# Linear Forms in Logarithms

**Sanda Bujačić and Alan Filipin**

**2000 Mathematics Subject Classification** 11J13 · 11J81 · 11J86 · 11K60

## Introduction

These lecture notes cover the course *Linear Forms in Logarithms* created for the Summer School *Diophantine Analysis* organized in Würzburg, Germany in 2014. The notes intend to be an introduction to Diophantine approximation and linear forms in logarithms.

We begin with the theory of Diophantine approximation which has an extremely important application in the study of Diophantine equations. One of the main topics is the question how well a given real number $\alpha$ can be approximated by rational numbers. By placing certain constraints on the rational numbers used in the approximation, we are able to classify the real number $\alpha$ as either a *rational* or an *irrational* number, or as an *algebraic* or a *transcendental* number. Diophantine approximation and transcendence theory are very close areas that share many theorems and methods which will be useful in the second part of these lecture notes.

There, we introduce linear forms in logarithms and provide lower bounds for linear forms in logarithms of algebraic numbers due to Alan Baker, one of the most famous mathematician in this field of mathematics. Baker was awarded the Fields Medal in 1970 because of his profound and significant contributions to number theory. To

S. Bujačić (✉)
Department of Mathematics, University of Rijeka, Radmile Matejčić 2,
51 000 Rijeka, Croatia
e-mail: sbujacic@math.uniri.hr

A. Filipin
Faculty of Civil Engineering, University of Zagreb, Fra Andrije Kačića-Miošića 26,
10 000 Zagreb, Croatia
e-mail: filipin@grad.hr



J. Steuding (ed.), *Diophantine Analysis*, Trends in Mathematics,
DOI 10.1007/978-3-319-48817-2_1

illustrate the importance of his machinery, many useful and interesting applications of the introduced concepts are presented.

# 1 Diophantine Approximation

Rational numbers are in every interval of the real line, no matter how small that interval is because the set of rational numbers is *dense* in the set of real numbers. As a consequence, for any given real number $\alpha$, we are able to find a rational number as close as we like to $\alpha$.

Approximating a real number by rational numbers helps us to better understand the set of real numbers and gives us a surprising insight in the properties of real numbers. By placing certain constraints on the rational numbers used in the approximation of the real number $\alpha$, properties of the real number $\alpha$ can be observed such that classify it as either a *rational* or an *irrational* number, or as an *algebraic* or a *transcendental* number.

As rational numbers approach a fixed real number, their denominators grow arbitrarily large. We study how closely real numbers can be approximated by rational numbers that have a fixed bound on the growth of their denominators.

## *1.1 Dirichlet's Theorem*

One of the main questions in Diophantine approximation is whether there exists *any* rational number $\frac{p}{q}$ satisfying the inequality

$$\left|\frac{a}{b}-\frac{p}{q}\right|<\frac{1}{q^2}.$$

The affirmative answer follows from the fundamental result due to Dirichlet[1] on rational approximation of real numbers.

**Theorem 1.1.1** (Dirichlet 1842) *Let $\alpha$ be a real number and $n$ a positive integer. There exists a rational number $\frac{p}{q}$, $0<q\leq n$, satisfying the inequality*

$$\left|\alpha-\frac{p}{q}\right|\leq\frac{1}{(n+1)q}. \tag{1.1}$$

*Proof* For $n=1$, $\frac{p}{q}=\frac{\lfloor\alpha\rfloor}{1}$ or $\frac{p}{q}=\frac{\lfloor\alpha\rfloor+1}{1}$ satisfies

[1] Peter Gustav Lejeune Dirichlet (1805–1859), a German mathematician.

$$\left|\alpha - \frac{p}{q}\right| \leq \frac{1}{2},$$

where $\lfloor\ \rfloor$ stands for floor function. For $n \geq 2$, we consider $n+2$ elements

$$0,\ \alpha - \lfloor\alpha\rfloor,\ 2\alpha - \lfloor 2\alpha\rfloor,\ \ldots,\ n\alpha - \lfloor n\alpha\rfloor,\ 1,$$

of the interval $[0, 1]$.

Assume first that these elements are distinct as they are in the case $\alpha$ is an irrational number. The interval $[0, 1]$ can be subdivided into $n+1$ subintervals of the length $\frac{1}{n+1}$ and the pigeonhole principle guarantees that two of these numbers differ in absolute value by at most $\frac{1}{n+1}$. If one of the numbers is 0 and the other is $i\alpha - \lfloor i\alpha\rfloor$, then $i \leq n$, $|i\alpha - \lfloor i\alpha\rfloor| < \frac{1}{n+1}$ and

$$\left|\alpha - \frac{\lfloor i\alpha\rfloor}{i}\right| \leq \frac{1}{(n+1)i}.$$

After $\frac{\lfloor i\alpha\rfloor}{i}$ is reduced to lowest terms $\frac{p}{q}$, the rational number $\frac{p}{q}$ satisfies (1.1). Similarly, if the two numbers in question are $j\alpha - \lfloor j\alpha\rfloor$ and 1, then $j \leq n$ and reducing $\frac{\lfloor j\alpha\rfloor+1}{j}$ to lowest terms $\frac{p}{q}$, we have that $\frac{p}{q}$ satisfies (1.1). Finally, if the two numbers are $i\alpha - \lfloor i\alpha\rfloor$ and $j\alpha - \lfloor j\alpha\rfloor$ with $i < j$, then

$$|j\alpha - \lfloor j\alpha\rfloor - (i\alpha - \lfloor i\alpha\rfloor)| = |(j-i)\alpha - (\lfloor j\alpha\rfloor - \lfloor i\alpha\rfloor)| \leq \frac{1}{n+1}.$$

Consequently, $j - i < n$ and

$$\left|\alpha - \frac{\lfloor j\alpha\rfloor - \lfloor i\alpha\rfloor}{j-i}\right| \leq \frac{1}{(n+1)(j-i)}.$$

Thus, after $\frac{\lfloor j\alpha\rfloor - \lfloor i\alpha\rfloor}{j-i}$ is reduced to lowest terms $\frac{p}{q}$, the rational number $\frac{p}{q}$ satisfies (1.1).

If the $n+2$ numbers from the beginning are not distinct, then $\alpha$ itself is a rational number with denominator at most $n$. In this case, there exist $i < j$ so that $\alpha$ is equal to one of the following fractions

$$\frac{\lfloor i\alpha\rfloor}{i},\ \frac{\lfloor j\alpha\rfloor - \lfloor i\alpha\rfloor}{j-i}$$

reduced to lowest terms. If the numbers are not distinct, the required inequality (1.1) is trivially satisfied by $\alpha$ itself.

**Corollary 1.1.2** *For $\alpha$ irrational, there exist infinitely many relatively prime numbers $p, q$ such that*

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{q^2}. \tag{1.2}$$

*Proof* Suppose there are only finitely many rationals

$$\frac{p_1}{q_1}, \frac{p_2}{q_2}, \ldots, \frac{p_k}{q_k}$$

satisfying (1.2). In this case,

$$\left|\alpha - \frac{p_i}{q_i}\right| > 0$$

for $1 \leq i \leq k$. Consequently, since $\alpha$ is irrational, there exists a positive integer $n$ such that the inequality

$$\left|\alpha - \frac{p_i}{q_i}\right| > \frac{1}{n+1}$$

holds for $1 \leq i \leq k$. However, this contradicts Dirichlet's Theorem 1.1.1 which asserts that, for this $n$, there exists a rational number $\frac{p}{q}$ with $q \leq n$ such that

$$\left|\alpha - \frac{p}{q}\right| \leq \frac{1}{(n+1)q} < \frac{1}{q^2}.$$

*Remark 1.1.3* Corollary 1.1.2 does not hold for $\alpha$ rational. Assume $\alpha = \frac{u}{v}$. For $\frac{p}{q} \neq \alpha$, we have

$$\left|\alpha - \frac{p}{q}\right| = \left|\frac{u}{v} - \frac{p}{q}\right| \geq \frac{1}{vq},$$

so (1.1) implies $q < v$, hence the inequality (1.1) can be satisfied only for finitely many relatively prime integers $p, q$.

**Corollary 1.1.4** *A real number $\alpha$ is irrational if and only if there are infinitely many rational numbers $\frac{p}{q}$ such that*

$$\left|\alpha - \frac{p}{q}\right| \leq \frac{1}{q^2}.$$

A proof can be found in [44]. It appears that irrational numbers can be distinguished from rational numbers by the fact that they can be approximated by infinitely many rational numbers $\frac{p}{q}$ with an error less than $\frac{1}{q^2}$.

We may ask for the best possible value $C > 0$ such that the statement of the Corollary 1.1.4 holds with $\frac{1}{Cq^2}$ in place of $\frac{1}{q^2}$? The answer will be given in Hurwitz's[2] Theorem 1.3.5 which characterizes the best Dirichlet-type inequality.

[2] Adolf Hurwitz (1859–1919), a German mathematician.

## 1.2 Continued Fractions

**Definition 1.2.1** • An *infinite generalized continued fraction* is an expression of the form

$$a_0 + \cfrac{b_1}{a_1 + \cfrac{b_2}{a_2 + \cfrac{b_3}{\ddots}}}, \tag{1.3}$$

where $a_0, a_1, a_2, \ldots$ and $b_1, b_2, \ldots$ are either rational, real or complex numbers or functions of such variables.

- For $b_i = 1,\ i \in \mathbb{N}$, (1.3) is called an *infinite simple continued fraction*. Its abbreviated notation is

$$[a_0, a_1, a_2, \ldots].$$

- An expression

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

is called a *finite simple continued fraction* with $a_i \geq 1,\ i = 1, \ldots, n$ and $a_n \geq 2$ integers that are called *partial quotients*. The rational numbers

$$\frac{p_0}{q_0} = [a_0],\ \frac{p_1}{q_1} = [a_0, a_1],\ \frac{p_2}{q_2} = [a_0, a_1, a_2],\ \ldots,\ \frac{p_n}{q_n} = [a_0, a_1, a_2, \ldots, a_n]$$

are called the *convergents* of $\frac{p}{q}$ and $n$ is its *length*.

*Remark 1.2.2* We set $p_{-2} := 0,\ p_{-1} := 1,\ q_{-2} := 1,\ q_{-1} = 0$.

**Lemma 1.2.3** (Law of formation of the convergents) *For $n \geq 0$,*

$$p_n = a_n p_{n-1} + p_{n-2},\ \ q_n = a_n q_{n-1} + q_{n-2}. \tag{1.4}$$

*Proof* The equalities (1.4) are satisfied for $n = 0$. We assume that (1.4) is satisfied for $n - 1$, i.e.,

$$p_{n-1} = a_{n-1} p_{n-2} + p_{n-3},\ \ q_{n-1} = a_{n-1} q_{n-2} + q_{n-3}.$$

Then we get

$$\begin{aligned}\frac{p_n}{q_n} &= [a_0, a_1, \ldots, a_{n-1} + 1/a_n] \\ &= \frac{(a_{n-1} + \frac{1}{a_n})p_{n-1} + p_{n-2}}{(a_{n-1} + \frac{1}{a_n})q_{n-1} + q_{n-2}} \\ &= \frac{(a_n a_{n-1} + 1)p_{n-2} + a_n p_{n-1}}{(a_n a_{n-1} + 1)q_{n-2} + a_n q_{n-1}} = \frac{a_n p_{n-1} + p_{n-2}}{a_n q_{n-1} + q_{n-2}}.\end{aligned}$$

**Lemma 1.2.4** *For $n \geq -1$,*

$$q_n p_{n-1} - p_n q_{n-1} = (-1)^n. \tag{1.5}$$

*Proof* Let $n = -1$. We observe that $q_{-1}p_{-2} - p_{-1}q_{-2} = (-1)^{-1}$. We assume that (1.5) is satisfied for $n - 1$. Using Lemma 1.2.3, we find

$$\begin{aligned}q_n p_{n-1} - p_n q_{n-1} &= (a_n q_{n-1} + q_{n-2})p_{n-1} - (a_n p_{n-1} + p_{n-2})q_{n-1} = \\ &= -(q_{n-1}p_{n-2} - p_{n-1}q_{n-2}) = (-1)^n.\end{aligned}$$

**Lemma 1.2.5** *For $n \geq 0$,*

$$q_n p_{n-2} - p_n q_{n-2} = (-1)^{n-1} a_n.$$

*Proof* It follows from Lemmas 1.2.3 and 1.2.4 that

$$\begin{aligned}q_n p_{n-2} - p_n q_{n-2} &= (a_n q_{n-1} + q_{n-2})p_{n-2} - (a_n p_{n-1} + p_{n-2})q_{n-2} = \\ &= a_n(q_{n-1}p_{n-2} - p_{n-1}q_{n-2}) = (-1)^{n-1}a_n.\end{aligned}$$

**Theorem 1.2.6** *The convergents $\frac{p_k}{q_k}$ satisfy the following inequalities:*

*(i)* $\frac{p_0}{q_0} < \frac{p_2}{q_2} < \frac{p_4}{q_4} < \ldots,$
*(ii)* $\frac{p_1}{q_1} > \frac{p_3}{q_3} > \frac{p_5}{q_5} > \ldots,$
*(iii) for $n$ even and $m$ odd,*

$$\frac{p_n}{q_n} < \frac{p_m}{q_m}.$$

*Proof* Using Lemma 1.2.5, we find

$$\frac{p_{n-2}}{q_{n-2}} - \frac{p_n}{q_n} = \frac{(-1)^{n-1}a_n}{q_{n-2}q_n}.$$

For $n \geq 2$ and $n$ even, we obtain $\frac{p_{n-2}}{q_{n-2}} < \frac{p_n}{q_n}$, while $\frac{p_{n-2}}{q_{n-2}} > \frac{p_n}{q_n}$, for $n \geq 3$ and $n$ odd.

It remains to prove the last inequality. Let $n < m$. Since $\frac{p_n}{q_n} \leq \frac{p_{m-1}}{q_{m-1}}$, it is sufficient to prove $\frac{p_{m-1}}{q_{m-1}} < \frac{p_m}{q_m}$, which is satisfied by Lemma 1.2.4,

$$q_m p_{m-1} - p_m q_{m-1} = (-1)^m = -1 < 0.$$

The proof for $n > m$ follows analogously.

**Lemma 1.2.7** *For an integer $a_0$ and positive integers $a_1, a_2, \ldots, a_n$, the continued fraction $[a_0, a_1, \ldots, a_n]$ is rational. Conversely, for every rational number $\frac{u}{v}$ there exist $n \geq 0$, an integer $a_0$ and positive integers $a_1, a_2, \ldots, a_n$ such that*

$$\frac{u}{v} = [a_0, a_1, \ldots, a_n].$$

*For $\frac{u}{v} \geq 1$, we have $a_0 \geq 1$.*

*Proof* Using Lemma 1.2.3, we find

$$[a_0, a_1, \ldots, a_n] = [a_0, a_1, \ldots, a_{k-1}, [a_k, a_{k+1}, \ldots, a_n]] = \frac{p_{k-1} r_k + p_{k-2}}{q_{k-1} r_k + q_{k-2}},$$

where $r_k := [a_k, a_{k+1}, \ldots, a_n]$.

Conversely, let $v > 0$ and $\gcd(u, v) = 1$. For $v = 1$, clearly $\frac{u}{v} \in \mathbb{Z}$, hence, setting $a_0 = \frac{u}{v}$, we obtain $\frac{u}{v} = [a_0]$.

If $v > 1$, then there exist $q, r \in \mathbb{Z}$ such that $u = vq + r,\ 1 \leq r < v$. We assume $\frac{v}{r} = [a_1, \ldots, a_n]$. Since $\frac{v}{r} > 1$, we conclude that $a_1, \ldots, a_n \in \mathbb{N}$. Hence,

$$\frac{u}{v} = q + \frac{1}{\frac{v}{r}} = q + \frac{1}{[a_1, \ldots, a_n]} = [q, a_1, \ldots, a_n],$$

where $a_0 = q$. Clearly, if $\frac{u}{v} \geq 1$, then $a_0 = q \geq 1$.

*Remark 1.2.8* There is a one-to-one correspondence between rational numbers and finite simple continued fractions.

*Remark 1.2.9* Let $\frac{u}{v}$ be rational, $\gcd(u, v) = 1$ and $u > v > 0$. It follows from Euclid's algorithm that

$$u = vq_1 + r_1,\ v = r_1 q_2 + r_2,\ \ldots,\ r_{j-1} = r_j q_{j+1},$$

hence

$$\frac{u}{v} = q_1 + \frac{1}{\frac{c}{r_1}} = q_1 + \frac{1}{q_2 + \frac{1}{\frac{r_1}{r_2}}} = \cdots = [q_1, q_2, \ldots, q_{j+1}].$$

*Example 1.2.10*

$$\frac{7}{11} = 0 + \frac{1}{\frac{11}{7}} = 0 + \frac{1}{1 + \frac{4}{7}} = 0 + \frac{1}{1 + \frac{1}{\frac{7}{4}}} =$$

$$= 0 + \frac{1}{1 + \frac{1}{1 + \frac{3}{4}}} = 0 + \frac{1}{1 + \frac{1}{1 + \frac{1}{\frac{4}{3}}}} = 0 + \frac{1}{1 + \frac{1}{1 + \frac{1}{1 + \frac{1}{3}}}},$$

which can be written as

$$\frac{7}{11} = [0, 1, 1, 1, 3].$$

*Example 1.2.11* The number $e$ is irrational.
The proof goes as follows: if we assume that $e$ is rational, then it can be represented as

$$e = \sum_{i=0}^{\infty} \frac{1}{i!} = \frac{u}{v}.$$

Let $n$ be an integer such that $n > v$. We define $\frac{p}{q} = \sum_{i=0}^{n} \frac{1}{i!}$, with $q = n!$. Using Remark 1.2.9, we get

$$\frac{1}{v} \leq q \left| e - \frac{p}{q} \right| = n! \sum_{j=1}^{\infty} \frac{1}{(n+j)!}$$

$$< n! \sum_{k=0}^{\infty} \frac{1}{(n+1)!} \frac{1}{(n+1)^k} \leq \frac{1}{n+1} \frac{1}{1 - \frac{1}{n+1}} = \frac{1}{n},$$

a contradiction to $n > v$.

