PELLIAN EQUATIONS OF A SPECIAL TYPE

MIRELA JUKIĆ BOKUN* AND IVAN SOLDO**

ABSTRACT. In this paper, we consider the solubility of the Pellian equation

$$x^2 - (d^2+1)y^2 = -m,$$

in cases $d = n^k, m = n^{2l-1}$, k, l are positive integers, n is a composite positive integer and $d = pq$, $m = pq^2$, p, q are primes.

We use obtained results to prove results on extensibility of some $D(-1)$-pairs to quadruples in the ring $\mathbb{Z}[\sqrt{-t}]$, with $t > 0$.

1. Introduction

Suppose that k, l, n are positive integers. In [7], for $n = p$, where p is an odd prime, it was considered the solubility of equation

$$x^2 - (n^{2k}+1)y^2 = -n^{2l-1} \tag{1.1}$$

in positive integers. There is shown that for $0 < l \leq k$ equation (1.1) is not solvable in positive integers x and y. In Section 2, we investigate the solubility in integers of equation (1.1) with composite n. In Theorem 2.1, we give generalized result concerning equation of this type with right-hand side equals to $-m$ with some positive integer m. That result will generate results about solubility of our initial equation (1.1) (see Corollary 2.1.1 and its consequences). Moreover, we observe equation

$$x^2 - (p^2q^2+1)y^2 = -pq^2, \tag{1.2}$$

where p, q are primes. In Theorem 2.3, we completely solve the problem of its solubility in integers.

A Diophantine m-tuple with the property $D(-1)$ or just a $D(-1)$-m-tuple in a commutative ring R is a set of m non-zero elements of R such that $ab - 1$ is a square in R for any two distinct elements a, b in R. Extendibility of $D(-1)$-m-tuples is a topic which is actively researched (for example, see [1, 2, 3, 6, 11, 10, 14, 15, 16]). In Section 3, we consider the existence of some $D(-1)$-quadruples in rings of integers of the imaginary quadratic fields. To prove our main result (see Theorem 3.1) we apply the results of Section 2.

2. Pellian equations

At the beginning of this section, we will discuss solubility of the Pellian equation which is closely related to equation (1.1).

Theorem 2.1. *Let d and m be positive integers and (x^*, y^*) a fundamental solution of equation*

$$x^2 - (d^2+1)y^2 = -m. \tag{2.1}$$

Then

$$0 < y^* < \frac{m+1}{2d}, \qquad |x^*| < \frac{m+1}{2},$$

2010 *Mathematics Subject Classification.* 11D09, 11R11, 11J86.

Key words and phrases. Pellian equation, Diophantine m-tuple, quadratic field.

The second author was supported by the Croatian Science Foundation under the project no. IP-2018-01-1313.

and, in the case of m is a square,

$$y^* = \sqrt{m}, \qquad |x^*| = d\sqrt{m}.$$

Proof. One can conclude that

$$\begin{aligned} x_0 &= 2d^2+1, \\ y_0 &= 2d, \end{aligned}$$

is the fundamental solution of the Pell equation

$$x^2 - (d^2+1)y^2 = 1.$$

Thus, by following the Nagell's approach (see [12]) for the fundamental solution (x^*, y^*) of equation (2.1) we obtain

$$0 < y^* \leq \sqrt{m}.$$

It implies

$$|x^*| \leq dy^*.$$

Suppose that $y^* < \sqrt{m}$. Then $|x^*| < dy^*$.

On the other hand,

$$x^{*2} = (dy^*)^2 + y^{*2} - m > (dy^*)^2 - m = (dy^* - 1)^2 + 2dy^* - m - 1.$$

For $y^* \geq \frac{m+1}{2d}$, we obtain

$$|x^*| > dy^* - 1.$$

Therefore, we have

$$dy^* - 1 < |x^*| < dy^*,$$

which is not possible. This implies

$$0 < y^* < \frac{m+1}{2d}, \qquad |x^*| < \frac{m+1}{2}$$

and, in the case of m is a square,

$$|x^*| = d\sqrt{m}, \qquad y^* = \sqrt{m}.$$

□

As a direct consequence of Theorem 2.1 we get the next result:

Corollary 2.1.1. *Let d and m be positive integers. If $d \geq m$, then equation* (2.1) *has a solution in integers x and y only in the case of m is a square.*

Proof. Theorem 2.1 imples that $0 < y* < 1$ or $y^* = \sqrt{m}$, and m has to be a square. □

By Corollary 2.1.1, we are able to conclude that for $k \geq 2l - 1$ equation (1.1) has an integer solution only in the case of n is a square and its fundamental solution is given by

$$\begin{aligned} y^* &= n^{l-1}\sqrt{n}, \\ |x^*| &= n^{k+l-1}\sqrt{n}. \end{aligned} \tag{2.2}$$

This yields that equation (1.1) is solvable for a composite n. Like we will emphasize in the next remark, this is not the only case where the solution of equation (1.1) exists.

Remark 1.

(i) If n is a square, then (2.2) is the solution of equation (1.1) for an arbitrary positive integers k, l.

