VILNIUS UNIVERSITY

Tomas Plankis

COMPUTER CALCULATIONS FOR SOME SEQUENCES AND POLYNOMIALS

Doctoral dissertation

Physical sciences, mathematics (01P)

Vilnius, 2009

The scientific work was carried out in 2005–2009 at Vilnius University.

Scientific supervisor:

Prof. Dr. Habil. Artūras Dubickas (Vilnius University, Physical sciences, Mathematics - 01P)

Scientific adviser:

Prof. Dr. Habil. Ramūnas Garunkštis (Vilnius University, Physical sciences, Mathematics - 01P)

VILNIAUS UNIVERSITETAS

Tomas Plankis

KOMPIUTERINIAI SKAIČIAVIMAI KAI KURIOMS SEKOMS IR POLINOMAMS

Daktaro disertacija

Fiziniai mokslai, matematika (01P)

Vilnius, 2009

Disertacija rengta 2005–2009 metais Vilniaus universitete.

Mokslinis vadovas:

prof. habil. dr. Artūras Dubickas (Vilniaus universitetas, fiziniai mokslai, matematika - 01P)

Konsultantas:

prof. habil. dr. Ramūnas Garunkštis (Vilniaus universitetas, fiziniai mokslai, matematika - 01P)

Contents

Žymėjimai

$\mathbb{N}$	natūraliųjų skaičių aibė
$\mathbb{Z}$	sveikųjų skaičių aibė
$\mathbb{P}_n$	n-tojo laipsnio Niumano polinomų aibė
$\deg P$	polinomo P laipsnis
$H(P)$	polinomo P aukštis
$\mathbb{P}$	$\bigcup_{n=1}^{\infty} \mathbb{P}_n$ (visų Niumano polinomų aibė)

Įvadas

Šioje disertacijoje bus nagrinėjamos problemos kurias sprendžiau studijuodamas Vilniaus universitete matematikos doktorantūros studijų programoje. Čia bus nagrinėjamos rekurenčiųjų sekų dalumo savybės, Niumano polinomai ir kompiuterių panaudojimas atliekant įvairius matematinius skaičiavimus, susijusius su minėtais skaičių teorijos klausimais.

Aktualumas. Matematika ir skaičiavimai glaudžiai tarpusavyje susiję. Pirmuosius mechaninius skaičiavimo įrenginius naudojo dar antikos laikų matematikai, inžinieriai ir prekeiviai. Tobulėjant technologijoms įrenginiai keitėsi ir tobulėjo. Sukūrus kompiuterius ėmė vystytis nauja mokslo šaka - informatika - tyrinėjanti informacijos apdorojimą. Dėl savo universalumo kompiuteriai yra tinkami įvairiems sudėtingiems matematiniams skaičiavimams arba modeliavimui atlikti bei patikrinti įvairioms hipotezėms. Tačiau tokiuose uždaviniuose iškyla algoritmų sudėtingumo problema. Sudėtingumo teorija yra informatikos šaka, nagrinėjanti įvairias algoritmų savybes, dažnai jų įvykdymo greitį. Teorija atsako į klausimą kaip palyginti skirtingus algoritmus sprendžiančius tą pačią užduotį ir kurie algoritmai yra geriausi. Dažniausiai svarbus yra algoritmo veikimo laikas, bet taip pat nagrinėjama kiek algoritmas sunaudoja atminties, ar jis apskritai baigia darbą, ar galima jį vykdyti lygiagrečiai su keliais kompiuteriais. Kadangi matematika yra labai platus mokslas buvo nuspręsta patyrinėti kompiuterinio skaičiavimo galimybes rekurentinėse sekose, nes sveikųjų skaičių sekos, turinčios be galo daug pirminių skaičių, radimas yra vienas seniausių uždavinių skaičių teorijoje. Kita tyrimo dalis buvo susijusi su Niumano polinomais, nes pastaruoju metu jų tyrimui skiriama daug dėmesio. Jų pagalba ieškoma atsakymų į kitus skaičių teorijos klausimus, susijusius su adityviąja skaičių teorija, Sidono aibėmis ir kitais uždaviniais.

Tikslai ir uždaviniai. Pirmasis šio darbo tikslas – ištirti tam tikrų rekurenčiųjų sekų dalumo savybes. Šiam tikslui pasiekti buvo nagrinėjami tokie uždaviniai:

- Kada seka moduliu g yra periodinė?
- Ar šeka moduliu g turi be galo daug nulių?
- Ar sekos nulių kiekis priklauso nuo pirmojo sekos elemento pasirinkimo?

Antrasis šio darbo tikslas – efektyvių algoritmų paieška. Algoritmų buvo ieškoma šiems atvejams:

- rekurenčiųjų sekų dalumo savybių tyrimui
- skaičiuojant $\inf_{P\in\mathbb{P}_n} Q_2(P)$, kur P yra Niumano polinomas, o

$$Q_2(P) = (\deg(P)+1)H(P^2)/P(1)^2.$$

Metodai. Pirmoje dalyje naudojami aritmetiniai metodai: skaičiavimo moduliu savybės, indukcija, kai kurie klasikiniai skaičių teorijos rezultatai, kaip Ferma ir Oilerio teoremos. Algoritmai buvo kuriami pasinaudojant Maple matematiniu paketu. Algoritmų sudėtingumui vertinti naudojama sudėtingumo teorija.

Antroje dalyje naudojamos programavimo C++ kalba žinios, kombinatorika ir statistiniai metodai kaip regresinė analizė.

Darbo struktūra. Disertacija parašyta lietuvių kalba. Ją sudaro įvadas, du skyriai, išvados, literatūros ir publikacijų disertacijos tema sąrašai. Bendra darbo apimtis - 67 puslapiai.

Naujumas ir praktinė vertė. Šioje disertacijoje pateikti pagrindiniai rezultatai yra nauji. Jie buvo pristatyti konferencijose (žiūrėti skyrelį "Aprobacija") ir išspausdinti įvairiuose žurnaluose ir leidiniuose (žiūrėti skyrelį "Publikacijų sąrašas"). Gauti rezultatai yra ir teorinio, ir praktinio pobūdžio.

Aprobacija. Disertacijos rezultatai buvo pristatyti Vilniaus universiteto matematikos ir informatikos fakulteto tikimybių teorijos ir skaičių teorijos katedros skaičių teorijos seminaruose, taip pat ketvirtojoje tarptautinėje konferencijoje (Palanga, Lietuva, 2006) ir tikimybių teorijos ir skaičių teorijos doktorantų vasaros mokykloje 2007 (Druskininkai, Lietuva, 2007).

Publikacijų sąrašas. Pagrindiniai disertacijos rezultatai yra išspausdinti straipsniuose:

- T. Plankis, *Divisibility properties of a recurrent sequence,* in A. Laurinčikas and E. Manstavičius (eds.): Analytic and Probabilistic Methods in Number Theory (Proceedings of the fourth international conference in honour of J. Kubilius, Palanga, Lithuania, 25-29 September 2006), (2007), 150–155.
- T. Plankis, *Divisibility properties of recurrent sequences,* Nonlinear analysis : modelling and control, **13 (4)** (2008), 503–511.
- A. Dubickas, T. Plankis, *Periodicity of some recurrence sequences modulo m,* Integers, **8 (1)** (2008), #A42, 6 p.
- T. Plankis, *Calculations for Newman polynomials,* Šiauliai mathematical seminar **4 (12)** (2009), 157–165.

Padėkos. Norėčiau išreikšti ypatingą padėką savo vadovui profesoriui Artūrui Dubickui. Man labai padėjo jo vadovavimas, įžvalga ir žinios. Taip pat norėčiau padėkoti savo tėvams už palaikymą rašant šią disertaciją.

Apžvalga ir svarbiausi rezultatai. Egzistuoja keletas neišspręstų problemų, susijusių su sekomis $[\alpha^n]$, $n = 1, 2, 3, \ldots$, kur $\alpha > 1$ yra fiksuotas realusis skaičius ir

$[x]$ yra sveikoji realiojo skaičiaus x dalis. Stebina, kad kai kurios iš jų yra neišspręstos. Pavyzdžiui, jei α nėra sveikasis skaičius, toks paprastas klausimas, ar seka $[\alpha^n]$, $n = 1, 2, 3, \ldots$, turi be galo daug sudėtinių skaičių, lieka neatsakytas išskyrus kelis atskirus atvejus. Tikėtina, kad egzistuoja be galo daug sudėtinių skaičių pavidalo $[\alpha^n]$, $n \in \mathbb{N}$, su visais $\alpha > 1$. Formanas (Forman) ir Šapiro (Shapiro) [37] tą įrodė, kai $\alpha = 3/2$ ir $\alpha = 4/3$, o Dubickas ir Novikas [32] tą įrodė, kai $\alpha = 5/4$. Daugiau nėra žinoma racionaliųjų skaičių α, nepriklausančių sveikųjų skaičių aibei, kuriems seka $[\alpha^n]$, $n = 1, 2, 3, \ldots$, turėtų be galo daug sudėtinių skaičių. Apie rezultatus, susijusius su algebriniu iracionaliu skaičiumi α, galima pasiskaityti straipsniuose [16, 29, 31]. Gajus (Guy) [40] suformuluotoje problemoje E19 klausė, ar seka $[\alpha^n]$, $n = 1, 2, 3, \ldots$, kur α yra racionalieji, nepriklausantys sveikųjų skaičių aibei, skaičiai, turiu be galo daug pirminių skaičių. Tikėtina, kad ši problema yra dar sudėtingesnė. Vis dar lieka nežinomi tokie α su minėtąja savybe. Vis dėlto, straipsniuose [51, 71] ir [7] pateiktas tokių skaičių egzistavimo įrodymas. Pastebėsime, kad metriniai rezultatai yra gerai žinomi. Juos nesunku išsivesti iš 1935 metų Koksma darbo [44]: su kiekvienu $\xi \neq 0$, trupmeninių dalių seka $\{\xi\alpha^n\}$, $n = 1, 2, 3, \ldots$, yra tolygiai pasisikirsčiusi intervale $[0, 1)$ beveik visiems $\alpha > 1$. Pritaikius šį rezultatą, kai $\xi = 1/2$, matome, kad tokiems α, $\{\alpha^n/2\} < 1/2$ su be galo daug n. Taigi, seka $[\alpha^n]$, $n = 1, 2, 3, \ldots$, turi be galo daug lyginių skaičių beveik visiems $\alpha > 1$. ([10] straipsnyje pateikti naujausi metriniai rezultatai.) Vadinasi, rezultatai apie sveikąsias dalis yra glaudžiai susiję su atitinkamais rezultatais apie trupmenines dalis. Apie trupmeninių dalių $\{\xi\alpha^n\}$, $n = 1, 2, 3, \ldots$, pasiskirstymą galima daugiau sužinoti straipsniuose [1, 2, 14, 26, 36, 49, 67].

Daugiau apie įvairias sekas galima sužinoti straipsniuose [63, 42, 65, 48, 57, 21, 23, 20, 17, 9, 56, 68, 25, 59, 46]. Pavyzdžiui, Stivensas (Stevens) [63] tyrinėjo Konelio (Connell) seką $1, 2, 4, 5, 7, 9, 10, 12, 14, 16, \ldots$, kurios bendrojo nario formulė yra

$$x_n = 2n - \left[\frac{1}{2}(1 + \sqrt{8n - 7})\right].$$

Jis pateikė du apibendrinimus šiai sekai, iš kurių vienam panaudojamas skaičiavimas moduliu. Apibendrinta Konelio k-seka tuomet apibrėžiama taip: imamas

vienas natūralusis skaičius tapačiai lygus 1 moduliu k, tada imami du natūralieji skaičiai tapačiai lygūs 2 moduliu k, toliau imami trys natūralieji skaičiai tapačiai lygūs 3 moduliu k ir t.t., kur k yra fiksuotas natūralusis skaičius. Apie kai kurių sekų savybes plačiau galima sužinoti straipsniuose [33, 47, 62, 41, 60, 61, 19, 66, 4, 70, 52, 53, 11]. Pavyzdžiui, Klarkas (Clark) [19] pateikė paprastą Katalono-Lakombe-Franko (Catalan-Larcombe-French) sekos asimptotinio tęsinio įrodymą. Apie sekų sąsajas su kitomis matematikos šakomis galima plačiau pasidomėti straipsniuose [15, 22, 35, 8, 38, 12, 43, 34, 58, 3, 24, 39]. Pavyzdžiui, Konrojus (Conroy) [22] tyrinėjo sekas, susijusias su Šincelio (Schinzel) hipoteze, kuri tvirtina, kad visus natūraliuosius skaičius galima užrašyti kaip

$$\frac{p+1}{q+1},$$

kur p ir q yra pirminiai skaičiai. Kaip sekos susijusios su muzika galima pasiskaityti straipsnyje [5].

Šio darbo pradžia galima laikyti Alkausko ir Dubicko darbe [7] suformuluotą teoremą. Čia pateiksime šiek tiek performuluotą teiginį:

TEOREMA. *Tegul sekos rekurentinis sąryšis yra* $x_n \equiv (x_{n-1}^n + n - 1) \bmod g$, *kur* $n \in \mathbb{N}$, $x_0 \in \mathbb{N}$. *Seka turi be galo daug nulių, jei* g *yra pirminis skaičius, didesnis už* 2.

Įrodymas. Tegul $n = p(p-1)k$, kur $k \in \mathbb{N}$. Tvirtiname, kad arba x_{n-1}, arba x_n dalijasi iš p. Tikrai, jei x_{n-1} nesidalija iš p, tuomet, remiantis Mažąja Ferma teorema

$$x_{n-1}^n = x_{n-1}^{p(p-1)k} \equiv 1 \pmod{p}.$$

Iš čia gauname, kad $x_n = x_{n-1}^n - 1 + p(p-1)k$ dalijasi iš p. □

Atkreipsime dėmesį, kad tiek šioje teoremoje, tiek tolimesniame darbe rekurentinė seka moduliu g suprantama kaip seka sudaryta iš skaičių, priklausančių aibei $\{0, 1, 2, \ldots, g-1\}$.

Mus domino tokie klausimai:

- ar rekurentinės sekos yra periodinės?
- ar periodinės rekurentinės sekos kokiam nors moduliui g turi be galo daug nulių?
- kaip priklauso rekurentinės sekos nulių skaičius nuo pirmojo tos sekos nario?

Pirmajame tyrimo etape buvo nagrinėjamas teoremoje pateiktas rekurentinis sąryšis. Buvo suformuluoti ir įrodyti keli teiginiai ir atlikti paprasčiausi kompiuteriniai skaičiavimai tyrinėjant sekų sandarą.

Toliau pateiktas teiginys įdomus tuo, kad jį pavyko įrodyti paprastu aritmetiniu metodu.

TEIGINYS 1.1. *Tegul rekurentinis sąryšis yra* $x_n \equiv x_{n-1}^n + n - 1 \pmod{g}$, *čia* $n, x_0 \in \mathbb{N}$. *Jei* $g = 2^m$, *kur* $m > 1$ *ir* $m \in \mathbb{N}$, *tuomet sekoje yra be galo daug nulių, jei* x_0 *yra bet koks lyginis skaičius.*

Atskirą grupę sudaro Karmaiklo skaičiai [6].

APIBRĖŽIMAS 1.2. *Karmaiklo skaičiumi vadinamas sudėtinis skaičius* $n \in \mathbb{N}$, *kuris tenkina tapatybę* $b^{n-1} \equiv 1 \pmod{n}$, *su visais* $b \in \mathbb{Z}$ *tarpusavyje pirminiais su* n.

TEOREMA (KORSELTO [73]). *Sudėtinis skaičius* $n \in \mathbb{N}$ *yra Karmaiklo skaičius tada ir tiktai tada, kai* n *yra bekvadratis ir visiems skaičiaus* n *pirminiams dalikliams* p *teisingas sąryšis* $(p-1)|(n-1)$.

Karmaiklo skaičiai kartais vadinamis "absoliučiai pseudopirminiais" ir tenkina Korselto kriterijų.

R. D. Karmaiklas pirmą kartą pastebėjo tokių skaičių egzistavimą 1910 metais, apskaičiavo 15 reikšmių ir numatė, kad jų yra be galo daug.

Pirmieji Karmaiklo skaičiai yra 561, 1105, 1729, 2465, 2821, 6601, 8911, 10585, 15841, 29341, ...

Karmaiklo skaičiai tenkina sekančias savybes:

(1) Jei pirminis skaičius p dalija Karmaiklo skaičių n, tada $n \equiv 1 \pmod{p-1}$ reiškia, kad $n \equiv p \pmod{p(p-1)}$.
(2) Kiekvienas Karmaiklo skaičius yra bekvadratis.
(3) Nelyginis sudėtinis bekvadratis skaičius n yra Karmaiklo skaičius, jei n dalija Bernulio skaičiaus B_{n-1} vardiklį.
(4) Karmaiklo skaičiai turi mažiausiai tris pirminius daugiklius.

Karmaiklo skaičių yra be galo daug. Tai buvo įrodyta Alfordo (Alford), Granvilio (Granville) ir Pomeranco (Pomerance) [6].

TEIGINYS 1.3. *Jeigu g yra Karmaiklo skaičius, tuomet seka $x_n \equiv x_{n-1}^n + n - 1 \pmod{g}$, čia $n, x_0 \in \mathbb{N}$, turi be galo daug nulių.*

Atkreipkime dėmesį į rekurentinį sąryšį. Kaip matome, seka generuojama pridedant n. Tačiau, kai nagrinėjame modulį, pastebime, kad iš esmės mes pridedame skaičius $0, ..., g-1$ didėjimo tvarka ir vėliau kartojame tą patį ciklą. Todėl sekos periodiškumas bus funkcija priklausanti nuo g. Teiginiai lengvai įrodomi remiantis matematinės indukcijos metodu ir Mažąja Ferma teorema.

APIBRĖŽIMAS 1.4. *Seką $x_1, x_2, x_3, ...$ vadinsime periodine, jei egzistuoja toks $t \in \mathbb{N}$ ir $N \in \mathbb{N}$, kad $x_n = x_{n+t}$, su visais $n > N$. Skaičius t vadinamas šios sekos periodu.*

TEIGINYS 1.5. *Tegul rekurentinis sąryšis yra $x_n \equiv (x_{n-1}^n + n - 1) \pmod{g}$, čia $n, x_0 \in \mathbb{N}$. Jei g yra pirminis ir $g > 2$, tuomet sekos periodas yra $g(g-1)$. Kai $g = 2$, sekos periodas yra 4.*

TEIGINYS 1.7. *Jei $g = 2^m$, $m > 1$, tuomet seka $x_n \equiv (x_{n-1}^n + n - 1) \pmod{g}$, čia $n, x_0 \in \mathbb{N}$, yra periodinė, su periodu g.*

TEIGINYS 1.8. *Tarkime, kad g yra Karmaiklo skaičius. Tada seka $x_n \equiv (x_{n-1}^n + n - 1) \pmod{g}$, čia $n, x_0 \in \mathbb{N}$, yra periodinė, su periodu $g(g-1)$.*

Pastebėsime, kad periodas nebūtinai yra mažiausias. Pavyzdžiui, kai $g = 3$, mažiausias periodas yra 3, o ne 6.

