ROCKY MOUNTAIN
JOURNAL OF MATHEMATICS
Volume 37, Number 2, 2007

ON DIFFERENCES OF TWO SQUARES IN SOME QUADRATIC FIELDS

ANDREJ DUJELLA AND ZRINKA FRANUŠIĆ

ABSTRACT. In this paper, we study the problem of determining the elements in the rings of integers of quadratic fields $\mathbf{Q}(\sqrt{d})$ which are representable as a difference of two squares. The complete solution of the problem is obtained for integers d which satisfy conditions given in terms of solvability of certain Pellian equations.

1. Introduction. It is well known that an integer n can be represented as a difference of squares of two integers if and only if $n \not\equiv 2 \pmod 4$. A similar result holds in the ring $\mathbf{Z}[i]$ of Gaussian integers. Namely, a Gaussian integer $z = a + bi$ is representable as a difference of squares of two Gaussian integers if and only if b is even and not both a and b are congruent to 2 modulo 4, see [**14**], [**16**, p. 449]. Actually, the result for Gaussian integers is usually stated in terms of sums of two squares, but since -1 is a square in $\mathbf{Z}[i]$, these two problems in $\mathbf{Z}[i]$ are identical. However, it seems that in more general rings, the problem of representability as a sum of two squares is much better studied. In particular, in [**14**] this problem was completely solved for integers in quadratic fields.

It this paper, we will consider the problem of representability as a difference of two squares in the rings of integers of quadratic fields $\mathbf{Q}(\sqrt{d})$. Let $d \neq 1$ be a square-free integer. If $d \equiv 2, 3 \pmod 4$, then algebraic integers of the quadratic field $\mathbf{Q}(\sqrt{d})$ form the ring $\mathbf{Z}[d]$ while, if $d \equiv 1 \pmod 4$, then they form the ring $\mathbf{Z}[(1+\sqrt{d})/2]$. Since the square-free assumption is not essential for our investigation, we will consider the problem of representability as a difference of two squares in rings $\mathbf{Z}[\sqrt{d}]$ for nonsquare integers d and in rings $\mathbf{Z}[(1+\sqrt{d})/2]$ for nonsquare integers $d \equiv 1 \pmod 4$. Some of our results are valid

2000 AMS *Mathematics Subject Classification.* Primary 11D09, 11E25, 11R11.
Key words and phrases. Difference of squares, quadratic fields, Pellian equations.
This work was supported by the Ministry of Sci., Educ. and Sport, Republic of Croatia, grant 0037110.
Received by the editors on July 19, 2004, and in revised form on Aug. 23, 2004.

for all such integers d, but the complete solution of the problem is obtained only for integers which satisfy some additional conditions. These conditions are given in terms of solvability of certain Pellian equations.

Theorem 1. *If $d \equiv 3 \pmod 4$ and the equation $x^2 - dy^2 = \pm 2$ is solvable, then $z \in \mathbf{Z}[\sqrt{d}]$ is representable as a difference of two squares in $\mathbf{Z}[\sqrt{d}]$ if and only if z has one the following forms*

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

If $d \equiv 0 \pmod 4$ and the equation $x^2 - dy^2 = \pm 4$ is solvable with odd y, then $z \in \mathbf{Z}[\sqrt{d}]$ is representable as a difference of two squares in $\mathbf{Z}[\sqrt{d}]$ if and only if z has one the following forms

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

If $d \equiv 2 \pmod 4$ and the equation $x^2 - dy^2 = \pm 2$ is solvable, then $z \in \mathbf{Z}[\sqrt{d}]$ is representable as a difference of two squares in $\mathbf{Z}[\sqrt{d}]$ if and only if z has one the following forms

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

If $d \equiv 5 \pmod 8$ and the equation $x^2 - dy^2 = \pm 4$ is solvable in odd integers x and y, then $z \in \mathbf{Z}[\sqrt{d}]$ is representable as a difference of two squares in $\mathbf{Z}[\sqrt{d}]$ if and only if z has one of the following forms

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

If $d \equiv 1 \pmod 8$ and the equation $x^2 - dy^2 = \pm 8$ is solvable, then $z \in \mathbf{Z}[\sqrt{d}]$ is representable as a difference of two squares in $\mathbf{Z}[\sqrt{d}]$ if and only if z has one the following forms

$$\begin{gathered} 2m + 1 + 2n\sqrt{d}, \quad 4m + 4n\sqrt{d}, \\ 16m + l + (16n + l - \delta)\sqrt{d}, \quad 16m + l + (16n - l + \delta)\sqrt{d}, \end{gathered}$$

where $l \in \{2, 6, 10, 14\}$ and $\delta = 0$ if $d \equiv 1 \pmod{16}$, $\delta = 8$ if $d \equiv 9 \pmod{16}$.

Let us note that $d = -1$ is the only negative integer $d \equiv 3 \pmod 4$ which satisfies the conditions of Theorem 1. In that way, the above mentioned result on Gaussian integers becomes an immediate corollary of Theorem 1.

Theorem 2. *If* $d \equiv 5 \pmod 8$ *and the equation* $x^2 - dy^2 = \pm 4$ *is solvable in odd integers* x *and* y*, then* $z \in \mathbf{Z}[(1+\sqrt{d})/2]$ *is representable as a difference of two squares in* $\mathbf{Z}[(1+\sqrt{d})/2]$ *if and only if* z *has one the following forms*

$$\begin{gathered} 2m+1+2n\sqrt{d}, \quad 2m+(2n+1)\sqrt{d}, \\ 4m+4n\sqrt{d}, \quad 4m+2+(4n+2)\sqrt{d}, \\ \frac{2m+1}{2}+\frac{2n+1}{2}\sqrt{d}. \end{gathered}$$

One motivation for studying the problem of determination of elements which are representable as a difference of two squares comes from its close connection with the problem of the existence of Diophantine quadruples.

Let n be a given nonzero integer. A set of m positive integers $\{a_1, a_2, \dots, a_m\}$ is called a $D(n)$*-m-tuple*, or a *Diophantine m-tuple with the property* $D(n)$, if $a_i a_j + n$ is a perfect square for all $1 \le i < j \le m$. Diophantus himself found the $D(256)$-quadruple {1, 33, 68, 105}, while the first $D(1)$-quadruple, {1, 3, 8, 120}, was found by Fermat, see [**3**, Volume 2, pp. 513–520]. Using the theory on linear forms in logarithms of algebraic numbers and a reduction method based on continued fractions, Baker and Davenport [**1**] proved that this Fermat's set cannot be extended to a $D(1)$-quintuple. A famous conjecture is that there does not exist a $D(1)$-quintuple. The first author proved recently that there does not exist a $D(1)$-sextuple and that there are only finitely many, effectively computable, $D(1)$-quintuples, see [**6**]. Furthermore, the first author and C. Fuchs proved that there does not exist a $D(-1)$-quintuple, see [**7**].

Considering congruences modulo 4, it is easy to prove that, if $n \equiv 2 \pmod 4$, then there does not exist a $D(n)$-quadruple, see [**2, 8, 12**]. On the other hand, if $n \not\equiv 2 \pmod 4$ and $n \notin$

$\{-4, -3, -1, 3, 5, 8, 12, 20\}$, then there exists at least one $D(n)$-quadruple, see [**4**]. These results were generalized to Gaussian integers in [**5**]. It was proved that if b is odd or $a \equiv b \equiv 2 \pmod 4$, then there does not exist a $D(a+bi)$-quadruple, and if $a+bi$ is not of the above form and $a+bi \notin \{2, -2, 1+2i, -1-2i, 4i, -4i\}$, then there exists at least one $D(a+bi)$-quadruple. We see that in $\mathbf{Z}$ and $\mathbf{Z}[i]$, the elements n for which there exist a $D(n)$-quadruple are exactly (up to at most finitely many exceptions) the elements which are representable as a difference of two squares.

