Diophantine m-tuples

Zrinka Franušić

Istanbul, June, 2025

Contents

Chapter 1

Introduction to Diophantine m-tuples

1.1 Definition

Definition 1.1. *The set of m (distinct) non-zero integers $\{a_1, a_2, \ldots, a_m\}$ is called a* ***Diophantine m-tuples*** *if*

$$a_i a_j + 1 \text{ is a perfect square in } \mathbb{Z},$$

for all $1 \leq i < j \leq m$. (A perfect square is often denoted by $\square$.)

The set is named after the ancient Greek mathematician **Diophantus** from the 3rd century AD who found the set of four rational numbers

$$\left\{\frac{1}{16}, \frac{33}{16}, \frac{17}{4}, \frac{105}{16}\right\} \tag{1.1}$$

with the property that the product of each two elements increased by 1 equals a perfect square of some rational number. Indeed,

$$\frac{1}{16}\cdot\frac{33}{16}+1=\left(\frac{17}{16}\right)^2, \frac{1}{16}\cdot\frac{17}{4}+1=\left(\frac{9}{8}\right)^2, \frac{1}{16}\cdot\frac{105}{16}+1=\left(\frac{19}{16}\right)^2,$$

$$\frac{33}{16}\cdot\frac{17}{4}+1=\left(\frac{25}{8}\right)^2, \frac{33}{16}\cdot\frac{105}{16}+1=\left(\frac{61}{16}\right)^2, \frac{17}{4}\cdot\frac{105}{16}+1=\left(\frac{43}{8}\right)^2.$$

Let us note that Diophantine m-tuples can be observed in any commutative ring with unity. If we observe them in the field of rational numbers $\mathbb{Q}$, then they are called *rational Diophantine m-tuples*. So, (1.1) is an example of a rational Diophantine quadruple.

The first Diophantine quadruple (in $\mathbb{Z}$) was found by the French mathematician (and lawyer) Pierre de Fermat (17th century):

$$\{1, 3, 8, 120\}. \tag{1.2}$$

Indeed, we have

$$1\cdot 3+1=2^2, 1\cdot 8+1=3^2, 1\cdot 120+1=11^2, 3\cdot 8+1=5^2, 3\cdot 120+1=19^2, 8\cdot 120+1=31^2.$$

The set (1.1) is sometimes called *Fermat's quadruple*.

The problem that mathematicians are most concerned with is how large these sets can be. This, of course, depends on the ring in which we observe these sets. In the ring of integers, this problem is almost completely solved.

In this course we mainly talk about Diophantine m-tuples in the ring of integers. Note that (integer) Diophantine m-tuples have either all positive or all negative elements, so we will focus on those with positive elements, i.e. on m-tuples in the set of natural numbers. (The only Diophantine m-tuple with mixed signs is the Diophantine pair $\{-1, 1\}$.)

1.2 On Diophantine pairs

There are infinitely many Diophantine pairs in $\mathbb{N}$. Indeed, for any integer $r > 1$, consider the pairs

$$(a, b) = (1, r^2 - 1) \quad \text{or} \quad (a, b) = (r - 1, r + 1).$$

In both cases, we have

$$ab + 1 = r^2,$$

which shows that $\{a, b\}$ is a Diophantine pair.

Moreover, for any $a \in \mathbb{N}$, there are infinitely many b's in $\mathbb{N}$ such that $\{a, b\}$ is a Diophantine pair. This is because a divides $r^2 - 1$ for values of r satisfying

$$r - 1 = ka \quad \text{or } r + 1 = ka,$$

where k is non-zero integer. Solving for b yields

$$b = k^2 a \pm 2k.$$

Thus, for any positive integers a and k , the pair

$$\{a, k^2 a \pm 2k\}$$

is a Diophantine pair.

1.3 On Diophantine triples

There are infinitely many Diophantine triples. For any integer $k > 1$, the set

$$\{k - 1, k + 1, 4k\}$$

forms a Diophantine triple, since:

$$(k - 1)(k + 1) + 1 = k^2,\ 4k(k - 1) + 1 = (2k - 1)^2,\ 4k(k + 1) + 1 = (2k + 1)^2.$$

Now we may ask: given a Diophantine pair $\{a, b\}$, how many Diophantine triples $\{a, b, c\}$ can be formed by extending it? The answer is: *infinitely many.*

To see this, assume $\{a, b\}$ is a Diophantine pair, so that $ab + 1 = r^2$ for some integer r. Then both sets

$$\{a, b, a + b + 2r\} \quad \text{and} \quad \{a, b, a + b - 2r\}$$

are Diophantine triples if $a+b\pm 2r \notin \{0,a,b\}$. Let's verify that these extensions satisfy the required conditions. Indeed,

$$a(a+b+2r)+1 = a^2+ab+2ar+1 = a^2+r^2+2ar = (a+r)^2$$

and similarly:

$$a(a+b\pm 2r)+1 = (a\pm r)^2,\ b(a+b\pm 2r)+1 = (b\pm r)^2.$$

This construction guarantees at least one valid extension, since

$$a+b+2r > \max\{a,b\} \quad \text{for} \quad r>0.$$

It is possible that $a+b-2r=0$ (for example for pairs $\{1,3\}$ and $\{2,4\}$), but it is never equal to a or b. So, it makes sense to assume that $a<b<c$ and $r>0$ (since $\{a,a+b+2r\}$ can be extended by $a+(a+b+2r)-2(a+r)=b$). In this case the extension is $c=a+b+2r$ and the Diophantine triple of the form

$$\{a,b,a+b+2r\}$$

is called a **regular Diophantine triple**.

In what follows, we will see that there are infinitely many c's that extend a given pair $\{a,b\}$. Suppose we want to extend a Diophantine pair $\{a,b\}$, $a<b$, by an element c such that

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

for some $s,t>0$. By multiplying the first equation by b and the second by a and subtracting them, we eliminate c and get Diophantine equation

$$at^2-bs^2=a-b.$$

Multiplying both sides by a, we get

$$(at)^2-abs^2=a(a-b). \tag{1.3}$$

This equation is of the form

$$X^2-DY^2=N, \tag{1.4}$$

where $D>0$ and $D\neq\square$, and is better known as **Pellian** or **generalized Pell's equation**. Pellian equation might not have solutions, but if it does, it has infinitely many solutions. Unlike that, Pell's equation

$$X^2-DY^2=1, \tag{1.5}$$

always has infinitely many solutions (if D is a nonsquare positive integer).

If $(X,Y)\in\mathbb{N}^2$ is a solution of (1.4) and $(U,V)\in\mathbb{N}^2$ is a solution of the associated Pell's equation (1.5) then (X',Y') given by

$$X'+\sqrt{D}Y' = (X+\sqrt{D}Y)(U+\sqrt{D}V)$$

is a solution of (1.4). Indeed,

$$\begin{aligned} X'^2-DY'^2 &= (X'+\sqrt{D}Y')(X'-\sqrt{D}Y') \\ &= (X+\sqrt{D}Y)(U+\sqrt{D}V)(X-\sqrt{D}Y)(U-\sqrt{D}V) \\ &= (X^2-DY^2)(U^2-DV^2) \\ &= N\cdot 1 = N \end{aligned}$$

Since every Pell's equation has infinitely many solutions in $\mathbb{N}$, we conclude that (1.4) also has infinitely many solutions in $\mathbb{N}$ (if it is solvable). Equation (1.3) has a solution that arises from the regular expansion $c = a + b + 2r$. So, $(T, s) = (a(b + r), a + r)$ is a solution of (1.3) (where $T := at$). Another solution of (1.3) can be constructed in the following way:

$$(a(b + r) + \sqrt{ab}(a + r))(U + \sqrt{ab}V) = T' + \sqrt{ab}s',$$

where (U, V) is a solution of the related Pell's equation $X^2 - abY^2 = 1$. We get

$$s' = (a + r)U + a(b + r)V.$$

Note that

$$s'^2 - 1 \equiv 0 \pmod{a}.$$

Indeed,

$$s'^2 - 1 \equiv r^2U^2 - 1 = (ab + 1)U^2 - 1 \equiv U^2 - 1 \pmod{a}$$

and $U^2 - 1 = abV^2 \equiv 0 \pmod{a}$. Therefore, the following is well defined

$$c' := \frac{s'^2 - 1}{a} = \frac{((a + r)U + a(b + r)V)^2 - 1}{a}$$

and $\{a, b, c'\}$ is a Diophantine triple.

Solutions to Pellian equations can be described using recurrence sequences. More precisely, the solutions to a Pellian equation in one variable can be generated by a second-order linear recurrence. This will be discussed in one of the following chapters.

1.4 On Diophantine quadruples

There exist infinitely many Diophantine quadruples. Here are some examples of families of Diophantine quadruples:

$$\{k, k + 2, 4k + 4, 4(k + 1)(2k + 1)(2k + 3)\},\ k \geq 1$$

$$\{F_{2n}, F_{2n+2}, F_{2n+4}, 4F_{2n+1}F_{2n+2}F_{2n+3}\},\ n \geq 0.$$

Previous sets are taken to be generalizations of Fermat's quadruple $\{1, 3, 8, 120\}$. More general, if the sequence (g_n) be defined as:

$$g_0 = 0, g_1 = 1, g_n = pg_{n-1} - g_{n-2},\ n \geq 2,$$

where $p \geq 2$ is an integer, then the set

$$\{g_n, g_{n+2}, (p \pm 2)g_{n+1}, 4g_{n+1}((p \pm 2)g_{2n+1} \mp 1)\}$$

had the property of Diophantus. For $p = 2, 3$ we get the previous sets.

More examples with with Pell numbers P_n and Pell-Lucas numbers $Q'_n = 2Q_n$:

$$\{P_{2n}, P_{2n+2}, 2P_{2n}, 4Q_{2n}P_{2n+1}Q_{2n+1}\},$$

$$\{P_{2n}, P_{2n+2}, 2P_{2n+2}, 4P_{2n+1}Q_{2n+1}Q_{2n+2}\}$$

(These numbers are defined by

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

$$Q_0 = 1, Q_1 = 1, Q_{n+2} = 2Q_{n+1} + Q_n, n \geq 0.)$$

What can we say about the extensions of a Diophantine pair or triple to a Diophantine quadruple? The following propositions show that this is always possible.

Proposition 1.2 (Euler,18th century)**.** *If $\{a, b\}$ is a Diophantine pair, then*

$$\{a, b, a + b + 2r, 4r(a + r)(b + r)\}$$

is a Diophantine quadruple, where $ab + 1 = r^2$.

Proposition 1.3 (Arkin, Hogatt and Strauss, 1979)**.** *If $\{a, b, c\}$ is a Diophantine triple, then*

$$\{a, b, c, a + b + c + 2abc + 2rst\} \tag{1.6}$$

is a Diophantine quadruple, where $ab + 1 = r^2$, $ac + 1 = s^2$, $bc + 1 = t^2$.

A Diophantine quadruple of the form (1.6), where $a < b < c$, is called **regular**. It can be shown that $\{a, b, c, d\}$ is a regular Diophantine quadruple if and only if

$$(a + b - c - d)^2 = 4(ab + 1)(cd + 1).$$

The problem of extending the Diophantine triple $\{a, b, c\}$ to a Diophantine quadruple $\{a, b, c, d\}$ is equivalent to determining an integer triple (x, y, z) such that

$$ad + 1 = x^2,\ bd + 1 = y^2,\ cd + 1 = z^2.$$

By eliminating d, the previous equations reduce to a system of Diophantine equations:

$$ay^2 - bx^2 = a - b, \tag{1.7}$$

$$az^2 - cx^2 = a - c, \tag{1.8}$$

i.e. to a system of Pellian equations:

$$(ay)^2 - (ab)x^2 = a(a - b), \tag{1.9}$$

$$(az)^2 - (ac)x^2 = a(a - c), \tag{1.10}$$

Systems of the form (6.19) and (6.23), or (1.9) and (1.10), are not easy to solve. For some specific values of the elements a, b and c, we will show how they can be treated by applying *Baker's theory on linear forms in logarithms of algebraic numbers.* A linear form in logarithms of algebraic numbers is an expression of the form

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

where $b_1, \ldots, b_n$ are rational numbers and $\alpha_1, \ldots, \alpha_n$ are algebraic numbers. Also, we will need so called *Baker-Davenport's reduction* base on the expansion into a continued fraction.

How is the problem of finding solutions to the system (1.9), (1.10) related to Baker's theory on linear forms in logarithms?

Each of these equations has solutions that can be described by binary (second-order) recurrence sequences. So, solving the system means finding the intersection of two such sequences. This leads to the problem of finding positive integers m and n such that:

$$\gamma\alpha^m \approx \delta\beta^n$$

for certain algebraic numbers $\alpha, \beta, \gamma, \delta$.Taking logarithms of both sides, we get

$$m \log \alpha - n \log \beta + \log \frac{\gamma}{\delta} \approx 0.$$

Now, Baker's theory tells us that a nonzero linear combination of logarithms of algebraic numbers cannot be too close to zero. In fact, Baker's result gives an explicit lower bound on how far from zero such an expression must be—unless it is exactly zero. As a result, we can obtain an explicit upper bound for the possible values of m and n. However, this bound is usually too large to check directly, so we apply a refinement method developed by Baker and Davenport to reduce the search range.

Another way to obtain an upper bound on the solutions is by using results on the simultaneous approximation of square roots — this is known as the *hypergeometric method* in Diophantine approximation. Specifically, if we assume that the system (6.19),(6.23) has some relatively large solution x, y, z, then y/x and z/x provide very good rational approximations (with a common denominator) to the irrational numbers $\sqrt{a/c}$ and $\sqrt{b/c}$, respecively.

Conjecture 1.4. *If $\{a, b, c, d\}$ is a Diophantine quadruple and $d > \max\{a, b, c\}$, then*

$$d = a + b + c + 2abc + 2rst.$$

Conjecture (1.4) implies that all quadruples are regular and thta there is no Diophantine quintuple.

1.5 On Diophantine quintuples

For many years, mathematicians have studied the well-known *Diophantine quintuple conjecture*, which asserts that no Diophantine quintuple exists. The first significant step toward resolving this conjecture was made in 1969 by Baker and Davenport [3], who showed that Fermat's quadruple $\{1, 3, 8, 120\}$ cannot be extended to a Diophantine quintuple. Using Baker's theory of linear forms in logarithms of algebraic numbers, along with a reduction method based on continued fractions, they proved that if d is a positive integer such that $\{1, 3, 8, d\}$ forms a Diophantine quadruple, then $d = 120$. This implies that the triple $\{1, 3, 8\}$ cannot be extended to a quintuple. Similar results have been established for many families of Diophantine pairs and triples.

Euler was able to extend Fermat's quadruple to the rational quintuple

$$\{1, 3, 8, 120, \frac{777480}{8288641}\}.$$

Dujella ([12]) generalized Euler's construction and extended an arbitrary Diophantine quadruple $\{a, b, c, d\}$ to a (rational) Diophantine quintuple:

$$\{a, b, c, d, e = \frac{(a + b + c + d)(abcd + 1) + 2abc + 2abd + 2acd + 2bcd \pm 2r_1r_2r_3r_4r_5r_6}{(abcd - 1)^2}\}$$

where $ab+1=r_1^2$, $ac+1=r_2^2$, $ad+1=r_3^2$, $bc+1=r_4^2$, $bd+1=r_5^2$, $cd+1=r_6^2$.

In 2004 Dujella ([15]) made an important breakthrough showing that a Diophantine sextuple does not exist and that there are only finitely many Diophantine quintuples. The bound for the number of possible Diophantine quintuples has been improved by several authors and finally in 2019, He, Togbé and Ziegler ([22]) published the proof of Diophantine quintuple conjecture.

Theorem 1.5. *There does not exist a Diophantine quintuple.*

1.6 $D(n)$-tuples

There are several generalizations of classical Diophantine quadruples. One natural generalization is to replace the original condition - where the product of any two elements increased by 1 yields a perfect square - with the more general condition of adding an arbitrary element $n \in \mathcal{R}$. This leads to the broader concept of sets with the property $D(n)$.

Definition 1.6. *Let $\mathcal{R}$ be a commutative ring with unity, let $m \in \mathbb{N}$, and let $n \in \mathcal{R}$. A set $\{a_1, \ldots, a_m\} \subseteq \mathcal{R}$ is said to have the* property $D(n)$ *if for every pair of distinct elements in the set, the expression $a_i a_j + n$ is a perfect square in $\mathcal{R}$.*

A set with the property $D(n)$ contained in $\mathcal{R} \setminus \{0\}$ is called a Diophantine m-tuple with the property $D(n)$ *in the ring $\mathcal{R}$, or more briefly, a* $D(n)$-m-tuple.

Interestingly, in certain integer rings of number fields - such as the ring of rational integers, the rings of integers of some quadratic fields, and specific cubic and quartic fields - the existence of $D(n)$-quadruples is closely related to the representability of n as a difference of two squares. More precisely, a $D(n)$-quadruple exists in such rings if and only if $n = a^2 - b^2$ for some elements a, b in the ring (up to finitely many exceptions). However, recent results show that in some rings of quadratic integers, there exist elements n that are **not** expressible as a difference of two squares, yet a $D(n)$-quadruple still exists.

We will investigate $D(n)$-m-tuples in the ring of integers $\mathbb{Z}$ and briefly show the equivalence between the existence of $D(n)$-quadruples and the representability of n as a difference of two squares, up to finitely many exceptions. Note that if $ab + n = r^2$, then

$$\{a, b, a + b \pm 2r\}$$

is a $D(n)$-triple - this can be verified in the same way as for the case $n = 1$. Furthermore, all c's such that a given Diophantine $D(n)$-pair $\{a, b\}$ can be extended to a $D(n)$-triple $\{a, b, c\}$ are connected to the following Pell-type equation:

$$bx^2 - ay^2 = n(b - a).$$

Assignment 1. *a) Show Proposition 1.3*

b) If $ab + 1 = r^2$, show that $\{a, b, a + b + 2r, 4r(a + r)(b + r)\}$ is a regular *Diophantine quadruple.*

c) Show that

$$\{F_{2n}, F_{2n+6}, 4F_{2n+2}, 4F_{2n+1}F_{2n+3}F_{2n+4}\}$$

is a $D(4)$-quadruple for $n \in \mathbb{N}$. (F_n is the nth Fibonacci number.)

Chapter 2

Simple continued fractions

2.1 Simple continued fraction expansion

Let $\alpha \in \mathbb{R}$ and

$$a_0 = \lfloor \alpha \rfloor \in \mathbb{Z},$$

where $\lfloor \alpha \rfloor$ denote the floor of α, that is the greatest integer less than or equal to α.

