TARTU ÜLIKOOL
Matemaatika-informaatikateaduskond
Matemaatika instituut

Ave Räni

Agrawali, Kayali ja Saxena teoreem algarvulisuse kohta

Bakalaureusetöö matemaatika erialal

Juhendaja: Valdis Laan, PhD

Tartu 2013

Sisukord

Sissejuhatus

Käesoleva bakalaureusetöö üldiseks valdkonnaks on arvuteooria. Juttu on algarvudest ning sellest, kuidas kontrollida algarvulisust. Eesmärgiks on uurida täpsemalt Agrawali, Kayali ja Saxena teoreemi selle kohta, kuidas teha kindlaks, kas antud arv on algarv või mitte. Teoreemi esitasid Manindra Agrawal, Neeraj Kayal ja Nitin Saxena aastal 2002 töös "PRIMES is in P". Antud bakalaureusetöö on referatiivne ning selles on kasutatud peamiselt Andrew Granville'i 2004. aastal ilmunud artiklit "It is easy to determine whether a given integer is prime", kus Andrew Granville kirjeldab erinevaid algarvulisuse testimise võimalusi ja esitab ka Agrawali, Kayali ja Saxena teoreemi ning selle tõestuse.

Töö koosneb 3 peatükist. Esimeses peatükis on ära toodud peamised definitsioonid ning mõned lihtsamad abiteoreemid. Teises peatükis esitatakse mõned teoreemid algarvude kohta, millel põhinevaid algoritme on algarvulisuse kontrollimiseks kasutatud enne Agrawali, Kayali ja Saxena teoreemi tõestamist. Töö põhitulemusena tõestatakse kolmandas peatükis Agrawali, Kayali ja Saxena teoreem algarvulisuse kohta.

Manindra Agrawal ja Neeraj Kayal on arvutiteadlased. Nitin Saxena aladeks on matemaatika ja teoreetiline arvutiteadus. Nende teoreemil põhinev algoritm on polünomiaalse keerukusega kontrollitava arvu numbrite arvu suhtes. Sellise keerukusega algoritmi algarvulisuse kontrollimiseks pole varem suudetud esitada. Algarvulisuse kiire kontrollimine on tähtis krüptograafias, mistõttu on see teoreem väga oluline.

1 Põhidefinitsioonid ja teoreemid

Kõigepealt esitame mõned põhidefinitsioonid ja teoreemid, mida kasutame käesolevas töös.

Definitsioon 1. Öeldakse, et täisarv a **jagab** täisarvu b ja tähistatakse $a \mid b$, kui leidub selline täisarv c, et $ac = b$.

Eeldame, et lugeja on tuttav täisarvude jaguvusseose omadustega ([5]).

Definitsioon 2. Algarvuks nimetatakse naturaalarvu $p > 1$, mille ainsad naturaalarvulised jagajad on 1 ja p.

Definitsioon 3. Rühmaks nimetatakse hulka A, millel on defineeritud üks kahekohaline algebraline tehe *, mis rahuldab tingimusi:

- $(\forall a, b, c \in A)((a * b) * c = a * (b * c))$,
- $(\exists e \in A)(\forall a \in A)(a * e = e * a = a)$,
- $(\forall a \in A)(\exists a^{-1} \in A)(a * a^{-1} = a^{-1} * a = e)$.

Definitsioon 4. Elementi e nimetatakse rühma A **ühikelemendiks** ja tähistatakse tihti sümboliga 1.

Definitsioon 5. Hulka A nimetatakse **poolrühmaks**, kui hulgal A on defineeritud kahekohaline assotsiatiivne algebraline tehe.

Definitsioon 6. Monoidiks nimetatakse poolrühma, milles leidub ühikelement.

Definitsioon 7. Abeli rühmaks nimetatakse rühma, mille tehe on kommutatiivne.

Definitsioon 8. Ringiks nimetatakse hulka R, millel on defineeritud kaks kahekohalist algebralist tehet, $+$ (liitmine) ja $\cdot$ (korrutamine), mis rahuldab tingimusi:

- $(R, +)$ on Abeli rühm,
- $(R, \cdot)$ on monoid,
- $(\forall a, b, c \in R)(a \cdot (b + c) = a \cdot b + a \cdot c)$ ja $((a + b) \cdot c = a \cdot c + b \cdot c)$.

Tähistame sümboliga R^* ringi R pööratavate elementide hulka.

Definitsioon 9. Ringi $(R, +, \cdot)$ nimetatakse **korpuseks**, kui temas on vähemalt 2 elementi ja tema igal nullist erineval elemendil on olemas pöördelement.

Definitsioon 10. m-elemendilist rühma G nimetatakse **tsükliliseks**, kui leidub selline element $a \in G$, et $G = \{a, a^2, \ldots, a^m = 1\}$.

Definitsioon 11. Olgu G rühm ja $g \in G$. Kui elemendi g poolt moodustatud alamrühm $\langle g \rangle$ (s.t. vähim G alamrühm, mis elementi g sisaldab) koosneb n elemendist, siis öeldakse, et elemendi g **järk** on n.

Elemendi g järku tähistame järgmiselt: $\operatorname{ord} g$. Teisisõnu, $\operatorname{ord} g = n$ tähendab, et n on vähim naturaalarv, mille korral $g^n = 1$. Seega lõplik rühm on tsükliline, kui temas leidub element, mille järk on võrdne rühma järguga.

Lause 1 ([5])**.** *Olgu G lõplik rühm, $g \in G$, $k = \operatorname{ord} g$ ja $l \in \mathbb{Z}$. Siis $g^l = 1$ parajasti siis, kui $k \mid l$.*

Definitsioon 12. Olgu R nulliteguriteta kommutatiivne ring ja $a, b \in R$. Elementide a ja b **suurimaks ühisteguriks** nimetatakse elementi $d \in R$, kui

- $d \mid a$ ja $d \mid b$,
- iga elemendi $c \in R$ korral, kui $c \mid a$ ja $c \mid b$, siis $c \mid d$.

Elementide a ja b suurimat ühistegurit tähistame sümboliga (a, b).

