Algarvuvalemitest

Kadri Sügis[10]

Tartu Ülikool

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

Esimesed algarvud saab leida lihtsalt proovimise teel: $p_1 = 2$, $p_2 = 3$, $p_3 = 5$, $p_4 = 7$, $p_5 = 11$, $p_6 = 13$, $p_7 = 17$, $p_8 = 19$, $p_9 = 23$, $p_{10} = 29$. 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 tunneme *Eratosthenese sõelana*.

Algarvuvalemid ei ole väga vanad: 18. sajandil uuris L. Euler sellest seisukohast polünoome, esimesed valemid ilmusid 19. sajandi lõpus. 20. sajandi alguses tõestas L. Landau, et

$$p_n \sim n \log n,$$

st $\frac{p_n}{n \log n} \to 1$ protsessis $n \to \infty$. Viimane aga ei ole täpne valem. Proovitud on leida ka täpseid valemeid. P. Ribenboim [6] jagab probleemi kolmeks erinevaks ülesandeks:
(a) leida selline funktsioon f, et $f(n) = p_n$ iga naturaalarvu n korral,

[10]Kadri Sügise bakalaureusetöö *Algarvuvalemitest* pälvis Eesti Matemaatika Seltsi 2018. a. üliõpilaspreemia.

(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.
Käesolevas artiklis esitatakse erinevat liiki valemeid, mis kokku esindavad kõiki kolme Ribenboimi ülesannete klassi.

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

Järgnevas tutvustame väikest valikut algarvuliste väärtustega valemitest ja nendega seotud tulemustest ning toome näiteid, mis demonstreerivad käsitletud valemite arvutuslikku ebaefektiivsust algarvude leidmisel.

Algarvuliste väärtustega 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

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

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 kirjas J. Bernoullile, et polünoomi

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

väärtused on algarvud, kui $x = 1, \ldots, 40$. 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 on Euleri polünoomiks nimetatud ka polünoomi $g(x) = x^2 + x + 41$, mille puhul A. M. Legendre pani 1798. aastal tähele, et selle väärtused

on algarvud, kui $x = 0, 1, \ldots, 39$. Euleri polünoomi diskriminanti $D = -163$ aluseks võttes on leitud rida polünoome, mis samuti annavad väärtustena algarve. Näiteks E. B. Escotti poolt 1899. aastal välja pakutud polünoom $g(x-40) = x^2 - 79x + 1601$, mille väärtuseks on algarvud, kui $x = 0, 1, \ldots, 79$.

On leitud ka kõrgema astme polünoome, mis teatud piirini genereerivad algarve. Näiteks Wroblewski ja Meyrignaci polünoom $n^5 - 99n^4 + 3588n^3 - 56822n^2 + 348272n - 286397$, mis annab algarve $n = 0, 1, \ldots, 46$ korral.

Toetudes varasematele tulemustele, tõestasid J. P. Jones, D. Sato, H. Wada ja D. Wiens [3] 1976. aastal, et 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 $a, b, c, \ldots, z$ ja selle aste on 25. Kui muutujad asendada positiivsete täisarvudega, siis polünoomi positiivsed väärtused vastavad täpselt algarvude hulgale $2, 3, 5, \ldots$.

Jones, Sato, Wada ja Wiens püstitasid ka küsimuse, milline on sellise polünoomi vähim võimalik aste ja kui väheste muutujatega on üldse võimalik algarvude hulka esitada. Nende väitel on võimalik polünoomi astet vähendada kuni viieni, aga sellisel juhul oleks muutujate arv 42. 1977. aastal tõestas J. V. Matijasevitš [4], kelle eelnevale tööle Jones, Sato, Wada ja Wiens toetusid, et saab koostada ka ainult kümne muutujaga polünoomi, mille positiivsete

väärtuste hulk vastab täpselt algarvude hulgale. Polünoomi aste on sellisel juhul 15905.

Mitmesugused algarvuvalemid. Meenutame kõigepealt, et *arvu (alumine) täisosa* on funktsioon, mis on määratud reaalarvude hulgal ja mille väärtused on täisarvud. Kui m on täisarv ja kehtivad võrratused $m \le x < m+1$, siis öeldakse, et reaalarvu x (alumine) täisosa on m ja kirjutatakse $\lfloor x \rfloor = m$.

