ŠIAULIŲ UNIVERSITETAS

MATEMATIKOS IR INFORMATIKOS FAKULTETAS

MATEMATIKOS KATEDRA

Asta Mižutavičiūtė

Pirminių skaičių generavimas Mažosios Ferma teoremos metodu

Bakalauro darbas

Darbo vadovas:

Prof. dr. D.Šiaučiūnas

Šiauliai, 2012

Turinys

Įvadas

Pirminių skaičių pasiskirstymo klausimai sprendžiami nuo Euklido (Euclid). Jis įrodė, kad pirminių skaičių yra be galo daug, o Oileris (Euler) įrodė, jog eilutė $\sum_p \frac{1}{p}$ diverguoja, bei, kad pirminių skaičių yra daug mažiau negu natūraliųjų. Nagrinėjama ir daugybė įvairių kitų matematinių problemų, susijusių su pirminių skaičių pasiskirstymu.

Yra du faktai apie pirminių skaičių pasiskirstymą, kuriuos amerikiečių matematikas Don‘as Zagier‘as pakomentavo taip: „*Pirmasis, kad nepaisant jų elementaraus apibrėžimo ir statybinių blokų vaidmens natūriniams skaičiams, jie veši tarsi piktžolės tarp natūrinių skaičių ir atrodo, kad nėra jokio dėsningumo, o tik atsitiktinumas, todėl niekas negali nuspėti, kur išdygs kitas. Antrasis faktas dar labiau nustebina, nes teigia visiškai priešingai – kad pirminiai skaičiai pasirodo stebėtinai reguliariai, kad yra dėsniai, nusakantys jų elgseną, ir kad jie tų dėsningumų prisilaiko beveik kariška drausme*“.

Labai svarbi matematikos užduotis yra pirminių skaičių radimas. Patį paprasčiausią metodą pasiūlė garsus senovės graikų matematikas Eratostenas. Šis metodas dabar yra vadinamas Eratosteno rėčiu. Tačiau šis metodas yra neefektyvus, kai reikia rasti didelius pirminius skaičius. Šių skaičių radimui yra pasitelkiami kompiuteriai. Bakalauro darbe matematiniu paketu *MathCAD* sukursime programą dideliems pirminiams skaičiams rasti.

Darbo tikslas ir uždaviniai

Darbo tikslas:

- Sudaryti patogią programą rasti „dideliems“ pirminiams skaičiams ir nustatyti kai kurias jų išsidėstymo sąvybes.

Darbo uždaviniai:

- Užrašyti pirminių skaičių generavimo algoritmo pagrindimą pritaikant Niutono binomo savybes.
- Sudaryti patogią programą pirminiams skaičiams rasti ir pateikti pirminių skaičių išsidėstymo grafinį vaizdavimą programa *MathCAD*.
- Programa *MathCAD* pateikti grafinį vaizdą tikrųjų, netikrųjų ir pseudopirminių skaičių pasiskirstymo palyginimui.

1. Pirminiai skaičiai

1.1 apibrėžimas. *Pirminiu yra vadinamas natūralusis skaičius p, toks, kad* $p > 1$ *ir neturi kitų sveikų teigiamų daliklių be 1 ir savęs paties (t. y. p)*

Pavyzdžiui, 2, 3, 5, 13, 17, 37 yra pirminiai skaičiai. *Natūralieji skaičiai, kurie nėra pirminiai, yra vadinami sudėtiniais*. *Pavyzdžiui*, $6 = 3 \cdot 2$, $363 = 3 \cdot 11 \cdot 11$ yra sudėtiniai skaičiai. Vienetas yra specialus atvejis, nes jis nelaikomas nei pirminiu, nei sudėtiniu skaičiumi. Visi pirminiai skaičiai yra nelyginiai, išskyrus vienintelį atvejį – 2 yra pirminis skaičius.

1.1 teorema. *Bet koks skaičius* $m \in N$, $m > 1$*, turi pirminį daliklį.*

Įrodymas. Tarkime priešingai, jog yra toks skaičius $m \in N$, $m > 1$, kuris neturi pirminių daliklių. Tuomet aibė tokių m, $m \in N$, $m > 1$, neturinčių pirminių daliklių, yra netuščia, todėl pagal visiško sutvarkymo aksiomą yra mažiausias natūralusis skaičius $k > 1$, kuris neturi pirminių daliklių. Kadangi *k* neturi pirminių daliklių ir$k \mid k$, tai matome, jog *k* nėra pirminis skaičius. Todėl galime parašyti, kad $k = ab$ su $1 < a < k$, $1 < b < k$. Kadangi $a < k$, tai *a* turi turėti pirminį daliklį. Tačiau kiekvienas skaičius *a* daliklis yra ir skaičiaus *k* daliklis, todėl ir *k* turi pirminį daliklį, kas prieštarauja tam, jog *k* neturi pirminių daliklių. Šis prieštaravimas ir įrodo teoremą.

Skaičiaus $m \in N$ dalikliai 1 ir m paprastai yra vadinami trivialiaisiais, o visi kiti – netrivialiaisiais.

Iš teoremos įrodymo aišku, jog mažiausias natūraliojo skaičiaus netrivialus daliklis yra pirminis skaičius.

1.2 teorema (fundamentalioji aritmetikos teorema). *Kiekvienas sveikasis skaičius* $n > 1$ *gali būti išskaidytas pirminiais dauginamaisiais vieninteliu būdu, tai yra*

$$n = p_1^{n_1} \cdot p_2^{n_2} \cdot \ldots \cdot p_k^{n_k}, \qquad (1.1)$$

čia $p_1 < p_2 < \ldots < p_k$ *– pirminiai skaičiai, o* $n_1, n_2, \ldots, n_k$ *– natūralieji skaičiai* ($n_i > 0$, $i = 1, 2, \ldots, k$), $k \geq 1$.

Kai kurios pirminių skaičių savybės [5]

- Pirminis skaičius p yra n dauginamasis tada ir tik tada, kai p yra vienas iš dauginamųjų $p_i, i = 1, \dots k,$ (1.1) išraiškoje;
- Euklido lema: Jeigu p yra pirminis skaičius ir ab dalijasi iš p, tai arba a dalijasi iš p arba b dalijasi iš p;
- Mažoji Ferma teorema: Jei p – pirminis, o a – natūralusis, tai $a^p - a$ dalijasi iš p;
- Vilsono teorema: Natūralusis $p > 1$ yra pirminiu tada ir tik tada, kai $(p-1)! + 1$ dalijasi iš p;
- Bertrano postulatas: Natūraliam $p > 1$ egzistuoja pirminis p toks, kad $n < p < 2n$;
- Dirichlė teorema: Bet kuri aritmetinė progresija $a, a+q, a+2q, \dots.$, kai a, $q > 1$ – sveiki tarpusavyje pirminiai skaičiai, turi begalinį pirminių skaičių kiekį;
- Skaičių, atvirkštinių pirminiams, seka diverguoja. Be to, kai $n \to \infty$, tai $\sum_{p<x} \frac{1}{p} = ln\ lnx$;
- Bet kuris pirminis skaičius, didesnis už 3, išreiškiamas pavidalu $6k+1$ arba $6k-1$, kur k tam tikras natūralusis skaičius;
- Jei $p > 3$ yra pirminis, tai $p^2 - 1$ yra 24 kartotinis.

2. Pirminių skaičių pasiskirstymas

Euklidas (Euclid) įrodė, kad pirminių skaičių yra be galo daug, bet tai nieko pasako apie jų pasiskirstymą. Pateikiame Euklido rezultatą ir kai kuriuos paprasčiausius pirminių skaičių skaičiaus

$$\pi(x) = \sum_{p \le x} 1,\ x > 0,$$

įverčius, kai $x \to \infty$. Pavyzdžiui, $\pi(1) = 0, \pi(2) = 1, \pi(3) = 2, \pi(4) = 2,...$

2.1 teorema. *Turime, kad*

$$\lim_{x>\infty} \frac{\pi(x)}{\frac{x}{lnx}} = 1.$$

2.1. Pirminių skaičių skaičius $\pi(x)$

Šiame skyrelyje aptarsime funkcijos $\pi(x)$ savybes.

2.1.1 teorema. *Pirminių skaičių yra be galo daug.*

Yra daug šio įrodymo būdų. Pateiksime porą iš jų.

