VILNIAUS UNIVERSITETAS
MATEMATIKOS IR INFORMATIKOS FAKULTETAS
MATEMATIKOS MAGISTRANTŪROS STUDIJŲ PROGRAMA

Logaritmų tiesinės formos

Linear Forms in Logarithms

Baigiamasis magistro darbas

Atliko: Mantas Rasinskas
VU el. p.: mantas.rasinskas@mif.stud.vu.lt

Vadovas: Vyr. M. D. Habil. dr. Artūras Dubickas

Vilnius
2023

Turinys

Įvadas 2

1 Teorinė dalis **4**

1.1 Transcendentieji skaičiai 4

1.2 Teoremos apie tiesines logaritmų formas 4

1.3 Teoremos atsikratant logaritmų ir Tijdeman teorema 6

1.4 Papildoma teorija 11

2 Taikymai Diofanto lygtyse **16**

2.1 Catalan hipotezė 16

2.2 Kiti taikymai Diofanto lygtyse 17

Summary 25

Literatūra 26

Įvadas

Šiame magistro baigiamajame darbe aprašomos teoremos, išvados, teorija apie tiesines logaritmų formas ir kaip šios formos naudingai pritaikomos skaičių teorijoje Diofanto lygtyse, ypač eksponentinėse. Dalis teorijos remiasi faktais apie transcendenčiuosius, algebrinius skaičius. Dauguma Diofanto lygčių šiame darbe yra eksponentinės, kadangi po teoremų, tiesiogiai apibūdinančių logaritmų tiesines formas, galima gauti kitas teoremos, kurios vietoje logaritmų turi laipsnius. Naudojamasi, pvz., $\exp(b \log a) = a^b$, kur $a > 0$, $a, b \in \mathbb{R}$, išraiška $\log a$ pažymime $\ln a$. Tiesinių logaritmų formų taikymams, pvz., gaunami Diofanto lygčių sprendinių rėžiai, parodomas rėžių egzistavimas, įrodoma, jog egzistuoja baigtinis skaičius sprendinių, gaunami visi sprendiniai ir pan. Didelis dėmesys skiriamas Catalan hipotezei, kuri dabar yra teorema.

1 skyrius

Teorinė dalis

1.1 Transcendentieji skaičiai

Dalis šio 1.1 poskyrio teorijos yra [8] 1 psl.

Transcendentusis skaičius yra (galimai kompleksinis) skaičius, kuris nėra jokio sveikojo daugianario šaknis. Jis nėra jokio laipsnio algebrinis skaičius (žr. [30]).

1 teorema. *Tegul α, β algebriniai skaičiai aibėje $\mathbb{C}$, kur taip pat $\alpha \neq 0$, $\alpha \neq 1$ ir $\beta \notin \mathbb{Q}$. Tada α^β yra transcendentusis.*

1 teoremą įrodė Gel'fond ir Schneider 1934 metais (žr. [8] ir [17]). Čia $\alpha^\beta := e^{\beta \ln \alpha}$, kur $e^z = \sum_{n=0}^{\infty} \frac{z^n}{n!}$ ir $\ln \alpha = \ln |\alpha| + i \arg(\alpha)$. Skaičiaus α argumentas yra nustatytas tik iki 2π kartotinio. Todėl $\ln \alpha$ ir α^β yra daugiareikšmiai. 1 teorema galioja bet kokiai pasirinktai $\arg \alpha$ reikšmei.

2 išvada. *Tegul β yra algebrinis skaičius iš aibės $\mathbb{C}$ su $i\beta \notin \mathbb{Q}$. Tada $e^{\pi\beta}$ yra transcendentusis.*

Įrodymas. $e^{\pi\beta} = e^{\pi i \cdot (-i\beta)} = (-1)^{-i\beta}$. Tada pasinaudokime 1 teorema. □

1.2 Teoremos apie tiesines logaritmų formas

Dalis šio 1.2 poskyrio teorijos yra [8] 1, 2 psl.

Kai duotas žiedo $\mathbb{C}$ požiedis R (pvz., $\mathbb{Z}$, $\mathbb{Q}$, algebrinių skaičių kūnas), sakome, jog kompleksiniai skaičiai $\theta_1, \ldots, \theta_m$ yra vadinami tiesiškai nepriklausomais virš R, jei lygtis $x_1\theta_1 + \cdots + x_m\theta_m = 0$ neturi sprendinių $(x_1, \ldots, x_m) \in R^m \setminus \{\mathbf{0}\}$ (žr. [8]).

3 išvada. *Tegul α, β yra algebriniai skaičiai iš $\mathbb{C} \setminus \{0; 1\}$ ir yra tokie, kad $\log\alpha$, $\log\beta$ yra tiesiškai nepriklausomi virš $\mathbb{Q}$. Tada visiems nenuliniams algebriniems skaičiams γ, δ iš aibės $\mathbb{C}$ turime, jog $\gamma\log\alpha + \delta\log\beta \neq 0$.*

Įrodymas. Įrodysime išvadą prieštaros būdu. Tariame, kad $\gamma\log\alpha + \delta\log\beta = 0$. Tada $\log\alpha = -(\delta/\gamma)\log\beta$, todėl $\alpha = \beta^{-\delta/\gamma}$. Pagal 1 teoremą tai gali būti tik tada, kai $a := \delta/\gamma \in \mathbb{Q}$. Bet tuomet $\log\alpha - a\log\beta = 0$, prieštara prielaidai. □

Sekanti teorema yra Baker apibendrinimas tiesinėms bet kokio kiekio algebrinių skaičių logaritmų formoms. Ji įrodyta Baker 1966 metais.

4 teorema. *Tegul $\alpha_1, \ldots, \alpha_m$ yra algebriniai skaičiai iš $\mathbb{C} \setminus \{0; 1\}$ ir yra tokie, kad $\log\alpha_1, \ldots, \log\alpha_m$ yra tiesiškai nepriklausomi virš $\mathbb{Q}$. Tada bet kokiam algebrinių skaičių iš $\mathbb{C}$ rinkiniui $(\beta_0, \beta_1, \ldots, \beta_m)$ $((\beta_0, \beta_1, \ldots, \beta_m) \neq (0, 0, \ldots, 0))$ turime, jog*

$$\beta_0 + \beta_1\log\alpha_1 + \cdots + \beta_m\log\alpha_m \neq 0.$$

Taikymams Diofanto uždaviniuose yra svarbu, kad ne tik 4 teoremos tiesinė forma yra nenulinė, bet ir tai, jog turime pakankamai stiprų šitos tiesinės formos modulio apatinį rėžį. Sekanti teorema, įrodyta Baker 1975 metais, nurodo atskirą atvejį, kai $\beta_0 = 0$ ir $\beta_1, \ldots, \beta_m$ yra racionalūs sveikieji skaičiai (t. y. tiesiog sveikieji skaičiai aibėje $\mathbb{Z}$ (žr. [31])).

5 teorema. *Tegul $\alpha_1, \ldots, \alpha_m$ yra algebriniai skaičiai iš $\mathbb{C} \setminus \{0; 1\}$. Be to, tegu $b_1, \ldots, b_m$ yra racionalūs sveikieji skaičiai tokie, kad*

$$b_1\log\alpha_1 + \cdots + b_m\log\alpha_m \neq 0.$$

Tada

$$|b_1\log\alpha_1 + \cdots + b_m\log\alpha_m| \geq (eB)^{-C},$$

kur $B := \max(|b_1|, \ldots, |b_m|)$ ir C yra efektyviai apskaičiuojama konstanta, priklausanti tik nuo m ir nuo $\alpha_1, \ldots, \alpha_m$.

1.3 Teoremos atsikratant logaritmų ir Tijdeman teorema

Dalis šio 1.3 poskyrio teorijos yra [8] 2-6, 13 psl.

Galima atsikratyti logaritmų. 5 teorema veda į sekančią išvadą: u

6 išvada. *Tegul $\alpha_1, \ldots, \alpha_m$ yra algebriniai skaičiai iš $\mathbb{C} \setminus \{0; 1\}$ ir tegu $b_1, \ldots, b_m$ yra racionalūs sveikieji skaičiai tokie, kad*

$$\alpha_1^{b_1} \cdots \alpha_m^{b_m} \neq 1.$$

Tada

$$\left|\alpha_1^{b_1} \cdots \alpha_m^{b_m} - 1\right| \geq (eB)^{-C'},$$

kur vėl $B := \max(|b_1|, \ldots, |b_m|)$ ir kur C' yra efektyviai apskaičiuojama konstanta, priklausanti tik nuo m bei nuo $\alpha_1, \ldots, \alpha_m$.