Atlikti statistiniai skaičiavimai leidžia teigti, kad sąryšiui minėti klausimai yra teisingi. Duomenys buvo gauti nagrinėjant įvairias skaičių grupes: pirminiai, dvejeto laipsniai ir t.t. Sekos yra periodinės, tačiau nulių skaičius priklauso nuo pradinio elemento pasirinkimo. Suformuluosime hipotezę:

HIPOTEZĖ 1.9. *Tegul rekurentinis sąryšis yra* $x_n \equiv (x_{n-1}^n + n - 1) \pmod{g}$, *čia* $n, g \in \mathbb{N}$, $g > 1$. *Seka turi be galo daug nulių, kai* $x_0 = 2k$, $k = 0, 1, 2, ...$

Kai kurios grupės pasižymi įdomiomis savybėmis.

APIBRĖŽIMAS 1.10. *Fiksuokime* $g > 1$. *Tegul turime sekų grupę genruotą rekurentinio sąryšio moduliu* g *ir pradinių sekos narių aibės* $\{0, 1, \ldots, g-1\}$. *Tokią grupę vadinsime g-stabilia, jei, nuo tam tikro sekos eilės numerio* N, *sekos nariai nepriklauso nuo pradinio elemento* x_0.

PAVYZYDYS 1.11. *Tegul* $a_0 = 2$, $g = 5$. *Tada:*

x_0	x_1	x_2	x_3	x_4	x_5	x_6	x_7	x_8	x_9	x_{10}	x_{11}	x_{12}	x_{13}	x_{14}
0	1	3	4	3	4	0	2	0	4	4	2	4	4	3
1	2	0	3	2	4	0	2	0	4	4	2	4	4	3
2	0	2	4	3	4	0	2	0	4	4	2	4	4	3
3	0	2	4	3	4	0	2	0	4	4	2	4	4	3
4	2	0	3	2	4	0	2	0	4	4	2	4	4	3

APIBRĖŽIMAS 1.12. *P(g) - žymėsime funkciją, apibrėžiančią mažiausią rekurentinės sekos periodą.*

HIPOTEZĖ 1.13. *Tegul rekurentinis sąryšis yra* $x_n \equiv (x_{n-1}^n + n - 1) \pmod{g}$, *čia* $n, g \in \mathbb{N}$, $g > 2$, $g = p^a$, $a = 0, 1, 2, ...$ *Tuomet seka turi be galo daug nulių.*

HIPOTEZĖ 1.14. *Tegul rekurentinis sąryšis yra* $x_n \equiv (x_{n-1}^n + n - 1) \pmod{g}$, *čia* $n, g \in \mathbb{N}$, $g > 2$, $g = p^a$, $a = 0, 1, 2, ...$ *Tuomet sekos periodas yra* $gP(p) = p^a(p-1)$.

Pastarosios dvi hipotezės glaudžiai susijusios tarpusavyje, kaip ir pirminių skaičių atveju. Griežto įrodymo nėra, bet tai galima iš dalies paaiškinti Oilerio teorema:

OILERIO TEOREMA. *Tegul $\varphi(n)$ yra Oilerio funkcija, apibrėžianti natūraliųjų skaičių $\leqslant n$ ir tarpusavyje pirminių su n kiekį. Tuomet, su visais $a \in \mathbb{N}$, tokiais, kad $(a, n) = 1$, galioja tapatybė:*

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

Straipsnyje [27] Dubickas įrodė periodiškumą bendresniu atveju:

TEOREMA. *Tegul $x_0, g \in \mathbb{N}$, $m > 1$, ir $F(z)$ - polinomas su sveikaisiais koeficientais. Tada seka apibrėžta rekurentiniu sąryšiu $x_n \equiv x_{n-1}^n + F(n) \pmod{g}$, $n = 1, 2, 3, ...$ yra periodinė.*

Įrodymas. Tegul D_g yra skaičiaus g daliklių didesnių už 1 aibė. Mažiausią bendrą kartotinį skaičių g ir $\{\varphi(d), d \in D_g\}$ pažymėkime $l(g)$. Čia φ yra Oilerio funkcija.

Tegul s yra sveikasis skaičius didesnis už $\log_2 g$, t. y. $s = [\log_2 g] + 1$. Nagrinėsime seką $x_{s+kl(g)}, k = 0, 1, 2, ...$, moduliu g. Paimkime du sekos elementus x_t ir $x_{t+ul(g)}$, kurie yra lygūs moduliu g. (Visada galima parinkti tokius $u \leqslant g$ ir $t \leqslant s+g = g+[\log_2 g]+1$.) Tvirtiname, kad $x_{n+ul(g)} - x_n$ dalijasi iš g su kiekvienu $n \geqslant t$. Taigi, matome, kad seka $x_n, n = 1, 2, 3, ...$ yra periodinė moduliu g. (Be to, aukščiau minėti įverčiai leis spėti, kad periodo ilgis $\leqslant gl(g)$ ir priešperiodinė dalis $\leqslant g + [\log_2 g] + 1$.)

$x_{n+ul(g)} - x_n$ dalumas iš g įrodomas naudojantis indukcijos metodu. Tarkime, kad taip yra, kai $n = t$. Tegul ši savybė galioja, kai $n := n - 1$. T. y., x_{n-1} ir $x_{n-1+ul(g)}$ yra lygūs moduliu g ir, tarkime, kad jie abu lygūs r moduliu g, kur $0 \leqslant r \leqslant m - 1$. Pastebėsime, kad $F(n + ul(g)) - F(n)$ dalijasi iš g, nes $g|l(g)$. Iš sąryšių

$$x_{n+ul(g)} = x_{n-1+ul(g)}^{n+ul(g)} + F(n + ul(g))$$

ir $x_n = x_{n-1}^n + F(n)$, naudodamiesi tuo, kad $g|(F(n + ul(g) - F(n))$, gauname, kad $x_{n+ul(g)-x_n}$ moduliu g lygus

$$r^{n+ul(g)} - r^n = r^n(r^{ul(g)} - 1)$$

moduliu g. Matome, kad tai lygu nuliui moduliu g, jei $r = 0$. Tarkime, kad $r > 0$. Užrašykime

$$r = r'p_1^{u_1} \dots p_k^{u_k}, \qquad g = g'p_1^{v_1} \dots p_k^{v_k},$$

kur $p_1, \dots, p_k$ yra pirminiai skaičiai, $u_1, \dots, u_k, v_1, \dots, v_k \geqslant 1$, $\gcd(r', g') = 1$ ir $\gcd(r'g', p_1p_2 \dots p_k) = 1$.

Kadangi $n \geqslant t \geqslant s > \log_2 g$, gauname, kad $p_i^{u_i n} \geqslant p_i^n \geqslant 2^n > g \geqslant p_i^{v_i}$. Gauname, kad skaičius r^n dalijasi iš $p_1^{u_1}, p_2^{u_2}, \dots, p_k^{u_k}$. Liko įrodyti, kad skaičius $r^{ul(g)} - 1$ dalijasi iš g'. Remiantis tuo, kad $\gcd(g', r) = 1$ ir Oilerio teorema, gauname, kad $r^{\varphi(g')} - 1$ dalijasi iš g'. Kadangi $\varphi(g')$ dalija $l(g)$, gauname, kad $r^{ul(g)} - 1$ dalijasi iš g'. □

Sekančiame etape buvo išnagrinėtos sudėtingesnės sekos ir detaliau ištirtos kompiuterinio skaičiavimo galimybės. Buvo nagrinėjamos tokios rekurentinės sekos:

(1) $x_n \equiv x_{n-1}^{n^r} + 1 \pmod g$

(2) $x_n \equiv x_{n-1}^{n!} + 1 \pmod g$

(3) $x_n \equiv x_{n-1}^{r^n} + 1 \pmod g$

Šioms sekoms buvo suformuluoti toliau pateikti teiginiai.

TEOREMA 1.15. *Seka* $x_n \equiv x_{n-1}^{n^r} + 1 \pmod g$ *yra periodinė su periodu* $T \leqslant g\varphi(g)$ *ir priešperiodine dalimi* $t \leqslant [\sqrt[r]{\log_2(g)}] + 1 + g$.

TEOREMA 1.16. *Seka* $x_n \equiv x_{n-1}^{n!} + 1 \pmod g$ *yra periodinė su periodu* $T \leqslant 2$ *ir priešperiodine dalimi* $t \leqslant \varphi(g)$.

TEOREMA 1.17. *Seka* $x_n \equiv x_{n-1}^{r^n} + 1 \pmod g$ *yra periodinė su periodu* $T \leqslant g\varphi(\varphi(g))$ *ir priešperiodine dalimi* $t \leqslant [\log_2 \log_2(g)] + 1 + g\varphi(\varphi(g))$.

Remiantis šiais teiginiais buvo sukonstruotas ir vėliau patobulintas algoritmas, apskaičiuojantis periodo ir priešperiodinės dalies ilgius. Kaip ir anksčiau nagrinėtu atveju, gautieji duomenys pasižymi panašiomis savybėmis. Pavyzdžiui, pirminiams skaičiams reikia kur kas daugiau laiko norint apskaičiuoti periodą. Paprasto algoritmo sudėtingumą pavyko sumažinti iki polinominio vietoje eksponentinio, būdingo nuodugnios paieškos metodui. Gautieji rezultatai leido suformuluoti keletą svarbių apibendrinančių teiginių.

TEOREMA 1.18. *Tegul d yra natūralusis skaičius,*

$$F(z_0, \ldots, z_{d-1}) \in \mathbb{Z}[z_0, \ldots, z_{d-1}],$$

$f : \mathbb{N} \mapsto \mathbb{N}$ ir $h : \mathbb{Z} \mapsto \mathbb{Z}$. Tarkime, kad f ir h yra periodinės moduliu q kiekvienam $q \geqslant 2$, ir $\lim_{n\to\infty} f(n) = \infty$. Tegul $x_1, \ldots, x_d \in \mathbb{Z}$ ir

$$x_{n+1} = F(x_n, \ldots, x_{n-d+1})^{f(n)} + h(n),$$

kiekvienam $n = 1, 2, 3, \ldots$. Tuomet, su kiekvienu sveikuoju $g \geqslant 2$, seka

$$x_n \pmod{g},$$

$n = 1, 2, 3, \ldots$, yra periodinė.

Ši teorema apibrėžia reikalavimus funkcijoms $f(n)$ ir $h(n)$, tam, kad rekurentinė seka būtų periodinė.

IŠVADA 1.19. *Tegul $f : \mathbb{N} \mapsto \mathbb{N}$ ir $h : \mathbb{Z} \mapsto \mathbb{Z}$ yra dvi funkcijos, kurios yra periodinės moduliu q, kiekvienam sveikajam $q \geqslant 2$, ir $\lim_{n\to\infty} f(n) = \infty$. Tarkime, kad $x_1 \in \mathbb{N}$ ir*

$$x_{n+1} = x_n^{f(n)} + h(n),$$

kai $n = 1, 2, 3, \ldots$. Tuomet, kiekvienam sveikajam $g \geqslant 2$, seka $x_n \pmod{g}$, $n = 1, 2, 3, \ldots$, yra periodinė.

Pastaroji išvada apibendrina [27] straipsnyje suformuluotą pagrindinį rezultatą.

TEIGINYS 1.20. *Tegul $g \geqslant 3$ yra natūralusis skaičius, kuris nėra 2 laipsnis, ir $f : \mathbb{N} \mapsto \mathbb{N}$. Tarkime, kad $x_1 \in \mathbb{N}$ ir*

$$x_{n+1} = x_n^{f(n)} + 1,$$

kur $n = 1, 2, 3, \ldots$. Jei seka $x_n \pmod g$, $n = 1, 2, 3, \ldots$, yra periodinė, tuomet egzistuoja tokie natūralieji skaičiai q, n_0, t, kur $2 \leqslant q \leqslant g - 1$, kuriems seka $f(n_0 + ut) \pmod q$, $u = 0, 1, 2, \ldots$, yra pilnai periodinė.

Šis teiginys leidžia, priklausomai nuo g savybių, taip parinkti pradinius duomenis, kad funkcijos $f(n_0 + ut)$ generuojama seka būtų pilnai periodinė moduliu q.

APIBRĖŽIMAS 1.21. *Tegul $n \in \mathbb{N}$ ir seka $f(n) \pmod q$ - yra periodinė su periodu k. Jei $f(n_0) = f(n_0 + km)$, $m \in \mathbb{N}$, kur n_0 yra pirmasis sekos elementas, tuomet seka yra pilnai periodinė.*

Nesunku pastebėti, kad pilnai periodinės sekos yra:

- $f(n) = 1$, kur $n \in \mathbb{N}$. Ši seka bus sudaryta iš 1.
- $f(n) \equiv n \pmod g$, kur $n, g \in \mathbb{N}$ ir $g > 1$. Šią seką sudarys posekis $\ldots, 1, 2, \ldots, g - 1, 0, \ldots$.

LEMA 1.22. *Tegul $f : \mathbb{N} \mapsto \mathbb{N}$ yra nemažėjanti funkcija, tenkinanti sąlygą*

$$\lim_{n \to \infty} f(n) = \infty,$$

su savybe, kad kiekvienam $l \in \mathbb{N}$ egzistuoja sveikasis skaičius n_l toks, kad $f(n + l) - f(n) \leqslant 1$, su visais $n \geqslant n_l$. Tuomet neegzistuoja tokia aritmetinė progresija $au + b$, $u = 0, 1, 2, \ldots$, kur $a, b \in \mathbb{N}$ yra tokie, kad, fiksuotam $q \geqslant 2$, seka $f(au + b) \pmod q$, $u = 0, 1, 2, \ldots$, būtų periodinė.

Remiantis pastaraisiais teiginiais galima sukonstruoti daug neperiodinių sekų pavyzdžių. Nesunku pastebėti, kad funkcijos $f(n) = [\gamma \log n]$, $f(n) = [\alpha n^\sigma]$, kur $\alpha, \gamma > 0$ ir $0 < \sigma < 1$, tenkina lemos sąlygas. Tuomet, remiantis teiginiu, sekos

$x_1 \in \mathbb{N}$ ir

$$x_{n+1} = x_n^{[\gamma \log n]} + 1,$$

arba

$$x_{n+1} = x_n^{[\alpha n^\sigma]} + 1,$$

yra periodinės moduliu $g \in \mathbb{N}$, tada ir tiktai tada, kai $g = 2^s$, kur $s \geqslant 0$ yra fiksuotas sveikasis skaičius.

Pastaruoju metu daug dirbama tyrinėjant Sidono (Sidon) aibes (dar vadinamas sekomis) [55]. Abelio grupės (dažniausiai $\mathbb{Z}$) poaibiui $\mathcal{A}$ apibrėžkime

$$\mathcal{A}^*(k) := |\{(a_1, a_2) \in \mathcal{A} \times \mathcal{A} : a_1 + a_2 = k\}|$$

ir

$$\mathcal{A}^\circ(k) := |\{(a_1, a_2) \in \mathcal{A} \times \mathcal{A} : a_1 - a_2 = k\}|.$$

1932 metais S. Sidonas tyrinėjo sveikųjų skaičių sekas, kurioms $\mathcal{A}^*$ ir $\mathcal{A}^\circ$ buvo aprėžti. Nesunku įrodyti, kad $\mathcal{A}^*(k) \leqslant 2$ visiems k tada ir tiktai tada, kai $\mathcal{A}^\circ(k) \leqslant 1$ su visais $k \neq 0$. Kokio dydžio gali būti poaibis $\mathcal{A}$, kai $\mathcal{A}^*(k) \leqslant 2$? Sidonui uždavus šį klausimą tokio tipo aibės dabar vadinamos Sidono sekomis. Pavyzdžiui, seka $\{1, 2, 5, 7\}$ yra Sidono seka. Kitaip tariant, $\mathcal{A}$ yra Sidono seka, jei eilutės

$$\Big(\sum_{a \in \mathcal{A}} z^a\Big)^2$$

koeficientai ne didesni už 2. Toliau pateiksime apibendrintosios Sidono sekos (su parametrais h ir g) apibrėžimą, kai eilutės

$$\Big(\sum_{a \in \mathcal{A}} z^a\Big)^h$$

koeficientai yra aprėžti g. Pažymėkime z^k koeficientą $\mathcal{A}^{*h}(k)$. Šis skaičius parodo, kiek būdų yra užrašyti skaičių k, kaip h elementų iš aibės $\mathcal{A}$ (nebūtinai skirtingų) sumą. Pastebėsime, kad šis apibrėžimas teisingas ir tuo atveju, kai $\mathcal{A}$ yra bet kokios Abelio grupės poaibis.

$B_h^*[g]$ SEKOS APIBRĖŽIMAS. *Seka $\mathcal{A}$ yra vadinama $B_h^*[g]$ seka, jei $\left(\sum_{a\in\mathcal{A}} z^a\right)^h$ eilutės koeficientai yra aprėžti skaičiumi g. Jei $\mathcal{A}\subseteq G\neq\mathbb{Z}$, tuomet $\mathcal{A}$ vadinsime $B_h^*[G]$ seka. Kai G yra adityvioji sveikųjų skaičių moduliu n grupė, tuomet kalbėsime apie $B_h^*[g] \pmod n$ sekas. Taip pat, jei $\mathcal{A}$ yra $B_h^*[g]$ seka, šį sąryšį žymėsime $\mathcal{A}\in B_h^*[g]$.*

Taigi, Sidono sekos yra būtent $B_2^*[2]$ sekos. Priminsime, kad $\mathcal{A}^\circ$ yra aprėžtas 1 tada ir tiktai tada, kai $\mathcal{A}^*$ yra aprėžtas 2. Kai $\mathcal{A}^\circ(k)>1$, $k>0$, tuomet egzistuoja tokie $a_1,a_2,a_3,a_4\in\mathcal{A}$, kad $k=a_1-a_2=a_3-a_4$ ir daugiausiai du iš a_i yra lygūs. Tai reiškia, kad $a_4+a_1=a_1+a_4=a_2+a_3=a_3+a_2$, taigi, $\mathcal{A}^*(a_1+a_4)\geqslant 3$ (gali būti, kad $a_2=a_3$ arba $a_4=a_1$, bet ne abi lygybės kartu). Pastebėsime, kad, jei $\mathcal{A}=\{2^k,2^k+1:k\geqslant 1\}$, tuomet $\mathcal{A}^*(k)\leqslant 4$, visiems k, kai $\mathcal{A}^\circ(1)=\infty$; jei $\mathcal{A}=\{\pm 2^k:k\geqslant 1\}$, tuomet $\mathcal{A}^\circ(k)\leqslant 3$, su visais $k\neq 0$, bet $\mathcal{A}^*(0)=\infty$. Esmė ta, kad $B_2^*[2]$ sekos svarbios ne tik istoriškai, bet su jomis lengviau dirbti. Iš esmės yra daugiau žinoma apie Sidono sekas nei apie $B_h^*[g]$ sekas, kai $h>2$ ar $g>3$.