Pirmasis įrodymo būdas. Imkime natūralųjį skaičių

$$Q_n = n! + 1, n \ge 1.$$

Žinoma, jog Q_n turi bent vieną pirminį daliklį [2], tarkime, q_n. Aišku, jog turi būti $q_n > n$, nes jei būtų $q_n \le n$, tai tuomet turėtų q_n dalyti $n!$. Bet tuomet iš dalumo savybių išplauktų, kad $q_n \mid (Q_n - n!) \mid = 1$, kas negalima.

Antras įrodymo būdas. Tarkime, kad egzistuoja tam tikras pirminių skaičių $p_1, p_2, \dots, p_k$ kiekis.

Užrašysime sandaugą:

$$\prod_{i=1}^{r}(1 - \frac{1}{p_i})^{-1} = \prod_{i=1}^{r}(1 + \frac{1}{p_i} + \frac{1}{p_i^2} + \cdots). \qquad (2.1.1)$$

Dešinioji lygybės pusė konverguoja absoliučiai, vadinasi šias eilutes galima sudauginti panariui ir gauta eilutė vėl turėtų konverguoti absoliučiai. Taigi, gauname

$$\prod_{i=1}^{r}(1 + \frac{1}{p_i} + \frac{1}{p_i^2} + \cdots) = \sum_{n}{}' \frac{1}{n} \qquad (2.1.2)$$

čia $\sum' \frac{1}{n}$ reiškia, jog sumuojame pagal tuos *n*, kurių pirminiai dalikliai neviršyja *x* ir 1. Taip pat žinoma, kad kiekvieną skaičių n >1 galima užrašyti pirminių skaičių sandauga. Vadinasi, dešinėje (2.1.2) lygybės pusėje gali būti bet koks skaičius *n*, kadangi priėmėme, jog $p_1, p_2, \dots, p_r$ – pirminiai skaičiai. Todėl eilutės dešinėje pusėje turi būti eilutė $\sum \frac{1}{n}$, kuri, kaip žinome, diverguoja. Gavome prieštaravimą, kas įrodo teoremą.

3. Mažoji Ferma teorema

Prancūzų matematikas Pjeras Ferma suformulavo vieną teoremą, kuri dabar yra vadinama Mažosios Ferma teoremos (MFT) vardu.

3.1 teorema. MFT skelbia, kad: Jeigu *a* nesidalija iš *p* ir jei *p* yra pirminis skaičius, tai $(a^{p-1}-1)$ dalijasi iš *p*.

Įrodymas. Visi skaičiai nuo 1 iki $p-1$ dalijami iš p duoda skirtingas liekanas. Įrodysime, kad jei,

$$a(mod\ p) \neq 0,$$

tai visi sekos $(p-1)\cdot a$ nariai dalijami iš *p* irgi duos skirtingas liekanas.

Tarkime, kad egzistuoja tokie du sekos nariai, kurie duoda vienodas liekanas:

$$a \cdot k \equiv a \cdot m(mod\ p).$$

Tada

$$ak - am \equiv 0(mod\ p).$$

Iškeliame *a*:

$$a \cdot (k-m) \equiv 0(mod\ p).$$

Tačiau

$$a(mod\ p) \neq 0 \rightarrow k - m \equiv 0(mod\ p).$$

Kadangi $k < p\ ir\ m < p$, gauname $k = m$.

Išeina, kad sekoje negali egzistuoti du skirtingi nariai

$$a \cdot m \equiv a \cdot k(mod\ p).$$

Pertvarkome seką:

$$1 \cdot a \cdot 2 \cdot a \cdot \ldots \cdot (p-1) \cdot a = (p-1)! \cdot a^{p-1};$$

$$(p-1)! \cdot a^{p-1} \equiv (p-1)!\,(mod\ p);$$

dalijame abi puses iš $(p-1)!$:

$$a^{p-1} \equiv 1(mod\ p).$$

Tą patį galima užrašyti ir kaip

$$a^{p-1}(mod\ p) = 0.$$

Įrodymas baigtas.

Taigi, MFT teigia, kad jei *p* yra pirminis skaičius, o sveikasis skaičius *a* nesidalija iš *p*, tai

$$a^{p-1} \equiv 1 mod\ p.$$

Yra žinomas šiek tiek stipresnis MFT formulavimas, priklausantis L. Oileriui.

3.2 teorema. *Sakykime, kad* $(a,m) = 1$ *(yra tarpusavyje pirminiai). Tuomet*

$$a^{\varphi}(m) \equiv 1(mod\ m).$$

4. Pseudo pirminių skaičių generavimo algoritmo pagrindimas Niutono binomo metodu

Binomo formulė – dažnai dar vadinama Niutono formule, yra svarbi matematikos teorema, padedanti rasti dvinario, pakelto n – uoju laipsniu, skleidinį.

4.1 teorema. *Turime formulę*

$$(a+b)^p = \sum_{k=0}^{p} a^k \cdot C_p^k \cdot b^{p-k},$$

Formulės dėmenys $a^k \cdot C_p^k \cdot b^{p-k}$, $k = 0, 1, 2, \dots, p$, vadinami Niutono binomo nariais, o koficientai C_p^k, $k = 0, 1, 2, \dots, p$ – binominiai koeficientais.

Pagal Niutono binomo formulę gauname laipsnio $(a+b)^p$ skleidinį (išraišką):

$$(a+b)^p = a^p + p \cdot a^{p-1} \cdot b + \frac{p(p-1)}{2!} \cdot a^{p-2} \cdot b^2 + \cdots + \frac{pa\,b^{p-1}}{1!} + b^p.$$

Jei p pirminis skaičius, tai keliant $(a+b)^p$ gauname liekaną b^p arba b.

Kadangi atvirkštinė Ferma teorema [4] yra tik būtina, tačiau nepakankama, tai reiškia, kad Ferma teoremos savybes gali turėti ir kai kurie sudėtiniai skaičiai. Konkrečiai, jeigu a ir p tarpusavyje pirminiai ir tokie, kad $a^{p-1} - 1$ dalijasi iš p, tai skaičius p gali būti ir sudėtinis. Jei p yra sudėtinis, tai jis vadinamas pseudopirminiu skaičiumi pagrindu a.

Pavyzdžiui, 1820 m. F. Sarrus nustatė, kad skaičius $N = 2^{341-1} - 1$ dalijasi iš 341 (nes $2^{10} - 1 = 3 \cdot 341$). Bet 341 – sudėtinis skaičius $341 = 11 \cdot 31$. Tai pirmasis tokio tipo pagrindu 2 skaičius. Minėtus skaičius vadiname Karmailo skaičiais. Mažiausias iš jų yra 561.

Nors Mažoji Ferma teorema negarantuoja, kad p yra pirminis skaičius, tačiau ji gali paversti skaičių testavimui: jeigu $(a^p - a)$ nesidalija iš p, tai p – sudėtinis skaičius.

4.1. Metodo pagrindimas pritaikant Niutono binomo savybes

Pagal Niutono binomo formulę

$$(a+b)^p = \sum_{k=0}^{p} a^k \cdot C_p^k \cdot b^{p-k},$$

kai abu nariai yra vienetai: $a = 1$; $b = 1$, tuomet gauname, kad:

$$(1+1)^p = \sum_{k=0}^{p} 1^k \cdot C_p^k \cdot 1^{p-k} = 1 + p + \frac{p(p-1)}{2!} + \cdots + 1 = 2 + \sum_{k=1}^{p-1} C_p^k.$$

$$(1+1)^p = \sum_{k=0}^{p} \frac{p!}{k!(p-k)!} = 1 + 1 + \sum_{k=1}^{p-1} \frac{p!}{k!(p-k)!}.$$

Šią išraišką padalijus iš p gauname liekaną 2. Jeigu 2^p dalijame iš 2, tuomet gauname išraiškos 2^{p-1} liekaną lygią vienetui.

Imame mažiausią iš nustakytų Ferma teoremoje pagrindo reikšme 2^{p-1} todėl, kad norime analizuoti mažiausią iš visų galimų reikšmę. [6]

5. Vieno „pirminio“ skaičiaus radimo metodas

Susitarkime, kad „pirminiais“ skaičiais sąlyginai pavadiname tuos skaičius, kuriems galioja Mažoji Ferma teorema, t. y – tikrų pirminių ir pseudopirminių skaičių aibė. k – ieškomasis skaičius.

