Kodutöö nr. 10

Joosep Näks ja Uku Hannes Arismaa

1. Leida elementide $\overline{9}$, $\overline{19}$, $\overline{29}$, $\overline{39}$, $\overline{40}$ ja $\overline{41}$ järgud rühmas $U(\mathbb{Z}_{58})$. Kas mõni arvudest 9, 19, 29, 39, 40 või 41 on algjuur mooduli 58 järgi?

Tegurdades saame $\varphi(58) = 28 = 2^2 \cdot 7$. Paneme tähele, et $\overline{19}^4 = \overline{53}$ ning $\overline{19}^{14} = \overline{-1}$, seega $\overline{19}$ on algjuur ehk tema järk on 28.
$\overline{29}$ ei kuulu sellesse rühma, kuna pole pööratav.
Paneme tähele, et $\overline{19}^{15} = \overline{39}$, seega kuna $(15, 28) = 1$, on $\overline{39}$ algjuur ning järguga 28.
$\overline{40}$ ei kuulu sellesse rühma, kuna pole pööratav.
Paneme tähele, et $\overline{19}^7 = \overline{41}$, seega kõige varem $\overline{41}^4 = \overline{1}$ ning $\overline{41}$ järk on 4.
Paneme tähele, et $\overline{19}^{26} = \overline{9}$, seega kõige varem $\overline{9}^{14} = \overline{1}$ ning $\overline{9}$ järk on 14.

2. Olgu meil 40-st mängukaardist koosnev kaardipakk (näiteks šveitsi regionaalsest kaardimängust *Kaiserspiel*). Nummerdame kaardid ülemisest alumiseni numbritega $1, 2, \ldots, 40$. Võtame pakist ülemise poole ja asetame lauale alumisest poolest paremale. Moodustame uue kaardipaki, võttes järjest ülemisi kaarte vasakpoolsest ja parempoolsest pakist. Sellisel viisil kaardipaki segamist illustreerib järgmine tabel:

koht vanas pakis	1	2	3	...	20	21	22	23	24	...	40
koht uues pakis	2	4	6	...	40	1	3	5	7	...	39

.

Mitu korda peab pakki niimoodi segama, et kaardid oleksid jälle esialgses järjekorras?

Märkan, et segamine on ekvivalentne kujutusega $f(\overline{a}) = \overline{2a}$ ringis $\mathbb{Z}_{41}$, kuna esimesed 20 kohta uues pakis saavad lihtsalt väärtuse vanast pakist kaks korda suuremalt asukohalt, uue paki teise poole jaoks vaatlen, mis nende väärtustega juhtuks leitud kujutuse puhul. Kuna need väärtused on suuremad, kui $\frac{41}{2}$, tuleb neist lahutada 41 vähemalt üks kord et saada vähim naturaalarvuline $\mathbb{Z}_{41}$ esindaja, ning rohkem kui üks kord pole vaja lahutada kuna suurim tekkiv arv on $40 \cdot 2 < 41 \cdot 2$. Seega saan $f(20 + a) = 2(20 + a) - 41 = 2a - 1$, mis annabki paarituid arve, nagu vaja.
Kuna on vaja leida, mitu korda kujutust rakendada tuleb, et saavutada algne element, taandub ülesanne elemendi 2 järgu leidmisele. Vaatlen 2 astmeid:

k	0	1	2	3	4	5	6	7	8	9	10
$\overline{2^k}$	1	2	4	8	16	-9	-18	5	10	20	-1

On lihtne näha, et edasi järgmised 10 väärtust tabelis on samade arvude vastandarvud ning seega esimene kord kui 1 tuleb tulemuseks, on 2^{20} ehk 2 järk on 20 ning pakki tuleb ka segada 20 korda antud meetodil et saada algse järjestusega pakk tagasi.

3. Näidata otse, **kõiki** jäägiklassiringi $\mathbb{Z}_{30}$ elemente järjest astendades, et mooduli 30 järgi ei leidu algjuuri.

Paneme tähele, et $\overline{7}^4 = \overline{1}$, seega on selle järk liiga väike, et olla algjuur.
Paneme tähele, et $\overline{11}^2 = \overline{1}$, seega on selle järk liiga väike, et olla algjuur.
Paneme tähele, et $\overline{13}^4 = \overline{1}$, seega on selle järk liiga väike, et olla algjuur.
Paneme tähele, et $\overline{17}^4 = \overline{1}$, seega on selle järk liiga väike, et olla algjuur.
Paneme tähele, et $\overline{19}^2 = \overline{1}$, seega on selle järk liiga väike, et olla algjuur.
Paneme tähele, et $\overline{23}^4 = \overline{1}$, seega on selle järk liiga väike, et olla algjuur.
Paneme tähele, et $\overline{29}^2 = \overline{1}$, seega on selle järk liiga väike, et olla algjuur.
Teised $\mathbb{Z}_{30}$ elemendid ei ole pööratavad ehk ei saa olla algjuured.

