Kodutöö nr. 16

Joosep Näks ja Uku Hannes Arismaa

1. Tõestada, et kui $n \in \mathbb{N}$, siis $[1, 2, \dots, n] \geq \left(\sqrt{n}\right)^{\pi(n)}$.

Võtame võrratuse mõlemad pooled ruutu ning parema poole jagame algteguriteks. Algtegureid on sama palju, kui on n-st väiksemaid algarve, kuna need kõik peavad jagama VÜKi. Iga algarvu astmete puhul peab vähiamt ühiskordset jagama mingi algarvu nii suur aste, kui ta maksimaalselt arvude 1 kuni n hulgas esineb. Seega iga p^k puhul $p^k \leq n$ ning $p^{k+1} > n$, kusjuures $k > 0$, kuna vastasel juhul esineks vähimas ühiskordses vähmalt üks p aste, mis ei jaga lõpptulemust. Seega võrratuses vastab igale n-le paremal pool algarvu aste vaakul pool, kusjuures algarvu aste on kujul p^{2k}, seega kuna $p^{2k} \geq p^{k+1} > n$, saame, et iga vasaku poole tegur on vastavast parema poole tegurist suurem, seeega on seda ka korrutis vasakul pool.

2. Tõestada, et iga $m, n \in \mathbb{N}$ korral $(m!)^n \mid (mn)!$.

Parema poole saab ümber kirjutada kui $(mn)! = \prod_{i=0}^{n-1} \prod_{j=1}^{m} (j + mi)$ ehk on kokku korrutatud m järjestikust arvu n korda. Iga m järjestikuse arvu kokku korrutis jagub arvuga $m!$, sest selles on esimesed m arvu kokku korrutatud ning kui võtta näiteks selle tegur m, siis iga m järjestiku arvu hulgas leidub täpselt üks m kordne arv, samuti iga $m - 1$ järjestikuse arvu hulgas leidub üks $m - 1$ kordne arv ja nii edasi ehk iga m järjestikuse arvu hulgas leiduvad kõigi esimese m arvu kordsed arvud. Kattuvusi tekib vaid juhul kui mingi arv a on mingi teise arvu b kordne, kuid siis leidub b järjestikuse arvu hulgas üks b kordne ning $\frac{b}{a} > 1$ tükki a kordseid arve ehk saab a kordseks arvuks valida mõne sellise, mis ei ole b kordne. Seega iga m järjestikuse arvu korrutis jagub arvuga $m!$ ehk kuna $(mn)!$ sisaldab n sellist korrutist, jagub see arvuga $(m!)^n$.

3. Leida diofantilise võrrandi $4x + 12y + 16z = 2024$ positiivsete lahendite arv.

Ülesanne on samaväärne ülesandega $x + 3y + 4z = 506$. Saame lahendeid hakata loendama, kui alustame seisust, kus $x = y = z = 1$, ning uurime, kui mitu väärtust saab olla y-l iga võimaliku z väärtuse korral. x väärtus on alati eelmise kahe põhjal üheselt määratud. Kui $z = 1$, siis on y jaoks $\frac{506 - 4 - 3 - 1}{3} + 1 = 167$ väärtust. Suurendades z 1 võrra saame $\frac{498 - 4}{3} + 1 = 165$ väärtust. Veel 1 võrra z suurendades saame 164 väärtust. Kokku on juba 493 väärtust. Seega saime, et kui meil on z vahemikus 1-4, siis on meil 496 väärtustust, mille korral saame soovitud tulemuse. suurendades z võiamlike väärtuste piire 3 võrra (5-7), saame y võiamlike väärtuste arvuks samad tulemused, lihtsalt 4 võrra väiksemad. Nii saame konstrueerida aritmeetilise jada, kus alguses on 1 võimalus, kui $z = 124$ ning iga järgmine elemet kuni $496 = 4 + 12 * 41$ on eelmisest 12 võrra suurem. Matemaatika järgi on selle jada summa 10500.

