MPhil Kwok Chi Chim

Linear Forms in Logarithms and Applications to Diophantine Problems

DOCTORAL THESIS

to achieve the university degree of
Doktorin der Naturwissenschaften
submitted to

Graz University of Technology

Supervisors

Prof. Gisbert Wüstholz
Honorary Professor, Institute of Analysis and Number Theory, TU Graz
Professor Emeritus, Department of Mathematics, ETH Zürich

Prof. Robert Tichy
Institute of Analysis and Number Theory, TU Graz

Graz, February 2018

Affidavit

I declare that I have authored this thesis independently, that I have not used other than the declared sources/resources, and that I have explicitly indicated all material which has been quoted either literally or by content from the sources used. The text document uploaded to TUGRAZonline is identical to the present doctoral thesis.

Date

Signature

Preface

In 1900 Hilbert posed twenty-three problems, which since then have aroused significant attention and flourished many mathematical disciplines. Among them, the seventh problem addresses to the transcendence of numbers of the form a^b, where a, b are algebraic, $a \notin \{0, 1\}$ and b is irrational, whereas the tenth problem asks for a general algorithm which can decide the existence of solution for any given Diophantine equation. The seventh problem was solved affirmatively by Gelfond and Schneider independently in 1934, whereas the tenth problem was solved negatively by Matiyasevich in 1970.

The quest for generalizing the results of Hilbert's seventh problem lead to the pioneering work of Alan Baker on the theory of linear forms in logarithms in the 1960's. Amazingly, this theory also provides essential machinery for solving many types of Diophantine equations effectively, hence furnishes the understanding of Hilbert's tenth problem. Since Baker's first series of publications, the theory (which is also known as Baker's method) has been widely studied by many mathematicians and its advancement brings forth the solving of many long-standing classical problems in number theory, such as the class number problem, the solving of Thue equation effectively, the Catalan's equation and so on. The theory of linear forms in logarithms we have nowadays (in Archimedean, non-Archimedean and elliptic settings) are the collective contributions of many mathematicians within these decades, and is still regarded as one of the crucial tools for solving Diophantine equations and other problems in number theory effectively.

In this thesis, we focus on Baker's method in the Archimedean and non-Archimedean settings. The plot is as follows. First, we shall give an overview of some important milestones in the historical development of the theory in **Chapter 1**. We shall also give a brief description of some selected problems which are solved with the aid of Baker's method. These serve as a purpose to give the readers a brief idea on the usage, strength and limitation of the theory, the demand for improvement, the issues of concern when improving the existing theory, as well as the difficulty in achieving the improvement. **Chapter 2** gives a brief description and background of my work achieved during my doctoral studies. These include the work on the lower bounds for linear forms in two p-adic logarithms (more precisely, the lower bounds of $|\alpha_1^{b_1} - \alpha_2^{b_2}|_p$, where α_1, α_2 are numbers algebraic over $\mathbb{Q}$ and b_1, b_2 are positive rational integers), the solving of two variants of a problem of Pillai (namely $F_n - T_m = c$ which involves Fibonacci and Tribonacci sequences, and $U_n - V_m = c$

which involves linear recurrence sequences), and the solving of two Diophantine equations (namely $F_{n_1} + F_{n_2} = 2^{a_1} + 2^{a_2} + 2^{a_3}$ and $F_{m_1} + F_{m_2} + F_{m_3} = 2^{t_1} + 2^{t_2}$). **Chapter 3 to Chapter 6** are the documentary of my manuscripts and journal publications.

I am very grateful to Prof. Gisbert Wüstholz, my supervisor, for taking me as his doctoral student. I am very thankful to have his guidance to explore the field of linear forms in logarithms and related issues, and to further enhance my understanding and interest to this topic. I wish to express my deepest gratitude to him for his great effort to cultivate me in the research and for taking care of my difficulties encountered. I am indebted to him for his endless support, encouragement and his lead to achieve goals persistently and optimistically.

I would like to express my special thanks to Prof. Robert Tichy, my supervisor, for his support on providing academic resources and for suggesting a Salzburg collaboration.

My thanks are due to Volker Ziegler and István Pink for their ideas and advice on working towards the joint papers. My thanks extend to Volker Ziegler for the hospitality during my research visits to Universität Salzburg and for his kind help with my queries.

My thanks also extend to my course teachers, colleagues from the Institute of Analysis and Number Theory and from the Discrete Mathematics program, friends and mathematicians that I discussed with for their help, kindness and advice to make my studies a fruitful and memorable one.

I wish to acknowledge the support from the Austrian Science Fund (FWF) under the projects P26114 and W1230.

Finally, I am very grateful to my mother for always prioritizing my wishes and fostering a favorable condition in every circumstance.

Publication List

(In preparation) K. C. Chim, Linear forms in two p-adic logarithms.

K. C. Chim, I. Pink, and V. Ziegler, On a variant of Pillai's problem. *Int. J. Number Theory* **13** (2017) No. 7, 1711–1727.

K. C. Chim, I. Pink, and V. Ziegler, On a variant of Pillai's problem II. *J. Number Theory* **183** (2018) 269–290.

K. C. Chim and V. Ziegler, On Diophantine equations involving sums of Fibonacci numbers and powers of 2. *Submitted.*

Contents

Chapter 1

Linear Forms in Logarithms

Diophantine equation is usually referred to as a polynomial equation in two or more unknowns such that only integer solutions are sought. An exponential Diophantine equation is a Diophantine equation with variable(s) at the exponent(s). The solving of Diophantine equations or Diophantine problems in general is very fascinating because it is usually simple to be stated but it can be very difficult to be solved. The Fermat's last equation, the Catalan's equation and the generalized Fermat equation are illustrative examples.

The theory of linear forms in logarithms of algebraic numbers (Baker's method) has vast applications on solving Diophantine equations (in particular exponential Diophantine equations) and Diophantine problems. Plainly speaking, it obtains the upper bounds for the size of possible solutions to a wide class of Diophantine equations having finitely many solutions. Provided that the bound is explicit and practically small, one can solve the equations completely by extracting all solutions from computer enumeration.

In this chapter, we shall give an overview of some important milestones in the development of linear forms in logarithms, and a brief description of some selected problems being solved with the aid of this method. These help revealing the usage, strength and limitation of the theory, the demand for improvement, the issues of concern when improving the existing theory, as well as the difficulty in achieving the improvement.

1.1 Origins and background

The existence of transcendental numbers was first proved by Liouville in 1844 and the Liouville constant was constructed in 1851 as one of the first illustrated decimal examples. In 1873, Hermite proved that e is transcendental. Cantor showed in 1874 that there are only countably many algebraic numbers but uncountably many transcendental numbers. In 1882, Lindemann proved that for any nonzero algebraic number α, the number e^{α} is transcendental. Hence π is transcendental from the fact that $e^{i\pi} = -1$. The approach was generalized by Weierstrass to give the Lindemann-Weierstrass theorem in 1885. Besides, the ancient problem of squaring the circle involving compass and straightedge was proven to be impossible as a consequence of the transcendence of π.

In 1900 Hilbert posed twenty-three problems, which since then have flourished many mathematical disciplines. Among them, the seventh problem addresses to the quest for the transcendence of numbers of the form α^{β}, where α, β are algebraic, $\alpha \notin \{0,1\}$ and β is irrational. Hilbert believed that,

"the expression α^{β} for an algebraic base $\alpha \neq 0,1$ and an irrational algebraic exponent β, e.g. the number $2^{\sqrt{2}}$ or e^{π}, always represents a transcendental or at least an irrational number."

The Hilbert's seventh problem was solved affirmatively by Gelfond [45] and Schneider [75] independently in 1934. They proved the following Gelfond-Schneider Theorem.

Theorem 1.1 (Gelfond-Schneider Theorem)**.** *Suppose that $\alpha \neq 0,1$ and β is irrational. Then α, β and α^{β} cannot all be algebraic.*

Equivalently, for any non-zero algebraic numbers α_1, α_2, β_1, β_2 such that $\log\alpha_1$ and $\log\alpha_2$ are linearly independent over the rationals, we have

$$\beta_1 \log\alpha_1 + \beta_2 \log\alpha_2 \neq 0.$$

The common scheme of the methods of Gelfond and Schneider is to construct auxiliary functions with a large number of zeros in a certain disc, and enlarge the set of zeros by using a combination of number-theoretic and analytic means.

In 1935, Gelfond [46] obtained a positive lower bound for $|\beta_1 \log\alpha_1 + \beta_2 \log\alpha_2|$. Suppose β_1, β_2 are algebraic numbers not all zero with classical heights at most $B\,(\geq 4)$, α_1, α_2 are algebraic numbers not 0 or 1, the field $\mathbb{K}$ generated by the α's and β's over the rationals has degree at most d and $\frac{\log\alpha_1}{\log\alpha_2}$ is irrational. He proved that

$$|\beta_1 \log\alpha_1 + \beta_2 \log\alpha_2| > Ce^{-(\log B)^{\kappa}} \tag{1.1.1}$$

where $\kappa > 5$ and $C > 0$ is effectively computable in terms of α_1, α_2, d and κ. As a remark, the classical height of an algebraic number is the maximum of the absolute values of the relatively prime integer coefficients in the minimal defining polynomial. He foresaw the strength and significance of extending this effective result to arbitrarily many logarithms of algebraic numbers in solving very difficult problems in modern number theory. In [47, p.177], he mentioned that

"... one may assume... that the most pressing problem in the theory of transcendental numbers is the investigation of the measures of transcendence of finite sets of logarithms of algebraic numbers."

1.2 Baker's first results

The generalization of Gelfond's results was eventually achieved by Alan Baker in 1960's in his series of papers including [1, 2, 3]. Denote

$$|\Lambda| = |\beta_0 + \beta_1 \log \alpha_1 + \cdots + \beta_n \log \alpha_n|. \tag{1.2.1}$$

In [1, 2] Baker obtained lower bound of $|\Lambda|$ for the homogeneous case (i.e. taking $\beta_0 = 0$) whereas in [3], he obtained lower bound of $|\Lambda|$ for the non-homogeneous case (i.e. $\beta_0 \neq 0$) and strengthened slightly the results for the homogeneous case in [1, 2]. His theorems are as follows.

Theorem 1.2 (Baker [3], Theorem 1)**.** *Let $\alpha_1, \ldots, \alpha_n$ and $\beta_0, \beta_1, \ldots, \beta_n$ denote non-zero algebraic numbers. Suppose that $\kappa > n+1$, and let d and B denote respectively the maximum of the degrees and heights of $\beta_0, \ldots, \beta_n$. Then*

$$|\beta_0 + \beta_1 \log \alpha_1 + \cdots + \beta_n \log \alpha_n| > Ce^{-(\log B)^{\kappa}}$$

for some effectively computable number

$$C = C\left(n, \alpha_1, \ldots, \alpha_n, \kappa, d\right) > 0.$$

Theorem 1.3 (Baker [3], Theorem 2)**.** *Let $\alpha_1, \ldots, \alpha_n$ and $\beta_1, \ldots, \beta_n$ denote non-zero algebraic numbers. Suppose that either $\log \alpha_1, \ldots, \log \alpha_n$ or $\beta_1, \ldots, \beta_n$ are linearly independent over the rationals. Suppose further that $\kappa > n$, and let d and B denote respectively the maximum of the degrees and heights of $\beta_1, \ldots, \beta_n$. Then*

$$|\beta_1 \log \alpha_1 + \cdots + \beta_n \log \alpha_n| > Ce^{-(\log B)^{\kappa}}$$

for some effectively computable number

$$C = C\left(n, \alpha_1, \ldots, \alpha_n, \kappa, d\right) > 0.$$

In the above two theorems, the height is referred to as the classical height. The proof of Baker's theorems involves the construction of auxiliary functions in several complex variables, with zeros to high order on a certain set of points. With the hypothesis that $|\Lambda|$ is small, number-theoretic and analytic means are used. With an ingenious extrapolation technique, it can be shown that a subset of the original set of auxiliary functions has even more zeros on a larger set. By applying the extrapolation step several times, it can be deduced that an auxiliary function vanishes, leading to contradiction by using for example the non-vanishing of Vandermonde determinant. The expression of parameters involved in the derivation are carefully and appropriately chosen which are adequate to yield the contradiction so that the proof can be established.

There are a handful of immediate consequences and applications of Baker's first series of results. To name a few,

1. Theorem 1.2 implies that $e^{\beta_0}\alpha_1^{\beta_1}\cdots\alpha_n^{\beta_n}$ is transcendental for any non-zero algebraic numbers $\alpha_1,\dots,\alpha_n$, β_0, $\beta_1,\dots,\beta_n$;

2. the theorem facilitates the determination of explicit upper bounds for the size of all solutions of Diophantine equations of the type
$$f(x,y) = 1,$$
where f denotes any irreducible binary form with integer coefficients and degree at least 3 (see Section 1.6.1);

3. at least in principle, the theorem suffices to settle the celebrated conjecture dating back to Gauss that there are only nine imaginary quadratic fields with class number 1 (see Section 1.6.2).

Among Hilbert's twenty-three problems, the tenth problem asks for a general algorithm which can decide the existence of solution for any given Diophantine equation. Baker's method, being an essential machinery for solving many types of Diophantine equations effectively, furnishes the understanding of this problem. It was eventually solved negatively by Matiyasevich in 1970.

Baker was awarded the Fields Medal in 1970 for his achievement to have "generalized the Gelfond-Schneider theorem (the solution to Hilbert's seventh problem). From this work he generated transcendental numbers not previously identified."

1.3 Further development of Baker's method and general strategy of solving Diophantine equations

Since Baker's first series of results, there were developments on the theory of linear forms in logarithms towards several directions, namely, the improvement on the dependence on B and other parameters in the lower bound, the explicit determination of the constant C, and the generalization of the theory in ultrametric case. Readers can refer to [15] and [20] for more details.

In 1968, Feldman [43, 44] achieved the best dependence of B in the lower bound as follows.

Theorem 1.4 (Feldman [43, 44])**.** *Let $n \geq 2$ be an integer and $a_1,\dots,a_n$ be positive rational numbers which are multiplicatively independent. Let $b_1,\dots,b_n$ be rational integers, not all of which being zero, and set $B = \max\{|b_1|,\dots,|b_n|,3\}$. Then, there exists a positive, effectively computable number C, depending only on $a_1,\dots,a_n$, such that*
$$\left|a_1^{b_1}\cdots a_n^{b_n} - 1\right| \geq \exp\left(-C\log B\right) = B^{-C}.$$

On the other hand, Baker [4] gave the first explicit results in 1968. Let $\alpha_1, \ldots, \alpha_n$ $(n \geq 2)$ denote non-zero algebraic numbers. Suppose the heights and degrees of $\alpha_1, \ldots, \alpha_n$ do not exceed integers A, d respectively, where $A \geq 4$, $d \geq 4$. Suppose further that $0 < \delta \leq 1$ and $\log \alpha_1, \ldots, \log \alpha_n$ are the principal values of the logarithms.

Theorem 1.5 (Baker [4], Theorem)**.** *If rational integers $b_1, \ldots, b_n$ exist, with absolute values at most B, such that*

$$0 < |b_1 \log \alpha_1 + \cdots + b_n \log \alpha_n| < e^{-\delta B},$$

then

$$B < \left(4^{n^2} \delta^{-1} d^{2n} \log A\right)^{(2n+1)^2}.$$

This is the first explicit results by Baker about his theory. This was applied by Baker and Davenport [17] to demonstrated that there is no other Diophantine quadruple containing $1, 3, 8$ than the set $\{1, 3, 8, 120\}$. As a remark, their paper [17] is the origination of the Baker-Davenport reduction method. (See Section 1.5.)

Whereas in 1972, Baker [11] obtained the following results, which gives the best possible dependence with respect to B when A is fixed and with respect to A when B is fixed. Let $\alpha_1, \ldots, \alpha_n$ be non-zero algebraic numbers with degrees at most d and let the heights of $\alpha_1, \ldots, \alpha_{n-1}$ and α_n be at most A' and A (≥ 2) respectively.

Theorem 1.6 (Baker [11], Theorem)**.** *For some effectively computable number $C > 0$ depending only on n, d and A', the inequalities*

$$0 < |b_1 \log \alpha_1 + \cdots + b_n \log \alpha_n| < C^{-\log A \log B}$$

has no solution in rational integers $b_1, \ldots, b_n$ with absolute values at most B (≥ 2).

A more generalized result was given in [12]. As a remark, the generalized Δ-function (refer to [11, Lemma 1]) and the Kummer's condition were used in [11, 12].

Lemma 1.7 (Kummer's condition)**.** *Let $\alpha_1, \ldots, \alpha_n$ be non-zero elements of an algebraic number field $\mathbb{K}$ and let $\alpha_1^{1/p}, \ldots, \alpha_n^{1/p}$ denote fixed p-th roots for some prime p. Further let $\mathbb{K}' = \mathbb{K}\left(\alpha_1^{1/p}, \ldots, \alpha_{n-1}^{1/p}\right)$. Then either $\mathbb{K}'\left(\alpha_n^{1/p}\right)$ is an extension of $\mathbb{K}'$ of degree p, or we have*

$$\alpha_n = \alpha_1^{j_1} \cdots \alpha_{n-1}^{j_{n-1}} \gamma^p.$$

for some $\gamma \in \mathbb{K}$ and some integers $j_1, \ldots, j_{n-1}$ with $0 \leq j_r < p$.

In 1973, Baker [12] obtained the following result which fosters general strategy of solving Diophantine equations.

Theorem 1.8 (Baker [12], Theorem 2). *Let $\alpha_1, \dots, \alpha_n$ be non-zero algebraic numbers with degrees at most d and let the heights of $\alpha_1, \dots, \alpha_{n-1}$ and α_n be at most A' and A (≥ 2) respectively. If for some $\varepsilon > 0$, there exist rational integers $b_1, \dots, b_{n-1}$ with absolute values at most B such that*

$$0 < |b_1 \log \alpha_1 + \cdots + b_{n-1} \log \alpha_{n-1} - \log \alpha_n| < e^{-\varepsilon B}, \tag{1.3.1}$$

then $B < C \log A$ for some effectively computable number C depending only on n, d, A' and ε.

It means that having (1.3.1) guarantees the finiteness of the size of b's in the equation. We can utilize the above theorem to sketch a general strategy of deriving explicit upper bounds for the size of possible solutions by Baker's method (refer to Győry in [96, Chapter 4]):

1. Formulate the Diophantine problem into equation(s) to which Baker's method is applicable.
2. Reduce the equation(s) to inequalities of the form

$$0 < |\alpha_1^{b_1} \cdots \alpha_{n-1}^{b_{n-1}} - \alpha_n| < c_1 \exp\{-c_2 B\} \tag{1.3.2}$$

   where $\alpha_1, \dots, \alpha_n$ are non-zero algebraic numbers, $b_1, \dots, b_{n-1}$ are unknown rational integers, $B = \max_i |b_i|$ and c_1, c_2 as well as c_3, c_4 below denote effectively computable positive constants which are independent of $b_1, \dots, b_{n-1}$. If B is large, (1.3.2) implies that

$$|\Lambda| \leq c_3 \exp\{-c_2 B\} \tag{1.3.3}$$

   where $\Lambda = b_1 \log \alpha_1 + \cdots + b_r \log \alpha_{n-1} - \log \alpha_n$. For simplicity, it is assumed here that $\alpha_1, \dots, \alpha_n$ are real and positive.

3. The application of Baker's method gives

$$\exp\{-c_4 (\log B)^\kappa\} \leq |\Lambda|. \tag{1.3.4}$$

   Together with (1.3.3) we come across the inequality

$$c_2 B \leq c_4 (\log B)^\kappa + \log c_3 \tag{1.3.5}$$

   which yields an explicit upper bound for B, denoted by B_0.

4. Deduce an explicit upper bound for the size of unknowns in the initial Diophantine problem.

The essential issue here is that inequality (1.3.5) reveals the desire of keeping $\kappa = 1$ and a small c_4 for getting a smaller B_0. It should be noted that in solving some equations one may need to apply Baker's method several times in a cascaded way so that the explicit upper bound for B obtained would inevitably be larger. Although further reduction tool may be available to reduce the upper bound to a greater extent (see Section 1.5), it requires a preliminary upper bound for B

to start with which should be small enough for initial computer enumeration. All these reinforce our demand for a small B_0 and hence a good dependence on $\log B$ and a small c_4.

There are further development in this regard. In 1975, Baker announced in [13] the following sharpening of his previous results. Let $\alpha_1, \ldots, \alpha_n$ be non-zero algebraic numbers with degrees at most d and suppose that the height of α_j is at most A_j (≥ 4). Further, let $b_1, \ldots, b_n$ be rational integers with absolute values at most B (≥ 4), and let

$$\Lambda = b_1 \log \alpha_1 + \cdots + b_n \log \alpha_n,$$

where the logarithms are assumed to have their principal values.

Theorem 1.9 (Baker [13], Theorem). *If $\Lambda \neq 0$, then $|\Lambda| > B^{-C\Omega \log \Omega}$, where*

$$\Omega = \log A_1 \cdots \log A_n,$$

and C is an effectively computable number depending only on n and d.

Baker mentioned in the paper that *"it would be of much interest to eliminate* $\log \Omega$ *and to generalize Λ so as to incorporate these results."*

In 1977, Baker [15] further improved his results as follows. Denote

$$|\Lambda| = |\beta_0 + \beta_1 \log \alpha_1 + \cdots + \beta_n \log \alpha_n|$$

where α_j and β_j are algebraic numbers with heights at most $A_j \geq 4$ and $B \geq 4$ respectively. The field $\mathbb{K}$ generated by the α's and β's over the rationals has degree at most d, $\Omega = \log A_1 \cdots \log A_n$, and $\Omega' = \frac{\Omega}{\log A_n}$.

Theorem 1.10 (Baker [15], Theorem 1). *if $\Lambda \neq 0$, then $|\Lambda| > (B\Omega)^{-C\Omega \log \Omega'}$, where $C = (16nd)^{200n}$.*

When $\beta_0 = 0$ and $\beta_1, \ldots, \beta_n$ are rational integers, the bracketed factor Ω can be eliminated to yield:

Theorem 1.11 (Baker [15], Theorem 2). *If, in the rational case, $\Lambda \neq 0$, then $|\Lambda| > B^{-C\Omega \log \Omega'}$, where $C = (16nd)^{200n}$.*

1.3.1 Results of Baker and Wüstholz

One of the main problems concerning Baker's results in 1977 was to eliminate the term $\log \Omega'$ in Theorem 1.11. This has been established by Wüstholz [92, 93], as well as Philippon and Waldschmidt [70] independently in 1988. The advancement achieved by Wüstholz was made possible by the use of the theory of multiplicity estimates of group varieties (see [95] and also [62, 63]), which replaced the use of Kummer's theory in the derivation.

In Wüstholz's results [93], the Weil height, which has advantages over the classical height, is used instead. Let K be an algebraic number field and v a place of K. Denote by K_v the completion of K at v and set $d_v = [K_v : \mathbb{Q}_v]$ if $d = [K : \mathbb{Q}]$. We write $v|p$ if v is a finite place of K lying over the prime p and $v|\infty$ if v is an infinite place. For every place v of K the absolute value $|\ \ |_v$ is normalized as follows:

$$\begin{aligned} &\text{(i).} \qquad |p|_v = p^{-d_v/v} &&\text{if } v|p,\\ &\text{(ii).} \qquad |x|_v = |x|^{-d_v/v} &&\text{if } v|\infty, x \in K_v. \end{aligned}$$

The product formula $\prod_v |x|_v = 1$ follows for $0 \neq x \in K$. Let $x = (x_1, \dots, x_N)$ be in K^N. We put

$$H(x) := \prod_v \max_n(|x_n|_v)$$

and the logarithmic height

$$h(x) := \sum_v \max_n \log(|x_n|_v). \tag{1.3.6}$$

Both heights depend only on the projective coordinates of x due to the product formula. If $\alpha \in K^*$ is any algebraic number then we put

$$H(\alpha) := H((1,\alpha)) \qquad \text{and} \qquad h(\alpha) := h((1,\alpha)).$$

For the linear form $L = \beta_1 z_1 + \cdots + \beta_n z_n$ we put $h(L) = h((\beta_1, \dots, \beta_n))$. The following states the Theorem of Wüstholz [93].

Theorem 1.12 (Wüstholz [93], Theorem)**.**
If $\beta_1, \dots, \beta_n$ are rational integers, $\Lambda = L(\log\alpha_1, \dots, \log\alpha_n) \neq 0$, then

$$\log|\Lambda| > -c(n,d)h(L)h(\alpha_1)\cdots h(\alpha_n)$$

for an effectively computable positive constant $c = c(n,d)$ depending only on n, d.

In 1993, Baker and Wüstholz [19] obtained the explicit formula for $c(n,d)$ in Theorem 1.12 while keeping the same structure of dependence of parameters in the lower bound. This celebrated result signifies a new stage of the Baker's method. Before stating the results, we shall introduce some notations. Denote by $\alpha_1, \dots, \alpha_n$ algebraic numbers, not 0 or 1, and by $\log\alpha_1, \dots, \log\alpha_n$ a fixed determination of the logarithms. Let K be the field generated by $\alpha_1, \dots, \alpha_n$ over the rationals $\mathbb{Q}$ and let d be the degree of K. For each $\alpha \in K$ and any given determination of $\log\alpha$ we define the modified height $h'(\alpha)$ by

$$h'(\alpha) = \frac{1}{d}\max(h(\alpha), |\log\alpha|, 1),$$

where $h(\alpha)$ is the standard logarithmic Weil height of α in (1.3.6). Consider the linear form

$$L(z_1, \dots, z_n) = b_1 z_1 + \cdots + b_n z_n,$$

where $b_1, \dots, b_n$ are rational integers, not all 0. In analogy with the modified height introduced above, we define

$$h'(L) = \frac{1}{d}\max(h(L), 1),$$

where $h(L)$ is the logarithmic Weil height of L (and $h'(L) = \max\left(\log\left(\frac{\max(|b_1|,\dots,|b_n|)}{\gcd(b_1,\dots,b_n)}\right), \frac{1}{d}\right)$). Baker and Wüstholz [19] obtained the following

Theorem 1.13 (Baker and Wüstholz [19], Theorem)**.** *If $\Lambda = L(\log\alpha_1, \dots, \log\alpha_n) \neq 0$ then*

$$\log|\Lambda| > -C(n,d)h'(\alpha_1)\cdots h'(\alpha_n)h'(L),$$

where

$$C(n,d) = 18(n+1)!\, n^{n+1}(32d)^{n+2}\log(2nd).$$

The following version is also provided in order to compare with previous results. Suppose that $B \geq \max|b_j|$, and for any α as above we take A as an upper bound for the absolute values of the relatively prime integer coefficients in the minimal defining polynomial for α. Define A_j like A with $\alpha = \alpha_j$. Then if $A \geq e$, $B \geq e$ and $\log\alpha$ has its principal value we have

$$h'(L) \leq \log B, \quad h'(\alpha) \leq \pi + \log A \leq 4 \cdot 2\log A.$$

Since $n! \leq n^{n+1}e^{-n+1}$ we have

$$C(n,d) \leq 2400(3 \cdot 5n)^{2n+3}d^{n+2}\log(2nd),$$

whence

$$\log|\Lambda| > -(16nd)^{2(n+2)}\log A_1 \cdots \log A_n \log B. \tag{1.3.7}$$

Theorem 1.13 has vast significance and applications to solving Diophantine problems and became widely used by many mathematicians since then. A p-adic analogue of [19] is proposed by Yu in his series [100]–[102].

1.3.2 Other results of linear forms in n logarithms

There are other mathematicians, whose results are not mentioned above, giving contributions to the development of the Baker's method. For a more comprehensive account on the historical development of Baker's method, readers can refer to [15, Section 1] and [20].

A more recent result is performed by Matveev [64] in 2000, in which he obtained an improved form c^n for the expression of n in the absolute constant. There are also far-reaching conjectures for an improved dependence of $h'(\alpha_j)$ in the lower bound (see [20] and [53]).

1.3.3 Linear forms in two logarithms by Laurent *et al.*

Studies by some French mathematicians such as Laurent were performed to use interpolation determinant method to obtain the bound for linear forms in logarithms. In particular, Laurent's study in [54] was for $n = 2$, with

$$|\Lambda| = |b_2 \log \alpha_2 - b_1 \log \alpha_1|,$$

where $\alpha_1, \alpha_2 \geq 1$ are two real and multiplicatively independent algebraic numbers, b_1 and b_2 are rational integers ≥ 1 without loss of generality. He obtained a lower bound of the form

$$\log |\Lambda| > -CD^4 \log a_1 \log a_2 (\log b')^2, \tag{1.3.8}$$

where $D = [\mathbb{Q}(\alpha_1, \alpha_2) : \mathbb{Q}]$, a_1, a_2 are two real numbers > 1 such that $h(\alpha_i) \leq \log a_i$ $(i = 1, 2)$, with $h(\alpha)$ being the absolute logarithmic Weil height, and

$$b' = \frac{b_1}{D \log a_2} + \frac{b_2}{D \log a_1}$$

which has a different expression but analogue role as that in Baker and Wüstholz [19]. It should be noted that (1.3.8) has a weaker dependence on b' as that of B in (1.3.7). The interest in Laurent's result lies in the constant c which gets a size of less than 100. In particular, [54, Theorem 2] was stated as follows:

Theorem 1.14 (Laurent [54], Theorem 2). *Suppose that* $\log a_1 \geq 1$, $\log a_2 \geq 1$ *and* $\log b' \geq 25$. *Then*

$$\log |\Lambda| \geq -87D^4 (0.5 + \log b')^2 \log a_1 \log a_2.$$

The interpolation determinant method used in [54] is different from the classical Baker's method. It begins with considering the determinant of a square matrix with maximal rank (as demonstrated by theory of multiplicity estimates), which represents a non-zero polynomial in α_1 and α_2. The lower and upper bounds of the determinant are estimated respectively by arithmetic and analytic means. Under the hypothesis that $|\Lambda|$ is small and with further conditions, contradiction arises. By asserting appropriate expressions to the intermediate parameters, various theorems in the form of (1.3.8), such as Theorem 1.14, are obtained.

Laurent's result was further improved by Laurent, Mignotte and Nesterenko [56], yielding a constant of roughly 30 and keeping the shape in (1.3.8). Further reduction on the constant was also given by Laurent in [55]. A p-adic analogue of [54] and [56] was proposed by Bugeaud and Laurent in 1996 [33]. In 2006, Gouillon [50] modified [54] and succeeded in yielding the lower bound with a dependence on $\log B$ instead of $(\log B)^2$ (note that here B has a different expression but analogue role as B in Baker and Wüstholz [19]), maintaining the constant C to be of a reasonable size.

1.4 p-Adic analogue

The evolution of the theory of p-adic linear forms in logarithms follows closely the development of the theory of linear forms in logarithms in the complex domain described in previous sections. It begins with the studies by Mahler who proved the p-adic analogue of the Hermite-Lindemann theorem [59] in 1932 and obtained the p-adic analogue of the Gelfond-Schneider theorem [60] in 1935. He also founded the p-adic theory of analytic function.

Since Baker's remarkable results in 1966, several mathematicians provide p-adic analogue of Baker's series of results. The p-adic analogue of the tools for proving linear forms in logarithms in the p-adic case are developed. One of the main challenges in the p-adic domain is to ensure the convergence of the exponential function. In this regard, appropriate setting has to be adopted so that similar methodology as in the complex case can be well applied in the p-adic case.

1.4.1 Results of Kunrui Yu

Among all the p-adic analogue results, Kunrui Yu performed p-adic analogues of Baker's results [12] and [15, Theorem 2] in his series [97]–[99]. Besides, he performed p-adic analogues of the results of Baker and Wüstholz [19] and subsequent improvement in his series [100]–[102]. He proposed the idea of supernormality in dealing with the convergence issue for the exponential function in the p-adic domain (see [100]).

The following is a consequence of the Main Theorem in Yu [102]. Let $\alpha_1, \ldots, \alpha_n$ $(n \geq 2)$ be non-zero algebraic numbers and K be a number field containing $\alpha_1, \ldots, \alpha_n$ with $d = [K : \mathbb{Q}]$. Denote by $\mathfrak{p}$ a prime ideal of the ring of integers in K, lying above the prime number p, by $e_{\mathfrak{p}}$ the ramification index of $\mathfrak{p}$, and by $f_{\mathfrak{p}}$ the residue class degree of $\mathfrak{p}$. It is noted that $e_{\mathfrak{p}} \leq d$ and $f_{\mathfrak{p}} \leq d$.

Theorem 1.15 (Yu [102] p.190)**.** *Denote $\Xi = \alpha_1^{b_1}\alpha_2^{b_2}\cdots\alpha_n^{b_n} - 1$, where $b_1, \ldots, b_n$ are rational integers, not all zero, and $\Xi \neq 1$. Let $h_0(\alpha)$ denotes the absolute logarithic Weil height of an algebraic number α, and $h_j = \max\left(h_0(\alpha_j), \frac{1}{16e^2d^2}\right)$ $(j = 1, \ldots, n)$. Let B be a real number satisfying $B \geq \max\{|b_1|, \ldots, |b_n|, 3\}$. Then*

$$\mathrm{ord}_p(\Xi - 1) < nC(n,d,p)h_1 \cdots h_n \log B,$$

where

$$C(n,d,p) = (16ed)^{2(n+1)} n^{3/2} \log(2nd) \log(2d) e_{\mathfrak{p}}^n \frac{p^{f_{\mathfrak{p}}}}{(f_{\mathfrak{p}} \log p)^2}.$$

Besides getting accord with the development of Baker's method in the complex case, the development of the p-adic case is also driven by practical use in solving Diophantine problems. Section 1.6.4 and Section 1.6.5 provide further illustrations. Readers can also refer to [96, Chapter 2] for a more comprehensive description on the development of the Baker's method in p-adic domain.

1.4.2 Linear forms in two p-adic logarithms by Bugeaud and Laurent

In line with the results of linear forms in two logarithms in [54] and [56], a p-adic analogue was proposed by Bugeaud and Laurent in 1996 [33] as follows.

Let p be a prime number. Denote $\overline{\mathbb{Q}}_p$ as the algebraic closure of $\mathbb{Q}_p$. The field $\overline{\mathbb{Q}}_p$ has the ultrametric absolute value $|x|_p = p^{-v_p(x)}$, where v_p is the extension of p-adic valuation in $\mathbb{Q}_p$ normalized by $v_p(p) = 1$. Let α_1, α_2 be two numbers algebraic over $\mathbb{Q}$ and we regard them as elements of the field $\overline{\mathbb{Q}}_p$. Denote $K_v = \mathbb{Q}_p(\alpha_1, \alpha_2)$. Denote by e the ramification index of the valuation group from $\mathbb{Q}_p$ to K_v and by f the residue class degree of the extension. Set $D = \frac{[\mathbb{Q}(\alpha_1,\alpha_2):\mathbb{Q}]}{f}$.

Theorem 1.16 (Bugeaud and Laurent [33], Corollary 2)**.** *Let α_1 and α_2 be multiplicatively independent and satisfy $v_p(\alpha_1) = v_p(\alpha_2) = 0$. Let A_1 and A_2 be real numbers such that*

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

Let b_1 and b_2 be positive integers and let

$$H = \max\left\{\log\left(\frac{b_1}{D\log A_2} + \frac{b_2}{D\log A_1}\right) + \log\log p + 0.4, \frac{10\log p}{D}, 10\right\}.$$

Then, we have the upper bound

$$v_p\left(\alpha_1^{b_1} - \alpha_2^{b_2}\right) \leq \frac{24p\left(p^f - 1\right)}{(p-1)(\log p)^4} D^4 \log A_1 \log A_2 H^2.$$

The interest of this result is the very small size of the constant, though in sacrificed by a worse dependence on $\log B$ (which is analogous to H) as compared to the results by Yu.

1.5 Supplementary tools for solving Diophantine equations completely

As demonstrated in (1.3.5), linear forms in logarithms is capable of obtaining B_0, an explicit upper bound of the size of unknowns in the Diophantine equation. The tightness of the bound matters much on c_4 and κ. The state of the art is having $\kappa = 1$ which is the best possible, and having c_4 which depends on n, d and heights of α_j explicitly. The size of B_0 can reach 10^{10} and typically higher (e.g. 10^{30}) especially when n is larger or if linear forms in logarithms is used several times in a cascaded way. In view of solving the equations completely, it is desirable if B_0 is reduced to a greater extent.

A tool of this kind, which is regarded as Baker-Davenport reduction method, is first proposed by Baker and Davenport [17] in 1969. They demonstrated for the first time that linear forms in logarithms is applied to solve Diophantine equations completely. The tool is modified by Dujella and Pethő in [42]. In the following, we present a lemma from Bravo *et al.* [27], which is a slight variation of the result in [42]. We denote by $\|x\| = \min\{|x-n| : n \in \mathbb{Z}\}$ the distance from $x \in \mathbb{R}$ to the nearest integer.

Lemma 1.17 (Bravo *et al.* [27], Lemma 2.4)**.** *Let M be a positive integer, let $\frac{p}{q}$ be a convergent of the continued fraction of the irrational γ such that $q > 6M$, and let A, K, μ be some real numbers with $A > 0$ and $K > 1$. Let $\varepsilon := \|\mu q\| - M\|\gamma q\|$. If $\varepsilon > 0$, then there is no solution to the inequality*

$$0 < |u\gamma - v + \mu| < AK^{-w}, \tag{1.5.1}$$

in positive integers u, v and w with $u \le M$ and $w \ge \frac{\log(Aq/\varepsilon)}{\log K}$.

Lemma 1.17 is used for linear forms in three logarithms, by rewriting the equation of the form (1.5.1), where w, M are respectively B, B_0 in our previous notation. We take the smallest $q > 6M$ and test whether $\varepsilon > 0$. If $\varepsilon > 0$ we have a new, usually much smaller upper bound for w than B_0. If $\varepsilon \le 0$ we test whether $\varepsilon > 0$ for the next larger denominator q and so on. In case odd scenarios happen, that is having $\varepsilon \le 0$ for repeated trials of q, it can normally be tackled by arguments from continued fractions.

The reduction method is generalized by Lenstra, Lenstra and Lovász in 1982 [57] to the so-called LLL-algorithm. To illustrate, we consider for simplicity the case of real approximation lattices. Let $\mathcal{L} \subseteq \mathbb{R}^k$ be a k-dimensional lattice. Further, we define

$$l(\mathcal{L}, y) = \begin{cases} \min_{x \in \mathcal{L}}\{||x-y||\}, & y \notin \mathcal{L} \\ \min_{0 \ne x \in \mathcal{L}}\{||x||\}, & y \in \mathcal{L}, \end{cases}$$

where $||\cdot||$ denotes the Euclidean norm on $\mathbb{R}^k$. By applying the LLL-algorithm it is possible to give a lower bound for $l(\mathcal{L}, y) \ge c_1$ in a polynomial time. (See e.g. [76, Section 5.4], for details.) For application, suppose we are given $\delta_0, \delta_1, \ldots, \delta_k \in \mathbb{R}$ linearly independent over $\mathbb{Q}$ and two positive constants c_2, c_3 such that

$$|\delta_0 + x_1\delta_1 + \cdots + x_k\delta_k| \le c_2 \exp(-c_3 B), \tag{1.5.2}$$

where $x_i \in \mathbb{Z}$ with $1 \le i \le k$ are bounded by $|x_i| \le X_i$ with X_i given upper bounds for $1 \le i \le k$. Set $X_0 = \max_{1 \le i \le s}\{X_i\}$. This associates with inequality (1.3.3) before. Referring to de Weger [90] and [91, Section VI.3]), the basic idea is to approximate the linear form (1.5.2) by an approximation lattice. Namely, we consider the lattice $\mathcal{L}$ generated by the columns of the matrix

$$\begin{pmatrix} 1 & 0 & \ldots & 0 & 0 \\ 0 & 1 & \ldots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \ldots & 1 & 0 \\ \lfloor C\delta_1 \rfloor & \lfloor C\delta_2 \rfloor & \ldots & \lfloor C\delta_{k-1} \rfloor & \lfloor C\delta_k \rfloor \end{pmatrix}$$

where C is a large constant usually of size about X_0^k and $y = (0, 0, \ldots, -\lfloor C\delta_0 \rfloor)$. If we have a lower bound $l(\mathcal{L}, y) \geq c_1$, then we hope to obtain a much reduced upper bound for B in inequality (1.5.2) by the following lemma from [76].

Lemma 1.18 (Lemma VI.1 in Smart [76]). *Assume that* $S = \sum_{i=1}^{k-1} X_i^2$ *and* $T = \frac{1+\sum_{i=1}^{k} X_i}{2}$. *If* $c_1^2 \geq T^2 + S$, *then we have either* $x_1 = x_2 = \cdots = x_{k-1} = 0$ *and* $x_k = -\frac{\lfloor C\delta_0 \rfloor}{\lfloor C\delta_k \rfloor}$ *or*

$$B \leq \frac{1}{c_3}\left(\log(Cc_2) - \log\left(\sqrt{c_1^2 - S} - T\right)\right).$$

Both the Baker-Davenport reduction method and the LLL-algorithm can be used repetitively to reduce B_0 to a greater extent. For the LLL-algorithm in the p-adic domain, readers can refer to [76, 91]. Nevertheless, it should be emphasized that their usage require a definite knowledge on the values of α_j and in particular B_0, which should be small enough for the initial computer enumeration. Therefore, these reduction strategies cannot substitute linear forms in logarithms. These considerations reinforce the importance of maintaining a good dependence on $\log B$ and a small constant from the results of linear forms in logarithms.

1.6 Some applications of linear forms in logarithms

The evolution of the theory of linear forms in logarithms brings forth the solving of many long-standing classical problems in number theory. Here we shall only mention a few of the many applications that prosper from linear forms in logarithms in either the Archimedean or non-Archimedean domain, or both. Readers can refer to [14, 20, 69, 76, 86] for more detail accounts.

1.6.1 Effective results of the Thue equation

A Thue equation is a Diophantine equation of the form

$$F(X, Y) = m \tag{1.6.1}$$

where $F \in \mathbb{Z}[X, Y]$ is a homogeneous, irreducible polynomial of degree $n \geq 3$ and m is a non-zero integer. It is well known that many Diophantine equations in two unknowns can readily be reduced to a finite number of equations of the type (1.6.1). The equation is named in honour of A. Thue who proved in 1909 [88] the following

Theorem 1.19 (Thue). *The equation* (1.6.1) *has only finitely many solutions in integers x and y.*

Thue's original proof is based on a result of the rational approximations of algebraic numbers which is ineffective. The advancement on the proof and studies of the Thue equation is brought up by mathematicians such as Siegel and Mahler. Besides, there are flows of new ideas and methods on solving the Thue equation. However, most suggested methods are ineffective except for bounds for the number of solutions and hence fail to obtain complete solutions.

Baker gave breakthrough by providing an effective bound to the size of solutions to the Thue equation. The first result of this kind [5], established in 1968, depends essentially on Baker's theory in [1, 2]. Let m be any positive integer, without loss of generality.

Theorem 1.20 (Baker [5], Theorem 1)**.** *All solution of* (1.6.1) *in integers* x, y *satisfy*

$$\max(|x|, |y|) < Ce^{(\log m)^{\kappa}}, \tag{1.6.2}$$

where $\kappa > n+1$*,* C *is an effectively computable number depending only on* n, κ *and the coefficients of* F*.*

The proof also brings forth an effective improvement on Liouville's inequality. In [6], Baker exploited the results to obtain an effective upper bound for $\max(|x|, |y|)$ for the solutions of

$$y^2 = x^3 + k$$

where k is any non-zero integer. The advancement on Baker's method over the decades also lead to a better dependence on m in (1.6.2).

1.6.2 Class number problem

Gauss conjectured that the only imaginary quadratic fields $\mathbb{Q}(\sqrt{-d})$ with class number 1, where d is a square-free positive integer, are given by $d = 1$, 2, 3, 7, 11, 19, 43, 67 and 163. Heilbronn and Linfoot [52] showed that there can be at most ten such field, whereas Stark [77] showed that the tenth field with d_{10}, if exists, would satisfy $d_{10} > \exp(2.2 \times 10^7)$. Gelfond and Linnik proved in [48] that if the tenth field exists then

$$|x_1 \log \alpha_1 + x_2 \log \alpha_2 + \log \alpha_3| < e^{-\gamma_1 \sqrt{d_{10}}} \tag{1.6.3}$$

holds, where $\alpha_1, \alpha_2, \alpha_3$ are fixed algebric numbers whose logarithms are linearly independent over $\mathbb{Q}$, $x_1, x_2 \in \mathbb{Z}$ with $|x_1|, |x_2| < \gamma_2 \sqrt{d_{10}}$ and γ_1, γ_2 are effective constants.

Baker's first results [1] obtains a lower bound for the linear forms in (1.6.3) which together with the upper bound in (1.6.3) yields an upper bound for d_{10}. In principle, with adequate sharpness of the bound, it can be shown that the tenth field does not exist if this upper bound contradicts with $d_{10} > \exp(2.2 \times 10^7)$. The non-existence of the tenth field is also given by Stark [78] independently with another approach.

Studies on adapting Baker's method to determine all the imaginary quadratic fields with class number 2 proceeded soon after. The determination concerns linear forms in three logarithms and requires sharp version of Baker's first series of results (see Baker [7, 9, 10], Baker and Stark [18] and Stark [79, 80, 81]). The problem is finally completely solved with precisely eighteen such fields.

1.6.3 Catalan's equation

Catalan, dated back to 1844, states the following

Conjecture 1.21 (Catalan's Conjecture). *The equation*

$$x^p - y^q = 1 \tag{1.6.4}$$

has no solutions in integers x, y, p, $q > 1$ other than $3^2 - 2^3 = 1$.

A weaker conjecture that equation (1.6.4) has only a finite number of solutions is given by Cassels [34] in 1953. Only partial results were obtained before Tijdeman's breakthrough [89] in 1976, in which he proved the conjecture by Cassels.

Tijdeman deduced a improved version of Baker's results in [11] for obtaining the upper bounds for p and q. A novelty in Tijdeman's version is the explicitly given dependence on the upper bound of the heights of $\alpha_1, \dots, \alpha_{n-1}$ in the linear forms. Next, an explicit upper bound for $\max(|x|, |y|)$ can be obtained using Baker's results on hyperelliptic equation in [8]. In conclusion there are only finitely many values of x, y, p, q to check for satisfying (1.6.4), though the quantity is very large. The Catalan's conjecture is proved affirmatively by Mihăilescu [67] in 2004 by another approach (see also [23, 24]).

1.6.4 Results related to the abc-conjecture

Let x, y and z be positive integers and denote by $G = G(x, y, z)$ the greatest square-free factor of xyz. In 1985, Masser proposed the abc-conjecture [61] as stated below, which is a refinement of a conjecture formulated by Oesterlé and has profound consequences.

Conjecture 1.22 (abc-Conjecture). *For each positive real number ε there is a positive number $c(\varepsilon)$, which depends on ε only, such that, for all positive integers x, y, and z with $x + y = z$ and $(x, y, z) = 1$, we have*

$$z < c(\varepsilon) G^{1+\varepsilon}.$$

In 1991, Stewart and Yu [84] obtained results towards the abc-conjecture by adopting both the Archimedean and non-Archimedean estimates of linear forms in logarithms. They proved that there exists an effectively computable positive constant c_1 such that, for all positive integers x, y and z, with $z > 2$ satisfying $x + y = z$ and $(x, y, z) = 1$,

$$z < \exp\left(G^{2/3+c_1/\log\log G}\right). \tag{1.6.5}$$

In 2001 Stewart and Yu [85] strengthened (1.6.5) and yield the following

Theorem 1.23 (Stewart and Yu [85], Theorem 1)**.** *There exists an effectively computable positive number c such that, for all positive integers x, y, and z with $x + y = z$ and $(x, y, z) = 1$,*

$$z < \exp\left(c\, G^{1/3}(\log G)^3\right).$$

They also proved a stronger bound when the greatest prime factor of one of x, y and z is small relative to G. One of the reasons for these improvements is the use of the non-Archimedean estimates by Yu [101] which has a better dependence on n (the number of α's in the logarithmic forms) and the Archimedean estimates by Baker and Wüstholz [19].

1.6.5 A problem of Erdős and its generalization

In 1965, Erdős conjectured that

$$\frac{P\left(2^n - 1\right)}{n} \to \infty \quad \text{as } n \to \infty,$$

where $P(m)$ denotes the greatest prime divisor of $m \in \mathbb{Z}$ with the convention that $P(m) = 1$ when $m \in \{1, 0, -1\}$. There is also a generalization of the conjecture to Lucas numbers u_n and Lehmer numbers $\tilde{u}_n$ that $\frac{P(u_n)}{n} \to \infty$ and $\frac{P(\tilde{u}_n)}{n} \to \infty$ respectively as $n \to \infty$.

The problem and its generalization were studied by Stewart and Yu and were finally proved in 2013. The primary proof in [83] appeals to the intensive work of Yu in [103] which succeeded in achieving three main refinements in the results of p-adic linear forms in logarithms as compared to preceding versions. In particular, the refinement in the dependence on p in the p-adic logarithmic forms is crucial for the proof. Section 9 of [103] remarks the roles of [102] and [103] in solving the problem and its generalization.

1.6.6 Diophantine m-tuples

A set of m distinct, positive integers $\{a_1, \ldots, a_m\}$ is called a $D(n)$-m-tuple if $a_i a_j + n$ is a perfect square for all $1 \le i < j \le m$ (or simply a Diophantine m-tuple when $n = 1$). The Diophantine m-tuples problem originates from Diophantus who studied sets of positive rational numbers with the same property. The first example for an integral Diophantine quadruple $\{1, 3, 8, 120\}$ was found by Fermat and it was found that the set cannot be extended to a Diophantine quintuple by Baker and Davenport [17]. It is a general belief that no Diophantine quintuple exists.

This conjecture is extensively studied by many mathematicians in particular Dujella and his collaborators. Dujella established many results paving the path of development. Among them the milestone result in [41] states that there are only finitely many Diophantine quintuples, with $d < 10^{2171}$ and $e < 10^{10^{26}}$ if $\{a, b, c, d, e\}$ is a Diophantine quintuple and $a < b < c < d < e$.

In 2016 He, Togbé and Ziegler [51] announced the proof of the above conjecture. This attributes to the definition of an operator on Diophantine triples and their classification, the use of sharp bound for linear forms in three logarithms obtained by applying a result due to Mignotte [66] iteratively, and the use of new congruences in certain cases. In 2017, Bliznac Trebješanin and Filipin [25] announced the nonexistence of $D(4)$-quintuples using similar arguments and further tools.

The conjecture that no Diophantine quintuple exists is regarded as the weak version of the following Diophantine quintuple conjecture. Let $\{a, b, c\}$ be a Diophantine triple and

$$ab + 1 = r^2, \quad ac + 1 = s^2, \quad bc + 1 = t^2,$$

where r, s, t are positive integers. Define $d_+ = a+b+c+2abc+2rst$. Then $\{a, b, c, d_+\}$ is a Diophantine quadruple since $ad_+ + 1 = (at + rs)^2$, $bd_+ + 1 = (bs + rt)^2$ and $cd_+ + 1 = (cr + st)^2$.

Conjecture 1.24 (Diophantine quintuple conjecture)**.** *If $\{a, b, c, d\}$ is a Diophantine quadruple and $d > \max\{a, b, c\}$, then $d = d_+$.*

It remains an open problem. The website [40] prepared by Dujella provides rich resources on the Diophantine m-tuple problem and the generalization.

1.6.7 Final remark

As a final remark, the theory of linear forms in logarithms is still regarded nowadays as one of the crucial tools for solving Diophantine equations and other problems in number theory effectively. There are still demands for the reduction of the size of the constant and the improvement on the dependence on certain parameters in the results of linear forms in logarithms to suit the practical use in solving specific Diophantine problems.

Chapter 2

Description of my work

In this chapter, we shall give a brief background and description of the work achieved during my doctoral studies. The first work (described in Section 2.1) concerns the deduction of a lower bound for linear forms in two p-adic logarithms. The other work (described in Section 2.2 and Section 2.3) showcase the application of the results of linear forms in logarithms (taking $n = 3$) by Baker and Wüstholz [19], together with a version of reduction method (for the work described in Section 2.2.1 and Section 2.3).

To avoid repetition of the introductory information, we try to make it brief here. Readers can refer to the first section of **Chapter 3 to Chapter 6** for more descriptions on each topic.

2.1 Linear forms in two p-adic logarithms

In **Chapter 3**, we shall develop the lower bounds for linear forms in two p-adic logarithms. More precisely, we establish the lower bounds for the p-adic distance between two integral powers of algebraic numbers, i.e. $|\Lambda|_p = |\alpha_1^{b_1} - \alpha_2^{b_2}|_p$, where α_1, α_2 are numbers algebraic over $\mathbb{Q}$ and b_1, b_2 are positive rational integers. The chapter is the manuscript of my main research work on linear forms in two p-adic logarithms.

As mentioned in Chapter 1, there are results on linear forms in n logarithms for complex case and p-adic case with the dependence on $\log B$, which is regarded as the best possible. For example, Kunrui Yu published several series of celebrated work on various refinements on the results of p-adic linear forms in n logarithms with the dependence on $\log B$.

For the particular case when $n = 2$, Laurent [54] and Laurent, Mignotte and Nesterenko in [56] obtained results in 1994 and 1995 respectively. They achieve very sharp bound on numerical constant (to a size of less than 30 in [56]) with the cost of worsening the dependence of $\log B$ to $(\log B)^2$. Bugeaud and Laurent [33] adopted the same format of matrix as in [54, 56] and obtained the p-adic analogue of these results.

By introducing one more variable to the matrix in [54, 56] and using an improved version on multiplicity estimates, Gouillon [50] in 2006 suceeded in obtaining the dependence back to $\log B$ and maintaining the numerical constant of reasonable size. He obtained the lower bound of $|\Lambda| = |b_2 \log \alpha_2 - b_1 \log \alpha_1|$, where α_1, α_2 are two non-zero complex algebraic numbers, $\log \alpha_1, \log \alpha_2$ are any nonzero determinations of their logarithms and b_1, b_2 are two nonzero rational integers. The following states one of his corollaries.

Let $D = [\mathbb{Q}(\alpha_1, \alpha_2) : \mathbb{Q}]/[\mathbb{R}(\alpha_1, \alpha_2) : \mathbb{R}]$. Put $b = \frac{b_1}{D \log A_2} + \frac{b_2}{D \log A_1}$, with A_1, A_2 real numbers > 1 so that $\log A_i \geq \max\left\{h(\alpha_i), \frac{|\log \alpha_i|}{D}, \frac{1}{D}\right\}$, $(i = 1, 2)$ in which $h(\alpha_i)$ is the usual (Weil's) absolute logarithmic height of α.

Corollary 2.2 of Gouillon [50]. Suppose that α_1 and α_2 are multiplicatively independent. Then

$$\log |\Lambda| \geq -9400 \left(3.317 + \frac{1.888}{D} + 0.946 \log D \right) D^4 h \log A_1 \log A_2$$

with

$$h = \max\left\{ \log b + 3.1, \frac{1000}{D}, 498 + \frac{284}{D} + 142 \log D \right\}.$$

Our results presented in Chapter 3 is a p-adic analogue of Gouillon's results [49, 50]. It is the first work of linear forms in two p-adic logarithms using interpolation determinant method with an explicit determination of numerical constant and a dependence on H (which is analogous to $\log B$ in Yu's results), where H is bounded below by terms involving a logarithm of b_1 and b_2. We manage to maintain a reasonable size for the numerical constant.

We follow a similar proof from Bugeaud and Laurent [33] for the arithmetic lower bound of $|\gamma|_p$, where γ is the determinant of an extracted square matrix, by means of Liouville's estimate. For deducing the analytic upper bound, we refer to the development in the proof of Bugeaud and Laurent [33] and in Gouillon [49, 50]. We obtain the analytic upper bound by means of Schwarz's lemma (p-adic version).

It should be noted that our results as well as results in [33, 49, 50, 54, 56] are established with the assumption that α_1 and α_2 are multiplicatively independent.

2.2 Diophantine equations of Pillai's type

S. S. Pillai considered Diophantine problems on perfect powers and in particular posed in [71] the following famous

Conjecture 2.1 (Pillai's Conjecture). *For any integer $c \geq 1$, the Diophantine equation*

$$a^x - b^y = c \tag{2.2.1}$$

has only finitely many positive integer solutions (a, b, x, y), with $x \geq 2$ and $y \geq 2$.

