Ülevaade Agrawal-Kayal-Saxena algarvulisuse testist

Sven Laur

14. oktoober 2002. a.

Kokkuvõte

Algarvude ja kordarvude eristamise probleem on oma lihtsuses arusaadav pea kõigile. Samas pole teada ühtegi lihtsat kuid samas efektiivset lahendust – algarvulisuse testi. See on innustanud matemaatikuid otsima erinevaid võimalusi algarvude eristamiseks kordarvudest. Lisaks intellektuaalsele väljakutsele on ülesandel palju praktilisi rakendusi. Üheks olulisemaks valdkonnaks, mis vajab suuri algarve, on avaliku võtme krüptograafia. Krüptosüsteemi RSA leiutamisele(R.L.Rivest, A.Shamir ja L.M.Adleman 1977) järgnes kiire areng algarvulisuse kontrolli algoritmises. Juba 1980. aastaks oli algarvulisuse kontroll kui praktiline probleem lahendatud. Samas olid tuntud algoritmid tõenäosuslikud ning ei suutnud genereerida algarvulisuse tõestusi. Sellele järgnes paarkümmend aastat pingsat uurimistööd, mis tipnes 2002. aastal M.Agrawal, N.Kayal ja N.Saxena poolt garanteeritult polünomiaalses ajas töötava algoritmi avastamisega. Kuigi avastusel pole hetkel praktilist väärtust, anname ülevaate algoritmist ning võimalikest täiustustest.

1 Ajalooline ülevaade

Algarvulisus kui mõiste on juba üle kahe aastatuhande vana. Juba Vana-Kreeka matemaatik Eukleides avaldas oma "Elementides"tõestuse selle kohta, et algrvude hulk $\mathbb{P}$ on lõpmatu. Järgmiseks oluliseks tulemuseks on 17. sajandil sõnastatud ja tõestatud Fermat' väike teoreem, mis tõestati alles 1736. aastal Euleri poolt(teada on ka Leibnitzi tõestus aastast 1683).

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

See on üks olulisemaid vahendeid tänapäevastes algarvulisuse testides. Pakkudes välja mingi naturaalarvu a, mille korral $a^p \not\equiv a \mod p$, on võimalik tõestada, et arv p on kordarv. See on tunduvalt lihtsam kui mõne mittetriviaalse teguri leidmine. Enamus tänapäevastest algarvutestidest kasutavad nii või teisiti just seda omadust. 18. sajandi lõppus püstitas Gauss teise olulise hüpoteesi, tuginedes ulatuslikele arvutustele.

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

Hüpoteesi korrektsuse tõestasid Hadamard ja de la Vallée-Poussin alles 1896. aastal, kasutades selleks analüütilise arvuteooria vahendeid. See oli üks esimesi tõestusi arvuteoorias, mis kasutas kompleksnalüüsi tulemusi. Samaaegsetest tulemustest on üks olulisemaid Bertrand'i postulaat, mille 1851. aastal tõestas Tšebõšev.

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

Need tulemused annavad efektiivse teoreetilise baasi kuitahes suurte algarvude leidmiseks. Piiratud arvutusvõimsus ning peaaegu puuduv praktiline vajadus suurte algarvude järele oli ilmselt üks peamisi põhjuseid, miks ükski efektiivne algarvulisuse kontrolli algoritm ei pärine enne 1977 aastat[1], kuigi kõik selleks vajalikud teoreetilised tulemused olid olemas. Aasta enne seda panid Diffie ja Hellman aluse avaliku võtme krüptograafiale, publitseerides oma võtmevahetuse skeemi. Sellele järgnes 1977. aastal R.L.Rivesti, A.Shamiri ja L.M.Adlemani poolt loodud krüptosüsteem RSA. Mõlemad skeemid vajasid turvalisuse tagamiseks suuri algarve. Juba samal aastal publitseerisid R.Solovay ja V.Strassen esimese efektiivse tõenäosusliku testi algarvulisuse kontrollimiseks. 1975-1976. aastal avaldas G.L.Miller artiklid algarvutestist, mis töötab polünomiaalses ajas arvu p pikkusest, kui kehtib Riemanni laiendatud hüpotees[2]. 1980. aastal näitasid L.Monier ja M.O.Rabin oma töödes, et Milleri algoritm on suurema eduga tõenäosuslik algoritm kui Solovay-Strasseni algoritm.

Üldiselt võib öelda, et 80-nendate alguseks oli kordarvulisuse probleem edukalt lahendatud, sest mõlemad testid kindlustasid praktiliselt polünomiaalses ajas leitava kordarvulisuse sertifikaadi. Kõrvalmärkusena olgu öeldud, et kummalisel kombel kasutasid veel 90-nendate aastate alguses loodud arvutialgebra paketid Maple V, Mathemathica, Axiom jt. valesti realiseeritud tõenäosuslikke algoritme[Pin93]. Ilmselt oli põhjuseks arvutusvõimsuse piiratus, seetõttu realiseeriti testid fikseeritud prooviastendajatega ning prooviti saavutada õigsust mitme erineva algarvu testi kombineerimisel.

Ikka oli veel lahendamata algarvulisuse tõestamine, st. mitte ükski efektiivne algoritm ei andnud välja kontrollitavat sertifikaati, mis oleks tõestanud algarvulisust. Olid olemas prantsuse kooliõpetaja E.Lucase süstematiseeritud tulemused 19. sajandist, mis lubasid tõestada erikujuliste arvude algarvulisust polünomiaalses ajas. 1930-nendatel üldistas D.H. Lehmer Lucase tulemusi, saadud Lucas-Lehmeri algoritmid kasutavad tõestuse genereerimiseks ära $n \pm 1$ tegurdust. Selle silmapaistvamaks rakenduseks on Mersenne'i algarvude otsimine. 70-ndtate lõpus andsid L.M.Adleman, C.Pomerance ja R.S.Rumley üldise algarvulisuse tõestamise algoritmi. Sellele järgnes mitu eri valdkonna tulemustel

[1] Välja arvatud Fermat-Euleri' test, mis on otsene järeldus vastavast teoreemist.

[2] Hilberti kaheksas probleem, mis on siiamaani lahendamata, hoolimata matemaatikute igakülgsetest pingutustest.

põhinevat tõestusalgoritmi, kuid tõestatult polünomiaalses ajas toimiv algarvulisuse algoritm jäi siiski leidmata. Alles 2002. aastal avaldasid M.Agrawal, N.Kayal ja N.Saxena tõestatult polünomiaalses ajas toimiva algarvulisuse kontrolli algoritmi. Algoritm erineb teistest uudse vaatenurga poolest, mis kindlustabki polünomiaalse keerukuse[3]. Kuigi algoritm on ülimalt ebaefektiive on loota[4], et edasised täiustused muudavad selle ka praktiliselt rakendatavaks.