If $\alpha \neq a_0$, then $0 < \alpha - a_0 < 1$ and

$$\alpha_1 = \frac{1}{\alpha - a_0} > 1.$$

So,

$$\alpha = a_0 + \frac{1}{\alpha_1}.$$

Now we put

$$a_1 = \lfloor \alpha_1 \rfloor \in \mathbb{N}$$

and if $\alpha_1 \neq a_1$, then

$$\alpha_1 = a_1 + \frac{1}{\alpha_2},$$

where

$$\alpha_2 = \frac{1}{\alpha_1 - a_1} > 1.$$

Hence,

$$\alpha = a_0 + \cfrac{1}{a_1 + \cfrac{1}{\alpha_2}}.$$

This procedure can be repeated as long as $a_k \neq \alpha_k$. Suppose that $a_n = \alpha_n$ for some $n \in \mathbb{N}$. Then the procedure terminates and we get

$$\alpha = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\ddots + \cfrac{1}{a_n}}}}. \tag{2.1}$$

We say that (2.1) is a *finite simple continued fraction expansion* of α (or finite simple continued fraction representation). In what follows, we will omit the word "simple". In short, we write it as

$$\alpha = [a_0; a_1, a_2, \ldots, a_n]. \tag{2.2}$$

Integers $a_0, a_1, \ldots, a_n$ are called the *partial quotients* (sometimes *coefficients* or *terms*) of the continued fraction. Note that $a_1, \ldots, a_n$ are positive integers. Also, if $a_n \geq 2$ in (2.2), then $[a_0, a_1, \ldots, a_{n-1}, a_n - 1, 1]$. This means that we can have two continued fraction expansions of α (in some cases).

It is important to point out that finite simple continued fractions correspond to rational numbers and every rational number has a finite (simple) continued fraction expression. In that case, that is if

$$\alpha = \frac{b}{c} \in \mathbb{Q},$$

coefficients of continued fraction can be computed by *Euclid's algorithm* applied on b and c:

$$\begin{aligned}
b &= ca_0 + r_0, \ 0 < r_0 < c, \\
c &= r_0a_1 + r_1, \ 0 < r_1 < r_0, \\
r_0 &= r_1a_2 + r_2, \ 0 < r_2 < r_1, \\
&\vdots \\
r_{n-2} &= r_{n-1}a_n + r_n, \ 0 < r_n < r_{n-1}, \\
r_{n-1} &= r_na_{n+1}.
\end{aligned}$$

Example 1. *Find continued fraction expansion of* $\dfrac{173}{119}$ *using the Euclid's Algorithm.*

$$\begin{aligned}
173 = 119 \cdot 1 + 54 \quad &\Rightarrow \quad \frac{173}{119} = 1 + \frac{54}{119}, \\
119 = 54 \cdot 2 + 11 \quad &\Rightarrow \quad \frac{119}{54} = 2 + \frac{11}{54}, \\
54 = 11 \cdot 4 + 10 \quad &\Rightarrow \quad \frac{54}{11} = 4 + \frac{10}{11}, \\
11 = 10 \cdot 1 + 1 \quad &\Rightarrow \quad \frac{11}{10} = 1 + \frac{1}{10}, \\
10 = 1 \cdot 10 + 0 \quad &\Rightarrow \quad \frac{10}{1} = 10.
\end{aligned}$$

So, $\dfrac{173}{119} = [1; 2, 4, 1, 10]$.

On the other hand, the process for finding the simple continued fraction continues indefinitely if and only if α is an irracional number. In this case

$$\alpha = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\ddots + \cfrac{1}{\alpha_n}}}} = [a_0; a_1, a_2, \ldots, \alpha_n].$$

and $a_k \neq \alpha_k$, for all k. So, we get an *infinite simple continued fraction representation* of α which can be written as

$$\alpha = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\ddots}}} = [a_0; a_1, a_2, \ldots]. \tag{2.3}$$

But what the right-hand object means? That is, in what sense do we have the equality in (2.3). This will be argued in the following section.

2.2 Convergents

Let $a_0, a_1, \ldots, a_k$ be coefficients of the continued fraction representation of α. The rational number

$$\frac{p_k}{q_k} = [a_0; a_1, \ldots, a_k],$$

is called the k-th *convergent* of the continued fraction. Here are the first few convergents:

$$\frac{p_0}{q_0} = a_0, \ \frac{p_1}{q_1} = \frac{a_0a_1 + 1}{a_1}, \ \frac{p_2}{q_2} = \frac{a_0a_1a_2 + a_0 + a_2}{a_1a_2 + 1}, \ \ldots$$

Theorem 2.1 (Convergents' properties). *Let* $\left(\frac{p_n}{q_n}\right)$ *be convergents of* α. *Then following properties hold:*

(a)

$$p_n = a_n p_{n-1} + p_{n-2}, \ p_{-2} = 0, \ p_{-1} = 1, \tag{2.4}$$
$$q_n = a_n q_{n-1} + q_{n-2}, \ q_{-2} = 1, \ q_{-1} = 0, \ n \geq 0; \tag{2.5}$$

(b) $q_n p_{n-1} - p_n q_{n-1} = (-1)^n$, $n \geq -1$;

(c) $\gcd(p_n, q_n) = 1$, $n \geq -2$;

(d) $\left(\frac{p_{2n}}{q_{2n}}\right)$ *is an increasing sequence,* $\left(\frac{p_{2n+1}}{q_{2n+1}}\right)$ *is a decreasing sequence;*

(e)

$$\frac{p_{2n}}{q_{2n}} < \frac{p_{2m+1}}{q_{2m+1}}, \ m, n \in \mathbb{N}_0;$$

(f)

$$\lim_{n\to\infty} \frac{p_n}{q_n} = \alpha; \tag{2.6}$$

(g)

$$\left|\alpha - \frac{p_n}{q_n}\right| < \frac{1}{q_n^2}, \ n \in \mathbb{N}_0. \tag{2.7}$$

Proofs of the above properties can be found in [**?**], 8.13 – 8.22.

Now we can argue that the equality in relation (2.3) makes sense due to the convergence of (p_n/q_n).

The numerator and denominator of convergents satisfy two-term linear recursions (2.4) and (2.5) that allow efficient calculations.

2.3 On approximation of irrationals by continued fractions

According to (2.7), the convergents are very good rational approximations to rationals.

Theorem 2.2. *If* $\frac{p_{n-1}}{q_{n-1}}$ *and* $\frac{p_n}{q_n}$ *are two consecutive convergents of* α*, then at least one of them satisfies*

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

Proof. Since numbers $\alpha - \frac{p_n}{q_n}$ and $\alpha - \frac{p_{n-1}}{q_{n-1}}$ have the opposite signs, we have

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

Assuming that $\left|\alpha - \frac{p_n}{q_n}\right| \geq \frac{1}{2q_n^2}$ and $\left|\alpha - \frac{p_{n-1}}{q_{n-1}}\right| \geq \frac{1}{2q_{n-1}^2}$, we get

$$\frac{1}{q_n q_{n-1}} \geq \frac{1}{2q_n^2} + \frac{1}{2q_{n-1}^2} \iff (q_n - q_{n-1})^2 \leq 0,$$

a contradiction! Hence,

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

□

The following theorem is a kind of reversal of the previous one. It will play a key role in determining the fundamental solution to Pell's equation.

Theorem 2.3 (Legendre)**.** *Let* p *and* q *be integers such that*

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

Then $\frac{p}{q}$ *is a convergent of the continued fraction expansion of* α*.*

Sketch of proof. If $\alpha = \frac{p}{q}$, then the statement is trivially satisfied. So, assume that $\alpha \neq \frac{p}{q}$ and $\alpha - \frac{p}{q} = \frac{\varepsilon\vartheta}{q^2}$, where $0 < \vartheta < \frac{1}{2}$ and $\varepsilon = \pm 1$. Let $\frac{p}{q} = [b_0, b_1, \ldots, b_{n-1}]$ be a continued fraction

representation of $\frac{p}{q}$ where n is such that $(-1)^{n-1} = \varepsilon$. (We can always achieve this because $[a_0, a_1, \ldots, a_m] = [a_0, a_1, \ldots, a_m - 1, 1]$.)

We now define ω as

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

Hence,

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

ane

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

Due to the properties of convergents and the conveniently chosen n, it can be shown that $\omega > 1$ and this means that $[b_0, b_1, \ldots, b_{n-1}] = \frac{p}{q}$ is a convergent of the continued fraction expansion of α. □

2.4 Periodic continued fractions

A *periodic continued fraction* is an infinite continued fraction of the form

$$[a_0, a_1, \ldots, a_{k-1}, \overline{a_k, a_{k+1}, \ldots, a_{k+m-1}}], \tag{2.8}$$

where a vinculum (horizontal line) marks the repeating block. If (2.8) represents the continued fraction of α, then

$$\beta = [\overline{a_k, a_{k+1}, \ldots, a_{k+m-1}}]$$

is its *purely periodic part*. The length m of the minimal repeating block is called the *period* of the continued fraction.

Theorem 2.4 (Euler, Lagrange)**.** *A continued fraction expansion of α is* periodic *if and only if α is a* quadratic irrational *(i.e. α is an irrational solution to a quadratic equation with integer coefficients).*

Sketch of Proof. Suppose that α has a periodic continued fraction expansion:

$$\alpha = [b_0, b_1, \ldots, b_{k-1}, \overline{a_0, a_1, \ldots, a_{m-1}}].$$

Define its purely periodic part as

$$\beta = [\overline{a_0, a_1, \ldots, a_{m-1}}] = [a_0, a_1, \ldots, a_{m-1}, \beta].$$

From formulas (2.4) and (2.5), we obtain

$$\beta = \frac{\beta p_{m-1} + p_{m-2}}{\beta q_{m-1} + q_{m-2}}$$

which implies that β satisfies a quadratic equation and is therefore a quadratic irrational. Consequently, α is also a quadratic irrational.

To prove the converse, let α be a quadratic irrationality. Then there exist $d, s_0, t_0 \in \mathbb{Z}$, $t_0 \neq 0$, $d \neq \square$ such that

$$\alpha = \frac{s_0 + \sqrt{d}}{t_0} \quad \text{and} \quad t_0 \mid (d - s_0^2).$$

(If $t_0 \nmid (d-s_0^2)$, then multiplying numerator and denominator by t_0 yields $t_0^2 \mid (dt_0^2-(s_0t_0)^2)$). To compute the continued fraction expansion of α the following iterative algorithm (or recurrence) is performed for $a_0 = \lfloor \alpha \rfloor$ and $i \geq 0$:

$$s_{i+1} = a_i t_i - s_i,\ t_{i+1} = \frac{d - s_{i+1}^2}{t_i},\ a_{i+1} = \left\lfloor \frac{s_{i+1} + \sqrt{d}}{t_{i+1}} \right\rfloor. \tag{2.9}$$

It turns out that there exist $j, k \in \mathbb{N}$, $j < k$, such that $(s_j, t_j) = (s_k, t_k)$. Therefore, the sequence becomes periodic and

$$\alpha = [a_0, \ldots, a_{j-1}, \overline{a_j, a_{j+1}, \ldots, a_{k-1}}].$$

□

In particular, the continued fraction expansion of $\sqrt{d}$, $d \neq \square$, is a bit more specific. These expansions are especially important due to their connection with Pell's equation.

Theorem 2.5. *Let d be a non-square positive integer. The continued fraction expansion of $\sqrt{d}$ is of the form*

$$\sqrt{d} = [a_0, \overline{a_1, a_2, \ldots, a_{r-1}, 2a_0}],$$

where $a_0 = \lfloor \sqrt{d} \rfloor$, and the remaining coefficients are computed by the recurrence:

$$s_{i+1} = a_i t_i - s_i,\ t_{i+1} = \frac{d - s_{i+1}^2}{t_i},\ a_{i+1} = \left\lfloor \frac{s_{i+1} + a_0}{t_{i+1}} \right\rfloor,\ i = 0, \ldots, r-1, \tag{2.10}$$

with the initial terms $s_0 = 0$, $t_0 = 1$.

Moreover, the sequence $a_1, a_2, \ldots, a_{r-1}$ forms a palindromic string*:*

$$a_1 = a_{r-1}, a_2 = a_{r-2}, \ldots$$

Proof. See Theorem 8.41 in [**?**]. □

Remark 2.6. *Since the period of the continued fraction for $\sqrt{d}$ is not known in advance, we continue applying the recurrence (2.10) until the pair (s_1, t_1) repeats. If the period is r, we will have $(s_1, t_1) = (s_{r+1}, t_{r+1})$ which signals that the process can stop.*

Chapter 3

Pell's equation

3.1 Existence of solutions to Pell's equation

Definition 3.1. *Let d be a positive integer that is not a perfect square. Diophantine equation of the form*

$$x^2 - dy^2 = 1 \tag{3.1}$$

is called Pell's equation.

Pellian equation *or* generalized Pell's equation *is of the form*

$$x^2 - dy^2 = N, \tag{3.2}$$

where N is an integer.

Equation (3.1) is named after the English 17th-century mathematician John Pell, who did not significantly contribute to its solution. Credit was incorrectly attributed to him by Euler. However, the equation had been of interest to mathematicians much earlier. Thus, the equation $x^2 - 2y^2 = 1$ appears among ancient Greek mathematicians (6th century BC) in connection with their research into the nature of the number $\sqrt{2}$. Furthermore, it was also studied by the Indian 7th-century mathematicians Brahmagupta and Bhaskara, who found solutions for some special values of the number d, specifically $d = 11, 31, 61, 67$. These values are not chosen at random, but are such that the smallest solution in the set of natural numbers is unexpectedly large. Thus, the smallest solution to the equation $x^2 - 61y^2 = 1$ is equal to $x = 1776319049$, $y = 22615390$. Five centuries later, Bhaskara II perfected the method for solving the Pell equations of his predecessors and called this method the *caravala* (cyclic procedure). What he did not prove was whether the method was effective for each d. The first Europeans to participate significantly in the study were Fermat, Frenicle de Bessy, Brouncker and Wallis in the mid-17th century, but the greatest credit goes to Lagrange (18th century) who would offer a completely new approach based on continued fractions.

Pell's equation (3.1) has infinitely many solutions in the set of positive integers, in contrast to (3.2) which is not necessarily solvable. (For example, $X^2 - 5y^2 = 2$ has no solution.)

Theorem 3.2. *There is at least one pair of positive integers (x, y) that satisfies Pell's equation (3.1).*

Theorem 3.2 was stated (without proof) by Fermat. The proof is based on the following consequence of Dirichlet's theorem (see, for example, Theorem 6.1. in [**?**]) which we state without proof, but it also follows directly from the proposition 2.1(g)).

Lemma 3.3. *If α is an irrational number, then there are infinitely many relatively prime integers p and q such that*

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{q^2}. \tag{3.3}$$

Corollary 3.4. *Let d be a positive integer that is not a perfect square. There are infinitely many pairs of positive integers (x, y) such that*

$$|x^2 - dy^2| < 1 + 2\sqrt{d}. \tag{3.4}$$

Proof. Since $\sqrt{d}$ is an irrational number, Lemma 3.3 implies that there exist infinitely many pairs of positive integers (x, y) such that

$$\left|\frac{x}{y} - \sqrt{d}\right| < \frac{1}{y^2}.$$

Also,

$$\left|\frac{x}{y} + \sqrt{d}\right| = \left|\frac{x}{y} - \sqrt{d} + 2\sqrt{d}\right| < \frac{1}{y^2} + 2\sqrt{d}.$$

Hence,

$$|x^2 - dy^2| = |(x - y\sqrt{d})(x + y\sqrt{d})| < 1 + 2\sqrt{d}.$$

□

Proof of Theorema 3.2. According to Corollary 3.4 there exists an non-zero integer $k \neq 0$ such that $x^2 - dy^2 = k$ is valid for infinitely many pairs of positive integers (x, y). Since there are infinitely many of such pairs, there exist at least two pairs (x_1, y_1) and (x_2, y_2) such that $|x_1| \neq |x_2|$ and

$$x_1 \equiv x_2 \pmod{|k|}, \quad y_1 \equiv y_2 \pmod{|k|}. \tag{3.5}$$

We have

$$(x_1 - y_1\sqrt{d})(x_2 + y_2\sqrt{d}) = x_1x_2 - y_1y_2d + (x_1y_2 - x_2y_1)\sqrt{d}.$$

According to (3.5) and $x_1^2 - dy_1^2 = x_2^2 - dy_2^2 = k$, the following congruences are valid

$$x_1x_2 - y_1y_2d \equiv x_1^2 - y_1^2d \equiv 0 \pmod{|k|},\ x_1y_2 - x_2y_1 \equiv x_1y_1 - x_1y_1 \equiv 0 \pmod{|k|}.$$

Hence,

$$x_1x_2 - y_1y_2d = ku,\ x_1y_2 - x_2y_1 = kv,$$

for some integers u, v and

$$(x_1 - y_1\sqrt{d})(x_2 + y_2\sqrt{d}) = k(u + v\sqrt{d}),$$
$$(x_1 + y_1\sqrt{d})(x_2 - y_2\sqrt{d}) = k(u - v\sqrt{d}).$$

Multiplying these two equations gives

$$k^2 = (x_1^2 - dy_1^2)(x_2^2 - dy_2^2) = k^2(u^2 - dv^2)$$

which means that $u^2 - dv^2 = 1$.

To complete the proof, we have to see that $v \neq 0$. Let us assume the opposite, $v = 0$. Then $x_1y_2 = x_2y_1$, $u = \pm 1$ and

$$(x_1 - y_1\sqrt{d})k = (x_1 - y_1\sqrt{d})(x_2 + y_2\sqrt{d})(x_2 - y_2\sqrt{d}) = \pm k(x_2 - y_2\sqrt{d}).$$

So, $x_1 = \pm x_2$ and $y_1 = \pm y_2$. This is a contradiction with $|x_1| \neq |x_2|$. Hence, $v \neq 0$ and $(|u|, |v|)$ is a positive integer solution of Pell's equation. □

We formally denote the solution of Pell's equation (3.1) by

$$u + v\sqrt{d},$$

that is as an element of the quadratic field $\mathbb{Q}(\sqrt{d})$. Among other things, such a notation has some technical advantages. If $u + v\sqrt{d} < u' + v'\sqrt{d}$ (in the numerical sense), then the solution $u + v\sqrt{d}$ is less the solution $u' + v'\sqrt{d}$. The smallest (or minimal) positive integer solution of Pell's equation is called *fundamental solution* and is usually denoted by $x_1 + y_1\sqrt{d}$. The solution $x_0 + y_0\sqrt{d} = 1 + 0\sqrt{d}$ is called *trivial*.

