DIOPHANTINE QUADRUPLES IN $\mathbb{Z}[\sqrt{4k+3}]$

ZRINKA FRANUŠIĆ

ABSTRACT. It this paper, we study the existence of Diofantine quadruples with property $D(z)$ in the ring $\mathbb{Z}[\sqrt{d}]$, where d is such that the Pellian equation $x^2 - dy^2 = \pm 2$ is solvable. This existence is characterized by the representability of z as a difference of two squares.

1. Introduction

Let R be a commutative ring and $z \in R$. A set $\{a_1, a_2, \cdots, a_m\}$ of distinct elements in $R \backslash \{0\}$ such that $a_i a_j + z$ is a perfect square in R, for $1 \leq i < j \leq m$, is called a *Diophantine m-tuple with the property $D(z)$* or a *$D(z)$-m-tuple.* Let us give few examples of such sets in the ring of integers $\mathbb{Z}$. The set $\{1, 2, 5\}$ is a $D(-1)$-triple, $\{1, 33, 68, 105\}$ is a $D(256)$-quadruple (famous one, because this set was found by Diophantus of Alexandria himself), $\{1, 3, 8, 120\}$ is a $D(1)$-quadruple (found by Fermat, while Baker and Davenport in [2] proved that it cannot be extended to a $D(1)$-quintuple), $\{99, 315, 9920, 32768, 44460, 19534284\}$ is a $D(2985984)$-sextuple (found by Gibbs in [9]).

Here, we deal with Diophantine quadruples. A problem of the existence of Diophantine quadruples with the property $D(z)$ is almost completely solved in the ring of integers $\mathbb{Z}$ and the ring of Gaussian integers $\mathbb{Z}[i]$. Namely, in [3] (and in [10] and in [13], also) it was shown that if n is an integer of the form $n \equiv 2 (\mathrm{mod}\ 4)$, then a $D(n)$-quadruple does not exist in $\mathbb{Z}$. On the other hand, if $n \not\equiv 2 (\mathrm{mod}\ 4)$ and if $n \notin S = \{-4, -3, -1, 3, 5, 8, 12, 20\}$, then there exist a $D(n)$-quadruple (see [4]). Let us note that an integer n can be represented as a difference of two squares of integers if and only if n is not of the form $4k + 2$ for $k \in \mathbb{Z}$. Thus, we can conclude that a $D(n)$-quadruple exists if and only if n can be represented as a difference of two squares of integers, up to finitely many cases. (For the elements of the set S, it is still not known if such a quadruple exists. Recently, Dujella, Filipin and Fuchs [7] proved that there exist only finitely many $D(-1)$-quadruples and $D(-4)$-quadruples.) In the ring of Gaussian integers $\mathbb{Z}[i]$, the analogous statement can be proved (see [6]).

In this paper, the connection between the existence of a $D(z)$-quadruple and the re presentability of z as a difference of two squares is investigated

2000 *Mathematics Subject Classification.* 11D09, 11R11.

Key words and phrases. Diophantine quadruples, Pellian equations, Difference of squares.

in the ring $\mathbb{Z}[\sqrt{d}]$ for $d \in \mathbb{N}$ such that $d \equiv 3 (\mathrm{mod}\ 4)$ and that the equation $x^2 - dy^2 = \pm 2$ is solvable. Precisely, we prove the following theorem

Theorem 1. *Let $d \in \mathbb{N}$ such that d is not a perfect square and that the equation $x^2 - dy^2 = \pm 2$ is solvable in odd integers. Let z be an element of the ring $\mathbb{Z}[\sqrt{d}]$. Then there exists infinitely many $D(z)$-quadruples in $\mathbb{Z}[\sqrt{d}]$ if and only if z can be represented as a difference of two squares of elements in $\mathbb{Z}[\sqrt{d}]$.*

The first step in proving this theorem has already been made by giving the characterization of the set of all elements in $\mathbb{Z}[\sqrt{d}]$ that can be represented as a difference of two squares (see [8]). Concretely, $z \in \mathbb{Z}[\sqrt{d}]$ is represented as a difference of two squares if and only if z has one of the form $2m+1+2n\sqrt{d}$, $4m + 4n\sqrt{d}$, $4m + (4n + 2)\sqrt{d}$ or $4m + 2 + 4n\sqrt{d}$ for $m, n \in \mathbb{N}$. Thanks to this characterization, the proof of one direction of Theorem 1 is based on the effective construction of a $D(z)$-quadruples where z has one of given forms above. In some constructions, polynomial formulas for Diophantine quadruples derived in [5] are used. The fact that there are infinitely many solutions of the equation $x^2 - dy^2 = \pm 2$, under our assumption, is the reason why there exists infinitely Diophantine quadruples. This part of the proof can be found in Section 2.