Polünomiaalse algoritmi leidmine ei tähenda olulist murrangut keerukusteoorias ega krüptograafias. Keerukusteoorias on algarvulisuse probleem PRIMES olnud näide probleemist, mis kuulub keerukusklasside NP ja co-NP lõikesse ja pole ilmselt polünomiaalses ajas lahenduv. Ajaloost on teada veel teinegi arvatavalt raske ülesanne lõikest NP $\cap$ co-NP, mis osutus polünomiaalses ajas lahenduvaks – täisarvulise lineaarplaneerimise ülesanne LP. 1979. aastal leiutas Khatšjan elliptilise lahendusmeetodi, mis töötas garanteeritult polünomiaalses ajas. Praktikas osutus see meetod liiga keerukaks. Kulus umbes viis aastat enne, kui leiti esimene efektiivne polünomiaalne algoritm.

2 Algarvulisuse tõestused ehk sertifikaadid

Harilikult jaguneb väite tõestamine kolmeks loomulikuks etapiks: tõestuse idee otsimine, tõestuse genereerimine ning tõestuse verifitseerimine kolmanda osapoole poolt. Enamus klassifitseerivaid algoritme toimib just nii. Ainult idee asemel on esimese etapi väljundiks sertifikaat ning teine ja kolmas etapp on võetud kokku. Algarvulisuse korral on olemas loomulik definitsioonist lähtuv sertifikaat.

Lause (Definitsioonist lähtuv sertifikaat). *Naturaalarv p on algarv parajasti siis, kui kõik algarvud lõigust $[0, \sqrt{p}]$ ei jaga arvu p.*

TÕESTUS. On selge, et igal kordarvul n on olemas tegur, mis on väiksem või võrdne $\sqrt{n}$. Seega piisab kui kontrollida algarvulisust teguritega lõigust $[0, \sqrt{p}]$. □

On ilmne, et selline sertifikaat pole polünomiaalne arvu p pikkusest $\log p$ ning selle tõttu pole selle polünomiaalses ajas kontrollimine võimalik.

Järeldus. *Definitsioonist lähtuv sertifikaat on pikkusega $\Omega(\sqrt{p}(\log p)^{-1})$.*

TÕESTUS. Kuna x väiksemate algarvude arv $\pi(x) = \Theta(x(\log x)^{-1})$, siis on järeldus otsene. □

Kuna sellised sertifikaadid on kontrollimiseks liiga pikad, siis kasutatakse algarvulisuse kontrollimiseks Fermat' väikese teoreemi järeldust.

Teoreem. *Naturaalarv p on algarv parajasti siis, kui $\mathbb{Z}_p^* = \mathbb{Z}_p \setminus \{0\}$ omab moodustajat r, mille astmetena avalduvad kõik ülejäänud jäägiklassid.*

[3]Võrreldes Milleri algoritmiga on prooviastendajate arv tunduvalt suurem, aga tõestus väldib laiendatud Riemanni hüpoteesi.

[4]Ajalugu on korduvalt näidanud, et kui leitakse polünomiaalses ajas töötav algoritm, siis leitakse ka praktiliselt rakendatav algoritm.

TÕESTUS. Jäägiklassi ring $\mathbb{Z}_p$ on lõplik korpus parajasti siis, kui $p \in \mathbb{P}$. Kuna lõpliku korpuse multiplikatiivne rühm omab moodustajat, siis leidub moodustaja r nii, et $1 < r < p$. Teisalt kui $\mathbb{Z}_p^*$ on tsükliline, siis on iga nullist erinev element pööratav. □

Multiplikatiivne rühm $\mathbb{Z}_n^*$ on tsükline parajasti siis, kui leidub $r \in \mathbb{Z}_n$, mille poolt moodustatud multiplikatiivses rühmas $\langle r\rangle = \{1, r, \cdots, r^{k-1}\}$ on täpselt $n-1$ elementi. Elemendi r järk $\mathrm{ord}(r) = \#\langle r\rangle$ on vähim aste, mille korral kehtib kongruents $r^k \equiv 1 \mod n$. See annab lihtsa algarvulisuse sertifikaadi.

Järeldus (Klassikaline algarvulisuse sertifikaat). *Naturaalarv p on algarv parajasti siis, kui leidub selline arv $r \in [1, p-1]$ nii, et $r^{p-1} \equiv 1 \mod p$ ja iga $p-1$ algarvulise teguri q korral $r^{(p-1)/q} \not\equiv 1 \mod p$.*

TÕESTUS. Piisab kui kontrollida $r^{(p-1)/q} \not\equiv 1 \mod p$, sest kui mingi $p-1$ päristeguri d korral $r^{(p-1)/d} \equiv 1 \mod p$, siis siit järeldub, et leidub algarvuline tegur $q \mid d$ nii, et $r^{(p-1)/q} \equiv \left(r^{(p-1)/d}\right)^{d/q} \equiv 1 \mod p$. □

E.Lucase ja D.H.Lehmeri algarvulisuse testid kasutasid ära teada olevat[5] $n \pm 1$ tegurdust ning näitasid just nii arvu n algarvulisust. Üldisem lahendus on lisaks moodustajale r anda kaasa kõik $p-1$ algarvulised tegurid $q_1, q_2 \ldots, q_k$ ning seejärel lisada rekursiivselt q_i algarvulisuse sertifikaadid. Formaalselt kirja pannes saame algarvu p sertifikaadiks järjendi

$$S_p = (r, q_1, q_2 \ldots, q_k, S_{q_1}, S_{q_2}, \ldots, S_{q_k}), \quad p > 2, \qquad S_2 = (2).$$

Saab tõestada, et selline serifikaat on polünomiaalses ajas kontrollitav. Praktikas pole sellise sertifikaadi konstrueerimine reaalne. Seetõttu praagivad tõenäosuslikud algoritmid enamasti suure tõenäosusega kordarvud välja valides juhuslikult prooviastendaja, mis annab Fermat' väikese teoreemiga vastuolulise tulemuse.