$B_h[g]$ SEKOS APIBRĖŽIMAS. *Seka $B_h^*[h!g]$ yra vadinama $B_h[g]$ seka. Jei $g=1$, tuomet kalbame tiesiog apie B_h sekas.*

Pastebėsime, kad daugelis autorių apibrėžia $B_h[g]$ seką kaip seką $B_h^*[h!(g+1)-1]$. Tuomet Sidono seka yra seka, kuriai $\mathcal{A}^{*h}(k)\leqslant 3$. Tokio žymėjimo priežastis ta, kad, jei $k=a_1+\cdots+a_h$ ir a_i yra skirtingi, tuomet egzistuoja $h!$ perstatų tam pačiam koeficientui $\mathcal{A}^{*h}(k)$.

Tam, kad paprasčiau būtų įsivaizduoti, kokios tai sekos, pateiksime kitą Sidono sekų apibrėžimą.

SIDONO SEKOS APIBRĖŽIMAS. *Sidono seka vadinama natūraliųjų skaičių seka $A=a_0,a_1,a_2,\ldots$, tokia, kad visos sumos $a_i+a_j, i\leqslant j$, yra skirtingos.*

Prieš kurį laiką Ju savo darbe [72] tyrinėjo dydį

$$\liminf_{k\to\infty}\deg(P_k)H(P_k^2)/P_k^2(1),$$

kur $P_k, k = 1, 2, \ldots,$ yra Niumano polinomų seka, tenkinanti $\deg(P_1) < \deg(P_2) < \ldots$. Jis teigė, kad ši riba nemažesnė už 1, jei $P_k(1)/\deg(P_k) \to 0$, kai $k \to \infty$. Šis tvirtinimas, jei būtų įrodytas, suteiktų taip vadinamoms $B_2[g]$ aibėms, kurios apibendrina klasikines Sidono sekas $B_2[1]$, griežtą įvertį. Priminsime, kad Niumano polinomais vadinami tokie polinomai, kurių koeficientai priklauso aibei $\{0, 1\}$.

Dubickas [28] įrodė, kad pakanka nagrinėti dydį

$$Q_2(P) = (\deg(P) + 1)H(P^2)/P(1)^2,$$

nes visada egzistuoja Niumano polinomų seka $P_k, k = 1, 2, ...,$ su didėjančiais laipsniais, tokia, kad

$$\liminf_{k\to\infty} Q_2(P_k) = Q_2(P).$$

Taip pat buvo pateikti šio dydžio apskaičiavimai Niumano polinomams iki 20 laipsnio imtinai.

Paskutiniojo mano darbo tikslas buvo pamėginti sukurti pakankamai efektyvų algoritmą minėtam dydžiui apskaičiuoti. Taip pat patikrinti VU MIF superkompiuterio **SGI Altix 4700** galimybes. Pagrindinis darbo rezultatas yra suformuluotas žemiau pateiktoje teoremoje.

TEOREMA 2.3. *Visiems Niumano polinomams P, kuriems* $\deg P \leqslant 36$*, teisinga nelygybė*

$$Q_2(P) \geqslant Q_2(P_0) = 432/529 = 0.816635\ldots,$$

kur P_0 yra 35*-to laipsnio polinomas su koeficientais*

$$11011101011111111010100000110101111,$$

kur koeficientai pateikti didėjimo tvarka.

Pastebėsime, kad teoremoje pateiktas sprendinys nėra vienintelis. Jei koeficientus imtume mažėjimo tvarka, tuomet gautume kitą polinomą su tokiu pačiu Q_2.

Taip pat buvo atsakyta į Berenhauto (Berenhaut) ir Saidako (Saidak) [13] iškeltą klausimą. Jie klausė, ar tik tos polinomų šeimos, kurioms santykis $\frac{P(1)}{\deg P}$ yra toks pat, įgyja tą pačią Q_2 reikšmę. Kaip matome iš žemiau pateiktos lentelės, į klausimą atsakome neigiamai.

1 lentelė. $Q_2(P)$ reikšmės kai kuriems polinomams P

Q_2	$\deg P$	$\frac{P(1)}{\deg P}$
$\frac{8}{9}$	3, 7, 11, 15	1, $\frac{6}{7}$, $\frac{9}{11}$, $\frac{4}{5}$
$\frac{15}{16}$	4, 9	1, $\frac{8}{9}$
$\frac{21}{25}$	13, 27, 34	$\frac{10}{13}$, $\frac{20}{27}$, $\frac{25}{34}$
$\frac{5}{6}$	19, 26	$\frac{12}{19}$, $\frac{9}{13}$
$\frac{240}{289}$	23, 29	$\frac{17}{23}$, $\frac{17}{29}$

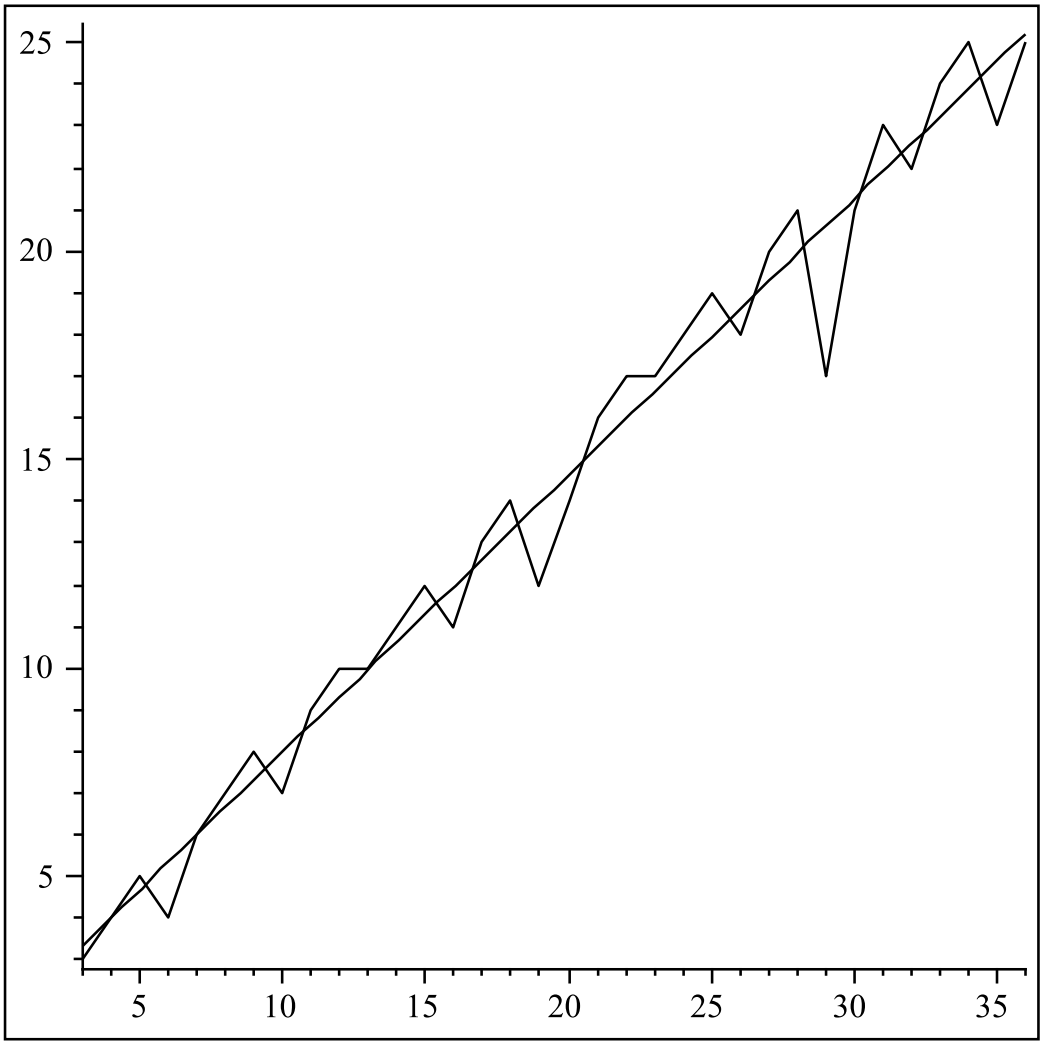
Nepaisant nemažų pastangų, efektyvaus algoritmo sukurti nepavyko. Vis dėlto, buvo aptikti tam tikri dėsningumai, kurie galėtų ženkliai sumažinti algoritmo laiko sąnaudas. Pavyzdžiui, buvo pastebėta, kad minėto dydžio $P(1)$ reikšmės pasižymi tiesinės regresijos savybėmis (žr. 1 pav.).

Tikėtina, kad nuo 23-čiojo laipsnio skaičiuojamojo minimumo reikšmės pasižymi periodiškumu. Jei ši hipotezė teisinga, tuomet, ieškant minimumo, pakaktų imti tik tuos polinomus, kuriems

$$\deg P = 2 \pmod 3.$$

Išvados. Darbe buvo pasiekti tokie rezultatai (žr. poskyrį "Tikslai ir uždaviniai"):

- Buvo iš esmės išnagrinėtos sekų periodiškumo sąlygos ir suformuluotos vienoje iš teoremų.
- Kai kurių sekų atveju nustatytas nulių sekoje egzistavimas.



1 pav. $P(1)$ reikšmės

- Kai kurių sekų atveju nustatyta priklausomybė tarp nulių egzistavimo ir pirmojo sekos elemento pasirinkimo.
- Sukonstruotas pakankamai efektyvus algoritmas nustatantis sekos periodiškumą tirtoms rekurenčiosioms sekoms.
- Atsakyta į Berenhauto ir Saidako [13] iškeltą klausimą.
- Sukonstruotas algoritmas apskaičiuoti $\inf_{P\in\mathbb{P}_n} Q_2(P)$ ir atrasti tam tikri dėsningumai, kurių pagalba būtų galima sukonstruoti geresnį algoritmą.

1. Rekurentinių sekų dalumo savybės

Šiame skyriuje nagrinėsime tokias rekurentines sekas:

(1) $x_n \equiv x_{n-1}^n + n - 1 \pmod{g}$

(2) $x_n \equiv x_{n-1}^{n^r} + 1 \pmod{g}$

(3) $x_n \equiv x_{n-1}^{n!} + 1 \pmod{g}$

(4) $x_n \equiv x_{n-1}^{r^n} + 1 \pmod{g}$

(5) $x_{n+1} \equiv F(x_n, \ldots, x_{n-d+1})^{f(n)} + h(n) \pmod{g}$

1.1. Rekurentinės sekos $x_n \equiv x_{n-1}^n + n - 1 \pmod{g}$ dalumo savybės.

Teiginys 1.1. *Tegul rekurentinis sąryšis yra $x_n \equiv x_{n-1}^n + n - 1 \pmod{g}$, čia $n, x_0 \in \mathbb{N}$. Jei $g = 2^m$, kur $m > 1$ ir $m \in \mathbb{N}$, tuomet sekoje yra be galo daug nulių, jei x_0 yra bet koks lyginis skaičius.*

Įrodymas. Tegul $n - 1 = gk$. Pastebėsime, kad x_{n-1} yra lyginis, ką įrodysime vėliau. Tuomet $x_n \equiv 0 \pmod{g}$, nes:

(1) $n - 1$ dalijasi iš g

(2) x_{n-1}^n dalijasi iš g, nes x_{n-1} lyginis

Panagrinėkime sekos sandarą.

Jei x_0 yra lyginis, tuomet x_1 - taip pat, $x_2 = x_1^1 + 1$ - nelyginis, kadangi sekantis sekos narys bus generuojamas iš nelyginio skaičiaus ir pridedamas lyginis, tai x_3 bus nelyginis. Nuo x_4 ciklas kartojasi. Taigi, galima išskirti periodą - 4-o kartotinį. Kadangi $n - 1 = gk$ ir $g = 2^m$, tai $n - 1$ narys bus lyginis. □

Apibrėžimas 1.2. *Karmaiklo skaičiumi vadinamas sudėtinis skaičius $n \in \mathbb{N}$, kuris tenkina tapatybę $b^{n-1} \equiv 1 \pmod{n}$, su visais $b \in \mathbb{Z}$ tarpusavyje pirminiais su n.*

TEOREMA (KORSELTO [73]). *Sudėtinis skaičius $n \in \mathbb{N}$ yra Karmaiklo skaičius tada ir tiktai tada, kai n yra bekvadratis ir visiems skaičiaus n pirminiams dalikliams p teisingas sąryšis $(p-1)|(n-1)$.*

TEIGINYS 1.3. *Jeigu g yra Karmaiklo skaičius, tuomet seka turi be galo daug nulių.*

Įrodymas. Tegul $n = g(g-1)k$, kur $k \in \mathbb{N}$. Tvirtiname, kad arba x_{n-1}, arba x_n dalijasi iš g. Jei x_{n-1} nesidalija iš g, tuomet, remiantis Mažąja Ferma teorema $x_{n-1}^n = x_{n-1}^{g(g-1)k} \equiv 1 \pmod{g}$. Todėl $x_n = (x_{n-1}^n - 1) + g(g-1)k$ dalijasi iš g. □

APIBRĖŽIMAS 1.4. *Seką $x_1, x_2, x_3, ...$ vadinsime periodine, jei egzistuoja toks $t \in \mathbb{N}$ ir $N \in \mathbb{N}$, kad $x_n = x_{n+t}$, su visais $n > N$. Skaičius t vadinamas šios sekos periodu.*

TEIGINYS 1.5. *Tegul rekurentinis sąryšis yra $x_n \equiv (x_{n-1}^n + n - 1) \pmod{g}$, čia $n, x_0 \in \mathbb{N}$. Jei g yra pirminis ir $g > 2$, tuomet sekos periodas yra $g(g-1)$. Kai $g = 2$, sekos periodas yra 4.*

Įrodymas. Pasinaudosime matematinės indukcijos metodu. Tegul $k, l \in \mathbb{N}$ tokie, kad

$$x_{g(g-1)k+(l-1)} = x_{g(g-1)(k+1)+(l-1)}.$$

Tuomet reikia įrodyti, kad

$$x_{g(g-1)k+l} = x_{g(g-1)(k+1)+l}.$$

Pagal sekos apibrėžimą

$$x_{g(g-1)k+l} \equiv x_{g(g-1)k+(l-1)}^{g(g-1)k+l} + g(g-1)k + (l-1) \pmod{g},$$

$$x_{g(g-1)(k+1)+l} \equiv x_{g(g-1)(k+1)+(l-1)}^{g(g-1)(k+1)+l} + g(g-1)(k+1) + (l-1) \pmod{g}.$$

Sulyginame dešiniąsias puses ir sutvarkome. Lieka įsitikinti, kad

$$x_{g(g-1)k+(l-1)}^{g(g-1)k+l} \equiv x_{g(g-1)(k+1)+(l-1)}^{g(g-1)(k+1)+l} \pmod{g}.$$

Jei $x_{g(g-1)k+(l-1)} = 0$, tuomet įrodymas baigtas. Priešingu atveju, pasinaudojus skaičiavimo moduliu savybėmis, gauname, kad

$$x^{g(g-1)k+l}_{g(g-1)k+(l-1)} \equiv (x^{g(g-1)k+l}_{g(g-1)(k+1)+(l-1)} \pmod g)(x^{g(g-1)}_{g(g-1)(k+1)+(l-1)} \pmod g).$$

Remiantis Mažąja Ferma teorema $x^{g(g-1)}_{g(g-1)(k+1)+(l-1)} \equiv 1 \ (mod\ g)$.