Another interpretation of Conjecture 2.1 is mentioned in Pillai's another paper in 1945 [72]. It refers to the arrangement of all perfect powers of integers in ascending order as

$$1,\ 4,\ 8,\ 9,\ 16,\ 25,\ 27,\ 32,\ 36,\ 49,\ 64,\ 81,\ 100,\ 121,\ 125,\ 128, \ldots .$$

Denote by a_n the n-th term in the above series so that $a_1 = 1, a_2 = 4, a_3 = 8$ etc. Then Conjecture 2.1 is equivalent to

$$\liminf_{n \to \infty} (a_n - a_{n-1}) = \infty.$$

For $c = 1$ it becomes Catalan's conjecture, dated back to 1844 [35] and is eventually solved by Mihăilescu [67]. For $c \neq 1$ Conjecture 2.1 is still open. If one of the four variables a, b, x, y is fixed, it is known that (2.2.1) has only finitely many solutions. Moreover, there is more understanding on the solutions of this problem when a and b are fixed. For a more recent results we can refer for example to the work by Bennett [21], in which he showed that for fixed a and b equation (2.2.1) has at most two solutions. Besides, he gives the following

Conjecture 2.2 (Bennett [21], Conjecture 1.2). *If a, b, c are positive integers with $a, b \geq 2$, then equation (2.2.1) has at most one solution in positive integers x and y, except for those triples (a, b, c) corresponding to the following set of equations:*

$$
\begin{array}{cc}
3 - 2 = 3^2 - 2^3 = 1 & 2^3 - 3 = 2^5 - 3^3 = 5 \\
2^4 - 3 = 2^8 - 3^5 = 13 & 2^3 - 5 = 2^7 - 5^3 = 3 \\
13 - 3 = 13^3 - 3^7 = 10 & 91 - 2 = 91^2 - 2^{13} = 89 \\
6 - 2 = 6^2 - 2^5 = 4 & 15 - 6 = 15^2 - 6^3 = 9 \\
280 - 5 = 280^2 - 5^7 = 275 & 4930 - 30 = 4930^2 - 30^5 = 4900 \\
6^4 - 3^4 = 6^5 - 3^8 = 1215. &
\end{array}
$$

2.2.1 On a variant of Pillai's problem: $F_n - T_m = c$

The solving of equations involving linear recurrence sequences instead of the sequence of perfect powers can be regarded as a variant of Pillai's problem.

In **Chapter 4**, we find all integers c having at least two representations of the form $F_n - T_m$ for some positive integers n and m, with $\{F_n\}_{n\geq 0}$ and $\{T_m\}_{m\geq 0}$ representing the sequences of Fibonacci number and Tribonacci number respectively.

The content of Chapter 4 is the same as the joint paper with István Pink and Volker Ziegler titled "On a variant of Pillai's problem" [36], which is published in the International Jounal of Number Theory.

2.2.2 On a variant of Pillai's problem: $U_n - V_m = c$

In **Chapter 5**, we generalize the setting considered in Chapter 4 and show that under mild conditions there are only finitely many c such that the equation $U_n - V_m = c$ has at least two distinct solutions (n, m), where $\{U_n\}_{n\geq 0}$ and $\{V_m\}_{m\geq 0}$ are given linear recurrence sequences.

The content of Chapter 5 is the same as the joint paper with István Pink and Volker Ziegler titled "On a variant of Pillai's problem II" [37], which is published in the Journal of Number Theory.

2.3 Sums of Fibonacci numbers and powers of two

A Zeckendorf representation is to express a number as a sum of nonconsecutive Fibonacci numbers, that is

$$n = \sum_{k=0}^{L} \epsilon_k F_k$$

where $\epsilon_i \in \{0, 1\}$ and $\epsilon_k \epsilon_{k+1} = 0$. Every positive integer can be written uniquely in this form.

There has been vast studies on solving Diophantine equations involving linear recurrence sequences, especially the Fibonacci sequence. In **Chapter 6**, we shall completely solve the Diophantine equations

$$F_{n_1} + F_{n_2} = 2^{a_1} + 2^{a_2} + 2^{a_3} \quad \text{and} \quad F_{m_1} + F_{m_2} + F_{m_3} = 2^{t_1} + 2^{t_2}, \tag{2.3.1}$$

where F_k denotes the k-th Fibonacci number. In particular, we prove that $\max\{n_1, n_2, a_1, a_2, a_3\} \leq 18$ and $\max\{m_1, m_2, m_3, t_1, t_2\} \leq 16$. The solving of (2.3.1) amounts to determining all integers that have few non-zero integer digits in their binary as well as in their Zeckendorf expansion.[1]

[1]In Chapter 6 and in [38] we used sequence $\{F_n\}_{n\geq 0}$ of Fibonacci numbers defined by $F_0 = 0$, $F_1 = 1$ and $F_{n+2} = F_{n+1} + F_n$ for $n \geq 0$. There should be a shift of the index by two (into $F_0 = 1$, $F_1 = 2$ and $F_{n+2} = F_{n+1} + F_n$ for $n \geq 0$) when we refer to the Zeckendorf representation.

The content of Chapter 6 is similar to the submitted joint paper with Volker Ziegler titled "On Diophantine equations involving sums of Fibonacci numbers and powers of 2" [38].

Chapter 3

Linear forms in two p-adic logarithms

This chapter is the manuscript of the main research work on linear forms in two p-adic logarithms by the author.

3.1 Introduction

In 1960's, Baker [1, 2, 3, 4] published a series of papers on linear forms in logarithms. He obtained in [2] that

$$|\Lambda| = |\beta_1 \log \alpha_1 + \ldots + \beta_n \log \alpha_n| > Ce^{-(\log h)^{\kappa}},$$

where $\alpha_1, \ldots, \alpha_n$ are non-zero algebraic numbers such that $\log \alpha_1, \ldots, \log \alpha_n$ are linearly independent over the rationals, $\beta_1, \ldots, \beta_n$ are algebraic numbers not all 0. Also, d and h denote the maximum of the degrees and the classical heights of $\beta_1, \ldots, \beta_n$ respectively, $\kappa > 2n + 1$ $(n \geq 2)$ and $C = C(n, \alpha_1, \ldots, \alpha_n, \kappa, d) > 0$ is an effectively computable number.

The studies were performed subsequently by other mathematicians. In particular, Baker and Wüstholz [19] refined the lower bound for $|\Lambda| = |b_1 \log \alpha_1 + \cdots + b_n \log \alpha_n|$ with an explicit constant and a dependence on $\log B$, where $B = \max\{|b_1|, \ldots, |b_n|\}$ essentially and $b_1, \ldots, b_n$ are rational integers (not all 0). It is a vast improvement to the lower bound with a dependence on $(\log B)^2$ in preceding publications by other mathematicians especially Baker's original results [1, 2, 3, 4]. The final structure for the lower bound for linear forms in logarithms without an explicit determination of the constant $C(k, d)$ involved has been established by Wüstholz [93] and the precise determination of that constant is the central aspect of [19] (see also [20]). An extension theory on generalizing studies on logarithmic forms to the p-adic domain was also developed. In particular, Kunrui Yu [100]–[102] performed p-adic analogies of Baker and Wüstholz [19] and subsequent improvement.

Studies by some French mathematicians such as Laurent were performed to use interpolation determinant method to obtain the bound for linear forms in logarithms. In particular, his study in [54] was for $n = 2$, with

$$|\Lambda| = |b_2 \log \alpha_2 - b_1 \log \alpha_1|,$$

where $\alpha_1, \alpha_2 \geq 1$ are two real and multiplicatively independent algebraic numbers, b_1 and b_2 are rational integers. The result involves a dependence of $(\log B)^2$ for the bound (here B has a different but analogous expression as Baker and Wüstholz [19]) but the constant C for the lower bound of was greatly reduced to a size of less than 100. Further improvements on the constant were given by Laurent, Mignotte and Nesterenko in [56] and Laurent in [55]. Bugeaud and Laurent [33] obtained the p-adic analogy.

In 2006, Gouillon [50] modified that of Laurent [54] and succeeded in yielding the lower bound of linear forms in two logarithms with a dependence on $\log B$, and maintain the constant C to be of reasonable size.

The purpose of this chapter is to obtain an analogy of Gouillon's results for the non-Archimedean case. We make use of the method of interpolation determinants in our derivation, and manage to obtain the lower bound with a dependence of H (which is analogous to $\log B$) and an explicit constant of reasonable size.

We shall first state the theorem (Theorem 3.1) and the Main Proposition in Section 3.2. A brief description on the p-adic setting, multiplicity estimates and the Δ-functions will be presented in Section 3.3. After the construction of the square matrix δ with non-vanishing determinant γ in Section 3.4, we proceed with deducing the arithmetic lower bound for $|\gamma|_p$, analytic upper bound for $|\gamma|_p$ and the Main Proposition in Section 3.5, Section 3.6 and Section 3.7 respectively. Next, we derive Theorem 3.1 using the Main Proposition and appropriate choices of parameters in Section 3.8 and Section 3.9. Finally, we present results of variants of Theorem 3.1 in Section 3.10. In proving the Main Proposition, we follow a similar proof from Bugeaud and Laurent [33] for the arithmetic lower bound of $|\gamma|_p$ by means of Liouville's estimate. By referring to the development in the proof of Bugeaud and Laurent [33] and the proof in Gouillon [49, 50], we obtain the analytic upper bound by means of Schwarz's lemma (p-adic version).

3.2 Statements of the results

Before stating Theorem 3.1 and the Main Proposition, we shall introduce some notations and the setting. Let p be a prime number. Denote $\overline{\mathbb{Q}}_p$ as the algebraic closure of $\mathbb{Q}_p$. The field $\overline{\mathbb{Q}}_p$ has the ultrametric absolute value $|x|_p = p^{-v_p(x)}$, where v_p is the extension of p-adic valuation in $\mathbb{Q}_p$ normalized by $v_p(p) = 1$. Let α_1, α_2 be two numbers algebraic over $\mathbb{Q}$ and we regard them as elements of the field $\overline{\mathbb{Q}}_p$. We consider obtaining the lower bound of

$$\Lambda = {\alpha_1}^{b_1} - {\alpha_2}^{b_2},$$

where b_1, b_2 are positive rational integers. As in the complex case in [54] and [56], we denote by $h(\alpha)$ the absolute logarithmic height of α, that is,

$$h(\alpha) = \frac{1}{d}\left(\log|a| + \sum_{i=1}^{d} \log\max(1, |\alpha^{(i)}|)\right),$$

where the minimal polynomial of α is written as $a\prod_{i=1}^{d}(X - \alpha^{(i)})$.

The results depends in addition on several parameters related to the field $\mathrm{K}_v = \mathbb{Q}_p(\alpha_1, \alpha_2)$. Denote by e the ramification index of the valuation group from $\mathbb{Q}_p$ to K_v and by f the residue class degree of the extension. Denote U_v as the multiplicative group of units K_v^* (formed of $x \in \mathrm{K}_v$ with $v_p(x) = 0$). Denote by U_v^1 the subgroup of principal units (for which $v_p(x-1) > 0$). Put

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

We assume that α_1 and α_2 belongs to U_v (i.e. $v_p(\alpha_1) = v_p(\alpha_2) = 0$) in the rest of the chapter. Denote by g the smallest positive integer such that

$$\alpha_i{}^g \in U_v^1 \quad (i = 1, 2). \tag{3.2.1}$$

That is, we have $v_p(\alpha_1{}^g - 1) > 0$ and $v_p(\alpha_2{}^g - 1) > 0$. It should be noted that g divides $p^f - 1$. (See [33, Lemma 4].) Let $A_1, A_2 > 1$ be two real numbers such that

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

Furthermore, we denote

$$b' = \frac{b_1}{D\log A_2} + \frac{b_2}{D\log A_1}.$$

We shall state the theorem.

Theorem 3.1. *Suppose that α_1 and α_2 are multiplicatively independent. Then we have the upper bound*

$$v_p(\Lambda) < C\left(\frac{p}{p-1}\right)\frac{gD^4}{(\log p)^3}\left(\frac{Z_1\log p}{2D} + 4.85 + \log D\right)\log A_1 \log A_2\, H$$

where

$$\begin{cases} C = 4300, & Z_1 = 4, \quad \text{if } p = 2, \\ C = 4700, & Z_1 = 3, \quad \text{if } p = 3, \\ C = 27600, & Z_1 = 1, \quad \text{if } p \geq 5, \end{cases}$$

$$H = \max\left\{\log b' + \log\log p, \frac{1000\log p}{D}, 180\left(\frac{Z_1\log p}{2D} + 4.85 + \log D\right)\log p\right\},$$

$$g \leq p^f - 1.$$

It should be noted that the values 1000 and 180 in the above expression of H can be changed and the value of C in the upper bound will be changed accordingly. For example, for the case when $p \geq 5$ if we take

$$H = \max\left\{\log b' + \log\log p, \frac{10000\log p}{D}, 1800\left(\frac{\log p}{2D} + 4.85 + \log D\right)\log p\right\},$$

then C becomes 27210.

We have a rough estimation that for the case when $p \geq 5$ the value of C in the upper bound can be reduced to roughly 27100 if H is asymptotically large.

If we compare Theorem 3.1 with Theorem 3 from Bugeaud and Laurent [33], we notice that their final constant is much smaller and the dependence on $\log p$ is slightly better. The main difference however is that our result yields a dependence of H instead of H^2 in their results.

Theorem 3.1 can be obtained from the Main Proposition to be stated below. Let us consider the following additional setting and notations.

Fix in $\overline{\mathbb{Q}}_p$ a root of unity ζ with order exactly g. [33, Lemma 4] shows that ζ belongs to the subfield K_v. We can write α_1 and α_2 uniquely as

$$\alpha_i = \zeta^{m_i}\theta_i, \quad \theta_i \in U_v^1 \quad (i = 1, 2) \tag{3.2.2}$$

with integers m_1, m_2 determined modulo g. Besides, we have $v_p(\theta_1 - 1) > 0$ and $v_p(\theta_2 - 1) > 0$. Denote by $\kappa \geq 0$ the integer satisfying the inequalities

$$p^{\kappa-1} \leq \frac{2e}{p-1} < p^{\kappa} \tag{3.2.3}$$

where e is the ramification index of the valuation group from $\mathbb{Q}_p$ to K_v defined before. Let K and L be integers ≥ 1, let $T_1, T_2, T_3, R_1, R_2, R_3, S_1, S_2$ and S_3 be integers ≥ 0. We set

$$R = R_1 + R_2 + R_3, \qquad S = S_1 + S_2 + S_3, \qquad T = T_1 + T_2 + T_3.$$

For any pair of positive integers (b_1, b_2), denote p^u as the greatest power of p that divides simultaneously b_1 and b_2. Denote

$$N = \frac{(K+1)(K+2)(L+1)}{2}, \quad \widetilde{B} = \frac{Rb_2 + Sb_1}{2K} \quad \text{and} \quad \Psi(n) = (R+n)(S+n)(T+1). \tag{3.2.4}$$

Denote by g_0, ω and ω_0 real numbers which satisfy the lower bounds:

$$g_0 \geq \frac{1}{4} - \frac{gN}{12\Psi(g)}, \qquad \omega \geq 1 - \frac{gN}{2\Psi(g)}, \qquad \omega_0 \geq \frac{3\Psi(g)}{2gN}. \tag{3.2.5}$$

We introduce the sets

$$
\begin{aligned}
\mathcal{E}_{1A} &= \{rb_2 + sb_1; 0 \le r \le R_1, 0 \le s \le S_1,\ m_1 r + m_2 s \equiv c_1 \mod g\},\\
\mathcal{E}_{1B} &= \left\{\alpha_1^{p^\kappa r}\alpha_2^{p^\kappa s}; 0 \le r \le R_1, 0 \le s \le S_1,\ m_1 r + m_2 s \equiv c_1 \mod g\right\},\\
\mathcal{E}_{2A} &= \{rb_2 + sb_1; 0 \le r \le R_2, 0 \le s \le S_2,\ m_1 r + m_2 s \equiv c_2 \mod g\},\\
\mathcal{E}_{2B} &= \left\{\alpha_1^{p^\kappa r}\alpha_2^{p^\kappa s}; 0 \le r \le R_2, 0 \le s \le S_2,\ m_1 r + m_2 s \equiv c_2 \mod g\right\},\\
\mathcal{E}_{3} &= \left\{(rb_2 + sb_1, \alpha_1^{p^\kappa r}\alpha_2^{p^\kappa s}); 0 \le r \le R_3, 0 \le s \le S_3,\ m_1 r + m_2 s \equiv c_3 \mod g\right\}
\end{aligned}
$$

with c_1, c_2, c_3 residue classes modulo g such that they satisfy the following condition:

$$
\begin{aligned}
T_1 &\ge K,\\
\mathrm{Card}\,\mathcal{E}_{1A} &\ge K + 1,\\
(T_1 + 1)\mathrm{Card}\,\mathcal{E}_{1B} &\ge L + 1,\\
(T_2 + 1)\mathrm{Card}\,\mathcal{E}_{2B} &\ge 2KL + 1,\\
(T_2 + 1)\mathrm{Card}\,\mathcal{E}_{2A} &\ge K^2 + 1,\\
(T_3 + 1)\mathrm{Card}\,\mathcal{E}_{3} &\ge 3K^2L + 1.
\end{aligned}
\tag{3.2.6}
$$

Furthermore, we introduce

$$
V = \frac{1}{4}\left(1 - \frac{1}{L+1} + \sqrt{1 - \frac{2}{L+1}}\right)(K+2)(L+1)\lambda, \tag{3.2.7}
$$

where

$$
V > \frac{1}{p-1} \tag{3.2.8}
$$

and

$$
\lambda = \frac{\eta p^\kappa}{2e} \qquad \text{with} \qquad \eta = 1 - 10^{-50}. \tag{3.2.9}
$$

Our Main Proposition is as follows.

Main Proposition. Suppose the following **Condition (1a)** holds:

$$
\begin{aligned}
\frac{V}{2} \ge \left(T + \frac{K}{3}\right)\lambda + \frac{K}{3(p-1)} + \frac{D}{e\log p}\Bigg(\log\left(\frac{N}{2}\right) + \frac{K}{3}\left(\log\widetilde{B} + \log\left(\frac{T}{KL}\right) + \frac{1454}{309}\right)\\
+ (\omega T + \omega_0)\left(2 + \log\left(\frac{107(K+3)L}{309\omega T} + 1\right)\right) + 1 + p^\kappa(L+1)g_0\left((R+g)h(\alpha_1) + (S+g)h(\alpha_2)\right)\Bigg).
\end{aligned}
\tag{3.2.10}
$$

Then

$$
|\Lambda|_p > p^{-(V+u)}. \tag{3.2.11}
$$

3.3 Backgrounds on the p-adic setting, multiplicity estimates and the Δ-functions

In this section, backgrounds on the p-adic exponential and logarithmic functions, multiplicity estimates and the Δ-function will be addressed.

3.3.1 The p-adic exponential and logarithmic functions

The convergence of exponential and logarithmic functions is an important issue in the p-adic setting. There is a comprehensive description on the p-adic exponential and logarithmic functions, normal series and functions as well as supernormality in Yu [97, Sections 1.1–1.3]. We shall make use of some facts described there in our work.

Here we shall briefly presents some technical tools about the p-adic exponential function and the p-adic logarithm. As usual let $\mathbb{C}_p$ be the p-adic analogue of the field of complex numbers and $\mathbb{B}(r)$ the open disc $|x|_p < r$. Furthermore we introduce $\mathbb{O}_p$ as the set of $x \in \mathbb{C}_p$ such that $|x|_p \leq 1$ and write $\mathbb{M}$ for the set of $x \in \mathbb{O}_p$ such that $|x|_p < p^{-\frac{1}{p-1}}$. The main object is to establish the following

Proposition 3.1. *For $x \in \mathbb{M}$, $z \in \mathbb{O}_p$ we have*

$$(1+x)^z = 1 + xzv(x,z)$$

with some power series $v(S,T) \in \mathbb{Q}_p[[S,T]]$ such that $v(x,z) \in \mathbb{Q}_p$ with $|v(x,z)|_p \leq 1$.

Proof. Some properties of the exponential function e^z and the logarithm $\log z$ are derived which are necessary to deal with the proof of the proposition. This means that we have to study the formal power series

$$\mathrm{Exp}(X) = \sum_{n\geq 0} \frac{X^n}{n!}$$

for the exponential function and at the same time its inverse, the power series

$$\mathrm{Log}(1+X) = \sum_{n\geq 1} \frac{(-1)^{n-1}X^n}{n}$$

for the logarithm.

Exp. The formal power series for $\mathrm{Exp}(X)$ can be expressed as

$$\mathrm{Exp}(X) = 1 + X\varepsilon(X) \tag{3.3.1}$$

for

$$\varepsilon(X) = \sum_{n\geq 1} \frac{X^{n-1}}{n!} = 1 + \frac{X}{2} + \frac{X^2}{3!} + \text{higher order terms.}$$

We write $e^z = \mathrm{Exp}(X)|_{X=z}$. Then (3.3.1) means that $|e^z|_p = 1$ for $z \in \mathbb{M}$.

Log. Similar to $\mathrm{Exp}(X)$ the formal power series for the logarithm can be rewritten as

$$\mathrm{Log}(1+X) = X\lambda(X) \tag{3.3.2}$$

where

$$\lambda(X) = \sum_{n\geq 1} \frac{(-1)^{n-1}X^{n-1}}{n} = 1 - \frac{X}{2} + \text{higher order terms.}$$

It maps $\mathbb{M}$ isomorphically onto itself and has the property that the composition of the two power series $\mathrm{Exp}(X)$ and $\mathrm{Log}(X)$ give the identity:

$$z \in \mathbb{M}^m \mapsto e^z \in 1 + \mathbb{M}^m \mapsto z \in \mathbb{M}^m,$$

where M^m is the the ideal $\{x \in \mathbb{O}_p \mid \ |x|_p < p^{-\frac{m}{p-1}}\}$.

One derives that

$$\log(1+z) = z\lambda(z)$$

and deduces that

$$|\log(1+z)|_p = |z|_p$$

for $z \in \mathbb{M}$.

Exponential function $(1+X)^Y$**.** We define

$$(1+X)^Y = \mathrm{Exp}(Y\log(1+X)) \tag{3.3.3}$$

and easily one sees that the series on the right exists as a formal power series. The reason is that its constant term is zero and one applies standard results from [26]. We then define

$$(1+a)^z := (1+X)^Y\big|_{X=a, Y=z}$$

for $a \in \mathbb{M}$ and $z \in \mathbb{O}_p$. From above and (3.3.3) it becomes clear that

$$(1+X)^Y = 1 + XYv(X,Y),$$

with $|v(X,Y)|_p \leq 1$ and that $(1+a)^z$ maps $\mathbb{O}_p$ into $1+\mathbb{M}$. The latter holds for $\mathbb{Z}$ and then by continuity also for $\mathbb{O}_p$. This establishes Proposition 3.1. □

3.3.2 Multiplicity estimates

We now state the multiplicity estimate used in [49, 50]. We shall adopt the same theory of multiplicity estimate for our case with $m = 2$.

We work with the product group $\mathbb{C}^2 \times \mathbb{C}^\times$ whose group law is written additively by the symbol +. For any element w in $\mathbb{C}^\times$ and any element (v_0, v_1) in $\mathbb{C}^2$ we denote briefly $(\underline{v}, w) = (v_0, v_1, w) \in \mathbb{C}^2 \times \mathbb{C}^\times$. Let $\mathfrak{D} := \frac{\partial}{\partial X_0} + Y\frac{\partial}{\partial Y}$ be a derivation operating on the polynomial's ring $\mathbb{C}[\underline{X}, Y]$. Let T be a non-negative integer. We say that a polynomial $P \in \mathbb{C}[\underline{X}, Y]$ vanishes to order $> T$ with respect to $\mathfrak{D}$ on the set $\Sigma \subseteq \mathbb{C}^2 \times \mathbb{C}^\times$, if for any integer $0 \le t \le T$, $\mathfrak{D}^t P$ vanishes identically on Σ.

Theorem 3.2. *Let K, L be integers ≥ 1, let T_1, T_2, T_3 be integers ≥ 0 and let $\Sigma_1, \Sigma_2, \Sigma_3$ be nonempty finite sets of $\mathbb{C}^2 \times \mathbb{C}^\times$. Denote by $\mu_j(W \times \mathbb{C}^\times)$ and $\mu_j(W \times \{1\})$ the number of distinct elements of Σ_j modulo $W \times \mathbb{C}^\times$ and $W \times \{1\}$ respectively. Assume that for all $j = 1, 2$ and any vector subspace W of $\mathbb{C}^2$ with dimension $\le 2 - j$, we have*

$$\binom{T_j + 1}{\varepsilon_j} \mu_j(W \times \mathbb{C}^\times) > K^j, \text{ where } \varepsilon_j = \begin{cases} 1, & \text{if } (1,0) \notin W, \\ 0, & \text{otherwise.} \end{cases} \tag{3.3.4}$$

Assume further that for all $j = 1, 2, 3$ and any vector subspace W of $\mathbb{C}^2$ with dimension $\le 3 - j$, we have

$$(T_j + 1)\, \mu_j(W \times \{1\}) > jK^{j-1}L. \tag{3.3.5}$$

Then any polynomial $P \in \mathbb{C}[\underline{X}, Y]$ of total degree $\le K$ in $\underline{X}$ and of degree $\le L$ in Y which vanishes on $\Sigma_1 + \Sigma_2 + \Sigma_3$ to order $> T_1 + T_2 + T_3$ with respect to $\mathfrak{D}$ is identically zero.

Proof. See the proof of [50, Theorem 3.1] and [49, Theorem 2.1]. □

3.3.3 The Δ-functions and the variation

We shall introduce the Δ-functions and the variation. Define for any $z \in \mathbb{C}$ and any $n \in \mathbb{N}$ the functions Δ, which were introduced by Feldman [43], by

$$\Delta(z; n) = \frac{(z+1)\cdots(z+n)}{n!},$$

with $\Delta(z; 0) = 1$ for $n = 0$. It is clear that $\Delta(z; n)$ takes integer value for all integers z. It should also be noted that $\Delta(z; 0), \Delta(z; 1), \ldots, \Delta(z; n)$ forms a basis for the vector space of polynomials of degree $\le n$. On top of the Δ-function we perform further variation. For any $a \in \mathbb{N}$ and any $b \in \mathbb{N}^*$ we define the polynomial $\Delta(z; b, a) \in \mathbb{Q}[z]$ of degree a by

$$\Delta(z; b, a) = \Delta(z; b)^q \Delta(z; r),$$

where by Euclidean division $a = bq + r$. For any integer $c \ge 0$ denote furthermore

$$\pi(z; b, a, c) = \frac{1}{c!}\left(\frac{d}{dz}\right)^c \Delta(z; b, a) = \frac{1}{c!}\left(\frac{d}{dz}\right)^c \Delta(z; b)^q \Delta(z; r).$$

Denote by $\nu(b)$ the least common multiple of $1, 2, \ldots, b$. Finally, denote

$$\Delta(l; b, a, c) = \nu(b)^c \pi(l; b, a, c). \tag{3.3.6}$$

A nice property of $\Delta(l; b, a, c)$ is described in

Lemma 3.3. *Let a, b and c be integers ≥ 0 with $b \geq 1$ and $c \leq a$. Then for $l \in \mathbb{N}$,*

$$\Delta(l; b, a, c) \in \mathbb{Z}.$$

Proof. It is a modified version of the proof of [89, Lemma T1] since our $\Delta(l; b, a, c)$ is defined differently. First, note that

$$\pi(l; b, a, c) = \frac{1}{b!^q r!}\left((l+1)\cdots(l+b)\right)^q (l+1)\cdots(l+r)\sum(l+j_1)^{-1}\cdots(l+j_c)^{-1} \tag{3.3.7}$$

where $j_1, \ldots, j_c$ runs through all the selections of integers from the set $1, \ldots, b, 1, \ldots, r$ with $1, \ldots, b$ repeated q times and the right hand side is read as 0 if $c > a$.
Write $\pi(l; b, a, c) = \frac{m}{n}$, where $m, n \in \mathbb{Z}$, $(m, n) = 1$. If p is a prime with $p|n$, then from (3.3.7), $p|(b!^q r!)$ and hence $p|b!$ and hence $p \leq b$. Then the number of factors p of $b!^q r!$ is exactly

$$l\left(\left[\frac{b}{p}\right] + \cdots + \left[\frac{b}{p^{u_1}}\right]\right) + \left[\frac{r}{p}\right] + \cdots + \left[\frac{r}{p^{u_2}}\right]$$

where $u_1 = \left[\frac{\log b}{\log p}\right]$ and $u_2 = \left[\frac{\log r}{\log p}\right]$. Since $\Delta(l; b, a) = \frac{((l+1)\cdots(l+b))^q (l+1)\cdots(l+r)}{b!^q r!} \in \mathbb{Z}$, the product $((l+1)\cdots(l+b))^q (l+1)\cdots(l+r)$ contains at least as many factors p as in $b!^q r!$. In fact, there may be more than u_1 factors p in a certain factor $l + j$ $(1 \leq j \leq c)$ which we have not counted. Hence if c factors are removed out of this product, the remaining product contains at least

$$l\left(\left[\frac{b}{p}\right] + \cdots + \left[\frac{b}{p^{u_1}}\right]\right) + \left[\frac{r}{p}\right] + \cdots + \left[\frac{r}{p^{u_2}}\right] - cu_1 \tag{3.3.8}$$

factors p. It follows that the number of factors p that

$$\left((l+1)\cdots(l+b)\right)^q (l+1)\cdots(l+r)\sum(l+j_1)^{-1}\cdots(l+j_c)^{-1}$$

contains is at least that of (3.3.8). As a result, n contains at most $cu_1 = c\left[\frac{b}{p}\right]$ factors p. This is exactly the number of factors p of $\nu(b)^c$. Therefore Lemma 3.3 follows. □

The following lemma reveals an upper bound for $|\Delta(l; b, a, c)|$.

Lemma 3.4. *Let a, b, q, r, l be non-negative integers with $a = bq + r$ and $0 \leq r < b$. Then we have*

$$|\Delta(l; b, a, c)| < e^{\frac{107bc}{103}} \binom{a}{c} \frac{(l+b)^{a-c}}{b^a} e^{a+b}.$$

Proof. First, by referring to the Taylor expansion of e^x, we have $e^b = 1 + b + \cdots + \frac{b^r}{r!} + \cdots + \frac{b^b}{b!} + \cdots$ so that $\left(\frac{b^b}{b!}\right)^q\left(\frac{b^r}{r!}\right) \le e^{bq}e^r \le e^{a+b}$ and thus $\frac{1}{b!^q r!} \le \frac{1}{b^a}e^{a+b}$. Next,

$$\begin{aligned}
\Delta(l;b,a,c) &= \frac{\nu(b)^c}{c!}\left(\left(\frac{d}{dz}\right)^c \Delta(z;b)^q\Delta(z;r)\right)_{z=l}\\
&= \frac{\nu(b)^c}{c!b!^q r!}\left(\left(\frac{d}{dz}\right)^c ((z+1)\cdots(z+b))^q (z+1)\cdots(z+r)\right)_{z=l}\\
&= \frac{\nu(b)^c}{b!^q r!}((l+1)\cdots(l+b))^q(l+1)\cdots(l+r)\sum(l+j_1)^{-1}\cdots(l+j_c)^{-1}\\
&= \nu(b)^c\Delta(l;b,a)\underbrace{\sum(l+j_1)^{-1}\cdots(l+j_c)^{-1}}_{\binom{a}{c}\text{ terms}}
\end{aligned}$$

where the sum is over all selections $j_1,\ldots,j_c$ from the set $\{1,2,\ldots,b,1,\ldots,r\}$ in which $\{1,\ldots,b\}$ is repeated q times. We use the estimate $\nu(b) < \exp(1.03883b) < \exp\left(\frac{107b}{103}\right)$ (see [74, p.71, (3.35)]). Since $\Delta(l;b,a)(l+j_1)^{-1}\cdots(l+j_c)^{-1} \le \frac{(l+b)^{a-c}}{b!^q r!}$, the upper bound in Lemma 3.4 follows. □

3.4 Construction of matrices M, $\mathcal{M}$, $\widetilde{\mathcal{M}}$ and δ

Our goal of this section is to obtain a square matrix δ with $\det\delta \ne 0$ under condition (3.2.6). Recall N and $\Psi(1)$ are in (3.2.4). To begin with, we denote by $\mathbf{M}$ a matrix of size $N\times\Psi(1)$ with $N\le\Psi(1)$ whose coefficients are the numbers

$$\mathfrak{D}^t\left(\frac{X_0^{k_0}}{k_0!}X_1^{k_1}Y^l\right)\Big|_{(0,rb_2+sb_1,\alpha_1^{p^\kappa r}\alpha_2^{p^\kappa s})} = (rb_2+sb_1)^{k_1}l^{t-k_0}\binom{t}{k_0}\alpha_1^{p^\kappa rl}\alpha_2^{p^\kappa sl} \tag{3.4.1}$$

where (k_0,k_1,l) with $(0\le k_0+k_1\le K, 0\le l\le L)$ is the row index, while (r,s,t) with $(0\le t\le T, 0\le r\le R, 0\le s\le S)$ is the column index. Next, we extract a matrix $\mathcal{M}$, formed by columns (r,s,t) of $\mathbf{M}$ satisfying $m_1r+m_2s\equiv c$ modulo g, where $c=c_1+c_2+c_3$ and c_1,c_2 and c_3 are fixed integers satisfying (3.2.6). The numbering of the rows and columns for $\mathbf{M}$ and $\mathcal{M}$ are not important.

Lemma 3.5. *The matrix $\mathcal{M}$ has maximal rank, equal to the number of rows N.*

Proof. The proof follows along the same line as in [49] with α_1 and α_2 replaced by $\alpha_1^{p^\kappa}$ and $\alpha_2^{p^\kappa}$ and changes made to the sets Σ_1, Σ_2 and Σ_3.
We proceed by contradiction assuming that rank$(\mathcal{M}) < N$. Then there exists $\lambda_1,\ldots,\lambda_N\in\mathbb{C}$, not all zero, such that if we denote by L_i $(i=1,\ldots,N)$ the rows of $\mathcal{M}$, we have the linear relationship

$$\sum_{i=1}^N \lambda_i L_i = 0.$$

Let

$$P = \sum_{i=1}^N \lambda_i \frac{X_0^{k_{0,i}}}{k_{0,i}!}X_1^{k_{1,i}}Y^{l_i}.$$

Note that P is not identically zero. Besides, by definition $0 \le k_{0,i} + k_{1,i} \le K$ and $0 \le l_i \le L$ for all $i = 1, \dots, N$, so that

$$\deg_{\underline{X}} P = \max_{1\le i\le N}\{k_{0,i} + k_{1,i}\} \le K, \qquad \deg_Y P = \max_{1\le i\le N}\{l_i\} \le L.$$

By the composition of $\mathcal{M}$, we also notice that $\mathfrak{D}^t P$ vanishes on the set

$$\Sigma_{RS} = \{(0, rb_2 + sb_1, \alpha_1^{p^\kappa r}\alpha_2^{p^\kappa s}); 0 \le r \le R, 0 \le s \le S, m_1 r + m_2 s \equiv c \mod g\}$$

for all $0 \le t \le T$. Now, let

$$\begin{aligned}
\Sigma_1 &= \{(0, rb_2 + sb_1, \alpha_1^{p^\kappa r}\alpha_2^{p^\kappa s}); 0 \le r \le R_1, 0 \le s \le S_1, m_1 r + m_2 s \equiv c_1 \mod g\},\\
\Sigma_2 &= \{(0, rb_2 + sb_1, \alpha_1^{p^\kappa r}\alpha_2^{p^\kappa s}); 0 \le r \le R_2, 0 \le s \le S_2, m_1 r + m_2 s \equiv c_2 \mod g\},\\
\Sigma_3 &= \{(0, rb_2 + sb_1, \alpha_1^{p^\kappa r}\alpha_2^{p^\kappa s}); 0 \le r \le R_3, 0 \le s \le S_3, m_1 r + m_2 s \equiv c_3 \mod g\}
\end{aligned}$$

with $c_1 + c_2 + c_3 \equiv c \mod g$. It can be easily checked that

$$\Sigma_{RS} \supseteq \Sigma_1 + \Sigma_2 + \Sigma_3$$

since $R = R_1 + R_2 + R_3$, $S = S_1 + S_2 + S_3$ and $c = c_1 + c_2 + c_3$. It follows that the polynomial P vanishes on $\Sigma_1 + \Sigma_2 + \Sigma_3$ with order $> T = T_1 + T_2 + T_3$ with respect to the derivation $\mathfrak{D}$.

We shall now apply Theorem 3.2 to obtain a contradiction by verifying assumptions (3.3.4) and (3.3.5) of Theorem 3.2. For this we note that W is a subspace of $\mathbb{C}^2$. We first check the assumption (3.3.4). There are three scenarios. For $j = 1$, the dimension W must be ≤ 1. We have two cases, either $(1,0) \notin W$, or $(1,0) \in W$. If $(1,0) \notin W$, we have to check that

$$(T_1 + 1)\, \mu_1(W \times \mathbb{C}^\times) \ge K + 1. \tag{3.4.2}$$

As $\mu_1(W \times \mathbb{C}^\times) \ge 1$, assumption (3.4.2) is therefore implied by the inequality

$$T_1 \ge K$$

which is the first condition in (3.2.6). Therefore, assumption (3.4.2) is verified. If $(1,0) \in W$, we have a check on the inequality

$$\mu_1(W \times \mathbb{C}^\times) \ge K + 1. \tag{3.4.3}$$

Since $\dim W \le 1$, it is necessary that $W = \mathbb{C}(1,0)$. So,

$$\mu_1(\mathbb{C} \times \{0\} \times \mathbb{C}^\times) = \operatorname{Card} \mathcal{E}_{1A}.$$

Assumption (3.4.3) is thus implied by the second condition in (3.2.6). For $j = 2$, we have $\dim W \le 0$ and hence $W = \{0,0\}$. We have a check on the inequality

$$(T_2 + 1)\, \mu_2(\{0,0\} \times \mathbb{C}^\times) \ge K^2 + 1. \tag{3.4.4}$$

Since

$$\mu_2(\{0,0\} \times \mathbb{C}^\times) = \mathrm{Card}\,\mathcal{E}_{2A},$$

the fifth condition in (3.2.6) implies (3.4.4).

By similar deduction, we can check that the third, forth and sixth conditions in (3.2.6) imply assumption (3.3.5). According to Theorem 3.2, the polynomial is identically zero. However, it contradicts the fact that λ_i $(i = 1, \ldots, N)$ are not all zero. Therefore, $\mathrm{rank}(\mathcal{M}) = N$. □

Now we follow a similar line as in [50] to modify $\mathcal{M}$. First we translate the term $(rb_2 + sb_1)^{k_1}$ in (3.4.1) to $\Delta(rb_2+sb_1; k_1)$ by row operations to obtain the first intermediate matrix whose coefficients are

$$\Delta(rb_2 + sb_1; k_1) l^{t-k_0} \binom{t}{k_0} \alpha_1^{p^\kappa rl} \alpha_2^{p^\kappa sl} \tag{3.4.5}$$

and whose rank is the same as $\mathrm{rank}(\mathcal{M})$. Next, we are about to replace l^{t-k_0} by $\pi(l; T', t, k_0)$. Note that

$$l^{t-k_0} \binom{t}{k_0} = \frac{1}{k_0!} \left(\frac{d}{dl}\right)^{k_0} l^t.$$

We shall make use of Lemma 3.6 (which corresponds to [50, Lemma 4.2]) below and replace z^t by a well chosen polynomial with the same degree.

Lemma 3.6. *Let $T, T' \in \mathbb{N}^*$ and $0 < T' < T$. Let $Q \in GL_{T+1}(\mathbb{Q})$ be the matrix defined by*

$$(1, z, \ldots, z^T) Q = (\Delta(z; T', 0), \ldots, \Delta(z; T', T)). \tag{3.4.6}$$

Then for any $l \in \mathbb{N}$, any $k_0 \in \mathbb{N}$ and $0 \le t \le T$,

$$\pi(l; T', t, k_0) = \sum_{\nu=0}^{T} q_{\nu,t} \binom{\nu}{k_0} l^{\nu - k_0},$$

where the $q_{\nu,t}$ are the coefficients of Q.

***Proof*.** Since each of $\Delta(z; T', 0), \ldots, \Delta(z; T', T)$ is a polynomial in z with rational coefficients, hence $Q \in GL_{T+1}(\mathbb{Q})$. Let us denote by $q_{\nu,t}$ the (ν, t)-th entry of Q. From (3.4.6), we have

$$\Delta(z; T', t) = \sum_{\nu=0}^{T} q_{\nu,t}\, z^\nu, \qquad \forall 0 \le t \le T.$$

Differentiate k_0 times with respect to z and divide by $k_0!$, we have

$$\begin{aligned}
\pi(l; T', t, k_0) &= \frac{1}{k_0!} \left(\frac{d}{dl}\right)^{k_0} \Delta(l; T', t) \\
&= \frac{1}{k_0!} \left(\frac{d}{dl}\right)^{k_0} \sum_{\nu=0}^{T} q_{\nu,t}\, l^\nu = \sum_{\nu=0}^{T} \frac{q_{\nu,t}}{k_0!} \left(\frac{d}{dl}\right)^{k_0} l^\nu \\
&= \sum_{\nu=0}^{T} q_{\nu,t} \binom{\nu}{k_0} l^{\nu-k_0}.
\end{aligned}$$

□

Lemma 3.6 shows that a second intermediate matrix with coefficient

$$\Delta(rb_2 + sb_1; k_1)\, \pi(l; T', t, k_0)\alpha_1^{p^\kappa rl}\alpha_2^{p^\kappa sl}$$

can be deduced from the first intermediate matrix by linear operations among columns of which r and s are fixed, hence maintaining the same rank as $\mathcal{M}$.

Furthermore, we multiply each row by $\nu(T')^{k_0}$, where T' is a parameter with $0 < T' < T$ to be chosen later. It should be noted from (3.3.6) that $\Delta(l; T', t, k_0) = \nu(T')^{k_0}\pi(l; T', t, k_0)$. As a result, we get a new matrix, denoted by $\widetilde{\mathcal{M}}$, with coefficients

$$\Delta(rb_2 + sb_1; k_1)\Delta(l; T', t, k_0)\alpha_1^{p^\kappa rl}\alpha_2^{p^\kappa sl} \tag{3.4.7}$$

in which $\Delta(rb_2+sb_1; k_1) \in \mathbb{Z}$ clearly and $\Delta(l; T', t, k_0) \in \mathbb{Z}$ by Lemma 3.3. It is trivial that $\operatorname{rank}(\widetilde{\mathcal{M}}) = \operatorname{rank}(\mathcal{M}) = N$.

For the last step we extract a square matrix of size $N \times N$, denoted by δ, with $\det \delta \neq 0$ from $\widetilde{\mathcal{M}}$. With a suitable ordering of rows and columns in δ we can write

$$\gamma = \det \delta = \det\left(\Delta(r_j b_2 + s_j b_1; k_{1,i})\Delta(l_i; T', t_j, k_{0,i})\alpha_1^{p^\kappa r_j l_i}\alpha_2^{p^\kappa s_j l_i}\right)_{1\le i,j\le N}. \tag{3.4.8}$$

Recall from (3.4.1) that (k_0, k_1, l) satisfies $(0 \le k_0 + k_1 \le K, 0 \le l \le L)$. Denote i and j as the row index and column index of δ respectively. Let us suppose the rows in δ are ordered in a way that

- $l_i = \left\lfloor \frac{i-1}{\left(\frac{(K+1)(K+2)}{2}\right)} \right\rfloor$,
- $k_{0,i} \le k_{0,i+1}$, and
- whenever $k_{0,i} = k_{0,i+1}$ we have $k_{1,i} \le k_{1,i+1}$

for $1 \le i \le N$. With this ordering we have $k_{1,i} = 0$ whenever $i = 1$ or $k_{0,i-1} + k_{1,i-1} = K$. Consider the polynomial

$$P(X,Y) = \sum_\sigma \operatorname{sgn}(\sigma) \prod_{i=1}^N \Delta(b_2 r_{\sigma(i)} + b_1 s_{\sigma(i)}; k_{1,i})\Delta(l_i; T', t_{\sigma(i)}, k_{0,i}) \cdot X^{\sum_{i=1}^N l_i r_{\sigma(i)}} Y^{\sum_{i=1}^N l_i s_{\sigma(i)}}, \tag{3.4.9}$$

where σ runs over all permutations $\sigma \in \mathfrak{S}_N$ and where $\operatorname{sgn}(n)$ is the signature of the permutation σ. As discussed in (3.4.7), we notice that $P(X,Y)$ has integer coefficients. By expanding the determinant γ, we get $\gamma = P\left(\alpha_1^{p^\kappa}, \alpha_2^{p^\kappa}\right)$. We shall present the following lemma for $P(X,Y)$.

Lemma 3.7. *Let $P(X,Y)$ be in (3.4.9). Then for any $q \in \mathbb{C}_p$, we have*

$$P(X,Y) = \det\left(\frac{(b_2 r_j + b_1 s_j - q)^{k_{1,i}}}{k_{1,i}!}\Delta(l_i; T', t_j, k_{0,i}) X^{l_i r_j} Y^{l_i s_j}\right)_{1\le i,j\le N}. \tag{3.4.10}$$

Proof. Referring to (3.4.9), we have

$$P(X,Y) = \det\left(\Delta(r_j b_2 + s_j b_1; k_{1,i})\Delta(l_i; T', t_j, k_{0,i}) X^{l_i r_j} Y^{l_i s_j}\right)_{1\le i,j\le N}. \tag{3.4.11}$$

Denote $\mathfrak{a}_i$ as the i-th row in $P(X,Y)$, i.e.

$$\mathfrak{a}_i = \left(\Delta(r_j b_2 + s_j b_1; k_{1,i})\Delta(l_i; T', t_j, k_{0,i}) X^{l_i r_j} Y^{l_i s_j}\right), \qquad 1 \le j \le N$$

so that

$$P(X,Y) = \det\begin{pmatrix} \mathfrak{a}_1 \\ \vdots \\ \mathfrak{a}_N \end{pmatrix}_{1\le i,j\le N}.$$

Next, denote

$$Q(q) = \det\begin{pmatrix} \mathfrak{b}_1(q) \\ \vdots \\ \mathfrak{b}_N(q) \end{pmatrix}_{1\le i,j\le N} \qquad \text{and} \qquad Q = \det\begin{pmatrix} \mathfrak{b}_1 \\ \vdots \\ \mathfrak{b}_N \end{pmatrix}_{1\le i,j\le N}$$

where

$$\mathfrak{b}_i(q) = \left(\frac{(b_2 r_j + b_1 s_j - q)^{k_{1,i}}}{k_{1,i}!}\Delta(l_i; T', t_j, k_{0,i}) X^{l_i r_j} Y^{l_i s_j}\right), \qquad 1 \le j \le N$$

and $\mathfrak{b}_i = \mathfrak{b}_i(0)$. Further, denote $\mathfrak{b}_0(q) = \mathbf{0}$. It suffices to show that
(a). $P(X,Y) = Q$ and
(b). $Q(q) = Q$.
To prove (a), note that $\mathfrak{a}_i$ can be expressed as

$$\mathfrak{a}_i = \begin{cases} \mathfrak{b}_i, & \text{if } k_{1,i} = 0, \\ \mathfrak{b}_i + \sum_{x=1}^{k_{1,i}} m_x\, \mathfrak{a}_{i-x}, & \text{otherwise} \end{cases}$$

where $m_x \in \mathbb{C}_p$. Thus, if we start rewriting from the last row, we obtain

$$P(X,Y) = \det\begin{pmatrix} \mathfrak{a}_1 \\ \vdots \\ \mathfrak{a}_{N-1} \\ \mathfrak{b}_N \end{pmatrix} + \sum_{x=1}^{k_{1,N}} m_x \det\begin{pmatrix} \mathfrak{a}_1 \\ \vdots \\ \mathfrak{a}_{N-1} \\ \mathfrak{a}_{N-x} \end{pmatrix} = \det\begin{pmatrix} \mathfrak{a}_1 \\ \vdots \\ \mathfrak{a}_{N-1} \\ \mathfrak{b}_N \end{pmatrix}.$$

We proceed similarly to the next preceding row and so on and finally obtain $P(X,Y) = Q$.
To prove (b), note that

$$\frac{d}{dq}\mathfrak{b}_i(q) = \begin{cases} \mathbf{0}, & \text{if } k_{1,i} = 0, \\ \mathfrak{b}_{i-1}(q), & \text{otherwise.} \end{cases}$$

Therefore,

$$Q'(q) = \det\begin{pmatrix} \frac{d}{dq}\mathfrak{b}_1(q) \\ \mathfrak{b}_2(q) \\ \vdots \\ \mathfrak{b}_N(q) \end{pmatrix} + \det\begin{pmatrix} \mathfrak{b}_1(q) \\ \frac{d}{dq}\mathfrak{b}_2(q) \\ \vdots \\ \mathfrak{b}_N(q) \end{pmatrix} + \cdots + \det\begin{pmatrix} \mathfrak{b}_1(q) \\ \mathfrak{b}_2(q) \\ \vdots \\ \frac{d}{dq}\mathfrak{b}_N(q) \end{pmatrix} = \mathbf{0}.$$

Thus, $Q(q)$ is a constant function for all $q \in \mathbb{C}_p$ and we have $Q(q) = Q(0) = Q$. □

3.5 Arithmetic lower bound for $|\gamma|_p$

Our goal of this section is to deduce the arithmetic lower bound for $|\gamma|_p$. It is stated in the following

Proposition 3.2 (Arithmetic lower bound)**.** *We have the lower bound*

$$\begin{aligned}\log|\gamma|_p > -\frac{D}{e}\Bigg(\log(N!) + \frac{KN}{3}\left(\log\widetilde{B} + \log\left(\frac{T}{K(L+T')}\right) + \frac{11}{3} + \frac{107T'}{103}\right) \\ + (\omega T + \omega_0)N\left(1 + \log\left(\frac{L+T'}{T'}\right)\right) + NT' + 2p^\kappa\left(G_1 h(\alpha_1) + G_2 h(\alpha_2)\right)\Bigg)\end{aligned} \tag{3.5.1}$$

where G_1, G_2 are defined in Lemma 3.13 and ω, ω_0 are defined in (3.2.5)*.*

3.5.1 Some auxiliary results

Before giving a proof to Proposition 3.2, we shall present some technical lemmas.

Lemma 3.8. *Let K, L be integers ≥ 1 and N be in* (3.2.4)*. We have the upper bound*

$$\log\left(\prod_{l=0}^{L}\prod_{\substack{(k_0,k_1)\in\mathbb{N}^2 \\ k_0+k_1\leq K}} \frac{1}{k_0!}\right) \leq \left(\frac{11}{6\log K} - 1\right)\frac{KN\log K}{3}.$$

***Proof*.** This follows from [49, Lemma A.1 p.73–75]. The above inequality is estimated with the use of Stirling formula and the Euler-MacLaurin formula

$$\sum_{k_0=1}^{K} f(k_0) = \int_1^K f(x)dx + \frac{f(K)+f(1)}{2} + \frac{f'(K)-f'(1)}{12} + \int_1^K 2f^{(3)}(x)\sum_{n=1}^{\infty}\frac{\sin(2\pi nx)}{(2\pi n)^3}dx.$$

There were slight typos in the proof in [49] but the inequality still holds. We shall omit the proof. □

Lemma 3.9. *Let N be an integer ≥ 1, R, S, T be integers ≥ 0, $\Psi(1)$ be in (3.2.4) with $\Psi(1) \geq N$. Let $(t_1, \ldots, t_N)$ be a sequence of integers between 0 and T with each value appearing at most $(R+1)(S+1)$ times. Then we have*

$$\sum_{i=1}^{N} t_i \leq N\left(\left(1 - \frac{N}{2\Psi(1)}\right)T + \frac{3\Psi(1)}{2N}\right). \tag{3.5.2}$$

Proof. We define $a = \left[\frac{N}{(R+1)(S+1)}\right]$ and consider the scenarios $\Psi(1) > N$ and $\Psi(1) = N$ separately. For $\Psi(1) > N$,

$$\sum_{i=1}^{N} t_i \leq (R+1)(S+1)\sum_{j=0}^{a}(T-j).$$

Whereas for $\Psi(1) = N$, we have $a = \left[\frac{N}{(R+1)(S+1)}\right] = T+1$ and

$$\sum_{i=1}^{N} t_i \leq (R+1)(S+1)\sum_{j=1}^{a}((T+1)-j).$$

Both are bounded above by $NT + (R+1)(S+1)T - \frac{N^2}{2(R+1)(S+1)} + \frac{N}{2} + \frac{1}{2}(R+1)(S+1)$ and hence by $N\left(\left(1 - \frac{N}{2\Psi(1)}\right)T + \frac{3\Psi(1)}{2N}\right)$. □

Corollary 3.10. *Let N be an integer ≥ 1 and let R, S, T be integers ≥ 0. Further, let $R'+1 = \left[\frac{R}{g'}\right]$ and $S'+1 = \left[\frac{S}{g''}\right]$ be integers ≥ 0, with $g = g'g''$ where g', g'' are positive integers. Let $(R'+1)(S'+1)(T+1) \geq N$. Let $(t_1, \ldots, t_N)$ be a sequence of integers between 0 and T with each value appearing at most $(R'+1)(S'+1)$ times. Then we have*

$$\sum_{i=1}^{N} t_i \leq N(\omega T + \omega_0)$$

where ω and ω_0 are defined in (3.2.5).

Proof. It is obtained immediately from inequality (3.5.2) of Lemma 3.9 after using the trivial bounds $g'(R'+1) \leq R+g$ and $g''(S'+1) \leq S+g$. □

Lemma 3.11. *Let T and T' be two integers so that $0 < T' < T$. Let $(t_{k_0,k_1,l})$ be a sequence of N integers between 0 and T where $0 \leq k_0 + k_1 \leq K$ and $0 \leq l \leq L$. Assume that each $t_{k_0,k_1,l}$ appears at most $(R+1)(S+1)$ times, then we have*

$$\log\left(\prod_{l=0}^{L}\prod_{k_0+k_1\leq K}\left|\Delta(l;T',t_{k_0,k_1,l},k_0)\right|\right)$$
$$< \frac{KN}{3}\left(\log\left(\frac{T}{K(L+T')}\right) + \frac{11}{6} + \frac{107T'}{103}\right) + (\omega T + \omega_0)N\left(1 + \log\frac{L+T'}{T'}\right) + T'N$$

with ω and ω_0 defined in (3.2.5).

Proof. This is similar to [50, Lemma 4.5], by using Lemma 3.4, Lemma 3.8 and Corollary 3.10. The proof is presented as follows.
First, by Lemmma 3.4 and $\binom{t_{k_0,k_1,l}}{k_0} \le \frac{T^{k_0}}{k_0!}$,

$$\begin{aligned}\left|\Delta(l;T',t_{k_0,k_1,l},k_0)\right| &< e^{\frac{107T'k_0}{103}}\binom{t_{k_0,k_1,l}}{k_0}\frac{(l+T')^{t_{k_0,k_1,l}-k_0}}{T'^{t_{k_0,k_1,l}}}e^{t_{k_0,k_1,l}+T'}\\ &\le \frac{T^{k_0}}{k_0!}\frac{(L+T')^{t_{k_0,k_1,l}-k_0}}{T'^{t_{k_0,k_1,l}}}e^{t_{k_0,k_1,l}+T'+\frac{107T'k_0}{103}}.\end{aligned}$$

Next, by using Lemma 3.8, Corollary 3.10 and $\sum_{l=0}^{L}\sum_{k_0+k_1\le K}k_0=\frac{KN}{3}$,

$$\begin{aligned}&\prod_{l=0}^{L}\prod_{k_0+k_1\le K}\left|\Delta(l;T',t_{k_0,k_1,l},k_0)\right|\\ &\quad<\prod_{l=0}^{L}\prod_{k_0+k_1\le K}\frac{T^{k_0}}{k_0!}\frac{(L+T')^{t_{k_0,k_1,l}-k_0}}{T'^{t_{k_0,k_1,l}}}e^{t_{k_0,k_1,l}+T'+\frac{107T'k_0}{103}}\\ &\quad\le\left(\prod_{l=0}^{L}\prod_{k_0+k_1\le K}\frac{1}{k_0!}\right)\left(\prod_{l=0}^{L}\prod_{k_0+k_1\le K}T^{k_0}\right)\left(\prod_{l=0}^{L}\prod_{k_0+k_1\le K}\left(\frac{L+T'}{T'}\right)^{t_{k_0,k_1,l}}\right)\\ &\qquad\qquad\left(\prod_{l=0}^{L}\prod_{k_0+k_1\le K}(L+T')^{-k_0}\right)\left(\prod_{l=0}^{L}\prod_{k_0+k_1\le K}e^{t_{k_0,k_1,l}+T'+\frac{107T'k_0}{103}}\right)\\ &\quad\le e^{\left(\frac{11}{6\log K}-1\right)\frac{KN\log K}{3}}\cdot T^{\frac{KN}{3}}\cdot\left(\frac{L+T'}{T'}\right)^{N(\omega T+\omega_0)}\cdot(L+T')^{-\frac{KN}{3}}\cdot e^{N(\omega T+\omega_0+T'+\frac{107KT'}{309})}.\end{aligned}$$

Thus, the upper bound in Lemma 3.11 follows. □

Lemma 3.12. *Let K, L, R, S, T be integers ≥ 0, N and $\Psi(1)$ be in (3.2.4) with $\Psi(1)\ge N$. Let $l_\nu=\left[\frac{\nu-1}{(K+1)(K+2)/2}\right]$, $(1\le\nu\le N)$. For each sequence of integers $(r'_1,\dots,r'_N)$ between 0 and R such that none of them is repeated more than $(S+1)(T+1)$ times, we have the estimates*

$$M'_1-G'_1\le\sum_{\nu=1}^{N}l_\nu r'_\nu\le M'_1+G'_1\quad\textit{and}\quad M'_2-G'_2\le\sum_{\nu=1}^{N}l_\nu s'_\nu\le M'_2+G'_2$$

where

$$\begin{aligned}M'_1&=\frac{L(r'_1+\cdots+r'_N)}{2},\quad G'_1=\frac{N(L+1)(R+1)}{2}\left(\frac{1}{4}-\frac{N}{12\Psi(1)}\right),\\ M'_2&=\frac{L(s'_1+\cdots+s'_N)}{2},\quad G'_2=\frac{N(L+1)(S+1)}{2}\left(\frac{1}{4}-\frac{N}{12\Psi(1)}\right).\end{aligned}$$

Proof. The estimate for $\sum_{\nu=1}^{N}l_\nu r'_\nu$ is Lemma A.2 in [49]. The estimate for $\sum_{\nu=1}^{N}l_\nu s'_\nu$ can be obtained similarly. □

The following Lemma coincides with Lemma 3.12 when $g = 1$.