**Lemma 1.2.12** *For every integer $r$, there exist exactly two different simple continued fraction expansions representing $r$, namely $r = [r]$ and $r = [r-1, 1]$. For $r$ rational, there exist exactly two different simple continued fraction expansions representing $r$, namely $[a_0, a_1, \ldots, a_n]$ with $a_n \geq 2$ and $[a_0, a_1, \ldots, a_{n-1}, a_n - 1, 1]$.*

*Proof* Every $r \in \mathbb{Q}$ can be represented as a finite simple continued fraction, namely

$$r = [a_0, a_1, \ldots, a_n], \quad a_0 \in \mathbb{Z}, \quad a_1, a_2, \ldots, a_n \in \mathbb{N}.$$

If $r \in \mathbb{Z}$, then $n = 0$ and $r = [a_0] = a_0$, resp. $r = [r]$. Otherwise, when $n > 0$, then

$$r = a_0 + \frac{1}{[a_1, \dots, a_n]},$$

with $[a_1, \dots, a_n] \geq 1$. In view of $r - a_0 \in \mathbb{Z}$, we conclude that $[a_1, \dots, a_n] = 1$. Since $a_1 \geq 1$, we get $a_1 = 1, n = 1$, so $a_0 = r - 1$ and $r = [r - 1, 1]$.

Now consider $r = \frac{u}{v}$, $\gcd(u, v) = 1$, $v > 0$. We use induction on $v$ in order to prove the second claim. The case when $v = 1$ has already been considered. If $v > 1$, we get $\frac{u}{v} = a_0 + \frac{u_1}{v}$, where $u_1 < v$. Let $\alpha_1 := \frac{u_1}{v}$. Using the hypothesis of the induction, we conclude that $\alpha_1$ has two continued fraction expansions $[a_1, a_2, \dots, a_{n-1}, a_n]$, $a_n \geq 2$ and $[a_1, a_2, \dots, a_n - 1, 1]$.

**Lemma 1.2.13** *Let $a_0$ be an integer and $a_1, a_2, \dots,$ be positive integers. Then, the limit $\lim_{n\to\infty} \frac{p_n}{q_n}$ exists and its value is irrational. Conversely, for $\alpha$ irrational, there exist a unique integer $a_0$ and unique positive integers $a_1, a_2, \dots$ such that $\alpha = \lim_{n\to\infty} \frac{p_n}{q_n}$.*

*Proof* In view of $\frac{p_0}{q_0} < \frac{p_2}{q_2} < \cdots < \frac{p_1}{q_1}$, it is clear that both limits

$$\lim_{\substack{n\to\infty \\ n \text{ even}}} \frac{p_n}{q_n} \quad \text{and} \quad \lim_{\substack{n\to\infty \\ n \text{ odd}}} \frac{p_n}{q_n}$$

exist, and it is easily shown that both limits are equal. We put $\alpha = \lim_{n\to\infty} \frac{p_n}{q_n}$ and compute

$$\left|\alpha - \frac{p_n}{q_n}\right| < \left|\frac{p_{n+1}}{q_{n+1}} - \frac{p_n}{q_n}\right| = \frac{1}{q_n q_{n+1}} < \frac{1}{q_n^2}.$$

Since $p_n, q_n$ are relatively prime, there exist infinitely many rational numbers $\frac{p}{q}$ such that $|\alpha - \frac{p}{q}| < \frac{1}{q^2}$, so $\alpha$ is irrational.

Conversely, let $\alpha$ be irrational, $a_0 = \lfloor \alpha \rfloor$, and let $\alpha_1 := a_0 + \frac{1}{\alpha_1}$. We notice that $\alpha_1 > 1$ is irrational. For $k \geq 1$ let $a_k = \lfloor \alpha_k \rfloor$ and $\alpha_k = a_k + \frac{1}{\alpha_{k+1}}$. We observe that $a_k \geq 1$, $\alpha_{k+1} > 1$, and $\alpha_{k+1}$ is irrational. Our goal is to show

$$\alpha = [a_0, a_1, a_2, \dots].$$

Using Lemmas 1.2.3 and 1.2.4 with $\alpha = [a_0, a_1, \dots, \alpha_{n+1}]$, we find

$$\begin{aligned} q_n\alpha - p_n &= q_n \frac{\alpha_{n+1}p_n + p_{n-1}}{\alpha_{n+1}q_n + q_{n-1}} - p_n \\ &= \frac{q_n(\alpha_{n+1}p_n + p_{n-1}) - p_n(\alpha_{n+1}q_n + q_{n-1})}{\alpha_{n+1}q_n + q_{n-1}} = \frac{(-1)^n}{\alpha_{n+1}q_n + q_{n-1}}. \end{aligned}$$

Hence,

$$\left|\alpha - \frac{p_n}{q_n}\right| < \frac{1}{q_n^2}, \tag{1.6}$$

which implies $\lim_{n\to\infty} \frac{p_n}{q_n} = \alpha$. Finally, it remains to prove that the integers $a_0, a_1 \geq 1, a_2 \geq 1, \ldots$ are uniquely determined. In view of

$$\alpha = [a_0, a_1, a_2, \ldots] = a_0 + \frac{1}{[a_1, a_2, \ldots]},$$

and $0 \leq \alpha - a_0 < 1$, we find $a_0 = \lfloor \alpha \rfloor$ which implies that $a_0$ is unique and $\alpha_1 = [a_1, a_2, \ldots]$ is uniquely determined by $\alpha$. Because $a_1 = \lfloor \alpha_1 \rfloor$, $a_1$ is unique, etc. This proves the lemma.

## 1.3 Hurwitz's Theorem

In the sequel we assume $\alpha$ to be irrational. According to (1.6), we conclude that each convergent of $\alpha$ satisfies the inequality

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

Vahlen[3] and Borel[4] have proved the following theorems that deal with approximation properties of two and three consecutive convergents, respectively.

**Theorem 1.3.1** (Vahlen 1895, [48]) *Let $\alpha$ be an irrational number and denote by $\frac{p_{n-1}}{q_{n-1}}, \frac{p_n}{q_n}$ two consecutive convergents of $\alpha$. Then, at least one of them satisfies*

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

*Proof* We observe that

$$\left| \alpha - \frac{p_n}{q_n} \right| + \left| \alpha - \frac{p_{n-1}}{q_{n-1}} \right| = \left| \frac{p_n}{q_n} - \frac{p_{n-1}}{q_{n-1}} \right| = \frac{1}{q_n q_{n-1}} < \frac{1}{2q_n^2} + \frac{1}{2q_{n-1}^2}.$$

Thus,

$$\left| \alpha - \frac{p_n}{q_n} \right| < \frac{1}{2q_n^2} \quad \text{or} \quad \left| \alpha - \frac{p_{n-1}}{q_{n-1}} \right| < \frac{1}{2q_{n-1}^2}.$$

**Theorem 1.3.2** (Borel 1903, [9]) *Let $\alpha$ be an irrational number and denote by $\frac{p_{n-1}}{q_{n-1}}, \frac{p_n}{q_n}, \frac{p_{n+1}}{q_{n+1}}$ three consecutive convergents of $\alpha$. Then at least one of them satisfies the inequality*

$$\left| \alpha - \frac{p}{q} \right| < \frac{1}{\sqrt{5}q^2}.$$

[3] Theodor Vahlen (1869–1945), an Austrian mathematician.

[4] Émile Borel (1871–1956), a French mathematician.

*Proof* Let $\alpha = [a_0, a_1, \dots]$, $\alpha_i = [a_i, a_{i+1}, \dots]$, $\beta_i = \frac{q_{i-2}}{q_{i-1}}$, $q \geq 1$. It is not difficult to deduce that

$$\left|\alpha - \frac{p_n}{q_n}\right| = \frac{1}{q_n^2(\alpha_{n+1} + \beta_{n+1})}.$$

We show that there does not exist a positive integer $n$ satisfying

$$\alpha_i + \beta_i < \sqrt{5} \tag{1.7}$$

for $i = n-1, n, n+1$. Our reasoning is indirect. We assume that (1.7) is satisfied for $i = n-1, n$. It follows from

$$\alpha_{n-1} = a_{n-1} + \frac{1}{\alpha_n}, \quad \frac{1}{\beta_n} = \frac{q_{n-1}}{q_{n-2}} = a_{n-1} + \frac{q_{n-3}}{q_{n-2}} = a_{n-1} + \beta_{n-1}$$

that

$$\frac{1}{\alpha_n} + \frac{1}{\beta_n} = \alpha_{n-1} + \beta_{n-1} \leq \sqrt{5}.$$

Hence, $1 = \alpha_n \cdot \frac{1}{\alpha_n} \leq (\sqrt{5} - \beta_n)(\sqrt{5} - \frac{1}{\beta_n})$ or, equivalently, $\beta_n^2 - \sqrt{5}\beta_n + 1 \leq 0$ which implies $\beta_n \geq \frac{\sqrt{5}-1}{2}$. For $\beta_n$ rational, we conclude that $\beta_n > \frac{\sqrt{5}-1}{2}$. Now, if (1.7) is satisfied for $i = n, n+1$, then again $\beta_{n+1} > \frac{\sqrt{5}-1}{2}$, so we deduce

$$1 \leq a_n = \frac{q_n}{q_{n-1}} - \frac{q_{n-2}}{q_{n-1}} = \frac{1}{\beta_{n+1}} - \beta_n < \frac{2}{\sqrt{5}-1} - \frac{\sqrt{5}-1}{2} < 1,$$

the desired contradiction.

Legendre[5] proved with the following important theorem a converse to the previous results.

**Theorem 1.3.3** (Legendre, [32]) *Let $p, q$ be integers such that $q \geq 1$ and*

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

*Then $\frac{p}{q}$ is a convergent of $\alpha$.*

*Proof* Let $\alpha - \frac{p}{q} = \frac{\varepsilon\nu}{q^2}$ with $0 < \nu < \frac{1}{2}$ and $\varepsilon = \pm 1$. In view of Lemma 1.2.12 there exists a simple continued fraction

$$\frac{p}{q} = [b_0, b_1, \dots, b_{n-1}]$$

[5] Adrien-Marie Legendre (1752–1833), a French matheamtician.

satisfying $(-1)^{n-1} = \varepsilon$. We define $\omega$ by

$$\alpha = \frac{\omega p_{n-1} + p_{n-2}}{\omega q_{n-1} + q_{n-2}},$$

such that $\alpha = [b_0, b_1, \ldots, b_{n-1}, \omega]$. Hence,

$$\frac{\varepsilon\nu}{q^2} = \alpha - \frac{p}{q} = \frac{1}{q_{n-1}}(\alpha q_{n-1} - p_{n-1}) = \frac{1}{q_{n-1}} \cdot \frac{(-1)^{n-1}}{\omega q_{n-1} + q_{n-2}},$$

giving $\nu = \frac{q_{n-1}}{\omega q_{n-1}+q_{n-2}}$ and $\omega = \frac{1}{\nu} - \frac{q_{n-2}}{q_{n-1}} > 1$. Next we consider the finite or infinite continued fraction of $\omega$,

$$\omega = [b_n, b_{n+1}, b_{n+2}, \ldots].$$

Since $\omega > 1$, we conclude $b_j \in \mathbb{N}$, $j = n, n+1, n+2, \ldots$. Consequently,

$$\alpha = [b_0, b_1, \ldots, b_{n-1}, b_n, b_{n+1}, \ldots]$$

which is the continued fraction expansion for $\alpha$ and

$$\frac{p}{q} = \frac{p_{n-1}}{q_{n-1}} = [b_0, b_1, \ldots, b_{n-1}]$$

is indeed a convergent to $\alpha$.

**Lemma 1.3.4** *Assume the continued fraction expansion for $\alpha$ is given by*

$$\alpha = [a_0, a_1, \ldots, a_N, 1, 1, \ldots]. \tag{1.8}$$

*Then*

$$\lim_{n\to\infty} q_n^2 \left|\alpha - \frac{p_n}{q_n}\right| = \frac{1}{\sqrt{5}}.$$

A proof can be found in [45].

**Theorem 1.3.5** (Hurwitz, [31]) *Let $\alpha$ be an irrational number.*

*(i) Then there are infinitely many rational numbers $\frac{p}{q}$ such that*

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{\sqrt{5}q^2}.$$

*(ii) If $\sqrt{5}$ is replaced by $C > \sqrt{5}$, then there are irrational numbers $\alpha$ for which statement (i) does not hold.*

*Proof* Claim (i) follows directly from Theorem 1.3.2, while claim (ii) follows from Theorem 1.3.3 and Lemma 1.3.4. Namely, if $\alpha$ is irrational and of the form (1.8),

then according to Theorem 1.3.3, all solutions of $|\alpha - \frac{p}{q}| < \frac{1}{Cq^2}$ with $C > \sqrt{5}$ can be found among the convergents to $\alpha$, however, in view of Lemma 1.3.4 this inequality is satisfied by only finitely many convergents to $\alpha$.

**Definition 1.3.6** An irrational number $\alpha$ is said to be a *quadratic irrational number* if it is the solution of some quadratic equation with rational coefficients.

**Definition 1.3.7** The continued fraction expansion $[a_0, a_1, \dots]$ of a real number $\alpha$ is said to be *eventually periodic* if there exist integers $m \geq 0$ and $h > 0$ such that

$$a_n = a_{n+h}, \quad \text{for all } n \geq m.$$

In this case the continued fraction expansion is denoted by

$$[a_0, a_1, \dots, a_{m-1}, \overline{a_m, a_{m+1}, \dots, a_{m+h-1}}].$$

The continued fraction expansion is said to be *periodic* if it is eventually periodic with $m = 0$.

Euler[6] and Lagrange[7] have proved an important characterization of quadratic irrationals in terms of their continued fraction expansion:

**Theorem 1.3.8** (Euler 1737; Lagrange 1770) *A real number $\alpha$ is quadratic irrational if and only if its continued fraction expansion is eventually periodic.*

A proof can be found in [46].

**Theorem 1.3.9** *Let $d > 1$ be an integer which is not a perfect square. Then the continued fraction expansion of $\sqrt{d}$ is of the form*

$$[a_0, \overline{a_1, \dots, a_{n-1}, 2a_0}]$$

*with $a_0 = \lfloor \sqrt{d} \rfloor$, $a_1 = a_{n-1}$, $a_2 = a_{n-2}$, ....*

A proof can be found in [41].

*Remark 1.3.10* Let $E > 1$ be an integer which is not a perfect square. Let

$$\alpha_0 = \frac{s_0 + \sqrt{E}}{t_0}$$

be a quadratic irrational with $s_0, t_0 \in \mathbb{Z}$, $t_0 \neq 0$ such that $t_0 \mid (E - s_0^2)$. Then the partial quotients $a_i$ are given by the recursion

$$a_i = \lfloor \sqrt{\alpha_i} \rfloor, \quad s_{i+1} = a_i t_i - s_i, \quad t_{i+1} = \frac{E - s_{i+1}^2}{t_i}, \quad \alpha_{i+1} = \left\lfloor \frac{s_{i+1} + \sqrt{E}}{t_{i+1}} \right\rfloor.$$

[6] Leonhard Euler (1707–1783), a Swiss mathematician.

[7] Joseph-Louis Lagrange (1736–1813), an Italian-French mathematician.

*Example 1.3.11* For $d \in \mathbb{N}$,

$$\sqrt{2d(2d-1)} = [2d-1; \overline{2, 4d-2}],$$

$$\sqrt{2d(8d-1)} = [4d-1; \overline{1, 2, 1, 8d-2}].$$

**Definition 1.3.12** An irrational number $\alpha$ is said to be *badly approximable* if there is a real number $c(\alpha) > 0$, depending only on $\alpha$, such that

$$\left|\alpha - \frac{p}{q}\right| > \frac{c(\alpha)}{q^2}$$

for all rational numbers $\frac{p}{q}$.

**Proposition 1.3.13** *If an irrational number $\alpha$ is badly approximable, then for every $\varepsilon > 0$, there are only finitely many rational numbers $\frac{p}{q}$ satisfying*

$$\left|\alpha - \frac{p}{q}\right| \leq \frac{1}{q^{2+\varepsilon}}.$$

*Proof* Let $c(\alpha)$ be a positive real number such that

$$\left|\alpha - \frac{p}{q}\right| > \frac{c(\alpha)}{q^2}$$

for all rational numbers $\frac{p}{q}$. Now suppose that there are infinitely many rational numbers $\frac{p}{q}$ satisfying

$$\left|\alpha - \frac{p}{q}\right| \leq \frac{1}{q^{2+\varepsilon}}.$$

Consequently, there exists a rational number $\frac{p_1}{q_1}$ for which the inequality

$$q_1^{\varepsilon} > \frac{1}{c(\alpha)}$$

holds. It follows that

$$\left|\alpha - \frac{p_1}{q_1}\right| \leq \frac{1}{q_1^2 q_1^{\varepsilon}} < \frac{c(\alpha)}{q_1^2},$$

which is a contradiction.

**Corollary 1.3.14** *For quadratic irrational numbers $\alpha$ and any $\varepsilon > 0$, there are only finitely many rational numbers $\frac{p}{q}$ satisfying*

$$\left|\alpha - \frac{p}{q}\right| \leq \frac{1}{q^{2+\varepsilon}}.$$

A proof can be found in [44]. Hence, the exponent in the upper bound $\frac{1}{q^2}$ in Dirichlet's Theorem 1.1.1 cannot be improved for real quadratic irrational numbers.

