Tartu Ülikool
Loodus- ja täppisteaduste valdkond
Matemaatika ja statistika instituut

Kadri Sügis

Algarvuvalemitest

Matemaatika eriala
Bakalaureusetöö (9 EAP)

Juhendaja Lauri Tart

Tartu 2018

Algarvuvalemitest

Bakalaureusetöö

Kadri Sügis

Lühikokkuvõte. Peamiselt eelmisel sajandil püüti algarvude uurimisel leida abi nn algarvuvalemitest, st (osaliselt) algarvuliste väärtustega funktsioonidest. Bakalaureusetöös tehakse ülevaade valitud algarvuvalemitest ja nendega seotud tulemustest. Vaadeldakse algarvuliste väärtustega polünoome, Willansi, Sierpiński, Gandhi, Millsi, Wrighti ja veel mitmeid algarvuvalemeid. Töös antakse üksikasjalik tõestus Isenkrahe, Hardy ja Wrighti ning Saouteri valemile. Tuuakse rida näited, mis muuseas demonstreerivad kõigi käsitletud valemite arvutuslikku ebaefektiivsust algarvude leidmisel.

CERCS teaduseriala: P120 Arvuteooria, väljateooria, algebraline geomeetria, algebra, rühmateooria.
Märksõnad: Algarvud, valemid.

On Formulae for Primes

Bachelor's thesis

Kadri Sügis

Abstract. Primarily during the last century, there have been a number of attempts to study primes via the use of "prime formulae", i.e. (partially) prime-valued functions. The thesis gives an overview of selected prime formulae and related results. Specifically, we consider prime-valued polynomials, the formulae of Willans, Sierpiński, Gandhi, Mills, Wright and several others. Moreover, those due to Isenkrahe, Hardy and Wright, and Saouter are provided with detailed proofs. Finally, the thesis contains a number of worked-out examples that coincidentally demonstrate the computational inefficiency of using any of the above formulae to generate primes.

CERCS research specialisation: P120 Number theory, field theory, algebraic geometry, algebra, group theory.
Keywords: Prime numbers, formulae.

Sisukord

Sissejuhatus

„Valemid lummavad. Loomulikult mitte kõiki, ja isegi mitte kõiki matemaatikuid, aga mõnede jaoks on võrdusmärki sisaldav sümbolite rida palju jõulisem ja ligitõmbavam kui sama asi ükskõik millisel teisel kujul. Selle põhjus võrsub tõenäoliselt inimese matemaatilises imikueas, kus me avastame, et sümbolitega manipuleerimine ja valemite kasutamine võib probleemidele tõesti vastuseid anda. Väljaarenemata matemaatilisele mõistusele tundub see peaaegu maagilisena: tundub, et me saame midagi eimillegi eest! Esimesed armastused ei unune, seega pole üllatav, et ka armastus valemite vastu, teadlik või mitte, püsib edasi isiksuse matemaatilisse täiskasvanuikka jõudmisel.“ U. Dudley [7, lk 17].

Algarvuvalemid kui sellised ei ole väga vanad: 18. sajandil uuris L. Euler sellest seisukohast polünoome, esimesed valemid ilmusid 19. sajandi lõpus [7]. L. Landau tõestas [21, lk 213–215], et

$$p_n \sim n \log n$$

st, et $\frac{p_n}{n \log n} \to 1$ protsessis $n \to \infty$. Viimane aga ei ole täpne valem. Proovitud on leida ka täpseid valemeid. Seejuures on ülesannet sõnastatud erinevalt. Näiteks G. H. Hardy ja E. M. Wright tõstatavad [15, lk 17] küsimuse, kas saaks leida lihtsat funktsiooni, mis annaks tulemuseks

(1) täpselt kõik algarvud;

(2) ainult algarve;

(3) lõpmata palju algarve ja mingi hulga kordarve.

On ka teisi lähenemisi. Ribenboim [30] jagab probleemi kolmeks erinevaks ülesandeks:

(a) Leida selline funktsioon f, et $f(n) = p_n$ iga naturaalarvu n korral.

(b) Leida selline funktsioon f, et $f(n)$ on algarv iga naturaalarvu n korral ja kui $m \neq n$, siis $f(m) \neq f(n)$.

(c) Kirjeldada algarvude hulka polünoomide abil.

Käesolevast tööst leiab erinevat liiki valemeid, mis kokku esindavad kõiki kolme Ribenboimi ülesannete klassi.

Ideaalis oodatakse lisaks täpsusele ka seda, et valem oleks efektiivne, st arvutamise jaoks oleks vaja vähem aega ja resursse kui seda kulutavad teised ebaefektiivseted meetodid, näiteks Eratosthenese sõel või tegelikult kõik seniajani teadaolevad algarvuvalemid.

Käesoleva bakalaureusetöö eesmärk on tutvustada erinevaid algarvuliste väärtustega valemeid ja nendega seotud tulemusi. Käsitlemist leiavad polünoomid, Isenkrahe, Willansi, Hardy ja Wrighti, Mackinnoni, Millsi, Wrighti, Sierpiński, Gandhi ning Saouteri algarvuvalemid. Kolmel lihtsamal juhul on valem esitatud koos tõestusega.

Bakalaureusetöö koosneb neljast peatükist. Esimeses neist tutvustakse töös kasutatavaid mõisteid ja tähistusi. Samuti esitatakse mõned edaspidises vajaminevad tulemused algarvu p_n ülemiste tõkete kohta.

Teises peatükis antakse ülevaade algarvuliste väärtustega polünoomidest. Keskendutakse *Euleri polünoomile* ja sellega seotud tulemustele ning tõestatakse Goldbachi teoreem mittekonstantse polünoomi $f(n)$ väärtustest. Tähelepanu pööratakse ka mitmemuutuja polünoomidele.

Teine peatükk on pühendatud rea 19. ja 20. sajandil leitud valemite ja nendega seotud tulemuste kirjeldamisele. Üksikasjalik tõestus esitatakse Isenkrahe ning Hardy ja Wrighti valemile. Valemite kasutamist ja sellega seotud kitsaskohti illustreerivad näited.

Kolmandas peatükis esitatakse ja tõestatakse üks 2017. aastal avaldatud ainult aritmeetikatehteid ja täisosa võtmist sisaldav algarvuvalem. Lisaks suhtelisele lihtsusele ja hiljutisele ilmumisaastale on Saouteri valem tähelepanuväärne ka selle poolest, et tõestuse täielik läbiviimine ei nõua isegi ülikoolitasemel eelteadmisi.

Bakalaureusetöö on referatiivne, kuid ei põhine otseselt ühelgi üksikul algallikal. Isenkrahe, Hardy ja Wrighti ning Saouteri valemite tõestused toetuvad originaalallikatele [17], [15] ja [31].

1 Põhimõisted ja -tulemused

Meenutame kõigepealt, et*algarvuks* nimetatakse naturaalarvu p, millel on parajasti kaks erinevat naturaalarvulist jagajat, nimelt 1 ja p. Naturaalarvu, mis on suurem kui 1 ja mis ei ole algarv, nimetatakse *kordarvuks*. Algarvude hulka tähistame edaspidises sümboliga $\mathbb{P}$ ja algarve sümboliga p, kasutades vajadusel indekseid. Sümboliga p_n, $n = 1, 2, ...$, tähistame suuruselt n-ndat algarvu ja sümboliga $\pi(x)$ *reaalarvu x mitteületavate algarvude arvu*, st

$$\pi(x) = |\{n \in \mathbb{N} \mid 1 \leq n \leq x, n \in \mathbb{P}\}|.$$

Formaalsustest ette rutates võib esimesed algarvud lihtsalt proovimise teel leida:

$$\begin{array}{lllll} p_1 = 2, & p_2 = 3, & p_3 = 5, & p_4 = 7, & p_5 = 11, \\ p_6 = 13, & p_7 = 17, & p_8 = 19, & p_9 = 23, & p_{10} = 29, \\ p_{11} = 31, & p_{12} = 37, & p_{13} = 41, & p_{14} = 43, & p_{15} = 47. \end{array}$$

Samas nende asukoht naturaalarvude reas ei tundu esmapilgul alluvat mingile konkreetsele reeglile. Teades algarvu p_n, ei saa selle järgi otseselt leida järgmist algarvu p_{n+1}. Üheks lahenduseks on siin olnud algarvude tabelite koostamine.

Kreeka matemaatiku Eratosthenese poolt III sajandil eKr algarvude tabeli koostamiseks loodud algoritmi, mida tuntakse *Eratosthenese sõelana*. Nicomachos [27] kirjeldab seda järgmiselt: paneme ritta võimalikult palju paarituid arve alates algarvust 3:

$$3, 5, 7, 9, 11, 13, 15, 17, 19, 21, 23, 25, 27, 29, 31, 33, 35, 37, \ldots$$

Jättes vahele kaks arvu, leiame esimese arvuga 3 jaguva arvu $3 \cdot 3$. Nii leiame kahte arvu vahele jättes kõik arvu 3 kordsed. Järgmine algarv on 5. Nüüd saab sellest alustades leida nelja arvu vahele jättes kõik arvu 5 kordsed alates arvust $5 \cdot 5$. Siis on järjekorras 7 ja me leiame selle kordsed kuus arvu vahele jättes. Analoogiliselt toimitakse edasi.