Definitsioon 13. Olgu $a, b \in \mathbb{Z}, n \in \mathbb{N}$ ja $(a, n) = 1$. Arve a ja b nimetatakse **kongruentseteks** mooduli n järgi ja märgitakse

$$a \equiv b \pmod{n},$$

kui a ja b annavad jagamisel arvuga n ühe ja sama jäägi.

Saab näidata, et $a \equiv b \pmod{n}$ parajasti siis, kui $n \mid a - b$ ([5]).

Definitsioon 14. Olgu $a \in \mathbb{Z}, n \in \mathbb{N}$ ja $(a, n) = 1$. Arvu a **järguks** mooduli n järgi nimetatakse vähimat naturaalarvu c, mille korral

$$a^c \equiv 1 \pmod{n}.$$

Definitsioon 15. Polünoomiks üle ringi R muutuja x suhtes nimetatakse avaldist

$$a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0,$$

kus $n \in \mathbb{N} \cup \{0\}, a_n, a_{n-1}, \ldots, a_0 \in R$ ja $a_n \neq 0$.

Eeldame, et lugeja on tuttav polünoomide liitmise ja korrutamisega ([4]). Kõigi polünoomide hulka üle ringi R muutuja x suhtes tähistame sümboliga $R[x]$. See hulk on ring polünoomide liitmise ja korrutamise suhtes.

Definitsioon 16. Mittekonstantset polünoomi $p(x)$ ringis $R[x]$ nimetatakse **taandumatuks polünoomiks**, kui teda ei saa esitada kahe mittekonstantse polünoomi korrutisena.

Teoreem 2. (Euleri teoreem) *Kui $a \in \mathbb{Z}, n \in \mathbb{N}$ ja $(a, n) = 1$, siis*

$$a^{\varphi(n)} \equiv 1 \pmod{n},$$

kus φ on Euleri funktsioon.

Definitsioon 17. Täisarvu a nimetatakse **algjuureks** mooduli n järgi ($n \in \mathbb{N}$), kui $(a, n) = 1$ ja $\varphi(n)$ on vähim naturaalarv, mille korral

$$a^{\varphi(n)} \equiv 1 \pmod{n}.$$

Definitsioon 18. Olgu K korpus, $b \in K$ ja $n \in \mathbb{N}$. Elementi $a \in K$ nimetatakse n-astme **juureks** elemendist b, kui $a^n = b$.

Definitsioon 19. n-astme juurt korpuse K ühikelemendist **1** nimetatakse n-astme **ühejuureks**.

Definitsioon 20. **n-astme ringpolünoomiks** nimetatakse polünoomi

$$\Phi_n(x) = \prod_{\substack{1 \leq k \leq n-1 \\ (k,n)=1}} (x - e^{2i\pi k/n}),$$

kus $e^{2i\pi k/n}$ ($k \in \{1, \ldots, n-1\}$) on n-astme ühejuured korpuses $\mathbb{C}$.

Toome ära mõned ringpolünoomide kohta käivad tähtsamad tulemused.

Lemma 3 ([3])**.** *Polünoomi $x^r - 1$ saab ringis $\mathbb{Z}[x]$ lahutada teguriteks kui korrutise $\prod_{n|r} \Phi_n(x)$, s.t.*

$$x^r - 1 = \prod_{n|r} \Phi_n(x).$$

Järeldus 4 ([3]). *Iga $n \in \mathbb{N}$ korral $\Phi_n(x) \in \mathbb{Z}[x]$.*

Teoreem 5 ([3]). *Iga $n \in \mathbb{N}$ korral on n-astme ringpolünoom $\Phi_n(x)$ taandumatu ringis $\mathbb{Z}[x]$.*

Definitsioon 21. Jäägiklassideks mooduli n järgi nimetatakse sellistest täisarvudest koosnevaid hulki, mis on kongruentsed mingi täisarvuga a mooduli n järgi, s.o. hulki

$$\bar{a} = \{b \in \mathbb{Z} \mid a \equiv b \pmod{n}\} = \{a + kn \mid k \in \mathbb{Z}\}.$$

Definitsioon 22. Jäägiklassiringiks $\mathbb{Z}_n$ nimetatakse kõigi jäägiklasside hulka (mooduli n järgi), millel liitmine ja korrutamine on defineeritud võrdustega

$$\bar{a} + \bar{b} = \overline{a + b},$$

$$\bar{a}\bar{b} = \overline{ab},$$

iga $\bar{a}, \bar{b} \in \mathbb{Z}_n$ korral.

Saab näidata, et need definitsioonid on korrektsed, s.t. et sõltu jäägiklasside esindajate valikust ([5]). Samuti saab näidata, et jäägiklassiring $\mathbb{Z}_n$ on korpus parajasti siis, kui n on algarv ([5]).

Jäägiklassiringi $\mathbb{Z}_n$ kõik pööratavad elemendid moodustavad korrutamise suhtes rühma, mida tähistame sümboliga $\mathbb{Z}_n^*$.

Olgu $f(x), g(x) \in \mathbb{Z}[x]$ ja $n \in \mathbb{N}$. Me kirjutame $n \mid f(x)$, kui n jagab polünoomi $f(x)$ kõiki kordajaid, ja

$$f(x) \equiv g(x) \pmod{n},$$

kui n jagab polünoomi $f(x) - g(x) \in \mathbb{Z}[x]$ kõiki kordajaid, s.t. $n \mid f(x) - g(x)$.

Näide. Olgu $f(x) = 5x^3 - 7x^2 + 4x, g(x) = 3x^2 - x + 5$ ja $n = 5$. Siis

$$5 \mid 5x^3 - 7x^2 + 4x - (3x^2 - x + 5) = 5x^3 - 10x^2 + 5x - 5$$

ja seega

$$5x^3 - 7x^2 + 4x \equiv 3x^2 - x + 5 \pmod{5}.$$

Olgu $f(x), g(x), h(x) \in \mathbb{Z}[x]$ ja $n \in \mathbb{N}$, $n > 1$. Me kirjutame

$$f(x) \equiv g(x) \bmod (n,\ h(x)),$$

kui, vaadeldes neid polünoome üle ringi $\mathbb{Z}_n$, kehtib $h(x) \mid f(x) - g(x)$. Teiste sõnadega,

$$f(x) \equiv g(x) \bmod (n,\ h(x))$$

parajasti siis, kui leidub selline $k(x) \in \mathbb{Z}[x]$, et $n \mid f(x) - g(x) + h(x)k(x)$.