The other direction of Theorem 1 is showed in Section 3. The main idea is to verify that there is no $D(z)$-quadruple if z has the form $2m + (2n + 1)\sqrt{d}$ or the form $4m+2+(4n+2)\sqrt{d}$, i.e. for those elements in $\mathbb{Z}[\sqrt{d}]$ that cannot be represented as a difference of two squares. We are, actually, able to prove this for even a lager class of rings of the form $\mathbb{Z}[\sqrt{d}]$.

Theorem 1 generalizes the corresponding result for Diophantine quadruples in the ring of Gaussian integers to the arbitrary ring $\mathbb{Z}[\sqrt{d}]$, under given assumptions on d. Let us mention that this result is also proved by the author for the ring $\mathbb{Z}[\sqrt{2}]$ in [11] and for the ring $\mathbb{Z}[(1 + \sqrt{d})/2]$, where $d \in \mathbb{N}$ is such that the Pellian equation $x^2 - dy^2 = \pm 4$ is solvable in odd x and y, in [12].

2. The existence of Diophantine quadruples

In this section, the necessity part of Theorem 1 will be proved. We assume that d is an integer which is not a perfect square and that the equation

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

is solvable in odd integers. We can, also, assume that d is positive, because the only negative d for which the equation (1) has solutions is -1 and this case has already been solved in [6]. It is easy to see that $d \equiv 3 (\mathrm{mod}\ 4)$. We denote

$$\mathbb{Z}[\sqrt{d}] = \{m + n\sqrt{d} \ : \ m, n \in \mathbb{Z}\}.$$

This ring represents the set of all integers in the quadratic field $\mathbb{Q}(\sqrt{d})$ and, accordingly, the term 'integer' is sometimes used for an element of the ring $\mathbb{Z}[\sqrt{d}]$.

The following lemma describes the set of all elements that can be represented as a difference of two squares in $\mathbb{Z}[\sqrt{d}]$ under the above assumptions.

Lemma 1. [8, Theorem 1] *An element $z \in \mathbb{Z}[\sqrt{d}]$ can be represented as a difference of two squares in $\mathbb{Z}[\sqrt{d}]$ if and only if z has one of the following forms*

$$2m+1+2n\sqrt{d},\ 4m+4n\sqrt{d},\ 4m+(4n+2)\sqrt{d},\ 4m+2+4n\sqrt{d},$$

where $m, n \in \mathbb{Z}$.

We will construct a Diophantine quadruple for each integer z that can be represented as a difference of two squares, i.e. for an integer of the forms $2m+1+2n\sqrt{d}$, $4m+4n\sqrt{d}$, $4m+(4n+2)\sqrt{d}$, $4m+2+4n\sqrt{d}$. The following facts will be used in these constructions.

Lemma 2. *(*[5, Theorem 1]*) The sets*

$$\{m, (3k+1)^2m+2k, (3k+2)^2m+2k+2, 9(2k+1)^2m+8k+4\},$$

$$\{m, mk^2-2k-2, m(k+1)^2-2k, m(2k+1)^2-8k-4\}$$

have the property $D(2m(2k+1)+1)$.

The term *set with the property $D(z)$* is used for a set which is a good candidate for a $D(z)$-quadruple, but it might have two equal elements or an element equals to zero or its elements are not integers.

Lemma 3. *(* [4]*) The set*

$$\{1, 9k^2-8k, 9k^2-2k+1, 36k^2-20k+1\}$$

has the property $D(8k)$, and the set

$$\{4, 9k^2-5k, 9k^2+7k+2, 36k^2+4k\}$$

has the property $D(8k+1)$.

Lemma 4. *Let $\{z_1, z_2, z_3, z_4\} \subset \mathbb{Z}[\sqrt{d}]$ be a set with the property $D(z)$ and $w \in \mathbb{Z}[\sqrt{d}]$. Then $\{z_1w, z_2w, z_3w, z_4w\}$ is a set with the property $D(zw^2)$.*

Proof. It is obvious from the definition of the set with the property $D(z)$. □

Instead of the assumption of solvability the equation $x^2 - dy^2 = \pm 2$, we will often use the following consequence:

Lemma 5. *Let $d \in \mathbb{N}$ such that d is not a perfect square. If the equation $x^2 - dy^2 = \pm 2$ has a solution in odd numbers x and y, then the Pell equation $x^2 - dy^2 = 1$ has infinitely many solutions in even x and odd y.*

Proof. Let α and β be the odd solutions of the equation $x^2 - dy^2 = \pm 2$. Then $x = \alpha^2 \mp 1$ and $y = \alpha\beta$ are solutions of $x^2 - dy^2 = 1$ and the parity conditions hold as well. Also, it is clear that there exist infinitely many of such solutions. □

Proposition 1. *Let $z \in \mathbb{Z}[\sqrt{d}]$ be of the form*

$$2m + 1 + 2n\sqrt{d},$$

for $m, n \in \mathbb{Z}$. Then there exist infinitely many $D(z)$-quadruples in $\mathbb{Z}[\sqrt{d}]$.