Įrodymas. Kompleksinio skaičiaus z logaritmui pasirenkame $\log z = \log|z| + i \arg z$ su $-\pi < \arg z \leq \pi$. Su šiuo log pasirinkimu turime, kad $\log(1+w) = \sum_{n=1}^{\infty} \frac{(-1)^{n-1} w^n}{n}$ skaičiui $w \in \mathbb{C}$ su $|w| < 1$ (realiesiems skaičiams šis laipsninės eilutės skleidinys yra įrodytas 1.4 poskyrio 20 teoremos įrodyme). Naudojantis šiuo laipsninės eilutės skleidiniu galima lengvai parodyti, jog

$$|\log(1+w)| \leq 2|w|, \text{ jei } |w| \leq \frac{1}{2}$$

(pilnas įrodymas yra 1.4 poskyrio 20 teoremos įrodyme). Panaudojame tai su $w := \alpha_1^{b_1} \cdots \alpha_m^{b_m} - 1$. Jei $|w| > \frac{1}{2}$, tai įrodymas baigtas, kadangi

$$|w| > \frac{1}{2} > \frac{1}{e \cdot 1} \geq \frac{1}{eB} = (eB)^{-1}, \; C' = 1,$$

nes $B \geq 1$ ($B := \max(|b_1|, \ldots, |b_m|)$, $b_1, \ldots, b_m \in \mathbb{Z}$, $(b_1, \ldots, b_m) \neq (0, \ldots, 0)$ ($\alpha_1^{b_1} \cdots \alpha_m^{b_m} \neq 1$)). Praeitas sakinys yra dalis baigiamojo darbo uždavinio (paaiškinti teoriją). Pamatymui, kas yra paaiškinta teorijoje kaip dalis baigiamojo darbo uždavinio, reikia palyginti įrodymo užrašą Evertse straipsnyje [8] 2, 3 psl. su šiuo baigiamojo darbo įrodymu. Tarkime, kad $|w| \leq \frac{1}{2}$. Turime rasti apatinį $|\log(1+w)|$ rėžį.

Prisiminkime, kad kompleksinis logaritmas yra adityvus tik modulo $2\pi i$. T. y.

$$\log(1+w) = b_1 \log \alpha_1 + \cdots + b_m \log \alpha_m + 2k\pi i$$

kažkokiam $k \in \mathbb{Z}$ ($e^{2k\pi i} = \cos(2k\pi) + i \cdot \sin(2k\pi) = 1 + i \cdot 0 = 1$). Galima panaudoti 5 teoremą, kadangi $2k\pi i = 2k \log(-1)$ ($e^{\pi i} = \cos(\pi) + i \cdot \sin(\pi) = -1 + i \cdot 0 = -1$). Todėl gauname, jog

$$|\log(1+w)| \geq (e \max(B, |2k|))^{-C_1},$$

kur C_1 yra efektyviai apskaičiuojama konstanta, priklausanti tik nuo m bei nuo $\alpha_1, \ldots, \alpha_m$. Kadangi $|\log(1+w)| \leq 2|w| \leq 1$, tai turime, kad (trikampio nelygybės panaudojimas yra sugalvotas kaip dalis baigiamojo darbo uždavinio (paaiškinti teoriją))

$$|2k\pi i| = |\log(1+w) - b_1 \cdot \log \alpha_1 - \ldots - b_m \cdot \log \alpha_m| \overset{\text{trikampio nelygybė}}{\leq} |\log(1+w)| +$$

$$+|b_1 \cdot \log \alpha_1| + \ldots + |b_m \cdot \log \alpha_m| = |\log(1+w)| + |b_1| \cdot |\log \alpha_1| + \ldots + |b_m| \cdot |\log \alpha_m| \leq$$

$$\leq 1 + |b_1| \cdot |\log \alpha_1| + \ldots + |b_m| \cdot |\log \alpha_m| = \underbrace{1}_{\leq B} + \sum_{j=1}^{m} |\log \alpha_j| \cdot |b_j| \leq \left(1 + \sum_{j=1}^{m} |\log \alpha_j|\right) B$$

($B \geq 1$, $B \geq |b_i|$, $i \in \{1, 2, \ldots, m\}$). Vadinasi, $|2k| \leq C_2 B \leq C_3 B$, kur $C_2 = \frac{1 + \sum_{j=1}^{m} |\log \alpha_j|}{|\pi i|}$ bei $C_3 = \max(C_2, 1) \geq 1$. Suprantame, kad $C_1 \geq 0$, nes 5 teoremoje, įrodytoje Baker 1975 m., suprantame, jog $C \geq 0$.

$$(e \max(B, |2k|))^{-C_1} = \frac{1}{(e \max(B, |2k|))^{C_1}} \geq$$

$$\geq \frac{1}{(e \max(B, C_3 B))^{C_1}} = \frac{1}{(eC_3 B)^{C_1}} = (eC_3 B)^{-C_1}.$$

Taigi

$$|\log(1+w)| \geq (e \max(B, |2k|))^{-C_1} \geq (eC_3 B)^{-C_1}.$$

$$|\log(1+w)| \geq (eC_3 B)^{-C_1}.$$

$$2|w| \geq |\log(1+w)| \geq (eC_3 B)^{-C_1}.$$

Tai parodo, kad

$$|w| \geq \frac{1}{2} \cdot (eC_3 B)^{-C_1}.$$

Lieka įrodyti, kad

$$\frac{1}{2}(eC_3 B)^{-C_1} \geq (eB)^{-C'}$$

tinkamam C'. Šio C' suradimas yra dalis baigiamajomo darbo uždavinio (paaiškinti teoriją). Parodysiu, kad

$$C' := C_1 + \underbrace{C_1}_{\geq 0} \ln \underbrace{C_3}_{\geq 1} + \ln 2$$

tinka.

$$(eB)^{-C'} = (eB)^{-(C_1+C_1\ln C_3+\ln 2)} =$$

$$= (eB)^{-C_1}(eB)^{-(C_1\ln C_3+\ln 2)} = (eB)^{-C_1}(eB)^{-\frac{C_1\ln C_3+\ln 2}{\ln(e\cdot 1)}} \leq$$

$$\leq (eB)^{-C_1}(eB)^{-\frac{C_1\ln C_3+\ln 2}{\ln(e\cdot B)}} = (eB)^{-C_1}(eB)^{-\frac{C_1\ln C_3-\ln\frac{1}{2}}{\ln(e\cdot B)}} =$$

$$= (eB)^{-C_1}(eB)^{-\frac{\ln C_3^{C_1}-\ln\frac{1}{2}}{\ln(e\cdot B)}} = (eB)^{-C_1}(eB)^{-\frac{\ln\frac{C_3^{C_1}}{\frac{1}{2}}}{\ln(e\cdot B)}} =$$

$$= (eB)^{-C_1}(eB)^{-\log_{eB}\left(\frac{C_3^{C_1}}{\frac{1}{2}}\right)} = (eB)^{-C_1}\frac{1}{(eB)^{\log_{eB}\left(\frac{C_3^{C_1}}{\frac{1}{2}}\right)}} =$$

$$= (eB)^{-C_1}\frac{1}{\left(\frac{C_3^{C_1}}{\frac{1}{2}}\right)} = (eB)^{-C_1}\frac{1}{2C_3^{C_1}} =$$

$$= (eB)^{-C_1}\cdot\frac{1}{2}\cdot C_3^{-C_1} = \frac{1}{2}(eC_3B)^{-C_1}.$$

Tą ir reikėjo įrodyti. □

Sekanti teorema, įrodyta Matveev 2000 metais, yra 6 išvados versija atveju, kai $\alpha_1,\ldots,\alpha_m \in \mathbb{Z}$. Racionalaus skaičiaus $a = \frac{x}{y}$ su $x, y \in \mathbb{Z}$, $\mathrm{DBD}(x,y) = 1$ *aukščiu* vadiname $H(a) := \max(|x|,|y|)$. Aukštis kitoje literatūroje gali būti labiau apibendrintas (žr. [24] antro skyriaus pirmą ir antrą sakinius) (aukščio paaiškinimas ir apibendrinimas yra sugalvoti kaip dalis baigiamojo darbo uždavinio (paaiškinti teoriją)). Dabar apibrėžiu apibendrintą aukštį. Tegul d yra algebrinis skaičius. Pažymime išraiška $P(X) = d_0X^D + \ldots + d_D$ skaičiaus d minimalų daugianarį virš $\mathbb{Z}$ (žr. [28]). Tada skaičiaus d „įprastas aukštis“ yra

$$H(d) = \max_{0\leq j\leq D}|d_j|.$$

Apibrėžimą baigiau. $a = \frac{x}{y}$ yra algebrinis skaičius su minimaliu daugianariu virš $\mathbb{Z}$ (žr. [28]) esančiu $P(X) = yX - x$, kur daugianario koeficientai yra y, $-x$. Tada a aukštis yra $H(a) = \max(|y|,|-x|) = \max(|x|,|y|)$.