Näide. Olgu $f(x) = 3x^4 + 5x^3 - x$, $g(x) = 15x^2 + 10$, $h(x) = 2x^3 + 6$ ja $n = 5$. Siis

$$3x^4 + 5x^3 - x \equiv 15x^2 + 10 \bmod (2x^3 + 6, 5),$$

sest kui $k(x) = x$, siis

$$5 \mid 3x^4 + 5x^3 - x - (15x^2 + 10) + (2x^3 + 6)x = 5x^4 + 5x^3 - 15x^2 + 5x - 10.$$

Olgu nüüd $n = p$ algarv. Saab näidata, et seos $\equiv \bmod (p, h(x))$ on ekvivalentsiseos hulgal $\mathbb{Z}[x]$. Tähistame hulga $\mathbb{Z}[x]$ faktorhulka seose $\equiv \bmod (p, h(x))$ järgi sümboliga $\mathbb{Z}_p[x]/h(x)$ ja tähistame polünoomi $f(x)$ ekvivalentsiklassi seose $\equiv \bmod (p, h(x))$ järgi sümboliga $[f(x)]$. Seega mistahes $f(x), g(x) \in \mathbb{Z}[x]$ korral

$$[f(x)] = [g(x)] \iff f(x) \equiv g(x) \bmod (p, h(x)). \tag{1}$$

Defineerime hulgal $\mathbb{Z}_p[x]/h(x)$ tehted võrdustega

$$[f(x)] + [g(x)] = [f(x) + g(x)]$$

ja

$$[f(x)] \cdot [g(x)] = [f(x) \cdot g(x)].$$

Saab näidata, et tulemus on ring. See ring $\mathbb{Z}_p[x]/h(x)$ on korpus, kui polünoom $h(x)$ on taandumatu üle $\mathbb{Z}_p$. Kui polünoomi $h(x)$ aste ringis $\mathbb{Z}_p[x]$ on m, siis selles korpuses on p^m elementi ([5]).

Kuna antud töös kasutame ringi $\mathbb{Z}_p[x]/h(x)$, siis teeme näitena läbi, kuidas

leitakse ringi $F := \mathbb{Z}_p[x]/h(x)$ elemendid ([5]).

Näide. Olgu $\mathbb{Z}_5 = \{0, 1, 2, 3, 4\}$ (samastame jäägiklassi tema esindajaga) ja polünoom $h(x) = x^2 + x + 1$ üle $\mathbb{Z}_5$. Esiteks kontrollime, kas polünoom $h(x)$ on taandumatu. Kui polünoom oleks taanduv, siis leiduks tal lineaartegur. Kuna $h(0) \neq 0$, $h(1) \neq 0$, $h(2) \neq 0$, $h(3) \neq 0$ ja $h(4) \neq 0$, siis polünoomil $h(x)$ pole lineaartegureid.

Kuna polünoomi $h(x)$ aste on 2, siis ringis $F = \mathbb{Z}_5[x]/(x^2+x+1)$ on $5^2 = 25$ elementi. Tähistame $[x] = a$ ja samastame kõrvalklassid $[0], [1], [2], [3]$ ja $[4]$ esindajatega $0, 1, 2, 3$ ja 4. Ringi F elemendid võime esitada ülimalt esimese astme polünoomidena a suhtes ([5]):

• konstantsed polünoomid: $0, 1, 2, 3, 4$,

• lineaarsed polünoomid: $a, a+1, a+2, a+3, a+4, 2a, 2a+1, 2a+2, 2a+3$, $2a + 4, 3a, 3a + 1, 3a + 2, 3a + 3, 3a + 4, 4a, 4a + 1, 4a + 2, 4a + 3, 4a + 4$.

Definitsioon 23. Iga $n, m \in \mathbb{N} \bigcup \{0\}, m \leq n$, korral defineeritakse binoomkordaja $\binom{n}{m} \in \mathbb{Z}$ võrdusega

$$\binom{n}{m} = \frac{n \cdot (n-1) \cdot \ldots \cdot (n-(m-1))}{m \cdot (m-1) \cdot \ldots \cdot 2 \cdot 1}.$$

Teoreem 6. (Binoomteoreem) *Ringis $\mathbb{Z}[x, y]$ kehtib iga naturaalarvu n korral võrdus*

$$(x+y)^n = \sum_{i=0}^{n} \binom{n}{i} x^i \cdot y^{n-i}.$$

Lemma 7. *Kui p on algarv ja $0 < k < p$, siis $p \mid \binom{p}{k}$.*

TÕESTUS. Teame, et

$$\binom{p}{k} = \frac{p \cdot (p-1) \cdot \ldots \cdot (p-(k-1))}{k \cdot (k-1) \cdot \ldots \cdot 2 \cdot 1}$$

ja et $\binom{p}{k} \in \mathbb{Z}$, siis $k! \mid p(p-1)\ldots(p-(k-1))$. Kuna $k < p$, siis $(k!, p) = 1$ ja seega $k! \mid (p-1)\ldots(p-(k-1))$, millest järeldub, et $p \mid \binom{p}{k}$. □

Lemma 8. *Olgu $r, n \in \mathbb{N}$. Kui $r \mid n$, siis*

$$x^r - 1 \mid x^n - 1.$$

TÕESTUS. Kuna $r \mid n$, siis leidub $k \in \mathbb{Z}$ nii, et $n = rk$. Lahutame polünoomi $x^n - 1$ teguriteks:

$$x^n - 1 = (x^r - 1)(x^{r(k-1)} + x^{r(k-2)} + \ldots + x^r + 1).$$

Seega $x^r - 1 \mid x^n - 1$. □

Lemma 9. *Olgu $g(x) \in \mathbb{Z}[x]$, siis iga $a, b \in \mathbb{N}$ korral kehtib*

$$x^a - x^b \mid g(x^a) - g(x^b).$$

TÕESTUS. Olgu $g(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$ $(n \in \mathbb{N} \bigcup \{0\})$. Vaatame vahet $g(x^a) - g(x^b)$:

$$\begin{aligned} g(x^a) - g(x^b) &= a_n x^{an} + \ldots + a_1 x^a + a_0 - (a_n x^{bn} + \ldots + a_1 x^b + a_0) \\ &= a_n(x^{an} - x^{bn}) + \ldots + a_1(x^a - x^b). \end{aligned}$$