Pervedame šį skaičių į dvejetainę skaičiavimo sistemą ir skaičiuojame aukščiausią dvejetainės sistemos laipsnį $\frac{ln(k)}{ln(r)}$, kuris programa *MathCAD* užrašomas taip

$$J = floor\left(\frac{ln(k)}{ln(r)}\right).$$

Pavyzdžiui, kai k=9999991, aukščiausias dvejetainės sistemos laipsnis yra

$$J = 30.$$

s_j yra reikšmės $k-1$, paverstos į dvejetainę sistemą, $k-1 = s_0 + 2s_1 + 2^2 s_2 + 2^3 s_3 + \cdots$ nariai. *MathCAD'u* jie išreiškiami tokiu būdu

$$s_j = mod\left(floor\left(\frac{k-1}{r^j}\right), r\right).$$

q_0 skaičiuoja skaičiaus s_0 liekaną

$$q_0 = mod\left(2^{s_0}, k\right),$$

$$Q_0 = q_0,$$

taip pat skaičiuojame skaičiaus 2^r liekaną, kuri yra

$$q_1 = mod\left(2^r, k\right).$$

Q_1 rodo išraiškos $(q_l)^{s_l}$ liekaną

$$Q_1 = mod\left[\left(q_1\right)^{s_1}, k\right],$$

kai

$$m = 2..J,\ l' = 1..J.$$

Skaičiuojame prieš tai esančio skaičiaus kvadrato liekaną

$$q_m = mod\left[\left(q_{m-1}\right)^r, k\right].$$

Q_m rodo išraiškos $(q_m)^{s_m}$ liekaną

$$Q_m = mod\left[\left(q_m\right)^{s_m}, k\right],$$

kai

$$v_0 = q_0.$$

$v_{l'}$ parodo paskutinę liekaną

$$v_{l'} := mod\left(v_{l'-1} \cdot Q_{l'}, k\right) .$$

Randame galutinę liekaną

$$p = v_J$$

ir jei liekana yra 1, tai tuomet ieškomas skaičius k yra pirminis

$$p = 1.$$

5.1 lentelė. Dvejetainės sistemos koeficientai

	0
0	0
1	1
2	1
3	0
4	1
5	1
6	1
7	0
8	0
9	1
10	1
11	0
12	1
13	0
14	0
15	1
16	0
17	0
18	0
19	1
20	1
21	0
22	0
23	1
24	

5.2 lentelė. 2^j liekanos skaičiaus k atžvilgiu

	0
0	1
1	4
2	16
3	256
4	65536
5	4971157
6	4159827
7	6243682
8	2364
9	5588496
10	5650195
11	2270282
12	4998286
13	5422388
14	8084623
15	7877191
16	3895652
17	8163603
18	3921632
19	1384713
20	1818056
21	593933
22	6725964
23	2444063
24	

5.3 lentelė. Dviejų gretimų dvejetainių skaičių sandaugos liekanos

	0
0	1
1	4
2	64
3	64
4	4194304
5	2455232
6	9556870
7	9556870
8	9556870
9	7835233
10	4164002
11	4164002
12	1632173
13	1632173
14	1632173
15	37298
16	37298
17	37298
18	37298
19	7071950
20	2700689
21	2700689
22	2700689
23	1
24	

Liekanos paskaičiuotos dviem etapais. Pirmiausia paskaičiuojame 2^j liekanas q (5.2 lentelė), poto skaičiuojame dviejų gretimų išraiškų liekanų sandaugų liekanas v (5.3 lentelė). Jeigu paskutinė v liekana yra 1, tai k yra pirminis skaičius.

6. „Pirminių“ skaičių radimas skaidymo metodu

Tarkime, kad intervalo pradžia

$$K1 = 1110001,$$

o ilgis N yra

$$N = 5090,\ n = 0..N,$$

čia kintamasis $k1_n$ kinta žingsniu $2n$

$$k1_n = K1 + 2n,$$

o k_n yra vienetu mažesnis už $k1_n$

$$k_n = k1_n - 1.$$

Aukščiausias laipsnis, kuris lygus logaritmo pagrindu 2 sveikajai daliai $log_2 k_n = \frac{\ln(k_N)}{\ln(2)}$.

Programa *MathCAD* užrašomas taip

$$J = floor\left(\frac{ln(k_N)}{ln(2)}\right).$$

$$j = 0..J,\ J = 20,$$

$$K2 = k1_N.$$

Laikykime, kad intervalo pabaiga yra $K2 = 1120181$.

Tarkime, kad $\frac{k_n}{2^j}$ yra sveikosios santykio dalies modulis pagrindu 2. Programa *MathCAD* užrašome taip

$$s_{j,n} = mod\left(floor\left(\frac{k_n}{2^j}\right), 2\right),\ m = 1..J,$$

o $q_{0,n}$ – dvejetainių skaičių pagrindas (pirmasis - 2^0, antrasis - 2^1,..)

$$q_{0,n} = 2.$$

$q_{m,n}$ – modulis, pagrindu $k1_n$. *MathCAD* išraiška yra tokia

$$q_{m,n} = mod\left[\left(q_{m-1,n}\right)^2, k1_n\right],$$

$$P_{0,n} = 1.$$

$P_{m,n}$ yra skaičiaus modulis, pagrindu $k1_n$. Programa *MathCAD* užrašome taip

$$p_{m,n} = mod\left[p_{m-1,n}\left(q_{m,n}\right)^{s_{m,n}}, k1_n\right],$$

$$Q_n = p_{J,n}.$$

g yra matrica gauta sujungus dviejų matricų stulpelius į vieną matricą. Tai įvykdoma tokiu būdu

$$g = augment(k1, Q),$$

o $g1$ yra matrica gauta iš matricos g surūšiavus jos elementus didėjimo tvarka

$$g1 = csort(g, 1).$$

Panaudojame loginę komandą, kuri, kai patenkinta sąlyga $g1_{n,1}=1$ tą vienetą palieka, o kai sąlyga $g1_{n,1}=0$ nepatenkinta, ji verčiama nuliu

$$L := \sum_{n=0}^{N} \left(g1_{n,1} = 1\right) - 1,$$

$$L + 1 = 727.$$

Paliekame stulpelio tik tą matricos dalį, kurios g_1 reikšmės lygios 1 ir jų skaičius lygus $L + 1$

$$g2 = submatrix(g1, 0, L, 0, 0)$$

ir pirminius skaičius sudedame eilės tvarka

$$G = sort(g2),$$

$$l = 1..L,\ sk_0 = 0,$$

sk_l parodo skirtumus tarp šalia esančių sekos narių

$$sk_l = G_l - G_{l-1},$$

o v – didžiausią skirtumą

$$V = 0.5 \cdot max(sk),\ v = 0..V.$$

Sumuojame tik tuos narius, kur patenkinta sąlyga $2v=sk_k$

$$z_v = \sum_{k=0}^{L} \left(2v = sk_k\right).$$

Įvedame naują kintamąjį

$$w_v = 2v,$$

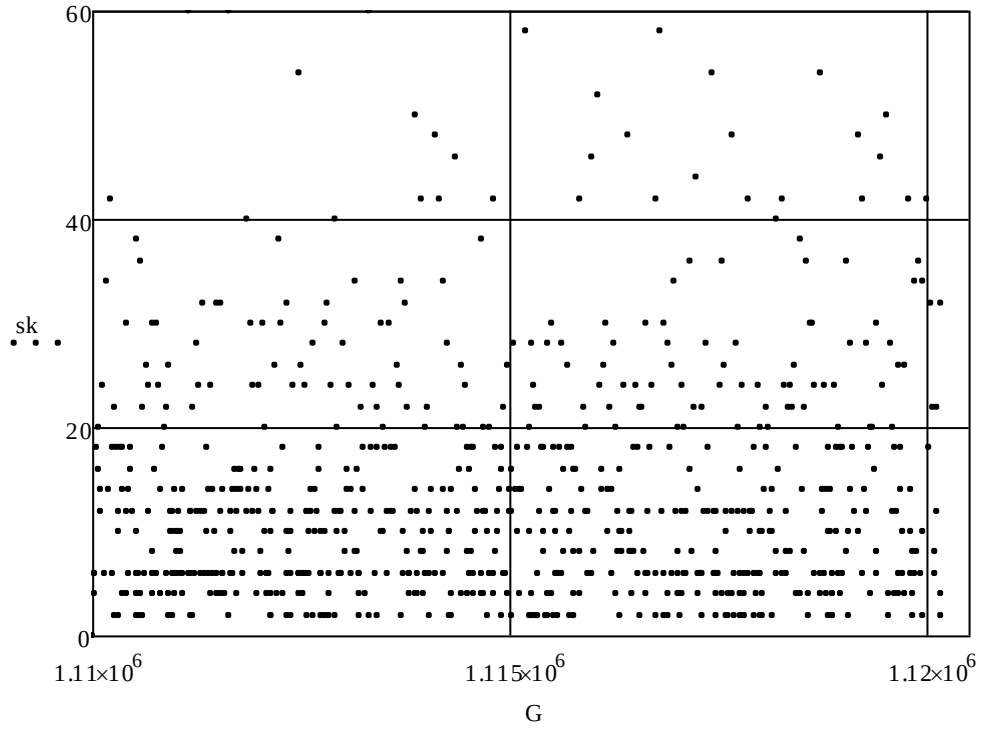
Z' matricą gauname sujungus w ir z stulpelius į vieną matricą

