# Algjuurte leidmine

Joosep Näks

Tartu Ülikool

April 8, 2021

## Teoreem 7.19

*Kui $a$ on algjuur mooduli $p^k$ järgi, kus $p > 2$ on algarv, siis üheks algjuureks mooduli $2p^k$ järgi on paaritu arv arvudest $a$ ja $a + p^k$.*

**Tõestus:** Eeldame et $a$ on paaritu (vastasel juhul toimib analoogselt arvuga $a + p^k$). Kuna $\overline{a}$ on algjuur $p^k$ järgi, on ta $\mathbb{Z}_{p^k}$ pööratav element ehk $(a, p^k) = 1$. Samuti $(a, 2) = 1$. Seega $(a, 2p^k) = 1$ ehk $\overline{a} \in U(\mathbb{Z}_{2p^k})$. Kuna $a$ on algjuur mooduli $p^k$ järgi, on $\overline{a}$ järk $U(\mathbb{Z}_{p^k})$ rühmas $m = |U(\mathbb{Z}_{p^k})| = p^{k-1}(p-1)$. Olgu $n$ elemendi $\overline{a}$ järk rühmas $U(\mathbb{Z}_{2p^k})$, siis $n||U(\mathbb{Z}_{2p^k})| = p^{k-1}(p-1) = m$ ehk $n \leq m$.
Teiselt poolt $a^n \equiv 1 \pmod{2p^k} \Rightarrow a^n \equiv 1 \pmod{p^k}$ ehk lemma 7.6 põhjal $m \leq n$. Seega kehtib $n = m$, mis tähendabki et $a$ on algjuur mooduli $2p^k$ järgi. □

## Teoreem 7.21

*Mooduli $n$ järgi leidub algjuuri parajasti siis, kui $n$ on kujul $2, 4, p^k$ või $2p^k$, kus $p > 2$ on algarv.*

**Tõestus:** Ühtepidi tuleb lausest 7.11, et kui $n$ järgi leidub algjuuri, on $n$ sellisel kujul.
Teistpidi järelduse 7.13 põhjal leidub algarvulise mooduli $p$ järgi $\varphi(p-1)$ algjuurt, mis on rohkem kui 0.
Kui juba $p$ järgi on algjuur olemas, aitab teoreem 7.14 leida $p^2$ järgi algjuure, teoreem 7.18 $p^k$ järgi ja teoreem 7.19 $2p^k$ järgi algjuure.
Seega kui $n$ on sellisel kujul, leidub tema järgi algjuuri. □

## Lemma 7.22

*Olgu $G$ lõplik rühm, mille järk $|G| = n = p_1^{k_1}...p_s^{k_s}$ on antud standardkujul. Iga $a \in G$ korral, $\langle a \rangle \neq G$ parajasti siis, kui leidub selline $i \in \{1, ..., s\}$, et $a^{\frac{n}{p_i}} = 1$.*

**Tõestus:**

Tarvilikkus: Oletame et $\langle a \rangle \neq G$. Olgu $m$ elemendi $a$ järk. Siis $m|n$ ning seega $m = p_1^{l_1}...p_s^{l_s}$, kus $0 \leq l_i \leq k_i$ iga $i \in \{1, ..., s\}$ korral. Kuna $\langle a \rangle \neq G$, on $m < n$ ehk peab leiduma $i$, mille korral $l_i < k_i$. Sellisel juhul $m|\frac{n}{p_i}$ ja seega $a^{\frac{n}{p_i}} = 1$.