More on Diophantine approximation can be found in [13, 19, 20, 44, 45].

## *1.4 Algebraic and Transcendental Numbers*

### 1.4.1 Basic Theorems and Definitions

**Definition 1.4.1** Given fields $F$ and $E$ such that $F \subseteq E$, then $E$ is called an *extension* of $F$, denoted by $F \leq E$ or $E/F$. The dimension of the extension is called the *degree* of the extension and it is abbreviated by $[E : F]$. If $[E : F] = n < \infty$, $E$ is said to be a *finite* extension of $F$.

*Remark 1.4.2* It can be shown that, if $f$ is a nonconstant polynomial over the field $F$, then there is an extension $E$ of the field $F$ and $\alpha \in E$ such that

$$f(\alpha) = 0.$$

Hence, the field extension of the initial field $F$ is often obtained from the field $F$ by adjoining a root $\alpha$ of a nonconstant polynomial $f$ over the field $F$; in this case the minimal field containing $\alpha$ and $F$ is denoted by $F(\alpha)$.

**Definition 1.4.3** A real number $\alpha$ is called *algebraic* over $\mathbb{Q}$ if it is a root of a polynomial equation with coefficients in $\mathbb{Q}$. A real number is said to be *transcendental* if it is not algebraic.

**Definition 1.4.4** The *minimal polynomial* $p$ of an algebraic number $\alpha$ over $\mathbb{Q}$ is the uniquely determined irreducible monic polynomial of minimal degree with rational coefficients satisfying

$$p(\alpha) = 0.$$

Elements that are algebraic over $\mathbb{Q}$ and have the same minimal polynomial are called *conjugates* over $\mathbb{Q}$.

**Definition 1.4.5** Let $\alpha$ be an algebraic number. Then the degree of $\alpha$ is the degree of the minimal polynomial of $\alpha$ over $\mathbb{Q}$.

*Remark 1.4.6* If

$$X^d + r_{d-1}X^{d-1} + \cdots + r_1X + r_0$$

is the minimal polynomial of an algebraic number $\alpha$ over $\mathbb{Q}$, then multiplication by the least common multiple of the denominators of the coefficients $r_i$, $i = 0, \ldots,$

$d-1$, produces a unique polynomial $P$ with $P(\alpha)=0$ having the form

$$P(X)=a_dX^d+a_{d-1}X^{d-1}+\cdots+a_1X+a_0,$$

where the coefficients $a_i,\ i=0,\ldots,d$, are relatively prime integers and $a_d>0$. We will call this polynomial the *minimal polynomial of* $\alpha$ over $\mathbb{Z}$.

*Example 1.4.7* A real number is rational if and only if it is an algebraic number of degree 1.

*Example 1.4.8* We shall show that

$$x=\frac{10^{\frac{2}{3}}-1}{\sqrt{-3}}$$

is an algebraic number.

To see that, we write $\sqrt{-3}x+1=10^{2/3}$ and get $(\sqrt{-3}x+1)^3=100$. Expanding the left-hand side, it follows that

$$3\sqrt{-3}x^3+9x^2-3\sqrt{-3}x+99=0.$$

Dividing by $3\sqrt{-3}$, we get

$$x^3-\sqrt{-3}x^2-x-11\sqrt{-3}=0.$$

From this we deduce the minimal polynomial of $x$ as

$$\begin{aligned}P(x)&=\Big((x^3-x)-\sqrt{-3}(x^2+11)\Big)\Big((x^3-x)+\sqrt{-3}(x^2+11)\Big)=\\&=x^6+x^4+67x^2+363.\end{aligned}$$

### 1.4.2 Liouville's Theorem

The main task in Diophantine approximation is to figure out how well a real number $\alpha$ can be approximated by rational numbers. In view of this problem, as we have mentioned earlier, a rational number $\frac{p}{q}$ is considered to be a "good" approximation of a real number $\alpha$ if the absolute value of the difference between $\frac{p}{q}$ and $\alpha$ may not decrease when $\frac{p}{q}$ is replaced by another rational number with a *smaller* denominator. This problem was solved during the 18th century by means of continued fractions.

Knowing the "best" approximation of a given number, the main problem is to find sharp upper and lower bounds of the mentioned difference, expressed as a function of the denominator.

It appears that these bounds depend on the nature of the real numbers to be approximated: the lower bound for the approximation of a rational number by another

rational number is larger than the lower bound for algebraic numbers, which is itself larger than the lower bound for all real numbers. Thus, a real number that may be better approximated than an algebraic number is certainly a *transcendental number*. This statement had been proved by Liouville[8] in 1844, and it produced the first explicit transcendental numbers. The later proofs on the transcendency of $\pi$ and $e$ were obtained by a similar idea.

**Theorem 1.4.9** (Liouville 1844) *Let $\alpha$ be a real algebraic number of degree $d \geq 2$. Then there exists a constant $c(\alpha) > 0$, depending only on $\alpha$, such that*

$$\left|\alpha - \frac{p}{q}\right| \geq \frac{c(\alpha)}{q^d}$$

*for all rational numbers $\frac{p}{q}$.*

There are a few ways of proving Liouville's Theorem 1.4.9: one can be found in [12]; a second, and maybe the most familiar one, uses the mean value theorem, an interesting variant concerning the constant $c(\alpha)$ is given in [45].

**Corollary 1.4.10** *Let $\alpha$ be a real algebraic number of degree $d \geq 2$. For every $\delta > 0$, there are only finitely many rational numbers $\frac{p}{q}$ satisfying the inequality*

$$\left|\alpha - \frac{p}{q}\right| \leq \frac{1}{q^{d+\delta}}.$$

A proof can be found in [44].

We observe that the denominators of rational numbers which are getting closer and closer to a fixed real number $\alpha$ grow *arbitrarily large*. Liouville's Theorem 1.4.9 proves that this is indeed the case for real algebraic numbers $\alpha$. For example, Liouville's Theorem 1.4.9 implies that, if $\frac{p}{q}$ is within a distance $\frac{1}{10^{10}}$ of $\alpha$, then

$$q^d \geq 10^{10} c(\alpha).$$

*Remark 1.4.11* Consider the rational numbers $\frac{p}{q}$ and $\frac{p'}{q'}$ satisfying

$$q\left|\alpha - \frac{p}{q}\right| < q'\left|\alpha - \frac{p'}{q'}\right|.$$

The theory of continued fractions provides an efficient algorithm for constructing the best approximations to $\alpha$ in this case.

Liouville's Theorem 1.4.9 can be used to find transcendental numbers explicitly. His construction of transcendental numbers (1844) predates Cantor's[9] proof (1874) of their existence.

[8] Joseph Liouville (1809–1882), a French mathematician.

[9] Georg Ferdinand Ludwig Philipp Cantor (1845–1918), a German mathematician.

*Example 1.4.12* Let

$$\alpha = \sum_{n=1}^{\infty} \frac{1}{10^{n!}} = 0.11000100000000000000000001000....$$

The digit 1 appears in the 1st, 2nd, 6th, 24th, ..., $(n!)$th,... decimal place. For $k \geq 1$, let $q(k) = 10^{k!}$ and $p(k) = 10^{k!} \sum_{n=1}^{k} \frac{1}{10^{n!}}$. We notice that $p(k)$ and $q(k)$ are relatively prime integers, $\frac{p_k}{q_k} = \sum_{n=1}^{k} \frac{1}{10^{n!}}$ and

$$\left| \alpha - \frac{p(k)}{q(k)} \right| = \sum_{n=k+1}^{\infty} \frac{1}{10^{n!}}.$$

Comparing with a geometric series, we find

$$\sum_{n=k+1}^{\infty} \frac{1}{10^{n!}} < \frac{1}{10^{(k+1)!}} \sum_{n=0}^{\infty} \frac{1}{10^{n}} = \frac{10}{9} \frac{1}{q(k)^{k+1}},$$

and

$$\left| \alpha - \frac{p(k)}{q(k)} \right| < \frac{\frac{10}{9}}{q(k)^{k+1}}.$$

Finally, we observe that $\alpha$ does not satisfy Liouville's Theorem 1.4.9. It follows from the calculations above that for any $c > 0$ and any $d > 0$, selecting $k$ such that $\frac{10}{9} < c \cdot q(k)^{k+1-d}$, leads to

$$\left| \alpha - \frac{p(k)}{q(k)} \right| < \frac{c}{q(k)^{d}}$$

for large $k$. Thus, $\alpha$ must be a transcendental number.

In 1873, Charles Hermite[10] proved that $e$ is transcendental and nine years later Ferdinand von Lindemann[11] proved the transcendence of $\pi$. Hermite even showed that $e^a$ is transcendental when $a$ is algebraic and nonzero. This approach was generalized by Weierstrass[12] to the Lindemann-Weierstrass theorem.

**Theorem 1.4.13** (Hermite) *$e$ is transcendental.*

A proof can be found in [4, 28].

[10] Charles Hermite (1822–1901), a French mathematician.

[11] Ferdinand von Lindemann (1852–1939), a German mathematician.

[12] Karl Weierstrass (1815–1897), a German mathematician.

**Theorem 1.4.14** (Lindemann) *$\pi$ is transcendental.*

A proof can be found in [34].

**Theorem 1.4.15** (Lindemann, Weierstrass) *Let $\beta_1, \ldots, \beta_n$ be nonzero algebraic numbers and $\alpha_1, \ldots, \alpha_n$ distinct algebraic numbers. Then*

$$\beta_1 e^{\alpha_1} + \cdots + \beta_n e^{\alpha_n} \neq 0.$$

A proof can be found in [4].

**Corollary 1.4.16** *If $\alpha$ is a nonzero algebraic integer, then*

$$e^{\alpha}, \ \sin\alpha, \ \cos\alpha$$

*are transcendental numbers.*

**Definition 1.4.17** A real number $\alpha$ is a *Liouville number* if for every positive integer $n$, there exist integers $p, q$ with $q > 1$ such that

$$0 < \left|\alpha - \frac{p}{q}\right| < \frac{1}{q^n}.$$

*Remark 1.4.18* It is known that $\pi$ and $e$ are not Liouville numbers (see [37, 41], respectively). Mahler [38] found conditions on the expansion of a real number $\alpha$ in base $g$ that imply that $\alpha$ is transcendental but not a Liouville number. One such example is the decimal number called Champernowne's constant (Mahler's number).

**Theorem 1.4.19** *All Liouville numbers are transcendental.*

A proof can be found in [46].

*Example 1.4.20* We show that

$$\alpha = \sum_{j=0}^{\infty} \frac{1}{2^{j!}}$$

is a Liouville number.

First, we observe that the binary expansion of $\alpha$ has arbitrarily long strings of 0's, so it cannot be rational. Fix a positive integer $n$ and consider $\frac{p}{q} = \sum_{j=0}^{n} \frac{1}{2^{j!}}$ with $p$ and $q = 2^{j!} > 1$ integers. Then

$$0 < \left|\alpha - \frac{p}{q}\right| = \sum_{j=n+1}^{\infty} \frac{1}{2^{j!}} < \sum_{j=(n+1)!}^{\infty} \frac{1}{2^{j!}} = \frac{1}{2^{(n+1)!-1}} \leq \frac{1}{2^{n(n!)}} = \frac{1}{q^n},$$

which proves that $\alpha$ is indeed a Liouville number.

### 1.4.3 Roth's Theorem

It is natural to ask for stronger versions of Liouville's Theorem 1.4.9. First improvements were made by Thue,[13] Siegel[14] and Dyson.[15] In 1955, K.F. Roth[16] proved the most far-reaching extension, now known as the Thue-Siegel-Roth theorem, but also just as Roth's theorem, for which he was awarded a Fields Medal in 1958. We quote from Roth's paper [43].

**Theorem 1.4.21** (Roth 1955) *Let $\alpha$ be a real algebraic number of degree $d \geq 2$. Then, for every $\delta > 0$, the inequality*

$$\left|\alpha - \frac{p}{q}\right| \leq \frac{1}{q^{2+\delta}}$$

*has only finitely many rational solutions $\frac{p}{q}$.*

A complete proof of Roth's Theorem 1.4.21 can be found in [45], and for a generalized version we refer to [30].

**Corollary 1.4.22** *Let $\alpha$ be an algebraic number of degree $d \geq 2$. Then, for every $\delta > 0$, there is a constant $c(\alpha, \delta) > 0$ such that*

$$\left|\alpha - \frac{p}{q}\right| \geq \frac{c(\alpha, \delta)}{q^{2+\delta}}$$

*for all rational numbers $\frac{p}{q}$.*

A proof can be found in [44]. Note that, if $\alpha$ is a real algebraic number of degree 2, then Liouville's Theorem 1.4.9 is stronger than Roth's Theorem 1.4.21. Whereas the latter one gives the estimate

$$\left|\alpha - \frac{p}{q}\right| \geq \frac{c(\alpha, \delta)}{q^{2+\delta}}$$

for every $\delta > 0$, Liouville's Theorem 1.4.9 states that there is a constant $c(\alpha) > 0$ such that

$$\left|\alpha - \frac{p}{q}\right| \geq \frac{c(\alpha)}{q^2}$$

for all rational numbers $\frac{p}{q}$. The analogous result for real algebraic numbers $\alpha$ of degree $\geq$3, namely, that there is a constant $c(\alpha) > 0$ such that an inequality of the form

[13] Axel Thue (1863–1922), a Norwegian mathematician.

[14] Carl Ludwig Siegel (1896–1981), a German mathematician.

[15] Freeman Dyson (1923), an English-born American mathematician.

[16] Klaus Friedrich Roth (1925–2015), a German-born British mathematician.

$$\left|\alpha - \frac{p}{q}\right| \geq \frac{c(\alpha)}{q^2}$$

holds for all rational numbers $\frac{p}{q}$, is conjectured to be false for all such $\alpha$. However, this is not known at the present time to be false for a single real algebraic number.

### Champernowne's Constant

The transcendental numbers (except $e$ and $\pi$) we have encountered so far are transcendental because their decimal (or dyadic) expansions have infinitely many runs of zeros whose lengths grow so quickly that the simple truncation of the decimal (or dyadic) expansion before each run of zeros leads to amazingly good approximations. However, for most numbers a collection of best rational approximations is not so easily detected from their decimal expansions. For most numbers even the best rational approximations are not close enough to allow us to conclude transcendency.

As an illustration of the difficulty of finding suitable rational approximations in general, we consider Champernowne's constant (resp. Mahler's[17] number).

**Definition 1.4.23** *Champernowne's constant (Mahler's number)*

$$\mathcal{M} = 0.123456789101112131415161718192021\ldots$$

is[18] the number obtained by concatenating the positive integers in base 10 and interpreting them as decimal digits to the right of a the decimal point.

We mention a method worked out in detail in [11]. Firstly, rational approximations created by long runs of zeros are used, and $\mathcal{M}$ is truncated just after the 1 that appears whenever a power of 10 is reached. Following this truncation procedure, we see that the number of decimal digits before each run of zeros exceeds the length of that run by far. For example, to get a run of just one zero, $\mathcal{M}$ has to be truncated after 10 digits, i.e., 0.123456789. In general, if we want to come across a run of $k$ zeros, we have to travel on the order of $k \cdot 10^k$ digits from the previous run of $k-1$ zeros. Thus, this truncation method cannot generate rational approximations having relatively small denominators that are sufficiently close to $\mathcal{M}$ in order to prove transcendence via Liouville's Theorem 1.4.9.

Using a more clever construction to build rational approximations to $\mathcal{M}$, described in [11], one can find approximations all having relatively small denominators that allow to apply Liouville's Theorem 1.4.9 to derive the following partial result.

**Theorem 1.4.24** (Mahler 1937) *The number*

$$\mathcal{M} = 0.123456789101112131415161718192021\ldots$$

*is either a transcendental number or an algebraic number of a degree at least* 5.

[17] Kurt Mahler (1903–1988), a German/British mathematician.

[18] OEIS A033307.

A proof can be found in [11, 38]. Theorem 1.4.24 does not guarantee that $\mathcal{M}$ is transcendental, however, it does imply that $\mathcal{M}$ is neither a quadratic irrational, nor a cubic or even quartic algebraic number. A more advanced analysis building on Liouville's Theorem 1.4.9 and Roth's Theorem 1.4.21 would ensure that $\mathcal{M}$ is transcendental.

**Theorem 1.4.25** (Mahler 1937) *Champernowne's constant $\mathcal{M}$ is a transcendental number.*

A proof can be found in [11, 38].

### 1.4.4 Thue's Theorem

Thue's work was already a major breakthrough for those kind of questions:

**Theorem 1.4.26** (Thue) *Let $\alpha$ be a real algebraic number of degree $d$. Then, for every $\delta > 0$, the inequality*

$$\left|\alpha - \frac{p}{q}\right| \leq \frac{1}{q^{\frac{1}{2}d+1+\delta}}$$

*has only finitely many rational solutions $\frac{p}{q}$.*

A proof can be found in [44].

**Corollary 1.4.27** *Let $\alpha$ be a real algebraic number of degree $d$. Then, for every $\delta > 0$, there is a constant $c(\alpha, \delta) > 0$ such that*

$$\left|\alpha - \frac{p}{q}\right| \geq \frac{c(\alpha, \delta)}{q^{\frac{1}{2}d+1+\delta}}$$

*for all rational numbers $\frac{p}{q}$.*

A proof can be found in [44].

The proof of Roth's Theorem 1.4.21 is immensely more complex than those for the theorems of Liouville and Thue, even though, the framework is in essence the same. The proof of Roth's Theorem 1.4.21 is not effective, that is, as noted in [30], for a given $\alpha$, the proof does not provide a method that guarantees to find the finitely many rational numbers $\frac{p}{q}$ satisfying

$$\left|\alpha - \frac{p}{q}\right| \leq \frac{1}{q^{2+\delta}}.$$

In other words, the proof does not give a lower bound on $c(\alpha, \delta)$. It is with respect to the work of Thue and Siegel that Roth's Theorem 1.4.21 is often named the Thue-Siegel-Roth theorem.