Kui algarvust p väiksemate algarvude kordsed on leitud, siis kõik allesjäänud arvud, mis on väiksemad kui p^2, on algarvud. Nii saab leida kõik algarvud vahemikus $1, \ldots, n$, kus n on mingi etteantud naturaalarv. Eratosthenese sõela kasutatigi algarvude tabelite koostamiseks.

Töös kasutatakse mitmeid üldtuntud tähiseid: kõigi reaalarvude hulka tähistatakse sümboliga $\mathbb{R}$, naturaalarvude hulka sümboliga $\mathbb{N}$, täisarvude hulka sümboliga $\mathbb{Z}$ ning ratsionaalarvude hulka sümboliga $\mathbb{Q}$. Lisaks neile vajame veel mõningaid mõisteid ja tähistusi.

Arvu (alumine) täisosa on funktsioon, mis on määratud reaalarvude hulgal ja mille väärtused on täisarvud. Kui m on täisarv ja kehtivad võrratused

$$m \leq x < m + 1,$$

siis öeldakse, et reaalarvu x (alumine) täisosa on m ja kirjutatakse

$$\lfloor x \rfloor = m.$$

Sümboliga $\{x\}$ tähistame *reaalarvu x murdosa*, st

$$\{x\} = x - \lfloor x \rfloor.$$

Möbiuse funktsioon $\mu : \mathbb{N} \to \{-1, 0, 1\}$ defineeritakse seosega

$$\mu(n) = \begin{cases} 1, & \text{kui } n = 1; \\ 0, & \text{kui mingi algarvu } p \text{ korral } p^2 \text{ jagab naturaalavu } n; \\ (-1)^n, & \text{kui } n = p_1 p_2 ... p_n, \text{ kus } p_1, p_2, ..., p_n \text{ on erinevad algarvud.} \end{cases}$$

Mitmed töös käsitletavad algarvuvalemid toetuvad järgmistele järeldustele *Bertrandi postulaadina* tuntud väitest, mille tõestas 1852. aastal P. Tšebõšov [33].

Teoreem 1.1 (Bertrandi postulaat)**.** *Kui $n > 3$ on naturaalarv, siis n ja $2n - 2$ vahel leidub vähemalt üks algarv.*

Esimese järgmistest järeldustest näitas ära L. Landau [21, lk 92].

Järeldus 1.2. *Iga naturaalarvu $N \geq 1$ korral leidub vähemalt üks niisugune algarv p , et*

$$N < p \leq 2N. \tag{1.1}$$

Juhul $n \geq 2$ saame nüüd algarvu p_n jaoks järgmise ülemise tõkke.

Järeldus 1.3. *Iga naturaalarvu $n \geq 2$ korral kehtib*

$$p_n \leq 2^n.$$

Tõestus. Tõestame väite induktsiooniga üle n.
Kontrollime, et väide kehtib, kui $n = 2$. Tõepoolest, $p_2 = 2 \leq 2^2$.
Oletame, et väide kehtib juhul $n = k$, ehk $p_k \leq 2^k$. Näitame, et väide kehtib siis ka $n = k + 1$ korral. Võrratusest (1.1) saame juhul $N = p_k$ järeldada, et

$$p_k < p_{k+1} \leq p \leq 2p_k,$$

kui p_{k+1} on vähim tingimusele $p_k < p \leq 2p_k$ vastavatest algarvudest. Seega

$$p_{k+1} \leq 2p_k \leq 2^{k+1}$$

□

Tuletame meelde ka *aritmeetika põhiteoreemi*, mille tõestuse leiab aine „Arvuteooria“ konspektist [20].

Teoreem 1.4 (Aritmeetika põhiteoreem)**.** *Iga naturaalarvu $n > 1$ saab esitada algarvude korrutisena, st leiduvad naturaalarv k ja algarvud $p_1, ..., p_k$ nii, et*

$$n = p_1 \cdot ... \cdot p_k,$$

ning see esitus on ühene tegurite järjekorra täpsuseni.

2 Algarvuliste väärtustega polünoomid

2.1 Ühemuutuja polünoomid

Teades, et kõik algarvud peale arvu 2 on paaritud, ei ole raske kirja panna esimese astme ühemuutuja polünoomi, mille väärtuste hulgas on lõpmata palju algarve. Täpsemalt, kõiki algarve, välja arvatud arv 2, saab esitada kujul

$$2n+1,\ n \in \mathbb{N}.$$

Üldiselt kehtib 1837. aastal P. G. Dirichlet' poolt [23] tõestatud teoreem

Teoreem 2.1. *Kui a ja b on ühistegurita naturaalarvud, siis aritmeetilises jadas*

$$a, a+b, a+2b, a+3b, ...$$

on lõpmata palju algarve.

Seega saab konstrueerida lõpmatu arvu erinevaid lineaarpolünoome, millest igaühel on lõpmata palju algarvulisi väärtusi.

Leidub terve hulk teise astme ühemuutuja polünoome, mis on matemaatikutele huvi pakkunud seetõttu, et nende järjestikusteks väärtuseks on rida algarve. Kuulsaim neist on kindlasti *Euleri polünoom.*

1771. aastal mainis Euler oma kirjas [11] J. Bernoullile , et polünoomi

$$f(x) = x^2 - x + 41$$

väärtused on algarvud, kui $x = 1, ..., 40$. Kui $x = 41$, siis

$$f(41) = 41^2 - 41 + 41 = 41(41 - 1 + 1) = 41^2.$$

Kui $x > 40$, on polünoomi väärtuste hulgas lõpmata palju kordarve. Näiteks sellised, mis jaguvad arvuga 41: kui $x = 41k,\ k \in \mathbb{N}$, siis

$$f(41k) = (41k)^2 - 41k + 41 = 41(41k^2 - k + 1).$$

Kordarvude vahele jääb ka algarvulisi väärtusi, näiteks $f(43) = 1847$. Vahel (vt näiteks [30]) on Euleri polünoomiks nimetatud ka polünoomi

$$g(x) = x^2 + x + 41,$$

mille puhul A. M. Legendre pani 1798. aastal tähele [22, lk 10], et selle väärtused on algarvud, kui $x = 0, 1, ..., 39$. Legendre mainis samas ka polünoomi

$$x^2 - x + 17,$$

mille väärtused on algarvud, kui $x = 0, 1, ..., 16$.

G. Rabinowitsch näitas 1913. aastal [29], et $q \in \{2, 3, 5, 11, 17, 41\}$ korral on polünoomi

$$x^2 + x + q$$

väärtuseks algarv iga täisarvu $0 \leq x < q - 2$ korral.

Tähistame polünoomi $x^2 + x + c$ diskriminandi sümboliga D, st $D = 1 - 4c$. Euleri polünoomi diskriminanti $D = -163$ aluseks võttes on leitud rida polünoome, mis samuti annavad väärtustena algarve. Näiteks E. B. Escotti poolt [9] 1899. aastal välja pakutud polünoom

$$g(x - 40) = x^2 - 79x + 1601,$$

mille väärtuseks on algarvud, kui $x = 0, 1, ..., 79$. On leitud ka kõrgema astme polünoome, mis teatud piirini genereerivad algarve. O. Cira ja F. Smarandache [4, lk 13] on näiteks toonud Kazmenko ja Trofimovi polünoomi

$$-66n^3 + 3845n^2 - 60897n + 251831,$$

mille väärtused on algarvud, kui $n = 0, 1, ..., 45$, või Wroblewski and Meyrignaci polünoomi

$$n^5 - 99n^4 + 3588n^3 - 56822n^2 + 348272n - 286397,$$

mis annab algarve $n = 0, 1, ..., 46$ korral.

1752. aastal märkis C. Goldbach kirjas Eulerile [12, lk 595], et ei leidu polünoomi, mille väärtuseks oleksid ainult algarvud ja tõestas selle väite kolmanda astme polünoomide jaoks. Euleri esituses ilmus see teoreem koos üldise tõestusega 1764. aastal [10, lk 102].

Teoreem 2.2. *Ei leidu täisarvuliste kordajatega mittekonstantset polünoomi $f(n)$, mille kõik väärtused oleksid algarvud iga täisarvu n korral või kõigi piisavalt suurte n väärtuste korral.*

Tõestus. Tähistame $f(n) = \sum_{i=0}^{k} a_i n^i$. Eeldame üldsust kitsendamata, et polünoomi pealiikme kordaja a_k on positiivne. Siis $f(n) \to \infty$, kui $n \to \infty$, seega leidub täisarv N nii, et $f(n) > 1$, kui $n > N$. Olgu nüüd $x > N$, siis

$$f(x) = a_k x^k + ... + a_1 x + a_0 = y > 1.$$

Kui y on kordarv, siis on teoreem tõestatud. Olgu y algarv. Valime suvalise täisarvu $r \geq 0$, siis

$$f(x+ry) = a_k(x+ry)^k + ... + a_1(x+ry) + a_0 > 1.$$

Avades sulud ja koondades liikmed, kus puudub y, saame polünoomi väärtuse kohal x, st $f(x) = y$. Niisiis

$$\begin{aligned} f(x+ry) &= a_k \sum_{m=0}^{k} \binom{k}{m} x^m (ry)^{k-m} + ... + a_1 x + a_1 ry + a_0 \\ &= f(x) + \left(a_k \sum_{m=0}^{k-1} \binom{k}{m} x^m (ry)^{k-m} + ... + a_1 ry \right). \end{aligned}$$