Our goal is to investigate whether this analogy between differences of two squares and existence of Diophantine quadruples is valid in some other situations, e.g., in the rings of integers of (some) quadratic fields. Therefore, the results of this paper can be viewed as the first step in that direction.

2. Differences of two squares in the ring $\mathbf{Z}[\sqrt{d}]$. Let d be an integer which is not a perfect square, and let

$$\mathbf{Z}[\sqrt{d}] = \{x + y\sqrt{d} : \ x, y \in \mathbf{Z}\}.$$

In this section, we will prove Theorem 1, i.e., we will describe a set of all elements of the ring $\mathbf{Z}[\sqrt{d}]$ that can be represented as the difference of squares of two elements of $\mathbf{Z}[\sqrt{d}]$, for integers d which satisfy the conditions from Theorem 1. We start with some results which are valid for all nonsquare integers d.

Proposition 1. *If b is odd, then $z = a + b\sqrt{d}$ is not representable as a difference of two squares in $\mathbf{Z}[\sqrt{d}]$.*

Proof. Assume that z is a difference of two squares in $\mathbf{Z}[\sqrt{d}]$. Then there exist $x_1 + y_1\sqrt{d}$, $x_2 + y_2\sqrt{d} \in \mathbf{Z}[\sqrt{d}]$ such that

$$a + b\sqrt{d} = (x_1 + y_1\sqrt{d})^2 - (x_2 + y_2\sqrt{d})^2.$$

This gives $b = 2(x_1y_1 - x_2y_2)$, a contradiction. □

Proposition 2. *If a is odd and b is even, then $z = a + b\sqrt{d}$ can be represented as a difference of two squares in $\mathbf{Z}[\sqrt{d}]$.*

Proof. Let $z = 2m + 1 + 2n\sqrt{d}$, where $m, n \in \mathbf{Z}$. The statement follows from

$$z = (m + 1 + n\sqrt{d})^2 - (m + n\sqrt{d})^2. \qquad \square$$

Proposition 3. *If $z \in \mathbf{Z}[\sqrt{d}]$ is of the form $4m + 4n\sqrt{d}$, then z can be represented as a difference of two squares in $\mathbf{Z}[\sqrt{d}]$.*

Proof. We have

$$z = 4m + 4n\sqrt{d} = (m + 1 + n\sqrt{d})^2 - (m - 1 + n\sqrt{d})^2. \qquad \square$$

If $z \in \mathbf{Z}[\sqrt{d}]$ has one of the following forms:

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

then we cannot give a simple general answer about representability of z as a difference of two squares. The representability depends on properties of the number d, which is not the case in Propositions 1, 2 and 3.

Suppose that a number z of the form $4m + (4n + 2)\sqrt{d}$ can be represented as a difference of two squares. Then there exist $z_i = x_i + y_i\sqrt{d} \in \mathbf{Z}[\sqrt{d}]$, $i = 1, 2$, such that

$$z = (x_1 + y_1\sqrt{d})^2 - (x_2 + y_2\sqrt{d})^2.$$

It follows that

$$4m = x_1^2 - x_2^2 + (y_1^2 - y_2^2)d, \tag{1}$$

$$2n + 1 = x_1y_1 - x_2y_2. \tag{2}$$

We conclude from (2) that x_1 and y_1 are odd, and at least one of the numbers x_2 and y_2 is even or, conversely, x_2 and y_2 are odd, and at least one of the numbers x_1 and y_1 is even. Further, (1) gives us the following two sets of conditions:

$$\begin{gathered} x_1 \equiv y_1 \equiv 1 \pmod 2, \quad x_2 \equiv y_2 \equiv 0 \pmod 2, \\ d \equiv 3 \pmod 4, \end{gathered} \tag{3}$$

or

$$x_1 \equiv y_1 \equiv 1 \pmod{2}, \quad x_2 \equiv 1 \pmod{2}, \quad y_2 \equiv 0 \pmod{2}, \\ d \equiv 0 \pmod{4} \tag{4}$$

(up to the order of numbers z_1 and z_2).

Unfortunately, the condition $d \equiv 0$ or $3 \pmod{4}$ is not sufficient so that all numbers of the form $4m + (4n+2)\sqrt{d}$ are differences of two squares. The following proposition gives us necessary and sufficient conditions.

Proposition 4. *All numbers of the form $z = 4m + (4n+2)\sqrt{d}$ are representable as a difference of two squares in $\mathbf{Z}[\sqrt{d}]$ if and only if one of the following conditions is satisfied*:

(i) $d \equiv 3 \pmod{4}$ *and the equation $x^2 - dy^2 = \pm 2$ is solvable*,

(ii) $d \equiv 0 \pmod{4}$ *and the equation $x^2 - dy^2 = \pm 4$ has a solution with odd y.*

Proof. Assume that all numbers of the form $4m + (4n+2)\sqrt{d}$ are representable as a difference of two squares. Thus, for all $m, n \in \mathbf{Z}$, there exist $x_1, y_1, x_2, y_2 \in \mathbf{Z}$ satisfying equations (1) and (2). Now, the proof naturally falls into two parts, according to which set of conditions, (3) or (4), is valid.

(i) Assume that conditions (3) are valid. If we make the substitutions $x_1 = x_2 + \alpha$ and $y_1 = y_2 + \beta$ in equations (1) and (2), we obtain

$$\begin{aligned} \alpha x_2 + d\beta y_2 &= 2m - \frac{\alpha^2 + d\beta^2}{2}, \\ \beta x_2 + \alpha y_2 &= 2n + 1 - \alpha\beta, \end{aligned} \tag{5}$$

which we will consider as a linear system in two unknowns x_2 and y_2. Solutions of the system (5) are given by

$$\begin{aligned} x_2 &= \left(\left(2m - \frac{\alpha^2 + d\beta^2}{2} \right) \alpha - (2n + 1 - \alpha\beta) d\beta \right) \Big/ (\alpha^2 - d\beta^2), \\ y_2 &= \left((2n + 1 - \alpha\beta)\alpha - \left(2m - \frac{\alpha^2 + d\beta^2}{2} \right) \beta \right) \Big/ (\alpha^2 - d\beta^2). \end{aligned} \tag{6}$$

According to the assumption that $x_i, y_i \in \mathbf{Z}$ for $i = 1, 2$, this system must have integral solutions for all $m, n \in \mathbf{Z}$. Thus, the determinant of the system, $\alpha^2 - d\beta^2$, divides the numerators in (6). In fact, the following conditions must be satisfied

$$\begin{aligned} &\alpha^2 - d\beta^2 \mid 4m\alpha - 2(2n+1)d\beta, \\ &\alpha^2 - d\beta^2 \mid 4m\beta - 2(2n+1)\alpha. \end{aligned} \tag{7}$$

Specially, for $m, n = 0$ we obtain that there exist integers α_0 and β_0 such that

$$\alpha_0{}^2 - d\beta_0{}^2 \mid 2\alpha_0 \quad \text{and} \quad \alpha_0{}^2 - d\beta_0{}^2 \mid 2d\beta_0.$$

If $g = \gcd(\alpha_0, d\beta_0)$, then

$$\alpha_0{}^2 - d\beta_0{}^2 \mid 2g. \tag{8}$$

On the other hand, $g^2 \mid d\alpha_0{}^2 - d^2\beta_0{}^2$ implies $g^2 \mid 2dg$. Conditions (3) imply that α_0 and β_0 are odd. Hence, g is also odd and thus $g \mid d$. So, there exist two odd integers δ, a such that $d = g\delta$ and $\alpha_0 = ga$. From (8) we get that $ga^2 - \delta\beta_0{}^2 \mid 2$. Since $ga^2 - \delta\beta_0{}^2$ is even, we conclude that

$$ga^2 - \delta\beta_0{}^2 = \pm 2. \tag{9}$$

Multiplying equation (9) by ga^2, we obtain:

$$(ga^2 \mp 1)^2 - d(\beta_0 a)^2 = 1,$$

which means that we have found a solution of the Pell equation $s^2 - dt^2 = 1$ in even s and odd t.

