UNIVERZITET U NOVOM SADU
PRIRODNO-MATEMATIČKI FAKULTET
DEPARTMAN ZA MATEMATIKU I INFORMATIKU

LINEARNE FORME LOGARITAMA U REŠAVANJU DIOFANTOVIH JEDNAČINA

-master rad-

Mentor:
dr Bojan Bašić

Student:
Stefan Hačko

Novi Sad, avgust 2016.

Predgovor

Svima nam je verovatno dobro poznata scena sa slike i istog trenutka znate da će Pera Kojot neslavno završiti: ozbiljno povređen. Svaki put kada ga vidite kako očajnički pokušava da uhvati Pticu Trkačicu, verovatno se pitate zašto Kojot ne koristi svoje urođene instinkte (pretpostavljamo da je Pera Kojot *Canis latrans*, vrsta vuka koja se između ostalog hrani i pticama), i zašto mu je potrebna sva ta „teška artiljerija". I naravno, pitanje koje nam se upravo postavilo: kakve veze sve ovo ima sa matematikom?

Posmatrajmo dokaz sledećeg tvrđenja.

Tvrđenje. *Za* $n \geq 3$ *broj* $\sqrt[n]{2}$ *je iracionalan.*

Dokaz. Pretpostavimo suprotno, tj. $\sqrt[n]{2} = p/q$. Sledi $p^n = q^n + q^n$, kontradikcija sa Velikom Fermaovom teoremom. $\square$

Složićemo se, ovo je mnogo zanimljiviji dokaz nego da smo koristili elementarnu matematiku i „igrali se" osobinama deljivosti (svi podsvesno volimo kad se topom ide na komarca). Ovo je pravi primer dokaza koji bi osmislio Pera Kojot matematičar. Njega ne interesuju „troškovi", nije mu važno što je dokaz Velike Fermaove teoreme dug preko 150 strana, što većina profesionalnih matematičara ne može u potpunosti ni da shvati taj dokaz, nije mu značajna elegancija, mali broj slučajeva... jedino mu je važno da se posao završi.

Ovaj rad se upravo bavi jednom metodom u teoriji brojeva koja ne pita za „troškove". Većina dokaza u ovom radu nema posebnu eleganciju, onih „aha momenata", često razmatramo na desetine slučajeva, intenzivno se oslanjamo na računare (skoro svi dokazi glavnih teorema su praktično nemogući bez upotrebe računara), ali daleko od toga da su nezanimljivi za čitanje. U radu možete videti kako se na prvi pogled nepovezane matematičke teorije sjedinjuju da bi dale zadivljujuće rezultate.

Za početak krećemo sa istorijom:

Na Drugom internacionalnom kongresu matematičara u Parizu, 8. avgusta 1900. godine, David Hilbert je prezentovao, u izlaganju nazvanom „Problemi matematike", listu nerešenih problema. U izlaganju je želeo da zaokruži matematički uspešan 19. vek i predvidi razvoj matematike u budućnosti. Tom prilikom je rekao: „Ako verujemo u razvoj matematičkog znanja u bliskoj budućnosti, moramo se pozabaviti nedovršenim pitanjima i rešiti probleme koje zadaje današnja nauka, a čija rešenja očekujemo." Pojedini problemi, kao što je Rimanova hipoteza, nisu ni do danas rešeni. Sa druge strane, rešeni problemi dali su nove metode rešavanja koje se mogu primeniti na širok spektar drugih, na prvi pogled nepovezanih problema.

Jedan od rešenih problema je sedmi Hilbertov problem. Naime, trebalo je dokazati transcedentnost broja α^β, gde je $\alpha \neq 0, 1$ algebarski broj i β algebarski iracionalan broj. Taj problem su nezavisno 1934. godine rešili Gelfond i Schneider, tako što su pokazali da: ako su α_1 i α_2 nenula algebarski brojevi takvi da su $\ln \alpha_1$ i $\ln \alpha_2$ linearno nezavisni nad $\mathbb{Q}$, onda je

$$\beta_1 \ln \alpha_1 + \beta_2 \ln \alpha_2 \neq 0$$

za algebarske iracionalne brojeve β_1 i β_2.

Postavilo se pitanje da li se ovaj rezultat može uopštiti za više od dva uočena broja. Odgovor na ovo pitanje dao je Baker u seriji radova započetoj 1966. godine: on je ne samo dokazao da je izraz

$$|\beta_0 + \beta_1 \ln \alpha_1 + \beta_2 \ln \alpha_2 + \cdots + \beta_n \ln \alpha_n|$$

različit od nule, gde su $\alpha_1, \alpha_2, \ldots, \alpha_n$ nenula algebarski brojevi takvi da su $\ln \alpha_1, \ln \alpha_2, \ldots, \ln \alpha_n$ linearno nezavisni nad $\mathbb{Q}$, a $\beta_1, \beta_2, \ldots, \beta_n$ su proizvoljni algebarski brojevi koji nisu svi jednaki nuli, već je našao donje ograničenje tog izraza u zavisnosti samo od n i $\beta_1, \beta_2, \ldots, \beta_n$. Za ovaj proboj, kao i za demonstraciju kako se dobijeni rezultati mogu primeniti za rešavanje Diofantovih jednačina, Baker je 1970. godine dobio Fildsovu medalju.

Izraz oblika

$$\beta_1 \ln \alpha_1 + \beta_2 \ln \alpha_2 + \cdots + \beta_n \ln \alpha_n,$$

gde su brojevi n i $\beta_1, \beta_2, \ldots, \beta_n$ fiksirani, naziva se *linearna forma logaritama*. Ove forme nalaze primenu ne samo u teoriji transcendentnosti (kojim povodom su i nastale), već i u algebarskoj teoriji brojeva i u, što će biti predmet ovog master rada, rešavanju Diofantovih jednačina. Grubo govoreći, „strategija" je ovakva: uspostavljamo korespondenciju između „velikih" rešenja razmatrane Diofantove jednačine i „malih" vrednosti određene linearne forme logaritama. U literaturi se mogu naći razna donja ograničenja za linearne forme logaritama (znatno bolja od originalnog Bakerovog rezultata), pa da bi ova ograničenja bila ispunjena, dobijamo da razmatrana Diofantova jednačina ne može imati rešenja veća od određene granice. Time se njeno rešavanje svodi na ispitivanje konačnog broja slučajeva, koje proveravamo pomoću računara. Nažalost, granica dobijena na ovaj način često je prilično velika te ispitivanje preostalih slučajeva nije moguće praktično izvesti, ali postoje i tehnike za svođenje tih granica na razuman nivo, što će takođe biti prikazano u ovom radu.

Pregled rada

Prvo izlažemo kratak pregled teorije polja, teorije verižnih razlomaka, uvodimo pojam kvadratnog ostatka i navodimo, bez dokaza, najvažnija tvrđenja i teoreme koje su potrebne za dalje razumevanje teksta. Zatim definišemo pojam linearnih formi logaritama i na jednom mestu izdvajamo sve teoreme korišćene u dokazima ovog rada koje daju donja ograničenja za linearne forme logaritama.

U narednom delu bavimo se jednačinom oblika $a^x - b^y = c$, poznatom i pod nazivom Pillaieva jednačina. Prvo rešavamo Mordellovu jednačinu, čija rešenja će nam biti potrebna u dokazu naredne teoreme. Zatim dokazujemo centralnu teoremu ovog rada, koja tvrdi da Pillaieva jednačina ima najviše dva rešenja, da bismo na kraju ispitali datu jednačinu za male vrednosti parametra c.

Četvrti odeljak posvećen je problemu Erdősa i Grahama, tj. pronalaženju svih rešenja jednačine $(p-1)! + a^{p-1} = p^k$ (očigledno inspirisana kombinacijom Vilsonove i male Fermaove teoreme). Prvo rešavamo specijalne slučajeve $a = 1$ (teorema Liouvillea), $p = 3$ (teorema Aperyja) i pokazujemo da za $p \geq 5$ i k neparno nemamo rešenja. Posle nekoliko pomoćnih tvrđenja, izlažemo dokaz glavne teoreme sekcije, tj. rešavamo problem Erdősa i Grahama u potpunosti.

Na pitanje kada je proizvod dva k-ta stepena umanjena za jedan ponovo k-ti stepen umanjen za jedan, tj. kada Diofantova jednačina $(x^k-1)(y^k-1) = z^k-1$ ima rešenje, parcijalno daje odgovor peti odeljak. Naime, pokazujemo da za $k > 75$ data jednačina nema rešenje.

Poslednja dva dela rada bave se problemima koji na prvi pogled nemaju veze sa Diofantovim jednačinama: koji je najveći monocifarski Fibonačijev broj (odgovor: $F_{10} = 55$) i kada je broj $10^n \pm 1$ binarni palindrom (odgovor: samo za $n = 1, 2$)? Prvo date probleme svodimo na problem rešavanja Diofantovih jednačina, a zatim ih rešavamo pomoću linearnih formi logaritama.

Zahvalnosti

Na prvom mestu zahvaljujem se mom srednjoškolskom profesoru Živku Jovanovskom i dr Vladimiru Božinu, koji su me upoznali sa predivnim svetom matematike. Zahvaljujem se svim profesorima sa Prirodno-matematičkog fakulteta, koji su me vodili tokom studija i nesebično delili svoja znanja sa mnom. Velika čast mi je bila saradnja sa mojim mentorom dr Bojanom Bašićem, kome dugujem posebnu zahvalnost za sve savete, ideje, odvojeno vreme i podršku kako u toku studija tako i prilikom izrade ovog rada. Takođe zahvaljujem se i prof. dr Siniši Crvenkoviću i prof. dr Igoru Dolinki što su pristali da budu u komisiji za odbranu ovog rada i na svim komentarima i primedbama koje su pomogle da ovaj rad dobije svoj konačan oblik.

Najveću zahvalnost dugujem svojim roditeljima, Branislavu i Slavici Hačko, bez čije nesebične podrške i saveta nikako ne bih uspeo da stignem do kraja ovog dela studija. Zahvaljujem se i svoj rodbini i prijateljima koji su mi ulepšali ove studentske dane.

Novi Sad, avgust 2016. **Stefan Hačko**

Sadržaj

1 Osnovne definicije i tvrđenja

Radi lakšeg razumevanja sadržaja ovog rada, na samom početku izlažemo neke osnovne definicije i teoreme teorije polja, teorije verižnih razlomaka i teorije kvadratnih ostataka. Radoznalog čitaoca koji želi da proširi svoja znanja iz ovih teorija upućujemo na [12], [9], [18] i [5].

1.1 Teorija polja

Definicija 1.1. Neka je $\mathbb{L}$ polje i neka je $\mathbb{F}$ potpolje polja $\mathbb{L}$. Tada je $\mathbb{L}$ *ekstenzija polja* $\mathbb{F}$, u oznaci $\mathbb{L}/\mathbb{F}$.

Dimenzija baze vektorskog prostora $\mathbb{L}$ nad poljem $\mathbb{F}$ (elemente iz L posmatramo kao vektore, a elemente iz K kao skalare) naziva se *stepen ekstenzije polja* $\mathbb{L}$ u odnosu na polje $\mathbb{F}$ u oznaci $[\mathbb{L} : \mathbb{F}]$.

Tvrđenje 1.2. *Neka* $\mathbb{L}/\mathbb{K}$ *i* $\mathbb{K}/\mathbb{F}$. *Tada važi*

$$[\mathbb{L} : \mathbb{F}] = [\mathbb{L} : \mathbb{K}] \cdot [\mathbb{K} : \mathbb{F}].$$

Definicija 1.3. Neka $\mathbb{L}/\mathbb{F}$. Element $\alpha \in L$ je *algebarski* nad $\mathbb{F}$ akko postoji $f(x) \in F[x]$ tako da važi $f(\alpha) = 0$.

Normiran polinom najmanjeg stepena čija je nula α naziva se *minimalni polinom* elementa α u odnosu na polje $\mathbb{F}$ i označava se sa $p_\alpha^F(x)$.

Ekstenzija polja u kojoj je svaki element algebarski naziva se *algebarska ekstenzija.*

Može se pokazati da postoji minimalno proširenje polja $\mathbb{F}$ tako da sadrži algebarski element $\alpha \in L\setminus K$ i označavamo ga sa $\mathbb{F}[\alpha]$. Sada navodimo tvrđenje koje je osnovno oruđe za računanje stepena algebarskih ekstenzija.

Tvrđenje 1.4. *Neka je* α *algebarski element nad* $\mathbb{F}$. *Tada je*

$$[\mathbb{F}[\alpha] : \mathbb{F}] = \deg(p_\alpha^F(x)).$$

1.2 Verižni razlomci

Prvo definišemo konačne verižne razlomke.

Definicija 1.5. *Konačan verižni razlomak* je izraz sledećeg oblika

$$a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cdots + \cfrac{1}{a_{n-1} + \cfrac{1}{a_n}}}},$$

gde su $a_i \in \mathbb{Z}, i = 0, 1, \ldots, n$. Gornji izraz obeležava se sa $C_n = [a_0, a_1, \ldots, a_n]$.

Broj a_k, $0 \leq k \leq n$, naziva se k-ti *parcijalni količnik* verižnog razlomka C_n.

Za svako k, $0 \leq k \leq n$, verižni razlomak $C_k = [a_0, a_1, a_2, \ldots, a_k]$ naziva se k-ta *konvergenta* verižnog razlomka $[a_0, a_1, a_2, \ldots, a_n]$.

Napominjemo da se u nekoj literaturi ovako definisani verižni razlomci nazivaju jednostavni verižni razlomci[1], a verižni razlomci se definišu na isti način samo se za članove a_i uzima da su iz skupa $\mathbb{R}$. U ovom radu nema potrebe za uvođenje ovakvih verižnih razlomaka, pa se zbog toga opredeljujemo za prethodnu definiciju.

Iz Euklidovog algoritma direktno sledi da se svaki racionalan broj može predstaviti pomoću konačnog verižnog razlomka.

Za svaki verižni razlomak $[a_0, a_1, a_2, \ldots, a_n]$ definišemo brojeve $p_0, \ldots, p_n$, $q_0, \ldots, q_n$ na sledeći način

$$\begin{aligned} p_0 &= a_0, & q_0 &= 1; \\ p_1 &= a_0 a_1 + 1, & q_1 &= a_1; \\ p_k &= a_k p_{k-1} + p_{k-2}, & q_k &= a_k q_{k-1} + q_{k-2}, \end{aligned}$$

za svako $2 \leq k \leq n$. Lako se pokazuje da $C_k = \frac{p_k}{q_k}$.

Može se pokazati da je sledeća definicija dobra, tj. limes iz definicije postoji za svaki niz prirodnih brojeva.

Definicija 1.6. Neka je $(a_n)_{n \in \mathbb{N}}$ niz prirodnih brojeva, gde a_0 može biti 0. *Beskonačan verižni razlomak* se definiše kao limes niza konačnih verižnih razlomaka

$$[a_0, a_1, \ldots] = \lim_{n \to \infty} C_n.$$

Iz definicije se vidi da svaki beskonačan verižni razlomak odgovara nekom iracionalnom broju. Važi i obratno, svakom pozitivnom iracionalnom broju odgovara jedan beskonačan verižan razlomak. Postupak konstrukcije beskonačnog verižnog razlomka od iracionalnog broja neće biti izložen u ovom radu, pa kad god nam bude potrebna n-ta konvergenta tog verižnog razlomka, C_n, nju ćemo računati pomoću funkcije `ContinuedFraction[`γ, n`]`, iz programskog paketa *Mathematica*, gde je γ iracionalan broj.

Sledeće tvrđenje nam daje dovoljan uslov da neki racionalan broj $\frac{p}{q}$ bude neka konvergenta verižnog razlomka koji predstavlja iracionalan broj α.

Tvrđenje 1.7. *Ako je α iracionalan, a p/q racionalan broj i $s > 0$ tako da važi*

$$\left| \alpha - \frac{p}{q} \right| < \frac{1}{2s^2},$$

tada je $\frac{p}{q}$ konvergenta od α.

Vezu između konvergenti i parcijalnih količnika daje nam sledeće tvrđenje:

[1] eng. Simple Continued Fraction

Tvrđenje 1.8. *Neka je α iracionalan broj i $\frac{p_r}{q_r}$ r-ta konvergenta u razvoju broja α u verižni razlomak. Neka je a_{r+1} $(r+1)$-vi parcijalni količnik od istog razvoja. Tada važi*

$$\left|\frac{\ln b}{\ln a} - \frac{p_r}{q_r}\right| > \frac{1}{(a_{r+1}+2)q_r^2}.$$

Na kraju ovog dela dokazujemo jednu jednostavnu lemu, koju ćemo kasnije koristiti. Posmatrajmo sledeću normu $\|x\| = \min\{|x-n| : n \in \mathbb{Z}\}$, tj. udaljenost broja x od najbližeg celog broja.

Lema 1.9. *Neka je M prirodan broj, μ proizvoljan realan broj i neka je $\frac{p}{q}$ konvergenta verižnog razlomka iracionalnog broja γ takva da je $q > 6M$. Neka je $\varepsilon = \|\mu q\| - M\|\gamma q\|$. Ako je $\varepsilon > 0$, tada nejednačina*

$$0 < m\gamma - n + \mu < AB^{-m}$$

nema rešenja po m i n, m, n su prirodni brojevi, tako da važi

$$\frac{\ln(Aq/\varepsilon)}{\ln B} \leq m \leq M.$$

Dokaz. Neka je $0 \leq m \leq M$ i pretpostavimo da važi

$$0 < m\gamma - n + \mu < AB^{-m}.$$

Tada sledi

$$m(\gamma q - p) + mp - nq + \mu q \leq qAB^{-m},$$

pa dobijamo

$$qAB^{-m} > |\mu q - (nq - mp)| - m\|\gamma q\| \geq \|\mu q\| - M\|\gamma q\| := \varepsilon.$$

Sledi

$$m < \frac{\ln(Aq/\varepsilon)}{\ln B}.$$

□

1.3 Kvadratni ostaci

Definicija 1.10. Za broj a kažemo da je *ostatak k-tog reda po modulu p*, gde $p \nmid a$, ako i samo ako postoji x za koje važi $x^k \equiv a \pmod{p}$.