4. Leida kõik algarvud p, mille korral $p^2 \mid 5^{p^2} + 1$.

Vaatan arvu $5^{p^2} + 1$ mooduli p järgi. Et see saaks jaguda arvuga p^2, peab see olema kongruentne arvuga 0. Kui $p = 5$, siis $5^{p^2} + 1 \equiv 1 \not\equiv 0 \pmod{p}$. Muudel juhtudel saab FVT põhjal $5^{p^2} + 1 \equiv 5^{p^2-(p-1)(p+1)} + 1 = 5^1 + 1 = 6 \pmod{p}$. Ainsad algarvulised moodulid, mille järgi 6 saab olla kongruentne nulliga on 2 ja 3. Proovin need läbi: $5^{2^2} + 1 = 626 \equiv 2 \pmod{2^2}$ ja $5^{3^2} + 1 = 1953126 \equiv 0 \pmod{3^2}$ ehk ainus algarv, mille puhul jaguvus kehtib, on $p = 3$.

5. Leida ringi $\mathbb{Z}_{40336800}$ kõigi selliste elementide $\overline{x}$ arv, mille korral $x^2 \equiv 0 \pmod{40336800}$.

Peam lihtsalt näitama, kui mitme x^2 korral see 40336800-ga jagub. Selleks peavad x^2 algtegurduses leiduma need algarvud, mis on 40336800 algtegurduses (2,3,5,7), ning need peavad leiduma vähemalt selles astmes, mis need leiduvad 40336800 algetegurduses (vastavalt 5,1,2,5) ühtlasi, peavad need seega ka leiduma x algtegurduses, kusjuures väiksemas astmes kui 40336800 omas. Nii saame , et x algtegurduses peab olema minimaalselt 2^3, 3, 5, 7^3. Kõik selle arvu kordsed sobivad samuti x-ks. Neid on 40336800-st väiksemaid $\dfrac{40336800}{2^3 \cdot 5 \cdot 3 \cdot 7^3} = 980$. Saimegi vastuse.

6. Lahendada diofantiline võrrand $x^3 + y^4 = 2100$.

Vaatlen võrrandit mooduli 13 järgi. Kuupide ja neljandate astmete tabelid mooduli 13 järgi:

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

Ehk x^3 võimalikud väärtused on 0, 1, 3, 5, 8, 12 ning y^4 võimalikud väärtused on 0, 1, 3 ja 9. Arv 2100 on kongruentne arvuga 7 mooduli 13 järgi, kuid leitud x^3 ja y^4 väärtuste summana ei ole võimalik arvu 7 ega ka 7+13 saavutada (ning suurim võimalik summa on 12+9 mis on väiksem kui järgmine arvuga 7 kongruentne arv) ehk võrrandil puuduvad lahendid.

7. Olgu $n \equiv -1 \pmod{8}$. Tõestada, et $\sigma(n) \equiv 0 \pmod{8}$.

8. Lahendada kongruents

$$x^4 - 6x^3 - 7x^2 + 96x + 6 \equiv 0 \pmod{1125}.$$

Tegurdades saab $1125 = 3^2 \cdot 5^3$ seega vaatlen kõigepealt võrrandit moodulite 3 ja 5 järgi.

$$x^4 - 6x^3 - 7x^2 + 96x + 6 \equiv 1 - 0 - 1 + 0 + 0 \equiv 0 \pmod{3}.$$

Ehk mooduli 3 järgi sobivad kõik lahendid. Järgmise sammu jaoks võtan algsest funktsioonist tuletise:

$$f'(x) = 4x^3 - 18x^2 - 14x + 96$$

Otsin lahendit kujul $x = 1 + 3y$. Kuna $f(1) = 90$ ja $f'(1) = 68 \equiv -1 \pmod{3}$, tuleb lahendada lineaarkongruents