Toome sulgudesse jäänud liikmete ühise teguri y sulgude ette, siis sulgudesse jääva avaldise väärtus on mingi täisarv t. Arvestades, et ka $f(x) = y$, võime kirjutada, et

$$f(x+ry) = y + yt = y(1+t).$$

Seega jagub $f(ry+x)$ arvuga y. Kuna sulgudesse jääva polünoomi pealiikme kordaja on $a_k > 0$, siis $f(ry+x) \to \infty$, kui $r \to \infty$. Seega on polünoomil $f(x)$ lõpmata palju kordarvulisi väärtusi. $\square$

2.2 Mitmemuutuja polünoomid

Toetudes varasematele tulemustele, tõestasid J. P. Jones, D. Sato, H. Wada ja D. Wiens 1976. aastal järgmise teoreemi [18]:

Teoreem 2.3. *Algarvude hulk on identne polünoomi*

$$\begin{aligned} &(k+2)[1-(wz+h+j-q)^2-[(gk+2g+k+1)(h+j)+h-z]^2 \\ &-(2n+p+q+z-e)^2-[16(k+1)^3(k+2)(n+1)^2+1-f^2]^2 \\ &-[e^3(e+2)(a+1)^2+1-o^2]^2-[(a^2-1)y^2+1-x^2]^2 \\ &-[16r^2y^4(a^2-1)+1-u^2]^2 \\ &-[((a+u^2(u^2-a))^2-1)(n+4dy)^2+1-(x+cu)^2]^2 \\ &-[n+l+v-y]^2-[(a^2-1)l^2+1-m^2]^2-[ai+k+1-l-i]^2 \\ &-[p+l(a-n-1)+b(2an+2a-n^2-2n-2)-m]^2 \\ &-[q+y(a-p-1)+s(2ap+2a-p^2-2p-2)-x]^2 \\ &-[z+pl(a-p)+t(2ap-p^2-1)-pm]^2] \end{aligned}$$

positiivsete väärtuste hulgaga.

Antud polünoomis on 26 muutujat $a, b, c, ..., z$ ja selle aste on 25. Kui muutujad asendada positiivsete täisarvudega, siis polünoomi positiivsed väärtused vastavad täpselt algarvude hulgale $2, 3, 5, ...$ [18].

Samas püstitavad Jones, Sato, Wada ja Wiens küsimuse, milline on sellise polünoomi vähim võimalik aste ja kui väheste muutujatega on üldse võimalik algarvude hulka esitada. Nende väitel [18] on võimalik polünoomi astet vähendada kuni viieni, aga sellisel juhul oleks muutujate arv 42.

1977. aastal tõestas J. V. Matijasevitš [25], et saab koostada ka ainult kümne muutujaga polünoomi, mille positiivsete väärtuste hulk vastab täpselt algarvude hulgale. Polünoomi aste on sellisel juhul 15905.

3 Mitmesugused algarvuvalemid

Selles peatükis anname ülevaate reast 19. ja 20. sajandil välja töötatud algarvuvalemitest. Lihtsaimad neist esitame koos üksikasjaliku tõestusega.

3.1 Isenkrahe valem

1899. aastal pakkus C. Isenkrahe [17] välja lahenduse ülesandele esitada iga algarv talle eelnevate algarvude funktsioonina. Oma väite tõestamisel toetus Isenkrahe järgmisele tulemusele.

Teoreem 3.1. *Kui algarv p on korrutise $x!$ algtegur, siis on tema astendaja arvu $x!$ algteguriteks lahutuses*

$$\left\lfloor \frac{x}{p} \right\rfloor + \left\lfloor \frac{x}{p^2} \right\rfloor + \left\lfloor \frac{x}{p^3} \right\rfloor + ... + \left\lfloor \frac{x}{p^{\lfloor \log_p x \rfloor}} \right\rfloor .$$

Tõestus. Kui korrutises

$$x! = x(x-1) \cdot ... \cdot 2 \cdot 1$$

leidub tegureid, mis on algarvu p kordsed, saab need kirja panna kujul

$$1p,\ 2p,\ 3p,\ ...,\ \left\lfloor \frac{x}{p} \right\rfloor p.$$

Kokku on selliseid tegureid $\left\lfloor \frac{x}{p} \right\rfloor$ tükki. Eraldades faktoriaalis $x!$ igast sellisest tegurist p, saame teguri $p^{\lfloor \frac{x}{p} \rfloor}$. Nüüd jäävad algarvu p kordsetest alles tegurid

$$1,\ 2,\ 3,\ ...,\ \left\lfloor \frac{x}{p} \right\rfloor ,$$

mille hulgas võib omakorda leiduda arvu p kordseid. Sellised tegurid on

$$1p,\ 2p,\ 3p,\ ...,\ \left\lfloor \frac{\lfloor \frac{x}{p} \rfloor}{p} \right\rfloor p.$$

Tegurdades neist kõigist p, saame teguri $p^{\left\lfloor \frac{\lfloor \frac{x}{p} \rfloor}{p} \right\rfloor}$.. Esitades nüüd arvu x kujul

$$x = ap^2 + bp + c;\ a > 0,\ 0 \leq b,\ c \leq p - 1,$$

näeme, et

$$\left\lfloor \frac{\left\lfloor \frac{x}{p} \right\rfloor}{p} \right\rfloor = \left\lfloor \frac{\left\lfloor ap + b + \frac{c}{p} \right\rfloor}{p} \right\rfloor = \left\lfloor \frac{ap+b}{p} \right\rfloor = a,$$

aga samas ka

$$\left\lfloor \frac{x}{p^2} \right\rfloor = \left\lfloor \frac{ap^2 + bp + c}{p^2} \right\rfloor = \left\lfloor a + \frac{b}{p} + \frac{c}{p^2} \right\rfloor = a.$$

Seetõttu võime kirjutada

$$p^{\left\lfloor \frac{\left\lfloor \frac{x}{p} \right\rfloor}{p} \right\rfloor} = p^{\left\lfloor \frac{\frac{x}{p}}{p} \right\rfloor} = p^{\left\lfloor \frac{x}{p^2} \right\rfloor}$$

ja järele jäävad arvud

$$1,\ 2,\ ...,\ \left\lfloor \frac{x}{p^2} \right\rfloor.$$

Nende hulgast saab jälle välja eraldada p kordsed, mis annab meile $p^{\left\lfloor \frac{x}{p^3} \right\rfloor}$. Sama mõttekäiku saame jätkata nii kaua kui $p^r \leq x$, st $r \leq \log_p x$. Seega on meil korrutises $x!$ tegurid

$$p^{\left\lfloor \frac{x}{p} \right\rfloor},\ p^{\left\lfloor \frac{x}{p^2} \right\rfloor},\ p^{\left\lfloor \frac{x}{p^3} \right\rfloor}, ..., p^{\left\lfloor \frac{x}{p^{\lfloor \log_p x \rfloor}} \right\rfloor}.$$

Kui $p^r > x$, siis $\left\lfloor \frac{x}{p^r} \right\rfloor = 0$ ja kokkuvõttes võime p astendaja tõepoolest kirjutada summana

$$\left\lfloor \frac{x}{p} \right\rfloor + \left\lfloor \frac{x}{p^2} \right\rfloor + \left\lfloor \frac{x}{p^3} \right\rfloor + ... + \left\lfloor \frac{x}{p^{\lfloor \log_p x \rfloor}} \right\rfloor.$$

□

Teoreem 3.2. *Olgu antud algarvud $p_1, ..., p_n$. Siis leidub niisugune funktsioon $F(n, x)$, et*

$$F(n,x) = \begin{cases} x+1, & \textit{kui } p_n < x < p_{n+1}, \\ x, & \textit{kui } x = p_{n+1}. \end{cases}$$

Tõestus. Olgu algarv p_i korrutise $x!$ algtegur, siis vastavalt teoreemile 3.1 on tema astendaja

$$S(i,x) = \left\lfloor \frac{x}{p_i} \right\rfloor + \left\lfloor \frac{x}{{p_i}^2} \right\rfloor + \left\lfloor \frac{x}{{p_i}^3} \right\rfloor + ... + \left\lfloor \frac{x}{p^{\lfloor \log_p x \rfloor}} \right\rfloor.$$

Tähistades $p(i,x) = {p_i}^{S(i,x)}$ ja $P(n,x) = \prod_{i=1}^{n} p(i,x)$, saame võrduse

$$\frac{x!}{P(n,x)} = 1, \tag{3.1}$$

mis kehtib, kui nimetaja sisaldab kõiki algarve $p_i \leq x$, st $x < p_{n+1}$. Defineerime nüüd funktsiooni

$$F(n,x) = \frac{x!}{P(n,x)} + \frac{P(n,x)}{(x-1)!} - \left\lfloor \frac{(x-1)!}{P(n,x)} \right\rfloor \tag{3.2}$$

ning uurime eraldi juhte $p_n \leq x < p_{n+1}$ ja $x = p_{n+1}$.

Kui $p_n \leq x < p_{n+1}$, kehtib võrdus (3.1) ja seega

$$\frac{(x-1)!}{P(n,x)} = \frac{1}{x}.$$

Viimasest tuleneb aga ühelt poolt, et

$$\frac{P(n,x)}{(x-1)!} = x$$

ja teiselt poolt, et

$$\left\lfloor \frac{(x-1)!}{P(n,x)} \right\rfloor = 0.$$

Seega $F(n,x) = 1 + x - 0 = 1 + x$.