Teoreem (Fermat' kordarvulisuse sertifikaat). *Naturaalarv n on kordarv parajasti siis, kui leidub $a \in \mathbb{Z}_n^*$ nii, et $a^{n-1} \not\equiv 1 \mod n$.*

TÕESTUS. On ilmne, et kordarvu teguri $a \mid n$ aste ei saa kunagi olla kongurentne 1, sest siis oleks a pööratav, mis on oodatud vastuolu. □

Kahjuks on olemas Carmichael'i arvud, mille korral iga pööratava $a \in \mathbb{Z}_n^*$ kehtib kongruents $a^{n-1} \equiv 1 \mod n$. Tõenäosus, et suvaliselt valitud arvude $\gcd(a, n) \neq 1$ on üldiselt tühine[6] ja seetõttu on Fermat' algarvu test liiga nõrk. Rabin-Milleri parandus põhineb lihtsal tähelepanekul, et algarvulise p korral on korpuses $\mathbb{Z}_p$ vaid kaks ruutjuurt arvust 1.

[5]Teatavaid arvuteoreetilisi konstruktsioone kasutades on võimalik asendada vajalik $n-1$ tegurdus $n+1$ tegurdusega.

[6]Eriti ilmekalt tuleb see välja, kui arvul on kaks algarvulist tegurit $n = p_1 p_2$ ja $p_1 \approx p_2$.

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

$$\begin{aligned} &\gcd(a,n) = 1 \\ &a^r \not\equiv 1 \mod n \\ &a^{2^i r} \not\equiv -1 \mod n, \qquad i = 1, \ldots, k-1 \end{aligned}$$

siis n on kordarv.

TÕESTUS. Kui n on algarv ja $\gcd(n,a) = 1$ ja $a^r \not\equiv 1 \mod n$, siis tekib meil ruutude jada

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

Lihtne on veenduda, et jadas peab olema selline aste $a^{2^j r}$ nii, et see pole kongruentne 1 ja millele järgnev $a^{2^{j+1}r} \equiv 1 \mod p$. Kuna korpuses $\mathbb{Z}_p$ ei saa polünoomil olla rohkem juuri, kui selle aste, siis 1 ja -1 on ainsad ruutjuured arvust 1. Seetõttu peab $a^{2^j r} \equiv -1 \mod n$.

Kui leidub tingimusi rahuldav arv a, siis kas $a^{n-1} \not\equiv 1 \mod n$ või viimane ühest erinev aste $a^{2^j r}$ on ruutjuureks 1 ning samas pole kongruentne 1 või -1. □

Rabin-Milleri algoritmi annab kordarvu korral välja kordarvulisuse sertifikaadi tõenäosusega vähemalt $1/2$, mis praktiliselt lahendab kogu algarvulisuse kontrolli, kuna algoritmi keerukus on $O(\log^3 n)$.

Uus lähenemine, mis võimaldab polünomiaalses ajas toimivat algarvu testi, põhineb väga lihtsal modulaarsel võrratusel.

Lause 1. *Olgu naturaalarvud a ja p ühistegurita, siis p on algarv parajasti siis, kui kehtib modulaarne võrdus $(x-a)^p \equiv x^p - a^p \mod p$.*

TÕESTUS. Tõestuseks paneme tähele, et kui $p \in \mathbb{P}$ ja $i \neq 0,\ i \neq p$, siis $p \mid \binom{p}{i}$ ning Newtoni binoomvalemi vahepealsed liikmed taanduvad välja. Teisalt kui $1 < q < p$ on p tegur, siis leidub suurim aste k nii, et $q^k \mid p$. Binomiaalkordaja $\binom{p}{q}$ ei jagu arvuga p, sest binoomkordaja

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

lugejas pole ühtegi tegurit peale p, mis jaguks arvuga q. Kuna a ja p on ühistegurita, siis $a^q \not\equiv 0 \mod p$ ja seega kongurents $(x-a)^p \equiv x^p - a^p \mod p$ ei saa kehtida. □

Otseselt on võrduse kontrollimine liiga töömahukas kuna võrratuse vasakul poolel on tarvis arvutada $\Omega(p)$ tegurit. Et vähendada töömahtu võib vaadata polünoome ringis $\mathbb{Z}_p[x]/(x^r - 1)$. Loomulikult kui p on algarv, siis kehtib kongruents $(x-a)^p \equiv x^p - a^p \pmod{p, x^r - 1}$. Kuid iga r ja a valiku korral pole garanteeritud vastupidine implikatsioon. Järgnevalt keskendumegi probleemile, kuidas valida r ja a nii, et test eristaks kõik kordarvud algarvudest.

3 Agrawal-Kayal-Saxena sertifikaat

3.1 Fakte lõplike korpuste teooriast

Lemma 1. *Iga lõplik korpus on isomorfne korpusega $\mathbb{F}_{p^t}$, mis on polünoomi $x^{p^t} - x = 0$ lahutuskorpus. Lõpliku korpuse multiplikatiivne $\mathbb{F}^*_{p^t}$ rühm on tsükliline.*

TÕESTUS. Vaata näiteks raamatut [LP98, lk.138-140]. □

Lemma 2. *Iga täisarvulise kordajatega polünoomi f korral kehtib kongruents $f(x)^p \equiv f(x^p) \mod p$.*

TÕESTUS. Kõige lihtsam tõestus on induktsiooniga üle polünoomi f astme. Kui $\deg f = 1$, siis järeldub see Fermat' väikesest teoreemist. Iga n-astme polünoomist saab eraldada pealiikme $f(x) = f_1(x) + a_0x^n$, kus $\deg f_1 < n$. Lause 1 tõttu

$$f(x)^p \equiv (f_1 + a_0x^n)^p \equiv f_1(x)^p + a_0^p x^{np} \equiv f_1(x)^p + a_0(x^p)^n \equiv f(x^p) \mod p.$$

□

Lemma 3. *Kui r algarv ja $h(x) \in \mathbb{Z}[x]$ on polünoomi $x^r - 1$ tegur, siis kehtib implikatsioon*

$$k \equiv l \mod r \qquad \Rightarrow \qquad x^k \equiv x^l \mod h(x).$$

TÕESTUS. Et $x^r \equiv 1 \mod x^r - 1$, siis iga $q \in \mathbb{Z}$ korral $x^{qr} \equiv 1 \mod x^r - 1$. Kuna $k \equiv l \mod r$, siis $k = qr + l$ ning $x^l \equiv x^k x^{qr} \equiv x^k \mod x^r - 1$, millest järeldubki antud kongruents. □

Lemma 4. *Olgu algarvu p järk d algarvulise mooduli r järgi, siis korpuses[7] $\mathbb{F}_p$ lahutub polünoom $1+x+\cdots+x^{r-1} = \frac{x^r-1}{x-1}$ taandumatuteks d astme polünoomide korrutiseks.*

