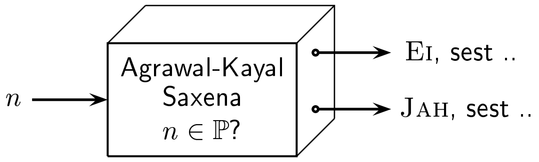
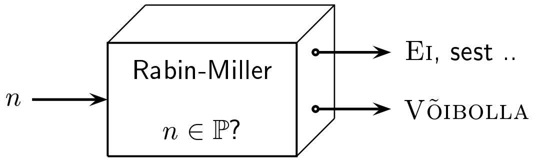
# Algarvulisuse testid

Sven Laur
swen@math.ut.ee

Tartu Ülikool




## Mõistete ja teadmiste kogumine

3. sajand e.m.a. Eukleides

– algarvulisuse mõiste
– suurima ühisteguri leidmise algoritm
– aritmeetika põhiteoreem

**Teoreem (Fermat 1640).**
*Kui arv $p$ on algarv, siis iga naturaalarvu $a$ korral vahe $a^p - a$ jagub arvuga $p$.*

□ Tõestati Euleri(1736) ja Leibnitzi(1683) poolt.

**Teoreem (Gauss 1792).**
*Algarvude arv $\pi(x)$ intervallis $[0, x)$ on asümptootiliselt ekvivalentne suurusega $x/\ln x$,*

□ Tõestus 1896.a. Hadamard ja de la Vallée-Poussin.

**Teoreem (Bertrand 1845).**
*Iga naturaalarvu $n > 3$ korral leidub lõigus $[n, 2n-2]$ vähemalt üks algarv.*

□ Tõestus 1851.a. Tšebõšev.

## Tänapäevased algarvutestid

- 1976. Diffie ja Hellmani võtmevahetusprotokoll.
  1977. Rivest, Shamiri ja Adleman RSA.

  – Praktiline vajadus suurte algarvude leidmiseks.

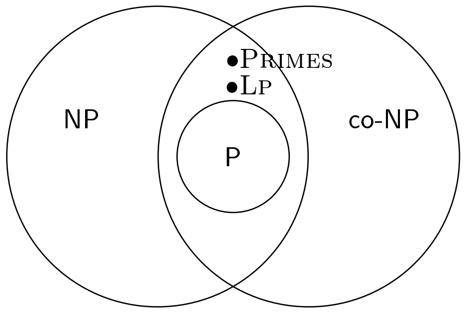
- 1977. Solovay ja Strassen tõenäosuslik algoritm
  – algarvu korral PRIME
  – kordarvu korral tõenäosusega vähemalt $1/2$ COMP
  – ei genereeri algarvulisuse tõestust
  – keerukus $\widetilde{O}(\log^2 n)$

- 1975-1980 Rabin-Milleri tõenäosuslik algoritm
  – algarvu korral PRIME
  – kordarvu korral tõenäosusega vähemalt $3/4$ COMP
  – ei genereeri algarvulisuse tõestust
  – keerukus $\widetilde{O}(\log^2 n)$

- 2002. Agrawal-Kayal-Saxena det. algoritm
  – algarvu korral PRIME
  – kordarvu korral COMPOSITE
  – genereerib alg- ja kordarvulisuse tõestused
  – garanteeritud keerukus $\widetilde{O}(\log^{12} n)$
  – arvatav keerukus $\widetilde{O}(\log^6 n)$

## Asetus keerukusklasside suhtes

- 70-nendate alguse levinud arusaam keerukusklasside vahekorrast.




- 1979. Khatšjan elliptiline lahendusmeetod LP -ülesande lahendamiseks, st. LP ∈ P.

- 1976. Milleri polünomiaalne algoritm eeldusel kehtib ERH.

- 2002. Agrawal, Kayal ja Saxena näitasid, et PRIMES ∈ P.