Kai $g = 2$, tereikia apskaičiuoti seką. Gausime ketverto periodą $...0, 0, 1, 1, ...$

□

PASTABA 1.6. *Šis periodas nebūtinai yra mažiausias. Pavyzdžiui, kai* $g = 3$*, periodas bus* 6*, bet mažiausias periodas yra* 3*.*

TEIGINYS 1.7. *Jei* $g = 2^m$*,* $m > 1$*, tuomet seka yra periodinė, su periodu* g*.*

Įrodymas. Pasinaudosime matematinės indukcijos metodu. Tegul $k, l \in \mathbb{N}$ tokie, kad

$$x_{gk+(l-1)} = x_{g(k+1)+(l-1)}.$$

Tuomet reikia įrodyti, kad

$$x_{gk+l} = x_{g(k+1)+l}.$$

Pagal sekos apibrėžimą

$$x_{gk+l} \equiv x^{gk+l}_{gk+(l-1)} + gk + (l-1) \pmod g,$$

$$x_{g(k+1)+l} \equiv x^{g(k+1)+l}_{g(k+1)+(l-1)} + g(k+1) + (l-1) \pmod g.$$

Sulyginame dešiniąsias puses ir sutvarkome. Lieka įsitikinti, kad

$$x^{gk+l}_{gk+(l-1)} \equiv x^{g(k+1)+l}_{g(k+1)+(l-1)} \pmod g.$$

Jei $x_{gk+(l-1)} = 0$, tuomet įrodymas baigtas. Priešingu atveju, pasinaudojus skaičiavimo moduliu savybėmis, gauname, kad

$$x^{gk+l}_{gk+(l-1)} \equiv (x^{gk+l}_{g(k+1)+(l-1)} \pmod g)(x^{g}_{g(k+1)+(l-1)} \pmod g).$$

Remiantis teiginio įrodymu apie nulių egzistavimą, kai $g = 2^m$, pastebėsime, kad $x_{g(k+1)+(l-1)}$ yra nelyginis. Tokiu atveju jį galime pakeisti išraiška $2k + 1$. Belieka

įsitikinti, kad $(2k+1)^g \equiv 1 \pmod{g}$. Pakeitus kairiąją pusę binomine išraiška gauname, kad g dalija eilutės koeficientus 2^g ir $\binom{g}{g-j}$, kur $j = 1, ..., g-1$. □

TEIGINYS 1.8. *Tarkime, kad g yra Karmaiklo skaičius. Tada seka yra periodinė, su periodu $g(g-1)$.*

Įrodymas. Pasinaudosime matematinės indukcijos metodu. Tegul $k, l \in \mathbb{N}$ tokie, kad

$$x_{g(g-1)k+(l-1)} = x_{g(g-1)(k+1)+(l-1)}.$$

Tuomet reikia įrodyti, kad

$$x_{g(g-1)k+l} = x_{g(g-1)(k+1)+l}.$$

Pagal sekos apibrėžimą

$$x_{g(g-1)k+l} \equiv x^{g(g-1)k+l}_{g(g-1)k+(l-1)} + g(g-1)k + (l-1) \pmod{g},$$

$$x_{g(g-1)(k+1)+l} \equiv x^{g(g-1)(k+1)+l}_{g(g-1)(k+1)+(l-1)} + g(g-1)(k+1) + (l-1) \pmod{g}$$

Sulyginame dešiniąsias puses ir sutvarkome. Lieka įsitikinti, kad

$$x^{g(g-1)k+l}_{g(g-1)k+(l-1)} \equiv x^{g(g-1)(k+1)+l}_{g(g-1)(k+1)+(l-1)} \pmod{g}.$$

Jei $x_{g(g-1)k+(l-1)} = 0$, tuomet įrodymas baigtas. Priešingu atveju, pasinaudojus skaičiavimo moduliu savybėmis, gauname, kad

$$x^{g(g-1)k+l}_{g(g-1)k+(l-1)} \equiv (x^{g(g-1)k+l}_{g(g-1)(k+1)+(l-1)} \pmod{g})(x^{g(g-1)}_{g(g-1)(k+1)+(l-1)} \pmod{g}).$$

Remiantis Mažąja Ferma teorema $x^{g(g-1)}_{g(g-1)(k+1)+(l-1)} \equiv 1 \pmod{g}$. □

Kompiuteriniai skaičiavimai

Skaičiavimų duomenys buvo gauti nagrinėjant įvairias skaičių grupes: pirminiai, dvejeto laipsniai ir t.t. Sekos iš tiesų yra periodinės, tačiau nulių skaičius priklauso nuo x_0 pasirinkimo. Suformuluosime hipotezę:

HIPOTEZĖ 1.9. *Tegul rekurentinis sąryšis yra* $x_n \equiv (x_{n-1}^n + n - 1) \pmod{g}$, *čia* $n, g \in \mathbb{N}$, $g > 1$. *Seka turi be galo daug nulių, kai* $x_0 = 2k$, $k = 0, 1, 2, ...$

Vis dėlto kai kurios grupės pasižymi įdomiomis savybėmis.

APIBRĖŽIMAS 1.10. *Fiksuokime* $g > 1$. *Tegul turime sekų grupę genruotą rekurentinio sąryšio moduliu* g *ir pradinių sekos narių aibės* $\{0, 1, \ldots, g-1\}$. *Tokią grupę vadinsime g-stabilia, jei, nuo tam tikro sekos eilės numerio* N, *sekos nariai nepriklauso nuo pradinio elemento* x_0.

PAVYZYDYS 1.11. *Tegul* $a_0 = 2$, $g = 5$. *Tada:*

x_0	x_1	x_2	x_3	x_4	x_5	x_6	x_7	x_8	x_9	x_{10}	x_{11}	x_{12}	x_{13}	x_{14}
0	1	3	4	3	4	0	2	0	4	4	2	4	4	3
1	2	0	3	2	4	0	2	0	4	4	2	4	4	3
2	0	2	4	3	4	0	2	0	4	4	2	4	4	3
3	0	2	4	3	4	0	2	0	4	4	2	4	4	3
4	2	0	3	2	4	0	2	0	4	4	2	4	4	3

APIBRĖŽIMAS 1.12. *P(g) - žymėsime funkciją, apibrėžiančią rekurentinės sekos periodą.*

HIPOTEZĖ 1.13. *Tegul rekurentinis sąryšis yra* $x_n \equiv (x_{n-1}^n + n - 1) \pmod{g}$, *čia* $n, g \in \mathbb{N}$, $g > 2$, $g = p^a$, $a = 0, 1, 2, ...$ *Tuomet seka turi be galo daug nulių.*

HIPOTEZĖ 1.14. *Tegul rekurentinis sąryšis yra* $x_n \equiv (x_{n-1}^n + n - 1) \pmod{g}$, *čia* $n, g \in \mathbb{N}$, $g > 2$, $g = p^a$, $a = 0, 1, 2, ...$ *Tuomet sekos periodas yra* $gP(p) = p^a(p-1)$.

Pastarosios dvi hipotezės glaudžiai susijusios tarpusavyje, kaip ir pirminių skaičių atveju. Griežto įrodymo nebuvo pateikta, bet tai galima iš dalies paaiškinti Oilerio teorema:

OILERIO TEOREMA. *Tegul* $\phi(n)$ *yra Oilerio funkcija, apibrėžianti natūraliųjų skaičių* $\leqslant n$ *ir tarpusavyje pirminių su n kiekį. Tuomet, su visais* $a \in \mathbb{N}$, *tokiais,*

kad $(a, n) = 1$ *galioja tokia lygybė:*

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

Algoritmas

Šio algoritmo pagalba apskaičiuoti duomenys pateikti lentelėse. Algoritmas yra paprastas, todėl skaičiavimo greitis tiesiogiai priklauso nuo periodo ilgio, tačiau atsižvelgiant į gautus rezultatus jis sukonstruotas taip, kad neveikia su skaičiais $2, 3$.

Algoritmas 1 Paprastas algoritmas

Įvedimas: Modulis g
Rezultatas: Periodas ir priešperiodinė dalis

```
restart;
g := readstat(‘Iveskite g(nepamirskite padeti kabliataskio!!! : ‘) :
x[0] := 2 :
A := [] :
for n from 1 to g*(g-1)*2+g*(g-1) do
  x[n] := ((x[n − 1])^n (mod g) + (n − 1) (mod g)) (mod g) :
  A := [op(A), x[n]] :
end for
k := 1 :
while k ⩽ g do
  i := 1 :
  while i ⩽ g do
    B := [] :
    C := [] :
    for j from i to i + g*k-1 do
      B := [op(B), A[j]] :
    end for
    for o from i+g*k to i+g*k*2-1 do
      C := [op(C), A[o]] :
    end for
    if B=C then
      lprint(‘Periodas : ‘, nops(B)/g, ‘ ∗ ‘, g, ‘Prasideda nuo : ‘, i) :
      k := g :
      i := g^2 :
      break :
    else
      i := i + 1 :
    end if:
  end while
  k := k + 1 :
end while
```

Žemiau pateiksime sekos periodo ilgį, kai $1 < g \leqslant 91$ ir $x_0 = 2$. Kadangi periodas yra tiesinė g funkcija $f(g) = cg$, tai lentelėse pateisime tik koeficientą c.

2 lentelė. Rezultatai pirminiams skaičiams

Laipsniai	1	2	3	4	5	6
g						
2	2	1	1	1	1	1
3	1	1	1	1		
5	4	4				
7	6	6				
11	10	10				
13	12	12				
17	16					
19	18					
23	22					
29	28					
31	30					
37	36					
41	40					
43	42					
47	46					

3 lentelė. Rezultatai sudėtiniams skaičiams

Laipsniai	1	2	3	4	5	6
g						
6	2	1	1	1		
10	2	1	1			
12	1	1	1			
14	6					
15	4					
18	2					
20	1					
21	2					
22	10					
24	1					
26	6					
28	3					
30	2					
33	10					
34	8					
35	12					
38	18					
39	4					
40	1					
42	2					
44	5					
45	4					
46	22					
48	1					
50	2					
51	16					
55	4					
65	12					
77	30					
91	12					

1.2. **Rekurentinių sekų dalumo savybės.**

Sekantis etapas buvo išnagrinėti sudėtingesnes sekas ir detaliau ištirti kompiuterinio skaičiavimo galimybes. Šiame poskyryje nagrinėsime tokias rekurentines sekas:

(1) $x_n \equiv x_{n-1}^{n^r} + 1 \pmod{g}$

(2) $x_n \equiv x_{n-1}^{n!} + 1 \pmod{g}$

(3) $x_n \equiv x_{n-1}^{r^n} + 1 \pmod{g}$

TEOREMA 1.15. *Seka* $x_n \equiv x_{n-1}^{n^r} + 1 \pmod{g}$ *yra periodinė su periodu* $T \leqslant g\varphi(g)$ *ir priešperiodine dalimi* $t \leqslant [\sqrt[r]{\log_2(g)}] + 1 + g$.

TEOREMA 1.16. *Seka* $x_n \equiv x_{n-1}^{n!} + 1 \pmod{g}$ *yra periodinė su periodu* $T \leqslant 2$ *ir priešperiodine dalimi* $t \leqslant \varphi(g)$.

TEOREMA 1.17. *Seka* $x_n \equiv x_{n-1}^{r^n} + 1 \pmod{g}$ *yra periodinė su periodu* $T \leqslant g\varphi(\varphi(g))$ *ir priešperiodine dalimi* $t \leqslant [\log_2 \log_2(g)] + 1 + g\varphi(\varphi(g))$.

Įrodymai

Oilerio teorema tvirtina, kad $a^{\phi(g)} \equiv 1 \pmod{g}$, jei a ir g yra tarpusavyje pirminiai. Galime iš karto atmesti prielaidą, kad a ir g yra tarpusavyje pirminiai, teigdami, kad, jei $u := u(g)$ yra didžiausias rodiklis, kuriam pirminis p egzistuoja skaičiaus g faktorizacijoje, tada $a^{\phi(g)+u} \equiv a^u \pmod{g}$), ir tai galioja su visais a nepriklausomai nuo to ar a ir g yra tarpusavyje pirminiai. Seka $(a^m)_{m \geqslant u}$ yra periodinė moduliu g su periodu $\phi(g)$. Tarkime, kad $(f(n))_{n \geqslant 1}$ yra didėjanti natūraliųjų skaičių seka, kuri yra periodinė moduliu $\phi(g)$ su periodu T_f. Tegul m_f yra natūralusis skaičius, toks, kad $f(m_f) \geqslant u$. Tuomet seka $(a^{f(n)})_{n \geqslant m_f}$ yra periodinė moduliu g su periodu T_f, nes, kai $m \geqslant m_f$, gauname, kad $f(m) \geqslant u$ ir

$$\varphi(g) \mid (f(m + T_f) - f(m)),$$

iš čia $a^{f(m)} \equiv a^{f(m+T_f)} \pmod{g}$. Nagrinėjamoms sekoms egzistuoja tokie $n > m \geqslant m_f$, kad galioja tapatybės $n \equiv m \pmod{T_f}$ ir $x_n \equiv x_m \pmod{g}$. Tegul a yra sekos reikšmė minėtiems m ir n, tuomet

$$x_{m+1} \equiv a^{f(m+1)} + 1 \pmod{g} \quad \text{ir} \quad x_{n+1} \equiv a^{f(n+1)} + 1 \pmod{g}.$$

Taigi, $x_{n+1} \equiv x_{m+1} \pmod{g}$. Remiantis indukcija gauname, kad

$$x_{n+k} \equiv x_{m+k} \pmod{g},$$

$k \geqslant 0$, su periodu $n - m$. Tiksliau, du tokie m ir n gali būti rasti intervale ilgio gT_f, t.y., $n - m \leqslant gT_f$.

Teoremos 1.15 įrodymas. Tegul $f(n)$ yra bet koks polinomas. Tuomet $T_f = \varphi(g)$, nes polinomams $f(n + m) \equiv f(n) \pmod{m}$ visiems natūraliesiems m ir n. Kai $f(n) = n^r$, gauname, kad $m_f = [\sqrt[r]{\log_2(g)}] + 1$, nes $u \leqslant \log_2(g)$. □

Teoremos 1.16 įrodymas. Tegul n yra pakankamai didelis, toks, kad $n! \geqslant g$. Tegul $x_n = ab$, kur visi pirminiai, dalijantys a, dalija g ir visi pirminiai, dalijantys b, yra tarpusavyje pirminiai su g. Tegul $g = g_1 g_2$, kur g_1 yra sudarytas iš pirminių a daliklių ir g_2 yra tarpusavyje pirminis su x_n. Tuomet $a^{n!} \equiv 0 \pmod{g_1}$, $b^{n!} \equiv 1 \pmod{g_2}$ ir $x_n^{n!} \equiv c \pmod{g}$, kur c, remiantis Kiniškąja likinių lema, yra vienintelė modulio g klasė, kuri lygi 0 moduliu g_1 ir 1 moduliu g_2. Todėl $x_{n+1} \equiv c + 1 \pmod{g}$ yra būtent minėtoji klasė, kuri lygi 1 moduliu g_1 ir 2 moduliu g_2. Iš pradžių tarkime, kad g_2 yra nelyginis. Tuomet x_{n+1} ir g yra tarpusavyje pirminiai. n pakeisdami $n + 1$ galime priskirti $a = 1, b = c + 1$, taigi, $x_{n+2} \equiv 2 \pmod{g}$. Jei g yra nelyginis, tuomet x_{n+2} ir g yra tarpusavyje pirminiai, todėl $x_{n+3} \equiv 2 \pmod{g}$ ir mes gauname $T = 1$. Tarkime, kad g_2 yra nelyginis, bet g – lyginis. Tuomet, pakeičiant n į $n + 2$, mes galime užrašyti $x_{n+2} \equiv ab \pmod{g}$, kur $a = 2$ ir $b \equiv 1 \pmod{g/2}$ yra klasė tarpusavyje pirminė su g. Pakeisdami n į $n + 2$, fiksuokime, kad g_1 yra 2 laipsnis dalijantis g ir $g_2 = g/g_1$. Pastebėsime, kad g_2 iš tiesų yra nelyginis. Tuomet gauname, kad x_{n+3} yra minėtoji klasė moduliu g, kuri lygi 1 moduliu g_1 ir 2 moduliu g_2, todėl $x_{n+4} \equiv 2 \pmod{g}$. Gauname, kad

šiu atveju $T = 2$. Pagaliau tarkime, kad g_2 yra lyginis. Tuomet g_1 yra nelyginis ir $x_{n+1} \equiv 2((c+1)/2) \pmod{g}$. Tegul $a = 2$ ir $b = (c+1)/2$ yra klasė tarpusavyje pirminė su g_1 (nes ji yra 2 atvirkštinė moduliu g_1) ir taip pat su g_2 (nes ji lygi 1 moduliu g_2). Tuomet b ir g yra tarpusavyje pirminiai. Dabar pakeiskime n į $n+1$, g_1 dvejeto laipsniu dalijančiu g ir $g_2 = g/g_1$. Pastebėsime, kad gavome ankstesnį atvejį, kai g buvo lyginis, bet g_2 buvo nelyginis, todėl periodo ilgis yra 2. □

Teoremos 1.17 įrodymas. Kai $f(n) = r^n$, tuomet $T_f = \varphi(\varphi(g))$, nes $r^{u_1+\varphi(g)} \equiv r^{u_1} \pmod{\phi(\phi(g))}$, kur u_1 yra didžiausias $\phi(g)$ faktorizacijos pirminiais daugikliais rodiklis, ir $m_f \geqslant \log_2(u)$. □

Algoritmas

Periodo ilgio apskaičiavimo algoritmo problema yra panaši į "Ciklo aptikimo algoritmo problemą" [74]. Vis dėlto, ji yra skirtinga, nes mes turime funkciją, kuri priklauso nuo kintamųjų $x_0, \ldots, x_{d-1}, n$. Taigi, algoritmai, tokie, kaip "Vėžlio ir kiškio" ar "Brento" [74], mums netiks. Pagrindinė problema yra ne rasti tokius $x_i = x_j$, bet du lygius poaibius. Galima nesunkiai parašyti "Jėgos" algoritmą, kuris patikrintų visas galimybes, bet skaičiavimai gali užimti labai daug laiko. Todėl mums reikia algotimo, kuris atliktų paskaičiavimus per pakankamai trumpą laiko tarpą.

Iš [27] galime rasti bendrą įvertį periodui ir priešperiodinei daliai.

$$T \leqslant g^{d+1} M,$$

$$t \leqslant g + [\log_2(g)] + 1,$$

kur M yra mažiausias bendras kartotinis skaičių $\{\phi(j) : j > 1, j|g\}$, ir d yra vektoriaus $(x_0, \ldots, x_{d-1})$ dimensija.

Algoritmas 2 Periodo ir priešperiodinės dalies apskaičiavimas

Įvedimas: rekurentinė funkcija $f(x_n, ..., x_{n-d+1}, n)$ ir reikšmė d, modulis g ir reikšmės $x_0, ..., x_d$
Rezultatas: T ir t arba $KLAIDOS$ pranešimas

```
M ← lcm(φ(D_m))
T_e ← g^{d+1} * M
t_e ← g + [log_2 g] + 1
N ← 2 * T_e + t_e
seka X
i ← 0
b ← true
Z ← {}
while b = true do
  if x_{N-i} = x_{N-T_e-i} AND i < Te then
    i ← i + 1
  else if i = T_e then
    Z ⊂ X
    b ← false
  else if Te > 0 then
    Te ← Te − 1
    i ← 0
  else
    b ← false
  end if
end while
if Z <> {} then
  T ← rastiMazesniPerioda(Z)
  t ← rastiPriesperiodi()
  print T, t
else
  print KLAIDA
end if
```

Algoritme Te, te žymi T, t įverčius ir N yra sekos dydis. Pastebėsime, kad, jei sekos ilgis lygus T_e, tuomet mažesnis periodas T (jei egzistuoja): $T|T_e$. Remdamiesi aukščiau minėtu faktu mes parašysime algoritmą mažesnio periodo paieškai.

Dabar pateiksime patobulintą algoritmo versiją, bet prieš tai pateiksime keletą pastebėjimų:

- Remiantis minėtų šaltinių teoremomis $M = \varphi(g)$ pirmaisiais dviem atvejais ir $M = \varphi(\varphi(g))$ trečiuoju.

Algoritmas 3 $rastiMazesniPerioda(Z)$

if Z sudaro vienas elementas **then**
  $T \leftarrow 1$
else
  $T \leftarrow Te$
  for all j tokiems, kad $1 < j < T_e$ ir $j|Te$ downto 1 **do**
    ieskome mažesnio periodo Z'
    if RASTA **then**
      if Z' sudaro vienas elementas **then**
        BAIGTI
      else
        $T \leftarrow |Z'|$
      end if
    end if
  end for
end if

Algoritmas 4 $rastiPriesperiodi()$

$N \leftarrow te + 2 * T$
$i \leftarrow 0$
while $i < te + T + 1$ and $x[N - i] = x[N - T - i]$ **do**
  $i \leftarrow i + 1$
end while

- Remiantis realiais paskaičiavimais $Te \leqslant 2g^d M$.
- Pastebėsime, kad tikrajam periodui T arba $T|M$, arba $M|T$, todėl pakanka ieškoti mažesnio periodo, tokio, kad $j|M$ arba $M|j$.