7 teorema. *Tegul $a_1,\ldots,a_m \in \mathbb{Q}_{\neq 0}$ ir tegu $b_1,\ldots,b_m \in \mathbb{Z}$ yra tokie, kad*

$$a_1^{b_1}\cdots a_m^{b_m} \neq 1.$$

Tada $\left|a_1^{b_1}\cdots a_m^{b_m} - 1\right| \geq (eB)^{-C'}$, kur

$$B = \max(|b_1|,\ldots,|b_m|),$$

$$C' = \frac{1}{2}e\cdot m^{4,5}30^{m+3}\prod_{j=1}^{m}\max(1,\log H(a_j)).$$

8 išvada. *Tegul $a, b \in \mathbb{N}_{\geq 2}$. Tada egzistuoja efektyviai apskaičiuojamas skaičius $C_1 > 0$, priklausantis tik nuo a, b, toks, kad bet kokiem dviem $m, n \in \mathbb{N}_{\geq 1}$ turime, jog*

$$|a^m - b^n| \geq \frac{\max(a^m, b^n)}{(e \max(m,n))^{C_1}}.$$

9 išvada. *Bet kokiam $k \in \mathbb{Z}_{\neq 0}$ egzistuoja efektyviai apskaičiuojamas skaičius C_2, priklausantis nuo a, b, k, toks, kad jei $m, n \in \mathbb{N}_{\geq 1}$ su $a^m - b^n = k$, tai $m, n \leq C_2$. Taigi egzistuoja baigtinis skaičius sprendinių m, n.*

8, 9 išvadų įrodymai. Tegul $m, n \in \mathbb{N}_{\geq 1}$, $B := \max(m, n)$. Neprarasdami bendrumo tarkime, kad $a^m \geq b^n$. Pagal 6 išvadą arba 7 teoremą turime, jog

$$\left|1 - b^n a^{-m}\right| \geq (eB)^{-C_1},$$

kur C_1 yra efektyviai apskaičiuojamas skaičius, priklausantis tik nuo a, b. Padauginę iš a^m gauname 8 išvadą.

Dabar tegul $m, n \in \mathbb{N}_{\geq 1}$ su $a^m - b^n = k$. Tegu vėl $B := \max(m, n)$. Tada, kadangi $a, b \geq 2$,

$$|k| \geq 2^B \cdot (eB)^{-C_1}.$$

Tai įrodo, jog B yra aprėžtas iš viršaus su rėžiu, kuris yra efektyviai apskaičiuojamas skaičius, priklausantis nuo a, b, k. Gauname 9 išvadą. □

Pasižiūrėkime į seką $\{a_n\}$ su $a_n = 2^n$, $n = 0, 1, 2, \ldots$. Pastebėkime, kad $a_{n+1} - a_n = a_n$. Panašiai galime pasižiūrėti į didėjančią skaičių, sudarytų iš pirminių skaičių iš $\{2, 3\}$, seką $\{a_n\}$, t. y. $1, 2, 3, 4, 6, 8, 9, 12, 16, 18, 24, 27, 32, \ldots$, ir paklausti, kaip galima palyginti tarpą $a_{n+1} - a_n$ su a_n, kai $n \to \infty$. Galime apibendrinti ir paimti baigtinę pirminių skaičių aibę. Galime paklausti analogišką klausimą apie iš eilės einančių sveikųjų skaičių seką, sudarytą iš tų pirminių skaičių. Sekanti teorema buvo įrodyta Tijdeman 1974 metais.

10 teorema. *Tegul $S = \{p_1, \ldots, p_t\}$ yra baigtinė skirtingų pirminių skaičių aibė ir tegu $a_1 < a_2 < a_3 < \cdots$ yra iš eilės einančių teigiamų sveikųjų skaičių, sudarytų iš pirminių skaičių iš S, seka. Tada egzistuoja efektyviai apskaičiuojami teigiami skaičiai c_1, c_2, priklausantys nuo $t, p_1, \ldots, p_t$, tokie, kad*

$$a_{n+1} - a_n \geq \frac{a_n}{c_1 (\log a_n)^{c_2}}$$

skaičiams $n = 1, 2, \ldots$.

Įrodymas. Turime, kad $a_n = p_1^{k_1} \cdots p_t^{k_t}$ ir $a_{n+1} = p_1^{l_1} \cdots p_t^{l_t}$ su $k_i, l_i \in \mathbb{Z}_{\geq 0}$. Pagal 6 išvadą gauname, jog

$$\left| \frac{a_{n+1}}{a_n} - 1 \right| = \left| p_1^{l_1 - k_1} \cdots p_t^{l_t - k_t} - 1 \right| \geq (eB)^{-C},$$

kur $B := \max(|l_1 - k_1|, \ldots, |l_t - k_t|)$. Pirma pastebėkime, kad

$$k_i \leq \frac{\log a_n}{\log p_i} \leq \frac{\log a_n}{\log 2}$$

skaičiams $i = 1, \ldots, t$. Dar žinome, jog $a_{n+1} \leq a_n^2$. Todėl

$$l_i \leq \frac{\log a_{n+1}}{\log p_i} \leq \frac{\log a_n^2}{\log 2}$$

skaičiams $i = 1, \ldots, t$. Vadinasi, $B \leq \frac{2 \log a_n}{\log 2}$. Todėl $a_{n+1} - a_n \geq a_n \left(\frac{2e \log a_n}{\log 2} \right)^{-C}$. $\square$

Dauguma Diofanto aproksimacijų rezultatų, kurie buvo įrodyti algebriniems skaičiams iš $\mathbb{C}$, turi analogą p-adiniams skaičiams. Galime apibrėžti p-adinį kėlimą laipsniu, p-adinius logaritmus ir t. t., ir tai leidžia mums suformuluoti analogus 1-7 teoremoms/išvadoms p-adinėje situacijoje. Parodome 6 išvados analogą tuo atveju, kai $\alpha_1, \ldots, \alpha_m \in \mathbb{Q}$. Egzistuoja bendresnė versija algebriniems $\alpha_1, \ldots, \alpha_m$, bet tą teiginį sunkiau suformuluoti. Sekanti teorema buvo įrodyta Yu 1986 metais.

11 teorema. *Tegul p yra pirminis skaičius ir tegu $a_1, \ldots, a_m \in \mathbb{Q}_{\neq 0}$ yra tokie, kad $p \nmid a_1 a_2 \cdots a_m$. Tegul $b_1, \ldots, b_m \in \mathbb{Z}$ yra tokie, kad*

$$a_1^{b_1} \cdots a_m^{b_m} \neq 1.$$

Tegu $B := \max(|b_1|, \ldots, |b_m|)$. Tada

$$\left| a_1^{b_1} \cdots a_m^{b_m} - 1 \right|_p \geq (eB)^{-C},$$

kur C yra efektyviai apskaičiuojamas skaičius, priklausantis nuo p, m bei nuo $a_1, \ldots, a_m$.

Kai $m \geq 2$, tai 11 teoremos įrodymas yra labai sudėtingas. Kai $m = 1$, tai egzistuoja stipresnis rezultatas (žr. sekančią teoremą), kuris gali būti įrodytas elementariai.

12 teorema. *Tegul $a \in \mathbb{Z}$, p yra pirminis skaičius ir a, p yra tokie, kad $|a|_p \leq p^{-1}$, jei $p > 2$, ir $|a|_2 \leq 2^{-2}$, jei $p = 2$. Tada bet kokiam $b \in \mathbb{N}_{\geq 1}$ turime, jog*

$$\left| (1 + a)^b - 1 \right|_p = |ab|_p \geq \frac{1}{ab}.$$

1.4 Papildoma teorija

13 teorema. *Apibrėžiame*

$$\mathbb{Z}_S^* = \{\pm p_1^{z_1} \cdots p_t^{z_t} \ : \ z_1, \ldots, z_t \in \mathbb{Z}\},$$

kur $S = \{p_1, \ldots, p_t\}$ *yra baigtinė pirminių skaičių aibė. Tada lygtis*

$$x + y = 1$$

su kintamaisiais $x, y \in \mathbb{Z}_S^*$ *turi baigtinį skaičių sprendinių, ir jos sprendinių aibė gali būti nustatyta efektyviai (žr. [8] 7 psl.).*