## Sertifikaadi mõiste

Väite tõestamine jaguneb
- tõestuse idee osimine
- tõestuse genereerimine
- tõestuse kontrollimine kolmanda osapoole poolt

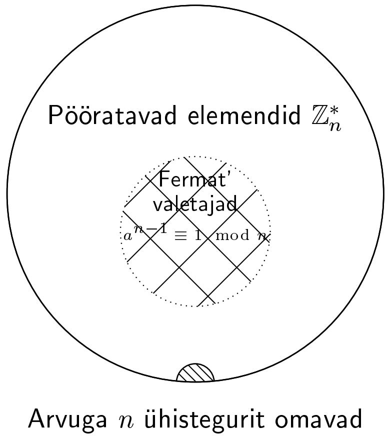
Kui algoritm annab välja vaid vastuseid Jah ja Ei
- pole võimalik vastust kontrollida
- vigade korral tuleb otsast alustada

**Definitsioon.** *Sertifikaadiks nimetatakse algoritmi väljundit, mis võimaldab vastust kontrollida, ilma et peaks kordama arvutusi täies mahus.*

- ☐ Sertifikaat põhineb harilikult mingil teoreemil.
- ☐ Sertifikaatide leidmise ja kontrollimise efektiivsus määrab ära algoritmi efektiivsuse.
- ☐ Keerulist probleemi lahendusalgoritm
  - potensiaalsete sertifikaatide genereerija
  - sertifikaadi kontrollija

## Fermat-Euleri test

**Teoreem.**
*Naturaalarv $n$ kordarv parajasti siis, kui leidub arv $a \in \mathbb{Z}_n^*$ nii, et $a^{n-1} \not\equiv 1 \mod n$.*




- Carmichaeli arvud muudavad testi kasutuks.

## Rabin-Milleri test

**Teoreem.**
*Kui naturaalarvu $n$ lahutusega $n-1 = 2^k r$ ($r$ on paaritu) korral leidub $a \in \mathbb{Z}_n^*$, mis täidab tingimusi*

$$\gcd(a,n) = 1$$
$$a^r \not\equiv 1 \mod n$$
$$a^{2^i r} \not\equiv -1 \mod n, \qquad i = 1, \dots, k-1$$

*siis $n$ on kordarv.*

- Arvutades $a^{n-1}$ tekib järjestikune ruutude jada

$$a^r, a^{2r}, a^{4r}, \dots, a^{2^{k-1} r}, a^{n-1} \equiv 1.$$

- Korpuses $\mathbb{Z}_p$ on igal arvul ülimalt kaks ruutjuurt.
- Kui jadas 1 eelnev arv pole $\pm 1$, siis on $n$ kordarv.
- Test väljastab iga kordarvu korral Prime tõenäosusega tõenäosusega vähem kui 1/4.

## Lihtne algarvulisuse sertifikaat

**Teoreem.** *Olgu naturaalarvud $a$ ja $n$ ühistegurita, siis $n$ on algarv parajasti siis, kui kehtib modulaarne võrdus*

$$(x-a)^n \equiv x^n - a^n \mod n.$$

Tõestus.
Tarvilikkus. Kui $n$ on algarv.

- Fermat' väikesest teoreemist $a^n \equiv a \mod n$.
- Iga $k \neq 0$ ja $k \neq n$ korral

$$n \,\Big|\, \binom{n}{k} = n \frac{(n-1)\cdots(n-k+1)}{k(k-1)\cdots 1}$$

Piisavus. Olgu teguri $q$ aste arvus $n$ on $k$.

- Kui $k = q$, siis

$$q^k \nmid \binom{n}{q} = \frac{n(n-1)\cdots(n-q+1)}{q(q-1)\cdots 1}$$

□

## Mõned järeldused

- Kongruentsvõrrandi kontrollimine võtab $\Omega(n)$ elementaaroperatsiooni.
- Selle põhjuseks on polünoomide astme tõkestamatu kasv.
- Võrrandis $(x-a)^n \equiv x^n - a^n \pmod{n,\ x^r - 1}$ kasvab aste kuni arvuni $r$.
- Eesmärgiks on leida sobiv $r = O(\mathrm{poly}(\log n))$, nii et kongruentsvõrrand kehtiks vaid algarvude korral.
- Ühest võrrandist ei piisa, kuid leidub sobilik võrrandite süsteem.