Algoritmas 5 Patobulintas algoritmas

Įvedimas: rekurentinė funkcija $f(x_n, ..., x_{n-d+1}, n)$, M įvertis, reikšmė d, modulis g ir reikšmės $x_0, ..., x_d$
Rezultatas: T ir t arba $KLAIDOS$ pranešimas

```
M ← H(g)
T_e ← 2 * g^d * M
t_e ← g + [log_2 g] + 1
N ← 2 * T_e + t_e
seka X
i ← 0
b ← true
while b = true do
  if x_{N-i} = x_{N-Te-i} AND i < Te then
    i ← i + 1
  else if i = T_e then
    Z ⊂ X
    b ← false
  else if Te > 0 then
    Te ← Te − M
    i ← 0
  else
    b ← false
  end if
end while
if Z <> {} then
  patobulintasRastiMazesniPerioda(Z)
  rastiPriesperiodi()
  print T, t
else
  print KLAIDA
end if
```

Algoritmas 6 *improvedFindSmallerPeriod*(Z)

if Z consists from one element **then**
  $T \leftarrow 1$
else
  $T \leftarrow Te$
  for all j such that $j|T_e$ and $j < T_e$ and $(j|M$ or $M|j)$ from biggest j **do**
    check for smaller period Z'
    if FOUND **then**
      if Z' consists from one element **then**
        STOP
      else
        $T \leftarrow |Z'|$
      end if
    end if
  end for
end if

Dabar įvertinsime algoritmo sudėtingumą ir laiko sąnaudas.

- Norint apskaičiuoti reikiamų sekos elementų kiekį reikia N operacijų. Maple turi pakankamai išvystytą algoritmą modulio skaičiavimui. Pakanka 0.03 sekundės norint apskaičiuoti $1000545^{6265461} + 65465 \pmod{564654}$, todėl tarkime, kad sekos apskaičiavimui pakaks N operacijų.
- While ciklui blogiausiu atveju reikės $Te * 2g^d$ operacijų, o vidutiniškai turėtų užtekti Te operacijų.
- Posekio suradimui reikės Te operacijų.
- Ieškant mažesnio periodo reikės $Te * \sqrt{Te}$ operacijų.
- Apskaičiuojant preišperiodinę dalį reikės $Te + te$ operacijų.

Dabar susumuosime visas operacijas. Galime įvertinti $M \leqslant \varphi(g) \leqslant g - 1$ blogiausiu atveju ir vertindami visą algortimą O žymėjimu, gauname:

- Blogiausiu atveju $O(g^{2d+1})$
- Vidutiniu atveju $O((g^{d+1})^{3/2})$

Algortimo kodas buvo parašytas su "Maple 9" ir skaičiavimai atlikti AK su Pentium(R) 4 CPU 2.00 GHz procesorium.

Rezultatai

Mūsų tikslas buvo rasti algoritmą, kurio skaičiavimo laikas būtų geresnis nei eksponentinis. Mums pavyko sukonstruoti pavyzdį su polinominėmis laiko sąnaudomis.

Grafikuose pilka linija pateikia lentelių duomenis, taškinė - vidutinį ir brūkšninė - blogiausią atvejus. Pastebėsime, kad grafikų trendai sutampa.

Remiantis gautais duomenimis, pastebėsime, kad laiko sąnaudos staigiai išauga pirminiams skaičiams, kai sudėtiniams skaičiams laiko sąnaudų augimas yra daug nuosaikesnis, ypač tada, kai $\varphi(g)$ yra labai mažas lyginant su g.

4 lentelė. Skaičiavimai lygčiai (1), kai $x_0 = 1$, $d = 1$, $r = 1$

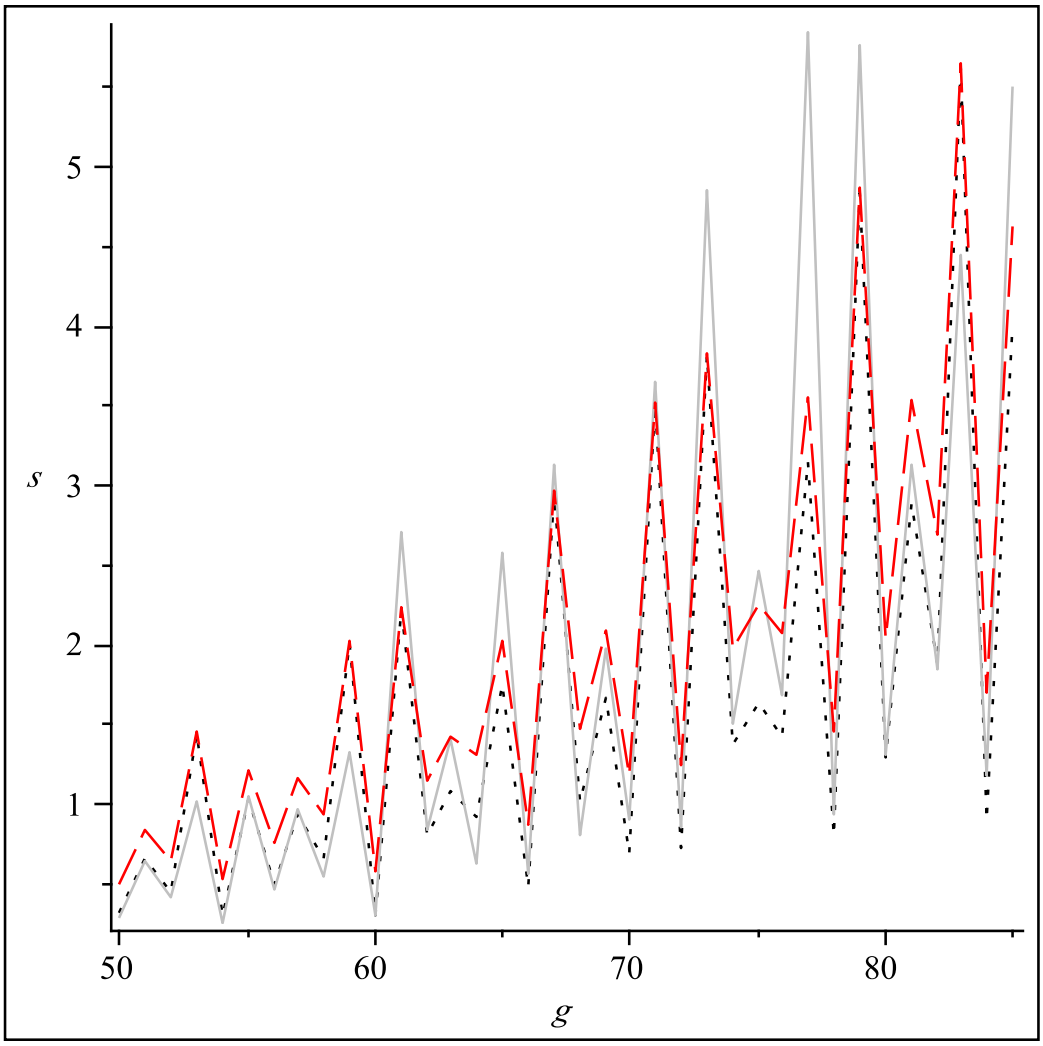
g	$\varphi(g)$	T	$\log_2 g$	t	s
50	20	20	5.643856	3	0.290000
51	32	16	5.672425	8	0.651000
52	24	12	5.700440	6	0.411000
53	52	52	5.727920	24	1.011000
54	18	36	5.754888	0	0.261000
55	40	20	5.781360	10	1.051000
56	24	6	5.807355	4	0.471000
57	36	36	5.832890	6	0.971000
58	28	28	5.857981	14	0.551000
59	58	58	5.882643	48	1.332000
60	16	4	5.906891	2	0.310000
61	60	60	5.930737	12	2.714000
62	30	30	5.954196	6	0.832000
63	36	12	5.977280	3	1.412000
64	32	2	6.000000	6	0.631000
65	48	12	6.022368	6	2.573000
66	20	20	6.044394	10	0.561000
67	66	66	6.066089	24	3.135000
68	32	16	6.087463	8	0.811000
69	44	44	6.108524	4	1.973000
70	24	12	6.129283	3	0.901000
71	70	70	6.149747	15	3.645000
72	24	12	6.169925	4	0.851000
73	72	72	6.189825	12	4.857000
74	36	36	6.209453	9	1.513000
75	40	20	6.228819	3	2.463000
76	36	18	6.247928	6	1.692000
77	60	30	6.266787	10	5.839000
78	24	12	6.285402	6	0.941000
79	78	78	6.303781	13	5.769000
80	32	4	6.321928	4	1.311000
81	54	108	6.339850	1	3.125000
82	40	40	6.357552	10	1.843000
83	82	82	6.375039	82	4.446000
84	24	12	6.392317	3	1.172000
85	64	16	6.409391	8	5.508000

5 lentelė. Skaičiavimai lygčiai (2), kai $x_0 = 1$, $d = 1$

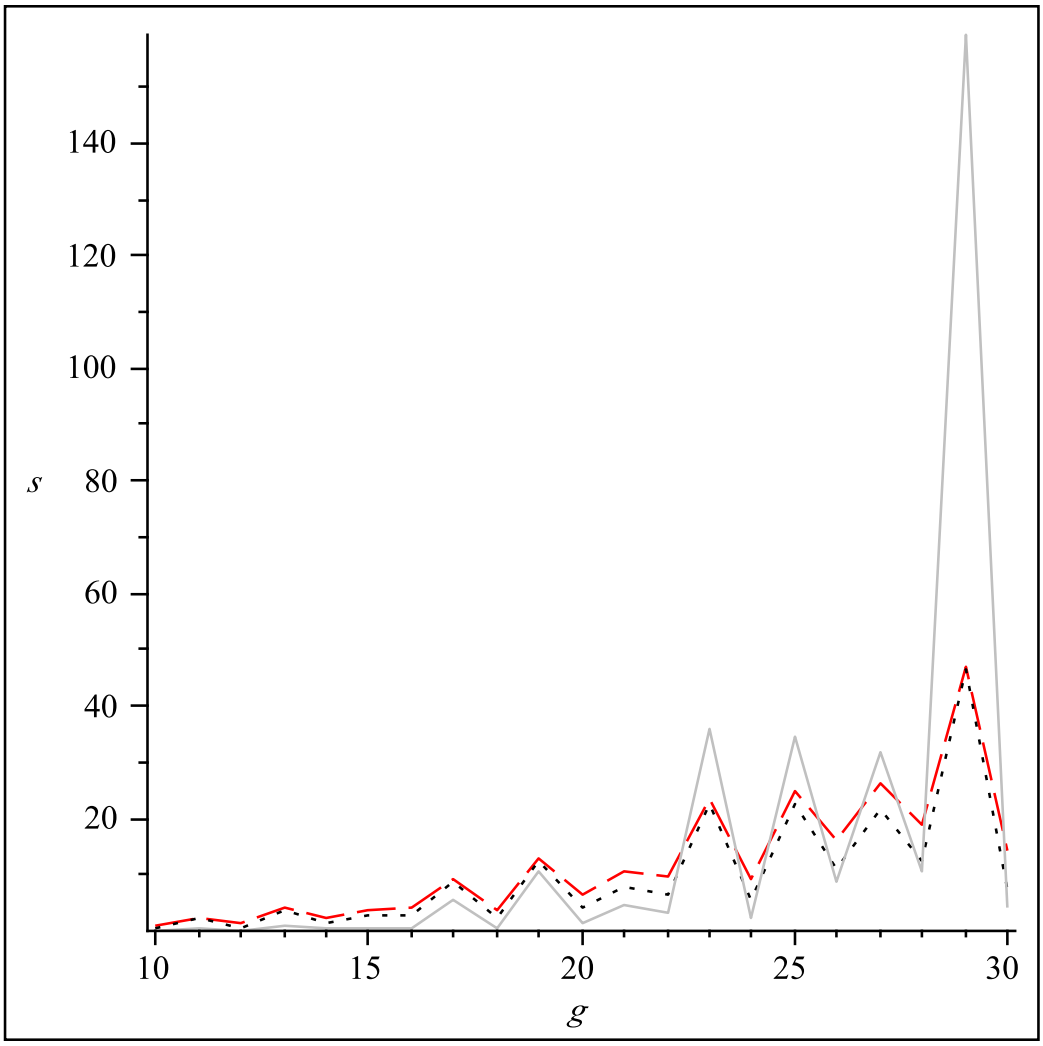
g	$\varphi(g)$	T	$\log_2 g$	t	s
10	4	2	3.321928	4	0.080000
11	10	1	3.459432	5	0.481000
12	4	2	3.584962	1	0.060000
13	12	1	3.700440	5	1.071000
14	6	2	3.807355	3	0.230000
15	8	1	3.906891	4	0.531000
16	8	2	4.000000	4	0.331000
17	16	1	4.087463	6	5.458000
18	6	2	4.169925	3	0.460000
19	18	1	4.247928	6	10.746000
20	8	2	4.321928	4	1.211000
21	12	1	4.392317	3	4.477000
22	10	2	4.459432	5	3.024000
23	22	1	4.523562	11	35.672000
24	8	2	4.584962	3	2.093000
25	20	1	4.643856	4	34.639000
26	12	2	4.700440	5	8.523000
27	18	1	4.754888	6	31.835000
28	12	2	4.807355	3	10.456000
29	28	1	4.857981	7	159.449000
30	8	2	4.906891	4	3.966000

6 lentelė. Skaičiavimai lygčiai (3), kai $x_0 = 1$, $d = 1$

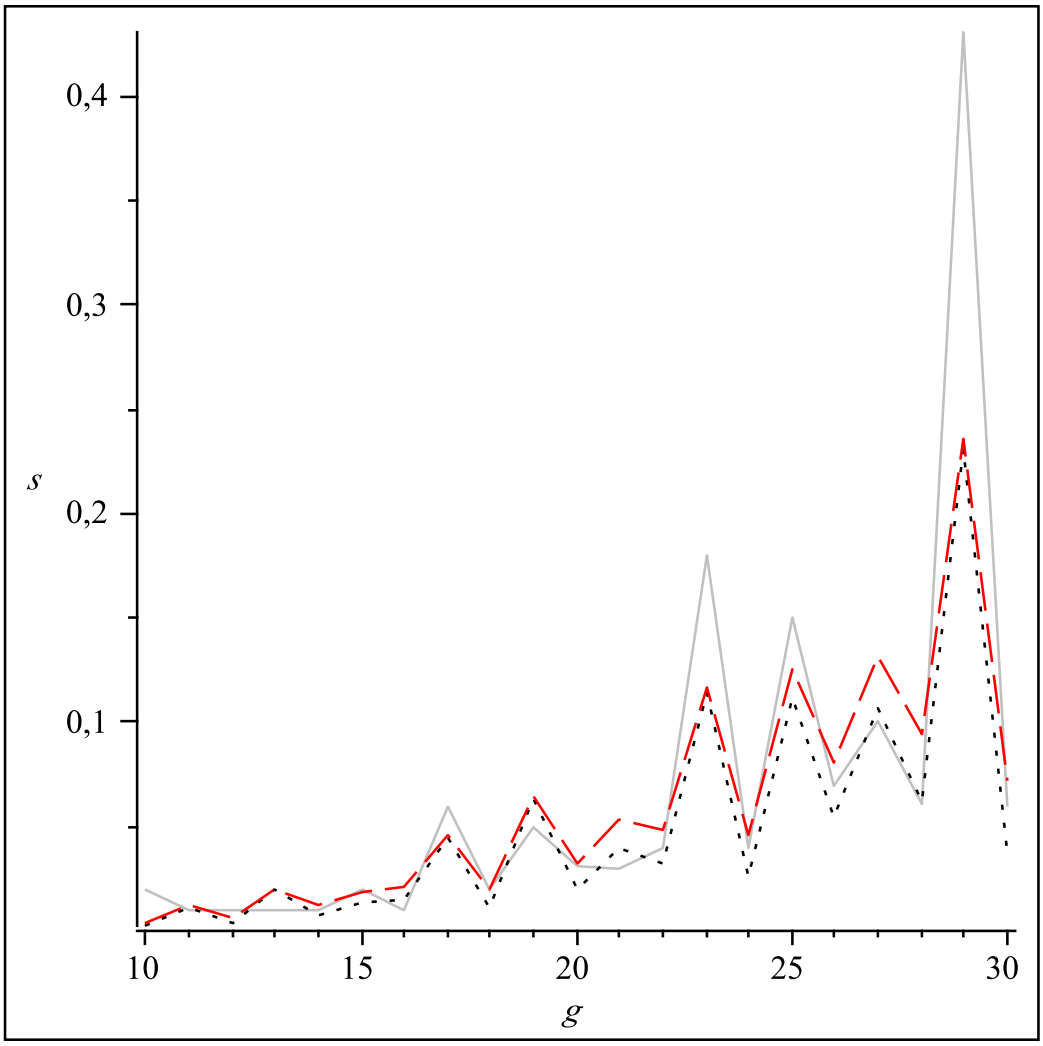
g	$\varphi(\varphi(g))$	T	$\log_2 g$	t	s
10	2	2	3.321928	1	0.020000
11	4	12	3.459432	1	0.010000
12	2	2	3.584962	1	0.010000
13	4	4	3.700440	2	0.010000
14	2	4	3.807355	2	0.010000
15	4	1	3.906891	1	0.020000
16	4	2	4.000000	0	0.010000
17	8	1	4.087463	4	0.060000
18	2	2	4.169925	1	0.020000
19	6	4	4.247928	12	0.050000
20	4	2	4.321928	1	0.031000
21	4	4	4.392317	2	0.030000
22	4	12	4.459432	1	0.040000
23	10	10	4.523562	15	0.180000
24	4	2	4.584962	1	0.040000
25	8	4	4.643856	1	0.150000
26	4	4	4.700440	2	0.070000
27	6	12	4.754888	1	0.100000
28	4	4	4.807355	2	0.061000
29	12	3	4.857981	6	0.430000
30	4	2	4.906891	1	0.060000



2 pav. Grafikas 4 lentelei



3 pav. Grafikas 5 lentelei



4 pav. Grafikas 5 lentelei

1.3. **Rekurentinių sekų dalumo savybės moduliu g.**

Šioje dalyje nagrinėsime sveikųjų skaičių sekas generuojamas rekurenčiojo sąryšio

$$x_{n+1} = F(x_n, x_{n-1}, \ldots, x_{n-d+1})^{f(n)} + h(n),$$

kur $F(z_0, z_1, \ldots, z_{d-1})$ yra d kintamųjų su sveikaisiais koeficientais polinomas, $f : \mathbb{N} \mapsto \mathbb{N}$ and $h : \mathbb{Z} \mapsto \mathbb{Z}$. Šio tipo sekų pavyzdžiai būtų

$$y_{n+1} = (y_n + 2y_{n-1}^3)^{n^2+2^n} + n, \quad n = 2, 3, 4, \ldots,$$

ir

$$u_{n+1} = u_n^{[n\sqrt{2}]} + 1, \quad n = 1, 2, 3, \ldots,$$

kur $y_1, y_2, u_1 \in \mathbb{Z}$.