TÕESTUS. Tähistame $d = \operatorname{ord}_r(p)$. Olgu $h(x)$ polünoomi $1 + x + \cdots + x^{r-1}$ taandumatu tegur astmega k. Siis saame lõpmatu korpuse $\mathbb{F}_p[x]/\big(h(x)\big) \simeq \mathbb{F}_{p^k}$. Tähistame selle korpuse multiplikatiivse rühma moodustajat $g(x) \in \mathbb{F}_p[x]$. Tänu lemmadele 2 ja 3 saame kongruentside ahela

$$\begin{aligned}
& & g(x)^p &\equiv g(x^p) \quad \mod p \\
& \Rightarrow & g(x)^{p^d} &\equiv g\Big(x^{p^d}\Big) \quad \mod p \\
p^d \equiv 1 \mod r \quad & \Rightarrow & g(x)^{p^d} &\equiv g(x) \quad \big(\operatorname{mod} p, h(x)\big)
\end{aligned}$$

Kuna $F[x]/\big(h(x)\big)$ on korpus, siis $x^{p^d-1} \equiv 1 \ \big(\operatorname{mod} p,^h(x)\big)$. Teisalt moodustaja $g(x)$ järk on $p^k - 1$, millest $(p^k - 1) \mid (p^d - 1)$. Tingimus$(p^k - 1) \mid (p^d - 1)$ on samaväärne tingimusega[8] $k \mid d$. Kuna $h(x) \mid x^r - 1 \mod p$, siis korpuses $\mathbb{F}_{p^k}$ on $x^r \equiv 1 \ \big(\operatorname{mod} p, h(x)\big)$. Kuna r on algarv, siis x järk korpuses $\mathbb{F}_{p^k}$ on r, millest $r \mid p^k - 1$ ehk $p^k \equiv 1 \mod r$. Algarvu p järk d peab jagama k ning $k = d$. □

[7] Edaspidi tähistame $\mathbb{Z}_p$ sümboliga $\mathbb{F}_p$ rõhutamaks fakti, et $\mathbb{Z}_p$ on korpus.
[8] Seda on kõige lihtsam tõestada induktsiooniga üle d.

Lemma 5. *Olgu r ja p algarvud ning $d = \operatorname{ord}_r(p)$. Kui h 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*

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

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

TÕESTUS. On selge, et struktuur G on kinnine korrutamise ja ühikelemendi võtmise suhtes. Teisalt teame $x - a_i \not\equiv 0 \big(\operatorname{mod} p, h(x)\big)$ ja seega lineaarpolünoomi $x - a_i$ astmed moodustavad tsüklilise rühma korpuses $\mathbb{F}_p[x]/\big(h(x)\big)$. See annabki G kinnisuse pöördelemendi võtmise suhtes. Rühma G tsüklilisus tuleneb korpuse multiplikatiivse rühma tsüklilisusest.

Vaatame nüüd G alamhulka S, mis on defineeritud järgnevalt

$$S = \left\{ \prod_{i=1}^{l} (x-a_i)^{\beta_i} \;\Big|\; \sum_{i=1}^{l} \beta_i \le d-1,\ 0 \le \beta_i, a = 1, 2, \ldots, l \right\}.$$

Veendume, et kõik paremal pool toodud elemendid eristuvad teineteisest korpuses $F_p[x]/\big(h(x)\big)$. Kuna lineaartegurid $x - a_i$ ei ole kongurentsed mooduli p järgi, siis eristuvad polünoomid mooduli p järgi, kuna neil on erinevad juured korpuses $\mathbb{F}_p$. Et lemma 4 järgi peab polünoomi h aste olema $d = \operatorname{ord}_r(p)$ ja polünoomide aste on ülimalt $d - 1$, siis eristuvad korrutised ka suuremas korpuses.

Et iga korrutis on üheselt määratud selle astmetega, siis on hulgas S sama palju elemente kui kordumistega kombinatsioone $F(l+1, d-1)$, st.

$$F(l+1, d-1) = \binom{l+d-1}{l} = \frac{(l+d-1)(l+d-2)\cdots(d)}{l!} > \left(\frac{d}{l}\right)^l.$$

□

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

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

Lemma 6. *Polünoomi $g(x)$ võrdsustajate hulk $I_{g(x)}$ on kinnine korrutamise suhtes.*

TÕESTUS. Olgu $m_1, m_2 \in I_{g(x)}$, siis kehtib kongruentside paar

$$\begin{aligned} g(x)^{m_1} &\equiv g(x^{m_1}) \ (\operatorname{mod} p, x^r - 1), \\ g(x)^{m_1} &\equiv g(x^{m_1}) \ (\operatorname{mod} p, x^r - 1). \end{aligned}$$

Asendades teise võrdusesse x asemel x^{m_1}, saame kongruentsi

$$g(x^{m_1})^{m_2} \equiv g(x^{m_1 m_2}) \ (\operatorname{mod} p, x^{m_1 r} - 1).$$

Kuna $x^r - 1$ jagab $x^{rm_1} - 1$, siis kehtib ka järgmine kongruents

$$g(x^{m_1})^{m_2} \equiv g(x^{m_1 m_2}) \pmod{p, x^r - 1}$$

ning seega saame teisendada

$$g(x)^{m_1 m_2} \equiv (g(x)^{m_1})^{m_2} \equiv g(x^{m_1})^{m_2} \equiv g(x^{m_1 m_2}) \pmod{p, x^r - 1}.$$

□

Lemma 7. *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. Tõestuseks kasutame ära hulga $I_{g(x)}$ omadusi. Esmalt kuna $m_1 \equiv m_2 \mod r$, siis $m_1 = kr + m_2$ ning kehtib kongruents

$$g(x)^{m_2} \equiv g(x^{m_2}) \pmod{p, x^r - 1} \qquad \Rightarrow \qquad g(x)^{m_2} \equiv g(x^{m_2}) \big(\operatorname{mod} p, h(x)\big).$$

Kasutades ära lemmat 3 ja arvu m_2 esitust $m_2 = kr + m_1$ saame kongruentsi

$$g(x)^{m_1} g(x)^{kr} \equiv g(x)^{m_2} \equiv g(x^{m_1 + kr}) \equiv g(x^{m_1}) \big(\operatorname{mod} p, h(x)\big).$$

Kuna $m_1 \in I_{g(x)}$, siis viimasest kongruentsist järeldub

$$g(x)^{m_1} g(x)^{kr} \equiv g(x)^{m_1} \big(\operatorname{mod} p, h(x)\big).$$

Et korpuses $F_p[x]/\big(h(x)\big)$ saab elemendiga $g(x)$ taandada, siis kehtib kongruents $g(x)^{kr} \equiv 1 \big(\operatorname{mod} p, h(x)\big)$. Seetõttu jagab $g(x)$ järk korrutist kr, millest tuleneb kongruents $m_2 \equiv m_1 \mod d_g$. □

3.2 Sertifikaadi korrektsus

Järgnevas defineerime Agrawal-Kayal-Saxena sertifikaadi ning veendume, et saadud sertifikaat on korrektne. Siin me ei käsitle, kas iga arvu korral on sellist sertifikaati üldse võimalik leida. Me näitame, et kui serifikaat teatud omadustega algarv r on olemas ja n pole täisarvu aste, siis on võimalik veenduda, kas n on algarv või kordarv. Selleks tõestame esmalt kaks tehnilist abilemmat.

