Kevad 2018

Arvuteooria 12. praktikumi ülesanded:

Algjuured III.

1. Leida arvu 9 indeks kõigil võimalikel alustel mooduli 17 järgi.

2. Koostada indeksite tabel alusel 7 mooduli 23 järgi.

3. Leida arvu 7 indeks alusel 5 mooduli 23 järgi. Kasutades saadud indeksit, koostada indeksite tabel alusel 5 mooduli 23 järgi.

4. Leida kõigi rühma $U(\mathbb{Z}_{29})$ elementide järgud ja kõik algjuured indeksite tabeli abil.

5. Lahendada kongruents $2016 \cdot x^{2018} \equiv 2020 \pmod{23}$ indeksite tabeli abil.

6. Milline kongruentsidest $8^{x^2} \equiv 3^2 \pmod{43}$ ja $8^{x^3} \equiv 3^3 \pmod{43}$ on lahenduv? Mis on selle lahendid?

7. Leida, milliste arvude $1 \leq a \leq 19$ korral on kongruents $x^4 \equiv a \pmod{p}$ lahenduv korraga moodulite 7, 13 ja 19 järgi.

8. Leidugu mooduli n järgi algjuuri. Tõestada, et arvul a on olemas ruutjuur mooduli n järgi (st $a \equiv b^2 \pmod{p}$) parajasti siis, kui a indeks mistahes alusel on paarisarv.

9*. Olgu $n > 1$ naturaalarv. Leida selliste arvuga n ühistegurita arvude m arv, mille korral $1 \leq m < n$ ja $m^{n-1} \equiv 1 \pmod{n}$.

10*. Tõestada, et $\prod_{a \in U(\mathbb{Z}_n)} a \equiv \begin{cases} 1 \pmod{n}, & \text{kui ei leidu algjuuri modulo } n, \\ -1 \pmod{n}, & \text{kui leidub algjuuri modulo } n. \end{cases}$