We give an application of the Thue–Siegel–Roth theorem to Diophantine equations. It follows from the fact that the approximation exponent of an algebraic

number $\alpha$ of degree $d \geq 3$ is strictly less than $d$. It appears that the full force of Roth's Theorem 1.4.21 is not needed, Thue's Theorem 1.4.26 is sufficient.

**Theorem 1.4.28** *Let*

$$a_d X^d + a_{d-1} X^{d-1} + \cdots + a_1 X + a_0 \in \mathbb{Z}[X] \tag{1.9}$$

*be an irreducible polynomial over* $\mathbb{Q}$ *of degree* $d \geq 3$. *Then, for every nonzero integer* $m$, *the Diophantine equation*

$$a_d X^d + a_{d-1} X^{d-1} Y + \cdots + a_1 X Y^{d-1} + a_0 Y^d = m \tag{1.10}$$

*has only finitely many integer solutions* $(p, q)$.

A proof can be found in [47]. An equation of the form (1.10) is called a *Thue equation*. It is interesting to note that equations of the form $X^2 - dY^2 = 1$, where $d$ is a positive and a square free integer, the so called Pellian equations, have infinitely many integer solutions, but equations of the form $X^3 - dY^3 = 1$ with an arbitrary integer $d$ have at most finitely many integer solutions. The books [11, 46] provide nice introductions to various aspects of Diophantine approximation, transcendence theory and Diophantine equations.

# 2 Linear Forms in Logarithms

## *2.1 Introduction*

Hilbert's problems form a list of twenty-three major problems in mathematics collected, proposed and published by D. Hilbert[19] in 1900. The problems were all unsolved at the time and several of them turned out to be very influential for 20th century mathematics. Hilbert believed that new machinery and methods were needed for solving these problems. He presented ten of them at the International Congress of Mathematicians in Paris in 1900. The complete list of his 23 problems was published later, most notably an English translation appeared 1902 in the *Bulletin of the American Mathematical Society*.

Hilbert's seventh problem, entitled "irrationality and transcendence of certain numbers", is dealing with the transcendence of the number

$$\alpha^\beta$$

for algebraic $\alpha \neq 0, 1$ and irrational algebraic $\beta$. He believed that the proof of this problem would only be given in more distant future than proofs of Riemann's hypothesis or Fermat's last theorem. Even though Hilbert was mistaken, he was correct when

[19] David Hilbert (1862–1943), a German mathematician.

he expressed his belief that the proof of that problem would be extremely intriguing and influential for 20th century mathematics. The seventh problem was solved independently by Gelfond[20] and Schneider[21] in 1935. They proved that, if $\alpha_1, \alpha_2 \neq 0$ are algebraic numbers such that $\log \alpha_1, \log \alpha_2$ are linearly independent over $\mathbb{Q}$, then

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

for all algebraic numbers $\beta_1, \beta_2$.

In 1935, Gelfond found a lower bound for the absolute value of the linear form

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

He proved that

$$\log |\Lambda| \gg -h(\Lambda)^{\kappa},$$

where $h(\Lambda)$ is the logarithmic height of the linear form $\Lambda$, $\kappa > 5$ and $\gg$ is Vinogradov's notation for an inequality that is valid up to an unspecified constant factor. Gelfond also noticed that generalization of his results would lead to a powerful new analytic method by which mathematicians could prove a huge amount of unsolved problems in number theory.

## 2.2 Basic Theorems and Definitions

In 1966 in 1967, A. Baker[22] gave in his papers "Linear forms in logarithms of algebraic numbers I, II, III", [1–3] an effective lower bound on the absolute value of a nonzero linear form in logarithms of algebraic numbers, that is, for a nonzero expression of the form

$$\sum_{i=1}^{n} b_i \log \alpha_i,$$

where $\alpha_1, \ldots, \alpha_n$ are algebraic numbers and $b_1, \ldots, b_n$ are integers. This result initiated the era of effective resolution of Diophantine equations that can be reduced to exponential ones (where the unknown variables are in the exponents). The generalization of the Gelfond-Schneider theorem was only the beginning of a new and very interesting branch in number theory called *Baker's theory*.

**Definition 2.2.1** Let $\alpha_1, \alpha_2, \ldots, \alpha_n$ be $n$ (real or complex) numbers. We call $\alpha_1, \alpha_2, \ldots, \alpha_n$ *linearly dependent* over the rationals (equivalently integers) if there are rational numbers (integer numbers) $r_1, r_2, \ldots, r_n$, not all zero, such that

[20] Alexander Osipovich Gelfond (1906–1968), a Soviet mathematician.

[21] Theodor Schneider (1911–1988), a German mathematician.

[22] Alan Baker (1939), an English mathematician.

$$r_1\alpha_1 + r_2\alpha_2 + \cdots + r_n\alpha_n = 0.$$

If $\alpha_1, \alpha_2, \ldots, \alpha_n$ are not linearly dependent over the rationals (integers), they are *linearly independent* over the rationals (integers).

**Definition 2.2.2** A *linear form in logarithms* of algebraic numbers is an expression of the form

$$\Lambda = \beta_0 + \beta_1 \log \alpha_1 + \beta_2 \log \alpha_2 + \cdots + \beta_n \log \alpha_n,$$

where $\alpha_i,\ i = 1, \ldots, n$ and $\beta_i,\ i = 0, \ldots, n$ are complex algebraic numbers and log denotes any determination of the logarithm.

*Remark 2.2.3* We are interested in the degenerate case when $\beta_0 = 0$ and $\beta_i \in \mathbb{Z},\ i = 1, \ldots, n$. In the sequel we write $\beta_i = b_i,\ i = 1, \ldots, n$ and log always represents the principal value of the complex logarithm.

A generalization of the Gelfond-Schneider theorem to arbitrarily many logarithms was obtained by Baker in 1966 [1]. In 1970, he was awarded the Fields Medal for his work in number theory, especially in the areas of transcendence and Diophantine geometry. One of his major contributions is the following

**Theorem 2.2.4** (Baker 1966) *If $\alpha_1, \alpha_2, \ldots, \alpha_n \neq 0, 1$ are algebraic numbers such that $\log \alpha_1, \log \alpha_2, \ldots, \log \alpha_n, 2\pi i$ are linearly independent over the rationals, then*

$$\beta_0 + \beta_1 \log \alpha_1 + \cdots + \beta_n \log \alpha_n \neq 0$$

*for any algebraic numbers $\beta_0, \beta_1, \ldots, \beta_n$ that are not all zero.*

A proof can be found in [1].

*Remark 2.2.5* Linear independence over the rationals implies linear independence over the algebraic numbers (see [4]).

**Theorem 2.2.6** (Baker 1967) *The number $e^{\beta_0}\alpha_1^{\beta_1} \ldots \alpha_n^{\beta_n}$ is transcendental for all nonzero algebraic numbers $\alpha_i,\ i = 1, \ldots, n$ and $\beta_i,\ i = 0, \ldots, n$. Furthermore, the number $\alpha_1^{\beta_1} \ldots \alpha_n^{\beta_n}$ is transcendental if $1, \beta_1, \ldots, \beta_n$ are linearly independent over the rationals.*

A proof can be found in [3].

**Definition 2.2.7** The *height* $H$ of a rational number $\frac{p}{q}$ is defined by

$$H\left(\frac{p}{q}\right) = \max\{|p|, |q|\}.$$

**Definition 2.2.8** Let $\mathbb{L}$ be a number field of the degree $D, \alpha \in \mathbb{L}$ an algebraic number of degree $d \mid D$ and let $\sum_{0 \leq k \leq d} a_k X^k$ be its minimal polynomial in $\mathbb{Z}[X]$ with $a_d \neq 0$. We define the *absolute logarithmic height* $h(\alpha)$ by

$$h(\alpha) = \frac{1}{d}\left(\log(|a_d|) + \sum_{1\le i\le d} \max\{\log(|\alpha_i|, 0)\}\right), \tag{2.1}$$

where $\alpha_i$ are the conjugates of $\alpha$.

*Example 2.2.9* The absolute logarithmic height $h$ of a rational number $\frac{p}{q}$ is

$$h\left(\frac{p}{q}\right) = \log \max\{|p|, |q|\}.$$

*Example 2.2.10* Let $\alpha = \sqrt{2}$. The absolute logarithmic height of $\alpha$ is

$$h(\alpha) = h(\sqrt{2}) = \frac{1}{2}\left(\log|\sqrt{2}| + \log|-\sqrt{2}|\right) = \frac{1}{2}\log 2.$$

*Example 2.2.11* Let

$$\alpha_1 = \frac{1}{\sqrt{3}+\sqrt{5}}.$$

Before calculating the absolute logarithmic height of $\alpha_1$, we compute the degree of the field extension $\mathbb{Q}\left(\frac{1}{\sqrt{3}+\sqrt{5}}\right)$ over $\mathbb{Q}$ as

$$\left[\mathbb{Q}\left(\frac{1}{\sqrt{3}+\sqrt{5}}\right) : \mathbb{Q}\right] = 4,$$

so the degree of the algebraic number $\alpha_1 = \frac{1}{\sqrt{3}+\sqrt{5}}$ over $\mathbb{Q}$ is 4.

The minimal polynomial of $\alpha_1$ is given by

$$\begin{aligned} P_{\alpha_1}(x) &= \left(x - \frac{1}{\sqrt{3}+\sqrt{5}}\right)\left(x - \frac{1}{-\sqrt{3}-\sqrt{5}}\right) \times \\ &\quad \times \left(x - \frac{1}{-\sqrt{3}+\sqrt{5}}\right)\left(x - \frac{1}{\sqrt{3}-\sqrt{5}}\right) \\ &= x^4 - 4x^2 + \frac{1}{4}, \end{aligned}$$

over the rationals, and

$$P_{\alpha_1}(x) = 4x^4 - 16x^2 + 1$$

over the integers. The conjugates of $\alpha_1$ are

$$\alpha_1 = \frac{1}{\sqrt{3}+\sqrt{5}},\ \alpha_2 = \frac{1}{-\sqrt{3}+\sqrt{5}},\ \alpha_3 = \frac{1}{\sqrt{3}-\sqrt{5}},\ \alpha_4 = \frac{1}{-\sqrt{3}-\sqrt{5}}.$$

Hence, using (2.1), the absolute logarithmic height of $\alpha_1$ is equal to

$$
\begin{aligned}
h(\alpha_1) &= h\left(\frac{1}{\sqrt{3}+\sqrt{5}}\right) \\
&= \frac{1}{4}\Bigg(\log|4| + \max\left\{\log\left|\frac{1}{\sqrt{3}+\sqrt{5}}\right|, 0\right\} + \max\left\{\log\left|\frac{1}{-\sqrt{3}+\sqrt{5}}\right|, 0\right\} + \\
&\quad + \max\left\{\log\left|\frac{1}{\sqrt{3}-\sqrt{5}}\right|, 0\right\} + \max\left\{\log\left|\frac{1}{-\sqrt{3}-\sqrt{5}}\right|, 0\right\}\Bigg) \\
&= 0.689146.
\end{aligned}
$$

Let $\mathbb{L}$ be a number field of degree $D$, $\alpha_1, \alpha_2, \ldots, \alpha_n$ nonzero elements of $\mathbb{L}$ and let $b_1, b_2, \ldots, b_n$ be integers. We define

$$B = \max\{|b_1|, |b_2|, \ldots, |b_n|\}$$

and

$$\Lambda^* = \alpha_1^{b_1}\alpha_2^{b_2}\ldots\alpha_n^{b_n} - 1.$$

We wish to bound $|\Lambda^*|$ from below, assuming that it is nonzero.

Since $\log(1+x)$ is asymptotically equal to $x$ as $|x|$ tends to 0, our problem consists of finding a lower bound for the linear form in logarithms

$$\Lambda = b_1\log\alpha_1 + \cdots + b_n\log\alpha_n + b_{n+1}\log(-1),$$

where $b_{n+1} = 0$ if $\mathbb{L}$ is real and $|b_{n+1}| \le nB$, otherwise.

**Definition 2.2.12** Let $A_1, A_2, \ldots, A_n$ be real numbers such that

$$A_j \ge h'(\alpha_j) := \max\{Dh(\alpha_j),\ |\log\alpha_j|,\ 0.16\},\ \ 1 \le j \le n.$$

Then $h'$ is called the *modified height* with respect to the field $\mathbb{L}$.

A. Baker, E.M. Matveev[23] and G. Wüstholz[24] proved the following theorems.

**Theorem 2.2.13** (Baker–Wüstholz 1993) *Assume that*

$$\Lambda = b_1\log\alpha_1 + \cdots + b_n\log\alpha_n \ne 0$$

*for algebraic $\alpha_i$ and integers $b_i$, $i = 1, \ldots, n$. Then*

$$\log|\Lambda| \ge -18(n+1)!n^{n+1}(32D)^{n+2}\log(2nD)h''(\alpha_1)\ldots h''(\alpha_n)\log B,$$

*where $D$ is the degree of the extension $\mathbb{Q}(\alpha_1, \ldots, \alpha_n)$, $B = \max\{|b_i|,\ i = 1, \ldots, n\}$ and $h''(\alpha) = \max\{h(\alpha),\ \frac{1}{D}|\log(\alpha)|,\ \frac{1}{D}\}$.*

[23] Eugene Mikhailovich Mateveev (1955), a Russian mathematician.

[24] Gisbert Wüstholz (1948), a German mathematician.

A proof can be found in [6].

**Theorem 2.2.14** (Matveev 2001) *Assume that $\Lambda^*$ is nonzero. Then*

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

*If $\mathbb{L}$ is real, then*

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

**Theorem 2.2.15** (Matveev 2001) *Assume that*

$$\Lambda = b_1 \log \alpha_1 + \dots + b_n \log \alpha_n \neq 0$$

*for algebraic $\alpha_i$ and integers $b_i$, $i = 1, \dots, n$. Then*

$$\log |\Lambda| > -2 \cdot 30^{n+4}(n+1)^6 D^2 A_1 \dots A_n (1 + \log D)(1 + \log B),$$

*where $B = \max\{|b_i|,\ 1 \leq i \leq n\}$.*

Proofs for Matveev's theorems can be found in [39].

## 2.3 A Variation of Baker–Davenport Lemma

For a real number $x$ we introduce the notation

$$||x|| = \min\{|x - n| : n \in \mathbb{Z}\}$$

for the distance from $x$ to the nearest integer.

The following result is a variation of a lemma of Baker and Davenport[25] [5], it is due to Dujella[26] and Pethő,[27] [22].

**Lemma 2.3.1** *Let $N$ be a positive integer, $\frac{p}{q}$ a convergent of the continued fraction expansion of an irrational number $\kappa$ such that $q > 6N$ and let $\mu$ be some real number. Let $\varepsilon = ||\mu q|| - N||\kappa q||$. If $\varepsilon > 0$, then there is no solution to the inequality*

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

*in positive integers $m$ and $n$ with*

[25] Harold Davenport (1907–1969), an English mathematician.

[26] Andrej Dujella (1966), a Croatian mathematician.

[27] Attila Pethő (1950), a Hungarian mathematician.

$$\frac{\log(Aq/\varepsilon)}{\log B} \leq m \leq N.$$

*Proof* Suppose that $0 \leq m \leq N$. Then

$$m(\kappa q - p) + mp - nq + \mu q < qAB^{-m}.$$

Thus,

$$qAB^{-m} > |\mu q - (nq - mp)| - m||\kappa q|| \geq ||\mu q|| - N||\kappa q|| := \varepsilon,$$

from where we deduce that

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

*Remark 2.3.2* The method from Lemma 2.3.1 is called Baker–Davenport reduction.

*Example 2.3.3* Find all nonnegative integers that satisfy

$$0 < |x_1 \log 2 - x_2 \log 3 + \log 5| < 40e^{-X}, \tag{2.2}$$

where $X = \max\{x_1, x_2\} \leq 10^{30}$.

Let

$$x_1 \log 2 - x_2 \log 3 + \log 5 > 0.$$

First, we divide (2.2) by $\log 3$, in order to get inequalities of the form as in Lemma 2.3.1. We get

$$0 < x_1 \frac{\log 2}{\log 3} - x_2 + \frac{\log 5}{\log 3} < \frac{40}{\log 3} e^{-X}.$$

Now, we define

$$\kappa = \frac{\log 2}{\log 3}, \quad \mu = \frac{\log 5}{\log 3}, \quad A = \frac{40}{\log 3}, \quad B = e.$$

We observe that the inequalities $A > 0$, $B > 1$ are satisfied.

We shall try to find a convergent $\frac{p}{q}$ of the continued fraction expansion of $\kappa$ that satisfies the condition $q > 6N$. Since $\kappa$ does not have a finite or periodic continued fraction expansion, we give only the first 25 terms of its continued fraction expansion:

$$\kappa = [0, 1, 1, 1, 2, 2, 3, 1, 5, 2, 23, 2, 2, 1, 1, 55, 1, 4, 3, 1, 1, 15, 1, 9, 2, \dots].$$

The first convergent $\frac{p}{q}$ that satisfies the inequality $q > 6N$ is

$$\frac{p}{q} = \frac{352708924597706758360421784753 39}{559030419157051019225366955202 22}.$$

We therefore obtain

$$||\kappa q||N \approx 0.007651391, \qquad ||\mu q|| \approx 0.466714899.$$

Hence,

$$\varepsilon = ||\mu q|| - ||\kappa q||N = 0.4590635078 > 0.$$

The given inequality does not have any solution in integers $m$ such that

$$\frac{\ln\left(\frac{40}{\log 3}\cdot q\cdot\frac{1}{0.4590635}\right)}{\ln e} \le m \le N.$$

We observe that $m \le 77.4746$, so $N = 77$. Repeating Baker–Davenport reduction one more time, but now with $N = 77$, we find convergents $\frac{p}{q}$ of the continued fraction expansion of $\kappa$ that satisfies the condition $> 6N$, $N = 77$. The first such convergent is

$$\frac{p}{q} = \frac{306}{485}.$$

We get

$$||\kappa q||N \approx 0.071647126, \qquad ||\mu q|| \approx 0.487842451.$$

Finally, we obtain

$$\varepsilon \approx 0.4161953257.$$

After applying Baker–Davenport reduction, we get $m \le 10.6556$, resp. $N = 10$. Therefore, we can find pairs $(x_1, x_2)$ satisfying the introduced inequalities. Using a simple computer algorithm, it turns out that the following pairs

$$(0,0),\ (0,1),\ (1,0),\ (1,1),\ (1,2),\ (2,0),\ (2,1),\ (2,2),\ (3,0),\ (3,1),\ (3,2),\ (3,3),\ (4,3)$$

satisfy (2.2).

