

Arvuteooria 11. praktikumi ülesanded

1. Leia kõik algjuured mooduli 29 järgi.
2. Tee kindlaks, kas mooduli n järgi leidub algjuuri ning kui leidub, siis leia nende arv ja üks algjuur, kui
a) $n = 50$, b) $n = 53$, c) $n = 56$.
3. Tee kindlaks, kas mooduli n järgi leidub algjuuri ning kui leidub, siis leia nende arv ja üks algjuur, kui
a) $n = 484$, b) $n = 486$, c) $n = 488$.
4. Lahenda kongruents $1 + x + x^2 + x^3 + x^4 + x^5 + x^6 \equiv 0 \pmod{29}$.
5. Tõesta, et kui g on algjuur mooduli $p \in \mathbb{P}$, $p \neq 2$, järgi, siis kas g või g^2 on algjuur mooduli p^2 järgi.
6. Olgu p algarv ja $k, a \in \mathbb{N}$. Tõesta, et kui elemendi $\bar{a}$ järk mooduli p^k järgi on γ , siis elemendi $\bar{a}$ järk mooduli p^{k+1} järgi on kas γ või γp .
7. Olgu $p > 3$ algarv. Tõesta, et mooduli p järgi leidub iga algjuure a jaoks teine algjuur b nii, et $ab \equiv 1 \pmod{p}$.
8. Olgu p algarv kujul $4k+3$, $k \in \mathbb{N}$ ja olgu a algjuur mooduli p järgi. Tõesta, et $-a$ ei ole algjuur mooduli p järgi.
- 9*. Tõesta, et iga algarvu p korral on jadas $1 + p, 1 + 2p, 1 + 3p, \dots$ lõpmata palju algarve.
- 10** . Tõesta, et iga naturaalarvu n korral on jadas $1 + n, 1 + 2n, 1 + 3n, \dots$ lõpmata palju algarve.

1. Järeldused 7.21 ja 7.10.
2. Teoreem 7.18 ja vastavad tulemused 7.9 – 7.24.
3. Teoreem 7.18 ja vastavad tulemused 7.9 – 7.24.
4. Korrutades sobiva esimese astme polünoomiga viia polünoom lihtsamale kujule. Kasutada teoreemi 7.9 tõestus (K_d hulkade kohta).
5. Väide ei kehti. Leia kontranäide (piisab vaadata juhtu $p = 3$). Vaata algjuure definitsioon.
6. Järgu definitsioon ja teoreemi 7.15 tõestuses esinevate argumentidega sarnased arutelud.
7. Algjuure definitsioon.
8. Vaadata, millal need algjuured moodustaksid elementi $\overline{-1}$. Algjuure ja järgu definitsioonid.