Example 2. *If $u+v\sqrt{d}$ and $u'+v'\sqrt{d}$ are solutions of Pell's equation (3.1), then $(u+v\sqrt{d})(u'+v'\sqrt{d})$ is also a solution of (3.1).*

If $a+b\sqrt{d}$ is a solution of Pellian equation $x^2 - dy^2 = -1$, then $(a+b\sqrt{d})^2$ is a solution of Pell's equation (3.1).

Basic facts on quadratic fields

Let us assume that d is a square-free integer. The set

$$\mathbb{Q}(\sqrt{d}) = \{a + b\sqrt{d} \,:\, a, b \in \mathbb{Q}\}$$

a field under operations under standard addition and multiplication, called *quadratic field*. In other words, it is an algebraic number field of degree two over $\mathbb{Q}$. Elements of $\mathbb{Q}(\sqrt{d})$ are roots of unique monic polynomials with rational coefficients of degree one or two. If the element $\alpha \in \mathbb{Q}(\sqrt{d})$ is a root of a monic polynomial with integer coefficients, then α is an *algebraic integer*. The set of all algebraic integers in any number field, $\mathbb{K}$, forms a ring that is frequently denoted as $\mathcal{O}_{\mathbb{K}}$. For $\mathbb{K} = \mathbb{Q}(\sqrt{d})$ a ring of integers depends on d:

$$\mathcal{O}_{\mathbb{Q}(\sqrt{d})} = \begin{cases} \mathbb{Z}[\sqrt{d}] = \{a + b\sqrt{d} \,:\, a, b \in \mathbb{Z}\}, \ d \equiv 2 \text{ or } 3 \pmod 4, \\ \mathbb{Z}[\frac{1+\sqrt{d}}{2}] = \{a + b\frac{1+\sqrt{d}}{2} \,:\, a, b \in \mathbb{Z}\}, \\ \qquad\qquad = \{\frac{u+v\sqrt{d}}{2} \,:\, u, v \in \mathbb{Z}, u \equiv v \pmod 2\}, \ d \equiv 1 \pmod 4. \end{cases}$$

The set of all invertible elements in $\mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ forms a (multiplicative) group called the *group of units* or *unit group*.

The *norm* of the element $\alpha = a + b\sqrt{d}$ is

$$N(\alpha) = \alpha\overline{\alpha} = (a + b\sqrt{d})(a - b\sqrt{d}) = a^2 - db^2.$$

The norm satisfies the following properties:

- $N(\alpha\beta) = N(\alpha)N(\beta)$, for all $\alpha, \beta \in \mathbb{Q}(\sqrt{d})$,
- $N(\alpha) = 0$ if and only if $\alpha = 0$,
- $\alpha \in \mathcal{O}_{\mathbb{Q}(\sqrt{d})} \Rightarrow N(\alpha) \in \mathbb{Z}$,
- $\alpha \in \mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ is a unit if and only if $N(\alpha) \in \{-1, 1\}$.

The last property establishes a connection between the units of $\mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ and Pell's equation, or Pellian equations. So, if $d \equiv 2$ or $3 \pmod 4$, $\alpha = a+b\sqrt{d}$ is a unit if and only if it is a solution to one of equations $x^2 - dy^2 = \pm 1$. If $d \equiv 1 \pmod 4$, $\alpha = a + b\sqrt{d}$ is a unit if and only if it is a solution to one of equations $x^2 - dy^2 = \pm 4$.

3.2 Structure of the solution set of Pell's equation

Theorem 3.5. *Let $x_1+y_1\sqrt{d}$ be a fundamental solution to Pell's equation (3.1). All solutions in positive integers are given by*

$$x_n + y_n\sqrt{d} = (x_1 + y_1\sqrt{d})^n. \tag{3.6}$$

Furthermore.

$$\begin{aligned} x_n &= \sum_{k=0}^{\lfloor n/2 \rfloor} \binom{n}{2k} x_1^{n-2k} y_1^{2k} d^k, \\ y_n &= \sum_{k=0}^{\lfloor n/2 \rfloor} \binom{n}{2k+1} x_1^{n-2k-1} y_1^{2k+1} d^k. \end{aligned}$$

Proof. It is easy to see that $x_n+y_n\sqrt{d}$ is a solution. By multiplying the expressions $x_n+y_n\sqrt{d} = (x_1 + y_1\sqrt{d})^n$ and $x_n - y_n\sqrt{d} = (x_1 - y_1\sqrt{d})^n$, we get

$$x_n^2 - dy_n^2 = (x_1 + y_1\sqrt{d})^n(x_1 - y_1\sqrt{d})^n = (x_1^2 - dy_1^2)^n = 1.$$

In the following, it is necessary to prove that there are no other solutions than (3.6). Assume that $u + v\sqrt{d}$, $u, v \in \mathbb{N}$, is a solution that is not obtained by formula (3.6). Hence, there exits $n \in \mathbb{N}$ such that

$$(x_1 + y_1\sqrt{d})^n < u + v\sqrt{d} < (x_1 + y_1\sqrt{d})^{n+1}.$$

This yields

$$1 < (u + v\sqrt{d})(x_1 + y_1\sqrt{d})^{-n} < x_1 + y_1\sqrt{d},$$

and since $(x_1 + y_1\sqrt{d})^{-1} = x_1 - y_1\sqrt{d}$

$$1 < (u + v\sqrt{d})(x_1 - y_1\sqrt{d})^{n} < x_1 + y_1\sqrt{d}.$$

Obviously,

$$a + b\sqrt{d} = (u + v\sqrt{d})(x_1 - y_1\sqrt{d})^n$$

is a solution to Pell's equation. If we show that a and b are positive integers, than we have a contradiction with the fact that $x_1 + y_1\sqrt{d}$ is a fundamental solution. Indeed,

$$2a = a + b\sqrt{d} + (a - b\sqrt{d}) = a + b\sqrt{d} + (a + b\sqrt{d})^{-1} > 0,$$

and

$$2b\sqrt{d} = a + b\sqrt{d} - (a - b\sqrt{d}) = a + b\sqrt{d} - (a + b\sqrt{d})^{-1} > 0,$$

because $a + b\sqrt{d} > 1$ and $0 < (a - b\sqrt{d}) = (a + b\sqrt{d})^{-1} < 1$. □

Let S be a set of all integer solutions (x, y) to Pell's equation such that $x > 0$, that is

$$S = \{x + y\sqrt{d} : x^2 - dy^2 = 1, (x, y) \in \mathbb{N} \times \mathbb{Z}\}.$$

Note that points (x, y) of S lie on the right branch of the hyperbola $x^2 - dy^2 = 1$. In addition, S has a strong algebraic structure under common multiplication.

Theorem 3.6. *The S is a multiplicative cyclic group.*

Proof. First, let us verify that S is closed under multiplication. Let $x+y\sqrt{d}$ and $x'+y'\sqrt{d}$ be elements of S. Then

$$(x+y\sqrt{d})(x'+y'\sqrt{d}) = xx'+yy'd+(xy'+x'y)\sqrt{d}.$$

is a solution to Pell's equation since

$$(xx'+yy'd)^2-d(xy'+x'y)^2 = x^2(x'^2-dy'^2)-dy^2(x'^2-dy'^2) = x^2-dy^2 = 1.$$

Also, $xx'+yy'd > 0$ because $x^2 = 1+dy^2 > dy^2$, that is $x > \sqrt{d}|y|$ and therefore $xx' > d|yy'|$. Hence, $(x+y\sqrt{d})(x'+y'\sqrt{d}) \in S$.

Obviously, the neutral element for multiplication $1 \in S$.The invertible element of $x+y\sqrt{d} \in S$ is $x-y\sqrt{d} \in S$. According to Theorem 3.5, the fundamental solution $x_1+y_1\sqrt{d}$ is a generator of the group S. □

3.3 Recurrence relations for solutions of Pell's equation

Theorem 3.7. *All solutions of Pell's equation (3.1) in positive integers (x_n, y_n) satisfy the following recurrence relations*

$$\begin{aligned} x_n &= x_1x_{n-1}+dy_1y_{n-1}, \\ y_n &= y_1x_{n-1}+x_1y_{n-1},\ n \geq 1, \end{aligned} \tag{3.7}$$

where (x_1, y_1) and $(x_0, y_0) = (1, 0)$ are fundamental and trivial solution of (3.1), respectively.

Furthermore,

$$\begin{aligned} x_n &= 2x_1x_{n-1}-x_{n-2}, \\ y_n &= 2x_1y_{n-1}-y_{n-2},\ n \geq 2. \end{aligned} \tag{3.8}$$

with the same initial conditions (x_1, y_1) and $(x_0, y_0) = (1, 0)$.

Proof. Recurrences in (3.7) follow straight forward by (3.6), that is

$$(x_{n-1}+y_{n-1}\sqrt{d})(x_1+y_1\sqrt{d}) = x_n+y_n\sqrt{d}.$$

Since $x_1-y_1\sqrt{d} = (x_1+y_1\sqrt{d})^{-1}$, we have

$$(x_{n-1}+y_{n-1}\sqrt{d})(x_1-y_1\sqrt{d}) = x_{n-2}+y_{n-2}\sqrt{d}.$$

Last two relations can be rewritten as

$$\begin{aligned} x_1x_{n-1}+y_1x_{n-1}\sqrt{d}+x_1y_{n-1}\sqrt{d}+y_1y_{n-1}d &= x_n+y_n\sqrt{d}, \\ x_1x_{n-1}-y_1x_{n-1}\sqrt{d}+x_1y_{n-1}\sqrt{d}-y_1y_{n-1}d &= x_{n-2}+y_{n-2}\sqrt{d}. \end{aligned}$$

By adding them, we get (6.1). □

Recurrences (3.7) can be rewritten in a matrix multiplication form:

$$\begin{pmatrix} x_n \\ y_n \end{pmatrix} = \begin{pmatrix} x_1 & dy_1 \\ y_1 & x_1 \end{pmatrix} \begin{pmatrix} x_{n-1} \\ y_{n-1} \end{pmatrix} = \begin{pmatrix} x_1 & dy_1 \\ y_1 & x_1 \end{pmatrix}^n \begin{pmatrix} 1 \\ 0 \end{pmatrix}. \tag{3.9}$$

In addition, we have:

$$\begin{pmatrix} x_n & dy_n \\ y_n & x_n \end{pmatrix} = \begin{pmatrix} x_1 & dy_1 \\ y_1 & x_1 \end{pmatrix} \begin{pmatrix} x_{n-1} & dy_{n-1} \\ y_{n-1} & x_{n-1} \end{pmatrix} = \begin{pmatrix} x_1 & dy_1 \\ y_1 & x_1 \end{pmatrix}^n \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} x_1 & dy_1 \\ y_1 & x_1 \end{pmatrix}^n. \tag{3.10}$$

This matrix form of the recursions allows us to derive useful identities satisfied by the solutions of the Pell equation.

3.4 Solving Pell's equation using continued fractions

We have established that Pell's equation is always solvable and described its set of solutions. However, we still do not know how to determine a *fundamental solution*. The smallest positive solution of Pell's equation can, in principle, be found by inspection: we check whether $1 + dy^2$ is a perfect square for $y = 1, 2, \ldots$. However, this method is inefficient, since even for small values of d, the fundamental solution can be extremely large. For example, the fundamental solution of the equation $x^2 - 61y^2 = 1$ is $(1\,766\,319\,049, 226\,153\,980)$. An effective method is based on the continued fraction expansion of $\sqrt{d}$ into a *simple continued fraction* (described in Section 2.4).

Theorem 3.8. *If $(u, v) \in \mathbb{N}^2$ is a solution of Pell's equation $x^2 - dy^2 = 1$, then $\frac{u}{v}$ is a convergent of the continued fraction expansion of $\sqrt{d}$.*

Proof. Since

$$(u - v\sqrt{d})(u + v\sqrt{d}) = 1, \tag{3.11}$$

we conclude that $u - v\sqrt{d} > 0$ and $\frac{u}{v} > \sqrt{d}$. Also, (3.11) implies that $u - v\sqrt{d} = \frac{1}{u + v\sqrt{d}}$. Hence,

$$\frac{u}{v} - \sqrt{d} = \frac{1}{v(u + v\sqrt{d})} = \frac{1}{v^2\left(\frac{u}{v} + \sqrt{d}\right)} < \frac{1}{2\sqrt{d}v^2} < \frac{1}{2v^2}.$$

Note that $0 < \frac{u}{v} - \sqrt{d} = \left|\frac{u}{v} - \sqrt{d}\right| < \frac{1}{2v^2}$. According to Theorem 2.3 $\frac{u}{v}$ is a convergent of $\sqrt{d}$. □

Remark 3.9. *With slight modifications, it can be shown that the statement of Theorem 3.4 is also valid for all equations of the form $x^2 - dy^2 = N$ where $|N| < \sqrt{d}$.*

Theorem tells us that all positive integer solutions of Pell's equation are among the convergents of $\sqrt{d}$. Moreover, we can determine exactly which convergents are solutions.

Theorem 3.10. *Let r be the length of the period in the continued fraction expansion of $\sqrt{d}$ and let (p_n/q_n) denote the convergents of $\sqrt{d}$.*

If r is even, then the equation $x^2 - dy^2 = -1$ has no solution, and all solutions of $x^2 - dy^2 = 1$ are (p_{nr-1}, q_{nr-1}) for $n \in \mathbb{N}$.

If r is odd, all solutions of $x^2 - dy^2 = -1$ are (p_{nr-1}, q_{nr-1}) for odd $n \in \mathbb{N}$ and all solutions of $x^2 - dy^2 = 1$ are (p_{nr-1}, q_{nr-1}) for even $n \in \mathbb{N}$.

Remark 3.11. *If r is even, then the fundamental solution of $x^2 - dy^2 = 1$ is (p_{r-1}, q_{r-1}). If r is odd, then the fundamental solution of $x^2 - dy^2 = -1$ is $(p_{r-1}, q_{r-1})$and the fundamental solution of $x^2 - dy^2 = 1$ is (p_{2r-1}, q_{2r-1}), since*

$$p_{2r-1} + q_{2r-1}\sqrt{d} = (p_{r-1} + q_{r-1}\sqrt{d})^2.$$

From the previous remark, we now understand why some fundamental solutions of Pell's equation can be very large even for small values of d. So, for $d = 61$ we get

$$\sqrt{61} = [7, \overline{1, 4, 3, 1, 2, 2, 1, 3, 4, 1, 14}],$$

and since the period is large and odd ($r = 11$), the fundamental solution of $x^2 - 61y^2 = 1$ is

$$(x_0, y_0) = (p_{21}, q_{21}) = (1\,766\,319\,049, 226\,153\,980).$$

Assignment 2. .

i) Find the continued fraction of F_{13}/F_{12}, where F_n is nth Fibonacci number. (Use the Euclidean algorithm).

ii) Find the value of the real number $\alpha = [1, 2, \overline{1, 2, 3}]$.

iii) Find the continued fraction of $\alpha = \dfrac{-5+\sqrt{10}}{4}$ using the algorithm (2.9).

iv) Find the continued fraction of $\alpha = \sqrt{29}$ using the algorithm (2.10).

v) With notations as in Theorem 3.5 and 3.7, prove the following sum and subtraction identities*:*

$$\begin{aligned} x_{m\pm n} &= x_m x_n \pm d y_m y_n, \\ y_{m\pm n} &= x_n y_m \pm x_m y_n, \ m \geq n. \end{aligned}$$

In particular, "double angle identities" hold,

$$\begin{aligned} x_{2n} &= 2x_n^2 - 1, \\ y_{2n} &= 2x_n y_n, \ n \geq 0. \end{aligned}$$

Hint: Use (3.10)

vi) Find the fundamental solution of Pell's equation $x^2 - dy^2 = 1$ for $d = 29$ and $d = 39$. Also, list all solutions such that $y < 10^6$.

Determine whether the negative Pell's equation $x^2 - dy^2 = -1$ is solvable for these values of d's?

Chapter 4

Extension of a Diophantine pair to a triple

In Section 1.3 we showed that the problem of extending Diophantine pairs to triples leads to solving certain Pellian equations. Let us briefly recall this connection. Given a Diophantine pair $\{a, b\}$, $a < b$, we seek an element c such that

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

for some $s, t > 0$. By eliminating c from previous two equations, we reduce the problem to a Pell-type equation in two unknowns t and s:

$$at^2 - bs^2 = a - b,$$

which can be rewritten as

$$(at)^2 - abs^2 = a(a - b).$$

Hence, in this chapter we turn to the theory of Pellian equations, i.e., equations of the form

$$X^2 - DY^2 = N.$$

We have already observed that if a Pellian equation is solvable, then it has infinitely many solutions, because the product of a solution to the Pellian equation and a solution to the associated Pell equation yields another solution to the same Pellian equation. Moreover, the specific Pellian equation that arises from our extension problem is always solvable, since one solution comes from the regular extension of the pair $\{a, b\}$, namely $c = a + b + 2r$.

4.1 Pellian equations

Assume that

$$a + b\sqrt{d} \text{ is a solution to the Pellian eq. } x^2 - dy^2 = N$$

and that

$$u + v\sqrt{d} \text{ is a solution to the Pell equation } x^2 - dy^2 = 1.$$

Then

$$(a+b\sqrt{d})(u+v\sqrt{d}) = (ua+vb)+(av+ub)\sqrt{d}$$

is again a solution of $x^2 - dy^2 = N$.

If $a+b\sqrt{d}$ and $a'+b'\sqrt{d}$ are solutions of the Pellian equation, we say that $a'+b'\sqrt{d}$ is *associated* with $a+b\sqrt{d}$ (3.2) if

$$a'+b'\sqrt{d} = (a+b\sqrt{d})(u+v\sqrt{d}),$$

for some solution $u+v\sqrt{d}$ of Pell's equation (3.1).

Proposition 4.1. *The relation of* being associated *is an equivalence relation on the set of all solutions of the Pellian equation* $x^2 - dy^2 = N$.

Proof. We verify the three properties of an equivalence relation:

Reflexivity. Any solution $a+b\sqrt{d}$ is associated with itself because we can multiply it by the trivial solution, $1+0\sqrt{d}$, of Pell's equation .

