Arvuteooria 10. praktikumi ülesanded:

Algjuured I.

1. Leida elementide $\overline{7}$, $\overline{11}$, $\overline{15}$ ja $\overline{21}$ järgud rühmas $U(\mathbb{Z}_{22})$. Kas mõni arvudest $7, 11$, 15 või 21 on algjuur mooduli 22 järgi?

2. Olgu meil 40-st mängukaardist koosnev kaardipakk (näiteks šveitsi regionaalsest kaardimängust *Kaiserspiel*). Nummerdame kaardid ülemisest alumiseni numbritega $1, 2, \ldots, 40$. 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, jäägiklassiringi $\mathbb{Z}_{16}$ elemente järjest astendades, et mooduli 16 järgi ei leidu algjuuri.

4. Leida kõik algjuured moodulite 9, 10, 11, 12 ja 14 järgi.

5. Olgu n täisarv ja olgu elemendi $\overline{a} \in U(\mathbb{Z}_n)$ järk kl. Tõestada, et elemendi $\overline{a}^k$ järk on l.

6. Tõestada, et iga naturaalarvu $n > 1$ korral $n \mid \varphi(2^n - 1)$.

7. Olgu $p > 2$ algarv ja n naturaalarv, kusjuures $p - 1 \nmid n$. Tõestada, et

$$1^n + 2^n + 3^n + \ldots + (p-1)^n \equiv 0 \pmod{p}.$$

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

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

9*. 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.

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.

Ajapäevik: 10. nädal

Aeg	Tegevus	Kommentaarid