

Arvuteooria 12. praktikumi ülesanded:

Algjuured III.

1. Leida arvu 13 indeks *kõigil* võimalikel alustel mooduli 34 järgi.
2. Koostada indeksite tabel alusel 3 mooduli 29 järgi.
3. Leida $\text{ind}_{19} 3$ mooduli 29 järgi. *Kasutades saadud indeksit*, koostada indeksite tabel alusel 19 mooduli 29 järgi.
4. Leida kõigi rühma $U(\mathbb{Z}_{49})$ elementide järgud ja kõik algjuured mooduli 49 järgi indeksite tabeli abil. Kontrollida vastust ilma astendamist kasutamata.
5. Milline kongruentsidest $11^{x^2} \equiv 10^8 \pmod{49}$ ja $11^{x^3} \equiv 10^{12} \pmod{49}$ on lahenduv? Leida selle üldlahend.
6. Leida, milliste arvude $1 \leq a \leq 25$ korral on kongruents $x^{2026} \equiv a \pmod{n}$ lahenduv korraga *kõigi* moodulite $n = 13, 17, 25$ järgi.
7. Olgu $p \in \mathbb{P}$ ja $a \in \mathbb{Z}$. Öeldakse, et a on *Fibonacci algjuur* mooduli p järgi, kui a on algjuur mooduli p järgi ja $a^{k+2} \equiv a^{k+1} + a^k \pmod{p}$ iga $k \in \mathbb{N}_0$ korral. Tõestada, et kui a on Fibonacci algjuur ja algarv p on kujul $p = 4k + 3$, $k \in \mathbb{N}_0$, siis ka $a - 2$ on algjuur. Kas $a - 2$ on samuti Fibonacci algjuur?
8. Leidugu mooduli n järgi algjuuri. Leida $\prod_{\bar{b} \in U(\mathbb{Z}_n)} \text{ind } b \pmod{n}$.
- 9*. Olgu $p > 2$ algarv ja A rühma $\mathbb{Z}_p^*$ alamrühm, kusjuures $6 \mid |A|$. Tõestada, et leiduvad $a, b, c \in A$ nii, et $a + b = c$.
- 10*. Olgu $n \in \mathbb{N}$. Tõestada, et leidub lõpmata palju selliseid algarve p , et mooduli p järgi vähima positiivse algjuure a jaoks kehtib $a > n$.