Symmetry. Assume that

$$a'+b'\sqrt{d} \text{ is associated with } a+b\sqrt{d} \text{ via } u+v\sqrt{d}.$$

By multiplying the expression

$$a'+b'\sqrt{d} = (a+b\sqrt{d})(u+v\sqrt{d})$$

by $u-v\sqrt{d}$ (also a solution of the Pell's equation), we get

$$(a'+b'\sqrt{d})(u-v\sqrt{d}) = a+b\sqrt{d}$$

Hence, $a+b\sqrt{d}$ is associated with $a'+b'\sqrt{d}$.

Transitivity. Assume that

$$a'+b'\sqrt{d} \text{ is associated with } a+b\sqrt{d} \text{ via } u+v\sqrt{d}$$

and that

$$a''+b''\sqrt{d} \text{ is associated with } a'+b'\sqrt{d} \text{ via } u'+v'\sqrt{d}.$$

Then

$$a''+b''\sqrt{d} = (a'+b'\sqrt{d})(u'+v'\sqrt{d}) = (a+b\sqrt{d})(u+v\sqrt{d})(u'+v'\sqrt{d}).$$

Since the product $(u+v\sqrt{d})(u'+v'\sqrt{d})$ is again a solution of the Pell's equation, and thus $a''+b''\sqrt{d}$ is associated with $a+b\sqrt{d}$. □

In the light of Proposition 4.1, we speak of *two associated solutions* of the Pellian equations. Also, all mutually associated solutions form a single *class of solutions.*

The following proposition provides a simple criterion for determining when two solutions are associated.

Proposition 4.2. *Two solution* $a+b\sqrt{d}$ *and* $a'+b'\sqrt{d}$ *of* $x^2-dy^2 = N$ *are* associated *solutions if and only if*

$$aa' \equiv bb'd \pmod{N},\ ab' \equiv a'b \pmod{N}.$$

Proof. We prove both directions of the statement.

Necessity: Left as an exercise. (Part of Assignment 3.)

Sufficiency: The congruences $aa' \equiv bb'd \pmod{N}$ and $ab' \equiv a'b \pmod{N}$, imply that there exist $k, l \in \mathbb{Z}$ such that

$$aa' = bb'd + kN \tag{4.1}$$
$$ab' = a'b + lN. \tag{4.2}$$

Multiplying (4.1) by b' and (4.2) by $-a'$, and adding them we obtain

$$0 = b(\underbrace{b'^2 d - a'^2}_{=-N}) + N(kb' - la').$$

This implies that

$$b = b'k - a'l. \tag{4.3}$$

Similarly, multiplying (4.1) by a' and (4.2) by $-b'd$, and adding them we have

$$a(\underbrace{-b'^2 d + a'^2}_{=N}) = N(a'k - lb'd).$$

So,

$$a = a'k - db'l. \tag{4.4}$$

Now, if we show that (k, l) is a solution to the Pell's equation $x^2 - dy^2 = 1$, then from (4.4) and (4.3) we conclude that (a, b) and (a', b') are associated. Squaring both equations (4.1) and (4.2), and combining them appropriately, we get

$$a^2 a'^2 + b^2 b'^2 d^2 - 2aba'b'd = k^2 N^2,$$

$$a^2 b'^2 + a'^2 b^2 - 2aba'b'd = l^2 N^2.$$

Multiplying the last expression by $-d$ and then adding these two equalities yields to

$$a^2(\underbrace{a'^2 - b'^2 d}_{=N}) - db^2(\underbrace{a'^2 - b'^2 d}_{N}) = (k^2 - dl^2)N^2.$$

Hence,

$$N(a^2 - db^2) = N^2 = (k^2 - dl^2)N^2$$

shows that (k, l) is solution of the Pell's equation. □

Let K be a class of solutions, that is

$$K = \{x_i + y_i\sqrt{d} \,:\, i \in \mathbb{N}\},$$

then the class

$$\overline{K} = \{x_i - y_i\sqrt{d} \,:\, i \in \mathbb{N}\}$$

is called the *conjugate class*. If $K = \overline{K}$ holds, we say that the class K is *ambiguous*. Note that if the class K is generated by a solution $a + b\sqrt{d}$, then the conjugate class $\overline{K}$ is generated by $a - b\sqrt{d}$. Therefore, if $a + b\sqrt{d}$ and $a - b\sqrt{d}$ belong to the same class, i.e., are associated solutions, then $K = \overline{K}$ and the class is ambiguous. In other words, a class is ambiguous

precisely when it is invariant under conjugation. This situation occurs when the generator of the class, say $a + b\sqrt{d}$, is associated with its own conjugate $a - b\sqrt{d}$.

Within a class K, we define the *fundamental solution* as the solution $x^* + y^*\sqrt{d}$ for which y^* is the smallest possible non-negative value among all elements in K. Under this condition, x^* is uniquely determined unless the class K is ambiguous. If K is ambiguous, then we choose x^* such that $x^* \geq 0$. Note that $|x^*|$ has the least possible value within the class K. Such a solution $x^* + y^*\sqrt{d}$ is called the *fundamental solution* of the Pellian equation in the class K.

The following result shows that there are only finitely many classes, that is finitely many fundamental solutions of equation $x^2 - dy^2 = N$.

Theorem 4.3. *Let $u + v\sqrt{d}$ be the fundamental solution of Pell's equation $x^2 - dy^2 = 1$. Then all fundamental solutions $x^* + y^*\sqrt{d}$ of Pellian equation $x^2 - dy^2 = N$ satisfy the inequalities*

$$0 \leq y^* \leq \frac{v}{\sqrt{2(u+\varepsilon)}}\sqrt{|N|},\ |x^*| \leq \sqrt{\frac{1}{2}(u+\varepsilon)|N|}, \tag{4.5}$$

where $\varepsilon = 1$ if $N > 0$ and $\varepsilon = -1$ if $N < 0$.

Proof. Assume that $N < 0$ and let

$$x' + y'\sqrt{d} = (x^* + y^*\sqrt{d})(u - \delta v\sqrt{d}),$$

where

$$\delta = \begin{cases} 1, & x^* \geq 0, \\ -1, & x^* < 0. \end{cases}$$

Apparently $x' + y'\sqrt{d}$ is a solution of $x^2 - dy^2 = N$ that belongs to the class represented with the fundamental solution, $[x^* + y^*\sqrt{d}]$. Hence

$$y' = y^*u - x^*\delta v \geq y^*$$

and

$$0 < \underbrace{x^*\delta}_{|x^*|} v = y^*u - y' \leq y^*(u-1).$$

Squaring the previous inequality, gives

$$x^{*2}v^2 \leq y^{*2}(u^2 - 2u + 1),$$

i.e.

$$v^2(dy^{*2} + N) \leq y^{*2}(u^2 - 2u + 1).$$

Further, we have

$$y^{*2}(\underbrace{dv^2 - u^2}_{-1} + 2u - 1) \leq \underbrace{-N}_{|N|} v^2$$

and this implies the first inequality in (4.5). The second one follows from

$$x^{*2} = dy^{*2} + N \leq -\frac{Nv^2d}{2(u-1)} + N = -N\frac{u-1}{2}.$$

□

4.1.1 Steps for solving the Pellian equation $x^2 - dy^2 = N$

1. **Solve Pell's equation** $x^2 - dy^2 = 1$

   (a) Expand $\sqrt{d}$ into a continued fraction using the following algorithm:

   Continued fraction for $\sqrt{d}$

   Initial terms: $s_0 = 0, \quad t_0 = 1, \quad a_0 = \lfloor \sqrt{d} \rfloor$

   Recurrence relations:

   $$s_{i+1} = a_i t_i - s_i, \quad t_{i+1} = \frac{d - s_{i+1}^2}{t_i}, \quad a_{i+1} = \left\lfloor \frac{s_{i+1} + a_0}{t_{i+1}} \right\rfloor, \quad \text{for } i = 0, 1, 2, \ldots$$

   Termination condition: repeat until $(s_1, t_1) = (s_{r+1}, t_{r+1})$

   We get

   $$\sqrt{d} = [a_0, \overline{a_1, a_2, \ldots, a_{r-1}, 2a_0}],$$

   (b) Find the fundamental solution $u + v\sqrt{d}$ of Pell's equation from the convergents of $\sqrt{d}$ (according to Theorem (3.10) and Remark (3.11)):

   $$u + v\sqrt{d} = p_{r-1} + q_{r-1}\sqrt{d}, \text{ if } r \text{ is even}$$

   $$u + v\sqrt{d} = (p_{r-1} + q_{r-1}\sqrt{d})^2 = p_{2r-1} + q_{2r-1}\sqrt{d}, \text{ if } r \text{ is odd.}$$

   (Here (p_n/q_n) denotes the convergents.)

   Fundamental solution to Pell's equation

   Compute the denominators $q_0, \ldots, q_{r-1}$ of the convergents using the recurrence:

   $$q_n = a_n q_{n-1} + q_{n-2}, \quad q_{-2} = 1, \; q_{-1} = 0, \; n \geq 0.$$

i	-2	-1	0	1	2	...	r_{i-1}
a_i			a_0	a_1	a_2	...	a_{r-1}
q_i	1	0	q_0	q_1	q_2	...	q_{r-1}

   Calculate the numerator of $(r-1)$st convergent: $p_{r-1} = \sqrt{1 + dq_{r-1}^2}$. Then

   $$u + v\sqrt{d} = \begin{cases} p_{r-1} + q_{r-1}\sqrt{d}, & \text{if } r \text{ is even} \\ (p_{r-1} + q_{r-1}\sqrt{d})^2, & \text{if } r \text{ is odd} \end{cases}$$

   (c) Optional step.

All solution to the Pell's equation in $\mathbb{N}$

$$u_n + v_n\sqrt{d} = (u + v\sqrt{d})^n,\ n = 1, 2, \ldots$$

Recurrence relations for sequences (x_n) and (y_n):

$$\begin{array}{rcl} u_n & = & 2uu_{n-1} - u_{n-2}, \\ v_n & = & 2uv_{n-1} - v_{n-2},\ n \geq 2, \end{array}$$

with the initial conditions $(u_1, v_1) = (u, v)$ and $(u_0, v_0) = (1, 0)$.

2. Solve the general Pellian equation $x^2 - dy^2 = N$.

   (a) Find fundamental solutions to $x^2 - dy^2 = N$ (according to Theorem 4).

All fundamentals solution to the Pellian equation

Find all values of y^* satisfying:

$$0 \leq y^* \leq \frac{v}{\sqrt{2(u+\varepsilon)}}\sqrt{|N|},$$

where $\varepsilon = 1$ if $N > 0$ and $\varepsilon = -1$ if $N < 0$.
For each such y^* compute:

$$x^* = \pm\sqrt{N + d(y^*)^2}.$$

This yields a list of fundamental solutions:

$$x_0^{(1)} + y_0^{(1)}\sqrt{d}, \ldots, x_0^{(\ell)} + y_0^{(\ell)}\sqrt{d}$$

To eliminate associated duplicates, apply the criterion from Proposition (4.2)):

$$x_0^{(i)}x_0^{(j)} \equiv y_0^{(i)}y_0^{(j)}d \pmod{N},\ x_0^{(i)}y_0^{(j)} \equiv y_0^{(i)}x_0^{(j)} \pmod{N},\ 1 \leq i < j \leq \ell.$$

The final list of non-associated fundamental solutions is:

$$x_0^{(1)} + y_0^{(1)}\sqrt{d}, \ldots, x_0^{(k)} + y_0^{k)}\sqrt{d},$$

where $k \leq \ell$.

   (b) Generate all solutions

All solution to the Pellian equation

$$x_n^{(j)} + y_n^{(j)}\sqrt{d} = (x_0^{(j)} + y_0^{(j)}\sqrt{d})(u + v\sqrt{d})^n,\ n = 0, 1, 2, \ldots,$$

for $j = 1, \ldots, k$.
Reccurence relations for $(x_n^{(j)})$ and $(y_n^{(j)})$:

$$\boxed{\begin{array}{rcl} x_n^{(j)} & = & 2ux_{n-1}^{(j)} - x_{n-2}^{(j)}, \\ y_n^{(j)} & = & 2uy_{n-1}^{(j)} - y_{n-2}^{(j)},\ n \geq 2. \end{array}}$$

with the initial conditions $(x_0^{(j)}, y_0^{(j)})$ and $(x_1^{(j)}, y_1^{(j)}) = (x_0^{(j)}u + dy_0^{(j)}v, x_0^{(j)}v + y_0^{(j)}u)$, where (u, v) is the fundamental solution of $x^2 - dy^2 = 1$.

Example 3. *Let us solve the equation*

$$x^2 - 6y^2 = -29.$$

The fundamental solution of related Pell equation $x^2 - 6y^2 = 1$ is $5 + 2\sqrt{6}$. According to Theorem , fundamental solutions of $x^2 - 6y^2 = -29$ satisfy the inequalities

$$0 \leq y^* \leq \frac{2}{\sqrt{2 \cdot 4}} \cdot \sqrt{29} < 4,$$

$$0 < |x^*| \leq \sqrt{\frac{1}{2} \cdot 4 \cdot 29} < 8.$$

By testing, we get that the only fundamental solutions are $5 + 3\sqrt{6}$ and $-5 + 3\sqrt{6}$ and they are not associated since

$$5 \cdot (-5) \not\equiv 3 \cdot 3 \cdot 6 \pmod{29}.$$

Hence all integer solutions of $x^2 - 6y^2 = -29$ are

$$x + y\sqrt{6} = \pm(5 + 3\sqrt{6})(5 + 2\sqrt{6})^n,$$

$$x + y\sqrt{6} = \pm(-5 + 3\sqrt{6})(5 + 2\sqrt{6})^n,\ n \in \mathbb{Z}.$$

Example 4. *The equation*

$$x^2 - 82y^2 = 23$$

has no integer solutions. The fundamental solution of related Pell equation $x^2 - 82y^2 = 1$ is $162 + 18\sqrt{82}$. Theorem gives us bounds for the fundamental solution $x^* + y^*\sqrt{82}$. So, $y^* < 5$. We conclude that $x^2 - 82y^2 = 23$ has no integer solutions by testing for $y = 1, 2, 3, 4$.

4.2 Extension of the Diophantine pair $\{1, 3\}$

We seek for $c \in \mathbb{N}$ such that

$$c + 1 = y^2,\ 3c + 1 = x^2.$$

Eliminating c, we obtain the Pellian equation

$$x^2 - 3y^2 = -2.$$

It is easy see that the fundamental solution of related Pell's equation $x^2 - 3y^2 = 1$ is

$$u + v\sqrt{3} = 2 + \sqrt{3}.$$

Now let us find all fundamental solution y^* of $x^2 - 3y^2 = -2$:

$$0 \leq y^* \leq \frac{v}{\sqrt{2(u+\varepsilon)}}\sqrt{|N|}.$$

Here, $N = -2$, $\varepsilon = -1$ and $(u, v) = (2, 1)$. Thus,

$$0 \leq y^* \leq 1 \implies y^* = 1.$$

Next, we compute

$$(x^*)^2 - 3(y^*)^2 = 1 \implies x^* = \pm 1.$$

Therefore, all fundamental solutions of $x^2 - 3y^2 = -2$ are

$$(x^*, y^*) = (\pm 1, 1) \text{ or } \pm 1 + \sqrt{3}.$$

Since

$$1 \cdot (-1) \equiv 1 \cdot 1 \cdot 3 \pmod 2,\ 1 \cdot 1 \equiv 1 \cdots (-1) \pmod 2$$

these solutions are associated. All solution in $\mathbb{N}$ are given by

$$x_n + y_n\sqrt{3} = (1 + \sqrt{3})(2 + \sqrt{3})^n,\ n \geq 0.$$

Here is a list of the first few solutions together with the corresponding values c_n that extend the pair $\{1, 3\}$:

n	$x_n + y_n\sqrt{3}$	$c_n = y_n^2 - 1$
0	$1 + \sqrt{3}$	0
1	$5 + 3\sqrt{3}$	8
2	$19 + 11\sqrt{3}$	120
3	$71 + 41\sqrt{3}$	1680
4	$265 + 153\sqrt{3}$	23408
5	$989 + 571\sqrt{3}$	326040
6	$691 + 2131\sqrt{3}$	4541160
7	$13775 + 7953\sqrt{3}$	63250208
8	$51409 + 29681\sqrt{3}$	880961760

Note that the values of x_n, y_n and c_n grow quite rapidly. In fact, this growth is exponential. Moreover, the products of consecutive c_n's increased by 1 are prefect squares:

$$8 \cdot 120 + 1 = 31^2,\ 120 \cdot 1680 + 1 = 449^2,\ 1680 \cdot 23408 + 1 = 6271^2, \ldots$$

Hence, the Diophantine pair $\{1, 3\}$ can be extended to Diophantine quadruples:

$$\{1, 3, 8, 120\}, \{1, 3, 120, 1680\}, \{1, 3, 1680, 23408\}, \ldots$$

Let us now derive a formula for c_n and demonstrate that the observed properties hold in general. By subtracting the expressions for the solutions:

$$\begin{aligned} x_n + y_n\sqrt{3} &= (1+\sqrt{3})(2+\sqrt{3})^n, \\ x_n - y_n\sqrt{3} &= (1-\sqrt{3})(2-\sqrt{3})^n, \end{aligned}$$

we get

$$\begin{aligned} y_n &= \frac{1}{2\sqrt{3}}\left((1+\sqrt{3})(2+\sqrt{3})^n - (1-\sqrt{3})(2-\sqrt{3})^n\right) \\ &= \frac{1}{2\sqrt{3}}\left((1+\sqrt{3})(2+\sqrt{3})^n - (1-\sqrt{3})(2+\sqrt{3})^{-n}\right). \end{aligned} \tag{4.6}$$

Thus, after simplification, we obtain

$$\begin{aligned} c_n &= y_n^2 - 1 \\ &= \frac{1}{6}\left(-4 + (2-\sqrt{3})^{1+2n} + (2+\sqrt{3})^{1+2n}\right). \end{aligned}$$

We now verify that

$$c_n c_{n+1} + 1 = \square.$$

Indeed,

$$\begin{aligned} c_n c_{n+1} + 1 &= \frac{1}{36}\Big((97-56\sqrt{3})(2-\sqrt{3})^{4n} + 16(4\sqrt{3}-7)(2-\sqrt{3})^{2n} \\ &\quad - 16(7+4\sqrt{3})(2+\sqrt{3})^{2n} + (97+56\sqrt{3})(2+\sqrt{3})^{4n} + 66\Big) \\ &= \frac{1}{36}\left((2+\sqrt{3})^{4+4n} - 16(2-\sqrt{3})^{2+2n} - 16(2+\sqrt{3})^{2+2n} + (2-\sqrt{3})^{4+4n} + 66\right) \\ &= \frac{1}{36}\left((2-\sqrt{3})^{2+2n} + (2+\sqrt{3})^{2+2n} - 8\right)^2 \end{aligned}$$