Lemma 8. *Kui algarv q jagab kordarvu n järku $\operatorname{ord}_r(n)$ ja n ja r on ühistegurita, siis leidub arvu n selline algarvuline tegur p, mille korral $q \mid \operatorname{ord}_r(p)$.*

TÕESTUS. Avaldades $n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$ on selge $n^{\operatorname{lcm}_i \operatorname{ord}_r(p_i)} \equiv 1 \mod r$ ning seega $\operatorname{ord}_r(n) \mid \operatorname{lcm}_i \operatorname{ord}_r(p_i)$. Kuna q on algarv, siis peab tõesti leiduma p_j nii, et $q \mid \operatorname{ord}_r(p_j)$. □

Lemma 9. *Iga reaalarvu $x > 2$ kehtib järgmine võrratus $\left(\frac{x}{\lfloor \frac{x}{2} \rfloor}\right)^{\lfloor \frac{x}{2} \rfloor} \geq 2^{\frac{x}{2}}$.*

Tõestus. Esmalt paneme tähele, et suurus $x/\lfloor x/2 \rfloor$ kuulub alati lõiku $[2, 4]$. Nüüd vaatame abifunktsiooni $f(y) = y - 2^{y/2}$ ning veendume, et lõigus $[2, 4]$ on funktsioon kumer(allapoole kaardus). Kuna $f'(y) = 1 - \ln 2 \cdot 2^{y/2}/2$ on monotoonselt kahanev funktsioon, siis on kumerus ilmne. Kumera funktsiooni väärtused lõigus on suuremad kui otspunktides ning $f(2) = 0$ ja $f(4) = 0$, siis $f(y) \geq 0$ lõigus $[2, 4]$, millest järeldubki esialgne võrratus. □

Teoreem 1 (Agrawal-Kayal-Saxena sertifikaat).
Olgu meid huvitav naturaalarv n, mis ei ole ühegi naturaalarvu m aste. Kui r on selline algarv, mis rahuldab kolme tingimust:
1) iga algarv $s \leq r$ on arvuga n ühistegurita,
2) leidub $r - 1$ algarvuline tegur $q \geq 4\sqrt{r} \log n$,
3) $q \mid \operatorname{ord}_r(n)$,
siis n on algarv parajasti siis, kui on täidetud kongruentside süsteem

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

Tõestus.
Tarvilikkus. Kui n on algarv, siis iga naturaalarvu a korral kehtib kongruents $(x - a)^n \equiv x^n - a^n \mod p$ ning seega ka AKS-testi kongruentsid.

Piisavus. Oletame vastuväiteliselt, et n on kordarv ning on täidetud AKS-testi kongruentsid. Siis lemmast 8 järeldub, et leidub n algarvuline tegur p, mille korral $q \mid d = \operatorname{ord}_r(p)$. Lemma 4 tõttu on iga polünoomi $x^r - 1$ taandumatu teguri $h(x)$ aste on $d = \operatorname{ord}_r(p)$. Seega on mõtet vaadate korpust $\mathbb{F}_p[x]/(h(x))$ ning selle $l = \lfloor 2\sqrt{r} \log n \rfloor < q < r$ lineaarteguri $x - a$ poolt genereeritud tsüklilist rühma

$$G = \langle (x - a), \ a = 1, 2, \ldots, l \rangle.$$

Rühma G generaator $g(x)$ on korrutis lineaartegurite $x - a$ astmetest ning seega järeldub AKS-testi kehtimisest kongruents

$$g(x)^n \equiv g(x^n) \ (\operatorname{mod} p, x^r - 1).$$

See tähendab, et polünoomi $g(x)$ võrdsustajate hulka kuulub $n \in I_{g(x)}$. Teisalt on selge, et $1 \in I_{g(x)}$ ja tänu lemmale 2 ka $p \in I_{g(x)}$. Olgu polünoomi $g(x)$ järk korpuses $F_p[x]/(h(x))$ arv d_g. Järgnevalt näitame, et võrdsustajas $I_{g(x)}$ leidub palju elemente, mis on väiksemad kui d_g. Selleks vaatame hulka

$$E = \{ n^i p^j \mid 0 \leq i, j \leq \lfloor \sqrt{r} \rfloor \}.$$

Kuna elemendid on n ja p poolt genereeritud, siis lemmast 6 järeldub $E \subseteq I_{g(x)}$. Kuna hulga E elementide arv $\#E = (1 + \lfloor \sqrt{r} \rfloor)^2 > r$, siis leidub kaks erinevat elementi, mis on kongruentsed mooduli r järgi. Lemmast 7 järeldub sellest

$$n^{i_1} p^{j_1} \equiv n^{i_2} p^{j_2} \mod r \qquad \Rightarrow \qquad n^{i_1} p^{j_1} \equiv n^{i_2} p^{j_2} \mod d_g$$

Vastavalt i_1, i_2, j_1 ja j_2 valikule $p^{j_1}, p^{j_2} < n^{\sqrt{r}}$ ja $n^{i_1}, n^{i_2} \leq n^{\sqrt{r}}$. Kui meil õnnestub näidata $d_g \geq n^{2\sqrt{r}}$, siis muutub kongruents võrduseks. Rühma G genereerivad lineaartegurid peavad olema erinevad mooduli p järgi, vastasel korral leiduks tegur $a_i - a_j < r$, mis jagaks n. Polünoomi $g(x)$ järk on sama, mis rühma G elementide arv. Kuna q jagab d, siis saame alumise hinnangu

$$d_g = \#G > \left(\frac{d}{l}\right)^l \geq \left(\frac{q}{l}\right)^l = \left(\frac{4\sqrt{r}\log n}{\lfloor 2\sqrt{r}\log n\rfloor}\right)^{\lfloor 2\sqrt{r}\log n\rfloor}$$

Tehnilist lemmat 9 rakendades saame võrratuse $d_g \geq n^{2\sqrt{r}}$, mistõttu kehtib võrdus $n^{i_1}p^{j_1} = n^{i_2}p^{j_2}$. Seda teisendades saame $n^{i_1-i_2} = p^{j_2-j_1}$, mis on võimalik vaid siis, kui n on algarvu p aste. See on vastuolus teoreemi eeldustega ning seega ei saa ükski teoreemi eeldustele vastav kordarv rahuldada AKS-testi. $\square$

3.3 Sertifikaadi leidumine

Eelnevas osas näitasime, et algarvulisuse kontrollimiseks on piisav leida algarv r, mis rahuldas kolme tingimust:

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

Seejärel taandus algarvulisuse kontroll teatud kongruentside süsteemi kehtivusele. See annab meile õiguse nimetada r alg- või kordarvulisuse sertifikaadiks olenevalt arvu n ehitusest. Järgnevas näitame, et iga naturaalarvu n korral leidub selline sertifikaat või on n kergesti tegurdatav. Ühtlasi on see ka ainus tõestuse osa, mis kasutab algarvude kohta käivaid fundamentaalseid tulemusi.