For

$$x_1 \log 2 - x_2 \log 3 + \log 5 < 0,$$

we have

$$0 < x_2\frac{\log 3}{\log 2} - x_1 - \frac{\log 5}{\log 2} < \frac{40}{\log 2}e^{-X}.$$

We define

$$\kappa = \frac{\log 3}{\log 2}, \quad \mu = -\frac{\log 5}{\log 2}, \quad A = \frac{40}{\log 2}, \quad B = e.$$

Then the inequalities $A > 0$, $B > 1$ are satisfied. The next step is to find a convergent $\frac{p}{q}$ of the continued fraction expansion of $\kappa$ satisfying $q > 6N$. For

$$\frac{p}{q} = \frac{1522076097743333607781100045449522888}{960323097266207036440783078900790949}$$

we get

$$\varepsilon = 0.124406274 > 0.$$

Analogously, we find $N = 89$ after the first reduction and $N = 13$ after the second one. Finally, we get that the following pairs

$$(0, 2), (0, 3), (1, 3), (2, 3), (2, 4), (3, 4), (4, 4), (5, 5).$$

that satisfy (2.2), as well.

## 2.4 Applications

For the applications of linear forms in logarithms to Diophantine equations, the strategy is as follows: first, we use various algebraic manipulations to associate "relatively big" solutions of the equations to a "very small" value of the specific linear form in logarithms which implies that we are able to find upper bound for values of the linear form in the logarithms that corresponds to a solution of the equation. If we compare that upper bound with the lower bound (using the Baker–Wüstholz Theorem 2.2.13 or Matveev's Theorems 2.2.14 and 2.2.15), we get an absolute upper bound $M$ for the absolute values of the unknowns of the equations.

It often happens that the upper bound $M$ is not too large and using various methods, including reductions and sieves, we can find the complete set of solutions below $M$. In order to realize this, it is crucial to get a reasonably small value for $M$. Its size is directly related to the size of the "numerical constant" that appears in Matveev's Theorem 2.2.14 which is $1.4 \cdot 30^{n+3} n^{4.5}$. Many celebrated Diophantine equations lead to estimates of linear forms in two or three logarithms and in these cases Matveev's Theorem 2.2.14 gives numerical constants around $10^{12}$ and $10^{14}$, respectively.

### 2.4.1 A Lower Bound for $|2^m - 3^n|$

One of the simplest applications of linear forms in logarithms is to prove that $|2^m - 3^n|$ tends to infinity with $m + n$; in addition one can even get an explicit lower bound for this quantity. The following material is presented in detail in [14].

Let $n \geq 2$ be an integer and $m$ and $m'$ are defined by the conditions

$$2^{m'} < 3^n < 2^{m'+1}, \quad |3^n - 2^m| = \min\{3^n - 2^{m'}, 2^{m'+1} - 3^n\}.$$

Then

$$|2^m - 3^n| < 2^m, \ \ (m-1)\log 2 < n \log 3 < (m+1)\log 2,$$

and the problem of finding a lower bound for $|2^m - 3^n|$ clearly reduces to this special case.

Consider the linear form

$$\Lambda = 3^n 2^{-m} - 1.$$

Applying Matveev's Theorem 2.2.14, we get

$$\log |\Lambda| > -c_0(1 + \log m).$$

It is easy to verify that we can take $c_0 = 5.87 \cdot 10^8$. Hence, the following theorem is proved.

**Theorem 2.4.1** *Let $m, n$ be positive integers. Then*

$$|2^m - 3^n| > 2^m (em)^{-5.87 \cdot 10^8}$$

This theorem enables us to find the list of all powers of 3 that increased by 5 give a power of 2.

**Corollary 2.4.2** *The only integer solutions to the Diophantine equation*

$$2^m - 3^n = 5$$

*are* $(m, n) = (3, 1), (5, 3)$.

Applying Theorem 2.4.1, we get

$$5 > 2^m (em)^{-5.87 \cdot 10^8},$$

which implies

$$\log 5 > m \log 2 - 5.87 \cdot 10^8 (1 + \log m),$$

so that $m < 2.1 \cdot 10^{10}$ and $n < m \frac{\log 2}{\log 3} < 1.4 \cdot 10^{10}$. Moreover, the equality $2^m - 3^n = 5$ implies

$$\left| m - n \frac{\log 3}{\log 2} \right| < \frac{5}{\log 2} 3^{-n}.$$

Since

$$\frac{5}{\log 2} \cdot 3^{-n} < \frac{1}{2n}$$

for $n \geq 4$, we observe that, if $(m, n)$ is a solution to our problem with $n \geq 4$, then $\frac{m}{n}$ is a convergent of the continued fraction expansion of $\xi = \frac{\log 3}{\log 2}$. Also, for $n < N =$

$1.4 \cdot 10^{10}$ the smallest value of $|m - n\xi|$ is obtained for the largest convergent of the continued fraction expansion of $\xi$ with the denominator less then $N$. We thus get

$$\frac{5}{\log 2} \cdot 3^{-n} > \left| m - n\frac{\log 3}{\log 2} \right| > 10^{-11}, \ 0 < n < 1.4 \cdot 10^{10}.$$

Hence, $n \leq 24$. Now, it is very easy to prove the initial statement.

More generally, the following result can be obtained.

**Theorem 2.4.3** (Bennett, [7]) *For given nonzero integers $a, b, c$ the equation*

$$a^m - b^n = c$$

*has at most two integer solutions.*

### 2.4.2 Rep-Digit of Fibonacci Numbers

The Fibonacci sequence $(F_n)_{n\geq 0}$ is given by

$$F_0 = 0, \ F_1 = 1, \ \ldots, \ F_{n+2} = F_{n+1} + F_n, \ n \geq 0.$$

Its characteristic equation is

$$f(X) = X^2 - X - 1 = (X - \alpha)(X - \beta),$$

where $\alpha = \frac{1+\sqrt{5}}{2}$ and $\beta = \frac{1-\sqrt{5}}{2}$. We can also write

$$F_n = \frac{\alpha^n - \beta^n}{\alpha - \beta}, \ n \geq 0.$$

In this subsection we are concerned with those Fibonacci numbers $F_n$ that have equal digits in base 10. Putting $d$ for the repeated digit and assuming that $F_n$ has $m$ digits, the problem reduces to finding all solutions of the Diophantine equation

$$F_n = \overline{dd\ldots d}_{(10)} = d10^{m-1} + d10^{m-1} + \cdots + d = d\frac{10^m - 1}{10 - 1}, \ d \in \{1, 2, \ldots 9\}. \tag{2.3}$$

**Theorem 2.4.4** *The largest solution of Eq. (2.3) is $F_{10} = 55$.*

*Proof* Suppose that $n > 1000$. We start by proving something weaker. Our goal is to obtain some bound on $n$. We rewrite Eq. (2.3) as

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

Next we separate *large* and *small terms* on both sides of the equation. It is easy to obtain $\alpha = \frac{-1}{\beta}$ or $\beta = \frac{-1}{\alpha}$ which implies

$$\left|\alpha^n - \frac{d\sqrt{5}}{9}10^m\right| = \left|\beta^n - \frac{d\sqrt{5}}{9}\right| \leq |\beta^n| + \left|\frac{d\sqrt{5}}{9}\right| \leq \alpha^{-1000} + \sqrt{5} < 2.5. \quad (2.4)$$

Our goal is to get some estimates for $m$ in terms of $n$. By induction on $n$, it is easy to prove that

$$\alpha^{n-2} < F_n < \alpha^{n-1}, \ n \geq 3.$$

Thus,

$$\alpha^{n-2} < F_n < 10^m \ \text{ or } \ n < m\frac{\log 10}{\log \alpha} + 2,$$

and

$$10^{m-1} < F_n < \alpha^{n-1}.$$

On the other hand,

$$n > \frac{\log 10}{\log \alpha}(m-1) + 1 = \frac{\log 10}{\log \alpha}m - \left(\frac{\log 10}{\log \alpha} - 1\right) > \frac{\log 10}{\log \alpha}m - 4.$$

We deduce that

$$n \in [c_1 m - 4, \ c_1 m + 2], \qquad c_1 = \frac{\log 10}{\log \alpha} = 4.78497..$$

Since $c_1 > 4$, for $n > 1000$, we have $n \geq m$. Hence,

$$|\Lambda| = \left|\frac{d\sqrt{5}}{9}\alpha^{-n}10^m - 1\right| < \frac{2.5}{\alpha^n} < \frac{1}{\alpha^{n-2}},$$

which leads to

$$\log|\Lambda| = \log\frac{d\sqrt{5}}{9} - n\log\alpha + m\log 10 < -(n-2)\log\alpha.$$

Let

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

as well as $\mathbb{L} = \mathbb{Q}(\alpha_1, \alpha_2, \alpha_3) = \mathbb{Q}(\sqrt{5})$, so $D = 2$ and $B = n$. The minimal polynomial of $\alpha_1$ over $\mathbb{Z}$ is

$$P_{\alpha_1}(X) = 81X^2 - 5d^2.$$

Hence,

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

and

$$h(\alpha_2) = \frac{1}{2}(\log\alpha + 1) < 0.75, \;\; h(\alpha_3) = \log 10 < 2.31.$$

We may take

$$A_1 = 6.02, \;\; A_2 = 1.5, \;\; A_3 = 4.62.$$

Then Matveev's Theorem 2.2.14 gives us a lower bound for $\Lambda$, namely

$$\log\Lambda > -1.4 \cdot 30^6 \cdot 3^{4.5} \cdot 4(1+\log 4)6.02 \cdot 1.5 \cdot 4.62(1+\log n).$$

Comparing the above inequality with

$$\log\Lambda < -(n-2)\log\alpha,$$

we get

$$(n-2)\log\alpha < 1.41 \cdot 30^6 \cdot 3^{4.5} \cdot 4(1+\log 4)6.02 \cdot 1.5 \cdot 4.62(1+\log n),$$

and

$$n < 4.5 \cdot 10^{15}.$$

*Reducing the bound.* Observe that the right-hand side of the inequality

$$1 - \frac{d\sqrt{5}}{9}\alpha^{-n}10^m \le \frac{1}{\alpha^n}\left(\beta^n - \frac{d\sqrt{5}}{9}\right)$$

is negative. Writing

$$z = \log\alpha_1 - n\log\alpha_2 + m\log\alpha_3,$$

we get that

$$-\frac{2.5}{\alpha^n} < 1 - e^z < 0.$$

In particular, $z > 0$. Furthermore, we have $e^z < 1.5$ for $n > 1000$. Thus,

$$0 < e^z - 1 < \frac{2.5e^z}{\alpha^n} < \frac{4}{\alpha^n}.$$

Since $e^z - 1 > z$, we get

$$0 < m\left(\frac{\log \alpha_3}{\log \alpha_2}\right) - n + \left(\frac{\log \alpha_1}{\log \alpha_2}\right) < \frac{4}{\alpha^n \log \alpha_2} < \frac{9}{\alpha^n}.$$

We notice that

$$\left(\frac{10^m d\sqrt{5}}{\alpha^n}\right) < 2$$

and therefore

$$\alpha^n > \frac{10^m d\sqrt{5}}{2} > 10^m.$$

Hence,

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

Since $n < 4.5 \cdot 10^{15}$, the previous inequality implies $m < 9.5 \cdot 10^{14}$. With

$$\kappa = \frac{\log \alpha_3}{\log \alpha_2}, \ \ \mu = \frac{\log \alpha_1}{\log \alpha_2}, \ \ A = 9, \ \ B = 10$$

we get

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

where $m < N := 10^{15}$. Observe that

$$\frac{p_{35}}{q_{35}} = C_{35} = \frac{970939497358931987}{202914354378543655}$$

and $q_{35} > 202914354378543655 > 2 \cdot 10^{17} > 6N$.

For each one of the values of $d \in \{1, \ldots, 9\}$, we compute $||q_{35}\mu||$. The minimal value of this expression is obtained when $d = 5$ and is

$$0.029... > 0.02.$$

Thus, we can take $\varepsilon = 0.01 < 0.02 - 0.01 < ||q_{35}\mu|| - N||q_{35}\kappa||$. Since

$$\frac{\log(Aq_{35}/\varepsilon)}{\log B} = 21.2313...,$$

we observe that there is no solution in the range $m \in \left[22, 10^{15}\right]$. Thus, $m \leq 21$, and $n \leq 102$. However, we have assumed that $n > 1000$. To finish, we compute the values of all Fibonacci numbers modulo 10000 (their last four digits) and convince ourselves that there are no Fibonacci numbers with the desired pattern in the range $11 \leq n \leq 1000$. This example stems from [25, 36].

### 2.4.3 Simultaneous Pellian Equations

The following result is due to Baker and Davenport and was historically the first example of a successful use of lower bounds for linear forms in logarithms of algebraic numbers; it actually allowed the effective computation of all common members of two binary recurrent sequences with real roots; for more details see [19, 25, 36].

**Theorem 2.4.5** *The only positive integer $d$ such that $d+1,\ 3d+1,\ 8d+1$ are all perfect squares is $d = 120$.*

*Proof* If $d+1,\ 3d+1,\ 8d+1$ are all perfect squares, then we write

$$d+1 = x^2,\ \ 3d+1 = y^2,\ \ 8d+1 = z^2.$$

Eliminating $d$ from the above equations, we get

$$3x^2 - y^2 = 2,\ \ 8x^2 - z^2 = 7,$$

which is a *system of simultaneous Pellian equations* since it consists of two Pellian equations with a component in common. If we want $x$ to be positive, the solutions of the above system are

$$y + x\sqrt{3} = (1+\sqrt{3})(2+\sqrt{3})^m,$$
$$z + x\sqrt{8} = (\pm 1+\sqrt{8})(3+\sqrt{8})^n,$$

where $m, n$ are nonnegative integers. Let the sequence $(v_m)$ be given by the recursion formula

$$v_0 = 1,\ \ v_1 = 3,\ \ v_{m+2} = 4v_{m+1} - v_m,$$

and put $x = w_n^{+,-}$, for some $n \geq 0$, where the sequences $(w_n^+)$, $(w_n^-)$ are defined by

$$w_0^+ = 1,\ \ w_1^+ = 4,\ \ w_{n+2}^+ = 6w_{n+1}^+ - w_n^+,\ \ n \in \mathbb{N},$$

$$w_0^- = 1,\ \ w_1^- = 2,\ \ w_{n+2}^- = 6w_{n+1}^- - w_n^-,\ \ n \in \mathbb{N}.$$

We want to solve the equation

$$v_m = w_n^{+,-}.$$

For this aim we shall use the following lemmas.

**Lemma 2.4.6** *If $v_m = w_n^{+,-}$, $m, n > 2$, then*

$$0 < |\Lambda| < 7.3(2+\sqrt{3})^{-2m},$$

*where $\Lambda$ is*

$$\Lambda = m\log(2+\sqrt{3}) - n\log(3+2\sqrt{2}) + \log\frac{2\sqrt{2}(1+\sqrt{3})}{\sqrt{3}(2\sqrt{2}\pm 1)}.$$

*Proof* The expression $v_m = w_n^{+,-}$ implies

$$\begin{aligned}&\frac{(1+\sqrt{3})(2+\sqrt{3})^m - (1-\sqrt{3})(2-\sqrt{3})^m}{2\sqrt{3}}\\ &= \frac{(2\sqrt{2}\pm 1)(3+2\sqrt{2})^n + (2\sqrt{2}\mp 1)(3-2\sqrt{2})^n}{4\sqrt{2}}.\end{aligned} \tag{2.5}$$

Obviously,

$$v_m > \frac{(1+\sqrt{3})(2+\sqrt{3})^m}{2\sqrt{3}},$$

$$w_n^{+,-} < \frac{(2\sqrt{2}+1)(3+2\sqrt{2})^n}{2\sqrt{2}},$$

hence

$$\frac{(1+\sqrt{3})(2+\sqrt{3})^m}{2\sqrt{3}} < \frac{(2\sqrt{2}+1)(3+2\sqrt{2})^n}{2\sqrt{2}},$$

$$(3-2\sqrt{2})^n < \frac{\sqrt{3}(2\sqrt{2}+1)}{\sqrt{2}(\sqrt{3}+1)}(2-\sqrt{3})^m < 1.7163(2-\sqrt{3})^m.$$

Dividing (2.5) by $\frac{2\sqrt{2}\pm 1}{4\sqrt{2}}(3+2\sqrt{2})^n$, we obtain

$$\begin{aligned}&\left|\frac{2\sqrt{2}(1+\sqrt{3})}{\sqrt{3}(2\sqrt{2}\pm 1)}\cdot\frac{(2+\sqrt{3})^m}{(3+2\sqrt{2})^n} - 1\right|\\ &\le \frac{2\sqrt{2}+1}{2\sqrt{2}-1}(3-2\sqrt{2})^{2n} + \frac{2\sqrt{2}(\sqrt{3}-1)}{\sqrt{3}(2\sqrt{2}-1)}(2-\sqrt{3})^m(3-2\sqrt{2})^n\\ &< \frac{2\sqrt{2}+1}{2\sqrt{2}-1}\cdot 1.7163^2(2-\sqrt{3})^{2m} + \frac{2\sqrt{2}(\sqrt{3}-1)}{\sqrt{3}(2\sqrt{2}-1)}\cdot 1.7163(2-\sqrt{3})^{2m}\\ &< 7.29(2-\sqrt{3})^{2m},\end{aligned}$$

which proves Lemma 2.4.6.