4.3 Extension of the Diophantine pair $\{k-1, k+1\}$

Here we deal with the extension of a parametric Diophantine pair $\{k-1, k+1\}$ for positive integer $k > 2$. The procedure is the same as in the previous section. So, we are looking for positive integer c and integers x, y such that

$$(k-1)c + 1 = y^2,\ (k+1)c + 1 = x^2.$$

By default, by eliminating c we get the Pellian equation

$$x^2 - (k^2-1)y^2 = -2(k-1). \tag{4.7}$$

Related Pell's equation $x^2 - (k^2-1)y^2 = 1$ has an obvious fundamental solution:

$$(u, v) = (k, 1) \ \text{ or } \ k + \sqrt{k^2-1}.$$

All fundamental solutions of (4.7) satisfy the inequality

$$0 \le y^* \le \frac{v}{\sqrt{2(u+\varepsilon)}}\sqrt{|N|} \ \text{ for } \ N = -2(k-1), \varepsilon = -1, u = k, v = 1.$$

Hence,

$$0 \leq y^* \leq \frac{1}{\sqrt{2(k-1)}}\sqrt{2(k-1)} = 1$$

and $y^* = 1$ and $x^* = \pm(k-1)$. There are two possible fundamental solutions of (4.7):

$$(k-1, 1),\ (-(k-1), 1).$$

These solutions are associated since

$$(k-1)\cdot(-(k-1)) \equiv 1 \cdot 1 \cdot (k^2-1) \pmod{2(k-1)} \iff -2k^2 + 2k \equiv 0 \pmod{2(k-1)}$$

and

$$(k-1)\cdot 1 \equiv 1 \cdot (-(k-1)) \pmod{2(k-1)} \iff 2(k-1) \equiv 0 \pmod{2(k-1)}.$$

So, we reject one fundamental solution. All solutions in positive integers of (4.7) are:

$$x_n + y_n\sqrt{k^2-1} = (k-1+\sqrt{k^2-1})(k+\sqrt{k^2-1})^n,\ n \geq 0.$$

For the extension $c_n = y_n^2 - 1$, we need the expression for y_n which can be obtained by subtracting

$$\begin{aligned} x_n + y_n\sqrt{k^2-1} &= (k-1+\sqrt{k^2-1})(k+\sqrt{k^2-1})^n, \\ x_n - y_n\sqrt{k^2-1} &= (k-1-\sqrt{k^2-1})(k-\sqrt{k^2-1})^n. \end{aligned}$$

Thus,

$$y_n = \frac{1}{2\sqrt{k^2-1}}\left((k-1+\sqrt{k^2-1})(k+\sqrt{k^2-1})^n - (k-1-\sqrt{k^2-1})(k+\sqrt{k^2-1})^{-n}\right)$$

After simplification we have

$$c_n = \frac{1}{2(k^2-1)}\left((k+\sqrt{k^2-1})^{2n+1} + (k-\sqrt{k^2-1})^{2n+1} - 2k\right)$$

and the product of two consecutives c_n and c_{n+1} plus 1 is a perfect square:

$$c_n c_{n+1} + 1 = \left(\frac{1}{2(k^2-1)}\left((k+\sqrt{k^2-1})^{2n+2} + (k-\sqrt{k^2-1})^{2n+2} - 2k^2\right)\right)^2.$$

Finally, we showed that

$$\{k-1, k+1, c_n, c_{n+1}\}$$

is a Diophantine quadruple for $n > 0$.

Assignment 3. *(i) Find all non-associated fundamental solutions of*

$$x^2 - 7y^2 = 57.$$

(ii) Find all c's such that $\{8, 15, c\}$ is a Diophantine triple and $c < 10^{10}$.

Chapter 5

Extension of a Diophantine triple to a quadruple

5.1 Linear forms in logarithms

5.1.1 Brief historical overview

In this chapter, we describe the key results from Baker's theory of linear forms in logarithms of algebraic numbers. These results will be used to solve simultaneous Pell equations.

We begin with a brief overview of the historical development of the theory. In 1900, at the International Congress of Mathematicians in Paris, David Hilbert presented a list of 23 problems he believed would be solved in the next century, and that their solution would require the development of new methods. One of these was **Hilbert's Seventh Problem**, which asked for a proof of the transcendence of the number α^β for any algebraic number $\alpha \neq 0, 1$ and any irrational algebraic number β.

This problem was solved in 1934 independently by Gelfond and Schneider. Their result, now known as the *Gelfond–Schneider Theorem*, states that if $\alpha_1, \alpha_2 \neq 0$ are algebraic numbers such that $\log \alpha_1$ and $\log \alpha_2$ are linearly independent over $\mathbb{Q}$, then

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

for all algebaric numbers β_1 and β_2. In 1935, Gelfond also obtained a lower bound for the linear form

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

During the 1940s, he recognized that generalizing this result could enable the solution of various problems in number theory.

In 1966, the British mathematician **Alan Baker** achieved this generalization. He proved the following:

If

- $\alpha_1, \ldots, \alpha_n, \beta_1, \ldots, \beta_n$ are non-zero algebraic numbers different from 1,
- $\beta_1, \ldots, \beta_n$ are irrational,
- the set $\{1, \beta_1, \ldots, \beta_n\}$ is linearly independent over $\mathbb{Q}$,

then the number

$$\alpha_1^{\beta_1}\alpha_2^{\beta_2}\cdots\alpha_n^{\beta_n}$$

is **transcedental**. Additionally, Baker proved that for any algebraic number α_{n+1}

$$\alpha_1^{\beta_1}\alpha_2^{\beta_2}\cdots\alpha_n^{\beta_n} \neq \alpha_{n+1},$$

and the absolute value $|\alpha_1^{\beta_1}\alpha_2^{\beta_2}\cdots\alpha_n^{\beta_n} - \alpha_{n+1}|$ cannot be "very small".

The most important part of that was that Baker got an effective result in the form of lower bound for the apsolute value of linear form of logarithms of algebraic numbers. This result is known as *Baker's theorem* and it is a powerful tool in solving various problems in number theory, especially related to Diophantine equations. In 1970, Baker was awarded the Fields Medal for his contributions.

The problem of finding a lower bound for

$$\Lambda^* = \alpha_1^{\beta_1}\cdots\alpha_n^{\beta_n} - 1$$

(for $\Lambda^* \neq 0$) can be reduced to estimating a linear form in logarithms:

$$\Lambda = \beta_1 \log\alpha_1 + \cdots + \beta_n \log\alpha_n \neq 0,$$

since $\lim_{x\to 0}\frac{\log(1+x)}{x} = 1$ and $\log(1+x) \approx x$ for small values of x. Also, $\Lambda^* = 0$ if and only if $\Lambda = 0$.

5.1.2 An overview of the most important theorems

We now present the original Baker's theorem on linear forms in logarithms of algebraic numbers, along with several variants relevant to the solution of simultaneous Pell equations. We begin by defining some standard terms and notation.

Definition 5.1. *A* linear form in logarithms of algebraic numbers *is an expression of the form*

$$\Lambda = \beta_1 \log\alpha_1 + \ldots + \beta_n \log\alpha_n,$$

where α_i, β_i, $i = 1,\ldots,n$ *complex algebraic numbers and* log *denotes the principle value (branch) of the complex logarithm.*

In our applications, the coefficients $\beta_1,\ldots,\beta_n$ will be integers and denoted by $b_1,\ldots,b_n$. Furthermore, $\alpha_1,\ldots,\alpha_n$ will be real algebraic numbers. So, log is the natural logarithm.

It is useful to recall the following terms:

- *Algebraic number* - a number that is a root of a nonzero polynomial in one variable with integer (or rational) coefficients.
- *Minimal polynomial of an algebraic number* - a unique monic polynomial with rational coefficients of least degree that has the number as a root.
- *Degree of an algebraic number* - an algebraic number is said to be of degree d if its minimal polynomial has degree d.

- *Algebraic number field* - an extension field K of the field of rational numbers $\mathbb{Q}$ such that the field extension $K/\mathbb{Q}$ has a finite degree. (The degree means the dimension of the field K as a vector space over $\mathbb{Q}$.) Every subfield of $\mathbb{C}$ having finite degree over $\mathbb{Q}$ is of the form $\mathbb{Q}(\alpha)$ for some algebraic number $\alpha \in \mathbb{C}$. If α is a root of an irreducible polynomial over $\mathbb{Q}$ having degree d, then

$$\mathbb{Q}(\alpha) = \{a_0 + a_1\alpha + \cdots + a_{d-1}\alpha^{d-1} \,:\, a_0, \ldots, a_{d-1} \in \mathbb{Q}\}$$

  and representation in this form is unique. In other words, $\{1, \alpha, \ldots, \alpha^{d-1}\}$ is a basis for $\mathbb{Q}(\alpha)$ as a vector space over $\mathbb{Q}$.

The following theorem is the original Baker's theorem on linear form in logarithms of algebraic numbers.

Theorem 5.2 (Baker, 1968)**.** *Suppose that $k \geq 2$, and that $\alpha_1, \ldots, \alpha_k$ are non-zero algebraic numbers, whose degrees do not exceed d and whose heights do not exceed A, where $d \geq 4$ and $A \geq 4$. If the rational integers $b_1, \ldots, b_k \in \mathbb{Q}$ satisfy*

$$0 < |b_1 \log \alpha_1 + \cdots + b_k \log \alpha_k| < e^{-\delta H},$$

where $0 < \delta \leq 1$ and

$$H = \max\{|b_1|, \ldots, |b_k|\},$$

then

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

Note: Here, the term *height* refers to the *naive height*, defined as the maximum absolute value of the coefficients of the minimal polynomial of the algebraic number.

Over time, the bound in Baker's theorem has been improved, among other things, using more sophisticated definitions of height (of an algebraic number).

On heights of algebraic numbers

The height of algebraic number is a key concept in Diophantine approximation. Assume that α is an algebraic number of degree d and its minimal polynomial over $\mathbb{Z}$ is

$$p(x) = a_d x^d + \cdots + a_2 x + a_0 = a_d \prod_{i=1}^{d}(x - \alpha_i),\ a_0, \ldots, a_d \in \mathbb{Z}, \tag{5.1}$$

where $\alpha_1 = \alpha$ and $\alpha_2, \ldots, \alpha_n$ are the complex conjugates (roots) of α.

- *Standard* or *naive height*:

$$H(\alpha) = \max\{|a_0|, |a_1|, \ldots, |a_d|\}. \tag{5.2}$$

- *Mahler measure*:

$$M(\alpha) = |a_d| \prod_{i=1}^{d} \max\{1, |\alpha_i|\}.$$

  (It captures both the size of the coefficients and the size of the roots outside the unit circle.)

- **Absolute logarithmic height** or standard **Weil's height**:

$$h(\alpha) = \frac{1}{d} \log M(\alpha),$$

that is

$$h(\alpha) = \frac{1}{d} \left(\log |a_d| + \sum_{i=1}^{d} \underbrace{\log \max\{1, |\alpha_i|\}}_{=\max\{0, \log|\alpha_i|\}} \right). \tag{5.3}$$

We may say that $h(\alpha)$ roughly measures how "arithmetically complex" α is, i.e. how large the coefficients in its minimal polynomial are and how large its conjugates are.

Example 5. *Let's compute the Weil's height of the golden ratio,*

$$\alpha = \frac{1+\sqrt{5}}{2}.$$

The minimal polynomial of α over $\mathbb{Q}$ is

$$p(x) = x^2 - x - 1 = \left(x - \underbrace{\frac{1+\sqrt{5}}{2}}_{\approx 1.618} \right) \left(x - \underbrace{\frac{1-\sqrt{5}}{2}}_{\approx -0.618} \right)$$

So, α is an algebraic number of degree 2. Its Weil's height is

$$h(\alpha) = \frac{1}{2} \left(\log 1 + \max\{0, \log \frac{1+\sqrt{5}}{2}\} + \max\{0, \log \frac{-1+\sqrt{5}}{2}\} \right) = \frac{1}{2} \log \frac{1+\sqrt{5}}{2} \approx 0.2406$$

In improved versions of Baker's theorem, the following *modified heights* are used:

$$h'(\alpha) = \max\{Dh(\alpha), \log|\alpha|, 0.16\},$$

and

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

where $d \mid D$.

Variants of Baker's theorem

Theorem 5.3 (Baker-Wüstholz, 1993)**.** *Let*

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

where α_i are algebraic numbers and the coefficients b_i are integers, $i = 1, \ldots, n$. Then

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

where D degree of the field extension $\mathbb{Q}(\alpha_1, \ldots, \alpha_n)$, $B = \max\{|b_1|, \ldots, |b_n|\}$.

(The degree of the field extension $\mathbb{Q}(\alpha_1, \ldots, \alpha_n)$ over $\mathbb{Q}$, denoted $D = [\mathbb{Q}(\alpha_1, \ldots, \alpha_n) : \mathbb{Q}]$, is the degree of the smallest field containing all $\alpha_1, \ldots, \alpha_n$ and $\mathbb{Q}$.)

Theorem 5.4 (Matveev, 2001)**.** *With the assumptions from Theorem 5.3, we have*

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

where $A_i \geq h'(\alpha_i)$, $i = 1, \ldots, n$.

5.1.3 The Baker–Davenport reduction method

In this section, we present a result known as the Baker–Davenport reduction, which we will frequently use to sharpen upper bounds for the size of solutions to Diophantine equations. We state a practical version of the reduction method, as given in [14], which we will apply throughout this work:

Lemma 5.5 (Baker–Davenport Reduction)**.** *Let κ, μ be real numbers and $N \in \mathbb{N}$. Let $\frac{p}{q}$ be a convergent of the continued fraction expansion of κ such that $q > 6N$. Define*

$$\varepsilon = ||\mu q|| - N \cdot ||\kappa q||,$$

where $||x||$ denotes the distance from x to the nearest integer. If $\varepsilon > 0$, then for any constants $A > 0$ and $B > 1$, the inequality

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

has no solutions in natural numbers m and n satisfying

$$\frac{\log\left(\frac{Aq}{\varepsilon}\right)}{\log B} \leq n \leq N.$$

Proof. Assume $1 \leq n \leq N$. Then we have:

$$0 < n(\kappa q - p) + np - mq + \mu q < qAB^{-n},$$

which implies

$$qAB^{-n} > |\mu q - (mq - np)| - n||\kappa q|| \geq ||\mu q|| - N||\kappa q|| = \varepsilon,$$

and consequently,

$$n < \frac{\log\left(\frac{Aq}{\varepsilon}\right)}{\log B}.$$

□

Remark 5.6. *The condition $q > 6N$ in Lemma 5.5 is somewhat arbitrary. On the one hand, we want to increase the likelihood that $\varepsilon > 0$ holds; on the other hand, we prefer smaller values of q to obtain tighter bounds. From the properties of continued fractions, we know that $\|\kappa q\| < \frac{1}{q}$, while in general, we have no control over $\|\mu q\|$. For this reason, it is reasonable to assume $q > 2N$, and the choice $q > 6N$ has been found to work well in practice.*

Remark 5.7. *If the condition $\varepsilon > 0$ is not satisfied, one may try using the next convergent of κ and check whether the condition is then fulfilled.*

5.2 Extension of the Diophantine Triple $\{1, 3, 8\}$

In this section, we demonstrate how the application of Baker's theory of linear forms in logarithms of algebraic numbers—specifically, using Baker–Wüstholz's theorem 5.3 or a similar result—can be used to prove following theorem:

Theorem 5.8 (Baker, Davenport, 1969)**.** *If* $\{1, 3, 8, d\}$ *is a Diophantine quadruple, then* $d = 120$*.*

As previously mentioned, this was first accomplished by Baker and Davenport in [2]. The problem was introduced to them by J.H. van Lint (in March 1968), who had proved Theorem 5.8 under the assumption $d < 10^{1\,700\,000}$.

Assume d is a natural number such that $\{1, 3, 8, d\}$ forms a Diophantine quadruple. Then there exist $x, y, z \in \mathbb{N}$ satisfying:

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

By eliminating d from the above equations, we obtain the system of Pell-type equations:

$$y^2 - 3x^2 = -2, \tag{5.4}$$
$$z^2 - 8x^2 = -7. \tag{5.5}$$

Thus, the problem of extending the Diophantine triple $\{1, 3, 8\}$ is equivalent to solving the system (5.4)–(5.5). One solution is clearly $(1, 1, 1)$, which corresponds to the *trivial extension* $d = 0$. Another solution, $(11, 19, 31)$, yields the extension $d = 120$. Our aim is to determine whether any other solutions exist. First, we note that there can only be finitely many such solutions, which follows from the following theorem from [23]:

Theorem 5.9 (Siegel, 1926)**.** *Let* $f(x)$ *be a polynomial with integer coefficients having at least three distinct complex roots. Then the equation*

$$y^2 = f(x)$$

has only finitely many integer solutions.

Multiplying equations (5.4) and (5.5), and denoting $t = yz$, yields the equation

$$t^2 = (3x^2 - 2)(8x^2 - 7),$$

which, by Theorem 5.9, has finitely many integer solutions. Hence, there are only finitely many possible extensions of the set $\{1, 3, 8\}$.

The approach taken by Baker and Davenport in their paper involved the following steps:

(i) Express all solutions of the equations (5.4) and (5.5) using sequences involving powers of quadratic irrationalities.

(ii) Derive an inequality involving an integer linear combination of logarithms of algebraic numbers, i.e., a so-called linear form in logarithms.

(iii) Use Baker's result, which provides a lower bound for such linear forms, to find $X > 0$ such that the system (5.4)–(5.5) has no solution for $x > X$.

(iv) Reduce the upper bound X using the method described in Section 5.1.3, which was originally detailed in [2].