Seega, teades jaguvusseose omadusi, peame näitama, et $x^a - x^b \mid x^{ak} - x^{bk}$ iga $k \in \{1, 2, \ldots, n\}$ korral. Kuna

$$x^{ak} - x^{bk} = (x^a - x^b)(x^{a(k-1)} + x^{a(k-2)}x^b + \ldots + x^a x^{b(k-2)} + x^{b(k-1)})$$

iga $k \in \mathbb{N}$ korral, mistõttu saamegi, et $x^a - x^b \mid g(x^a) - g(x^b)$. □

2 Meetodeid algarvulisuse kontrollimiseks enne Agrawali, Kayali ja Saxena teoreemi

Algarvu mõiste on rohkem kui kaks tuhat aastat vana ning juba Eukleides tõestas, et algarve on lõpmata palju, mistõttu ei ole võimalik teha tabelit, kus on kirjas kõik algarvud. Seega on vaja lihtsat ja efektiivset algoritmi, mis teeks kindlaks, kas arv on algarv või mitte. Selle probleemi lahendamisega on matemaatikud tegelenud aastasadu ja selles peatükis vaatleme mõnda neist lahendustest.

Algarvulisustestid jagunevad kaheks: deterministlikud ning tõenäosuslikud. Deterministlikud testid määravad 100% kindlusega ära, kas arv on algarv või mitte. Tõenäosuslikud testid annavad aga mõne kordarvu korral anda vastuseks, et see on algarv (vastupidi mitte, s.t. kui arv on algarv, siis tõenäosuslik test ei määra valesti, et tegemist oleks kordarvuga).

Üheks lihtsamaks, kuid samas väga töömahukaks meetodiks on jagada antud arv kõigi talle eelnevate naturaalarvudega, mis on suuremad kui 1. Kui ta ühegagi neist ei jagu, siis ta on algarv; vastasel juhul on tegemist kordarvuga.

Teiseks võimaluseks on kasutada kordarvu omadust: kui arv a on kordarv, siis tal leidub algarvuline tegur p nii, et $p \leq \sqrt{a}$ ([5]). Seega piisab, kui kontollida, kas arv jagub algarvudega $p \leq \sqrt{a}$; kui ei jagu, siis arv on algarv. See meetod on küll vähem mahukas kui esimene, kuid suuremate arvude korral on ikkagi liiga palju arvutamist.

Teoreem 10. (Fermat' väike teoreem) *Kui arv p on algarv ja a on täisarv, mis ei jagu arvuga p, siis*

$$a^{p-1} \equiv 1 \pmod{p}$$

ehk

$$p \mid a^{p-1} - 1.$$

Fermat' väikesele teoreemile tuginev algarvulisustest on tõenäosuslik ning seega on selle probleemiks, et mõni kordarv oleks selle testi järgi algarv. Algoritmile antakse ette kontrollimist vajav arv n, järgmisena valitakse suvaliselt arv $a \in \{2, \ldots, n-1\}$. Kui $n \nmid a^{n-1} - 1$, siis algoritm annab tulemuseks "n on kordarv". Kui $n \mid a^{n-1} - 1$, siis algoritm annab tulemuse "n on tõenäoliselt algarv".

Mida rohkem kordi test läbi tehakse erinevate juhuslikult valitud arvudega a, seda suurem on tõenäosus, et test väljastab õige tulemuse.

Näiteks kontrollime arvu 341. Olgu $n = 341$ ja $a = 2$. Kuna

$$2^{341-1} = 2^{340} = (2^{10})^{34} = 1024^{34} \equiv 1^{34} \equiv 1 \pmod{341},$$

siis Fermat' testi põhjal on arv 341 tõenäoliselt algarv, kuigi tegelikult on ta kordarv, sest $341 = 11 \cdot 31$. Selliseid arve nimetatakse libaalgarvudeks.

Fermat' väikesest teoreemist saab teha järgmise järelduse.

Järeldus 11. *Kui arv p on algarv, siis iga täisarvu a korral*

$$a^p \equiv a \pmod{p}$$

ehk

$$p \mid a^p - a.$$

Teoreem 12. (Wilsoni teoreem) *Naturaalarv $n \leq 2$ on algarv siis ja ainult siis, kui n jagab arvu $(n-1)! + 1$.*

Järgnevas kahes tulemuses sisalduvad ideed, millest Agrawal, Kayal ja Saxena oma töös lähtusid.

Lause 13. *Kui p on algarv ja $a \in \mathbb{Z}$, siis*

$$(x + a)^p \equiv x^p + a \pmod{p}.$$

TÕESTUS. Olgu p algarv, siis Newtoni binoomvalemi, lemma 7 ja järelduse 11 põhjal kehtib

$$(x + a)^p - x^p - a \equiv x^p + a^p - x^p - a = a^p - a \equiv 0 \pmod{p}.$$

□

Teoreem 14. *Täisarv n on algarv siis ja ainult siis, kui*

$$(x + 1)^n \equiv x^n + 1 \pmod{n}.$$

TÕESTUS. *Tarvilikkus.* Järeldub lausest 13, kui võtame $a = 1$.

Piisavus. Teame, et

$$(x+1)^n - (x^n+1) = \sum_{1 \le j \le n-1} \binom{n}{j} x^j.$$

Seega

$$(x+1)^n \equiv x^n + 1 \pmod{n}$$

siis ja ainult siis, kui n jagab arvu $\binom{n}{j}$ iga j korral, $j \in \{1, \ldots, n-1\}$, kusjuures

$$\binom{n}{j} = \frac{n \cdot (n-1) \cdot \ldots \cdot (n-(j-1))}{j \cdot (j-1) \cdot \ldots \cdot 2 \cdot 1}.$$

Kui oletada, et n on kordarv, siis olgu p mingi algarv, mis jagab arvu n. Siis kehtib

$$\binom{n}{p} = \frac{n \cdot (n-1) \cdot \ldots \cdot (n-(p-1))}{p \cdot (p-1) \cdot \ldots \cdot 2 \cdot 1}.$$

Näeme, et ainsad tegurid, mida p jagab, on lugejas olev n ja nimetajas olev p. Seega, kui p^k on suurim p aste, mis jagab arvu n, siis p^{k-1} on suurim p aste, mis jagab arvu $\binom{n}{p}$, mistõttu n ei jaga arvu $\binom{n}{p}$ ja saame vastuolu. Järelikult n on algarv.