$$Z' := augment(w, z)$$

ir ją pertvarkome – Z' pirmojo stulpelio reikšmes didėjimo tvarka

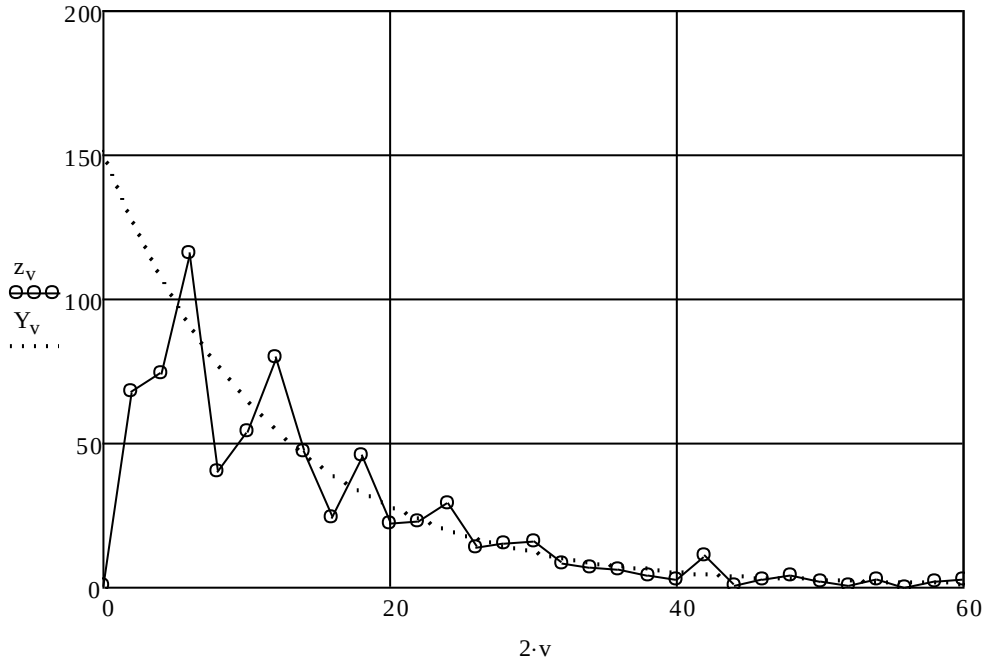
$$Z := -csort(-Z', 1),\ V = 30$$

Grafinį vaizdą pateikiame programa *MathCAD*. Šie keli grafikai taip pat tinka aproksimavimo kubiniu polinomu (K=3) ir tiese (K=1) metodui ir skiriasi tik tuo, kad grafikai yra kitame, didesniame eilės numerių intervale.



6.1 pav. Skirtumas tarp pirminių skaičių

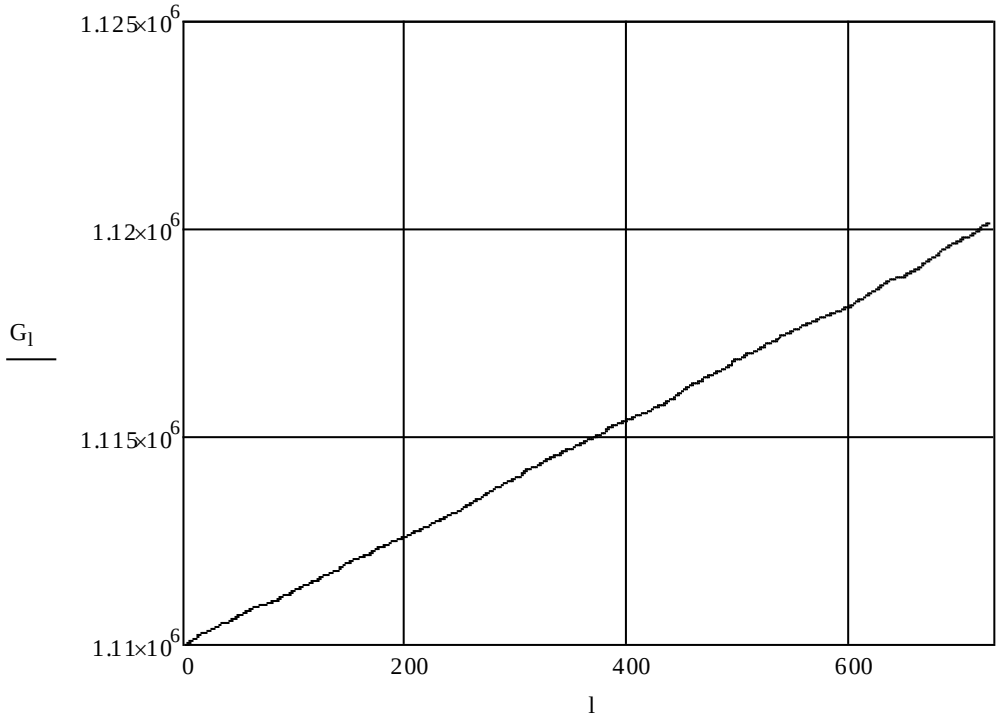
Šiame grafike sumodeliuotas atsitiktinis išsidėstymas pagal eksponentinį dėsnį, kai atsitiktinės reikšmės yra sveikieji skaičiai. Pastebime, kad didėjant pirminių skaičių eilės numeriui, išsidėsčiūsių pirminių skaičių yra vis mažiau.



6.2 pav. Pasikartojančių tų pačių pirminių skaičių skirtumai

Pirminiai skaičiai, tarp kurių skirtumas yra lygus 2 vadinami pirminiais dvyniais. Tai poros (3, 5), (5, 7),.. Mažesnis iš dvynių vadinamas Čano pirminiu skaičiumi. Betkurių pirminių dvynių forma yra (6n-1, 6n+1), kur n – tam tikras natūralusis skaičius.

Šiame grafike pastebime dėsningumą ir pademonstruojame, kad daugiausiai yra šešetukų ir jiems kartotinių skaičių.



6.3 pav. Pirminių skaičių priklausomybės nuo eilės numerio

6.3 paveiksle matome, kad pirminio skaičiaus didumas tiesiškai priklauso nuo eilės numerio. Kai G_l – pirminio skaičiaus dydis, o l – pirminio skaičiaus eilės numeris.

Pirminio skaičiaus dydis yra beveik tiesiog proporcingas eilės numeriui.

6.1.1 lentelė. Skirtumų tarp gretimų pirminių skaičių fragmentas

	0
0	0
1	6
2	6
3	4
4	18
5	20
6	16
7	12
8	14
9	24
10	6
11	34
12	14
13	42
14	6
15	...

6.2.1 lentelė. Pasikartojantys vienodi skirtumai tarp gretimų pirminių skaičių

	0	1
0	6	116
1	12	80
2	4	74
3	2	68
4	10	54
5	14	47
6	18	46
7	8	40
8	24	29
9	16	24
10	22	23
11	20	22
12	30	16
13	28	15
14	26	14
15	42	...

6.3.1 lentelė. Gautieji pirminiai skaičiai

	0
0	1110007
1	1110013
2	1110019
3	1110023
4	1110041
5	1110061
6	1110077
7	1110089
8	1110103
9	1110127
10	1110133
11	1110167
12	1110181
13	1110223
14	1110229
15	...

Iš 6.3.1 lentelės paskaičiuoti skirtumai tarp gretimų pirminių skaičių (6.1.1 lentelė). Suvedus tų skirtumų statistiką išaiškėja, kad dažniausias skirtumas 6 (116 kartų), po to 12 (80 kartų) ir t.t. Pastebime, kad dominuoja 6skirtumai.

7. Aproksimavimas kubiniu polinomu ir tiese

Kelis grafikus, tinkančius šiam metodui jau matėme pirminių skaičių skaidymo metode (žr. 5.1 pav ir 5.2 pav).