Solutions of equations

In Section 4.2 we found all of (5.4), see (4.6) with the note that in this part we have swapped the unknowns x and y. So, x is a solution in positive integers of (5.4) if $x = v_m$, for some $m \geq 0$, where

$$v_m = \frac{1+\sqrt{3}}{2\sqrt{3}}(2+\sqrt{3})^m - \frac{1-\sqrt{3}}{2\sqrt{3}}(2+\sqrt{3})^{-m}, \quad m \geq 0.$$

Now consider equation (5.5). The fundamental solution of the related Pell equation $z^2 - 8x^2 = 1$ is $(u, v) = (3, 1)$. By Theorem 4, we obtain:

$$0 \leq x^* \leq \frac{\sqrt{7}}{2}, \quad |z^*| \leq \sqrt{7}.$$

Thus, $(z^*, x^*) \in \{(1, 1), (-1, 1)\}$. By Proposition 4.2, these solutions are not associated, so all solutions (z, x) in positive integers of (5.5) are given by

$$z + x\sqrt{8} = (\pm 1 + \sqrt{8})(3+\sqrt{8})^n, \quad n \geq 0,$$

which leads to

$$2x\sqrt{8} = (\pm 1 + \sqrt{8})(3+\sqrt{8})^n - (\pm 1 - \sqrt{8})(3-\sqrt{8})^n, \quad n \geq 0. \tag{5.6}$$

As in the previous case, we define sequences $(w_n)_{n\geq 0}$ and $(w'_n)_{n\geq 0}$ to represent all solutions in x:

$$w_n = \frac{1+\sqrt{8}}{2\sqrt{8}}(3+\sqrt{8})^n - \frac{1-\sqrt{8}}{2\sqrt{8}}(3+\sqrt{8})^{-n},$$
$$w'_n = \frac{-1+\sqrt{8}}{2\sqrt{8}}(3+\sqrt{8})^n - \frac{-1-\sqrt{8}}{2\sqrt{8}}(3+\sqrt{8})^{-n}.$$

Finding x that satisfies both equations (5.4) and (5.5) is equivalent to finding non-negative integers m and n such that

$$v_m = w_n \text{ or } v_m = w'_n,$$

that is, to finding the intersections of sequences (v_m) with (w_n) and (v_m) with (w'_n). These sequences intersect for $m = n = 0$ and $m = n = 2$, yielding $d = 0$ (trivial) and $d = 120$. In what follows, we show that these are the only such intersections.

Application of Baker's Theory of Linear Forms in Logarithms

Here, we demonstrate how Baker and Davenport, in [2], applied Theorem 5.2, which concerns lower bounds for linear forms in logarithms of algebraic numbers.

Assume $v_m = w_n$ for some $m, n \geq 2$, i.e.,

$$\frac{1+\sqrt{3}}{\sqrt{3}}(2+\sqrt{3})^m - \frac{1-\sqrt{3}}{\sqrt{3}}(2+\sqrt{3})^{-m} = \frac{1+\sqrt{8}}{\sqrt{8}}(3+\sqrt{8})^n - \frac{1-\sqrt{8}}{\sqrt{8}}(3+\sqrt{8})^{-n} = 2x. \tag{5.7}$$

Note that $(2+\sqrt{3})^{-m}$ and $(3+\sqrt{8})^{-n}$ tend to zero as $n, m \to \infty$. Therefore, we focus on the dominant contributions in these expressions and define

$$P = \frac{1+\sqrt{3}}{\sqrt{3}}(2+\sqrt{3})^m, \quad Q = \frac{1+\sqrt{8}}{\sqrt{8}}(3+\sqrt{8})^n.$$

For sufficiently large m and n, if $v_m = w_n$, then $P \approx Q$. Since $2+\sqrt{3} < 3+\sqrt{8}$, we expect $m \geq n$. That can be shown precisely. In terms of P and Q (5.7) becomes

$$P + \frac{2}{3}P^{-1} = Q + \frac{7}{8}Q^{-1}.$$

From the inequality

$$P - Q = \frac{7}{8}Q^{-1} - \frac{2}{3}P^{-1} > \frac{2}{3}(Q^{-1} - P^{-1}) = \frac{2}{3}(P-Q)Q^{-1}P^{-1},$$

it follows that $P > Q$, hence $m \geq n$. Define

$$\Lambda = \log\left(\frac{P}{Q}\right) = m\log(2+\sqrt{3}) - n\log(3+\sqrt{8}) + \log\left(\frac{(1+\sqrt{3})\sqrt{8}}{(1+\sqrt{8})\sqrt{3}}\right).$$

Then Λ is a linear form in logarithms of the algebraic numbers

$$\alpha_1 = 2+\sqrt{3}, \quad \alpha_2 = 3+\sqrt{8}, \quad \alpha_3 = \frac{(1+\sqrt{3})\sqrt{8}}{(1+\sqrt{8})\sqrt{3}},$$

and since $P/Q > 1$, clearly $\Lambda > 0$. If we can show $\Lambda < e^{-m}$, Baker's theorem 5.2 yields an explicit upper bound on m.

We have

$$P - Q = \frac{7}{8}Q^{-1} - \frac{2}{3}P^{-1} = \frac{7}{8}(P - \frac{7}{8})^{-1} - \frac{2}{3}P^{-1} < \frac{1}{4}P^{-1},$$

since $Q > P - \frac{7}{8}Q^{-1} > P - \frac{7}{8}$ and when $P > 80$ for $m \geq 3$. Therefrom,

$$0 < \Lambda = \log\frac{P}{Q} = -\log\left(1 - \frac{P-Q}{P}\right) < \frac{1}{4}P^{-2} + \left(\frac{1}{4}P^{-2}\right)^2 < 0.26P^{-2},$$

where in the previous inequality we used that

$$-\log(1-x) < x + x^2, \quad \text{for} \quad |x| < 0.5.$$

Hence

$$\Lambda < 0.26\left(\frac{1+\sqrt{3}}{\sqrt{3}}\right)^{-2}(7+4\sqrt{3})^{-m} < 13^{-m} < e^{-m}. \tag{5.8}$$

Since we want to calculate an upper bound for m using Baker's theory, we need to determine the minimal polynomials of the algebraic numbers $\alpha_1, \alpha_2, \alpha_3$. We get

$$\begin{aligned} p_1(t) &= t^2 - 4t + 1, \\ p_2(t) &= t^2 - 6t + 1, \\ p_3(t) &= 441t^4 - 2016t^3 + 2880t^2 - 1536t + 256, \end{aligned}$$

respectively. We first apply the original Baker's theorem 5.2. The inputs to this theorem are:

- $d = 4$, since α_1 and α_2 are of degree 2, and α_3 is of degree 4,
- $A = \max\{H(\alpha_1), H(\alpha_2), H(\alpha_3)\} = 2880$ where denotes the naive height of $H(\alpha_i)$ (see (5.2)),

- $H = \max\{b_1 = m, |b_2| = n, b_3 = 1\} = m$ $(k = 3)$,
- $\delta = 1$.

Therefore, if $v_m = w_n$, Theorem 5.2 yields

$$n \leq m < 10^{487}.$$

This means that the equation $v_m = w_n$ has no solution for $m \geq 10^{487}$.

Now, we also apply a stronger version of Theorem 5.2, namely the Baker–Wüstholz theorem (Theorem 5.3), to compare the bounds for m. In the notation of that theorem, the coefficients b_i and the numbers α_i, $i = 1, 2, 3$, are as before. Since $\mathbb{Q}(\alpha_1, \alpha_2, \alpha_3) = \mathbb{Q}(\alpha_3)$, it follows that $D = 4$.

IWe compute the standard logarithmic (Weil) heights of the algebraic numbers using the formula

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

where a_d is the leading coefficient of the minimal polynomial of α, d is the degree of α, and the $\alpha^{(i)}$ are the roots (i.e., conjugates) of the minimal polynomial of α. We obtain

$$\begin{aligned} h(\alpha_1) &= \frac{1}{2} \log \alpha_1 < 0.66, \\ h(\alpha_2) &= \frac{1}{2} \log \alpha_2 < 0.89, \\ h(\alpha_3) &= \frac{1}{4} \log(441 \alpha_3 \alpha_3') < 1.88, \end{aligned}$$

where $\alpha_3' = \frac{4}{21}(\sqrt{3(2+\sqrt{3})} - 2(3+\sqrt{3})) > 1$ and the other two roots of p_3 are less than 1 in absolute value.The modified heights are computed as

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

so we see that $h''(\alpha_i) = h(\alpha_i)$, $i = 1, 2, 3$.

Now the estimate from Theorem 5.3 becomes

$$\log \Lambda > -18(3+1)!3^{3+1}(32 \cdot 4)^{3+2} \log(2 \cdot 3 \cdot 4) 0.66 \cdot 0.89 \cdot 1.88 \log m > -4.22 \cdot 10^{15} \log m,$$

and comparing with (5.8), we get

$$-m \log 13 > -4.22 \cdot 10^{15} \log m,$$

which implies

$$\frac{m}{\log m} < 1.65 \cdot 10^{15}.$$

Since the function $m \mapsto \frac{m}{\log m}$ is increasing, the above inequality fails for sufficiently large m. Specifically, for

$$m > 6.4 \cdot 10^{16}, \tag{5.9}$$

we obtain a contradiction with (5.9). Therefore, if $v_m = w_n$, then

$$n \leq m < 6.4 \cdot 10^{16},$$

which is a significantly better bound for the indices m and n than the one provided by Theorem 5.2.

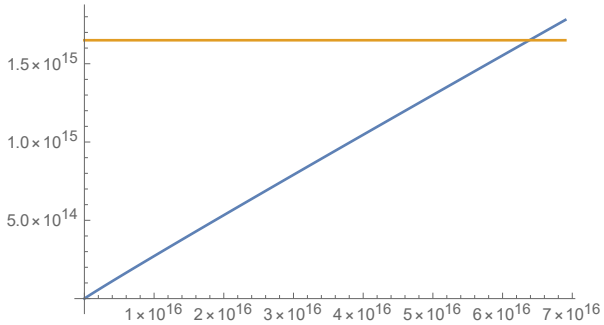

Figure 5.1: $x \mapsto \frac{x}{\log x}$, $x \mapsto 1.65 \cdot 10^{15}$

5.2.1 Application of the Baker–Davenport reduction method

In the previous section, we showed that $\Lambda < 13^{-m}$ and $m < M$ where $M = 6.4 \cdot 10^{16}$. Dividing the inequality

$$0 < m \log \alpha_1 - n \log \alpha_2 + \log \alpha_3 < 13^{-m}.$$

by $\log \alpha_2$ we obtain

$$0 < m \frac{\log \alpha_1}{\log \alpha_2} - n + \frac{\log \alpha_3}{\log \alpha_2} < \frac{1}{\log \alpha_2} 13^{-m}, \tag{5.10}$$

which corresponds exactly to the inequality that appears in Lemma 5.5. With the notation

$$\kappa = \frac{\log \alpha_1}{\log \alpha_2}, \ \mu = \frac{\log \alpha_3}{\log \alpha_2}, \ A = \frac{1}{\log \alpha_2}, \ B = 13,$$

Lemma 5.5 implies that inequality (5.10) has no solution in natural numbers m and n such that

$$\frac{\log\left(\frac{Aq}{\varepsilon}\right)}{\log B} \leq m \leq M, \tag{5.11}$$

where $\frac{p}{q}$ is a convergent from the continued fraction expansion of κ such that $q > 6M$, and $\varepsilon = ||\mu q|| - M \cdot ||\kappa q|| > 0$.

The first convergent satisfying $q > 6M$ is 36th convergent, no $\varepsilon < 0$ not all conditions of the lemma are fulfilled. The next one, the 37. th convergent, satisfies both conditions:

$$q = 3\,075\,296\,607\,888\,933\,649 > 6M, \ \varepsilon \approx 0.295,$$

so according to (5.11), the **new** bound is $M = 16$.

The 7th convergent, $q = 518$, satisfies the lemma's conditions for $M = 16$ (and $\varepsilon \approx 0.0262$) so the bound is further reduced to just $M = 4$.

An analogous procedure, as described in Sections 5.2 and 5.2.1, is carried out for the equation $v_m = w'_n$, $m, n \geq 2$, after which the proof of Theorem 5.8 is finally completed.

Remark 5.10. *The extension problem of the parametric Diophantine triple $\{k-1, k+1, 4k\}$is considerably more complex and requires additional techniques, such as the congruence method and the application of results from Diophantine approximations, particularly the hypergeometric method (see [10]).*

```
M = N[6.4 * 10^16, 100];
m = 2; q = Denominator[Convergents[κ][[m]]]; M6 = 6 * M;
While[q < M6, m = m + 1; q = Denominator[Convergents[κ][[m]]];
 miq = μ * q;
 kappaq = κ * q;
 ϵ = Min[miq - Floor[miq], Ceiling[miq] - miq] - M * Min[kappaq - Floor[kappaq], Ceiling[kappaq] - kappaq];
Print[m - 1, "th conv", " , ", "q=", q, " , ", "ϵ=", N[ϵ, 3]];
While[ϵ < 0, m = m + 1; q = Denominator[Convergents[κ][[m]]];
  miq = μ * q; kappaq = κ * q;
  ϵ = Min[miq - Floor[miq], Ceiling[miq] - miq] - M * Min[kappaq - Floor[kappaq], Ceiling[kappaq] - kappaq]];
Print[m - 1, "th conv", " , ", "q=", q, " , ", "ϵ=", N[ϵ, 3]];
Print["new bound is ", Log[A * q / ϵ] / Log[B]]
```

```
36th conv , q=993 522 360 732 597 120 , ϵ=-0.0124086
37th conv , q=3 075 296 607 888 933 649 , ϵ=0.296501
new bound is 16.8498
```

Figure 5.2: Reduction algorithm (WolframAlpha)

Assignment 4. *Show that the Diophantine triple* $\{1, 8, 15\}$ *extends uniquely to a Diophantine quadruple. Apply the Baker-Wüstholz Theorem 5.3 and reduction method to one pair of sequences obtained by solving the related Pellian equations.*

Chapter 6

Diophantine quadruples with the property $D(n)$

Definition 6.1. *Let n be an integer. A set of integers $\{a_1, a_2, \ldots, a_m\}$ is said to have the* ***Diophantine property*** *$D(n)$ if the product of any two distinct elements of the set, increased by n, is a perfect square; that is, if*

$$a_i a_j + n = n_{ij}^2, \quad 1 \leq i < j \leq m \tag{6.1}$$

for some $n_{ij} \in \mathbb{Z}$. If all elements of the set are nonzero, i.e. $a_i \neq 0$, $i = 1, \ldots, m$, then such a set is called a ***Diophantine m-tuple with the property*** *$D(n)$, or more briefly, a $D(n)$, or more briefly, a $D(n)$-m-tuple.*

Remark 6.2. *Definition 6.1 generalizes the classical notion of a Diophantine m-tuple. Specifically, a* Diophantine m-tuple with the property $D(1)$ *is exactly a classical* Diophantine m-tuple.

Proposition 6.3. *Let $\{a_1, a_2, \ldots, a_m\}$ be a Diophantine m-tuple with the property$D(n)$. Then for every $w \in \mathbb{Z}$, $w \neq 0$,*

$$\{a_1 w, a_2 w, \ldots, a_m w\}$$

is a Diophantine m-tuple with the property $D(nw^2)$.

Proof. Multiplying the relations in (6.1) by w^2, we obtain

$$(a_i w)(a_j w) + nw^2 = (n_{ij} w)^2, \ 1 \leq i < j \leq m,$$

from which the proposition follows directly. □

Example 6. *Multiplying the rational Diophantine quadruple*

$$\left\{\frac{1}{16}, \frac{33}{16}, \frac{17}{4}, \frac{105}{16}\right\}$$

by 16 *yields the Diophantine $D(256)$ quadruple: $\{1, 33, 68, 105\}$*

Remark 6.4. *Proposition 6.3 can also be applied to rational Diophantine m-tuples with the property $D(n)$, as we saw in the previous example. In such cases, if we are interested only in integer sets, we must verify that the set $\{a_1 w, a_2 w, \ldots, a_m w\} \subset \mathbb{Z}$, and if $n \notin \mathbb{Z}$, and that if $n \notin \mathbb{Z}$, then $nw^2 \in \mathbb{Z}$.*

We aim to describe the set of all integers n for which there exists a Diophantine quadruple with the property $D(n)$. Parametric, or polynomial, formulas for $D(n)$-quadruples play an important role in addressing this problem. We will describe their construction in the next section. First, let us highlight an immediate consequence of Proposition 6.3, based on the fact that there exist infinitely many Diophantine quadruples with the property $D(1)$.

Corollary 6.5. *For every $l \in \mathbb{Z}$, $l \neq 0$, there exist infinitely many Diophantine quadruples with the property $D(l^2)$.*

6.1 Polynomial formulas for $D(n)$-quadruples

Since the elements of our Diophantine sets, i.e. $D(n)$-m-tuples, will be polynomials in one or more variables with integer (and sometimes rational) coefficients, we adopt the following convention: we say that a set of polynomials has the property $D(P)$ if the product of any two distinct elements, increased by P, is equal to the square of some polynomial with integer (or rational) coefficients.

The idea behind constructing polynomial Diophantine sets can be illustrated by the following set of polynomials:

$$\{x, x+2, 4x+4, 9x+6\}.$$

Verifying the condition (6.1) for $n = 1$, we obtain:

$$x(x+2)+1 = (x+1)^2, x(4x+4)+1 = (2x+1)^2, x(9x+6)+1 = (3x+1)^2,$$

$$(x+2)(4x+4)+1 = (2x+3)^2, \underline{(x+2)(9x+6)+1 = 13+24x+9x^2}, (4x+4)(9x+6)+1 = (6x+5)^2,$$

from which we can conclude that this set of polynomials is *almost* a Diophantine quadruple. What is missing is the "underlined condition", i.e. the condition that the product of the second and fourth elements, increased by one, yields the square of some linear polynomial. Therefore, if there exists a rational number x that satisfies the equation

$$(x+2)(9x+6)+1 = y^2,$$

then the given set is a (rational) Diophantine quadruple. It turns out that one solution is $(x, y) = (\frac{1}{16}, \frac{61}{16})$ which corresponds precisely to the rational quadruple discovered by Diophantus himself.

Let $\{a, b\}$ be an arbitrary set with the property $D(n)$ for some integer n. Then, by definition, there exists an $x \in \mathbb{Z}$ such that

$$ab + n = x^2. \tag{6.2}$$

We can extend the set $\{a, b\}$ to the set $\{a, b, a+b+2x\}$. Let's verify that the new set also has the $D(n)$ property:

$$a(a+b+2x)+n = a^2+ab+2ax+n = a^2+2ax+x^2 = (a+x)^2, \tag{6.3}$$

and similarly

$$b(a+b+2x)+n = (b+x)^2. \tag{6.4}$$

To obtain a quadruple, we apply the same construction to the set

$$\{b, a+b+2x\},$$

that is we add the element

$$b + (a + b + 2x) + 2(b + x) = a + 4b + 4x.$$

Hence, the triple $\{b, a+b+2x, a+4b+4x\}$ has the property $D(n)$. Similarly to (6.3) and (6.4) we have

$$b(a + 4b + 4x) + n = (b + (b + x))^2 = (2b + x)^2, \tag{6.5}$$

$$(a + b + 2x)(a + 4b + 4x) + n = (a + b + 2x + (b + x))^2 = (a + 2b + 3x)^2, \tag{6.6}$$

assuming that (6.2) holds.