Įrodymas. Tegul (x, y) yra sprendinys. Galime užrašyti $x = \frac{u}{w}$, $y = \frac{v}{w}$, kur $u, v, w \in \mathbb{Z}$ su $\gcd(u, v, w) = 1$. Tada

$$u + v = w.$$

Sveikieji skaičiai u, v, w yra sudaryti iš pirminių skaičių iš S, ir taip pat joks pirminis nedalija dviejų skaičių tarp u, v, w, nes $\gcd(u, v, w) = 1$ (pvz., jei dėl prieštaros $p \mid u, w$, tai $p \mid w - u = v$, $p \mid u, w, v$, $\gcd(u, v, w) \geq p > 1$, prieštara). Po pirminių skaičių $p_1, \ldots, p_t$ pertvarkymų galime tarti, kad

$$u = \pm p_1^{b_1} \cdots p_r^{b_r},$$

$$v = \pm p_{r+1}^{b_{r+1}} \cdots p_s^{b_s},$$

$$w = \pm p_{s+1}^{b_{s+1}} \cdots p_t^{b_t},$$

kur $0 \leq r \leq s \leq t$ ir $b_i \in \mathbb{Z}_{\geq 0}$ (tuščios sandaugos yra lygios 1; pvz., jei $r = 0$, tai $u = \pm 1$). Turime įrodyti, jog $B := \max(b_1, \ldots, b_t)$ yra aprėžtas iš viršaus efektyviai apskaičiojamu skaičiumi, priklausomu tik nuo $p_1, \ldots, p_t$. Pagal simetriją, galime tarti, kad $B = b_t$. Tada naudodamiesi $-\frac{u}{v} - 1 = -\frac{w}{v}$ gauname, jog

$$0 < \left|\pm p_1^{b_1} \cdots p_r^{b_r} p_{r+1}^{-b_{r+1}} \cdots p_s^{-b_s} - 1\right|_{p_t} =$$

$$= \left|\frac{w}{v}\right|_{p_t} = p_t^{-b^t} = p_t^{-B}.$$

Iš 11 teoremos gauname, kad

$$|\cdots|_{p_t} \geq (eB)^{-C},$$

kur C yra efektyviai apskaičiuojamas pagal $p_1, \ldots, p_t$. Vadinasi,

$$(eB)^{-C_2} \leq p_t^{-B}.$$

Todėl iš tikrųjų B yra aprėžtas iš viršaus efektyviai apskaičiuojamu skaičiumi, priklausančiu nuo $p_1, \ldots, p_t$. □

Pastaba: 1988 metais savo daktaro disertacijoje de Weger davė praktinį algoritmą, paremtą stipriomis tiesinių logaritmų formų nelygybėmis ir LLL-bazės redukcijos algoritmu, išspręsti 13 teoremoje nurodytos lygties tipo lygtis. Taip jis parodė, jog lygtis $x + y = z$ turi lygiai 545 sprendinius $x, y, z \in \mathbb{N}_{\geq 1}$ su $x \leq y$ bei su forma $2^{b_1}3^{b_2}5^{b_3}7^{b_4}11^{b_5}13^{b_6}$ su $b_i \in \mathbb{Z}$ (žr. [8] 8 psl.).

14 teorema. *Tegul $F(X, Y) = a_0X^d + a_1X^{d-1}Y + \cdots + a_dY^d$ yra dvejetainė forma iš $\mathbb{Z}[X, Y]$ tokia, kad $F(X, 1)$ turi bent tris skirtingas šaknis aibėje $\mathbb{C}$, ir tegu $m \in \mathbb{Z}_{\neq 0}$. Tada lygtis*

$$F(x, y) = m$$

su kintamaisiais $x, y \in \mathbb{Z}$ turi baigtinį skaičių sprendinių, ir jos sprendinių aibė gali būti nustatyta efektyviai (žr. [8] 8 psl.).

15 teorema. *Tegul $f(X) \in \mathbb{Z}[X]$ yra daugianaris be kartotinių šaknų ir $n \in \mathbb{N}_{\geq 2}$. Tegu f turi bent du nulius aibėje $\mathbb{C}$, jei $n \geq 3$, ir bent tris nulius aibėje $\mathbb{C}$, jei $n = 2$. Tada lygtis*

$$y^n = f(x)$$

su kintamaisiais $x, y \in \mathbb{Z}$ turi baigtinį skaičių sprendinių, ir jos sprendinių aibė gali būti nustatyta efektyviai (žr. [8] 8 psl.).

Remiantis [8] teorija galima įrodyti sekančias tris teoremas. Jas galima rasti [8] 11, 12 psl.

16 teorema. *Tegul $p_1, \ldots, p_s, p_{s+1}, \ldots, p_t$ yra skirtingi pirminiai skaičiai. Tegu A yra teigiamų sveikųjų skaičių, sudarytų iš pirminių skaičių $p_1, \ldots, p_s$, aibė, ir tegul B yra teigiamų sveikųjų skaičių, sudarytų iš pirminių skaičių $p_{s=1}, \ldots, p_t$, aibė. Tada yra teisingi sekantys (a) ir (b) teiginiai.*

(a) Egzistuoja efektyviai apskaičiuojami pagal $p_1, \ldots, p_t$ teigiami skaičiai c_1, c_2 tokie, kad

$$|x - y| \geq \frac{\max(x, y)}{c_1(\log \max(x, y))^{c_2}}, \ \forall x \in A, y \in B.$$

(b) Kai duotas $a \in \mathbb{Z}_{\neq 0}$, pažymėkime užrašu $P(a)$ didžiausią pirminį skaičių, dalijantį a, su $P(\pm 1) := 1$. Tada

$$\lim_{x\in A, y\in B, \max(|x|,|y|)\to\infty} P(x-y) = \infty.$$

17 teorema. *Tegul $f(X) = X^2 - AX - B$ yra (antro laipsnio) daugianaris su koeficientais $A, B \in \mathbb{Z}$. Tegu α, β yra du funkcijos f nuliai aibėje $\mathbb{C}$. Tegul f yra neredukuojamas ir tegu $\frac{\alpha}{\beta}$ nėra vienybės šaknis, t. y. $\frac{\alpha}{\beta} \neq \pm 1$ ($x^2 - 1 = (x-1)(x-(-1))$) (sekančioje 18 teoremoje vienybės šaknys yra ne tokios trivialios, nes ten trečio, o ne antro, laipsnio daugianaris). Tegul seka $U = \{u_n\}_{n=0}^{\infty}$ aibėje $\mathbb{Z}$ yra tokia, kad*

$$u_n = Au_{n-1} + Bu_{n-2} \quad (n \geq 0),$$

ir tegu šios sekos pradinės reikšmės yra $u_0, u_1 \in \mathbb{Z}$ su $u_0^2 + u_1^2 \neq 0$ (negalioja $u_0 = u_1 = 0$).

(a) Tada $M := \max(|\alpha|, |\beta|) > 1$.

(b) Tuomet egzistuoja nenuliniai algebriniai skaičiai γ_1, γ_2 tokie, kad $u_n = \gamma_1\alpha^n + \gamma_2\beta^n$ skaičiams $n \geq 0$.

(c) Tada egzistuoja efektyviai apskaičiuojamas skaičius C toks, kad $u_n \neq 0$ skaičiams $n \geq C$.

(d) Tuomet egzistuoja efektyviai apskaičiuojami teigiami skaičiai c_1, c_2 tokie, kad $|u_n| \geq \frac{M^n}{c_1 n^{c_2}}$ skaičiams $n \geq C$.

18 teorema. *Tegul $A, B, C \in \mathbb{Z}$ tokie, kad $C \neq 0$ ir*

$$X^3 - AX^2 - BX - C = (X-\alpha_1)(X-\alpha_2)(X-\alpha_3),$$

kur $\alpha_1, \alpha_2, \alpha_3 \in \mathbb{C}$, ir nei vienas iš dalmenų $\frac{\alpha_i}{\alpha_j}$ ($1 \leq i < j \leq 3$) nėra vienybės šaknis, t. y. $\frac{\alpha_i}{\alpha_j} \notin \{1, \frac{-1\pm i\sqrt{3}}{2}\}$ ($1 \leq i < j \leq 3$) ($x^3 - 1 = (x-1)\,(x^2+x+1) = (x-1)\left(x - \left(\frac{-1+i\sqrt{3}}{2}\right)\right)\left(x - \left(\frac{-1-i\sqrt{3}}{2}\right)\right)$). Tegu $U = \{u_n\}_{n=0}^{\infty}$ yra tiesinė rekurentinė seka tokia, kad

$$u_n = Au_{n-1} + Bu_{n-2} + Cu_{n-3} \ (n \geq 3),$$

ir tegul šios sekos pradinės reikšmės yra $u_0, u_1, u_2 \in \mathbb{Z}$ su $u_0^2 + u_1^2 + u_2^2 \neq 0$ (negalioja $u_0 = u_1 = u_2 = 0$).