Kui $x = p_{n+1}$, omandab võrdus (3.1) kuju

$$\frac{x!}{P(n,x) \cdot p(n+1,x)} = \frac{x!}{P(n,x) \cdot {p_{n+1}}^{\left\lfloor \frac{x}{p_{n+1}} \right\rfloor}} = \frac{x!}{P(n,x) \cdot p_{n+1}} = 1,$$

millest saame, et

$$\frac{x!}{P(n,x)} = x \quad \iff \quad \frac{(x-1)!}{P(n,x)} = 1 \quad \iff \quad \frac{P(n,x)}{(x-1)!} = 1$$

ja

$$\left\lfloor \frac{(x-1)!}{P(n,x)} \right\rfloor = 1.$$

Sellisel juhul $F(n,x) = x + 1 - 1 = x$.

Kokkuvõttes olemegi saanud, et

$$F(n,x)=\begin{cases}1+x, & \text{kui } p_n < x < p_{n+1},\\ x, & \text{kui } x = p_{n+1}.\end{cases} \tag{3.3}$$

□

Võrdust (3.2) võib nimetada Isenkrahe valemiks. Arvestades funktsiooni $F(n,x)$ definitsiooni ja võrdust (3.3), võib ka kirjutada, et

$$p_{n+1} = \lim_{x\to(p_{n+1})^-} F(n,x).$$

Piisavalt väikeste arvude korral saab seda valemit veel kasutada.

Näide 1. Teades algarve $p_1 = 2, p_2 = 3$ ja $p_3 = 5$, on

$$P(3,x) = 2^{\lfloor\frac{x}{2}\rfloor+\lfloor\frac{x}{4}\rfloor+\lfloor\frac{x}{8}\rfloor+\ldots+\lfloor\frac{x}{2^{\lfloor\log_2 x\rfloor}}\rfloor}\cdot 3^{\lfloor\frac{x}{3}\rfloor+\lfloor\frac{x}{9}\rfloor+\ldots+\lfloor\frac{x}{3^{\lfloor\log_3 x\rfloor}}\rfloor}\cdot 5^{\lfloor\frac{x}{5}\rfloor+\lfloor\frac{x}{25}\rfloor+\ldots+\lfloor\frac{x}{5^{\lfloor\log_5 x\rfloor}}\rfloor}.$$

Olgu nüüd $x = 6$, siis

$$\begin{aligned}P(3,6) &= 2^{\lfloor\frac{6}{2}\rfloor+\lfloor\frac{6}{4}\rfloor+\lfloor\frac{6}{8}\rfloor+\ldots+\lfloor\frac{6}{2^{\lfloor\log_2 6\rfloor}}\rfloor}\cdot 3^{\lfloor\frac{6}{3}\rfloor+\lfloor\frac{6}{9}\rfloor+\ldots+\lfloor\frac{6}{3^{\lfloor\log_3 6\rfloor}}\rfloor}\cdot 5^{\lfloor\frac{6}{5}\rfloor+\lfloor\frac{6}{25}\rfloor+\ldots+\lfloor\frac{6}{5^{\lfloor\log_5 6\rfloor}}\rfloor}\\ &= 2^{3+1}\cdot 3^2\cdot 5^1 = 2^4\cdot 3^2\cdot 5^1 = 6!.\end{aligned}$$

Asendades selle valemisse, saame

$$\begin{aligned}F(3,6) &= \frac{6!}{P(3,6)} + \frac{P(3,6)}{5!} - \left\lfloor\frac{5!}{P(3,6)}\right\rfloor\\ &= \frac{6!}{6!} + \frac{6!}{5!} - \left\lfloor\frac{5!}{6!}\right\rfloor = 1+6-0 = 7.\end{aligned}$$

Seega $x = 6$ ei ole algarv. Kui valime järgmiseks $x = 7$, siis

$$\begin{aligned}P(3,7) &= 2^{\lfloor\frac{7}{2}\rfloor+\lfloor\frac{7}{4}\rfloor+\lfloor\frac{7}{8}\rfloor+\ldots+\lfloor\frac{7}{2^{\lfloor\log_2 7\rfloor}}\rfloor}\cdot 3^{\lfloor\frac{7}{3}\rfloor+\lfloor\frac{7}{9}\rfloor+\ldots+\lfloor\frac{7}{3^{\lfloor\log_3 7\rfloor}}\rfloor}\cdot 5^{\lfloor\frac{7}{5}\rfloor+\lfloor\frac{7}{25}\rfloor+\ldots+\lfloor\frac{7}{5^{\lfloor\log_5 7\rfloor}}\rfloor}\\ &= 2^{3+1}\cdot 3^2\cdot 5^1 = 2^4\cdot 3^2\cdot 5^1 = 6!,\end{aligned}$$

mille asendamisel valemisse saame

$$\begin{aligned}F(3,7) &= \frac{7!}{P(3,7)} + \frac{P(3,7)}{6!} - \left\lfloor\frac{6!}{P(3,7)}\right\rfloor\\ &= \frac{7!}{6!} + \frac{6!}{6!} - \left\lfloor\frac{6!}{6!}\right\rfloor = 7+1-1 = 7\end{aligned}$$

ja me oleme leidnud uue algarvu $p_4 = 7$.

Tegelikult me teame, et kui esitada $x!$ algarvude astmete korrutisena, siis vastavasse korrutisse $(x+1)!$ lisandub uus algarvuline tegur ainult juhul, kui $x+1$ on algarv. Seega me võiksime algarve otsida lihtsalt järjestikuste naturaalarvude faktoriaale algteguriteks lahutades, mis taandub lisanduva teguri $x+1$ algteguriteks lahutamisele. See on aga arvutuslikult raske ülesanne. Ka juba eelnevast näitest on näha, et praktilist väärtust valemil ei ole.

3.2 Wilsoni teoreemil põhinevad valemid

Wilsoni teoreemina tuntakse järgmist tulemust.

Teoreem 3.3. *Naturaalarv $n > 1$ on algarv parajasti siis, kui arv $(n-1)!+1$ jagub arvuga n.*

Kõrvalepõikena mainime, et *Wilsoni algarvudeks* nimetatakse algarve p, mille korral $(p-1)!+1$ jagub arvuga p^2. Ainsad teadaolevad Wilsoni algarvud on 5, 13 ja 563. R. Crandall, K. Dilcher ja C. Pomerance näitasid [6] 1997. aastal, et rohkem Wilsoni algarve $p < 5 \cdot 10^8$ ei leidu. 2012. aastal näitasid E. Costa, R. Gerbicz ja D. Harvey [5], et ei leidu teisi Wilsoni algarve, mis oleksid väiksemad kui $2 \cdot 10^{13}$.

3.2.1 Willansi valem

1964. aastal märkas [35] C. P. Willans, et Wilsoni teoreemi põhjal on

$$\frac{(x-1)!+1}{x}$$

täisarv, kui $x = 1$ või x on algarv, aga kui x on kordarv, tuleb tulemuseks alati murdarv. Et $\cos^2 k\pi = 1$, kui $k \in \mathbb{Z}$ ja $0 \leq \cos^2 k\pi < 1$, kui $k \in \mathbb{Q} \setminus \mathbb{Z}$, siis on funktsiooni

$$F(x) = \left\lfloor \cos^2 \left(\pi \frac{(x-1)!+1}{x} \right) \right\rfloor, \quad x \in \mathbb{N},$$

väärtused

$$F(x) = \begin{cases} 1, & \text{kui } x = 1 \text{ või } x \in \mathbb{P}, \\ 0, & \text{kui } x \in \mathbb{N} \setminus (\mathbb{P} \cup \{1\}). \end{cases}$$

Seega võib kirjutada, et

$$\pi(m) = -1 + \sum_{x=1}^{m} F(x).$$

Kui nüüd tähistada

$$A_n(a) = \left\lfloor \sqrt[n]{\frac{n}{1+a}} \right\rfloor, \quad n = 1, 2, ...; \quad a = 0, 1, 2...,$$

siis

$$A_n(a) = \begin{cases} 1, & \text{kui } a < n, \\ 0, & \text{kui } a \geq n. \end{cases} \tag{3.4}$$

Arvestades järeldust 1.3 ja võrdust (3.4), võime kirjutada, et

$$p_n = 1 + \sum_{m=1}^{2^n} A_n(\pi(m)) \tag{3.5}$$

ehk

$$p_n = 1 + \sum_{m=1}^{2^n} \left\lfloor \sqrt[n]{\frac{n}{\sum_{x=1}^{m} \left\lfloor \cos^2 \pi \frac{(x-1)!+1}{x} \right\rfloor}} \right\rfloor. \tag{3.6}$$

Valemit (3.6) nimetatakse Willansi valemiks.

Willansi valemit on kujul (3.5) lihtne kasutada, kui n on väike ja $\pi(n)$ väärtused on teada.

Näide 2. Olgu $n = 6$, siis:

$$\begin{aligned} p_6 &= 1 + A_6(\pi(1)) + A_6(\pi(2)) + ... + A_6(\pi(12)) + A_6(\pi(13)) + ... + A_6(\pi(64)) \\ &= 1 + A_6(0) + A_6(1) + ... + A_6(5) + A_6(6) + ... + A_6(18) \\ &= 1 + 1 + 1 + ... + 1 + 0 + ... + 0 \\ &= 13. \end{aligned}$$

Juba $n = 10$ korral on summas $2^{10} = 1024$ liidetavat ja arvu $p_{10} = 29$ saab kiiremini leida isegi Eratosthenese sõelaga.