Rezultatai leidžia tvirtinti, kad pirmoji seka $y_1, y_2, y_3, \ldots$ yra periodinė moduliu g kiekvienam sveikajam skaičiui $g \geqslant 2$, kai antroji seka $u_1, u_2, u_3, \ldots$ yra periodinė moduliu g, tada ir tiktai tada, kai g yra dvejeto laipsnis.

Turime dvi funkcijas $f : \mathbb{N} \mapsto \mathbb{N}$, $h : \mathbb{Z} \mapsto \mathbb{Z}$. Tegul x_n, $n = 1, 2, 3, \ldots$, yra sveikųjų skaičių seka apibrėžta taip: $x_1 \in \mathbb{Z}$ ir

$$x_{n+1} = x_n^{f(n)} + h(n),$$

su kiekvienu sveikuoju $n \geqslant 1$. Tegul $g \geqslant 2$ yra natūralusis skaičius. Mūsų tikslas yra ištirti funkcijas f ir h ir nustatyti, kokioms sąlygoms esant seka $x_n \pmod g$, $n = 1, 2, 3, \ldots$, yra periodinė. Ar egzistuoja tokios "paprastos" funkcijos f, h, kurioms ši seka nėra periodinė?

Toliau įrodysime, kad ši seka yra periodinė, kai funkcijos f ir h taip pat yra periodinės sekos kiekvienam moduliui $q \geqslant 2$. Toliau suformuluotoji teorema yra ankstesniųjų rezultatų apibendrinimas. Taip pat pateiksime atvirkščią rezultatą laikydami, kad neegzistuoja joks $f(n)$, $n = 1, 2, 3, \ldots$, posekis periodinis moduliu $q \geqslant 2$ ir sudarantis begalinę aritmetinę progresiją. Pabaigoje pateiksime keletą pavyzdžių.

TEOREMA 1.18. *Tegul d yra natūralusis skaičius,*

$$F(z_0, \dots, z_{d-1}) \in \mathbb{Z}[z_0, \dots, z_{d-1}],$$

$f : \mathbb{N} \mapsto \mathbb{N}$ *ir* $h : \mathbb{Z} \mapsto \mathbb{Z}$. *Tarkime, kad* f *ir* h *yra periodinės moduliu* q *su kiekvienu sveikuoju* $q \geqslant 2$, *ir* $\lim_{n\to\infty} f(n) = \infty$. *Tegul* $x_1, \dots, x_d \in \mathbb{Z}$ *ir*

$$x_{n+1} = F(x_n, \dots, x_{n-d+1})^{f(n)} + h(n),$$

kiekvienam $n = 1, 2, 3, \dots$. *Tuomet, su kiekvienu sveikuoju* $g \geqslant 2$, *seka*

$$x_n \pmod{g},$$

$n = 1, 2, 3, \dots$, *yra periodinė.*

Įrodymas. Tegul D_g yra g daliklių, didesnių už 1, aibė, įskaitant g. Mažiausią bendrą kartotinį skaičių $\{\varphi(j) \,:\, j \in D_g\}$, kur φ yra Oilerio funkcija, pažymėkime M.

Kadangi h yra periodinė moduliu g ir f yra periodinė moduliu M, egzistuoja $n_0, s, \ell \in \mathbb{N}$ tokie, kad $g|(h(n+s)-h(n))$ ir $M|(f(n+\ell)-f(n))$ visiems sveikiesiems $n \geqslant n_0$. Pažymėkime $l = s\ell$. Iš to seka, kad

$$g|(h(n+ul) - h(n)) \;\text{ ir }\; M|(f(n+ul) - f(n))$$

su visais $u \in \mathbb{N}$ ir $n \geqslant n_0$.

Tvirtiname, kad egzistuoja sveikasis $n_1 \geqslant n_0$ toks, kad $g|(a^{f(n+l)} - a^{f(n)})$ visiems $n \geqslant n_1$ ir $a \in \{0, 1, \dots, g-1\}$. Tuomet teorema įrodoma indukcijos būdu skaičiui n. Vektorių seka $(x_{n_1+kl}, \dots, x_{n_1+kl-d+1})$, $k = 0, 1, 2, \dots$, turi du lygius elementus moduliu g, nes egzistuoja tik g^d skirtingų vektorių. Atitinkamos polinomų

$F(x_{n_1+k_1l},\dots,x_{n_1+k_1l-d+1})$ ir $F(x_{n_1+k_2l},\dots,x_{n_1+k_2l-d+1})$ reikšmės yra taip pat lygios moduliu g. Pažymėkime

$$a \equiv F(x_{n_1+k_1l},\dots,x_{n_1+k_1l-d+1}) \pmod g \equiv$$
$$\equiv F(x_{n_1+k_2l},\dots,x_{n_1+k_2l-d+1}) \pmod g,$$

kur $k_1 > k_2 \geqslant 0$, $n = n_1 + k_2l$, $u = k_1 - k_2$. Atimant

$$x_{n+1} = F(x_n,\dots,x_{n-d+1})^{f(n)} + h(n)$$

iš

$$x_{n+ul+1} = F(x_{n+ul},\dots,x_{n+ul-d+1})^{f(n+ul)} + h(n+ul),$$

gauname, kad $x_{n+ul+1} - x_{n+1}$ moduliu g lygus $a^{f(n+ul)} - a^{f(n)}$ moduliu g, kuris lygus nuliui, remiantis ankstesniu tvirtinimu. Taigi,

$$x_{n+ul+1} \equiv x_{n+1} \pmod g,$$

todėl, remiantis indukcija skaičiui n, seka $x_n \pmod g$, $n = 1, 2, 3, \dots$, yra periodinė.

Norint įrodyti tvirtinimą, mums reikia įrodyti, kad g dalija

$$a^{f(n)}(a^{f(n+l)-f(n)} - 1).$$

Tai akivaizdu, kai $a = 0$ arba $a = 1$. Tarkime, kad $a \geqslant 2$. Jei $\mathrm{bmd}(a, g) > 1$ (bmd - bendrasis mažiausias daliklis), pažymime $a = a'p_1^{u_1}\dots p_k^{u_k}$ ir $g = g'p_1^{v_1}\dots p_k^{v_k}$, kur $p_1,\dots,p_k$ yra pirminiai skaičiai, $u_1,\dots,u_k, v_1,\dots,v_k \in \mathbb{N}$ ir $\mathrm{bmd}(a', g') = 1$. (Priešingu atveju, jeigu $\mathrm{bmd}(a, g) = 1$, imame $a' = a$ and $g' = g$.)

Neprarasdami bendrumo tarkime, kad $f(n + l) \geqslant f(n)$. Pasinaudoję tuo, kad $\lim_{n\to\infty} f(n) = \infty$, matome, kad $p_1^{v_1}\dots p_k^{v_k}$ dalija $a^{f(n)}$ visiems pakankamai dideliems n. Pavyzdžiui, kai $n \geqslant n_1 \geqslant n_0$. Tai įrodo tvirtinimą, kai $g' = 1$. Tarkime, kad $g' \geqslant 2$. Tada, remiantis Oilerio teorema, $g'|(a^{\varphi(g')} - 1)$, nes $\mathrm{mbk}(a, g') = 1$. Lieka įrodyti, kad $f(n+l)-f(n)$ dalijasi iš $\varphi(g')$. Priklausomai nuo M pasirinkimo $\varphi(g')|M$. Kadangi $M|(f(n+l)-f(n))$, iš to seka, kad $\varphi(g')$ dalija $f(n+l)-f(n)$.

Kai $f(n+l) < f(n)$, šio teiginio įrodymas yra toks pat, nes $a^{f(n)}(a^{f(n+l)-f(n)} - 1)$ galime užrašyti sekančiu pavidalu $a^{f(n+l)}(1 - a^{f(n)-f(n+l)})$. □

Pastebėsime, kad ši teorema yra teisinga esant silpnesnėms f ir h sąlygoms. Mums nereikia, kad jos būtų periodinės su kiekvienu moduliu $q \geqslant 2$. Pakanka, kad $h : \mathbb{Z} \mapsto \mathbb{Z}$ būtų periodinė moduliu g ir $f : \mathbb{N} \mapsto \mathbb{N}$ būtų periodinė moduliu M, kur M apibrėžtas įrodyme ir priklauso tik nuo g.

Sekanti išvada apibendrina [27] straipsnyje suformuluotą pagrindinį rezultatą:

IŠVADA 1.19. *Tegul $f : \mathbb{N} \mapsto \mathbb{N}$ ir $h : \mathbb{Z} \mapsto \mathbb{Z}$ yra dvi funkcijos, kurios yra periodinės moduliu q, su kiekvienu sveikuoju $q \geqslant 2$, ir $\lim_{n\to\infty} f(n) = \infty$. Tarkime, kad $x_1 \in \mathbb{N}$ ir*

$$x_{n+1} = x_n^{f(n)} + h(n),$$

kai $n = 1, 2, 3, \ldots$. Tuomet, su kiekvienu sveikuoju $g \geqslant 2$, seka $x_n \pmod g$, $n = 1, 2, 3, \ldots$, yra periodinė.

Taip pat pateiksime atvirkščią teiginį prieš tai suformulavę pilnai periodinės sekos apibrėžimą.

APIBRĖŽIMAS 1.21. *Tegul $n \in \mathbb{N}$ ir seka $f(n) \pmod q$ - yra periodinė su periodu k. Jei $f(n_0) = f(n_0 + km)$, $m \in \mathbb{N}$, kur n_0 yra pirmasis sekos elementas, tuomet seka yra visiškai periodinė.*

TEIGINYS 1.20. *Tegul $g \geqslant 3$ yra natūralusis skaičius, kuris nėra 2 laipsnis, ir $f : \mathbb{N} \mapsto \mathbb{N}$. Tarkime, kad $x_1 \in \mathbb{N}$ ir*

$$x_{n+1} = x_n^{f(n)} + 1,$$

kur $n = 1, 2, 3, \ldots$. Jei seka $x_n \pmod g$, $n = 1, 2, 3, \ldots$, yra periodinė, tuomet egzistuoja tokie natūralieji skaičiai q, n_0, t, kur $2 \leqslant q \leqslant g - 1$, kuriems seka $f(n_0 + ut) \pmod q$, $u = 0, 1, 2, \ldots$, yra pilnai periodinė.

Įrodymas. Kadangi g nėra 2 laipsnis, tai jis turi nelyginį pirminį daliklį, tarkime, p. Seka $x_n \pmod g$, $n = 1, 2, 3, \ldots$, yra periodinė, todėl seka $x_n \pmod p$, $n =$

$1, 2, 3, \ldots$, taip pat turi būti periodinė. Egzistuoja n_1 ir t tokie, kad $p|(x_{n+t} - x_n)$ visiems $n \geqslant n_1$. Fiksuokime kokį nors $n \geqslant n_1$, kuriam $a \equiv x_n \pmod{p} \notin \{0, 1\}$. Toks n egzistuoja, nes $p \geqslant 3$, taigi, kiekvienas sekos $x_n \pmod{p}$ nulis yra keičiamas 1, kuris vėliau yra keičiamas 2. Apibendrinant, $x_{n+ut} \equiv a \pmod{p}$ visiems natūraliesiems skaičiams u.

Atimdami $x_{n+1} = x_n^{f(n)} + 1$ iš $x_{n+ut+1} = x_{n+ut}^{f(n+ut)} + 1$ gausime, kad $p|(a^{f(n+ut)} - a^{f(n)})$. Kadangi $2 \leqslant a \leqslant p-1$ ir p yra pirminis skaičius, gauname, kad $\gcd(a, p) = 1$. Iš to seka, kad $p|(a^{|f(n+ut)-f(n)|} - 1)$. Tegul q yra mažiausias natūralusis skaičius, kuriam $p|(a^q - 1)$. Kadangi $a < p$, gauname, kad $2 \leqslant q \leqslant \varphi(p) = p - 1 \leqslant g - 1$. Be to, q dalija skirtumą $|f(n + ut) - f(n)|$ visiems natūraliesiems $u \geqslant 0$. Taigi, seka $f(n + ut) \pmod{q}$, $u = 0, 1, 2, \ldots$, yra pilnai periodinė. □

Sąlyga, kad g nėra 2 laipsnis, yra esminė. Bet kokia seka pavidalo $x_{n+1} = x_n^{f(n)} + 1$, kur $f : \mathbb{N} \mapsto \mathbb{N}$, yra pilnai periodinė moduliu 2. Jei $g = 2^s$, kur $s \geqslant 2$, galima pasirinkti bet kokią funkciją $f : \mathbb{N} \mapsto \mathbb{N}$, tenkinančią nelygybę $f(n) \geqslant s$, visiems pakankamai dideliems n. Lengva pastebėti, kad pradedant kokiu tai n_0, seka $x_n \pmod{2^s}$ įgyja pavidalą $1, 2, 1, 2, 1, 2, \ldots$, taigi, $x_n \pmod{2^s}$, $n = 1, 2, 3, \ldots$, yra periodinė.

Apibendrinant, rekurentinių sekų liekanų periodiškumo problema gali būti labai sudėtinga net "paprastoms" sekoms. Straipsnyje [7] autoriai tyrinėjo seką $x_{n+1} = -[\lambda x_n] - x_{n-1}$, $n = 1, 2, 3, \ldots$. Buvo padaryta prielaida, kad visiems $x_0, x_1 \in \mathbb{Z}$ ir $\lambda \in [2, 2]$ seka $x_n, n = 0, 1, 2, \ldots$ yra pilnai periodinė. Netrivialus atvejis, kai $\lambda \in (-2, 2)\backslash\{-1, 0, 1\}$. Jei $\lambda = 1/2$, seka įgyja pavidalą $x_0, x_1 \in \mathbb{Z}, x_{n+1} = -[x_n/2] - x_{n-1}$, kur $n = 1, 2, 3, \ldots$. Pastebėsime, kad $[x_n/2] = x_n/2$ lyginiams x_n ir $[x_n/2] = (x_n - 1)/2$ nelyginiams x_n. Taigi, seka $x_n, n = 0, 1, 2, \ldots$ yra pilnai periodinė tada ir tiktai tada, kai seka $x_n \pmod{2}, n = 0, 1, 2, \ldots$, yra periodinė. Vis dėlto, panašu, kad įrodyti sekos $x_n \pmod{2}, n = 0, 1, 2, \ldots$, periodiškumą yra labai sudėtinga.

Pavyzdžiai

Tegul $a, g \geqslant 2$ yra natūralieji skaičiai. Funkcijos $f(n) = a^n$, $f(n) = P(n)$, kur $P(z) \in \mathbb{Z}[z]$, $P(n) \geqslant 1$ visiems $n \geqslant 1$, $f(n) = n!$ ir jų tiesinės kombinacijos yra periodinės moduliu g. Taigi, remiantis teorema, seka $y_1, y_2 \in \mathbb{Z}$ ir $y_{n+1} = (y_n + 2y_{n-1}^3)^{n^2+2^n} + n$ visiems $n \geqslant 2$ yra periodinė moduliu g. Panašiai seka $x_1 \in \mathbb{Z}$ ir $x_{n+1} = x_n^{n^a} + 1$, kur $n \geqslant 1$, yra periodinė moduliu g. Tas pats galioja ir sekai $x_1 \in \mathbb{Z}$, $x_{n+1} = x_n^{a^n} + 1$, $n = 1, 2, 3, \ldots$.

Tegul $\alpha > 0$ ir $\beta \geqslant 0$ yra realieji skaičiai. Tarkime, kad skaičius α yra iracionalus. Nagrinėkime seką $x_1 \in \mathbb{Z}$,

$$x_{n+1} = x_n^{[\alpha n+\beta]} + 1,$$

$n = 1, 2, 3, \ldots$. Tvirtiname, kad ši seka nėra periodinė moduliu g, jei $g \neq 2^s$ su sveikaisiais skaičiais $s \geqslant 0$.

Tarkime, kad seka $x_n \pmod g$, $n = 1, 2, 3, \ldots$, yra periodinė. Remiantis teiginiu, egzistuoja natūralieji skaičiai q, n_0, t, kur $2 \leqslant q \leqslant g - 1$, tokie, kad seka $[\alpha(n_0 + ut) + \beta] \pmod q$, $u = 0, 1, 2, \ldots$, yra pilnai periodinė. Tarkime, kad periodo ilgis yra $\ell \geqslant 1$. Tuomet q dalija skirtumą

$$[\alpha(n_0 + ut + \ell t) + \beta] - [\alpha(n_0 + ut) + \beta].$$

Bet kuriems realiesiems skaičiams x, y, teisinga lygybė $[x + y] = [x] + [y]$, jei trupmeninių dalių suma $\{x\} + \{y\}$ yra mažesnė už 1 ir $[x + y] = [x] + [y] + 1$, jei $\{x\} + \{y\} \geqslant 1$. Pažymėję $x = \alpha(n_0 + ut) + \beta$ ir $y = \alpha\ell t$, gauname, kad

$$[\alpha(n_0 + ut + \ell t) + \beta] - [\alpha(n_0 + ut) + \beta] =$$

$$= \begin{cases} [\alpha\ell t], \text{ jei } \{\alpha(n_0 + ut) + \beta\} < 1 - \{\alpha\ell t\}, \\ [\alpha\ell t] + 1, \text{ jei } \{\alpha(n_0 + ut) + \beta\} \geqslant 1 - \{\alpha\ell t\}. \end{cases}$$

Remiantis Veilio kriterijumi, $\alpha t \notin \mathbb{Q}$, o seka $\{\alpha(n_0 + ut) + \beta\}$, $u = 0, 1, 2, \ldots$, yra tolygiai pasiskirsčiusi intervale $[0, 1]$ (ž.r. [69] arba 2.8 skyrių straipsnyje

[64]). Taigi, abi $u \in \mathbb{N}$ aibės, kurioms galioja pirmoji ir antroji alternatyvos, yra netuščios. Pažymėjus $N = [\alpha \ell t]$, gauname prieštarą: $q|N$ ir $q|(N+1)$.