Piisavus: Olgu $a^{\frac{n}{p_i}} = 1$, siis lemma 7.6 põhjal elemendi $a$ järk jagab arvu $\frac{n}{p_i}$ ehk $a$ järk on väiksem kui $n$ ning järelikult $\langle a \rangle \neq G$. □

## Järeldus 7.23

*Olgu $G$ lõplik rühm, mille järk $|G| = n = p_1^{k_1}...p_s^{k_s}$ on antud standardkujul. Iga $a \in G$ korral $\langle a \rangle = G$ parajasti siis, kui iga $i \in \{1, ..., s\}$ korral $a^{\frac{n}{p_i}} \neq 1$.*

## Järeldus 7.24

*Olgu $p > 2$ algarv. Siis $a$ on algjuur mooduli $p$ järgi parajasti siis, kui arvu $p - 1$ iga algteguri $q$ korral $a^{\frac{p-1}{q}} \not\equiv 1 \pmod{p}$.*

## Lause 7.26

*Olgu $n$ naturaalarv. Siis $n$-elemendilisel tsüklilisel rühmal on täpselt $\varphi(n)$ moodustajat.*

**Tõestus:**

Olgu $G = \{1, a, a^2, ..., a^{n-1}\}$ tsükliline rühm, kus $a^n = 1$. Esitame $n$ standardkujul $n = p_1^{k_1}...p_s^{k_s}$. Piisab näidata et iga $k \in \{1, ..., n\}$ korral $\langle a^k \rangle = G$ parajasti siis, kui $(k, n) = 1$. Tõestame selleks, et $\langle a^k \rangle \neq G$ parajasti siis, kui $(k, n) \neq 1$.

## Lause 7.26

*Olgu $n$ naturaalarv. Siis $n$-elemendilisel tsüklilisel rühmal on täpselt $\varphi(n)$ moodustajat.*

**Tõestus (jätk):**

Tarvilikkus: Eeldame, et $\langle a^k \rangle \neq G$. Lemma 7.22 põhjal leidub siis selline $i \in \{1, ..., s\}$, et $(a^k)^{\frac{n}{p_i}} = 1$ rühmas G. Lemma 7.6 põhjal $n | \frac{kn}{p_i}$ ehk leidub selline $u \in \mathbb{N}$ et $nu = \frac{kn}{p_i}$. Seega $up_i = k$, millest saame, et $p_i | k$. Seega $(n, k) \geq p_i > 1$.

Piisavus: Eeldame, et $(k, n) = d > 1$. Siis leidub selline $i \in \{1, ..., s\}$, et $p_i | d$ ning seega ka $p_i | k$. Olgu $k = p_i k'$, siis $(a^k)^{\frac{n}{p_i}} = a^{k'n} = (a^n)^{k'} = 1$ ehk lemma 7.22 põhjal $\langle a^k \rangle \neq G$. □

## Teoreem 7.27

*Kui mooduli $n$ järgi leidub algjuuri, siis on neid täpselt $\varphi(\varphi(n))$ tükki.*

**Tõestus:**

Jäägiklassiringi $\mathbb{Z}_n$ pööratavate elementide arv on Euleri funktsiooni definitsiooni põhjal $\varphi(n)$ ning rakendades lauset 7.26 rühma $U(\mathbb{Z}_n)$ peal saame, et algjuurte kogus on $\varphi(|U(\mathbb{Z}_n)|) = \varphi(\varphi(n))$. □

**Näide $2 \cdot 19^{2021}$ algjuure leidmisest:**

Leian kõigepealt ühe $19$ algjuure, pakun algjuureks 2.

$\varphi(19) = 19 - 1 = 18 = 2 \cdot 3^2$

$2^6 = 64 \equiv 7 \not\equiv 1 \pmod{19}$

$2^9 = 7 \cdot 2^3 = 56 \equiv -1 \not\equiv 1 \pmod{19}$

Seega 2 on algjuur mooduli 19 järgi. Algjuur $19^2$ järgi on $2$ või $2 + 19$.

$2^{19-1} = 2^9 \cdot 2^9 \equiv 151 \cdot 151 = 22801 \equiv 58 \not\equiv 1 \pmod{361}$

Ehk $2$ on algjuur ka $19^2$ järgi ning ka $19^{2021}$ järgi.

Kuna 2 on paarisarv, on $2 \cdot 19^{2021}$ järgi algjuur $2 + 19^{2021}$.