## Agrawal-Kayal-Saxena algoritm

**Sisend:** naturaalarv $n > 1$.
**Väljund:** PRIME või COMPOSITE.

*** Eraldame naturaalarvude täisastmed ***
**if** $(\exists a, b \in \mathbb{N} :\ a^b = n)$ **return** COMPOSITE;
$r = 2$;
*** Otsime Agrawal-Kayal-Saxena setrifikaati ***
**while** $(r < n)$
{
  *** Kui $\gcd(n, r) \neq 1$, siis on $n$ kordarv ***
  *** Selle sündmuse tõenäosus on kaduvväike ***
  **if** $(\gcd(n, r) \neq 1)$ **return** COMPOSITE;
  *** Kontrollime, kas $r$ on sobib sertifikaadiks ***
  **if** $(r \in \mathbb{P})$
  {
    $q = P(r-1)$;
    **if** $(q \geq 4\sqrt{r}\log n$ **and** $n^{(r-1)/q} \not\equiv 1 \mod r)$ **break**;
  }
  $r = r + 1$;
}
*** Kontrollime saadud sertifikaati ***
**for** $a = 1$ **to** $\lfloor 2\sqrt{r}\log n \rfloor$
{
  *** Kui $n$ on algarv, siis $a^n \equiv a \mod n$ ***
  **if** $((x-a)^n \not\equiv x^n - a \pmod{n, x^r - 1})$
    **return** COMPOSITE;
}
**return** PRIME;

## Agrawal-Kayal-Saxena sertifikaat

**Teoreem.**
*Olgu meid huvitav naturaalarv $n$, mis ei ole ühegi naturaalarvu $m$ aste. Kui $r$ on selline algarv, mis rahuldab kolme tingimust:*

- *iga algarv $s \leq r$ on arvuga $n$ ühistegurita,*
- *leidub $r-1$ algarvuline tegur $q \geq 4\sqrt{r}\log n$,*
- $q \mid \mathrm{ord}_r(n)$,

*siis $n$ on algarv parajasti siis, kui on täidetud kongruentside süsteem*

$$\begin{cases} (x-a)^n \equiv x^n - a^n \pmod{n, x^r - 1}, \\ \qquad a = 1, 2, \ldots, \lfloor 2\sqrt{r}\log n \rfloor. \end{cases}$$

TÕESTUS
TARVILIKKUS. Iga algarv rahuldab AKS-testi.

PIISAVUS. Selleks näitame, et kordarv, mis rahuldab AKS-testi on algarvu aste. Seda tehakse läbi kongruentside.

?

## Genereeritud alamrühm

- Leidub $n$ selline algarvuline tegur $p$ nii, et $q \mid d = \mathrm{ord}_r(p) \quad \Rightarrow \quad q \leq d$.
- Polünoomi $x^r - 1$ iga taandumatu teguri $h(x)$ üle $\mathbb{F}_p$ aste on $d$.
- Tekib lõplik korpus $\mathbb{F}_p[x]/(h(x))$ elementide arvuga $p^d$.
- Vaatleme elementide $x - a$ poolt genereeritud multiplikatiivset rühma

$$G = \left\{ \prod_{i=1}^{l} (x-i)^{\beta_i} \mid 0 \leq \beta_i, i = 1, 2 \ldots, l \right\}$$

- AKS-testis olevad lineaarpolünoomid $x - a$ ei saa mooduli $p$ järgi kokku langeda

$$\begin{aligned} & a_i \equiv a_j \mod p \\ \Rightarrow\quad & p \mid \gcd(a_i - a_j, n) \text{ ja } |a_i - a_j| < r \end{aligned}$$

- Vastuolu $r$ esimese tingimusega.

## Alamrühma generaatorpolünoom

- Alamrühma $G$ genererib $\lfloor 2\sqrt{r}\log n\rfloor < q < r < p$ erinevat polünoomi.