$$-1 \cdot y + \frac{90}{3} \equiv 0 \pmod{3}$$

Selle lahendiks on $y \equiv 0 \pmod{3}$ ehk siit saab lahendi $x \equiv 1 \pmod{9}$. Järgmiseks otsin lahendit kujul $x = 2 + 3y$. Kuna $f(2) = 138$ ja $f'(1) = 28 \equiv 1 \pmod{3}$, tuleb lahendada lineaarkongruents

$$1 \cdot y + \frac{138}{3} \equiv 0 \pmod{3}$$

Selle lahendiks on $y \equiv 2 \pmod{3}$ ehk siit saab lahendi $x \equiv 2 + 3 \cdot 2 = 8 \pmod{9}$. Viimaks otsin lahendit kujul $x = 0 + 3y$. Kuna $f(0) = 6$ ja $f'(0) = 96 \equiv 0 \pmod{3}$, tuleb lahendada lineaarkongruents

$$0 \cdot y + \frac{6}{3} \equiv 0 \pmod{3}$$

Sellel puuduvad lahendid ehk siit lahendeid juurde ei tule.

Nüüd vaatan võrrandit mooduli 5 järgi:

$$x^4 - 6x^3 - 7x^2 + 96x + 6 \equiv -x^3 - 2x^2 + x + 2 \pmod{5}.$$

Läbi proovides saab, et selle lahendid on 1, 3 ja 4. Leian järgmiseks lahendid mooduli 25 järgi. Otsin lahendit kujul $x = 1 + 5y$. Kuna $f(1) = 90$ ja $f'(1) = 68 \equiv 3 \pmod{5}$, tuleb lahendada lineaarkongruents

$$3 \cdot y + \frac{90}{5} \equiv 0 \pmod{5}$$

Selle lahendiks on $y \equiv 4 \pmod{5}$ ehk siit saab lahendi $x \equiv 1 + 4 \cdot 5 = 21 \pmod{25}$.

Järgmiseks otsin lahendit kujul $x = 3 + 5y$. Kuna $f(3) = 150$ ja $f'(3) = 0$, tuleb lahendada lineaarkongruents

$$0 \cdot y + \frac{150}{5} \equiv 0 \pmod{5}$$

See võrrand kehtib y väärtusest sõltumatult ehk kõik lahendid kujul $z \in \{3, 8, 13, 18, 23\}, x \equiv z \pmod{25}$ kehtivad.

Viimaks otsin lahendit kujul $x = 4 + 5y$. Kuna $f(4) = 150$ ja $f'(4) = 8 \equiv 3 \pmod{5}$, tuleb lahendada lineaarkongruents

$$3 \cdot y + \frac{150}{5} \equiv 0 \pmod{5}$$

Selle ainsaks lahendiks on $y \equiv 0 \pmod{5}$ ehk siit saab lahendi $x \equiv 4 \pmod{25}$.

Seega tulid mooduli 25 järgi lahendid $21, 3, 8, 13, 18, 23, 4$. Vaatan ka lahendeid mooduli 125 järgi. Kõigepealt otsin lahendit kujul $x = 21 + 25y$. Kuna $\frac{f(21)}{5^2} = 5514 \equiv 4 \pmod{5}$ ja $f'(21) = 28908 \equiv 3 \pmod{5}$, tuleb lahendada kongruents $3y + 4 \equiv 0 \pmod{5}$, mille ainsaks lahendiks on $y \equiv 2 \pmod{5}$ ehk $x \equiv 71 \pmod{125}$.