Let now $m, n \in \mathbf{Z}$ be such that

$$(2m)^2 - d(2n+1)^2 = 1. \tag{10}$$

For corresponding α and β, defined as before, relations (7) are satisfied. Specially, the determinant $\alpha^2 - d\beta^2$ must divide the following expression

$$(2\alpha(2n+1) - 4\beta m)\, d(2n+1) + (2d\beta(2n+1) - 4\alpha m)2m.$$

Since equation (10) holds, we get that $\alpha^2 - d\beta^2 \mid 2\alpha$. Similarly, we show that $\alpha^2 - d\beta^2 \mid 2\beta$. Therefore, $\alpha^2 - d\beta^2 \mid 2q$, where $q = \gcd(\alpha, \beta)$. Since $q^2 \mid \alpha^2 - d\beta^2$, it follows that $q^2 \mid 2q$. But q is an odd integer (because α and β are odd), and we conclude that $q = 1$. This immediately implies that $\alpha^2 - d\beta^2 = \pm 2$.

(ii) In this case we assume that conditions (4) are valid. Integers α and β are defined as in the previous case and conditions (4) imply that α is even and β is odd. The relation (7) implies that

$$\begin{aligned} \alpha^2 - d\beta^2 &\mid 2((2m)^2 - d(2n+1)^2)\alpha, \\ \alpha^2 - d\beta^2 &\mid 2((2m)^2 - d(2n+1)^2)\beta. \end{aligned}$$

Note that $(2m)^2 - d(2n+1)^2 \equiv 0 \pmod 4$. Let s be the smallest positive integer s such that

$$(2m_0)^2 - d(2n_0+1)^2 = \pm 4s,$$

for some $m_0, n_0 \in \mathbf{Z}$. It follows immediately that $2m_0$ and $2n_0 + 1$ are relatively prime. Numbers α_0 and β_0, corresponding to m_0 and n_0, satisfy the relations ${\alpha_0}^2 - d{\beta_0}^2 \mid 8s\alpha_0$, ${\alpha_0}^2 - d{\beta_0}^2 \mid 8s\beta_0$. Equation (5) implies that integers α_0 and β_0 are also relatively prime. Hence, we obtain that

$${\alpha_0}^2 - d{\beta_0}^2 \mid 8s.$$

By the minimality of s, it follows that we have only two possibilities:

(a) ${\alpha_0}^2 - d{\beta_0}^2 = \pm 8s$, or

(b) ${\alpha_0}^2 - d{\beta_0}^2 = \pm 4s$.

Now, let us define rational numbers x and y by the formula

$$x + y\sqrt{d} = \frac{2m_0 + (2n_0+1)\sqrt{d}}{\alpha_0 + \beta_0\sqrt{d}}.$$

We have

$$x = \frac{2m_0\alpha_0 - (2n_0+1)d\beta_0}{{\alpha_0}^2 - d{\beta_0}^2}, \quad y = \frac{(2n_0+1)\alpha_0 - 2m_0\beta_0}{{\alpha_0}^2 - d{\beta_0}^2},$$

and

$$x^2 - dy^2 = \frac{(2m_0)^2 - d(2n_0+1)^2}{{\alpha_0}^2 - d{\beta_0}^2}. \tag{11}$$

Since (6) implies that

$$\alpha_0{}^2 - d\beta_0{}^2 \mid x(\alpha_0{}^2 - d\beta_0{}^2) - \frac{\alpha_0{}^2 - d\beta_0{}^2}{2}\,\alpha_0,$$
$$\alpha_0{}^2 - d\beta_0{}^2 \mid y(\alpha_0{}^2 - d\beta_0{}^2) - \frac{\alpha_0{}^2 - d\beta_0{}^2}{2}\,\beta_0,$$

we conclude that $x - (\alpha_0/2)$ and $y - (\beta_0/2)$ are integers. We define $x_1 = 2x$, $y_1 = 2y$. Obviously, x_1 is even and y_1 is odd, since α_0 is even and β_0 is odd. If case (a) is valid, then the right-hand side of equation (11) is equal to $\pm 1/2$. Therefore $x_1{}^2 - dy_1{}^2 = \pm 2$, which contradicts the fact that $x_1{}^2 - dy_1{}^2 \equiv 0 \pmod 4$.

Suppose that case (b) is valid. Since the right-hand side of (11) is equal to ± 1, it follows that $x_1{}^2 - dy_1{}^2 = \pm 4$, and that is what we needed to prove.

Now, we will show the converse. Suppose that α and β are odd integers satisfying $\alpha^2 - d\beta^2 = \pm 2$. We will show that system (5) has integral solutions x_2 and y_2. Indeed, the numerators in (6) are even integers:

$$(12)\quad \left(2m - \frac{\alpha^2 + d\beta^2}{2}\right)\alpha - (2n+1-\alpha\beta)d\beta \equiv 2\alpha - 2d\beta \equiv 0 \pmod 2,$$

$$(13)\quad (2n+1-\alpha\beta)\alpha - \left(2m - \frac{\alpha^2 + d\beta^2}{2}\right)\beta \equiv 2\beta - 2\alpha \equiv 0 \pmod 2.$$

Let $x_1 + y_1\sqrt{d} = x_2 + \alpha + (y_2 + \beta)\sqrt{d}$. Then it follows that $4m + (4n + 2)\sqrt{d} = (x_1 + y_1\sqrt{d})^2 - (x_2 + y_2\sqrt{d})^2$.

Similarly, if the equation $\alpha^2 - d\beta^2 = \pm 4$ is solvable with α even and β odd, then it can be easily verified that the numerators in (6) are divisible by 4. Thus, we obtain again that solutions x_2, y_2 of system (5) are integers, which implies that $4m + (4n + 2)\sqrt{d}$ is representable as a difference of two squares. □

Proposition 5. *All numbers of the form* $z = 4m + 2 + 4n\sqrt{d}$ *can be represented as a difference of two squares if and only if the equation* $x^2 - dy^2 = \pm 2$ *is solvable.*

Proof. Assume that there exist $x_1, y_1, x_2, y_2 \in \mathbf{Z}$ such that

$$4m + 2 + 4n\sqrt{d} = (x_1 + y_1\sqrt{d})^2 - (x_2 + y_2\sqrt{d})^2,$$

i.e.,

$$4m+2=x_1^2-x_2^2+(y_1^2-y_2^2)d, \tag{14}$$
$$2n=x_1y_1-x_2y_2. \tag{15}$$

From these equations we get the following conditions:

$$\begin{gathered} x_1\equiv y_1\equiv 0 \pmod 2, \quad x_2\equiv 0 \pmod 2, \quad y_2\equiv 1 \pmod 2, \\ d\equiv 2 \pmod 4, \end{gathered} \tag{16}$$

or

$$\begin{gathered} x_1\equiv 0 \pmod 2, \quad y_1\equiv 1 \pmod 2, \\ x_2\equiv 1 \pmod 2, \quad y_2\equiv 0 \pmod 2, \quad d\equiv 3 \pmod 4 \end{gathered} \tag{17}$$

(up to the order of numbers $x_1+y_1\sqrt{d}$ and $x_2+y_2\sqrt{d}$).