3.2.2 Hardy ja Wrighti valem

Wilsoni teoreemist järeldasid G. H. Hardy ja E. M. Wright [15, lk 414], et naturaalarvu $j \geq 5$ korral annab arv $(j-2)!$ arvuga j jagamisel jäägi 1, kui j on algarv ja jäägi 0, kui j on kordarv. Seetõttu on kordarvu $j \geq 5$ korral

$$(j-2)! = j \left\lfloor \frac{(j-2)!}{j} \right\rfloor$$

ja algarvu $j \geq 5$ korral

$$(j-2)! - 1 = j \left\lfloor \frac{(j-2)!}{j} \right\rfloor.$$

Teades, et $\pi(4) = 2$, siis võib tehtud järeldusest tulenevalt naturaalavu $k \geq 5$ korral kirjutada:

$$\pi(k) = 2 + \sum_{j=5}^{k} \left((j-2)! - j \left\lfloor \frac{(j-2)!}{j} \right\rfloor \right).$$

Defineerime funktsiooni

$$f(x,y) = \begin{cases} 0, & \text{kui } x = y, \\ \frac{1}{2}\left(1 + \frac{x-y}{|x-y|}\right), & \text{kui } x \neq y. \end{cases}$$

Ilmselt

$$\frac{1}{2}\left(1 + \frac{x-y}{|x-y|}\right) = \begin{cases} 1, & \text{kui } x > y, \\ 0, & \text{kui } x < y, \end{cases}$$

mistõttu

$$f(n, \pi(k)) = \begin{cases} 0, & \text{kui } n \leq \pi(k), \\ 1, & \text{kui } n > \pi(k). \end{cases}$$

Et $\pi(k) \leq n$ parajasti siis, kui $k < p_{n+1}$, siis

$$f(n, \pi(k)) = \begin{cases} 0, & \text{kui } k \geq p_n, \\ 1, & \text{kui } k < p_n. \end{cases} \tag{3.7}$$

Arvestades võrdust (3.7) ja järeldust 1.3, võime iga naturaalarvu n korral kirjutada, et

$$p_n = 1 + \sum_{k=1}^{2^n} f(n, \pi(k)).$$

Hardy ja Wrighti valemi abil saab jällegi väikeste n väärtuste korral algarve p_n veel leida, seda eriti juhul, kui juba eelnevalt on teda $\pi(x)$ väärtused.

Näide 3. Olgu $n = 3$, siis

$$\begin{aligned} p_3 &= 1 + \sum_{k=1}^{8} f(3, \pi(k)) \\ &= 1 + f(3,\pi(1)) + f(3,\pi(2)) + f(3,\pi(3)) + f(3,\pi(4)) \\ &\quad + f(3,\pi(5)) + f(3,\pi(6)) + f(3,\pi(7)) + f(3,\pi(8)) \\ &= 1 + f(3,0) + f(3,1) + f(3,2) + f(3,2) \\ &\quad + f(3,3) + f(3,3) + f(3,4) + f(3,4) \\ &= 1+1+1+1+1+0+0+0+0 = 5. \end{aligned}$$

Sarnaselt Willansi valemile, on ka siin summas 2^n liidetavat ja valemi kasutegur on küsitav.

3.2.3 Mackinnoni valem

N. Mackinnon tuletas 1987. aastal [24] Wilsoni teoreemist funktsiooni $f : \mathbb{N} \to \mathbb{N}$, kus

$$f(n) = (n-2) \cdot 0^{\left\{\frac{(n-1)!+1}{n}\right\}} + 2, \quad n \in \mathbb{N}, \quad n \geq 1, \tag{3.8}$$

mille väärtuste hulk on täpselt algarvude hulk $\mathbb{P}$.

Wilsoni teoreemi järgi kehtib

$$\left\{\frac{(n-1)!+1}{n}\right\} = 0$$

parajasti siis, kui n on algarv. Et $0^x = 0$, kui $x \neq 0$ ja $0^0 = 1$, siis on funktsiooni $f(n)$ väärtusteks ainult algarvud. Täpsemalt,

$$f(n) = \begin{cases} n, & \text{kui } n \text{ on algarv,} \\ 2, & \text{kui } n \text{ on kordarv või } 1. \end{cases}$$

Väikeste n väärtuste korral on valemit (3.8) lihtne otse kasutada.

Näide 4. Olgu $n = 7$, siis

$$f(7) = 5 \cdot 0^{\left(\frac{6!+1}{7} - \left\lfloor \frac{6!+1}{7} \right\rfloor\right)} + 2 = 5 \cdot 0^{(103 - \lfloor 103 \rfloor)} + 2 = 5 \cdot 0^0 + 2 = 7.$$

Samamoodi $n = 10$ korral

$$f(10) = 8 \cdot 0^{\left(\frac{9!+1}{10} - \left\lfloor \frac{9!+1}{10} \right\rfloor\right)} + 2 = 5 \cdot 0^{(36288{,}1 - \lfloor 36288{,}1 \rfloor)} + 2 = 5 \cdot 0^{0{,}1} + 2 = 2.$$

Samas sisaldab faktoriaal $(n-1)!$ endas $n-3$ korrutamistehet, mistõttu on valem (3.8) uute algarvude leidmiseks täiesti ebapraktiline.

3.3 Millsi valem

1947. aastal tõestas W. H. Mills [26] järgmise teoreemi:

Teoreem 3.4. *Eksisteerib niisugune reaalarv A, et*

$$\left\lfloor A^{3^x} \right\rfloor$$

on algarv iga täisarvu $x \geq 1$ korral.

Millsi tõestus toetus A. E. Inghami [16] poolt tõestatud väitele, et leidub niisugune positiivne reaalarv K, et suvalise kahe järjestikuse algarvu p_n ja p_{n+1} korral

$$p_{n+1} - p_n < Kp_n^{\frac{5}{8}}.$$

Reaalarvu A väärtust Mills kindlaks ei määranud, sest juba Ingham ei andnud konstandile K täpset väärtust.

L. Kuipers [19] üldistas 1950. aastal Millsi tulemust ja näitas, et iga täisarvu $c \geq 3$ korral on võimalik leida selline reaalarv $A = A(c)$, et

$$\lfloor A^{c^x} \rfloor \tag{3.9}$$

on algarv iga positiivse täisarvu x korral. Samas sai tõestatud ka väide, et kahe erineva c väärtuse korral niiviisi saadud algarvude jadad ei ole teineteise osajadad.

I. Niven [28] omakorda üldistas Kuipersi valemit (3.9) ja tõestas esiteks, et igale etteantud reaalarvule $c > \dfrac{8}{3}$ vastab niisugune reaalarv A, et $\lfloor A^{c^x} \rfloor$ on algarv iga positiivse täisarvu x korral, ja teiseks, et iga reaalarvu $A > 1$ korral leidub mingi niisugune täisarv c, et valem (3.9) annab algarvu. Niven jõudis ka järeldusele, et esimese algarvulise väärtuse A^c võib valida vabalt. A. R. Ansari näitas [1] 1951. aastal, et valemis (3.9) võib võtta juba $c > \dfrac{77}{29}$.

Vähimat positiivset reaalarvu A, mille korral $\lfloor A^{3^x} \rfloor$ on alati algarv, nimetatakse *Millsi konstandiks.* C. K. Caldwell ja Y. Cheng [3] võtsid esimeseks algarvuliseks väärtuseks 2 ja tegid 2005. aastal kindlaks, et juhul $c = 3$ on Millsi konstandi A väärtus ligikaudu 1,3063778838 ning arvutasid välja selle esimesed 6850 kümnendkohta. Samuti leidsid nad vastavad minimaalsed 10 esimest Millsi algarvu:

$$2, 11, 1361, 2521008887, 16022236204009818131831320183, \ldots.$$

Neist viimane on 6854-kohaline.

3.4 Wrighti valem

Millsi valemiga analoogilise valemi leidis Wright [36], kes esitas selle koos tõestusega 1951. aastal.

Teoreem 3.5. *Leidub selline arv α , et kui*

$$g_0 = \alpha, \qquad g_{n+1} = 2^{g_n}, \quad n \geq 0,$$

siis

$$\lfloor g_n \rfloor = \left\lfloor 2^{2^{\cdot^{\cdot^{\cdot^{2^\alpha}}}}} \right\rfloor, \quad n \geq 1,$$

on alati algarv.

Teoreemi tõestuses kasutas Wright Bertrandi postulaati. Wright tõi näitena ühe võimalikest α väärtustest $\alpha = 1,9287800...$, mis annab algarvud

$$\lfloor g_1 \rfloor = \lfloor 2^\alpha \rfloor = 3, \quad \lfloor g_2 \rfloor = 13 \quad \lfloor g_3 \rfloor = 16381$$

ja $\lfloor g_4 \rfloor$ on umbes 5000-kohaline algarv.

R. Baillie [2] näitas 2017. aastal, et kui piirduda ainult Wrighti andmetega ja võtta $\alpha = 1,9287800$, siis $\lfloor g_4 \rfloor$ on 4932-kohaline kordarv, aga $\alpha = 1,9287800 + 8.2843 \cdot 10^{-4933}$ annab kolm esimest Wrighti algarvu ja 4932-kohalise algarvu $\lfloor g_4 \rfloor$.