Proof. The proof splits into four parts.
1) Let $k \in \mathbb{Z}[\sqrt{d}]$. We will prove the existence of a $D(4k+3)$-quadruple. The set

$$\{1, 9k^2 + 8k + 1, 9k^2 + 14k + 6, 36k^2 + 44k + 13\},\ k \in \mathbb{Z}[\sqrt{d}] \tag{2}$$

has the property $D(4k+3)$, according to Lemma 2 (for $m = 1$). If the elements of the set (2) are nonzero distinct integers, then this set represents the $D(4k+3)$-quadruple. It is easy to see that this holds for all $k \in \mathbb{Z}[\sqrt{d}]\backslash\{0, 1, -1, 2, 3\}$. So, we show the existence of the $D(4m + 3 + 4n\sqrt{d})$-quadruple, for $m, n \in \mathbb{Z}$ and $m \neq 0, 1, -1, 2, 3$, i.e. for $4m + 3 + 4n\sqrt{d} \in \mathbb{Z}[\sqrt{d}]\backslash\{3, 7, -1, 11, 15\}$

In the cases where $z = 7, 11, 15$, we are able to find a Diophantine quadruples in $\mathbb{Z}$ and these are $\{1, 18, 29, 93\}$, $\{1, 53, 70, 245\}$, $\{1, 106, 129, 469\}$, respectively.

Now, let us show the existence of a $D(-1)$-quadruple. Suppose that $s, t \in \mathbb{Z}$ are solutions of the equation $x^2 - dx^2 = 1$, where s is even and t is odd (according to Lemma 5). We define

$$w = -(s + t\sqrt{d})^4 = -(s^4 + 4ds^2t^2 + d^2t^4) - 4st(s^2 + dt^2)\sqrt{d}.$$

It can be immediately seen that w has the form $4m + 3 + 4n\sqrt{d}$ and that $w \neq -1, 3$ (unless $d = -1$). Hence, there exists a Diophantine quadruple $\{c_1, c_2, c_3, c_4\}$ with the property $D(w)$. Lemma 4 implies that the set $\{c_1(s - t\sqrt{d})^2, c_2(s - t\sqrt{d})^2, c_3(s - t\sqrt{d})^2, c_4(s - t\sqrt{d})^2\}$ is the $D(-1)$-quadruple, because $-1 = -(s^2 - dt^2)^4 = -(s + t\sqrt{d})^4(s - t\sqrt{d})^4 = w(s - t\sqrt{d})^4$.

Analogously, the existence of $D(3)$-quadruple can be proved. We start with the number $w = 3(s + t\sqrt{d})^4$ and the rest of the proof is the same as in the previous case $z = -1$.

Finally, let us explain the existence of infinitely many $D(4m + 3 + 4n\sqrt{d})$-quadruples. Let z be an integer of the form $4m + 3 + 4n\sqrt{d}$. If $w = s + t\sqrt{d}$ is a solution of the Pell equation $x^2 - dy^2 = 1$ in even s and in odd t, then zw^4 is, also, of the form $4m + 3 + 4n\sqrt{d}$. Indeed, $w^4 \equiv 1 (\mathrm{mod}\ 4)$. Suppose that sets $\{c_1, c_2, c_3, c_4\}$ and $\{d_1, d_2, d_3, d_4\}$ represent Diophantine quadruples with properties $D(z)$ and $D(zw^4)$, respectively, which are obtained by the described construction. According to Lemma 4, the set $\{d_1(s - t\sqrt{d})^2, d_2(s - t\sqrt{d})^2, d_3(s - t\sqrt{d})^2, d_4(s - t\sqrt{d})^2\}$ is a $D(z)$-quadruple and it is, obviously, different from the quadruple $\{c_1, c_2, c_3, c_4\}$. Furthermore, we see that there exist infinitely many Diophantine quadruples, because w is chosen as a solution of the Pell equation.