**Lemma 2.4.7** *Let $a \in \mathbb{R}\setminus\{0\}$, $a > 1$. If $|x| < a$, then*

$$|\log(1+x)| < \frac{-\log(1-a)}{a}|x|. \tag{2.6}$$

*Proof* We observe that the function

$$\frac{\log(1+x)}{x}$$

is positive and strictly decreasing for $|x| < 1$. Consequently, for $|x| < a$, Inequality (2.6) holds for $x = -a$.

We shall investigate the following linear form in three logarithms:

$$\Lambda = m\log(2+\sqrt{3}) - n\log(2\sqrt{2}+3) + \log\frac{2\sqrt{2}(\sqrt{3}+1)}{\sqrt{3}(2\sqrt{2}\pm 1)}.$$

Let

$$\alpha_1 = 2+\sqrt{3},\ \ \alpha_2 = 3+2\sqrt{2},\ \ \alpha_3 = \frac{2\sqrt{2}(1+\sqrt{3})}{\sqrt{3}(2\sqrt{2}\pm 1)},$$

$$b_1 = m,\ \ b_2 = -n,\ \ b_3 = 1,\ \ D = [\mathbb{Q}(\alpha_1,\alpha_2,\alpha_3):\mathbb{Q}] = 4.$$

The minimal polynomials over $\mathbb{Z}$ are

$$\begin{aligned} P_{\alpha_1}(x) &= x^2 - 4x + 1,\\ P_{\alpha_2}(x) &= x^2 - 6x + 1,\\ P_{\alpha_3}(x) &= 441x^4 - 2016x^3 + 2880x^2 - 1536x + 256, \end{aligned}$$

hence

$$\begin{aligned} h''(\alpha_1) &= \frac{1}{2}\log(2+\sqrt{3}) < 0.6585,\\ h''(\alpha_2) &= \frac{1}{2}\log(3+2\sqrt{2}) < 0.8814, \end{aligned}$$

and

$$h''(\alpha_3) = \frac{1}{4}\log\left(441\frac{2(4+\sqrt{2})(3+\sqrt{3})}{21}\frac{2(4-\sqrt{2})(3+\sqrt{3})}{21}\right) < 1.7836.$$

Applying the Baker–Wüstholz Theorem 2.2.13, we get a lower bound for $\Lambda$, namely

$$\log|\Lambda| \geq -3.96\cdot 10^{15}\log m.$$

According to Lemma 2.4.6, we may conclude that

$$m < 6\cdot 10^{16}.$$

This upper bound is rather big so we reduce it using Baker–Davenport reduction. Applying Lemma 2.4.6, we get the upper bound

$$\Lambda = m\log(2+\sqrt{3}) - n\log(2\sqrt{2}+3) + \log\frac{2\sqrt{2}(\sqrt{3}+1)}{\sqrt{3}(2\sqrt{2}\pm 1)} < 7.29(2+\sqrt{3})^{-2m}.$$

Let

$$N = 6\cdot 10^{16},\ \ \kappa = \frac{\log\alpha_1}{\log\alpha_2},\ \ \mu = \frac{\log\alpha_3}{\log\alpha_2},\ \ A = \frac{7.3}{\log\alpha_2},\ \ B = (2+\sqrt{3})^2.$$

The next step is to find a convergent $\frac{p}{q}$ of the continued fraction expansion of $\kappa = \frac{\log\alpha_1}{\log\alpha_2}$ such that $q > 6N$. The first such convergent is

$$\frac{p}{q} = \frac{742265900639684111}{9935223607325971 20}.$$

Before calculating $\varepsilon$, we observe that

$$||\kappa q||N \approx 0.0187822, \qquad ||\mu q|| \approx 0.00762577.$$

Unfortunately,

$$\varepsilon = ||\mu q|| - ||\kappa q||N < 0.$$

If we want to use Baker–Davenport reduction, we have to find another convergent $\frac{p}{q}$ of the continued fraction expansion for which the condition $\varepsilon > 0$ is satisfied.

The next convergent $\frac{p}{q}$ of $\kappa$ that satisfies condition $q > 6N$ is

$$\frac{p}{q} = \frac{2297570640187354392}{3075296607888933649}.$$

It follows that

$$\varepsilon = ||\mu q|| - ||\kappa q||N \approx 0.296651 > 0.$$

The given inequality does not have any solutions in integers $m$ such that

$$\frac{\log\left(\frac{Aq}{\varepsilon}\right)}{\log B} \le m < N.$$

Thus, the new upper bound for $m$ is 17. Repeating the procedure once again, we get $m \le 4$, and there are only two solutions, namely

$$v_0 = w_0^{+,-} = 1,$$

which is the trivial solutions of our Diophantine equation with $d = 0$, and

$$v_2 = w_2^{-} = 11,$$

which suits the case when $d = 120$.

### 2.4.4 Fibonacci Numbers and the Property of Diophantus

The next result is due to Dujella [17]. He proved that, if $k$ and $d$ are positive integers such that the set

$$\{F_{2k}, F_{2k+2}, F_{2k+4}, d\}$$

is a $D(1)$-quadruple, then $d = 4F_{2k+1}F_{2k+2}F_{2k+3}$, where $F_k$ is $k$-th Fibonacci number. This is a generalization of the Theorem 2.4.5 of Baker and Davenport for $k = 1$. Here a set $\{a_1, a_2, a_3, a_4\}$ of distinct positive integers is called *a $D(1)$-quadruple*, if $a_i a_j + n$ is a perfect square for every $i, j$ with $1 \leq i < j \leq 4$.

*Proof* (Sketch) Let $k \geq 2$ be a positive integer and

$$a = F_{2k},\ b = F_{2k+2},\ c = F_{2k+4}.$$

Then $c = 3b - a$. Furthermore,

$$ab + 1 = (b - a)^2,\ ac + 1 = b^2,\ bc + 1 = (a + b)^2.$$

If we assume that $d$ is a positive number such that $\{a, b, c, d\}$ has the property $D(1)$ of Diophantus, it implies that there exist positive integers $x, y, z$ such that

$$ad + 1 = x^2,\ bd + 1 = y^2,\ (3b - a)d + 1 = z^2.$$

Eliminating $d$, we get a system of Pellian equations

$$ay^2 - bx^2 = a - b, \quad az^2 - (3b - a)x^2 = 2a - 3b. \tag{2.7}$$

Dujella proved the following lemmas.

**Lemma 2.4.8** *Let $x, y, z$ be positive integer solutions of the system of Pellian equations (2.7). Then there exist integers $m$ and $n$ such that*

$$x = v_m = w_n,$$

*where $(v_m)$ is given by*

$$v_0 = 1,\ v_1 = b,\ v_{m+2} = 2(b - a)v_{m+1} - v_m,\ m \in \mathbb{Z},$$

*and the two-sided sequence $(w_n)$ is defined by*

$$w_0 = 1,\ w_1 = a + b,\ w_{n+2} = 2bw_{n+1} - w_n,\ n \in \mathbb{Z}.$$

In order to apply Baker's method, it is convenient to consider the two-sided sequence as two ordinary sequences. Therefore, instead of the sequence $(v_m)_{m\in\mathbb{Z}}$, Dujella considered two sequences $(v_m)_{m\geq 0}$ and $(v_m)_{m\leq 0}$ and applied the same method for the sequence $(w_n)_{n\in\mathbb{Z}}$. Thus, four equations of the form

$$v_m = w_n$$

have to be considered.

**Lemma 2.4.9** *If $v_m = w_n$, and $m \neq 0$, then*

$$0 < m\log(b-a+\sqrt{ab}) - n\log(b+\sqrt{ac}) + \\ + \log\frac{\sqrt{c}(\pm\sqrt{a}+\sqrt{b})}{\sqrt{b}(\pm\sqrt{a}+\sqrt{c})} < 4(b-a+\sqrt{ab})^{-2m}.$$

In the present situation, $l = 3$, $d = 4$, $B = m$ and

$$\alpha_1 = b-a+\sqrt{ab},\ \alpha_2 = b+\sqrt{ac},\ \alpha_3 = \frac{\sqrt{c}(\pm\sqrt{a}+\sqrt{b})}{\sqrt{b}(\pm\sqrt{a}+\sqrt{c})},$$

$$h'(\alpha_1) = \frac{1}{2}\log\alpha_1 < 1.05\log,\ h'(\alpha_2) = \frac{1}{2}\log\alpha_2 < 1.27\log a,$$

$$h'(\alpha_3) = \frac{1}{4}\log(bc(c-a)(\sqrt{a}+\sqrt{b})^2) < 2.52\log a,$$

$$\log 4(b-a+\sqrt{ab})^{-2m} < \log a^{-2m} = -2m\log a.$$

Hence,

$$2m\log a < 3.822\cdot 10^{15}\cdot 3.361\log^3 a\log m,$$

and

$$\frac{m}{\log m} < 6.423\cdot 10^{15}\log^2 a. \tag{2.8}$$

Applying Lemma 2.4.8, we get

$$|m| \geq 2b-2 > 4a. \tag{2.9}$$

Comparing (2.8) and (2.9), we obtain

$$\frac{m}{\log^3 m} < 6.423\cdot 10^{15},$$

which implies $m < 8\cdot 10^{20}$, $a = F_{2k} < 2\cdot 10^{20}$. The author has proved the theorem for $k \geq 49$.

It remains to prove the theorem for $2 \leq k \leq 48$. Dujella used Lemma 2.3.1 with

$$\kappa = \frac{\log \alpha_1}{\log \alpha_2},\ \mu = \frac{\log \alpha_3}{\log \alpha_2},\ A = \frac{4}{\log \alpha_3},\ B = (b - a + \sqrt{ab})^2$$

as well as $N = 8 \cdot 10^{20}$ and gets a new bound $m \leq N_0$, where $N_0 \leq 12$. Repeating the method one more time, he obtained a new upper bound $m \leq 2$ which completes the proof.

### 2.4.5 The Non-extendibility of Some Parametric Families of $D(-1)$-Triples

**Definition 2.1** Let $n$ be a nonzero integer. A set $\{a_1, \ldots, a_m\}$ of $m$ distinct positive integers is called *a Diophantine $m$-tuple with the property $D(n)$*, or simply *a $D(n)$-$m$-tuple*, if $a_i a_j + n$ is a perfect square for any $i, j$ with $1 \leq i < j \leq m$.

The set $\{1, 3, 8, 120\}$ considered in the previous Sect. 2.4.3 is known as the first example of a $D(1)$-quadruple found by Fermat.[28] In 1969, Baker and Davenport proved that $\{1, 3, 8\}$ cannot be extended to a $D(1)$-quintuple (see [5]). This result was generalized by Dujella [15], who showed that the $D(1)$-triple $\{k - 1, k + 1, 4k\}$ for an integer $k$ cannot be extended to a $D(1)$-quintuple, and by Dujella and Pethő [22], who proved that the $D(1)$-pair $\{1, 3\}$ cannot be extended to a $D(1)$-quintuple. It is a conjectured that there does not exist a $D(1)$-quintuple. The most general results on this conjecture are due to Dujella [18] who proved that there does not exist a $D(1)$-sextuple and that there exist at most finitely many $D(1)$-quintuples. There have been some improvements on those results recently, but the conjecture still remains open.

In contrast to the case $n = 1$, it is conjectured that there does not exist a $D(-1)$-quadruple (see [16]). The first important step in this direction was done by Dujella and Fuchs [21] who showed that, if $\{a, b, c, d\}$ is a $D(-1)$-quadruple with $a < b < c < d$, then $a = 1$. Later Dujella, Filipin and Fuchs [23] showed that there exist at most finitely many $D(-1)$-quadruples. The number of $D(-1)$-quadruples is now known to be bounded by $5 \cdot 10^{60}$ (see [24]). However, this bound is too large for verifying the conjecture by present day computers. Recently, He and Togbé [29] proved that the $D(-1)$-triple $\{1, k^2 + 1, k^2 + 2k + 2\}$ cannot be extended to a $D(-1)$-quadruple. Their result and the proof appears to be very important because of their use of a linear form in two logarithms (instead of three) for the first time; this leads to a much better upper bound for the solutions which shortens the reduction time significantly. In this subsection, we extend their method and apply it to several other families of $D(-1)$-triples. Let us also mention that it is not always possible to use linear forms in two logarithms. In the sequel we only explain the idea and give a sketch of the proofs; more details can be found in [26].

[28] Pierre de Fermat (1601–1665), a French mathematician.

**Introduction**

Let $\{1, b, c\}$ be a $D(-1)$-triple with $b < c$. We define positive integers $r$, $s$ and $t$ by

$$b - 1 = r^2,\ c - 1 = s^2,\ bc - 1 = t^2.$$

Then, $s$ and $t$ satisfy

$$t^2 - bs^2 = r^2. \tag{2.10}$$

It can be proven that Diophantine equation (2.10) has at least three classes of solutions belonging to

$$(t_0, s_0) = (r, 0),\ (b - r, \pm(r - 1))$$

(see [27, p. 111]). We call a positive solution $(t, s)$ of (2.10) *regular* if $(t, s)$ belongs to one of these three classes. However, it is possible for a solution $(t, s)$ not to be regular. In general, we do not know in advance how many classes of solutions we have, except for some special type of $b$.

*Remark 2.4.10* An example having non-regular solutions can be found in the case of $r = 2q^2$, where $q$ is a positive integer. Then (2.10) has two more classes of solutions belonging to

$$(t_0', s_0') = (2q^3 + q, \pm q).$$

Our goal is to prove the following theorem.

**Theorem 2.2** *Let $(t, s)$ be a regular solution of (2.10) and let $c = s^2 + 1$. Then, the system of Diophantine equations*

$$y^2 - bx^2 = r^2,$$
$$z^2 - cx^2 = s^2$$

*has only trivial solutions $(x, y, z) = (0, \pm r, \pm s)$. Furthermore, if $r = 2q^2$ for some positive integer $q$, then the same is true for any positive solution $(t, s)$ of (2.10) belonging to the same class as one of $(2q^3 + q, \pm q)$.*

By [23, Theorem 1] we have that $c < 11b^6$ (using the hyper-geometric method), hence the above-mentioned result of He and Togbé shows that it is enough to prove Theorem 2.2 for $c = c_i$ with $2 \leq i \leq 7$, where

$$
\begin{aligned}
c_2 &= 4r^4 + 1,\\
c_3 &= (4r^3 - 4r^2 + 3r - 1)^2 + 1,\\
c_4 &= (4r^3 + 4r^2 + 3r + 1)^2 + 1,\\
c_5 &= (8r^4 + 4r^2)^2 + 1,\\
c_6 &= (16r^5 - 16r^4 + 20r^3 - 12r^2 + 5r - 1)^2 + 1,\\
c_7 &= (16r^5 + 16r^4 + 20r^3 + 12r^2 + 5r + 1)^2 + 1
\end{aligned}
$$

(see [27, p. 111]), and in the case of $r = 2q^2$, additionally for $c = c_i'$ with $1 \le i \le 5$, where

$$
\begin{aligned}
c_1' &= (4q^3 - q)^2 + 1,\\
c_2' &= (16q^5 + 4q^3 + q)^2 + 1,\\
c_3' &= (64q^7 - 16q^5 + 8q^3 - q)^2 + 1,\\
c_4' &= (256q^9 + 64q^7 + 48q^5 + 8q^3 + q)^2 + 1,\\
c_5' &= (1024q^{11} - 256q^9 + 256q^7 - 48q^5 + 12q^3 - q)^2 + 1.
\end{aligned}
$$

It is easy to see that Theorem 2.2 immediately implies

**Corollary 2.4.11** *Let $(t, s)$ be either a regular solution of (2.10) or, in the case of $r = 2q^2$ for some positive integer $q$, a regular solution or a positive solution of (2.10) belonging to the same class as one of $(2q^3 + q, \pm q)$. Let $c = s^2 + 1$. Then, the $D(-1)$-triple $\{1, b, c\}$ cannot be extended to a $D(-1)$-quadruple.*

It was proven in [27, p. 111], that if $r$ is prime, then (2.10) has only regular solutions. We can generalize this to find that, if $r = p^k$ or $2p^k$ for an odd prime $p$ and a positive integer $k$, then (2.10) has only regular solutions, except in the case of $r = 2p^k$ with $k$ even. In the latter case, there are exactly five classes of solutions. Furthermore, if $b = p$ or $2p^k$, then (2.10) has only regular solutions ($b = p^k$ can occur only if $k = 1$, since $b = r^2 + 1$; [35]). Hence, we get another corollary of the Theorem 2.2.