Pasinaudoję polinomine regresijos formule, paėmus duomenis iš skaičiavimo parašyto 6 skyrelyje rezultatų, pateiksime dar keletą grafikų. Šiuo atveju aproksimavimas vykdomas mažiausiu kvadrato metodu.

$$K = 3,\ k = 0..K.$$

Pagal jį užrašoma kairiosios lygčių sistemos

$$A_{l,k} = l^k,$$

pusės matrica kiekvienam eilės numeriui, o dešiniosios lygčių sistemos pusės matrica yra G – pseudo atsitiktinių skaičių matrica.

Išsprendus lygčių sistemą, kurioje nežinomųjų daug kartų mažiau nei lygčių, paprastųjų iteracijų metodu gaunama aproksimuojančios funkcijos matrica c

$$c = lsolve(A, G).$$

Turėdami šią matricą, gauname aproksimuojančios funkcijos reikšmes kiekvienam y_l

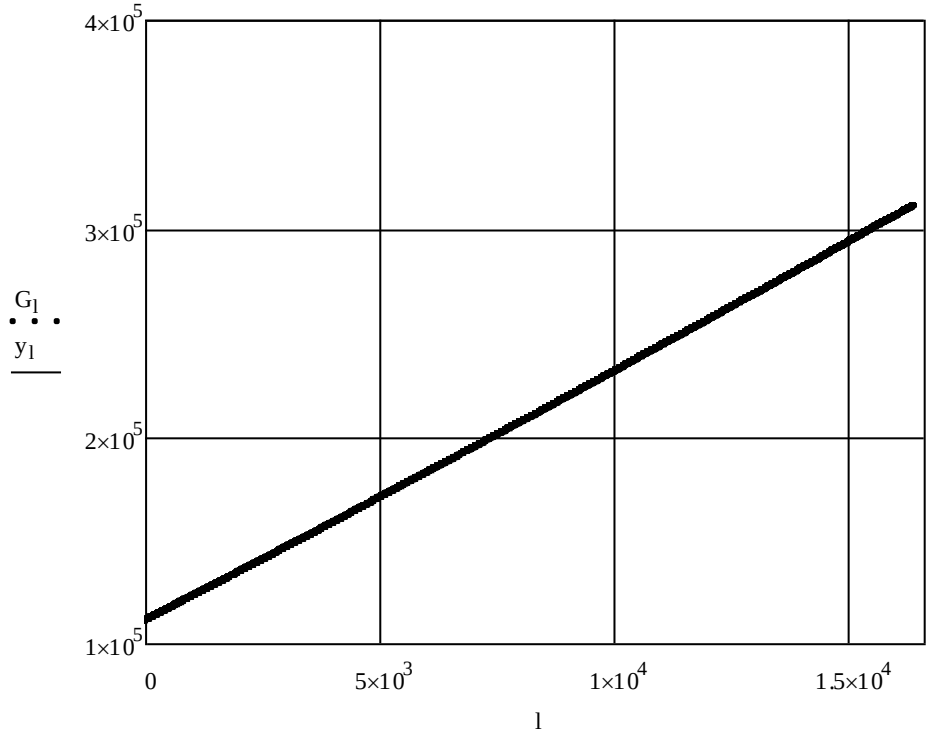
$$y_l = \sum_{k=0}^{K} \left(c_k \cdot l^k \right).$$

Kai polinomo laipsnis $K = 3$, aproksimavimo paklaida yra gaunama komanda *stdev*

$$stdev(y - G) = 871.731.$$

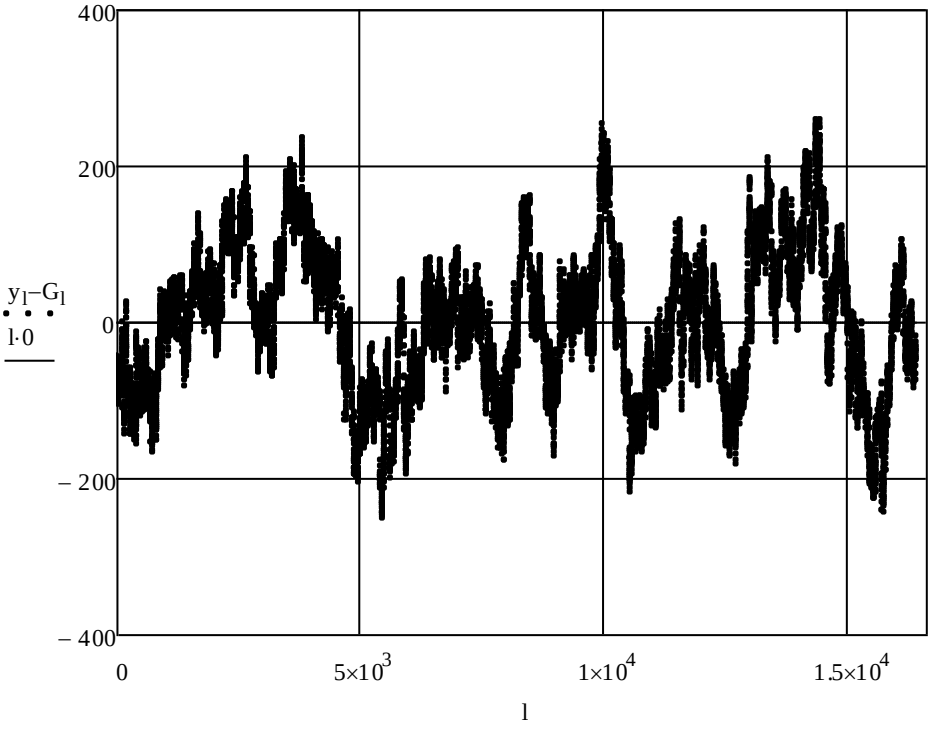
Matricos c elementai yra aproksimavimo polinomo koeficientai

$$c = \begin{pmatrix} 1.11 \times 10^{5} \\ 11.649 \\ 3.774 \times 10^{-5} \\ -2.697 \times 10^{-10} \end{pmatrix}.$$



7.1 pav. Pirminių skaičių priklausomybės nuo aproksimavimo 3 eilės polinomu kreivė

Šiame grafike matoma aproksimavimo kreivė einanti praktiškai beveik per konkrečius taškus, tačiau detalizuojant paklaidas (7.2 pav) pastebime aproksimavimo paklaidų „šokinėjimą“.



7.2 pav. Pirminių skaičių priklausomybės nuo aproksimavimo 3 eilės polinomu paklaidų kreivė

Šiuo atveju aproksimuojama tiese (pirmos eilės polinomu)

$$K1 = 1,\ k1 = 0..K1$$

ir atlikę analogiškus veiksmus kaip ir $K = 3$ atveju, gaunama aproksimavimo kreivė, kuri eina praktiškai beveik per konkrečius taškus (7.1 pav).

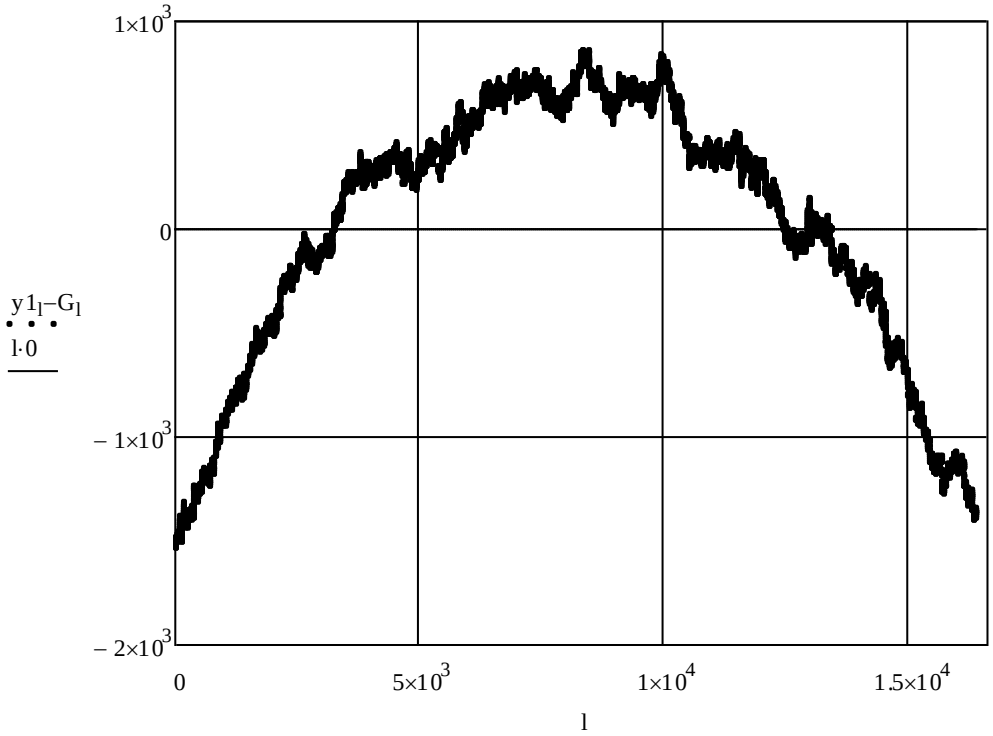
Matrica *c* nusako aproksimavimo tiese koeficientus