Teoreem 2 ([Fou85][BH96]). *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 3 ([Apo97]). *Tähistagu $\pi(n)$ algarvude arvu, mis on väiksemad kui n. Siis iga $n \in \mathbb{N}$ kehtivad võrratused*

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

Teoreem 4 (Sertifikaadi olemasolu 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 $q \geq 4\sqrt{r}\log n$ ja q jagab n järku $\mathrm{ord}_r(n)$.*

TÕESTUS. Tõestuseks vaatame eriliste algarvude hulka

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

Kasutades teoreemides 2 ja 3 toodud tulemusi on lihtne hinnata hulga $\mathcal{R}$ elementide arvu

$$\#\mathcal{R} \geq \#\mathcal{Q}_{c_2 \log^6 n} - \pi(c_1 \log^6 n) \geq \frac{cc_2 \log^6 n}{7 \log\log n} - \frac{8c_1 \log^6 n}{6 \log\log n},$$
$$\#\mathcal{R} \geq \frac{\log^6 n}{\log\log n}\left(\frac{cc_2}{7} - \frac{8c_1}{6}\right) = c_3 \frac{\log^6 n}{\log\log n},$$

kui vaid $c_2 \leq \log n$. Kui valida $c_1 > 4^6$, siis on võimalik valida c_2 nii, et $c_3 > 0$. On lihtne veenduda, et hulgas $\mathcal{R}$ olevad algarvud r rahuldavad esimest kahte tingimust, sest $q \geq r^{2/3} \geq 4\sqrt{r}\log n$. Kindlustame kolmanda tingimuse $q \mid \mathrm{ord}_r(n)$. Selleks näitame, et leidub selline $r \in \mathcal{R}$ nii, et $\lfloor r^{1/3} \rfloor < \mathrm{ord}_r(n)$. Eelduste tõttu on $\mathrm{ord}_r(n) \mid r-1$ ning $r-1$ suurim tegur $q > r^{2/3}$, millest järeldub $q \mid \mathrm{ord}_r(n)$. Paneme tähele, et kui moodustada korrutis

$$\Pi = (n-1)(n^2-1)\cdots(n^{\lfloor x^{1/3} \rfloor} - 1),\ \text{kus } x = c_2 \log^6 n,$$

siis selles korrutises on ülimalt $x^{2/3}\log n$ algarvulist tegurit. Sest arvul $10 \leq m$ saab olla vaid $\log m/\log 3 \geq 0.63 \log m$ erinevat algarvulist tegurit ning seega saame

$$0.63 \log \Pi \geq 0.63 \log n \sum_{i=1}^{\lfloor x^{1/3} \rfloor} i \geq x^{2/3} \log n.$$

Samas saab kergesti kontrollida, et kui n on piisavalt suur, siis

$$x^{2/3} \log n < \log^5 n < \frac{c_3 \log^6 n}{\log\log n} \leq \#\mathcal{R}.$$

Seetõttu peab tõesti leiduma $r \in \mathcal{R}$, mis ei jaga korrutist Π. □

3.4 Sertifikaadi kontrollimise keerukus

Teoreem 5 (Sertifikaadi kontrollimise polünomiaalsus).
Olgu r algarv intervallist $[c_1 \log^6 n, c_2 \log^6 n]$, siis kongruentside süsteemi

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

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

TÕESTUS. On selge, et tuleb väärtustada $O(\log^4 n)$ kongruentsi vasakut poolt. Kui kasutada kiiret astendamisalgoritmi, siis tuleb ühe astendamise korral teha $O(\log n)$ korrutamist. Kuna arvutamine käib mooduli $x^r - 1$ järgi, siis saab polünoomide astme hoida väiksema kui r. Koolimatemaatikast tuntud korrutamise ja jagamise algoritmid kasutavad r astme polünoomide korrutamiseks $O(r^2)$ tehet ringis $\mathbb{Z}_n$. Analoogsete algoritmide kasutamisel võtab üks $\mathbb{Z}_n$ tehe $O(\log^2 n)$ elementaaroperatsiooni. Astendamine võtab kokku $O(r^2 \log^3 n)$ elementaaroperatsiooni. Kogu süsteemi kontrollimiseks kulub $O(\log^{19} n)$ elementaaroperatsiooni.

Efektiivsed arvutialgebra algorimid võimaldavad keerukust oluliselt vähendada. Kahe polünoomi f ja g korrutis mooduli $x^r - 1$ järgi nimetatakse polünoomide konvolutsiooniks. Kui ring $\mathbb{Z}_n$ sisaldaks primitiivset r astme ühejuurt, siis oleks võimalik kasutada astendamisel kiiret Fourier' diskreetset teisendust, mis tähendaks $O(\log n \log \log n)$ ringi tehet. Et ringis $\mathbb{Z}_n$ ei pruugi olla primitiivset r astme ühejuurt, siis peaks kasutama Schönhage ja Strasseni(1971) algoritmi, mis lisab vajalikud ühejuured ning teeb seejärel kiire Fourier' teisenduse. Algoritmi analoogi saab kasutada $\mathbb{Z}_n$ tehete tegemisel, mis teeb ühe kongruentsi kontrollimiseks $\widetilde{O}(r \log^2 n)$ elementaaroperatsiooni. See teeb kogu kongruentside süsteemi kontrollimiseks $\widetilde{O}(\log^{12} n)$. $\square$

4 Agrawal-Kayal-Saxena algarvutest

Kuna Agrawal-Kayal-Saxena sertifikaat algarv r on $O(\log^6 n)$, siis hoolimata sertifikaadile seatud keerulistest tingimustest, saame polünomiaalses ajas eraldada kordarvud ja algarvud. Tuleb vaid lisada täisarvu astmete eraldamine, kuna sertifikaat ei kehti täisarvu astme korral. Seejärel kindlustame sertifikaadi või teguri leidmise.