Lemma 3.13. *Let K, L, R, S, T be integers ≥ 0 and m_1, m_2, g, c be rational integers with m_1, m_2 and g coprime. Let $l_\nu = \left[\frac{\nu-1}{(K+1)(K+2)/2}\right]$, $(1 \leq \nu \leq N)$. Let $(r_1, s_1), \dots, (r_N, s_N)$ be sequence of N pairs of integers, which among them the same paired value appears at most $(T+1)$ times, satisfying the condition*

$$0 \leq r_\nu \leq R, \quad 0 \leq s_\nu \leq S, \quad m_1 r_\nu + m_2 s_\nu \equiv c \mod g \tag{3.5.3}$$

for all $\nu = 1, \dots, N$. Then we have the estimates

$$M_1 - G_1 \leq \sum_{\nu=1}^{N} l_\nu r_\nu \leq M_1 + G_1, \qquad M_2 - G_2 \leq \sum_{\nu=1}^{N} l_\nu s_\nu \leq M_2 + G_2 \tag{3.5.4}$$

where

$$M_1 = \frac{L(r_1 + \cdots + r_N)}{2}, \qquad G_1 = \frac{N(L+1)(R+g)g_0}{2},$$
$$M_2 = \frac{L(s_1 + \cdots + s_N)}{2}, \qquad G_2 = \frac{N(L+1)(S+g)g_0}{2}$$

and g_0 is defined in (3.2.5).

Proof. The proof follows closely the proof of [33, Lemma 10]. Here we shall show that $M_1 - G_1 \leq \sum_{\nu=1}^{N} l_\nu r_\nu \leq M_1 + G_1$. The second result $M_2 - G_2 \leq \sum_{\nu=1}^{N} l_\nu s_\nu \leq M_2 + G_2$ can be obtained similary by simply replacing r with s. Denote

$$g' = \gcd(m_2, g), \quad g'' = g/g'.$$

Since m_1, m_2 and g are coprime, we have $\gcd(m_1, g') = 1$. Denote by c' an integer between 0 and $g' - 1$ that satisfies

$$m_1 c' \equiv c \mod g'.$$

Note that such condition for c' is always valid since $\gcd(m_1, g') = 1$. Then it can be shown that the condition (3.5.3) implies

$$r_\nu = c' + g' r'_\nu, \quad 0 \leq r'_\nu \leq R' := \left[\frac{R}{g'}\right].$$

To show this, we write $r_\nu = c_{r\nu} + g' r'_v$ with $0 \leq c_{r\nu} \leq g' - 1$ and substitute into (3.5.3) to get

$$m_1(c_{r\nu} + g' r'_\nu) + m_2 s_\nu \equiv c \mod g$$

which, by writing $m_2 = g' u_2$, implies

$$m_1 c_{r\nu} + m_1 g' r'_\nu + g' u_2 s_\nu \equiv m_1 c' \mod g.$$

This gives

$$m_1(c_{r\nu} - c') + g'(m_1 r'_\nu + u_2 s_\nu) \equiv 0 \mod g.$$

Noting that $g = g'g''$ and $m_1c' \equiv c \mod g'$, the above relation can be further written as

$$m_1(c_{r\nu} - c') \equiv 0 \mod g'$$

which gives

$$c_{r\nu} \equiv c' \mod g' \qquad \text{since } \gcd(m_1, g') = 1$$

and we deduce that

$$c_{r\nu} = c'.$$

In addition, the same congruence (3.5.3) shows that for r fixed, the class of s modulo g'' is uniquely determined. To show this, we write $s_\nu = c_{s\nu} + g''s'_\nu$ with $0 \le s'_\nu \le S' := \left[\frac{S}{g''}\right]$, $0 \le c_{s\nu} \le g'' - 1$. We substitute the expression into (3.5.3) to get

$$m_1r_v + m_2(c_{s\nu} + g''s'_\nu) \equiv c \mod g$$

which, by writing $m_2 = g'u_2$ and $r_\nu = c' + g'r'_\nu$, implies

$$m_1(c' + g'r'_\nu) + g'u_2(c_{s\nu} + g''s'_v) \equiv c \mod g.$$

This gives

$$g'(m_1r'_\nu + u_2c_{s\nu}) \equiv c - m_1c' \mod g. \tag{3.5.5}$$

Therefore, when r is fixed, c' and r'_ν are fixed, so that $c_{s\nu}$ can be determined by (3.5.5). To show that $c_{s\nu}$ is uniquely determined modulo g'', suppose there exist $c_{s\nu_1}, c_{s\nu_2}$ such that

$$\begin{aligned}
g'(m_1r'_\nu + u_2c_{s\nu_1}) &\equiv c - m_1c' \mod (g'g'') \\
g'(m_1r'_\nu + u_2c_{s\nu_2}) &\equiv c - m_1c' \mod (g'g'') \\
g'(m_1r'_\nu + u_2c_{s\nu_1}) &\equiv g'(m_1r'_\nu + u_2c_{s\nu_2}) \mod (g'g'') \\
m_1r'_\nu + u_2c_{s\nu_1} &\equiv m_1r'_\nu + u_2c_{s\nu_2} \mod g'' \\
u_2c_{s\nu_1} &\equiv u_2c_{s\nu_2} \mod g'' \\
c_{s\nu_1} &\equiv c_{s\nu_2} \mod g'' \qquad \text{since } \gcd(u_2, g'') = 1
\end{aligned}$$

Thus, the class of s modulo g'' is uniquely determined. This means that while r is fixed, there are at most $\left(\left[\frac{S}{g''}\right] + 1\right)(T + 1)$ pairs of integers (r, s) satisfying condition (3.5.3), i.e.

$$0 \le r_\nu \le R, \quad 0 \le s_\nu \le S, \quad m_1r_\nu + m_2s_\nu \equiv c \mod g.$$

By applying Lemma 3.12 to the above sequence of integers $(r'_1, \dots, r'_N)$ gives

$$M'_1 - G'_1 \le \sum_{\nu=1}^{N} l_\nu r'_\nu \le M'_1 + G'_1$$

where $\quad M_1' = \frac{L(r_1'+\cdots+r_N')}{2}, \quad G_1' = \frac{N(L+1)(R'+1)}{2}\left(\frac{1}{4} - \frac{N}{12(R'+1)(S'+1)(T+1)}\right).$
Recall that $r_\nu = c' + g' r_\nu'$ and $l_\nu = \left[\frac{\nu-1}{(K+1)(K+2)/2}\right]$ for $1 \le \nu \le N$. We obtain $\sum_{\nu=1}^N l_\nu = \frac{NL}{2}$ and thus

$$M_1' g' + c' \sum_{\nu=1}^N l_\nu - g' G_1' \le \sum_{\nu=1}^N l_\nu (c' + g' r_\nu') \le M_1' g' + c' \sum_{\nu=1}^N l_\nu + g' G_1'$$
$$M_1 - g' G_1' \le \sum_{\nu=1}^N l_\nu r_\nu \le M_1 + g' G_1'.$$

Trivially, we have the upper bound $R' + 1 = \left[\frac{R}{g'}\right] + 1 \le \frac{R+g'}{g'}$ (i.e. $(R'+1)g' \le R + g' \le R + g$) and $g''(S'+1) \le S + g$. Therefore,

$$g' G_1' = \frac{N(L+1)(R'+1)g'}{8} - \frac{N^2(L+1)g'}{24(S'+1)(T+1)} \le \frac{N(L+1)(R+g)}{8} - \frac{N^2(L+1)g}{24(S+g)(T+1)} \le G_1.$$

The proof is completed. □

3.5.2 Deduction of Proposition 3.2

We shall prove Proposition 3.2. It is based on the following p-adic analogue of Liouville inequality which is also used in [33].

Lemma 3.14 (p-adic analogue of Liouville inequality)**.** *For any polynomial $P(X,Y)$, with integer coefficients and all algebraic numbers ξ and ζ contained in $\overline{\mathbb{Q}}_p$ such that $P(\xi,\zeta) \ne 0$, we have the lower bound*

$$\log|P(\xi,\zeta)|_p \ge -\frac{[\mathbb{Q}(\xi,\zeta):\mathbb{Q}]}{ef}\left(\log|P| + (\deg_X P)h(\xi) + (\deg_Y P)h(\zeta)\right),$$

where e and f denote as before the ramification index and the residue degree of the extension of $\mathbb{Q}_p(\xi,\zeta)$ over $\mathbb{Q}_p$, and where

$$|P| = \max\{|P(x,y)|; x \in \mathbb{C}, y \in \mathbb{C}, |x| = |y| = 1\} \tag{3.5.6}$$

denotes the maximum norm of the polynomial P.

Proof. See Yu [97, Lemma 2.1]. □

Proof of Proposition 3.2. By referring to $P(X,Y)$ in (3.4.9), γ in (3.4.8) and Lemma 3.7, we notice that $\gamma = P\left(\alpha_1^{p^\kappa}, \alpha_2^{p^\kappa}\right)$, which can be expressed as

$$\gamma = \sum_\sigma \mathrm{sgn}(\sigma) \prod_{i=1}^N \frac{(b_2 r_{\sigma(i)} + b_1 s_{\sigma(i)} - q)^{k_{1,i}}}{k_{1,i}!} \Delta(l_i; T', t_{\sigma(i)}, k_{0,i}) \cdot \alpha_1^{p^\kappa \sum_{i=1}^N l_i r_{\sigma(i)}} \alpha_2^{p^\kappa \sum_{i=1}^N l_i s_{\sigma(i)}} \tag{3.5.7}$$

for any $q \in \mathbb{C}_p$, where σ runs over all permutations $\sigma \in \mathfrak{S}_N$ and where $\operatorname{sgn}(n)$ is the signature of the permutation σ. We choose $q = \frac{Rb_2+Sb_1}{2}$. Then using (3.5.6), Lemma 3.8, Lemma 3.9 and Lemma 3.11 we deduce that

$$\begin{aligned}|P| &\le \sum_{\sigma}\left|\prod_{i=1}^{N}\frac{(b_2 r_{\sigma(i)}+b_1 s_{\sigma(i)}-q)^{k_{1,i}}}{k_{1,i}!}\Delta(l_i;T',t_{\sigma(i)},k_{0,i})\right| \\ &\le N!\max_{\sigma}\left|\prod_{i=1}^{N}\frac{(b_2 r_{\sigma(i)}+b_1 s_{\sigma(i)}-q)^{k_{1,i}}}{k_{1,i}!}\right|\max_{\sigma}\left|\prod_{i=1}^{N}\Delta(l_i;T',t_{\sigma(i)},k_{0,i})\right| \\ &< N!\widetilde{B}^{\frac{KN}{3}}\left(\frac{T}{K(L+T')}\right)^{\frac{KN}{3}}\left(\frac{L+T'}{T'}\right)^{(\omega T+\omega_0)N}\exp\left(\frac{11KN}{9}+\frac{107KNT'}{309}+(\omega T+\omega_0+T')N\right).\end{aligned} \tag{3.5.8}$$

It should be noted that, due to the definition of g in (3.2.1), the integers m_1, m_2 and g are coprime. We use (3.5.4) from Lemma 3.13 to estimate $\sum_{i=1}^{N} l_i r_{\sigma(i)}$ and $\sum_{i=1}^{N} l_i s_{\sigma(i)}$ in (3.5.7). Denote by V_1 (resp. V_2) the integral part of M_1+G_1 (resp. M_2+G_2), and by U_1 (resp. U_2) the smallest integer $\ge M_1-G_1$ (resp. M_2-G_2). Then

$$\gamma = P\left(\alpha_1^{p^\kappa},\alpha_2^{p^\kappa}\right) = \alpha_1^{p^\kappa V_1}\alpha_2^{p^\kappa V_2}\widetilde{P}\left(\frac{1}{\alpha_1^{p^\kappa}},\frac{1}{\alpha_2^{p^\kappa}}\right),$$

where $\widetilde{P}(X,Y)$ is a polynomial with integer coefficients, the norm $\left|\widetilde{P}\right| = \max\{\left|\widetilde{P}(x,y)\right|; x\in\mathbb{C}, y\in\mathbb{C}, |x|=|y|=1\}$ is equal to $|P|$, Also, the degree of X and Y for $\widetilde{P}(X,Y)$ are bounded respectively by V_1-U_1 and V_2-U_2.

Now we apply the version of Liouville inequality in Lemma 3.14 to the polynomial $\widetilde{P}$, knowing that $h(\alpha_i^{p^\kappa}) = p^\kappa h(\alpha_i)$ and note that $D = \frac{[\mathbb{Q}(\alpha_1,\alpha_2):\mathbb{Q}]}{f}$, to give the lower bound

$$\begin{aligned}\log\left|\widetilde{P}\left(\alpha_1^{p^\kappa},\alpha_2^{p^\kappa}\right)\right|_p &\ge -\frac{D}{e}\left(\log\left|\widetilde{P}\right| + (\deg_X\widetilde{P})h(\alpha_1^{p^\kappa}) + (\deg_Y\widetilde{P})h(\alpha_2^{p^\kappa})\right) \\ &\ge -\frac{D}{e}\left(\log\left|\widetilde{P}\right| + p^\kappa(V_1-U_1)h(\alpha_1) + p^\kappa(V_2-U_2)h(\alpha_2)\right).\end{aligned}$$

Note that $\left|\widetilde{P}\right| = |P|$, $|\alpha_1|_p = |\alpha_2|_p = 1$ and $V_i - U_i \le 2G_i$ for $i = 1,2$. Thus,

$$\begin{aligned}\log|\gamma|_p &= \log\left|\widetilde{P}\left(\alpha_1^{p^\kappa},\alpha_2^{p^\kappa}\right)\right|_p \\ &\ge -\frac{D}{e}\left(\log|\widetilde{P}| + p^\kappa(V_1-U_1)h(\alpha_1) + p^\kappa(V_2-U_2)h(\alpha_2)\right) \\ &\ge -\frac{D}{e}\left(\log|\widetilde{P}| + 2p^\kappa\left(G_1h(\alpha_1)+G_2h(\alpha_2)\right)\right).\end{aligned}$$

The lower bound in (3.5.1) can be obtained after using the upper bound of $|P|$ in (3.5.8). □

3.6 Analytic upper bound for $|\gamma|_p$

The goal of this section is to deduce the analytic upper bound for $|\gamma|_p$, which is stated in

Proposition 3.3 (Analytic upper bound)**.** *Suppose that*

$$|\Lambda|_p \leq p^{-(V+u)}, \tag{3.6.1}$$

where $V > \frac{1}{p-1}$ *is defined in* (3.2.7)*. Then*

$$\log|\gamma|_p < N\left(T\lambda - \frac{V}{2} + \frac{K}{3}\left(\lambda + \frac{1}{p-1}\right)\right)\log p. \tag{3.6.2}$$

3.6.1 Some auxiliary results

We first present some technical lemmas and the p-adic Schwarz's lemma.

Lemma 3.15. *Let n be a positive integer. Then* $v_p(n!) < \dfrac{n}{p-1}$.

Proof. See for example Neukirch [68], p.138–139. □

Lemma 3.16. *Let θ be an element of $\overline{\mathbb{Q}}_p$ such that* $v_p(\theta - 1) > 0$*. Then*

$$v_p(\theta^p - 1) = \begin{cases} p\, v_p(\theta - 1), & \text{if } v_p(\theta-1) < \dfrac{1}{p-1}, \\ v_p(\theta-1) + 1, & \text{if } v_p(\theta-1) > \dfrac{1}{p-1} \text{ and} \end{cases}$$

$$v_p(\theta^p - 1) \geq \frac{p}{p-1} = \frac{1}{p-1} + 1, \quad \text{if } v_p(\theta-1) = \frac{1}{p-1}.$$

Proof. It has been used for example in the papers of Yu ([97]–[103]). We omit the proof here. □

Lemma 3.17. *Suppose $\theta \in K_v$ satisfying $v_p(\theta - 1) > 0$ and let $\kappa \geq 0$ be the integer satisfying the inequalities* (3.2.3)*, i.e.*

$$p^{\kappa-1} \leq \frac{2e}{p-1} < p^{\kappa}.$$

Then

$$v_p(\theta^{p^\kappa} - 1) \geq \frac{p^\kappa}{2e} + \frac{1}{p-1} > \frac{1}{p-1}. \tag{3.6.3}$$

Proof. The proof follows similar line as in Yu [99, Lemma 1.1]. We omit the details here. □

Lemma 3.18. *Let u be a positive integer. For any root of unity ξ of order p^u, the ramification index of the extension $\mathbb{Q}_p(\xi)/\mathbb{Q}_p$ is equal to $p^{u-1}(p-1)$. Furthermore, for any positive integer m not divisible by p, we have*

$$\sum_{\substack{\xi^{mp^u}=1\\ \xi\neq 1}} v_p(\xi-1)=u.$$

Proof. This is rephrased from [33, Lemma 5, p.319]. □

Lemma 3.19 (Krasner's Lemma)**.** *Let ξ and σ be in an algebraic closure of $\mathbb{Q}_p$. Let $\xi_1=\xi$, $\xi_2,\dots,\xi_d$ denote the Galois conjugates of ξ over $\mathbb{Q}_p$. If*

$$v_p(\sigma-\xi)>v_p(\sigma-\xi_i),\qquad i=2,\dots,d,$$

then ξ belongs to the field $\mathbb{Q}_p(\sigma)$.

Proof. See for example [73, p.130]. □

Before stating the p-adic Schwarz's lemma, we introduce some notations. Let K be a complete ultrametric valuation field, of characteristic 0 with residual characteristic p. Let $f=\sum_{n\geq 0}a_nX^n$ be a formal power series with coefficients in K such that there exists a real number $R>0$ satisfying $\lim_{n\to+\infty}|a_n|_pR^n=0$. Then, f defines an analytic function on the disc $\{z\in \mathrm{K}, |z|_p\leq R\}$. For any real number r such that $0\leq r\leq R$, we put $|f|_r=\sup_{n\geq 0}|a_n|_pr^n$. We have

$$|f|_r\leq |f|_R. \tag{3.6.4}$$

In particular, if K is algebraically closed, then $|f|_r=\sup_{|z|_p\leq r}|f(z)|_p$ and inequality (3.6.4) expresses the maximum principle.

Lemma 3.20 (p-Adic Schwarz's Lemma)**.** *Let p be a prime number. Let T_I be a nonnegative integer, r and R be real numbers satisfying $0<r\leq R$ and f be an analytic function on the disc $\{z\in\mathbb{C}_p : |z|_p\leq R\}$. Assume f has a zero of multiplicity at least T_I at 0. Then*

$$|f|_r\leq\left(\frac{R}{r}\right)^{-T_I}|f|_R.$$

Proof. We consider the function $z\mapsto g(z)=z^{-T_I}f(z)$ which is analytic in the disc $\{z\in\mathbb{C}_p : |z|_p\leq R\}$. Since $r\leq R$, we have $|g|_r\leq|g|_R$ with

$$|g|_r=r^{-T_I}|f|_r\qquad\text{and}\qquad |g|_R=R^{-T_I}|f|_R.$$

This completes the proof.
Remark: See also Bertrand [22] and Mahler [60]. □

3.6.2 Deduction of Proposition 3.3

In this section we deduce the analytic upper bound for $|\gamma|_p$ in Proposition 3.3. Our derivation follows first the similar line of [33] and then [50] with the development by the p-adic Schwarz's lemma. It is established based on several results which can be best presented by the following lemmas subsequently. We assumed (3.6.1) holds in this section.

Lemma 3.21. *Recall θ_1 and θ_2 as in* (3.2.2). *Let*

$$\gamma' = \det\left(\frac{(b_2 r_j + b_1 s_j - q)^{k_{1,i}}}{k_{1,i}!}\Delta(l_i; T', t_j, k_{0,i})\theta_1^{p^\kappa l_i r_j}\theta_2^{p^\kappa l_i s_j}\right)_{1\le i,j\le N} \tag{3.6.5}$$

where q is any number in $\mathbb{C}_p$ and set

$$\widetilde{\Lambda} = \theta_1^{b_1} - \theta_2^{b_2}.$$

Then we have $v_p(\gamma) = v_p(\gamma')$ and $v_p(\Lambda) = v_p(\widetilde{\Lambda})$.

Proof. We consider the determinant γ stated in (3.4.8) and refer to $P(X,Y)$ in (3.4.9). Recall that $\gamma = P\left(\alpha_1^{p^\kappa}, \alpha_2^{p^\kappa}\right)$. By referring to $P(X,Y)$ in (3.4.10), we get

$$\gamma = \det\left(\frac{(b_2 r_j + b_1 s_j - q)^{k_{1,i}}}{k_{1,i}!}\Delta(l_i; T', t_j, k_{0,i})\alpha_1^{p^\kappa l_i r_j}\alpha_2^{p^\kappa l_i s_j}\right)_{1\le i,j\le N}.$$

Since $m_1 r_j + m_2 s_j \equiv c \bmod g \quad (j = 1, \dots, N)$, by rewriting α_1, α_2 as in (3.2.2), we obtain

$$\gamma = \zeta^{cp^\kappa(\sum l_i)}\gamma'.$$

Therefore, $v_p(\gamma) = v_p(\gamma')$ follows because $v_p(\zeta) = 0$. Next, according to the assumption (3.6.1), since

$$\Lambda = \alpha_1^{b_1} - \alpha_2^{b_2} = \zeta^{m_1 b_1}\theta_1^{b_1} - \zeta^{m_2 b_2}\theta_2^{b_2}$$

has positive valuation, $m_1 b_1$ and $m_2 b_2$ are necessarily in the same class modulo g. Thus, it follows that $v_p(\Lambda) = v_p(\widetilde{\Lambda})$. □

Lemma 3.21 reveals that it suffices to verify Proposition 3.3 with $\alpha_1 = \theta_1$ $\alpha_2 = \theta_2$ being principal units. Next, we recall that u denotes the integer such that p^u divides exactly $\gcd(b_1, b_2)$. In case that $u > 0$, we set

$$b_1' = \frac{b_1}{p^u}, \qquad b_2' = \frac{b_2}{p^u}, \qquad \beta = \frac{b_1}{b_2} = \frac{b_1'}{b_2'}, \qquad \sigma = \frac{\theta_1^{b_1'}}{\theta_2^{b_2'}} \tag{3.6.6}$$

and we can assume without restriction that p does not divide b_2'. Let $\xi_1, \dots, \xi_{p^u}$ be all the p^u-th roots of unity in $\overline{\mathbb{Q}}_p$ with the ordering

$$v_p(\sigma - \xi_1) \ge \cdots \ge v_p(\sigma - \xi_{p^u}). \tag{3.6.7}$$

Let

$$\Lambda' = \theta_1^{b_1'} - \xi_1 \theta_1^{b_2'}. \tag{3.6.8}$$

Lemma 3.22. *Suppose that (3.6.1) holds. Then we have $\xi_1^{p^\kappa} = 1$ and the lower bound*

$$v_p(\Lambda') = v_p(\Lambda) - u \geq V. \tag{3.6.9}$$

***Proof*.** We follow the line of [33] to achieve this. Note by using Lemma 3.21 and the hypothesis that

$$v_p(\sigma^{p^u} - 1) = v_p\left(\frac{\theta_1^{b_1'p^u} - \theta_2^{b_2'p^u}}{\theta_2^{b_2'p^u}}\right) = v_p\left(\frac{\widetilde{\Lambda}}{\theta_2^{b_2}}\right) = v_p\left(\widetilde{\Lambda}\right) + v_p\left(\theta_2^{-b_2}\right) = v_p(\Lambda) \geq V + u > \frac{1}{p-1} + u.$$

In other words, we have

$$\sum_{v=1}^{p^u} v_p(\sigma - \xi_v) = v_p(\Lambda) \geq V + u > \frac{1}{p-1} + u, \tag{3.6.10}$$

where the summation involves all the p^u-th roots of unity ξ_v $(v = 1, \dots, p^u)$ in $\overline{\mathbb{Q}}_p$. With the ordering of these roots as in (3.6.7), we shall show that in fact $v_p(\sigma - \xi_1) > v_p(\sigma - \xi_2)$. By the ultrametric inequality,

$$v_p\left(\frac{\xi_v}{\xi_1} - 1\right) = v_p(\xi_v - \xi_1) \geq \min\{v_p(\sigma - \xi_v), v_p(\sigma - \xi_1)\} = v_p(\sigma - \xi_v) \qquad (v = 2, \dots, p^u). \tag{3.6.11}$$

Next, we consider $\sum_{\substack{\xi^{p^u}=1\\ \xi\neq 1}} v_p(\xi - 1)$, where each of the ξ in the summation represents $\xi = \frac{\xi_v}{\xi_1}$ $(v = 2, 3, \dots, p^u)$, so that $\xi \neq 1$ and $\xi^{p^u} = 1$. Besides, for each of these valuations $v_p(\xi - 1)$, we have $v_p(\xi - 1) = v_p\left(\frac{\xi_v}{\xi_1} - 1\right) \geq v_p(\sigma - \xi_v)$ from (3.6.11). Therefore, using (3.6.10),

$$v_p(\sigma - \xi_1) + \sum_{\substack{\xi^{p^u}=1\\ \xi\neq 1}} v_p(\xi - 1) \geq v_p(\sigma - \xi_1) + \sum_{v=2}^{p^u} v_p(\sigma - \xi_v) = v_p\left(\sigma^{p^u} - 1\right) \geq V + u > \frac{1}{p-1} + u.$$

According to Lemma 3.18, $\sum_{\substack{\xi^{p^u}=1\\ \xi\neq 1}} v_p(\xi - 1) = u$, yielding $v_p(\sigma - \xi_1) > \frac{1}{p-1}$. We claim that this implies $v_p(\sigma - \xi_1) > v_p(\sigma - \xi_2)$. Indeed, if $v_p(\sigma - \xi_1) = v_p(\sigma - \xi_2)$, then with the ultrametric inequality,

$$\frac{1}{p^{w-1}(p-1)} = v_p\left(\frac{\xi_2}{\xi_1} - 1\right) = v_p(\xi_2 - \xi_1) \geq v_p(\sigma - \xi_2) > \frac{1}{p-1},$$

where p^w denotes the exact order of the root of unity $\frac{\xi_2}{\xi_1} \neq 1$. Hence there is a contradiction. Krasner's Lemma 3.19 then shows that ξ_1 belongs to the field $\mathbb{Q}_p(\sigma) \subseteq \mathrm{K}_v$. If we denote by p^w the order of the root of unity ξ_1, then the ramification index of the extension $\mathbb{Q}_p(\xi_1)/\mathbb{Q}_p$ equals

$p^{w-1}(p-1)$ by Lemma 3.18. It follows from $\mathbb{Q}_p(\sigma) \subseteq \mathrm{K}_v$ that $p^{w-1}(p-1) \leq e$. Together with (3.2.3) we have

$$p^{w-1}(p-1) \leq e < \frac{1}{2}p^{\kappa}(p-1).$$

It follows that $w \leq \kappa$, and

$$\xi_1^{p^{\kappa}} = 1.$$

To prove (3.6.9), since $\xi_1^{p^u} = 1$, Lemma 3.16 and Lemma 3.21 then shows that

$$v_p(\Lambda) = v_p(\widetilde{\Lambda}) = v_p(\sigma^{p^u} - 1) = v_p\left(\left(\frac{\sigma}{\xi_1}\right)^{p^u} - 1\right) = v_p(\sigma - \xi_1) + u = v_p(\Lambda') + u.$$

Alternatively, it is noted that the inequality $v_p(\Lambda) = v_p(\Lambda') + u$ results also directly from the ultrametric inequality above. By (3.6.1), the lower bound (3.6.9) follows. □

Now we introduce the function $\Phi_I(z)$ for $z \in \mathbb{C}_p$, represented in the form of a determinant with (i,j) indicating the i-th row and j-column respectively, satisfying

$$|z|_p \leq p^{\lambda} \tag{3.6.12}$$

where λ is in (3.2.9). Let $I \subseteq \{1, \dots, N\}$ be any set, $\sigma_{i,j} \in \overline{\mathbb{Q}}_p$ with $|\sigma_{i,j}|_p \leq 1$. We define

$$\Phi_I(z) := \pm \det \begin{pmatrix} \Phi_I^+(z) \\ \Phi_I^-(z) \end{pmatrix} \tag{3.6.13}$$

where

$$\Phi_I^+(z) = (C_{i,j}(z)) \text{ for } i \in I, \qquad \Phi_I^-(z) = (\sigma_{i,j} C_{i,j}(z)) \text{ for } i \notin I$$

with

$$C_{i,j}(z) = \frac{(z(r_j + s_j\beta))^{k_{1,i}}}{k_{1,i}!} \Delta(l_i; T', t_j, k_{0,i}) \theta_1{}^{p^{\kappa} l_i z (r_j + s_j \beta)} \tag{3.6.14}$$

and ± 1 is chosen for the determinant depending on the positioning of the rows. (Lemma 3.24 and (3.6.23) reveal another representation for $\Phi_I(z)$.)

The following lemma (Lemma 3.23) provides a lower bound for $v_p(\Phi_I(z))$.

Lemma 3.23. *For any set $I \subseteq \{1, \dots, N\}$ and for any $z \in \mathbb{C}_p$ so that $|z|_p \leq p^{\lambda}$,*

$$v_p(\Phi_I(z)) > -\frac{KN}{3}\left(\lambda + \frac{1}{p-1}\right).$$

Proof. We develop the determinant $\Phi_I(z)$ in (3.6.13) to get

$$\Phi_I(z) = \sum_{\sigma\in\mathfrak{S}_N} \operatorname{sgn}(\sigma){\theta_1}^{p^\kappa z\sum_{i=1}^N l_i\xi_{1,\sigma(i)}} \prod_{i=1}^N \left(\frac{(z\xi_{1,\sigma(i)})^{k_{1,i}}}{k_{1,i}!}\Delta(l_i;T',t_{\sigma(i)},k_{0,i})\right)\prod_{i\notin I}\sigma_{i,\sigma(i)}.$$

Moreover, $|\sigma_{i,j}|_p \le 1$ as adopted in $\Phi_I(z)$. Thus,

$$\begin{aligned}
&v_p(\Phi_I(z))\\
&\ge \min_{\sigma\in\mathfrak{S}_N}\left\{v_p\left({\theta_1}^{p^\kappa z\sum_{i=1}^N l_i\xi_{1,\sigma(i)}}\prod_{i=1}^N\left(\frac{(z\xi_{1,\sigma(i)})^{k_{1,i}}}{k_{1,i}!}\Delta(l_i;T',t_{\sigma(i)},k_{0,i})\right)\prod_{i\notin I}\sigma_{i,\sigma(i)}\right)\right\}\\
&= \min_{\sigma\in\mathfrak{S}_N}\left\{\underbrace{v_p\left({\theta_1}^{p^\kappa z\sum_{i=1}^N l_i\xi_{1,\sigma(i)}}\right)}_{\text{(i)}} + \underbrace{v_p\left(\prod_{i=1}^N\frac{(z\xi_{1,\sigma(i)})^{k_{1,i}}}{k_{1,i}!}\right)}_{\text{(ii)}} + \underbrace{v_p\left(\prod_{i=1}^N\Delta(l_i;T',t_{\sigma(i)},k_{0,i})\right)}_{\text{(iii)}} + \sum_{i\notin I}\underbrace{v_p\left(\sigma_{i,\sigma(i)}\right)}_{\ge 0}\right\}.
\end{aligned}$$

(i) To determine $v_p\left({\theta_1}^{p^\kappa z\sum_{i=1}^N l_i\xi_{1,\sigma(i)}}\right)$.

We shall have similar argument as Proposition 3.1 in Section 3.3.1 to ${\theta_1}^{p^\kappa z\sum_{i=1}^N l_i\xi_{1,\sigma(i)}}$. First consider

$$\exp\left(\left(z\sum_{i=1}^N l_i\xi_{1,\sigma(i)}\right)\log_p\left(1+\left({\theta_1}^{p^\kappa}-1\right)\right)\right). \tag{3.6.15}$$

(Note: $\log_p$ denotes the p-adic logarithms.) We shall show that

$$\left|\left(z\sum_{i=1}^N l_i\xi_{1,\sigma(i)}\right)\log_p\left(1+\left({\theta_1}^{p^\kappa}-1\right)\right)\right|_p < p^{-\frac{1}{p-1}}. \tag{3.6.16}$$

By Lemma 3.17, we have inequalities (3.6.3), i.e. $v_p(\theta_1^{p^\kappa}-1)\ge\frac{p^\kappa}{2e}+\frac{1}{p-1}>\frac{1}{p-1}$. Therefore, $\log_p\left(1+\left({\theta_1}^{p^\kappa}-1\right)\right)$ converges and

$$\left|\log_p\left(1+\left({\theta_1}^{p^\kappa}-1\right)\right)\right|_p = \left|{\theta_1}^{p^\kappa}-1\right|_p \le p^{-\left(\frac{p^\kappa}{2e}+\frac{1}{p-1}\right)} < p^{-\frac{1}{p-1}}.$$

Besides, since $l_i, r_{\sigma(i)}, s_{\sigma(i)}\in\mathbb{Z}\subset\mathbb{Z}_p$, $|\beta|_p = \left|\frac{b_1'}{b_2'}\right|_p \le 1$, so that $\xi_{1,\sigma(i)} = r_{\sigma(i)}+s_{\sigma(i)}\beta\in\mathbb{Z}_p$ and hence $\sum_{i=1}^N l_i\xi_{1,\sigma(i)}\in\mathbb{Z}_p$. Therefore, $\left|\sum_{i=1}^N l_i\xi_{1,\sigma(i)}\right|_p\le 1$.

Further, for $z\in\mathbb{C}_p$ such that $|z|_p\le p^\lambda$,

$$\left|z\sum_{i=1}^N l_i\xi_{1,\sigma(i)}\right|_p = |z|_p\left|\sum_{i=1}^N l_i\xi_{1,\sigma(i)}\right|_p < p^{\frac{p^\kappa}{2e}}.$$

Therefore,

$$\left|\left(z\sum_{i=1}^{N} l_i\xi_{1,\sigma(i)}\right)\log_p\left(1+\left({\theta_1}^{p^\kappa}-1\right)\right)\right|_p < p^{\frac{p^\kappa}{2e}}p^{-\left(\frac{p^\kappa}{2e}+\frac{1}{p-1}\right)} = p^{-\frac{1}{p-1}}.$$

Therefore, $\exp\left(\left(z\sum_{i=1}^{N} l_i\xi_{1,\sigma(i)}\right)\log_p\left(1+\left({\theta_1}^{p^\kappa}-1\right)\right)\right)$ converges and

$$\left|\exp\left(\left(z\sum_{i=1}^{N} l_i\xi_{1,\sigma(i)}\right)\log_p\left(1+\left({\theta_1}^{p^\kappa}-1\right)\right)\right)\right|_p = 1 \tag{3.6.17}$$

by Proposition 3.1. We have

$$\begin{aligned}{\theta_1}^{p^\kappa z\sum_{i=1}^{N} l_i\xi_{1,\sigma(i)}} &= \left(1+\left({\theta_1}^{p^\kappa}-1\right)\right)^{z\sum_{i=1}^{N} l_i\xi_{1,\sigma(i)}}\\ &= \exp\left(\left(z\sum_{i=1}^{N} l_i\xi_{1,\sigma(i)}\right)\log_p\left(1+\left({\theta_1}^{p^\kappa}-1\right)\right)\right)\end{aligned}$$

and thus

$$\left|{\theta_1}^{p^\kappa z\sum_{i=1}^{N} l_i\xi_{1,\sigma(i)}}\right|_p = 1.$$

Equivalently,

$$v_p\left({\theta_1}^{p^\kappa z\sum_{i=1}^{N} l_i\xi_{1,\sigma(i)}}\right) = 0. \tag{3.6.18}$$

(ii) To determine $v_p\left(\prod_{i=1}^{N}\dfrac{(z\xi_{1,\sigma(i)})^{k_{1,i}}}{k_{1,i}!}\right)$.

Since $\xi_{1,j} = r_j + s_j\beta$, so that $v_p(\xi_{1,\sigma(i)}) \geq 0$.

$$v_p\left(\prod_{i=1}^{N}\frac{(z\xi_{1,\sigma(i)})^{k_{1,i}}}{k_{1,i}!}\right) = -v_p\left(\prod_{i=1}^{N}k_{1,i}!\right)+\sum_{i=1}^{N}k_{1,i}\,v_p\left(z\xi_{1,\sigma(i)}\right) \geq -v_p\left(\prod_{i=1}^{N}k_{1,i}!\right)+\frac{KN}{3}v_p(z),$$

where, using Lemma 3.15,

$$\begin{aligned}v_p\left(\prod_{i=1}^{N}k_{1,i}!\right) &= (L+1)v_p\left(\prod_{k_0+k_1\leq K}k_{1,i}!\right) = (L+1)\sum_{n=2}^{K}(K+1-n)v_p(n!)\\ &< (L+1)\sum_{n=2}^{K}(K+1-n)\frac{n}{p-1} = \frac{L+1}{p-1}\cdot\frac{K}{6}(K+4)(K-1)\\ &< \frac{KN}{3(p-1)}.\end{aligned}$$

Therefore with $|z|_p \leq p^\lambda$ we have

$$v_p\left(\prod_{i=1}^{N}\frac{(z\xi_{1,\sigma(i)})^{k_{1,i}}}{k_{1,i}!}\right) > -\frac{KN}{3}\left(\lambda+\frac{1}{p-1}\right). \tag{3.6.19}$$

(iii) To determine $v_p\left(\prod_{i=1}^N \Delta(l_i;T',t_{\sigma(i)},k_{0,i})\right)$.

By Lemma 3.3,

$$v_p\left(\prod_{i=1}^N \Delta(l_i;T',t_{\sigma(i)},k_{0,i})\right) = \sum_{i=1}^N v_p\left(\Delta(l_i;T',t_{\sigma(i)},k_{0,i})\right) \geq 0. \tag{3.6.20}$$

Summing (3.6.18), (3.6.19) and (3.6.20), we obtain the result in Lemma 3.23. □

Next we wish to obtain a lemma (Lemma 3.25) which concerns the multiplicity of zeros for $\Phi_I(z)$. Before achieving this, we start with rewriting $\Phi_I(z)$. The following lemma concerns $C_{i,j}(z)$ in (3.6.14).

Lemma 3.24. *For all $1 \leq j \leq N$ and $i \in I$, we have*

$$C_{i,j}(z) = \sum_{\nu=0}^{T} q_{\nu,t_j}\left(\frac{\partial}{\partial z_0}\right)^{\nu_j} \varphi_i(z\underline{\xi_j}) \tag{3.6.21}$$

where q_{ν,t_j} is in Lemma 3.6, $\left(\frac{\partial}{\partial z_0}\right)^{\nu_j} \varphi_i(z\underline{\xi_j})$ represents $\left(\frac{\partial}{\partial z_0}\right)^{\nu_j} \varphi_i(z_0,z_1)\big|_{(z_0,z_1)=(z\underline{\xi_j})}$, with

$$\varphi_i(z_0,z_1) = \frac{z_1^{k_{1,i}}}{k_{1,i}!}\frac{\nu(T')^{k_{0,i}}}{k_{0,i}!} z_0^{k_{0,i}} e^{z_0 l_i}\theta_1^{p^\kappa l_i z_1}, \qquad \underline{\xi_j} = (\xi_{0,j},\xi_{1,j}) = (0, r_j + s_j\beta). \tag{3.6.22}$$

Proof. This lemma can be deduced from Lemma 3.6. Indeed, if $\nu_j \geq k_{0,i}$,

$$\left(\frac{\partial}{\partial z_0}\right)^{\nu_j} z_0^{k_{0,i}} e^{z_0 l_i} = \sum_{\substack{x=0\\x\neq k_{0,i}}}^{\nu_j} \binom{\nu_j}{x}\frac{k_{0,i}!}{(k_{0,i}-x)!} z_0^{k_{0,i}-x} l_i^{\nu_j-k_{0,i}} e^{z_0 l_i} + \binom{\nu_j}{k_{0,i}} k_{0,i}!\, l_i^{\nu_j-k_{0,i}} e^{z_0 l_i}$$

so that

$$\sum_{\nu=0}^{T} q_{\nu,t_j}\left(\frac{\partial}{\partial z_0}\right)^{\nu_j} \varphi_i(z\underline{\xi_j}) = \frac{(z\xi_{1,j})^{k_{1,i}}}{k_{1,i}!}\nu(T')^{k_{0,i}}\theta_1^{p^\kappa l_i z\xi_{1,j}} \sum_{\nu=0}^{T} q_{\nu,t_j}\binom{\nu_j}{k_{0,i}} l_i^{\nu_j-k_{0,i}} = C_{i,j}(z).$$

Whereas if $\nu_j < k_{0,i}$, $\binom{\nu_j}{k_{0,i}} = 0$, and

$$\left(\frac{\partial}{\partial z_0}\right)^{\nu_j} z_0^{k_{0,i}} e^{z_0 l_i} = \sum_{x=0}^{\nu_j} \binom{\nu_j}{x}\frac{k_{0,i}!}{(k_{0,i}-x)!} z_0^{k_{0,i}-x} l_i^{\nu_j-k_{0,i}} e^{z_0 l_i}$$

thus $\sum_{\nu=0}^{T} q_{\nu,t_j}\left(\frac{\partial}{\partial z_0}\right)^{\nu_j} \varphi_i(z\underline{\xi_j}) = 0 = C_{i,j}(z)$ by Lemma 3.6. □

We can develop the determinant $\Phi_I(z)$ in (3.6.13) to yield

$$\Phi_I(z) = \sum_{\substack{(\nu_1,\ldots,\nu_N)\in\mathbb{N}^N \\ \nu_j\le T, 1\le j\le N}} \prod_{j=1}^{N} q_{\nu_j,t_j} \Phi_{I,\underline{\nu}}(z) \tag{3.6.23}$$

where

$$\Phi_{I,\underline{\nu}}(z) = \pm \det \begin{pmatrix} \Phi^+_{I,\underline{\nu}}(z) \\ \Phi^-_{I,\underline{\nu}}(z) \end{pmatrix}$$

with

$$\Phi^+_{I,\underline{\nu}}(z) = \left(\left(\frac{\partial}{\partial z_0}\right)^{\nu_j} \varphi_i(z\underline{\xi_j})\right) \text{ for } i \in I, \qquad \Phi^-_{I,\underline{\nu}}(z) = \left(\sigma_{i,j}\left(\frac{\partial}{\partial z_0}\right)^{\nu_j} \varphi_i(z\underline{\xi_j})\right) \text{ for } i \notin I \tag{3.6.24}$$

and ± 1 is chosen for the determinant depending on the positioning of the rows. Therefore, in order to obtain a lower bound for the multiplicity of zero for $\Phi_I(z)$, it suffices to obtain the lower bound for the multiplicity of zero for $\Phi_{I,\underline{\nu}}(z)$, denoted by T_I, for all N-tuples $(\nu_1,\ldots,\nu_N)$, $\nu_i \le T$ $(i = 1,\ldots,N)$.

We rewrite

$$\varphi_i(z_0,z_1) = p_i(z_0,z_1)e^{l_i(z_0+z_1w)} \tag{3.6.25}$$

where

$$w = \log_p(\theta_1^{p^\kappa}) \tag{3.6.26}$$

(Note: $\log_p$ denotes p-adic logarithm) and

$$p_i(z_0,z_1) = \frac{1}{k_{1,i}!}\frac{\nu(T')^{k_{0,i}}}{k_{0,i}!}{z_0}^{k_{0,i}}{z_1}^{k_{1,i}}$$

is a monomial of total degree $\le K$, since $k_{0,i}+k_{1,i} \le K$. We apply the change of variable $Z_0 = z_0+z_1w$ so that $e^{l_i(z_0+z_1w)} = e^{l_iZ_0}$. This change of variable, being a translation with respect to the variable z_0, is evident as for any continuous function

$$\left(\frac{\partial}{\partial z_0}\right) f(z_0,z_1)\Big|_{(z_0,\,z_1)=(0,\,z\xi_{1,j})} = \left(\frac{\partial}{\partial Z_0}\right) f(Z_0 - z_1w, z_1)\Big|_{(Z_0,\,z_1)=(z\xi_{1,j}w,\,z\xi_{1,j})}.$$

We denote

$$\Psi^+_{I,\underline{\nu}}(z) = \left(\left(\frac{\partial}{\partial Z_0}\right)^{\nu_j} \phi_i(z\underline{x_j})\right);\ \text{for } i \in I, \qquad \Psi^-_{I,\underline{\nu}}(z) = \left(\sigma_{i,j}\left(\frac{\partial}{\partial Z_0}\right)^{\nu_j} \phi_i(z\underline{x_j})\right);\ \text{for } i \notin I,$$

$$\phi_i(Z_0,z_1) = q_i(Z_0,z_1)e^{l_iZ_0};\ \ 1 \le i \le N, \qquad \underline{x_j} = ((r_j+s_j\beta)w, r_j+s_j\beta);\ \ 1 \le j \le N,$$

$$q_i(Z_0,z_1) = \sum_{\tau=0}^{k_{0,i}} p_{i,\underline{\tau}}{Z_0}^{k_{0,i}-\tau}{z_1}^{\tau+k_{1,i}};\ \ 1 \le i \le N \qquad p_{i,\underline{\tau}} = \frac{1}{k_{1,i}!}\frac{\nu(T')^{k_{0,i}}}{k_{0,i}!}(-w)^\tau\binom{k_{0,i}}{\tau}\ \ 1 \le i \le N.$$

Note that the degree of z_1 in the polynomial $q_i(Z_0, z_1)$ is $\leq K$. It can be verified that the function $\Phi_{I,\underline{\nu}}(z)$ then becomes

$$\Phi_{I,\underline{\nu}}(z) = \Psi_{I,\underline{\nu}}(z) = \pm \det \begin{pmatrix} \Psi^+_{I,\underline{\nu}}(z) \\ \Psi^-_{I,\underline{\nu}}(z) \end{pmatrix} \tag{3.6.27}$$

where ± 1 is chosen for the determinant depending on the positioning of the rows. Furthermore, it should be noted that $\beta \in \mathbb{Z}_p$ from (3.6.6), $v_p(z) > -\frac{p^\kappa}{2e}$ from (3.6.12) and that $v_p(w) \geq \frac{p^\kappa}{2e} + \frac{1}{p-1}$ from (3.6.26), (3.3.2) and Lemma 3.17. Thus, for the substitution of the value $z(r_j + s_j\beta)w$ to Z_0 in the exponential function $e^{l_i Z_0}$, we have

$$v_p(l_i z(r_j + s_j\beta)w) = v_p(l_i(r_j + s_j\beta)) + v_p(z) + v_p(w) > \frac{1}{p-1}. \tag{3.6.28}$$

Now we present the following lemma (Lemma 3.25) which concerns the multiplicity of zeros for $\Phi_I(z)$. As illustrated before, it suffices to obtain the lower bound for the multiplicity of zero for $\Phi_{I,\underline{\nu}}(z)$ for all N-tuples $(\nu_1, \ldots, \nu_N)$, $\nu_i \leq T$ $(i = 1, \ldots, N)$.

Lemma 3.25. *For any set $I \subseteq \{1, \ldots, N\}$ of cardinality $|I|$, the function $\Phi_I(z)$ has a zero at the origin with multiplicity $\geq T_I$, where*

$$T_I \geq \max\left\{\frac{|I|}{2}\left(\frac{|I|+1}{K+1} - \frac{K}{2} - 1\right) - TN, 0\right\}.$$

Proof. First, we take the Taylor's expansion with respect to the variable Z_0 for the function $\phi_i(Z_0, z_1)$. That is,

$$\phi_i(Z_0, z_1) = q_i(Z_0, z_1) \sum_{u=0}^{\infty} \frac{(l_i Z_0)^u}{u!} = \sum_{u \geq 0} \sum_{\tau=0}^{k_{0,i}} p_{i,\underline{\tau}} \frac{{l_i}^u}{u!} {z_1}^{\tau + k_{1,i}} {Z_0}^{u + k_{0,i} - \tau}.$$

It gives, for all $1 \leq j \leq N$, a development of the form

$$\frac{1}{\nu_j!}\left(\frac{\partial}{\partial Z_0}\right)^{\nu_j} \phi_i(Z_0, z_1) = \sum_{u \geq 0} \sum_{\tau=0}^{k_{0,i}} p_{i,\underline{\tau}} \frac{{l_i}^u}{u!} \binom{u + k_{0,i} - \tau}{\nu_j} {z_1}^{\tau + k_{1,i}} {Z_0}^{u + k_{0,i} - \tau - \nu_j}.$$

Further, with the change of variable $\tau_0 = u + k_{0,i} - \tau$ and $\tau_1 = \tau + k_{1,i}$, we get

$$\begin{aligned} \frac{1}{\nu_j!}\left(\frac{\partial}{\partial Z_0}\right)^{\nu_j} \phi_i(Z_0, z_1) &= \sum_{\tau_1 = k_{1,i}}^{k_{0,i} + k_{1,i}} \sum_{\tau_0 + \tau_1 \geq k_{0,i} + k_{1,i}} \binom{\tau_0}{\nu_j} d_{i,\tau_0,\tau_1} {Z_0}^{\tau_0 - \nu_j} {z_1}^{\tau_1} \\ &= \sum_{\tau_0 \geq 0} \sum_{\tau_1 = 0}^{K} \binom{\tau_0}{\nu_j} d_{i,\tau_0,\tau_1} {Z_0}^{\tau_0 - \nu_j} {z_1}^{\tau_1} \end{aligned} \tag{3.6.29}$$

where $d_{i,\tau_0,\tau_1} = p_{i,\underline{\tau}} \frac{{l_i}^{\tau_0 + \tau - k_{0,i}}}{\tau_0 + \tau - k_{0,i}!}$ with $d_{i,\tau_0,\tau_1} = 0$ in the i-th row $(1 \leq j \leq N)$ when $\tau_1 < k_{1,i}$, $\tau_1 > k_{0,i} + k_{1,i}$, $\tau_0 + \tau_1 < k_{0,i} + k_{1,i}$ if $l_i > 0$ and when $\tau_0 + \tau_1 \neq k_{0,i} + k_{1,i}$ if $l_i = 0$.

Using the expression (3.6.29) above, we can develop $\Phi_{I,\underline{\nu}}(z)$ (i.e. $\Psi_{I,\underline{\nu}}(z)$) by modifying the entries in the submatrix $\Psi^{+}_{I,\underline{\nu}}(z)$ as

$$\sum_{\tau_{0,i}\geq 0}\sum_{\tau_{1,i}=0}^{K}\binom{\tau_{0,i}}{\nu_j}\nu_j!\,d_{i,\tau_{0,i},\tau_{1,i}}(z(r_j+s_j\beta)w)^{\tau_{0,i}-\nu_j}(z(r_j+s_j\beta))^{\tau_{1,i}}.$$

Now $\Phi_{I,\underline{\nu}}(z)$ (i.e. $\Psi_{I,\underline{\nu}}(z)$) can be written as

$$\begin{aligned}
\Phi_{I,\underline{\nu}}(z) &= \pm\det\begin{pmatrix} \sum_{\tau_{0,i}\geq 0}\sum_{\tau_{1,i}=0}^{K}\binom{\tau_{0,i}}{\nu_j}\nu_j!\,d_{i,\tau_{0,i},\tau_{1,i}}(z(r_j+s_j\beta)w)^{\tau_{0,i}-\nu_j}(z(r_j+s_j\beta))^{\tau_{1,i}} \\ \sigma_{i,j}\left(\frac{\partial}{\partial Z_0}\right)^{\nu_j}\phi_i(z\underline{x_j}) \end{pmatrix} \begin{matrix}\}i\in I\\ \}i\notin I\end{matrix}\\
&= \sum_{\substack{(\tau_{0,i},\tau_{1,i}),i\in I\\ \tau_{0,i}\geq 0,\ \tau_{1,i}\leq K}} \pm\det\begin{pmatrix} \binom{\tau_{0,i}}{\nu_j}\nu_j!\,d_{i,\tau_{0,i},\tau_{1,i}}\,w^{\tau_{0,i}-\nu_j}\xi_{1,j}^{\tau_{0,i}+\tau_{1,i}-\nu_j}z^{\tau_{0,i}+\tau_{1,i}-\nu_j} \\ \sigma_{i,j}\left(\frac{\partial}{\partial Z_0}\right)^{\nu_j}\phi_i(z\underline{x_j}) \end{pmatrix} \begin{matrix}\}i\in I\\ \}i\notin I\end{matrix}\\
&= \sum_{\substack{(\tau_{0,i},\tau_{1,i}),i\in I\\ \tau_{0,i}\geq 0,\ \tau_{1,i}\leq K}}\left(\prod_{i\in I}d_{i,\tau_{0,i},\tau_{1,i}}z^{\tau_{0,i}+\tau_{1,i}-T}\right)(\pm\det\Omega_{I,\underline{\tau}}(z)), \qquad (3.6.30)
\end{aligned}$$

where the entries in $\Omega_{I,\underline{\tau}}(z)$ are the functions

$$W_{i,j}(z)=\begin{cases}\binom{\tau_{0,i}}{\nu_j}\nu_j!\,w^{\tau_{0,i}-\nu_j}\xi_{1,j}^{\tau_{0,i}+\tau_{1,i}-\nu_j}z^{T-\nu_j}, & i\in I,\\ \sigma_{i,j}\left(\frac{\partial}{\partial Z_0}\right)^{\nu_j}\phi_i(z\underline{x_j}), & i\notin I\end{cases}$$

with $0\leq\nu_j\leq T$. The matrix $\Omega_{I,\underline{\tau}}(z)$ is of rank $<N$, in the case where there exists $i,i'\in I$, such that $i\neq i'$ and $(\tau_{0,i},\tau_{1,i})=(\tau_{0,i'},\tau_{1,i'})$. It follows that the multiplicity of zero of $\Phi_{I,\underline{\nu}}(z)$ is greater than or equal to the minimum value of the sums

$$\sum_{\substack{(\tau_{0,i},\tau_{1,i}),i\in I\\ \tau_{1,i}\leq K}}(\tau_{0,i}+\tau_{1,i}-T), \qquad (3.6.31)$$

where all couples $(\tau_{0,i},\tau_{1,i})$ are pairwise distinct, while excluding the scenarios that $d_{i,\tau_0,\tau_1}=0$ in the i-th row $(1\leq j\leq N)$ for $i\in I$.

By referring to the proof of [49, Lemma A.4], it is noted that the derivation involved still applies to our scenario for obtaining the lower bound of the multiplicity of zero of $\Phi_{I,\underline{\nu}}(z)$, after taking into account scenarios with $d_{i,\tau_0,\tau_1}=0$ mentioned above. Therefore, it suffices to adopt the bound obtained in [49, Lemma A.4], that is

$$\frac{|I|}{2}\left(\frac{|I|+1}{K+1}-\frac{K}{2}-1\right)-TN.$$

Finally, it should be noted that due to the way that $\Phi_{I,\underline{\nu}}(z)$ is defined, the actual minimum possible value of T_I is zero. Thus the lower bound $T_I\geq\max\left\{\frac{|I|}{2}\left(\frac{|I|+1}{K+1}-\frac{K}{2}-1\right)-TN,0\right\}$ results. □

We have acquired all necessary lemmas to deduce the analytic upper bound for $|\gamma|_p$ (i.e. the lower bound for $v_p(\gamma)$) in Proposition 3.3 as follows.