Now consider the set

$$\{a, b, a + b + 2x, a + 4b + 4x\}. \tag{6.7}$$

It is easy to see that (6.7) is almost a set with the property $D(n)$. Out of the six conditions that should be satisfied, five are fulfilled, namely (6.2)–(6.6). Therefore, we conclude that (6.7) has the $D(n)$ property if and only if the product of the first and fourth elements, increased by n, is a perfect square, that is, if and only if

$$a(a + 4b + 4x) + n = y^2, \tag{6.8}$$

for some $x, y \in \mathbb{Z}$. Let us expand this equation and use (6.2):

$$\begin{aligned} a^2 + 4ab + 4ax + n &= y^2, \\ a^2 + 4(x^2 - n) + 4ax + n &= y^2, \\ a^2 + 4ax + 4x^2 - 3n &= y^2. \end{aligned}$$

From which we get:

$$\begin{aligned} 3n &= a^2 + 4x^2 + 4ax - y^2 \\ &= (a + 2x)^2 - y^2 \\ &= (a + 2x - y)(a + 2x + y). \end{aligned}$$

We will solve equation (6.8) by assuming some of the possible factorizations of the number $3n$, which will lead us to linear systems in x and y. We proceed by assuming one of the following two cases:

1.
$$\begin{aligned} a + 2x - y &= 3, \\ a + 2x + y &= n. \end{aligned} \tag{6.9}$$

2.
$$\begin{aligned} a + 2x - y &= 1, \\ a + 2x + y &= 3n. \end{aligned} \tag{6.10}$$

CASE 1. Solving the system (6.9) yields the solution

$$(x, y) = \left(\frac{1}{4}(n - 2a + 3), \frac{1}{2}(n - 3)\right). \tag{6.11}$$

The components of the solution (6.11) must be integers, which gives us the conditions

$$n - 2a + 3 \equiv 0 \pmod 4, \ n - 3 \equiv 0 \pmod 2.$$

The second condition implies that n must be odd, i.e., $n = 2l + 1$ for some $l \in \mathbb{Z}$. Substituting into the first condition gives

$$\begin{aligned} 2l - 2a + 4 &\equiv 0 \pmod 4, \\ 2l &\equiv 2a \pmod 4, \\ l &\equiv a \pmod 2. \end{aligned}$$

Thus, $l = a + 2k$ for some $k \in \mathbb{Z}$, so that

$$n = 2(a + 2k) + 1. \tag{6.12}$$

From (6.11), we find that

$$x = \frac{1}{4}(n - 2a + 3) = \frac{1}{4}(2(a + 2k) + 1 - 2a + 3) = k + 1,$$

so the set in (6.7) becomes

$$\{a, b, a + b + 2(k + 1), a + 4b + 4(k + 1)\} \tag{6.13}$$

and has the property $D(2(a+2k)+1)$ under condition (6.2). We use this condition to eliminate the parameter b:

$$\begin{aligned} b = \frac{x^2 - n}{a} &= \frac{(k + 1)^2 - (2(a + 2k) + 1)}{a}, \\ &= \frac{k^2 - 2k - 2a}{a} = \frac{k^2 - 2k}{a} - 2. \end{aligned}$$

The last condition we must satisfy is that the parameter b is an integer, i.e.

$$k^2 - 2k = k(k - 2) \equiv 0 \pmod a.$$

We see that b will be an integer if k takes one of the following forms:

$$k = ak', \tag{6.14}$$
$$k = ak' + 2, \tag{6.15}$$

for $k' \in \mathbb{Z}$. Since k can take either of these two forms, we consider two subcases separately.

1.A) Under assumption (6.14), we get

$$b = \frac{ak'(ak' - 2)}{a} - 2 = k'(ak' - 2) - 2,$$

$$n = 2(a + 2ak') + 1 = 2a(2k' + 1) + 1,$$

and substituting into (6.13) yields the set

$$\{a, k'(ak' - 2) - 2, a + k'(ak' - 2) - 2 + 2(ak' + 1), a + 4(k'(ak' - 2) - 2) + 4(ak' + 1)\},$$

which simplifies to

$$\{a, ak'^2 - 2k' - 2, a(k' + 1)^2 - 2k', a(2k' + 1)^2 - 4(2k' + 1)\}$$

with the property $D(2a(2k' + 1) + 1)$, for all $a, k' \in \mathbb{Z}$.

1.B) Under assumption (6.15), we get

$$b = \frac{(ak'+2)(ak')}{a} - 2 = k'(ak'+2) - 2,$$

$$n = 2(a + 2(ak'+2)) + 1 = 2a(2k'+1) + 9,$$

and according to (6.13), the set

$$\{a, ak'^2 + 2k' - 2+, a(k'+1)^2 + 2(k'+2), a(2k'+1)^2 + 4(2k'+1)\}$$

has the property $D(2a(2k'+1)+9)$ for all $a, k' \in \mathbb{Z}$.

CASE 2. Similarly, as in the previous case, by solving (6.10) we get the set

$$\{a, a(1+3k')^2 + 2k', a(2+3k')^2 + 2(1+k'), 9a(1+2k')^2 + 4(1+2k')\}$$

which has $D(2a(2k'+1)+1)$-property, and several other similar formulas that we will omit.

Theorem 6.6. *Let $m, k \in \mathbb{Z}$. The sets*

$$\{m, mk^2 - 2k - 2, m(k+1)^2 - 2k, m(2k+1)^2 - 4(2k+1)\}, \tag{6.16}$$

$$\{m, m(1+3k)^2 + 2k, m(2+3k)^2 + 2(1+k), 9m(1+2k)^2 + 4(1+2k)\} \tag{6.17}$$

have the $D(2m(2k+1)+1)$-property, and the set

$$\{m, mk^2 + 2k - 2+, m(k+1)^2 + 2(k+2), m(2k+1)^2 + 4(2k+1)\} \tag{6.18}$$

has the $D(2m(2k+1)+9)$-property.

Remark 6.7. *Theorem 6.6 is valid in any commutative ring with unity.*

Remark 6.8. *The sets given in Theorem 6.6 will be $D(n)$-quadruples if all elements are nonzero and mutually distinct. For instance, $m = 2$ and $k = 3$, (6.18) gives*

$$\{-2, -14, -22, -70\},$$

and that is a $D(-19)$-quadruple. On the other hand, for $m = 1$ and $k = -3$ (6.18) gives

$$\{1, 1, 2, 5\},$$

which is not a $D(-1)$-quadruple.

6.2 Nonexistence of a $D(n)$-quadruple in $\mathbb{Z}$

Theorem 6.9. *Let n be an integer such that $n \equiv 2 \pmod 4$. Then there is no $D(n)$-quadruple in $\mathbb{Z}$.*

Proof. Assume the contrary: let $n = 4k+2$ for some $k \in \mathbb{Z}$, and suppose that $\{a_1, a_2, a_3, a_4\} \subset \mathbb{Z}$ is a set with $D(4k+2)$-property. Then

$$a_i a_j + (4k+2) = b_{ij}^2, \ 1 \le i < j \le 4,$$

where $b_{ij} \in \mathbb{Z}$. Since $b_{ij}^2 \equiv 0$ or $1 \pmod 4$, it follows that

$$a_i a_j \equiv 2 \text{ or } 3 \pmod 4.$$

Therefore, none of the a_i is divisible by 4, and hence

$$a_1, a_2, a_3, a_4 \pmod 4 \in \{1, 2, 3\}.$$

By *Dirichlet's box principle* (or the *pigeonhole principle*), among these four residues there must be at least two equal, say $a_s \equiv a_t \pmod 4$ with $s \neq t$. This means that

$$a_s a_t \equiv m^2 \equiv 0 \text{ or } 1 \pmod 4,$$

which is a contradiction since $a_s a_t \mod 4 \in \{2, 3\}$. □

6.3 Existence of $D(n)$-quadruples in $\mathbb{Z}$

Theorem 6.10. *If n is not of the form $4k+2$ and n is not in the set*

$$S = \{-4, -3, -1, 3, 5, 8, 12, 20\},$$

then there exists at least one $D(n)$-quadruple.

Proof. We assume that

$$n = 2N + 1 \text{ or } n = 4N,\ N \in \mathbb{Z}.$$

We aim to find integers m and k such that $2m(2k+1)+1 = n$, since the set (6.17) has the $D(2m(2k+1)+1)$-property. We will consider the cases $n \equiv 1 \pmod 2$ and $n \equiv 0 \pmod 4$ separately.

Step I: $\boxed{n = 2N+1}$ (n is odd)
We seek integer solutions to

$$2m(2k+1)+1 = 2N+1 \iff m(2k+1) = N. \tag{6.19}$$

- For $m = 1$, we have $N = 2k+1$, so $n = 4k+3$ and set

  $$\{1, 9k^2+8k+1, 9k^2+14k+6, 36k^2+44k+13\} \tag{6.20}$$

  has the $D(4k+3)$-property.

- If $N = 2l$ is even, then

  $$m(2k+1) = 2l.$$

  Assume that $m = 2$. Hence $l = 2k+1$ and $n = 4(2k+1)+1 = 8k+5$. For $(m, k) = (2, k)$ the set (6.17)

  $$\{2, 18k^2+14k+2, 18k^2+26k+10, 72k^2+80k+22\} \tag{6.21}$$

  has the $D(8k+5)$-property.

- If $N = 4l$, then $m(2k+1) = 4l$. Choose $m = 4$ and $k = \frac{l-1}{2}$, yielding the set

  $$\{4, 9l^2-5l, 9l^2+7l+2, 36l^2+4l\} \tag{6.22}$$

  with property $D(8l+1)$.

Thus, for any odd n, there exists a $D(n)$-quadruple, provided the sets do not contain duplicate or zero elements (to be analyzed in the third stage of the proof).

Step II: $\boxed{n = 4N}$

We attempt to solve

$$2m(2k+1)+1 = 4N. \tag{6.23}$$

but there are no integers m, k satisfying this equation directly, so the set (6.17) might not yield integer entries. To resolve this, we apply Proposition 6.3, which allows multiplying a $D(n)$-set by a rational w to obtain a $D(nw^2)$-set.

- Choose $(m,k) = \left(\frac{1}{2}, l-1\right)$. Then (6.17) becomes:

$$\left\{\frac{1}{2}, \frac{9l^2}{2} - 4l, \frac{9l^2}{2} - l + \frac{1}{2}, 18l^2 - 10l + \frac{1}{2}\right\} \tag{6.24}$$

  a set with the $D(2l)$-propery. Multiply each element by 2 to get an integer $D(8l)$-set:

$$\{1, 9l^2 - 8l, 9l^2 - 2l + 1, 36l^2 - 20l + 1\}. \tag{6.25}$$

- For $n = 8l + 4 = 4(2l+1)$, we aim for a $D(16l+12)$-quadruple. Take the set (6.20) for $k = l$ and multiply it by 2:

$$\{2, 18l^2 + 16l + 2, 18l^2 + 28l + 12, 72l^2 + 88l + 26\}. \tag{6.26}$$

- For $n = 16l + 4 = 4(4l+1)$, solve

$$2m(2k+1)+1 = 4l+1.$$

  Choose $(m,k) = \left(2, \frac{l-1}{2}\right)$, yielding a $D(4l+1)$-set:

$$\left\{2, \frac{9l^2}{2} - 2l - \frac{1}{2}, \frac{9l^2}{2} + 4l + \frac{3}{2}, 18l^2 + 4l\right\}$$

  Multiplying by 2, we get the set with the $D(16l+4)$-property:

$$\{4, 9l^2 - 4l - 1, 9l^2 + 8l + 3, 36l^2 + 8l\}. \tag{6.27}$$

  Thus, for every $n \equiv 0 \pmod 4$ (excluding the problematic form $n = 4k+2$), we can construct a $D(n)$-quadruple.

Step III: Elimination of degenerate cases

While the constructions in Steps I and II produce parameterized $D(n)$-quadruples, we must exclude specific parameter values that lead to degenerate sets. We focus on ensuring that all elements are distinct and nonzero.

We illustrate this process with one concrete example – the set (6.20). Denote the elements of (6.20) as:

$$\begin{aligned} p_1(k) &= 1, \\ p_2(k) &= 9k^2 + 8k + 1, \\ p_3(k) &= 9k^2 + 14k + 6, \\ p_4(k) &= 36k^2 + 44k + 13 \end{aligned}$$

We analyze possible degeneracies:

- Check for zero elements.

  None of the previous polynomials have integer zeros.

- Check for duplicates:

  If
  $$p_i(k) = p_j(k),\ 1 \leq i < j \leq 4,$$
  for some $k \in \mathbb{Z}$. So, we are looking for integer zeros of the following polynomials:
  $$\begin{aligned}(p_2 - p_1)(k) &= 9k^2 + 8k,\\ (p_3 - p_1)(k) &= 9k^2 + 14k + 5,\\ (p_4 - p_1)(k) &= 36k^2 + 44k + 12,\\ (p_3 - p_2)(k) &= 6k + 5,\\ (p_4 - p_2)(k) &= 27k^2 + 36k + 12,\\ (p_4 - p_3)(k) &= 27k^2 + 30k + 7,\end{aligned}$$
  So, for $l = 0$ and corresponding $n = 3$ we have a set whose first two elements are
  $$\{1, 1, 6, 13\},$$
  and for $l = -1$ and corresponding $n = -1$ we have a set whose first and third elements are
  $$\{1, 2, 1, 5\}.$$

By examining the possibilities for the remaining sets, we obtain the following exceptions:

$$\{-12, -7, -4, -3, -1, 0, 1, 3, 4, 5, 8, 9, 12, 20\}.$$

The case $n = 1$ is resolved (since there exist infinitely many Diophantine quadruples). The sets $\{1, 12, 28, 76\}$ and $\{1, 8, 11, 16\}$ are $D(-12)$ and $D(-7)$ quadruples, respectively. Furthermore, there are infinitely many $D(0)$ quadruples. Indeed, a^2, b^2, c^2, d^2 is a $D(0)$ quadruple for any four nonzero integers a, b, c, d. Moreover, for n that is a perfect square, there are infinitely many $D(n)$ quadruples (Corollary 6.5), so we can eliminate the cases $n = 4, 9$. Therefore, we have not found a $D(n)$ quadruple only for $n \in \{-4, -3, -1, 3, 5, 8, 12, 20\}$. □

For clarity, we highlight the results obtained in the proof of the previous theorem in the following corollary.

Corollary 6.11. *Let $k \in \mathbb{Z}$. Then, for n of the given form, with finitely many specified exceptions, the following sets represent $D(n)$ quadruples:*

- $n = 4k + 3$:
  $$1, 9k^2 + 8k + 1, 9k^2 + 14k + 6, 36k^2 + 44k + 13, \tag{6.28}$$
  for $k \neq 0, -1$, i.e., $n \neq 3, -1$,

- $n = 8k + 1$:
  $$\{4, 9k^2 - 5k, 9k^2 + 7k + 2, 36k^2 + 4k\}, \tag{6.29}$$
  for $k \neq 0, 1, -1$, i.e., $n \neq 1, 9, -7$,

- $n = 8k + 5$:
$$\{2, 18k^2 + 14k + 2, 18k^2 + 26k + 10, 72k^2 + 80k + 22\}, \tag{6.30}$$
for $k \neq 0, -1$, *i.e.,* $n \neq 5, -3$,

- $n = 8k$:
$$\{1, 9k^2 - 8k, 9k^2 - 2k + 1, 36k^2 - 20k + 1\}, \tag{6.31}$$
for $k \neq 0, 1$, *i.e.,* $n \neq 0, 8$,

- $n = 16k + 4$:
$$\{4, 9k^2 - 4k - 1, 9k^2 + 8k + 3, 36k^2 + 8k\}, \tag{6.32}$$
for $k \neq 0, 1, -1$, *i.e.,* $n \neq 4, 20, -12$,

- $n = 16k + 12$:
$$\{2, 18k^2 + 16k + 2, 18k^2 + 28k + 12, 72k^2 + 88k + 26\}, \tag{6.33}$$
for $k \neq 0, -1$, *i.e.,* $n \neq 12, -4$.

Corollary 6.12. *For every rational number q, there exists a four-element set of rational numbers such that the product of any two distinct elements of the set, increased by q, is a square of a rational number.*

Proof. Let $q = \frac{m}{n}, m \in \mathbb{Z}, n \in \mathbb{N}$. Then, for $k = 100n^2q$, it holds that $k \in \mathbb{Z}, k \equiv 0 \pmod 4$ i $|k| \geq 100$. Therefore, by Theorem 6.10, there exists a Diophantine quadruple $\{a_1, a_2, a_3, a_4\}$ with the property $D(k)$. It follows that the set $\left\{\frac{a_1}{10n}, \frac{a_2}{10n}, \frac{a_3}{10n}, \frac{a_4}{10n}\right\}$ has the property $D(q)$. □

6.4 Connection between $D(n)$ quadruples and the *difference of two squares*

Theorem 6.13. *An integer n can be expressed as the difference of squares of two integers if and only if $n \not\equiv 2 \pmod 4$.*

Proof. Assume $n = x^2 - y^2,\ x, y \in \mathbb{Z}$. Since the square of an integer leaves a remainder of 0 or 1 modulo 4, it follows that n leaves a remainder of 0, 1, or 3 modulo 4.

Conversely, if we assume $n \not\equiv 2 \pmod 4$, then $n = 4k$ or $n = 4k+1$ or $n = 4k+3$ for $k \in \mathbb{Z}$. The numbers of these forms can be represented as a difference of two squares of integers:

$$4k = (k + 1)^2 - (k - 1)^2,$$

$$2k + 1 = (k + 1)^2 - k^2$$

□

Based on what has been shown in the previous sections, we have the following:

Theorem 6.14. *Let $n \in \mathbb{Z}$, and suppose $n \notin S = \{-4, -3, -1, 3, 5, 8, 12, 20\}$. A Diophantine quadruple with the property $D(n)$ exists if and only if n can be expressed as the difference of squares of two integers.*

For the elements of the set S, it is unknown whether a $D(n)$ quadruple exists. In particular, the case of a $D(-1)$ quadruple has proven to be especially difficult and is the subject of numerous articles. In fact, it is now known that there is no $D(-1)$-quadruple ([4]) but this was preceded by the laborious work of a number of mathematicians, over 30 years. Also, this result implies the nonexistence of a $D(-4)$-quadruple, since all elements of a $D(-4)$-quadruple are even.