3.5 Sierpiński valem

1952. aastal konstrueeris W. Sierpiński [32] algarvude leidmiseks valemi, tõestades järgmise teoreemi :

Teoreem 3.6. *Leidub reaalarv*

$$\alpha = \sum_{m=1}^{\infty} p_m 10^{-2^m},$$

mille korral kehtib

$$p_n = \left\lfloor 10^{2^n} \alpha \right\rfloor - 10^{2^{n-1}} \left\lfloor 10^{2^{n-1}} \alpha \right\rfloor, \tag{3.10}$$

kus $n = 1, 2, ...$ ja p_n tähistab n-ndat algarvu.

Kuna

$$\begin{aligned} \alpha &= 2 \cdot 10^{-2} + 3 \cdot 10^{-4} + 5 \cdot 10^{-8} + 7 \cdot 10^{-16} + 11 \cdot 10^{-32} + ... = \\ &= 0,0203000500000007000000000000000110..., \end{aligned}$$

siis saame esimesi algarve (neid juba ette teades!) muretult arvutada.

Näide 5. Leiame Sierpiński valemit kasutades esimesed kolm algarvu:

$$p_1 = \lfloor 10^2\alpha \rfloor - 10^{2^0} \left\lfloor 10^{2^0}\alpha \right\rfloor = \lfloor 100\alpha \rfloor - 10 \lfloor 10\alpha \rfloor = 2 - 10 \cdot 0 = 2,$$
$$p_2 = \lfloor 10^4\alpha \rfloor - 10^2 \lfloor 10^2\alpha \rfloor = \lfloor 10000\alpha \rfloor - 100 \lfloor 100\alpha \rfloor = 203 - 100 \cdot 2 = 3,$$
$$p_3 = \lfloor 10^8\alpha \rfloor - 10^4 \lfloor 10^4\alpha \rfloor = \lfloor 100000000\alpha \rfloor - 10000 \lfloor 10000\alpha \rfloor$$
$$= 2030005 - 10000 \cdot 203 = 5.$$

Samas on valem (3.10) täiesti kasutu, sest p_n arvutamiseks on vaja teada α täpset väärtust kuni 2^n kümnendkohani, mis omakorda nõuab, et me teaksime algarvude $p_1, ..., p_n$ väärtusi [15, lk 344]. Sama viga on ka Mackinnoni poolt välja pakutud [24] sarnasel valemil

$$p_n = 10^{2^{n-1}} \left\{ \frac{\lfloor 10^{2^n}\alpha \rfloor}{10^{2^{n-1}}} \right\},$$

kus α on sama konstant, mis Sierpińskil.

Valemile (3.10) esitasid tõestuse ka Hardy ja Wright, kes näitasid [15, lk 345], et sama tüüpi valemeid saab koostada palju: kui $r > 1$ on mingi naturaalarv, siis võib võtta

$$\alpha_r = \sum_{m=1}^{\infty} p_m r^{-m^2}$$

ja saada, et

$$p_n = \left\lfloor r^{n^2}\alpha_r \right\rfloor - r^{2n-1} \left\lfloor r^{(n-1)^2}\alpha_r \right\rfloor.$$

3.6 Gandhi valem

1971. aastal esitas J. M. Gandhi [13] tõestuse järgmisele tulemusele. Algarvu p_n jaoks kehtib

$$1 < 2^{p_n} \left(-\frac{1}{2} + \sum_{d|Q_n} \frac{\mu(d)}{2^d - 1} \right) < 2. \tag{3.11}$$

kus sümbol $\sum\limits_{d|Q_n}$ tähistab summat üle arvu $Q_n = \prod\limits_{i=1}^{n-1} p_i$ kõigi naturaalarvuliste jagajate d.

Kui α on mistahes reaalarv, siis võrratused $1 < 2^k \cdot \alpha < 2$ kehtivad täpselt ühe täisarvu k korral, sest

$$\log_2 1 < \log_2(2^k \cdot \alpha) < \log_2 2,$$

millest

$$0 < k + \log_2 \alpha < 1$$

ja

$$-\log_2 \alpha < k < 1 - \log_2 \alpha.$$

Viimast ahelvõrratust rahuldab täpselt üks täisarv k. Seetõttu määravad võrratused (3.11) üheselt ära arvu p_n.

Näide 6. Olgu $n = 3$, siis $Q_3 = 2 \cdot 3 = 6$ ja

$$-\frac{1}{2} + \sum_{d|6} \frac{\mu(d)}{2^d - 1} = -\frac{1}{2} + \frac{1}{1} - \frac{1}{3} - \frac{1}{7} + \frac{1}{63} = \frac{5}{126}.$$

Seega

$$1 < 2^{p_3} \cdot \frac{5}{126} < 2,$$

kust

$$\frac{126}{5} < 2^{p_3} < \frac{252}{5}$$

ja järelikult

$$25,2 < 2^{p_3} < 50,4.$$

Ainsana rahuldab viimaseid võrratusi $2^{p_3} = 32$, seega $p_3 = 5$.

Tähistades

$$\sigma_n = \sum_{d|Q_n} \frac{\mu(d)}{2^d - 1}$$

ja logaritmides võrratusi (3.11) alusel 2 saame, et

$$\log_2 1 < \log_2 2^{p_n} \left(\sigma_n - \frac{1}{2}\right) < \log_2 2,$$

kust

$$0 < p_n + \log_2 \left(\sigma_n - \frac{1}{2}\right) < 1,$$

seega

$$-\log_2 \left(\sigma_n - \frac{1}{2}\right) < p_n < 1 - \log_2 \left(\sigma_n - \frac{1}{2}\right),$$

millest

$$p_n = \left\lfloor 1 - \log_2 \left(\sigma_n - \frac{1}{2}\right) \right\rfloor. \tag{3.12}$$

Gandhi valem esitatakse sageli kujul (3.12).

C. Vanden Eynden pakkus [34] 1972. aastal välja Gandhi valemi tõestuse, milles kasutas vaid elementaarseid arvuteoreetilisi vahendeid.

J. R. Ellis näitas 1981. aastal [8], et Gandhi valem annab arvutamiseks Eratosthenese sõelale sarnaneva algoritmi, kui kasutada σ_n esitamisel kahendaritmeetikat.

Paneme tähele, et kahendsüsteemis

$$2^1 = 10, \quad 2^2 = 100, \quad ..., \quad 2^d = 1\underbrace{000...000}_{d \text{ nulli}}$$

ja kahendmurdudena

$$2^{-1} = 0,1; \quad 2^{-2} = 0,01; \quad ...; \quad 2^{-d} = 0,\underbrace{000...000}_{d-1 \text{ nulli}}1.$$

Arvestades, et

$$\frac{1}{2} + \frac{1}{4} + \frac{1}{8} + \frac{1}{16} + ... = 1,$$

võime arvu 1 esitada kahendmurruna $0,1111...$. Kuna kahendsüsteemis

$$2^1 - 1 = 11, \quad 2^2 - 1 = 111, \quad ..., \quad 2^d - 1 = \underbrace{111...111}_{d \text{ ühte}},$$

siis vastavad pöördarvud on kahendmurdudena

$$(2^1 - 1)^{-1} = 0,1111... : 1 = 0,1111..., \text{ sest } 1 \cdot 0,1111... = 0,1111...,$$
$$(2^2 - 1)^{-1} = 0,1111... : 11 = 0,0101..., \text{ sest } 11 \cdot 0,0101... = 0,1111...,$$
$$(2^3 - 1)^{-1} = 0,111111... : 111 = 0,001001..., \text{ sest } 111 \cdot 0,001001... = 0,1111....$$

Samamoodi

$$(2^d - 1)^{-1} = 0,1111... : \underbrace{111...111}_{d \text{ ühte}} = 0,\underbrace{000...000}_{d-1 \text{ nulli}}1\underbrace{000...000}_{d-1 \text{ nulli}}1000....$$

Nüüd võime kahendsüsteemis välja arvutada summad σ_n:

$$Q_2 = 2, \qquad \sigma_2 = 0,1111... - 0,0101... = 0,10\boxed{1}01010...$$
$$Q_3 = 2 \cdot 3, \qquad \sigma_3 = 0,1111... - 0,0101... - 0,001001... + 0,000001000001... =$$
$$= 0,1000\boxed{1}0100010...$$

Analoogiliselt saame, et

$$Q_4 = 2 \cdot 3 \cdot 5, \quad \sigma_4 = 0,100000\boxed{1}0001010001010001000010...$$

Paneme tähele, et kahendmurru σ_n perioodi pikkus on Q_n ja järgmise algarvu p_n leiame nii, et teeme kindlaks, mitmendal kohal pärast koma asub teine number 1. Numbri 1 kolmas asukoht annab p_{n+1}, neljas asukoht p_{n+2}, jne. Nii on iga σ_n korral leitavad ka kõik algarvud, mis jäävad p_n ja ${p_n}^2$ vahele. Kui arvutada välja ka vahe $\sigma_n - \frac{1}{2}$, annab algarvu p_n numbri 1 esimene asukoht, sest arvu $\frac{1}{2}$ kahendesitus on $0,1$.
Sisuliselt sarnaneb σ_n arvutamine Eratosthenese sõelale [8]. Näiteks σ_3 arvutamisel sõelutakse esimese sammuna välja teisel kohal olevad arvud (paarisarvud), siis kolmandal kohal olevad arvud (arvu 3 kordsed) ja liidetakse seejärel kuuendal kohal olevad arvud, mida on kaks korda lahutatud. Samale järeldusele jõudis 1974. aastal S. W. Golomb, kelle artiklist leiab ka Gandhi valemi tõestuse, milles kasutatakse tõenäosusteooria mõisteid [14].