Proof of Proposition 3.3. It is clear from Lemma 3.21 that $v_p(\gamma) = v_p(\gamma')$. We now develop γ' defined in (3.6.5). Recall from (3.6.6) that we assume $p \nmid b_2'$. From the relation

$$\theta_2^{b_2'} = \frac{\theta_1^{b_1'} - \Lambda'}{\xi_1} = \frac{\theta_1^{b_1'}(1 - \theta_1^{-b_1'}\Lambda')}{\xi_1}$$

and noting that $\xi_1^{p^\kappa} = 1$ from Lemma 3.22, we obtain

$$\theta_2^{b_2' p^\kappa l_i s_j} = \theta_1^{b_1' p^\kappa l_i s_j}(1 - \theta_1^{-b_1'}\Lambda')^{p^\kappa l_i s_j} \qquad (1 \le i, j \le N). \tag{3.6.32}$$

By inequalities (3.6.3) in Lemma 3.17,

$$v_p(\theta_i^{p^\kappa} - 1) \ge \frac{p^\kappa}{2e} + \frac{1}{p-1} > \frac{1}{p-1} \qquad (i = 1, 2).$$

Secondly, by Lemma 3.22 and (3.2.8), $v_p(\Lambda') \ge V > \frac{1}{p-1}$ so that

$$v_p(\theta_1^{-b_1'}\Lambda') > \frac{1}{p-1}.$$

It should also be noted that $v_p(p^\kappa l_i s_j / b_2') \ge \kappa \ge 0$. Raising both sides of (3.6.32) by the power $\frac{1}{b_2'}$ and taking β as in (3.6.6) gives

$$\theta_2^{p^\kappa l_i s_j} = \theta_1^{p^\kappa \beta l_i s_j}(1 - \theta_1^{-b_1'}\Lambda')^{p^\kappa l_i s_j / b_2'}.$$

By applying Proposition 3.1 in Section 3.3.1 to $(1 - \theta_1^{-b_1'}\Lambda')^{p^\kappa l_i s_j / b_2'}$ with $x = -\theta_1^{-b_1'}\Lambda'$ and $z = p^\kappa l_i s_j / b_2'$, we get

$$\theta_2^{p^\kappa l_i s_j} = \theta_1^{p^\kappa \beta l_i s_j}(1 + \sigma_{i,j}\Lambda') \qquad (1 \le i, j \le N), \tag{3.6.33}$$

where $\sigma_{i,j} = -\theta_1^{-b_1'} p^\kappa l_i s_j / b_2' v(x, z) \in \overline{\mathbb{Q}}_p$ with $|v(x, z)|_p \le 1$. In addition, as $l_i s_j / b_2' \in \mathbb{Z}_p$, we deduce that

$$|\sigma_{i,j}|_p \le p^{-\kappa} \le 1. \tag{3.6.34}$$

Now we substitute (3.6.33) into the determinant γ' displayed in (3.6.5). By Lemma 3.6, multilinearity of determinants, taking $q = 0$ and noting (3.3.6),

$$\gamma' = b_2^{\sum_{i=1}^N k_{1,i}} \gamma''$$

where

$$\gamma'' = \det\left(c_{i,j}(1 + \sigma_{i,j}\Lambda')\right)_{1 \le i, j \le N}$$

with

$$c_{i,j} = \frac{(r_j + s_j\beta)^{k_{1,i}}}{k_{1,i}!}\Delta(l_i; T', t_j, k_{0,i})\theta_1^{p^\kappa l_i(r_j+s_j\beta)}. \tag{3.6.35}$$

Trivially,

$$v_p(\gamma') = \underbrace{v_p\left(b_2^{\sum_{i=1}^N k_{1,i}}\right)}_{\geq 0} + v_p(\gamma'') \geq v_p(\gamma''), \tag{3.6.36}$$

so from now on we shall focus on obtaining the lower bound for $v_p(\gamma'')$. By further developing γ'',

$$\gamma'' = \sum_{I \subseteq \{1,\dots,N\}} (\Lambda')^{N-|I|}\gamma_I \tag{3.6.37}$$

where $|I|$ is the cardinality of I and

$$\gamma_I := \pm\det\begin{pmatrix} {\gamma_I}^+ \\ {\gamma_I}^- \end{pmatrix} \tag{3.6.38}$$

with ${\gamma_I}^+ = (c_{i,j})$ for $i \in I$, ${\gamma_I}^- = (\sigma_{i,j}\, c_{i,j})$ for $i \notin I$ and ± 1 is chosen for the determinant depending on the positioning of the rows. Refering to the function $\Phi_I(z)$ defined in (3.6.13), it can be observed that

$$\Phi_I(1) = \gamma_I. \tag{3.6.39}$$

We have shown in Lemma 3.25 that the function $\Phi_I(z)$ has a zero at the origin with multiplicity $\geq T_I$. We shall apply Lemma 3.20 (p-adic Schwarz's lemma) with $r = 1$, $R = p^\lambda$, $f = \Phi_I(z)$ to get

$$|\gamma_I|_p = |\Phi_I(1)|_p \leq \left(p^\lambda\right)^{-T_I} \max_{|z|_p = p^\lambda} |\Phi_I(z)|_p. \tag{3.6.40}$$

We refer to the lower bound of $v_p(\Phi_I(z)))$ obtained in Lemma 3.23, which essentially gives an upper bound for $\max_{|z|_p=p^\lambda}|\Phi_I(z)|_p$. With the fact that $p^\lambda > 1$ from (3.2.9), we obtain

$$\begin{aligned} |\gamma_I|_p &< p^{-\lambda\max\left\{\frac{|I|}{2}\left(\frac{|I|+1}{K+1}-\frac{K}{2}-1\right)-TN,0\right\}} p^{\frac{KN}{3}\left(\lambda+\frac{1}{p-1}\right)} \\ &\leq p^{-\left(\frac{|I|}{2}\left(\frac{|I|+1}{K+1}-\frac{K}{2}-1\right)-TN\right)\lambda+\frac{KN}{3}\left(\lambda+\frac{1}{p-1}\right)}. \end{aligned}$$

Equivalently,

$$v_p(\gamma_I) > \left(\frac{|I|}{2}\left(\frac{|I|+1}{K+1} - \frac{K}{2} - 1\right) - TN\right)\lambda - \frac{KN}{3}\left(\lambda + \frac{1}{p-1}\right). \tag{3.6.41}$$

We shall now obtain the upper bound for $|\gamma|_p$, which is the same as the upper bound for $|\gamma'|_p$ due to Lemma 3.21 and we already have $|\gamma'|_p \leq |\gamma''|_p$ due to (3.6.36). We refer to (3.6.37) and note from Lemma 3.6.9 that $v_p(\Lambda') \geq V$. Hence,

$$v_p(\gamma'') \geq \min_{I\subseteq\{1,\dots,N\}} \{(N - |I|)V + v_p(\gamma_I)\}$$

where $|I|$ is the cardinality of I. But the upper bound of $|\gamma_I|_p$ derived before does not depend on I. So the minimum for $(N-|I|)V + v_p(\gamma_I)$ is independent of I. Thus,

$$v_p(\gamma') \geq v_p(\gamma'') > \min_{|I|}\left\{(N-|I|)V + \left(\frac{|I|}{2}\left(\frac{|I|+1}{K+1} - \frac{K}{2} - 1\right) - TN\right)\lambda - \frac{KN}{3}\left(\lambda + \frac{1}{p-1}\right)\right\}.$$

We shall minimize the following expression with respect to $|I|$:

$$(N-|I|)V + \left(\frac{|I|}{2}\left(\frac{|I|+1}{K+1} - \frac{K}{2} - 1\right) - TN\right)\lambda. \tag{3.6.42}$$

Note that (3.6.42) is a second degree polynomial in variable $|I|$. The minimum is reached on $\mathbb{R}$ at the value

$$|I| = \left(\frac{V}{\lambda} + \frac{K+2}{4} - \frac{1}{2(K+1)}\right)(K+1).$$

The minimum value is then

$$NV - \frac{V^2(K+1)}{2\lambda} - \frac{K(K+3)}{4}V - \frac{K^2(K+3)^2\lambda}{32(K+1)} - NT\lambda. \tag{3.6.43}$$

Similar to [50], we wish to simplify (3.6.43) by obtaining its lower bound in the form $\frac{NV}{2} - NT\lambda$ instead. It suffices to find the value of parameter V satisfying the quadratic inequality

$$\frac{V^2(K+1)}{2\lambda} + \frac{K(K+3)}{4}V + \frac{K^2(K+3)^2\lambda}{32(K+1)} \leq \frac{NV}{2}. \tag{3.6.44}$$

It can be checked that condition (3.6.44) is satisfied for V defined in (3.2.7). As a result,

$$v_p(\gamma) = v_p(\gamma') > \frac{NV}{2} - NT\lambda - \frac{KN}{3}\left(\lambda + \frac{1}{p-1}\right)$$

where λ is in (3.2.9). It is equivalent to (3.6.2). The proof of Proposition 3.3 (Analytic upper bound) is completed. □

3.7 Proof of the Main Proposition

As a final step, we now present the proof of the Main Proposition.

Proof of the Main Proposition. Suppose on the contrary of (3.2.11) we have (3.6.1), that is

$$|\Lambda|_p \leq p^{-(V+u)}. \tag{3.6.1}$$

We shall demonstrate that there is a contradiction to Condition (1a) (i.e. (3.2.10)) in the Main Proposition. Combining the results from Proposition 3.2, Proposition 3.3, using the inequality $N! \le \left(\frac{N}{2}\right)^N$ and the fact that $\log\left(\frac{T}{K(L+T')}\right) < \log\left(\frac{T}{KL}\right)$, we obtain

$$\begin{aligned}\frac{V}{2} < \left(T+\frac{K}{3}\right)\lambda + \frac{K}{3(p-1)} + \frac{D}{e\log p}\Bigg(\log\left(\frac{N}{2}\right) + \frac{K}{3}\left(\log\widetilde{B} + \log\left(\frac{T}{KL}\right) + \frac{11}{3} + \frac{107T'}{103}\right) \\ + (\omega T+\omega_0)\left(1+\log\left(\frac{L+T'}{T'}\right)\right) + T' + \frac{2p^{\kappa}}{N}\left(G_1 h(\alpha_1) + G_2 h(\alpha_2)\right)\Bigg)\end{aligned} \tag{3.7.1}$$

The value of the variable T' is now chosen so that RHS of (3.7.1) is preferably the smallest. By a similar derivation as in [49], we take for simplicity

$$T' = \left[\frac{309\omega T}{309+107K}\right] + 1 \ge \frac{309\omega T}{107(K+3)}.$$

This gives $\log\left(\frac{L+T'}{T'}\right) < \log\left(\frac{107(K+3)L}{309\omega T}+1\right)$ and $\left(\frac{107K}{309}+1\right)T' \le \frac{107K}{309} + 1 + \omega T$. Using the definitions of G_1 and G_2 in Lemma 3.13 it follows that

$$\begin{aligned}\frac{V}{2} < \left(T+\frac{K}{3}\right)\lambda + \frac{K}{3(p-1)} + \frac{D}{e\log p}\Bigg(\log\left(\frac{N}{2}\right) + \frac{K}{3}\left(\log\widetilde{B} + \log\left(\frac{T}{KL}\right) + \frac{1454}{309}\right) \\ + (\omega T+\omega_0)\left(2+\log\left(\frac{107(K+3)L}{309\omega T}+1\right)\right) + 1 + p^{\kappa}(L+1)g_0\left((R+g)h(\alpha_1)+(S+g)h(\alpha_2)\right)\Bigg).\end{aligned}$$

However, it contradicts Condition (1a) (i.e. (3.2.10)) in the Main Proposition. The hypothesis (3.6.1) has to be reversed. The proof of the Main Proposition is completed. □

3.8 Preparation for the proof of Theorem 3.1

Our goal of this section is to obtain Theorem 3.1 by using appropriate formulae and numerical choices of parameters involved in the Main Proposition. The proof will be divided into two cases which will be further described in Section 3.9.

3.8.1 Choice of parameters and estimates

We list the choices and assumptions of parameters appeared in the Main Proposition and generated during the derivation. Recall $N = \frac{(K+2)(K+1)(L+1)}{2}$ in (3.2.4) and $\lambda = \frac{\eta p^\kappa}{2e}$ in (3.2.9). We adopt

$$\begin{cases} g_0 = 0.24, & \omega = 0.94, & \omega_0 = 12.45, & \vartheta = 4.35, & \text{if } p = 2, 3, \\ g_0 = 0.239, & \omega = 0.933, & \omega_0 = 11.06, & \vartheta = 2.35, & \text{if } p \geq 5. \end{cases} \tag{3.8.1}$$

Let C_0 and C_1 be positive real numbers to be specified later. Denote

$$J = \left(\frac{2D\log E^*}{g_0\sqrt{a_1 a_2}}\right)^{1/3}, \quad \Gamma = \min\left\{\frac{K+1}{2}, L+1\right\},$$

$$R^* = g^{1/3}J(K+1)^{2/3}\sqrt{\frac{a_2}{a_1}}, \quad S^* = g^{1/3}J(K+1)^{2/3}\sqrt{\frac{a_1}{a_2}}, \quad \text{and} \quad T^* = \frac{g^{1/3}(L+1)(K+1)^{2/3}}{J^2}.$$

We have the following expressions for the parameters:

$$K = [C_0 g a_1 a_2 D \log E^*], \tag{3.8.2}$$

$$L = \left[\frac{C_1 DH}{\log p}\right], \tag{3.8.3}$$

$$R_1 = \left[\frac{R^*}{J}\left(\frac{g}{K+1}\right)^{1/6}\right], \tag{3.8.4}$$

$$R_2 = \left[\frac{R^*}{\Gamma^{1/3}}\right], \tag{3.8.5}$$

$$R_3 = \left[3^{1/3}R^*\right], \tag{3.8.6}$$

$$S_1 = \left[\frac{S^*}{J}\left(\frac{g}{K+1}\right)^{1/6}\right], \tag{3.8.7}$$

$$S_2 = \left[\frac{S^*}{\Gamma^{1/3}}\right], \tag{3.8.8}$$

$$S_3 = \left[3^{1/3}S^*\right], \tag{3.8.9}$$

$$T_1 = \max\left\{\left[\frac{L+1}{K+1}\right], K\right\}, \tag{3.8.10}$$

$$T_2 = \left[\frac{T^*}{\Gamma^{1/3}}\right], \tag{3.8.11}$$

$$T_3 = \left[3^{1/3} T^*\right]. \tag{3.8.12}$$

We further pose some conditions to our parameters.

$$a_i = \frac{D \log A_i}{\log p} \geq \max\left\{\frac{Dh(\alpha_i)}{\log p}, 1\right\}, \qquad (i = 1, 2) \tag{3.8.13}$$

$$D \log E^* \geq \begin{cases} 1.5, & \text{if } p = 2, 3, \\ 2.5, & \text{if } p \geq 5, \end{cases} \tag{3.8.14}$$

$$\log E^* \geq \begin{cases} \frac{1}{4}\left(\frac{2\eta \log p}{D} + 2 + \frac{\omega}{3}\log C_0 + \omega \log D\right), & \text{if } p = 2, \\ \frac{1}{4}\left(\frac{3\eta \log p}{2D} + 2 + \frac{\omega}{3}\log C_0 + \omega \log D\right), & \text{if } p = 3, \\ \frac{1}{2}\left(\frac{\eta \log p}{2D} + 2 + \frac{\omega}{3}\log C_0 + \omega \log D\right), & \text{if } p \geq 5, \end{cases} \tag{3.8.15}$$

$$H \geq \begin{cases} \max\left\{\log\left(\frac{b_2}{a_1} + \frac{b_1}{a_2}\right), \frac{1000 \log p}{D}, 720 \log E^* \log p\right\}, & \text{if } p = 2, 3, \\ \max\left\{\log\left(\frac{b_2}{a_1} + \frac{b_1}{a_2}\right), \frac{1000 \log p}{D}, 360 \log E^* \log p\right\}, & \text{if } p \geq 5, \end{cases} \tag{3.8.16}$$

$$8000 \leq C_0 \leq 10000, \tag{3.8.17}$$

$$C_1 \geq \begin{cases} 2, & \text{if } p = 2, 3, \\ 10, & \text{if } p \geq 5. \end{cases} \tag{3.8.18}$$

We deduce from (3.8.1), (3.8.13), (3.8.14), (3.8.15), (3.8.16) and (3.8.18) that

$$\log E^* \geq \begin{cases} 1.5, & \text{if } p = 2, 3, \\ 2.5, & \text{if } p \geq 5, \end{cases} \tag{3.8.19}$$

$$K + 1 \geq \begin{cases} 12000g \geq 12000, & \text{if } p = 2, 3, \\ 20000g \geq 20000, & \text{if } p \geq 5, \end{cases} \tag{3.8.20}$$

$$L + 1 \geq \begin{cases} 2000, & \text{if } p = 2, 3, \\ 10000, & \text{if } p \geq 5, \end{cases} \tag{3.8.21}$$

$$3^{1/3} + \frac{1}{\Gamma^{1/3}} \leq \begin{cases} 1.522, & \text{if } p = 2, 3, \\ 1.4887, & \text{if } p \geq 5. \end{cases} \tag{3.8.22}$$

Besides, recalling that $R = R_1 + R_2 + R_3$, $S = S_1 + S_2 + S_3$ and $T = T_1 + T_2 + T_3$, we can obtain the bounds

$$R \leq R^* \left(\frac{1}{J}\left(\frac{g}{K+1}\right)^{1/6} + 3^{1/3} + \frac{1}{\Gamma^{1/3}}\right), \tag{3.8.23}$$

$$S \leq S^* \left(\frac{1}{J}\left(\frac{g}{K+1}\right)^{1/6} + 3^{1/3} + \frac{1}{\Gamma^{1/3}}\right), \tag{3.8.24}$$

$$\frac{(L+1)(K+1)}{D \log E^*} \cdot \frac{g_0^{2/3}\left(3^{1/3} + \frac{1}{\Gamma^{1/3}}\right)}{2^{2/3} C_0^{1/3}\left(1 + \frac{1}{gX_1}\right)^{1/3}} \leq T \leq \max\left\{\left[\frac{L+1}{K+1}\right], K\right\} + T^*\left(3^{1/3} + \frac{1}{\Gamma^{1/3}}\right) \tag{3.8.25}$$

where $X_1 = 11999$ when $p = 2, 3$ and $X_1 = 19999$ when $p \geq 5$.

These enable us to show that the values chosen for g_0, ω and ω_0 in (3.8.1) satisfy (3.2.5). The main step involved is to obtain an estimate for the upper bound

$$\frac{\Psi(g)}{gN} = \frac{(R+g)(S+g)(T+1)}{gN} < 2g \cdot \frac{\frac{R}{g}+1}{(K+1)^{2/3}} \cdot \frac{\frac{S}{g}+1}{(K+1)^{2/3}} \cdot \frac{T+1}{(L+1)(K+1)^{2/3}}.$$

The computations are tedious but elementary. We omit the deductions here.

3.8.2 Modification of Condition (1a) (i.e. (3.2.10)) with choices of parameters

Our target in this section is to establish inequality (3.8.43), which is given at the end of this section. We shall show that using our choice and conditions of parameters in Section 3.8.1, Condition (1a) (i.e. (3.2.10)) in the Main Proposition can be implied by inequality (3.8.43). We achieve this with deductions involving several lemmas and a proposition. Denote

$$\Theta = \frac{1}{8}\left(1 - \frac{1}{L+1} + \sqrt{1 - \frac{2}{L+1}}\right). \tag{3.8.26}$$

Using (3.2.7) and (3.2.9), Condition (1a) (i.e. (3.2.10)) becomes:

$$\begin{aligned} &\Theta(K+2)(L+1)\left(\frac{\eta p^\kappa}{2e}\right) \\ &\quad \geq \left(T + \frac{K}{3}\right)\left(\frac{\eta p^\kappa}{2e}\right) + \frac{K}{3(p-1)} + \frac{D}{e\log p}\left(\log\left(\frac{N}{2}\right) + \frac{K}{3}\left(\log \widetilde{B} + \log\left(\frac{T}{KL}\right) + \frac{1454}{309}\right)\right. \\ &\qquad \left. + (\omega T + \omega_0)\left(2 + \log\left(\frac{107(K+3)L}{309\omega T} + 1\right)\right) + 1 + p^\kappa (L+1) g_0 \left((R+g)h(\alpha_1) + (S+g)h(\alpha_2)\right)\right). \end{aligned} \tag{3.8.27}$$

It is rearranged to yield

$$\frac{\Theta(K+1)(L+1)\eta}{2} \geq \Xi \tag{3.8.28}$$

where

$$\begin{aligned} \Xi = &-\frac{\Theta(L+1)\eta}{2} + \left(T + \frac{K}{3}\right)\frac{\eta}{2} + \frac{e}{p^\kappa} \cdot \frac{K}{3(p-1)} + \frac{D}{p^\kappa \log p}\left(\log\left(\frac{N}{2}\right) + \frac{K}{3}\left(\log \widetilde{B} + \log\left(\frac{T}{KL}\right) + \frac{1454}{309}\right)\right. \\ &\left. + (\omega T + \omega_0)\left(2 + \log\left(\frac{107(K+3)L}{309\omega T} + 1\right)\right) + 1\right) + \frac{D}{\log p} \cdot (L+1) g_0 \left((R+g)h(\alpha_1) + (S+g)h(\alpha_2)\right). \end{aligned} \tag{3.8.29}$$

We begin with several steps to obtain the first upper bound for Ξ. The steps involved are:

- We refer to (3.2.3) and observe that $\kappa \geq \begin{cases} 2, & \text{if } p = 2, \\ 1, & \text{if } p = 3, \\ 0, & \text{if } p \geq 5, \end{cases}$ so that $p^\kappa \geq \begin{cases} 4, & \text{if } p = 2, \\ 3, & \text{if } p = 3, \\ 1, & \text{if } p \geq 5, \end{cases}$
- use $e \leq D$, $\log \frac{N}{2} < 2\log\left(\frac{K+2}{2}\right) + \log(L+1)$ and
- use $h(\alpha_i) \leq \log A_i = \frac{a_i \log p}{D}$, $(i = 1, 2)$ by referring to (3.8.13).

These give

$$\begin{aligned}\Xi < &\underbrace{\frac{DK}{3Z_1 \log p}\left(\log \widetilde{B} + \frac{1454}{309} + \frac{6}{K}\log\left(\frac{K+2}{2}\right) + \log\left(\frac{T}{KL}\right) + \frac{Z_1 \eta \log p}{2D} + \frac{\log p}{p-1}\right)}_{\text{terms with } K \text{ as key term}} \\ &+ \underbrace{\frac{DT}{Z_1 \log p}\left(\frac{Z_1 \eta \log p}{2D} + 2\omega + \omega \log\left(\frac{107(K+3)L}{309\omega T} + 1\right)\right)}_{\text{terms with } T \text{ as key term}} + \underbrace{g_0(L+1)\left((R+g)a_1 + (S+g)a_2\right)}_{\text{terms with } g_0} \\ &+ \frac{D}{Z_1 \log p}\left(2\omega_0 + \omega_0 \log\left(\frac{107(K+3)L}{309\omega T} + 1\right) + 1 + \log(L+1)\right) - \frac{\Theta(L+1)\eta}{2}\end{aligned} \tag{3.8.30}$$

where

$$Z_1 = \begin{cases} 4, & \text{if } p = 2, \\ 3, & \text{if } p = 3, \\ 1, & \text{if } p \geq 5. \end{cases}$$

We shall now derive a sequence of lemmata a larger upper bound for Ξ, a proposition to obtain the upper bound for $\frac{\Xi}{(K+1)(L+1)}$ and then a lower bound for $\frac{\Theta\eta}{2}$. Then we require that the lower bound for $\frac{\Theta\eta}{2}$ supersedes the upper bound obtained for $\frac{\Xi}{(K+1)(L+1)}$. This assertion will be justified in Section 3.9.1. These show that Condition (1a) (i.e. (3.2.10)) is satisfied with our choice of parameters.

We shall derive the case when $p \geq 5$. The derivation for the case when $p = 2$ and $p = 3$ are similar and shall be omitted. We start with obtaining an upper bound for the terms with K as key term in (3.8.30). The following lemma is similar to [49, Lemma 5.2] and [50, Lemma 5.1].

Lemma 3.26. *With the use of* (3.8.1), (3.8.2) *and* (3.8.13) *to* (3.8.25), *we have*

$$\log \widetilde{B} + \frac{1454}{309} + \frac{6}{K}\log\left(\frac{K+2}{2}\right) + \log\left(\frac{T}{KL}\right) + \frac{\eta \log p}{2D} + \frac{\log p}{p-1} \leq H - 2.23 + \frac{\eta \log p}{2D}. \tag{3.8.31}$$

Proof. Going back to the definition of $\widetilde{B}$ in (3.2.4), we start with deducing the upper bound for $\frac{R}{K}$ and $\frac{S}{K}$. This can be achieved by adopting the upper bound of R and S in (3.8.23) and (3.8.24) respectively and the choice of K in (3.8.2). We obtain

$$\frac{R}{K} = \frac{R}{K+1}\left(1+\frac{1}{K}\right) \le \frac{1}{a_1}\left(1+\frac{1}{K}\right)\left(\frac{1}{\sqrt{C_0 D \log E^*}} + \left(\frac{2}{g_0 C_0}\right)^{1/3}\left(3^{1/3} + \frac{1}{\Gamma^{1/3}}\right)\right)$$
$$\frac{S}{K} = \frac{S}{K+1}\left(1+\frac{1}{K}\right) \le \frac{1}{a_2}\left(1+\frac{1}{K}\right)\left(\frac{1}{\sqrt{C_0 D \log E^*}} + \left(\frac{2}{g_0 C_0}\right)^{1/3}\left(3^{1/3} + \frac{1}{\Gamma^{1/3}}\right)\right).$$

Together with (3.8.14), (3.8.18) and (3.8.20), we get

$$\frac{R}{K} \le \frac{0.16}{a_1} \qquad \text{and} \qquad \frac{S}{K} \le \frac{0.16}{a_2}$$

and hence

$$\log \widetilde{B} \le \log\left(\frac{b_2}{a_1} + \frac{b_1}{a_2}\right) - 2.52. \tag{3.8.32}$$

Next, we make use of (3.8.20) to obtain

$$\frac{6}{K}\log\left(\frac{K+2}{2}\right) \le 0.003 \tag{3.8.33}$$

and use (3.8.14), (3.8.17), (3.8.20), (3.8.21), g_0 in (3.8.1) and the upper bound of T in (3.8.25) to get

$$\frac{T}{KL} \le \left(1+\frac{2}{K+1}\right)\left(1+\frac{2}{L+1}\right)\frac{T}{(K+1)(L+1)} \le 0.008. \tag{3.8.34}$$

Now making use of (3.8.16), (3.8.32), (3.8.33) and (3.8.34), Lemma 3.8.31 follows. □

Next, we shall obtain an upper bound for terms with T as key term in (3.8.30).

Lemma 3.27. *With the use of* (3.8.1), (3.8.14), (3.8.15), (3.8.17) *and the inequalities* (3.8.20) *and* (3.8.25), *we have the upper bound*

$$\frac{DT}{\log p}\left(\frac{\eta \log p}{2D} + 2\omega + \omega \log\left(\frac{107(K+3)L}{309\omega T} + 1\right)\right) < \frac{DT\vartheta \log E^*}{\log p}.$$

Proof. We begin with obtaining the upper bound of $\log\left(\frac{107(K+3)L}{309\omega T} + 1\right)$. First, we use (3.8.1), (3.8.20) and the lower bound of T in (3.8.25) to get

$$\frac{(K+3)L}{T} < \frac{K+3}{K+1} \cdot \frac{(K+1)(L+1)}{T} \le 2.86 C_0^{1/3} D \log E^*.$$

Next, we note by using (3.8.1), (3.8.14) and (3.8.17) that

$$\frac{107}{309\omega} \cdot 2.86 C_0^{1/3} D \log E^* > 53.$$

Finally, by referring to (3.8.1) and (3.8.15), we deduce that

$$\begin{aligned}\frac{\eta\log p}{2D}+2\omega+\omega\log\left(\frac{107(K+3)L}{309\omega T}+1\right) &< \frac{\eta\log p}{2D}+2\omega+\omega\log\left(\frac{54}{53}\cdot\frac{107}{309\omega}2.86C_0^{1/3}D\log E^*\right)\\ &< \left(\frac{\eta\log p}{2D}+2+\frac{\omega}{3}\log C_0+\omega\log D\right)+\omega\log\log E^*\\ &\le 2\log E^*+\omega\log\log E^*\\ &= \left(2+\frac{\omega\log\log E^*}{\log E^*}\right)\log E^*\\ &< \vartheta\log E^*. \end{aligned}\tag{3.8.35}$$

The last step is due to the fact that the function $f(x)=\frac{\log x}{x}$, $x>0$ attains maximum at $x=e$ ($=2.718\dots$). □

Remark. *As a consequence to* (3.8.35)*, we obtain an upper bound for two terms in* (3.8.30)*, namely*

$$2\omega_0+\omega_0\log\left(\frac{107(K+3)L}{309\omega T}+1\right)<\frac{\omega_0\vartheta}{\omega}\log E^*.$$

Now we group the term $\frac{DT\vartheta\log E^*}{\log p}$ obtained at the upper bound in Lemma 3.27 with the terms with g_0 in (3.8.30). We make use of the upper bounds of R, S in (3.8.23) and(3.8.24) to obtain

$$Ra_1+Sa_2\le 2g^{1/3}\sqrt{a_1a_2}\left(g^{1/6}\sqrt{K+1}+J(K+1)^{2/3}\left(3^{1/3}+\frac{1}{\Gamma^{1/3}}\right)\right),\tag{3.8.36}$$

which is used together with the upper bound of T in (3.8.25) to yield

$$\frac{DT\vartheta\log E^*}{\log p}+g_0(L+1)\left((R+g)a_1+(S+g)a_2\right)<\Phi+\frac{D\vartheta\log E^*}{\log p}\left(\frac{L+1}{K+1}\right)$$

where

$$\begin{aligned}\Phi=&\ \frac{D\vartheta\log E^*K}{\log p}+gg_0(L+1)(a_1+a_2)+2g_0(L+1)\sqrt{ga_1a_2(K+1)}\\ &+\left(\frac{\vartheta}{2\log p}+2\right)g_0^{2/3}(2ga_1a_2D\log E^*)^{1/3}(L+1)(K+1)^{2/3}\left(3^{1/3}+\frac{1}{\Gamma^{1/3}}\right).\end{aligned}\tag{3.8.37}$$

Up to now, we have deduced the upper bound

$$\begin{aligned}\Xi<&\ \frac{DKH}{3\log p}+\frac{\eta K}{6}-\frac{2.23DK}{3\log p}+\Phi+\frac{D\vartheta\log E^*}{\log p}\left(\frac{L+1}{K+1}\right)\\ &+\frac{D}{\log p}\left(\frac{\omega_0\vartheta}{\omega}\log E^*+1+\log(L+1)\right)-\frac{\Theta(L+1)\eta}{2}.\end{aligned}\tag{3.8.38}$$

We rewrite the upper bound for Ξ in (3.8.38) as

$$\frac{D(K+1)H}{3\log p}+\frac{K\eta}{6}-\frac{2.23DK}{3\log p}+\Phi+\Omega,$$

where Φ is in (3.8.37) and

$$\Omega = -\frac{\Theta(L+1)\eta}{2} + \frac{D}{\log p}\left(-\frac{H}{3} + \frac{\omega_0\vartheta}{\omega}\log E^* + 1 + \log(L+1) + \vartheta\left(\frac{L+1}{K+1}\right)\log E^*\right). \tag{3.8.39}$$

We shall deduce a larger upper bound for Ξ than that stated above. We proceed by deducing that $\Omega < 0$ in the following lemma.

Lemma 3.28. *Let Φ and Ω be in* (3.8.37) *and* (3.8.39) *respectively. We have $\Omega < 0$ and*

$$\Xi < \frac{D(K+1)H}{3\log p} + \frac{K\eta}{6} - \frac{2.23DK}{3\log p} + \Phi. \tag{3.8.40}$$

Proof. First we note by using (3.8.2), (3.8.3) and (3.8.21) that $\Omega < \Omega_1 + \Omega_2$, where

$$\begin{aligned}\Omega_1 &= -\frac{\Theta(L+1)\eta}{2} + \frac{D}{\log p}\left(1.00011 + \log(C_1 H)\right) + \frac{\vartheta(L+1)}{C_0 g\log p},\\ \Omega_2 &= \frac{D}{\log p}\left(-\frac{H}{3} + \frac{\omega_0\vartheta}{\omega}\log E^* + \log\left(\frac{D}{\log p}\right)\right).\end{aligned}$$

To show that $\Omega_1 < 0$, we make use of (3.8.3), (3.8.21) and the fact that $\Theta \geq 0.2499$ by referring to (3.8.26) to verify that Ω_1 is a decreasing function in the variable C_1H. Then we deduce from (3.8.16) and (3.8.18) to get $\Omega_1 < 0$.

Next, we can show that $\Omega_2 < 0$ by using (3.8.1) and (3.8.16). This gives

$$\Omega_2 < \frac{D}{\log p}\left(-\frac{H}{3} + \frac{\omega_0\vartheta}{\omega}\log E^* + \log D - 0.47\right) < \frac{D}{\log p}\left(-150\log E^* + \log D - 0.47\right) < 0.$$

Thus, we have $\Omega < 0$ and Lemma 3.28 is proved. $\square$

As a last deduction to Ξ, we present the following Proposition, which gives an upper bound for $\frac{\Xi}{(K+1)(L+1)}$.

Proposition 3.4. *We have*

$$\begin{aligned}\frac{\Xi}{(K+1)(L+1)} &< \frac{1}{3C_1} + \frac{2g_0}{C_0 D\log E^*\min\{a_1,a_2\}} + \frac{\vartheta\log E^*}{C_1H} + \frac{\eta\log p}{6C_1DH} - \frac{2.2}{3C_1H} + \frac{2g_0}{(C_0D\log E^*)^{1/2}}\\ &\quad + \frac{\left(\frac{\vartheta}{2\log p}+2\right)g_0^{2/3}2^{1/3}}{C_0^{1/3}}\left(3^{1/3} + \left(\min\left\{\frac{C_1DH}{\log p}, \frac{1}{2}(C_0ga_1a_2D\log E^*)\right\}\right)^{-1/3}\right).\end{aligned}$$

Proof of Proposition 3.4. We begin with dividing (3.8.40) in Lemma 3.28 by $(K+1)(L+1)$ and then using the choices of K and L in (3.8.2) and (3.8.3) respectively to get

$$\frac{\Xi}{(K+1)(L+1)} < \frac{1}{3C_1} + \frac{\eta \log p}{6C_1DH} - \frac{2.2}{3C_1H} + \frac{\Phi}{(K+1)(L+1)}. \tag{3.8.41}$$

The result follows by adopting the definition of Φ in (3.8.37) and using again the choices of K and L in (3.8.2) and (3.8.3) respectively. □

Finally, we obtain a lower bound for the term $\frac{\Theta\eta}{2}$, which is actually the LHS of (3.8.28) divided by $(K+1)(L+1)$. This is simply done by referring to the definition of Θ in (3.8.26) and to the choice of L in (3.8.3). This yields

$$\frac{\Theta\eta}{2} \geq \frac{\eta}{16}\left(1 - \frac{\log p}{C_1DH} + \sqrt{1 - \frac{2\log p}{C_1DH}}\right). \tag{3.8.42}$$

We require that the lower bound for $\frac{\Theta\eta}{2}$ obtained in (3.8.42) supersedes the upper bound for $\frac{\Xi}{(K+1)(L+1)}$ obtained in Proposition 3.4. That is, we require that

$$\begin{aligned}
&\frac{\eta}{16}\left(1 - \frac{\log p}{C_1DH} + \sqrt{1 - \frac{2\log p}{C_1DH}}\right) - \frac{2g_0}{(C_0D\log E^*)^{1/2}} \\
&\quad - \frac{\left(\frac{\vartheta}{2\log p} + 2\right) g_0^{2/3} 2^{1/3}}{C_0^{1/3}} \left(3^{1/3} + \left(\min\left\{\frac{C_1DH}{\log p}, \frac{1}{2}(C_0 g a_1 a_2 D \log E^*)\right\}\right)^{-1/3}\right) \\
&\quad \geq \frac{1}{3C_1} + \frac{2g_0}{C_0 D \log E^* \min\{a_1, a_2\}} + \frac{\vartheta \log E^*}{C_1H} + \frac{\eta \log p}{6C_1DH} - \frac{2.2}{3C_1H}
\end{aligned} \tag{3.8.43}$$

holds. This would imply that Condition (1a) (i.e. (3.2.10)) in the Main Proposition holds. As a conclusion, for the case when $p \geq 5$, we have shown that under the choices and conditions of parameters in Section 3.8.1, (3.8.43) implies Condition (1a) (i.e. (3.2.10)) in the Main Proposition.

3.9 Proof of Theorem 3.1

In this section we assume that α_1 and α_2 are multiplicatively independent. We shall prove Theorem 3.1 by considering separately the following two cases:

Case 1 ($rb_2 + sb_1$ are all distinct):
For any class $c \mod g$ and for $i = 1, 2, 3$,

$$\begin{aligned}
&\mathrm{Card}\{rb_2 + sb_1; 0 \leq r \leq R_i, 0 \leq s \leq S_i, m_1r + m_2s \equiv c \mod g\} \\
&= \mathrm{Card}\{(r,s); 0 \leq r \leq R_i, 0 \leq s \leq S_i, m_1r + m_2s \equiv c \mod g\}.
\end{aligned} \tag{3.9.1}$$

Case 2 ($rb_2 + sb_1$ are not all distinct):
There exists a class c modulo g and a certain $i \in \{1,2,3\}$ such that

$$\begin{aligned} &\mathrm{Card}\,\{rb_2 + sb_1; 0 \le r \le R_i, 0 \le s \le S_i, m_1 r + m_2 s \equiv c \mod g\} \\ &< \mathrm{Card}\,\{(r,s); 0 \le r \le R_i, 0 \le s \le S_i, m_1 r + m_2 s \equiv c \mod g\}. \end{aligned} \tag{3.9.2}$$

3.9.1 Derivation for Case 1

Since α_1 and α_2 are multiplicatively independent, condition (3.2.6) can be rewritten as

$$\begin{aligned} T_1 &\ge K, \\ (R_1+1)(S_1+1) &\ge g \cdot \max\left\{K+1, \frac{L+1}{T_1+1}\right\}, \\ (R_2+1)(S_2+1) &\ge g \cdot \max\left\{\frac{2KL+1}{T_2+1}, \frac{K^2+1}{T_2+1}\right\}, \\ (R_3+1)(S_3+1) &\ge g \cdot \frac{(3K^2L+1)}{T_3+1}. \end{aligned} \tag{3.9.3}$$

These inequalities are clearly verified with our choice of parameters (3.8.2) to (3.8.12).

Next we adopt the following explicit expressions for parameters, which can be shown to fulfill conditions (3.8.13) to (3.8.18) and (3.2.8) trivially.

For $p = 2$ we take

$$\begin{aligned} C_0 = 8800, \qquad C_1 = 3.9, \qquad \log E^* &= \frac{1}{4}\left(\frac{2\log p}{D} + 4.85 + \log D\right), \\ H = \max\left\{\log\left(\frac{b_2}{a_1} + \frac{b_1}{a_2}\right), \frac{1000\log p}{D}, 180\left(\frac{2\log p}{D} + 4.85 + \log D\right)\log p\right\}, \end{aligned}$$

for $p = 3$ we take

$$\begin{aligned} C_0 = 8800, \qquad C_1 = 4.25, \qquad \log E^* &= \frac{1}{4}\left(\frac{3\log p}{2D} + 4.85 + \log D\right), \\ H = \max\left\{\log\left(\frac{b_2}{a_1} + \frac{b_1}{a_2}\right), \frac{1000\log p}{D}, 180\left(\frac{3\log p}{2D} + 4.85 + \log D\right)\log p\right\} \end{aligned}$$

and for $p \ge 5$ we take

$$\begin{aligned} C_0 &= 9500, \\ C_1 &= 11.6, \\ \log E^* &= \frac{1}{2}\left(\frac{\log p}{2D} + 4.85 + \log D\right), \\ H &= \max\left\{\log\left(\frac{b_2}{a_1} + \frac{b_1}{a_2}\right), \frac{1000\log p}{D}, 180\left(\frac{\log p}{2D} + 4.85 + \log D\right)\log p\right\}. \end{aligned} \tag{3.9.4}$$

Again we shall consider the case when $p \geq 5$. The derivation for the case of $p = 2$ and $p = 3$ are similar and shall be omitted.

It remains to show that the choices fulfill inequality (3.8.43), and hence Condition (1a) (i.e. (3.2.10)). We substitute all the parameters in (3.9.4) and (3.8.1) into both the LHS and RHS of inequality (3.8.43). Besides, notice that $\log E^* = \frac{1}{2}\left(\frac{\log p}{2D} + 4.85 + \log D\right) \geq \frac{1}{2}\left(\frac{\log 5}{2} + 4.85\right) \geq 2.827$, so that $H \geq \max\left\{\frac{1000 \log p}{D}, 360(2.827)\log p\right\}$. We get:

$$
\begin{aligned}
\text{LHS} \geq{}& \frac{\eta}{16}\left(1 - \frac{1}{1000C_1} + \sqrt{1 - \frac{2}{1000C_1}}\right) - \frac{2(0.239)}{(9500\,(2.827))^{1/2}} \\
&- \frac{\left(\frac{2.35}{2\log 5} + 2\right)0.239^{2/3}2^{1/3}}{9500^{1/3}}\left(3^{1/3} + \left(\min\left\{1000C_1, \frac{C_0 g}{2}\,(2.827)\right\}\right)^{-1/3}\right) \\
\geq{}& 0.0291
\end{aligned}
$$

$$
\begin{aligned}
\text{RHS} &\leq \frac{1}{3C_1} + \frac{2g_0}{C_0 \log E^*} + \frac{1}{360C_1(\log E^*)(\log p)}\left(\vartheta \log E^* + \frac{\eta \log p}{6D} - \frac{2.2}{3}\right) \\
&\leq \frac{1}{3C_1} + \frac{2g_0}{C_0 \log E^*} + \frac{1}{360C_1}\left(\frac{\vartheta}{\log p} - \frac{2.2}{3(\log E^*)(\log p)} + \frac{\eta}{6\log E^*}\right) \\
&\leq \frac{1}{3C_1} + \frac{2g_0}{C_0 \log E^*} + \frac{1}{360C_1}\left(\frac{1}{\log 5}\left(\vartheta - \frac{2.2}{3\log E^*}\right) + \frac{\eta}{6\log E^*}\right) \\
&= \frac{1}{3C_1} + \frac{1}{360C_1 \log E^*}\underbrace{\left(\frac{2(0.239)(360)(11.6)}{9500} - \frac{2.2}{3\log 5} + \frac{\eta}{6}\right)}_{<0} + \frac{\vartheta}{360C_1 \log 5} \\
&< 0.029086 \\
&< \text{LHS}
\end{aligned}
$$

Thus, (3.8.43) is fulfilled, which implies that Condition (1a) is fulfilled.

Note that p^u is the greatest power of p dividing both b_1 and b_2. Using $u \leq \frac{\log \min\{b_1, b_2\}}{\log p}$, the upper bound $\log b_1 \leq a_2 \max\left\{\log\left(\frac{b_1}{a_2}\right), 1\right\}$ and (3.8.13), we can obtain the upper bound of u as

$$
u \leq \frac{D^2}{(\log p)^3} \log A_1 \log A_2\, H. \tag{3.9.5}
$$

Finally, we refer to the lower bound for $|\Lambda|_p$ in (3.2.11), use (3.8.2), (3.8.3), (3.8.13), (3.9.4), (3.9.5), the fact that

$$
V = \frac{1}{4}\left(1 - \frac{1}{L+1} + \sqrt{1 - \frac{2}{L+1}}\right)(K+2)(L+1)\lambda < \frac{1}{2}(K+2)(L+1)\lambda
$$

and from (3.2.3) and (3.2.9) that

$$\lambda = \frac{\eta p^{\kappa}}{2e} \le \frac{\eta p}{p-1},$$

we get

$$\begin{aligned}
v_p(\Lambda) &< \frac{1}{2}(K+2)(L+1)\lambda + u \\
&\le \frac{1}{2}\left(\frac{9500 g D^3 \log A_1 \log A_2}{2(\log p)^2}\left(\frac{\log p}{2D} + 4.85 + \log D\right) + 2\right) \\
&\qquad \cdot \left(\frac{11.6 DH}{\log p} + 1\right)\frac{\eta p}{p-1} + \frac{D^2}{(\log p)^3}\log A_1 \log A_2\, H \\
&< \frac{1}{4}\cdot\frac{g\eta p}{p-1}(1.0001)(1.0001)(9500)(11.6)\left(1 + \frac{1}{150000}\right)\left(\frac{\log p}{2D} + 4.85 + \log D\right) \\
&\qquad \cdot \frac{D^4}{(\log p)^3}\log A_1 \log A_2\, H \\
&< 27600\left(\frac{p}{p-1}\right)\frac{gD^4}{(\log p)^3}\left(\frac{\log p}{2D} + 4.85 + \log D\right)\log A_1 \log A_2\, H.
\end{aligned}$$

Thus, Theorem 3.1 is proved for Case 1, $p \ge 5$.

3.9.2 Derivation for Case 2

We shall derive a stronger upper bound of $v_p(\Lambda)$ for Case 2 using Liouville's inequality, referring to the derivation in [33]. From (3.9.2), there exist at least two pairs $(r_1, s_1), (r_2, s_2)$ with $0 \le r_1, r_2 \le R_i$ and $0 \le s_1, s_2 \le S_i$ such that

$$\begin{aligned}
& b_2(r_1 - r_2) + b_1(s_1 - s_2) = 0 \\
\text{and} \quad & m_1(r_1 - r_2) + m_2(s_1 - s_2) \equiv c - c \equiv 0 \mod g.
\end{aligned}$$

Observe that $|r_1 - r_2| \le R_i \le R$ and $|s_1 - s_2| \le S_i \le S$, thus there is a pair of integers $(r_0, s_0) \ne (0,0)$ satisfying $|r_0| \le R_i \le R$ and $|s_0| \le S_i \le S$ with

$$r_0 b_2 + s_0 b_1 = 0, \qquad m_1 r_0 + m_2 s_0 \equiv 0 \mod g. \tag{3.9.6}$$

Let

$$r = \frac{r_0}{\gcd(r_0, s_0)}, \qquad s = \frac{s_0}{\gcd(r_0, s_0)}$$

in a way that

$$b_1 = nr, \qquad b_2 = -ns, \qquad n \in \mathbb{Z}.$$

Then we can write

$$\Lambda = \alpha_1^{b_1} - \alpha_2^{b_2} = \alpha_1^{nr} - \alpha_2^{-ns} = \alpha_2^{-ns}\left(\left(\frac{\alpha_1^r}{\alpha_2^{-s}}\right)^n - 1\right) = \prod_{\xi^n = 1}\left(\alpha_1^r - \xi\alpha_2^{-s}\right).$$

As $n = \gcd(b_1, b_2) = n' p^u$ with $(n', p) = 1$, Lemma 3.18 shows that

$$\sum_{\substack{\xi^n = 1 \\ \xi \neq 1}} v_p(\xi - 1) = u.$$

Proceeding as in the proof of Lemma 3.3, there exists a unique n-th root of unity μ such that

$$\begin{aligned} &v_p\left(\alpha_1^r - \mu\alpha_2^{-s}\right) \geq v_p(\Lambda) - u \\ &v_p\left(\alpha_1^r - \mu\alpha_2^{-s}\right) > v_p\left(\alpha_1^r - \xi\alpha_2^{-s}\right) \qquad (\xi^n = 1, \xi \neq \mu) \end{aligned} \tag{3.9.7}$$

since $v_p(\Lambda) > \frac{1}{p-1} + u$. Then, Lemma 3.19 shows that μ belongs to the field $\mathbb{Q}_p(\alpha_1^r \alpha_2^s) \subseteq K_v$. Consider that ζ is a root of unity of order exactly g. We can write $\mu = \zeta^m \xi$, for an integer m and a p^κ-th root of unity ξ. The reason is that the class in U_v/U_v^1 of the component of μ of order prime to p is generated by the classes of α_1 and α_2, and the order of the p-primary component of μ divides p^κ. Since $\xi \in U_v^1$ and that $v_p\left(\alpha_1^r - \mu\alpha_2^{-s}\right) > 0$, a reduction modulo U_v^1 implies the congruence

$$m_1 r \equiv -m_2 s + m \mod g.$$

Then,

$$m \times \gcd(r, s) \equiv m_1 r + m_2 s \equiv 0 \mod g.$$

Now, let $g' = \frac{g}{\gcd(m,g)}$. The congruence above shows that $\gcd(r, s)$ is divisible by g'. This gives the upper bound

$$|r| \leq \frac{R}{g'}, \qquad |s| \leq \frac{S}{g'}.$$

We apply the Liouville's inequality to the polynomial $X - Y$ and obtain

$$\begin{aligned} \log|\alpha_1^r - \mu\alpha_2^{-s}|_p &\geq -\frac{[\mathbb{Q}(\alpha_1, \alpha_2, \mu) : \mathbb{Q}]}{[\mathbb{Q}_p(\alpha_1, \alpha_2, \mu) : \mathbb{Q}_p]}\left(\log 2 + \frac{R}{g'}h(\alpha_1) + \frac{S}{g'}h(\alpha_2)\right) \\ &\geq -\frac{[\mathbb{Q}(\alpha_1, \alpha_2, \mu) : \mathbb{Q}]}{ef}\left(\log 2 + \frac{R}{g'}h(\alpha_1) + \frac{S}{g'}h(\alpha_2)\right). \end{aligned}$$

Furthermore, ζ^m is the root of unity of order exactly g'. We have the upper bound

$$\frac{[\mathbb{Q}(\alpha_1, \alpha_2, \mu) : \mathbb{Q}]}{ef} \leq \frac{[\mathbb{Q}(\alpha_1, \alpha_2) : \mathbb{Q}] \times [\mathbb{Q}(\zeta^m) : \mathbb{Q}] \times [\mathbb{Q}(\xi) : \mathbb{Q}]}{ef} \leq \frac{Dg' p^{\kappa-1}(p-1)}{e} \leq 2Dg.$$

By (3.8.13), we get

$$\begin{aligned} \log|\alpha_1^r - \mu\alpha_2^{-s}|_p &\geq -2Dg\left(\log 2 + \frac{R}{g'}h(\alpha_1) + \frac{S}{g'}h(\alpha_2)\right) \\ &\geq -2\left(\frac{gD\log 2}{\log p} + \frac{D}{\log p}Rh(\alpha_1) + \frac{D}{\log p}Sh(\alpha_2)\right)\log p \\ &\geq -2\left(\frac{gD\log 2}{\log p} + Ra_1 + Sa_2\right)\log p. \end{aligned}$$

Using (3.8.2), (3.8.14) and (3.8.36),

$$\begin{aligned}
&\log|\alpha_1^r - \mu\alpha_2^{-s}|_p \\
\geq & -2\left(\frac{gD\log 2}{\log p} + 2g^{1/3}(K+1)\left(g^{1/6}\sqrt{\frac{a_1a_2}{K+1}} + \left(\frac{2D\log E^* a_1a_2}{g_0(K+1)}\right)^{1/3}\left(3^{1/3} + \frac{1}{\Gamma^{1/3}}\right)\right)\right)\log p \\
\geq & -2(K+1)\left(\frac{gD\log 2}{(K+1)\log p} + 2\left(\frac{1}{\sqrt{D\log E^* C_0}} + \left(\frac{2}{g_0C_0}\right)^{1/3}\left(3^{1/3} + \frac{1}{\Gamma^{1/3}}\right)\right)\right)\log p.
\end{aligned}$$

By (3.8.1), (3.8.2), (3.8.13), (3.8.17), (3.8.19), (3.8.20) and (3.8.21),

$$\frac{gD\log 2}{(K+1)\log p} + 2\left(\frac{1}{\sqrt{D\log E^* C_0}} + \left(\frac{2}{g_0C_0}\right)^{1/3}\left(3^{1/3} + \frac{1}{\Gamma^{1/3}}\right)\right) < 1.$$

Thus,

$$v_p\left(\alpha_1^r - \mu\alpha_2^{-s}\right) < 2(K+1).$$

Together with (3.9.7) we get the result

$$v_p(\Lambda) \leq v_p\left(\alpha_1^r - \mu\alpha_2^{-s}\right) + u < 2(K+1) + u. \tag{3.9.8}$$

However, the upper bound for Case 2 in (3.9.8) is obviously stronger than that obtained in Case 1, i.e.

$$v_p(\Lambda) < V + u < \frac{1}{2}(K+2)(L+1)\lambda + u.$$

As a conclusion, Theorem 3.1 is proved for the case when $p \geq 5$. The deduction for $p = 2$ and $p = 3$ are similar and therefore omitted.

3.10 Proof of variants of Theorem 3.1

By applying the Main Proposition, we can obtain various theorems by having proper choice of parameters and the values of intermediate constants within the derivation.

The values 1000 and 180 in the expression of H of Theorem 3.1 can be changed and the value of C in the upper bound will be changed accordingly. In fact, if we change the values 1000 and 180 in the expression of H of Theorem 3.1, we can use the same derivations as before to obtain new values for (3.8.1) and other intermediate inequalities correspondingly. Then we use new choices for C_0, C_1 in (3.9.4) and go through the derivations thereafter.

As an illustration for the case when $p \geq 5$, we shall give a list of the modifications to the values of the parameters/intermediate constants in each scenario and state the corresponding variants obtained in Table 3.1. Here,

$$H = \max\left\{\log b' + \log\log p, \frac{x_1\log p}{D}, x_2\left(\frac{\log p}{2D} + 4.85 + \log D\right)\log p\right\}$$

and

$$v_p(\Lambda) < C_2 \cdot \frac{p}{(p-1)} \frac{gD^4}{(\log p)^3} \left(\frac{\log p}{2D} + 4.85 + \log D \right) \log A_1 \log A_2 \, H.$$

The derivations are very similar to the previous sections and we shall omit the derivations here.

Table 3.1: Summary of results for the case when $p \geq 5$

x_1	x_2	C_0	C_1	C_2	**Remark**
650	120	9450	11.93	28200	
850	150	9500	11.7	27800	
1000	180	9500	11.6	27600	This is Theorem 3.1 when $p \geq 5$.
5000	900	9500	11.49	27300	
10000	1800	9500	11.45	27210	
15000	2700	9500	11.42	27140	

We have a rough estimation that the value of C in the upper bound of Theorem 3.1 for the case when $p \geq 5$ can be reduced to roughly 27100 when H is asymptotically large.

Remark: For simplicity in comparison, the value of C_0 is kept almost unchanged so that the expression $\frac{\log p}{2D} + 4.85 + \log D$ is unchanged. In fact, if C_0 is reduced, the value 4.85 in the expression will be reduced and vice versa. The value of C_2 may be reduced with more flexible choices of C_0 and C_1.

Chapter 4

On a variant of Pillai's problem

The content of this chapter is the same as the joint paper with István Pink and Volker Ziegler [36], which is published in the International Jounal of Number Theory.[1]

4.1 Introduction

Pillai's famous conjecture first formulated in [71] states that the Diophantine equation

$$a^x - b^y = c \tag{4.1.1}$$

has for any fixed integer $c > 0$ at most finitely many solutions a, b, x, y in positive integers. This conjecture is still open for all $c \neq 1$. Note that the case $c = 1$ is Catalan's conjecture which has been solved by Mihăilescu [67]. If we leave a, b and c fixed, then much more is known about the solutions (x, y). For instance Pillai [71] showed that if c is larger than some constant depending on a and b, then Diophantine equation (4.1.1) has at most one solution. In particular, he conjectured that in the case that $a = 3$ and $b = 2$ Diophantine equation (4.1.1) has at most one solution if $c > 13$. This conjecture was confirmed by Stroeker and Tijdeman [87] and their result was further improved by Bennett [21], who showed that for fixed a, b and c equation (4.1.1) has at most two solutions.

Recently Ddamulira, Luca and Rakotomalala [39] considered the Diophantine equation

$$F_n - 2^m = c, \tag{4.1.2}$$

where c is a fixed integer and $\{F_n\}_{n\geq 0}$ is the sequence of Fibonacci numbers given by $F_0 = 0$, $F_1 = 1$ and $F_{n+2} = F_{n+1} + F_n$ for all $n \geq 0$. This type of equation can be seen as a variation

[1] K. C. Chim was supported by the Austrian Science Fund (FWF) under the projects P24574, P26114 and W1230. I. Pink and V. Ziegler were supported by the Austrian Science Fund (FWF) under the project P 24801-N26.

of Pillai's equation. However Ddamulira *et al.* proved that the only integers c having at least two representations of the form $F_n - 2^m$ are contained in the set $\mathcal{C} = \{0, -1, 1, -3, 5, -11, -30, 85\}$. Moreover, they computed for all $c \in \mathcal{C}$ all representations of the form (4.1.2).