2) In this part we prove the existence of a Diophantine quadruple with the property $D(4m+1+4n\sqrt{d})$, $m, n \in \mathbb{Z}$. We will show that there exist integers $p, q, s, t \in \mathbb{Z}$ such that the following equality

$$(4p+3+4q\sqrt{d})(s+t\sqrt{d})^2 = 4m+1+4n\sqrt{d} \tag{3}$$

holds. Indeed, the equality (3) is equivalent to the linear system in unknowns $4p+3$ and $4q$:

$$\begin{array}{rcrcl} (s^2+dt^2)(4p+3) & + & (2std)4q & = & 4m+1 \\ (2st)(4p+3) & + & (s^2+dt^2)4q & = & 4n. \end{array} \tag{4}$$

According to Lemma 5, we can choose $s, t \in \mathbb{Z}$ such that $s^2 - dt^2 = 1$ where s is even and t is odd. Hence, the determinant of (4) is $(s^2-dt^2)^2$ and the solutions of (4) are

$$4p+3 = (4m+1)(s^2+dt^2) - 8stdn, \tag{5}$$

$$4q = 4n(s^2+dt^2) - 2std(4m+1). \tag{6}$$

Integers p and q, given by (5) and (6), are well defined, because the right sides of formulas (5) and (6) are congruent to 3 modulo 4, and 0 modulo 4, respectively.

Finally, the equality (3), Lemma 4 and previous case 1), imply the existence of infinitely many $D(4m+1+4n\sqrt{d})$-quadruples.

3) Let $z = 4m+1+(4n+2)\sqrt{d}$, where $m, n \in \mathbb{Z}$. We will prove that z can be represented as

$$z = 2l(2k+1)+1, \tag{7}$$

for some $l, k \in \mathbb{Z}[\sqrt{d}]$. In fact, (7) can be written as

$$\begin{array}{rcrcl} 2\alpha\gamma & + & 2d\beta\delta & = & 2m-\alpha, \\ 2\beta\gamma & + & 2\alpha\delta & = & 2n+1-\beta. \end{array} \tag{8}$$

where $l = \alpha+\beta\sqrt{d}$ and $k = \gamma+\delta\sqrt{d}$, $\alpha, \beta, \gamma, \delta \in \mathbb{Z}$. We choose α and $\beta \in \mathbb{Z}$ such that $\alpha^2 - d\beta^2 = 1$ and α is even and β is odd (according to Lemma 5). Let solve the system (8) in unknowns γ and δ. The determinant of the system (8) is $4\alpha^2 - 4d\beta^2 = 4$ and the solutions are

$$\gamma = ((2m-\alpha)2\alpha - (2n+1-\beta)2\beta)/4, \tag{9}$$

$$\delta = ((2n+1-\beta)2\alpha - (2m-\alpha)2\beta)/4. \tag{10}$$

It can be easily seen that the numerators in (9) and (10) are divisible by 4. Hence, γ and δ are integers.

Lemma 2 implies that the set

$$\{l, (3k+1)^2l+2l, (3k+2)^2l+2k+2, 9(2k+1)^2l+8k+4\} \tag{11}$$

has the property $D(4m+1+(4n+2)\sqrt{d})$. It is clear that we can construct infinitely many such sets, because the number l is one of infinitely many solutions of Pell equation $x^2-dy^2=1$.

Let us note that the set (11) does not represent a $D(4m+1+(4n+2)\sqrt{d})$-quadruple if some of it's elements is zero or if there exist two equal elements. This situation can be avoid by using a similar procedure as in the case 1).

4) Let $z=4m+3+(4n+2)\sqrt{d}$, $m,n\in\mathbb{Z}$. If there exist numbers $s+t\sqrt{d}\in\mathbb{Z}[\sqrt{d}]$ and $p,q\in\mathbb{Z}$ such that

$$(4p+1+(4q+2)\sqrt{d})(s+t\sqrt{d})^2=4m+3+(4n+2)\sqrt{d}, \tag{12}$$

then the $D(z)$-quadruple exists according to Lemma 4 and previous case 3). Therefore, let us solve the equation (12) or equivalently the system

$$\begin{array}{rcrcl} (s^2+dt^2)(4p+1) & + & (2std)(4q+2) & = & 4m+3 \\ (2st)(4p+1) & + & (s^2+dt^2)(4q+2) & = & 4n+2. \end{array} \tag{13}$$

Let s and t be integer solutions of $s^2-dt^2=1$ such that s is even and t is odd (according to Lemma 5). Then the solutions of (13) are given by

$$\begin{array}{rcl} 4p+1 & = & (4m+3)(s^2+dt^2)-(4n+2)2std, \\ 4q+2 & = & (4n+2)(s^2+dt^2)-(4m+3)2std. \end{array}$$

Obviously, p and q, as defined above, are integers. □

Proposition 2. *Let $z\in\mathbb{Z}[\sqrt{d}]$ be of the form*

$$z=4m+(4n+2)\sqrt{d},$$

$m,n\in\mathbb{Z}$. Then there exist infinitely many $D(z)$-quadruples in $\mathbb{Z}[\sqrt{d}]$.

