

Arvuteooria 10. praktikumi ülesanded

1. Leia elementide $\overline{3}, \overline{4}, \overline{15}, \overline{47}, \overline{49}$ järgud rühmas $U(\mathbb{Z}_{50})$. Kas mõni arvudest $3, 4, 15, 47, 49$ on algjuur mooduli 50 järgi?
2. Olgu meil 52-st mängukaardist koosnev kaartide pakk. Nummerdame kaardid ülemisest alumiseni numbritega $1, 2, \dots, 52$. 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	...	26	27	28	29	30	...	52
koht uues pakis	2	4	6	...	52	1	3	5	7	...	51

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

3. Näita otse, jäägiklassiringi $\mathbb{Z}_{30}$ elemente järjest astendades, et mooduli 30 järgi ei leidu algjuuri.
4. Leia kõik algjuured moodulite 9, 10, 11, 12 ja 14 järgi.
5. Leia kõik naturaalarvud n , mille korral 2 ei ole algjuur mooduli 3^n järgi.
6. Olgu n täisarv ja olgu elemendi $a \in U(\mathbb{Z}_n)$ järk kl . Tõesta, et elemendi a^k järk on l .
7. Olgu $n, m \in \mathbb{N}$ ja tähistagu $P_n(x)$ elemendi $\bar{x}$ järk rühmas $U(\mathbb{Z}_n)$. Tõesta, et

$$P_n(a^m) = \frac{P_n(a)}{(m, P_n(a))}.$$

8. Kasutades fakti, et algarvulise mooduli järgi leidub alati algjuuri, tõesta *Wilsoni teoreem*, s.t. näita, et kui p on algarv, siis

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

- 9*. Tõesta, et naturaalarv $n > 1$ on algarv parajasti siis, kui leidub selline naturaalarv a , et $a^{n-1} \equiv 1 \pmod{n}$, aga $a^d \not\equiv 1 \pmod{n}$ kõigi arvu $n-1$ pärisjagajate d korral.
- 10**. Olgu p algarv ja olgu iga naturaalarvu i korral r_i jääk, mis tekib arvu i^i jagamisel arvuga p . Tõesta, et jada (r_i) on perioodiline ja leida selle perioodi minimaalne pikkus.

1. Rühma elemendi järgu definitsioon.
2. Vaadelda sobiva elemendi järku rühmas $U(\mathbb{Z}_{53})$.
3. Algjuure ja elemendi järgu definitsioonid. Lagrange'i teoreem.
4. Algjuure ja elemendi järgu definitsioonid. Järeldus 7.10.
5. Induktsioon. Vaata ka teoreemi 7.15 tõestus.
6. Lemma 7.3.
7. Lemma 7.3. Teoreemi 7.9 tõestus.
8. Teoreem 7.9. Lause 2.9. Lemma 7.3.