The corresponding LLL-reduced basis consists of the columns of the matrix

$$\begin{pmatrix} 573 & 747 & 713 \\ -237 & 938 & -611 \\ -300 & -55 & 1794 \end{pmatrix}.$$

Furthermore, $c_1 = 1$, $c_4 = 474498$, $S = 47432$, $T = 231.5$, so Lemma 14.10 can be applied, which gives a new upper bound

$$X \leq 15.$$

The process can be continued further, however, the bound is now sufficiently small for all remaining possibilities to be directly checked. We find that the solutions are

$$\begin{aligned}(x_1, x_2, x_3) = {} & (-6,-5,6), (-4,4,-1), (-3,-4,4), (-3,-1,2), (-2,0,1), \\ & (-1,-1,1), (-1,0,0,), (-1,1,0), (-1,2,-1), (0,-3,2), \\ & (0,-1,1), (0,0,0), (0,1,-1), (0,3,-2), (1,-2,1), (1,-1,0), \\ & (1,0,0), (1,1,-1), (2,0,-1), (3,1,-2), (3,4,-4), (4,-4,1), \\ & (6,5,-6).\end{aligned}$$

Let us observe that these 23 solutions are in fact all solutions of inequality (14.34) because, from the Baker-Wüstholz theorem, it follows that (14.34) does not have solutions with $X > 10^{15}$. ♢

14.6 Diophantine m-tuples

Definition 14.1. *A* Diophantine m-tuple *is a set of m distinct positive integers with the property that the product of any two of its distinct elements plus 1 is a perfect square.*

The first example of a Diophantine quadruple was found by Fermat and it was the set $\{1, 3, 8, 120\}$, which we already discussed in Theorem 14.9. Indeed, we have

$$1 \cdot 3 + 1 = 2^2, \quad 1 \cdot 8 + 1 = 3^2, \quad 1 \cdot 120 + 1 = 11^2,$$

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

Definition 14.2. *A* rational Diophantine m-tuple *is a set of m distinct non-zero rational numbers with the property that the product of any two of its distinct elements plus 1 is the square of a rational number.*

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

$$\{1, 3, 8, 120, 777480/8288641\}. \tag{14.35}$$

The ancient Greek mathematician Diophantus of Alexandria (3rd century) was the first one who studied sets with this property. In the fourth part of his book *Arithmetica* [213], exercise no. 20 states:

> Find four numbers (for Diophantus, this meant positive rational numbers) such that the product of any two among them, increased by 1 gives a square.

We will describe how Diophantus solved this exercise (of course, by using contemporary mathematical notation). Two numbers with the required property can be obtained by taking $a = x$ and $b = x+2$, so $ab+1 = (x+1)^2$. A pair $\{a, b\}$ such that $ab + 1 = r^2$, can be extended to a triple by taking $c = a + b + 2r$. Indeed, then $ac + 1 = (a + r)^2$, $bc + 1 = (b + r)^2$. In this manner, we obtain $c = 4x + 4$. Now, we apply the same construction to the pair $\{a, c\}$ and the equality $ac + 1 = (2x + 1)^2$. We obtain $d = x + (4x + 4) + 2(2x + 1) = 9x + 6$. In this manner, we obtain the set $\{a, b, c, d\}$ which satisfies five out of six conditions from the definition of a Diophantine quadruple. The only condition which is missing is that $bd + 1$ is a square. Hence, it remains to find a rational solution of the equation

$$9x^2 + 24x + 13 = y^2.$$

Diophantus knew how to solve the equations of this kind. He searched for a solution in the form $y = 3x + t$, so after the substitution, he would obtain a linear equation in variable x. He did not search for a general solution of the equation (possibly, due to the difficulties with a mathematical notation of that time); instead, he would introduce a concrete value and obtain one solution. So, in this case, he took $y = 3x - 4$ and obtained the equation $48x = 3$ and the solution $x = 1/16$. Thus, he found the first example of what we call nowadays the rational Diophantine quadruple

$$\{1/16, 33/16, 17/4, 105/16\}.$$

It is natural to ask how large can these sets be. This question was recently completely solved in the integer case. On the other hand, in the rational case, the question is completely open, and we do not even have a widely accepted conjecture. In particular, no absolute upper bound for the size of rational Diophantine m-tuples is known.