Proof. We will show that for given $m,n\in\mathbb{Z}$ there exist $a,b\in\mathbb{Z}$ and $w\in\mathbb{Z}[\sqrt{d}]$ such that

$$(2a+1+2b\sqrt{d})w^2=4m+(4n+2)\sqrt{d}. \tag{14}$$

If $w=s+t\sqrt{d}$, where $s,t\in\mathbb{Z}$, then (14) implies

$$\begin{array}{rcrcl} (s^2+dt^2)(2a+1) & + & (2std)(2b) & = & 4m, \\ (2st)(2a+1) & + & (s^2+dt^2)(2b) & = & 4n+2. \end{array} \tag{15}$$

Let s and t be integer solutions of the equation $x^2-dy^2=\pm 2$. We solve the system (15) in unknowns $2a+1$ and $2b$. The determinant of the system (15) is equal to 4 and the solutions are given by the formulas

$$\begin{array}{rcl} 2a+1 & = & (4m(s^2+dt^2)-2std(4n+2))/4, \\ 2b & = & ((4n+2)(s^2+dt^2)-8stm)/4. \end{array} \tag{16}$$

These formulas define integers a and b. Indeed, for numerators in (16) we have

$$\begin{aligned} 4m(s^2+dt^2)-2std(4n+2) &\equiv -4std\equiv 4 (\text{mod } 8), \\ (4n+2)(s^2+dt^2)-8stm &\equiv 0 (\text{mod } 8), \end{aligned}$$

because s and t are odd and $s^2 + dt^2 \equiv 0 (\text{mod } 4)$.

According to Proposition 1 there exist infinitely many Diophantine quadruples with the property $D(2a + 1 + 2b\sqrt{d})$. Finally, it follows from (14) and Lemma 4 that there exist infinitely many Diophantine quadruples with the property $D(4m + (4n + 2)\sqrt{d})$. □

Proposition 3. *Let z be an integer in $\mathbb{Z}[\sqrt{d}]$ of the form*

$$4m + 4n\sqrt{d},$$

$m, n \in \mathbb{Z}$. Then there exist infinitely many $D(z)$-quadruples in $\mathbb{Z}[\sqrt{d}]$.

Proof. The proof splits into four parts. The existence of Diophantine quadruple will be shown for numbers of the following forms: $8m + 4 + 8n\sqrt{d}$, $8m + 8n\sqrt{d}$, $8m + (8n + 4)\sqrt{d}$ and $8m + 4 + (8n + 4)\sqrt{d}$.

1) Let $m, n \in \mathbb{Z}$ and $s, t \in \mathbb{Z}$ such that $s^2 - dt^2 = \pm 2$. Then there exist $a, b \in \mathbb{Z}$ such that

$$(4a + (4b + 2)\sqrt{d})(s + t\sqrt{d})^2 = 8m + 4 + 8n\sqrt{d}. \tag{17}$$

Indeed, (17) holds if and only if the following system

$$\begin{array}{rcrcl} (s^2 + dt^2)4a & + & 2std(4b + 2) & = & 8m + 4, \\ (2st)4a & + & (s^2 + dt^2)(4b + 2) & = & 8n, \end{array}$$

has integral solutions. Those solutions are given by formulas

$$\begin{array}{rcl} 4a & = & ((8m + 4)(s^2 + dt^2) - 16nstd)/4, \\ 4b + 2 & = & (8n(s^2 + dt^2) - (8m + 4)2st)/4. \end{array} \tag{18}$$

It is easy to see that numbers a and b are integers. Finally, Proposition 2, Lemma 4 and (17) imply the existence of infinitely many $D(8m+4+8n\sqrt{d})$-quadruples.

2) Let $z = 8m + 8n\sqrt{d}$, where $m, n \in \mathbb{Z}$. According to Lemma 3, the set

$$\{1, 9k^2 - 8k, 9k^2 - 2k + 1, 36k^2 - 20k + 1\}$$

has the property $D(8m + 8n\sqrt{d})$, where $k = m + n\sqrt{d}$. This set represents a $D(z)$-quadruple if its elements are nonzero and mutually distinct. We handle these possible undesirable cases as it was described in the proof of Proposition 1. Further, analogously as in Proposition 1, we conclude that there exist infinitely many $D(z)$-quadruples.