□

3 Agrawali, Kayali ja Saxena teoreem algarvulisuse kohta

Antud peatükis esitame ning tõestame selle bakalaureusetöö peamise teoreemi.

Teoreem 15. (Agrawali, Kayali ja Saxena teoreem)

Olgu $n, r \in \mathbb{N}, n > r$, kusjuures arvu n järk d mooduli r järgi on suurem kui $(\log_2 n)^2$. Arv n on algarv siis ja ainult siis, kui:

1) *n ei ole ühegi naturaalarvu ühest suurem aste,*

2) *arvul n ei ole ole algtegureid, mis oleksid $\leq r$,*

3) *iga naturaalarvu $a \in [1, A]$, kus $A = \sqrt{r} \cdot \log_2 n$, korral*

$$(x + a)^n \equiv x^n + a \bmod (n, x^r - 1). \tag{2}$$

TÕESTUS. *Tarvilikkus.* Olgu n algarv. Siis tingimused 1) ja 2) ilmselgelt kehtivad. Kuna lause 13 põhjal $n \mid (x+a)^n - x^n - a + 0 \cdot (x^r - 1)$, siis kehtib ka tingimus 3).

Piisavus. Eeldame, et kehtivad tingimused 1), 2) ja 3). Oletame vastuväiteliselt, et n on kordarv.

Olgu p algarv, mis jagab arvu n. Kuna eelduse põhjal $(x + a)^n \equiv x^n + a \bmod (n, x^r - 1)$, siis ka

$$(x + a)^n \equiv x^n + a \bmod (p, x^r - 1) \tag{3}$$

iga naturaalarvu a korral, kus $a \in [1, A]$.

Lemma 3 põhjal saame polünoomi $x^r - 1$ lahutada taandumatuteks teguriteks ringis $\mathbb{Z}[x]$ kui korrutise $\prod_{c|r} \Phi_c(x)$, kus $\Phi_c(x)$ on c-astme ringpolünoom. Ehk $x^r - 1 = \prod_{c|r} \Phi_c(x)$. Polünoom $\Phi_r(x)$ on taandumatu ringis $\mathbb{Z}[x]$, kuid võib olla taanduv ringis $\mathbb{Z}_p[x]$. Ka ringis $\mathbb{Z}_p[x]$ saame polünoomi $\Phi_r(x)$ lahutada taandumatute tegurite korrutiseks. Olgu $h(x) \in \mathbb{Z}[x]$ polünoom, mis vaadelduna üle $\mathbb{Z}_p$ on polünoomi $\Phi_r(x)$ mingi taandumatu tegur ringis $\mathbb{Z}_p[x]$. Siis

$$\Phi_r(x) \equiv h(x) \cdot t(x) \pmod p, \tag{4}$$

kus $t(x) \in \mathbb{Z}[x]$.

Lemma 16. *Kui* $f(x), g(x) \in \mathbb{Z}[x]$*, siis*

$$f(x) \equiv g(x) \bmod (p, x^r - 1) \Rightarrow f(x) \equiv g(x) \bmod (p, h(x)).$$

TÕESTUS. Kuna $\Phi_r(x) \mid x^r - 1$, siis leidub polünoom $l(x) \in \mathbb{Z}[x]$ nii, et

$$\Phi_r(x) \cdot l(x) = x^r - 1.$$

Korrutades seose (4) mõlemad pooled polünoomiga $l(x)$ saame, et

$$x^r - 1 \equiv h(x) \cdot t(x) \cdot l(x) \pmod{p}. \tag{5}$$

Kui $f(x) \equiv g(x) \bmod (p, x^r - 1)$, siis leidub polünoom $k(x) \in \mathbb{Z}[x]$ nii, et

$$f(x) \equiv g(x) + (x^r - 1) \cdot k(x) \pmod{p}.$$

Tänu kongruentsile (5) võime kirjutada, et

$$f(x) \equiv g(x) + h(x) \cdot t(x) \cdot l(x) \cdot k(x) \pmod{p},$$

kus $t(x) \cdot l(x) \cdot k(x) \in \mathbb{Z}[x]$. Järelikult

$$f(x) \equiv g(x) \bmod (p, h(x)).$$

□

Tänu lemmale 16 saame kongruentsist (3), et

$$(x + a)^n \equiv x^n + a \bmod (p, h(x)) \tag{6}$$

iga naturaalarvu $a \in [1, A]$ korral.

Vaatleme p^m-elemendilist korpust $\mathbb{F} := \mathbb{Z}_p[x]/h(x)$, kus $m = deg(h(x))$ on polünoomi $h(x)$ aste ringis $\mathbb{Z}_p[x]$. Kongruentsi (6) saab tõlgendada kui po-

lünoomidele $(x+a)^n$ ja x^n+a vastavate $\mathbb{F}$ elementide võrdust (vt. (1)):

$$[(x+a)^n] = [x^n + a]. \tag{7}$$

Nullelemendist erinevad $\mathbb{F}$ elemendid moodustavad tsüklilise rühma $\mathbb{F}^*$ järguga $p^m - 1$. Enamgi veel, saab näidata, et rühm $\mathbb{F}^*$ sisaldab elementi $[x]$, mille järk on r, seega r jagab arvu $p^m - 1$.