Järgmiseks otsin lahendit kujul $x = z + 25y$, kus $z \in \{3, 8, 13, 18, 23\}$. Kuna iga z väärtuse puhul $f'(z) \equiv 0 \pmod{5}$, saab siin olla lahendeid vaid juhul, kui kehtib $\frac{f(z)}{5^2} \equiv 0 \pmod{5}$. Vaatlen neid:

z	3	8	13	18	23
$\frac{f(z)}{25}$	6	54	618	2778	238214

Ükski saadud arvudest ei jagu arvuga 5 ehk siit lahendeid ei tule. Otsin veel lahendit kujul $x = 4+25y$. Kuna $\frac{f(4)}{5^2} = 6 \equiv 1 \pmod 5$ ja $f'(4) = 8 \equiv 3 \pmod 5$, tuleb lahendada kongruents $3y + 1 \equiv 0 \pmod 5$, mille ainsaks lahendiks on $y \equiv 3 \pmod 5$ ehk $x \equiv 79 \pmod{125}$.

Seega olen leidnud lahendid $x \equiv 8 \pmod 9$ ja $x \equiv 1 \pmod 9$ ning $x \equiv 71 \pmod{125}$ ja $x \equiv 79 \pmod{125}$. Kuna ringis $\mathbb{Z}_9$ on $\overline{125}^{-1} = \overline{8}$ ja ringis $\mathbb{Z}_{125}$ on $\overline{9}^{-1} = 14$, saab HJT põhjal lahendid kombineerida pannes need sisse valemisse $x = a \cdot 125 \cdot 8 + b \cdot 9 \cdot 14$, kus a on lahend mooduli 9 järgi ning b on lahend mooduli 125 järgi. Kui nii lahendid välja arvutada, saab et mooduli 1125 järgi on lahenditeks 71, 829, 946 ja 1079.

9. Teha kindlaks, kas mooduli n järgi leidub algjuuri ning kui leidub, siis leida nende arv ja üks algjuur, kui

a) $n = 2661$, b) $n = 2662$, c) $n = 2663$, d) $n = 2664$.

a) $2661 = 3 \cdot 887$, seega algjuuri ei leidu.
b) $2662 = 2 \cdot 11^3$, seega algjuuri leidub.
c) 2663 on algarv ehk algjuuri leidub.
d) $2664 = 4 \cdot 666$, seega algjuuri ei leidu.

10. Leida kõik algarvud p, mille järgi eksisteerib täpselt 32 algjuurt.

Algarvul p on $\varphi(\varphi(p)) = \varphi(p-1)$ algjuurt ehk leian kõik arvud n, mille puhul $\varphi(n) = 32$ ning kontrollin kas $n+1$ on algarv. Kui arvu n algtegurdus on $n = q_1^{k_1} q_2^{k_2} .. q_s^{k_s}$, siis $\varphi(n) = q_1^{k_1-1}(q_1-1) \cdot q_2^{k_2-1}(q_2-1) \cdot .. \cdot q_s^{k_s-1}(q_s-1)$. Kuna $32 = 2^5$, ei jaga ükski kahest suurem algarv arvu 32 ehk arvu n tegurites saavad kahest suuremad arvud olla ülimalt astendajaga 1. Kuna 32 tegurid on $2, 4, 8, 16, 32$, saaksid n algtegurite hulgas olla arvud $2+1 = 3, 4+1 = 5, 8+1 = 9, 16+1 = 17, 32+1 = 33$, kuid nendest sobivad vaid $3, 5, 17$ kuna teised pole algarvud. Leian kõik võimalikud n väärtused (2 on alati tegurite hulgas kuna $n+1$ peab lõpuks algarv olema ehk n on kas paarisarv või 1 ning $\varphi(1) \neq 32$):

Binaararv näitamaks, kas arv on tegurite hulgas				$\varphi(n)$	n
2	3	5	17		
1	0	0	0	$2^{k-1} = 32$	64
1	0	0	1	$2^{k-1}(17-1) = 32$	68
1	0	1	0	$2^{k-1}(5-1) = 32$	80
1	0	1	1	$2^{k-1}(5-1)(17-1) = 32$	ei leidu
1	1	0	0	$2^{k-1}(3-1) = 32$	96
1	1	0	1	$2^{k-1}(3-1)(17-1) = 32$	102
1	1	1	0	$2^{k-1}(3-1)(5-1) = 32$	120
1	1	1	1	$2^{k-1}(3-1)(5-1)(17-1) = 32$	ei leidu

Leitud n väärtustest on vaid 96 ja 102 sellised, et $n+1$ oleks algarv ehk sobivad algarvud on 97 ja 103.