Agrawal-Kayal-Saxena algoritm

Sisend: naturaalarv $n > 1$.

Väljund: PRIME või COMPOSITE.

```
*** Eraldame naturaalarvude täisastmed ***
if (∃a, b ∈ ℕ :   a^b = n)  return COMPOSITE;
r = 2;
*** Otsime Agrawal-Kayal-Saxena setrifikaati ***
while (r < n)
{
   *** Kui gcd(n, r) ≠ 1, siis on n kordarv ***
   *** Selle sündmuse tõenäosus on kaduvväike ***
   if (gcd(n, r) ≠ 1)  return COMPOSITE;
   *** Kontrollime, kas r on sobib sertifikaadiks ***
   if (r ∈ ℙ)
   {
      q = P(r − 1);
      if (q ≥ 4√r log n  and n^((r−1)/q) ≢ 1  mod r) break ;
   }
  r = r + 1;
}
*** Kontrollime saadud sertifikaati ***
for a = 1  to ⌊2√r log n⌋
{
   *** Kui n on algarv, siis a^n ≡ a  mod n ***
   if ((x − a)^n ≢ x^n − a (mod n, x^r − 1)) return COMPOSITE;
}
return PRIME;
```

Lemma 10. *Leidub determineeritud algoritm keerukusega $O(\log^3 n)$, mis iga naturaalarvu n korral teeb kindlaks, et n on täisaste st. leiab $a, b \in \mathbb{N}$ nii, et leidu$n = a^b$.*

TÕESTUS. Paneme tähele, et võimalik astendaja on tõkestatud $b < \log n$, mistõttu tuleb kontrollida vaid $O(\log n)$ esimest juurt. Teisalt on astmefunktsioon monotoonselt kasvav, seega piisab juure leidmiseks korraldada hulgas $\{0, 1, \ldots, n\}$ kahendotsing. Kahendotsingule kulub ülimalt $O(\log n)$ astme väärtustust. Ühe väärtustusele kulub kiiret astendamise algoritmi kasutades $O(\log b \log^2 n)$. Seega kõikide astmete kontrollimiseks kulub kokku $\widetilde{O}(\log^4 n)$. Jällegi on tegu ülehinnanguga, sest kehtib võrratus $2^{\lfloor \frac{\log n}{m} \rfloor} < \sqrt[b]{n} < 2^{\lceil \frac{\log n}{m} \rceil}$ ja juurte arvutamisel võib kasutada kiiremini koonduvaid meetodeid nagu Newtoni iteratsioonimeetod, mis on ruutkoonduvusega. □

Lemma 11. *Programm leiab $\widetilde{O}(\log^9 n)$ elementaaroperatsiooniga Agrawal-Kayal-Saxena sertifikaadi r või mõne mittetriviaalse n algteguri.*

TÕESTUS. Teoreemi 4 tõttu leidub selline $n_0 \in \mathbb{N}$ nii, et $n > n_0$, siis tehakse `while`-tsüklis ülimalt $O(\log^6 n)$ iteratsiooni. Suurima ühisteguri arvutamine võtab Eukleidese algoritmi kasutades $O(\log^2 r)$ elementaaroperatsiooni. Algarvulisuse kontrolliks võib kõik seni leitud algarvud salvestada ja kontrollida algarvulisust vastavalt definitsioonile. Kuna r väiksemaid algarve on $O(r)$, siis selle kontrollimine võtab ülimalt $O(r^3)$ elementaaroperatsiooni. Analoogselt $r-1$ suurima algarvulise teguri leidmine võtab ülimalt $O(r^3)$ elementaaroperatsiooni. Astendamine võtab kiiret astendamisalgoritmi kasutades $O(\log^3 r)$ elementaaroperatsiooni. Seega saame ülehinnangu $O(\log^{24} n)$. Tegelik hinnang efektiivselt realiseeritud algoritmi korral on $\widetilde{O}(\log^9 n)$. □

Teoreem 6 (Algoritmi keerukushinnang). *Agrawal-Kayal-Saxena algoritm teeb $\widetilde{O}(\log^{12} n)$ elementaaroperatsiooniga kindlaks, kas naturaalarv n on algarv või mitte.*

TÕESTUS. Algoritmi korrektsus järeldub teoreemist 1 ning hinnangud tööajale järelduvad lemmadest 10 ja 11 ning teoreemist 5. □

5 Võimalikud täiustused

Hetkel on teada kaks hüpoteesi, mis vähendaksid algarvulisuse kontrolli algoritmi keerukust. Esimene neist Sophie Germain'i algarvukaksikute tihedushinnang, mis võimaldab parandada algoritmi keerukushinnangut ilma algoritmi muutmata. Samas teine hüpotees võimaldaks algoritmi modifitseerida nii, et selle keerukus oleks $\widetilde{O}(log^3 n)$ elementaaroperatsiooni. See on vaid suurusjärgu võrra halvem Rabin-Milleri testi keerukusest $\widetilde{O}(\log^2)$.

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

Hüpotees 1 ([HL22]). *Sophie Germain kaasalgarvude arv $S(x)$ lõigus $[0, x]$ on asümptootiliselt ekvivalentne suurusega $\frac{Dx}{\log^2 x}$, kus konstant $D \approx 0.6617$.*

Lemma 12. *Kui kehtib hüpotees 1, siis leiduvad positiivsed konstandid c_2 ja n_0 nii, et iga naturaalarvu $n > n_0$ korral leidub intervallis $[65 \log^2 n, c_2 \log^2 n]$ on algarv r, mille korral $r-1$ omab algarvulist tegurit $q \geq 4\sqrt{r} \log n$ ja q jagab n järku $\mathrm{ord}_r(n)$.*

TÕESTUS. Kui r ja $q = \frac{r-1}{2}$ on algarvud, siis võimalikud n järgud mooduli r järgi on 1, 2, q ja $2q$. Kuna $n^2 - 1$ on ülimalt $2\log n$ algarvulist tegurit, siis on ülimalt $2\log n$ Sophie kaasalgarvude korral $\mathrm{ord}_r(n) \in \{1,2\}$. Nõue, et $q \geq 4\sqrt{r}\log n$ järeldub piisavalt suure n korral võrdusest

$$\begin{array}{rlcl} & r \geq 65\log^2 n & \Rightarrow & \sqrt{r} \geq 8\log n + 1 \\ \Rightarrow & \sqrt{r} - \dfrac{1}{\sqrt{r}} \geq 8\log n & \Rightarrow & \dfrac{r-1}{2} \geq 4\sqrt{r}\log n. \end{array}$$