4. Leida kõik algjuured moodulite 8, 9, 12, 14 ja 18 järgi.

Tegurdan moodulid: $8 = 2^3$, $9 = 3^2$, $12 = 2^2 \cdot 3$, $14 = 2 \cdot 7$, $18 = 2 \cdot 3^2$. Teoreemi 7.21 järgi leidub algjuuri vaid moodulite järgi, mis avalduvad kujul 2, 4, p^k või $2 \cdot p^k$, seega ei leidu moodulite 8 ja 12 järgi ühtegi moodulit.

Läbivaatlusel on näha, et mooduli 3 järgi on ainsaks algjuureks -1, seega teoreemi 7.14 järgi on 9 järgi vähemalt üks arvudest -1 ja $-1 + 3 = 2$ algjuur. On teada, et kui a on algjuur, siis a^k on algjuur parajasti siis, kui $(k, \varphi(m)) = 1$, kus m on moodul. Kuna $\varphi(9) = 6$ ja ainsad sobivad arvud, mis on väiksemad kui 6, on 1 ja 5. Seega on algjuured $\overline{2^1} = \overline{2}$ ja $\overline{2^5} = \overline{5}$.

Mooduli 14 jaoks leian kõigepealt mooduli 7 järgi algjuure. Et $\varphi(7) = 6 = 2 \cdot 3$, on element a algjuur parajasti siis, kui $a^2 \not\equiv 1 \pmod 7$ ja $a^3 \not\equiv 1 \pmod 7$. Hakkan läbi proovima: $2^2 = 4$, $2^3 \equiv 1 \pmod 7$ ehk 2 ei sobi, $3^2 \equiv 2 \pmod 7$ ja $3^3 \equiv -1 \pmod 7$ ehk 3 on algjuur. Mooduli 14 järgi on üks algjuur seega paaritu arv arvudest 3 või $3 + 7 = 10$ ehk 3. Kuna jällegi $\varphi(14) = 6$, on arvuga 6 suurim ühistegur arvudel 1 ja 5 ehk algjuurteks $\overline{3}$ ja $\overline{3^5} = \overline{5}$.

Leidsin juba, et mooduli 9 järgi on algjuured 2 ja 5, ehk 18 järgi on üks algjuur $2 + 9 = 11$ ja teine 5 (kuna 2 on paarisarv ja 5 paaritu). Kõigi algjuurte kogus on aga $\varphi(\varphi(18)) = 2$ ehk 5 ja 11 ongi kõik algjuured.

5. Olgu $a \in \mathbb{Z}$, $m, n \geq 2$ kõik kolm paarikaupa ühistegurita. Tõestada, et elemendi $\overline{a}$ järk rühmas $U(\mathbb{Z}_{mn})$ on vähim ühiskordne tema järkudest rühmades $U(\mathbb{Z}_m)$ ja $U(\mathbb{Z}_n)$. Kas väide jääb kehtima, kui mõni eeldustest on rikutud?

Otsime vähimat x nii, et $\overline{a}^x = \overline{1}$ rühmas $U(\mathbb{Z}_{mn})$. See on samaväärne ülesandega $(\overline{a}^x, \overline{a}^x) = (\overline{1}, \overline{1})$ rühmas $U(\mathbb{Z}_m) \times U(\mathbb{Z}_n)$. Teoreemist 7.6 saame, et $\overline{a}$ järgud rühmades $U(\mathbb{Z}_m)$ ning $U(\mathbb{Z}_n)$ peavad jagama arvu x. Kuna otsime vähimat x, siis saamegi, et tegelikult otsisimegi nende järkude vähimat ühiskordset. Kui m või n on 1, siis kuna kõik $\overline{a}$ on $\mathbb{Z}_1$ esimest järku, saame, et otistav ühistegur on sama, mis $\overline{a}$ järk teises rühmas, ning nende rühmade otsekorrutis on ekvivalentne teise rühmaga, seega väide kehtib. Kui a ei ole m, n ühistegurita, ei saa ta kuuluda $U(\mathbb{Z}_{mn})$. Kui m, n pole ühistegurita, siis saame võttes $a = 3, m = 2, n = 2$, et $\overline{a}$ järk $U(\mathbb{Z}_2)$ on 1, $[1, 1] = 1$, aga $\overline{a}$ järk $U(\mathbb{Z}_{2 \cdot 2}) = 2$, mis on vastuolu.

6. Tõestada, et kui a on algjuur mooduli n järgi ja $ab \equiv 1 \pmod n$, siis ka b on algjuur mooduli n järgi (s.t. algjuure pöördväärtus on algjuur.)

Kui korrutada võrrandi $ab \equiv 1 \pmod n$ mõlemad pooled arvuga $(ab)^{k-1}$ läbi, kus k on positiivne täisarv, saame $(ab)^k \equiv 1 \pmod n$ ehk $a^k b^k \equiv 1 \pmod n$. Eeldame, et b ei ole algjuur. Sel juhul on tema järk m väiksem kui arvu a järk t, ehk $b^m \equiv 1 \pmod n$. Võttes teisendatud võrrandis $k = m$, saame et $a^m \cdot 1 \equiv 1 \pmod n$ ehk $a^m \equiv 1 \pmod n$, kuid definitsiooni järgi on t vähim naturaalarv, mille puhul kehtib $a^t \equiv 1 \pmod n$, ehk kuna $m < t$, oleme saanud vastuolu, nii et arvude a ja b järgud peavad samad olema, ehk kui a on algjuur, on ka b algjuur.