Koliko nekongruentnih ostataka k-tog reda ima po nekom modulu p daje nam sledeće tvrđenje.

Tvrđenje 1.11. *Postoji tačno $\frac{p-1}{NZD(k,p-1)}$ ostataka k-tog reda po modulu p.*

U ovom radu, a i često u praksi, potreban nam je samo specijalan slučaj $k = 2$ ili kvadratni ostaci. Na osnovu prethodnog tvrđenja imamo da postoji $\frac{p-1}{2}$ nekongruentnih kvadratnih ostataka po modulu p.

Tesno povezan pojam sa kvadratnim ostacima je *Ležandrov simbol*, koga definišemo, za slučaj $p \nmid a$, kao

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{ako je } a \text{ kvadratni ostatak po modulu } p \\ -1 & \text{ako } a \text{ nije kvadratni ostatak po modulu } p \end{cases}.$$

Sledeća tvrđenja i teoremu koristimo za efektivno izračunavanje Ležandrovih simbola.

Tvrđenje 1.12. *Broj a je kvadratni ostatak po modulu p, gde $p \nmid a$, ako i samo ako*

$$a^{\frac{p-1}{2}} \equiv 1 \pmod{p},$$

tj. važi

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}.$$

Tvrđenje 1.13. *i)* $a \equiv b \pmod{p} \Rightarrow \left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$*;*

ii) $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$*;*

iii) $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = \begin{cases} 1, & p \equiv 1 \pmod{4}; \\ -1, & p \equiv 3 \pmod{4}. \end{cases}$

Iz prethodnog imamo: ako je $a = (\pm 1) \cdot 2^{\alpha_0} \cdot {q_1}^{\alpha_1} \cdot {q_2}^{\alpha_2} \cdots {q_k}^{\alpha_k}$, i p prost broj takav da $p \nmid a$, tada je

$$\left(\frac{a}{p}\right) = \left(\frac{\pm 1}{p}\right)\left(\frac{2}{p}\right)^{\alpha_0}\left(\frac{q_1}{p}\right)^{\alpha_1}\left(\frac{q_2}{p}\right)^{\alpha_2} \cdots \left(\frac{q_k}{p}\right)^{\alpha_k}. \tag{1.1}$$

Tvrđenje 1.14. *Ako je p prost broj, tada*

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = \begin{cases} 1, & \textit{za } p \equiv \pm 1 \pmod{8}; \\ -1, & \textit{za } p \equiv \pm 3 \pmod{8}. \end{cases}$$

Teorema 1.15 (Gausov zakon kvadratne recipročnosti[2])**.** *Neka su p i q prosti neparni brojevi. Tada*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}},$$

tj,

$$\left(\frac{p}{q}\right) = \begin{cases} \left(\frac{q}{p}\right), & \textit{ako je bar jedan od } p \textit{ i } q \textit{ oblika } 4k+1; \\ -\left(\frac{q}{p}\right), & \textit{inače}. \end{cases}$$

[2] *Aureum Theorema* (lat. *Zlatna teorema*).

1.4 Linearne forme logaritama

Prvo definišemo linearnu formu logaritama algebarskih brojeva u najopštijem slučaju.

Definicija 1.16. *Linearna forma logaritama algebarskih brojeva* je izraz oblika

$$\beta_1 \ln \alpha_1 + \cdots + \beta_n \ln \alpha_n.$$

gde su α_i, β_i kompleksni algebarski brojevi (uzimamo glavnu granu kompleksnog logaritma).

U okviru ovog rada, β_i su celi brojevi i označavamo ih sa b_i. Sa malopre navedenom formom usko je povezan izraz sledećeg oblika:

$$\Lambda = \prod_{i=1}^{n} \alpha_i^{b_i} - 1.$$

Uvedimo još nekoliko oznaka.

1.4.1 Visina i logaritamska visina algebarskog broja

Neka je α algebarski broj stepena d (stepen minimalnog polinoma) i neka je

$$f(x) = \sum_{i=0}^{d} a_i x^{d-1} \in \mathbb{Z}[x]$$

minimalan, primitivan (NZD$(a_0, \ldots, a_d)$=1) polinom od α, gde je $\alpha_0 > 0$. Definišemo *visinu* broja α, u oznaci $H(\alpha)$, kao

$$H(\alpha) := \max\{|a_i| : i = 0, \ldots, d\}.$$

Razlažući minimalni polinom na linearne faktore dobijamo

$$f(x) = a_0 \prod_{i=1}^{d} (x - \alpha^{(i)}),$$

gde je $\alpha = \alpha^{(1)}$. Sada možemo definisati *logaritamsku visinu* broja α, u oznaci $h(\alpha)$, kao

$$h(\alpha) := \frac{1}{d} \left(\ln |a_0| + \sum_{i=1}^{d} \ln \max\{|\alpha^{(i)}|, 1\} \right).$$

1.4.2 Donje ograničenje izraza Λ

Neka je $\mathbb{L}$ algebarska ekstenzija polja $\mathbb{Q}$ stepena D, neka su $\alpha_1, \ldots, \alpha_n$ nenula elementi iz $\mathbb{L}$ i neka su $b_1, \ldots, b_n$ celi brojevi. Označimo

$$B = \max\{|b_1|, \ldots, |b_n|\}.$$

Neka su $A_1, \ldots, A_n$ prirodni brojevi tako da važi

$$A_j \geq h'(\alpha_j) := \max\{Dh(\alpha_j), |\ln \alpha_j|, 0.16\}, \qquad j = 1, \ldots, n.$$

Kao direktnu posledicu rezultata Matveeva iz [13], kako je pokazano u [22, Theorem 9.4], dobijamo sledeću teoremu.

Teorema 1.17. *Ako $\Lambda \neq 0$, onda*

$$\ln |\Lambda| > -3 \cdot 30^{n+4}(n+1)^{5.5} D^2 (1 + \ln D)(1 + \ln nB) A_1 A_2 \cdots A_n.$$

Ako je pritom $\mathbb{L}$ polje realnih brojeva, tada

$$\ln |\Lambda| > -1.4 \cdot 30^{n+3} n^{4.5} D^2 (1 + \ln D)(1 + \ln B) A_1 A_2 \cdots A_n.$$

1.4.3 Linearne forme dva logaritma

Često je pogodnije koristiti linearnu formu sledećeg oblika

$$\Gamma = b_2 \ln \alpha_2 - b_1 \ln \alpha_1.$$

Sada navodimo bez dokaza teoreme koje daju donja ograničenja za ovakve linearne forme logaritama, koje ćemo u nastavku rada koristiti. Radoznalog čitaoca kojeg interesuju dokazi datih teorema upućujemo na radove [17] i [14].

Naredna teorema dokazana je u radu [17].

Teorema 1.18. *Neka je $\mathbb{L} = \mathbb{Q}[\alpha_1, \alpha_2]$ realna ekstenzija od $\mathbb{Q}$ stepena D, A_1, A_2 konstante takve da važi*

$$A_i \geq \max\{Dh(\alpha_i), |\ln \alpha_i|, 1\}, \qquad i = 1, 2,$$

i neka je

$$b' = \frac{b_1}{A_2} + \frac{b_2}{A_2}.$$

Ako su α_1 i α_2 multiplikativno nezavisni, pozitivni realni brojevi, tada važi

$$\ln |\Gamma| \geq -23.34 \cdot \max\{D \ln b' + 0.14D, 21, D/2\}^2 A_1 A_2.$$

U radu [14] je dokazana sledeća teorema.

Teorema 1.19. *Neka su b_1 i b_2 prirodni brojevi i α_1 i α_2 multiplikativno nezavisni algebarski brojevi. Dalje, neka je*

$$D = \frac{[\mathbb{Q}(\alpha_1, \alpha_2) : \mathbb{Q}]}{[\mathbb{R}(\alpha_1, \alpha_2) : \mathbb{R}]},$$

neka su a_1, a_2, h pozitivni realni brojevi i neka je $\rho > 1$. Označimo $\lambda = \ln \rho$ i

$\chi = \frac{h}{\lambda}$. Pretpostavimo da postoji realan broj $\chi_0 \geq 0$ takav da važi $\chi \geq \chi_0$ i

$$\begin{aligned} h &\geq D\left(\ln\left(\frac{b_1}{a_2} + \frac{b_2}{a_1}\right) + \ln\lambda + f(\lceil K_0 \rceil)\right) + 0.023, \\ a_i &\geq \max\{1, \rho|\ln\alpha_i| - \ln|\alpha_i| + 2Dh(\alpha_i)\}, \qquad (i = 1, 2), \\ a_1 a_2 &\geq \lambda^2, \end{aligned}$$

gde je

$$f(x) = \ln\frac{(1+\sqrt{x-1})\sqrt{x}}{x-1} + \frac{\ln x}{6x(x-1)} + \frac{3}{2} + \ln\frac{3}{4} + \frac{\ln\frac{x}{x-1}}{x-1},$$

i

$$K_0 = \frac{1}{\lambda}\left(\frac{\sqrt{2+2\chi_0}}{3} + \sqrt{\frac{2(1+\chi_0)}{9} + \frac{2\lambda}{3}\left(\frac{1}{a_1} + \frac{1}{a_2}\right) + \frac{4\lambda\sqrt{2+\chi_0}}{3\sqrt{a_1 a_2}}}\right)^2 a_1 a_2.$$

Ako je

$$v = 4\chi + 4 + \frac{1}{\chi} \quad \text{ i } \quad m = \max\{2^{5/2}(1+\chi)^{3/2}, (1+2\chi)^{5/2}/\chi\},$$

tada važi

$$\begin{aligned} \ln|\Gamma| \geq &-\frac{1}{\lambda}\left(\frac{v}{6} + \frac{1}{2}\sqrt{\frac{v^2}{9} + \frac{4\lambda v}{3}\left(\frac{1}{a_1} + \frac{1}{a_2}\right) + \frac{8\lambda m}{3\sqrt{a_1 a_2}}}\right)^2 a_1 a_2 \\ &- \max\{\lambda(1.5 + 2\chi) + \ln\Big(((2+2\chi)^{3/2} + (2+2\chi)^2\sqrt{k^*})A + (2+2\chi)\Big), \\ &D\ln 2\}, \end{aligned}$$

gde je

$$A = \max\{a_1, a_2\} \quad \text{ i } \quad k^* = \frac{1}{\lambda^2}\left(\frac{1+2\chi}{2\chi}\right)^2 + \frac{1}{\lambda}\left(\frac{2}{3\chi} + \frac{2}{3}\frac{0\sqrt{1+2\chi}}{\chi}\right).$$

Kao posledicu ove teoreme, možemo dobiti sledeću teoremu.

Teorema 1.20. *Neka su b_1 i b_2 prirodni brojevi i α_1 i α_2 multiplikativno nezavisni algebarski brojevi. Dalje, neka je*

$$D = \frac{[\mathbb{Q}(\alpha_1, \alpha_2) : \mathbb{Q}]}{[\mathbb{R}(\alpha_1, \alpha_2) : \mathbb{R}]}$$

i neka su ρ, λ, a_1 i a_2 pozitivni realni brojevi takvi da važi $\rho \geq 4$, $\lambda = \ln\rho$,

$$a_i \geq \max\{1, \rho|\ln\alpha_1| - \ln|\alpha_i| + 2Dh(\alpha_i)\} \quad \text{ i } \quad a_1 a_2 \geq \max\{20, 4\lambda^2\}.$$

Ako je

$$h \geq \max\left\{3.5, 1.5\lambda, D\left(\ln\left(\frac{b_1}{a_2}+\frac{b_2}{a_1}\right)+\ln\lambda+1.377\right)+0.023\right\},$$

$\chi = \frac{h}{\lambda}$ *i* $v = 4\chi + 1 + \frac{1}{\chi}$, *tada važi*

$$\ln|\Gamma| \geq -(C_0+0.06)(\lambda+h)^2 a_1 a_2,$$

gde je

$$C_0 = \frac{1}{\lambda^3}\left\{\frac{4\chi^2+4\chi+1}{2\chi(\chi+1)}\left(\frac{1}{3}+\sqrt{\frac{1}{9}+\frac{4\lambda}{3v}\left(\frac{1}{a_1}+\frac{1}{a_2}\right)+\frac{32\sqrt{2}(1+\chi)^{3/2}}{3v^2\sqrt{a_1a_2}}}\right)\right\}^2$$

Iz posledice 2, teoreme 2, rada [17], za vrednosti $(h_2, \rho, C_2) = (10, 4.9, 32.31)$, dobijamo sledeću teoremu.

Teorema 1.21. *Neka su* b_1 *i* b_2 *prirodni brojevi i* α_1 *i* α_2 *multiplikativno nezavisni algebarski brojevi. Dalje, neka je*

$$D = [\mathbb{Q}(\alpha_1, \alpha_2) : \mathbb{Q}]$$
$$b' = \frac{b_1}{D\ln A_2} + \frac{b_2}{D\ln A_1},$$

gde su A_1 *i* A_2 *realni brojevi veći od* 1 *koji zadovoljavaju*

$$\ln A_i \geq \max\left\{h(\alpha_i), \frac{\ln\alpha_i}{D}, \frac{1}{D}\right\}, \qquad i = 1, 2.$$

Tada važi

$$\ln|\Gamma| \geq -32.31 D^4\left(\max\left\{\ln b' + 0.71, \frac{10}{D}, \frac{1}{2}\right\}\right)^2 \ln A_1 \ln A_2.$$

2 Pillaieva jednačina

U nizu radova iz tridesetih i četrdesetih godina S. S. Pillai proučavao je jednačinu oblika

$$a^x - b^y = c, \tag{2.1}$$

gde su a, b, c i y prirodni brojevi, a c nenula ceo broj, pa otuda i njen naziv. Pillai je u radu [20] postavio hipotezu da jednačina ovog oblika, za fiksirano c ima najviše konačno mnogo rešenja. Ovo je do danas, u opštem slučaju nerešen problem. U slučaju $c = 1$ dobijamo jednačinu koju je posmatrao Katalan 1844. godine i postavio hipotezu da je jedino njeno rešenje $3^2 - 2^3 = 1$, što je bio otvoren problem sve do 2002. godine. Tijdeman je 1976. u radu [23] dokazao da u ovom slučaju jednačina ima konačno mnogo rešenja, dok je Mihăilescu 2002. godine u radu [15] pokazao da je jedino rešenje ove jednačine $(a, b, x, y) = (3, 2, 2, 3)$.

U ovom delu rada bavimo se specijalnim slučajem ove hipoteze, kada su brojevi a, b, c fiksirani i $a, b \geq 2$. Slučajem kada je a prost broj bavio se Scott, koji je u radu [21] dokazao sledeće tvrđenje.

Tvrđenje 2.1. *Ako su $b > 1$ i c prirodni brojevi i a prost broj, tada jednačina* (2.1) *ima najviše jedno rešenje (x, y) gde su x i y prirodni brojevi, osim ako $(a, b, c) \in \{(3, 2, 1), (2, 3, 5), (2, 3, 13), (2, 5, 3)\}$ ili $a > 2$, a ne deli b i red ostatka b po modulu a je neparan. U tim situacijama jednačina* (2.1) *ima najviše dva rešenja (x_1, y_1) i (x_2, y_2). Štaviše, pritom su y_1 i y_2 različite parnosti osim ako $(a, b, c) \in \{(3, 2, 1), (2, 3, 5), (2, 3, 13), (2, 5, 3), (13, 3, 10)\}$.*

Mi ćemo dokazati teoremu koja tvrdi da, pod malopre navedenim uslovima, jednačina (2.1) ima najviše dva rešenja, a zatim, kao posebnu teoremu, dokazujemo da za male vrednosti parametra c $(1 \leq c \leq 100)$ jednačina ima najviše jedno rešenje, osim u konačno mnogo tačno poznatih slučajeva, kada ima dva rešenja.

2.1 Mordellova jednačina

U jednom trenutku biće nam potrebna rešenja Mordellove jednačine. Radi bolje preglednosti, rešavanje ove jednačine navodimo izdvojeno.

Teorema 2.2 (Mordell [16])**.** *Jedina celobrojna rešenja jednačine*

$$y(y + 1) = x(x + 1)(x + 2)$$

su $x \in \{0, -1, -2\}, y \in \{0, -1\}; x = 1, y \in \{2, -3\}; x = 5, y \in \{14, -15\}$.

Dokaz. Na početku uvodimo smenu

$$2y + 1 = Y, \qquad 2x + 2 = X,$$

pa svodimo problem na traženje celobrojnih rešenja jednačine

$$2Y^2 = X^3 - 4X + 2. \tag{2.2}$$

Kako je

$$2Y^2 \equiv 0 \pmod 2 \qquad \text{i} \qquad X^3 - 4X + 2 \equiv X^3 \pmod 2,$$

imamo da X mora biti parno. Dovoljno je dokazati da mora biti

$$X \in \{0, \pm 2, 4, 12\}.$$

Posmatrajmo sada jednačinu (2.2) nad poljem $\mathbb{K} = \mathbb{Q}(\theta)$ gde je θ nula polinoma

$$f(\theta) = \theta^3 - 4\theta + 2.$$

Osobine ovog polja date su u [7, str. 141], a mi koristimo:

- Elementi prstena celih brojeva polja $\mathbb{K}$ (celi brojevi polja algebarskih brojeva definišu se kao nule moničnih polinoma sa racionalnim koeficijentima) su oblika $a + b\theta + c\theta^2$, gde su a, b, c racionalni celi brojevi.

- Prsten celih brojeva polja $\mathbb{K}$ je domen jedinstvene faktorizacije.

- Postoje dve fundamentalne jedinice (elementi koji generišu grupu jediničnih elemenata, tj. invertibilnih elemenata u prstenu celih brojeva polja $\mathbb{K}$)
$$\varepsilon = \theta - 1 \qquad \text{i} \qquad \eta = 2\theta - 1,$$
tj. svi jedinični elementi su oblika
$$\zeta = \pm \varepsilon^l \eta^m,$$
gde su $l, m \in \mathbb{Z}$.