(a) Tada egzistuoja algebriniai skaičiai $\gamma_1, \gamma_2, \gamma_3$ tokie, kad

$$u_n = \gamma_1\alpha_1^n + \gamma_2\alpha_2^n + \gamma_3\alpha_3^n \text{ skaičiams } n \geq 0.$$

(b) Tuomet negalioja $|\alpha_1| = |\alpha_2| = |\alpha_3|$.

(c) Tada egzistuoja efektyviai apskaičiuojamas skaičius C*, priklausantis nuo* A, B, C*, toks, kad, jei* $n \in \mathbb{Z}_{\geq 0}$ *su* $u_n = 0$*, tai* $n < C$*.*

1995 metais Laurent, Mignotte ir Nesterenko įrodė sekančią nelygybę tiesinėms dviejų logaritmų formoms (žr. [8] 12 psl.).

19 teorema. *Tegul* a_1, a_2 *yra teigiami racionalūs skaičiai ir yra nelygūs* 1*. Tegu* $b_1, b_2 \in \mathbb{Z}_{\neq 0}$*. Tegul* $\Lambda := b_1 \log a_1 - b_2 \log a_2 \neq 0$*. Tada*

$$\log |\Lambda| \geq$$

$$\geq -22 \left(\max\{\log \left(\frac{|b_1|}{\log H(a_2)} + \frac{|b_2|}{\log H(a_1)} \right) + 0,06; 21\} \right)^2 \log H(a_1) \log H(a_2).$$

Sekanti likusi poskyrio dalis yra paaiškinimai iš [8] 12, 13 psl. Šie paaiškinimai parodo, kaip galima įrodyti faktus. Tie paaiškinimai yra be pilnų įrodymų.

2.2 poskyrio (2.20) lygybės rezultatą galima įrodyti naudojantis 1.4 poskyrio 19 teorema ir sekančia 20 teorema:

20 teorema. *Kai* $|z| \leq \frac{1}{2}$*, tai* $|\log(1+z)| \leq 2|z|$.

Įrodymas. Jei $|z| < 1$, tai

$$\log(1+z) = \sum_{n=1}^{\infty} \frac{(-1)^{n-1} z^n}{n}.$$

Realiesiems skaičiams x su $|x| < 1$ ši Teiloro eilutė, kuri yra ir Makloreno eilutė, gali būti įrodyta šitaip (žr. [25]):

$$(\log(1+x))' = \frac{1}{1+x} \overset{\text{geometrinė eilutė, } |x|<1}{=} \sum_{i=0}^{\infty} (-x)^i,$$

$$\log(1+x) = \int \sum_{i=0}^{\infty} (-x)^i \, \mathrm{dx} = \sum_{i=0}^{\infty} \int (-x)^i \, \mathrm{dx} =$$

$$= -\sum_{i=0}^{\infty} \int (-x)^i \, \mathrm{d(-x)} =$$

$$= -\sum_{i=0}^{\infty} \frac{(-x)^{i+1}}{i+1} = \sum_{i=0}^{\infty} -\frac{(-1)^{i+1} x^{i+1}}{i+1} =$$

$$= \sum_{i=0}^{\infty} \frac{(-1)^{i+2} x^{i+1}}{i+1} =$$

$$= \sum_{i=0}^{\infty} \frac{(-1)^{i} x^{i+1}}{i+1} =$$

$$= \sum_{i=1}^{\infty} \frac{(-1)^{i-1} x^i}{i}.$$

Atveju $x = 1$ lygybė $\ln 2 = \sum_{i=1}^{\infty} \frac{(-1)^{n-1}}{n}$ (čia $\ln 2 = \log 2$) gali būti įrodyta atskirai ir dar yra vadinama alternuojančia harmonine eilute (žr. [26]).

Kai $|z| \leq \frac{1}{2}$, tai $|z| < 1$, todėl (žr. [27])

$$|\log(1+z)| = \left| \sum_{n=1}^{\infty} \frac{(-1)^{n-1} z^n}{n} \right| =$$

$$= \left| \sum_{n=0}^{\infty} \frac{(-1)^n z^{n+1}}{n+1} \right| \leq$$

$$\leq \sum_{n=0}^{\infty} \frac{|(-1)^n| \, |z^{n+1}|}{|n+1|} =$$

$$= \sum_{n=0}^{\infty} \frac{|z|^{n+1}}{n+1} =$$

$$= |z| \sum_{n=0}^{\infty} \frac{|z|^n}{n+1} \leq$$

$$\leq |z| \sum_{n=0}^{\infty} \frac{1}{2^n (n+1)} \leq$$

$$\leq |z| \sum_{n=0}^{\infty} \frac{1}{2^n} =$$

$$= |z| \cdot \frac{1}{1 - \frac{1}{2}} = 2|z|.$$

□

2.2 poskyrio (2.21) lygybės rezultatą galima įrodyti naudojantis 1.4 poskyrio 19 teorema tinkamai tiesinei dviejų logaritmų formai tokiai, kad gautume apatinį rėžį, priklausantį nuo n bei nuo x, y. Bet taip pat galima gauti viršutinį rėžį, kuris priklauso nuo n, x, y. Palyginus šiuos du rėžius galima gauti viršutinį rėžį skaičiui n nepriklausomai nuo x, y.

1.3 poskyrio 12 teoremą galima įrodyti parodant $\left| \binom{b}{k} a^k \right|_p < |ab|_p$ skaičiams $k \geq 2$ arba parašyti $b = up^t$, kur $u \in \mathbb{Z}$, $p \nmid u$ ir $t \in \mathbb{Z}_{\geq 0}$, ir naudoti indukciją pagal t.

2 skyrius

Taikymai Diofanto lygtyse

2.1 Catalan hipotezė

Faktas, kad eksponentinė Diofanto lygtis

$$x^m - y^n = 1 \tag{2.1}$$

su keturiais kintamaisiais $x, y, m, n \in \mathbb{N}_{\geq 2}$ turi lygiai vieną sprendinį $(x, y, m, n) = (3, 2, 2, 3)$, dabar yra teorema, įrodyta Mihăilescu 2000 metais (žr. [8] 4 psl.). Anksčiau tai buvo hipotezė, padaryta Catalan 1844 metais. Šis matematinis teiginys dabar yra žinomas kaip Catalan hipotezė ar Mihăilescu teorema.

Mihăilescu teorema yra susijusi su tiesinėmis logaritmų formomis todėl, nes 1976 metais Tijdeman (žr. [8] 4 psl. ir [22]) naudodamasis jomis įrodė (įrodymas bandytas [19] nuo 36 psl.), jog egzistuoja efektyviai apskaičiuojama konstanta C tokia, kad bet kokiam eksponentinės Diofanto (2.1) lygties sprendiniui (x, y, m, n) turime $x^m, y^n \leq C$. Ši konstanta C gali būti apskaičiuota, bet ji yra labai didelio dydžio. Taigi Tijdeman įrodė, kad egzistuoja baigtinis skaičius eksponentinės Diofanto (2.1) lygties su keturiais kintamaisiais $x, y, m, n \in \mathbb{N}_{\geq 2}$ sprendinių (žr. [11]). Kiti bandė įrodyti Catalan hipotezę stengdamiesi viena vertus mažinti konstantą C stipresnėmis tiesinių logaritmų formų nelygybėmis, kita vertus parodyti, jog x^m, y^n su $(x^m, y^n) \neq (3^2, 2^3)$ turi būti labai didelio dydžio, pagaliau dar naudoti sunkius apskaičiavimus. Visi šie bandymai nepavyko. Mihăilescu įrodė Catalan hipotezę naudodamasis algebriniu metodu, nesusijusiu su tiesinėmis logaritmų formomis.

Taigi logaritmų tiesinės formos buvo naudingos daliniam rezultatui, kad eksponentinė Diofanto (2.1) lygtis su keturiais kintamaisiais $x, y, m, n \in \mathbb{N}_{\geq 2}$ turi baigtinį skaičių sprendinių, tačiau stipresniam teiginiui, jog sprendinys yra lygiai vienas $(x, y, m, n) = (3, 2, 2, 3)$, logaritmų tiesinių formų iš vis neprireikė.

2.2 Kiti taikymai Diofanto lygtyse

Kažkokiam $P \geq 2$ pažymėkime raide S visų teigiamų sveikųjų skaičių, sudarytų iš pirminių skaičių, neviršijančių P, aibę. Kažkokiam $k > 0$ turime, kad lygtis

$$x - y = k$$

su kintamaisiais $x, y \in \mathbb{Z}$, $x \in S$, $y \in S$ (pagal S apibrėžimą turime, jog $x, y > 0$) su $\mathrm{DBD}(x, y) = 1$ turi baigtinį skaičių sprendinių ir gali turėti sprendinių tik tada, kai $x < C_4 = C_4(k, P)$ kažkokiam skaičiui C_4, priklausančiam tik nuo k, P. Turime, kad $y = x - k < C_4(k, P) - k = C_5(k, P)$ kažkokiam skaičiui C_5, priklausančiam tik nuo k, P (žr. [11]).