In the integer case, it is easy to show that there are infinitely many integer Diophantine quadruples. Namely, there are parametric families of Diophantine quadruples involving polynomial and Fibonacci numbers, such as

$$\{k, k+2, 4k+4, 16k^3+48k^2+44k+12\}, \tag{14.36}$$

$$\{F_{2k}, F_{2k+2}, F_{2k+4}, 4F_{2k+1}F_{2k+2}F_{2k+3}\} \tag{14.37}$$

for $k \geq 1$ (for (14.37) see Example 1.15 and [221]). More precisely, it was proved in [290] that the number of Diophantine quadruples with elements $\leq N$ is asymptotically equal to $C\sqrt[3]{N}\ln N$, where $C \approx 0.338285$.

On the other hand, recently, He, Togbé and Ziegler [212] proved that there is no Diophantine quintuple and so they solved a long-standing open problem. Previously, Dujella [117] proved in 2004 that there is no Diophantine sextuple and that there are at most finitely many Diophantine quintuples (with an explicit upper bound for the number of Diophantine quintuples, which was later improved in [79]). The first important result concerning this problem was obtained by Baker and Davenport in 1969 [25], when they proved that if d is a positive integer such that $\{1, 3, 8, d\}$ is a Diophantine quadruple, then d has to be 120 (Theorem 14.9), so that Fermat's set $\{1, 3, 8, 120\}$ cannot be extended to a Diophantine quintuple.

Let us note that in the definition of (rational) Diophantine m-tuple, we excluded the requirement that the product of an element with itself plus 1 gives a square. It is obvious that for integers such condition cannot be satisfied (the equation $a^2+1=r^2$ does not have solutions in positive integers). However, for rational numbers, there is no obvious reason why such sets (which we could call *strong Diophantine m-tuples*) would not exist. Each element a of such set should satisfy that a^2+1 is a square, so $a = X/Y$, where (X, Y, Z) is a Pythagorean triple, i.e. $X^2+Y^2=Z^2$. It was proved in [160] that there are infinitely many strong rational Diophantine triples (for instance $\{1976/5607, 3780/1691, 14596/1197\}$ is one such triple), but it is not known whether there is any strong Diophantine quadruple (see [150] for a generalization).

It is known that any Diophantine triple $\{a, b, c\}$ can be extended to a Diophantine quadruple $\{a, b, c, d\}$. Indeed, if $ab+1=r^2$, $ac+1=s^2$, $bc+1=t^2$, where $r, s, t \in \mathbb{N}$, then we may take

$$d = a+b+c+2abc+2rst, \tag{14.38}$$

and then $ad+1=(at+rs)^2$, $bd+1=(bs+rt)^2$, $cd+1=(cr+st)^2$. This was shown by Arkin, Hoggatt and Strauss [13] in 1979, and in the special case, when $c = a + b + 2r$, this was already known to Euler. Quadruples of this form are called *regular*. In other words, a Diophantine quadruple $\{a, b, c, d\}$ is regular if and only if

$$(a + b - c - d)^2 = 4(ab + 1)(cd + 1). \tag{14.39}$$

The conjecture that all Diophantine quadruples are regular is still open. Hence, the conjecture is that for each Diophantine triple $\{a, b, c\}$, there is a unique positive integer d, such that $d > \max(a, b, c)$ and that $\{a, b, c, d\}$ is a Diophantine quadruple. Let us mention that Cipu, Fujita and Miyazaki [78, 188] proved that any fixed Diophantine triple $\{a, b, c\}$ can be extended to a Diophantine quadruple with an element d such that $d > \max(a, b, c)$ in at most eight ways.

Apart from the number d defined by (14.38), which is often denoted by d_+, we can also consider the number $d_- = a+b+c+2abc-2rst$ (the other solution of quadratic equation (14.39)). We have

$$\begin{aligned} d_+d_- &= a^2 + b^2 + c^2 - 2ab - 2ac - 2bc - 4 = (c - a - b)^2 - 4r^2 \\ &= (c - a - b + 2r)(c - a - b - 2r), \end{aligned}$$

from where we see that $d_- = 0$ if and only if $c = a + b \pm 2r$ (such triples are called *regular*). If $d_- \neq 0$, then $\{a, b, c, d_-\}$ is also a Diophantine quadruple. Assume that $c = \max(a, b, c)$. Then

$$c = a + b + d_- + 2abd_- + 2\sqrt{(ab + 1)(ad_- + 1)(bd_- + 1)} > 4ab.$$

Hence, we proved the following result.