$$c1 = \begin{pmatrix} 1.095 \times 10^5 \\ 12.202 \end{pmatrix}.$$

Kai polinomo laipsnis $K = 1$ aproksimavimo paklaida yra gaunama komanda *stdev*

$$\text{stdev}(y1 - G) = 1.072 \times 10^3 .$$

Tačiau palyginę paklaidas, matome, kad jos yra sisteminės ir vidutinė paklaida didesnė negu aproksimuojant kubiniu polinomu.



7.3 pav. Pirminių skaičių priklausomybės nuo aproksimavimo tiese paklaidų kreivė

8. Atskyrimo pirminių skaičių nuo pseudopirminių metodas

Žinome, kad Ferma teoremą patenkina ir kai kurie ne pirminiai skaičiai (jų kelis šimtus kartų mažiau), tai visus gautuosius skaičius patikriname tiesiogiai dalydami juos iš visų nelyginių skaičių, mažesnių už pseudopirminio skaičiaus kvadratinę šaknį. Jei bent vienas dalmuo yra be liekanos, tai šiuos skaičius išmetame. Tarkime, kad intervalo pradžia

$$K1 = 1000001,$$

o ilgis

$$N := 50000, \quad n = 0..N$$

čia kintamasis $k1_n$ kinta žingsniu 2_n

$$k1_n = K1 + 2n,$$

o k_n yra vienetu mažesnis už $k1_n$:

$$k_n = k1_n - 1.$$

Aukščiausias laipsnis, kuris lygus logaritmo pagrindu 2 sveikąjai daliai $log_2 k_n = \frac{\ln(k_N)}{\ln(2)}$. Programa *MathCAD* užrašomas taip

$$J = floor\left(\frac{ln(k_N)}{ln(2)}\right).$$

$$j = 0..J, \quad J = 20.$$

$$K2 = k1_N.$$

Laikykime, kad intervalo pabaiga yra $K2 = 1100001$.

Tarkime, kad $\frac{k_n}{2^j}$ yra sveikosios santykio dalies modulis pagrindu 2. Programa *MathCAD* užrašome taip

$$s_{j,n} = mod\left(floor\left(\frac{k_n}{2^j}\right), 2\right).$$

$$m = 1..J, \quad q_{0,n} = 2.$$

$q_{m,n}$ – modulis, pagrindu $k1_n$. *MathCAD* išraiška yra tokia

$$q_{m,n} = mod\left[\left(q_{m-1,n}\right)^2, k1_n\right], \quad p_{0,n} = 1.$$

Čia $p_{m,n}$ yra modulis, pagrindu $k1_n$. Programa *MathCAD* užrašoma tokiu būdu

$$p_{m,n} = mod\left[p_{m-1,n}\left(q_{m,n}\right)^{s_{m,n}}, k1_n\right],$$

$$Q_n = p_{J,n}.$$

g yra matrica gauta sujungus dviejų matricų stulpelius į vieną matricą. Tai įvykdoma tokiu būdu

$$g = augment(k1, Q),$$

o $g1$ yra matrica gauta iš matricos g surūšiavus jos elementus didėjimo tvarka

$$g1 = csort(g, 1).$$

Panaudojame loginę komandą, kuri, kai patenkinta sąlyga $g1_{n,1} = 1$ tą vienetą palieka, o kai sąlyga $g1_{n,1} = 0$ nepatenkinta, ji verčiama nuliu

$$L := \sum_{n=0}^{N} \left(g1_{n,1} = 1\right) - 1,$$

$$L + 1 = 7.232 \cdot 10^3.$$

Paliekame stulpelio tik tą matricos dalį, kurios reikšmės lygios 1 ir jų skaičius lygus $L + 1$

$$g2 = submatrix(g1, 0, L, 0, 0).$$

o pirminius skaičius sudedame eilės tvarka

$$G = sort(g2), \quad l = 0..N,$$

Patikrinti ar duotasis skaičius $G`_l$ yra pirminis galima tokiu būdu: dalijame jį iš nelyginių skaičių nuo 3 iki $G`_l$ ir jeigu bent vieną kartą dalijant liekanos nelieka, tai tas daugiklis yra lygus nuliui, o visi kiti daugikliai lygūs vienetui. Taigi, jeigu ieškomasis skaičius nėra pirminis, tada sandauga yra lygi nuliui

$$w_l = \prod_{p=0}^{floor\left(\frac{\sqrt{G'_l}}{2}\right)} \left(mod\left(G'_l, 2p + 3\right) \neq 0\right).$$

Suskaičiuojame kiek yra nulinių sandaugų ir surūšiuojame pagal antrojo stulpelio, sudaryto iš vektoriaus $G`$ ir vektoriaus w_l didėjančias reikšmes

$$L' = \sum_{l=0}^{L} \left(w_l = 0\right), \quad L' = 16.$$

Po to atskiriame tą stulpelio dalį, kuri nusako pseudopirminius skaičius nuo tikrųjų pirminių skaičių

$$Gw = augment(G', w), \quad Gs = csort(Gw, 1).$$

nuo L` iki paskutinio

$$Pi = submatrix(Gs, L', L, 0, 0),$$

o Ps nuo nulio iki L`

$$Ps = submatrix(Gs, 0, L', -1, 0, 0).$$

8.1 lentelė. Tikrieji pirminiai skaičiai

	0
0	1000193
1	1000187
2	1000117
3	1000183
4	1000291
5	1000171
6	1000099
7	1000303
8	1000313
9	1000333
10	1000357
11	1000367
12	1000381
13	1000393
14	1000037
15	1000289
16	...

8.2 lentelė. MFT patenkinanti nepirminių skaičių dalis

	0
0	1082809
1	1092547
2	1023121
3	1024651
4	1073021
5	1052929
6	1093417
7	1082401
8	1004653
9	1064053
10	1052503
11	1018921
12	1050985
13	1016801
14	1033669
15	1053761

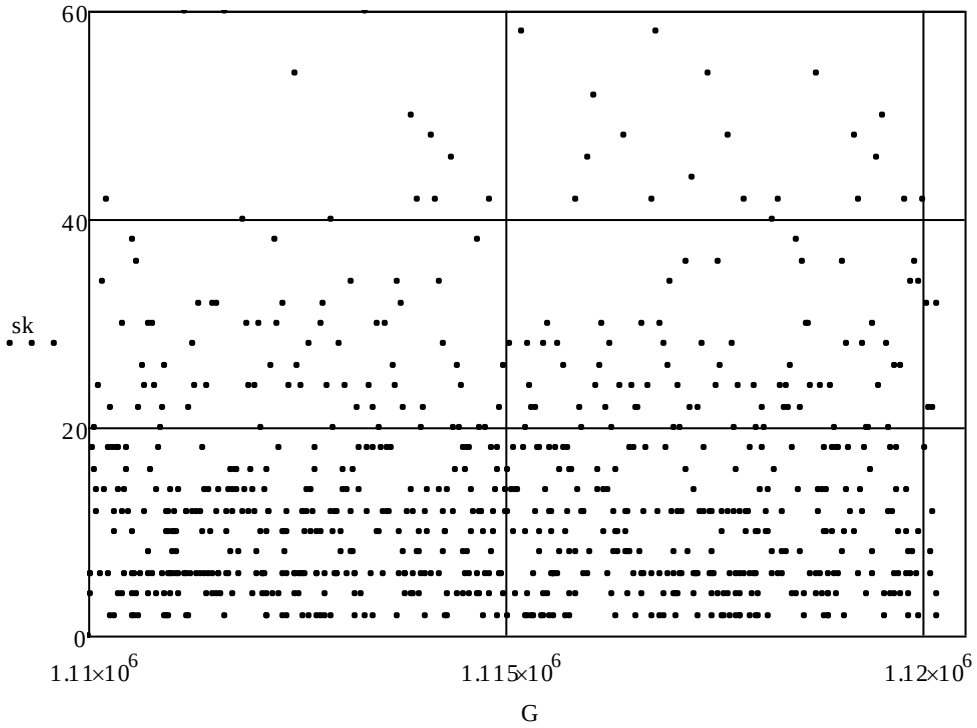
8.3 lentelė. Netikrieji pirminiai skaičiai

	0	1
0	1082809	0
1	1092547	0
2	1023121	0
3	1024651	0
4	1073021	0
5	1052929	0
6	1093417	0
7	1082401	0
8	1004653	0
9	1064053	0
10	1052503	0
11	1018921	0
12	1050985	0
13	1016801	0
14	1033669	0
15	1053761	0
16	1000193	1
17	1000187	1
18	1000117	1
19	1000183	1
20	1000291	1
21	1000171	...