Baker efektyvi Thue rezultato versija parodo, jog, kai $A, B, k \in \mathbb{Z}_{\neq 0}$, tai

$$Ax^m + By^m = k$$

su kintamaisiais $m \geq 3$, x, y su $|x| > 1$ turi baigtinį skaičių sprendinių (x, y, m) (žr. [11]).

Šiek tiek naudodamiesi logaritmais Erdős ir Selfridge (žr. [11], [7]) įrodė, kad lygtis

$$x(x + 1) \cdots (x + k - 1) = y^m \tag{2.2}$$

su kintamaisiais $x, y, k, m \in \mathbb{Z}$, $x > 0$, $y > 0$, $k > 1$, $m > 1$ neturi sprendinių. Įrodymas yra elementarus. Ši lygtis turi keturis kintamuosius. Taigi dviejų ar daugiau iš eilės einančių teigiamų sveikųjų skaičių sandauga negali būti teigiamo sveikojo skaičiaus laipsnis. Šis faktas yra susijęs su tiesinėmis logaritmų formomis todėl, nes naudodamiesi jomis Schinzel ir Tijdeman parodė, jog (2.2) lygtis turi baigtinį skaičių sprendinių (žr. [10], [11]).

Jei $A, B, C, D \in \mathbb{Z}$, $A \neq 0$, $B \neq 0$, tai Shorey (žr. [13]) įrodė, jog lygtis

$$Ax^m + By^m = Cx^n + Dy^n \tag{2.3}$$

turi baigtinį skaičių sprendinių su kintamaisiais $x, y, m, n \in \mathbb{Z}$, kuriems $|x| \neq |y|$, $0 \leqslant n < m$, $m > 2$, $Ax^m \neq Cx^n$, $Ax^m + By^m \neq 0$, $(m, n) \neq (4, 2)$. Nesunku pastebėti, kad šios sąlygos yra būtinos.

Shorey (žr. [14], [15]) įrodė, jog lygtis

$$y^m + 1 = \frac{x^n - 1}{x - 1} \tag{2.4}$$

su kintamaisiais $x, y, m, n \in \mathbb{Z}$, $x > 1$, $y > 1$, $m > 1$, $n > 2$ turi baigtinį skaičių sprendinių.

Tiesinių logaritmų formų teorija buvo pritaikyta lygtims

$$y^m = \frac{x^n - 1}{x - 1} \tag{2.5}$$

su kintamaisiais $x, y, m, n \in \mathbb{Z}$, $x > 1$, $y > 1$, $m > 1$, $n > 2$ ir

$$\frac{y^m - 1}{y - 1} = \frac{x^n - 1}{x - 1} \tag{2.6}$$

su kintamaisiais $x, y, m, n \in \mathbb{Z}$, $x > 1$, $y > 1$, $m > 2$, $n > 2$. Shorey ir Tijdeman (žr. [12]) parodė, kad (2.5) lygtis turi baigtinį skaičių sprendinių, kai x fiksuotas (x nėra kintamasis). Todėl, jei $x = 10$, tai gauname, jog yra baigtinis skaičius sveikųjų skaičių laipsnių su visais skaitmenimis (dešimtainėje sistemoje) lygiems 1. Dar Shorey (žr. [15]) įrodė, kad (2.5) lygtis turi baigtinį skaičių sprendinių, kai $\omega(n) > m - 2$, kur $\omega(n)$ žymi skačiaus n skirtingų pirminių daliklių skaičių (žr. [29]). Balasubramanian ir Shorey (žr. [3]) įrodė, jog (2.6) lygtis turi baigtinį skaičių sprendinių, kai x ir y yra sudaryti iš fiksuotų pirminių skaičių. (2.6) lygtyje yra ieškomi teigiami sveikieji skaičiai, kurių visi skaitmenys yra lygūs 1 atsižvelgiant į dvi skirtingas skaičių sistemas (bazes). Goormaghtigh pastebėjo, kad

$$31 = \frac{2^5 - 1}{2 - 1} = \frac{5^3 - 1}{5 - 1},\ 8191 = \frac{2^{13} - 1}{2 - 1} = \frac{90^3 - 1}{90 - 1}. \tag{2.7}$$

Shorey (žr. [16]) parodė, jog šie yra vieninteliai teigiami sveikieji skaičiai N su $\omega(N - 1) \leq 5$ (čia $\omega(N - 1)$ žymi skačiaus $N - 1$ skirtingų pirminių daliklių skaičių (žr. [29])) tokie, kad visi skaičiaus N skaitmenys yra lygūs 1 atsižvelgiant į dvi skirtingas skaičių sistemas (bazes). Įrodymas yra elementarus.

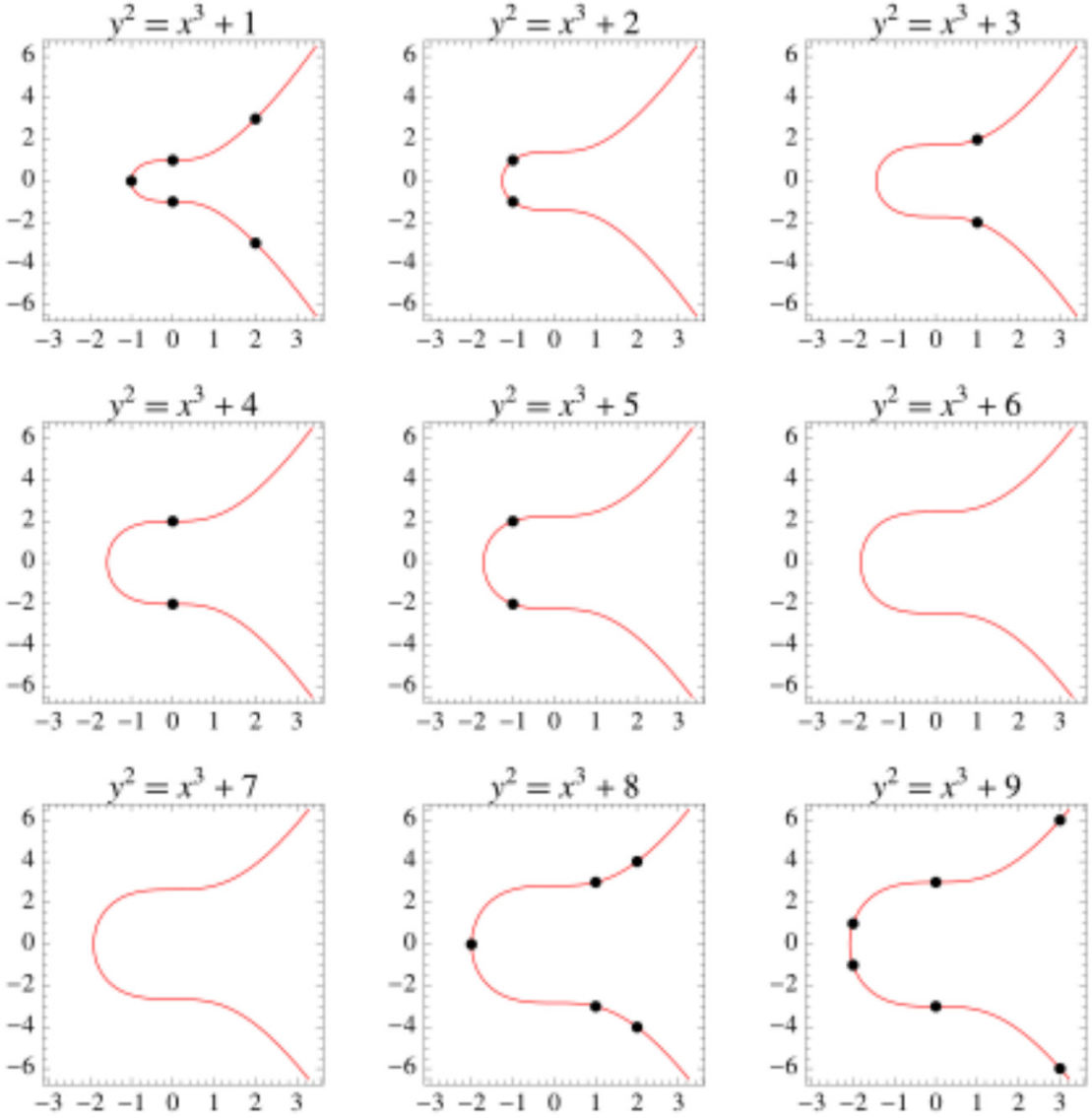
Baker panaudojo savo tiesinių formų nelygybes ir gavo efektyvias Thue ir Siegel rezultatų versijas (žr. [21]). Jis rado viršutinius rėžius (2.8), (2.9), (2.10), (2.11) lygčių sprendinių x, y moduliams. Taip jis įrodo, kad egzistuoja baigtinis skaičius sprendinių.

$$f(x, y) = m, \tag{2.8}$$

kur $f \in \mathbb{Z}[x, y]$ yra neredukuojamas homogeninis laipsnio $n \geq 3$ polinomas ir $m \in \mathbb{Z}_{\neq 0}$.

$$y^2 = x^3 + m, \tag{2.9}$$

kur $m \in \mathbb{Z}_{\neq 0}$. (2.9) lygtis apibrėžia Mordell kreivę (žr. [32]) ir dar yra vadinama Mordell lygtimi (žr. [4]). Mordell kreivė, kai $m = 1, 2, \ldots, 9$ (2.9) lygtyje, yra nurodyta 2.1 pav.



