Diophantine m-tuples

Zrinka Franušić

Istanbul, June, 2025

Contents

1 Introduction to Diophantine m-tuples **2**
1.1 Definition 2
1.2 On Diophantine pairs 3
1.3 On Diophantine triples 3
1.4 On Diophantine quadruples 5
1.5 On Diophantine quintuples 7
1.6 $D(n)$-tuples 8

2 Simple continued fractions **9**
2.1 Simple continued fraction expansion 9
2.2 Convergents 11
2.3 On approximation of irrationals by continued fractions 12
2.4 Periodic continued fractions 13

3 Pell's equation **15**
3.1 Existence of solutions to Pell's equation 15
3.2 Structure of the solution set of Pell's equation 18
3.3 Recurrence relations for solutions of Pell's equation 19
3.4 Solving Pell's equation using continued fractions 20

Bibliography **21**

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 (1.7) and (1.8), 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 (1.7),(1.8) 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 ([9]) 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 ([12]) 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 ([13]) published the proof of Diophantine quintuple conjecture.

Teorem 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,

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

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:

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

Teorem 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.

Teorem 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.

Teorem 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.

Teorem 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.

Teorem 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.)

Teorem 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

Teorem 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.

Teorem 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

Teorem 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 (3.8). □

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).

Teorem 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.

Teorem 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?

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] Y. Bugeaud, *Linear Forms in Logarithms and Applications*, IRMA Lectures in Mathematics and Theoretical Physics Vol. 28, European Mathematical Society, Zürich, 2018.

[5] A. Dujella, Diophantine m-tuples page, `https://web.math.pmf.unizg.hr/~duje/dtuples.html`

[6] A. Dujella, *Number Theory*, Školska knjiga, 2021.

[7] A. Dujella, *Diophantine m-tuples and Elliptic Curves*, Springer, Cham, 2024.

[8] 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.

[9] A. Dujella, *On Diophantine quintuples*, Acta Arith. 81 (1997), 69–79.

[10] A. Dujella, A. Filipin and C. Fuchs, *Effective solution of the* $D(-1)$*-quadruple conjecture*, Acta Arith. 128 (2007), 319–338.

[11] A. Dujella and A. Pethő, *A generalization of a theorem of Baker and Davenport*, Quart. J. Math. Oxford Ser. (2), 49 (1998), 291–306.

[12] A. Dujella, *There are only finitely many Diophantine quintuples*, J. Reine Angew. Math. 566 (2004), 183-214.

[13] B. He, A. Togbé, V. Ziegler, *There is no Diophantine quintuple*, Trans. Amer. Math. Soc. 371 (2019), 6665–6709.