Arvuteooria 9. praktikumi ülesanded: Algjuured I.

1. Leida elemendi a) $\overline{6}$, b) $\overline{15}$, c) $\overline{19}$, d) $\overline{21}$ järk rühmas $U(\mathbb{Z}_{22})$. Kas mõni arvudest $6, 15$, 19 või 21 on algjuur mooduli 22 järgi?

2. Olgu meil 36-st mängukaardist koosnev kaardipakk. Nummerdame kaardid alumisest ülemiseni numbritega $1, 2, \ldots, 36$. Võtame pakist ülemise poole ja asetame lauale alumisest poolest vasakule. Moodustame uue kaardipaki, võttes järjest alumisi kaarte vasakpoolsest ja parempoolsest pakist. Sellisel viisil kaardipaki segamist illustreerib järgmine tabel:

koht vanas pakis	1	2	3	...	18	19	20	21	22	...	36
koht uues pakis	2	4	6	...	36	1	3	5	7	...	35

.

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

3. Leida kõik algjuured moodulite 5, 9, 13 ja 15 järgi.

4. Näidata otse, $\mathbb{Z}_{15}$ elementide järke arvutades, et mooduli 15 järgi ei leidu algjuuri.

5. Näidata, et 2 on algjuur mooduli 29 järgi. Kasutada seda tulemust ja leida kongruentsi $x^7 \equiv 1 \pmod{29}$ kõik lahendid.

6. Tõestada, et kui a on algjuur mooduli p järgi ja $ab \equiv 1 \pmod{p}$, siis ka b on algjuur mooduli p järgi (s.t. kui $\overline{a} \in U(\mathbb{Z}_p)$ on algjuur, siis ka $\overline{a}^{-1} \in U(\mathbb{Z}_p)$ on algjuur.)

7. Tõestada, et kui p on paaritu algarv ja $a \in \mathbb{Z}$ on algjuur mooduli p järgi, siis $a^{\frac{p-1}{2}} \equiv -1 \pmod{p}$.

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

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

9*. Olgu $n \geq 3$ ja a paaritu naturaalarv. Leida $a^{2^{n-2}}$ jäägiklass mooduli 2^n järgi.

10*. Tõestada, et leidub lõpmata palju algarve, millel on kuju $4k+1$, kus $k \in \mathbb{N}$.