3) Let $z = l(2k + 1) + 1$, where $k, l \in \mathbb{Z}[\sqrt{d}]$. Lemma 3 implies that the set

$$\{\frac{1}{2}l, \frac{1}{2}lk^2 - 2k - 2, \frac{1}{2}l(k + 1)^2 - 2k, \frac{1}{2}l(2k + 1)^2 - 8k - 4\} \tag{19}$$

has the property $D(l(2k + 1) + 1)$. If we assume that $l = \alpha + \beta\sqrt{d}$, where α and β are odd and $k = \gamma + \delta\sqrt{d}$, then

$$z = 2\alpha\gamma + 2\beta\delta d + \alpha + 1 + (2\alpha\delta + 2\beta\gamma + \beta)\sqrt{d} \tag{20}$$

and z has the form $2\xi+(2\eta+1)\sqrt{d}$, $\xi,\eta\in\mathbb{Z}$. Vice versa, if $z=2\xi+(2\eta+1)\sqrt{d}$, then there exist $\alpha,\beta,\gamma,\delta\in\mathbb{Z}$ such that (20) holds. The numbers α,β are chosen as integral solution of the equation $x^2-dy^2=\pm2$ and γ,δ are solutions of the system

$$\begin{array}{rcrcl} 2\alpha\gamma & + & 2\beta d\delta & = & 2\xi-\alpha-1, \\ 2\beta\gamma & + & 2\alpha\delta & = & 2\eta+1-\beta. \end{array} \tag{21}$$

It remains us to show that γ,δ are integers. We have

$$\gamma=((2\xi-\alpha-1)2\alpha-(2\eta+1-\beta)2\beta d)/8, \tag{22}$$

$$\delta=((2\eta+1-\beta)2\alpha-(2\xi-1-\alpha)2\beta)/8. \tag{23}$$

and

$$(2\xi-\alpha-1)2\alpha-(2\eta+1-\beta)2\beta d\equiv 0(\mathrm{mod}\ 4),$$
$$(2\eta+1-\beta)2\alpha-(2\xi-1-\alpha)2\beta\equiv 0(\mathrm{mod}\ 4),$$

because α,β are odd. Let $\mu,\nu\in\mathbb{Z}$ be such that $2\xi-\alpha-1=2\mu$ and $2\eta+1-\beta=2\nu$. The numerator in (22), $4(\mu\alpha-\nu\beta d)$, is divisible by 8 if and only if μ and ν are of the same parity. The same conclusion holds for (23). So, we conclude that γ,δ are integers if and only if $2\xi-\alpha-1\equiv 2\eta+1-\beta\equiv 0$ or $2(\mathrm{mod}\ 4)$. These conditions can be always fulfilled. For instance, if we have that $2\xi-\alpha-1\equiv 0(\mathrm{mod}\ 4)$ and $2\eta+1-\beta\equiv 2(\mathrm{mod}\ 4)$, then we take $-\alpha$ instead of α.

So, we proved that for each $z=2\xi+(2\eta+1)\sqrt{d}\in\mathbb{Z}[\sqrt{d}]$ there exist $l,k\in\mathbb{Z}[\sqrt{d}]$ such that $z=l(2k+1)+1$. The elements of the set (19) multiplied by 2 are integers and this set has the property $D(4z)$, i.e. property $D(8\xi+(8\eta+4)\sqrt{d})$, according to Lemma 4. Obviously, infinitely many of such sets can be constructed, because α and β are solutions of a Pellian equation.

4) In this step we show the existence of the $D(8m+4+(8n+4)\sqrt{d})$-quadruple by using similar idea as in the previous case 3). If we prove that for arbitrary $m,n\in\mathbb{Z}$ there exist $l,k\in\mathbb{Z}[\sqrt{d}]$ such that

$$2m+1+(2n+1)\sqrt{d}=l(2k+1)+1, \tag{24}$$

than the set (19) multiplied by 2 represents the $D(8m+4+(8n+4)\sqrt{d})$-quadruple. The equation (24) is equivalent to the linear system

$$\begin{array}{rcrcl} 2\alpha\gamma & + & 2\beta d\delta & = & 2m-\alpha, \\ 2\beta\gamma & + & 2\alpha\delta & = & 2n+1-\beta, \end{array} \tag{25}$$

where $m=\alpha+\beta\sqrt{d}$ and $l=\gamma+\delta\sqrt{d}$. Now, we take even α and odd β as a solution of the Pell equation $x^2-dy^2=1$ and solve (25) in unknowns γ and δ,

$$\begin{array}{rcl} \gamma & = & ((2m-\alpha)2\alpha-(2n+1-\beta)2\beta d)/4, \\ \delta & = & ((2n+1-\beta)2\alpha-(2m-1-\alpha)2\beta)/4. \end{array}$$

It can be easily verified that γ and δ are integers.

□

Proposition 4. *Let $z \in \mathbb{Z}[\sqrt{d}]$ be of the form*

$$4m+2+4n\sqrt{d},$$

$m,n \in \mathbb{Z}$. There exist infinitely many $D(z)$-quadruples in $\mathbb{Z}[\sqrt{d}]$.

