

Arvuteooria 10. praktikumi ülesanded:

Algjuured I.

1. Leida elementide $\overline{17}$, $\overline{19}$, $\overline{21}$, $\overline{23}$ ja $\overline{33}$ järgud rühmas $U(\mathbb{Z}_{34})$. Kas mõni arvudest 17, 19, 21, 23 või 33 on algjuur mooduli 34 järgi?

2. Olgu meil hispaania stiilis mängukaartide pakk 48 kaardiga. Numbridame kaardid ülemisest alumiseni numbritega 1, 2, ..., 48. 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	...	24	25	26	27	28	...	48
koht uues pakis	2	4	6	...	48	1	3	5	7	...	47

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

3. Näidata otse, jäägiklassiringi \mathbb{Z}_{24} elemente järjest astendades, et mooduli 24 järgi ei leidu algjuuri.

4. Leida kõik algjuured moodulite 10, 11, 12, 14, 16 ja 18 järgi.

5. Tõestada, et $\frac{p-1}{2}$ on algjuur algarvulise mooduli $p > 2$ järgi parajasti siis, kui $2 \cdot (-1)^{\frac{p-1}{2}}$ on algjuur mooduli p järgi.

6. Tõestada, et ühegi naturaalarvulise mooduli $n > 1$ järgi ei saa leiduda täpselt 118, 218 või 318 mooduli n järgi mittekongruentset algjuurt.

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

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

8. Olgu $p > 2$ algarv. Leida kõik sellised naturaalarvud k , mille korral summa $S_k = 1^k + 2^k + \dots + (p-1)^k$ jagub arvuga p .

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**. 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.