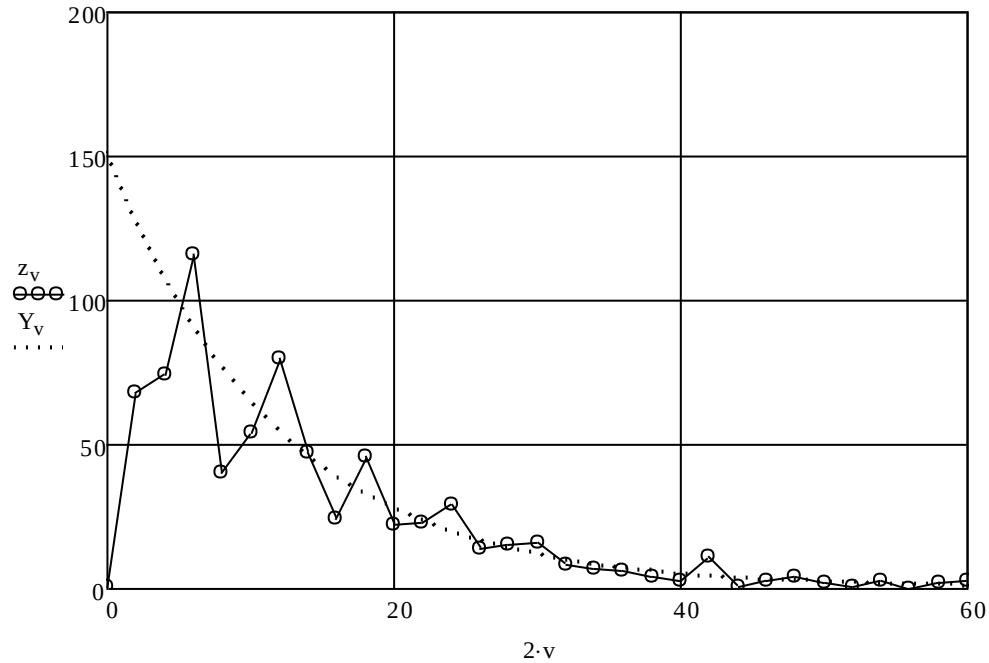
Ferma teoremą patenkinantys skaičiai sudėti į 8.3 lentelę, „įvertinti“ antrojo stulpelio nuline reikšme. Jie iškelti į 8.2 lentelę.

8.1. Netikrųjų („pirminių“), tikrųjų ir pseudopirminių skaičių pasiskirstymo grafinis palyginimas programa *MathCAD*

Palyginsime gautuosius „pirminių“, tikrųjų ir pseudopirminių skaičių pasiskirstymo grafinius vaizdus. Šiuo atveju pateikiami netikrųjų „pirminių“ skaičių grafikai