7. Kasutades fakti, et algarvulise mooduli järgi leidub algjuuri, tõestada
Wilsoni teoreem: $p \in \mathbb{N}$ on algarv siis ja ainult siis, kui

$$(p-1)! \equiv -1 \pmod{p}.$$

Kui p poleks algarv, leiduks sellel mingi sellest väiksem vähim algtegur, mis jagab nii p kui ka $(p-1)!$, mis tähendab, et $((p-1)!, p) \neq 1$, seega ei saa $(p-1)! \equiv -1 \pmod{p}$, kuna sellisel juhul oleks need ühistegurita.

Kui p on algarv, siis saame samaväärse väite $\overline{(p-1)!} = \overline{-1}$ $\mathbb{Z}_p$-s. Kuna p on algarv, on kõik $\mathbb{Z}_p \setminus \overline{0}$ elemendid pööratavad, seega ka mingi algjuure a mingid (unikaalsed) astmed. Saame $\overline{(p-1)!} = \overline{1} \cdot \overline{2} \cdot ... \cdot \overline{p-2} \cdot \overline{p-1} = \Pi_{i \in U(\mathbb{Z}_p)} i = \Pi_{i \in \{1,2,...,p-2,p-1\}} a^i = a^{\frac{p(p-1)}{2}}$. Kasutades fakti, et $a^{\frac{p-1}{2}} = \overline{-1}$, saame $a^{\frac{p(p-1)}{2}} = (-1)^p$, mis iga algarvu peale 2 korral on -1, kuid ringis $\mathbb{Z}_2$ on -1 ja 1 sama element, ehk võrrand siiski kehtib ka 2 puhul.

8. Olgu p algarv kujul $4k+3$ ja $a \in \mathbb{Z}$. Tõestada, et a on algjuur mooduli p järgi parajasti siis, kui $\overline{-a}$ järk rühmas $U(\mathbb{Z}_p)$ on $\dfrac{p-1}{2}$.

Olgu a algjuur mooduli p järgi. Märkan, et $(-a)^t = a^t \cdot (-1)^t$ ehk paarisarvuliste t väärtuste puhul on a^t ja $(-a)^t$ võrdsed ning paaritute väärtuste puhul vastandarvud. Seega saab $(-a)^t \equiv 1 \pmod{p}$ kehtida vaid juhul, kui $a^t \equiv 1 \pmod{p}$ või $a^t \equiv -1 \pmod{p}$. Märkan, et $\overline{a^{\frac{p-1}{2}}}$ on alati -1, sest $(-1)^2 = 1$ ehk -1 indeks on pool 1 indeksist ning kuna $\text{ind}_p 1 = p-1$, on ka $\text{ind}_p - 1 = \dfrac{p-1}{2}$. Seega esimene kord, kui a^t on -1 või 1 on juhul kui $t = \dfrac{p-1}{2} = \dfrac{4k+3-1}{2} = 2k+1$, mis on paaritu arv iga k väärtuse puhul, ehk $\overline{-a}$ järk on alati $\dfrac{p-1}{2}$.

Teistpidi eeldame et $\overline{-a}$ järk on $\dfrac{p-1}{2}$. Nagu enne näidatud, peab $\overline{(-a)^k}$ olema $\overline{1}$ või $\overline{-1}$, et saaks $\overline{a^k}$ olla 1. Kuna $\overline{(-a)^k} = 1$ sobib vaid juhul, kui k on $\dfrac{p-1}{2}$ kordne, saab $\overline{(-a)^k} = \overline{-1}$ kehtida vaid juhul kui k on $\dfrac{p-1}{4}$ kordne. Kuna $\dfrac{p-1}{2} = \dfrac{4k+3-1}{2} = 2k+1$, kehtib $\overline{1} = \overline{(-a)^{\frac{p-1}{2}}} = \overline{(-1)^{\frac{p-1}{2}}} \cdot \overline{a^{\frac{p-1}{2}}} = -\overline{a^{\frac{p-1}{2}}}$, saame et $\overline{a^{\frac{p-1}{2}}} = -1$ ehk ei saa kehtida $\overline{a^{\frac{p-1}{4}}} = 1$ (kuna poolte ruutu võtmisel saaks võrrandi, mis oleks eelmisega vastuolus), kuid kui $\overline{a^{\frac{p-1}{2}}} = -1$ pooled ruutu võtta, saab et $\overline{a^{p-1}} = 1$, ning kuna arvust $p-1$ väiksemaid $\dfrac{p-1}{4}$ kordseid pole, tähendab et a järk on $p-1$ ehk ta on algjuur.