

Arvuteooria 10. praktikumi ülesanded:

Algjuured I.

1. Leida elementide $\overline{9}$, $\overline{25}$, $\overline{35}$, $\overline{37}$, $\overline{41}$, $\overline{42}$ ja $\overline{43}$ järgud rühmas $U(\mathbb{Z}_{82})$. Kas mõni arvudest 9, 25, 35, 37, 41, 42 või 43 on algjuur mooduli 82 järgi?
2. Olgu meil 96-st mängukaardist koosnev jaapani laste kaardimängu *iroha karuta* kaartide komplekt. Nummerdame kaardid ülemisest alumiseni numbritega $1, 2, \dots, 96$. 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	...	48	49	50	51	52	...	96
koht uues pakis	2	4	6	...	96	1	3	5	7	...	95

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

3. Näidata otse, **kõiki** jäägiklassiringi $\mathbb{Z}_{35}$ elemente järjest astendades, et mooduli 35 järgi ei leidu algjuuri.
4. Leida kõik algjuured moodulite 9, 10, 12, 13, 15 ja 18 järgi.
5. Olgu $a, n \in \mathbb{N}$, $a > 1$. Tõestada, et

$$n \mid \varphi(a^n - 1).$$

6. Leidugu mooduli n järgi algjuuri. Leida jääk, mis tekib kõigi erinevate algjuurte (mooduli n järgi) korrutise jagamisel arvuga n .
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 ja q paaritud algarvud ning $k, l \in \mathbb{N}$. Tõestada, et rühmas $U(\mathbb{Z}_{p^k q^l})$ leidub *täpselt* $[p-1, q-1]$ järku element.

9*. Olgu p algarv kujul $p = 3k + 2$, $k \in \mathbb{N}$. Tõestada, et kuupfunktsioon $f(\bar{x}) = \bar{x}^3$ on jäägiklasside hulga $\mathbb{Z}_p$ permutatsioon, mis on paaris parajasti siis, kui $p \equiv 3 \pmod{4}$.

10**. Tõestada, et kui p on “piisavalt suur” algarv, siis leidub algjuur a mooduli p järgi nii, et $1 < a < p$ ja $(a, p-1) = 1$.