Kadangi $\sqrt{2} \notin \mathbb{Q}$, tai leidžia numanyti, kad seka $u_{n+1} = u_n^{[n\sqrt{2}]} + 1$, $n = 1, 2, 3, \ldots$, kur $u_1 \in \mathbb{Z}$, nėra periodinė moduliu g, jei g nėra dvejeto laipsnis.

Remiantis toliau suformuluota lema galima sukonstruoti daugiau neperiodinių sekų pavyzdžių.

LEMA 1.22. *Tegul $f : \mathbb{N} \mapsto \mathbb{N}$ yra nemažėjanti funkcija, tenkinati sąlygą*

$$\lim_{n\to\infty} f(n) = \infty,$$

su savybe, kad kiekvienam $l \in \mathbb{N}$ egzistuoja sveikasis skaičius n_l toks, kad $f(n+l) - f(n) \leqslant 1$, su visais $n \geqslant n_l$. Tuomet neegzistuoja tokia aritmetinė progresija $au+b$, $u = 0, 1, 2, \ldots$, kur $a, b \in \mathbb{N}$ yra tokie, kad, fiksuotam $q \geqslant 2$, seka $f(au+b) \pmod q$, $u = 0, 1, 2, \ldots$, būtų periodinė.

Įrodymas. Tarkime, kad turime du natūraliuosius skaičius a, b ir $q \geqslant 2$ yra toks, kad seka $f(au+b) \pmod q$, $u = 0, 1, 2, \ldots$, yra periodinė. Tuomet egzistuoja $r, \ell \in \mathbb{N}$ tokie, kad q dalija skirtumą $f(a(u+\ell)+b) - f(au+b)$ visiems $u \geqslant r$. Pagal lemos sąlygą, egzistuoja sveikasis skaičius v toks, kad $d_u = f(au+b+a\ell) - f(au+b) \leqslant 1$ visiems $u \geqslant v$. Jei $d_v = 1$, tuomet q nedalija d_v. Gavome prieštarą, todėl $d_v = 0$.

Pastebėsime, kad

$$d_v + d_{v+\ell} + \cdots + d_{v+k\ell} = f(av+b+a(k+1)\ell) - f(av+b).$$

Tuomet $\lim_{n\to\infty} f(n) = \infty$ sąlygoja, kad $d_v + d_{v+\ell} + \cdots + d_{v+k\ell}$ artėja į begalybę, kai $k \to \infty$. Taigi, egzistuoja natūralusis skaičius t toks, kad $d_v = d_{v+\ell} = \cdots = d_{v+(t-1)\ell} = 0$ ir $d_{v+t\ell} = 1$. Kadangi q dalija d_u visiems $u \geqslant v$, tuomet jis turi dalinti ir sumą $d_v + d_{v+\ell} + \cdots + d_{v+(t-1)\ell} + d_{v+t\ell} = 1$. Gavome prieštarą. □

Nesunku pastebėti, kad funkcijos $f(n) = [\gamma \log n]$, $f(n) = [\alpha n^\sigma]$, kur $\alpha, \gamma > 0$ ir $0 < \sigma < 1$, tenkina lemos sąlygas. Tuomet, remiantis teiginiu ir pastaba, sekančia

jo įrodymą, sekos $x_1 \in \mathbb{Z}$ ir, visiems $n \geqslant 1$,

$$x_{n+1} = x_n^{[\gamma \log n]} + 1,$$

arba

$$x_{n+1} = x_n^{[\alpha n^\sigma]} + 1,$$

yra periodinės moduliu $g \in \mathbb{N}$, tada ir tiktai tada, kai $g = 2^s$, kur $s \geqslant 0$ yra fiksuotas sveikasis skaičius.

Panagrinėkime seką $x_1 = 0, x_{n+1} = x_n^n + 1$, kai $n = 1, 2, 3, \ldots$. Seka $x_n \pmod 3, n = 1, 2, 3, \ldots$, yra tokio pavidalo $0, 1, 2, 0, 1, 2, \ldots$, taigi, yra pilnai periodinė. Remiantis pagrindine lema iš straipsnio [7], riba $\zeta = \lim_{n\to\infty} x_n^{1/n!}$ egzistuoja ir tai yra transcendentinis skaičius. Dar daugiau, $[\zeta^{n!}] = x_n$, su visais $n \in \mathbb{N}$. Taigi, seka $[\zeta^{n!}], n = 1, 2, 3, \ldots$, turi be galo daug elementų pavidalo $3k_0, 3k_1 + 1$ ir $3k_2 + 2$, kur $k_0, k_1, k_2 \in \mathbb{N}$.

2. Kompiuteriniai skaičiavimai Niumano polinomams

Pžymėkime polinomo $P = a_0 + a_1 x + \cdots + a_n x^n$ atvirkštinį polinomą $P^* = a_n + a_{n-1}x + \cdots + a_0 x^n$. Tarsime, kad $P \in \mathbb{P}_n$ yra pats sau simetriškas, jei $P = P^*$.

Pastebėsime, kad atvirkštiniai polinomai yra simetriški aukščio funkcijos H atžvilgiu. Iš simetriškumo gauname sekančias išvadas.

Išvada 2.1. *Aibė $\mathbb{P}_n$ gali būti padalinta į tris nesikertančius poaibius: sau simetriškų polinomų, polinomų S ir jų atvirkštinių polinomų S'. Remiantis simetriškumu, pakanka nagrinėti tik du iš jų - sau simetriškus polinomus ir aibę S.*

Išvada 2.2. *Remiantis simteriškumu, pakanka nagrinėti Niumano polinomus su koeficientu $a_0 = 1$.*

Toliau suformuluosime pagrindinį rezultatą.

Teorema 2.3. *Visiems Niumano polinomams P, kuriems* $\deg P \leqslant 36$*, teisinga nelygybė*

$$Q_2(P) \geqslant Q_2(P_0) = 432/529 = 0.816635\ldots,$$

kur P_0 yra 35*-to laipsnio polinomas su koeficientais*

$$11011101011111111010100000110101111,$$

kur koeficientai pateikti didėjimo tvarka.

Pastebėsime, kad teoremoje pateiktas sprendinys nėra vienintelis. Jei koeficientus imtume mažėjimo tvarka, tuomet gautume kitą polinomą su tokiu pačiu Q_2.

Remiantis duomenimis, pateiktais lentelėse 8 ir 9, mes galime atsakyti į klausimą pateiktą [13]. Minėtame straipsnyje autoriai klausė ar tik tos polinomų šeimos, kurioms santykis $\frac{P(1)}{\deg P}$ yra toks pat, įgyja tą pačią Q_2 reikšmę? Kaip matome iš rezultatų, kai $Q_2 = 0.83045...$, egzistuoja bent du skirtingi Niumano polinomai

laipsnių 23 ir 29. Toliau pateiktoje lentelėje mes pateiksime tokius Q_2. Tai atsako į klausimą straipsnyje [13].

7 lentelė. $Q_2(P)$ reikšmės kai kuriems polinomams P

Q_2	$\deg P$	$\frac{P(1)}{\deg P}$
$\frac{8}{9}$	3, 7, 11, 15	1, $\frac{6}{7}$, $\frac{9}{11}$, $\frac{4}{5}$
$\frac{15}{16}$	4, 9	1, $\frac{8}{9}$
$\frac{21}{25}$	13, 27, 34	$\frac{10}{13}$, $\frac{20}{27}$, $\frac{25}{34}$
$\frac{5}{6}$	19, 26	$\frac{12}{19}$, $\frac{9}{13}$
$\frac{240}{289}$	23, 29	$\frac{17}{23}$, $\frac{17}{29}$

Toliau mes analizuosime gautuosius duomenis. Žemiau esančiose lentelėse 8 ir 9 yra pateikti skaičiavimų duomenys. Čia pateikti dydžiai $\min_P(Q_2)$ polinomų aibėms $\mathbb{P}_n$.

Kiek polinomų aibėje $\mathbb{P}_n$ įgyja reikšmę $\min_P(Q_2)$? Atsakymas nėra paprastas. Atrodo, kad šis skaičius turėtų priklausyti nuo laipsnio n, bet taip nėra. Šiek tiek pakeitus žemiau pateiktą algoritmą galima gauti visus tokius polinomus duotajam laipsniui n. Buvo rasti tokie polinomai nuo 2 iki 20 laipsnių. Rezultatai yra įdomūs. (Toliau bus kalbama būtent apie tokius polinomus).

8 lentelė. Skaičiavimai (AK)

Laipsnis	$\min(Q_2)$	P(1)	$H(P^2)$	Polinomo koeficientai: $a_0, a_1, ..., a_{Degree}$
3	0.888889	3	2	1011
4	0.9375	4	3	10111
5	0.96	5	4	101111
6	0.875	4	2	1010011
7	0.888889	6	4	10101111
8	0.918367	7	5	101011111
9	0.9375	8	6	1010111111
10	0.897959	7	4	10010110111
11	0.888889	9	6	101010111111
12	0.91	10	7	1010101111111
13	0.84	10	6	10111111000111
14	0.867769	11	7	101111111000111
15	0.888889	12	8	1010101011111111
16	0.842975	11	6	11000110010111111
17	0.852071	13	8	101111111100001111
18	0.872449	14	9	1011111111100001111
19	0.833333	12	6	11000101001100111111
20	0.857143	14	8	10100101010110111111
21	0.859375	16	10	1010111111111000011111
22	0.875433	17	11	10101111111111000011111

9 lentelė. Skaičiavimai (Superkompiuteris)

Laipsnis	$\min(Q_2)$	P(1)	$H(P^2)$	Polinomo koeficientai: $a_0, a_1, ..., a_{Degree}$
23	0.83045	17	10	10101111111110000011111
24	0.848765	18	11	101011111111110000011111
25	0.864266	19	12	1010111111111011000011111
26	0.833333	18	10	1011101111111100000100101111
27	0.84	20	12	10101111111111110000000111111
28	0.854875	21	13	101011111111111110000000111111
29	0.83045	17	8	10101011101110110000000011111
30	0.843537	21	12	101010111111111111000000000111111
31	0.846881	23	14	1010101111111111111000000001111111
32	0.818182	22	12	1110111011111111010000000110101111
33	0.826389	24	14	10101011111111111111000000001111111
34	0.84	25	15	101010111111111111111000000001111111
35	0.816635	23	12	110111010111111111010100000110101111
36	0.8288	25	14	1100111111011111111100000010001111111

Tokių polinomų kiekis linkęs didėti didėjant laipsniui, tačiau svyravimas yra labai didelis. Tai ypač matosi pirminiams skaičiams. 10 lentelėje pateikti duomenys tą parodo.

Kitas svarbus klausimas – ar tokie polinomai turi ką nors bendro? Remiantis gautais duomenimis – beveik nieko, nes duotajam laipsniui polinomai gali būti:

- visi pirminiai
- visi sudėtiniai
- ir pirminiai, ir sudėtiniai

10 lentelė. Polinomų kiekis

degree n	2	3	4	5	6	7	8	9	10	11	12	13	14	...	19
Solutions	1	2	2	4	2	6	4	16	14	18	14	2	2	...	2

Deja, ši savybė nepriklauso nuo laipsnio n savybių. Bendra yra tai, kad $P(1)$ minėtiems sprendiniams yra toks pat. $P(1)$ reikšmės sudaro tiesinę regresiją (ž.r. 5 pav.): $y = a + b\,x$. Pasinaudoję Maple paketu apskaičiavome koeficientus ir gavome tokią lygtį:

$$y = \frac{9003}{6545} + \frac{4336}{6545}\,x$$

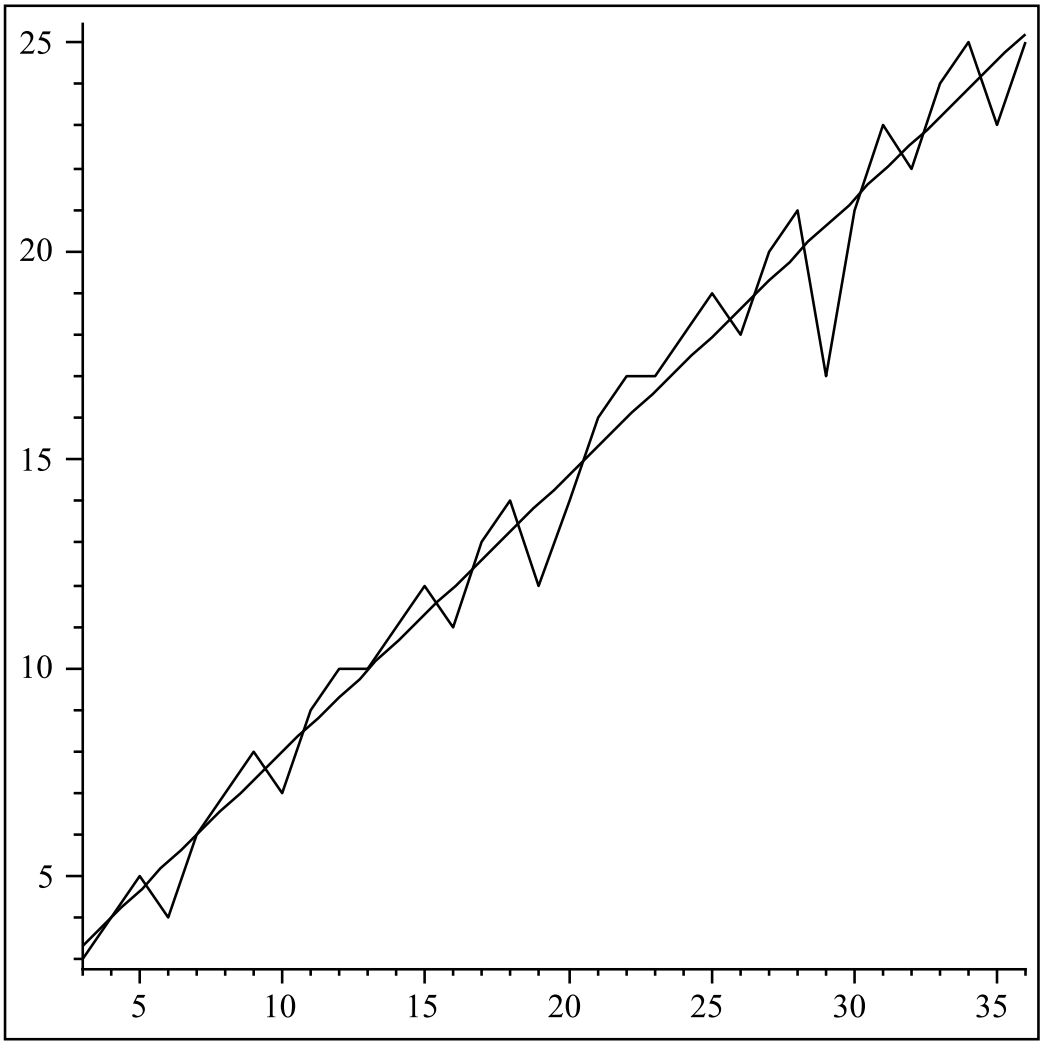
su dispersija $d = 3.458$. Apskaičiuoti koreliacijos koeficientai yra labai arti 1, kas parodo, kad tiesinis modelis tinka beveik idealiai. Lieka neatsakytas klausimas – ar dispersija teisinga, ar ji linkusi didėti didėjant laipsniui n?

Toliau ištirsime dydžio $\min_{P\in\mathbb{P}_n} Q_2(P)$ asimptotiką. Tam pasinaudosime regresine analize. Kaip matome iš 6 paveikslėlio, reikšmės mažėja pagal kažkokią tai funkciją. Buvo patikrinti keli dažniausiai naudojami netiesiniai modeliai:

- Logaritminis
- Laipsninis
- Asimptotinis

Paskutinysis pasirodė tinkamiausiu, nes kitų modelių riba artėja į begalybę arba nulį. Mūsų pasirinktas modelis yra toks:

$$a + be^{-cx}.$$

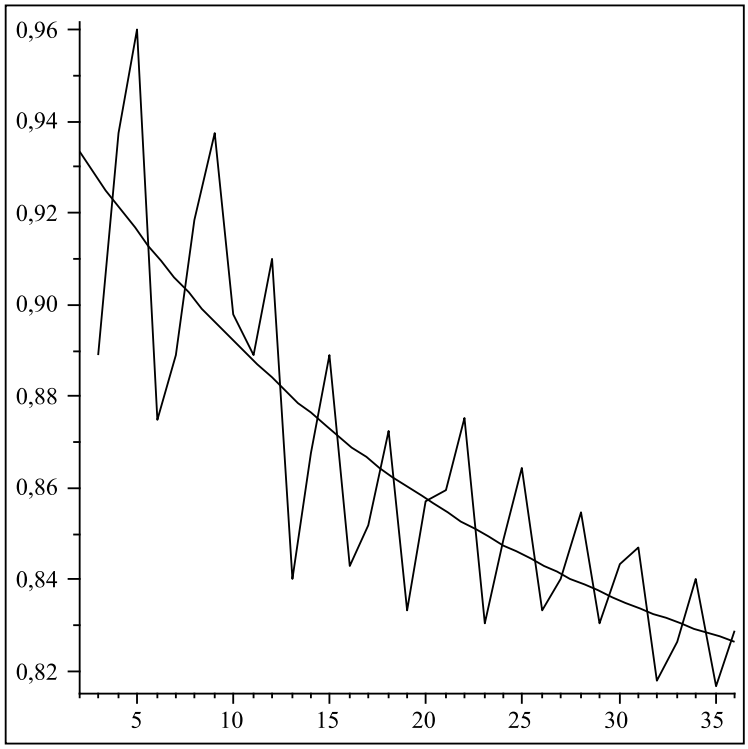


5 pav. $P(1)$ reikšmės

Pasinaudoję SPSS 16.0 statistiniu paketu apskaičiavome modelio koeficientus. Rezultatai pateikti 11 lentelėje.