The purpose of this paper is to consider a related problem. Denote by $\{T_m\}_{m\geq 0}$ the sequence of Tribonacci numbers given by $T_0 = 0$, $T_1 = T_2 = 1$ and $T_{m+3} = T_{m+2} + T_{m+1} + T_m$ for all $m \geq 0$. The main result of our paper is to find all integers c admitting at least two representations of the form $F_n - T_m$ for some positive integers n and m. It is assumed that representations with $n \in \{1, 2\}$ (for which $F_1 = F_2 = 1$) as well as representations with $m \in \{1, 2\}$ (for which $T_1 = T_2$) count as one representation to avoid trivial parametric families such as $1 - 1 = F_1 - T_1 = F_2 - T_1 = F_1 - T_2 = F_2 - T_2$. Therefore we assume that $n \geq 2$ and $m \geq 2$. We prove the following theorem:

Theorem 4.1. *The only integers c having at least two representations of the form $F_n - T_m$ come from the set*

$$\mathcal{C} = \{0, 1, -1, -2, -3, 4, -5, 6, 8, -10, 11, -11, -22, -23, -41, -60, -271\}.$$

Furthermore, for each $c \in \mathcal{C}$ all representations of the form $c = F_n - T_m$ with integers $n \geq 2$ and $m \geq 2$ are:

$$\begin{aligned}
0 &= 1 - 1 = 2 - 2 = 13 - 13 \ (= F_2 - T_2 = F_3 - T_3 = F_7 - T_6),\\
1 &= 2 - 1 = 3 - 2 = 5 - 4 = 8 - 7 \ (= F_3 - T_2 = F_4 - T_3 = F_5 - T_4 = F_6 - T_5),\\
-1 &= 1 - 2 = 3 - 4 \ (= F_2 - T_3 = F_4 - T_4),\\
-2 &= 2 - 4 = 5 - 7 \ (= F_3 - T_4 = F_5 - T_5),\\
-3 &= 1 - 4 = 21 - 24 \ (= F_2 - T_4 = F_8 - T_7),\\
4 &= 5 - 1 = 8 - 4 \ (= F_5 - T_2 = F_6 - T_4),\\
-5 &= 2 - 7 = 8 - 13 = 144 - 149 \ (= F_3 - T_5 = F_6 - T_6 = F_{12} - T_{10}),\\
6 &= 8 - 2 = 13 - 7 \ (= F_6 - T_3 = F_7 - T_5),\\
8 &= 21 - 13 = 89 - 81 \ (= F_8 - T_6 = F_{11} - T_9),\\
-10 &= 3 - 13 = 34 - 44 \ (= F_4 - T_6 = F_9 - T_8),\\
11 &= 13 - 2 = 55 - 44 \ (= F_7 - T_3 = F_{10} - T_8),\\
-11 &= 2 - 13 = 13 - 24 \ (= F_3 - T_6 = F_7 - T_7),\\
-22 &= 2 - 24 = 121393 - 121415 \ (= F_3 - T_7 = F_{26} - T_{21}),\\
-23 &= 1 - 24 = 21 - 44 \ (= F_2 - T_7 = F_8 - T_8),\\
-41 &= 3 - 44 = 233 - 274 \ (= F_4 - T_8 = F_{13} - T_{11}),\\
-60 &= 21 - 81 = 89 - 149 \ (= F_8 - T_9 = F_{11} - T_{10}),\\
-271 &= 3 - 274 = 233 - 504 \ (= F_4 - T_{11} = F_{13} - T_{12}).
\end{aligned}$$

4.2 Preliminaries

In this section, the result of linear forms in logarithms by Baker and Wüstholz [19] is stated. Besides, we state a lemma from [30], which is a slight variation of a result due to Dujella and Pethő [42], of which is a generalization of a result due to Baker and Davenport [17]. Both results will be used in the proof of Theorem 4.1.

4.2.1 A lower bound for linear forms in logarithms of algebraic numbers

In 1993, Baker and Wüstholz [19] obtained an explicit bound for linear forms in logarithms with a linear dependence on $\log B$, where $B \geq e$ denotes an upper bound for the height of the linear form (to be defined later in this section). It is a vast improvement compared with lower bounds with a dependence on higher powers of $\log B$ in preceding publications by other mathematicians in particular Baker's original results [1, 2, 3]. The final structure for the lower bound for linear forms in logarithms without an explicit determination of the constant involved has been established by Wüstholz [93] and the precise determination of that constant (which is denoted as $C(n,d)$ in [19] and later in this section as $C(k,d)$) is the central aspect of [19] (see also [20]). The improvement was mainly due to the use of the analytic subgroup theorem established by Wüstholz [94]. We shall now state the result of Baker and Wüstholz.

Denote by $\alpha_1, \ldots, \alpha_k$ algebraic numbers, not 0 or 1, and by $\log \alpha_1, \ldots, \log \alpha_k$ a fixed determination of their logarithms. Let $K = \mathbb{Q}(\alpha_1, \ldots, \alpha_k)$ and let $d = [K : \mathbb{Q}]$ be the degree of K over $\mathbb{Q}$. For any $\alpha \in K$, suppose that its minimal polynomial over the integers is

$$g(x) = a_0 x^{\delta} + a_1 x^{\delta - 1} + \cdots + a_{\delta} = a_0 \prod_{j=1}^{\delta} (x - \alpha^{(j)})$$

where $\alpha^{(j)}$ are all the roots of $g(x)$. The absolute logarithmic Weil height of α is defined as

$$h_0(\alpha) = \frac{1}{\delta} \left(\log |a_0| + \sum_{j=1}^{\delta} \log \left(\max\{|\alpha^{(j)}|, 1\} \right) \right).$$

Then the modified height $h'(\alpha)$ is defined by

$$h'(\alpha) = \frac{1}{d} \max\{h(\alpha), |\log \alpha|, 1\},$$

where $h(\alpha) = d h_0(\alpha)$ is the standard logarithmic Weil height of α.

Let us consider the linear form

$$L(z_1, \ldots, z_k) = b_1 z_1 + \cdots + b_k z_k,$$

where $b_1, \dots, b_k$ are rational integers, not all 0 and define

$$h'(L) = \frac{1}{d} \max\{h(L), 1\},$$

where $h(L) = d \log \left(\max_{1 \le j \le k} \left\{ \frac{|b_j|}{b} \right\} \right)$ is the logarithmic Weil height of L, where b is the greatest common divisor of $b_1, \dots, b_k$. If we write $B = \max\{|b_1|, \dots, |b_k|, e\}$, then we get

$$h'(L) \le \log B.$$

With these notations we are able to state the following result due to Baker and Wüstholz [19].

Theorem 4.2. *If $\Lambda = L(\log \alpha_1, \dots, \log \alpha_k) \neq 0$, then*

$$\log |\Lambda| \ge -C(k, d) h'(\alpha_1) \cdots h'(\alpha_k) h'(L),$$

where

$$C(k, d) = 18(k+1)!\, k^{k+1} (32d)^{k+2} \log(2kd).$$

With $|\Lambda| \le \frac{1}{2}$, we have $\frac{1}{2}|\Lambda| \le |\Phi| \le 2|\Lambda|$, where

$$\Phi = e^{\Lambda} - 1 = \alpha_1^{b_1} \cdots \alpha_k^{b_k} - 1,$$

so that

$$\log |\alpha_1^{b_1} \cdots \alpha_k^{b_k} - 1| \ge \log |\Lambda| - \log 2.$$

We apply Theorem 4.2 mainly in a situation where $k = 3$ and $d = 6$. In this case

$$C(3, 6) = 18(4!) 3^4 (32 \times 6)^5 (\log 36) \approx 3.2718 \ldots \times 10^{16}.$$

We will use this value throughout the paper without any further reference.

4.2.2 A generalized result of Baker and Davenport

The following result will be used to reduce the huge upper bounds for n and m which appear during the course of the proof of Theorem 4.1 (cf. Proposition 4.1). It is [30, Lemma 4], which is regarded as a slight variation of a result due to Dujella and Pethő [42], of which is a generalization of a result due to Baker and Davenport [17]. For a real number x, let $\|x\| = \min\{|x - n| : n \in \mathbb{Z}\}$ be the distance from x to the nearest integer.

Lemma 4.3. *Let M be a positive integer, let p/q be a convergent of the continued fraction of the irrational τ such that $q > 6M$, and let A, B, μ be some real numbers with $A > 0$ and $B > 1$. Let $\varepsilon := \|\mu q\| - M\|\tau q\|$. If $\varepsilon > 0$, then there is no solution to the inequality*

$$0 < m\tau - n + \mu < AB^{-k},$$

in positive integers m, n and k with

$$m \leq M \qquad \text{and} \qquad k \geq \frac{\log(Aq/\varepsilon)}{\log B}.$$

4.3 Proof of Theorem 4.1

4.3.1 Set up

Assume that $(n, m) \neq (n_1, m_1)$ are pairs of indices such that

$$F_n - F_{n_1} = T_m - T_{m_1}. \tag{4.3.1}$$

We may assume that $m \neq m_1$, since otherwise $(n, m) = (n_1, m_1)$. Furthermore we assume that $m > m_1$. Due to equation (4.3.1) and since the right hand side of equation (4.3.1) is positive, we get that the left hand side of equation (4.3.1) is also positive and thus $n > n_1$. Therefore, we have $n \geq 3$, $n_1 \geq 2$ and $m \geq 3$, $m_1 \geq 2$.

During the proof of Theorem 4.1 we use the Binet formulae for the Fibonacci sequence and Tribonacci sequence in the following form:

Fibonacci sequence:

$$F_k = \frac{\alpha^k - \beta^k}{\alpha - \beta} \quad \text{for all } k \geq 0,$$

where $\alpha = \frac{1+\sqrt{5}}{2}$ and $\beta = \frac{1-\sqrt{5}}{2}$ are the roots of the characteristic equation $x^2 - x - 1 = 0$. Besides, the inequality

$$\alpha^{k-2} \leq F_k \leq \alpha^{k-1}$$

holds for all $k \geq 1$.

Tribonacci sequence:

$$T_k = c_\alpha \alpha_T^k + c_\beta \beta_T^k + c_\gamma \gamma_T^k \quad \text{for all } k \geq 0,$$

where α_T, β_T and γ_T are the roots of the characteristic equation $x^3 - x^2 - x - 1 = 0$, with

$$\alpha_T = \frac{1}{3}\left(1 + \sqrt[3]{19 + 3\sqrt{33}} + \sqrt[3]{19 - 3\sqrt{33}}\right),$$
$$\beta_T = \frac{1}{6}\left(2 - \sqrt[3]{19 + 3\sqrt{33}} - \sqrt[3]{19 - 3\sqrt{33}}\right) + \frac{\sqrt{3}}{6}i\left(\sqrt[3]{19 + 3\sqrt{33}} - \sqrt[3]{19 - 3\sqrt{33}}\right),$$
$$\gamma_T = \frac{1}{6}\left(2 - \sqrt[3]{19 + 3\sqrt{33}} - \sqrt[3]{19 - 3\sqrt{33}}\right) - \frac{\sqrt{3}}{6}i\left(\sqrt[3]{19 + 3\sqrt{33}} - \sqrt[3]{19 - 3\sqrt{33}}\right),$$

and the coefficients

$$c_\alpha = \frac{\alpha_T}{(\alpha_T - \beta_T)(\alpha_T - \gamma_T)} = \frac{1}{-\alpha_T^2 + 4\alpha_T - 1},$$
$$c_\beta = \frac{\beta_T}{(\beta_T - \alpha_T)(\beta_T - \gamma_T)} = \frac{1}{-\beta_T^2 + 4\beta_T - 1},$$
$$c_\gamma = \frac{\gamma_T}{(\gamma_T - \alpha_T)(\gamma_T - \beta_T)} = \frac{1}{-\gamma_T^2 + 4\gamma_T - 1}$$

are the roots of the polynomial $44x^3 - 2x - 1$. Note that

$$\begin{array}{ll} 1.839 < \alpha_T < 1.840 & 0.336 < c_\alpha < 0.337 \\ \beta_T = \overline{\gamma_T} & 0.737 < |\beta_T| = |\gamma_T| < 0.738 \\ c_\beta = \overline{c_\gamma} & 0.259 < |c_\beta| = |c_\gamma| < 0.260. \end{array}$$

Finally let us state several useful inequalities. For instance

$$\alpha_T^{k-2} \le T_k \le \alpha_T^{k-1} \quad \text{for all } k \ge 1.$$

which was already shown in [29]. Using equation (4.3.1) we get that

$$\alpha^{n-4} \le F_{n-2} \le F_n - F_{n_1} = T_m - T_{m_1} < T_m \le \alpha_T^{m-1}, \tag{4.3.2}$$

and similarly we get

$$\alpha^{n-1} \ge F_n > F_n - F_{n_1} = T_m - T_{m_1} \ge T_m - T_{m-1} = T_{m-2} + T_{m-3} \ge \alpha_T^{m-4} + \alpha_T^{m-5} > 2.83\alpha_T^{m-5}. \tag{4.3.3}$$

Thus

$$n - 4 < \frac{\log \alpha_T}{\log \alpha}(m-1) \quad \text{and} \quad n - 3 > \frac{\log \alpha_T}{\log \alpha}(m-5), \tag{4.3.4}$$

where $\dfrac{\log \alpha_T}{\log \alpha} \approx 1.2663\ldots$.

Inequality (4.3.4) implies that if $n < 300$, then $m < 240$. By a brute force computer enumeration for $2 \le n_1 < n < 300$ and $2 \le m_1 < m < 240$ we found all solutions listed in Theorem 4.1. Thus we may assume from now on that $n \ge 300$.

4.3.2 Linear forms in logarithms

Since $n \geq 300$, by the first inequality of (4.3.4) we obtain that $m \geq 235$ which combined with the second inequality of (4.3.4) implies that $n > m$. Moreover, we have

$$\frac{\alpha^n - \beta^n}{\sqrt{5}} - \frac{\alpha^{n_1} - \beta^{n_1}}{\sqrt{5}} = \left(c_\alpha \alpha_T^m + c_\beta \beta_T^m + c_\gamma \gamma_T^m\right) - \left(c_\alpha \alpha_T^{m_1} + c_\beta \beta_T^{m_1} + c_\gamma \gamma_T^{m_1}\right).$$

Collecting the "large" terms on the left hand side of the equation we obtain

$$\begin{aligned}\left|\frac{\alpha^n}{\sqrt{5}} - c_\alpha \alpha_T^m\right| &= \left|\frac{\beta^n}{\sqrt{5}} + \frac{\alpha^{n_1} - \beta^{n_1}}{\sqrt{5}} + \left(c_\beta \beta_T^m + c_\gamma \gamma_T^m\right) - \left(c_\alpha \alpha_T^{m_1} + c_\beta \beta_T^{m_1} + c_\gamma \gamma_T^{m_1}\right)\right| \\ &\leq \frac{\alpha^{n_1}}{\sqrt{5}} + c_\alpha \alpha_T^{m_1} + \frac{|\beta|^n}{\sqrt{5}} + \frac{|\beta|^{n_1}}{\sqrt{5}} + |c_\beta|\,|\beta_T|^m + |c_\gamma|\,|\gamma_T|^m + |c_\beta|\,|\beta_T|^{m_1} + |c_\gamma|\,|\gamma_T|^{m_1} \\ &< \frac{\alpha^{n_1}}{\sqrt{5}} + c_\alpha \alpha_T^{m_1} + 0.46 \\ &< 0.92 \max\{\alpha^{n_1}, \alpha_T^{m_1}\}.\end{aligned}$$

Dividing by $c_\alpha \alpha_T^m$ we get

$$\begin{aligned}\left|(\sqrt{5}c_\alpha)^{-1}\alpha^n \alpha_T^{-m} - 1\right| &< \max\left\{\frac{0.92}{c_\alpha \alpha_T^m}\alpha^{n_1}, \frac{0.92}{c_\alpha}\alpha_T^{m_1-m}\right\} \\ &< \max\left\{2.74\frac{\alpha^{n_1}}{\alpha_T}\frac{1}{\alpha^{n-4}}, 2.74\alpha_T^{m_1-m}\right\}.\end{aligned}$$

Hence we obtain the inequality

$$\left|(\sqrt{5}c_\alpha)^{-1}\alpha^n \alpha_T^{-m} - 1\right| < \max\{\alpha^{n_1-n+5}, \alpha_T^{m_1-m+2}\}. \tag{4.3.5}$$

Let us introduce

$$\Lambda = n \log \alpha - m \log \alpha_T - \log(\sqrt{5}c_\alpha)$$

and assume that $|\Lambda| \leq 0.5$. Further, we put

$$\Phi = e^\Lambda - 1 = (\sqrt{5}c_\alpha)^{-1}\alpha^n \alpha_T^{-m} - 1$$

and use the theorem of Baker and Wüstholz (Theorem 4.2) with the data

$$k = 3, \quad \alpha_1 = \sqrt{5}c_\alpha, \quad b_1 = -1, \quad \alpha_2 = \alpha, \quad b_2 = n, \quad \alpha_3 = \alpha_T, \quad b_3 = -m.$$

With this data we have $K = \mathbb{Q}(\sqrt{5}, \alpha_T)$, i.e. $d = 6$, and $B = n$. Notice that the minimal polynomial of α_1 is $1936x^6 - 880x^4 + 100x^2 - 125$, and we conclude that $h'(\alpha_1) = \frac{1}{6}\log 1936$. Further we obtain by a simple computation that $h'(\alpha_2) = \frac{1}{2}\log\alpha$ and $h'(\alpha_3) = \frac{1}{3}\log\alpha_T$.

Before we can apply Theorem 4.2 we have to show that $\Phi \neq 0$. Assume to the contrary that $\Phi = 0$, then $\alpha^n(\alpha_T^{-1})^m = \sqrt{5}c_\alpha$. But $\alpha^n(\alpha_T^{-1})^m \in \mathcal{O}_K$ whereas $\sqrt{5}c_\alpha$ does not, as can be observed immediately from its minimal polynomial. Thus $\Phi = 0$ is impossible.

Theorem 4.2 yields

$$\log|\Phi| \geq -C(3,6)\left(\frac{1}{6}\log 1936\right)\left(\frac{1}{2}\log\alpha\right)\left(\frac{1}{3}\log\alpha_T\right)\log n - \log 2$$

and together with inequality (4.3.5) we have

$$\min\{(n-n_1-5)\log\alpha, (m-m_1-2)\log\alpha_T\} \leq 2.02\times 10^{15}\log n.$$

Thus we have proved so far:

Lemma 4.4. *Assume that (n,m,n_1,m_1) is a solution to equation (4.3.1) with $m > m_1$. Then we have*

$$\min\{(n-n_1)\log\alpha, (m-m_1)\log\alpha_T\} < 2.03\times 10^{15}\log n.$$

Note that in the case that $|\Lambda| > 0.5$ inequality (4.3.5) is possible only if either $n-n_1 \leq 5$ or $m-m_1 \leq 2$, which is covered by the bound provided by Lemma 4.4.

Now we have to distinguish between the following two cases:

Case 1. Let us assume that

$$\min\{(n-n_1)\log\alpha, (m-m_1)\log\alpha_T\} = (n-n_1)\log\alpha.$$

We rewrite equation (4.3.1) as

$$\begin{aligned}\left|\frac{\alpha^n-\alpha^{n_1}}{\sqrt{5}} - c_\alpha\alpha_T^m\right| &= \left|-c_\alpha\alpha_T^{m_1} + \frac{\beta^n}{\sqrt{5}} - \frac{\beta^{n_1}}{\sqrt{5}} + \left(c_\beta\beta_T^m + c_\gamma\gamma_T^m\right) - \left(c_\beta\beta_T^{m_1} + c_\gamma\gamma_T^{m_1}\right)\right| \\ &\leq c_\alpha\alpha_T^{m_1} + \frac{|\beta^n|}{\sqrt{5}} + \frac{|\beta^{n_1}|}{\sqrt{5}} + |c_\beta|\,|\beta_T^m| + |c_\gamma|\,|\gamma_T^m| + |c_\beta|\,|\beta_T^{m_1}| + |c_\gamma|\,|\gamma_T^{m_1}|\end{aligned}$$

and obtain that

$$\left|\frac{\alpha^{n-n_1}-1}{\sqrt{5}}\alpha^{n_1} - c_\alpha\alpha_T^m\right| < (c_\alpha + 0.14)\alpha_T^{m_1}.$$

Dividing by $c_\alpha\alpha_T^m$ we get the inequality

$$\left|\frac{\alpha^{n-n_1}-1}{\sqrt{5}c_\alpha}\alpha^{n_1}\alpha_T^{-m} - 1\right| < 1.42\alpha_T^{m_1-m}. \tag{4.3.6}$$

Case 2. Let us assume that

$$\min\{(n-n_1)\log\alpha, (m-m_1)\log\alpha_T\} = (m-m_1)\log\alpha_T.$$

We rewrite equation (4.3.1) as

$$\begin{aligned}\left|\frac{\alpha^n}{\sqrt{5}} - c_\alpha \alpha_T^m + c_\alpha \alpha_T^{m_1}\right| &= \left|\frac{\beta^n}{\sqrt{5}} + \frac{\alpha^{n_1} - \beta^{n_1}}{\sqrt{5}} + c_\beta \beta_T^m + c_\gamma \gamma_T^m - c_\beta \beta_T^{m_1} - c_\gamma \gamma_T^{m_1}\right| \\ &\leq \frac{|\beta^n|}{\sqrt{5}} + \frac{\alpha^{n_1}}{\sqrt{5}} + \frac{|\beta^{n_1}|}{\sqrt{5}} + \left|c_\beta\right| |\beta_T^m| + |c_\gamma| |\gamma_T^m| + \left|c_\beta\right| \left|\beta_T^{m_1}\right| + |c_\gamma| \left|\gamma_T^{m_1}\right|.\end{aligned}$$

Thus we get

$$\left|\alpha^n - \sqrt{5} c_\alpha (\alpha_T^{m-m_1} - 1)\alpha_T^{m_1}\right| < 1.4\alpha^{n_1}.$$

Dividing both sides by $\sqrt{5}c_\alpha(\alpha_T^{m-m_1} - 1)\alpha_T^{m_1}$ we get by using (4.3.2) the following inequality:

$$\left|\frac{\alpha^n \alpha_T^{-m_1}}{\sqrt{5}\, c_\alpha (\alpha_T^{m-m_1} - 1)} - 1\right| < \frac{1.4}{\sqrt{5}\, c_\alpha (1 - \alpha_T^{m_1 - m})\alpha_T} \frac{\alpha^{n_1}}{\alpha_T^{m-1}} < 2.22\alpha^{n_1 - n + 4}. \tag{4.3.7}$$

We want to apply Theorem 4.2 to both inequalities (4.3.6) and (4.3.7) respectively. Let us consider the first case more closely. We write

$$\varLambda_1 = n_1 \log \alpha - m \log \alpha_T + \log\left(\frac{\alpha^{n-n_1} - 1}{\sqrt{5} c_\alpha}\right)$$

and assume that $|\varLambda_1| \leq 0.5$. Further, we put

$$\varPhi_1 = e^{\varLambda_1} - 1 = \frac{\alpha^{n-n_1} - 1}{\sqrt{5} c_\alpha} \alpha^{n_1} \alpha_T^{-m} - 1$$

and aim to apply Theorem 4.2 by taking $K = \mathbb{Q}(\sqrt{5}, \alpha_T)$, i.e. $d = 6$, $k = 3$ and $B = n$. Further, we have

$$\alpha_1 = \frac{\alpha^{n-n_1} - 1}{\sqrt{5} c_\alpha}, \quad b_1 = 1, \quad \alpha_2 = \alpha, \quad b_2 = n_1, \quad \alpha_3 = \alpha_T, \quad b_3 = -m.$$

Let us estimate the height of α_1. Notice that $h(\alpha_1) \leq h(\eta_1) + h(\eta_2)$, where $\eta_1 = \frac{\alpha^{n-n_1} - 1}{\sqrt{5}}$ and $\eta_2 = \frac{1}{c_\alpha}$. The minimal polynomial of η_1 divides (e.g. see [39])

$$5X^2 - 5F_{n-n_1} X - ((-1)^{n-n_1} + 1 - L_{n-n_1}),$$

where $\{L_k\}_{k \geq 0}$ is the Lucas companion sequence of the Fibonacci sequence given by $L_0 = 2, L_1 = 1, L_{k+2} = L_{k+1} + L_k$ for $k \geq 0$. Its Binet formula for the general term is $L_k = \alpha^k + \beta^k$ for all $k \geq 0$. Thus (cf. [39]),

$$h_0(\eta_1) \leq \frac{1}{2}\left(\log 5 + \log\left(\frac{\alpha^{n-n_1} + 1}{\sqrt{5}}\right)\right).$$

Thus Lemma 4.4 yields an upper bound

$$h_0(\eta_1) < \frac{1}{2} \log\left(2\sqrt{5}\alpha^{n-n_1}\right) < \frac{1}{2}(n - n_1 + 4) \log \alpha < 1.02 \times 10^{15} \log n,$$

i.e. $h(\eta_1) < 6 \times 1.02 \times 10^{15} \log n$. Since $h_0(\eta_2) = h_0(c_\alpha) = \frac{1}{3}\log 44$, i.e. $h(\eta_2) = 2\log 44$, we have $h(\alpha_1) \le 6 \times 1.02 \times 10^{15} \log n + 2\log 44$ and finally we obtain that

$$h'(\alpha_1) < 1.03 \times 10^{15} \log n.$$

Moreover, we have that $h'(\alpha_2) = \frac{1}{2}\log\alpha$ and $h'(\alpha_3) = \frac{1}{3}\log\alpha_T$ as before.

Now let us turn to the second case. We write

$$\Lambda_2 = n\log\alpha - m_1\log\alpha_T - \log\left(\sqrt{5}\,c_\alpha(\alpha_T^{m-m_1} - 1)\right)$$

and assume that $|\Lambda_2| \le 0.5$. Further, we put

$$\Phi_2 = e^{\Lambda_2} - 1 = (\sqrt{5}\,c_\alpha(\alpha_T^{m-m_1} - 1))^{-1}\alpha^n\alpha_T^{-m_1} - 1$$

and aim to apply Theorem 4.2. As in the previous case we take $K = \mathbb{Q}(\sqrt{5}, \alpha_T)$, i.e. $d = 6$, $k = 3$ and $B = n$. Further, we have

$$\alpha_1 = \sqrt{5}\,c_\alpha(\alpha_T^{m-m_1} - 1), \quad b_1 = -1, \quad \alpha_2 = \alpha, \quad b_2 = n, \quad \alpha_3 = \alpha_T, \quad b_3 = -m_1.$$

Again, we have to estimate $h(\alpha_1)$ and therefore note that $h(\alpha_1) \le h(\eta_1) + h(\eta_2) + h(\eta_3)$, where $\eta_1 = \alpha_T^{m-m_1} - 1$, $\eta_2 = c_\alpha$ and $\eta_3 = \sqrt{5}$. By applying Lemma 4.4 we get

$$\begin{aligned} h_0(\eta_1) &\le h_0(\alpha_T^{m-m_1}) + h_0(-1) + \log 2 \\ &= (m - m_1)h_0(\alpha_T) + \log 2 = \frac{m - m_1}{3}\log\alpha_T + \log 2 \\ &< \frac{1}{3} \times 2.03 \times 10^{15} \log n + \log 2. \end{aligned}$$

Thus

$$h(\alpha_1) < 6\left(\frac{1}{3} \times 2.03 \times 10^{15} \log n + \log 2 + \frac{1}{3}\log 44 + \log\sqrt{5}\right)$$

and therefore

$$h'(\alpha_1) < 6.77 \times 10^{14} \log n < 1.03 \times 10^{15} \log n.$$

Once again, we have that $h'(\alpha_2) = \frac{1}{2}\log\alpha$ and $h'(\alpha_3) = \frac{1}{3}\log\alpha_T$.

In particular, we have shown in both cases that

$$h'(\alpha_1) < 1.03 \times 10^{15} \log n, \quad h'(\alpha_2) = \frac{1}{2}\log\alpha, \quad h'(\alpha_3) = \frac{1}{3}\log\alpha_T, \quad B = n.$$

But, before we can apply Theorem 4.2 we have to ensure that $\Phi_i \ne 0$ for $i = 1, 2$. Firstly we deal with the assumption that $\Phi_1 = 0$, i.e. $\alpha^n - \alpha^{n_1} = \sqrt{5}c_\alpha\alpha_T^m$. This is impossible if $\sqrt{5}c_\alpha\alpha_T^m \in \mathbb{Q}(\sqrt{5}, \alpha_T)$ but $\notin \mathbb{Q}(\sqrt{5})$. Therefore let us assume that $\sqrt{5}c_\alpha\alpha_T^m \in \mathbb{Q}(\sqrt{5})$. Since $c_\alpha\alpha_T^m \in \mathbb{Q}(\alpha_T)$

and $\mathbb{Q}(\alpha_T) \cap \mathbb{Q}(\sqrt{5}) = \mathbb{Q}$, we deduce from $\sqrt{5}c_\alpha \alpha_T^m \in \mathbb{Q}(\sqrt{5})$ that we have $\sqrt{5}c_\alpha \alpha_T^m = y\sqrt{5}$ for some $y \in \mathbb{Q}$. Let $\sigma \neq \mathrm{id}$ be the unique non-trivial $\mathbb{Q}$-automorphism over $\mathbb{Q}(\sqrt{5})$. Then we get

$$\alpha^n - \alpha^{n_1} = \sqrt{5}c_\alpha \alpha_T^m = y\sqrt{5} = -\sigma(\sqrt{5}c_\alpha \alpha_T^m) = -\sigma(\alpha^n - \alpha^{n_1}) = \beta^{n_1} - \beta^n.$$

However, the absolute value of $\alpha^n - \alpha^{n_1}$ is at least $\alpha^n - \alpha^{n_1} \geq \alpha^{n-2} \geq \alpha^{298} > 2$ whereas the absolute value of $\beta^{n_1} - \beta^n$ is at most $|\beta^{n_1} - \beta^n| \leq |\beta|^{n_1} + |\beta|^n < 2$. By this obvious contradiction we conclude that $\Phi_1 \neq 0$.

Now let us consider the second case and assume for the moment that $\Phi_2 = 0$, i.e. $\alpha^{2n} = 5\alpha_T^{2m_1} c_\alpha^2 (\alpha_T^{m-m_1} - 1)^2$. However, $\alpha^{2n} \in \mathbb{Q}(\sqrt{5}) \setminus \mathbb{Q}$, whereas $5\alpha_T^{2m_1} c_\alpha^2 (\alpha_T^{m-m_1} - 1)^2 \in \mathbb{Q}(\alpha_T)$. Thus we obtain also in this case a contradiction and we also conclude in this case that $\Phi_2 \neq 0$.

Now, we are ready to apply Theorem 4.2 and get

$$\begin{aligned}\log|\Phi_i| &> -C(3,6)\left(1.03 \times 10^{15} \log n\right)\left(\frac{1}{2}\log\alpha\right)\left(\frac{1}{3}\log\alpha_T\right)\log n - \log 2 \\ &> -1.65 \times 10^{30} (\log n)^2\end{aligned}$$

for $i = 1, 2$. Combining this inequality with the inequalities (4.3.6) and (4.3.7), we obtain

$$(m_1 - m)\log\alpha_T + \log 1.42 > -1.65 \times 10^{30} (\log n)^2$$

and

$$(n_1 - n + 4)\log\alpha + \log 2.22 > -1.65 \times 10^{30} (\log n)^2$$

respectively. These two inequalities yield together with Lemma 4.4 the following lemma:

Lemma 4.5. *Assume that (n, m, n_1, m_1) is a solution to equation (4.3.1) with $m > m_1$. Then we have*

$$\max\{(n - n_1)\log\alpha, (m - m_1)\log\alpha_T\} < 1.66 \times 10^{30} (\log n)^2.$$

Note that in the case of $|\Lambda_1| > 0.5$, inequality (4.3.6) is possible only if $m - m_1 = 1$ and in the case of $|\Lambda_2| > 0.5$, inequality (4.3.7) is possible only if $n - n_1 \leq 6$. Both cases are covered by the bound provided by Lemma 4.5.

One more time we have to apply Theorem 4.2. This time we rewrite equation (4.3.1) as

$$\left|\frac{\alpha^n}{\sqrt{5}} - \frac{\alpha^{n_1}}{\sqrt{5}} - c_\alpha \alpha_T^m + c_\alpha \alpha_T^{m_1}\right| = \left|\frac{\beta^n}{\sqrt{5}} - \frac{\beta^{n_1}}{\sqrt{5}} + c_\beta \beta_T^m + c_\gamma \gamma_T^m - c_\beta \beta_T^{m_1} - c_\gamma \gamma_T^{m_1}\right| < 0.46.$$

Dividing both sides by $c_\alpha \alpha_T^{m_1}(\alpha_T^{m-m_1} - 1)$ we get by applying inequality (4.3.2)

$$\left|\frac{\alpha^{n-n_1} - 1}{\sqrt{5}\, c_\alpha (\alpha_T^{m-m_1} - 1)} \alpha^{n_1} \alpha_T^{-m_1} - 1\right| < \frac{0.46}{c_\alpha (1 - \alpha_T^{m_1 - m})\alpha_T} \frac{1}{\alpha_T^{m-1}} < 1.64\alpha^{4-n}. \tag{4.3.8}$$

In this final step we consider the linear form

$$\Lambda_3 = n_1 \log \alpha - m_1 \log \alpha_T + \log \left(\frac{\alpha_T^{n-n_1} - 1}{\sqrt{5}\, c_\alpha (\alpha_T^{m-m_1} - 1)} \right)$$

and assume that $|\Lambda_3| \leq 0.5$. Further, we put

$$\Phi_3 = e^{\Lambda_3} - 1 = \frac{\alpha^{n-n_1} - 1}{\sqrt{5}\, c_\alpha (\alpha_T^{m-m_1} - 1)} \alpha^{n_1} \alpha_T^{-m_1} - 1.$$

As before we take $K = \mathbb{Q}(\sqrt{5}, \alpha_T)$, i.e. $d = 6$, $k = 3$, $B = n$ and we have

$$\alpha_1 = \frac{\alpha^{n-n_1} - 1}{\sqrt{5}\, c_\alpha (\alpha_T^{m-m_1} - 1)}, \quad b_1 = 1, \quad \alpha_2 = \alpha, \quad b_2 = n_1, \quad \alpha_3 = \alpha_T, \quad b_3 = -m_1.$$

By Lemma 4.5 and similar computations as done before we obtain that

$$h\left(\frac{\alpha^{n-n_1} - 1}{\sqrt{5} c_\alpha} \right) \leq 6 \left(\frac{1}{2} (n - n_1 + 4) \log \alpha \right) + 2 \log 44 < 3 \times \left(1.67 \times 10^{30} (\log n)^2 \right)$$

and

$$h(\alpha_T^{m-m_1} - 1) \leq 6 \left(\frac{m - m_1}{3} \log \alpha_T + \log 2 \right) < 2 \times \left(1.67 \times 10^{30} (\log n)^2 \right).$$

Therefore we find the upper bound

$$h(\alpha_1) \leq h(\frac{\alpha^{n-n_1} - 1}{\sqrt{5} c_\alpha}) + h(\alpha_T^{m-m_1} - 1) < 5 \times \left(1.67 \times 10^{30} (\log n)^2 \right)$$

and thus

$$h'(\alpha_1) < \frac{5}{6} \times \left(1.67 \times 10^{30} (\log n)^2 \right).$$

As before, we have $h'(\alpha_2) = \frac{1}{2} \log \alpha$ and $h'(\alpha_3) = \frac{1}{3} \log \alpha_T$.

Using similar arguments as in the proof that $\Phi_1 \neq 0$ we can show that $\Phi_3 \neq 0$. Now an application of Theorem 4.2 yields

$$\log |\Phi_3| > -C(3,6) \left(\frac{5}{6} \times 1.67 \times 10^{30} (\log n)^2 \right) \left(\frac{1}{2} \log \alpha \right) \left(\frac{1}{3} \log \alpha_T \right) \log n - \log 2.$$

Combining this inequality with inequality (4.3.8) we get

$$(n - 4) \log \alpha < 2.23 \times 10^{45} (\log n)^3$$

which yields $n < 8 \times 10^{51}$.

Similarly as in the cases above the assumption that $|\Lambda_3| > 0.5$ leads in view of inequality (4.3.8) to $n \leq 5$. Let us summarize the results of this subsection:

Proposition 4.1. *Assume that* (n, m, n_1, m_1) *is a solution to equation* (4.3.1) *with* $m > m_1$. *Then we have that* $n < 8 \times 10^{51}$.

Remark 1. The theorem of Baker and Wüstholz (Theorem 4.2) [19] has a significant role in the development of linear forms in logarithms. It is the first quantitative version of Baker's theorem with a linear dependence of $\log B$ at the lower bound instead of higher powers of $\log B$ in other preceding work of Baker's theorem. It also showcased the use of the analytic subgroup theorem [95]. It is fully explicit to all parameters and can be easily applied. The reader may note that a slightly sharper bound for n, namely $n < 6 \times 10^{48}$, may be obtained if Matveev's result [64] is used instead. However, the improvement is insignificant in view of our next step, i.e. the use of the method of Baker and Davenport (Lemma 4.3), in which our upper bound for n can be further reduced to a great extent.

4.3.3 Generalized method of Baker and Davenport

In our final step we reduce the huge upper bound for n from Proposition 4.1 by applying several times Lemma 4.3. In this subsection we follow the ideas from [39]. First, we consider inequality (4.3.5) and recall that

$$\Lambda = n \log \alpha - m \log \alpha_T - \log(\sqrt{5} c_\alpha).$$

For technical reasons we assume that $\min\{n - n_1, m - m_1\} \geq 20$. In the case that this condition fails we consider one of the following inequalities instead:

- if $n - n_1 < 20$ but $m - m_1 \geq 20$, we consider inequality (4.3.6);
- if $n - n_1 \geq 20$ but $m - m_1 < 20$, we consider inequality (4.3.7);
- if both $n - n_1 < 20$ and $m - m_1 < 20$, we consider inequality (4.3.8).

Let us start by considering inequality (4.3.5). Since we assume that $\min\{n - n_1, m - m_1\} \geq 20$ we get $|\Phi| = |e^\Lambda - 1| < \frac{1}{4}$, hence $|\Lambda| < \frac{1}{2}$. And, since $|x| < 2|e^x - 1|$ holds for all $x \in (-\frac{1}{2}, \frac{1}{2})$ we get

$$|\Lambda| < 2\max\{\alpha^{n_1-n+5}, \alpha_T^{m_1-m+2}\} \leq \max\{\alpha^{n_1-n+7}, \alpha_T^{m_1-m+4}\}.$$

Assume that $\Lambda > 0$. Then we have the inequality

$$\begin{aligned} 0 < n\left(\frac{\log \alpha}{\log \alpha_T}\right) - m + \frac{\log(1/(\sqrt{5}c_\alpha))}{\log \alpha_T} &< \max\left\{\frac{\alpha^7}{\log \alpha_T}\alpha^{-(n-n_1)}, \frac{\alpha_T^4}{\log \alpha_T}\alpha_T^{-(m-m_1)}\right\} \\ &< \max\left\{48\alpha^{-(n-n_1)}, 19\alpha_T^{-(m-m_1)}\right\} \end{aligned}$$

and we apply Lemma 4.3 with

$$\tau = \frac{\log \alpha}{\log \alpha_T}, \quad \mu = \frac{\log(1/(\sqrt{5}c_\alpha))}{\log \alpha_T}, \quad (A, B) = (48, \alpha) \text{ or } (19, \alpha_T).$$

We first show that that τ is irrational. Let us assume for the moment that it is rational. Then $\tau = \frac{a}{b}$ with coprime integers a and b, thus $\alpha^b = {\alpha_T}^a$. The fact that $\alpha^b \in \mathbb{Q}(\alpha)$, ${\alpha_T}^a \in \mathbb{Q}(\alpha_T)$ and $\mathbb{Q}(\alpha) \cap \mathbb{Q}(\alpha_T) = \mathbb{Q}$ implies that $\alpha^b, {\alpha_T}^a \in \mathbb{Q}$, which can easily be seen to be not the case. Therefore $\alpha^b \neq {\alpha_T}^a$ and hence τ is irrational. Let $\tau = [a_0, a_1, a_2, \dots] = [0, 1, 3, 1, 3, 13, 2, 1, 8, 3, 1, 5, \dots]$ be the continued fraction of τ. Moreover, we choose $M = 8 \times 10^{51}$ and consider the 104th convergent

$$\frac{p}{q} = \frac{p_{104}}{q_{104}} = \frac{52841963647885529119220800813840965784230907639792403 3}{66915901128412992013946827929750445311260816077167181 0},$$

with $q = q_{104} > 6M$. This yields $\varepsilon > 0.068$ and therefore either

$$n - n_1 \leq \frac{\log(48q/0.068)}{\log \alpha} < 272, \quad \text{or} \quad m - m_1 \leq \frac{\log(19q/0.068)}{\log \alpha_T} < 213.$$

Thus, we have either $n - n_1 \leq 271$, or $m - m_1 \leq 212$.

In the case of $\Lambda < 0$ we consider the following inequality:

$$\begin{aligned} 0 < m\left(\frac{\log \alpha_T}{\log \alpha}\right) - n + \frac{\log(\sqrt{5}c_\alpha)}{\log \alpha} &< \max\left\{\frac{\alpha^7}{\log \alpha_T}\alpha^{-(n-n_1)}, \frac{\alpha_T^4}{\log \alpha_T}\alpha_T^{-(m-m_1)}\right\} \\ &< \max\left\{61\alpha^{-(n-n_1)}, 24\alpha_T^{-(m-m_1)}\right\} \end{aligned}$$

instead and apply Lemma 4.3 with

$$\tau = \frac{\log \alpha_T}{\log \alpha}, \quad \mu = \frac{\log(\sqrt{5}c_\alpha)}{\log \alpha}, \quad (A, B) = (61, \alpha) \text{ or } (24, \alpha_T).$$

Let $\tau = [a_0, a_1, a_2, \dots] = [1, 3, 1, 3, 13, 2, 1, 8, 3, 1, 5, 2, \dots]$ be the continued fraction of τ. Again, we choose $M = 8 \times 10^{51}$ but in this case we consider instead of the 104th convergent the 103rd convergent

$$\frac{p}{q} = \frac{p_{103}}{q_{103}} = \frac{66915901128412992013946827929750445311260816077167181 0}{52841963647885529119220800813840965784230907639792403 3},$$

with $q > 6M$. This yields $\varepsilon > 0.067$ and again we obtain either

$$n - n_1 < \frac{\log(61q/0.067)}{\log \alpha} < 272, \quad \text{or} \quad m - m_1 < \frac{\log(24q/0.067)}{\log \alpha_T} < 213.$$

These bounds agree with the bounds obtained in the case that $\Lambda > 0$. As a conclusion, we have either $n - n_1 \leq 271$ or $m - m_1 \leq 212$.

Now, we have to distinguish between the two cases $n - n_1 \leq 271$ and $m - m_1 \leq 212$. First, let us assume that $n - n_1 \leq 271$. In this case we consider inequality (4.3.6) and assume that $m - m_1 \geq 20$. Recall that

$$\Lambda_1 = n_1 \log \alpha - m \log \alpha_T + \log\left(\frac{\alpha^{n-n_1} - 1}{\sqrt{5}c_\alpha}\right)$$

and inequality (4.3.6) yields that

$$|\Lambda_1| < \alpha_T^{m_1-m+2}.$$

If we further assume that $\Lambda_1 > 0$, then we get

$$0 < n_1\left(\frac{\log\alpha}{\log\alpha_T}\right) - m + \frac{\log((\alpha^{n-n_1}-1)/(\sqrt{5}c_\alpha))}{\log\alpha_T} < \frac{\alpha_T^2}{\log\alpha_T}\alpha_T^{-(m-m_1)} < 6\alpha_T^{-(m-m_1)}.$$

Again we apply Lemma 4.3 with the same τ and M as in the case that $\Lambda > 0$. We use the 104th convergent $\frac{p}{q} = \frac{p_{104}}{q_{104}}$ of τ as before. But, in this case we choose $(A,B) = (6, \alpha_T)$ and use

$$\mu_k = \frac{\log((\alpha^k-1)/(\sqrt{5}c_\alpha))}{\log\alpha_T},$$

instead of μ for each possible value of $n - n_1 = k = 1, 2, \ldots, 271$. A quick computer aid computation yields that $\varepsilon > 0.00038$ for all $1 \le k \le 271$. Hence, by Lemma 4.3, we get

$$m - m_1 < \frac{\log(6q/0.00038)}{\log\alpha_T} < 220.$$

Thus, $n - n_1 \le 271$ implies $m - m_1 \le 219$.

In the case that $\Lambda_1 < 0$ we follow the ideas from the case that $\Lambda_1 > 0$. We use the same τ as in the case that $\Lambda < 0$ but instead of μ we take

$$\mu_k = \frac{\log(\sqrt{5}c_\alpha/(\alpha^k-1))}{\log\alpha}$$

for each possible value of $n - n_1 = k = 1, 2, \ldots, 271$. Using Lemma 4.3 with this setting we also obtain in this case that $n - n_1 \le 271$ implies $m - m_1 \le 219$.

Now let us turn to the case that $m - m_1 \le 212$ and let us consider inequality (4.3.7). Recall that

$$\Lambda_2 = n\log\alpha - m_1\log\alpha_T + \log\left(\frac{1}{\sqrt{5}\,c_\alpha(\alpha_T^{m-m_1}-1)}\right)$$

and let us assume that $n - n_1 \ge 20$. Then we have

$$|\Lambda_2| < \frac{4.44\alpha^4}{\alpha^{n-n_1}}.$$

Assuming that $\Lambda_2 > 0$, we get

$$0 < n\left(\frac{\log\alpha}{\log\alpha_T}\right) - m_1 + \frac{\log(1/(\sqrt{5}\,c_\alpha(\alpha_T^{m-m_1}-1)))}{\log\alpha_T} < \frac{4.44\alpha^4}{(\log\alpha_T)\alpha^{n-n_1}} < 50\alpha^{-(n-n_1)}.$$

Once again we apply Lemma 4.3 with the same τ and M as for the case $\Lambda > 0$ before. We take $(A,B) = (50, \alpha)$ and

$$\mu_k = \frac{\log(1/(\sqrt{5}\,c_\alpha(\alpha_T^k-1)))}{\log\alpha_T}$$

for every possible value $m - m_1 = k = 1, 2, \ldots, 212$. If we use again the 104th convergent of τ, i.e. we put $q = q_{104}$, then for each k that yields a positive ε, we get $\varepsilon > 0.0012$. Therefore we get

$$n - n_1 < \frac{\log(50 q_{104}/0.0012)}{\log \alpha} < 280$$

in these cases. But for $k = 90$ we get a negative ε. In this case we consider the 105th convergent $\frac{p}{q} = \frac{p_{105}}{q_{105}}$ of τ instead. Let us note that

$$q_{105} = 20120013979896675119357414743592977629715414121119669783.$$

Now we obtain in the case $k = 90$ that $\varepsilon > 0.46$. Thus

$$n - n_1 < \frac{\log(50 q_{105}/0.46)}{\log \alpha} < 275.$$

In the case that $\Lambda_2 < 0$ we follow again the ideas from the case that $\Lambda_2 > 0$. Of course we choose

$$\tau = \frac{\log \alpha_T}{\log \alpha} \quad \text{and} \quad \mu_k = \frac{\log(\sqrt{5}\, c_\alpha (\alpha_T^k - 1))}{\log \alpha}.$$

Applying Lemma 4.3 for all possible values of $m - m_1 = k = 1, \ldots, 212$ also yields in this case that $n - n_1 \leq 279$.

Let us summarize the above computations. First we got that either $n - n_1 \leq 271$, or $m - m_1 \leq 212$. If we assume that $n - n_1 \leq 271$, then we deduce that $m - m_1 \leq 219$, and if we assume that $m - m_1 \leq 212$, then we deduce that $n - n_1 \leq 279$. Altogether we obtain $n - n_1 \leq 279$ and $m - m_1 \leq 219$.

For the last step in our reduction process we consider inequality (4.3.8). Recall that

$$\Lambda_3 = n_1 \log \alpha - m_1 \log \alpha_T + \log\left(\frac{\alpha^{n - n_1} - 1}{\sqrt{5}\, c_\alpha (\alpha_T^{m - m_1} - 1)} \right).$$

Since we assume that $n \geq 300$, inequality (4.3.8) implies that

$$|\Lambda_3| < \frac{3.28 \alpha^4}{\alpha^n}.$$

Let us assume that $\Lambda_3 > 0$. Then

$$0 < n_1 \left(\frac{\log \alpha}{\log \alpha_T} \right) - m_1 + \frac{\log\left((\alpha^k - 1)/(\sqrt{5}\, c_\alpha (\alpha_T^l - 1)) \right)}{\log \alpha_T} < \frac{3.28 \alpha^4}{(\log \alpha_T) \alpha^n} < 37 \alpha^{-n},$$

where $(k, l) = (n - n_1, m - m_1)$. We apply Lemma 4.3 once more with the same τ and M as for the case when $\Lambda > 0$. Moreover, we take $(A, B) = (37, \alpha)$, and put

$$\mu_{k,l} = \frac{\log\left((\alpha^k - 1)/(\sqrt{5}\, c_\alpha (\alpha_T^l - 1)) \right)}{\log \alpha_T}$$

for $1 \le k \le 279$ and $1 \le l \le 219$. We consider the 104th convergent $\frac{p}{q} = \frac{p_{104}}{q_{104}}$. For all pairs (k, l) such that ε is positive we have indeed $\varepsilon > 2.8 \times 10^{-6}$. Thus for these pairs (k, l) Lemma 4.3 yields that

$$n < \frac{\log(37 q_{104}/0.0000028)}{\log \alpha} < 292.$$

For all the remaining pairs (k, l) which yield a negative ε, we consider the 105th convergent $\frac{p}{q} = \frac{p_{105}}{q_{105}}$ instead. And for all those pairs (k, l) the quantity ε is positive for this choice of q. In particular, we have that $\varepsilon > 0.0018$ for all these cases, hence

$$n < \frac{\log(37 q_{105}/0.0018)}{\log \alpha} < 286.$$

In the case that $\Lambda_3 < 0$ the method is similar. In particular we have to apply Lemma 4.3 with

$$\tau = \frac{\log \alpha_T}{\log \alpha} \quad \text{and} \quad \mu_{k,l} = \frac{\log\left((\sqrt{5}\, c_\alpha (\alpha_T^l - 1))/(\alpha^k - 1)\right)}{\log \alpha}.$$

However, we obtain in this case the slightly smaller bound $n < 289$.

Altogether our reduction procedure yields the upper bound $n \le 291$. However, this contradicts our assumption that $n \ge 300$. Thus Theorem 4.1 is proved.

Chapter 5

On a variant of Pillai's problem II

The content of this chapter is the same as the joint paper with István Pink and Volker Ziegler [37], which is published in the Journal of Number Theory.[1]

5.1 Introduction

A linear recurrence sequence is a sequence $\{U_n\}_{n\geq 0}$ such that for some $k \geq 1$, we have

$$U_{n+k} = c_1 U_{n+k-1} + \cdots + c_k U_n$$

for all $n \geq 0$, where $c_1, \ldots, c_k$ are given complex numbers with $c_k \neq 0$. When $c_1, \ldots, c_k$ are integers and $U_0, \ldots, U_{k-1}$ are also integers, U_n is an integer for all $n \geq 0$ and we say that $\{U_n\}_{n\geq 0}$ is defined over the integers. In what follows we will always assume that $\{U_n\}_{n\geq 0}$ is defined over the integers.

It is known that if we write

$$F(X) = X^k - c_1 X^{k-1} - \cdots - c_k = \prod_{i=1}^{t} (X - \alpha_i)^{\sigma_i},$$

where $\alpha_1, \ldots, \alpha_t$ are distinct complex numbers, and $\sigma_1, \ldots, \sigma_t$ are positive integers whose sum is k, then there exist polynomials $a_1(X), \ldots, a_t(X)$ whose coefficients are in $\mathbb{Q}(\alpha_1, \ldots, \alpha_t)$ such that $a_i(X)$ is of degree at most $\sigma_i - 1$ for $i = 1, \ldots, t$, and such that furthermore the formula

$$U_n = \sum_{i=1}^{t} a_i(n) \alpha_i^n$$

[1]K. C. Chim was supported by the Austrian Science Fund (FWF) under the projects P26114 and W1230. I. Pink and V. Ziegler were supported by the Austrian Science Fund (FWF) under the project P 24801-N26.

holds for all $n \geq 0$. We may certainly assume that $a_i(X)$ is not the zero polynomial for any $i = 1, \dots, t$. We call $\alpha = \alpha_1$ a dominant root of $\{U_n\}_{n\geq 0}$, if $|\alpha_1| > |\alpha_2| \geq \cdots \geq |\alpha_t|$. In this case the sequence $\{U_n\}_{n\geq 0}$ is said to satisfy the dominant root condition.

This paper is a follow-up to our previous work [36], in which we found all integers c admitting at least two distinct representations of the form $F_n - T_m$ for some positive integers $n \geq 2$ and $m \geq 2$. Here we denote by $\{F_n\}_{n\geq 0}$ the sequence of Fibonacci numbers given by $F_0 = 0$, $F_1 = 1$ and $F_{n+2} = F_{n+1} + F_n$ for all $n \geq 0$, and denote by $\{T_m\}_{m\geq 0}$ the sequence of Tribonacci numbers given by $T_0 = 0$, $T_1 = T_2 = 1$ and $T_{m+3} = T_m + T_{m+1} + T_{m+2}$ for all $m \geq 0$. In [36] the main result is the following:

Theorem 5.1. *The only integers c having at least two representations of the form $F_n - T_m$ come from the set*

$$\mathcal{C} = \{0, 1, -1, -2, -3, 4, -5, 6, 8, -10, 11, -11, -22, -23, -41, -60, -271\}.$$

Furthermore, for each $c \in \mathcal{C}$ all representations of the form $c = F_n - T_m$ with integers $n \geq 2$ and $m \geq 2$ are obtained.

The above problem of obtaining all integers c having at least two representations of the form $F_n - T_m$ can be regarded as a variant of Pillai's problem. Readers can refer to [36] for the complete list of representations and some historical development of the Pillai's problem. The interested reader may also refer to the paper of Pillai [71] for the original problem, the papers of Stroeker and Tijdeman [87] and Bennett [21] for tackling special cases and the papers of Ddamulira, Luca and Rakotomalala [39] and Bravo, Luca and Yazán [32] for other variants.

The purpose of this paper is to generalize Theorem 5.1. Assume that we are given two linear recurrence sequences $\{U_n\}_{n\geq 0}$ and $\{V_m\}_{m\geq 0}$ defined over the integers which satisfy the dominant root condition, then under some mild restrictions there exist only finitely many integers c such that the equation

$$U_n - V_m = c$$

has at least two distinct solutions $(n, m) \in \mathbb{N} \times \mathbb{N}$, where $\mathbb{N} = \{0, 1, \dots\}$ is the set of natural numbers. That is, we want to solve

$$U_n - U_{n_1} = V_m - V_{m_1} \tag{5.1.1}$$

for $(n, m) \neq (n_1, m_1)$.

In order to avoid linear recurrence sequences which would yield infinitely many solutions trivially, we assume that both $\{U_n\}_{n\geq 0}$ and $\{V_m\}_{m\geq 0}$ are eventually strictly increasing in absolute values. That is, we assume that there exist constants N_0 and M_0 such that $|U_{n+1}| > |U_n| > 0$ for all $n \geq N_0$ and $|V_{m+1}| > |V_m| > 0$ for all $m \geq M_0$. We shall therefore require $n \geq N_0$ and $m \geq M_0$ when solving equation (5.1.1). For instance in the case that $\{U_n\}_{n\geq 0}$ is the Fibonacci sequence we would find infinitely many integers c such that c has at least two distinct representations of the form $U_n - V_m$. Indeed all integers of the form $c = 1 - V_m$ would yield the two representations $F_1 - V_m = F_2 - V_m = c$.

Throughout this paper, we denote by $C_0, C_1, \dots, C_{45}$ effectively computable constants. We prove the following theorem:

Theorem 5.2. *Suppose that $\{U_n\}_{n\geq 0}$ and $\{V_m\}_{m\geq 0}$ are two linear recurrence sequences defined over the integers with dominant roots α and β respectively. Furthermore, suppose that α and β are multiplicatively independent. Suppose also that $\{U_n\}_{n\geq 0}$ and $\{V_m\}_{m\geq 0}$ are strictly increasing in absolute values for $n \geq N_0$ and $m \geq M_0$ respectively. Then there exists a finite set $\mathcal{C}$ such that the integer c has at least two distinct representations of the form $U_n - V_m$ with $n \geq N_0$ and $m \geq M_0$, if and only if $c \in \mathcal{C}$. The set $\mathcal{C}$ is effectively computable.*

Besides, the assumption that α and β are multiplicatively independent is needed to avoid scenarios such as having $\{U_n\}_{n\geq 0} = \{F_n\}_{n\geq 0}$, $\{V_m\}_{m\geq 0} = \{F_m\}_{m\geq 0}$. In this case equation $c = F_{n+2} - F_{n+1} = F_{n+1} - F_{n-1}$ holds for all $n \geq 1$ and we have infinitely many c that yield at least two solutions to equation $U_n - V_m = c$.

It should be also noted that the assumption that α and β are multiplicatively independent is not necessary for the existence of only finitely many c. Consider the case where $\{U_n\}_{n\geq 0} = \{2^n + 1\}_{n\geq 0}$ and $\{V_m\}_{n\geq 0} = \{4^m + 2\}_{m\geq 0}$. By elementary divisbility criteria one can easily verify that the only solutions to (5.1.1) with $n \neq n_1$ satisfy $n = 2m$ and $n_1 = 2m_1$, i.e. $c = -1$. Although (5.1.1) has infinitely many solutions the only c such that $U_n - V_m = c$ has at least two solutions is $c = -1$.

In view of the two examples above it seems to be an interesting problem to relax the condition that α and β are multiplicatively independent in Theorem 5.2.

We shall prove Theorem 5.2 by applying the results of linear forms in logarithms and some results on the heights of algebraic numbers several times to obtain an effectively computable upper bound for the value of the largest unknown among $\{n, m, n_1, m_1\}$.