**Corollary 2.4.12** *Let $r$ be a positive integer and let $b = r^2 + 1$. Suppose that one of the following assumptions holds for an odd prime $p$ and a positive integer $k$:*
(i) $b = p$; (ii) $b = 2p^k$; (iii) $r = p^k$; (iv) $r = 2p^k$.
*Then, the system of Diophantine equations*

$$
\begin{aligned}
y^2 - bx^2 &= r^2,\\
z^2 - cx^2 &= s^2
\end{aligned}
$$

*has only the trivial solutions $(x, y, z) = (0, \pm r, \pm s)$, where $(t, s)$ is a positive solution of (2.10) and $c = s^2 + 1$. Moreover, the $D(-1)$-pair $\{1, b\}$ cannot be extended to a $D(-1)$-quadruple.*

**The System of Pellian Equations**

Let $\{1, b, c\}$ be a $D(-1)$-triple with $b < c$, and let $r, s, t$ be positive integers defined by $b - 1 = r^2$, $c - 1 = s^2$, $bc - 1 = t^2$. Suppose that we can extend the triple $\{1, b, c\}$ to a $D(-1)$-quadruple with element $d$. Then, there exist integers $x$, $y$, $z$ such that

$$d - 1 = x^2, \quad bd - 1 = y^2, \quad cd - 1 = z^2.$$

Eliminating $d$, we obtain the system of simultaneous Diophantine equations

$$z^2 - cx^2 = s^2, \tag{2.11}$$
$$bz^2 - cy^2 = c - b, \tag{2.12}$$
$$y^2 - bx^2 = r^2. \tag{2.13}$$

We may assume that $c < 11b^6$ (according to Theorem 1, [23]). The positive solutions $(z, x)$ of Eq. (2.11) and $(z, y)$ of Eq. (2.12) are respectively given by

$$z + x\sqrt{c} = s(s + \sqrt{c})^{2m} \qquad (m \geq 0),$$
$$z\sqrt{b} + y\sqrt{c} = (s\sqrt{b} \pm r\sqrt{c})(t + \sqrt{bc})^{2n} \qquad (n \geq 0)$$

(see Lemmas 1 and 5 in [23]). Using that $y$ is a common solution of Eqs. (2.12) and (2.13), He and Togbé proved that the positive solutions $(y, x)$ of Eq. (2.13) are given by

$$y + x\sqrt{b} = r(r + \sqrt{b})^{2l}, \qquad l \geq 0,$$

and, moreover, they proved the following proposition.

**Proposition 2.4.13** ([29, Proposition 2.1]) *The $D(-1)$-triple $\{1, b, c\}$ can be extended to a $D(-1)$-quadruple if and only if the system of simultaneous Pellian equations*

$$(z/s)^2 - c(x/s)^2 = 1,$$
$$(y/r)^2 - b(x/r)^2 = 1$$

*has a positive integer solution $(x, y, z)$.*

Proposition 2.4.13 implies that we can write $x = sv_m = ru_l$, where

$$v_m = \frac{\alpha^{2m} - \alpha^{-2m}}{2\sqrt{c}} \quad \text{and} \quad u_l = \frac{\beta^{2l} - \beta^{-2l}}{2\sqrt{b}}$$

are positive solutions of the Pellian equations $Z^2 - cX^2 = 1$ and $Y^2 - bW^2 = 1$, respectively, where $\alpha = s + \sqrt{c}$ and $\beta = r + \sqrt{b}$. We have mentioned before that we cannot always use linear forms in two logarithms. More precisely, for our approach

$\alpha$ and $\beta$ should be near to each other or one of them has to be near to a power of the other one.

**Gap Principles**

We next consider the extension of $D(-1)$-triples $\{1, b, c\}$ with

$$c = c_2, c_3, c_4, c_5, c_6, c_7, c_1', c_2', c_3', c_4', c_5'$$

from above. We shall establish gap principles for these special cases.

Let us define the linear form $\Lambda$ in three logarithms

$$\Lambda = 2m \log \alpha - 2l \log \beta + \log \frac{s\sqrt{b}}{r\sqrt{c}}.$$

The proofs of the following lemmas can be found in [29]; the results rely on Baker's theory of linear forms in logarithms.

**Lemma 2.4.14** ([29, Lemma 3.1]) *If $sv_m = ru_l$ has a solution with $m \neq 0$, then*

$$0 < \Lambda < \frac{b}{b-1} \cdot \beta^{-4l}.$$

**Lemma 2.4.15** ([29, Lemma 3.3]) *If $sv_m = ru_l$ has a solution with $m \neq 0$, then $m \log \alpha < l \log \beta$.*

The proofs of the following lemmas can be found in [26]; these results are based on the property that an algebraic number $\alpha$ is close to some power of $\beta$.

**Lemma 2.4.16** *Let $c = c_2 = 4r^4 + 1$. If the equation $sv_m = ru_l$ has a solution with $m \neq 0$, then*

$$m > \frac{\Delta}{2} \cdot \alpha \log \beta,$$

*where $\Delta$ is a positive integer.*

**Lemma 2.4.17** *Let $c = c_3 = (4r^3 - 4r^2 + 3r - 1)^2 + 1$ or $c = c_4 = (4r^3 + 4r^2 + 3r + 1)^2 + 1$. If the equation $sv_m = ru_l$ has a solution with $m \neq 0$, then*

$$m > \frac{3\Delta - 1}{3} \cdot \frac{8r}{9} \log \beta,$$

*where $\Delta$ is a positive integer.*

**Lemma 2.4.18** *Let $c = c_1' = (4q^3 - q)^2 + 1$. If the equation $sv_m = ru_l$ has a solution with $m \neq 0$, then*

$$m > \frac{\Delta}{6} \cdot \alpha \log \beta,$$

*where $\Delta$ is a positive integer.*

Similar lemmas for other choices of $c$ can be obtained. The following table contains information how to choose $\Delta$ and a lower bound for $m$.

| $c$ | $\Delta$ | a lower bound for $m$ |
|---|---|---|
| $c_5$ | $4m-l$ | $m > \Delta \cdot \frac{8r^4}{4r^2+1} \log\beta$ |
| $c_6$ | $5m-l$ | $m > \frac{5\Delta-1}{5} \cdot \frac{32r}{33} \log\beta$ |
| $c_7$ | $l-5m$ | $m > \frac{5\Delta-1}{5} \cdot \frac{32r}{33} \log\beta$ |
| $c_2'$ | $2l-5m$ | $m > \frac{10\Delta-4}{5} \cdot q^2 \log\beta$ |
| $c_3'$ | $7m-2l$ | $m > \frac{3\Delta}{2} \cdot q^2 \log\beta$ |
| $c_4'$ | $2l-9m$ | $m > \frac{18\Delta-4}{9} \cdot q^2 \log\beta$ |
| $c_5'$ | $11m-2l$ | $m > \frac{3\Delta}{2} \cdot q^2 \log\beta$ |

### Linear Forms in Two Logarithms

Next we shall apply the following result due to Laurent,[29] M. Mignotte[30] and Y. Nesterenko[31] to our linear form $\Lambda$.

**Lemma 2.4.19** ([33, Corollary 2]) *Let $\gamma_1$ and $\gamma_2$ be multiplicatively independent, positive algebraic numbers, $b_1, b_2 \in \mathbb{Z}$ and*

$$\Lambda = b_1 \log\gamma_1 + b_2 \log\gamma_2.$$

*Let $D := [\mathbb{Q}(\gamma_1, \gamma_2) : \mathbb{Q}]$, for $i = 1, 2$ let*

$$h_i \geq \max\left\{h(\gamma_i), \frac{|\log\gamma_i|}{D}, \frac{1}{D}\right\},$$

*where $h(\gamma)$ is the absolute logarithmic height of $\gamma$, and*

$$b' \geq \frac{|b_1|}{Dh_2} + \frac{|b_2|}{Dh_1}.$$

*If $\Lambda \neq 0$, then*

$$\log|\Lambda| \geq -24.34 \cdot D^4 \left(\max\left\{\log b' + 0.14, \frac{21}{D}, \frac{1}{2}\right\}\right)^2 h_1 h_2.$$

[29] Michel Laurent, a French mathematician.

[30] Maurice Mignotte, a French mathematician.

[31] Yuri Valentinovich Nesterenko (1946), a Soviet and Russian mathematician.

This lemma has also been used by He and Togbé in [29]. We are dealing with the same linear form, but only with a different $c$. Using the same method to transform our form to a linear form in two logarithms, then applying Lemma 2.4.19 for $c = c_2, c_3, \ldots, c_7, c_1', \ldots, c_5'$, and combining the lower bound for $|\Lambda|$ together with the gap principles, we can prove Theorem 2.2 for large values of $r$. That $\gamma_1$ and $\gamma_2$ are multiplicatively independent follows from the fact that $\alpha$ and $\beta$ are multiplicatively independent algebraic units and $\frac{r\sqrt{c}}{s\sqrt{b}}$ is not an algebraic unit.

As an example we consider the case $c = c_2 = 4r^4 + 1$. We can write

$$\Lambda = 2m \log\left(\frac{\alpha}{\beta^2}\right) - \log\left(\beta^{-2\Delta} \cdot \frac{r\sqrt{c}}{s\sqrt{r^2+1}}\right),$$

where $\Delta = 2m - l$ is defined as in Lemma 2.4.16. In the notation of Lemma 2.4.19 we have

$$D = 4,\ b_1 = 2m,\ b_2 = -1,\ \gamma_1 = \frac{\alpha}{\beta^2},\ \gamma_2 = \beta^{-2\Delta} \cdot \frac{r\sqrt{c}}{s\sqrt{b}}.$$

Furthermore,

$$h(\gamma_1) \le h\left(\frac{\alpha}{\beta}\right) + h(\beta) = \frac{1}{2}\log\alpha + \frac{1}{2}\log\beta < \log\alpha,$$

hence, for $h_1$, we can take $h_1 = \log\alpha$. Moreover,

$$h\left(\frac{r\sqrt{c}}{s\sqrt{b}}\right) = \frac{1}{2}\log((c-1)b) < \frac{1}{2}\log\beta^6 = 3\log\beta,$$

which yields

$$h(\gamma_2) < (\Delta + 3)\log\beta =: h_2.$$

For $r \ge 10$, we find

$$\frac{|b_2|}{Dh_1} = \frac{1}{4\log\alpha} < 0.042,$$

and then

$$b' = \frac{m}{2(\Delta+3)\log\beta} + 0.042.$$

Now Lemma 2.4.16 implies

$$\frac{m}{2(\Delta+3)\log\beta} > \frac{\Delta}{4(\Delta+3)} \cdot \alpha \ge \frac{\alpha}{16} > 169$$

for $r \ge 26$. Thus, for $r \ge 26$, we get $\log b' + 0.14 > \frac{21}{D}$ and applying Lemma 2.4.19 we conclude

$$\log|\Lambda| \geq -24.34 \cdot 4^4 \cdot (\log b' + 0.14)^2 \cdot \log\alpha \cdot (\Delta + 3)\log\beta.$$

On the other hand, Lemma 2.4.14 yields

$$\log|\Lambda| < 0.002 - 4l\log\beta.$$

Combining these lower and upper bounds for $\Lambda$, we obtain

$$\frac{l}{\log\alpha} < \frac{0.002}{4\log\alpha\log\beta} + 24.34 \cdot 64(\log b' + 0.14)^2(\Delta + 3).$$

Furthermore, $m\log\alpha < l\log\beta$ gives us

$$\frac{m}{2(\Delta+3)\log\beta} < 0.0001 + 24.34 \cdot 32(\log b' + 0.14)^2$$

and finally

$$b' < 0.042 + 778.88(\log b' + 0.14)^2,$$

which implies $b' < 106996$. It furthermore gives $m < 213992(\Delta + 3)\log\beta$ and

$$\alpha < \frac{2m}{\Delta\log\beta} < 427983 \cdot \frac{\Delta+3}{\Delta} < 1.72 \cdot 10^6,$$

from which we deduce $r < 656$. Thus, we have proved Theorem 2.2 for $c = c_2$ and $r \geq 656$.

The cases $c = c_3, c_4 = (4r^3 \mp 4r^2 + 3r \mp 1)^2 + 1$ are described in details in [26]. The upper bounds for $r$ and $q$ in the remaining cases are given in the following table.

| $c$ | an upper bound for $r$ or $q$ |
|---|---|
| $c_3$ | $r < 1.81 \cdot 10^6$ |
| $c_4$ | $r < 1.81 \cdot 10^6$ |
| $c_5$ | $r < 802$ |
| $c_6$ | $r < 1.94 \cdot 10^6$ |
| $c_7$ | $r < 1.94 \cdot 10^6$ |
| $c_2'$ | $q < 846$ |
| $c_3'$ | $q < 846$ |
| $c_4'$ | $q < 949$ |
| $c_5'$ | $q < 1000$ |

**The Reduction Method and the Proof of Theorem 2.2**

We have just proven Theorem 2.2 for large parameters $r$ and $q$. We are left to consider the cases of small $r$ and $q$. Using Baker–Davenport reduction, it turns out that in all remaining cases there is no extension of the triple $\{1, b, c\}$ to a quadruple $\{1, b, c, d\}$.

Some useful results from [23] can be used. We know that, if we have the extension of our triple with the element $d$, then $cd - 1 = z^2$, where $z = V_m = W_n$ such that

$$V_0 = s,\ V_1 = (2c-1)s,\ V_{m+2} = (4c-2)V_{m+1} - V_m$$

and

$$W_0 = s,\ W_1 = (2bc-1)s \pm 2rtc,\ W_{n+2} = (4bc-2)W_{n+1} - W_n.$$

We use the following lemmas.

**Lemma 2.4.20** ([23, Lemma 11]) *If $V_m = W_n$, $n \neq 0$, then*

$$0 < 2n\log(t+\sqrt{bc}) - 2m\log(s+\sqrt{c}) + \log\frac{s\sqrt{b} \pm r\sqrt{c}}{2\sqrt{b}} < (3.96bc)^{-n+1}.$$

From the proofs of Propositions 2, 3, 4 in [23] we know that $n < 10^{20}$ in all cases. Applying Baker–Davenport reduction with

$$\kappa = \frac{\log(t+\sqrt{bc})}{\log(s+\sqrt{c})},\quad \mu = \frac{\log\frac{s\sqrt{b}\pm r\sqrt{c}}{2\sqrt{b}}}{2\log(s+\sqrt{c})},\quad A = \frac{3.96bc}{2\log(s+\sqrt{c})},\quad B = 3.96bc$$

and $N = 10^{21}$ with any choice of $r$ and $c$ left, we get after two steps that $n < 2$. Here, one may also use that $D(-1)$-triples $\{1, b, c\}$ cannot be extended to a quadruple for $r \leq 143000$, which was verified by computer. Hence, in some cases one can avoid to use reduction at all.

We are still left to deal with the cases of small indices $m$ and $n$ in the equation $z = V_m = W_n$. From [21] we know that $n \geq 3$; otherwise we have only the trivial solution (corresponding with an extension with $d = 1$, which is no real extension, because we ask for elements in $D(n)$-$m$-tuple to be distinct).

The following lemma, which was proved in [26], and which examines the fundamental solutions of (2.10) in the cases of $b = p,\ 2p^k$ and $r = p^k,\ 2p^k$, together with Theorem 2.2 implies Corollary 2.4.12.

**Lemma 2.4.21**

*(1) If $b = p$ or $2p^k$ for an odd prime $p$ and a positive integer $k$, then Diophantine Equation (2.10) has only regular solutions.*

*(2) If $r = p^k$ or $2p^k$ for an odd prime $p$ and a positive integer $k$, then Diophantine Equation (2.10) has only regular solutions, except in the case of $r = 2p^{2i}$ with $i$ a positive integer, where it in addition has exactly two classes of solutions belonging to $(2p^{3i} + p^i, \pm p^i)$.*

### 2.4.6 Pure Powers in Binary Recurrent Sequences

The Lucas numbers $(L_n)_{n\geq 0}$ are given by

$$L_0 = 2,\ L_1 = 1,\ \ldots,\ L_{n+2} = L_{n+1} + L_n,\ n \geq 0.$$

Recall that Fibonacci numbers $(F_n)$ as well as Lucas numbers $(L_n)$ are defined by

$$F_n = \frac{\alpha^n - \beta^n}{\sqrt{5}},\ L_n = \alpha^n + \beta^n,\ \alpha = \frac{1+\sqrt{5}}{2},\ \beta = \frac{1-\sqrt{5}}{2},$$

respectively. Now suppose

$$F_n = y^p$$

is a pure power. Since

$$\alpha^n - \sqrt{5}y^p = O(\alpha^{-n}),$$

we find

$$\Lambda = n\log\alpha - p\log y - \log\sqrt{5} = O(\alpha^{-2n}) = O(y^{-2p}).$$

There exist integers $k, r$ such that $n = kp + r$ with $|r| \leq \frac{p}{2}$, hence we have

$$\Lambda = p\log\left(\frac{\alpha^k}{y}\right) + r\log\alpha - \log\sqrt{5}$$

which is a linear form in three logarithms. If we apply Matveev's Theorem 2.2.14, we get

$$\log|\Lambda| \geq -c^*\log y\log p.$$

Comparing both estimates of $|\Lambda|$, we see that the exponent $p$ is bounded. Matveev's Theorem 2.2.14 implies $p < 3\cdot 10^{13}$, but a special estimate for linear forms in three logarithms implies the sharper upper bound is $p < 2\cdot 10^8$ which is suitable for computer calculations.

For Lucas numbers a similar study leads to a linear form in two logarithms and $p < 300$ provided that $L_n = y^p$. By this reasoning, it can be proved [10] that all perfect powers in the Fibonacci and Lucas sequences are

$$F_0 = 0,\ F_1 = F_2 = 1,\ F_6 = 8 = 2^3,\ F_{12} = 144 = 12^2;$$

$$L_1 = 1,\ L_3 = 4 = 2^2.$$

Using this method we can solve many similar problems, for example, all Pell numbers for which $P_n + 4$ is a perfect square are given by $P_0 = 0$, $P_3 = 5$ and $P_4 = 12$. Recall that the Pell numbers are given by the recursion

$$P_0 = 0,\ P_1 = 1,\ \ldots,\ P_{n+2} = 2P_{n+1} + P_n,\ n \geq 0.$$

### 2.4.7 Lucas Numbers and the Biggest Prime Factor

Next we are interested in finding all Lucas numbers for which the biggest prime factor is less than or equal to 5.