**Lemma.** *Olgu $r$ ja $p$ algarvud ning $d = \operatorname{ord}_r(p)$. Kui $h(x)$ on polünoomi $x^r - 1$ taandumatu tegur üle $\mathbb{F}_p$, siis $l < p$ erineva lineaarpolünoomi $x - a_i$ üle $\mathbb{F}_p$ poolt genereeritud rühm*

$$G = \left\{ \prod_{i=1}^{l} (x - a_i)^{\beta_i} \mid 0 \le \beta_i, i = 1, 2 \ldots, l \right\}$$

*on korpuses $\mathbb{F}_p[x]/\big(h(x)\big)$ tsükliline ja selle elementide arv $\#G > \left(\frac{d}{l}\right)^l$.*

- Seega leidub $G$ generaatorpolünoom $g(x)$ ning selle järk on

$$d_g \ge \left(\frac{q}{l}\right)^l = \left(\frac{4\sqrt{r}\log n}{\lfloor 2\sqrt{r}\log n\rfloor}\right)^{\lfloor 2\sqrt{r}\log n\rfloor} \ge n^{2\sqrt{r}}.$$

- Kuna $d_g \ge n^{2\sqrt{r}}$, siis hakkame otsima sobivat kongruentsi mooduli $d_g$ järgi.

## Polünoomi võrdsustate hulk

**Definitsioon 1.** *Polünoomi $g(x) \in \mathbb{F}_p$ võrdsustajatehulgaks mooduli $p$ ja polünoomi $x^r - 1$ suhtes nimetatakse hulka*

$$I_{g(x)} = \left\{ m \in \mathbb{N}_0 \mid g(x)^m \equiv g(x^m) \big(\operatorname{mod} p, x^r - 1\big) \right\}.$$

**Lemma.** *Polünoomi $g(x)$ võrdsustajate hulk $I_{g(x)}$ on kinnine korrutamise suhtes.*

**Lemma.** *Iga täisarvulise kordajatega polünoomi $f$ korral kehtib kongruents $f(x)^p \equiv f(x^p) \mod p$.*

- Generaatorpolünoomi $g(x)$ võrdsustajatehulka kuulub $n$, sest see on korrutis $x - a_i$ astmetest.

- Arvude $n$ ja $p$ poolt genereeritud hulk on võrdsustajas

$$E = \left\{ n^i p^j \mid 0 \le i, j \le \lfloor\sqrt{r}\rfloor \right\} \subseteq I_{g(x)}.$$

- Hulgas $E$ on rohkem kui $r$ elementi, seega leiduvad paarid

$$n^{i_1} p^{j_1} \equiv n^{i_2} p^{j_2} \mod r, \qquad i_1 \ne i_2 \text{ või } j_1 \ne j_2.$$

## Mooduli vahetus

- Meil on olemas kongruents mooduli $r$ järgi

$$n^{i_1} p^{j_1} \equiv n^{i_2} p^{j_2} \mod r, \qquad i_1 \ne i_2 \text{ või } j_1 \ne j_2.$$

aga vaja on kongruentsi mooduli $d_g$ järgi.

**Lemma 1.**
*Olgu nullist erineva polünoomi $g(x) \in \mathbb{F}_p[x]$ järk $d_g$ korpuses $\mathbb{F}_p[x]/\big(h(x)\big)$, kus $h(x) \mid x^r - 1$, ning $m_1, m_2 \in I_{g(x)}$, siis kongruentsist $m_1 \equiv m_2 \mod r$ järeldub $m_1 \equiv m_2 \mod d_g$.*

TÕESTUS.
- Kuna $m_1 \equiv m_2 \mod r$, siis $m_2 = kr + m_1$.

$$\begin{aligned} \Rightarrow \quad & g(x)^{m_2} \equiv g(x^{m_2}) \ \big(\operatorname{mod} p, h(x)\big) \\ & x^{kr} \equiv 1 \mod x^r - 1 \\ \Rightarrow \quad & g(x^{m_1 + kr}) \equiv g(x^{m_1}) \ \big(\operatorname{mod} p, h(x)\big). \end{aligned}$$

$$\begin{aligned} & g(x)^{m_1} g(x)^{kr} \equiv g(x)^{m_2} \equiv g(x^{m_1}) \ \big(\operatorname{mod} p, h(x)\big) \\ \Rightarrow \quad & g(x)^{kr} \equiv 1 \ \big(\operatorname{mod} p, h(x)\big). \end{aligned}$$