Veendume, et ükski elementidest $[x], [x+1], \ldots, [x+\lfloor A \rfloor] \in \mathbb{F}$ ei ole nullelement. Selleks oletame vastuväiteliselt, et korpuses $\mathbb{F}$

$$[x + \alpha] = [0],$$

kus $\alpha \in \{0, 1, \ldots, \lfloor A \rfloor\}$. Siis seose (7) põhjal

$$[x^n + \alpha] = [(x+\alpha)^n] = [x+\alpha]^n = [0]^n = [0]$$

korpuses $\mathbb{F}$, mistõttu

$$[x^n] = -[\alpha] = [x]$$

korpuses $\mathbb{F}$. Kuna $[x] \in \mathbb{F}$ on pööratav, siis korrutades viimase võrduse mõlemaid pooli elemendiga $[x]^{-1}$ saame tulemuseks

$$[x^{n-1}] = [1].$$

Kuna $\operatorname{ord}_{\mathbb{F}^*}[x] = r$, siis viimasest võrdusest järeldub lause 1 põhjal, et $r \mid n-1$. Seega $n \equiv 1 \pmod{r}$, mistõttu $d = 1$, kuid see on vastuolus eeldusega, et $d > (\log_2 n)^2 \geq (\log_2 4)^2 > 1$. Seega $[x+\alpha] \neq [0]$ ja $[x], [x+1], \ldots, [x+\lfloor A \rfloor] \in \mathbb{F}^*$.

Olgu H ringi $\mathbb{Z}_p[x]/(x^r - 1)$ multiplikatiivse poolrühma alampoolrühm, mis on tekitatud elementide $[x], [x+1], \ldots, [x+\lfloor A \rfloor]$ poolt. Seega

$$H = \left\{ \prod_{0 \leq a \leq A} [x+a]^{e_a} \mid e_a \in \{0, 1, \ldots\} \right\}.$$

Olgu G korpuse $\mathbb{F}$ multiplikatiivse rühma $\mathbb{F}^*$ alamrühm, mis on tekitatud ele-

mentide $[x], [x+1], \ldots, [x+\lfloor A \rfloor]$ poolt.

Defineerime hulga S, mis koosneb naturaalarvudest k, mille korral

$$g(x^k) \equiv g(x)^k \bmod (p, x^r - 1) \; \forall \; [g(x)] \in H.$$

Ehk

$$S = \{k \in \mathbb{N} \mid g(x^k) \equiv g(x)^k \bmod (p, x^r - 1) \; iga \; [g(x)] \in H \; korral\}.$$

Lemma 17. *Arvud p ja n kuuluvad hulka S.*

TÕESTUS. Kui $g(x) = \prod_{0 \le a \le A} (x+a)^{e_a}$, $e_a \in \{0, 1, 2, \ldots\}$ ja $[g(x)] \in H$, siis seose (3) põhjal

$$g(x)^n = \prod_{0 \le a \le A} ((x+a)^n)^{e_a} \equiv \prod_{0 \le a \le A} (x^n + a)^{e_a} = g(x^n) \bmod (p, x^r - 1).$$

Seega arv n kuulub hulka S.

Vaatame nüüd arvu p. Lause 13 põhjal saame

$$g(x)^p = \prod_{0 \le a \le A} ((x+a)^p)^{e_a} \equiv \prod_{0 \le a \le A} (x^p + a)^{e_a} = g(x^p) \bmod (p, x^r - 1),$$

s.t. $p \in S$. □

Plaanis on anda rühma G elementide arvule ülemine ja alumine tõke, et saada vastuolu.

ÜLEMINE TÕKE $|G|$ JAOKS

Lemma 18. *Kui $a, b \in S$, siis $a \cdot b \in S$.*

TÕESTUS. Kui $[g(x)] \in H$, siis

$$g(x^b) \equiv g(x)^b \bmod (p, x^r - 1).$$

Võttes muutuja x asemele x^a, saame

$$g((x^a)^b) \equiv g(x^a)^b \bmod (p, (x^a)^r - 1),$$

seega definitsiooni põhjal ka $g((x^a)^b) \equiv g(x^a)^b \bmod (p, x^r - 1)$, sest lemma 8 tõttu jagab polünoom $x^r - 1$ polünoomi $x^{ar} - 1$. Järelikult

$$g(x)^{ab} = (g(x)^a)^b \equiv g(x^a)^b \equiv g((x^a)^b) = g(x^{ab}) \bmod (p, x^r - 1)$$

nagu soovitud. □

Lemma 19. *Kui* $a, b \in S$ *ja* $a \equiv b \pmod r$*, siis* $a \equiv b \pmod{|G|}$.

TÕESTUS. Kuna G on tsüklilise rühma $\mathbb{F}^*$ alamrühm, siis on ta tsükliline rühm. Olgu $g(x) \in \mathbb{Z}[x]$ selline polünoom, et $[g(x)]$ on rühma G moodustaja. Siis $\mathrm{ord}_G[g(x)] = |G|$ ja $g(x) = \prod_{0 \le a \le A}(x + a)^{e_a}$, kus $e_a \in \{0, 1, \ldots\}$. Kuna $a \equiv b \pmod r$, siis lemma 8 ja lemma 9 põhjal

$$x^r - 1 \mid x^{a-b} - 1 \mid x^a - x^b \mid g(x^a) - g(x^b).$$

Vaadeldes ekvivalentsiklassi $[g(x)] \in H$ võime öelda, et

$$g(x)^a \equiv g(x^a) \equiv g(x^b) \equiv g(x)^b \bmod (p, x^r - 1).$$

Lemma 16 põhjal kehtib ka $g(x)^a \equiv g(x)^b \bmod (p, h(x))$, s.t. $[g(x)]^a = [g(x)]^b$ rühmas G. Järelikult

$$[g(x)]^{a-b} = [1]$$

rühmas G. Lause 1 põhjal $|G|$ jagab arvu $a - b$. □

Olgu rühma $\mathbb{Z}_r^*$ alamrühm R moodustatud $\overline{n}$ ja $\overline{p}$ poolt. Kuna arvu p astendamisel ei saa vastuseks arvu n, siis naturaalarvud $n^i p^j$ $(i, j \ge 0)$ on erinevad. Kuna hulgas $\{n^i p^j | 0 \le i, j \le \sqrt{|R|}\}$ on rohkem kui $|R|$ arvu ja kõik $\overline{n^i p^j} \in R \subseteq \mathbb{Z}_r^*$, siis peavad leiduma $i, j, I, J \in \mathbb{N}$ nii, et $0 \le i, j, I, J \le \sqrt{|R|}$, $n^i p^j \ne n^I p^J$ ja

$$n^i p^j \equiv n^I p^J \pmod r.$$

Lemma 18 põhjal kuuluvad need naturaalarvud $n^i p^j, n^I p^J$ hulka S, lemma 19 põhjal jagub nende vahe arvuga $|G|$, mistõttu

$$|G| \leq |n^i p^j - n^I p^J| \leq (np)^{\sqrt{|R|}} - 1 < n^{2\sqrt{|R|}} - 1.$$

Seda hinnangut G võimsusele saab parandada, kui näitame, et $n/p \in S$. Siis asendades eelpool toodud tõestuses arvu n arvuga n/p, saame hinnangu

$$|G| \leq n^{\sqrt{|R|}} - 1. \tag{8}$$

Niisiis tõestame, et $n/p \in S$. Kuna arvu n järk on mooduli r järgi d, siis $n^d \equiv 1 \pmod{r}$.