As in the proof of Proposition 4, let $x_1=x_2+\alpha$, $y_1=y_2+\beta$. Equations (14) and (15) can be written in the following form

$$\begin{aligned} \alpha x_2+d\beta y_2 &= 2m+1-\frac{\alpha^2+d\beta^2}{2}, \\ \beta x_2+\alpha y_2 &= 2n-\alpha\beta. \end{aligned} \tag{18}$$

Solutions x_2, y_2 of system (18) are given by

$$\begin{aligned} x_2 &= \left(\left(2m+1-\frac{\alpha^2+d\beta^2}{2}\right)\alpha-(2n-\alpha\beta)d\beta\right)\Big/(\alpha^2-d\beta^2), \\ y_2 &= \left((2n-\alpha\beta)\alpha-\left(2m+1-\frac{\alpha^2+d\beta^2}{2}\right)\beta\right)\Big/(\alpha^2-d\beta^2). \end{aligned} \tag{19}$$

Since α is even, β is odd and $d\equiv 2 \pmod 4$ (if condition (16) is valid) or α, β are odd and $d\equiv 3 \pmod 4$ (if condition (17) is valid), the determinant of system (18), $\alpha^2-d\beta^2$, is even. It remains to show that there exist integers α and β such that the determinant is equal to 2 or -2. Formulas (19) imply

$$\begin{aligned} &\alpha^2-d\beta^2 \mid 2(2m+1)\alpha-4dn\beta, \\ &\alpha^2-d\beta^2 \mid 4n\alpha-2(2m+1)\beta. \end{aligned}$$

Specially, for $m = n = 0$ we obtain integers α_0 and β_0 such that ${\alpha_0}^2 - d{\beta_0}^2 \mid 2\alpha_0$ and ${\alpha_0}^2 - d{\beta_0}^2 \mid 2\beta_0$. Let $g = \gcd(\alpha_0, \beta_0)$. Then ${\alpha_0}^2 - d{\beta_0}^2 \mid 2g$. On the other hand, we have $g^2 \mid {\alpha_0}^2 - d{\beta_0}^2$. So, it follows that $g^2 \mid 2g$. Since g is odd, we have $g = 1$ and we obtain that ${\alpha_0}^2 - d{\beta_0}^2 = \pm 2$.

The converse of the statement can be shown in the same manner as in the proof of Proposition 4. □

It remains to consider the case $z = 4m+2+(4n+2)\sqrt{d}$. Suppose that this number is representable as a difference of squares of two elements in $\mathbf{Z}[\sqrt{d}]$, i.e.,

$$4m + 2 + (4n + 2)\sqrt{d} = (x_1 + y_1\sqrt{d})^2 - (x_2 + y_2\sqrt{d})^2. \tag{20}$$

Then the numbers x_1, y_1, x_2, y_2 and d satisfy one of the following conditions:

$$\begin{gathered} x_1 \equiv y_1 \equiv 1 \pmod 2, \quad x_2 \equiv y_2 \equiv 0 \pmod 2, \\ d \equiv 1 \pmod 4, \end{gathered} \tag{21}$$

or

$$\begin{gathered} x_1 \equiv y_1 \equiv 1 \pmod 2, \quad x_2 \equiv 1 \pmod 2, \\ y_2 \equiv 0 \pmod 2, \quad d \equiv 2 \pmod 4. \end{gathered} \tag{22}$$

As in the proofs of Propositions 4 and 5, let $\alpha = x_1 - x_2$, $\beta = y_1 - y_2$. In case (21), we obtain

$$\alpha \equiv 1 \pmod 2, \quad \beta \equiv 1 \pmod 2 \quad \text{and} \quad \alpha^2 - d\beta^2 \equiv 0 \pmod 4,$$

and in case (22), we obtain

$$\alpha \equiv 0 \pmod 2, \quad \beta \equiv 1 \pmod 2 \quad \text{and} \quad \alpha^2 - d\beta^2 \equiv 2 \pmod 4.$$

Proposition 6. *All numbers of the form $4m + 2 + (4n + 2)\sqrt{d}$ are representable as a difference of two squares if and only if one of the following conditions is satisfied*:

(i) $d \equiv 1 \pmod 4$ *and the equation* $x^2 - dy^2 = \pm 4$ *is solvable in odd integers* x, y,

(ii) $d \equiv 2 \pmod 4$ *and the equation* $x^2 - dy^2 = \pm 2$ *is solvable.*

Proof. First, we show that the conditions are necessary.

(i) Assume that (21) is satisfied. From (20) we obtain the following system

$$\begin{aligned} \alpha x_2 + d\beta y_2 &= 2m + 1 - \frac{\alpha^2 + d\beta^2}{2}, \\ \beta x_2 + \alpha y_2 &= 2n + 1 - \alpha\beta. \end{aligned} \tag{23}$$

The solutions are

(24)

$$\begin{aligned} x_2 &= \left(\left(2m + 1 - \frac{\alpha^2 + d\beta^2}{2}\right)\alpha - (2n + 1 - \alpha\beta)d\beta\right)\Big/(\alpha^2 - d\beta^2) \\ y_2 &= \left((2n + 1 - \alpha\beta)\alpha - \left(2m + 1 - \frac{\alpha^2 + d\beta^2}{2}\right)\beta\right)\Big/(\alpha^2 - d\beta^2). \end{aligned}$$

Since x_2 and y_2 are integers, we have that

$$\alpha^2 - d\beta^2 \mid 2(2m + 1)\alpha - 2(2n + 1)d\beta, \tag{25}$$

$$\alpha^2 - d\beta^2 \mid 2(2n + 1)\alpha - 2(2m + 1)\beta. \tag{26}$$

Multiplying the right-hand sides of (25) and (26) by $2m + 1$ and $d(2n + 1)$, respectively, and then adding the results, we get

$$\alpha^2 - d\beta^2 \mid 2\alpha((2m + 1)^2 - d(2n + 1)^2). \tag{27}$$

Similarly, we obtain

$$\alpha^2 - d\beta^2 \mid 2\beta((2m + 1)^2 - d(2n + 1)^2). \tag{28}$$

Now, the proof falls into two parts depending on whether $d \equiv 5 \pmod 8$ or $d \equiv 1 \pmod 8$.

(a) Suppose that $d \equiv 5 \pmod 8$. Then $(2m + 1)^2 - d(2n + 1)^2 \equiv 4 \pmod 8$, for all $m, n \in \mathbf{Z}$. Let s be the smallest positive integer with the property that there exist $m, n \in \mathbf{Z}$ such that

$$(2m + 1)^2 - d(2n + 1)^2 = \pm 4s.$$

Obviously, s must be odd. According to the minimality of s, numbers $2m+1$ and $2n+1$ are relatively prime. Thus, from (23), it follows that corresponding α and β are also relatively prime. Relations (27) and (28) imply that

$$\alpha^2 - d\beta^2 \mid 2((2m+1)^2 - d(2n+1)^2),$$

i.e., $\alpha^2 - d\beta^2 \mid 8s$. From the minimality of s, we conclude that

$$\alpha^2 - d\beta^2 = \pm 4s.$$

Let us define rational numbers x and y by

$$x + y\sqrt{d} = \frac{2m+1+(2n+1)\sqrt{d}}{\alpha + \beta\sqrt{d}}, \tag{29}$$

i.e.,

$$x = \frac{(2m+1)\alpha - (2n+1)d\beta}{\alpha^2 - d\beta^2}, \quad y = \frac{(2n+1)\alpha - (2m+1)\beta}{\alpha^2 - d\beta^2}.$$

Then we have

$$x^2 - dy^2 = \frac{(2m+1)^2 - d(2n+1)^2}{\alpha^2 - d\beta^2} = \frac{\pm 4s}{\pm 4s} = \pm 1. \tag{30}$$

Since x_2 and y_2 are integers, from (24) it follows that

$$\alpha^2 - d\beta^2 \mid x(\alpha^2 - d\beta^2) - \frac{\alpha^2 - d\beta^2}{2}\alpha,$$
$$\alpha^2 - d\beta^2 \mid y(\alpha^2 - d\beta^2) - \frac{\alpha^2 - d\beta^2}{2}\beta.$$

Therefore, the numbers $x - (\alpha/2)$ and $y - (\beta/2)$ are also integers. Let $x_1 = 2x$, $y_1 = 2y$. It is obvious that x_1 and y_1 are odd and ${x_1}^2 - d{y_1}^2 = \pm 4$, which proves our assertion.