Proof. First, let us prove that for each integer $4m+2+4n\sqrt{d}$ there exist $l,k,w \in \mathbb{Z}[\sqrt{d}]$ such that

$$4m+2+4n\sqrt{d} = (l(2k+1)+1)w^2. \tag{26}$$

In the case 3) of Proposition 3, it was shown that for given $\xi, \eta \in \mathbb{Z}$ there exist $l=\alpha+\beta\sqrt{d}$ and $k=\gamma+\delta\sqrt{d}$ in $\mathbb{Z}[\sqrt{d}]$ such that $2\xi+(2\eta+1)\sqrt{d} = l(2k+1)+1$ and α, β are the solutions of $x^2-dy^2=\pm 2$. Hence, instead of proving (26), we will prove that there exist $\xi, \eta \in \mathbb{Z}$ and $w \in \mathbb{Z}[\sqrt{d}]$ such that

$$4m+2+4n\sqrt{d} = (2\xi+(2\eta+1)\sqrt{d})w^2. \tag{27}$$

The equation (27) is equivalent to the system

$$\begin{array}{rcrcl} (s^2+dt^2)2\xi & + & (2std)(2\eta+1) & = & 4m+2, \\ (2st)2\xi & + & (s^2+dt^2)(2\eta+1) & = & 4n, \end{array} \tag{28}$$

where $w=s+t\sqrt{d}$. We solve this system in unknowns 2ξ and $2\eta+1$. If s,t are chosen to be solutions of the equation $x^2-dy^2=\pm 2$, then the solutions of (28) are given by the formulas

$$\begin{aligned} 2\xi &= ((4m+2)(s^2+dt^2)-(4n)2std)/4, \\ 2\eta+1 &= (4n(s^2+dt^2)-(4m+2)2st)/4. \end{aligned}$$

It can be easily verified that ξ and η are integers, because s,t are odd and $s^2+dt^2 \equiv 0 (\mathrm{mod}\ 4)$.

Now, the equation (26), Lemma 2 and Lemma 4 imply that the set

$$\{\frac{1}{2}lw, (\frac{1}{2}lk^2-2k-2)w, (\frac{1}{2}l(k+1)^2-2k)w, (\frac{1}{2}l(2k+1)^2-8k-4)w\} \tag{29}$$

has the property $D(4m+2+4n\sqrt{d})$. Even more, (29) is the $D(4m+2+4n\sqrt{d})$-quadruple, because the elements of (29) are in $\mathbb{Z}[\sqrt{d}]$. Indeed, the element

$$\frac{1}{2}lw = \frac{1}{2}(\alpha+\beta\sqrt{d})(s+t\sqrt{d}) = \frac{1}{2}(\alpha s+\beta td+(\alpha t+\beta s)\sqrt{d})$$

is obviously in $\mathbb{Z}[\sqrt{d}]$, because α, β, s, t are odd. The same can be checked for other elements of (29). Also, it is clear that there are infinitely many such sets because s and t (and so are α and β) are solutions of the equation $x^2-dy^2=\pm 2$.

□

3. The nonexistence of Diophantine quadruple

In this part, we will show the sufficiency part of Theorem 1. In fact, we will show even stronger claims, because we will do not use the assumption of solvability of the equation $x^2 - dy^2 = \pm 2$ in this section.

Proposition 5. *Let $d \in \mathbb{Z}$ such that $d \equiv 3(mod\ 4)$. If*

$$z = 4m + 2 + (4n+2)\sqrt{d},$$

$m, n \in \mathbb{Z}$, then there does not exist a Diophantine quadruple with the property $D(z)$ in the ring $\mathbb{Z}[\sqrt{d}]$.

Proof. Let us assume that the set $\{z_1, z_2, z_3, z_4\}$ represents the $D(4m+2+(4n+2)\sqrt{d})$-quadruple. Let $z_i = x_i + y_i\sqrt{d}$, for $i = 1,2,3,4$. From the definition of a Diophantine quadruple, there exist $\xi_{ij}, \eta_{ij} \in \mathbb{Z}$ for $1 \le i < j \le 4$ such that

$$(x_i + y_i\sqrt{d})(x_j + y_j\sqrt{d}) + z = (\xi_{ij} + \eta_{ij}\sqrt{d})^2, \tag{30}$$

for all $1 \le i < j \le 4$. The equation (30) can be written in the following form

$$\begin{aligned} x_ix_j + y_iy_jd + 4m + 2 &= {\xi_{ij}}^2 + d{\eta_{ij}}^2, \\ x_iy_j + x_jy_i + 4n + 2 &= 2\xi_{ij}\eta_{ij}. \end{aligned} \tag{31}$$

By analyzing left sides of (31) in the set of remainders modulo 4, we obtain that the following condition
(32)

$$(x_ix_j + y_iy_j + 2, x_iy_j + x_jy_i + 2) \mod 4 \in \{(0,0),(0,2),(1,0),(3,0)\} = S$$

has to be satisfied. Our intention is to show that there is no quadruple in $\mathbb{Z}[\sqrt{d}]$ such that the condition (32) is satisfied.