2.1 pav.: Mordell kreivė, kai $m = 1, 2, \ldots, 9$ (2.9) lygtyje (žr. [32]).

$$f(x) = y^2, \tag{2.10}$$

kur $f(x) \in \mathbb{Z}[x]$ turi bent tris paprastuosius nulius. Panašus rezultatas (2.10) lygčiai yra ir [19] 34 psl. Ten $f(x)$ aukščiausio laipsnio nario koeficientas yra lygus 1.

$$f(x) = y^m, \tag{2.11}$$

kur $f(x) \in \mathbb{Z}[x]$ turi bent du paprastuosius nulius ir $m \geq 3$ (dar galima žr. [11] tiem patiems (2.10), (2.11) lygčių rezultatams, įrodytiems Baker, kuris naudojosi Thue lygtis rezultatu, kuriam Baker reikėjo tiesinių logaritmų formų) (žr. [1]). Panašus rezultatas (2.11) lygčiai yra ir [19] 32 psl. Ten $f(x)$ aukščiausio laipsnio nario koeficientas yra lygus 1. [19] yra ir įrodymas nuo 33 psl.

(2.8) lygties pavyzdys yra

$$ax^n - by^n = c, \tag{2.12}$$

kur $a, b, c \in \mathbb{Z}_{\neq 0}$ ir $n \geq 3$. Taigi (2.12) lygtis turi baigtinį skaičių sprendinių (x, y). Įdomus rezultatas yra tas, kad naudojantis Baker metodu pavyksta rasti rėžį rodikliui n, kol laipsnio pagrindas yra kintamasis.

1988 metais Tijdeman ir Wang (žr. [23]) išsprendė visus (2.13), (2.14) lygčių atvejus, kai $p = 2$, $q = 3$ su dviem teigiamais ir dviem neigiamais nariais (žr. [9], [5]).

$$p^x q^y \pm p^z \pm q^w \pm 1 = 0 \quad (x, y, z, w \in \mathbb{Z}_{\geq 0}) \tag{2.13}$$

$$p^x \pm p^y \pm q^z \pm q^w = 0 \quad (x, y, z, w \in \mathbb{Z}_{\geq 0}) \tag{2.14}$$

[5] autorių Deze ir Tijdeman metodas yra pagrįstas de Weger rezultatu, kuris įrodomas naudojantis Baker tiesinių logaritmų formų teorijos gautomis nelygybėmis. Šis metodas panaudojamas bet kuriai pirminių skaičių p, q porai, tokiu būdu išsprendžiant (2.13), (2.14) lygtis bet kuriai pirminių skaičių porai p, q.

Egzistuoja efektyviai apskaičiuojami Diofanto lygties

$$ap^x + bq^y = c + dp^z q^w \tag{2.15}$$

rėžiai (žr. [9], [18]). Šioje lygtyje p, q yra fiksuoti tarpusavyje pirminiai teigiami sveikieji skaičiai ir $a, b, c, d \in \mathbb{Z}_{\geq 1}$ yra fiksuoti, $\mathrm{DBD}(abcd, pq) = 1$. [18] metodai panaudoja tiesines ir realių, ir p-adinių logaritmų formas. Taigi (2.15) lygtis turi baigtinį skaičių sprendinių (x, y, z, w).

$$5 \cdot 2^x + 7 \cdot 3^y = 11 + 2^z 3^w \text{ su kintamaisiais } x, y, z, w \in \mathbb{Z}_{\geq 0}. \tag{2.16}$$

$$2^x + 3^y = 1 + 2^z 3^w \text{ su kintamaisiais } x, y, z, w \in \mathbb{Z}_{\geq 0}. \tag{2.17}$$

(2.16) lygtis turi lygiai septynis sprendinius: $(x, y, z, w) = (0, 0, 0, 0)$, $(1, 0, 1, 1)$, $(2, 0, 4, 0)$, $(2, 2, 3, 2)$, $(2, 4, 6, 2)$, $(3, 0, 2, 2)$, $(8, 3, 1, 6)$ (žr. [18], 2.1 lentelę).

(2.17) lygtis turi lygiai dešimt netrivialių sprendinių: $(x, y, z, w) = (0, 0, 0, 0)$, $(1, 1, 2, 0)$, $(2, 1, 1, 1)$, $(2, 2, 2, 1)$, $(3, 2, 4, 0)$, $(4, 1, 1, 2)$, $(4, 2, 3, 1)$, $(4, 4, 5, 1)$, $(6, 2, 3, 2)$, $(6, 4, 4, 2)$ (žr. [18], 2.2 lentelę).

x	y	z	w
0	0	0	0
1	0	1	1
2	0	4	0
2	2	3	2
2	4	6	2
3	0	2	2
8	3	1	6

2.1 lentelė: (2.16) lygties sprendiniai (x, y, z, w).

x	y	z	w
0	0	0	0
1	1	2	0
2	1	1	1
2	2	2	1
3	2	4	0
4	1	1	2
4	2	3	1
4	4	5	1
6	2	3	2
6	4	4	2

2.2 lentelė: (2.17) lygties sprendiniai (x, y, z, w).

Panaši į (2.8) lygties rezultatą yra teorema, įrodyta Thue (žr. [6], [20]):

21 teorema. *Tegul*

$$a_d X^d + a_{d-1} X^{d-1} + \cdots + a_1 X + a_0 \in \mathbb{Z}[X]$$

yra neredukuojamas laipsnio $d \geq 3$ daugianaris virš $\mathbb{Q}$. Tada bet kokiam $m \in \mathbb{Z}_{\neq 0}$ Diofanto lygtis

$$a_d X^d + a_{d-1} X^{d-1} Y + \cdots + a_1 X Y^{d-1} + a_0 Y^d = m$$

(Thue lygtis) turi baigtinį skaičių sprendinių ($X = p$, $Y = q$).

Pagal šią 21 teoremą lygtis $X^3 - dY^3 = 1$, kur $d \in \mathbb{Z}$, turi baigtinį skaičių sprendinių, kur kintamieji yra X, Y. Tai taip pat sektų iš (2.12) lygties rezultato.

Apibrėžiame Thue lygtį (žr. [19] 27 psl.). Tegul $F(x, y) = a_n x^n + a_{n-1} x^{n-1} y + \cdots + a_0 y^n$ yra dvejetainė forma su sveikaisiais koeficientais ir $n \geq 3$. Tegu $m \in \mathbb{Z}_{\neq 0}$. Tegul F turi nenulinį diskriminantą. Tada lygtis

$$F(x, y) = m \tag{2.18}$$

yra vadinama Thue lygtimi. Thue 1909 metais įrodė, kad, jei $a_n \neq 0$, $F(x, 1)$ yra neredukuojamas, tai (2.18) lygtis turi baigtinį skaičių sprendinių $x, y \in \mathbb{Z}$.

Lygtis

$$f(x, y) = p_1^{z_1} \cdots p_s^{z_s} \tag{2.19}$$

su kintamaisiais $x, y \in \mathbb{Z}$, $z_1, \ldots, z_s \in \mathbb{Z}_{\geq 0}$, kur $f(x, y)$ yra apibrėžta Thue lygtyje (Thue lygties apibrėžimui žr. (2.18) lygtį), yra vadinama Thue-Mahler lygtimi ir turi baigtinį skaičių sprendinių (žr. [19], 40 psl.).

Žr. 9 išvadą 1.3 poskyryje, 13 teoremą, pastabą po 13 teoremos, 14, 15 teoremas 1.4 poskyryje (žr. [8]). Iš viso tai yra dar penki taikymai Diofanto lygtyse.

Lygtis

$$97^m - 89^n = 8 \tag{2.20}$$

su kintamaisiais $m, n \in \mathbb{N}_{\geq 1}$ turi baigtinį skaičių sprendinių (žr. [8] 12 psl.) (egzistuoja skaičius C toks, kad, jei (2.20) lygybė galioja ir $m, n \in \mathbb{N}_{\geq 1}$, tai $m, n \leq C$).