4 Saouteri valem

2017. aasta märtsis ilmus ajakirjas The Mathematical Gazette Yannic Saouteri artikkel [31], mille pealkiri lubab kahes mõttes elementaarset valemit algarvude jaoks. Artikli ilmumisaasta näitab, et huvi algarvuvalemite vastu on jätkuvalt olemas. Vaatluse alla võtsime valemi osaliselt just sellesama kahekordse elementaarsuse tõttu: valem sisaldab ainult „elementaarsed“ aritmeetikatehteid ja täisosa võtmist ning selle tõestamisel ei ole vaja keerulisemaid arvuteoreetilisi tulemusi nagu Bertrandi postulaat vms. Põhimõtteliselt on tõestus arusaadav ka selle lugemiseks ette valmistunud gümnaasiumiõpilasele.

Kõigepealt tuletame meelde Eukleidese teoreemi tõestuse, mille abil saame ilma Bertrandi postulaati kasutamata leida tõkke p_n jaoks.

Teoreem 4.1 (Eukleides)**.** *Algarvude hulk on lõpmatu.*

Tõestus. Oletame vastuväiteliselt, et algarve on lõplik hulk, täpsemalt $\{p_1, p_2, ..., p_n\}$. Moodustame nüüd naturaalarvu

$$q = p_1 \cdot p_2 \cdot ... \cdot p_n + 1.$$

Kuna $q > 1$, siis aritmeetika põhiteoreemi kohaselt peab leiduma algarv, mis jagab arvu q. Eelduse kohaselt on $p_1, p_2, ..., p_n$ ainsad algarvud, järelikult peab leiduma selline indeks $i \in \{1, ..., n\}$, et p_i jagab arvu q. Et p_i jagab arvu $p_1 \cdot p_2 \cdot ... \cdot p_n$, siis ta peab jagama ka arvu $q - p_1 \cdot p_2 \cdot ... \cdot p_n = 1$, mis on vastuolus sellega, et $p_i > 1$. □

Järeldus 4.2. *Iga naturaalarvu n korral*

$$p_n < 2^{2^n}. \tag{4.1}$$

Tõestus. Tõestame väite induktsiooniga üle n.
Kontrollime, et väide kehtib, kui $n = 1$. Tõepoolest, $p_1 = 2 < 2^2$.
Oletame, et väide kehtib kuni arvuni $n = k - 1$, ehk $p_{k-1} < 2^{2^{k-1}}$. Näitame, et väide kehtib siis ka arvu $n = k$ korral.
Moodustame nüüd naturaalarvu $r = p_1 \cdot p_2 \cdot p_3 \cdot ... \cdot p_{k-1} + 1$. Eukleidese teoreemi tõestuse tõttu teame, et leidub mingi algarv $p_i \leq r$, $i > k - 1$, mis jagab arvu r. Seega võime kirjutada

$$\begin{aligned} p_k \leq p_i \leq r = p_1 \cdot p_2 \cdot p_3 \cdot ... \cdot p_{k-1} + 1 < 2^2 \cdot 2^4 \cdot 2^8 \cdot ... \cdot 2^{2^{k-1}} + 1 \\ = 2^{2+4+8+...+2^{k-1}} + 1 = 2^{2^k - 2} + 1 < 2^{2^k}. \end{aligned}$$

□

Esitame ja tõestame nüüd Saouteri algarvuvalemi.

Teoreem 4.3. *Kehtivad valemid*

$$\pi(x) = \sum_{i=2}^{\lfloor x \rfloor} \left\lfloor \frac{1}{\sum_{j=1}^{i} \left\lfloor \frac{1}{i+1-j\left\lfloor \frac{i}{j} \right\rfloor} \right\rfloor - 1} \right\rfloor \tag{4.2}$$

ja

$$p_n = \sum_{k=2}^{2^{2^n}} k \left\lfloor \frac{1}{1 + (\pi(k) + \pi(k-1) - 2n + 1)^2} \right\rfloor . \tag{4.3}$$

Tõestus. Tõestame kõigepealt valemi (4.2). Olgu r ja s suvalised reaalarvud, kusjuures $r \geq 0$. Sellisel juhul

$$\left\lfloor \frac{1}{1+r} \right\rfloor = \begin{cases} 1, & \text{kui } r = 0, \\ 0, & \text{kui } r > 0. \end{cases} \tag{4.4}$$

Kuna $(s-r)^2 \geq 0$, siis isegi $r < 0$ korral kehtib, et

$$\left\lfloor \frac{1}{1+(r-s)^2} \right\rfloor = \begin{cases} 1, & \text{kui } r = s \\ 0, & \text{kui } r \neq s. \end{cases} \tag{4.5}$$

Olgu $i > j \geq 1$ naturaalarvud. Tähistame sümboliga $r(i,j)$ jäägi, mis tekib arvu i jagamisel arvuga j. Sel juhul

$$r(i,j) = i - j \left\lfloor \frac{i}{j} \right\rfloor . \tag{4.6}$$

Võrduse (4.4) tõttu saame, et

$$\left\lfloor \frac{1}{1+r(i,j)} \right\rfloor = \begin{cases} 1, & \text{kui } j \text{ on } i \text{ jagaja}, \\ 0, & \text{kui } j \text{ ei ole } i \text{ jagaja}. \end{cases} \tag{4.7}$$

Tähistame arvu i jagajate arvu sümboliga $d(i)$ ja sümboliga $\sum_{d|i}$ summat üle arvu i kõigi naturaalarvuliste jagajate d. Siis

$$d(i) = \sum_{d|i} 1.$$

Arvestades võrdust (4.7) võime kirjutada, et

$$d(i) = \sum_{j=1}^{i} \left\lfloor \frac{1}{1 + r(i, j)} \right\rfloor. \tag{4.8}$$

Funktsiooni $d(i)$ väärtus iseloomustab naturaalarvu i järgmiselt:

$$d(i) = \begin{cases} 2, & \text{kui } i \text{ on algarv;} \\ a > 2, & \text{kui } i \text{ on kordarv.} \end{cases} \tag{4.9}$$

Olgu $P : \mathbb{N} \setminus \{1\} \to \{0, 1\}$ algarvude hulga karakteristlik funktsioon, st

$$P(i) = \begin{cases} 1, & \text{kui } i \text{ on algarv,} \\ 0, & \text{kui } i \text{ on kordarv.} \end{cases} \tag{4.10}$$

Võrduste (4.4) ja (4.9) kohaselt võime nüüd kirjutada, et

$$P(i) = \left\lfloor \frac{1}{1 + d(i) - 2} \right\rfloor = \left\lfloor \frac{1}{d(i) - 1} \right\rfloor.$$

Suvalise positiivse reaalarvu x korral on siis võrduse (4.10) tõttu

$$\pi(x) = \sum_{i=2}^{\lfloor x \rfloor} P(i) = \sum_{i=2}^{\lfloor x \rfloor} \left\lfloor \frac{1}{d(i) - 1} \right\rfloor,$$

millest seost (4.9) arvestades saame, et

$$\pi(x) = \sum_{i=2}^{\lfloor x \rfloor} \left\lfloor \frac{1}{\sum_{j=1}^{i} \left\lfloor \frac{1}{1+r(i,j)} \right\rfloor - 1} \right\rfloor.$$

Kasutades tähistust (4.6), olemegi näidanud, et

$$\pi(x) = \sum_{i=2}^{\lfloor x \rfloor} \left\lfloor \frac{1}{\sum_{j=1}^{i} \left\lfloor \frac{1}{i+1-j\left\lfloor \frac{i}{j} \right\rfloor} \right\rfloor - 1} \right\rfloor.$$

Tõestame nüüd valemi 4.3. Kui $n \geq 1$, siis on p_n vähim selline naturaalarv $k \geq 2$, mille korral $\pi(k) = n$. Seega $\pi(p_n) = n$ ja $\pi(p_n - 1) = n - 1$, mistõttu

$$\pi(p_n) + \pi(p_n - 1) = 2n - 1.$$

Olgu nüüd $k \geq 2$ suvaline naturaalarv, mille korral

$$\pi(k) + \pi(k-1) = 2n - 1.$$

Ilmselt

$$\pi(k) \leq \pi(k-1) + 1 = 2n - 1 - \pi(k) + 1 \quad \Longleftrightarrow \quad \pi(k) \leq n,$$

aga siis $\pi(k-1) \geq n-1$, millest saame, et $\pi(k) = n$ ja $\pi(k-1) = n-1$. Niisiis on k vähim selline naturaalarv, mille korral $\pi(k) = n$, ehk $k = p_n$. Järelikult

$$k = p_n \quad \Longleftrightarrow \quad \pi(k) + \pi(k-1) = 2n - 1.$$

Võrdust (4.5) arvestades saame nüüd, et

$$\left\lfloor \frac{1}{1 + (\pi(k) + \pi(k-1) - 2n + 1)^2} \right\rfloor = \begin{cases} 1, & \text{kui } k = p_n; \\ 0, & \text{kui } k \neq p_n. \end{cases}$$

Et kehtib ka võrratus (4.1), siis tõepoolest

$$p_n = \sum_{k=2}^{2^{2^n}} k \left\lfloor \frac{1}{1 + (\pi(k) + \pi(k-1) - 2n + 1)^2} \right\rfloor.$$