1947. aastal tõestas W. H. Mills [5], et eksisteerib niisugune reaalarv A, et

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

on algarv iga täisarvu $x \ge 1$ korral. Reaalarvu A väärtust Mills kindlaks ei määranud.

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

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

Neist viimane on 6854-kohaline.

Millsi valemiga analoogilise valemi leidis E. M. Wright [10], kes tõestas 1951. aastal, et leidub selline arv α, et kui $g_0 = \alpha$, $g_{n+1} = 2^{g_n}$, $n \ge 0$, siis

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

on alati algarv. Wright tõi näitena ühe võimalikest α väärtustest $\alpha = 1,9287800\ldots$, mis annab algarvud $\lfloor g_1 \rfloor = \lfloor 2^{\alpha} \rfloor = 3$, $\lfloor g_2 \rfloor = 13$, $\lfloor g_3 \rfloor = 16381$ ja $\lfloor g_4 \rfloor$ on umbes 5000-kohaline algarv.

R. Baillie [1] 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 $\lfloor g_4 \rfloor$.

1952. aastal konstrueeris W. Sierpiński [8] n-nda algarvu leidmiseks valemi

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

kus $n = 1, 2, \ldots$ ja reaalarv $\alpha = \sum_{m=1}^{\infty} p_m 10^{-2^m}$. Kuna

$$\begin{aligned}\alpha &= 2 \cdot 10^{-2} + 3 \cdot 10^{-4} + 5 \cdot 10^{-8} + 7 \cdot 10^{-16} + 11 \cdot 10^{-32} + \cdots = \\ &= 0,020300050000000700000000000000110\ldots,\end{aligned}$$

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

Näide 1. Leiame Sierpiński valemit kasutades esimesed kolm algarvu:

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

Samas on valem täiesti kasutu, sest p_n arvutamiseks on vaja teada α täpset väärtust kuni 2^n kümnendkohani, mis omakorda nõuab, et me teaksime algarvude $p_1, \ldots, p_n$ väärtusi.

Toome ära ka kaks Wilsoni teoreemile tuginevat valemit. Wilsoni teoreemina tuntakse järgmist tulemust.
Naturaalarv $n > 1$ on algarv parajasti siis, kui arv $(n-1)!+1$ jagub arvuga n.

1964. aastal näitas C. P. Willans [9] Wilsoni teoreemi põhjal, et

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

kus

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

Valemit on lihtne kasutada, kui n on väike ja $\pi(m)$ väärtused on teada.

Näide 2. Olgu $n = 6$, siis:

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

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

Wilsoni teoreemile tuginedes näitasid G. H. Hardy ja E. M. Wright, et iga naturaalarvu n korral võib kirjutada

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

kus

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

Hardy ja Wrighti valemi abil saab jällegi väikeste n väärtuste korral algarve p_n veel leida, seda eriti juhul, kui juba eelnevalt on teda $\pi(k)$ väärtused. Sarnaselt Willansi valemile, on ka siin summas 2^n liidetavat ja valemi kasutegur on küsitav.

2017. aasta märtsis ilmus ajakirjas *The Mathematical Gazette* Yannick Saouteri artikkel [7], mille pealkiri lubab kahes mõttes elementaarset valemit algarvude jaoks. Huvi äratas valem osaliselt just sellesama kahekordse elementaarsuse tõttu: valem sisaldab ainult „elementaarseid“ 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.
Saouter näitas, et n-nda algarvu saab leida valemiga

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

kus

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

Näide 3. Kui $n = 3$, siis

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

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. Arvutusi saaks mõnevõrra, aga kokkuvõttes ikkagi mitte oluliselt, kokku hoida arvust 2^{2^n} paremate tõketega p_n jaoks.

Artikli ilmumine näitab, et algarvuvalemite leiutamine jätkub tänapäevani. Kahjuks ei ole seniajani arvutuslikult efektiivset valemit leitud.

Kirjandus

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

[2] C. K. Caldwell, Y. Cheng, Determining Mills' constant and a note on Honaker's problem. *J. Integer Seq.* 8 (2005), Article 05.4.1, 9 pp.

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

[4] Ju. V. Matijasevič, Primes are enumerated by a polynomial in 10 variables. (Russian) Theoretical applications of the methods of mathematical logic, II. *Zap. Naučˇ. Sem. Leningrad. Otdel. Mat. Inst. Steklov. (LOMI)* 68 (1977), 62–82.

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

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

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

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

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

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