5.2 Preliminaries

In this section we present two basic tools needed in the proof of Theorem 5.2. Firstly, we state a result on lower bounds of linear forms in logarithms due to Baker and Wüstholz [19]. Secondly we provide a lower bound for the height of numbers of the form $\frac{\alpha^n}{\beta^m}$ provided that α and β are multiplicatively independent, and an upper bound for the height of $\frac{p(n)}{q(m)}$, where p, q are arbitrary but fixed polynomials.

5.2.1 A lower bound for linear forms in logarithms of algebraic numbers

In 1993, Baker and Wüstholz [19] obtained an explicit bound for linear forms in logarithms with a linear dependence on $\log B$, where $B \geq e$ denotes an upper bound for the height of the linear form (to be defined later in this section). It is a vast improvement compared with lower bounds with a dependence on higher powers of $\log B$ in preceding publications by other mathematicians in particular Baker's original results [1, 2, 3]. The final structure for the lower bound for linear forms in logarithms without an explicit determination of the constant involved has been established by Wüstholz [93] and the precise determination of that constant (which is denoted as $C(n,d)$ in [19] and later in this section as $C(k,d)$) is the central aspect of [19] (see also [20]). We shall now state the result of Baker and Wüstholz.

Denote by $\alpha_1,\ldots,\alpha_k$ algebraic numbers, not 0 or 1, and by $\log\alpha_1,\ldots,\log\alpha_k$ a fixed determination of their logarithms. Let $K = \mathbb{Q}(\alpha_1,\ldots,\alpha_k)$ and let $d = [K:\mathbb{Q}]$ be the degree of K over $\mathbb{Q}$. For any $\alpha \in K$, suppose that its minimal polynomial over the integers is

$$g(x) = a_0x^\delta + a_1x^{\delta-1} + \cdots + a_\delta = a_0\prod_{j=1}^{\delta}(x-\alpha^{(j)})$$

where $\alpha^{(j)}$, $j = 1,\ldots,\delta$ are all the roots of $g(x)$. The absolute logarithmic Weil height of α is defined as

$$h_0(\alpha) = \frac{1}{\delta}\left(\log|a_0| + \sum_{j=1}^{\delta}\log\left(\max\{|\alpha^{(j)}|,1\}\right)\right).$$

Then the modified height $h'(\alpha)$ is defined by

$$h'(\alpha) = \frac{1}{d}\max\{h(\alpha),|\log\alpha|,1\},$$

where $h(\alpha) = dh_0(\alpha)$ is the standard logarithmic Weil height of α.

Let us consider the linear form

$$L(z_1,\ldots,z_k) = b_1z_1 + \cdots + b_kz_k,$$

where $b_1,\ldots,b_k$ are rational integers, not all 0 and define

$$h'(L) = \frac{1}{d}\max\{h(L),1\},$$

where $h(L) = d\log\left(\max_{1\leq j\leq k}\left\{\frac{|b_j|}{b}\right\}\right)$ is the logarithmic Weil height of L, with b as the greatest common divisor of $b_1,\ldots,b_k$. If we write $B = \max\{|b_1|,\ldots,|b_k|,e\}$, then we get

$$h'(L) \leq \log B.$$

With these notations we are able to state the following result due to Baker and Wüstholz [19].

Theorem 5.3. *If $\Lambda = L(\log\alpha_1, \dots, \log\alpha_k) \neq 0$, then*

$$\log|\Lambda| \geq -C(k,d)h'(\alpha_1)\cdots h'(\alpha_k)h'(L),$$

where

$$C(k,d) = 18(k+1)!\,k^{k+1}(32d)^{k+2}\log(2kd).$$

With $|\Lambda| \leq \frac{1}{2}$, we have $\frac{1}{2}|\Lambda| \leq |\Phi| \leq 2|\Lambda|$, where

$$\Phi = e^{\Lambda} - 1 = \alpha_1^{b_1}\cdots\alpha_k^{b_k} - 1,$$

so that

$$\log|\alpha_1^{b_1}\cdots\alpha_k^{b_k} - 1| \geq \log|\Lambda| - \log 2. \tag{5.2.1}$$

5.2.2 Some results on heights

Before we state our results let us recall some well known properties of the absolute logarithmic height:

$$\begin{aligned} h_0(\eta \pm \gamma) &\leq h_0(\eta) + h_0(\gamma) + \log 2, \\ h_0(\eta\gamma^{\pm 1}) &\leq h_0(\eta) + h_0(\gamma), \\ h_0(\eta^{\ell}) &= |\ell| h_0(\eta), \qquad \text{for } \ell \in \mathbb{Z}, \end{aligned}$$

where η, γ are some algebraic numbers.

Upon applying inequality (5.2.1) from Theorem 5.3, which is only valid for $\Lambda \neq 0$, we need to treat the situation $\Lambda = 0$ separately. We shall make use of the following lemma repeatedly applied when dealing with this situation.

Lemma 5.4. *Let K be a number field and suppose that $\alpha, \beta \in K$ are two algebraic numbers which are multiplicatively independent. Moreover, let $n, m \in \mathbb{Z}$. Then there exists an effectively computable constant $C_0 > 0$ such that*

$$h_0\left(\frac{\alpha^n}{\beta^m}\right) \geq C_0 \max\{|n|, |m|\}.$$

Although Lemma 5.4 seems to be well known we found no apropriate reference. In order to keep the paper as self contained as possible we give a proof of this Lemma.

Before we start with the proof of Lemma 5.4 we want to fix some notations. Let K be a number field. We denote by M_K the set of places of K. For each $v \in M_K$ we denote by $\|\cdot\|_v$ the normalized absolute value corresponding to v, i.e., if v lies above $p \in M_{\mathbb{Q}} := \{\infty\} \cup \mathbb{P}$, where $\mathbb{P}$ is the set of rational primes, then the restriction of $\|\cdot\|_v$ to $\mathbb{Q}$ is $|\cdot|_p^{[K_v:\mathbb{Q}_p]/[K:\mathbb{Q}]}$, where $\mathbb{Q}_p$ and K_v are the p-adic and v-adic completions of $\mathbb{Q}$ and K respectively. Here, $|\cdot|_\infty$ is the usual absolute value and for a prime p the norm $|\cdot|_p$ is the usual p-adic norm such that $|p|_p = \frac{1}{p}$.

Let us note that with these notations the product formula (see e.g. [68, Chapter III, Theorem 1.3]) states that

$$\sum_{v \in M_K} \log \|\alpha\|_v = 0$$

and the height can be written as

$$h_0(\alpha) = \sum_{v \in M_K} \max\{0, \log \|\alpha\|_v\}.$$

With these notations at hand we can turn to the proof of Lemma 5.4.

Proof of Lemma 5.4. Denote by $S \subseteq M_K$ the finite set of places where the valuation of either α or β is non-zero. i.e.

$$S = \{v \in M_K : \|\alpha\|_v \neq 0 \text{ or } \|\beta\|_v \neq 0\}.$$

We consider a Log function defined as follows:

$$\operatorname{Log} : K \longrightarrow \prod_{v \in S} \mathbb{R} \qquad \alpha \longmapsto (\log \|\alpha\|_v)_{v \in S}.$$

Obviously, Log has the properties that

$$\alpha^n \longmapsto n \operatorname{Log}(\alpha), \quad \text{and} \quad \alpha \cdot \beta \longmapsto \operatorname{Log}(\alpha) + \operatorname{Log}(\beta),$$

so that

$$\operatorname{Log}\left(\frac{\alpha^n}{\beta^m}\right) = n \operatorname{Log}(\alpha) - m \operatorname{Log}(\beta).$$

Since α and β are multiplicatively independent, there exist valuations $v_1, v_2 \in S$ such that the matrix

$$M = \begin{pmatrix} \log \|\alpha\|_{v_1} & \log \|\beta\|_{v_1} \\ \log \|\alpha\|_{v_2} & \log \|\beta\|_{v_2} \end{pmatrix}$$

is non-singular. For the moment let us write $A = \frac{\alpha^n}{\beta^m}$. If we consider the system of linear equations

$$\begin{aligned} n \log \|\alpha\|_{v_1} - m \log \|\beta\|_{v_1} &= \log \|A\|_{v_1} \\ n \log \|\alpha\|_{v_2} - m \log \|\beta\|_{v_2} &= \log \|A\|_{v_2}, \end{aligned}$$

we obtain from Cramer's rule that

$$\begin{aligned} |n| &\leq \frac{2 \max\{|\log \|A\|_{v_1}|, |\log \|A\|_{v_2}|\} \cdot \max\{|\log \|\beta\|_{v_1}|, |\log \|\beta\|_{v_2}|\}}{\det M}, \\ |m| &\leq \frac{2 \max\{|\log \|A\|_{v_1}|, |\log \|A\|_{v_2}|\} \cdot \max\{|\log \|\alpha\|_{v_1}|, |\log \|\alpha\|_{v_2}|\}}{\det M}. \end{aligned}$$

From the above inequality, we have

$$\max\{|\log \|A\|_{v_1}|, |\log \|A\|_{v_2}|\} \geq \max\left\{\widetilde{C_1}|n|, \widetilde{C_2}|m|\right\},$$

where

$$\widetilde{C_1} = \frac{\det M}{2\max\{|\log \|\beta\|_{v_1}|, |\log \|\beta\|_{v_2}|\}} > 0$$

and

$$\widetilde{C_2} = \frac{\det M}{2\max\{|\log \|\alpha\|_{v_1}|, |\log \|\alpha\|_{v_2}|\}} > 0.$$

As noted above we have that

$$h_0(A) = \sum_{v \in M_K} \max\{\log \|A\|_v, 0\} \quad \text{and} \quad \sum_{v \in M_K} \log \|A\|_v = 0.$$

From the product formula we deduce that there exists $v \in M_K$ such that

$$\log \|A\|_v \geq \frac{1}{|S|} \cdot \max\{|\log \|A\|_{v_1}|, |\log \|A\|_{v_2}|\}.$$

Thus, we obtain

$$\begin{aligned} h_0(A) = h_0\left(\frac{\alpha^n}{\beta^m}\right) &\geq \frac{1}{|S|} \max\{|\log \|A\|_{v_1}|, |\log \|A\|_{v_2}|\} \\ &\geq \frac{1}{|S|} \max\left\{\widetilde{C_1}|n|, \widetilde{C_2}|m|\right\} \\ &\geq C_0 \max\{|n|, |m|\}, \end{aligned}$$

where we may choose $C_0 = \frac{1}{|S|} \min\left\{\widetilde{C_1}, \widetilde{C_2}\right\}$. □

Let us also state the following result as a lemma:

Lemma 5.5. *Let K be a number field and $p, q \in K[X]$ arbitrary but fixed polynomials. Then there exists an effectively computable constant $C = C(p, q)$ such that*

$$h_0\left(\frac{p(n)}{q(m)}\right) \leq C \log \max\{n, m\}.$$

Proof. Since $h_0\left(\frac{p(n)}{q(m)}\right) \leq h_0(p(n)) + h_0(q(m))$ it suffices to prove that there exists an effectively computable constant C such that $h_0(p(n)) \leq C \log n$ for some fixed polynomial $p \in K[X]$. Assume that $p(n) = c_k n^k + \cdots + c_1 n + c_0$, then we have

$$\begin{aligned} h_0(p(n)) &= h_0(c_k n^k + \cdots + c_1 n + c_0) \\ &\leq h_0(c_k) + k h_0(n) + \cdots + h_0(c_0) + k \log 2 \\ &\leq C \log n. \end{aligned}$$

□

5.3 Proof of Theorem 5.2

5.3.1 Set up

Recall that we wish to solve equation (5.1.1):

$$U_n - U_{n_1} = V_m - V_{m_1},$$

for $(n,m) \neq (n_1,m_1)$, with $n, n_1 \geq N_0$ and $m, m_1 \geq M_0$.

We may assume that $m \neq m_1$, since otherwise $(n,m) = (n_1,m_1)$. Without loss of generality we may assume that $m > m_1$. But, then we have to distinguish between the two cases $n > n_1$ and $n < n_1$. Since the proof of the second case is obtained by interchanging the roles of n and n_1, i.e. to interchange n_1 and n everywhere, we only give the proof of the first case. Therefore we assume from now on that $n > n_1 \geq N_0$ and $m > m_1 \geq M_0$.

In the following we use the L-notation. Assume $f(x)$, $g(x)$ and $k(x)$ are real functions and that $k(x) > 0$ for $x > 1$. We shall write

$$f(x) = g(x) + L(k(x))$$

for

$$g(x) - k(x) \leq f(x) \leq g(x) + k(x).$$

The use of the L-notation is like the use of the O-notation but with the advantage to have an explicit bound for the error term.

Let us consider the linear recurrence sequences $\{U_n\}_{n\geq 0}$ and $\{V_m\}_{m\geq 0}$ a bit closer. Let us assume that the characteristic polynomials of $\{U_n\}_{n\geq 0}$ and $\{V_m\}_{m\geq 0}$ are

$$F_U(X) = \prod_{i=1}^{t}(X-\alpha_i)^{\sigma_i} \quad \text{and} \quad F_V(X) = \prod_{i=1}^{s}(X-\beta_i)^{\tau_i}$$

respectively.

Let α and β be the dominant roots of $\{U_n\}_{n\geq 0}$ and $\{V_m\}_{m\geq 0}$ respectively. According to our assumptions we can write

$$\begin{aligned} U_n &= a(n)\alpha^n + a_2(n)\alpha_2^n + \cdots + a_t(n)\alpha_t^n \\ &= a(n)\alpha^n + L\left(a'' n^A \alpha_2^n\right) \\ &= a(n)\alpha^n + L(a'\alpha'^n) \end{aligned} \tag{5.3.1}$$

where a', a'', A are suitable but effectively computable, non-negative constants, $a(X)$, $a_i(X) \in \mathbb{Q}(\alpha_1,\dots,\alpha_t)[X]$, $2 \leq i \leq t$ and $\alpha' \in \mathbb{R}$ is such that $|\alpha_1| = |\alpha| > \alpha' > |\alpha_2|$. Note that in case that $t = 1$ we put $\alpha_2 = 1$ and $a' = a'' = A = 0$ and with this choice (5.3.1) still holds. Let us also note that by our assumption that $\{U_n\}_{n\geq 0}$ is non-degenerate and defined over the integers the dominant root α is a real algebraic integer which is not a root of unity, hence we have $|\alpha| > 1$. Thus we may assume that also $|\alpha| > \alpha' > 1$ holds. This also implies that $\{|U_n|\}_{n\geq 0}$ is eventually strictly increasing. Moreover we may assume that $|a(n)|$ is increasing for all $n \geq N_1$ for some suitable constant N_1. In addition, we choose N_1 large enough such that $|a(n)| \geq |a(n')|$ for all $n > N_1$ and $n > n' > 0$.

Similarly we may write

$$V_m = b(m)\beta^m + L(b'\beta'^m) \tag{5.3.2}$$

where b', β' are suitable constants. By the same arguments as above we may also assume that $|\beta| > \beta' > 1$ and $|b(m)|$ is increasing provided that $m \geq M_1$, where M_1 is some sufficiently large number. Moreover we assume that M_1 is chosen large enough such that $|b(m)| \geq |b(m')|$ for all $m \geq M_1$ and $m > m' > 0$.

Without loss of generality, let us assume that $|\alpha| > |\beta|$. We denote by σ and τ the degree of $a(n)$ and $b(m)$ respectively. Besides, we know that $|U_n| \sim an^\sigma|\alpha^n|$ as $n \to \infty$, where a is the leading coefficient of $a(n)$. Similarly we know that $|V_m| \sim bm^\tau|\beta^m|$ as $m \to \infty$, where b is the leading coefficient of $b(n)$. Therefore there are positive constants C_1, C_2 and C_3, C_4 such that $C_2/C_1 < |\alpha|$ and $C_4/C_3 < |\beta|$ with

$$\begin{aligned} C_1 n^\sigma|\alpha|^n \leq |U_n| &\leq C_2 n^\sigma|\alpha|^n & \text{for all } n \geq N_2 \\ C_3 m^\tau|\beta|^m \leq |V_m| &\leq C_4 m^\tau|\beta|^m & \text{for all } m \geq M_2, \end{aligned}$$

where N_2 and M_2 are sufficiently large.

Let us assume for the moment that $n > n_1 \geq N_2$ and $m > m_1 \geq M_2$. Using equation (5.1.1) we get that

$$\begin{aligned} |U_n - U_{n_1}| \leq |U_n| + |U_{n_1}| \leq C_2 n^\sigma\left(|\alpha|^n + |\alpha|^{n_1}\right) &= C_2 n^\sigma|\alpha|^n\left(1 + \frac{1}{|\alpha|^{n-n_1}}\right) \\ \leq C_2 n^\sigma|\alpha|^n\left(1 + \frac{1}{|\alpha|}\right) &= C_5 n^\sigma|\alpha|^n \end{aligned}$$

and

$$\begin{aligned} |U_n - U_{n_1}| \geq |U_n| - |U_{n_1}| \geq C_1 n^\sigma|\alpha|^n - C_2 n^\sigma|\alpha|^{n_1} &= C_1 n^\sigma|\alpha|^n\left(1 - \frac{C_2}{C_1|\alpha|^{n-n_1}}\right) \\ \geq C_1 n^\sigma|\alpha|^n\left(1 - \frac{C_2}{C_1|\alpha|}\right) &= C_6 n^\sigma|\alpha|^n. \end{aligned}$$

Similarly, we have

$$\begin{aligned} |V_m - V_{m_1}| \leq |V_m| + |V_{m_1}| \leq C_4 m^\tau\left(|\beta|^m + |\beta|^{m_1}\right) &= C_4 m^\tau|\beta|^m\left(1 + \frac{1}{|\beta|^{m-m_1}}\right) \\ \leq C_4 m^\tau|\beta|^m\left(1 + \frac{1}{|\beta|}\right) &= C_7 m^\tau|\beta|^m \end{aligned}$$

and

$$\begin{aligned}|V_m - V_{m_1}| \geq |V_m| - |V_{m_1}| &\geq C_3 m^\tau |\beta|^m - C_4 m^\tau |\beta|^{m_1} \\ &= C_3 m^\tau |\beta|^m \left(1 - \frac{C_4}{C_3 |\beta|^{m-m_1}}\right) \\ &\geq C_3 m^\tau |\beta|^m \left(1 - \frac{C_4}{C_3|\beta|}\right) = C_8 m^\tau |\beta|^m.\end{aligned}$$

Therefore, we have

$$C_6 n^\sigma |\alpha|^n \leq |U_n - U_{n_1}| = |V_m - V_{m_1}| \leq C_7 m^\tau |\beta|^m \tag{5.3.3}$$

and

$$C_5 n^\sigma |\alpha|^n \geq |U_n - U_{n_1}| = |V_m - V_{m_1}| \geq C_8 m^\tau |\beta|^m. \tag{5.3.4}$$

Note that we proved (5.3.3) and (5.3.4) only under the assumption that $n > n_1 \geq N_2$ and $m > m_1 \geq M_2$. However since by assumption $n > n_1 \geq N_0$ and $m > m_1 \geq M_0$ we have $|U_n| > |U_{n_1}|$ and $|V_m| > |V_{m_1}|$ respectively. Therefore by enlarging C_7 and C_5 respectively decreasing C_6 and C_8 we obtain that (5.3.3) and (5.3.4) also holds under the assumption that $n \geq N_2$, $n_1 \geq N_0$ and $m \geq M_2$, $m_1 \geq M_0$. Thus

$$n \leq m \frac{\log|\beta|}{\log|\alpha|} + \tau \frac{\log m}{\log|\alpha|} + C_9, \tag{5.3.5}$$

where $0 < \frac{\log|\beta|}{\log|\alpha|} < 1$.

Inequality (5.3.5) implies that $m > n$ for $m \geq M_3$, where M_3 is sufficiently large. Denote by N_3 the infimum for n when $m \geq M_3$. Let us assume in the following that $n > N_4 = \max\{N_0, N_1, N_2, N_3, 2\}$ and $m > M_4 = \max\{M_0, M_1, M_2, M_3, 2\}$ (and $n_1 \geq N_0$ and $m_1 \geq M_0$). Let us note that if m is bounded from above by an effectively computable constant as M_4 also n is bounded from above by an effective computable constant due to inequality (5.3.5). Thus we can deduce that also c is bounded and Theorem 5.2 holds in this case. Note that we assume for technical reasons that $N_4, M_4 \geq 2$. Therefore we may assume that $m > M_4$ and hence $m > n$.

Furthermore let us fix the following notation for the rest of the paper. Let us write

$$K = \mathbb{Q}(\alpha_1, \ldots, \alpha_t, \beta_1, \ldots, \beta_s) \quad \text{and} \quad d = [K : \mathbb{Q}].$$

5.3.2 Linear forms in logarithms

We refer to equation (5.1.1) and make use of the asymptotic estimates (5.3.1) and (5.3.2). Thus we get

$$\big(a(n)\alpha^n + L(a'\alpha'^n)\big) - \big(a(n_1)\alpha^{n_1} + L(a'\alpha'^{n_1})\big) = \big(b(m)\beta^m + L(b'\beta'^m)\big) - \big(b(m_1)\beta^{m_1} + L(b'\beta'^{m_1})\big)$$

Collecting the "large" terms on the left hand side of the equation we obtain

$$a(n)\alpha^n - b(m)\beta^m = a(n_1)\alpha^{n_1} - b(m_1)\beta^{m_1} + L\left(a'\alpha'^n + a'\alpha'^{n_1} + b'\beta'^m + b'\beta'^{m_1}\right)$$

and therefore the inequality

$$|a(n)\alpha^n - b(m)\beta^m| \le |a(n_1)||\alpha|^{n_1} + |b(m_1)||\beta|^{m_1} + a'\alpha'^n + a'\alpha'^{n_1} + b'\beta'^m + b'\beta'^{m_1}.$$

Dividing through $b(m)\beta^m$ and using the inequalities (5.3.3) and (5.3.4), we get (note that we assume $n \ge N_3$ and $m \ge M_3$, i.e. $|a(n)| \ge |a(n_1)|$ and $|b(m)| \ge |b(m_1)|$):

$$\begin{aligned}\left|\frac{a(n)\alpha^n}{b(m)\beta^m} - 1\right| &\le \frac{|a(n_1)||\alpha|^{n_1}}{|b(m)||\beta|^m} + \frac{|b(m_1)||\beta|^{m_1}}{|b(m)||\beta|^m} + \frac{a'\alpha'^n}{|b(m)||\beta|^m} + \frac{a'\alpha'^{n_1}}{|b(m)||\beta|^m} + \frac{b'\beta'^m}{|b(m)||\beta|^m} + \frac{b'\beta'^{m_1}}{|b(m)||\beta|^m}\\ &\le \frac{C_7 m^\tau |a(n_1)||\alpha|^{n_1}}{C_6 n^\sigma |b(m)||\alpha|^n} + \frac{|b(m_1)||\beta|^{m_1}}{|b(m)||\beta|^m} + \frac{C_7 m^\tau a'\alpha'^n}{C_6 n^\sigma |b(m)||\alpha|^n} + \frac{C_7 m^\tau a'\alpha'^{n_1}}{C_6 n^\sigma |b(m)||\alpha|^n}\\ &\quad + \frac{b'\beta'^m}{|b(m)||\beta|^m} + \frac{b'\beta'^{m_1}}{|b(m)||\beta|^m}\\ &\le C_{11}|\alpha|^{n_1-n} + |\beta|^{m_1-m} + C_{12}\left(\frac{|\alpha|}{\alpha'}\right)^{-n} + C_{13}|\alpha|^{n_1-n} + C_{14}\left(\frac{|\beta|}{\beta'}\right)^{-m} + C_{15}|\beta|^{m_1-m}\\ &\le C_{11}|\alpha|^{n_1-n} + |\beta|^{m_1-m} + C_{12}\left(\frac{|\alpha|}{\alpha'}\right)^{n_1-n} + C_{13}|\alpha|^{n_1-n} + C_{14}\left(\frac{|\beta|}{\beta'}\right)^{m_1-m} + C_{15}|\beta|^{m_1-m}\\ &\le \max\left\{C_{16}\left(\frac{|\alpha|}{\alpha'}\right)^{n_1-n}, C_{17}\left(\frac{|\beta|}{\beta'}\right)^{m_1-m}\right\}.\end{aligned}$$

Note that $\frac{m^\tau|a(n_1)|}{n^\sigma|b(m)|}\frac{m^\tau|a(n)|}{n^\sigma|b(m)|}$, $\frac{|b(m_1)|}{|b(m)|}$ and so on are bounded by absolute constants since $\deg(a) = \sigma$ and $\deg(b) = \tau$. Hence we obtain the inequality

$$\left|\frac{a(n)}{b(m)}\alpha^n\beta^{-m} - 1\right| \le \max\left\{C_{16}\left(\frac{|\alpha|}{\alpha'}\right)^{n_1-n}, C_{17}\left(\frac{|\beta|}{\beta'}\right)^{m_1-m}\right\}. \tag{5.3.6}$$

Let us introduce

$$\Lambda = n\log|\alpha| - m\log|\beta| + \log\left|\frac{a(n)}{b(m)}\right|$$

and assume that $|\Lambda| \le 0.5$ and $\frac{a(n)}{b(m)}\alpha^n\beta^{-m} > 0$. Further, we put

$$\Phi = e^\Lambda - 1 = \left|\frac{a(n)}{b(m)}\right||\alpha|^n|\beta|^{-m} - 1$$

and use the theorem of Baker and Wüstholz (Theorem 5.3) with the data

$$k = 3, \quad \eta_1 = \left|\frac{a(n)}{b(m)}\right|, \quad b_1 = 1, \quad \eta_2 = |\alpha|, \quad b_2 = n, \quad \eta_3 = |\beta|, \quad b_3 = -m.$$

Note that with this data we have $B = m$. It should be noted that we have complete information on the minimal polynomial of α and β. Therefore, $h'(\alpha)$, $h'(\beta)$ are effectively computable. Moreover, due to Lemma 5.5 we have $h_0\left(\frac{a(n)}{b(m)}\right) \le \widetilde{C}\log m$ and thus

$$h'\left(\frac{a(n)}{b(m)}\right) = \frac{1}{d}\max\left\{dh_0\left(\frac{a(n)}{b(m)}\right), \left|\log\left(\frac{a(n)}{b(m)}\right)\right|, 1\right\} \le \widetilde{C'}\log m.$$

Before we can apply Theorem 5.3 we have to ensure that $\Phi \ne 0$. Assume to the contrary that $\Phi = 0$, then $\frac{a(n)}{b(m)} = \pm\frac{\beta^m}{\alpha^n}$. With the use of Lemma 5.4 we get

$$\widetilde{C}\log m \ge h_0\left(\frac{a(n)}{b(m)}\right) = h_0\left(\frac{\beta^m}{\alpha^n}\right) \ge C_0\max\{n,m\} = C_0 m$$

which yields an absolute upper bound for m. Therefore also n and c are bounded, i.e. Theorem 5.2 holds in this special case.

An application of Theorem 5.3 yields

$$\log|\Phi| \ge -C(3,d)h'\left(\frac{a(n)}{b(m)}\right)h'(\alpha)h'(\beta)\log m - \log 2$$

and together with inequality (5.3.6) we have

$$\min\left\{(n-n_1)\log\left(\frac{|\alpha|}{\alpha'}\right), (m-m_1)\log\left(\frac{|\beta|}{\beta'}\right)\right\} < C_{18}(\log m)^2.$$

Thus we have proved so far:

Lemma 5.6. *Assume that* (n,m,n_1,m_1) *is a solution to equation* (5.1.1) *with* $m > m_1$. *Then we have*

$$\min\left\{(n-n_1)\log\left(\frac{|\alpha|}{\alpha'}\right), (m-m_1)\log\left(\frac{|\beta|}{\beta'}\right)\right\} < C_{18}(\log m)^2.$$

Note that in the case that $|\Lambda| > 0.5$ or $\frac{a(n)}{b(m)}\alpha^n\beta^{-m} < 0$ inequality (5.3.6) is possible only if

$$\max\left\{C_{16}\left(\frac{|\alpha|}{\alpha'}\right)^{n_1-n}, C_{17}\left(\frac{|\beta|}{\beta'}\right)^{m_1-m}\right\} \ge e^{\frac{1}{2}} - 1 > 0.648,$$

which leads to either

$$n - n_1 \le \frac{\log\left(\frac{C_{16}}{0.648}\right)}{\log\left(\frac{|\alpha|}{\alpha'}\right)}$$

or

$$m - m_1 \le \frac{\log\left(\frac{C_{17}}{0.648}\right)}{\log\left(\frac{|\beta|}{\beta'}\right)}.$$

These can be covered by the bound provided by Lemma 5.6 as long as we choose

$$C_{18} \ge \frac{1}{(\log M_3)^2} \max\left\{\log\left(\frac{C_{16}}{0.648}\right), \log\left(\frac{C_{17}}{0.648}\right)\right\}.$$

Now we have to distinguish between the following two cases:

Case 1. Let us assume that

$$\min\left\{(n-n_1)\log\left(\frac{|\alpha|}{\alpha'}\right), (m-m_1)\log\left(\frac{|\beta|}{\beta'}\right)\right\} = (n-n_1)\log\left(\frac{|\alpha|}{\alpha'}\right),$$

i.e. we assume that $\left(\frac{|\alpha|}{\alpha'}\right)^{n_1-n} \le \left(\frac{|\beta|}{\beta'}\right)^{m_1-m}$.

By collecting the "large terms" on the left hand side, we can rewrite equation (5.1.1) as

$$a(n)\alpha^n - a(n_1)\alpha^{n_1} - b(m)\beta^m = -b(m_1)\beta^{m_1} + L\left(a'\alpha'^n + a'\alpha'^{n_1} + b'\beta'^m + b'\beta'^{m_1}\right)$$

and obtain the inequality

$$\left|a(n)\alpha^{n_1}\left(\alpha^{n-n_1} - \frac{a(n_1)}{a(n)}\right) - b(m)\beta^m\right| \le |b(m_1)||\beta|^{m_1} + a'\alpha'^n + a'\alpha'^{n_1} + b'\beta'^m + b'\beta'^{m_1}.$$

Dividing through $b(m)\beta^m$ and using the inequalities (5.3.3) and (5.3.4), we get

$$\begin{aligned}\left|\frac{a(n)\alpha^{n_1}\left(\alpha^{n-n_1} - \frac{a(n_1)}{a(n)}\right)}{b(m)\beta^m} - 1\right| \le \frac{|b(m_1)||\beta|^{m_1}}{|b(m)||\beta|^m} + \frac{a'\alpha'^n}{|b(m)||\beta|^m} + \frac{a'\alpha'^{n_1}}{|b(m)||\beta|^m}\\ + \frac{b'\beta'^m}{|b(m)||\beta|^m} + \frac{b'\beta'^{m_1}}{|b(m)||\beta|^m},\end{aligned}$$

where

$$\begin{aligned}
\frac{|b(m_1)||\beta|^{m_1}}{|b(m)||\beta|^m} &\le \left(\frac{|\beta|}{\beta'}\right)^{m_1-m},\\
\frac{a'\alpha'^n}{|b(m)||\beta|^m} &\le \frac{C_7 m^\tau a'\alpha'^n}{C_6 n^\sigma |b(m)||\alpha|^n} \le C_{19}\left(\frac{|\alpha|}{\alpha'}\right)^{-n} \le C_{19}\left(\frac{|\alpha|}{\alpha'}\right)^{n_1-n} \le C_{19}\left(\frac{|\beta|}{\beta'}\right)^{m_1-m},\\
\frac{a'\alpha'^{n_1}}{|b(m)||\beta|^m} &\le \frac{C_7 m^\tau a'\alpha'^{n_1}}{C_6 n^\sigma |b(m)||\alpha|^n} \le C_{20}\left(\frac{|\alpha|}{\alpha'}\right)^{n_1-n} \le C_{20}\left(\frac{|\beta|}{\beta'}\right)^{m_1-m},\\
\frac{b'\beta'^m}{|b(m)||\beta|^m} &\le C_{21}\left(\frac{|\beta|}{\beta'}\right)^{-m} \le C_{21}\left(\frac{|\beta|}{\beta'}\right)^{m_1-m}\\
\frac{b'\beta'^{m_1}}{|b(m)||\beta|^m} &\le C_{22}|\beta|^{m_1-m} \le C_{22}\left(\frac{|\beta|}{\beta'}\right)^{m_1-m}.
\end{aligned}$$

Hence we obtain the inequality

$$\left|\frac{a(n)}{b(m)}\left(\alpha^{n-n_1}-\frac{a(n_1)}{a(n)}\right)\alpha^{n_1}\beta^{-m}-1\right|\le C_{23}\left(\frac{|\beta|}{\beta'}\right)^{m_1-m}. \tag{5.3.7}$$

Case 2. Let us assume that

$$\min\left\{(n-n_1)\log\left(\frac{|\alpha|}{\alpha'}\right),(m-m_1)\log\left(\frac{|\beta|}{\beta'}\right)\right\}=(m-m_1)\log\left(\frac{|\beta|}{\beta'}\right).$$

i.e. we assume that $\left(\frac{|\beta|}{\beta'}\right)^{m_1-m}\le\left(\frac{|\alpha|}{\alpha'}\right)^{n_1-n}$.

Similarly as in Case 1 we collect the "large terms" on the left hand side and rewrite equation (5.1.1) as

$$a(n)\alpha^n-b(m)\beta^m+b(m_1)\beta^{m_1}=-a(n_1)\alpha^{n_1}+L\left(a'\alpha'^n+a'\alpha'^{n_1}+b'\beta'^m+b'\beta'^{m_1}\right)$$

and obtain the inequality

$$\left|b(m)\beta^{m_1}\left(\beta^{m-m_1}-\frac{b(m_1)}{b(m)}\right)-a(n)\alpha^n\right|\le|a(n_1)||\alpha|^{n_1}+a'\alpha'^n+a'\alpha'^{n_1}+b'\beta'^m+b'\beta'^{m_1}.$$

We obtain the inequality

$$\left|\frac{b(m)}{a(n)}\left(\beta^{m-m_1}-\frac{b(m_1)}{b(m)}\right)\alpha^{-n}\beta^{m_1}-1\right|\le C_{28}\left(\frac{|\alpha|}{\alpha'}\right)^{n_1-n} \tag{5.3.8}$$

by the same arguments as in Case 1 by interchanging $a(n),\alpha,n,n_1,a'$ and α' with $b(m),\beta,m,m_1,b'$ and β'.

We want to apply Theorem 5.3 to both inequalities (5.3.7) and (5.3.8) respectively. Let us consider the first case more closely. We write

$$\Lambda_1=n_1\log|\alpha|-m\log|\beta|+\log\left|\frac{a(n)}{b(m)}\left(\alpha^{n-n_1}-\frac{a(n_1)}{a(n)}\right)\right|$$

and assume that $|\Lambda_1|\le 0.5$ and $\frac{a(n)}{b(m)}\left(\alpha^{n-n_1}-\frac{a(n_1)}{a(n)}\right)>0$. Further, we put

$$\Phi_1=e^{\Lambda_1}-1=\left|\frac{a(n)}{b(m)}\left(\alpha^{n-n_1}-\frac{a(n_1)}{a(n)}\right)\right||\alpha|^{n_1}|\beta|^{-m}-1$$

and aim to apply Theorem 5.3 with $B=m$. Further, we have

$$\eta_1=\left|\frac{a(n)}{b(m)}\left(\alpha^{n-n_1}-\frac{a(n_1)}{a(n)}\right)\right|,\quad b_1=1,\quad \eta_2=|\alpha|,\quad b_2=n_1,\quad \eta_3=|\beta|,\quad b_3=-m.$$

It should be noted that as before $h'(\alpha)$ and $h'(\beta)$ are effectively computable. For $h'(\eta_1)$, we can use the properties of height and the results of Lemma 5.6 and Lemma 5.5 to get

$$\begin{aligned} h_0(\eta_1) &= h_0\left(\frac{a(n)}{b(m)}\left(\alpha^{n-n_1} - \frac{a(n_1)}{a(n)}\right)\right) \\ &\leq h_0\left(\frac{a(n)}{b(m)}\right) + (n-n_1)h_0(\alpha) + h_0\left(\frac{a(n_1)}{a(n)}\right) + \log 2 \\ &\leq h_0\left(\frac{a(n)}{b(m)}\right) + \frac{C_{18}(\log m)^2}{\log\left(\frac{|\alpha|}{\alpha'}\right)} h_0(\alpha) + h_0\left(\frac{a(n_1)}{a(n)}\right) + \log 2 \\ &\leq C_{29}(\log m)^2 \end{aligned}$$

and thus

$$h'(\eta_1) = \frac{1}{d}\max\{dh_0(\eta_1), |\log \eta_1|, 1\} \leq C_{30}(\log m)^2.$$

Now let us turn to the second case. We write

$$\Lambda_2 = m_1 \log|\beta| - n\log|\alpha| + \log\left|\frac{b(m)}{a(n)}\left(\beta^{m-m_1} - \frac{b(m_1)}{b(m)}\right)\right|$$

and assume that $|\Lambda_2| \leq 0.5$ and $\frac{b(m)}{a(n)}\left(\beta^{m-m_1} - \frac{b(m_1)}{b(m)}\right) > 0$. Further, we put

$$\Phi_2 = e^{\Lambda_2} - 1 = \left|\frac{b(m)}{a(n)}\left(\beta^{m-m_1} - \frac{b(m_1)}{b(m)}\right)\right| |\alpha|^{-n}|\beta|^{m_1} - 1$$

and aim to apply Theorem 5.3. As in the previous case we also have $B = m$. Further, we have

$$\eta_1 = \left|\frac{b(m)}{a(n)}\left(\beta^{m-m_1} - \frac{b(m_1)}{b(m)}\right)\right|, \quad b_1 = 1, \quad \eta_2 = |\alpha|, \quad b_2 = -n, \quad \eta_3 = |\beta|, \quad b_3 = m_1.$$

It should be noted that as before $h'(\alpha)$ and $h'(\beta)$ are effectively computable. For $h'(\eta_1)$, we can use the properties of height and the results of Lemma 5.6 and Lemma 5.5 to get

$$\begin{aligned} h_0(\eta_1) &= h_0\left(\frac{b(m)}{a(n)}\left(\beta^{m-m_1} - \frac{b(m_1)}{b(m)}\right)\right) \\ &\leq h_0\left(\frac{b(m)}{a(n)}\right) + (m-m_1)h_0(\beta) + h_0\left(\frac{b(m_1)}{b(m)}\right) + \log 2 \\ &\leq h_0\left(\frac{b(m)}{a(n)}\right) + \frac{C_{18}(\log m)^2}{\log\left(\frac{|\beta|}{\beta'}\right)} h_0(\beta) + h_0\left(\frac{b(m_1)}{b(m)}\right) + \log 2 \\ &\leq C_{31}(\log m)^2 \end{aligned}$$

and thus

$$h'(\eta_1) = \frac{1}{d}\max\{dh_0(\eta_1), |\log \eta_1|, 1\} \leq C_{32}(\log m)^2.$$

Before we can apply Theorem 5.3 we have to ensure that $\Phi_i \neq 0$ for $i = 1, 2$. Firstly we deal with the assumption that $\Phi_1 = 0$, i.e. $\pm\frac{a(n)}{b(m)}\left(\alpha^{n-n_1} - \frac{a(n_1)}{a(n)}\right) = \frac{\beta^m}{\alpha^{n_1}}$. This together with Lemma 5.6 yields

$$h_0\left(\frac{\beta^m}{\alpha^n}\right) = h_0\left(\frac{a(n)}{b(m)}\left(\alpha^{n-n_1} - \frac{a(n_1)}{a(n)}\right)\right) < C_{29}(\log m)^2$$

as determined before. With the use of Lemma 5.4 we get

$$C_{29}(\log m)^2 > h_0\left(\frac{\beta^m}{\alpha^{n_1}}\right) \geq C_0 \max\{n_1, m\} \geq C_0 m.$$

Thus m is bounded by an effectively computable constant. Besides, since $m > n$ so n is also bounded and therefore also c, i.e. Theorem 5.2 holds in this case. A similar argument also applies to Case 2.

Now, we are ready to apply Theorem 5.3 and get

$$\log|\Phi_i| > -C(3,d)h'(\eta_1)h'(\alpha)h'(\beta)\log m - \log 2$$

for $i = 1, 2$. Combining this inequality with the inequalities (5.3.7) and (5.3.8), we obtain

$$(m - m_1)\log\left(\frac{|\beta|}{\beta'}\right) < C_{33}(\log m)^3 \quad \text{and} \quad (n - n_1)\log\left(\frac{|\alpha|}{\alpha'}\right) < C_{34}(\log m)^3$$

respectively. Let $C_{35} = \max\{C_{33}, C_{34}\}$. These two inequalities yield together with Lemma 5.6 the following lemma:

Lemma 5.7. *Assume that (n, m, n_1, m_1) is a solution to equation (5.1.1) with $m > m_1$. Then we have*

$$\max\left\{(n - n_1)\log\left(\frac{|\alpha|}{\alpha'}\right), (m - m_1)\log\left(\frac{|\beta|}{\beta'}\right)\right\} < C_{35}(\log m)^3.$$

Note that in view of $|\Lambda_1| > 0.5$ or $\frac{a(n)}{b(m)}\left(\alpha^{n-n_1} - \frac{a(n_1)}{a(n)}\right) < 0$, inequality (5.3.7) is possible only if

$$C_{23}\left(\frac{|\beta|}{\beta'}\right)^{m_1-m} \geq e^{\frac{1}{2}} - 1 > 0.648,$$

which leads to $m - m_1 \leq \frac{\log\left(\frac{C_{23}}{0.648}\right)}{\log\left(\frac{|\beta|}{\beta'}\right)}$. In view of $|\Lambda_2| > 0.5$ or $\frac{b(m)}{a(n)}\left(\beta^{m-m_1} - \frac{b(m_1)}{b(m)}\right) < 0$, inequality (5.3.8) is possible only if

$$C_{28}\left(\frac{|\alpha|}{\alpha'}\right)^{n_1-n} \geq e^{\frac{1}{2}} - 1 > 0.648,$$

which leads to $n - n_1 \leq \frac{\log\left(\frac{C_{28}}{0.648}\right)}{\log\left(\frac{|\alpha|}{\alpha'}\right)}$. Both cases can be covered by the bound provided by Lemma 5.7 as long as

$$C_{35} \geq \frac{1}{(\log M_3)^3}\max\left\{\log\left(\frac{C_{28}}{0.648}\right), \log\left(\frac{C_{23}}{0.648}\right)\right\}.$$

One more time we have to apply Theorem 5.3. This time we rewrite equation (5.1.1) by collecting "large" terms on the left hand side as

$$a(n)\alpha^n - a(n_1)\alpha^{n_1} - b(m)\beta^m + b(m_1)\beta^{m_1} = L\left(a'\alpha'^n + a'\alpha'^{n_1} + b'\beta'^m + b'\beta'^{m_1}\right)$$

and obtain

$$\left|a(n)\alpha^{n_1}\left(\alpha^{n-n_1} - \frac{a(n_1)}{a(n)}\right) - b(m)\beta^{m_1}\left(\beta^{m-m_1} - \frac{b(m_1)}{b(m)}\right)\right| \le a'\alpha'^n + a'\alpha'^{n_1} + b'\beta'^m + b'\beta'^{m_1}.$$

Dividing through $b(m)\beta^{m_1}\left(\beta^{m-m_1} - \frac{b(m_1)}{b(m)}\right)$ and using the inequalities (5.3.3) and (5.3.4) we get

$$\begin{aligned}\left|\frac{a(n)\alpha^{n_1}\left(\alpha^{n-n_1} - \frac{a(n_1)}{a(n)}\right)}{b(m)\beta^{m_1}\left(\beta^{m-m_1} - \frac{b(m_1)}{b(m)}\right)} - 1\right| \le{}& \frac{a'\alpha'^n}{|b(m)||\beta|^{m_1}\left|\beta^{m-m_1} - \frac{b(m_1)}{b(m)}\right|} + \frac{a'\alpha'^{n_1}}{|b(m)||\beta|^{m_1}\left|\beta^{m-m_1} - \frac{b(m_1)}{b(m)}\right|}\\ &+ \frac{b'\beta'^m}{|b(m)||\beta|^{m_1}\left|\beta^{m-m_1} - \frac{b(m_1)}{b(m)}\right|} + \frac{b'\beta'^{m_1}}{|b(m)||\beta|^{m_1}\left|\beta^{m-m_1} - \frac{b(m_1)}{b(m)}\right|}.\end{aligned}$$

We make use of inequality (5.3.5) to get

$$\begin{aligned}\alpha'^n &= \exp\left(n\log\alpha'\right)\\ &< \exp\left(m\frac{\log|\beta|}{\log|\alpha|}\log\alpha' + \tau\frac{\log\alpha'}{\log|\alpha|}\log m + C_9\log\alpha'\right)\\ &= \exp\left(m\frac{\log\alpha'}{\log|\alpha|}\log|\beta|\right)(m^\tau)^{\frac{\log\alpha'}{\log|\alpha|}}\exp\left(C_9\log\alpha'\right)\\ &< C_{36}m^\tau\gamma^m,\end{aligned}$$

where $\gamma = |\beta|^{\frac{\log\alpha'}{\log|\alpha|}}$. Note that since $|\alpha| > \alpha' > 1$ and $|\beta| > 1$ we have that $|\beta| > \gamma > 1$. So that

$$\begin{aligned}\frac{a'\alpha'^n}{|b(m)||\beta|^{m_1}\left|\beta^{m-m_1} - \frac{b(m_1)}{b(m)}\right|} &< \frac{C_{36}a'm^\tau\gamma^m}{|b(m)||\beta|^m\left|1 - \beta^{m_1-m}\frac{b(m_1)}{b(m)}\right|}\\ &= \frac{C_{36}a'm^\tau\gamma^m}{|b(m)||\beta|^m\left|1 - \frac{b(m_1)}{b(m)\beta^{m-m_1}}\right|}\\ &\le \frac{C_{36}a'm^\tau\gamma^m}{|b(m)||\beta|^m\left|1 - \frac{1}{\beta}\right|} \le C_{37}\left(\frac{|\beta|}{\gamma}\right)^{-m}.\end{aligned}$$

In addition, since we assume that $\alpha' > 1$, we have

$$\begin{aligned}\frac{a'\alpha'^{n_1}}{|b(m)||\beta|^{m_1}\left|\beta^{m-m_1} - \frac{b(m_1)}{b(m)}\right|} &< \frac{a'\alpha'^n}{|b(m)||\beta|^m\left|1 - \frac{b(m_1)}{b(m)\beta^{m-m_1}}\right|}\\ &< \frac{C_{36}a'm^\tau\gamma^m}{|b(m)||\beta|^m\left|1 - \frac{1}{\beta}\right|} \le C_{37}\left(\frac{|\beta|}{\gamma}\right)^{-m}.\end{aligned}$$

Furthermore,

$$\frac{b'\beta'^m}{|b(m)||\beta|^{m_1}\left|\beta^{m-m_1}-\frac{b(m_1)}{b(m)}\right|}\le\frac{b'\beta'^m}{|b(m)||\beta|^m\left|1-\frac{1}{\beta}\right|}\le C_{38}\left(\frac{|\beta|}{\beta'}\right)^{-m}.$$

Since we may assume that $\beta'>1$ we get

$$\frac{b'\beta'^{m_1}}{|b(m)||\beta|^{m_1}\left|\beta^{m-m_1}-\frac{b(m_1)}{b(m)}\right|}\le\frac{b'\beta'^m}{|b(m)||\beta|^m\left|1-\frac{1}{\beta}\right|}=C_{39}\left(\frac{|\beta|}{\beta'}\right)^{-m}.$$

Therefore,

$$\left|\frac{a(n)\left(\alpha^{n-n_1}-\frac{a(n_1)}{a(n)}\right)}{b(m)\left(\beta^{m-m_1}-\frac{b(m_1)}{b(m)}\right)}\alpha^{n_1}\beta^{-m_1}-1\right|\le C_{40}\Gamma^{-m}, \tag{5.3.9}$$

where $\Gamma=\min\left\{\frac{|\beta|}{\beta'},\frac{|\beta|}{\gamma}\right\}$. In this final step we consider the linear form

$$\Lambda_3=n_1\log|\alpha|-m_1\log|\beta|+\log\left|\frac{a(n)\left(\alpha^{n-n_1}-\frac{a(n_1)}{a(n)}\right)}{b(m)\left(\beta^{m-m_1}-\frac{b(m_1)}{b(m)}\right)}\right|$$

and assume that $|\Lambda_3|\le 0.5$ and $\frac{a(n)\left(\alpha^{n-n_1}-\frac{a(n_1)}{a(n)}\right)}{b(m)\left(\beta^{m-m_1}-\frac{b(m_1)}{b(m)}\right)}>0$. Further, we put

$$\Phi_3=e^{\Lambda_3}-1=\left|\frac{a(n)\left(\alpha^{n-n_1}-\frac{a(n_1)}{a(n)}\right)}{b(m)\left(\beta^{m-m_1}-\frac{b(m_1)}{b(m)}\right)}\right||\alpha|^{n_1}|\beta|^{-m_1}-1.$$

As before we take $B=m$ and we choose

$$\eta_1=\left|\frac{a(n)\left(\alpha^{n-n_1}-\frac{a(n_1)}{a(n)}\right)}{b(m)\left(\beta^{m-m_1}-\frac{b(m_1)}{b(m)}\right)}\right|,\quad b_1=1,\quad \eta_2=|\alpha|,\quad b_2=n_1,\quad \eta_3=|\beta|,\quad b_3=-m_1.$$

For $h'(\eta_1)$, we can use the properties of the height and the results of Lemma 5.5 and Lemma 5.7 to get

$$\begin{aligned}h_0(\eta_1)&=h_0\left(\frac{a(n)\left(\alpha^{n-n_1}-\frac{a(n_1)}{a(n)}\right)}{b(m)\left(\beta^{m-m_1}-\frac{b(m_1)}{b(m)}\right)}\right)\\&\le h_0\left(\frac{a(n)}{b(m)}\right)+(n-n_1)h_0(\alpha)+(m-m_1)h_0(\beta)+h_0\left(\frac{a(n_1)}{a(n)}\right)+h_0\left(\frac{b(m_1)}{b(m)}\right)+2\log 2\\&\le h_0\left(\frac{a(n)}{b(m)}\right)+\frac{C_{35}h_0(\alpha)(\log m)^3}{\log\left(\frac{|\alpha|}{\alpha'}\right)}+\frac{C_{35}h_0(\beta)(\log m)^3}{\log\left(\frac{|\beta|}{\beta'}\right)}+h_0\left(\frac{a(n_1)}{a(n)}\right)+h_0\left(\frac{b(m_1)}{b(m)}\right)+2\log 2\\&\le C_{41}(\log m)^3\end{aligned}$$

and thus

$$h'(\eta_1) = \frac{1}{d}\max\{dh_0(\eta_1), |\log \eta_1|, 1\} \leq C_{42}(\log m)^3.$$

It should be noted that as before $h'(\alpha)$ and $h'(\beta)$ are effectively computable.

Before we can apply Theorem 5.3 we have to ensure that $\Phi_3 \neq 0$, i.e.

$$\pm \frac{a(n)\left(1 - \frac{a(n_1)\alpha^{n_1-n}}{a(n)}\right)}{b(m)\left(1 - \frac{b(m_1)\beta^{m_1-m}}{b(m)}\right)} = \frac{\beta^m}{\alpha^n}.$$

This together with Lemma 5.7 yields

$$h_0\left(\frac{\beta^m}{\alpha^n}\right) = h_0\left(\frac{a(n)\left(1 - \frac{a(n_1)\alpha^{n_1-n}}{a(n)}\right)}{b(m)\left(1 - \frac{b(m_1)\beta^{m_1-m}}{b(m)}\right)}\right) < C_{43}(\log m)^3.$$

Similar to the argument in Case 1 and Case 2, we deduce by using Lemma 5.4 that

$$C_{43}(\log m)^3 > h_0\left(\frac{\beta^m}{\alpha^n}\right) \geq C_0 \max\{n, m\} \geq C_0 m.$$

Thus m is bounded by an effectively computable constant. Besides, since $m > n$ so n is also bounded and therefore also c and we deduce Theorem 5.2 in this case.

Now an application of Theorem 5.3 yields

$$\log|\Phi_3| > -C(3,d)h'(\eta_1)h'(\alpha)h'(\beta)\log m - \log 2.$$

Combining this inequality with inequality (5.3.9) we get

$$m \log \Gamma + \log C_{42} < C_{44}(\log m)^4 + \log 2.$$

which yields $m < C_{45}$.

Similarly as in the cases above the assumption that $|\Lambda_3| > 0.5$ or

$$\frac{a(n)\left(\alpha^{n-n_1} - \frac{a(n_1)}{a(n)}\right)}{b(m)\left(\beta^{m-m_1} - \frac{b(m_1)}{b(m)}\right)} < 0$$

leads in view of inequality (5.3.9) to

$$C_{40}\Gamma^{-m} \geq e^{\frac{1}{2}} - 1 > 0.648,$$

which leads to $m \leq \frac{\log\left(\frac{C_{40}}{0.648}\right)}{\log \Gamma}$. These can be covered by the above bound $m < C_{45}$ as long as

$$C_{45} \geq \frac{\log\left(\frac{C_{40}}{0.648}\right)}{\log \Gamma}.$$

As a conclusion, if $n \geq N_3$ and $m \geq M_3$, we have $n < m < C_{45}$, where C_{45} is an effectively computable constant. Therefore, together with those finitely many cases where $n \leq N_4$, $m \leq M_4$ and all possible cases of (m, n) which yield $|\Phi|, |\Phi_i| = 0$ for $i = 1, 2, 3$, there can only be finitely many integers c having at least two distinct representations of the form $U_n - V_m$. The number of integers c and the corresponding values of c are both effectively computable. Therefore Theorem 5.2 is proved.

Chapter 6

Sums of Fibonacci numbers and powers of two

The content of this chapter is similar to the submitted joint work with Volker Ziegler titled "On Diophantine equations involving sums of Fibonacci numbers and powers of 2" [38].[1]

6.1 Introduction

There is a vast literature on solving Diophantine equations involving the sequence $\{F_n\}_{n\geq 0}$ of Fibonacci numbers (defined by $F_0 = 0$, $F_1 = 1$ and $F_{n+2} = F_{n+1} + F_n$ for $n \geq 0$), the sequence $\{F_n^{(k)}\}_{n\geq 0}$ of k-generalized Fibonacci numbers, the sequence $\{P_n\}_{n\geq 0}$ of Pell numbers or other recurrence sequences. For instance, recent results include Bravo and Luca [31] where they studied the Diophantine equation

$$F_n + F_m = 2^a.$$

In [28] they extended their work to k-generalized Fibonacci number $F_n^{(k)}$, and studied the equation

$$F_n^{(k)} + F_m^{(k)} = 2^a.$$

Besides, Bravo, Faye and Luca [27] studied the Diophantine equation

$$P_l + P_m + P_n = 2^a.$$

The most general results in this respect are due to Stewart [82], who studied representations of integers in two different bases. Note that e.g. the result due to Bravo and Luca [31] can be seen

[1]K. C. Chim was supported by the Austrian Science Fund (FWF) under the projects P26114 and W1230.

as an attempt to find all integers that have only few digits in base 2 and the Zeckendorf expansion simultaneously. Also Luca [58] proves a similar result. Finally let us mention a recent result due to Meher and Rout [65] on the Diophantine equation

$$U_{n_1} + \cdots + U_{n_t} = b_1 p_1^{z_1} + \cdots + b_s p_s^{z_s}$$

in non-negative integers $n_1, \ldots, n_t, z_1, \ldots, z_s$, where $\{U_n\}_{n \geq 0}$ is a binary, non-degenerate recurrence sequence with positive discriminant, $b_1, \ldots, b_s$ are fixed non-negative integers and $p_1, \ldots, p_s$ are fixed primes.

Also recently Diophantine equations have been studied which can be regarded as variants of Pillai's problem [71]. For instance, Chim, Pink and Ziegler [36] obtained all the integers c such that the Diophantine equation

$$F_n - T_m = c$$

has at least two solutions. Here T_m denotes the m-th Tribonacci number. Ddamulira, Luca, and Rakotomalala [39] considered the Diophantine equation

$$F_n - 2^m = c$$

and found all integers c for which this Diophantine equation has at least two solutions. Recently, Bravo, Luca and Yazán [32] considered the Diophantine equation

$$T_n - 2^m = c$$

instead. The most general result is due to Chim, Pink and Ziegler [37] who considered the case, where U_n and V_m are the n-th and m-th numbers in linear recurrence sequences $\{U_n\}_{n \geq 0}$ and $\{V_m\}_{m \geq 0}$ respectively and found effective upper bounds for $|c|$ such that the Diophantine equation

$$U_n - V_m = c$$

has at least two solutions.

All the problems stated above are solved by a similar strategy, the iterated application of linear forms in logarithms. We extend this strategy and study the two Diophantine equations

$$F_{n_1} + F_{n_2} = 2^{a_1} + 2^{a_2} + 2^{a_3}$$

and

$$F_{m_1} + F_{m_2} + F_{m_3} = 2^{t_1} + 2^{t_2}.$$

In particular, we prove the following two theorems.