□

Näide 7. Kui $n = 3$, siis

$$\begin{aligned} p_3 = &\sum_{k=2}^{256} k \left\lfloor \frac{1}{1 + (\pi(k) + \pi(k-1) - 5)^2} \right\rfloor \\ &= 2 \cdot \left\lfloor \frac{1}{1 + (1 + 0 - 5)^2} \right\rfloor + 3 \cdot \left\lfloor \frac{1}{1 + (2 + 1 - 5)^2} \right\rfloor + 4 \cdot \left\lfloor \frac{1}{1 + (2 + 2 - 5)^2} \right\rfloor \\ &\quad + 5 \cdot \left\lfloor \frac{1}{1 + (3 + 2 - 5)^2} \right\rfloor + 6 \cdot \left\lfloor \frac{1}{1 + (3 + 3 - 5)^2} \right\rfloor + ... \\ &\quad + 256 \cdot \left\lfloor \frac{1}{1 + (54 + 54 - 5)^2} \right\rfloor \\ &= 2 \cdot 0 + 3 \cdot 0 + 4 \cdot 0 + 5 \cdot 1 + 6 \cdot 0 + ... + 256 \cdot 0 = 5. \end{aligned}$$

Tõepoolest $p_3 = 5$, aga isegi $n = 3$ korral oli summas 255 liidetavat ja arvutamisel hoidis aega kokku see, et $\pi(k)$ ja $\pi(k-1)$ väärtused olid meil juba teada.

Saouteri valemis küll kasutatakse vaid elementaarseid tehteid (liitmine, lahutamine, korrutamine, jagamine, astendamine ja reaalarvu täisosa leidmine), aga nende koguarv kasvab kiiresti ning suuremate n väärtuste korral tuleb eraldi tegeleda veel ka $\pi(k)$ ja $\pi(k-1)$ väärtuste leidmisega näiteks Saouteri esimese valemi (4.2) abil. Arvutusi saaks mõnevõrra, aga kokkuvõttes ikkagi mitte oluliselt, kokku hoida paremate tõketega p_n jaoks. Näiteks järeldust 1.3 kasutades võiksime valemi (4.3) üles kirjutada kujul

$$p_n = \sum_{k=2}^{2^n} k \left\lfloor \frac{1}{1 + (\pi(k) + \pi(k-1) - 2n + 1)^2} \right\rfloor,$$

mis vähendab oluliselt liidetavate arvu. Veel täpsemad tõkked, mida me siinkohal käsitleda ei jõua, pakkus teistele autoritele tuginedes välja Saouter ise [31]: kui $n \geq 6$, siis kehtib ka

$$p_n = \sum_{k=n(\log n + \log\log n - 1)}^{n(\log n + \log\log n)} k \left\lfloor \frac{1}{1 + (\pi(k) + \pi(k-1) - 2n + 1)^2} \right\rfloor.$$

Viited

[1] A. R. Ansari, *On prime representing function.* Ganita 2 (1951), 81–82.

[2] R. Baillie, *Wright's fourth prime.* arXiv:1705.09741v3 (2017).

[3] C. K. Caldwell, Y. Cheng, *Determining Mills' constant and a note on Honaker's problem.* J. Integer Seq. 8 (2005), artikkel 05.4.1.

[4] O. Cira, F. Smarandache, *Various Arithmetic Functions and their Applications.* Pons asbl, Brussels, 2016.

[5] E. Costa, R. Gerbicz, D. Harvey, *A search for Wilson primes.* Math. Comp. 83 (2014), 3071–3091.

[6] R. Crandall, K. Dilcher, C. Pomerance, *A search for Wieferich and Wilson primes.* Math. Comp. 66 (1997), 433–449.

[7] U. Dudley, *Formulas for primes.* Math. Magazine 56 (1983), 17–22.

[8] J. R. Ellis, *The computation of prime numbers by Gandhi's formula for the nth prime.* Math. Gaz. 65 (1981), 212–214.

[9] E. B. Escott, *Réponse 1133, Formule d'Euler* $x^2 + x + 41$ *et formules analogues.* L'Intermédiare des Math. 6 (1899), 10–11.

[10] L. Euler, *De numeris primis valde magnis.* Novi Comment. Acad. Sci. Imp. Petropol. 9 (1764), 99–153.

[11] L. Euler, *Extrait d'une lettre de M. Euler le Pere à M. Bernoulli concernant le Mémoire imprimé parmi ceux de 1771.* Nouveaux Mémoires de l'Académie des Sciences de Berlin, Histoire 1772 (1774), 35–36.

[12] P. H. Fuss (toim.), *Correspondance mathématique et physique de quelques célèbres géomètres du XVIIIème siècle, tome I.* L'Académie Impériale Des Sciences De Saint-Pétersbourg, St-Pétersbourg, 1843.

[13] J. M. Gandhi, *Formulae for the nth prime.* Proc. Washington State Univ. Conf. on Number Theory, Washington State University, Pullman, 1971, 96–107.

[14] S. W. Golomb, *A direct interpretation of Gandhi's formula.* Amer. Math. Monthly 81 (1974), 752–754.

[15] G. H. Hardy, E. M. Wright, *An Introduction to the Theory of Numbers*, fifth edition. Clarendon Press, Oxford, 1979.

[16] A. E. Ingham, *On the difference between consecutive primes.* Q. J. Math. 8 (1937), 255–266.

[17] C. Isenkrahe, *Ueber eine Lösung der Aufgabe, jede Primzahl als Function der vorhergehenden Primzahlen durch einen geschlossenen Ausdruck darzustellen.* Math. Ann. 53 (1900), 42–44.

[18] J. P. Jones, D. Sato, H. Wada, D. Wiens, *Diophantine representation of the set of prime numbers.* Amer. Math. Monthly 83 (1976), 449–464.

[19] L. Kuipers, *Prime-representing functions.* Nederl. Akad. Wetensch., Proc. 53 (1950), 309–310.

[20] V. Laan, L. Tart, aine „Arvuteooria“ loengukonspekt, 2018. https://courses.ms.ut.ee/2018/Arvuteooria/spring/Main/Lectures

[21] E. Landau, *Handbuch der Lehre von der Verteilung der Primzahlen* I. B. G. Teubner, Leipzig und Berlin, 1909.

[22] A. M. Legendre, *Essai sur la théorie des nombres.* Duprat, Paris, 1798.

[23] P. G. Lejeune-Dirichlet, *Beweis des Satzes, dass jede unbegrenzte arithmetische Progression, deren erstes Glied und Differenz ganze Zahlen ohne gemeinschaftlichen Factor sind, unendlich viele Primzahlen enthält.* Abh. K. Preuss. Akad. Wiss. 1837 (1839), 45–81.

[24] N. Mackinnon, *Prime number formulae.* Math. Gaz. 71 (1987), 113–114.

[25] Ю. В. Матиясевич, *Простые числа перечисляются полиномом от 10 переменных.* Зап. Науч. Сем. Ленинград. Отдел. Мат. Инст. Стеклов. 68 (1977), 62–82.

[26] W. H. Mills, *A prime-representing function.* Bull. Amer. Math. Soc. 53 (1947), 604.

[27] *Nicomachus of Gerasa: Introduction to Arithmetic.* M. L. D'Ooge tõlge, Macmillan, New York, 1926.

[28] I. Niven, *Functions which represent prime numbers.* Proc. Amer. Math. Soc. 2 (1951), 753–755.

[29] G. Rabinowitsch, *Eindeutigkeit der Zerlegung in Primzahlfaktoren in quadratischen Zahlkörpern.* J. Reine Angew. Math. 142 (1913), 153–164.

[30] P. Ribenboim, *Are there functions that generate prime numbers?* College Math. J. 28 (1997), 352–359.

[31] Y. Saouter, *A (doubly) elementary formula for prime numbers.* Math. Gaz. 101 (2017), 93–95.

[32] W. Sierpiński, *Sur une formule donnant tous les nombres premiers.* C. R. Acad. Sci. Paris 235 (1952), 1078–1079.

[33] П. Чебышев, *Mémoire sur les nombres premiers.* J. Math. Pures Appl. Sér. 1 17 (1852), 366–390.

[34] C. Vanden Eynden, *A Proof of Gandhi's formula for the nth prime.* Amer. Math. Monthly 79 (1972), 625.

[35] C. P. Willans, *On formulae for the nth prime number.* Math. Gaz. 48 (1964), 413–415.

[36] E. M. Wright *A prime-representing function.* Amer. Math. Monthly 58 (1951), 616–618.

Lihtlitsents lõputöö reprodutseerimiseks ja lõputöö üldsusele kättesaadavaks tegemiseks

Mina, Kadri Sügis (sünnikuupäev 21.10.1967),

1. annan Tartu Ülikoolile tasuta loa (lihtlitsentsi) enda loodud teose „Algarvuvalemitest", mille juhendaja on Lauri Tart,
   1.1 reprodutseerimiseks säilitamise ja üldsusele kättesaadavaks tegemise eesmärgil, sealhulgas digitaalarhiivi DSpace lisamise eesmärgil kuni autoriõiguse kehtivuse tähtaja lõppemiseni;
   1.2 üldsusele kättesaadavaks tegemiseks Tartu Ülikooli veebikeskkonna kaudu, sealhulgas digitaalarhiivi DSpace 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 intellektuaalomandit ega isikuandmete kaitse seadusest tulenevaid õigusi.

Tartu, 8. mai 2018