(b) Assume now that $d \equiv 1 \pmod 8$. Then $(2m+1)^2 - d(2n+1)^2 \equiv 0 \pmod 8$, for all $m, n \in \mathbf{Z}$. Moreover, we can choose $m, n \in \mathbf{Z}$ such that

$$(2m+1)^2 - d(2n+1)^2 \equiv 8 \pmod{16}.$$

Indeed, if $d \equiv 1 \pmod{16}$, then the above relation is satisfied for $m \equiv 1 \pmod{4}$ and $n \equiv 0 \pmod{4}$, and if $d \equiv 9 \pmod{16}$, then it is satisfied for $m \equiv n \equiv 0 \pmod{4}$. Let s be the smallest positive integer such that there exist $m, n \in \mathbf{Z}$ which satisfy the equation

$$(2m+1)^2 - d(2n+1)^2 = \pm 8s.$$

Numbers $2m+1$ and $2n+1$ are relatively prime and so are the corresponding numbers α and β, according to (23). From the minimality of s, as in case (a), we easily obtain that

$$\alpha^2 - d\beta^2 = \pm 8s \quad \text{or} \quad \alpha^2 - d\beta^2 = \pm 16s.$$

Now, let us define rational numbers x and y by formula (29). Analogously as in case (a), we obtain that odd integers $x_1 = 2x$ and $y_1 = 2y$ satisfy one of the following equations:

$${x_1}^2 - d{y_1}^2 = \pm 4 \quad \text{or} \quad {x_1}^2 - d{y_1}^2 = \pm 2.$$

So, we obtain a contradiction with the fact that ${x_1}^2 - d{y_1}^2 \equiv 0 \pmod{8}$. Hence, we have shown that if $d \equiv 1 \pmod{8}$, then there exist numbers of the form $4m+2+(4n+2)\sqrt{d}$ which are not representable as a difference of two squares.

(ii) Assume now that conditions (22) are satisfied.

Let $m, n \in \mathbf{Z}$ be such that

$$(2m+1)^2 - d(2n+1)^2 = p,$$

where p is a prime. Such m and n exist according to a fact, announced by Dirichlet and proved by Meyer and Mertens, which says that among the primes represented by the quadratic form $ax^2 + 2bxy + cy^2$, where $\gcd(a, 2b, c) = 1$, infinitely many of them are representable by any given linear form $Mx + N$, with $\gcd(M, N) = 1$, where a, b, c, M, N are such that the linear and quadratic forms can represent the same number [**3**, Volume I, pp. 417–418]. In our case, we can conclude that, for $d \equiv 2 \pmod{4}$, there are infinitely many primes of the form $x^2 - dy^2$ which also have the form $4k+3$. Obviously, if $p = x^2 - dy^2 \equiv 3 \pmod{4}$ and $d \equiv 2 \pmod{4}$, then x and y are odd.

Further, it is clear that numbers $2m+1$ and $2n+1$ are relatively prime, and so are the corresponding numbers α and β. Relations (27) and (28) imply that $\alpha^2 - d\beta^2 \mid 2p$. Hence, we have two possibilities:

$$\alpha^2 - d\beta^2 = \pm 2 \quad \text{or} \quad \alpha^2 - d\beta^2 = \pm 2p.$$

If the second possibility is fulfilled, then we can define rational numbers x and y by formula (29). Relation (30) implies that

$$x^2 - dy^2 = \pm \frac{p}{2p} = \pm \frac{1}{2}.$$

Similarly, as in case (i), we conclude that numbers $x - (\alpha/2)$ and $y - (\beta/2)$ are integers. It implies that $x_1 = 2x$ is even and $y_1 = 2y$ is odd. Obviously, integers x_1 and y_1 satisfy the desired equation $x_1^2 - dy_1^2 = \pm 2$.

It remains to prove that the conditions are sufficient. In order to do this, we will show that numbers x_2 and y_2 defined in (24) are integral (under the assumption that α and β are solutions of the corresponding Pellian equation). First, let us write the formulas from (24) in the more appropriate form

$$x_2 = \frac{(2m+1)\alpha - (2n+1)d\beta}{\alpha^2 - d\beta^2} - \frac{\alpha}{2}, \tag{31}$$

$$y_2 = \frac{(2n+1)\alpha - (2m+1)\beta}{\alpha^2 - d\beta^2} - \frac{\beta}{2}. \tag{32}$$

Assume that $\alpha^2 - d\beta^2 = \pm 2$, where α is even, β is odd and $d \equiv 2 \pmod 4$. Now, it can be easily checked that x_2 and y_2 are integers.

Assume that α, β are odd integers such that $\alpha^2 - d\beta^2 = \pm 4$. Then we have $d \equiv 5 \pmod 8$. Consider the case that the numbers $2m+1$ and $2n+1$ are congruent to 1 modulo 4. Then the numbers x_2 and y_2 are integers if and only if $(2m+1)\alpha - (2n+1)d\beta \equiv 2 \pmod 4$ and $(2n+1)\alpha - (2m+1)\beta \equiv 2 \pmod 4$. Evidently, those relations are fulfilled if and only if $\alpha \equiv 1 \pmod 4$, $\beta \equiv 3 \pmod 4$, or vice versa, and this can be always achieved (if, e.g., $\alpha \equiv \beta \equiv 1 \pmod 4$ then numbers α and $-\beta$ are also the solutions of the same equation and $-\beta \equiv 3 \pmod 4$).

In the same way, we can deal with the remaining cases: $2m+1 \equiv -(2n+1) \pmod 4$ or $2m+1 \equiv 2n+1 \equiv 3 \pmod 4$. □

Let us discuss the case (i)(b) from the proof of Proposition 6. We will describe numbers of the form $z = 4m+2+(4n+2)\sqrt{d}$ which can be represented as a difference of two squares in the case $d \equiv 1 \pmod 8$. We will restrict our attention to the integers d which satisfy the condition that the equation

$$\alpha^2 - d\beta^2 = \pm 8 \tag{33}$$

is solvable in odd integers α and β. We have to find conditions on $m, n \in \mathbf{Z}$ such that the numbers x_2 and y_2 defined by formulas (31) and (32) are integers. These conditions will depend on the form of solutions of equation (33). Obviously, x_2 and y_2 are integers if the following relations are satisfied

$$(2m+1)\alpha - (2n+1)d\beta \equiv 4 \pmod 8, \tag{34}$$

$$(2n+1)\alpha - (2m+1)\beta \equiv 4 \pmod 8 \tag{35}$$

(under the assumption (33)). Moreover, it is enough that one of these two conditions is fulfilled. Indeed, relation (35) multiplied by α gives relation (34). So, let us assume that condition (35) is satisfied. Since α and β are odd, one of the following congruences is valid: $\alpha \equiv \beta \pmod 8$, $\alpha \equiv \beta+4 \pmod 8$, $\alpha \equiv -\beta \pmod 8$ or $\alpha \equiv -\beta+4 \pmod 8$. We will find conditions on m and n in each of these cases. First, if $\alpha \equiv \beta \pmod 8$, then (35) implies $(2n+1)-(2m+1) \equiv 4 \pmod 8$, i.e., $n-m \equiv 2 \pmod 4$. If $\alpha \equiv \beta+4 \pmod 8$, then (35) implies

$$(2n+1)-(2m+1)+4(2m+1) \equiv 2(m-n)+4 \equiv 4 \pmod 8,$$

i.e., $n-m \equiv 0 \pmod 4$. Similarly, if $\alpha+\beta \equiv 4 \pmod 8$, then $m+n \equiv 3 \pmod 4$, and if $\alpha+\beta \equiv 0 \pmod 8$, then $m+n \equiv 1 \pmod 4$. Further, it can be shown that the form of solutions α, β of equation (33) is completely determined by d. To be more precise: $\alpha \equiv \beta \pmod 8$ or $\alpha+\beta \equiv 0 \pmod 8$ if and only if $d \equiv 9 \pmod{16}$, and $\alpha+\beta \equiv 4 \pmod 8$ or $\alpha-\beta \equiv 4 \pmod 8$ if and only if $d \equiv 1 \pmod{16}$. Those results follow easily if equation (33) is rearranged in the form $(\alpha^2-\beta^2)-(d-1)\beta^2 = \pm 8$.