- Ako element x ovog polja posmatramo kao vektor nad bazom $\{1, \theta, \theta^2\}$, tada normu od x, u oznaci $N(x)$, dobijamo kao determinantu čije su kolone vektori x, θx i $\theta^2 x$. U ovom dokazu biće nam potrebne norme samo elemenata oblika $a + b\theta$, gde su a i b racionalni celi brojevi. Lako dobijamo
$$N(x) = \begin{vmatrix} a & 0 & -2b \\ b & a & 4b \\ 0 & b & a \end{vmatrix} = a^3 - 2b^3 - 4ab^2.$$

Može se pokazati je $2 \pm \theta$ asociran sa θ, pa pošto važi

$$2 = \theta(2 + \theta)(2 - \theta),$$

imamo da je faktorizacija broja 2 oblika

$$2 = \zeta\theta^3,$$

gde je ζ neki jedinični element.

Jednačina (2.2) sada postaje

$$(X-\theta)(X^2+\theta X+\theta^2-4)=\zeta\theta^3Y^2. \tag{2.3}$$

Kako je $X \equiv 0 \pmod 2$, onda je i $X \equiv 0 \pmod{\theta^3}$, pa $\theta \mid X-\theta$ i $\theta \mid X^2+\theta X+\theta^2-4$, ali $\theta^2 \nmid X-\theta$. Pretpostavimo da je d neki drugi zajednički delilac za $X-\theta$ i $X^2+\theta X+\theta^2-4$. Tada imamo da $X \equiv \theta \pmod d$, pa d mora da deli

$$\theta^2+\theta^2+\theta^2-4=3\theta^2-4=\frac{3\theta^3-4\theta}{\theta}=\frac{2(4\theta-3)}{\theta}.$$

Pošto je $N(4\theta-3)=37$, sledi da je $4\theta-3$ prost, pa je d ili jediničan element ili asociran sa $4\theta-3$. Pretpostavimo prvo da $4\theta-3$ deli $X-\theta$. Tada je

$$X-\theta=\theta\cdot(4\theta-3)^n\cdot s,$$

za neko $n\in\mathbb{N}$. Iz (2.3) sledi da s mora biti asociran sa nekim potpunim kvadratom, pa imamo

$$X-\theta=\pm\theta\cdot(4\theta-3)^n\varepsilon^l\eta^m(a+b\theta+c\theta^2)^2. \tag{2.4}$$

Normiranjem leve i desne strane dobijamo, stavljajući $X=2X_1$,

$$4X_1^3-4X_1+2=\pm(37)^nz^2.$$

Leva strana ove jednakosti kongruentna je sa 1 po modulu 8, pa sledi da je n parno, ali tada $(a+b\theta+c\theta^2)^2$ može „apsorbovati” $(4\theta-3)^n$, što implicira da je umesto jednačine (2.4) dovoljno posmatrati slučaj

$$X-\theta=\pm\theta\varepsilon^l\eta^m(a+b\theta+c\theta^2)^2. \tag{2.5}$$

gde je

$$(l,m)=(0,0),(1,0),(0,1),(1,1).$$

Primetimo da važi, iz definicije polja,

$$\begin{aligned}(a+b\theta+c\theta^2)^2=a^2-4bc&+\theta(2ab+8bc-2c^2)\\&+\theta^2(b^2+2ac+4c^2)\\&-2(b^2+2ac+4c^2).\end{aligned}$$

Razmotrimo gore navedene slučajeve:

- $(l,m)=(0,0)$: Na osnovu definicije polja dobijamo

$$\begin{aligned}\theta\cdot(a+b\theta+c\theta^2)^2=&(2ab+8bc+2c^2)\theta^2\\&+(a^2+4bc+4(b^2+2ac+4c^2))\theta,\end{aligned}$$

izjednačavajući koeficijente uz θ i θ^2 u (2.5), dobijamo sistem jednačina

$$\begin{aligned} 0 &= 2ab + 8bc - 2c^2, \\ \mp 1 &= a^2 - 4bc + 4(b^2 + 2ac + 4c^2). \end{aligned}$$

Posmatrajući drugu jednačinu po modulu 4, dobijamo da slučaj -1 otpada. Sada zapišimo sistem na sledeći način:

$$\begin{aligned} b(a + 4c) &= c^2, \\ (a + 4c)^2 + 4b^2 - 4bc &= 1. \end{aligned}$$

Imamo dva podslučaja:

– $b = 0$: Lako se vidi da je rešenje sistema $(a, b, c) = (\pm 1, 0, 0)$.

– $b \neq 0$: Deleći i levu i desnu stranu prve jednačine sa b i uvrštavajući rezultat u drugu dobijamo jednačinu

$$\frac{c^4}{b^2} + 4b^2 - 4bc = 1.$$

Posmatranjem leve strane ove jednačine kao funkcije po c možemo videti da se njen minimum dostiže za $c = b$ i iznosi b^2; kako je b ceo nenula broj, jedina mogućnost je $c = b = \pm 1$, pa u ovom slučaju rešenje sistema je

$$(a, b, c) = (\mp 3, \pm 1, \pm 1).$$

Iz (2.5) sledi

$$X = 2(b^2 + 2ac + 4c^2),$$

pa se gornja rešenja svode na

$$X = 0 \quad \text{ili} \quad X = -2. \tag{2.6}$$

- $(l, m) = (1, 0)$: Slično kao u prethodnom slučaju iz

$$\begin{aligned} \pm(X - \theta) = (\theta - \theta^2)(a^2 - 4bc + \theta(2ab + 8bc - 2c^2) \\ + \theta^2(b^2 + 2ac + 4c^2)), \end{aligned}$$

dobijamo sistem

$$\begin{aligned} 0 &= 2ab + 8bc - 2c^2 - a^2 + 4bc - 4(b^2 + 2ac + 4c^2), \\ \mp 1 &= a^2 - 4bc + 6(2ac + b^2 + 4c^2) - 4(2ab + 8bc - 2c^2). \end{aligned}$$

Prva jednačina implicira da je a parno, a druga da je a neparno, kontradikcija. Sledi da u ovom slučaju nemamo rešenja.

- $(l, m) = (0, 1)$: Množeći levu i desnu stranu jednakosti (2.2) sa θ u ovom slučaju dobijamo

$$\begin{aligned}\pm(\theta X - \theta^2) = (1-2\theta)(a^2 - 4bc + \theta(2ab + 8bc - 2c^2) \\ + \theta^2(b^2 + 2ac + 4c^2)).\end{aligned}$$

Slično kao u prethodnim slučajevima stižemo do sistema

$$\begin{aligned}0 &= a^2 - 4bc + 4(2ac + b^2 + 4c^2), \\ \mp 1 &= 2ac + b^2 + 4c^2 - 2(2ab + 8bc - 2c^2), \\ \mp X &= 2ab + 8bc - 2c^2 - 2(a^2 - 4bc) - 8(2ac + b^2 + 4c^2).\end{aligned}$$

Iz prve jednačine vidimo da je a parno, pa slučaj -1 iz druge jednačine otpada. Zapišimo sistem prve dve jednačine kao

$$\begin{aligned}1 &= a(2c - 4b) + b^2 - 16bc + 8c^2, \\ 0 &= (a + 4c)^2 + 4b(b - c).\end{aligned}$$

Primetimo da rešenja (a, b, c) i $(-a, -b, -c)$ daju istu vrednost X. Imamo dva podslučaja:

- $c = 2b$: U ovom slučaju imamo $b^2 = 1$, a na osnovu prethodne napomene dovoljno je posmatrati samo rešenje $b = 1$, $c = 2$, pa lako dobijamo $a = -6, -10$. Imamo da je $X = 4$ ili $X = 12$.
- $c \neq 2b$: Iz prve jednačine dobijamo

  $$a = \frac{b^2 - 16bc + 8c^2 - 1}{4b - 2c},$$

  pa dodajući $4c$ i levoj i desnoj strani imamo

  $$a + 4c = \frac{b^2 - 1}{4b - 2c}.$$

  Uvrštavajući ovo u drugu jednačinu stižemo do

  $$\left(\frac{b^2 - 1}{4b - 2c}\right)^2 + 4b(b - c) = 0.$$

  Odavde sledi da $b \mid (b^2 - 1)^2$, što je moguće samo za $b = \pm 1$. Lako dobijamo rešenje sistema

  $$(a, b, c) = (\mp 4, \pm 1, \pm 1), \tag{2.7}$$

  što implicira $X = 4$ (primetimo da smo sada dobili sva rešenja iz tvrđenja teoreme).

- $(l, m) = (1, 1)$: Slično kao u prethodnim slučajevima dobijamo sistem

$$\begin{aligned} 0 &= a^2 - 4bc + 6(2ab + b^2 + 4c^2) - 4(2ab + 8bc - 2c^2), \\ \mp 1 &= 9(2ac + b^2 + 4c^2) - 3(2ab + 8bc - 2c^2) + 2(a^2 - 4bc). \end{aligned}$$

  Iz prve jednačine prvo dobijamo da je a parno, ali onda i b mora biti parno, jer kad je a parno, desna strana jednačine je deljiva sa 4. Druga jednačina implicira da je b neparno, kontradikcija. U ovom slučaju nemamo rešenja.

$\square$

2.2 Glavna teorema

Teorema 2.3 (Bennett [2]). *Ako su a, b i c nenula celi brojevi za koje važi $a, b \geq 2$, tada jednačina* (2.1) *ima najviše dva rešenja.*

Ideja dokaza je sledeća: Pretpostavićemo da postoje bar tri rešenja jednačine, zatim ćemo formirati pogodne linearne forme logaritama i ograničiti ih sa gornje strane. Pomoću teoreme 1.20 dobićemo i donje ograničenje. Dalje pokazujemo, da za određene „dovoljno velike" parametre naša pretpostavka vodi u kontradikciju, a preostale slučajeve, uz neke dodatne zaključke, pomoću računara ispitujemo i na taj način pokazujemo da nisu mogući.

Dokaz. Neka su $a, b \geq 2$ i c pozitivno (ako je $c < 0$ jednačinu množimo sa -1 i dobijamo oblik iz pretpostavke) i pretpostavimo da postoje bar tri rešenja jednačine (2.1). Obeležimo ih sa (x_i, y_i), $i = 1, 2, 3$, i neka važi

$$x_1 < x_2 < x_3 \quad \text{i} \quad y_1 < y_2 < y_3.$$

Dokažimo prvo jednu jednostavnu, ali kasnije vrlo korisnu lemu (pokazujemo da u određenom smislu rešenja su „dovoljno udaljena" jedna od drugog).

Lema 2.4. *Za $i = 1, 2$ važi*

$$y_{i+1}x_i - x_{i+1}y_i > 0. \tag{2.8}$$

Dokaz. Primetimo prvo da za $A > B > 1$ funkcija $f(x) = A^x - B^x$ je monotono rastuća za $x \geq 1$. Ako za A uzmemo $A = a^{x_i}$ i za $B = b^{x_i}$, a pošto iz $x_{i+1} > x_i$ sledi $\frac{x_{i+1}}{x_i} > 1$, imamo

$$a^{x_{i+1}} - b^{y_i \frac{x_{i+1}}{x_i}} = a^{x_i \frac{x_{i+1}}{x_i}} - b^{y_i \frac{x_{i+1}}{x_i}} > a^{x_i} - b^{x_i} = c = a^{x_{i+1}} - b^{y_{i+1}},$$

te odavde dobijamo

$$b^{y_i \frac{x_{i+1}}{x_i}} < b^{y_{i+1}},$$

što implicira

$$y_i \frac{x_{i+1}}{x_i} < y_{i+1},$$

pa sledi traženo. □

Dokažimo da su a i b uzajamno prosti. Pretpostavimo suprotno, postoji prost broj p koji deli i a i b. Pošto važi

$$a^{x_i} - b^{x_i} = c = a^{x_{i+1}} - b^{y_{i+1}},$$

sledi

$$a^{x_i}(a^{x_{i+1}-x_i} - 1) = b^{y_i}(b^{y_{i+1}-y_i} - 1). \tag{2.9}$$

Neka $ord_p x$ označava najveći stepen broja p koji deli x. Uzmimo $\alpha = ord_p a$ i $\beta = ord_p b$. Kako važi $p \nmid a^{x_{i+1}-x_i} - 1$ i $p \nmid b^{y_{i+1}-y_i} - 1$, dobijamo da je $\alpha x_i = \beta y_i$

za $i = 1, 2$, pa sledi

$$\frac{x_1}{y_1} = \frac{\beta}{\alpha} = \frac{x_2}{y_2},$$

kontradikcija sa lemom 2.4.

Do kraja dokaza pretpostavljamo da su a i b uzajamno prosti.

Definišimo sada linearne forme logaritama Λ_i, $i = 1, 2, 3$, u sledećem obliku

$$\Lambda_i = x_i \ln a - y_i \ln b.$$

Prvo dokazujemo da za $i = 2, 3$ važi

$$\ln|\Lambda_i| < \ln\left(\min\left\{\frac{a^{i-1}c}{(a^i - 1)a^{x_i}}, \frac{c}{b^{y_i}}\right\}\right). \tag{2.10}$$

Pošto važi $x < e^x - 1$, jednostavno dobijamo

$$\Lambda_i < e^{\Lambda_i} - 1 = \frac{a^{x_i}}{b^{y_i}} - 1 = \frac{c}{b^{y_i}}, \tag{2.11}$$

odakle direktno sledi

$$\ln|\Lambda_i| < \ln\frac{c}{b^{y_i}}. \tag{2.12}$$

Kako važi $x_3 > x_2 > x_1$ i $a > c$, lako dobijamo sledeće ocene

$$a^{x_3} \geq a^{x_1+2} > a^2c \quad \text{i} \quad a^{x_2} \geq a^{x_1+1} > ac.$$

Iz ovih nejednakosti, jednakosti

$$\frac{a^{x_i}}{b^{y_i}} = \frac{a^{x_i}}{a^{x_i} - c} = \frac{\frac{a^{x_i}}{c}}{\frac{a^{x_i}}{c} - 1},$$

kao i činjenice da je $\frac{x}{x-1}$ opadajuća funkcija, za $i = 2, 3$ važi

$$\frac{a^{x_i}}{b^{y_i}} < \frac{a^{i-1}}{a^{i-1} - 1}.$$

Množenjem leve i desne strane sa b^{y_i} i korišćenjem činjenice $b^{y_i} < a^{y_i}$ (pošto $c > 0$) dobijamo

$$b^{y_i} < \frac{a^{i-1}}{a^{i-1} - 1} b^{y_i}.$$

Odavde množenjem leve i desne strane nejednakosti sa $\frac{c}{a^{x_i}b^{y_i}}$ i koristeći (2.11), posle logaritmovanja dobijamo

$$\ln|\Lambda_i| < \ln\frac{a^{i-1}c}{(a^i - 1)a^{x_i}}. \tag{2.13}$$

Iz (2.12) i (2.13) sledi (2.10).

Kao posledicu leme 2.4 imamo

$$y_{i+1}\Lambda_i - y_i\Lambda_{i+1} = (y_{i+1}x_i - x_{i+1}y_i)\ln a \geq \ln a.$$

Kako je $\Lambda_{i+1} > 0$ važi

$$\frac{x_{i+1}}{\ln b} > \frac{y_{i+1}}{\ln a} \quad \text{i} \quad y_{i+1}\Lambda_i > y_{i+1}\Lambda_i - y_i\Lambda_{i+1}.$$

Kombinujući poslednje tri nejednakosti dobijamo

$$\frac{x_{i+1}}{\ln b} > \frac{y_{i+1}}{\ln a} > \frac{1}{\Lambda_i}. \tag{2.14}$$

Sada ćemo pomoću teoreme 1.20 sa donje strane ograničiti linearnu formu Λ_3. Koristeći oznake iz formulacije teoreme, uzimamo

$$D = 1, \quad \alpha_1 = b, \quad \alpha_2 = a, \quad b_1 = y_3, \quad b_2 = y_2, \quad \rho = 4.74.$$

Zbog tvrđenja 2.1 vidimo da možemo pretpostaviti da a ima bar dva prosta faktora, pa uzimamo $a \geq 6$. Takođe pretpostavljamo $b \geq 2$. Na osnovu ovoga lako se vidi da možemo uzeti

$$a_1 = (\rho+1)\ln b, \quad a_2 = (\rho+1)\ln a$$

i važi $a_1a_2 \geq \max\{20, 4\lambda^2\}$. Imamo

$$\ln\left(\frac{b_1}{a_2} + \frac{b_2}{a_1}\right) = \ln\left(\frac{y_3}{\ln a} + \frac{x_3}{\ln b}\right) - \ln(\rho+1),$$

pa iz (2.14) sledi da možemo uzeti

$$h = \max\left\{9.365, \ln\left(\frac{x_3}{\ln b}\right) + 0.788\right\}.$$

Pokazaćemo da u oba slučaja dobijamo kontradikciju. Pretpostavimo da je

$$h = \ln\left(\frac{x_3}{\ln b}\right) + 0.788,$$

tj.

$$\ln\left(\frac{x_3}{\ln b}\right) + 0.788 > 9.365.$$

Tada dobijamo

$$\frac{x_3}{\ln b} > 5308. \tag{2.15}$$

Da bismo primenili teoremu 1.20, potrebno je još da ocenimo vrednosti $\frac{1}{a_1} + \frac{1}{a_2}$ i $\frac{1}{a_1a_2}$. Koristeći tvrđenje 2.1, dobijamo da, ako je $b = 2$, tada je dovoljno posmatrati slučaj $a \geq 15$, a ako je $b \geq 3$, tada posmatramo slučaj $a \geq 6$; kombinujući oba slučaja dobijamo da se maksimum obe funkcije dobija za

$a = 15, b = 2$, pa sledi da je $C_0 < 0.615$. Sad iz teoreme 1.20 imamo

$$\ln|\Lambda_3| > -22.24 \left(\ln\left(\frac{x_3}{\ln b}\right) + 2.345\right)^2 \ln a \ln b,$$

odakle, kombinujući sa nejednakošću (2.10) i koristeći $a \geq 6$, sledi

$$\ln \frac{36c}{35a^{x_3}} > \ln|\Lambda_3| > -22.24 \left(\ln\left(\frac{x_3}{\ln b}\right) + 2.345\right)^2 \ln a \ln b,$$

pa dobijamo

$$\frac{x_3}{\ln b} < \frac{\ln c}{\ln a \ln b} + \frac{\ln(36/35)}{\ln a \ln b} + 22.24 \left(\ln\left(\frac{x_3}{\ln b}\right) + 2.345\right)^2.$$

Kako je $a^{x_1} > c$ i $\ln a \ln b > \ln 2 \ln 15$, prethodna nejednakost implicira

$$\frac{x_3 - x_1}{\ln b} < 0.01 + 22.24 \left(\ln\left(\frac{x_3}{\ln b}\right) + 2.345\right)^2. \tag{2.16}$$

Ponovo koristeći (2.9) i činjenicu da su a i b uzajamno prosti, dobijamo

$$a^{x_{i+1}-x_i} \equiv 1 \pmod{b)^{y_i}} \quad \text{i} \quad b^{y_{i+1}-y_i} \equiv 1 \pmod{a)^{x_i}}, \tag{2.17}$$

odakle lako sledi

$$b^{y_1} a^{x_1} < b^{y_2} < a^{x_3 - x_2},$$

te na kraju imamo $x_3 - x_1 > x_1$. Iz ove nejednakosti i (2.16) sledi

$$\frac{x_1}{\ln b} < 0.01 + 22.24 \left(\ln\left(\frac{x_3}{\ln b}\right) + 2.345\right)^2,$$

pa sabirajući to sa (2.16) dobijamo

$$\frac{x_3}{\ln b} < 0.02 + 44.48 \left(\ln\left(\frac{x_3}{\ln b}\right) + 2.345\right)^2.$$

Koristeći *Mathematicu* za rešavanje ove nejednačine po $\frac{x_3}{\ln b}$ dobijamo da

$$\frac{x_3}{\ln b} < 5305,$$

kontradikcija sa (2.15).

