moodul 7 järgi Horneri skeem:

	$\overline{2}$	$\overline{-1}$	$\overline{-3}$	$\overline{2}$	$\overline{-2}$
$\overline{0}$	$\overline{2}$	$\overline{-1}$	$\overline{-3}$	$\overline{2}$	$\overline{-2}$
$\overline{1}$	$\overline{2}$	$\overline{1}$	$\overline{-2}$	$\overline{0}$	$\overline{-2}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{3}$	$\overline{1}$	$\overline{0}$
$\overline{3}$	$\overline{2}$	$\overline{-2}$	$\overline{-2}$	$\overline{-4}$	$\overline{0}$
$\overline{-3}$	$\overline{2}$	$\overline{0}$	$\overline{-3}$	$\overline{-3}$	$\overline{0}$
$\overline{-2}$	$\overline{2}$	$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{2}$
$\overline{-1}$	$\overline{2}$	$\overline{-3}$	$\overline{0}$	$\overline{2}$	$\overline{3}$

Ehk 7 järgi on lahendid 2, 3 ja 4. Leian funktsiooni tuletise: $f'(x) \equiv x^3 - 3x^2 + x + 2 \pmod 7$.
Vaatlen kõigepealt lahendit 2 kõrgemate astmete puhul. Saan $f'(2) \equiv 0 \pmod 7$ ja $f(2) = 98$ ehk $\frac{f(2)}{7} = \frac{98}{7} = 14 \equiv 0 \pmod 7$. Sellest tuleneb, et kui tahame leida lahendeid kujul $x \equiv 2 + 7y \pmod{7^2}$, siis y saab leida võrrandist $0y + 0 \equiv 0 \pmod 7$. Selleks sobivad kõik $0 \leq y < 7$ ehk 7^2 järgi on lahendid . Järgise astme järgi lahendite leidmise jaoks on vaja kõigi $a \in \{2, 9, 16, 23, 30, 37, 44\}$ puhul leida $f'(a)b + \frac{f(a)}{7^2} \equiv 0 \pmod 7$ lahendid kuid kuna $f'(a) \equiv f'(2) = 0 \pmod 7$, ei sõltu võrrand arvust b ehk tuleb kontrollida, milliste a väärtuste puhul $7^3 \mid f(a)$. $f(2) \equiv 98 \pmod{7^3}$, $f(9) \equiv 294 \pmod{7^3}$, $f(16) \equiv 196 \pmod{7^3}$, $f(23) \equiv 147 \pmod{7^3}$, $f(30) \equiv 147 \pmod{7^3}$, $f(37) \equiv 196 \pmod{7^3}$, $f(44) \equiv 294 \pmod{7^3}$. Seega mooduli 7^3 järgi lahendeid kujul $a + 7^2 b$ ei leidu.

Järgmiseks vaatlen lahendit 3 kõrgemate astmete puhul. Saan $f'(3) \equiv -2 \pmod 7$ ja $f(3) = 357$, $\frac{357}{7} = 51 \equiv 2 \pmod 7$. Seega lahendite kujul $x \equiv 3 + 7y \pmod{7^2}$ jaoks tuleb leida y võrrandist $-2y + 2 \equiv 0 \pmod 7$. Selle ainus lahend on $y \equiv 1 \pmod 7$. Seega mooduli 7^2 järgi ainus lahend on $x \equiv 3 + 7 \cdot 1 = 10 \pmod{7^2}$. Kontrollin seda ka kolmanda 7 astme järgi. $f'(10) \equiv -2 \pmod 7$ ja $f(10) = 26362$ ehk $\frac{26362}{7^2} = 538 \equiv -1 \pmod 7$. Seega lahendite kujul $x \equiv 10 + 7^2 b \pmod{7^3}$ on vaja leida b võrrandist $-2b - 1 \equiv 0 \pmod 7$, mille ainsaks lahendiks on $x \equiv 3 \pmod 7$. Seega siit saab ainsaks lahendiks kujul $x = 4 + 7y$ järgi $x \equiv 157 \pmod{7^3}$.

Viimaseks vaatlen lahendit 4 kõrgemate astmete puhul. Saan $f'(4) \equiv 1 \pmod 7$ ja $f(4) = 952$, kus $\frac{952}{7} = 156 \equiv 3 \pmod 7$. Seega lahendite jaoks kujul $x \equiv 4 + 7y \pmod{7^2}$ tuleb leida y võrrandist

$y + 3 \equiv 0 \pmod 7$, mille ainsaks lahendiks on $y \equiv -3 \pmod 7$. Seega leidsin lahendi $x \equiv 4 - 7 \cdot 3 = -17 \pmod{7^2}$. Järgmiseks leian vastava lahendi kolmanda astme järgi. $f'(-17) \equiv 1 \pmod 7$ ja $f(-17) = 138817$ ning $\frac{138817}{7^2} = 2833 \equiv -2 \pmod 7$. Seega tuleb lahendada võrrand $b - 2 \equiv 0 \pmod 7$, mille ainsaks lahendiks on $b \equiv 2 \pmod 7$. Seega olen leidnud lahendi $x \equiv -17 + 2 \cdot 49 = 81$.

Kokkuvõttes olen saanud et võrrandil on mooduli 13 järgi lahendid -6 ja -5 ning mooduli 7^3 järgi lahendid 157 ja 81. HJT-st saame, et lõplikud lahendid on $x \equiv 3244 \pmod{4459}$, $x \equiv 1529 \pmod{4459}$, $x \equiv 424 \pmod{4459}$ ja $x \equiv 2139 \pmod{4459}$.