Therefore, we proved the sufficiency part of the following proposition.

Proposition 7. *Let* $d \equiv 1 \pmod 8$ *and assume the equation* $x^2 - dy^2 = \pm 8$ *is solvable.*

(i) *If* $d \equiv 1 \pmod{16}$*, then the number* $z = 4m+2+(4n+2)\sqrt{d}$ *can be represented as a difference of two squares if and only if* $m - n \equiv 0 \pmod 4$ *or* $m + n \equiv 3 \pmod 4$.

(ii) *If* $d \equiv 9 \pmod{16}$*, then the number* $z = 4m + 2 + (4n + 2)\sqrt{d}$ *can be represented as a difference of two squares if and only* $m - n \equiv 2 \pmod 4$ *or* $m + n \equiv 1 \pmod 4$.

Proof. We have to prove that the conditions are necessary. We will consider only the case $d \equiv 1 \pmod{16}$. The case $d \equiv 9 \pmod{16}$ can be handled in the same way.

Let us assume that $m, n \in \mathbf{Z}$ are such that $m - n \not\equiv 0 \pmod 4$, $m + n \not\equiv 3 \pmod 4$ and $z = 4m + 2 + (4n + 2)\sqrt{d}$ is representable as a difference of two squares. Then we obtain

$$(2m + 1)^2 - d(2n + 1)^2 \equiv 4(m - n)(m + n + 1) \equiv 8 \pmod{16}.$$

Indeed, if $m-n \equiv 1 \pmod 4$ or $m-n \equiv 3 \pmod 4$, than $m+n+1 \equiv 2 \pmod 4$, since $m + n \not\equiv 3 \pmod 4$. On the other hand, if $m - n \equiv 2 \pmod 4$, then $m + n + 1$ is odd.

Now, let s be an odd positive integer such that

$$(2m + 1)^2 - d(2n + 1)^2 = \pm 8s.$$

Corresponding (odd) numbers α and β satisfy relations (27) and (28), i.e., $\alpha^2 - d\beta^2 \mid 16s\alpha$ and $\alpha^2 - d\beta^2 \mid 16s\beta$. If we put $g = \gcd(\alpha, \beta)$, we get $g^2 \mid 16sg$. Hence, $g \mid s$. Let us denote $\alpha = \alpha_1 g$, $\beta = \beta_1 g$, $s = s'g$. Since α_1 and β_1 are relatively prime, we obtain ${\alpha_1}^2 - d{\beta_1}^2 \mid 16s'$. Since ${\alpha_1}^2 - d{\beta_1}^2 \equiv 0 \pmod 8$, there are only two possibilities

$${\alpha_1}^2 - d{\beta_1}^2 = \pm 8s_1 \quad \text{or} \quad {\alpha_1}^2 - d{\beta_1}^2 = \pm 16s_1,$$

where s_1 divides s, i.e., $s = s_1 s_2$. Now, similarly as in the proof of Proposition 6, it can be shown that $x_1 = 2x$ and $y_1 = 2y$, where x and

y are defined by formula (29), satisfy one of the following equations: ${x_1}^2 - d{y_1}^2 = \pm 4s_2$ or ${x_1}^2 - d{y_1}^2 = \pm 2s_2$. Since both equations are impossible (because x_1 and y_1 are odd and ${x_1}^2 - d{y_1}^2 \equiv 0 \pmod 8$), we obtain a contradiction. □

3. Differences of two squares in the ring $\mathbf{Z}[(1+\sqrt{d})/2]$.

In this section we will prove Theorem 2. Therefore, we assume that d is a nonsquare integer such that $d \equiv 1 \pmod 4$. Only in one result in this section (Proposition 11) will we also use the assumption that the equation $x^2 - dy^2 = \pm 4$ is solvable in odd integers. Let

$$\mathbf{Z}\left[\frac{1+\sqrt{d}}{2}\right] = \left\{\frac{x+y\sqrt{d}}{2} : x, y \in \mathbf{Z},\ x \equiv y \pmod 2\right\}.$$

We will describe a set of all elements of the ring $\mathbf{Z}[(1+\sqrt{d})/2]$ that can be represented as a difference of squares of two elements of $\mathbf{Z}[(1+\sqrt{d})/2]$.

In the previous section, we have shown that elements of the ring $\mathbf{Z}[\sqrt{d}]$, where $d \equiv 1 \pmod 4$, which can be represented as a difference of two squares, are elements of the form $2m+1+2n\sqrt{d}$, $4m+4n\sqrt{d}$ or $4m+2+(4n+2)\sqrt{d}$. (The last one under the assumption that the equation $x^2 - dy^2 = \pm 4$ is solvable in odd x and y.) It remains to examine which numbers of the form $a + b\sqrt{d}$ can be represented as a difference of squares of two elements in $\mathbf{Z}[(1+\sqrt{d})/2] \setminus \mathbf{Z}[\sqrt{d}]$. Also, we have to consider a representability of numbers of the form $(a+b\sqrt{d})/2$, where a and b are odd.

Let x_1, y_1, x_2, y_2 be odd integers. Then

$$\left(\frac{x_1}{2} + \frac{y_1}{2}\sqrt{d}\right)^2 - \left(\frac{x_2}{2} + \frac{y_2}{2}\sqrt{d}\right)^2 = a + b\sqrt{d}, \tag{36}$$

where $a, b \in \mathbf{Z}$. Moreover, a is even.

Proposition 8. *All numbers of the form $2m + (2n+1)\sqrt{d}$, $m, n \in \mathbf{Z}$, are representable as a difference of squares of two elements of $\mathbf{Z}[(1+\sqrt{d})/2]$.*

Proof. From the proof of Proposition 3, we have

$$4a + 4b\sqrt{d} = (a+1+b\sqrt{d})^2 - (a-1+b\sqrt{d})^2.$$

Specially, for $a = 2m$ i $b = 2n + 1$, we obtain

$$2m+(2n{+}1)\sqrt{d} = \left(\frac{2m{+}1}{2} + \frac{2n{+}1}{2}\sqrt{d}\right)^2 - \left(\frac{2m{-}1}{2} + \frac{2n{+}1}{2}\sqrt{d}\right)^2 . \ \square$$

By Proposition 6, all numbers of the form $4m + 2 + (4n + 2)\sqrt{d}$ are representable as a difference of squares in $\mathbf{Z}[\sqrt{d}]$ if and only if the equation $x^2 - dy^2 = \pm 4$ is solvable in odd integers. The next proposition shows that in $\mathbf{Z}[(1+\sqrt{d})/2]$, numbers $4m+2+(4n+2)\sqrt{d}$ are always representable as a difference of two squares, i.e., no condition is required on d.