Lygtis

$$x^n - 2y^n = 1 \tag{2.21}$$

su kintamaisiais $x, y \in \mathbb{N}_{\geq 2}$ neturi sprendinių, jei $n > 10000$ (žr. [8] 12 psl.).

Tegul $a, b, c \in \mathbb{N}_{\geq 1}$. Egzistuoja efektyviai apskaičiuojamas ir priklausantis nuo a, b, c skaičius C toks, kad lygtis

$$ax^n - by^n = c \tag{2.22}$$

neturi sprendinių, jei $n > C$ (žr. [8] 13 psl.).

Tegul k yra fiksuotas natūralusis skaičius ir $k \geq 2$. Tada lygtis

$$y^z = \binom{x}{k} \tag{2.23}$$

su kintamaisiais $x, y, z \in \mathbb{N}_{\geq 1}$, $y \geq 2$, $z \geq 3$ turi baigtinį skaičių sprendinių (žr. [8] 13 psl.).

Tegul p yra pirminis skaičius ir $p \geq 5$. Tada lygtis

$$p^x - 2^y = 1 \tag{2.24}$$

su kintamaisiais $x, y \in \mathbb{N}_{\geq 2}$ neturi sprendinių (žr. [8] 13 psl.). Taip pat lygtis

$$2^x - p^y = 1 \tag{2.25}$$

su kintamaisiais $x, y \in \mathbb{N}_{\geq 2}$ neturi sprendinių (žr. [8] 13 psl.).

Sekanti teorema buvo įrodyta Baker, kuris įrodyme naudojosi tiesinėmis logaritmų formomis (žr. [11], [2]).

22 teorema. *Tegul $f(X, Y)$ yra dvejetainė homogeninė forma tokia, kad $f(X, 1)$ turi bent tris skirtingas šaknis. Tegu $k \in \mathbb{Z}_{\neq 0}$. Tada lygtyje*

$$f(x, y) = k$$

su kintamaisiais x, y egzistuoja rėžiai sprendiniams, todėl taip pat ši lygtis turi baigtinį skaičių sprendinių.

Linear Forms in Logarithms

Summary

In this master thesis it is written about theorems, corollaries, theory of linear forms in logarithms and how the forms are usefully applied in number theory, especially Diophantine equations, mostly exponential. Some of the theory uses facts about transcendental, algebraic numbers. Most Diophantine equations in this thesis are exponential, because after the theorems that directly describe linear forms in logarithms it is written about other theorems that instead of logarithms have exponents with bases. The fact that, e.g., $\exp(b \log a) = a^b$, where $a > 0$, $a, b \in \mathbb{R}$, is used. For applications of linear forms in logarithms the bounds of Diophantine equation solutions are found, existence of the bounds is shown, the fact that there exists a finite number of solutions is proven, all solutions are found, etc. A lot of attention is given to the Catalan conjecture, which is now a theorem.

Literatūra

[1] A. Baker, *Bounds for the Solutions of the Hyperelliptic Equation,* Proc. Cambridge Phil. Soc. 65 (1969), 439-444.

[2] A. Baker, *Contributions to the Theory of Diophantine Equations,* Phil. Trans. Royal Soc. London A 263 (1968), 173-208.

[3] R. Balasubramanian, T.N. Shorey, *On the Equation* $a(x^m-1)/(x-1) = b(y^n-1)/(y-1)$*,* Math. Scand. 46 (1980), 177-182, https://www.mscand.dk/article/view/11861/9877.

[4] Keith Conrad, *Examples of Mordell's Equation,* https://kconrad.math.uconn.edu/blurbs/gradnumthy/mordelleqn1.pdf.

[5] Mo Deze, R. Tijdeman, *Exponential Diophantine Equations with Four Terms,* Indag. Mathem., N.S., 3 (l), 47-57, China, the Netherlands, 1992, https://doi.org/10.1016/0019-3577(92)90045-M.

[6] Benjamin Earp-Lynch, *Linear Forms in Logarithms and Fibonacci Numbers,* Brock University, 2019, https://dr.library.brocku.ca/bitstream/handle/10464/14406/Brock_Earp-Lynch_Benjamin_2019.pdf?isAllowed=y&sequence=1.

[7] P. Erdős, J.L. Selfridge *The Product of Consecutive Integers is Never a Power,* Illinois Jour. Math.19 (1975), 292-301, https://users.renyi.hu/~p_erdos/1975-46.pdf.

[8] Jan-Hendrik Evertse, *Linear Forms in Logarithms,* April 2011, https://www.math.leidenuniv.nl/~evertse/dio2011-linforms.pdf.

[9] Aaron Levin, *Algebra & Number Theory,* Volume 8, No. 3, p. 647-687, 2014, https://doi.org/10.2140/ant.2014.8.647.

[10] A. Schinzel, R. Tijdeman, *On the Equation $y^m = P(x)$,* Acta Arith. 31 (1976), 199-204, http://matwbn.icm.edu.pl/ksiazki/aa/aa31/aa3129.pdf.

[11] T.N. Shorey, *Applications of Baker's Theory of Linear Forms in Logarithms to Exponential Diophantine Equations,* Tata Institute, India, 1994, https://www.kurims.kyoto-u.ac.jp/~kyodo/kokyuroku/contents/pdf/0886-05.pdf.

[12] T.N. Shorey, R. Tijdeman, *New Applications of Diophantine Approximations to Diophantine Equations,* Mathematica Scandinavica Vol. 39, No. 1 (1976), pp. 5-18 (14 pages), https://www.jstor.org/stable/24491169.

[13] T.N. Shorey, R. Tijdeman, *Exponential Diophantine Equations,* Cambridge Tracts in Mathematics 87 (1986), Cambridge University Press, https://doi.org/10.1017/CBO9780511566042.

[14] T.N. Shorey, *Some Exponential Diophantine Equations (II),* Number Theory and Related Topics, Tata Institute of Fundamental Research, Bombay (1988), 217-229.

[15] T.N. Shorey, *On the Equation $z^q = (x^n - 1)/(x - 1)$,* Indag. Math. 48 (1986), 345-351.

[16] T.N. Shorey, *Integers with Identical Digits,* Acta Arith. 53 (1989), 81-99.

[17] T.N. Shorey, R. Tijdeman, *Exponential Diophantine Equations,* Cambridge University Press, 1986; reprinted 2008.

[18] Christopher M. Skinner, *On the Diophantine Equation $ap^x + bq^y = c + dp^z q^w$,* Journal of Number Theory 35, 194-207 (1990), Michigan, U.S, https://deepblue.lib.umich.edu/bitstream/handle/2027.42/28532/0000330.pdf?sequence=1&isAllowed=y.

[19] C.L. Stewart, D. Wolczuk *Linear Forms in Logarithms and Diophantine Equations*, https://uwaterloo.ca/pure-mathematics/sites/ca.pure-mathematics/files/uploads/files/stewart.notes_1_0_0.pdf.

[20] A. Thue, *Über Näherungswerte und Kettenbrüche,* J. Reine Angew. Math. (Crelle), 115(3), 221-233 (1895).

[21] R. Tijdeman, *Linear Forms in Logarithms and Exponential Diophantine Equations,* Hardy-Ramanujan Journal, 2019, https://hrj.episciences.org/6458/pdf.

[22] Robert Tijdeman, *On the Equation of Catalan,* Acta Arithmetica XXIX, 1976, http://matwbn.icm.edu.pl/ksiazki/aa/aa29/aa2929.pdf.

[23] Robert Tijdeman, Lianxiang Wang, *Sums of Products of Powers of Given Prime Numbers,* Pacific J. Math. 132, 177-193 (1988), Corr. 135, 396-398 (1988).

[24] Michel Waldschmidt, *A Lower Bound for Linear Forms in Logarithms,* Acta Arithmetica XXXVII, Paris, 1980, http://matwbn.icm.edu.pl/ksiazki/aa/aa37/aa37125.pdf.

[25] https://math.stackexchange.com/questions/2016337/maclaurin-series-of-ln1-z.

[26] https://math.stackexchange.com/questions/716/sum-of-the-alternating-harmonic-series-sum-k-1-infty-frac-1k1k.

[27] https://math.stackexchange.com/questions/2665500/log-1-z-leq-2-z-complex-inequality.

[28] https://mathworld.wolfram.com/AlgebraicNumberMinimalPolynomial.html.

[29] https://mathworld.wolfram.com/DistinctPrimeFactors.html.

[30] https://mathworld.wolfram.com/TranscendentalNumber.html.

[31] https://mathworld.wolfram.com/RationalInteger.html.

[32] https://mathworld.wolfram.com/MordellCurve.html.