Oletame, et $a \in S, b \in \mathbb{N}, b < a$ ja $b \equiv a \bmod (n^d - 1)$. Siis $r \mid n^d - 1 \mid a - b$ ja lemma 8 põhjal

$$x^r - 1 \mid x^{a-b} - 1 \mid x^a - x^b \mid g(x^a) - g(x^b) \tag{9}$$

iga $g(x) \in \mathbb{Z}[x]$ korral.

Kui $[g(x)] \in H$, siis lemma 18 põhjal saame, et

$$g(x)^{n^d} \equiv g(x^{n^d}) \bmod (p, x^r - 1),$$

sest $n \in S$ ja

$$g(x^{n^d}) \equiv g(x) \bmod (p, x^r - 1)$$

(sest et $x^r - 1 \mid x^{n^d-1} - 1 \mid x^{n^d} - x \mid g(x^{n^d}) - g(x)$). Seega

$$g(x)^{n^d} \equiv g(x) \bmod (p, x^r - 1)$$

ja

$$(g(x)^{n^d-1} - 1) \cdot g(x) \equiv 0 \bmod (p, x^r - 1). \tag{10}$$

Kuna $n^d - 1 \mid a - b$, siis

$$g(x)^{n^d-1}-1 \mid g(x)^{a-b}-1,$$

mis koos kongruentsiga (10) annab, et

$$(g(x)^{a-b}-1)\cdot g(x) \equiv 0 \bmod (p, x^r-1).$$

Järelikult

$$g(x)^{a-b+1} \equiv g(x) \bmod (p, x^r-1).$$

Korrutades mõlemad pooled polünoomiga $g(x)^{b-1}$ saame, et

$$g(x)^a \equiv g(x)^b \bmod (p, x^r-1).$$

Seega

$$g(x^b) \equiv g(x^a) \equiv g(x)^a \equiv g(x)^b \bmod (p, x^r-1),$$

kuna $a \in S$ ja kehtib (9). Sellest tuleneb, et ka $b \in S$. Nüüd olgu $b = n/p$ ja $a = n \cdot p^{\varphi(n^d-1)-1}$, kus φ on Euleri funktsioon. Lemma 19 põhjal $a \in S$, sest $p, n \in S$. Näitame, et $n/p \in S$. Euleri teoreemi põhjal

$$b-a = \frac{n}{p} - np^{\varphi(n^d-1)-1} = \frac{n}{p}(1-p^{\varphi(n^d-1)}) \equiv \frac{n}{p}(1-1) = 0 \bmod (n^d-1).$$

Seega $b \equiv a \pmod{n^d-1}$, mistõttu $b = n/p \in S$.

ALUMINE TÕKE $|G|$ JAOKS

Näitame, et hulga G võimsusel leidub alumine tõke.

Lemma 20. *Olgu $f(x), g(x) \in \mathbb{Z}[x], f(x) \equiv g(x) \bmod (p, h(x))$ ning polünoomidele $f(x)$ ja $g(x)$ vastavad elemendid korpuses $\mathbb{F}$ kuulugu rühma G. Kui polünoomide $f(x)$ ja $g(x)$ mõlema aste on $< |R|$, siis $f(x) \equiv g(x) \pmod p$.*

TÕESTUS. Vaatleme polünoomi $\triangle(y) := f(y) - g(y) \in \mathbb{Z}[y]$ polünoomina üle korpuse $\mathbb{F}$. Kui $k \in S$, siis tänu lemmale 16

$$\triangle(x^k) = f(x^k) - g(x^k) \equiv f(x)^k - g(x)^k \equiv 0 \bmod (p, h(x)).$$

On võimalik näidata, et elemendi $[x]$ järk korpuses $\mathbb{F}$ on r. Kuna $|R| < r$, siis $\left\{[x]^k \mid k \in \{1, \ldots, |R|\}\right\}$ on kõik erinevad $\triangle(y)$ juured korpuses $\mathbb{F}$. Polünoomi $\triangle(y)$ aste on väiksem kui $|R|$, aga tal on $\geq |R|$ erinevat juurt $\bmod(p, h(x))$, seega $\triangle(y)$ on nullpolünoom $\bmod(p, h(x))$ järgi, mis tähendab, et polünoomi $\triangle(y)$ kõik kordajad on nullid $\bmod(p, h(x))$ järgi. Kuna need kordajad ei sõltu muutujast x, siis peavad nad olema nullid $\bmod p$ järgi. Seega arv p peab jagama polünoomi $f(x) - g(x)$ kõiki kordajaid, mida oligi vaja tõestada. □

Definitsiooni põhjal sisaldab R kõik $\overline{n}^i \in \mathbb{Z}_r$, kus $i \geq 0$. Seega $|R| \geq d$ (arv d oli arvu n järk mooduli r järgi), mis on eelduse kohaselt suurem kui $(\log_2 n)^2$. Tähistame $B := \lfloor \sqrt{|R|} \cdot \log_2 n \rfloor$. Kuna $A = \sqrt{r} \cdot \log_2 n$ ja $|R| < r$, saame, et $A > B$. Kuna $|R| \geq d > (\log_2 n)^2$, siis $\sqrt{|R|} > \log_2 n$ ja seega

$$B \leq \sqrt{|R|} \cdot \log_2 n < \sqrt{|R|}^2 = |R|.$$

Tingimuse 2) kohaselt $p > r$. Seega $B < |R| < r < p$ ehk $p > B$. Olgu $T, U \subset \{0, 1, 2, \ldots, B\}$ erinevad alamhulgad. Vaatleme hulgale T vastavat polünoomi $f(x) = \prod_{a \in T}(x + a) \in \mathbb{Z}[x]$ ning hulgale U vastavat polünoomi $g(x) = \prod_{a \in U}(x + a) \in \mathbb{Z}[x]$. Siis need polünoomid on erinevad ringis $\mathbb{Z}[x]$. Kui oletada, et $f(x) \equiv g(x) \pmod p$, siis peaks leiduma bijektsioon $\sigma : T \to U$ nii, et $x + a \equiv x + \sigma(a) \pmod p$ iga $a \in T$ korral. Viimane tähendab, et $p \mid a - \sigma(a)$ iga $a \in T$ korral. Kuna aga $|a - \sigma(a)| \leq B < p$, siis peab iga $a \in T$ korral kehtima võrdus $a = \sigma(a)$. See aga tähendab, et $f(x) = g(x)$ ringis $\mathbb{Z}[x]$, mistõttu saame vastuolu.