Proposition 9. *All numbers of the form $4m{+}2{+}(4n{+}2)\sqrt{d}$, $m, n \in \mathbf{Z}$, are representable as a difference of two squares in $\mathbf{Z}[(1+\sqrt{d})/2]$.*

Proof. We have

$$8a + 8b\sqrt{d} = (a + 2 + b\sqrt{d})^2 - (a - 2 + b\sqrt{2})^2$$

for all $a, b \in \mathbf{Z}$. Specially, for $a = 2m + 1$ and $b = 2n + 1$ we get

$$\begin{aligned} 4m + 2 + (4n+2)\sqrt{d} = {} & \left(\frac{2m+3}{2} + \frac{2n+1}{2}\sqrt{d}\right)^2 \\ & - \left(\frac{2m-1}{2} + \frac{2n+1}{2}\sqrt{d}\right)^2 . \qquad \square \end{aligned}$$

Proposition 10. *If z is of the form $4m + (4n+2)\sqrt{d}$ or $4m + 2 + 4n\sqrt{d}$, then z cannot be represented as a difference of two squares in $\mathbf{Z}[(1+\sqrt{d})/2]$.*

Proof. Suppose that $a{+}b\sqrt{d} = 4m{+}(4n{+}2)\sqrt{d} = z_1^2{-}z_2^2$. If z_1 and z_2 belong to $\mathbf{Z}[\sqrt{d}]$, then by relations (3) and (4) we have $d \equiv 0 \pmod 4$ or $d \equiv 3 \pmod 4$, a contradiction. Now, suppose that z_i is of the form $(x_i + y_i\sqrt{d})/2$, where x_i and y_i are odd, for $i = 1, 2$, i.e., suppose that equality (36) is valid. Then we obtain that $x_1^2 - x_2^2 + y_1^2 d - y_2^2 d = 16m$.

Thus, $x_1 \equiv \pm x_2 \pmod 8$ and $y_1 \equiv \pm y_2 \pmod 8$, or $x_1 \equiv \pm x_2 + 4 \pmod 8$ and $y_1 \equiv \pm y_2 + 4 \pmod 8$. It follows that $x_1y_1 - x_2y_2 \equiv 0 \pmod 8$ or $x_1y_1 - x_2y_2 \equiv 2 \pmod 4$, which implies that $b \equiv 0 \pmod 4$ or $b \equiv 1 \pmod 2$, a contradiction.

Similarly, relations (16) and (17) imply that if $4m + 2 + 4n\sqrt{d}$ is a difference of two squares in $\mathbf{Z}[\sqrt{d}]$, then $d \equiv 2 \pmod 4$ or $d \equiv 3 \pmod 4$, which is a contradiction. Hence, relation (36) is valid, and it implies that $x_1 \equiv \pm x_2 \pmod 8$ and $y_1 \equiv \pm y_2 + 4 \pmod 8$ (or vice versa: $x_1 \equiv \pm x_2 + 4 \pmod 8$ and $y_1 \equiv \pm y_2 \pmod 8$). Now, we have $x_1y_1 - x_2y_2 \equiv 4 \pmod 8$ or $x_1y_1 - x_2y_2 \equiv 2 \pmod 4$. So, $b \equiv 2 \pmod 4$ or $b \equiv 1 \pmod 2$, and we obtain a contradiction again. □

Proposition 11. *All numbers of the form* $(2m+1)/2+((2n+1)/2)\sqrt{d}$ *can be represented as a difference of two squares in* $\mathbf{Z}[(1+\sqrt{d})/2]$ *if and only if the equation* $x^2 - dy^2 = \pm 4$ *is solvable in odd* x *and* y.

Proof. Assume that the equation $x^2 - dy^2 = \pm 4$ is solvable in odd integers. Then by Proposition 6, all numbers of the form $4m + 2 + (4n + 2)\sqrt{d}$ can be represented as a difference of two squares in $\mathbf{Z}[\sqrt{d}]$. Suppose that $x_1, y_1, x_2, y_2 \in \mathbf{Z}$ satisfy

$$4m + 2 + (4n + 2)\sqrt{d} = (x_1 + y_1\sqrt{d})^2 - (x_2 + y_2\sqrt{d})^2. \tag{37}$$

Then, x_1 and y_1 are odd, and x_2 and y_2 are even, or vice versa. Dividing the equality (37) by 4, we obtain

$$\frac{2m+1}{2} + \frac{2n+1}{2}\sqrt{d} = \left(\frac{2\xi_1+1}{2} + \frac{2\eta_1+1}{2}\sqrt{d}\right)^2 - (\xi_2 + \eta_2\sqrt{d})^2,$$

where $x_1 = 2\xi_1 + 1$, $y_1 = 2\eta_1 + 1$, $x_2 = 2\xi_2$ and $y_2 = 2\eta_2$.

In order to prove the converse statement, suppose that $(2m + 1)/2 + ((2n + 1)/2)\sqrt{d}$ can be represented as a difference of two squares in $\mathbf{Z}[(1 + \sqrt{d})/2]$ for all $m, n \in \mathbf{Z}$, i.e.,

$$\frac{2m+1}{2} + \frac{2n+1}{2}\sqrt{d} = (x_1 + y_1\sqrt{d})^2 - (x_2 + y_2\sqrt{d})^2.$$

Obviously, $4m + 2 + (4n + 2)\sqrt{d} = (2x_1 + 2y_1\sqrt{d})^2 - (2x_2 + 2y_2\sqrt{d})^2$. Thus, $4m+2+(4n+2)\sqrt{d}$ is a difference of two squares in $\mathbf{Z}[\sqrt{d}]$ for all

$m, n \in \mathbf{Z}$. Now, Proposition 6 implies that the equation $x^2 - dy^2 = \pm 4$ is solvable in odd x and y. □

Proposition 12. *Numbers $2m+1+(2n+1)\sqrt{d}$ are not representable as a difference of two squares in $\mathbf{Z}[(1+\sqrt{d})/2]$.*

Proof. By Proposition 1, $a + b\sqrt{d} = 2m + 1 + (2n + 1)\sqrt{d}$ is not representable as a difference of two squares in $\mathbf{Z}[\sqrt{d}]$. If $a + b\sqrt{d}$ satisfies the relation (36), then a must be even. Finally, if $a + b\sqrt{d} = (x_1/2 + (y_1/2)\sqrt{d})^2 - (x_2 + y_2\sqrt{d})^2$, then $a \notin \mathbf{Z}$. Hence, $a + b\sqrt{d}$ is not representable as a difference of two squares in $\mathbf{Z}[(1+\sqrt{d})/2]$. □

4. Certain Pellian equations.

As we saw in the previous two sections, the representability of certain integers in quadratic fields $\mathbf{Q}(\sqrt{d})$ as a difference of two squares is closely connected to the solvability of Pellian equations of the form

$$x^2 - dy^2 = c, \tag{38}$$

where $c = \pm 2, \pm 4, \pm 8$. In this section we give some information on the solvability of these equations. For an interpretation of the connection between these equations and continued fractions, see [**13**].

First, observe that equation (38) is obviously solvable for $d = n^2 - c$, $n \in \mathbf{Z}$. Therefore, all our conditions are satisfied by infinitely many integers d.

The condition that the equation

$$x^2 - dy^2 = \pm 2 \tag{39}$$

is solvable appeared in Propositions 4, 5 and 6, when we considered integers d such that $d \equiv 2$ or $3 \pmod 4$. It is well known, see [**10**] or [**15**, Section 28], that

- if p is a prime and $p \equiv 3 \pmod 8$, then $x^2 - py^2 = -2$ and $x^2 - 2py^2 = -2$ are solvable,
- if p is a prime and $p \equiv 7 \pmod 8$, then $x^2 - py^2 = 2$ and $x^2 - 2py^2 = 2$ are solvable.

We list all positive integers $d \equiv 2 \pmod 4$ up to 200 for which equation (39) is solvable:

$$2^{\pm}, 6^{-}, 14^{+}, 18^{-}, 22^{-}, 34^{+}, 38^{-}, 46^{+}, 54^{-}, 62^{+}, 66^{-}, 86^{-}, 94^{+}, 98^{+},$$
$$102^{-}, 114^{-}, 118^{-}, 134^{-}, 146^{-}, 158^{+}, 162^{-}, 166^{-}, 170^{-}, 178^{-}, 194^{+}, 198^{-}.$$

Here the superscript + indicates that the equation $x^2 - dy^2 = 2$ is solvable, while the superscript $-$ indicates that the equation $x^2 - dy^2 = -2$ is solvable.