Neka je sad $h = 9.365$. Tada imamo

$$\frac{x^3}{\ln b} < 5309. \tag{2.18}$$

Kako važi (2.1) i

$$a^{x_2} - a^{x_1} = b^{x_2} - b^{x_1} < b^{x_2},$$

onda zaključujemo $a^{x_2} > b^{x_2} > a^{x_2} - a^{x_1}$ i $a^{x_1} > c$. Takođe iz (2.12) lako dobijamo

$$\frac{1}{\Lambda_2} > \frac{b^{y_2}}{c}.$$

Koristeći sve ove činjenice i (2.14) stižemo do

$$\frac{x_3}{\ln b} > \frac{1}{\Lambda_2} > \frac{b^{y_2}}{c} > \frac{a^{x_2} - a^{x_1}}{c} = \frac{a^{x_2}(a^{x_2 - x_1} - 1)}{c} > a^{x_2 - x_1} - 1. \tag{2.19}$$

Kombinujući ovu nejednakost sa (2.18) dobijamo

$$a^{x_2 - x_1} \leq 5309.$$

Zbog pretpostavke $a \geq 6$ (takođe imamo u vidu da a ima bar dva prosta faktora) ostaje nam da proverimo slučajeve

$$\begin{aligned}
x_2 - x_1 &= 1, \qquad & 6 \leq a &\leq 5308;\\
x_2 - x_1 &= 2, \qquad & 6 \leq a &\leq 72;\\
x_2 - x_1 &= 3, \qquad & 6 \leq a &\leq 15;\\
x_2 - x_1 &= 4, \qquad & a &= 6.
\end{aligned}$$

Dokažimo sad da je $\frac{x_3}{y_3}$ konvergenta u razvoju $\frac{\ln b}{\ln a}$ u verižni razlomak. Iz tvrđenja 1.7 znamo da je dovoljno da pokažemo

$$\left|\frac{\ln b}{\ln a} - \frac{x_3}{y_3}\right| < \frac{1}{2y_3^2}.$$

Iz (2.11) imamo

$$\left|\frac{\ln b}{\ln a} - \frac{x_3}{y_3}\right| = \left|\Lambda_3 \frac{1}{y_3 \ln a}\right| < \frac{c}{y_3 b^{y_3} \ln a}. \tag{2.20}$$

Dakle, da bismo dobili traženo, dovoljno je pokazati

$$\frac{c}{y_3 b^{y_3} \ln a} < \frac{1}{2y_3^2},$$

ili ekvivalentno

$$\frac{b^{y_3} \ln a}{c y_3} > 2.$$

Ponovo koristeći (2.17) dobijamo

$$b^{y_{i+1} - y_i} > a^{x_i} > b^{y_i},$$

pa u kombinaciji sa $a^{x_i} > c$ sledi

$$\frac{b^{y_3} \ln a}{c y_3} > \frac{b^{y_3} \ln a}{a^{x_1} y_3} > \frac{b^{y_3} \ln a}{b^{y_2 - y_1} y_3} = \frac{b^{y_3 - y_2 + y_1}}{y_3} \ln a.$$

Takođe iz $b^{y_{i+1}-y_i} > a^{x_i} > b^{y_i}$ sledi $y_{i+1} - y_i > y_i$, pa dobijamo $y_3 \geq 2y_2 + 1$ i $y_3 \geq 7$. Pošto je $b \geq 2$, dobijamo

$$\frac{b^{y_3-y_2+y_1}}{y_3} \ln a \geq \frac{b^{\frac{1}{2}y_3+\frac{1}{2}+y_1}}{y_3} \ln a > 2,$$

pa imamo da je $\frac{x_3}{y_3}$ konvergenta u razvoju $\frac{\ln b}{\ln a}$ u verižni razlomak.

Neka je $\frac{x_3}{y_3}$ r-ta konvergenta u razvoju $\frac{\ln b}{\ln a}$, tj. $\frac{x_3}{y_3} = \frac{p_r}{q_r}$ i neka je a_{r+1} $(r+1)$-vi količnik u istom razvoju, tada na osnovu tvrđenja 1.8 imamo da važi

$$\left|\frac{\ln b}{\ln a} - \frac{x_3}{y_3}\right| > \frac{1}{(a_{r+1}+2)y_3^2}.$$

Kombinujući ovo sa (2.20) dobijamo

$$a_{r+1} > \frac{b^{y_3} \ln a}{cy_3} - 2 > \frac{b^{\frac{1}{2}y_3+\frac{1}{2}+y_1}}{y_3} \ln a - 2. \tag{2.21}$$

Imajući u vidu da $b \mid a^{x_2-x_1} - 1$ i koristeći *Mathematicu*, uz pomoć koda

```
For[a=6,a<=5308,a++,
For[b=2,b<=a,b++,
If[Divisible[a-1,b],
If[Not[Denominator[Convergents[Log[b]/Log[a],19][[19]]]
>=5309*Log[a]],
Print[a, b]]]];
```

(ovde navodimo kod za slučaj $x_2 - x_1 = 1$, ostali se lako dobijaju modifikacijom ovog koda) dobijamo da za sve a i b (osim za $(a,b) = (3257,148), (4551,25)$ i $(5261,526)$, ali ove slučajeve svejedno ne razmatramo, prvi i treći zbog tvrđenja 2.1, a drugi zbog $25 = 5^2$, pa se on svodi na slučaj $b = 5$) važi $q_{19} \geq 5309 \ln a$, gde je q_{19} imenilac 19-te konvergente $\frac{p_{19}}{q_{19}}$ razvoja $\frac{\ln b}{\ln a}$. Iz (2.14) i (2.18) sledi $y_3 < 5309 \ln a$, pa imamo da je $\frac{x_3}{y_3} = \frac{p_r}{q_r}$ za neko $r \in \{1, 2, \ldots, 18\}$.

Grubo ocenjujući (2.21), koristeći $b \geq 2$, kao i $a \geq 15$ za $b = 2$, dobijamo da je $a_{r+1} > 100000$ ako je $y_3 \geq 38$.

Ponovo koristeći *Mathematicu* tražimo one a i b za koje važi da je njihov parcijalni količnik $a_k \geq 100000$ i $k \leq 18$. Pomoću koda

```
For[a=6,a<=5308,a++,
For[b=2,b<=a,b++,
If[Divisible[a-1,b],
verizni=ContinuedFraction[Log[b]/Log[a],18];
max=Max[verizni];
If[max>=100000,
index=Positino[verizni,max]
Print[StringForm["``  `` a``=``",a,b,index,max]]]]]];
```

dobijamo

a	b	a_k
1029	257	a_4=146318
1837	204	a_{16}=1859087
2105	526	a_{14}=149863
2179	33	a_8=169118
2194	713	a_4 =251316
3714	5	a_{14}=197241
4348	621	a_{15}=132488.

Prema prethodnom zaključku, za sve a, b koje razmatramo možemo pretpostaviti $y_3 \leq 37$. Iz

$$\frac{y_3}{\ln a} > a^{x_2-x_1} - 1$$

sledi $(a^{x_2-x_1}-1)\ln a < 37$, odakle imamo $6 \leq a \leq 14$ i $x_2 - x_1 = 1$. Ostaju nam mogućnosti $(a,b) \in \{(6,5),(10,3),(14,13)\}$. Dobijamo da je $q_k \geq 5309 \ln a$ za redom $k = 12, 9, 9$, pa od svih parcijalnih količnika koje posmatramo najveći je $a_3 = 34$ od $\frac{\ln 13}{\ln 14}$, ali ovo je u kontradikciji sa (2.21) jer iz ranije diskusije znamo

$$y_3 \geq 2y_2 + 1 \geq 4y_1 + 3 \geq 7.$$

Ovo dokazuje teoremu. □

2.3 Male vrednosti parametra c

Teorema 2.5 (Bennett [2]). *Ako su a, b, c prirodni brojevi takvi da $a, b \geq 2$ i $1 \leq c \leq 100$, tada jednačina* (2.1) *ima najviše jedno rešenje gde su x i y prirodni brojevi, osim ako je*

$$(a,b,c) \in \{(3,2,1),(2,3,5),(2,3,13),(4,3,13),(16,3,13),\\ (2,5,3),(13,3,10),(91,2,89),(6,2,4),(15,6,9)\},$$

kada jednačina (2.1) *ima tačno dva rešenja.*

Dokaz. Pretpostavimo da su a i b uzajamno prosti i da imamo dva rešenja jednačine (2.1) (x_1, y_1) i (x_2, y_2) i da važi $x_1 < x_2$ i $y_1 < y_2$. Kao i u dokazu prethodne teoreme, posmatramo linearnu formu logaritama

$$\Lambda_2 = x_2 \ln a - y_2 \ln b.$$

Primetimo da uz ove pretpostavke imamo sve što smo koristili da dokažemo (**??**), pa imamo to gornje ograničenje za Λ_2.

Za donje ograničenje ponovo koristimo teoremu 1.20 uz iste parametre kao u prošlom dokazu, samo što uzimamo $\rho = 5.11$ i

$$h = \max\left\{8.56, \ln\left(\frac{x_2}{\ln b}\right) + 0.773\right\}.$$

Sada posmatramo dva slučaja. Neka je prvo

$$h = \ln\left(\frac{x_2}{\ln b}\right) + 0.773.$$

Tada sledi

$$\frac{x_2}{\ln b} > 2409. \tag{2.22}$$

Iz pretpostavki o a i b direktno se dobija da su $\frac{1}{a_1} + \frac{1}{a_2}$ i $\frac{1}{a_1 a_2}$ maksimalni za $(a, b) = (7, 2)$, pa sledi $C_0 < 0.556$. Na osnovu teoreme 1.20 imamo

$$\ln|\Lambda_2| > -22.997 \left(\ln\left(\frac{x_2}{\ln b}\right) + 2.405\right)^2 \ln a \ln b.$$

Kombinujući ovo sa (**??**) i koristeći pretpostavke za a, b i c (može se pretpostaviti i $a \geq 6$), slično kao u prethodnom dokazu dobijamo

$$\frac{x_2}{\ln b} < 3.715 + 22.997 \left(\ln\left(\frac{x_2}{\ln b}\right) + 2.405\right)^2.$$

Rešavajući ovu nejednačinu po $\frac{x_2}{\ln b}$, uz pomoć *Mathematice* dobijamo

$$\frac{x_2}{\ln b} < 2389,$$

kontradikcija sa (2.22).

Ostaje nam $h = 8.56$. Kao što smo u prošlom dokazu dobili prve dve nejednakosti u (2.19), tako i sad stižemo do

$$\frac{x_2}{\ln b} > \frac{b^{y_1}}{c},$$

pa odavde sledi

$$\frac{b^{y_1}}{c} < 2410,$$

a iz ovog dobijamo

$$b^{y_1} < 2410c \quad \text{i} \quad a^{y_1} < 2410c + c = 2411c,$$

što znači da za svako $c \in \{1, 2, \ldots 100\}$ imamo gornje ograničenje za a^{x_1} i b^{y_1}.

Lema 2.6. *Pod datim pretpostavkama x_2 i y_2 su uzajamno prosti.*

Dokaz. Pretpostavimo suprotno, tj. postoji $1 < d \in \mathbb{N}$ takvo da $x_2 = dx$ i $y_2 = dy$, za neko $x, y \in \mathbb{N}$. Tada lako dobijamo

$$c = a^{x_2} - b^{y_2} = (a^x - b^y) \cdot \sum_{i=0}^{d-1} a^{ix} b^{(d-i-1)y},$$

pa direktno sledi

$$\sum_{i=0}^{d-1} a^{ix} b^{(d-i-1)y} \leq c. \tag{2.23}$$

Razmatramo sledeće slučajeve:

- $x_1 = 1$: Iz (2.23) sledi $a \leq c$, ali to je u kontradikciji sa $a = a^{x_1} > c$.
- $x_1 = 2$: Iz pretpostavke imamo $x_2 \geq 3$, a iz (2.23) sledi $a^{(d-1)x} \leq c$, što je u kontradikciji sa $a^{(d-1)x} \geq a^2 > a^2 - b^{y_1} = c$.
- $x_1 \geq 3$: Tada sledi $x_2 \geq 4$. Posmatramo sledeće podslučajeve:
  - $d = 2$ **i** $x_2 = 4$: Iz pretpostavki o x_2 i y_2 sledi da $y_2 \geq 6$, pa $y \geq 3$, a onda iz (2.23) sledi

    $$a^2 + b^3 \leq c \leq 100.$$

    Pretpostavimo da a i b nisu potpuni kvadrati (ako jesu, jednačinu možemo lako transformisati u traženi oblik), tada se iz pretpostavke da su a i b uzajamno prosti i tvrđenja 2.1 jednostavno dobija da mora biti $(a, b) = (7, 2)$, ali to je u kontradikciji sa

    $$0 < a^4 - b^{y_2} = 7^4 - 2^{y_2} \leq 100$$

    ($7^4 - 2^{11} = 353$, a $7^4 - 2^{12} = -1695$).
  - $d = 2$ **i** $x_2 \geq 6$: Iz pretpostavke sledi $y_2 \geq 4$, pa iz (2.23) sledi $a^3 + b^2 \leq 100$, kontradikcija sa $a \geq 6$, tj. $6^3 = 216 > 100$.
  - $d \geq 3$ **i** $x_2 \geq 4$: Iz pretpostavke sledi $(d-1)x \geq 3$, pa iz (2.23) sledi $a^3 < 100$, kontradikcija sa $a \geq 6$.

Time je lema dokazana. □

Nastavljamo dokaz teoreme. Razmotrimo prvo slučaj

$$\frac{b^{y_2} \ln a}{c y_2} > 2.$$

Tada imamo (kao u prethodnom dokazu) da je $\frac{x_2}{y_2}$ konvergenta razvoja u verižni razlomak broja $\frac{\ln b}{\ln a}$, i neka je $\frac{x_2}{y_2} = \frac{p_r}{q_r}$ za neko $r \in \mathbb{N}$. Na osnovu prethodne leme sledi da mora biti $x_2 = p_r$ i $y_2 = q_r$. Dobijamo, kao i u prethodnom dokazu, da važi

$$a_{r+1} > \frac{b^{y_2} \ln a}{c y_2} - 2 = \frac{b^{q_r} \ln a}{c q_r} - 2 \tag{2.24}$$

Uz male modifikacije kodova iz prethodnog dokaza, uz pomoć *Mathematice* tražimo konvergente $\frac{p_r}{q_r}$ razvoja u verižni razlomak broja $\frac{\ln b}{\ln a}$ koje zadovoljavaju $p_r < 2410 \ln b$, $p_r \geq 2$, $q_r \geq 3$, i parcijalne količnike a_{r+1} koji zadovoljavaju (2.24). Na ovaj način, za svaki razmatran par (a, b) (oni koji nisu pokriveni slučajevima iz tvrđenja 2.1) važi da za konvergente i parcijalne količnike koji zadovoljavaju sve tražene uslove ili je $(p_r, q_r) = (2, 3)$ ili se nalaze u sledećoj tabeli

a	b	r	a_r	p_r	q_r	c
23	2	4	10	2	9	15,17,19,21
45	2	3	30	2	11	29,37,41,43
91	2	4	31	2	13	87,89
13	3	4	79	3	7	10,88
47	3	4	54	2	7	22,38,44
421	3	4	1034	2	11	94
56	5	4	228	2	5	11,31,51
130	7	4	175	2	5	93
6	11	3	21	4	3	95
3	13	3	79	7	3	14,68,74.

Ako važi $(p_r, q_r) = (2, 3)$, onda sledi da $(x_1, y_1) = (1, 1)$ i $(x_2, y_2) = (2, 3)$, pa dobijamo

$$a - b = a^2 - b^3.$$

Po teoremi 2.2 jednačina

$$y(y + 1) = x(x + 1)(x + 2)$$

ima rešenja $x \in \{0, -1, -2\}, y \in \{0, -1\}; x = 1, y \in \{2, -3\}; x = 5, y \in \{14, -15\}$. Stavljajući $y = a$ i $b = x + 1$ imamo da naša jednačina ima rešenja

$$\begin{aligned}(a, b) \in \{&(-14, 6), (-2, 2), (0, -1), (0, 0), (0, 1),\\ &(1, -1), (1, 0), (1, 1), (3, 2), (15, 6)\}.\end{aligned}$$

Odavde dobijamo da za $(a, b, c) \in \{(3, 2, 1), (15, 6, 9)\}$ imamo dva rešenja (što i tvrdi teorema).