- Järgu omadustest $d_g \mid kr = m_2 - m_1$. □

## Oodatud vastuolu

- Teame, et polünoomi $g(x)$ järk $d_g \ge n^{2\sqrt{r}}$

- Teame, et kehtib kongruents

$$n^{i_1} p^{j_1} \equiv n^{i_2} p^{j_2} \mod d_g \quad i_1 \ne i_2 \text{ või } j_1 \ne j_2.$$

- Kuna $0 \le i_1, i_2, j_1, j_2 \le \lfloor\sqrt{r}\rfloor$, siis

$$p^{j_1}, p^{j_2} < n^{\sqrt{r}} \qquad\qquad n^{i_1}, n^{i_2} \le n^{\sqrt{r}}$$

- Seega on kongruentsi vasak ja parem pool väiksemad kui $d_g$.

- Kongurents taandub võrduseks

$$n^{i_1} p^{j_1} = n^{i_2} p^{j_2} \quad \Rightarrow \quad n^{i_1 - i_2} = p^{j_2 - j_1}$$

- Vastuolu $n$ on algarvu $p$ aste.

□

## Sertifikaadi leidumine

**Teoreem.**
*Leiduvad positiivsed konstandid $c_1$, $c_2$ ja $n_0$ nii, et iga naturaalarvu $n > n_0$ korral*
• *leidub intervallis $[c_1 \log^6 n, c_2 \log^6 n]$ algarv $r$, mille korral*
• *$r-1$ omab algarvulist tegurit $q \geq 4\sqrt{r}\log n$,*
• *$q$ jagab $n$ järku $\mathrm{ord}_r(n)$.*

- ☐ Läbi tuleb vaadata lõik, mis on polünomiaalne arvu $n$ pikkusest $\log n$ ja milles olevate arvude pikkus on $O(\log\log n)$
- ☐ See tähendab, et otsimiseks võib kasutada eksponentsiaalse keerukusega algoritme.
- ☐ Kui pole täidetud sertifikaadi esimene tingimus on arvul päristegur.
- ☐ Tõestus põhineb kahel arvuteoreetilisel hinnangul.

## Vajalikud teoreemid

**Teoreem.**
*Tähistagu $P(n)$ suurimat arvu $n$ algarvulist tegurit, siis leiduvad konstandid $\varepsilon > 0$ ja $n_0 \in \mathbb{N}$ nii, et kõigi $x \geq n_0$ korral järgmise hulga*

$$\mathcal{Q}_x = \left\{p \in \mathbb{P} \mid p \leq x,\ P(p-1) > x^{2/3}\right\}$$

*elementide arv $\#\mathcal{Q}_x \geq c\frac{x}{\log x}$.*

**Teoreem.**
*Tähistagu $\pi(n)$ algarvude arvu, mis on väiksemad kui $n$. Siis iga $n \in \mathbb{N}$ kehtivad võrratused*

$$\frac{n}{6\log n} \leq \pi(n) \leq \frac{8n}{\log n}.$$

## Tõestus ise

- Tõestuseks vaatame peaaegu sobivate algarvude hulka

$$\mathcal{R} = \Big\{r \in \mathbb{P} \,|r \in [c_1 \log^6 n, c_2 \log^6 n],$$
$$P(r-1) > (c_2 \log^6 n)^{2/3} > r^{2/3}\Big\}.$$

- Hindame alt hulga $\mathcal{R}$ elementide arvu

$$\begin{aligned}\#\mathcal{R} \geq& \#\mathcal{Q}_{c_2\log^6 n} - \pi(c_1 \log^6 n)\\ &\dots\\ \geq& c_3\frac{\log^6 n}{\log\log n},\ \text{kus } c_3 > 0.\end{aligned}$$

- Tähistame $x = c_2 \log^6 n$ ja vaatame korrutist

$$\Pi = (n-1)(n^2-1)\cdots(n^{\lfloor x^{1/3}\rfloor}-1).$$

- Selles on vähem kui $\log\Pi \approx x^{3/2}\log x = O(\log^5 n)$ tegurit.
- Hulgas $\mathcal{R}$ on $\widehat{O}(\log^6 n)$ elementi.