Initially, let $x_1 \equiv 1(\text{mod } 4)$ and $y_1 \equiv 0(\text{mod } 4)$. We choose $x_2, y_2 \in \mathbb{Z}$ such that (32) is fulfilled for $i = 1$ and $j = 2$, i.e. such that $(x_2+2, y_2+2) \mod 4 \in S$. This implies that

$$(x_2, y_2) \mod 4 \in \{(2,2),(2,0),(3,2),(1,2)\}.$$

First, let us assume that $x_2 \equiv 2(\text{mod } 4)$ and $y_2 \equiv 2(\text{mod } 4)$. We add the third element $x_3 + y_3\sqrt{d}$ which has to satisfy (32) for $i = 1,2$ and $j = 3$. Obviously, we have $(x_3, y_3) \mod 4 \in \{(2,2),(2,0),(3,2),(1,2)\}$. From (32) for $i = 2$ and $j = 3$ we obtain that

$$(2x_3 + 2y_3 + 2, 2y_3 + 2x_3 + 2) \mod 4 \in S.$$

Hence,

$$(x_3, y_3) \mod 4 \in \{(3,2),(1,2)\} = T.$$

If $x_4 + y_4\sqrt{d}$ is the last element of the quadruple, then (32) for $i = 1,2$ and $j = 4$ implies that $(x_4, y_4) \mod 4 \in T$. The condition (32) for $i = 3$ and $j = 4$, gives us that

$$(x_3x_4 + y_3y_4 + 2, x_3y_4 + x_4y_3 + 2) \mod 4 \in S,$$

and, on the other hand, we have that

$$(x_3x_4 + y_3y_4 + 2, x_3y_4 + x_4y_3 + 2) \mod 4 \in T,$$

for $(x_3, y_3) \mod 4 \in T$ and $(x_4, y_4) \mod 4 \in T$. This is a contradiction, since $S \cap T = \emptyset$.

So, we showed that the set $\{z_1, z_2\}$ such that $z_1 \equiv 1 (\text{mod } 4)$ and $z_2 \equiv 2 + 2\sqrt{d} (\text{mod } 4)$ can not be extended to a Diophantine quadruple with the property $D(4m + 2 + (4n + 2)\sqrt{d})$. All the other cases are checked on a computer by using the algorithm described above. □

The statement in the following proposition is valid for an arbitrary ring $\mathbb{Z}[\sqrt{d}]$ without any assumptions on d.

Proposition 6. *Let $z = a + b\sqrt{d} \in \mathbb{Z}[\sqrt{d}]$, where b is odd. Then there is no Diophantine quadruple with the property $D(z)$ in the ring $\mathbb{Z}[\sqrt{d}]$.*

Proof. The proof of Proposition 1 in [1] for $d = -2$ can be immediately generalized for an arbitrary d.

□

References

[1] F. S. Abu Muriefah, A. Al-Rashed, *Some Diophantine quadruples in the ring* $\mathbb{Z}[\sqrt{-2}]$, Math. Commun. **9**(2004), 1-8.

[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] E. Brown, *Sets in which $xy+k$ is always a square*, Math. Comp. **45** (1985), 613–620.

[4] A. Dujella, *Generalization of a problem of Diophantus*, Acta Arith. **65** (1993), 15–27.

[5] A. Dujella, *Some polynomial formulas for Diophantine quadruples*, Grazer Math. Ber. **328**(1996), 25–30.

[6] A. Dujella, *The problem of Diophantus and Davenport for Gaussian integers*, Glas. Mat. Ser. III **32** (1997), 1–10.

[7] A. Dujella, A. Filipin and C. Fuchs, *Effective solution of the D(-1)-quadruple conjecture*, preprint.

[8] A. Dujella and Z. Franušić, *On differences of two squares in some quadratic fields*, Rocky Mountain J. Math., to appear.

[9] P. Gibbs, *Some rational Diophantine quadruples*, preprint, `math.NT/9902081`

[10] H. Gupta and K. Singh, *On k-triad sequences*, Internat. J. Math. Math. Sci. **8** (1985), 799–804.

[11] Z. Franušić, *Diophantine quadruples in the ring* $\mathbb{Z}[\sqrt{2}]$, Math. Commun. **9**(2004), 141–148.

[12] Z. Franušić,

[13] S. P. Mohanty and M. S. Ramasamy, *On $P_{r,k}$ sequences*, Fibonacci Quart. **23** (1985), 36–44.

[14] W. Sierpiński, *Elementary Theory of Numbers*, PWN, Warszawa; North Holland, Amsterdam, 1987.

Zrinka Franušić
Department of Mathematics
University of Zagreb

Bijenička cesta 30
10000 Zagreb, Croatia
e-mail: fran@math.hr