Posmatrajmo slučajeve navedene u prethodnoj tabeli. Lako se proverava da postoje x_1 i y_1, $x_1 < p_r$, $y_1 < q_r$, takvi da važi

$$a^{p_r} - b^{q_r} = a^{x_1} - b^{y_1} > 0,$$

samo za $(a, b, c) \in \{(91, 2, 89), (13, 3, 10)\}$ (što je ponovo obuhvaćeno tvrđenjem teoreme).

Posmatrajmo sada slučaj

$$\frac{b^{y_2} \ln a}{c y_2} \leq 2, \tag{2.25}$$

što je ekvivalentno sa

$$\frac{b^{y_2}}{y_2} \leq \frac{2c}{\ln a}.$$

Pošto imamo $a \geq 6$, $y_2 \geq 3$ i $1 \leq c \leq 100$, iz prethodnog lako dobijamo $2 \leq b \leq 6$. Ispitujemo sada svaku vrednost b posebno.

- $b = 2$: Iz pretpostavke sledi $a \geq 7$, pa u kombinaciji sa (2.25) dobijamo $y_2 \leq 10$, a iz (2.9) imamo da $a^{x_1} \mid 2^{y_2 - y_1} - 1$, gde je $2 \leq y_2 - y_1 \leq 9$. Kako je
$$a^2 \leq a^{x_2} \leq 2^{y_2} + 100 \leq 1124$$
sledi $a \leq 33$. Razlikujemo sledeće mogućnosti:
  - $a^{x_1} = 7$, $y_2 - y_1 \in \{3, 6, 9\}$: Iz (2.25) imamo $(y_1, y_2) = (1, 4)$, pa $7^{x_2} = 21$, kontradikcija.
  - $a^{x_1} = 15$, $y_2 - y_1 \in \{4, 8\}$: Slično prethodnom, dobijamo kontradikciju.
  - $a^{x_1} = 17$, $y_2 - y_1 = 8$: Direktna kontradikcija sa (2.25).
  - $a^{x_1} = 21$, $y_2 - y_1 = 6$: Slično prethodnom, dobijamo kontradikciju.
  - $a^{x_1} = 31$, $y_2 - y_1 = 5$: Kao u prvom slučaju, dobijamo kontradikciju.

  Sledi da je ovaj slučaj nemoguć.

- $b = 3$: Iz pretpostavke i tvrđenja 2.1 možemo pretpostaviti $a \geq 10$, pa iz (2.25) imamo $y_2 \leq 5$. Slično kao u prethodnom slučaju dolazimo do sledećih mogućnosti:
  - $a^{x_1} \mid 8$, $(y_1, y_2) = (1, 4)$: Ovaj slučaj je obuhvaćen tvrđenjem 2.1, pa ga ne razmatramo.
  - $a^{x_1} \mid 26$, $(y_1, y_2) \in \{(1, 4), (2, 5)\}$: Direktna kontradikcija sa (2.25).
  - $a^{x_1} \mid 80$, $(y_1, y_2) = (1, 5)$: Direktna kontradikcija sa (2.25).

  Sledi da je ovaj slučaj nemoguć.

- $b = 4$: Ne razmatramo jer je 4 potpun kvadrat.

- $b = 5$: Iz pretpostavke i (2.25) sledi $y_1 = 1$ i $y_2 \in \{3, 4\}$. Imamo mogućnosti:
  - $a^{x_1} \mid 24$, $y_2 = 3$: Iz pretpostavke imamo $a^{x_1} \in \{6, 12, 24\}$, ali je to u direktnoj kontradikciji sa (2.25).
  - $a^{x_1} \mid 124$, $y_2 = 4$: Iz pretpostavke imamo $a^{x_1} \in \{31, 62, 124\}$, ali je to u direktnoj kontradikciji sa (2.25).

  Sledi da je ovaj slučaj nemoguć.

- $b = 6$: Iz pretpostavke i (2.25) sledi $y_1 = 1$ i $y_2 = 3$, pa $a^{x_1} \mid 35$, što implicira $c \leq 35 - 6 = 29$, kontradikcija sa (2.25).

Ovim smo iscrpli sve mogućnosti, pa tvrđenje sledi za uzajamno proste a i b.

Neka je $NZD(a, b) = d > 0$ i neka $p \mid d$, gde je p prost broj. Uzmimo $\alpha = ord_p a$ i $\beta = ord_p b$, pa iz (2.9), kao u prethodnom dokazu dobijamo

$$x_1 \alpha = y_1 \beta, \tag{2.26}$$

a iz leme 2.4 sledi $x_2\alpha < y_2\beta$, tj.

$$x_2\alpha + 1 \leq y_2\beta. \tag{2.27}$$

Možemo zaključiti

$$ord_p c = x_2\alpha. \tag{2.28}$$

Iz (2.1) dobijamo

$$(b^{y_1} + c)^{\frac{x_2}{x_1}} - b^{y_2} = c, \tag{2.29}$$

pa za svako fiksirano c imamo ocene za a i b.

Ako je c kvadratno slobodno (nijedan potpun kvadrat osim 1 ga ne deli), onda iz (2.28) sledi da $x_2 = 1$, tj. ne možemo imati dva rešenja.

Posmatramo zato samo vrednosti c, gde c nije kvadratno slobodan. Dokaz dajemo za $c = 4, 8, 9$, a ostale vrednosti $c \leq 100$ se slično ispituju.

- $c = 4$: Iz pretpostavke i (2.28) sledi $NZD(a, b) = 2$, pa imamo $x_2 = 2$ i $\alpha = 1$, odakle dobijamo $x_1 = 1$. Koristeći (2.26) dobijamo i $y_1 = \beta = 1$. Sada iz (2.27) imamo $y_2 > 3$, pa iz (2.29) sledi

  $$(b + 4)^2 - b^3 \geq 4.$$

  Lako dobijamo da je $b \leq 3$, a pošto $2 \mid b$, sledi $b = 2$, odakle dobijamo $a \leq 7$. Direktnom proverom dobijamo da ovaj slučaj odgovara slučaju $(a, b, c) = (6, 2, 4)$ iz postavke teoreme.

- $c = 8$: Iz pretpostavke dobijamo $NZD(a, b) = 2$ i $\alpha x_2 = 3$, pa imamo $\alpha = 1$, $x_2 = 3$. Posmatramo dva slučaja:

  - $x_1 = 1$: Slično kao ranije dolazimo do

    $$(b + 8)^3 - b^4 \geq 8.$$

    Sledi $b \leq 7$, a iz $ord_2 b = 1$ sledi $b = 2$ ili $b = 6$. Tada imamo ili $2^{y_2} = 992$ ili $6^{y_2} = 2736$, kontradikcija.

  - $x_1 = 2$: Iz pretpostavke sledi, na osnovu (2.26), $y_1\beta = 2$.

    * $y_1 = 1$: Slično kao u prethodnim slučajevima imamo

      $$(b + 8)^{\frac{3}{2}} - b^3 \geq 8.$$

      Dakle $b \leq 3$, kontradikcija sa $\beta = 2$.

    * $y_1 = 2$: Lako dobijamo

      $$(b^2 + 8)^{\frac{3}{2}} - b^5 \geq 8.$$

      Sledi $b = 2$, odakle imamo $a^{x_1} = a^2 = 2^2 + 8 = 12$, kontradikcija.

  U ovom slučaju jednačina ima najviše jedno rešenje.

- $c = 9$: Iz pretpostavke slično kao u prethodnim slučajevima imamo $x_1 = y_1 = \alpha = \beta = 1$ i $x_2 = 2$. Sledi

$$(b+9)^2 - b^3 \geq 9,$$

što implicira $b \leq 6$. Imamo slučajeve $b = 3$ i $b = 6$, gde prvi implicira $3^{y_2} = 135$, kontradikcija, dok iz drugog dobijamo slučaj $(a, b, c) = (15, 6, 9)$, koji je naveden u tvrđenju teoreme.

$\square$

3 Problem Erdősa i Grahama

U knjizi [8, str. 80] Erdős i Graham postavljaju pitanje: da li jednačina

$$(p-1)! + a^{p-1} = p^k, \tag{3.1}$$

gde us a, p, k prirodni brojevi i $p > 2$ prost broj, ima konačno mnogo rešenja. Sam Erdős (u saradnji sa Brindzom) u radu [6] dokazao je da postoji efektivno izračunjiva konstanta C tako da sva rešenja jednačine (3.1) ispunjavaju $\max\{a, p, k\} \leq C$, što naravno implicira da jednačina ima samo konačno mnogo rešenja. U određenim specijalnim slučajevima: $a = 1$ odnosno $p = 3$, Liouville i Apery su pronašli sva rešenja ove jednačine. U ovom delu rada pokazujemo da su to i jedina rešenja ove jednačine.

3.1 Teoreme Liouvillea i Aperyja

Prvo nalazimo sva rešenja jednačine (3.1) u slučajevima $a = 1$ odnosno $p = 3$.

Liouville je u radu [10] pokazao sledeću teoremu.

Teorema 3.1 (Liouville)**.** *Ako $a = 1$, onda jednačina* (3.1) *ima tačno dva rešenja*

$$(p, a, k) \in \{(3, 1, 1), (5, 1, 2)\}. \tag{3.2}$$

Dokaz. Ako je $a = 1$, tada je jednačina (3.1) oblika

$$1 \cdot 2 \cdot 3 \cdot \dots \cdot (p-1) + 1 = p^k. \tag{3.3}$$

Za $2 < p \leq 5$ dobijamo rešenja iz pretpostavke teoreme, pa pretpostavimo $p \geq 7$. Oduzimajući 1 od leve i desne strane jednakosti (3.3) i deleći sa $p - 1$ dobijamo

$$1 \cdot 2 \cdot 3 \cdot \dots \cdot (p-2) = p^{k-1} + p^{k-2} + \cdots p + 1.$$

Kako je $p \geq 7$, onda su 2 i $\frac{p-1}{2}$ različiti faktori proizvoda sa leve strane prethodne jednakosti, pa je leva strana deljiva sa $p - 1$, odakle dobijamo

$$p - 1 \mid p^{k-1} + p^{k-2} + \cdots p + 1. \tag{3.4}$$

Koristeći činjenicu

$$p^i \equiv 1 \pmod{p-1},$$

sledi

$$p^{k-1} + p^{k-2} + \cdots p + 1 \equiv \underbrace{1 + 1 + \cdots + 1}_{k-1} + 1 = k \pmod{p-1},$$

te u kombinaciji sa (3.4) dobijamo $p - 1 \mid k$, pa specijalno

$$k \geq p - 1.$$

Sada imamo ocenu

$$1 \cdot 2 \cdot 3 \cdot \dots \cdot (p-1) = p^k - 1 \geq p^{p-1} - 1,$$

ali to je u kontradikciji sa

$$1 \cdot 2 \cdot 3 \cdot \dots \cdot (p-1) < (p-1)^{p-1} < p^{p-1} - 1.$$

Sledi da jednačina (3.3) nema rešenja za $p \geq 7$. $\square$

Na osnovu rezultata iz rada [1], imamo sledeću teoremu koja nam daje sva rešenja za slučaj $p = 3$. Dokaz koji ovde navodimo je nezavisan od dokaza iz rada [1], zbog nedostupnosti tog rada.

Teorema 3.2 (Apery). *Ako $p = 3$, onda jednačina* (3.1) *ima tačno dva rešenja:*

$$(p, a, k) \in \{(3, 1, 1), (3, 5, 3)\}. \tag{3.5}$$

Dokaz. Ako je $p = 3$, tada je jednačina (3.1) oblika

$$a^2 + 2 = 3^k$$

ili ekvivalentno

$$(a + \sqrt{-2})(a - \sqrt{-2}) = 3^k. \tag{3.6}$$

Sada posmatramo datu jednačinu nad prstenom $\mathbb{Z}[\sqrt{-2}]$, koji je domen jedinstvene faktorizacije. U ovom prstenu 3 nije prost broj, može se faktorisati kao $3 = (1 + \sqrt{-2})(1 - \sqrt{-2})$, pa jednačina postaje

$$(a + \sqrt{-2})(a - \sqrt{-2}) = (1 + \sqrt{-2})^k (1 - \sqrt{-2})^k.$$

Pokažimo da su $a + \sqrt{-2}$ i $a - \sqrt{-2}$ uzajamno prosti. Pretpostavimo suprotno, tj. postoji p, prost broj u $\mathbb{Z}[\sqrt{-2}]$, tako da $p \mid a + \sqrt{-2}$ i $p \mid a - \sqrt{-2}$. Onda p deli i njihovu razliku

$$p \mid (a + \sqrt{-2}) - (a - \sqrt{-2}) = 2\sqrt{-2}.$$

Neka je $N(a + b\sqrt{-2}) = (a + b\sqrt{-2})(a + b\sqrt{-2}) = a^2 + 2b^2$ norma prstena $\mathbb{Z}[\sqrt{-2}]$. Iz teorije prstena znamo da, ako $p \mid q$ u posmatranom prstenu, tada važi i $N(p) \mid N(q)$. U našem slučaju, kako je $N(2\sqrt{-2}) = 8$, dobijamo $N(p) \mid 8$, pa sledi $2 \mid N(p)$, ali onda imamo da $2 \mid N(3^k) = 9^k$, kontradikcija.

Sada, iz (3.6) sledi da mora važiti

$$a + \sqrt{-2} = (1 + \sqrt{-2})^k;$$
$$a - \sqrt{-2} = (1 - \sqrt{-2})^k$$

ili obrnuto. Dobijamo

$$\begin{aligned}
\pm 2\sqrt{-2} &= (1+\sqrt{-2})^k - (1-\sqrt{-2})^k \\
&= \sum_{i=0}^{k} \binom{k}{i} (\sqrt{-2})^i - \sum_{i=0}^{k} \binom{k}{i} (-\sqrt{-2})^i \\
&= \sum_{i=0}^{k} \binom{k}{i} \left((\sqrt{-2})^i - (-\sqrt{-2})^i\right) \\
&= \sum_{\substack{i=0 \\ 2\nmid i}}^{k} \binom{k}{i} 2(\sqrt{-2})^i.
\end{aligned}$$

Deleći levu i desnu stranu sa $2\sqrt{-2}$ stižemo do

$$\pm 1 = \sum_{\substack{i=0 \\ 2\nmid i}}^{k} \binom{k}{i} (\sqrt{-2})^{i-1} = \binom{k}{1} - 2\binom{k}{3} + 4\binom{k}{5} - 8\binom{k}{7} + 16\binom{k}{9} - \cdots .$$

Pokažimo da ova jednakost ne važi ni za jedno $k > 3$. Posmatrajući ovu jednakost po modulu 2 dobijamo

$$\pm 1 \equiv k \pmod 2,$$

sledi da je k neparno. Po modulu 4 imamo

$$\pm 1 \equiv k - \frac{k(k-1)(k-2)}{3} \pmod 4,$$

pa množeći sa 3 levu i desnu stranu dobijamo

$$\pm 3 \equiv 3k - k(k-1)(k-2) \pmod 4,$$

a i u slučaju $k \equiv 1 \pmod 4$ i slučaju $k \equiv 3 \pmod 4$ važi da je desna strana poslednje kongruencije kongruentna sa 3, pa slučaj -1 otpada.

Razmatramo dva slučaja:

- $k \equiv 1 \pmod 4$: Neka je $t = ord_2(k-1) \geq 2$. Za neparno $i \geq 7$ važi

$$(-2)^{\frac{i-1}{2}} \binom{k}{i} = (-2)^{\frac{i-1}{2}} \frac{k(k-1)}{i(i-1)} \binom{k-2}{i-2} \equiv 0 \pmod{2^{t+1}},$$

jer $|(-2)^{\frac{i-1}{2}}| > i-1$, pa $2 \mid \frac{(-2)^{\frac{i-1}{2}}}{i-1}$. Dobijamo

$$1 \equiv k - \frac{k(k-1)(k-2)}{3} + \frac{k(k-1)(k-2)(k-3)(k-4)}{30} \pmod{2^{t+1}}.$$

Kako je

$$k \equiv 2^t + 1 \pmod{2^{t+1}},$$

$$\frac{k(k-1)(k-2)}{3} \equiv 2^t \pmod{2^{t+1}}$$

(jer su $k(k-2)$ i 3^{-1}, posmatran kao inverz po modulu 2^{t+1}, neparni brojevi, pa imamo neparan umnožak broja $k-1$) i

$$\frac{k(k-1)(k-2)(k-3)(k-4)}{30} \equiv 2^t \pmod{2^{t+1}}$$

(jer su $k(k-2)(k-4)$, $\frac{k-3}{2}$ i 15^{-1} neparni brojevi), sledi

$$1 \equiv 2^t + 1 - 2^t + 2^t = 2^t + 1 \pmod{2^{t+1}},$$

kontradikcija.

- $k \equiv 3 \pmod 4$: Neka je $s = ord_2(k-3) \geq 2$. Za neparno $i \geq 7$, slično kao u prethodnom slučaju, dobijamo

$$\begin{aligned}(-2)^{\frac{i-1}{2}}\binom{k}{i} &= (-2)^{\frac{i-1}{2}}\frac{k(k-1)(k-2)(k-3)}{i(i-1)(i-2)(i-3)}\binom{k-4}{i-4}\\ &\equiv 0 \pmod{2^{t+1}},\end{aligned}$$

pa sledi

$$\begin{aligned}1 &\equiv k - \frac{k(k-1)(k-2)}{3} + \frac{k(k-1)(k-2)(k-3)(k-4)}{30}\\ &\equiv 2^s + 3 - (2^s+2) + 2^s\\ &\equiv 2^s + 1 \pmod{2^{s+1}},\end{aligned}$$

kontradikcija. Kongruencije za prvi i treći sabirak dobijamo slično kao u prethodnom slučaju, a za drugi sabirak imamo

$$3^{-1}(2^s+3)(2^s+2)(2^s+1) \equiv 3^{-1}(3\cdot 2^s\cdot 1 + 3\cdot 2\cdot 1) = 2^s + 2 \pmod{2^{s+1}}.$$

Trivijalno se proverava da su (3.5) zaista rešenja jednačine (3.6). Sledi tvrđenje teoreme. □

3.2 Pomoćna tvrđenja

Dokazujemo nekoliko tvrđenja koja su nam od izuzetnog značaja u dokazu glavne teoreme ovog dela rada.