Proposition 14.11. *Let $\{a, b, c\}$ be a Diophantine triple and $a < b < c$. Then either $c = a + b + 2\sqrt{ab + 1}$ or $c > 4ab$.*

We will sketch some of the ideas used in the proofs of the above-mentioned results on the non-extendibility of Diophantine triples and quadruples. The problem of extending the Diophantine triple $\{a, b, c\}$, $a < b < c$, to a Diophantine quadruple $\{a, b, c, d\}$ leads to the system of equations $ad + 1 = x^2$, $bd + 1 = y^2$, $cd + 1 = z^2$, and, by eliminating d, we obtain the system of simultaneous equations of Pellian type

$$cx^2 - az^2 = c - a, \quad cy^2 - bz^2 = c - b. \tag{14.40}$$

The solutions of such equations are contained in finitely many binary recurrence sequences. Therefore, the initial problem leads to finding the intersection of those sequences, i.e. to finitely many equations of the form $v_m = w_n$.

In Chapter 14.3, we saw that Baker's theory of linear forms in logarithms can be used for obtaining upper bounds on m, n.

Another method for obtaining upper bounds for solutions is by using results on simultaneous approximations of quadratic irrationalities (for instance, Bennett's result from [34], obtained by a generalization of the hypergeometric method from Chapter 13.3, which was originally applied for getting an estimate for the number of solutions of a system of Pell's equations (see also [35])). Namely, if we assume that system (14.40) has a large solution (x, y, z), then x/z and y/z are very good rational approximations (with a common denominator) of irrational numbers $\sqrt{a/c}$ and $\sqrt{b/c}$. If these approximations are better than those whose existence is guaranteed by Dirichlet's theorem on simultaneous approximations (Corollary 8.49), then we can expect that we will obtain a contradiction, which will imply that solutions cannot be large. This method usually gives significantly better (smaller) bounds for solutions than the ones obtained by using linear forms in logarithms. However, it is possible to apply it only to the triples which satisfy certain additional conditions. A typical condition is that there is a big "gap" between b and c (larger than the one which is given by Proposition 14.11 for non-regular triples; e.g. $c > b^5$).

The *congruence method*, which was introduced by Dujella and Pethő in 1998 in the paper [157], is usually used to obtain lower bounds. It consists of considering congruences such as $v_m \equiv w_n \pmod{c^2}$. If m, n are small (compared with c), then the congruence can be replaced by the equality, and this often leads to a contradiction (if $m, n > 2$, i.e. if d does not correspond to a regular quadruple). Therefore, we obtain lower bounds for m, n (which are small positive powers of c). Comparing the upper and lower bound, we get a contradiction for c large enough (since a positive power grows faster than a logarithmic function).

As we already mentioned, it is known that there is no integer Diophantine quintuple, thus, we can say that already Fermat found the largest possible set with that property. On the other hand, in the rational case, there are larger sets with the property of Diophantus. Euler proved that there are infinitely many rational Diophantine quintuples. However, the question of the existence of rational Diophantine sextuples remained open for more than two centuries. In 1999, Gibbs (see [194]) found the first rational sextuple

$$\{11/192, 35/192, 155/27, 512/27, 1235/48, 180873/16\},$$

while in 2017, Dujella, Kazalicki, Mikić and Szikszai [145] proved that there exist infinitely many rational Diophantine sextuples. For example, there are infinitely many such sextuples containing the triple $\{15/14,\ -16/21,\ 7/6\}$, with the simplest one being

$$\{15/14, -16/21, 7/6, -1680/3481, -910/1083, 624/847\}.$$

No example of a rational Diophantine septuple is known and whether there is such septuple is an open problem. However, there are examples of "almost" septuples, i.e. sets of seven elements for which only one condition is missing to be a rational Diophantine septuple. In other words, there are rational Diophantine quintuples which can be extended to sextuples in two different ways. For example, the quintuple

$$\{243/560, 1147/5040, 1100/63, 7820/567, 95/112\}$$

can be extended by $38269/6480$ or by $196/45$ (see [195]).

Let us mention that recently Stoll [390] proved that Euler's extension of Fermat's quadruple to the rational quintuple (14.35) is unique. In particular, this means that this quintuple cannot be extended to a rational Diophantine sextuple. The proof of this result uses modern techniques for finding all rational points on curves of genus ≥ 2 (see [82, Chapter 13]).

There are several natural generalizations of the notion of Diophantine m-tuples. We can replace squares by k-th powers for fixed $k \geq 3$ (Bugeaud and Dujella [64] showed that there are no such quadruples for $k \geq 177$) or by arbitrary perfect powers (Luca [281] proved (with the assumption that the abc-conjecture holds) that the size of such sets is uniformly bounded; see also [208]) or with elements of the Fibonacci sequence (Luca and Szalay [284] proved that there do not exist three distinct positive integers a, b, c such that $ab + 1$, $ac + 1$ and $bc + 1$ are Fibonacci numbers).