Kasutades ära hüpoteesi saame hinnata intervallis $[65\log^2 n, c_2\log^2 n]$ olevate Sophie kaasalgarvude hulka T, mis sobivad sertifikaadiks

$$T \geq c\big(S(c_2\log^2 n) - S(65\log^2 n) - 2\log n\big),$$
$$T \geq c\left(\frac{Dc_2\log^2 n}{\log^2(c_2\log^2 n)} - \frac{D64\log^2 n}{\log^2(64\log^2 n)} - 2\log n\right).$$

Kui n on piisavalt suur, siis $c \leq \log n$ ja $(\log\log n)^2 \leq \log n$, siis saame alumiseks hinnanguks

$$T \geq c\left(\frac{Dc_2\log^2 n}{9(\log\log n)^2} - \frac{D64\log^2 n + 2\log^2 n}{(\log\log n)^2}\right).$$

ning seega saab leida konstandi c_2 väärtuse, mille korral on sulgavaldis positiivne. Kuna c on positiivne konstant, mis ei sõltu n väärtusest, siis on lemma tõestatud. □

Teoreem 7 (Täpsustatud keerukushinnang). *Kui kehtib hüpotees 1 siis Agrawal-Kayal-Saxena algoritmi keerukuseks on $\widetilde{O}(\log^6 n)$ elementaaroperatsiooni.*

TÕESTUS. Kuna leitav setifikaat r on väiksem, siis langeb otsimise keerukus $\widetilde{O}(\log^3 n)$ ja kontrollimise keerukus $\widetilde{O}(\log^6 n)$ elementaaroperatsioonini. □

Hüpotees 2. *Kui algarv r ei jaga naturaalarvu n ja kehtib kongruents*

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

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

Kui see hüpotees on tõene, siis piisab algarvulisuse kontrollimiseks leida r, mis ei jagaks arvu $n^2 - 1$. Et k-nda algarvu p_k suurus on hinnatav

$$k(\ln k + \ln\ln k - 3/2) < p_k < k(\ln k + \ln\ln k - 1/2), \qquad k \geq 20,$$

siis tuleks läbi vaadata suurusjärgus $\widetilde{O}(\log n)$ algarvu. Jaguvuse kontroll võtab optimaalselt realiseerides $\widetilde{O}(\log n)$ ning algarvude leidmine naiivse algoritmiga $O(r^3)$ elementaaroperatsiooni. Kongurentsi kontrollimine kasutades efektiivset korrutamisalgoritmi võtab ülimalt $\widetilde{O}(\log^3 n)$ elementaaroperatsiooni. See jääks vaid suurusjärgu võrra alla hetkel teada olevatele parimatele algarvutestidele ning omaks praktilist rakendust tõenäosuslike algoritmide verifitseerijana.

6 Kokkuvõtte asemel

Töö esma-eesmärgiks oli tutvustada uut põhjapanevat tulemust arvutialgebra valdkonnast. Et lugejad tajuksid lahenduse uudsust ning sellest tulenevaid järeldusi, oleme omalt poolt püüdnud anda ka ülevaate probleemi ajaloost. Sealjuures selgitasime tulemuse seost teiste krüptoloogias ning keerukusteoorias esinevate probleemidega. Lühidalt käsitletud lahenduse tähtsuse(tuse)st keerukusteoorias tuues paralleele analoogilise staatusega lineaarplaneerimise ülesandega. Ajaloolise ülevaate koostamiseks kasutasime allikaid [Co91], [MOV97], [NoWr99], [Bur80], [Mih] ja [Pin93]. Arvuteoreetiliste faktide ja tõenäosuslike testide kirjeldused pärinevad peamiselt materjalidest [MOV97], [Ble96] ning [La01]. Mahult kõige suurem ning sisult olulisim osa on pühendatud Agrawal-Kayal-Saxena algoritmile [AKS02]. Arusaadavuse huvides on esialgset käsitlust veidi muudetud tuues sisse alg/kordarvulisuse sertifikaadi mõiste, mis peaks algoritmi korrektsuse tõestusest arusaamist lihtsustama. Ka on selguse mõttes välditud täpseid keerukushinnanguid, näidates lihtsaid ülemhinnanguid ja tuues ära hetkel teada olevate parimate algoritmide keerukuse. Täienduste ja hüpoteeside osa annab ligikaudse hinnangu kui head tulemust võiks üldse loota, viimane põhineb materjalidel [AKS02] ja [KS02].

Kokkuvõtlikult öeldes on AKS-algoritmi näol tegemist täiesti uue lähenemisega. See garanteerib polünomiaalse keerukuse, kuid on praktiliseks realiseerimiseks ebaefektiivne. Kuid on loota uutel ideedel põhinevaid efektiivsemaid ja praktilisemaid algoritme.

Viited

[AKS02] Manindra Agrawal, Neeraj Kayal, Nitin Saxena, *PRIMES is in P*, 2002.

[Apo97] T.M. Apostol,*Introduction to analytic Number Theory*, Springer-Verlag, 1997.

[BH96] R.C.Baker, G.Harman *The Brun-Titchmarsh Theorem on average*, In Procceedings of a converence in Honor of Heini Halberstam, Volume 1, pages 39-103, 1996.

[Ble96] D. Bleichenbacher, *Efficiency and Security of Cryptosystems based on Number Theory*, 1996.

[Bur80] D.Burton, *Elementary Number Theory*,1980.

[Co91] E.J.Borowsky, J.M.Borwein, *Dictionary of Mathemathics*,HarperCollinsPublishers, 1991.

[Fou85] E. Fouvry,*Theoreme de Brun-Titchmarsh; application au theoreme de Fermat*, Invent. Math.,79:383-407, 1985.

[HL22] G.H.Hardy, J.E.Littlewood,*Some problems of 'Partio Numeroum' III: On thr expression of a number as sum of primes*, Acta Mathematica, 44:1-70,1922.

[KS02] Neeraj Kayal and Nitin Saxena,*Towards a deterministic polynomial-time test*, Technical report, IIT Kanpur, 2002.

[MOV97] Alfred J. Menezes, Paul C. van Oorshot, *Handbook of Applied Crypthography*, CRC Press, 1997.

[NoWr99] Jorge Nocedal, *Numerical Optimization*, Springer, 1999.

[La01] V. Laan,*Arvutialgebra algoritmide loengukonspek: Alagarvulisuse kontrollimine*, 2001.

[LP98] R. Lidl, G.Pilz *Applied Abstract Algebra*, Springer, 1998.

[Mih] Preda Mihăilescu, *Recent Developments in Primality Proving.*

[Pin93] R.G.E. Pinch *Some primality testing algorithms*, 1993.