Lema 3.3. *Jednačina* (3.1) *nema rešenje* (p, a, k) *ako je* $p \geq 5$ *i* k *neparno.*

Dokaz. Dokaz sprovodimo koristeći teoriju kvadratnih ostataka.

Pretpostavimo suprotno, tj. postoji rešenje jednačine (3.1), (p, a, k), gde je $p \geq 5$ i k neparno. Tada važi

$$p^k - a^{p-1} = (p-1)! \equiv 0 \pmod q$$

za svaki prost broj $2 < q < p$. Kako $q \nmid p$ sledi i $q \nmid a$. Odavde, primenom tvrđenja 1.13 dobijamo

$$\left(\frac{p}{q}\right)^k = \left(\frac{a}{q}\right)^{p-1} = (\pm 1)^{p-1} = 1,$$

a kako je k neparno, ostaje da mora biti

$$\left(\frac{p}{q}\right) = 1. \tag{3.7}$$

Razmotrimo sad dva slučaja:

- $p \equiv 1 \pmod 4$: Iz tvrđenja 1.13 dobijamo

$$\left(\frac{p-1}{p}\right) = \left(\frac{-1}{p}\right) = 1.$$

  Na osnovu Gaussovog zakona kvadratne recipročnosti iz (3.7), pod datim uslovom, dobijamo

$$\left(\frac{q}{p}\right) = 1.$$

  Koristeći ovo u kombinaciji sa (1.1) dobijamo da za svako $k = 1, 2 \ldots, \frac{p-1}{2}$ važi

$$\left(\frac{2k-1}{p}\right) = 1.$$

  Iz ovoga sledi da su brojevi $1, 3, \ldots, p-2$ i $p-1$ kvadratni ostaci po modulu p, njih ima $\frac{p-1}{2} + 1$, što je u kontradikciji sa tvrđenjem 1.11.

- $p \equiv 3 \pmod 4$: Kombinujući (3.7) sa Gausovim zakonom kvadratne recipročnosti imamo

$$\begin{aligned}\left(\frac{q}{p}\right) &= \begin{cases} \left(\frac{p}{q}\right), & \text{ako je bar jedan od } p \text{ i } q \text{ oblika } 4k+1; \\ -\left(\frac{p}{q}\right), & \text{inače,} \end{cases} \\ &= \begin{cases} 1, & \text{ako } q \text{ prost, } q < p \text{ i } q \equiv 1 \pmod 4; \\ -1, & \text{ako } q \text{ prost, } q < p \text{ i } q \equiv 3 \pmod 4. \end{cases}\end{aligned}$$

  Sada dobijamo

$$\left(\frac{p-12}{p}\right) = \left(\frac{-3}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{3}{p}\right) = (-1)(-1) = 1. \tag{3.8}$$

  Sa druge strane, iz (3.7) sledi $\left(\frac{p}{3}\right) = 1$, pa iz tvrđenja 1.12 dobijamo $p \equiv 1 \pmod 3$. Kombinujući to sa pretpostavkom ovog slučaja dobija se da važi $4p \equiv 4 \pmod{12}$ i $3p \equiv 9 \pmod{12}$, pa oduzimanjem sledi $p \equiv 7 \pmod{12}$. Kako je $\left(\frac{7}{5}\right) = -1$ i $\left(\frac{11-12}{11}\right) = \left(\frac{-1}{11}\right) = -1$, sledi da $p = 7$ i

$p = 11$ ne zadovoljava (3.7) odnosno (3.8), pa mora biti $p \geq 19$. Ako bi $p - 12$ imao paran broj prostih faktora kongruentnih sa 3 po modulu 4, onda bismo imali

$$p \equiv p - 12 \equiv 3^2 \cdot 3^2 \cdots 3^2 \cdot 1 \cdot 1 \cdots 1 - 0 \equiv 1 \pmod 4,$$

što nije moguće jer je $p \equiv 3 \pmod 4$. Ali onda činjenica da $p - 12$ ima neparan broj prostih faktora kongruentnih sa 3 po modulu 4 implicira da

$$\left(\frac{p-12}{p}\right) = -1,$$

što je kontradikcija sa (3.8).

$\square$

Lema 3.4. *Ako je (p, a, q) rešenje jednačine (3.1), različito od rešenja datih u (3.2) i (3.5), tada je $p \geq 5$, $a \geq p + 2$, $2 \mid k$ i važi*

$$p + 1 \leq k < 2\frac{\ln \Gamma(p)}{\ln p} < 2p - 6. \tag{3.9}$$

Ako je i $p \equiv 1 \pmod 4$, onda imamo

$$k < 2\frac{\ln \Gamma(p) - (p-1)\ln 2 + \ln(p-1)}{\ln p}. \tag{3.10}$$

Ako je $p \geq 11$, tada

$$\frac{-1.02 \cdot (p-1)!}{p^k} < (p-1)\ln a - k \ln p < 0 \tag{3.11}$$

i

$$\{p^{\frac{k}{(p-1)}}\} < 1.02 \cdot (p-2)! p^{-\frac{(p+1)(p-2)}{p-1}}, \tag{3.12}$$

gde je $\{x\}$ razlomljeni deo od x.

Dokaz. Na osnovu teorema Liouvillea i Aperyja i leme 3.3 imamo $p \geq 5$, $a \geq p + 2$, $2 \mid k$.

Primetimo da je a neparno (u suprotnom imamo $2 \mid p$), i da najveći prost faktor od a mora biti veći od p (u suprotnom $p \mid (p-1)!$). Sledi da $a \geq p + 2$, pa kombinujući sa (3.1) direktno dobijamo ocenu

$$p^{p-1} < a^{p-1} < p^k.$$

Kako je k parno, odavde imamo $k \geq p + 1$. Ponovo koristeći 3.1 dobijamo

$$(p^{\frac{k}{2}} + a^{\frac{p-1}{2}})(p^{\frac{k}{2}} - a^{\frac{p-1}{2}}) = (p-1)!. \tag{3.13}$$

Pošto je $p^{\frac{k}{2}} > a^{\frac{p-1}{2}}$, sledi da je

$$p^{\frac{k}{2}} < (p-1)! < p^{p-3}$$

(koristili smo $2 \cdot 3 \cdot 4 < p^2$). Logaritmujući ovu nejednakost dobijamo (3.9).

Pretpostavimo sad da je $p \equiv 1 \pmod 4$. Tada broj $p-1$ zapisan u bazi 2 ima oblik

$$p - 1 = \sum_{j=2}^{t-1} a_j 2^j + 2^t,$$

gde $a_j \in \{0, 1\}$ za $2 \leq j \leq t-1$. Neka $s(x)$ označava zbir cifara broja x u bazi 2. Tada imamo

$$s(p-1) = a_2 + \cdots + a_{t-1} + 1 \leq t - 1 \leq \frac{\ln(p-1)}{\ln 2} - 1.$$

Primetimo da važi

$$ord_2(p-1)! = p - 1 - s(p-1).$$

Iz pretpostavke imamo $a^{\frac{p-1}{2}} \equiv p^{\frac{k}{2}} \equiv 1 \pmod 4$, pa sledi $p^{\frac{k}{2}} + a^{\frac{p-1}{2}} \equiv 2 \pmod 4$, odakle dobijamo

$$ord_2\left(p^{\frac{k}{2}} + a^{\frac{p-1}{2}}\right) = 1.$$

Iz (3.13) dobijamo

$$\begin{aligned} ord_2\left(p^{\frac{k}{2}} - a^{\frac{p-1}{2}}\right) &= ord_2(p-1)! - 1 \\ &= p - 1 - s(p-1) - 1 \\ &\geq p - 1 - \frac{\ln(p-1)}{\ln 2}, \end{aligned}$$

pa sledi

$$p^{\frac{k}{2}} - a^{\frac{p-1}{2}} \geq \frac{2^{p-1}}{p-1}.$$

Kombinujući sa (3.13) imamo

$$p^{\frac{k}{2}} < (p-1)! \frac{p-1}{2^{p-1}}.$$

Logaritmujući ovu nejednakost stižemo do (3.10).

Da bismo dokazali (3.11), posmatrajmo funkciju

$$f(x) = 1.02(1 - e^x) + x$$

na intervalu $(-0.01, 0)$. Na tom intervalu $f'(x) = -1.02e^x + 1 < 0$, tj. posmatrana funkcija opada, pa imamo da $f(x) > f(0) = 0$ za $x \in (-0.01, 0)$. Neka je

$$\lambda = (p-1) \ln a - k \ln p.$$

Tada važi, koristeći do sada dokazano i $p \geq 11$,

$$1 - e^{\lambda} = 1 - a^{p-1}p^{-k} = \frac{p^k - a^{p-1}}{p^k} = \frac{(p-1)!}{p^k} \leq \frac{10!}{11^{11+1}} = \frac{10}{11^{12}}.$$

Kako je $\lambda < 0$, iz prethodne nejednakosti zaključujemo $-0.01 < \lambda < 0$. Sve ukupno imamo $f(\lambda) > 0$, tj.

$$\lambda > -1.02\frac{(p-1)!}{p^k},$$

što je i traženo.

Ostaje nam jos da pokažemo (3.12). Iz dosada dokazanog imamo

$$1 < \frac{p+1}{p-1} \leq \frac{k}{p-1} < \frac{2p-6}{p-1} < 2,$$

što znači da $\frac{k}{p-1} \notin \mathbb{Z}$, pa onda i $d := p^{\frac{k}{p-1}} \notin \mathbb{Z}$. Neka je $c := d \cdot \exp(-1.02 \cdot \frac{(p-2)!}{p^k})$. Tada imamo

$$c = d \cdot \exp\left(-1.02 \cdot \frac{(p-2)!}{p^k}\right) < p^{\frac{k}{p-1}} \cdot \frac{a^{p-1}}{p^k} < a < d.$$

Pošto je $a \in \mathbb{Z}$, sledi

$$\begin{aligned}
\{d\} < d - c &= d\left(1 - \exp\left(-1.02 \cdot \frac{(p-2)!}{p^k}\right)\right) \\
&< 1.02 \cdot p^{\frac{k}{p-1}} \frac{(p-2)!}{p^k} \\
&= 1.02 \cdot (p-2)! p^{-\frac{k(p-2)}{p-1}} \\
&\leq 1.02 \cdot (p-2)! p^{-\frac{(p+1)(p-2)}{p-1}},
\end{aligned}$$

što je i traženo. □

Posebno naglašavamo poslednju nejednakost u prethodnoj lemi, nju ćemo koristiti kao efikasan indikator da pokažemo da nešto nije rešenje jednačine.

Lema 3.5. *Ako je $x > 2 \cdot 10^5$, tada je*

$$\frac{d}{dx} \ln \Gamma(x) < \ln x - \frac{1}{x} + 0.0001,$$

gde je $\Gamma(x)$, gama funkcija

$$\Gamma(x) = \int_0^{\infty} t^{x-1} e^{-t} dt.$$

Dokaz. Iz knjige [25, str. 241] koristimo činjenicu

$$\frac{d}{dx}\ln\Gamma(x) = -\gamma - \frac{1}{x} + x\sum_{n=0}^{\infty}\frac{1}{n(x+n)},$$

gde je γ Ojlerova konstanta

$$\gamma = \lim_{n\to\infty}\left(-\ln n + \sum_{n=1}^{\infty}\frac{1}{n}\right).$$

Važi

$$\begin{aligned}
\frac{d}{dx}\ln\Gamma(x) &\leq -\gamma - \frac{1}{x} + x\sum_{n=1}^{\infty}\frac{1}{n(\lfloor x\rfloor+n)}\\
&< -\gamma - \frac{1}{x} + \lfloor x\rfloor\sum_{n=1}^{\infty}\frac{1}{n(\lfloor x\rfloor+n)} + \sum_{n=1}^{\infty}\frac{1}{n(2\cdot 10^5+n)}\\
&= -\gamma - \frac{1}{x} + \left(1+\frac{1}{2}+\cdots+\frac{1}{\lfloor x\rfloor}\right) + \sum_{n=1}^{\infty}\frac{1}{n(2\cdot 10^5+n)}\\
&< \ln x + \frac{1}{x} + 0.0001;
\end{aligned}$$

zaista, gornja jednakost sledi zbog

$$\sum_{n=1}^{\infty}\frac{\lfloor x\rfloor}{n(\lfloor x\rfloor+n)} = \sum_{n=1}^{\infty}\left(\frac{1}{n} - \frac{1}{\lfloor x\rfloor+n}\right) = 1+\frac{1}{2}+\cdots+\frac{1}{\lfloor x\rfloor},$$

a za poslednju nejednakost koristimo činjenicu da za dovoljno veliko x važi

$$-\gamma + \left(1+\frac{1}{2}+\cdots+\frac{1}{\lfloor x\rfloor}\right) - \ln x \leq 2.5\cdot 10^{-6} \tag{3.14}$$

i

$$\sum_{n=1}^{\infty}\frac{1}{n(2\cdot 10^5+n)} < 9.9\cdot 10^{-5}.$$

□

3.3 Glavna teorema

Teorema 3.6 (Yu, Liu [11]). *Jednačina* (3.1) *nema rešenja osim* (3.2) *i* (3.5).

Dokaz. Pretpostavimo suprotno, neka je (p, a, k) rešenje različito od (3.2) i (3.5).

Posmatrajmo linearnu formu

$$\Lambda = \frac{1}{2}k\ln p - \frac{1}{2}(p-1)\ln a.$$

Iz (3.11) direktno dobijamo gornju ocenu za ovu linearnu formu

$$\ln|\Lambda| < \ln\left(\frac{1}{2}\cdot\frac{1.02\cdot(p-1)!}{p^k}\right) = \ln 0.51 + \ln(p-1)! - k\ln p. \tag{3.15}$$

Da bismo dobili donje ograničenje koristimo teoremu 1.21. Parametre iz teoreme biramo na sledeći način:

$$\alpha_1 = a, \qquad \alpha_2 = p, \qquad b_1 = \frac{p-1}{2}, \qquad b_2 = \frac{k}{2}.$$

Imamo da je $D = 1$, a uzmimo

$$A_1 = p^{\frac{k}{p-1}} \quad \text{ i } \quad A_2 = p.$$

Kako za $x \in \mathbb{N}$ važi $h(x) = \ln x$, imamo

$$\begin{aligned}\ln A_1 &= \frac{k}{p-1}\ln p > \max\{h(a), \ln(a), 1\},\\ \ln A_2 &= \ln p = \max\{h(p), \ln(p), 1\}\\ b' &= \frac{p-1}{\ln p}.\end{aligned}$$

Pretpostavimo $p > 2\cdot 10^5$. Tada je $\ln b' + 0.72 > 10 = \frac{10}{D}$, pa iz teoreme 1.21 sledi

$$\ln|\Lambda| \geq -32.31\left(\ln\left(\frac{p-1}{\ln p}\right) + 0.71\right)^2 \frac{k}{p-1}\ln^2 p.$$

Kombinujući sa (3.15) dobijamo

$$-32.31\left(\ln\left(\frac{p-1}{\ln p}\right) + 0.71\right)^2 \frac{k}{p-1}\ln^2 p \leq \ln|\Lambda| < \ln 0.51 + \ln(p-1)! - k\ln p,$$

što je ekvivalentno sa (koristimo $\Gamma(p) = (p-1)!$)

$$\frac{k\ln p}{p-1}\left\{p - 1 - 32.31\left(\ln\left(\frac{p-1}{\ln p}\right) + 0.71\right)^2 \ln p\right\} - \ln\Gamma(p) - \ln 0.51 < 0. \tag{3.16}$$

Posmatrajmo sad funkciju

$$\begin{aligned}f(x) = (x+1)\ln x - 32.31&\left(1 + \frac{2}{x-1}\right)\\ &\cdot\{\ln x\cdot(\ln(x-1) - \ln\ln x + 0.71)\}^2\\ &- \ln\Gamma(x) - \ln 0.51.\end{aligned}$$

Koristeći lemu 3.5 i pretpostavku $x > 2 \cdot 10^5$ dobijamo

$$\begin{aligned}f'(x) > 1 - 0.0001 - 64.62 &\left(1 + \frac{2}{x-1}\right) \ln x(\ln(x-1) - \ln\ln x + 0.71) \\ &\cdot \left\{ \frac{\ln(x-1) - \ln\ln x + 0.71}{x} + \ln x \cdot \left(\frac{1}{x-1} - \frac{1}{x \ln x} \right) \right\} \\ &> 0.1,\end{aligned}$$

što implicira da je $f(x)$ rastuća funkcija.

Pošto je $p > 2 \cdot 10^5$, tada se lako vidi da važi

$$p - 1 - 32.31 \left(\ln \left(\frac{p-1}{\ln p} \right) + 0.71 \right)^2 \ln p > 0, \tag{3.17}$$

pa koristeći (3.9) dobijamo da (3.16) važi za $k = p + 1$. Kako je $f(p)$ baš leva strana nejednakosti (3.16), imamo da je to rastuća funkcija. Uz pomoć *Mathematice* (imajući u vidu da je p prost) dobijamo da važi $f(823309) = -7.04293...$, a $f(823337) = 12.4182...$, pa zbog (3.16) mora da važi

$$p \leq 823309.$$

Posebno razmatramo dva slučaja:

- $p \in \{5, 7\}$: Na osnovu pretpostavke direktno dobijamo $p+1 \geq 2p-6$, što je kontradikcija sa (3.9). To znači da (3.1) nema rešenja u ovom slučaju.
- $11 \leq p \leq 823309$: U ovom slučaju uz pomoć *Mathematice* pokazaćemo da jednačina (3.1) nema rešenja. Prvo moramo naći granice za k. Da ne bismo u potpunosti pretraživali grubom silom, posmatramo dva podslučaja:
  - $p \equiv 1 \pmod 4$: Iz leme 3.4 tada znamo da za k mora važiti (3.9) i (3.10), pa posmatramo samo k za koja važe dva navedena uslova.
  - $p \equiv 3 \pmod 4$: Tada iz leme 3.4 samo znamo da za k mora važiti (3.9), pa posmatramo samo takva k.