## Sertifikaadi kontrollimise keerukus

**Teoreem.**
*Olgu $r$ algarv intervallist $[c_1 \log^6 n, c_2 \log^6 n]$, siis kongruentside süsteemi*

$$\begin{cases}(x-a)^n \equiv x^n - a^n \pmod{n, x^r - 1},\\ \qquad a = 1, 2, \dots, \lfloor 2\sqrt{r}\log n\rfloor.\end{cases}$$

*kontrollimiseks kulub $\widetilde{O}(\log^{12} n)$ elementaaroperatsiooni.*

Tõestus. Anname ülehinnangu.

- Tsüklit läbitakse $O(\log^4 n)$ korda.
- Ühe astendamise tegemiseks kulub $O(\log n)$ korrutamist.
- Polünoomi korrutamiseks kulub $O(r^2) = O(\log^{12} n)$ ringi $\mathbb{Z}_n$ tehet.
- Üks tehe ringis $\mathbb{Z}_n$ võtab $O(\log^2 n)$ elementaar-operatsiooni.
- Kokku seega $O\left(\log^{4+1+12+2} n\right) = O(\log^{19} n)$. ☐

## Algoritmi keerukushinnang

**Teoreem.**
*Agrawal-Kayal-Saxena algoritm teeb $\widetilde{O}(\log^{12} n)$ elementaaroperatsiooniga kindlaks, kas naturaalarv $n$ on algarv või mitte.*

TÕESTUS.

- Võimalikke mõistlikke astmeid on $\log n$.
- Kasutades kahendotsingut on võimalik leida juure väärtus $O(\log n)$ väärtustamisega.
- Üks väärtustamine võtab ülimalt $O(\log b \log^2 n)$ elementaaroperatsiooni. Kokku $O(\log^{1+1+3} n)$.
- Sertifikaadi otsimisel läbitakse $\mathrm{while}$-tsüklit $O(\log^6 n)$ korda.
- Algarvulisuse kindlakstegemine kirvemeetodiga võtab $O(r^3) = O(\log^{18} n)$ elementaaroperatsiooni.
- Kokku seega $O\Big(\log^{6+18} n\Big) = O(\log^{24} n)$.
- Sertifikaadi kontrollimisel kulub $O(\log^{19})$. □

## Arvatav keerukushinnang

**Definitsioon.**
*Kui naturaalarvud $r$ ja $\frac{r-1}{2}$ on algarvud, siis nimetatakse neid Sophie Germain kaasalgarvudeks.*

- Kui $r$ ja $\frac{r-1}{2}$ on Sophie kaasalgarvud, siis arvu $n$ järk mooduli $r$ järgi võib olla:
  $+\ 1,\ 2,\ q,\ 2q$
- Ülimalt saab olla $\log(n^2 - 1) \leq 2 \log n$ halba Sophie kaasalgarvupaari.
- Seetõttu väheneb sertifikaadi otsimisel vaadatav vahemik $[2, c_2 \log^2 n]$.
- See omakorda viib summaarse keerukuse $\widetilde{O}(\log^6 n)$.

## Loodetav keerukushinnang

**Hüpotees.**
*Kui algarv $r$ ei jaga naturaalarvu $n$ ja kehtib kongruentsvõrdus*

$$(x-1)^n \equiv x^n - 1 \pmod{x^r - 1, n}$$

*siis kas $n$ on algarv või $n^2 \equiv 1 \mod r$.*

- Vaadatav lõik väheneb $[2, 4 \log n]$.
- Kontrollide tuleb vaadata vaid ühte võrdust.
- Keerukuseks tuleks $\widetilde{O}(\log^3 n)$.
- Rabin-Milleri keerukus $\widetilde{O}(\log^2 n)$.