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.

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?

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.

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 $x^{13} + 12x + 13y^6 = 1$.

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 $\varphi(5x) = \varphi(6x)$.

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

11. Lahendada kongruentside süsteem

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

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 $x \equiv 2139 \pmod{4459}$.