11 lentelė. Modelio koeficientai

Parametras	Įvertis	Klaida	95% pasikliauties intervalas	
			Apatinis rėžis	Viršutinis rėžis
a	0.797	0.045	0.706	0.888
b	0.149	0.033	0.082	0.216
c	0.045	0.03	-0.016	0.105



6 pav. Q_2 grafikas

Galime apskaičiuoti apatinio rėžio įvertį, nes $\lim_{x\to\infty} a + be^{-cx} = a$ (ž.r. 6). Pastebėsime, kad ši riba yra labai arti $\pi/4$. Tiesą sakant, jei neužmiršime paklaidos, tuomet $\pi/4 \approx 0.785$ yra tinkamas būti apatiniu rėžiu. Straipsnyje [18] kaip tik ir buvo gautas šis apatinis rėžis tikimybiniais metodais. Taip pat pastebėsime, kad duomenys yra beveik periodiški su periodu $T = 3$. Tiksliau, nuo 23-čiojo laipsnio duomenys yra periodiniai su periodu $T = 3$. Jei tai tiesa, tuomet skaičiuojant minimumus pakanka imti ne visus Niumano polinomus, o tik tuos, kuriems

$$\deg P = 2 \pmod 3.$$

Toliau pateiksime pagrindinį algoritmą $Q(P)$ apskaičiavimui.

Pagrindinis algoritmas

Mums reikia apskaičiuoti $Q_2(P)$ visiems $P \in \mathbb{P}_n$. Tam mums reikia perbėgti visus polinomus ir papildomai apskaičiuoti du dydžius:

- polinomo aukštį $H(P^2)$
- polinomo ilgį $P(1)^2$

Prieš pateikiant algoritmą aptarsime, kaip bus aprašomas polinomas. Natūralu aprašyti polinomą naudojant jo koeficientus. Programavimo kalbose yra kelios patogios duomenų struktūros. Šiam tikslui pasinaudosime vektoriumi susiedami jo indeksus su polinomo koeficientų indeksais. Tegula A yra vektorius. Tuomet $A[0] = a_0$, $A[1] = a_1$, ... Prisiminus anksčiau pateiktas išvadas, pakanka atlikti esmines manipuliacijas su koeficientais $a_1, \ldots, a_{\deg P-1}$.

Algoritmas 7 Pagrindinis algoritmas

Įvedimas: deg(P)
Rezultatas: $min_{P\in\mathbb{P}}Q_2(P)$
  inicializavimas
  for $i \leftarrow 1$ to $2^{\deg(P-1)} - 1$ **do**
    padidinti vektorių 1
    sukurti $deg(P)$ laipsnio polinomą pridedant a_0 ir $a_{\deg P}$
    apskaičiuoti $H(P^2)$
    apskaičiuoti $P(1)$
    apskaičiuoti $Q(P)$
  end for

Vektoriaus didinimas gali būti realizuotas taikant sumą moduliu 2. Šios dalies sudėtingumas yra $\deg P$. Toliau apskaičiuosime P^2.

Algoritmas 8 Polinomo kvadratas

  for $i \leftarrow 0$ to $\deg P$ **do**
    for $j \leftarrow 0$ to $\deg P$ **do**
      apskaičiuojame naujo polinomo koeficientus $P^2[i+j] = P^2[i+j]+P[i]*P[j]$
    end for
  end for

Šios dalies sudėtingumas yra $(\deg(P))^2$, o $H(P^2)$ – $2\deg(P)$. Apskaičiuojant $P(1)$ sudėtingumas yra $\deg P$. Norint apskaičiuoti $Q(P)$ kokiam nors polinomui P, sudėtingumas yra $4\deg P + (\deg P)^2$. Visa tai duoda bendrą algoritmo sudėtingumą

$$(4n + n^2) * 2^{n-1},$$

norint rasti mažiausią $Q(P)$ visiems $P \in \mathbb{P}_n$. Pereinant prie labiau įprasto žymėjimo, tai būtų:

$$O(n^2 * 2^{n-1}).$$

Algoritmas buvo realizuotas C++ programavimo kalba ir vykdytas su asmeniniu kompiuteriu (2.4 GHz Intel Core 2 Duo) ir superkompiuteriu (SGI Altix 4700).

Kaip matome, algoritmas nėra labai greitas. Jei polinomo laipsnis padidėja 1, laiko sąnaudos, norint apskaičiuoti Q_2 visiems to laipsnio polinomams, dvigubėja. Reminatis išvadomis, laiko sąnaudas būtų galima sumažinti maždaug per pusę, bet tai nekeičia to, kad algoritmo sudėtingumas yra eksponentinis. Toliau nagrinėsime galimus patobulinimus.

Patobulinimai

Pirmiuasia paminėsime, kad, kai $\deg P = 22$, superkompiuteriui pakanka maždaug 20 sekundžių algoritmo įvykdymui. Nesunku apskaičiuoti, kad, kai $\deg(P) = 36$, mums reikės laukti kelias dienas, kol bus užbaigti skaičiavimai. Kokie patobulinimai galėtų būti įgyvendinti? Užuot tikrinę visus visus n-tojo laipsnio polinomus mes galėtume ieškoti tik polinomų su tuo pačiu $P(1)$, jei tiksli $P(1)$ reikšmė būtų žinoma (toliau visus tokius polinomus vadinsime poaibiu). Tada pakaktų patikrinti tik nedidelę dalį polinomų lyginant su visa aibe $\mathbb{P}_n$. Tiksliau, remiantis kombinatorika (ž.r. perstatos su pasikartojimais), pakaktų patikrinti

$$\frac{(\deg(P) - 1)!}{n_1! n_2!}$$

polinomų, kur $n_1 = P(1) - 2$ and $n_2 = \deg(P) - 1 - n_1$. 5 paveikslėlyje pateiktas grafikas leidžia manyti, kad pakaktų patikrinti intervalą $[[y - d], [y + d]]$. Tai reikštų, kad reikėtų patikrinti devynis poaibius. Algoritmas galėtų būti toks:

Algoritmas 9 Patobulintas algoritmas

Įvedimas: $\deg P$
Rezultatas: $min_{P \in \mathbb{P}} Q_2(P)$
  inicializavimas
  for $i \leftarrow [y - d]$ to $[y + d]$ **do**
    apskaičiuoti poaibį i-jai reikšmei
    for visiems j iš poaibio **do**
      sukurti $\deg P$ laipsnio polinoma
      apskaičiuoti $H(P^2)$
      apskaičiuoti $P(1)$
      apskaičiuoti $Q(P)$
    end for
  end for

Sunku įvertinti tokio algoritmo sudėtingumą. Jis neturėtų viršyti $\frac{n!}{\frac{n}{2}!\frac{n}{2}!}$, kur $n = \deg P - 1$. Kadangi $n! \approx \sqrt{2\pi n}(\frac{n}{e})^n$, gauname sudėtingumą $deg(P)^2 \frac{2^{\deg P}}{\sqrt{\deg P}}$. Panagrinėkime pavyzdį, kai $\deg P = 35$. Remiantis tiesinės regresijos lygtimi $N(P) = 24.56 \approx 25$. Reikia apskaičiuoti polinomus intervalui [21, 29]. Tai reiškia, kad mums reikia patikrinti 1'971'173'936 polinomus, o pagal mūsų pateiktą įvertį būtų 2'333'606'220. Jei pavyktų pritaikyti periodiškumą nuspėjant $P(1)$ reikšmę tiksliau, tuomet galėtume minėtą skaičių sumažinti keturis ar net daugiau kartų. Tai galėtų būti kito tyrimo tikslas.

Literatūros sąrašas

[1] S. D. Adhikari, P. Rath, and N. Saradha, *On the sets of uniqueness of the distribution function of* $\{\xi(p/q)^n\}$*,* Acta. Arith., **119**, 307–316 (2005).

[2] S. Akiyama, C. Frougny, and J. Sakarovitch, *Powers of rationals modulo 1 and rational base number systems,* Israel J. Math., **168**, 53–91 (2008).

[3] D. Applegate, B. Cloitre, P. Deléham, and N. J. A. Sloane, *Sloping Binary Numbers: A New Sequence Related to the Binary Numbers*, Journal of Integer Sequences **8** (3) (2005), 15 p.

[4] W. D. Banks and F. Luca, *Concatenations with Binary Recurrent Sequences*, Journal of Integer Sequences **8** (1) (2005), 19 p.

[5] K. Balasubramanian, *Combinatorial Enumeration of Ragas (Scales of Integer Sequences) of Indian Music*, Journal of Integer Sequences **5** (2) (2002), 21 p.

[6] W. R. Alford, A. Granville and C. Pomerance, *There are Infinitely Many Carmichael Numbers,* Ann. Math. **139**, 703-722 (1994).

[7] G. Alkauskas and A. Dubickas, *Prime and composite numbers as integer parts of powers,* Acta Math. Hung., **105**, 249–256 (2004).

[8] D. Andrica and I. Tomescu, *On an Integer Sequence Related to a Product of Trigonometric Functions, and Its Combinatorial Relevance″*, Journal of Integer Sequences **5** (2) (2002), 8 p.

[9] R. Astudillo, *On a Class of Thue-Morse Type Sequences*, Journal of Integer Sequences **6** (4) (2003), 11 p.

[10] R. C. Baker and G. Harman, *Primes of the form* $[c^p]$*,* Math. Zeitschr., **221**, 73–81 (1996).

[11] P. Barry, *A Catalan Transform and Related Transformations on Integer Sequences*, Journal of Integer Sequences **8** (4) (2005), 24 p.

[12] M. Benoumhani, *A Sequence of Binomial Coefficients Related to Lucas and Fibonacci Numbers*, Journal of Integer Sequences **6** (2) (2003), 10 p.

[13] K. S. Berenhaut and F. Saidak, *A note on the maximal coefficients of squares of Newman polynomials,* J. Number Theory **125**, 285–288 (2007).

[14] Y. Bugeaud, *Linear mod one transformations and the distribution of fractional parts* $\{\xi(p/q)^n\}$*,* Acta Arith., **114**, 301–311 (2004).

[15] P. J. Cameron, *Sequences Realized by Oligomorphic Permutation Groups*, Journal of Integer Sequences **3** (1) (2000).

[16] D. Cass, *Integer parts of powers of quadratic units,* Proc. Amer. Math. Soc., **101**, 610–612 (1987).

[17] P. Chinn and S. Heubach, *Integer Sequences Related to Compositions without 2's*, Journal of Integer Sequences **6** (2) (2003), 12 p.

[18] J. Cilleruelo, *Maximal coefficients of squares of Newman polynomials,* preprint (2008).

[19] L. Clark, *An Asymptotic Expansion for the Catalan-Larcombe-French Sequence*, Journal of Integer Sequences **7** (2) (2004), 5 p.

[20] B. Cloitre, N. J. A. Sloane, and M. J. Vandermast, *Numerical Analogues of Aronson's Sequence*, Journal of Integer Sequences **6** (2) (2003), 14 p.

[21] G. L. Cohen and D. E. Iannucci, *Derived Sequences*, Journal of Integer Sequences **6** (1) (2003), p. 10.

[22] M. M. Conroy, *A Sequence Related to a Conjecture of Schinzel*, Journal of Integer Sequences **4** (1) (2001).

[23] G. E. Cossali, *A Common Generating Function for Catalan Numbers and Other Integer Sequences*, Journal of Integer Sequences **6** (1) (2003), 8 p.

[24] T. Dana-Picard, *Sequences of Definite Integrals, Factorials and Double Factorials*, Journal of Integer Sequences **8** (4) (2005), 10 p.

[25] B.-S. Du, S.-Sh. Huang, and M.-Ch. Li, *Newton, Fermat, and Exactly Realizable Sequences*, Journal of Integer Sequences **8** (1) (2005), 8 p.

[26] A. Dubickas, *Arithmetical properties of powers of algebraic numbers,* Bull. London Math. Soc. **38** (1), 70–80 (2006).

[27] A. Dubickas, *Divisibility properties of some recurrent sequences,* Zapiski Nauchn. Semin. POMI, **322**, 76–82 (2005). (Reprinted in: *J. Math. Sciences* **137**, 4654–4657 (2006).)

[28] A. Dubickas, *Heights of powers of Newman and Littlewood polynomials,* Acta Arith., **128 (2)**, 167–176 (2007).

[29] A. Dubickas, *Integer parts of powers of Pisot and Salem numbers,* Archiv Math., **79**, 252–257 (2002).

[30] A. Dubickas, *On the powers of some transcendental numbers,* Bull. Austral. Math. Soc., **76**, 433–440 (2007).

[31] A. Dubickas, *Sequences with infinitely many composite numbers,* Analytic and Probabilistic Methods in Number Theory (eds. A. Dubickas et al.), Palanga, 2001 TEV, Vilnius, 57–60 (2002).

[32] A. Dubickas and A. Novikas, *Integer parts of powers of rational numbers,* Math. Z., **251**, 635–648 (2005).

[33] W. Duke, S. J. Greenfield and E. R. Speer, *Properties of a Quadratic Fibonacci Recurrence*, Journal of Integer Sequences **1** (1998).

[34] R. Euler, *The Fibonacci Number of a Grid Graph and a New Class of Integer Sequences*, Journal of Integer Sequences **8** (2) (2005), 16 p.

[35] G. Everest, A. J. van der Poorten, Y. Puri, and T. Ward, *Integer Sequences and Periodic Points*, Journal of Integer Sequences **5** (2) (2002), 10 p.

[36] L. Flatto, J. C. Lagarias, and A. D. Pollington, *On the range of fractional parts* $\{\xi(p/q)^n\}$*,* Acta Arith., **70**, 125–147 (1995).

[37] W. Forman and H. N. Shapiro, *An arithmetic property of certain rational powers,* Comm. Pure Appl. Math., **20**, 561–573 (1967).

[38] D. A. Gewurz and F. Merola, *Sequences Realized as Parker Vectors of Oligomorphic Permutation Groups*, Journal of Integer Sequences **6** (1) (2003), 11 p.

[39] I. P. Goulden, S. Litsyn, and V. Shevelev, *On a Sequence Arising in Algebraic Geometry*, Journal of Integer Sequences **8** (4) (2005), 9 p.

[40] R. K. Guy, *Unsolved problems in number theory,* Springer-Verlag, New York, (1994).

[41] K. G. Hare and S. Yazdani, *Further Results on Derived Sequences*, Journal of Integer Sequences **6** (2) (2003), 7 p.

[42] D. E. Iannucci and D. Mills-Taylor, *On Generalizing the Connell Sequence*, Journal of Integer Sequences **2** (1999).

[43] C. Kimberling, *Matrix Transformations of Integer Sequences*, Journal of Integer Sequences **6** (3) (2003), 11 p.

[44] J. F. Koksma, *Ein mengen-theoretischer Satz über Gleichverteilung modulo eins,* Compositio Math., **2**, 250–258 (1935).

[45] M. N. Kolountzakis, *Coefficients of squares of Newman polynomials,* preprint (2008), http://fourier.math.uoc.gr/~mk/publ/.

[46] N. Kube and F. Ruskey, *Sequences That Satisfy a(n-a(n))=0*, Journal of Integer Sequences **8** (5) (2005), 8 p.

[47] J. W. Layman, *Some Properties of a Certain Nonaveraging Sequence*, Journal of Integer Sequences **2** (1999).

[48] V.A. Liskovets, *Some Easily Derivable Integer Sequences*, Journal of Integer Sequences **3** (2) (2000), 15 p.

[49] K. Mahler, *An unsolved problem on the powers of 3/2,* J. Austral. Math. Soc., **8**, 313–321 (1968).

[50] G. Martin and K. O'Bryant, *Continuous Ramsey theory and Sidon sets,* preprint (2002), arXiv:math/0210041v1.

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

[52] T. Müller, *Prime and Composite Terms in Sloane's Sequence A056542*, Journal of Integer Sequences **8** (3) (2005), 9 p.

[53] T. D. Noe and J. V. Post, *Primes in Fibonacci n-step and Lucas n-step Sequences*, Journal of Integer Sequences **8** (4) (2005), 12 p.

[54] D.J. Newman, *An L^1 extremal problem for polynomials*, Proc. Amer. Math. Soc. **16**, 1287–1290 (1965).

[55] K. O'Bryant, *A complete annotated bibliography of work related to Sidon sequences*, Electronic Journal of Combinatorics (Dynamic Surveys) **11** (2004).

[56] J. A. Pelesko, *Generalizing the Conway-Hofstadter $10,000 Sequence*, Journal of Integer Sequences **7** (3) (2004), 11 p.

[57] A. Petojevic, *The Function ${}_vM_m(s;a;z)$ and Some Well-Known Sequences*, Journal of Integer Sequences **5** (1) (2002), 16 p.

[58] A. J. van der Poorten, *Curves of Genus 2, Continued Fractions, and Somos Sequences*, Journal of Integer Sequences **8** (3) (2005), 9 p.

[59] E. Preissmann, *A Self-Indexed Sequence*, Journal of Integer Sequences **8** (3) (2005), 6 p.

[60] J.-Ch. Schlage-Puchta, *A Criterion for Non-Automaticity of Sequences*, Journal of Integer Sequences **6** (3) (2003), 5 p.

[61] J.-Ch. Schlage-Puchta and J. Spilker, *The Greatest Common Divisor of Two Recursive Functions*, Journal of Integer Sequences **7** (1) (2004), 5 p.

[62] S. E. Speed, *The Integer Sequence A002620 and Upper Antagonistic Functions*, Journal of Integer Sequences **6** (1) (2003), 17 p.

[63] G. E. Stevens, *A Connell-Like Sequence*, Journal of Integer Sequences **1** (1998).

[64] O. Strauch and Š. Porubský, *Distribution of sequences: A sampler,* Schriftenreihe der Slowakischen Akademie der Wissenschaften, **1**, Peter Lang, Frankfurt, (2005).

[65] R. Suter, *Two Analogues of a Classical Sequence*, Journal of Integer Sequences **3** (1) (1998).

[66] R. Tauraso, *A New Domino Tiling Sequence*, Journal of Integer Sequences **7** (2) (2004), 5 p.

[67] T. Vijayaraghavan, *On the fractional parts of the powers of a number,* J. London Math. Soc., **15**, 159–160 (1940).

[68] M. Vsemirnov, *A New Fibonacci-like Sequence of Composite Numbers*, Journal of Integer Sequences **7** (3) (2004), 3 p.

[69] H. Weyl, *Über die Gleichverteilung von Zahlen modulo Eins,* Math. Ann., **77**, 313–352 (1916).

[70] W. Woan, *A Recursive Relation for Weighted Motzkin Sequences*, Journal of Integer Sequences **8** (1) (2005), 8 p.

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

[72] G. Yu, *An upper bound for $B_2[g]$ sets,* J. Number Theory **122**, 211–220 (2007).

[73] "Carmichael number", *Wikipedia,* 24 April 2009, http://en.wikipedia.org/wiki/Carmichael_number, 6 June 2009.

[74] "Cycle detection", *Wikipedia,* 28 May 2009, http://en.wikipedia.org/wiki/Floyd%27s_cycle-finding_algorithm, 6 June 2009.