

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?

2. Olgu meil 40-st mängukaardist koosnev kaardipakk (näiteks šveitsi regionaalsest kaardimängust *Kaiserspiel*). Nummerdame kaardid ülemisest alumiseni numbritega 1, 2, ..., 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?

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

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

Tegurdam 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?

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

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

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 $\frac{p-1}{2}$.

Olgu a algjuur mooduli p järgi. Siis tema järk on $\varphi(p) = p-1$. Kuna tegu on algarvuga kujul $4k+3$, on tegu paaritu arvuga, ehk $p-1$ on paarisarv. Tean, et -1 on \mathbb{Z}_p pööratav element, kuna $(p-1, p-2) = 1$, sest tegu on järjestike arvudega ning nende suurim ühistegur peaks jagama nende vahet ja ainus arv mis jagab arvu 1 on 1. Kuna a on algtegur, on arvud a^1, a^2, \dots, a^{p-1} kõik erinevad ning nende hulka kuulub ka -1 $(-1)^2 = 1$

9*. Leida kõik naturaalarvud n , mille korral $\frac{2^n + 1}{n^2}$ on täisarv.

10**. Olgu p algarv ja olgu iga naturaalarvu i korral r_i jääk, mis tekib arvu i^i jagamisel arvuga p . Tõestada, et jada (r_i) on perioodiline ja leida selle perioodi minimaalne pikkus.