Theorem 6.1. *Let $(n_1, n_2, a_1, a_2, a_3) \in \mathbb{N}^5$ be a solution to the Diophantine equation*

$$F_{n_1} + F_{n_2} = 2^{a_1} + 2^{a_2} + 2^{a_3} \tag{6.1.1}$$

such that $n_1 \geq n_2 \geq 0$ and $a_1 \geq a_2 \geq a_3 \geq 0$, then $n_1 \leq 18$ and $a_1 \leq 11$. In particular, equation (6.1.1) has exactly 78 solutions.

Theorem 6.2. *Let $(m_1, m_2, m_3, t_1, t_2) \in \mathbb{N}^5$ be a solution to the Diophantine equation*

$$F_{m_1} + F_{m_2} + F_{m_3} = 2^{t_1} + 2^{t_2} \tag{6.1.2}$$

such that $m_1 \geq m_2 \geq m_3 \geq 0$ and $t_1 \geq t_2 \geq 0$, then $m_1 \leq 16$ and $t_1 \leq 10$. In particular, equation (6.1.2) *has exactly* 116 *solutions.*

Remark 2. The list of solutions to equations (6.1.1) and (6.1.2) is given in the Appendix. So we keep the statement of Theorems 6.1.1 and 6.1.2 short and compact.

We shall prove both Theorems 6.1 and 6.2 by the typical strategy also performed in [31, 32, 36, 37, 39]. First we extract by a simple computer search all solutions $(n_1, n_2, a_1, a_2, a_3)$ with $n_1 < 360$ to equation (6.1.1) and all solutions $(m_1, m_2, m_3, t_1, t_2)$ with $m_1 < 360$ to equation (6.1.2), respectively. The key argument to obtain upper bounds for $n_1 = \max\{n_1, n_2, a_1, a_2, a_3\}$ and $m_1 = \max\{m_1, m_2, m_3, t_1, t_2\}$ respectively is to apply lower bounds for linear forms in logarithms. This is done in the seven steps described below, where $c_1, \dots, c_7$ denote effectively computable constants. These seven steps are in case of the proof of Theorem 6.1 the following:

Step 1 We obtain an upper bound

$$\min\{(a_1 - a_2)\log 2, (n_1 - n_2)\log\alpha\} \leq c_1 \log n_1.$$

Hence we have to distinguish between the following two cases:

Case 1 $\min\{(a_1 - a_2)\log 2, (n_1 - n_2)\log\alpha\} = (a_1 - a_2)\log 2 \leq c_1 \log n_1$

Case 2 $\min\{(a_1 - a_2)\log 2, (n_1 - n_2)\log\alpha\} = (n_1 - n_2)\log\alpha \leq c_1 \log n_1$

Step 2 We consider Case 1 and show that $(a_1 - a_2)\log 2 \leq c_1 \log n_1$ yields

$$\min\{(a_1 - a_3)\log 2, (n_1 - n_2)\log\alpha\} \leq c_2(\log n_1)^2.$$

Thus we have to further subdivide Case 1 into the following two cases:

Case 1A $\min\{(a_1 - a_3)\log 2, (n_1 - n_2)\log\alpha\} = (a_1 - a_3)\log 2 \leq c_2(\log n_1)^2$

Case 1B $\min\{(a_1 - a_3)\log 2, (n_1 - n_2)\log\alpha\} = (n_1 - n_2)\log\alpha \leq c_2(\log n_1)^2$

Step 3 We consider Case 1A and show that $(a_1 - a_3)\log 2 \leq c_2(\log n_1)^2$ implies that

$$(n_1 - n_2)\log\alpha \leq c_3(\log n_1)^3.$$

Step 4 We consider Case 1B and show that $(a_1 - a_2)\log 2 \leq c_1 \log n_1$ and $(n_1 - n_2)\log\alpha \leq c_2(\log n_1)^2$ yield the upper bound

$$(a_1 - a_3)\log 2 \leq c_4(\log n_1)^3.$$

Step 5 We consider Case 2 and show that $(n_1 - n_2)\log\alpha \leq c_1 \log n_1$ yields the upper bound

$$(a_1 - a_2)\log 2 \leq c_5(\log n_1)^2.$$

Step 6 We continue to consider Case 2 and show that assuming the upper bounds $(a_1-a_2)\log 2 \leq c_5(\log n_1)^2$ and $(n_1-n_2)\log\alpha \leq c_1 \log n_1$ yield the upper bound

$$(a_1-a_3)\log 2 \leq c_4(\log n_1)^3.$$

This is basically Step 4 again, but with probably slightly different constants. However after Step 6 we have found upper bounds for $(a_1-a_2)\log 2$, $(a_1-a_3)\log 2$ and $(n_1-n_2)\log\alpha$.

Step 7 We show that the upper bounds found in the previous steps yield an inequality of the form $n_1 \leq c_7(\log n_1)^4$. Thus we obtain an absolute bound for n_1.

As soon as we have found an upper bound for n_1 we go through all seven steps again but apply instead of lower bounds for linear forms in logarithms the Baker-Davenport reduction method and obtain in all steps small, absolute bounds respectively. In case the Baker-Davenport reduction method fails we can make use of a criteria of Legendre for continued fractions to reduce the huge upper bounds to rather small upper bounds. Indeed we succeed to show that all solutions satisfy $n_1 < 360$, which already have been found by our previous computer search.

Of course, a slight modification of these seven steps also leads to a proof of Theorem 6.2.

It should be noted that due to having more terms in each equation as compared to the equations considered in [31, 32, 36, 37, 39], we apply several times more the results of linear forms in logarithms and the reduction method. E.g. instead of using only twice the results on linear forms in logarithms and the reduction method as in [31] we apply them seven times.

6.2 Preliminaries

In this section, the result of linear forms in logarithms by Baker and Wüstholz [19] is stated. Besides, we state a lemma from [27], which is a generalization of a result due to Baker and Davenport [17] the so-called Baker-Davenport reduction method. Both results will be used to prove Theorems 6.1 and 6.2.

6.2.1 A lower bound for linear forms in logarithms of algebraic numbers

In 1993, Baker and Wüstholz [19] obtained an explicit bound for linear forms in logarithms with a linear dependence on $\log B$, where $B \geq e$ denotes an upper bound for the height of the linear form (to be defined later in this section). It is a vast improvement compared with lower bounds with a dependence on higher powers of $\log B$ in preceding publications by other mathematicians in particular Baker's original results [1, 2, 3].

Denote by $\alpha_1, \ldots, \alpha_k$ algebraic numbers, not 0 or 1, and by $\log \alpha_1, \ldots, \log \alpha_k$ a fixed determination of their logarithms. Let $K = \mathbb{Q}(\alpha_1, \ldots, \alpha_k)$ and let $d = [K : \mathbb{Q}]$ be the degree of K over $\mathbb{Q}$. For any $\alpha \in K$, suppose that its minimal polynomial over the integers is

$$g(x) = a_0 x^\delta + a_1 x^{\delta-1} + \cdots + a_\delta = a_0 \prod_{j=1}^{\delta} \left(x - \alpha^{(j)} \right)$$

where $\alpha^{(j)}$, $j = 1, \ldots, \delta$, are all the roots of $g(x)$. The absolute logarithmic Weil height of α is defined as

$$h_0(\alpha) = \frac{1}{\delta} \left(\log |a_0| + \sum_{j=1}^{\delta} \log \left(\max \left\{ |\alpha^{(j)}|, 1 \right\} \right) \right).$$

Then the modified height $h'(\alpha)$ is defined by

$$h'(\alpha) = \frac{1}{d} \max\{h(\alpha), |\log \alpha|, 1\},$$

where $h(\alpha) = d h_0(\alpha)$ is the standard logarithmic Weil height of α.

Let us consider the linear form

$$L(z_1, \ldots, z_k) = b_1 z_1 + \cdots + b_k z_k,$$

where $b_1, \ldots, b_k$ are rational integers, not all 0 and define

$$h'(L) = \frac{1}{d} \max\{h(L), 1\},$$

where $h(L) = d \log \left(\max_{1 \le j \le k} \left\{ \frac{|b_j|}{b} \right\} \right)$ is the logarithmic Weil height of L, with b as the greatest common divisor of $b_1, \ldots, b_k$. If we write $B = \max\{|b_1|, \ldots, |b_k|, e\}$, then we get

$$h'(L) \le \log B.$$

With these notations we are able to state the following result due to Baker and Wüstholz [19].

Theorem 6.3. *If $\Lambda = L(\log \alpha_1, \ldots, \log \alpha_k) \ne 0$, then*

$$\log |\Lambda| \ge -C(k, d) h'(\alpha_1) \cdots h'(\alpha_k) h'(L),$$

where

$$C(k, d) = 18(k+1)!\, k^{k+1} (32d)^{k+2} \log(2kd).$$

With $|\Lambda| \le \frac{1}{2}$, we have $\frac{1}{2}|\Lambda| \le |\Phi| \le 2|\Lambda|$, where

$$\Phi = e^\Lambda - 1 = \alpha_1^{b_1} \cdots \alpha_k^{b_k} - 1,$$

so that

$$\log\left|\alpha_1^{b_1}\cdots\alpha_k^{b_k}-1\right|\geq \log|\Lambda|-\log 2.$$

We apply Theorem 6.3 mainly in the situation where $K=\mathbb{Q}(\sqrt{5})$, $k=3$ and $d=2$. In this case we obtain

$$C(3,2)=18\cdot 4!\cdot 3^4\cdot 64^5\log 12<9.34\cdot 10^{13}.$$

We will use this value throughout the paper without any further reference. Besides, let us recall some well known properties of the absolute logarithmic height:

$$\begin{aligned} h_0(\eta\pm\gamma) &\leq h_0(\eta)+h_0(\gamma)+\log 2,\\ h_0(\eta\gamma^{\pm 1}) &\leq h_0(\eta)+h_0(\gamma),\\ h_0(\eta^{\ell}) &= |\ell|h_0(\eta), \end{aligned}$$

where η,γ are some algebraic numbers and $\ell\in\mathbb{Z}$.

6.2.2 A generalized result of Baker and Davenport

The following result will be used to reduce the huge upper bounds for n_1 and m_1 found in Propositions 6.1 and 6.2 respectively. Let us state Lemma 6 in [27] which is regarded as a generalization of a result due to Baker and Davenport [17]. We denote by $\|x\|=\min\{|x-n|:n\in\mathbb{Z}\}$ the distance from $x\in\mathbb{R}$ to the nearest integer.

Lemma 6.4. *Let M be a positive integer, let p/q be a convergent of the continued fraction of the irrational γ such that $q>6M$, and let A,B,μ be some real numbers with $A>0$ and $B>1$. Let $\varepsilon:=\|\mu q\|-M\|\gamma q\|$. If $\varepsilon>0$, then there is no solution to the inequality*

$$0<|u\gamma-v+\mu|<AB^{-w}, \tag{6.2.1}$$

in positive integers u,v and w with

$$u\leq M \qquad \text{and} \qquad w\geq\frac{\log(Aq/\varepsilon)}{\log B}.$$

Remark 3. Let us explain how we will make use of Lemma 6.4 and explain how we proceed, if we are given an inequality of the form (6.2.1) and an upper bound M for solutions with $u\leq M$. We start with the smallest denominator $q=q_j$ of the j-th convergent $\frac{p_j}{q_j}$ of γ that exceeds $6M$. If $\varepsilon=\|\mu q\|-M\|\gamma q\|>0$, we compute the respective upper bound $w<\frac{\log(Aq/\varepsilon)}{\log B}$. If we get a negative ε, we consider the denominator q_{j+1} of the $(j+1)$-th convergent p_{j+1}/q_{j+1} instead. If a positive ε is obtained we compute the respective upper bound for w. If also the denominator q_{j+1} of the $(j+1)$-th convergent yields a negative ε we consider the denominator of the next convergent until we obtain a positive ε. Let us note that it is very unlikely that after several iterations no instance occurs with a positive ε, without any good reason. Usually this reason is a rational linear dependence on

$1, \gamma$ and μ. If we find such a linear relation involving 1, γ and μ, inequality (6.2.1) turns into an inequality of the form

$$0 < |u'\gamma - v'| < AB^{-w}$$

and we are reduced to a classical approximation problem and may use the theory of continued fractions. We will treat such cases separately.

6.3 Set up

During the proof of both theorems we use the Binet formula for the Fibonacci sequence in the following form:

$$F_k = \frac{\alpha^k - \beta^k}{\alpha - \beta} \qquad \forall k \geq 0, \tag{6.3.1}$$

where $\alpha = \frac{1+\sqrt{5}}{2}$ and $\beta = \frac{1-\sqrt{5}}{2}$ are the roots of the characteristic polynomial $x^2 - x - 1$. Moreover, we have the inequality

$$\alpha^{k-2} \leq F_k \leq \alpha^{k-1} \qquad \forall k \geq 1. \tag{6.3.2}$$

Without loss of generality, we may assume that $n_1 \geq n_2 \geq 0$ and $a_1 \geq a_2 \geq a_3 \geq 0$. Similarly, we may assume that $m_1 \geq m_2 \geq m_3 \geq 0$ and $t_1 \geq t_2 \geq 0$ when solving equation (6.1.2).

6.3.1 Scenario for equation (6.1.1)

Recall that we would like to solve

$$F_{n_1} + F_{n_2} = 2^{a_1} + 2^{a_2} + 2^{a_3}$$

for n_1, n_2, a_1, a_2 and a_3. Thus we get

$$\alpha^{n_1-2} \leq F_{n_1} \leq F_{n_1} + F_{n_2} = 2^{a_1} + 2^{a_2} + 2^{a_3} \leq 3 \cdot 2^{a_1}, \tag{6.3.3}$$

and

$$2\alpha^{n_1-1} \geq 2F_{n_1} \geq F_{n_1} + F_{n_2} = 2^{a_1} + 2^{a_2} + 2^{a_3} > 2^{a_1}. \tag{6.3.4}$$

Hence

$$n_1 - 2 \leq a_1 \cdot \frac{\log 2}{\log \alpha} + \frac{\log 3}{\log \alpha} \quad \text{and} \quad n_1 - 1 \geq (a_1 - 1) \cdot \frac{\log 2}{\log \alpha}, \tag{6.3.5}$$

where $\frac{\log 2}{\log \alpha} = 1.4404\ldots$. In particular, we have $n_1 > a_1$.

In a first step, we solve equation (6.1.1) for all $n_1 < 360$. Inequality (6.3.5) implies that in this case we have $a_1 < 251$. By a brute force computer enumeration for $0 \leq n_2 \leq n_1 < 360$ and $0 \leq a_3 \leq a_2 \leq a_1 < 251$ we found all solutions listed in the Appendix.

6.3.2 Scenario for equation (6.1.2)

Recall that we would like to solve

$$F_{m_1} + F_{m_2} + F_{m_3} = 2^{t_1} + 2^{t_2}$$

for m_1, m_2, m_3, t_1 and t_2. Similarly as above we obtain

$$\alpha^{m_1-2} \leq F_{m_1} \leq F_{m_1} + F_{m_2} + F_{m_3} = 2^{t_1} + 2^{t_2} \leq 2^{t_1+1} \tag{6.3.6}$$

and

$$3\alpha^{m_1-1} \geq 3F_{m_1} \geq F_{m_1} + F_{m_2} + F_{m_3} = 2^{t_1} + 2^{t_2} > 2^{t_1}. \tag{6.3.7}$$

Thus

$$m_1 - 2 \leq t_1 \cdot \frac{\log 2}{\log \alpha} + \frac{\log 2}{\log \alpha} \quad \text{and} \quad m_1 - 1 > t_1 \cdot \frac{\log 2}{\log \alpha} - \frac{\log 3}{\log \alpha}. \tag{6.3.8}$$

In particular, we have $m_1 > t_1$.

We solve equation (6.1.2) for $0 \leq m_3 \leq m_2 \leq m_1 < 360$ and $0 \leq t_2 \leq t_1 < 251$ by a brute force computer enumeration and find all solutions listed in the Appendix.

By these computer searches we may assume now that $n_1 \geq 360$ for solving equation (6.1.1) (respectively $m_1 \geq 360$ for solving equation (6.1.2)). Moreover, we want to emphasize that the second inequality of (6.3.5) (respectively (6.3.8)) implies that $n_1 > a_1$ (respectively $m_1 > t_1$).

6.4 A first upper bound - Application of linear forms in logarithms

In this section, we shall establish the following two propositions concerning Diophantine equations (6.1.1) and (6.1.2) respectively.

Proposition 6.1. *Assume that* $(n_1, n_2, a_1, a_2, a_3)$ *is a solution to equation* (6.1.1) *with* $n_1 \geq n_2 \geq 0$ *and* $a_1 \geq a_2 \geq a_3 \geq 0$. *Then we have that* $n_1 < 4.1 \cdot 10^{62}$.

Proposition 6.2. *Assume that* $(m_1, m_2, m_3, t_1, t_2)$ *is a solution to equation* (6.1.2) *with* $m_1 \geq m_2 \geq m_3 \geq 0$ *and* $t_1 \geq t_2 \geq 0$. *Then we have that* $m_1 < 4.2 \cdot 10^{62}$.

6.4.1 Proof of Proposition 6.1

We follow the steps explained in the introduction. We start with

Step 1: *Show that*

$$\min\{(a_1 - a_2)\log 2, (n_1 - n_2)\log\alpha\} < 2.61 \cdot 10^{13} \log n_1.$$

Equation (6.1.1) can be rewritten as

$$\frac{\alpha^{n_1} - \beta^{n_1}}{\sqrt{5}} + \frac{\alpha^{n_2} - \beta^{n_2}}{\sqrt{5}} = 2^{a_1} + 2^{a_2} + 2^{a_3}.$$

In the first step we consider n_1 and a_1 to be large and by collecting "large" terms to the left hand side of the equation, we obtain

$$\left|\frac{\alpha^{n_1}}{\sqrt{5}} - 2^{a_1}\right| = \left|2^{a_2} + 2^{a_3} + \frac{\beta^{n_1}}{\sqrt{5}} - \frac{\alpha^{n_2} - \beta^{n_2}}{\sqrt{5}}\right| < 2^{a_2+1} + \frac{\alpha^{n_2}}{\sqrt{5}} + 0.45 < 2.9\max\{2^{a_2}, \alpha^{n_2}\}.$$

Dividing through 2^{a_1} we get

$$\left|\frac{\alpha^{n_1}}{\sqrt{5}}2^{-a_1} - 1\right| < \max\left\{2.9 \cdot 2^{a_2-a_1}, \frac{2.9\alpha^{n_2}}{2^{a_1}}\right\} < \max\left\{2.9 \cdot 2^{a_2-a_1}, \frac{8.7\alpha^{n_2}}{\alpha^{n_1-2}}\right\}.$$

Hence we obtain the inequality

$$\left|\frac{\alpha^{n_1}}{\sqrt{5}}2^{-a_1} - 1\right| < 22.78\max\left\{2^{a_2-a_1}, \alpha^{n_2-n_1}\right\}. \tag{6.4.1}$$

In Step 1 we consider the linear form

$$\Lambda = n_1 \log\alpha - a_1 \log 2 - \log\sqrt{5}$$

and assume that $|\Lambda| \le 0.5$. Further, we put

$$\Phi = e^{\Lambda} - 1 = \alpha^{n_1} 2^{-a_1} \sqrt{5}^{-1} - 1$$

and use the theorem of Baker and Wüstholz (Theorem 6.3) with the data

$$\alpha_1 = \alpha, \quad \alpha_2 = 2, \quad \alpha_3 = \sqrt{5}, \quad b_1 = n_1, \quad b_2 = -a_1, \quad b_3 = -1.$$

Since $n_1 > a_1$ we have $B = n_1$. By simple computations, we obtain $h'(\alpha_1) = \frac{1}{2}$, $h'(\alpha_2) = \log 2$ and $h'(\alpha_3) = \log\sqrt{5}$.

Before we can apply Theorem 6.3 we have to show that $\Phi \neq 0$. Assume to the contrary that $\Phi = 0$, then $\alpha^{n_1} = \sqrt{5} \cdot 2^{a_1}$. Let $\sigma \neq \mathrm{id}$ be the unique non-trivial $\mathbb{Q}$-automorphism over $\mathbb{Q}(\sqrt{5})$. Then we get

$$\alpha^{n_1} = \sqrt{5} \cdot 2^{a_1} = -\sigma\left(\sqrt{5} \cdot 2^{a_1}\right) = -\sigma\left(\alpha^{n_1}\right) = -\beta^{n_1}.$$

However, the absolute value of α^{n_1} is at least $\alpha^{360} > 2$ whereas the absolute value of $-\beta^{n_1}$ is at most $|\beta|^{360} < 1$. By this obvious contradiction we conclude that $\Phi \neq 0$.

Theorem 6.3 yields

$$\log|\Phi| \geq -C(3,2)\left(\frac{1}{2}\right)(\log 2)\left(\log\sqrt{5}\right)\log n_1 - \log 2$$

and together with inequality (6.4.1) we have

$$\min\{(a_1-a_2)\log 2, (n_1-n_2)\log\alpha\} < 2.61\cdot 10^{13}\log n_1.$$

Thus we have proved so far:

Lemma 6.5. *Assume that (n_1,n_2,a_1,a_2,a_3) is a solution to equation (6.1.1) with $n_1 \geq n_2 \geq 0$ and $a_1 \geq a_2 \geq a_3 \geq 0$. Then we have*

$$\min\{(a_1-a_2)\log 2, (n_1-n_2)\log\alpha\} < 2.61\cdot 10^{13}\log n_1.$$

Note that in the case that $|\Lambda| > 0.5$, inequality (6.4.1) is possible only if either $a_1 - a_2 \leq 5$ or $n_1 - n_2 \leq 7$, which are covered by the bound provided by Lemma 6.5.

Now we have to distinguish between

Case 1 $\min\{(a_1-a_2)\log 2, (n_1-n_2)\log\alpha\} = (a_1-a_2)\log 2$ and

Case 2 $\min\{(a_1-a_2)\log 2, (n_1-n_2)\log\alpha\} = (n_1-n_2)\log\alpha.$

We will deal with these two cases in the following steps.

Step 2: *We consider Case 1 and show that under the assumption that $(a_1-a_2)\log 2 < 2.61\cdot 10^{13}\log n_1$ we obtain*

$$\min\{(a_1-a_3)\log 2, (n_1-n_2)\log\alpha\} < 8.5\cdot 10^{26}(\log n_1)^2.$$

Since we consider Case 1 we assume that

$$\min\{(a_1-a_2)\log 2, (n_1-n_2)\log\alpha\} = (a_1-a_2)\log 2 < 2.61\cdot 10^{13}\log n_1.$$

By collecting "large" terms, i.e. terms involving n_1, a_1 and a_2, on the left hand side, we rewrite equation (6.1.1) as

$$\left|\frac{\alpha^{n_1}}{\sqrt{5}} - 2^{a_1} - 2^{a_2}\right| = \left|2^{a_3} + \frac{\beta^{n_1}}{\sqrt{5}} - \frac{\alpha^{n_2}}{\sqrt{5}} + \frac{\beta^{n_2}}{\sqrt{5}}\right| < 2^{a_3} + \frac{\alpha^{n_2}}{\sqrt{5}} + 0.45$$

and obtain that

$$\left|\frac{\alpha^{n_1}}{\sqrt{5}} - 2^{a_2}\left(2^{a_1-a_2}+1\right)\right| < 1.9\max\left\{2^{a_3},\alpha^{n_2}\right\}.$$

Dividing through $\frac{\alpha^{n_1}}{\sqrt{5}}$ we get by using inequality (6.3.4)

$$\begin{aligned}\left|\alpha^{-n_1}2^{a_2}\sqrt{5}\left(2^{a_1-a_2}+1\right)-1\right| &< \max\left\{\frac{1.9\sqrt{5}}{\alpha^{n_1}}\cdot 2^{a_3}, 1.9\sqrt{5}\alpha^{n_2-n_1}\right\}\\ &\le \max\left\{\frac{1.9\sqrt{5}}{2^{a_1-1}\alpha}\cdot 2^{a_3}, 1.9\sqrt{5}\alpha^{n_2-n_1}\right\}\end{aligned}$$

and obtain the inequality

$$\left|\alpha^{-n_1}2^{a_2}\sqrt{5}\left(2^{a_1-a_2}+1\right)-1\right| < 5.26\max\left\{2^{a_3-a_1},\alpha^{n_2-n_1}\right\}. \tag{6.4.2}$$

We shall apply Theorem 6.3 to inequality (6.4.2). Therefore we consider the following linear form in logarithms:

$$\Lambda_1 = -n_1\log\alpha + a_2\log 2 + \log\left(\sqrt{5}\left(2^{a_1-a_2}+1\right)\right).$$

Let us assume for the moment that $|\Lambda_1| \le 0.5$. Further, we put

$$\Phi_1 = e^{\Lambda_1} - 1 = \alpha^{-n_1}2^{a_2}\sqrt{5}\left(2^{a_1-a_2}+1\right) - 1$$

and aim to apply Theorem 6.3 by taking

$$\alpha_1 = \alpha, \quad \alpha_2 = 2, \quad \alpha_3 = \sqrt{5}\left(2^{a_1-a_2}+1\right), \quad b_1 = -n_1, \quad b_2 = a_2, \quad b_3 = 1.$$

Note that since $n_1 > a_1 > a_2$ we have $B = n_1$. Next, we estimate the height of α_3 by using the properties of heights and Lemma 6.5:

$$\begin{aligned}h_0(\alpha_3) &\le h_0(\sqrt{5}) + (a_1-a_2)h_0(2) + \log 2\\ &\le \log\sqrt{5} + (a_1-a_2)\log 2 + \log 2\\ &< 2.62\cdot 10^{13}\log n_1,\end{aligned}$$

which gives $h'(\alpha_3) < 2.62\cdot 10^{13}\log n_1$. As before we have $h'(\alpha_1) = \frac{1}{2}$ and $h'(\alpha_2) = \log 2$. By a similar argument as in Step 1 we conclude that $\Phi_1 \ne 0$. Now, we are ready to apply Theorem 6.3 and get

$$\begin{aligned}\log|\Phi_1| &> -C(3,2)\left(\frac{1}{2}\right)(\log 2)\left(2.62\cdot 10^{13}\log n_1\right)\log n_1 - \log 2\\ &> -8.49\cdot 10^{26}(\log n_1)^2.\end{aligned}$$

Combining this inequality with inequality (6.4.2), we obtain

$$\min\left\{(a_1-a_3)\log 2, (n_1-n_2)\log\alpha\right\} < 8.5\cdot 10^{26}(\log n_1)^2. \tag{6.4.3}$$

Note that in the case that $|\Lambda_1| > 0.5$ inequality (6.4.2) is possible, only if either $a_1 - a_3 \le 3$ or $n_1 - n_2 \le 4$. Both cases are covered by the bound provided by inequality (6.4.3).

At this stage, we have to consider two further sub-cases.

Case 1A $\min\{(a_1 - a_3)\log 2, (n_1 - n_2)\log\alpha\} = (a_1 - a_3)\log 2$ and

Case 1B $\min\{(a_1 - a_3)\log 2, (n_1 - n_2)\log\alpha\} = (n_1 - n_2)\log\alpha$.

We will deal with Case 1A in Step 3 and with Case 1B in Step 4.

Step 3: *We consider Case 1A and show that under the assumption that* $(a_1 - a_3)\log 2 < 8.5 \cdot 10^{26}(\log n_1)^2$ *and* $(a_1 - a_2)\log 2 < 2.61 \cdot 10^{13}\log n_1$ *we obtain that*

$$(n_1 - n_2)\log\alpha < 2.77 \cdot 10^{40}(\log n_1)^3.$$

In this step we consider n_1, a_1, a_2 and a_3 to be large. By collecting "large" terms on the left hand side we rewrite equation (6.1.1) as

$$\left|\frac{\alpha^{n_1}}{\sqrt{5}} - 2^{a_1} - 2^{a_2} - 2^{a_3}\right| = \left|\frac{\beta^{n_1}}{\sqrt{5}} - \frac{\alpha^{n_2}}{\sqrt{5}} + \frac{\beta^{n_2}}{\sqrt{5}}\right| < \frac{\alpha^{n_2}}{\sqrt{5}} + 0.45$$

and obtain that

$$\left|\frac{\alpha^{n_1}}{\sqrt{5}} - 2^{a_1}\left(1 + 2^{a_2 - a_1} + 2^{a_3 - a_1}\right)\right| < 0.9\alpha^{n_2}.$$

Dividing through $\frac{\alpha^{n_1}}{\sqrt{5}}$ yields the inequality

$$\left|\alpha^{-n_1}2^{a_1}\sqrt{5}\left(1 + 2^{a_2 - a_1} + 2^{a_3 - a_1}\right) - 1\right| < 2.02\alpha^{n_2 - n_1}. \tag{6.4.4}$$

We want to apply Theorem 6.3 to inequality (6.4.4) and consider the linear form

$$\Lambda_A = -n_1\log\alpha + a_1\log 2 + \log\left(\sqrt{5}\left(1 + 2^{a_2 - a_1} + 2^{a_3 - a_1}\right)\right).$$

Let us assume that $|\Lambda_A| \le 0.5$. Further, we put

$$\Phi_A = e^{\Lambda_A} - 1 = \alpha^{-n_1}2^{a_1}\sqrt{5}\left(1 + 2^{a_2 - a_1} + 2^{a_3 - a_1}\right) - 1$$

and aim to apply Theorem 6.3 with

$$\alpha_1 = \alpha, \quad \alpha_2 = 2, \quad \alpha_3 = \sqrt{5}\left(1 + 2^{a_2 - a_1} + 2^{a_3 - a_1}\right), \quad b_1 = -n_1, \quad b_2 = a_1, \quad b_3 = 1.$$

Similarly as before we get that $B = n_1$. Next, let us estimate the height of α_3. Using the properties of heights, Lemma 6.5 and inequality (6.4.3) we get

$$\begin{aligned}
h_0(\alpha_3) &\le h_0(\sqrt{5}) + (a_1 - a_2)h_0(2) + (a_1 - a_3)h_0(2) + \log 2 \\
&\le \log\sqrt{5} + (a_1 - a_2)\log 2 + (a_1 - a_3)\log 2 + \log 2 \\
&< 2.61 \cdot 10^{13}\log n_1 + 8.5 \cdot 10^{26}(\log n_1)^2 + \log 2\sqrt{5} \\
&< 8.51 \cdot 10^{26}(\log n_1)^2,
\end{aligned}$$

which gives $h'(\alpha_3) < 8.51 \cdot 10^{26} (\log n_1)^2$. As before we have $h'(\alpha_1) = \frac{1}{2}$, $h'(\alpha_2) = \log 2$ and $\Phi_A \neq 0$. An application of Theorem 6.3 yields

$$\begin{aligned} \log |\Phi_A| &> - C(3,2) \left(\frac{1}{2}\right) (\log 2) \left(8.51 \cdot 10^{26} (\log n_1)^2\right) \log n_1 - \log 2 \\ &> - 2.76 \cdot 10^{40} (\log n_1)^3. \end{aligned}$$

Combining this inequality with inequality (6.4.4) we obtain

$$(n_1 - n_2) \log \alpha < 2.77 \cdot 10^{40} (\log n_1)^3. \tag{6.4.5}$$

Note that in the case that $|\Lambda_A| > 0.5$ inequality (6.4.4) is possible only if $n_1 - n_2 \leq 2$. This is covered by the bound provided by inequality (6.4.5).

Step 4: *We consider Case 1B and show that under the assumption that* $(n_1 - n_2) \log 2 < 8.5 \cdot 10^{26} (\log n_1)^2$ *and* $(a_1 - a_2) \log 2 < 2.61 \cdot 10^{13} \log n_1$ *we obtain that*

$$(a_1 - a_3) \log 2 < 1.39 \cdot 10^{40} (\log n_1)^3.$$

By collecting "large" terms to the left hand side, where we consider n_1, n_2, a_1 and a_2 to be large, we rewrite equation (6.1.1) as

$$\left| \frac{\alpha^{n_1}}{\sqrt{5}} + \frac{\alpha^{n_2}}{\sqrt{5}} - 2^{a_1} - 2^{a_2} \right| = \left| 2^{a_3} + \frac{\beta^{n_1}}{\sqrt{5}} + \frac{\beta^{n_2}}{\sqrt{5}} \right| < 2^{a_3} + 0.45$$

and obtain that

$$\left| \frac{\alpha^{n_2}}{\sqrt{5}} \left(\alpha^{n_1 - n_2} + 1\right) - 2^{a_2} \left(2^{a_1 - a_2} + 1\right) \right| < 1.45 \cdot 2^{a_3}.$$

Dividing through $2^{a_2} \left(2^{a_1 - a_2} + 1\right)$ we obtain the inequality

$$\left| \alpha^{n_2} 2^{-a_2} \left(\frac{\alpha^{n_1 - n_2} + 1}{\sqrt{5} \left(2^{a_1 - a_2} + 1\right)} \right) - 1 \right| < 1.45 \cdot 2^{a_3 - a_1} \tag{6.4.6}$$

We want to apply Theorem 6.3 to inequality (6.4.6). Hence we consider the linear form

$$\Lambda_B = n_2 \log \alpha - a_2 \log 2 + \log \left(\frac{\alpha^{n_1 - n_2} + 1}{\sqrt{5} \left(2^{a_1 - a_2} + 1\right)} \right)$$

and assume that $|\Lambda_B| \leq 0.5$. Further, we put

$$\Phi_B = e^{\Lambda_B} - 1 = \alpha^{n_2} 2^{-a_2} \left(\frac{\alpha^{n_1 - n_2} + 1}{\sqrt{5} \left(2^{a_1 - a_2} + 1\right)} \right) - 1$$

and aim to apply Theorem 6.3 by taking

$$\alpha_1 = \alpha, \quad \alpha_2 = 2, \quad \alpha_3 = \frac{\alpha^{n_1-n_2}+1}{\sqrt{5}\,(2^{a_1-a_2}+1)}, \quad b_1 = n_2, \quad b_2 = -a_2, \quad b_3 = 1.$$

and get $B = n_1$ as in the steps before. Let us estimate the height of α_3. Using the properties of heights, Lemma 6.5 and inequality (6.4.3) we get

$$\begin{aligned} h_0(\alpha_3) &\le (n_1-n_2)h_0(\alpha) + \log 2 + h_0(\sqrt{5}) + (a_1-a_2)h_0(2) + \log 2 \\ &= \frac{1}{2}(n_1-n_2)\log\alpha + \log\sqrt{5} + (a_1-a_2)\log 2 + 2\log 2 \\ &< \frac{1}{2}\left(8.5\cdot 10^{26}(\log n_1)^2\right) + 2.61\cdot 10^{13}\log n_1 + \log 4\sqrt{5} \\ &< 4.26\cdot 10^{26}(\log n_1)^2, \end{aligned}$$

which gives $h'(\alpha_3) < 4.26\cdot 10^{26}(\log n_1)^2$. A similar deduction as before yields $h'(\alpha_1) = \frac{1}{2}$, $h'(\alpha_2) = \log 2$ and $\Phi_B \neq 0$. Now, we apply Theorem 6.3 and get

$$\begin{aligned} \log|\Phi_B| &> -C(3,2)\left(\frac{1}{2}\right)(\log 2)\left(4.26\cdot 10^{26}(\log n_1)^2\right)\log n_1 - \log 2 \\ &> -1.38\cdot 10^{40}(\log n_1)^3. \end{aligned}$$

Combining this inequality with inequality (6.4.6), we obtain

$$(a_1-a_3)\log 2 < 1.39\cdot 10^{40}(\log n_1)^3. \tag{6.4.7}$$

Note that in the case of $|\Lambda_B| > 0.5$, inequality (6.4.6) is possible only if $a_1 - a_3 \le 1$ which is covered by the bound provided by inequality (6.4.7).

Step 5: *We consider Case 2 and show that under the assumption that* $(n_1-n_2)\log\alpha < 2.61\cdot 10^{13}\log n_1$ *we obtain*

$$(a_1-a_2)\log 2 < 4.26\cdot 10^{26}(\log n_1)^2.$$

Since we consider Case 2 we assume that

$$\min\{(a_1-a_2)\log 2, (n_1-n_2)\log\alpha\} = (n_1-n_2)\log\alpha < 2.61\cdot 10^{13}\log n_1.$$

In this step we consider n_1, n_2 and a_1 to be large and by collecting "large" terms to the left hand side, we rewrite equation (6.1.1) as

$$\left|\frac{\alpha^{n_1}}{\sqrt{5}} + \frac{\alpha^{n_2}}{\sqrt{5}} - 2^{a_1}\right| = \left|2^{a_2} + 2^{a_3} + \frac{\beta^{n_1}}{\sqrt{5}} + \frac{\beta^{n_2}}{\sqrt{5}}\right| < 2\cdot 2^{a_2} + 0.45$$

and obtain that
$$\left|\frac{\alpha^{n_2}}{\sqrt{5}}\left(\alpha^{n_1-n_2}+1\right)-2^{a_1}\right| < 2.45\cdot 2^{a_2}.$$
Dividing through 2^{a_1} we get the inequality
$$\left|\alpha^{n_2}2^{-a_1}\left(\frac{\alpha^{n_1-n_2}+1}{\sqrt{5}}\right)-1\right| < 2.45\cdot 2^{-(a_1-a_2)}. \tag{6.4.8}$$

Similarly as above we shall apply Theorem 6.3 to inequality (6.4.8). Hence we consider the linear form
$$\Lambda_2 = n_2\log\alpha - a_1\log 2 + \log\left(\frac{\alpha^{n_1-n_2}+1}{\sqrt{5}}\right)$$
and assume that $|\Lambda_2| \le 0.5$. Further, we put
$$\Phi_2 = e^{\Lambda_2}-1 = \alpha^{n_2}2^{-a_1}\left(\frac{\alpha^{n_1-n_2}+1}{\sqrt{5}}\right)-1$$
and
$$\alpha_1 = \alpha,\quad \alpha_2 = 2,\quad \alpha_3 = \frac{\alpha^{n_1-n_2}+1}{\sqrt{5}},\quad b_1 = n_2,\quad b_2 = -a_1,\quad b_3 = 1.$$

Once again this choice yields $B = n_1$. Next, let us estimate the height of α_3. Using the properties of heights and Lemma 6.5 we find
$$\begin{aligned} h_0(\alpha_3) &\le (n_1-n_2)h_0(\alpha) + \log 2 + h_0(\sqrt{5})\\ &= \frac{1}{2}(n_1-n_2)\log\alpha + \log 2 + \log\sqrt{5}\\ &< \frac{1}{2}\left(2.61\cdot 10^{13}\log n_1\right) + \log 2\sqrt{5}\\ &< 1.31\cdot 10^{13}\log n_1, \end{aligned}$$
which gives $h'(\alpha_3) < 1.31\cdot 10^{13}\log n_1$. A similar deduction as before gives $h'(\alpha_1) = \frac{1}{2}$, $h'(\alpha_2) = \log 2$ and $\Phi_2 \ne 0$. Thus by applying Theorem 6.3 we get
$$\begin{aligned} \log|\Phi_2| &> -C(3,2)\left(\frac{1}{2}\right)(\log 2)\left(1.31\cdot 10^{13}\log n_1\right)\log n_1 - \log 2\\ &> -4.25\cdot 10^{26}(\log n_1)^2. \end{aligned}$$

Combining this inequality together with inequality (6.4.8), we obtain
$$(a_1-a_2)\log 2 < 4.26\cdot 10^{26}(\log n_1)^2. \tag{6.4.9}$$

Note that in the case of $|\Lambda_2| > 0.5$, inequality (6.4.8) is possible only if $a_1-a_2 \le 2$ which is covered by the bound provided by inequality (6.4.9).

Step 6: *We continue to consider Case 2 and show that under the assumption that* $(n_1 - n_2)\log\alpha < 2.61 \cdot 10^{13} \log n_1$ *and* $(a_1 - a_2)\log 2 < 4.26 \cdot 10^{26}(\log n_1)^2$ *we obtain*

$$(a_1 - a_3)\log 2 < 1.39 \cdot 10^{40}(\log n_1)^3.$$

We shall apply once more Theorem 6.3 to obtain an upper bound for $(a_1 - a_3)\log 2$. The derivation is very similar to Case 1B. By collecting "large" terms on the left hand side, we rewrite equation (6.1.1) as

$$\left|\frac{\alpha^{n_1}}{\sqrt{5}} + \frac{\alpha^{n_2}}{\sqrt{5}} - 2^{a_1} - 2^{a_2}\right| = \left|2^{a_3} + \frac{\beta^{n_1}}{\sqrt{5}} + \frac{\beta^{n_2}}{\sqrt{5}}\right| < 2^{a_3} + 0.45.$$

By the same derivation as in Step 4 we obtain inequality (6.4.6), i.e.

$$\left|\alpha^{n_2} 2^{-a_2}\left(\frac{\alpha^{n_1-n_2}+1}{\sqrt{5}\,(2^{a_1-a_2}+1)}\right) - 1\right| < 1.45 \cdot 2^{a_3-a_1}.$$

We have the same setting as in Case 1B, except that the estimate for the height of α_3 becomes

$$\begin{aligned}
h_0(\alpha_3) &\le (n_1 - n_2)h_0(\alpha) + \log 2 + h_0(\sqrt{5}) + (a_1 - a_2)h_0(2) + \log 2\\
&= \frac{1}{2}(n_1 - n_2)\log\alpha + \log\sqrt{5} + (a_1 - a_2)\log 2 + 2\log 2\\
&< \frac{1}{2}\left(2.61 \cdot 10^{13}\log n_1\right) + 4.26 \cdot 10^{26}(\log n_1)^2 + \log 4\sqrt{5}\\
&< 4.27 \cdot 10^{26}(\log n_1)^2,
\end{aligned}$$

which gives $h'(\alpha_3) < 4.27 \cdot 10^{26}(\log n_1)^2$ instead of $h'(\alpha_3) < 4.26 \cdot 10^{26}(\log n_1)^2$. Therefore by applying Theorem 6.3 similarly as before we obtain

$$(a_1 - a_3)\log 2 < 1.39 \cdot 10^{40}(\log n_1)^3 \tag{6.4.10}$$

which coincides with inequality (6.4.7). Table 6.1 summarizes our results obtained so far.

Table 6.1: Summary of results

Upper bound of	**Case 1A**	**Case 1B**	**Case 2**
$(a_1 - a_2)\log 2$	$2.61 \cdot 10^{13}\log n_1$	$2.61 \cdot 10^{13}\log n_1$	$4.26 \cdot 10^{26}(\log n_1)^2$
$(a_1 - a_3)\log 2$	$8.51 \cdot 10^{26}(\log n_1)^2$	$1.39 \cdot 10^{40}(\log n_1)^3$	$1.39 \cdot 10^{40}(\log n_1)^3$
$(n_1 - n_2)\log\alpha$	$2.77 \cdot 10^{40}(\log n_1)^3$	$8.5 \cdot 10^{26}(\log n_1)^2$	$2.61 \cdot 10^{13}\log n_1$

Step 7: *We assume the bounds given in Table 6.1 and show that* $n_1 \log\alpha < 4.54 \cdot 10^{53}(\log n_1)^4$, *hence* $n_1 < 4.1 \cdot 10^{62}$.

We have to apply Theorem 6.3 once more. This time we rewrite equation (6.1.1) as

$$\left|\frac{\alpha^{n_1}}{\sqrt{5}}\left(1+\alpha^{n_2-n_1}\right)-2^{a_1}\left(1+2^{a_2-a_1}+2^{a_3-a_1}\right)\right|=\left|\frac{\beta^{n_1}}{\sqrt{5}}+\frac{\beta^{n_2}}{\sqrt{5}}\right|<0.45.$$

Dividing through $\frac{\alpha^{n_1}}{\sqrt{5}}\left(1+\alpha^{n_2-n_1}\right)$ we obtain the inequality

$$\left|\alpha^{-n_1}2^{a_1}\left(\frac{\sqrt{5}(1+2^{a_2-a_1}+2^{a_3-a_1})}{1+\alpha^{n_2-n_1}}\right)-1\right|<1.01\alpha^{-n_1}. \tag{6.4.11}$$

In this final step we consider the linear form

$$\Lambda_3=-n_1\log\alpha+a_1\log 2+\log\left(\frac{\sqrt{5}(1+2^{a_2-a_1}+2^{a_3-a_1})}{1+\alpha^{n_2-n_1}}\right)$$

and assume that $|\Lambda_3|\leq 0.5$. Further, we put

$$\Phi_3=e^{\Lambda_3}-1=\alpha^{-n_1}2^{a_1}\left(\frac{\sqrt{5}(1+2^{a_2-a_1}+2^{a_3-a_1})}{1+\alpha^{n_2-n_1}}\right)-1.$$

We take

$$\alpha_1=\alpha,\quad \alpha_2=2,\quad \alpha_3=\frac{\sqrt{5}(1+2^{a_2-a_1}+2^{a_3-a_1})}{1+\alpha^{n_2-n_1}},\quad b_1=-n_1,\quad b_2=a_1,\quad b_3=1.$$

Thus we have $B=n_1$. By the results in Table 6.1 and similar computations done before we obtain

$$\begin{aligned} h_0(\alpha_3) &\leq h_0\left(\sqrt{5}\right)+(a_1-a_2)\ h_0(2)+(a_1-a_3)\ h_0(2)+(n_1-n_2)h_0(\alpha)+2\log 2\\ &\leq (a_1-a_2)\log 2+(a_1-a_3)\log 2+\frac{1}{2}(n_1-n_2)\log\alpha+\log 4\sqrt{5}\\ &< 1.4\cdot 10^{40}(\log n_1)^3, \end{aligned}$$

which gives $h'(\alpha_3)<1.4\cdot 10^{40}(\log n_1)^3$. As before we have $h'(\alpha_1)=\frac{1}{2}$, $h'(\alpha_2)=\log 2$ and $\Phi_3\neq 0$. Now an application of Theorem 6.3 yields

$$\log|\Phi_3|>-C(3,2)\left(\frac{1}{2}\right)(\log 2)\left(1.4\cdot 10^{40}(\log n_1)^3\right)\log n_1-\log 2.$$

Combining this inequality with inequality (6.4.11) we get

$$n_1\log\alpha<4.54\cdot 10^{53}(\log n_1)^4$$

which yields

$$n_1<4.1\cdot 10^{62}.$$

Similarly as in the cases above the assumption $|\Lambda_3|>0.5$ leads in view of inequality (6.4.11) to $n_1\leq 0$ which is impossible. Thus Proposition 6.1 is established.

6.4.2 Proof of Proposition 6.2

Since the deduction of an upper bound for solutions to (6.1.2) is similar to the proof of Proposition 6.1 we only sketch the argument. In the case of equation (6.1.2), we have

$$\frac{\alpha^{m_1}-\beta^{m_1}}{\sqrt{5}}+\frac{\alpha^{m_2}-\beta^{m_2}}{\sqrt{5}}+\frac{\alpha^{m_3}-\beta^{m_3}}{\sqrt{5}}=2^{t_1}+2^{t_2}.$$

Step 1: *Show that*

$$\min\{(t_1-t_2)\log 2,(m_1-m_2)\log\alpha\}<2.61\cdot 10^{13}\log m_1.$$

First, we rearrange equation (6.1.2) and make use of inequalities (6.3.6) and (6.3.7) to get

$$\left|\frac{\alpha^{m_1}2^{-t_1}}{\sqrt{5}}-1\right|<14.67\max\left\{2^{t_2-t_1},\alpha^{m_2-m_1}\right\}. \tag{6.4.12}$$

We consider $\Gamma=m_1\log\alpha-t_1\log 2-\log\sqrt{5}$ with $|\Gamma|\le 0.5$. Further, we put

$$\Psi=e^{\Gamma}-1=\alpha^{m_1}2^{-t_1}\sqrt{5}^{-1}-1$$

and apply the theorem of Baker and Wüstholz (Theorem 6.3) with the data

$$\alpha_1=\alpha,\quad \alpha_2=2,\quad \alpha_3=\sqrt{5},\quad b_1=m_1,\quad b_2=-t_1,\quad b_3=-1,$$

i.e. $B=m_1$. By a simple computation, we obtain $h'(\alpha_1)=\frac{1}{2}$, $h'(\alpha_2)=\log 2$ and $h'(\alpha_3)=\log\sqrt{5}$. Similarly as in the proof of Proposition 6.1 we may assume that $\Psi\neq 0$. Then Theorem 6.3 yields

$$\log|\Psi|\ge -C(3,2)\left(\frac{1}{2}\right)(\log 2)\left(\log\sqrt{5}\right)\log m_1-\log 2$$

and together with inequality (6.4.12) we have

$$\min\{(t_1-t_2)\log 2,(m_1-m_2)\log\alpha\}<2.61\cdot 10^{13}\log m_1.$$

Thus instead of Lemma 6.5 we obtain now

Lemma 6.6. *Assume that* (m_1,m_2,m_3,t_1,t_2) *is a solution to equation* (6.1.2) *with* $m_1\ge m_2\ge m_3\ge 0$ *and* $t_1\ge t_2\ge 0$. *Then we have*

$$\min\{(t_1-t_2)\log 2,(m_1-m_2)\log\alpha\}<2.61\cdot 10^{13}\log m_1.$$

The scenarios for which $|\Gamma|>0.5$ can be easily dealt with. Now we have to distinguish between two cases:

Case 1 $\min\{(t_1 - t_2)\log 2, (m_1 - m_2)\log\alpha\} = (m_1 - m_2)\log\alpha$ and

Case 2 $\min\{(t_1 - t_2)\log 2, (m_1 - m_3)\log\alpha\} = (t_1 - t_2)\log 2$

We will deal with these cases in the following steps.

Step 2: *We consider Case 1 and show that under the assumption that* $(m_1 - m_2)\log\alpha < 2.61 \cdot 10^{13}\log m_1$ *we obtain*

$$\min\{(t_1 - t_2)\log 2, (m_1 - m_3)\log\alpha\} < 4.26 \cdot 10^{26}(\log m_1)^2.$$

We rearrange equation (6.1.2) and make use of inequalities (6.3.6) and (6.3.7) to get

$$|\Psi_1| = \left|\frac{\alpha^{m_2}2^{-t_1}\left(\alpha^{m_1-m_2}+1\right)}{\sqrt{5}} - 1\right| < 12.31\max\left\{2^{-(t_1-t_2)}, \alpha^{-(m_1-m_3)}\right\}. \tag{6.4.13}$$

We apply Theorem 6.3 to inequality (6.4.13) by taking $b_1 = m_2$, $b_2 = -t_1$ and $b_3 = 1$, i.e. $B = m_1$ since $m_1 > m_2, t_1$. Further, we choose $\alpha_1 = \alpha$, $\alpha_2 = 2$ and $\alpha_3 = \frac{\alpha^{m_1-m_2+1}}{\sqrt{5}}$. Note that by our standard arguments we obtain that $h'(\alpha_3) < 1.31 \cdot 10^{13}\log m_1$ and $\Psi_1 \neq 0$. Finally we get

$$\min\{(t_1 - t_2)\log 2, (m_1 - m_3)\log\alpha\} < 4.26 \cdot 10^{26}(\log m_1)^2.$$

At this stage, we have to consider the following two sub-cases for Case 1:

Case 1A $\min\{(t_1 - t_2)\log 2, (m_1 - m_3)\log\alpha\} = (m_1 - m_3)\log\alpha$ and

Case 1B $\min\{(t_1 - t_2)\log 2, (m_1 - m_3)\log\alpha\} = (t_1 - t_2)\log 2$.

We will deal with these sub-cases in the steps below.

Step 3: *We consider Case 1A and show that under the assumption that* $(m_1 - m_2)\log\alpha < 2.61 \cdot 10^{13}\log m_1$ *and* $(m_1 - m_3)\log\alpha < 4.26 \cdot 10^{26}(\log m_1)^2$ *we obtain that*

$$(t_1 - t_2)\log 2 < 6.94 \cdot 10^{39}(\log m_1)^3.$$

We rearrange equation (6.1.2) and make use of inequalities (6.3.6) and (6.3.7) to get

$$|\Psi_A| = \left|\frac{\alpha^{m_1}2^{-t_1}\left(1+\alpha^{m_2-m_1}+\alpha^{m_3-m_1}\right)}{\sqrt{5}} - 1\right| < 1.9 \cdot 2^{t_2-t_1}. \tag{6.4.14}$$

We apply Theorem 6.3 to inequality (6.4.13) with $B = m_1$, $\alpha_1 = \alpha$, $\alpha_2 = 2$, $\alpha_3 = \frac{(1+\alpha^{m_2-m_1}+\alpha^{m_3-m_1})}{\sqrt{5}}$. Note that we have $h'(\alpha_3) < 2.14 \cdot 10^{26}(\log m_1)^2$ and $\Psi_A \neq 0$. Therefore, we get

$$(t_1 - t_2)\log 2 < 6.94 \cdot 10^{39}(\log m_1)^3.$$

Step 4: *We consider Case 1B and show that under the assumption that* $(m_1 - m_2)\log\alpha < 2.61 \cdot 10^{13}\log m_1$ *and* $(t_1 - t_2)\log 2 < 4.26 \cdot 10^{26}(\log m_1)^2$ *we obtain that*

$$(m_1 - m_3)\log\alpha < 1.4 \cdot 10^{40}(\log m_1)^3.$$

We rearrange equation (6.1.2) and make use of inequalities (6.3.6) and (6.3.7) to get

$$|\Psi_B| = \left|\alpha^{-m_2}2^{t_2}\sqrt{5}\left(\frac{2^{t_1-t_2}+1}{\alpha^{m_1-m_2}+1}\right) - 1\right| < 3.02\alpha^{m_3-m_1} \tag{6.4.15}$$

We apply Theorem 6.3 to inequality (6.4.15) by taking $B = m_1$, $\alpha_1 = \alpha$, $\alpha_2 = 2$ and $\alpha_3 = \frac{\sqrt{5}(2^{t_1-t_2}+1)}{\alpha^{m_1-m_2}+1}$. With this choice we have $h'(\alpha_3) < 4.27 \cdot 10^{26}(\log n_1)^2$ and $\Psi_B \neq 0$. and we obtain

$$(m_1 - m_3)\log\alpha < 1.4 \cdot 10^{40}(\log m_1)^3.$$

Step 5: *We consider Case 2 and show that under the assumption that* $(t_1 - t_2)\log 2 < 2.61 \cdot 10^{13}\log m_1$ *we obtain*

$$(m_1 - m_2)\log\alpha < 8.5 \cdot 10^{26}(\log m_1)^2.$$

We rearrange equation (6.1.2) and make use of inequalities (6.3.6) and (6.3.7) to get

$$|\Psi_2| = \left|\alpha^{-m_2}2^{t_2}\sqrt{5}\left(2^{t_1-t_2}+1\right) - 1\right| < 4.03\alpha^{-(m_1-m_2)}. \tag{6.4.16}$$

We apply Theorem 6.3 to inequality (6.4.16) by taking $B = m_1$, $\alpha_1 = \alpha$, $\alpha_2 = 2$, $\alpha_3 = \sqrt{5}\left(2^{t_1-t_2}+1\right)$. In this case we have that $h'(\alpha_3) < 2.62 \cdot 10^{13}\log m_1$ and also $\Psi_2 \neq 0$. Therefore we get

$$(m_1 - m_2)\log\alpha < 8.5 \cdot 10^{26}(\log m_1)^2.$$

Step 6: *We continue to consider Case 2 and show that under the assumption that* $(t_1 - t_2)\log 2 < 2.61 \cdot 10^{13}\log m_1$ *and* $(m_1 - m_2)\log\alpha < 8.5 \cdot 10^{26}(\log m_1)^2$ *we obtain that*

$$(m_1 - m_3)\log\alpha < 1.38 \cdot 10^{40}(\log m_1)^3.$$

Again we apply Theorem 6.3 to obtain an upper bound for $(m_1 - m_3)\log\alpha$. The derivation is very similar to Case 1B. In particular, we have

$$\left|\alpha^{-m_2}2^{t_2}\sqrt{5}\left(\frac{2^{t_1-t_2}+1}{\alpha^{m_1-m_2}+1}\right)-1\right| < 3.02\alpha^{m_3-m_1}$$

and the same setting as in Case 1B, except that $h'(\alpha_3) < 4.26\cdot 10^{26}(\log m_1)^2$. Therefore Theorem 6.3 gives us

$$(m_1 - m_3)\log\alpha < 1.38\cdot 10^{40}(\log m_1)^3.$$

Table 6.2 summarizes our results obtained so far.

Table 6.2: Summary of results

Upper bound of	**Case 1A**	**Case 1B**	**Case 2**
line $(m_1 - m_2)\log\alpha$	$2.61\cdot 10^{13}\log m_1$	$2.61\cdot 10^{13}\log m_1$	$8.5\cdot 10^{26}(\log m_1)^2$
$(m_1 - m_3)\log\alpha$	$4.26\cdot 10^{26}(\log m_1)^2$	$1.4\cdot 10^{40}(\log m_1)^3$	$1.38\cdot 10^{40}(\log m_1)^3$
$(t_1 - t_2)\log 2$	$6.94\cdot 10^{39}(\log m_1)^3$	$4.26\cdot 10^{26}(\log m_1)^2$	$2.61\cdot 10^{13}\log m_1$

Step 7: *We assume the bounds given in Table 6.2 and show that* $m_1 < 4.2\cdot 10^{62}$.