Niisiis $f(x) \not\equiv g(x) \pmod p$ ning polünoomide $f(x)$ ja $g(x)$ aste on $< |R|$. Lemma 20 põhjal teame, et $[f(x)] \neq [g(x)]$ rühmas G. Seega iga pärisalamhulga $T \subset \{0, 1, 2, \ldots, B\}$ korral annavad korrutised $\prod_{a \in T}(x + a)$ rühma G erinevad elemendid ja seega

$$|G| \geq 2^{B+1} - 1 > 2^{\sqrt{|R|} \cdot \log_2 n} - 1 = 2^{\log_2 n^{\sqrt{|R|}}} - 1 = n^{\sqrt{|R|}} - 1,$$

mis on vastuolus võrratusega (8).

Sellega on Agrawali, Kayali ja Saxena teoreem tõestatud.

□

Agrawali, Kayali ja Saxena algoritm

Toome lõpuks ära ka Agrawali, Kayali ja Saxena algoritmi algarvulisuse kontrollimise kohta ([1]).

Sisend: naturaalarv $n > 1$.

1) If ($\exists a, b \in \mathbb{N} \mid b > 1 \wedge a^b = n$) return COMPOSITE.

2) Leida väikseim $r \in \mathbb{N}$ nii, et $\mathrm{ord}_r\, n > (\log_2 n)^2$.

3) If ($(a, n) \neq 1$ mingi $a \in \mathbb{N}$ korral, kus $a \leq r$) return COMPOSITE.

4) If $n \leq r$ return PRIME.

5) Iga $a \in \{1, \ldots, \lfloor \sqrt{r} \log n \rfloor\}$ korral:
   if $((x + a)^n \neq x^n + a \pmod{(x^r - 1, n)})$ return COMPOSITE.

6) Return PRIME.

Algoritmile antakse alguses sisendiks naturaalarv n, mis on suurem kui 1. Kui arv n on kordarv, siis väljastab algoritm teate, et n on kordarv, vastasel juhul väljastab algoritm teate, et n on algarv.

Agrawal-Kayal-Saxena primality theorem

Bachelor's Thesis

Ave Räni

Summary

This bachelor's thesis gives an overview about prime numbers and different methods how to determine if an integer is prime or composite. It is based on Andrew Granville's article "It is easy to determine if a given integer is prime", where he introduces and gives a proof of the primality theorem of Agrawal, Kayal and Saxena. The theorem was first published in 2002 in a paper "PRIMES is in P" by Manindra Agrawal, Neeraj Kayal and Nitin Saxena.

This thesis consists of 3 parts. In the first part, the main definitions are given that are used throughout the whole thesis. The second part gives some examples about different theorems which have been used to determine primality before the theorem of Agrawal, Kayal and Saxena. In the third part we give a detailed proof of the main theorem of the thesis. It is formulated as follows.

For a given integer $n \geq 2$, let r be a positive integer $< n$, for which n has order $> (\log_2 n)^2 \pmod r$. Then n is prime if and only if

1) n is not a perfect power,

2) n does not have any prime factor $\leq r$,

3) $(x+a)^n \equiv x^n + a \bmod (n, x^r - 1)$ for each integer a, $1 \leq a \leq \sqrt{r} \log n$.

Based on this theorem M. Agrawal, N. Kayal and N. Saxena created a deterministic primality-proving algorithm. This algorithm determines whether a positive integer n is prime or composite within polynomial time with respect to the number of digits of n.

Viited

[1] M. Agrawal, N. Kayal, N. Saxena, *"PRIMES is in P"*, Indian Institute of Technology, 2002.

[2] A. Granville, *"It is easy to determine whether a given integer is prime"*, Bulletin of the American Mathematical Society, 42(1), 2004.

[3] K. Ireland, M. Rosen, *A classical introduction to modern number theory*, Springer-Verlag, 1990.

[4] M. Kilp, *Algebra I*, Eesti Matemaatika Selts, 2005.

[5] V. Laan, *Arvuteooria loengukonspekt*, Tartu Ülikool, 2012.

Lihtlitsents lõputöö reprodutseerimiseks ja lõputöö üldsusele kättesaadavaks tegemiseks

Mina Ave Räni
(*autori nimi*)
(sünnikuupäev: 24.11.1990)

1. annan Tartu Ülikoolile tasuta loa (lihtlitsentsi) enda loodud teose
Agrawali, Kayali ja Saxena teoreem algarvulisuse kohta ,
(*lõputöö pealkiri*)

mille juhendaja on
Valdis Laan ,
(*juhendaja nimi*)

1.1. reprodutseerimiseks säilitamise ja üldsusele kättesaadavaks tegemise eesmärgil, sealhulgas digitaalarhiivi DSpace-is lisamise eesmärgil kuni autoriõiguse kehtivuse tähtaja lõppemiseni;
1.2. üldsusele kättesaadavaks tegemiseks Tartu Ülikooli veebikeskkonna kaudu, sealhulgas digitaalarhiivi DSpace´i kaudu kuni autoriõiguse kehtivuse tähtaja lõppemiseni.

2. olen teadlik, et punktis 1 nimetatud õigused jäävad alles ka autorile.

3. kinnitan, et lihtlitsentsi andmisega ei rikuta teiste isikute intellektuaalomandi ega isikuandmete kaitse seadusest tulenevaid õigusi.

Tartus/Tallinnas/Narvas/Pärnus/Viljandis, **31.05.2013**