We can replace the number 1 in the condition "$ab + 1$ is a square" by a fixed integer n. Such sets are called *$D(n)$-m-tuples* or *Diophantine m-tuples with the property $D(n)$*. The case $n = 4$ has many similarities with the classical case $n = 1$. By multiplying all elements of a $D(1)$-m-tuple by 2, we obtain a $D(4)$-m-tuple. It is easy to see that in a $D(4)$-m-tuple, at most two elements can be odd ([163]). Indeed, if we have three odd elements, say a_1, a_2, a_3, then from $a_ia_j + 4 \equiv 1 \pmod 8$, it follows that $a_1a_2 \equiv 5 \pmod 8$, $a_1a_3 \equiv 5 \pmod 8$, $a_2a_3 \equiv 5 \pmod 8$. By multiplying these three congruences, we obtain $(a_1a_2a_3)^2 \equiv 5 \pmod 8$, which is impossible. Hence, any result on the size of $D(1)$-m-tuples has a direct, although a somewhat weaker, consequence on the size of $D(4)$-m-tuples. For example, the non-existence of $D(1)$-quintuples implies the non-existence of $D(4)$-septuples. However, by a careful and technically demanding modification of arguments from the case $n = 1$, Bliznac Trebješanin and Filipin managed to prove that there is no $D(4)$-quintuple [49] (the non-existence of $D(4)$-sextuples was proved in [180], and an upper bound for the number of $D(4)$-quintuples was given in [18]).

It is easy to show that there are no $D(n)$-quadruples if $n \equiv 2 \pmod 4$. This result was proved independently in 1985 by Brown, Gupta and Singh, as well as Mohanty and Ramasamy.

Theorem 14.12. *If* $n \equiv 2 \pmod 4$*, then there does not exist a* $D(n)$*-quadruple.*

Proof: From the assumption that $a_ia_j + n$ is a square and the fact that squares of integers are $\equiv 0$ or $1 \pmod 4$, it follows that $a_ia_j \equiv 2$ or $3 \pmod 4$. This implies that none of the numbers a_i is divisible by 4. Hence, we have four numbers, with three possible remainders: 1, 2 or 3. Therefore, two of these numbers give the same remainder. We may assume that $a_1 \equiv a_2 \pmod 4$. Then $a_1a_2 \equiv a_2^2 \equiv 0$ or $1 \pmod 4$, which is a contradiction to the previously shown $a_1a_2 \equiv 2$ or $3 \pmod 4$. □

On the other hand, it can be shown that if $n \not\equiv 2 \pmod 4$ and $n \notin S = \{-4, -3, -1, 3, 5, 8, 12, 20\}$, then there is at least one $D(n)$-quadruple. Indeed, an integer n which is not of the form $4k+2$ has one of the following forms:

$$4k + 3, \;\; 8k + 1, \;\; 8k + 5, \;\; 8k, \;\; 16k + 4, \;\; 16k + 12.$$

For each of these forms, in [109], by the method similar to the one used by Diophantus, a formula for $D(n)$-quadruple was found. For example

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

is a $D(4k + 3)$-quadruple. The exceptions from the set S occur because for some (small) k's, these quadruples may have two equal elements.

For $n \in S$, the question of the existence of $D(n)$-quadruples remains open. In the case $n = -1$, let us mention some results obtained by Dujella, Filipin and Fuchs [129, 131]. They proved that there does not exist a $D(-1)$-quintuple and that there are at most finitely many $D(-1)$-quadruples (and all of them have to contain the element 1). These results also solve a similar problem which was studied by Diophantus and Euler, showing that there does not exist a set of four positive integers with the property that the product of any of two of its distinct elements plus their sum is a perfect square. Indeed, since $xy+x+y = (x+1)(y+1)-1$, the existence of such set would imply the existence of a $D(-1)$-quadruple with elements ≥ 2.

Recent work of Bonciocat, Cipu and Mignotte [53] establish the non-existence of $D(-1)$-quadruples. The proof is based on several new ideas and combines in an innovative way techniques proved successful in dealing with $D(n)$-sets with less usual tools, developed for the study of different problems. Note that this result entails the non-existence of $D(-4)$-quadruples, because it was shown in [109] that all elements of a $D(-4)$-quadruple are even.