Positive integers $d \equiv 3 \pmod 4$ less than 200 for which equation (39) is solvable are:

$$3^{-}, 7^{+}, 11^{-}, 19^{-}, 23^{+}, 27^{-}, 31^{+}, 43^{-}, 51^{-}, 59^{-}, 67^{-},$$
$$71^{+}, 79^{+}, 83^{-}, 103^{+}, 107^{-}, 119^{+}, 123^{-}, 127^{+}, 131^{-},$$
$$143^{+}, 151^{+}, 163^{-}, 167^{+}, 179^{-}, 187^{-}, 191^{+}, 199^{+}.$$

The condition that equation

$$x^2 - dy^2 = \pm 4, \tag{40}$$

is solvable in odd integers appeared in Propositions 6 and 11. The problem of finding an a priori criterion for deciding whether equation (40), where $d \equiv 5 \pmod 8$, is solvable in odd integers is known as Eisenstein's problem. A solvability criterion in the terms of the period-length of continued fraction of $\sqrt{d}$ was given in [**9**]. Some empirical results in [**17**] indicate that (40) is solvable in odd integers for about 2/3 of the values of square-free $d \equiv 5 \pmod 8$. Let us note that it suffices to consider the solvability of the equation $x^2 - dy^2 = 4$, since if u any v are odd integers satisfying $u^2 - dv^2 = -4$, then $x = (u^2 + dv^2)/2$ and $y = uv$ are odd integers satisfying $x^2 - dy^2 = 4$.

Positive integer $d \equiv 5 \pmod 8$ less than 200 for which equation (40) is solvable in odd integers are:

$$5^{\pm}, 13^{\pm}, 21^{+}, 29^{\pm}, 45^{+}, 53^{\pm}, 61^{\pm}, 69^{+}, 77^{+}, 85^{\pm}, 93^{+},$$
$$109^{\pm}, 117^{+}, 125^{\pm}, 133^{+}, 149^{\pm}, 157^{+}, 165^{+}, 173^{\pm}, 181^{\pm}.$$

In Proposition 4 we had the condition that, for $d \equiv 0 \pmod 4$, equation (40) has a solution with odd y. Our condition is equivalent to solvability of the equation $x^2 - (d/4)y^2 = \pm 1$ with odd y. Although a solution of Pell equation

$$x^2 - Dy^2 = 1 \tag{41}$$

always exists, we cannot be sure that there is a solution of such parity. It is easy to see that such a solution exists if and only if in the minimal solution (u, v) of (41) the integer v is odd. This implies that if D is a prime and $D \equiv 3 \pmod 4$, then equation (41) has a solution with odd y. Indeed, if (u, v) is the minimal solution of (41) and v is even, then from $u^2 - 1 = Dv^2$ we obtain $u \pm 1 = 2Dt^2$, $u \mp 1 = 2s^2$ and $s^2 - Dt^2 = \mp 1$. But, the minimality of (u, v) implies that $+$ sign is not possible, while the assumption $D \equiv 3 \pmod 4$ implies that the $-$ sign is not possible. We conclude that for $d = 4p$, where p is a prime such that $p \equiv 3 \pmod 4$, equation (40) has a solution with odd y.

On the other hand, if the equation $x^2 - (d/4)y^2 = -1$ is solvable, then y is necessarily odd. Thus, we are interested in solvability conditions for the equation

$$x^2 - Dy^2 = -1. \tag{42}$$

It is well known, see [**10**], that equation (42) is solvable if

- $D = p$, where p is a prime and $p \equiv 1 \pmod 4$,
- $D = 2p$, where p is a prime and $p \equiv 5 \pmod 8$,
- $D = pq$, where p, q are primes, $p, q \equiv 1 \pmod 4$ and $(p/q) = -1$,
- $D = 2pq$, where p, q are primes and $p, q \equiv 5 \pmod 8$.

Positive integers $d \equiv 0 \pmod 4$, $4 < d < 200$, for which equation (40) is solvable with odd y are:

$$8^-, 12^+, 20^-, 28^+, 32^+, 40^-, 44^+, 52^-, 60^+, 68^-, 76^+, 92^+, 96^+, 104^-,$$
$$108^+, 116^-, 124^+, 128^+, 140^+, 148^-, 160^+, 164^-, 172^+, 188^+, 192^+.$$

Finally, very little is known about the solvability of equation

$$x^2 - dy^2 = \pm 8 \tag{43}$$

for $d \equiv 1 \pmod 8$, which appeared in our Proposition 7. Since, equation (39) is not solvable for such d, it follows that x and y have to be odd. In [**11**], in studying a classical correspondence between algebraic K3 surfaces, the conditions that $d \equiv 1 \pmod 8$ and (43) is solvable also appeared. The authors gave the list of all positive integers $d \leq 2009$ which satisfy these conditions. We list here only such nonsquare integers less than 200:

$$17^{\pm}, 33^{-}, 41^{\pm}, 57^{-}, 73^{\pm}, 89^{\pm}, 97^{\pm},$$
$$113^{\pm}, 129^{-}, 137^{\pm}, 153^{-}, 161^{+}, 177^{-}, 193^{\pm}.$$

Here we may notice that there exist integers d for which both equations $x^2 - dy^2 = 8$ and $x^2 - dy^2 = -8$ are solvable.

REFERENCES

1. A. Baker and H. Davenport, *The equations* $3x^2 - 2 = y^2$ *and* $8x^2 - 7 = z^2$, Quart. J. Math. Oxford **20** (1969), 129–137.

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

3. L.E. Dickson, *History of the theory of numbers*, Chelsea, New York, 1966.

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

5. ———, *The problem of Diophantus and Davenport for Gaussian integers*, Glas. Mat. Ser. III **32** (1997), 1–10.

6. ———, *There are only finitely many Diophantine quintuples*, J. Reine Angew. Math. **566** (2004), 183–214.

7. A. Dujella and C. Fuchs, *Complete solution of a problem of Diophantus and Euler*, J. London Math. Soc. **71** (2005), 33–52.

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

9. P. Kaplan and K.S. Williams, *Pell's equations* $x^2 - my^2 = -1, -4$ *and continued fractions*, J. Number Theory **23** (1986), 169–182.

10. F. Lemmermeyer, *Higher descent on Pell conics* I. *From Legendre to Selmer*, preprint, available at: `math.NT/0311309`.

11. C. Madonna and V.V. Nikulin, *On a classical corespodence between K3 surfaces*, Tr. Mat. Inst. Steklova **241** (2003), Teor. Chisel, Algebra i Algebr. Geom., 132–168 (in Russian); Proc. Steklov Inst. Math. **241** (2003), 120–153 (in English).

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

13. R.A. Mollin, *A continued fraction approach to the Diophantine equation* $ax^2 - by^2 = \pm 1$, J. Algebra Number Theory Appl. **4** (2004), 159–207.

14. I. Niven, *Integers of quadratic fields as sums of squares*, Trans. Amer. Math. Soc. **48** (1940), 405–417.

15. O. Perron, *Die Lehre von den Kettenbruchen*, Teubner, Stuttgart, 1954.

16. W. Sierpiński, *Elementary theory of numbers*, PWN, Warszawa; North Holland, Amsterdam, 1987.

17. A.J. Stephens and H.C. Williams, *Some computational results on a problem of Eisenstein*, in *Théorie des nombres* (Quebec, PQ, 1987), de Gruyter, Berlin, 1989, pp. 869–886.

Department of Mathematics, University of Zagreb, Bijenička cesta 30, 10000 Zagreb, Croatia
E-mail address: duje@math.hr

Department of Mathematics, University of Zagreb, Bijenička cesta 30, 10000 Zagreb, Croatia
E-mail address: fran@math.hr