Kevad 2014

Arvuteooria 9. praktikumi ülesanded:

Algjuured I.

1. Leida elemendi a) $\overline{8}$, b) $\overline{9}$, c) $\overline{11}$, d) $\overline{21}$ järk rühmas $U(\mathbb{Z}_{26})$. Kas mõni arvudest $8, 9$, 11 või 21 on algjuur mooduli 26 järgi?

2. Olgu meil 52-st mängukaardist koosnev kaardipakk. Nummerdame kaardid ülemisest alumiseni numbritega $1, 2, \ldots, 52$. 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. Leida kõik algjuured moodulite 7, 8, 9, 10 ja 11 järgi.

4. Näidata otse, $\mathbb{Z}_{12}$ elementide järke välja arvutades, et mooduli 12 järgi ei leidu algjuuri.

5. Näidata, et 3 on algjuur mooduli 43 järgi. Kasutada seda tulemust ja leida kongruentsi $x^7 \equiv 1 \pmod{43}$ kõik lahendid.

6. Olgu p algarv ja a algjuur mooduli p^2 järgi. Tõestada, et siis a on algjuur ka mooduli p järgi.

7. Olgu p algarv kujul $4k + 1, k \in \mathbb{N}$. Tõestada, et a on algjuur mooduli p järgi siis ja ainult siis, kui $-a$ on algjuur mooduli p järgi. Tuua mõni näide sellistest algjuurtest.

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

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

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

10*. Tõestada, 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.

11*. 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.