Let

$$M_n = \sup\{|\mathcal{S}| \,:\, \mathcal{S} \text{ has the property } D(n)\}$$

and

$$M = \sup\{M_n \,:\, n \in \mathbb{Z} \setminus \{0\}\}.$$

It is known that M_n is finite for any integer $n \neq 0$. The conjecture is that the number M is also finite, i.e. that the numbers M_n are bounded from above, by a constant independent of n. This is, however, an open problem. It is known that M_p for p prime is bounded by a constant independent of p (Dujella and Luca [146] proved that $M_p < 3 \cdot 2^{168}$). However, for the general n only results such as $M_n \leq 31$ for $|n| \leq 400$, $M_n < 15.476 \ln |n|$ for $|n| > 400$, $M_n < 2.6071 \ln |n|$ for $|n|$ large enough (see [116, 118, 31]) are known. Let us mention that in the proof of some of these results, the inequality from Example 4.5 is used.

If we combine two previously stated generalizations of Diophantine m-tuples, then we can obtain arbitrarily large sets. Namely, for any positive integer m, there is a positive integer n and a set of positive integers A such that $|A| \geq m$ and $ab + n$ is a power of a positive integer for any $a, b \in A$, $a \neq b$. To be more precise, for x large enough, we can take $m = \lfloor \left(\frac{\ln \ln x}{2 \ln \ln \ln x}\right)^{1/3} \rfloor$ and (by the Chinese remainder theorem) construct the set $A_m = \{a_1, \dots, a_m\} \subset [1, x]$ and the positive integer $n_m \in [1, x]$ such that $a_i a_j + n_m = x_{ij}^{k_{ij}}$ for $1 \leq i < j \leq m$, where x_{ij} are positive integers and exponents k_{ij} are the first $\binom{m}{2}$ prime numbers (see [36]).

Let us mention that in [37, 356], so-called (F, m)-Diophantine sets were considered, i.e. sets of integers with the property that for any two distinct elements a and b, $F(a, b)$ is an m-th power, where F a bivariate polynomial with integer coefficients and $m \geq 2$ an integer. The choice $F(x, y) = xy + 1$ and $m = 2$ gives the classical case.

Instead of over the integers and rationals, the problem of Diophantus can be considered over any commutative ring with unity. Let us mention results obtained by Franušić and Soldo [185, 186, 187] over rings of integers in quadratic fields, which show that there is a close (but still not completely clarified) connection between the existence of $D(n)$-quadruples and representability of n as a difference of two squares in the considered ring. Note that the integers $n \equiv 2 \pmod 4$ from Theorem 14.12 are exactly those integers which cannot be represented as a difference of two squares of integers (Example 5.2). Let us also mention that Adžaga recently proved that in the ring of integers in an imaginary quadratic field there does not exist a $D(1)$-m-tuple for $m \geq 43$ (see [4]; in the proof, a generalization of the previously mentioned Bennett's result [34] to imaginary quadratic fields from [233] was used).

Different versions of the problem of Diophantus were also studied in the rings of polynomials, starting with the paper [237] by Jones. In [130], it was proved that every Diophantine quadruple in $\mathbb{Z}[x]$ is regular, while in [183], the same result was proved for Diophantine quadruples in $\mathbb{R}[x]$. On the other hand, it was shown in [139] that this statement does not hold in $\mathbb{C}[x]$ because for any $p \in \mathbb{C}[x]$,

$$\left\{\frac{\sqrt{-3}}{2}, -\frac{2\sqrt{-3}}{3}(p^2-1), \frac{-3+\sqrt{-3}}{3}p^2 + \frac{2\sqrt{-3}}{3}, \frac{3+\sqrt{-3}}{3}p^2 + \frac{2\sqrt{-3}}{3}\right\}$$

is a Diophantine quadruple which is not regular.

A short overview of results on Diophantine m-tuples can be found in the review paper [125] and on the web page [126], which also contains a complete list of literature on this topic, which, at the time of writing of this book, contains 458 titles.

14.7 Exercises

1. Find all integer solutions of the equation
$$x^4 - 2x^3y + 2x^2y^2 - 4xy^3 + 4y^4 = 1.$$

2. Find all integer solutions of the equation
$$(x^3 - 2x^2y + y^3)(x^2 - 3y^2) = 1.$$

3. Let $\alpha = \sqrt{2} + \sqrt{3}$. Determine the height $H(\alpha)$ and the Mahler measure $M(\alpha)$.

4. Find all solutions of the system of equations
$$y^2 - 2x^2 = 1, \quad z^2 - 3x^2 = 1$$
in integers x, y, z.