  U oba slučaja za svaki posmatran par (p, k) dobijamo

  $$\{p^{\frac{k}{p-1}}\} > 1.02 \cdot (p-2)! p^{-\frac{(p+1)(p-2)}{p-1}},$$

  što je kontradikcija sa (3.12), pa ni u ovom slučaju nemamo rešenja jednačine (3.1).

$\square$

4 Jednačina oblika $(x^k-1)(y^k-1)=z^k-1$

Jedno zanimljivo pitanje je: kada je proizvod dva k-ta stepena umanjenih za jedan ponovo k-ti stepen umanjen za 1, tj. kada jednačina oblika

$$(x^k-1)(y^k-1)=z^k-1, \tag{4.1}$$

gde su x, y, z i k prirodni brojevi, ima rešenje. Npr. u slučaju $k=2$ imamo beskonačno mnogo rešenja, naime važi

$$(n^2-1)((n+1)^2-1)=(n^2+n-1)^2-1,$$

za $n \geq 2$. U ovom delu rada dajemo jedan parcijalni rezultat, tj. posmatramo specijalan slučaj $k>75$ i dokazujemo da jednačina (4.1) tada nema rešenja.

Prvo dokazujemo jednu pomoćnu lemu.

Lema 4.1. *Neka je $k \geq 3$ i neka su a i b prirodni bojevi za koje važi $2 \leq a \leq b$ i brojevi $a+1$, $b+1$ i $ab+1$ su k-ti stepeni. Tada je*

$$b \geq k^k \cdot \frac{a^{k-1}}{2}.$$

Dokaz. Iz

$$(a+1)(b+1)=ab+a+b+1>ab+1, \tag{4.2}$$

uzimajući k-ti koren leve i desne strane nejednakosti (i imajući u vidu da su posmatrani brojevi k-ti stepeni), lako dobijamo

$$(ab+1)^{\frac{1}{k}}+1 \leq ((a+1)(b+1))^{\frac{1}{k}}, \tag{4.3}$$

pa direktno sledi

$$\left((ab+1)^{\frac{1}{k}}+1\right)^k \leq (a+1)(b+1).$$

Primenom binomne formule imamo

$$\sum_{i=0}^{k}\binom{k}{i}(ab+1)^{\frac{k-i}{k}} \leq ab+1+a+b, \tag{4.4}$$

pa sledi (oduzmemo $ab+1$ od leve i desne strane)

$$k(ab+1)^{\frac{k-1}{k}} \leq a+b.$$

Stepenujući ovu nejednakost sa k dobijamo

$$k^k(ab)^{k-1} \leq k^k(ab+1)^{k-1} \leq (a+b)^k. \tag{4.5}$$

Ponovno primenom binomne formule dolazimo do sledeće nejednakosti

$$\begin{aligned}(a+b)^k &= b^k + \sum_{i=1}^{k} \binom{k}{i} a^i b^{k-i} \\ &\leq b^k + \sum_{i=1}^{k} \binom{k}{i} ab^{k-1} \\ &= b^k + ab^{k-1} \cdot \sum_{i=1}^{k} \binom{k}{i} \\ &\leq b^k + 2^k ab^{k-1},\end{aligned}$$

te u kombinaciji sa (4.5) sledi

$$k^k (ab)^{k-1} \leq b^k + 2^k ab^{k-1},$$

što je ekvivalentno sa

$$k^k a^{k-1} \leq b + 2^k a < b + k^k a.$$

Odavde dobijamo

$$b > k^k \cdot (a^{k-1} - 1),$$

pa sledi traženo. □

Teorema 4.2 (Bugeaud, [3]). *Jednačina* (4.1)*, gde su x, y, z, k prirodni brojevi i $z \geq 2$, nema rešenja za $k > 75$.*

Dokaz. Pretpostavimo suprotno, tj. postoje prirodni brojevi x, y, z, k takvi da važi $k > 75$ i $z \geq 2$ i da su oni rešenje jednačine (4.1). Tada očigledno postoje prirodni brojevi a i b takvi da važi

$$a + 1 = x^k, \qquad b + 1 = y^k, \qquad \text{i} \qquad ab + 1 = z^k.$$

Kako je $a^k + 1 \geq 2^k$, dobijamo

$$b \geq a > 2^{74}.$$

Posmatrajmo linearnu formu logaritama

$$\Lambda = \ln\left(\frac{a+1}{a}\right) - k \ln\left(\frac{xy}{z}\right).$$

Sada na ovu linearnu formu želimo da primenimo teoremu 1.19 sa parametrima

$$\alpha_1 = \frac{xy}{z}, \qquad \alpha_2 = \frac{a+1}{a}, \qquad b_1 = k, \qquad b_2 = 1.$$

Uzimamo $\rho = a$, pa $\lambda = \ln a$. Iz leme 4.1 sledi da je

$$\ln b \geq (k-1)\ln a + k \ln k - \ln 2, \tag{4.6}$$

a takođe važi

$$|\alpha_2 - 1| = \alpha_2 - 1 = \frac{1}{a},$$

pa se lako proverava da možemo uzeti

$$a_1 = 1 + \frac{2}{k}\ln((a+1)(b+1)) \quad \text{ i } \quad a_2 = 1 + 2\ln(a+1).$$

Pošto je $a \geq 2^{k-1}$, stavljamo $h = \frac{\lambda}{2}$ i $\chi = \chi_0 = \frac{1}{2}$. Onda imamo $v = 8$ i $m = 8\sqrt{2}$.

Primetimo da je među uslovima teoreme 1.19 i multiplikativna nezavisnost brojeva α_1 i α_2. Ova teorema se u radu [14] dokazuje preko teoreme 1.5, iz tog rada, a jedino mesto gde se koristi multiplikativna nezavisnost brojeva α_1 i α_2 jeste u dokazu teoreme 1.5 prilikom ustanovljavanja da skup $\{\alpha_1^r \alpha_2^s : 0 \leq r < R_1, 0 \leq s < S_1\}$ ima bar L elemenata (u skladu sa oznakama iz te teoreme). Međutim, kako pri našem izboru parametara važi $L = 2 + \lfloor \frac{2h}{\lambda} \rfloor = 2 + 1 = 3$, zapravo je dovoljno umesto multiplikativne nezavisnosti proveriti da su 1, α_1 i α_2 međusobno različiti (tada posmatrani skup ima bar 3 elementa), a ovo je očigledno ispunjeno. Dakle, možemo primeniti teoremu 1.19, iz koje sledi ocena

$$\ln|\lambda| \geq -\frac{17.64}{\ln a} a_1 a_2 - 2.5 \ln a - \ln(7.5 a_1). \tag{4.7}$$

Potrebna nam je još i gornja ocena za ovu linearnu formu. Pošto važi

$$\left| \frac{a+1}{a} - \left(\frac{xy}{z}\right)^k \right| = \frac{a^2-1}{b(a^2 + \frac{1}{b})} \leq \frac{a^2-1}{b(a^2-1)} \leq \frac{1}{b},$$

sledi

$$|\lambda| < e^{|\lambda|} - 1 = \frac{\left| \frac{a+1}{a} - \left(\frac{xy}{z}\right)^k \right|}{\left(\frac{xy}{z}\right)^k} \leq \frac{2}{b}.$$

Sada u kombinaciji sa (4.7) dobijamo

$$\frac{27}{k}\ln a + 2.5 \ln a + \ln(15 a_1) \geq \ln b - \frac{71.3}{k}\ln b,$$

pa uz pomoć (4.6) dobijamo

$$1 - \frac{71.3}{k} \leq \frac{72}{k(k-1)} + \frac{2.5}{k-1} + 0.003, \tag{4.8}$$

ali koristeći *Mathematicu* dobijamo da ova nejednakost važi za $k \leq 75$, kontradikcija. $\square$

5 Monocifarski Fibonačijevi brojevi

Fibonačijevi brojevi su zadati sledećom rekurentnom relacijom: $F_{n+2} = F_{n+1} + F_n$, sa početnim uslovima $F_1 = 1$, $F_2 = 1$. Rešavanjem ove rekurentne relacije dobijamo eksplicitan izraz za F_n,

$$F_n = \frac{\alpha^n - \beta^n}{\sqrt{5}},$$

gde je $\alpha = \frac{1+\sqrt{5}}{2}$ i $\beta = \frac{1-\sqrt{5}}{2}$ (oni su rešenja kvadratne jednačine $x^2 - x - 1 = 0$).

Monocifarski broj[3] je prirodan broj koji u bazi 10 ima sve cifre jednake.

U ovom delu rada tražimo sve monocifarske Fibonačijeve brojeve. Svedimo ovaj problem na problem rešavanja Diofantove jednačine. Ako je F_n m-tocifren monocifarski broj sa cifrom d, tada je on oblika

$$F_n = \overline{dd\cdots d}_{(10)} = d \cdot 10^{m-1} + d \cdot 10^{m-2} + \cdots + d = d\frac{10^m - 1}{10 - 1}, d \in \{1, \ldots, 9\}. \tag{5.1}$$

Za svako n, koje je rešenje ove Diofantove jednačine, F_n je monocifarski broj. Za $n = 10$ imamo $F_n = 55$. Dokažimo da je to najveće rešenje ove Diofantove jednačine.

Dokaz sprovodimo u dva koraka. Prvo primenom teoreme 1.17 dajemo grubu ocenu za n, a u drugom koraku primenom leme 1.9 smanjujemo tu granicu, tako da grubom silom „brzo” možemo ispitati preostale slučajeve za n.

Pretpostavimo da je $n > 1000$.

Gornja granica za n

Na početku dokažimo sledeću lemu.

Lema 5.1. *Za svako $n \geq 3$ važi $\alpha^{n-2} < F_n < \alpha^{n-1}$.*

Dokaz. Dokaz sprovodimo indukcijom po n. Za $n = 3, 4$ direktno proveravamo. Pretpostavimo da tvrđenje važi za $n - 2$ i $n - 1$. Tada imamo

$$\alpha^{n-4} < F_{n-2} < \alpha^{n-3};$$
$$\alpha^{n-3} < F_{n-1} < \alpha^{n-2},$$

pa sabiranjem datih nejednakosti dobijamo

$$\alpha^{n-4} + \alpha^{n-3} < F_{n-2} + F_{n-1} = F_n < \alpha^{n-3} + \alpha^{n-2}.$$

Pošto važi $\alpha^2 = \alpha + 1$, množenjem sa α^{n-3} dobijamo $\alpha^{n-1} = \alpha^{n-2} + \alpha^{n-3}$, pa sledi traženo. $\square$

[3]Eng. Monodigit ili Repdigit Number

Iz (5.1) dobijamo

$$\frac{\alpha^n - \beta^n}{\sqrt{5}} = d\frac{10^m - 1}{9},$$

što je ekvivalentno sa

$$\alpha^n - \frac{d\sqrt{5}}{9}10^m = \beta^n - \frac{d\sqrt{5}}{9}, \tag{5.2}$$

pa deljenjem leve i desne strane sa α^n sledi

$$1 - \frac{d\sqrt{5}}{9}10^m\alpha^{-n} = \frac{\beta^n - \frac{d\sqrt{5}}{9}}{\alpha^{-n}}.$$

Apsolutnu vrednost leve strane obeležimo sa Λ.

Sada uvedimo oznake tako da se podudaraju sa onim oznakama iz teoreme 1.17. Prirodno je uzeti sledeće vrednosti

$$\alpha_1 = \frac{d\sqrt{5}}{9}, \quad \alpha_2 = \alpha, \quad \alpha_3 = 10; \quad b_1 = 1, \quad b_2 = -n, \quad b_3 = m.$$

Za $\mathbb{L}$ uzimamo $\mathbb{Q}[\alpha_1, \alpha_2, \alpha_3] = \mathbb{Q}[\sqrt{5}]$, pošto $\alpha_1, \alpha_2\alpha_3 \in \mathbb{Q}[\sqrt{5}]$. Kako je $p^{\mathbb{Q}}_{\sqrt{5}}(x) = x^2 - 5$, a $\deg(p^{\mathbb{Q}}_{\sqrt{5}}(x)) = 2$, onda je $D = 2$.

Da bismo odredili $B = \max\{m, n, 1\} = \max\{m, n\}$, treba da uporedimo m i n. Kako je $F_n < 10^m$, onda iz nejednakosti iz prethodne leme imamo $\alpha^{n-2} < F_n < 10^m$, tj. logaritmovanjem leve i desne strane dobijamo

$$n < \frac{\ln 10}{\ln \alpha}m + 2.$$

Slično, koristeći prethodnu lemu i činjenicu da je $10^m < F_n$, dobijamo

$$n > \frac{\ln 10}{\ln \alpha}m - 4.$$

Sve ukupno imamo

$$\frac{\ln 10}{\ln \alpha}m - 4 < n < \frac{\ln 10}{\ln \alpha}m + 2,$$

tj.

$$4.78497... \cdot m - 4 < n < 4.78497... \cdot m + 2.$$

Iz pretpostavke $n > 1000$ i poslednje nejednakosti sledi da je $B = n$.

Odredimo konstante A_i, $i = 1, 2, 3$. Prvo određujemo logaritamske visine brojeva $\alpha_1, \alpha_2, \alpha_3$. Za α_1 minimalni polinom nad racionalnim brojevima je $x^2 - 5d^2/81 = (x - \alpha_1)(x + \alpha_1)$. Pošto je α_1 nula polinoma $81x^2 - 5d^2 \in \mathbb{Z}[x]$, onda minimalni polinom nad celim brojevima deli ovaj polinom. Primetimo da je jedini konjugat od α_1, $\alpha_1' = -\alpha_1$ i važi $|\alpha_1|, |\alpha_1'| < \sqrt{5}$. Sada imamo

$$h(\alpha_1) \leq \frac{1}{2}\left(\ln 81 + 2\ln\max\{\sqrt{5}, 1\}\right) = \frac{1}{2}\ln(405) < 3.01.$$

Treba nam $A_1 \geq \max\{2\cdot 3.01, |\ln\alpha_1|, 0.16\}$, pa možemo uzeti $A_1 = 6.02$. Slično se dobija da je $A_2 = 1.5$ i $A_3 = 4.62$.

Potrebno je još ispitati uslov teoreme, tj. proveriti da $\Lambda \neq 0$. Pretpostavimo suprotno. Tada je $\frac{d\sqrt{5}}{9}10^m\alpha^{-n} = 1$, pa $\sqrt{5}$ mora biti oblika $q\alpha^n$, $q \in \mathbb{Q}$. Ali tada je $5 = q^2\alpha^{2n} \in \mathbb{Q}$, a odatle sledi $\alpha^{2n} \in \mathbb{Q}$, kontradikcija.

Na osnovu teoreme 1.17 imamo

$$\ln|\Lambda| > -1.4\cdot 30^6\cdot 3^{4.5}\cdot 4\cdot(1+\ln 4)\cdot(1+\ln n)\cdot 6.02\cdot 1.5\cdot 4.62 \geq -5.77\cdot 10^{13}(1+\ln n).$$

Nađimo sada gornju ocenu za $\ln|\Lambda|$. Važi

$$|\Lambda| = \frac{1}{\alpha^n}\left|\beta^n - \frac{d\sqrt{5}}{9}\right| \leq \frac{1}{\alpha^n}\left(\left|\frac{-1}{\alpha^n}\right| + \sqrt{5}\right) < \frac{2.5}{\alpha^n} < \frac{1}{\alpha^{n-2}}$$

(kod prve nejednakosti koristili smo nejednakost trougla i činjenicu da je $\alpha\cdot\beta = -1$). Logaritmujući levu i desnu stranu ove nejednakosti dobijamo

$$\ln|\Lambda| < -(n-2)\ln\alpha.$$

Sve ukupno imamo

$$-1.2\cdot 10^{14}(1+\ln n) < \ln|\Lambda| < -(n-2),$$

tj.

$$n - 2 < 1.2\cdot 10^{14}(1+\ln n).$$

Uz pomoć *Mathematice* dobijamo da $n < 4.5\cdot 10^{15}$, a iz odnosa m i n imamo da je $m < 9.5\cdot 10^{14}$.