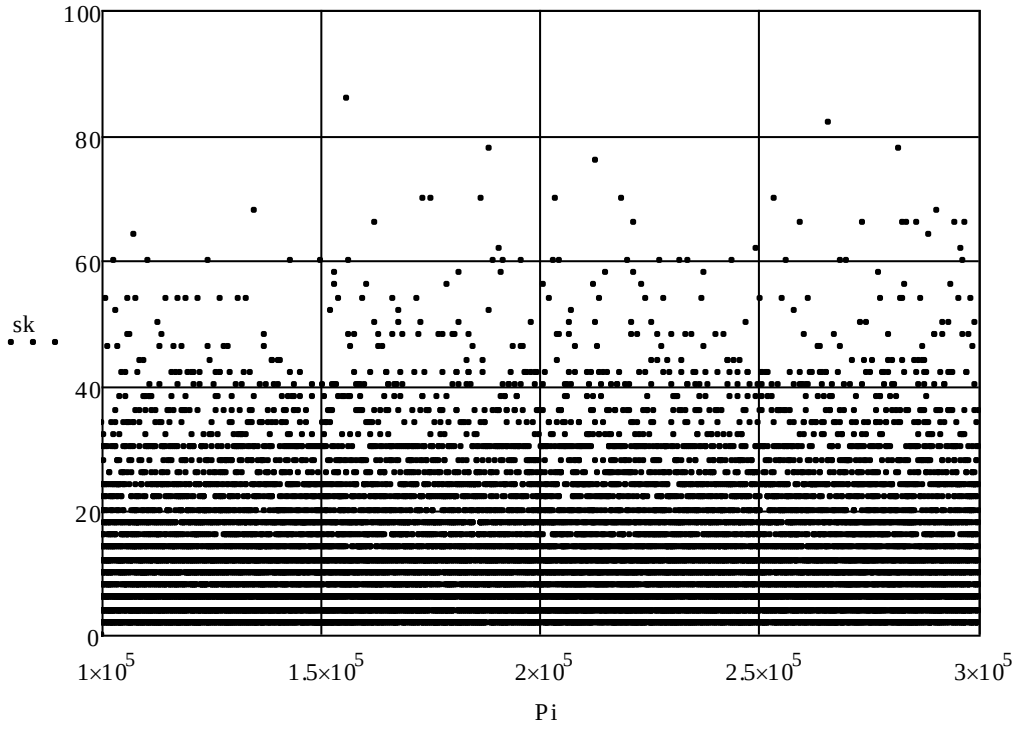


8.1.1 pav. Skirtumas tarp netikrų „pirminių“ skaičių

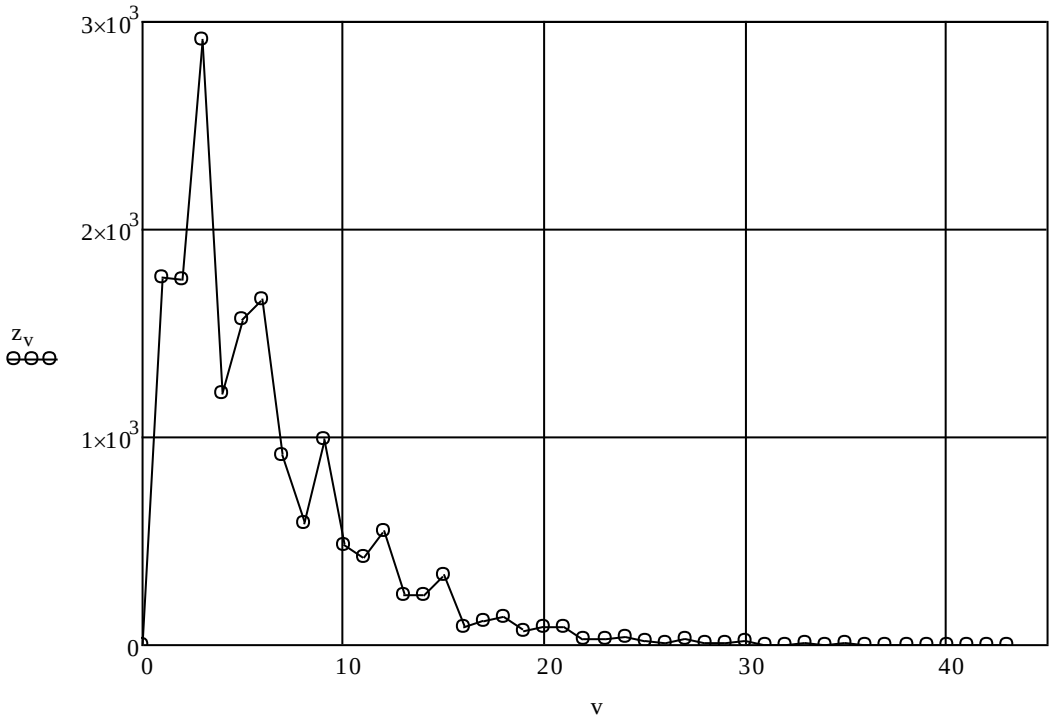


8.1.2 pav. Pasikartojančių tų pačių „netikrų“ pirminių skaičių skirtumai

Tikrųjų pirminių skaičių grafikai

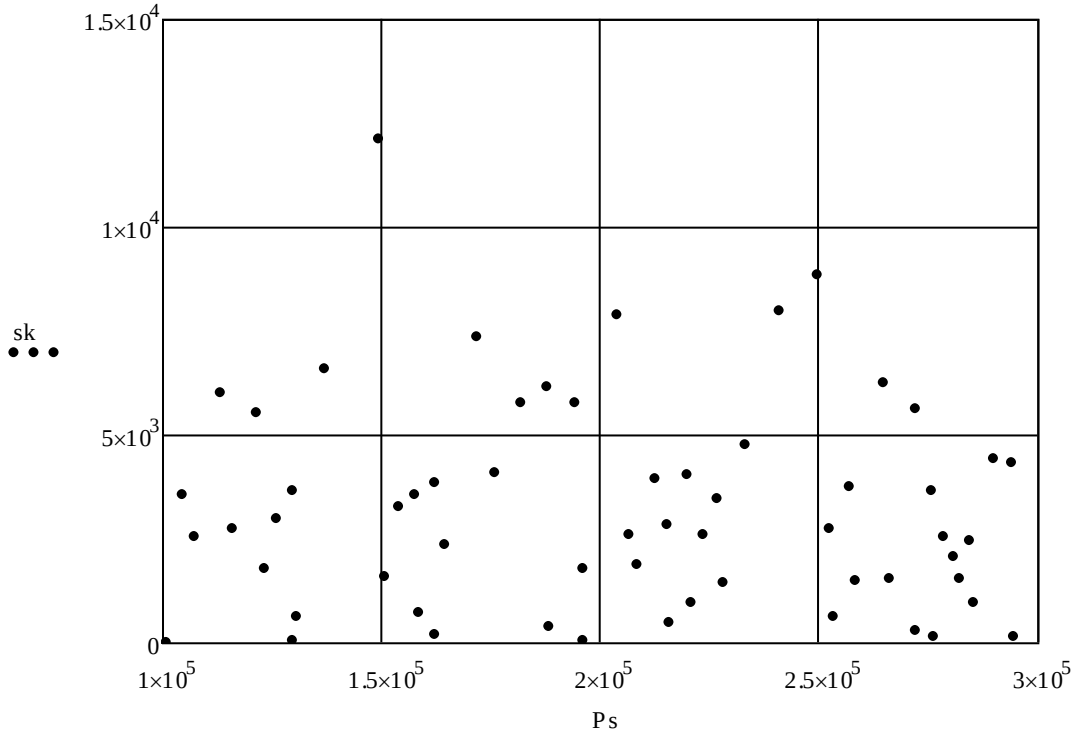


8.1.3 pav. Skirtumas tarp tikrų pirminių skaičių

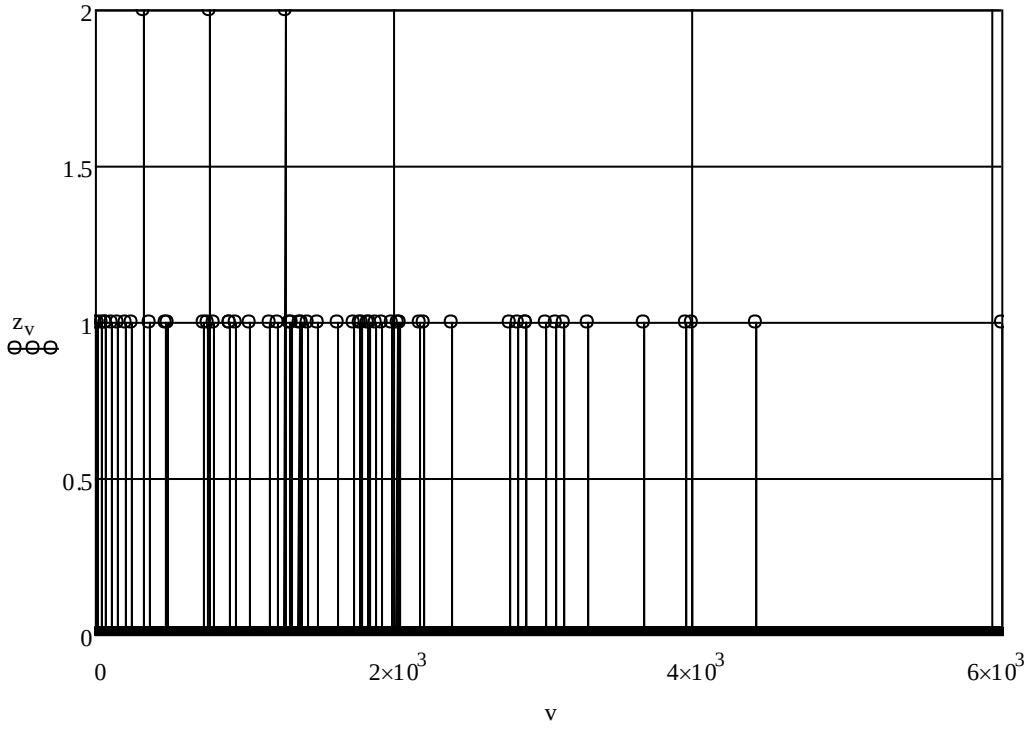


8.1.4 pav. Pasikartojančių tų pačių tikrų pirminių skaičių skirtumai

Pseudopirminių skaičių grafikai



8.1.5 pav. Skirtumas tarp pseudopirminių skaičių



8.1.6 pav. Pasikartojančių tų pačių pseudopirminių skaičių skirtumai

Kuo didesni skaičiai patenkinantys Ferma teoremą, tuo tarp jų mažiau nepirminių skaičių. Kai *K1=100.000* ir kai *K2=300.000*, tai santykis pirminių skaičių su pseudopirminiais yra *273*, o kai *K1=1.000.000* ir *K2=3.000.000*, tai *T/T'=720.401*.

Išvados

1. Remdamiesi Mažąja Ferma teorema ir atsijojimo procedūra, sudarėme patogią programą rasti daugeliui pirminių skaičių.
2. Radome ir pateikėme „pirminių“ skaičių išsidėstymo savybių grafinį vaizdą programa *MathCAD* (žr. 6.1 pav., 6.2 pav. ir 6.3 pav.).
3. Taip pat programa *MathCAD* pateikėme tikrųjų pirminių, netikrųjų („pirminių“) ir pseudopirminių skaičių pasiskirstymo palyginimui grafinį vaizdą.
4. Sugeneravus didelį kiekį pirminių skaičių, pastebėjome kad dažniausi skirtumai tarp gretimų pirminių skaičių yra ne dvejetai (Čano skaičiai), o šešetai ir jiems kartotiniai skaičiai (žr. 6.3.1 lentelė ir 6.2 pav.).

Šie metodai gali praversti analizuojant didelių grupių pirminių skaičių išsidėstymo savybes.

Summary

In this thesis by mathematical system *MathCAD* we created the program for finding large prime numbers. Also, we analysed distribution of unreal prime, pseudoprime and prime numbers.

Literatūra

1. A. Paukštienė, *Išmokime dirbti MathCAD programa,* Vilnius, 2006.
2. R. Kačinskaitė, A. Laurinčikas, *Pirminių skaičių pasiskirstymas,* Šiaulių universitetas, Šiauliai, 2003.
3. R. Skrabutėnas, *Algebra ir skaičių teorija. Konspektas 1,*Vilnius, 2004.
4. *МАЛАЯ ТЕОРЕМА ФЕРМА.* [Žiūrėta 2012 11 11]. Prieiga per internetą: <http://kvant.mccme.ru/1972/10/malaya_teorema_ferma.htm>.
5. *Pirminiai skaičiai.* [Žiūrėta 2012 10 29]. Prieiga per internetą: <http://www.spauda.lt/science/math/prime-numbers.htm>.
6. *5 tema. NIUTONO BINOMAS.* [Žiūrėta 2012 11 11]. Prieiga per internetą: <http://www.scribd.com/doc/100738865/2005-5-Niutono-Binomas-Ir-Jo-Taikymas>