We may express Lucas numbers as

$$L_n = \left(\frac{1+\sqrt{5}}{2}\right)^n + \left(\frac{1-\sqrt{5}}{2}\right)^n, \quad n \in \mathbb{N}.$$

For Lucas numbers the length of the period of the sequence $(L_n \mod 5)$ is equal to 4 with the cycle $\{1, 3, 4, 2\}$; therefore 5 can never be a divisor of any Lucas number. We want to find all Lucas numbers such that

$$2^k 3^l = \left(\frac{1+\sqrt{5}}{2}\right)^n + \left(\frac{1-\sqrt{5}}{2}\right)^n, \quad n, k, l, m \in \mathbb{N}.$$

Let $\alpha = \frac{1+\sqrt{5}}{2}$, so the previous expression can be rewritten as

$$2^k 3^l = \alpha^n - \alpha^{-n}, \quad k, l, n \in \mathbb{N}.$$

Thus the corresponding linear form in logarithms is

$$\Lambda = 2n \log \alpha - k \log 2 - l \log 3.$$

Now, applying Matveev's Theorem 2.2.14, we have $n = 3$, $D = 2$, and

$$A_1 \geq h'(2) = \max\{2 \log 2, |\log 2|, 0.16\} = 1.38 < 2,$$

$$A_2 \geq h'(3) = \max\{2 \log 3, |\log 3|, 0.16\} = 2.19 < 3,$$

$$A_3 \geq h'\left(\frac{1+\sqrt{5}}{2}\right) = \max\{2 \log \frac{1+\sqrt{5}}{2}, \left|\log \frac{1+\sqrt{5}}{2}\right|, 0.16\} = 0.48 < 1.$$

We get

$$\log |\Lambda| \geq -7.28022 \cdot 10^{15}(1 + \log 2n).$$

After finding the upper bound from the expression

$$\frac{L_n}{\alpha^n} - 1 = -\alpha^{-2n},$$

and

$$\log |\Lambda| < -2n \log \frac{1+\sqrt{5}}{2},$$

we find that $n < 3.17654 \cdot 10^{17}$. After applying Baker–Davenport reduction, we get $n < 14$, so we may conclude that the Lucas numbers for which the biggest prime factors are less or equal to 5 are

$$L_0 = 2, \ \ L_2 = 3, \ \ L_4 = 4 = 2^2, \ \ L_6 = 18 = 2 \cdot 3^2.$$

### 2.4.8 Pillai's Equation

Given positive integers $a > b > 1$, Pillai[32] [42] proved that there are only finitely many integers $c \neq 0$ admitting more than one representation of the form

$$c = a^x - b^y$$

in nonnegative integers $x, y$. In particular, the equation

$$a^x - b^y = a^{x_1} - b^{y_1}, \ \ \text{with } (x, y) \neq (x_1, y_1) \tag{2.14}$$

has only finitely many integer solutions. We shall apply the technique of lower bounds for linear forms in logarithms of algebraic numbers to find all the solutions for

$$(a, b) = (3, 2).$$

**Proposition 2.4.22** *The only nontrivial solutions of Eq. (2.14) with* $(a, b) = (3, 2)$ *are*

$$3^1 - 2^2 = 3^0 - 2^1, \ \ 3^2 - 2^4 = 3^0 - 2^3, \ \ 3^2 - 2^3 = 3^1 - 2^1,$$

$$3^3 - 2^5 = 3^1 - 2^3, \ \ 3^5 - 2^8 = 3^1 - 2^4.$$

*Proof* The initial equation can be rewritten as

$$3^x - 3^{x_1} = 2^y - 2^{y_1}.$$

After relabeling the variables, we may assume that $x > x_1$. Consequently, $y > y_1$. Since

$$2 \cdot 3^{x-1} = 3^x - 3^{x-1} \leq 3^x - 3^{x_1} = 2^y - 2^{y_1} < 2^y,$$

we get $x < y$. Let $B = y$. Now,

$$3^{x_1} \mid (2^y - 2^{y_1}) = 2^{y_1}(2^{y-y_1} - 1).$$

We observe that $3^m \mid (2^n - 1)$ if and only if $2 \cdot 3^{m-1} \mid n$. In particular,

[32] Subbayya Sivasankaranarayana Pillai (1901–1950), an Indian mathematician.

$$x_1 \leq 1 + \frac{\log((y - y_1)/2)}{\log 3} \leq \frac{\log(3B/2)}{\log 3}, \tag{2.15}$$

therefore,

$$3^{x_1} < \frac{3B}{2} < 2B.$$

Similarly,

$$2^{y_1} \mid (3^x - 3^{x_1}) = 3^{x_1}(3^{x-x_1} - 1).$$

Analogously, if $m \geq 3$, then $2^m \mid (3^n - 1)$ if and only if $2^{m-2} \mid n$. Thus,

$$y_1 \leq 2 + \frac{\log(x - x_1)}{\log 2} < \frac{\log(4B)}{\log 2}, \tag{2.16}$$

and therefore

$$2^{y_1} \leq 4B.$$

The original equation may be rewritten in such a way that the *large parts* are on one side and the *small parts* are on the other, namely

$$|3^x - 2^y| = |3^{x_1} - 2^{y_1}| < 2B,$$

which in turn gives an inequality of the form

$$|1 - 3^x 2^{-y}| < \frac{2B}{2^B}.$$

Thus the linear form $\Lambda$ to study is given by

$$\Lambda = x \log 3 - y \log 2.$$

If $\Lambda > 0$, then

$$e^{\Lambda} - 1 < \frac{2B}{2^B}.$$

If $\Lambda < 0$, assuming that $B > 10$, we find $\frac{2B}{2^B} < \frac{1}{2}$ and therefore, $|1 - e^{\Lambda}| < \frac{1}{2}$, which implies $e^{|\Lambda|} < 2$. In particular,

$$|\Lambda| < \frac{4B}{2^B}. \tag{2.17}$$

The last inequality holds independent of the sign of $\Lambda$. We observe that $\Lambda \neq 0$, since in the opposite case, we would get $3^x = 2^y$ which, by unique factorization, implies $x = y = 0$, a contradiction. Put

$$\alpha_1 = 2,\ \alpha_2 = 3,\ b_1 = y,\ b_2 = x,\ B = y,\ A_1 = 1,\ A_2 = \log 3$$

and

$$b' = \frac{y}{\log 3} + x < B\left(\frac{1}{\log 3} + 1\right) < 2B.$$

Since $\log 2$ and $\log 3$ are linearly independent, real and positive, Lemma 2.4.19 yields the estimate

$$\log|\Lambda| > -23.34(\max\{\log(2B) + 0.14, 21\})^2 \cdot \log 3.$$

Comparing the last inequality with (2.17), we get

$$B\log 2 - \log(4B) < 23.34 \cdot 3 \cdot (\max\{\log(2B) + 0.14, 21\})^2.$$

If the above maximum is 21, we get

$$B\log 2 - \log(4B) < 25.7 \cdot 21^2,$$

hence $B < 17000$. Otherwise, we have

$$B\log 2 - \log(4B) < 25.7(\log(2B) + 0.14)^2,$$

yielding $B < 2900$. Thus, we consider the inequality $B < 17000$. From (2.15) and (2.16), we get $x_1 \leq 9$ and $y_1 \leq 16$. Hence,

$$x - 1 \leq (y-1)\frac{\log 2}{\log 3} < B\frac{\log 2}{\log 3} < 11000.$$

Now, we reduce this bound. Suppose that $B \geq 30$, then we get

$$3^x > 3^x - 3^{x_1} = 2^y - 2^{y_1} \geq 2^{B-1} \geq 2^{29},$$

which implies $x \geq 19$. We check that the congruence

$$3^x - 3^{x_1} - 2^{y_1} \equiv 0 \pmod{2^{30}}$$

does not hold for any triple $(x, x_1, y_1)$ with $11 \leq x \leq 1100$, $0 \leq x_1 \leq 9$, and $0 \leq y_1 \leq 16$. This gives $B \leq 29$. Since $3^{x-1} < 2^{y-1} \leq 2^{28}$, we get $x \leq 18$. Now, it is easy to show that there are no solutions beyond those in the statement of the proposition. For details see [36].

### 2.4.9 The Diophantine Equation $ax^n - by^n = c$

We consider

$$ax^n - by^n = c,$$

where $a, b$ are strictly positive and $x, y, n$ are unknowns. If for some exponent $n$ there exists a solution $(x, y)$ with $|y| > 1$, then

$$\Lambda = \log\left|\frac{a}{b}\right| - n\log\left|\frac{x}{y}\right| = O(|y|^{-n}).$$

In the other direction, Matveev's Theorem 2.2.14 implies

$$\log|\Lambda| \geq -c_* \log|y| \log n.$$

Comparing both estimates, we get $n < c_{**}$, where $c_{**}$ depends only on $a, b, c$.

The following theorems give us explicit results.

**Theorem 2.4.23** (Mignotte, [40]) *Assume that the exponential Diophantine inequality*

$$|ax^n - by^n| \leq c, \ \ a, b, c \in \mathbb{Z}_+, \ \ a \neq b$$

*has a solution in positive integers $x, y$ with $\max\{x, y\} > 1$. Then*

$$n \leq \max\left\{3\log(1.5|c/b|), \ 7400\frac{\log A}{\log(1 + (\log A)/\log|a/b|)}\right\}, \ \ A = \max\{a, b, 3\}.$$

Bennett obtained the following definitive result for $c = \pm 1$.

**Theorem 2.4.24** (Bennett, [8]) *For $n \geq 3$, the equation*

$$|ax^n - by^n| = 1, \ \ a, b \in \mathbb{Z}_+$$

*has at most one solution in positive integers $x, y$.*

For more examples of applications of linear forms in logarithms we refer to [25, 36] which are highly recommended for this purpose.

**Acknowledgements** The first author, Sanda Bujačić, would like to express her sincere gratitude to Prof. Jörn Steuding for organizing summer school *Diophantine Analysis* in Würzburg in 2014 and for inviting her to organize the course *Linear forms in logarithms*. She thanks him for his patience, kindness and the motivation he provided to bring this notes to publishing.

Besides Prof. Steuding, she would like to thank her PhD supervisor, Prof. Andrej Dujella, for his insightful comments during her PhD study, great advices in literature that was used for creating these lecture notes and his constant encouragement. She would also like to thank her co-author, Prof. Alan Filipin, for his kind assistance, guidance, help and excellent cooperation.

Last but not the least, she would like to thank her family: parents, sister and boyfriend for supporting her throughout writing, teaching and her life in general.

Both authors are supported by Croatian Science Foundation grant number 6422.

## References


1. A. Baker, Linear forms in the logarithms of algebraic numbers, I. Mathematika J. Pure Appl. Math. **13**, 204–216 (1966)
2. A. Baker, Linear forms in the logarithms of algebraic numbers, II. Mathematika.J. Pure Appl. Math. **14**, 102–107 (1967)
3. A. Baker, Linear forms in the logarithms of algebraic numbers, III. Mathematika J. Pure Appl. Math. **14**, 220–228 (1967)
4. A. Baker, *Transcendental Number Theory* (Cambridge University Press, Cambridge, 1975)
5. A. Baker, H. Davenport, The equations $3x^2 - 2 = y^2$ and $8x^2 - 7 = z^2$. Quart. J. Math. Oxford Ser. **20**(2), 129–137 (1969)
6. A. Baker, G. Wüstholz, Logarithmic forms and group varieties. J. für die Reine und Angewandte Mathematik **442**, 19–62 (1993)
7. M. Bennett, On some exponential Diophantine equations of S. S. Pillai. Canad. J. Math. **53**, 897–922 (2001)
8. M. Bennett, Rational approximation to algebraic numbers of small height: the Diophantine equation $|ax^n - by^n| = 1$. J. Reine Angew. Math. **535**, 1–49 (2001)
9. E. Borel, Contribution a l'analyse arithmétique du continu. J. Math. Pures Appl. **9**, 329–375 (1903)
10. Y. Bugeaud, M. Mignotte, S. Siksek, Classical and modular approaches to exponential Diophantine equations I. Fibonacci and Lucas perfect powers. Ann. Math. **163**(3), 969–1018 (2006)
11. E.B. Burger, R. Tubbs, *Making Transcendence Transparent: An Intuitive Approach to Classical Transcendental Number Theory* (Springer, New York, 2004)
12. J.W.S. Cassels, *An Introduction to Diophantine Approximation, Cambridge Tracts in Mathematics and Mathematical Physics*, vol. 45 (Cambridge University Press, Cambridge, 1957)
13. H. Cohen, *Number Theory, Volume I: Tools and Diophantine Equations* (Springer, Berlin, 2007)
14. H. Cohen, *Number Theory, Volume II: Analytic And Modern Tools* (Springer, Berlin, 2007)
15. A. Dujella, The problem of the extension of a parametric family of Diophantine triples. Publ. Math. Debrecen **51**, 311–322 (1997)
16. A. Dujella, On the exceptional set in the problem of Diophantus and Davenport. Appl. Fibonacci Numbers **7**, 69–76 (1998)
17. A. Dujella, A proof of the Hoggatt–Bergum conjecture. Proc. Amer. Math. Soc. **127**, 1999–2005 (1999)
18. A. Dujella, There are only finitely many Diophantine quintuples. J. Reine Angew. Math. **566**, 183–214 (2004)
19. A. Dujella, Diofantske jednadžbe, course notes, Zagreb (2006/2007)
20. A. Dujella, Diofantske aproksimacije i primjene, course notes, Zagreb (2011/2012)
21. A. Dujella, C. Fuchs, Complete solution of a problem of Diophantus and Euler. J. London Math. Soc. **71**, 33–52 (2005)
22. A. Dujella, A. Pethő, Generalization of a theorem of Baker and Davenport. Quart. J. Math. Oxford Ser. (2) **49**, 291–306 (1998)
23. A. Dujella, A. Filipin, C. Fuchs, Effective solution of the $D(-1)$- quadruple conjecture. Acta Arith. **128**, 319–338 (2007)
24. C. Elsholtz, A. Filipin, Y. Fujita, On Diophantine quintuples and $D(-1)$ -quadruples. Monatsh. Math. **175**(2), 227–239 (2014)
25. A. Filipin, Linearne forme u logaritmima i diofantska analiza, course notes, Zagreb (2010)
26. A. Filipin, Y. Fujita, M. Mignotte, The non-extendibility of some parametric families of D(-1)-triples. Q. J. Math. **63**(3), 605–621 (2012)
27. Y. Fujita, The extensibility of $D(-1)$ -triples $\{1, b, c\}$. Publ. Math. Debrecen **70**, 103–117 (2007)
28. A.O. Gelfond, *Transcendental and Algebraic Numbers*, translated by Leo F. (Dover Publications, Boron, 1960)

29. B. He, A. Togbé, On the $D(-1)$ -triple $\{1, k^2+1, k^2+2k+2\}$ and its unique $D(1)$ -extension. J. Number Theory **131**, 120–137 (2011)
30. M. Hindry, J.H. Silverman, *Diophantine Geometry: An Introduction* (Springer, New York, 2000)
31. A. Hurwitz, Ueber die angenäherte Darstellung der Irrationalzahlen durch rationale Brüche (On the approximation of irrational numbers by rational numbers). Mathematische Annalen (in German) **39**(2), 279–284 (1891)
32. S. Lang, *Introduction to Diophantine Approximations* (Addison-Wesley, Reading, 1966)
33. M. Laurent, M. Mignotte, Yu. Nesterenko, Formes linéaires en deux logarithmes et déterminants d'interpolation. J. Number Theory **55**, 285–321 (1995)
34. F. Lindemann, Über die Zahl $\pi$. Mathematische Annalen **20**, 213–225 (1882)
35. V.A. Lebesgue, Sur l'impossbilité en nombres entiers de l'équation $x^m = y^2 + 1$. Nouv. Ann. Math. **9**, 178–181 (1850)
36. F. Luca, *Diophantine Equations*, lecture notes for Winter School on Explicit Methods in Number Theory (Debrecen, Hungary, 2009)
37. K. Mahler, Zur approximation der exponentialfunktion und des logarithmus, I, II. J. reine angew. Math. **166**, 118–136, 136–150 (1932)
38. K. Mahler, Arithmetische Eigenschaften einer Klasse von Dezimalbruchen. Proc. Kon. Nederlansche Akad. Wetensch. **40**, 421–428 (1937)
39. E. M. Matveev, An explicit lower bound for a homogeneous rational linear form in logarithms of algebraic numbers I, II, Izvestiya: Mathematics, **62**(4), 723–772 (1998); **64**(6), 125–180 (2000)
40. M. Mignotte, A note on the equation $ax^n - by^n = c$. Acta Arith. **75**, 287–295 (1996)
41. O. Perron, *Die Lehre von den Kettenbrüchen* (Chelsea, New York, 1950)
42. S. S. Pillai, *On* $a^x - b^y = c$, J. Indian Math. Soc. (N.S.) (2), 119–122 (1936)
43. K.F. Roth, Rational approximations to algebraic numbers. Mathematika **2**, 1–20 (1955)
44. J.D. Sally, P.J. Sally Jr., *Roots to Research: A Vertical Development of Mathematical Problems* (American Mathematical Society, Providence, 2007)
45. W.M. Schmidt, *Diophantine Approximation*, vol. 785, Lecture Notes in Mathematics (Springer, Berlin, 1980)
46. J. Steuding, *Diophantine Analysis (Discrete Mathematics and Its Applications)* (Chapman& Hall/CRC, Taylor & Francis Group, Boca Raton, 2005)
47. A. Thue, Über Annäherungswerte algebraischer Zahlen. J. Reine und Angew. Math. **135**, 284–305 (1909)
48. T. Vahlen, Über Näherungswerthe und Kettenbr üche, J. Reine Angew. Math. (Crelle), **115**(3),221–233 (1895)