Poboljšanje granice

Pošto je $n > 1000$, tada je $|\beta^n| < d\sqrt{5}/9$, pa je $(\beta^n - d\sqrt{5}/9) < 0$. Sledi $\Lambda < 0$. Koristeći činjenicu da je

$$|\Lambda| < \frac{2.5}{\alpha^n},$$

dobijamo

$$-\frac{2.5}{\alpha^n} < 1 - \frac{d\sqrt{5}}{9}\alpha^{-n}10^m < 0,$$

što je ekvivalentno sa

$$0 < \frac{d\sqrt{5}}{9}\alpha^{-n}10^m - 1 < \frac{2.5}{\alpha^n}.$$

Iz prethodnog sledi

$$0 < \frac{d\sqrt{5}}{9}\alpha^{-n}10^m - 1 < \frac{2.5}{\alpha^n} < \frac{4}{\alpha^n}.$$

U prethodnom delu dokaza dobili smo $\alpha^n > 10^{m-1}$, pa imamo

$$0 < \frac{d\sqrt{5}}{9}\alpha^{-n}10^m - 1 < \frac{4}{10^{m-1}}.$$

Iz $\frac{d\sqrt{5}}{9}\alpha^{-n}10^m > 0$ i činjenice da je za $x > 0$, $e^x - 1 > x$ sledi

$$\begin{aligned}0 < \ln\left(\frac{d\sqrt{5}}{9}\alpha^{-n}10^m\right) &< e^{\ln\left(\frac{d\sqrt{5}}{9}\alpha^{-n}10^m\right)} - 1 \\ &= \frac{d\sqrt{5}}{9}\alpha^{-n}10^m - 1 < \frac{4}{10^{m-1}},\end{aligned}$$

tj.

$$0 < m\ln 10 - n\ln\alpha + \ln\left(\frac{d\sqrt{5}}{9}\right) < \frac{4}{10^{m-1}}.$$

Uvodeći oznake iz prethodnog dela dokaza dobijamo

$$0 < m\left(\frac{\ln\alpha_3}{\ln\alpha_2}\right) - n + \left(\frac{\ln\alpha_1}{\ln\alpha_2}\right) < \frac{4}{10^{m-1}\ln\alpha_2} < \frac{9}{10^{m-1}} < \frac{90}{10^m}.$$

Na ovu nejednakost primenićemo lemu 1.9. Prvo uvedimo oznake tako da se podudaraju sa onima iz uslova date leme. Stavimo

$$\gamma = \frac{\ln\alpha_3}{\ln\alpha_2}, \quad \mu = \frac{\ln\alpha_1}{\ln\alpha_2}, \quad A = 90, \quad B = 10.$$

Iz ocene za m vidimo da možemo uzeti $M = 10^{15}$. Sada uz pomoć *Mathematice* dobijamo, $q_{35} > 6M$, gde je $p_{35}/q_{35} = C_{35}$, 35-ta konvergenta verižnog razlomka koji predstavlja γ. Za računanje norme $\|x\|$ u *Mathematici* koristimo funkciju `Abs[x-Round[x]]`, pa dobijamo $M\|q_{35}\gamma\| < 0.01$ i $\|q_{35}\mu\| > 0.02$. Treba napomenuti da μ zavisi od broja d, pa pomoću koda

```
alpha = (1 + Sqrt[5])/2;
mu[d_] := Log[d Sqrt[5]/9]/Log[alpha];
Min[Table[Abs[q35*mu[d] - Round[q35*mu[d]]], {d, 1, 9}]]
```

dobijamo traženi minimum. Za $\varepsilon = 0.01 < \|q_35\mu\| - M\|q_35\gamma\|$ dobijamo

$$\frac{\ln(Aq_{35}\varepsilon^{-1})}{\ln B} = 21.2616...,$$

pa na osnovu leme 1.9 imamo da za $m \in [22, 10^{15}]$ nejednačina

$$0 < m\gamma - n + \mu < \frac{A}{B^m},$$

nema rešenja po m i n. Dakle, $m \leq 21$, pa dobijamo $n \leq 102$, što je u suprotnosti sa pretpostavkom $n > 1000$. Slučaj $10 < n \leq 1000$ proveravamo grubom silom u *Mathematici* ispisivajući $F_n \pmod{10000}$ (poslednje četiri cifre).

6 Binarni palindromi oblika $10^n \pm 1$

Podsetimo se prvo, broj N je palindrom u bazi b akko važi

$$N = \overline{a_1 a_2 \dots a_k}_{(b)} = \overline{a_k a_{k_1} \dots a_1}_{(b)}.$$

Primetimo da su za svako n brojevi $10^n - 1 = \overline{99\dots9}_{(10)}$ $10^n + 1 = \overline{100\dots01}_{(10)}$ palindromi u bazi 10. Postavlja se pitanje za koje vrednosti n je $10^n \pm 1$ binarni plaindrom? Sledeća teorema daje nam odgovor na to pitanje (za originalan dokaz pogledati [24]).

Teorema 6.1. *Jedine vrednosti n za koje je $10^n \pm 1$ binarni palindrom su $n = 1, 2$, tj. $9 = \overline{1001}_{(2)}$ i $99 = \overline{1100011}_{(2)}$.*

Dokaz. Poslednju cifru u bazi 2 broja $N = 10^n \pm 1$ dobijamo kao ostatak pri deljenju broja $10^n \pm 1$ sa 2. U oba slučaja poslednja cifra je 1. Posmatrajmo sada „+" slučaj. Narednu cifru dobijamo kao ostatak pri deljenju broja $\frac{10^n+1-1}{2} = \frac{10^n}{2} = 5 \cdot 10^{n-1}$ sa 2, pa vidimo da je ta cifra 0. U sledećem koraku posmatramo broj $5^2 \cdot 10^{n-2}$, pa je treća cifra zdesna ponovo 0. Vidimo da postupak možemo da ponovimo još $n-2$ puta, sa rezultatom 0, a onda posmatramo broj 5^n. Zaključujemo da u ovom slučaju poslednjih $n+1$ cifara broja $10^n + 1$ su $100 \cdots 01$, $n-1$ nula u sredini. Slično se pokazuje da u „$-$" slučaju N se završava sa $011\dots11$, n jedinica. Pošto je N palindrom, u „+" slučaju imamo da N počinje sa $100\cdots01$, a u slučaju „$-$" imamo da N počinje sa $11\dots110$.

Pretpostavimo da $n > 1000$. Neka je m broj cifara broja N. Važi

$$m = \left\lfloor \frac{\ln(10^n \pm 1)}{\ln 2} \right\rfloor + 1 = \left\lfloor \frac{n \ln 10}{\ln 2} \right\rfloor + 1 = n + \left\lfloor \frac{n \ln 5}{\ln 2} \right\rfloor + 1.$$

Neka je l broj cifara broja 5^n. Onda imamo

$$m = n + l + 1.$$

Iz opisanog postupka za dobijanje cifara broja N vidimo da se prvih $l-1$ cifara, u oba slučaja, poklapa sa prvih $l-1$ cifara broja 5^n. Pošto je $l - 1 \geq n$, to važi i za prvih n cifara.

Iz do sada navedenog imamo sledeću nejednakost za „+" slučaj

$$2^l < 5^n \leq 2^l + 2^{l-n} + 2^{l-n-1} + \dots + 1 < 2^{l-n+1}.$$

Za „$-$" slučaj, polazeći od $2^{l+1} > 5^n$, dobija se da važi $2^{l+1} > 5^n > 2^{l+1} - 2^{l-n+1}$. Sada, stavljajući $k = l$, $k = l + 1$, redom za „+" i „$-$" slučaj dobijamo

$$|5^n 2^{-k} - 1| < 2^{l-k-n+1} \leq 2^{-n+1}. \tag{6.1}$$

Sledeće oznake uvodimo tako da možemo da primenimo teoremu 1.18. Neka je

$$\Gamma = n \ln 5 - k \ln 2.$$

Uzimamo

$$\alpha_1 = 2, \quad \alpha_2 = 5; \quad b_1 = k, \quad b_2 = n.$$

$\square$

Sada imamo $\mathbb{Q}[2,5] = \mathbb{Q}$, pa je $D = 1$, a $B = \max\{n, k\} = k$. Lako se dobija da možemo uzeti $A_1 = 1.61$ i $A_2 = 1$, pa dobijamo

$$b' = n + \frac{k}{1.61}.$$

Pošto su 2 i 5 uzajamno prosti, onda su ispunjeni svi uslovi teoreme 1.18, pa sledi

$$-\ln|\Gamma| \le 23.34\left(\ln\left(n + \frac{k}{1.61}\right) + 0.14\right)^2 \cdot 1.61 \cdot 1.$$

Iz nejednakosti

$$n + \frac{k}{1.61} \le 3n + 3$$

dobijamo

$$-\ln|\Gamma| \le 37.58(\ln(3n+3) + 0.14)^2.$$

Koristeći do sada uvedene oznake, (6.1) postaje

$$|e^\Gamma - 1| < 2^{n-1}.$$

Pokažimo da važi

$$|\Gamma| < 2^{-n+2}.$$

Ako $\Gamma > 0$, tada direktno dobijamo (koristimo $n > 2$)

$$|\Gamma| = \Gamma < e^\Gamma - 1 < 2^{-n+1} < 2^{-n+2}.$$

Ako $\Gamma < 0$, onda iz

$$1 - e^{-|\Gamma|} < 2^{-n+1}$$

sledi

$$|\Gamma| < e^{|\Gamma|} - 1 < \frac{1}{1 - 2^{-n+1}} - 1 < 2^{-n+2}.$$

Sada dobijamo da važi

$$(n-2)\ln 2 < -\ln|\Gamma| \le 37.58(\ln(3n+3) + 0.14)^2, \tag{6.2}$$

i uz pomoć *Mathematice* dobijamo $n \le 5204$. Takođe pomoću *Mathematice* brzo se proveravaju preostale vrednosti za n.


"That's all Folks!"

Literatura

[1] R. Apéry. Sur une équation diophantienne. *Comptes Rendus Mathematique*, 251:1451–1452, 1960.

[2] M. A. Bennett. On Some Exponential Equations of S. S. Pillai. *Canadian Journal of Mathematics*, 53(5):897–922, 2001.

[3] Y. Bugeaud. On the diophantine equation $(x^k - 1)(y^k - 1) = (z^k - 1)$. *Indagationes Mathematicae*, 15(1):21–28, 2004.

[4] H. Cohen. *Number Theory*, volume 239 of *Graduate Texts in Mathematics.* Springer New York, 2007.

[5] W.A. Coppel. *Number Theory.* Springer New York, 2009.

[6] B. Brindza, P. Erdős. On some diophantine problems involving powers and factorials. *Journal of the Australian Mathematical Society*, 51(01):1–7, 1991.

[7] B. N. Delone, D. K. Faddeev. *The Theory of Irrationalities of the Third Degree.* American Mathematical Society, 1964.

[8] P. Erdős, R. L. Graham. *Old and new problems and results in combinatorial number theory.* L'Enseignement mathématique, Université de Genève, 1980.

[9] A. Y. Khinchin. *Continued Fractions.* Dover Publications, 1997.

[10] J. Liouville. Sur l'équation $1 \cdot 2 \cdot 3 \cdots (p-1) + 1 = p^m$. *Journal de mathématiques pures et appliquées*, 2(1):351–352, 1856.

[11] K. Yu, D. Liu. A Complete Resolution of a Problem of Erdős and Graham. *Rocky Mountain Journal of Mathematics*, 26(3):1235–1244, 1996.

[12] F. Luca. *Diophantine Equations.* Bordeaux, 2009.

[13] E. M. Matveev. An explicit lower bound for a homogeneous rational linear form in the logarithms of algebraic numbers. II. *Izvestiya: Mathematics*, 64(6):125–180, 2000.

[14] M. Mignotte. A corollary to a theorem of Laurent-Mignotte-Nesterenko. *Acta Arithmetica*, 86(2):101–111, 1998.

[15] P. Mihăilescu. Primary cyclotomic units and a proof of Catalan's conjecture. *Journal für die reine und angewandte Mathematik (Crelles Journal)*, 2004(572):167–195, 2006.

[16] L. Mordell. On the integer solutions of $y(y+1) = x(x+1)(x+2)$. *Pacific Journal of Mathematics*, 13(4):1347–1351, 1963.

[17] M. Laurent, M. Mignotte, Y. Nesterenko. Formes lineaires en deux logarithmes et determinants d'interpolation. *Journal of Number Theory*, 55(2):285–321, 1995.

[18] V. Perić. *Algebra: Dio 2*. Svjetlost, 1989.

[19] A. Dujella, A. Pethő. A generalization of a theorem of Baker and Davenport. *The Quarterly Journal of Mathematics*, 49(195):291–306, 1998.

[20] S. S. Pillai. On $a^x - b^y = c$. *The Journal of the Indian Mathematical Society*, 19:1–11, 1931.

[21] R. Scott. On the Equations $p^x - b^y = c$ and $p^x + b^y = c^z$. *Journal of Number Theory*, 44(2):153–165, 1993.

[22] Y. Bugeaud, M. Mignotte, S. Siksek. Classical and modular approaches to exponential Diophantine equations I. Fibonacci and Lucas perfect powers. *Annals of Mathematics*, 163:969–1018, 2006.

[23] R. Tijdeman. On the equation of catalan. *Acta Arithmetica*, 29(2):197–209, 1976.

[24] F. Luca, F. Togbé. On binary palindromes of the form $10^n \pm 1$. *Comptes Rendus Mathematique*, 346(s 9–10):487–489, 2008.

[25] E. T. Whittaker, G. N. Watson. *A course of modern analysis: an introduction to the general theory of infinite processes and of analytic functions; with an account of the principal transcendental functions*. Cambridge mathematical library. Cambridge Univ. Press, 4. ed., 6. print edition, 2006.

Biografija

Stefan Hačko je rođen 11. 8. 1993. u Kikindi, gde je i odrastao. Osnovnu školu „Đura Jakšić" i gimnaziju „Dušan Vasiljev" završio je u Kikindi sa prosekom 5.00, a takođe je završio i osnovnu muzičku školu sa odličnim uspehom. Osnovne studije matematike upisao je 2012. godine, u Novom Sadu na Prirodno-matematičkom fakultetu. Iste je završio za 2 godine i 10 meseci, sa prosekom 10.00 i ostvarenih 235 ESPB bodova, što mu je omogućilo da se 2015. direktno upiše na drugu godinu master akademskih studija matematike na istom fakultetu. Sve ispite predviđene planom i programom položio je zaključno sa junskim rokom 2016, sa prosekom 10.00 i time je stekao uslov za odbranu ovog rada.

Dobitnik je mnogih nagrada, stipendija i priznanja, među kojima se ističe „Nagrada najboljem studentu fakulteta" za školsku 2014/2015. godinu. Takođe je, dve godine zaredom, stipendista fonda za mlade talente „Dositeja".

U slobodno vreme voli da putuje i sluša operu.

Novi Sad, avgust 2016. **Stefan Hačko**

UNIVERZITET U NOVOM SADU
PRIRODNO-MATEMATIČKI FAKULTET
KLJUČNA DOKUMENTACIJSKA INFORMACIJA

Redni broj:
RBR
Identifikacioni broj:
IBR
Tip dokumentacije: Monografska dokumentacija
TD
Tip zapisa: Tekstualni štampani materijal
TZ
Vrsta rada: Master rad
VR
Autor: Stefan Hačko
AU
Mentor: dr Bojan Bašić
MN
Naslov rada: Linearne forme logaritama u rešavanju Diofantovih jednačina
NR
Jezik publikacije: srpski (latinica)
JP
Jezik izvoda: srpski/engleski
JI
Zemlja publikovanja: Srbija
ZP
Uže geografsko područje: Vojvodina
UGP
Godina: 2016.
GO
Izdavač: Autorski reprint
IZ

Mesto i adresa: Novi Sad, Departman za matematiku i informatiku, Prirodno-matematički fakultet, Univerzitet u Novom Sadu, Trg Dositeja Obradovića 4
MA
Fizički opis rada: 6/iv+52/25/2/2/0/0
(broj poglavlja/strana/lit. citata/tabela/slika/grafika/priloga)
FO
Naučna oblast: Matematika
NO

Naučna disciplina: Teorija brojeva
ND
Predmetna odrednica/Ključne reči: Linearne forme logaritama, Diofantove jednačine, Pillaieva jednačina, Problem Erdősa i Grahama, Monocifarski Fibonačijevi brojevi
PO
UDK:
Čuva se: u biblioteci Departmana za matematiku i informatiku Prirodno-matematičkog fakulteta, Univerziteta u Novom Sadu
ČU
Važna napomena:
VN
Izvod: U ovom radu bavimo se primenom teorije linearnih formi logaritama u rešavanju Diofantovih jednačina. U radu, bez dokaza, navodimo osnovne rezultate teorije donjih ograničenja za linearne forme logaritama. Tu teoriju u nastavku rada koristimo da dokažemo: jednačina oblika $a^x+b^y=c$ ima najviše dva rešenja, jednačina $(p-1)!+a^{p-1}=p^k$ ima tačno tri rešenja i jednačina oblika $(x^k-1)(y^k-1)=z^k-1$ nema rešenja za $k>75$. Takođe, bavimo se problemima koji na prvi pogled nemaju veze sa Diofantovim jednačinama: koji je najveći monocifarski Fibonačijev broj i kada je broj oblika $10^n \pm 1$ binarni palindrom.
IZ
Datum prihvatanja teme od strane NN Veća: 9. 6. 2016.
DP
Datum odbrane:
DO
Članovi komisije:

Predsednik: dr Siniša Crvenković, redovni profesor, Prirodno-matematički fakultet, Univerzitet u Novom Sadu

Mentor: dr Bojan Bašić, docent, Prirodno-matematički fakultet, Univerzitet u Novom Sadu

Član: dr Igor Dolinka, redovni profesor, Prirodno-matematički fakultet, Univerzitet u Novom Sadu
KO

UNIVERSITY OF NOVI SAD
FACULTY OF SCIENCES
KEY WORDS DOCUMENTATION

Accession number:
ANO
Identification number:
INO
Document type: Monograph type
DT
Type of record: Printed text
TR
Contents code: Master's thesis
CC
Author: Stefan Hačko
AU
Mentor: Bojan Bašić, PhD
MN
Title: Linear forms in logarithms from the perspective of solving Diophantine equations
TI
Language of text: Serbian
LT
Language of abstract: Serbian/English
LA
Country of publication: Serbia
CP
Locality of publication: Vojvodina
LP
Publication year: 2015.
PY
Publisher: Author's reprint
PU

Publication place: Novi Sad, Department of Mathematics and Informatics, Faculty of Science, University of Novi Sad, Trg Dositeja Obradovića 4
PP
Physical description: 6/iv+52/25/2/2/0/0
(chapters/pages/literature/tables/pictures/graphics/appendices)
PD
Scientific field: Mathematics

SF
Scientific discipline: Number Theory
SD
Subject / Key words: Linear forms in logarithms, Diophantine equations, Pillai's equation, Problem of Erdős i Graham, Monodigit Fibonacci numbers
SKW
UC:
Holding data: The Library of the Department of Mathematics and Informatics, Faculty of Science, University of Novi Sad
HD
Note:
N
Abstract: In this master thesis we apply the theory of linear forms in logarithms in solving Diophantine equations. We give, without proof, some basic results of theory of lower bounds for linear forms in logarithms. We apply that theory to show: equation of form $a^x + b^y = c$ has at most two solutions, equation $(p-1)! + a^{p-1} = p^k$ has exactly three solutions and equation has $(x^k-1)(y^k-1) = z^k - 1$ no solutions for $k > 75$. Also, we consider problems that at first sight do not have any connection with Diophantine equations: what is the largest repdigit Fibonacci number and when is the number of form $10^n \pm 1$ binary palindrome.
AB
Accepted by Scientific Board on: April 21, 2015
ASB
Defended:
DE
Thesis defend board:

President: Siniša Crvenković, PhD, Full Professor, Faculty of Science, University of Novi Sad

Mentor: Bojan Bašić, PhD, Assistant Professor, Faculty of Science, University of Novi Sad

Member: Igor Dolinka, PhD,Full Professor, Faculty of Science, University of Novi Sad
DB