Once again we have to apply Theorem 6.3. We rearrange equation (6.1.2) and make use of inequalities (6.3.6) and (6.3.7) to get

$$|\Psi_3| = \left|\alpha^{-m_1}2^{t_1}\left(\frac{\sqrt{5}(1+2^{t_2-t_1})}{1+\alpha^{m_2-m_1}+\alpha^{m_3-m_1}}\right)-1\right| < 2.02\alpha^{-m_1}. \tag{6.4.17}$$

In our last step we apply Theorem 6.3 to inequality (6.4.17) by taking $B = m_1$, $\alpha_1 = \alpha$, $\alpha_2 = 2$, $\alpha_3 = \frac{\sqrt{5}(1+2^{t_2-t_1})}{1+\alpha^{m_2-m_1}+\alpha^{m_3-m_1}}$. By our usual arguments we show that $h'(\alpha_3) < 1.41\cdot 10^{40}(\log m_1)^3$ and $\Psi_3 \neq 0$. Thus we get

$$m_1 < 4.2\cdot 10^{62},$$

hence Proposition 6.2 is established.

Remark 4. The theorem of Baker and Wüstholz (cf. Theorem 6.3) [19] has a significant role in the development of linear forms in logarithms. The final structure for the lower bound for linear forms in logarithms without an explicit determination of the constant involved has been established by Wüstholz [93] and the precise determination of that constant is the central aspect of [19] (see also [20]). The reader may note that slightly sharper bounds for n_1 and m_1 could be obtained by using Matveev's result [64] instead. However, the improvement is insignificant in view of our next step, i.e. the use of the method of Baker and Davenport (Lemma 6.4), in which our upper bounds for n_1 and m_1 are further reduced to a great extent.

6.5 Reduction of the bound

In our final step we reduce the huge upper bound for n_1 obtained in Proposition 6.1 (respectively m_1 in Proposition 6.2) by applying several times Lemma 6.4.

6.5.1 Proof of Theorem 6.1

First, we consider inequality (6.4.1) and recall that

$$\Lambda = n_1 \log \alpha - a_1 \log 2 - \log \sqrt{5}.$$

For technical reasons we assume that $\min\{n_1 - n_2, a_1 - a_2, a_1 - a_3\} \geq 20$. In the case that this condition fails we do the following:

- if $a_1 - a_2 < 20$ but $a_1 - a_3, n_1 - n_2 \geq 20$, we consider inequality (6.4.2), i.e. we go to Step 2;
- if $a_1 - a_2, a_1 - a_3 < 20$ but $n_1 - n_2 \geq 20$, we consider inequality (6.4.4), i.e. we go to Step 3;
- if $a_1 - a_2, n_1 - n_2 < 20$ but $a_1 - a_3 \geq 20$, we consider inequality (6.4.6), i.e. we go to Step 4;
- if $n_1 - n_2 < 20$ but $a_1 - a_2, a_1 - a_3 \geq 20$, we consider inequality (6.4.8), i.e. we go to Step 5; then we consider inequality (6.4.6), i.e. we go to Step 6;
- if all $a_1 - a_2, a_1 - a_3, n_1 - n_2 < 20$, we consider inequality (6.4.11), i.e. we go to Step 7.

Step 1: *We show that* $a_1 - a_2 \leq 218$ *or* $n_1 - n_2 \leq 315$.

Let us start by considering inequality (6.4.1). Since we assume that $\min\{n_1 - n_2, a_1 - a_2\} \geq 20$ we get $|\Phi| = |e^{\Lambda} - 1| < \frac{1}{4}$, hence $|\Lambda| < \frac{1}{2}$. And, since $|x| < 2|e^x - 1|$ holds for all $x \in (-\frac{1}{2}, \frac{1}{2})$ we get $|\Lambda| < 45.56 \max\{2^{a_2 - a_1}, \alpha^{n_2 - n_1}\}$. Then we have the inequality

$$\begin{aligned} 0 < \left| n_1 \cdot \frac{\log \alpha}{\log 2} - a_1 + \frac{\log(1/\sqrt{5})}{\log 2} \right| &< \max\left\{ \frac{45.56}{\log 2} \cdot 2^{-(a_1 - a_2)}, \frac{45.56}{\log 2} \alpha^{-(n_1 - n_2)} \right\} \\ &< \max\left\{ 66 \cdot 2^{-(a_1 - a_2)}, 66 \alpha^{-(n_1 - n_2)} \right\} \end{aligned}$$

and we apply the algorithm described in Remark 3 with

$$\gamma = \frac{\log \alpha}{\log 2}, \quad \mu = \frac{\log(1/\sqrt{5})}{\log 2}, \quad (A, B) = (66, 2) \text{ or } (66, \alpha).$$

Let us be a bit more precise. We note that γ is irrational since 2 and α are multiplicatively independent, hence Lemma 6.4 is applicable. Let $\gamma = [s_0, s_1, s_2, \dots] = [0, 1, 2, 3, 1, 2, 3, 2, 4, 2, 1, 2, 11, \dots]$ be the continued fraction expansion of γ. Moreover, we choose $M = 4.1 \cdot 10^{62}$ and consider the 125-th convergent

$$\frac{p_{125}}{q_{125}} = \frac{20283120185714146064760096009855998406870191682305457762852408 37}{29216213811755119636182936699474703108832235816008862704262414 82},$$

with $q = q_{125} > 6M$. This yields $\varepsilon > 0.24$ and therefore either

$$a_1 - a_2 \leq \frac{\log(66q/0.24)}{\log 2} < 219 \quad \text{or} \quad n_1 - n_2 \leq \frac{\log(66q/0.24)}{\log \alpha} < 316.$$

Thus, we have either $a_1 - a_2 \leq 218$ or $n_1 - n_2 \leq 315$.

From this result we distinguish between

Case 1 $a_1 - a_2 \leq 218$ and

Case 2 $n_1 - n_2 \leq 315$.

Step 2: *We consider Case 1 and show that under the assumption that $a_1 - a_2 \leq 218$ we have that $a_1 - a_3 \leq 225$ or $n_1 - n_2 \leq 324$.*

In this step we consider inequality (6.4.2) and assume that $a_1 - a_3, n_1 - n_2 \geq 20$. Recall that

$$\Lambda_1 = -n_1 \log \alpha + a_2 \log 2 + \log\left(\sqrt{5}\,(2^{a_1 - a_2} + 1)\right)$$

and inequality (6.4.2) yields that $|\Lambda_1| < 10.52 \max\left\{2^{-(a_1 - a_3)}, \alpha^{-(n_1 - n_2)}\right\}$. Then we get

$$0 < \left| n_1 \cdot \frac{\log \alpha}{\log 2} - a_2 + \frac{\log\left(1/\left(\sqrt{5}\,(2^{a_1 - a_2} + 1)\right)\right)}{\log 2} \right| < 16 \max\left\{2^{-(a_1 - a_3)}, \alpha^{-(n_1 - n_2)}\right\}.$$

We apply the algorithm explained in Remark 3 again with the same γ and M as in Step 1, but now we choose $(A, B) = (16, 2)$ or $(16, \alpha)$ and

$$\mu = \mu_k = \frac{\log\left(1/\left(\sqrt{5}\left(2^k + 1\right)\right)\right)}{\log 2}$$

for each possible value of $a_1 - a_2 = k = 0, 1, \ldots, 218$. With these parameters we run our algorithm and obtain for each instance a new and rather small upper bound either for $a_1 - a_3$ or $n_1 - n_2$. In particular

$$q_{128} = 4931046768508562296640389954874358321967185393449272313464959 3651$$

is the largest denominator that appeared in applying our algorithm. Overall, we obtain

$$a_1 - a_3 \leq 225 \quad \text{or} \quad n_1 - n_2 \leq 324.$$

Within Case 1 we have to distinguish between two further sub-cases:

Case 1A $a_1 - a_3 \leq 225$ and

Case 1B $n_1 - n_2 \leq 324$.

Step 3: *We consider Case 1A and show that under the assumption that* $a_1 - a_2 \leq 218$ *and* $a_1 - a_3 \leq 225$ *we have that* $n_1 - n_2 \leq 334$.

In this step we consider inequality (6.4.4) and assume that $n_1 - n_2 \geq 20$. Recall that

$$\Lambda_A = -n_1 \log \alpha + a_1 \log 2 + \log\left(\sqrt{5}\,(1 + 2^{a_2 - a_1} + 2^{a_3 - a_1})\right)$$

and inequality (6.4.4) yields that $|\Lambda_A| < 4.04\alpha^{-(n_1-n_2)}$. Then we get

$$0 < \left| n_1 \cdot \frac{\log \alpha}{\log 2} - a_1 + \frac{\log\left(1/\sqrt{5}\,(1 + 2^{a_2-a_1} + 2^{a_3-a_1})\right)}{\log 2} \right| < 6\alpha^{-(n_1-n_2)}.$$

We proceed as in Remark 3 with the same γ and M as in Step 1, but we use $(A, B) = (6, \alpha)$ instead. Moreover we consider

$$\mu = \mu_{k,l} = \frac{\log\left(1/\sqrt{5}\left(1 + 2^{-k} + 2^{-l}\right)\right)}{\log 2}$$

for each possible value of $a_1 - a_2 = k = 0, 1, \ldots, 218$ and $a_1 - a_3 = l = 0, 1, \ldots, 225$ (with respect to the obvious condition that $a_1 - a_2 \leq a_1 - a_3$). As in the previous step we apply the algorithm described in Remark 3 to each instance (k, l) and start with the 125-th convergent $\frac{p}{q} = \frac{p_{125}}{q_{125}}$ of γ as before and continue with the algorithm until a positive ε is obtained for every k and l. Thus we can compute a new upper bound for $n_1 - n_2$ by the formula $n_1 - n_2 < \frac{\log(6q/\varepsilon)}{\log \alpha}$ for the respective choices of q and ε. Overall we obtain that

$$n_1 - n_2 \leq 334.$$

Step 4: *We consider Case 1B and show that under the assumption that* $a_1 - a_2 \leq 218$ *and* $n_1 - n_2 \leq 324$ *we have that* $a_1 - a_3 \leq 233$.

Thus we consider inequality (6.4.6) and assume that $a_1 - a_3 \geq 20$. In view of Step 6 we perform the following reduction by considering $a_1 - a_2 \leq 224$ instead of $a_1 - a_2 \leq 218$. Note that the same inequality (6.4.6) will be used once more with a slightly higher upper bound $a_1 - a_2 \leq 224$ in Step 6. Recall that

$$\Lambda_B = n_2 \log \alpha - a_2 \log 2 + \log\left(\frac{\alpha^{n_1-n_2} + 1}{\sqrt{5}\,(2^{a_1-a_2} + 1)}\right)$$

and inequality (6.4.6) yields that $|\Lambda_B| < 2.9 \cdot 2^{-(a_1-a_3)}$. Then we get

$$0 < \left| n_2 \cdot \frac{\log \alpha}{\log 2} - a_2 + \frac{\log\left((\alpha^{n_1-n_2} + 1)/\left(\sqrt{5}\,(2^{a_1-a_2} + 1)\right)\right)}{\log 2} \right| < 5 \cdot 2^{-(a_1-a_3)}.$$

We apply our algorithm with the same γ and M as in the previous steps, but we use $(A,B)=(5,2)$ and

$$\mu=\mu_{k,r}=\frac{\log\left((\alpha^r+1)/\left(\sqrt{5}\left(2^k+1\right)\right)\right)}{\log 2}$$

for each possible value of $a_1-a_2=k=0,1,\dots,224$ and $n_1-n_2=r=0,1,\dots,324$. We run our algorithm starting with $q=q_{125}$ and compute the upper bound for a_1-a_3 by the formula $a_1-a_3<\frac{\log(5q/\varepsilon)}{\log 2}$ for respective choices of q and ε, provided the algorithm terminates. For those pairs (k,r) for which the algorithm terminates we obtain

$$a_1-a_3\leq 233.$$

However, in case that $(k,r)\in\{(0,2),(0,6),(2,10),(4,18)\}$ problems arise and our algorithm does not terminate. This is because in these cases there exist multiplicative dependences between $\mu_{k,r}$, 2 and α. In particular, one can easily check that

$$\frac{\alpha^2+1}{2\sqrt{5}}=\frac{\alpha}{2},\quad \frac{\alpha^6+1}{2\sqrt{5}}=\alpha^3,\quad \frac{\alpha^{10}+1}{5\sqrt{5}}=\alpha^5,\quad \frac{\alpha^{18}+1}{17\sqrt{5}}=2\alpha^9.$$

Using these dependencies we obtain

$$\begin{aligned}
&\Lambda_B=(n_2+1)\log\alpha-(a_2+1)\log 2, && \Lambda_B=(n_2+3)\log\alpha-a_2\log 2,\\
&\Lambda_B=(n_2+5)\log\alpha-a_2\log 2 \quad\text{and} && \Lambda_B=(n_2+9)\log\alpha-(a_2-1)\log 2
\end{aligned}$$

for $(k,r)=(0,2),(0,6),(2,10),(4,18)$ respectively. Thus we get

$$\left|\gamma-\frac{a_2+1}{n_2+1}\right|<\frac{5}{2^{a_1-a_3}(n_2+1)},\qquad \left|\gamma-\frac{a_2}{n_2+3}\right|<\frac{5}{2^{a_1-a_3}(n_2+3)},$$
$$\left|\gamma-\frac{a_2}{n_2+5}\right|<\frac{5}{2^{a_1-a_3}(n_2+5)}\quad\text{and}\quad \left|\gamma-\frac{a_2-1}{n_2+9}\right|<\frac{5}{2^{a_1-a_3}(n_2+9)}$$

respectively. If $a_1-a_3\leq 211$ the previous bound is still true. Now assume $a_1-a_3>211$. Then $2^{a_1-a_3}>4.2\cdot 10^{63}>10(n_2+9)$, hence

$$\frac{5}{2^{a_1-a_3}(n_2+1)}<\frac{1}{2(n_2+1)^2},\qquad \frac{5}{2^{a_1-a_3}(n_2+3)}<\frac{1}{2(n_2+3)^2},$$
$$\frac{5}{2^{a_1-a_3}(n_2+5)}<\frac{1}{2(n_2+5)^2}\quad\text{and}\quad \frac{5}{2^{a_1-a_3}(n_2+9)}<\frac{1}{2(n_2+9)^2}$$

respectively. By a criterion of Legendre each of $\frac{a_2+1}{n_2+1}$, $\frac{a_2}{n_2+3}$, $\frac{a_2}{n_2+5}$ and $\frac{a_2-1}{n_2+9}$ is a convergent to γ and we may assume that $\frac{a_2+1}{n_2+1}$, $\frac{a_2}{n_2+3}$, $\frac{a_2}{n_2+5}$ and $\frac{a_2-1}{n_2+9}$ is of the form $\frac{p_j}{q_j}$ for some $j=0,1,2,\dots,124$. Indeed, we may assume that $j\leq 124$ since $q_{125}>4.2\cdot 10^{62}>n_2+9$ but $q_{124}<4.2\cdot 10^{62}$. However it is well known (see e.g. [16, page 47]) that

$$\frac{1}{(s_{j+1}+2)q_j^2}<\left|\gamma-\frac{p_j}{q_j}\right|.$$

and since $\max\{s_{j+1} : j = 0,1,2,\dots,124\} = 134$, we have

$$\frac{1}{136q_j^2} < \frac{5}{2^{a_1-a_3}q_j}$$

and q_j divides one of $\{n_2+1, n_2+3, n_2+5, n_2+9\}$. Thus the inequality

$$2^{a_1-a_3} < 5\cdot 136(n_2+9) < 5\cdot 136\cdot 4.2\cdot 10^{62}$$

yields $a_1 - a_3 < 218$. Hence even in the case that $(k,r) \in \{(0,2),(0,6),(2,10),(4,18)\}$ we obtain the upper bound $a_1 - a_3 \leq 233$.

Step 5: *We consider Case 2 and show that under the assumption that $n_1 - n_2 \leq 315$ we have that $a_1 - a_2 \leq 224$.*

In this step we consider inequality (6.4.8) and assume that $a_1 - a_2, a_1 - a_3 \geq 20$. Recall that

$$\Lambda_2 = n_2 \log\alpha - a_1 \log 2 + \log\left(\frac{\alpha^{n_1-n_2}+1}{\sqrt{5}}\right)$$

and inequality (6.4.8) yields that $|\Lambda_2| < 4.9\cdot 2^{-(a_1-a_2)}$. Then we get

$$0 < \left| n_2\cdot\frac{\log\alpha}{\log 2} - a_1 + \frac{\log((\alpha^{n_1-n_2}+1)/\sqrt{5})}{\log 2}\right| < 8\cdot 2^{-(a_1-a_2)}.$$

We apply our algorithm with the same γ and M, but we use $(A,B) = (8,2)$ and

$$\mu = \mu_r = \frac{\log((\alpha^r+1)/\sqrt{5})}{\log 2},$$

for each possible value of $n_1 - n_2 = r = 0,1,\dots,315$. Similar as in Step 4 we obtain $a_1 - a_2 \leq 224$, except in the problematic case that $r \in \{2,6\}$. However these two problematic cases can be treated in a similar way as the problematic cases in Step 4. That is we find a multiplicative relation between 2, α and $\frac{\log((\alpha^r+1)/\sqrt{5})}{\log 2}$ and reduce linear form Λ_2 to a linear form in two logarithms and use the theory of continued fractions to obtain also in these problematic cases upper bounds for $a_1 - a_2$. Thus in any case we obtain $a_1 - a_2 \leq 224$.

Step 6: *We continue to consider Case 2 and show that under the assumption that $n_1 - n_2 \leq 315$ and $a_1 - a_2 \leq 224$ we have that $a_1 - a_3 \leq 233$.*

Now we have $n_1 - n_2 \leq 315$ and $a_1 - a_2 \leq 224$ and we shall assume that $a_1 - a_3 \geq 20$ and attempt to reduce the huge upper bound for $a_1 - a_3$ with the use of inequality (6.4.6). This setting has already been considered in Case 1B, where we obtained

$$a_1 - a_3 \leq 233.$$

Table 6.3 summarizes our results obtained so far.

Table 6.3: Summary of results

Upper bound of ($\leq$)	**Case 1A**	**Case 1B**	**Case 2**	**Overall**
$a_1 - a_2$	218	218	224	224
$a_1 - a_3$	225	233	233	233
$n_1 - n_2$	334	324	315	334

Step 7: *Under the assumption that* $n_1 - n_2 \leq 334$, $a_1 - a_2 \leq 224$ *and* $a_1 - a_3 \leq 233$ *we show that* $n_1 \leq 343$.

For the last step we consider inequality (6.4.11). Recall that

$$\Lambda_3 = -n_1 \log \alpha + a_1 \log 2 + \log\left(\frac{\sqrt{5}(1 + 2^{a_2-a_1} + 2^{a_3-a_1})}{1 + \alpha^{n_2-n_1}}\right)$$

and inequality (6.4.11) yields that $|\Lambda_3| < 2.02\alpha^{-n_1}$. Then we get

$$0 < \left| n_1 \cdot \frac{\log \alpha}{\log 2} - a_1 + \frac{\log\left((1 + \alpha^{n_2-n_1}) / \left(\sqrt{5}\,(1 + 2^{a_2-a_1} + 2^{a_3-a_1})\right)\right)}{\log 2} \right| < 3\alpha^{-n_1}.$$

We proceed as described in Remark 3 with the same γ and M as in the previous steps, but we use $(A, B) = (3, \alpha)$ and

$$\mu = \mu_{k,l,r} = \frac{\log\left((1 + \alpha^{-r}) / \left(\sqrt{5}\left(1 + 2^{-k} + 2^{-l}\right)\right)\right)}{\log 2},$$

for each possible value of $a_1 - a_2 = k = 0, 1, \ldots, 224$, $a_1 - a_3 = l = 0, 1, \ldots, 233$ (with respect to the obvious condition that $a_1 - a_2 \leq a_1 - a_3$) and $n_1 - n_2 = r = 0, 1, \ldots, 334$. Starting with q_{125} we compute the upper bound for n_1 by the formula $n_1 < \frac{\log(3q/\varepsilon)}{\log \alpha}$ for the respective choices of q such that $\varepsilon > 0$. For all triples (k, l, r) except

$$(k, l, r) \in \{(0, 1, 10), (0, 3, 18), (1, 1, 2), (1, 1, 6), (1, 3, 14), (3, 3, 10), (5, 5, 18)\}$$

the algorithm terminates and yields

$$n_1 \leq 343. \tag{6.5.1}$$

The problematic cases can be treated in a similar way as in Step 4 and yield similarly small upper bounds for n_1. In particular we obtain that $n_1 \leq 343$ in all cases. However this upper bound contradicts our assumption that $n_1 \geq 360$. Therefore no further solutions to (6.1.1) exist and Theorem 6.1 is proved.

6.5.2 Proof of Theorem 6.2

We reduce the upper bound for m_1 obtained in Proposition 6.2 by applying several times our algorithm described in Remark 3. We do this in a similar manner as in the proof of Theorem 6.1.

Step 1: *We show that $t_1 - t_2 \le 218$ or $m_1 - m_2 \le 314$.*

First, we consider inequality (6.4.12) and deduce that

$$0 < \left| m_1 \cdot \frac{\log \alpha}{\log 2} - t_1 + \frac{\log(1/\sqrt{5})}{\log 2} \right| < \max\left\{ 43 \cdot 2^{-(t_1 - t_2)}, 43\alpha^{-(m_1 - m_2)} \right\}.$$

We apply Lemma 6.4 with the same $\gamma = \frac{\log \alpha}{\log 2}$ as in the case of Theorem 6.1.1, but we use $M = 4.2 \cdot 10^{62}$, $(A, B) = (43, 2)$ or $(43, \alpha)$ and $\mu = \frac{\log(1/\sqrt{5})}{\log 2}$. We consider the 125-th convergent $\frac{p_{125}}{q_{125}}$ of γ and obtain $\varepsilon > 0.24$ and therefore either

$$t_1 - t_2 \le \frac{\log(43q/0.24)}{\log 2} \le 218, \quad \text{or} \quad m_1 - m_2 \le \frac{\log(43q/0.24)}{\log \alpha} \le 314.$$

Now, we distinguish between

Case 1 $m_1 - m_2 \le 314$ and

Case 2 $t_1 - t_2 \le 218$.

Step 2: *We consider Case 1 and show that under the assumption that $m_1 - m_2 \le 314$ we have $t_1 - t_2 \le 226$ or $m_1 - m_3 \le 326$.*

We consider inequality (6.4.13) and get

$$0 < \left| m_2 \cdot \frac{\log \alpha}{\log 2} - t_1 + \frac{\log\left(\left(\alpha^{m_1 - m_2} + 1\right) / \sqrt{5} \right)}{\log 2} \right| < 36 \max\left\{ 2^{-(t_1 - t_2)}, \alpha^{-(m_1 - m_3)} \right\}.$$

We apply our algorithm (cf. Remark 3) for each possible value of $m_1 - m_2 = k \le 314$ and the algorithm yields $t_1 - t_2 \le 226$ or $m_1 - m_3 \le 326$ for all $k = 1, 2, \ldots, 314$ except $k \in \{2, 6\}$. These two problematic cases can be treated by using continued fractions and Legendre's criterion. Thus we obtain in all cases that $t_1 - t_2 \le 226$ or $m_1 - m_3 \le 326$.

Within Case 1, we distinguish between the following two sub-cases:

Case 1A $m_1 - m_3 \le 326$ and

Case 1B $t_1 - t_2 \le 226$.

Step 3: *We consider Case 1A and show that under the assumption that* $m_1 - m_2 \le 314$ *and* $m_1 - m_3 \le 326$ *we have* $t_1 - t_2 \le 231$.

We consider inequality (6.4.14) and get

$$0 < \left| m_1 \cdot \frac{\log \alpha}{\log 2} - t_1 + \frac{\log\left((1 + \alpha^{m_2-m_1} + \alpha^{m_3-m_1})/\sqrt{5}\right)}{\log 2} \right| < 6 \cdot 2^{-(t_1-t_2)}.$$

For each possible value of $m_1 - m_2 = k \le 314$ and $m_1 - m_3 = l \le 326$ (with respect to the obvious condition $m_1 - m_2 \le m_1 - m_3$) except for

$$(k, l) \in \{(0,3), (1,1), (1,5), (3,4), (7,8)\},$$

our algorithm yields $t_1 - t_2 \le 231$. Note that the same upper bound can be concluded for the exceptional cases by using continued fractions and Legendre's criterion.

Step 4: *We consider Case 1B and show that under the assumption that* $m_1 - m_2 \le 314$ *and* $t_1 - t_2 \le 226$ *we have* $m_1 - m_3 \le 336$.

In view of Step 6 we consider $m_1 - m_2 \le 323$ instead of $m_1 - m_2 \le 314$ as required in this step. We consider inequality (6.4.15) and get

$$0 < \left| m_2 \cdot \frac{\log \alpha}{\log 2} - t_2 + \frac{\log\left((\alpha^{m_1-m_2} + 1)/\left(\sqrt{5}\left(2^{t_1-t_2} + 1\right)\right)\right)}{\log 2} \right| < 9\alpha^{-(m_1-m_3)}.$$

By applying our algorithm for each possible value of $m_1 - m_2 = k \le 323$ and $t_1 - t_2 = r \le 226$ we get $m_1 - m_3 \le 336$, except for $(k, r) \in \{(2,0), (6,0), (10,2), (18,4)\})$. However, by using continued fractions and Legendre's criterion we obtain the same upper bound also for these exceptional cases.

Step 5: *We consider Case 2 and show that under the assumption that* $t_1 - t_2 \le 218$ *we have* $m_1 - m_2 \le 323$.

We consider inequality (6.4.16) and get

$$0 < \left| m_2 \cdot \frac{\log \alpha}{\log 2} - t_2 + \frac{\log\left(1/\left(\sqrt{5}\left(2^{t_1-t_2} + 1\right)\right)\right)}{\log 2} \right| < 12\alpha^{-(m_1-m_2)}.$$

For each possible value of $t_1 - t_2 = r \le 218$ our algorithm yields $m_1 - m_2 \le 323$.

Step 6: *We continue to consider Case 2 and show that under the assumption that $t_1 - t_2 \le 218$ and $m_1 - m_2 \le 323$ we have $m_1 - m_3 \le 336$.*

This situation is covered by Step 4 and we obtain that $m_1 - m_3 \le 336$. Table 6.4 summarizes our results obtained so far.

Table 6.4: Summary of results

Upper bound of ($\le$)	**Case 1A**	**Case 1B**	**Case 2**	**Overall**
$m_1 - m_2$	314	314	323	323
$m_1 - m_3$	326	336	336	336
$t_1 - t_2$	231	226	218	231

Step 7: *Under the assumption that $t_1 - t_2 \le 231$, $m_1 - m_2 \le 323$ and $m_1 - m_3 \le 336$ we show that $m_1 \le 353$.*

For the last step in our reduction process we consider inequality (6.4.17) and get

$$0 < \left| m_1 \cdot \frac{\log \alpha}{\log 2} - t_1 + \frac{\log\left((1 + \alpha^{m_2 - m_1} + \alpha^{m_3 - m_1}) / \left(\sqrt{5} \left(1 + 2^{t_2 - t_1} \right) \right) \right)}{\log 2} \right| < 6\alpha^{-m_1}.$$

We apply our algorithm for each possible value of $m_1 - m_2 = k \le 324$, $m_1 - m_3 = l \le 337$ (with respect to the obvious condition $m_1 - m_2 \le m_1 - m_3$) and $t_1 - t_2 = r \le 232$ and get $m_1 \le 353$ except in the case that

$$(k, l, r) \in \{(0,3,0), (1,1,0), (1,5,0), (3,4,0), (7,8,0), (1,9,2), (11,12,2), (1,17,4), (19,20,4)\}.$$

These exceptional cases can be treated by using continued fractions and Legendre's criterion. Thus we obtain the upper bound $m_1 \le 353$ in all cases. But this upper bound contradicts our assumption that $m_1 \ge 360$. Therefore, no further solutions to (6.1.2) exist and Theorem 6.2 is proved.

6.6 Appendix - Lists of solutions for Theorem 6.1 and Theorem 6.2

The solutions for Diophantine equation (6.1.1) in Theorem 6.1 are displayed below. Since $F_1 = F_2$, the solutions involving F_1 are not displayed for the sake of simplicity.

$F_3 + F_2 = 2^0 + 2^0 + 2^0 = 3,$ $\qquad$ $F_3 + F_3 = 2^1 + 2^0 + 2^0 = 4,$

$F_4 + F_0 = 2^0 + 2^0 + 2^0 = 3,$
$F_4 + F_2 = 2^1 + 2^0 + 2^0 = 4,$
$F_4 + F_3 = 2^1 + 2^1 + 2^0 = 5,$
$F_4 + F_4 = 2^1 + 2^1 + 2^1 = 6,$
$F_4 + F_4 = 2^2 + 2^0 + 2^0 = 6,$
$F_5 + F_0 = 2^1 + 2^1 + 2^0 = 5,$
$F_5 + F_2 = 2^1 + 2^1 + 2^1 = 6,$
$F_5 + F_2 = 2^2 + 2^0 + 2^0 = 6,$
$F_5 + F_3 = 2^2 + 2^1 + 2^0 = 7,$
$F_5 + F_4 = 2^2 + 2^1 + 2^1 = 8,$
$F_5 + F_5 = 2^2 + 2^2 + 2^1 = 10,$
$F_5 + F_5 = 2^3 + 2^0 + 2^0 = 10,$
$F_6 + F_0 = 2^2 + 2^1 + 2^1 = 8,$
$F_6 + F_2 = 2^2 + 2^2 + 2^0 = 9,$
$F_6 + F_3 = 2^2 + 2^2 + 2^1 = 10,$
$F_6 + F_3 = 2^3 + 2^0 + 2^0 = 10,$
$F_6 + F_4 = 2^3 + 2^1 + 2^0 = 11,$
$F_6 + F_5 = 2^3 + 2^2 + 2^0 = 13,$
$F_6 + F_6 = 2^3 + 2^2 + 2^2 = 16,$
$F_7 + F_0 = 2^3 + 2^2 + 2^0 = 13,$
$F_7 + F_2 = 2^3 + 2^2 + 2^1 = 14,$
$F_7 + F_4 = 2^3 + 2^2 + 2^2 = 16,$
$F_7 + F_5 = 2^3 + 2^3 + 2^1 = 18,$
$F_7 + F_5 = 2^4 + 2^0 + 2^0 = 18,$
$F_7 + F_6 = 2^4 + 2^2 + 2^0 = 21,$
$F_7 + F_7 = 2^4 + 2^3 + 2^1 = 26,$
$F_8 + F_0 = 2^4 + 2^2 + 2^0 = 21,$
$F_8 + F_2 = 2^4 + 2^2 + 2^1 = 22,$
$F_8 + F_4 = 2^3 + 2^3 + 2^3 = 24,$
$F_8 + F_4 = 2^4 + 2^2 + 2^2 = 24,$
$F_8 + F_5 = 2^4 + 2^3 + 2^1 = 26,$
$F_8 + F_7 = 2^4 + 2^4 + 2^1 = 34,$
$F_8 + F_7 = 2^5 + 2^0 + 2^0 = 34,$
$F_8 + F_8 = 2^5 + 2^3 + 2^1 = 42,$
$F_9 + F_0 = 2^4 + 2^4 + 2^1 = 34,$
$F_9 + F_0 = 2^5 + 2^0 + 2^0 = 34,$
$F_9 + F_2 = 2^5 + 2^1 + 2^0 = 35,$
$F_9 + F_3 = 2^4 + 2^4 + 2^2 = 36,$
$F_9 + F_3 = 2^5 + 2^1 + 2^1 = 36,$
$F_9 + F_4 = 2^5 + 2^2 + 2^0 = 37,$
$F_9 + F_6 = 2^5 + 2^3 + 2^1 = 42,$
$F_9 + F_9 = 2^5 + 2^5 + 2^2 = 68,$
$F_9 + F_9 = 2^6 + 2^1 + 2^1 = 68,$
$F_{10} + F_2 = 2^5 + 2^4 + 2^3 = 56,$
$F_{10} + F_7 = 2^5 + 2^5 + 2^2 = 68,$
$F_{10} + F_7 = 2^6 + 2^1 + 2^1 = 68,$
$F_{10} + F_8 = 2^6 + 2^3 + 2^2 = 76,$
$F_{11} + F_6 = 2^6 + 2^5 + 2^0 = 97,$
$F_{11} + F_{10} = 2^6 + 2^6 + 2^4 = 144,$
$F_{11} + F_{10} = 2^7 + 2^3 + 2^3 = 144,$
$F_{12} + F_0 = 2^6 + 2^6 + 2^4 = 144,$
$F_{12} + F_0 = 2^7 + 2^3 + 2^3 = 144,$
$F_{12} + F_2 = 2^7 + 2^4 + 2^0 = 145,$
$F_{12} + F_3 = 2^7 + 2^4 + 2^1 = 146,$
$F_{12} + F_6 = 2^7 + 2^4 + 2^3 = 152,$
$F_{12} + F_{12} = 2^7 + 2^7 + 2^5 = 288,$
$F_{12} + F_{12} = 2^8 + 2^4 + 2^4 = 288,$
$F_{13} + F_{10} = 2^7 + 2^7 + 2^5 = 288,$
$F_{13} + F_{10} = 2^8 + 2^4 + 2^4 = 288,$
$F_{13} + F_{11} = 2^8 + 2^6 + 2^1 = 322,$
$F_{14} + F_6 = 2^8 + 2^7 + 2^0 = 385,$
$F_{14} + F_{12} = 2^9 + 2^3 + 2^0 = 521,$
$F_{15} + F_9 = 2^9 + 2^7 + 2^2 = 644,$
$F_{16} + F_{10} = 2^{10} + 2^4 + 2^1 = 1042,$
$F_{17} + F_4 = 2^{10} + 2^9 + 2^6 = 1600,$
$F_{18} + F_6 = 2^{11} + 2^9 + 2^5 = 2592.$

The solutions for Diophantine equation (6.1.2) in Theorem 6.2 are displayed below. Since $F_1 = F_2$, the solutions involving F_1 are not displayed for the sake of simplicity.

$$F_2 + F_2 + F_0 = 2^0 + 2^0 = 2, \qquad F_2 + F_2 + F_2 = 2^1 + 2^0 = 3,$$
$$F_3 + F_0 + F_0 = 2^0 + 2^0 = 2, \qquad F_3 + F_2 + F_0 = 2^1 + 2^0 = 3,$$
$$F_3 + F_2 + F_2 = 2^1 + 2^1 = 4, \qquad F_3 + F_3 + F_0 = 2^1 + 2^1 = 4,$$
$$F_3 + F_3 + F_2 = 2^2 + 2^0 = 5, \qquad F_3 + F_3 + F_3 = 2^2 + 2^1 = 6,$$
$$F_4 + F_0 + F_0 = 2^1 + 2^0 = 3, \qquad F_4 + F_2 + F_0 = 2^1 + 2^1 = 4,$$
$$F_4 + F_2 + F_2 = 2^2 + 2^0 = 5, \qquad F_4 + F_3 + F_0 = 2^2 + 2^0 = 5,$$
$$F_4 + F_3 + F_2 = 2^2 + 2^1 = 6, \qquad F_4 + F_4 + F_0 = 2^2 + 2^1 = 6,$$
$$F_4 + F_4 + F_3 = 2^2 + 2^2 = 8, \qquad F_4 + F_4 + F_4 = 2^3 + 2^0 = 9,$$
$$F_5 + F_0 + F_0 = 2^2 + 2^0 = 5, \qquad F_5 + F_2 + F_0 = 2^2 + 2^1 = 6,$$
$$F_5 + F_3 + F_2 = 2^2 + 2^2 = 8, \qquad F_5 + F_3 + F_3 = 2^3 + 2^0 = 9,$$
$$F_5 + F_4 + F_0 = 2^2 + 2^2 = 8, \qquad F_5 + F_4 + F_2 = 2^3 + 2^0 = 9,$$
$$F_5 + F_4 + F_3 = 2^3 + 2^1 = 10, \qquad F_5 + F_5 + F_0 = 2^3 + 2^1 = 10,$$
$$F_5 + F_5 + F_3 = 2^3 + 2^2 = 12, \qquad F_6 + F_0 + F_0 = 2^2 + 2^2 = 8,$$
$$F_6 + F_2 + F_0 = 2^3 + 2^0 = 9, \qquad F_6 + F_2 + F_2 = 2^3 + 2^1 = 10,$$
$$F_6 + F_3 + F_0 = 2^3 + 2^1 = 10, \qquad F_6 + F_3 + F_3 = 2^3 + 2^2 = 12,$$
$$F_6 + F_4 + F_2 = 2^3 + 2^2 = 12, \qquad F_6 + F_5 + F_4 = 2^3 + 2^3 = 16,$$
$$F_6 + F_5 + F_5 = 2^4 + 2^1 = 18, \qquad F_6 + F_6 + F_0 = 2^3 + 2^3 = 16,$$
$$F_6 + F_6 + F_2 = 2^4 + 2^0 = 17, \qquad F_6 + F_6 + F_3 = 2^4 + 2^1 = 18,$$
$$F_6 + F_6 + F_6 = 2^4 + 2^3 = 24, \qquad F_7 + F_3 + F_2 = 2^3 + 2^3 = 16,$$
$$F_7 + F_3 + F_3 = 2^4 + 2^0 = 17, \qquad F_7 + F_4 + F_0 = 2^3 + 2^3 = 16,$$
$$F_7 + F_4 + F_2 = 2^4 + 2^0 = 17, \qquad F_7 + F_4 + F_3 = 2^4 + 2^1 = 18,$$
$$F_7 + F_5 + F_0 = 2^4 + 2^1 = 18, \qquad F_7 + F_5 + F_3 = 2^4 + 2^2 = 20,$$
$$F_7 + F_6 + F_4 = 2^4 + 2^3 = 24, \qquad F_7 + F_7 + F_6 = 2^5 + 2^1 = 34,$$
$$F_8 + F_3 + F_2 = 2^4 + 2^3 = 24, \qquad F_8 + F_4 + F_0 = 2^4 + 2^3 = 24,$$
$$F_8 + F_6 + F_4 = 2^4 + 2^4 = 32, \qquad F_8 + F_6 + F_5 = 2^5 + 2^1 = 34,$$
$$F_8 + F_7 + F_0 = 2^5 + 2^1 = 34, \qquad F_8 + F_7 + F_3 = 2^5 + 2^2 = 36,$$
$$F_9 + F_0 + F_0 = 2^5 + 2^1 = 34, \qquad F_9 + F_2 + F_2 = 2^5 + 2^2 = 36,$$
$$F_9 + F_3 + F_0 = 2^5 + 2^2 = 36, \qquad F_9 + F_4 + F_4 = 2^5 + 2^3 = 40,$$
$$F_9 + F_5 + F_2 = 2^5 + 2^3 = 40, \qquad F_9 + F_7 + F_2 = 2^5 + 2^4 = 48,$$
$$F_9 + F_8 + F_7 = 2^6 + 2^2 = 68, \qquad F_9 + F_9 + F_0 = 2^6 + 2^2 = 68,$$
$$F_{10} + F_5 + F_5 = 2^6 + 2^0 = 65, \qquad F_{10} + F_6 + F_2 = 2^5 + 2^5 = 64,$$

$F_{10} + F_6 + F_3 = 2^6 + 2^0 = 65,$

$F_{10} + F_6 + F_4 = 2^6 + 2^1 = 66,$

$F_{10} + F_6 + F_5 = 2^6 + 2^2 = 68,$

$F_{10} + F_7 + F_0 = 2^6 + 2^2 = 68,$

$F_{10} + F_{10} + F_9 = 2^7 + 2^4 = 144,$

$F_{11} + F_5 + F_3 = 2^6 + 2^5 = 96,$

$F_{11} + F_9 + F_5 = 2^6 + 2^6 = 128,$

$F_{11} + F_9 + F_7 = 2^7 + 2^3 = 136,$

$F_{11} + F_9 + F_8 = 2^7 + 2^4 = 144,$

$F_{11} + F_{10} + F_0 = 2^7 + 2^4 = 144,$

$F_{12} + F_0 + F_0 = 2^7 + 2^4 = 144,$

$F_{12} + F_6 + F_6 = 2^7 + 2^5 = 160,$

$F_{12} + F_7 + F_4 = 2^7 + 2^5 = 160,$

$F_{12} + F_{11} + F_{10} = 2^8 + 2^5 = 288,$

$F_{12} + F_{12} + F_0 = 2^8 + 2^5 = 288,$

$F_{13} + F_8 + F_3 = 2^7 + 2^7 = 256,$

$F_{13} + F_8 + F_4 = 2^8 + 2^0 = 257,$

$F_{13} + F_9 + F_5 = 2^8 + 2^4 = 272,$

$F_{13} + F_9 + F_8 = 2^8 + 2^5 = 288,$

$F_{13} + F_{10} + F_0 = 2^8 + 2^5 = 288,$

$F_{14} + F_5 + F_3 = 2^8 + 2^7 = 384,$

$F_{14} + F_{12} + F_{10} = 2^9 + 2^6 = 576,$

$F_{16} + F_9 + F_4 = 2^9 + 2^9 = 1024,$

$F_{16} + F_9 + F_5 = 2^{10} + 2^1 = 1026,$

$F_{16} + F_{12} + F_8 = 2^{10} + 2^7 = 1152.$

Bibliography

[1] A. Baker, Linear forms in the logarithms of algebraic numbers I, *Mathematatika* **13** (1966) 204–216.

[2] A. Baker, Linear forms in the logarithms of algebraic numbers II, *Mathematika* **14** (1967) 102–107.

[3] A. Baker, Linear forms in the logarithms of algebraic numbers III, *Mathematika* **14** (1967) 220–228.

[4] A. Baker, Linear forms in the logarithms of algebraic numbers IV, *Mathematika* **15** (1968) 204–216.

[5] A. Baker, Contributions to the theory of Diophantine equations I, On the representation of integers by binary forms. *Phil. Trans. R. Sol. London Series A* **263** (1968) 173–191.

[6] A. Baker, Contributions to the theory of Diophantine equations II, The Diophantine equation $y^2 = x^3 + k$. *Phil. Trans. R. Sol. London Series A* **263** (1968) 193–208.

[7] A. Baker, A remark on the class number of quadratic fields. *Bull. London Math. Soc.* **1** (1969) 98–102.

[8] A. Baker, Bounds for the solutions of the hyperelliptic equation. *Proc. Cambridge Philos. Soc.* **65** (1969) 439–444.

[9] A. Baker, Imaginary quadratic fields with class number 2. *Ann. of Math.* **94** (1971) 139–152.

[10] A. Baker, On the class number of imaginary quadratic fields. *Bull. American Math. Soc.* **77** No. 5 (1971) 678–684.

[11] A. Baker, A sharpening of the bounds for liner forms in logarithms I. *Acta Arith.* **21** (1972) 117–129.

[12] A. Baker, A sharpening of the bounds for liner forms in logarithms II. *Acta Arith.* **24** (1973) 33–36.

[13] A. Baker, A sharpening of the bounds for liner forms in logarithms III. *Acta Arith.* **27** (1975) 247–252.

[14] Alan Baker, *Transcendental number theory.* Cambridge University Press, London, 1975.

[15] A. Baker, The theory of linear forms in logarithms. *In: Transcendence theory: advances and applications* (Proc. Conf., Univ. Cambridge, Cambridge, 1976), pp. 1–27. Academic Press, London, 1977.

[16] A. Baker, A Concise Introduction to the Theory of Numbers, *Cambridge University Press, Cambridge*, 1984.

[17] A. Baker and H. Davenport, The equations $3x^2 - 2 = y^2$ and $8x^2 - 7 = z^2$. *Quart. J. Math. Oxford Ser. (2)*, **20** (1969) 129–137.

[18] A. Baker and H. M. Stark, On a fundamental inequality in number theory. *Ann. of Math. (2)* **94** (1971) 190–199.

[19] A. Baker and G. Wüstholz, Logarithmic forms and group varieties. *J. Reine Angew. Math.* **442** (1993) 19–62.

[20] A. Baker and G. Wüstholz, *Logarithmic forms and Diophantine geometry*, volume 9 of *New Mathematical Monographs.* Cambridge University Press, Cambridge, 2007.

[21] M. A. Bennett, On some exponential equations of S. S. Pillai. *Canad. J. Math.* **53**(5) (2001) 897–922.

[22] D. Bertrand, Lemmes de Schwarz et lemmes d'approximations dans les domaines ultramétriques. *Groupe d'Étude d'Analyse Ultramétrique (3e année: 1975/76), no. 2 (Marseille-Luminy, 1976), Exp. No. J8, 12 pp. Secrétariat Math., Paris, 1977.*

[23] Yu. F. Bilu, Catalan's conjecture (after Mihăilescu), Séminaire Bourbaki, Exposé **909**, 55ème année (2002–2003) *Astérisque.* **294** (2004) 1–26.

[24] Yu. Bilu, Y. Bugeaud and M. Mignotte, *The Problem of Catalan*, Springer, 2014.

[25] M. Bliznac Trebješanin, A. Filipin, Nonexistence of $D(4)$-quintuples, preprint.

[26] N. Bourbaki, *Algebra II, Ch. 4–7*, Springer (1990).

[27] J. J. Bravo, B. Faye and F. Luca, Powers of two as sums of three Pell numbers. *Taiwanese J. Math.* **21** (2017) No. 4, 730–751.

[28] J. J. Bravo, Carlos A. Gómez and F. Luca, Powers of two as sums of two k-Fibonacci numbers. *Miskolc Math. Notes* **17** (2016) No. 1, 85–100.

[29] J. J. Bravo and F. Luca, Powers of two in generalized Fibonacci sequences. *Rev. Colombiana Mat.* **46**(1) (2012) 67–79.

[30] J. J. Bravo and F. Luca, On a conjecture about repdigits in k-generalized Fibonacci sequences. *Publ. Math. Debrecen* **82**(3–4) (2013) 623–639.

[31] J. J. Bravo and F. Luca, On the Diophantine equation $F_n + F_m = 2^a$. *Quaest. Math.* **39** (2016) No. 3, 391–400.

[32] J. J. Bravo, F. Luca and K. Yazán, On Pillai's problem with tribonacci numbers and powers of 2. *Bull. Korean Math. Soc.* **54**(3) (2017) 1069–1080.

[33] Y. Bugeaud and M. Laurent, Minoration effective de la distance p-adique entre puissances de nombres algébriques, *Journal of Number Theory* **61** (1996) 311–342.

[34] J. W. S. Cassels, On the equation $a^x - b^y = 1$. *Amer. J. Math.* **75** (1953) 159–162.

[35] E. Catalan, Note extraite d'une lettre adressée à l' éditeur, *J. Reine Angew. Math.* **27** (1844) pp.192.

[36] K. C. Chim, I. Pink, and V. Ziegler, On a variant of Pillai's problem. *Int. J. Number Theory* **13** (2017) No. 7, 1711–1727.

[37] K. C. Chim, I. Pink, and V. Ziegler, On a variant of Pillai's problem II. *J. Number Theory* **183** (2018) 269–290.

[38] K. C. Chim and V. Ziegler, On Diophantine equations involving sums of Fibonacci numbers and powers of 2. *Submitted.*

[39] M. Ddamulira, F. Luca, and M. Rakotomalala, On a problem of Pillai with Fibonacci numbers and powers of 2. *Proc. Indian Acad. Sci. Math. Sci.* **127**(3) (2017) 411–421.

[40] A. Dujella, Diophantine m-tuples, available at `http://web.math.hr/~duje/dtuples.html`

[41] A. Dujella, There are only finitely many Diophantine quintuples. *J. Reine Angew. Math.* **566** (2004) 183–214.

[42] A. Dujella and A. Pethő, A generalization of a theorem of Baker and Davenport. *Quart. J. Math. Oxford Ser. (2)* **49**(195) (1998) 291–306.

[43] N. I. Feldman, Estimation of a linear form in the logarithms of algebraic numbers, Mat. Sb. 76 (1968), 304-319; and similar titles, *Mat. Sb.* **77** (1968), 423–436; *Usp. Mat. Nauk* **23** (1968), 185–186; *Dokl. Akad. Nauk* **182** (1968), 1278–1279.

[44] N. I. Feldman, Improved estimate for a linear form of the logarithms of algebraic numbers. *Mat. Sbornik.* **119** (1968) No.3, 393–406.

[45] A. O. Gelfond, On Hilbert's seventh problem. *Dokl. Akad. Nauk SSSR 2* (1934) 1–3 (in Russian) and 4–6 (in French) Sur le septième problème de Hilbert. *Izv. Akad. Nauk SSSR, Ser. Mat. 7* (1934) 623–630.

[46] A. O. Gelfond, On the approximation of transcendental numbers by algebraic numbers, Dokl. Akad. Nauk SSSR, **2** (1935) 177–182.

[47] A. O. Gelfond, Transcendental and algebraic numbers, Dover Phoenix editions, New York: Dover Publications. (1960).

[48] A. O. Gelfond and Yu. V. Linnik, On Thue's method and the problem of effectiveness in quadratic fields. *Dokl. Akad. Nauk SSSR.* **61** (1948) 773–776 (in Russian).

[49] N. Gouillon, *Minorations explicites de formes linéaires en deux logarithmes*. Thesis (2003).

[50] N. Gouillon, Explicit lower bounds for linear forms in two logarithms, Journal de Théorie des Nombres de Bordeaux **18** (2006) 125–146.

[51] B. He, A. Togbé, V. Ziegler, There is no Diophantine quintuple, preprint.

[52] H. Heilbronn and E. H. Linfoot, On the imaginary quadratic corpora of class-number one. *Quart. J. Math. Oxford Ser.* **5** (1934) 293–301.

[53] S. Lang, *Elliptic curves Diophantine analysis.* Springer-Verlag Berlin Heidelberg, 1978.

[54] M. Laurent, Linear forms in two logarithms and interpolation determinants, *Acta Arith.* **66** (1994) 181–199.

[55] M. Laurent, Linear forms in two logarithms and interpolation determinants II, *Acta Arith.* **133**(4) (2008) 325–348.

[56] M. Laurent, M. Mignotte, Y. Nesterenko, Formes linéaires en deux logarithms et déterminants d'interpolation, *J. Number Theory* **55**(2) (1995) 285–321.

[57] A. K. Lenstra, H. W. Lenstra and L. Lovász, Factoring polynomials with rational coefficients. *Math. Ann.* **261** (1982) No. 4, 515–534.

[58] F. Luca, Distinct digits in base b expansions of linear recurrence sequences. *Quaest. Math.* **23** (2000) No. 4, 389–404.

[59] K. Mahler, Ein Beweis der Transzendenz der P-adischen Exponential-funktion. *J. Reine Angew. Math.* **169** (1932) 61–66.

[60] K. Mahler, Über transzendente P-adische Zahlen. *Compositio. Math.* **2** (1935) 259–275.

[61] D. Masser, Conjecture in "Open problems" section in *Proceedings of the Symposium on Analytic Number Theory,* ed. W. W. L. Chen, Imperial College, London (1985) 25.

[62] D. W. Masser and G. Wüstholz, Zero estimates on group varieties I, *Invent. Math.* **64** (1981) 489–516.

[63] D. W. Masser and G. Wüstholz, Zero estimates on group varieties II, *Invent. Math.* **80** (1985) 233–267.

[64] E. M. Matveev, An explicit lower bound for a homogeneous rational linear form in logarithms of algebraic numbers. II, *Izv. Ross. Akad. Nauk Ser. Mat.* **64**(6) (2000) 125–180, translation in *Izv. Math.* **64**(6) (2000) 1217–1269.

[65] N. K. Meher and S. S. Rout, Linear combinations of prime powers in sums of terms of binary recurrence sequences. *Lith. Math. J.* **57** (2017) No. 4, 506–520.

[66] M. Mignotte, A kit on linear forms in three logarithms. *Preprint.*

[67] P. Mihăilescu, Primary cyclotomic units and a proof of Catalan's conjecture. *J. Reine Angew. Math.* **572** (2004) 167–195.

[68] J. Neukirch, *Algebraic number theory*, volume 322 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, Berlin, 1999. Translated from the 1992 German original and with a note by Norbert Schappacher, With a foreword by G. Harder.

[69] A. N. Parshin, I. R. Shafarevich editors. *A Number Theory IV Transcendental Numbers.* Springer. 1998.

[70] P. Philippon and M. Waldschmidt, Lower bounds for linear forms in logarithms. *In: New Advances in Transcendence Theory*, ed. A. Baker, Cambridge: Cambridge University Press (1988) 280–312.

[71] S. S. Pillai, On $a^x - b^y = c$. *J. Indian Math. Soc. (N.S.)* **2** (1936) 119–122.

[72] S. S. Pillai, On the equation $2^x - 3^y = 2^X + 3^Y$, *Bull. Calcutta Math. Soc.* **37** (1945) 15–20.

[73] A. M. Robert, *A Course in p-adic Analysis. Graduate Texts in Mathematics 198*, Springer-Verlag, New York (2000).

[74] J. B. Rosser and L. Schoenfeld, Approximate formulas for some functions of prime numbers. *Illinois J. Math.* **6** (1962) 64–94.

[75] Th. Schneider, Transzendenzuntersuchungen periodischer Funktionen. *J. Reine Angew. Math. 172*, 65–69 and 70–73. (1934).

[76] N. P. Smart, *The Algorithmic Resolution of Diophantine Equations. London Mathematical Society Student Texts 41.* Cambridge University Press. 1998.

[77] H. M. Stark, On complex quadratic fields with class-number equal to one. *Trans. Amer. Math. Soc.* **122** (1966) 112–119.

[78] H. M. Stark, A complete determination of the complex quadratic fields of class number one. *Michigan Math. J.* **14** (1967) 1–27.

[79] H. M. Stark, A transcendence theorem for class-number problems. *Ann. of Math. (2)* **94** (1971) 153–173.

[80] H. M. Stark, A transcendence theorem for class-number problems. II. *Ann. of Math. (2)* **96** (1972) 174–209.

[81] H. M. Stark, On complex quadratic fields wth class-number two. Collection of articles dedicated to Derrick Henry Lehmer on the occasion of his seventieth birthday. *Math. Comp.* **29** (1975) 289–302.

[82] C. L. Stewart, On the representation of an integer in two different bases. *J. Reine Angew. Math.* **319** (1980) 63–72.

[83] C. L. Stewart, On divisors of Lucas and Lehmer numbers. *Acta Math.* **211** (2013) 291–314.

[84] C. L. Stewart and Kunrui Yu, On the *abc* conjecture. *Math. Ann.* **291** (1991) 225–230.

[85] C. L. Stewart and Kunrui Yu, On the *abc* conjecture II. *Duke Math. J.* **108** (2001) 169–181.

[86] T. N. Shorey and R. Tijdeman, *Exponential Diophantine equations*, volume 87 of *Cambridge Tracts in Mathematics.* Cambridge University Press, Cambridge, 1986.

[87] R. J. Stroeker and R. Tijdeman, Diophantine equations. In *Computational methods in number theory, Part II*, Mathematical Centre Tracts, Vol. 155, pages 321–369. Math. Centrum, Amsterdam, 1982.

[88] A. Thue, Über Annäherungswerte algebraischer Zahlen. *J. Reine Angew. Math.* **135** (1909) 284–305.

[89] R. Tijdeman, On the equation of Catalan. *Acta Arith.* **29** (1976) 197–209.

[90] B. M. M. de Weger, Solving exponential Diophantine equations using lattice basis reduction algorithms. *J. Number Theory.* **26** (1987) 325–367. Erratum **31** (1989) 88–89.

[91] B. M. M. de Weger, *Algorithms for diophantine equations.* CWI Tract 65. 1989.

[92] G. Wüstholz, A new approach to Baker's theorem on linear forms in logarithms I, II. *In: Diophantine Approximation and Transcendence Theory*, ed. G. Wüstholz, Lecture Notes in Mathematics 1290, Berlin: Springer (1987) 189–202, 203–211.

[93] G. Wüstholz, A new approach to Baker's theorem on linear forms in logarithms III. *In: New advances in transcendence theory (Durham, 1986)*, 399–410. Cambridge Univ. Press, Cambridge (1988).

[94] G. Wüstholz, Algebraische Punkte auf analytischen Untergruppen algebraischer Gruppen. *Ann. of Math. (2)* **129**(3) (1989) 501–517.

[95] G. Wüstholz, Multiplicity estimates on group varieties, *Ann. Math.* **129** (1989) 471–500.

[96] G. Wüstholz, editor. *A Panorama of Number Theory or The View from Baker's Garden.* Cambridge University Press. 2002.

[97] Kunrui Yu, Linear forms in p-adic logarithms, *Acta Arith.* **53**(2) (1989) 107–186.

[98] Kunrui Yu, Linear forms in p-adic logarithms II, *Compositio Mathematica* **74**(1) (1990) 15–113.

[99] Kunrui Yu, Linear forms in p-adic logarithms III, *Compositio Mathematica* **91**(3) (1994) 241–276.

[100] Kunrui Yu, p-adic logarithmic forms and group varieties I, *J. Reine Angew. Math.* **502** (1998) 29–92.

[101] Kunrui Yu, p-adic logarithmic forms and group varieties II, *Acta Arith.* **89** (1999) 337–378.

[102] Kunrui Yu, p-adic logarithmic forms and group varieties III, *Forum Math.* **19** (2007) 187–280.

[103] Kunrui Yu, p-adic logarithmic forms and a problem of Erdős, *Acta Math.* **211**(2) (2013) 315–382.