Conjecture 6.15. *There exists no $D(n)$-quadruple in $n \in \{-3, 3, 5, 8, 12, 20\}$.*

It is interesting to note that the characterization of $D(n)$ quadruples in terms of the expressibility of n as a difference of squares of two integers cannot be proven directly, but rather using polynomial formulas for sets with the property $D(n)$ from Theorem 3.2. However, we can directly prove the following statement.

Proposition 6.16. *If $n = k^2 - a^2$, then for every integer m, the quadruple*

$$(a, a, (m^2+1)a + 2mk, (m^2+2m+2)a + 2(m+1)k)$$

has the property that the product of any two of its elements, increased by n, is a perfect square.

Proof. Directly from the following relations:

- $$a \cdot a + n = k^2$$
- $$a[(m^2+1)a + 2mk] + n = (am + k)^2$$
- $$a[(m^2+2m+2)a + 2k(m+1)] + n = [a(m+1) + k]^2$$
- $$[(m^2+1)a + 2mk][(m^2+2m+2)a + 2k(m+1)] + n = [a(m^2+m+1) + k(2m+1)]^2$$

□

Remark 6.17. *So far, the statement about the equivalence between the existence of a $D(n)$-quadruple and n being representable as a difference of two squares has been shown to hold in the rings of integers of many quadratic fields (both real and imaginary), as well as in some other number fields (see [11], [16], [17],[18], [19], [20],[21]). However, in [3], examples were found of certain rings in which the stated equivalence does not hold (where n cannot be represented as a difference of two squares and a $D(n)$-quadruple exists). Nevertheless, we believe it is worthwhile to further investigate the connection between $D(n)$-quadruples and differences of squares.*

6.5 Diophantine quadruples withe the $D(l^2)$-property

Let $\{a, b\}$, $0 < a < b$, be a Diophantine pair with the $D(l^2)$-property for some $l \in \mathbb{N}$. Hence,

$$ab + l^2 = k^2,\ k \in \mathbb{N} \tag{6.34}$$

We are looking for $x \in \mathbb{N}$ such that $\{a, b, x\}$ be a $D(l^2)$-triple. From

$$\begin{aligned} ax + l^2 &= y^2, \\ bx + l^2 &= z^2, \end{aligned} \tag{6.35}$$

we get, as before we get the equation of Pell's type

$$by^2 - az^2 = l^2(b - a), \tag{6.36}$$

in unknowns y and z. It is easy to see that this equations is always solvable:

$$(y, z) = (l, l),\ (y, z) = (k + a, k + b).$$

Solutions that are generated with this initial solutions will generate possible extensions of a Diophantine pair.

Let us solve equation (6.36). Assume that (s, t) is a fundamental solution to related Pell's equation $y^2 - abz^2 = 1$,

$$s^2 - abt^2 = 1 \tag{6.37}$$

So,

$$\begin{aligned} y_n\sqrt{b} + z_n\sqrt{a} &= (l\sqrt{b} + l\sqrt{a})(s + t\sqrt{ab})^n, \\ y'_n\sqrt{b} + z'_n\sqrt{a} &= ((k + a)\sqrt{b} + (k + b)\sqrt{a})(s + t\sqrt{ab})^n, \end{aligned}$$

are soutions of Pellian equation (6.36) for $n \in \mathbb{N}_0$. The sequences (y_n) i (y'_n) are binary recursive sequences:

$$y_n = 2sy_{n-1} - y_{n-2},\ n \geq 2 \tag{6.38}$$

with initial conditions $y_0 = l$ i $y_1 = (s + at)l$, and

$$y'_n = 2sy'_{n-1} - y'_{n-2},\ n \geq 2$$

with initial conditions $y'_0 = k + a$ and $y'_1 = s(k + a) + at(k + b)$. According to (6.35), we define the corresponding sequences:

$$x_n = \frac{y_n^2 - l^2}{a},\ x'_n = \frac{{y'_n}^2 - l^2}{a}. \tag{6.39}$$

It is clear that the sets $\{a, b, x_n\}$ and $\{a, b, x'_n\}$ are Diophantine sets with the property $D(l^2)$, but we need to show that x_x, x'_n are integers for every $n \in \mathbb{N}_0$.

Proposition 6.18. *The sequences (x_n) and (x'_n) defined by the relations in* (6.39)*, consist of integers.*

Proof. We will show that $a \mid y_n^2 - l^2$, for every $n \in \mathbb{N}_0$. The statement will be proved by mathematical induction.

1. **Base case**: $n = 0$ and $n = 1$,
$$y_0^2 - l^2 = 0,$$
$$y_1^2 - l^2 = (s+at)^2 l^2 - l^2 = l^2(s^2 + 2sat + a^2t^2 - 1) = l^2 \underbrace{(abt^2 + 2sat + a^2t^2)}_{a|}. \quad (6.40)$$
where the final equality follows from (6.37).

2. **Inductive step**: Assume that for some $n \in \mathbb{N}$, a devides $y_i^2 - l^2$ for all $i \leq n$. By the recurrence relation (6.38), we have
$$y_{n+1}^2 - l^2 = (2sy_n - y_{n-1})^2 - l^2 = 4s^2y_n^2 - 4sy_ny_{n-1} + \underbrace{y_{n-1}^2 - l^2}_{a|}. \quad (6.41)$$
Now, we will again use mathematical induction to show that $a \mid sy_n - y_{n-1}$.

   (a) **Base case**: $n = 1$,
$$\begin{aligned} sy_1 - y_0 &= s(s+at)l - l = l(s^2 - sat - 1) \\ &= l(abt + sat) = a(lbt + lst). \end{aligned}$$

   (b) **Inductive step**: Let $n \in \mathbb{N}$ and assume that $a \mid sy_i - y_{i-1}$ for all $i \leq n$, tj. $sy_i - y_{i-1} = ak, k \in \mathbb{Z}$.
   We verify the statement for $n+1$. Using the recurrence relation (6.38), we get
$$\begin{aligned} sy_{n+1} - y_n &= s(2sy_n - y_{n-1}) - y_n = s(sy_n + ak) - y_n \\ &= s^2y_n + aks - y_n = y_n(s^2 - 1) + aks \\ &= y_n \cdot abt + aks = a(y_nbt + ks). \end{aligned}$$

Thus, we have shown that $a \mid sy_{n+1} - y_n$, which implies that the expression in (6.41) is divisible by a, completing the induction. Therefore, the initial assumption holds for all $n \in \mathbb{N}_0$, that is (x_n) consists of integers..

Let us now prove an analogous statement for the sequence (x'_n), again using the principle of mathematical induction. Since the sequences (y_n) and (y'_n) satisfy the same recurrence relation, it is sufficient to verify the base case of the induction.

1. **Base case**: $n = 0$ and $n = 1$. We have
$${y'_0}^2 - l^2 = (k+a)^2 - l^2 = k^2 + 2ak + a^2 - l^2 = ab + 2ak + a^2 = a(a + b + 2k),$$
where we used identity (6.34). Furthermore:
$$\begin{aligned} {y'_1}^2 - l^2 &= (s(k+a) + at(k+b))^2 - l^2 \\ &= s^2(k+a)^2 + a^2t^2(k+b)^2 + 2sat(a+k)(b+k) - l^2 \\ &= (abt^2 + 1)(k+a)^2 + a^2t^2(k+b)^2 + 2sat(a+k)(b+k) - l^2 \\ &= abt^2(k+a)^2 + k^2 + 2ak + a^2 + a^2t^2(k+b)^2 + 2sat(a+k)(b+k) - l^2 \\ &= abt^2(k+a)^2 + ab + 2ak + a^2 + a^2t^2(k+b)^2 + 2sat(a+k)(b+k), \end{aligned}$$
where we used (6.34) and (6.37). It is clear that $a \mid {y'_1}^2 - l^2$.
It remains to prove that $a \mid sy'_n - y'_{n-1}$ and again it is sufficient to verify the base case of the induction:

(a) **Base case**: $n = 1$

$$\begin{aligned} sy_1' - y_0' &= s(s(k+a) + at(k+b)) - (k+a) \\ &= (s^2-1)(k+a) + at(k+b) \\ &= abt^2(k+a) + at(k+b) \\ &= a(bt^2(k+a) + t(k+b)). \end{aligned}$$

□

U [12] je Dujella pokazao da je
za sve $n \in \mathbb{N}_0$. Dokaz je tehnički složen i zahtijevao bi uvodjenje još nizova koji zadovoljavaju jednadžbu (6.36). Drugim riječima vrijedi sljedeća tvrdnja.

Theorem 6.19. *Let $l \in \mathbb{Z}$ and $\{a, b\}$ be a Diophantine pair with the property $D(l^2)$. Then the set*

$$\{a, b, x_n, x_n'\}$$

has the$D(l^2)$-property for all $n \in \mathbb{N}$.

Proof. It can be shown

$$x_n x_n' + l^2 = \left(\frac{y_n y_y' - lk}{a}\right)^2.$$

The proof is technically complex and would require introducing additional sequences (see (6.36)). □

We will demonstrate the described method on a concrete example, showing how a given $D(l^2)$-pair can be extended, in infinitely many ways, to a Diophantine quadruple with the same property.

Example 7. *Given is the $D(16)$-pair $\{4, 5\}$. So, the following parameter values are given:*

$$a = 4, b = 5, l = 4, k = 6.$$

To determine the sequences (x_n) and (x_n') we first need to determine the sequences (y_n) and (y_n') which are solutions to the Pell-type equation

$$5y^2 - 4z^2 = 16.$$

For that, we require the fundamental solution of the associated Pell equation $y^2 - 20z^2 = 1$. It is easy to verify that the fundamental solution is $(s, t) = (9, 2)$. The initial values of the sequences (y_n) and (y_n') are

$$y_0 = l = 4,\ y_1 = (s + at)l = 68,$$

$$y_0' = k + a = 10,\ y_1' = s(k+a) + at(k+b) = 178.$$

Since $x_0 = 0$, $\{a, b, x_0, x_0'\}$ does not represent a proper extension. However,

$$x_1 = \frac{y_1^2 - l^2}{a} = 1152,\ x_1' = \frac{{y_1'}^2 - l^2}{a} = 7917,$$

does yield a proper extension. Indeed, $\{4, 5, 1152, 7917\}$ *is a Diophantine quadruple with the property* $D(4^2)$*. Indeed, uvjeriti*

$$\begin{aligned} 4 \cdot 5 + 16 &= 6^2, \\ 4 \cdot 1152 + 16 &= 68^2, \\ 4 \cdot 7917 + 16 &= 178^2, \\ 5 \cdot 1152 + 16 &= 76^2, \\ 5 \cdot 7917 + 16 &= 199^2, \\ 1152 \cdot 7917 + 16 &= 3020^2. \end{aligned}$$

For $n = 2, 3, 4, \ldots$ *we obtain the sets:*

$$\begin{aligned} &\{4, 5, 372096, 2553600\}, \\ &\{4, 5, 119814912, 822255621\}, \\ &\{4, 5, 38580030720, 264763760700\}, \ldots \end{aligned}$$

Using the described construction for extending a $D(l^2)$-pair to a quadruple, one can obtain interesting examples whose elements are Fibonacci and Lucas numbers. The *Fibonacci sequence* is defined by the recurrence relation

$$F_{n+1} = F_n + F_{n-1},\ n \geq 1,$$

with initial conditions $F_0 = 1,\ F_1 = 1$. The Lucas sequence, denoted by (L_n) is given by the the same recurrence relation

$$L_{n+1} = L_n + L_{n-1},\ n \leq 1,$$

with initial conditions $L_0 = 2,\ L_1 = 1$.

Theorem 6.20. *For all* $n \geq 2$*, the sets*

$$\{2F_{n-1}, 2F_{n+1}, 2F_n^3 F_{n+1} F_{n+2}, 2F_{n+1} F_{n+2} F_{n+3}(2F_{n+1}^2 - F_n^2)\}, \tag{6.42}$$

$$\{F_{n-1}, 4F_{n+1}, F_n^3 F_{n+2} F_{n+3}, F_{n+1} F_{n+2} F_{n+4}[F_{n+2}^2 + 2(-1)^n]\}, \tag{6.43}$$

$$\{4F_{n-1}, F_{n+1}, F_n^3 L_n L_{n+1}, F_{n+1} F_{2n+4}(F_{2n+2} + 2(-1)^n)\} \tag{6.44}$$

ithe property $D(F_n^2)$*.*

For all $n \geq 3$*, the sets*

$$\{2F_{n-1}, 2F_{n+1}, 2F_{n-2} F_{n-1} F_n^3, 2F_n^3 F_{n+1} F_{n+2}\}, \tag{6.45}$$

$$\{F_{n-1}, 4F_{n+1}, F_{n-2} F_{n-1} F_{n+1}(2F_n^2 - F_{n-1}^2), F_n^3 F_{n+2} F_{n+3}\}, \tag{6.46}$$

$$\{4F_{n-1}, F_{n+1}, F_{n-2} F_{2n-2} F_{2n-1}, F_n^3 L_n L_{n+1}\} \tag{6.47}$$

the property $D(F_n^2)$

Theorem 6.20 can be proven by direct verification. Let us demonstrate this on the example of the set (6.43):

$$F_{n-1} \cdot 4F_{n+1} + F_n^2 = L_n^2,$$
$$F_{n-1} \cdot F_n^3 F_{n+2} F_{n+3} + F_n^2 = (F_n F_{n+1}^2)^2,$$
$$F_{n-1} \cdot F_{n+1} F_{n+2} F_{n+4}[F_{n+2}^2 + 2(-1)^n] + F_n^2 = [F_{n+1} F_{n+2}^2 + (-1)^n F_{n+3}]^2,$$
$$4F_{n+1} \cdot F_n^3 F_{n+2} F_{n+3} + F_n^2 = \{F_n[2F_{n+1} F_{n+2} - (-1)^n]\}^2,$$
$$4F_{n+1} \cdot F_{n+1} F_{n+2} F_{n+4}[F_{n+2}^2 + 2(-1)^n] + F_n^2 = \{F_{n+3}[2F_{n+1} F_{n+2} + (-1)^n]\}^2,$$
$$F_n^3 F_{n+2} F_{n+3} \cdot F_{n+1} F_{n+2} F_{n+4}[F_{n+2}^2 + 2(-1)^n] + F_n^2 = \{F_n[F_{n+2}^4 + (-1)^n F_{n+2}^2 - 1]\}^2.$$

We have already concluded at the beginning that there exist infinitely many $D(l^2)$- quadruples in the ring of integers. However, this does not hold for every integer n that is not a perfect square. This motivates the following conjecture:

Conjecture 6.21. *Let $n \in \mathbb{Z}$, $n \neq l^2$ za sve $l \in \mathbb{Z}$. Then there exist at most finitely many $D(n)$-conjectures.*

Bibliography

[1] A. Baker, *Linear forms in the logarithms of algebraic numbers*, Mathematika **15** (1968), 204–216.

[2] A. Baker and H. Davenport, *The equations* $3x^2-2=y^2$ *and* $8x^2-7=z^2$, Quart. J. Math. Oxford Ser. (2) **20** (1969), 129–137.

[3] M.A. Bennett, *On the number of solutions of simultaneous Pell equations*, J. Reine Angew. Math. **498** (1998) 173–199.

[4] N. C. Bonciocat, M. Cipu, M. Mignotte, *There is no Diophantine* $D(-1)$*-quadruple*, J. London Math. Soc. **105** (2022), 63–99.

[5] Y. Bugeaud, *Linear Forms in Logarithms and Applications*, IRMA Lectures in Mathematics and Theoretical Physics Vol. 28, European Mathematical Society, Zürich, 2018.

[6] A. Dujella, Diophantine m-tuples page, `https://web.math.pmf.unizg.hr/~duje/dtuples.html`

[7] A. Dujella, *Number Theory*, Školska knjiga, 2021.

[8] A. Dujella, *Diophantine m-tuples and Elliptic Curves*, Springer, Cham, 2024.

[9] A. Dujella, *Generalization of a problem of Diophantus*, Acta Arith. **65** (1993), 15–27.

Some polynomial formulas for Diophantine quadruples, Grazer Math. Ber. **328** (1996), 25–30.

[10] A. Dujella, *The problem of the extension of a parametric family of Diophantine triples*, Publ. Math. Debrecen **51** (1997), 311–322.

[11] A. Dujella, *The problem of Diophantus and Davenport for Gaussian integers*, Glas. Mat. Ser. III **32** (1997), 1–10.

[12] A. Dujella, *On Diophantine quintuples*, Acta Arith. **8**1 (1997), 69–79.

[13] A. Dujella, A. Filipin and C. Fuchs, *Effective solution of the* $D(-1)$*-quadruple conjecture*, Acta Arith. **128** (2007), 319–338.

[14] A. Dujella and A. Pethő, *A generalization of a theorem of Baker and Davenport*, Quart. J. Math. Oxford Ser. (2), **49** (1998), 291–306.

[15] A. Dujella, *There are only finitely many Diophantine quintuples*, J. Reine Angew. Math. **566** (2004), 183-214.

[16] Z. Franušić, *Diophantine quadruples in the ring* $\mathbb{Z}[\sqrt{2}]$, Math. Commun. **9** (2004), 141–148.

[17] Z. Franušić, *Diophantine quadruples in* $\mathbb{Z}[\sqrt{4k+3}]$, Ramanujan J. **17** (2008), 77–88.

[18] Z. Franušić, *A Diophantine problem in* $Z[(1+\sqrt{d})/2]$, Studia Sci. Math. Hungar. **46** (2009), 103–112.

[19] Z. Franušić, *Diophantine quadruples in the ring of integers of* $\mathbb{Q}(\sqrt[3]{2})$, Miskolc Math. Notes **14** (2013), 893–903.

[20] Z. Franušić, B. Soldo, *The problem of Diophantus for integers of* $\mathbb{Q}(\sqrt{-3})$, Rad Hrvat. Akad. Znan. Ser. III **49** (2014), 37–46.

[21] Z. Franušić, B. Jadrijević, *$D(n)$-quadruples in the ring of integers of* $\mathbb{Q}(\sqrt{2},\sqrt{3})$, Math. Slovaca **69** (2019), 1263–1278.

[22] B. He, A. Togbé, V. Ziegler, *There is no Diophantine quintuple*, Trans. Amer. Math. Soc. **371** (2019), 6665–6709.

[23] C. L. Siegel (pseudonim X): *The integer solutions of the equation* $y^2 = ax_n + bx_{n-1} + \cdots + k$, J. London Math. Soc. 1 (1926), 66–68.