11. Tõestada, et iga naturaalarvude paari (a, b) korral leidub naturaalarv n nii, et arvul $n^2 + an + b$ on vähemalt 2021 jagajat. (Vihje: $n^2 + an + b \equiv 0 \pmod p \iff a^2 - 4b$ on ruutjääk mooduli p järgi.)

Kui $a^2 - 4b$ on ruutjääk mooduli p järgi, ning $p > 2$, siis saame leida $n = (-a \pm \sqrt{a^2 - 4b})2^{-1}$, mille asendades valemisee $n^2 + an + b$, saame, et $n^2 + an + b \equiv 0 \pmod p$. Nüüd märkame ,et tähistades ümber $x := a^2 - 4b$, siis teame, et algarve kujul $1 + 4x$ on lõpmata palju. Siit teame, et need algarvud annavad nii x kui ka 4 järgi jäägi 1. Lahutades x algteguriteks saame $(\frac{x}{p}) = (\frac{q_1}{p}) \cdot ... \cdot (\frac{q_s}{p})$. Kui mõni neist algteguritest on p, siis saame korrutiseks 0, mis tähendaks, et $\sqrt{x} \equiv 0 \pmod p$, mis n leidmiseks mooduli p järgi on piisav. Kuna $p \equiv 1 \pmod 4$, saame need legendre'i sümbolid ümber pöörata, saades korrutise $(\frac{p}{q_!}) \cdot ... \cdot (\frac{p}{q_s})$. Kuna $p \equiv 1 \pmod x$, siis peab ka iga x algteguri korral kehtima, et $p \equiv 1 \pmod q$. Seega saame enda korrutises kõik Legendre'i sümbolid väärtustada ühtedega saades korrutiseks ühe. Seega on x ruutjääk mooduli p järgi siis, kui p on kujul $1 + 4x$. Nüüd peame lihtsalt valima 2021 sellist p, leidma iga ühe järgi ühe sobiva n ning need HJT järgi kokku panema üheks suureks n-ks, mille järgi saabki arvutada sobiva $n^2 + an + b$.

12. Kasutades loengukonspekti näites 9.8 toodud skeemi kaheksatäheliste (st. kuueteistnumbriliste) blokkide jaoks ja mooduli väiksust, dekodeerida avaliku võtmega $(9591149766518863, 2021)$ kodeeritud RSA sõnum

$$3358877268877051858078669576983881577303967231 43.$$

Avalikus võtmes oleva n lahti tegurdades saan $n = 9591149766518863 = 97435691 \cdot 98435693$ ehk $\varphi(n) = (97435691 - 1) \cdot (98435693 - 1) = 9591149570647480$. Kuna salajane astendaja on avaliku astendaja pöördarv mooduli $\varphi(n)$, saan leida salajase astendaja: $d \equiv 2021^{-1} \equiv 2026432888009141 \pmod{9591149570647480}$. Lõpuks jagan sõnumi blokkideks ja astendan need salajase astendajaga mooduli n järgi:

$$\begin{aligned}
3358877268877051^{2026432888009141} &\equiv 12\ 15\ 16\ 16\ 00\ 08\ 05\ 01 \pmod{9591149766518863}\\
8580786695769838^{2026432888009141} &\equiv 00\ 11\ 15\ 09\ 11\ 00\ 08\ 05 \pmod{9591149766518863}\\
8157730396723143^{2026432888009141} &\equiv 01\ 00\ 05\ 11\ 19\ 15\ 12\ 05 \pmod{9591149766518863}
\end{aligned}$$

Ehk sõnumi on "lopp hea koik hea eksole".