(ii) Let $0 \leq k < 2l-1$. If k is even, then

$$\begin{aligned} x &= \frac{1}{2}\sqrt{2n^{2l-k-1}}(n^k-1), \\ y &= \frac{1}{2}\sqrt{2n^{2l-k-1}}, \end{aligned}$$

is the solution of equation (1.1) in the case of n is a twice square.

(iii) Also, the solution of equation (1.1) exists in some other cases. For example, suppose that $k < l$ and $n = 2p$ with an odd prime p. If u is a positive integer and p is of the form $4u+1$, then there exists the solution for $(n,k,l) = (34,2,16)$, which yields the existence of the solution for all $l > 16$. Similarly, for p of the form $4u+3$, the solution exists for $(n,k,l) = (6,2,3)$ and consequently for all $l > 3$.

Remark 2. Our conjecture is that in the case of $k < l$ and $n = p$, where p is an odd prime, equation (1.1) is not solvable in integers x and y.

We will also emphasise next consequence of Theorem 2.1.

Corollary 2.1.2. *The fundamental solution of equation*

$$x^2 - (d^2+1)y^2 = -2d$$

is given by

$$|x^*| = d-1, \qquad y^* = 1.$$

Proof. If $m = 2d$, then from Theorem 2.1 we get $0 < y^* < 2$. It is easy to see that $y^* = 1$ implies $|x^*| = d-1$. □

Further, we will consider equation (1.2). To prove our result we will use the following results on Diophantine approximations of a real number and convergents of continued fraction expansion of irrational number.

Theorem 2.2 ([17, 4, Theorem 1])**.** *Let α be a real number and let a and b be coprime nonzero integers, satisfying the inequality*

$$\left|\alpha - \frac{a}{b}\right| < \frac{k}{b^2},$$

where k is a positive real number. Then $(a,b) = (rp_{m+1} \pm up_m, rq_{m+1} \pm uq_m)$, for some $m \geq -1$ and nonnegative integers r and u such that $ru < 2k$. Term p_m/q_m denote convergent of continued fraction expansion of α.

If $\alpha = \frac{s_0+\sqrt{d}}{t_0}$ is a quadratic irrational, then the simple continued fraction expansion of α is periodic and that expansion can be obtained by using the following algorithm (see [13, Chapter 7.7]):

$$a_n = \left\lfloor \frac{s_n+\sqrt{d}}{t_n} \right\rfloor, \quad s_{n+1} = a_n t_n - s_n, \quad t_{n+1} = \frac{d - s_{n+1}^2}{t_n}, \quad \text{for } n \geq 0. \tag{2.3}$$

If $(s_j, t_j) = (s_k, t_k)$ for $j < k$, then

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

Also, useful will be the following lemma:

Lemma 2.1 ([5, Lemma 2]). *Let $\alpha\beta$ be a positive integer which is not a perfect square, and let p_n/q_n denotes the n-th convergent of continued fraction expansion of $\sqrt{\frac{\alpha}{\beta}}$. Let the sequences (s_n) and (t_n) be defined by (2.3) for the quadratic irrational $\frac{\sqrt{\alpha\beta}}{\beta}$. Then*

$$\alpha(rq_{n+1}+uq_n)^2-\beta(rp_{n+1}+up_n)^2=(-1)^n(u^2t_{n+1}+2rus_{n+2}-r^2t_{n+2}),$$

for any real numbers r, u.

Theorem 2.3. *Let p, q be primes. The equation (1.2) has no integer solutions except in cases $p=q=2$ and p is odd, $q=2$.*

Proof. By Corollary 2.1.2, for $d=4$ and $d=2p$, we conclude the solubility of equation (1.2) in cases $p=q=2$ and p is odd, $q=2$, respectively.

In what follows, we will use the similar approach as in [7].

It is easy to see that $x, y \neq 0$. Thus we will consider the solubility of (1.2) in positive integers. The possibility $(x, y)>1$ implies that $(x, y)=q$ and then equation (1.2) generate equation of the form

$$x^2-(p^2q^2+1)y^2=-p$$

which, according to Corollary 2.1.1, has no solution. So we conclude that $(x, y)=1$.

$$\left|\sqrt{p^2q^2+1}-\frac{x}{y}\right|=\frac{pq^2}{y^2}\left|\sqrt{p^2q^2+1}+\frac{x}{y}\right|^{-1}. \tag{2.4}$$

The idea is to bound last term of the right-hand side in (2.4) and then apply Theorem 2.2. We will determine y such that inequality

$$\sqrt{p^2q^2+1}+\frac{x}{y}>2pq \tag{2.5}$$

holds. This inequality in combination with (1.2) implies

$$p^2q^2+1-\frac{pq^2}{y^2}>(2pq-\sqrt{p^2q^2+1})^2,$$

i.e.,

$$\frac{q}{y^2}<4(\sqrt{p^2q^2+1}-pq). \tag{2.6}$$

For $x \geq 1$ inequality $\sqrt{x^2+1}-x>\frac{1}{4x}$ holds and it implies

$$\frac{1}{pq}<4(\sqrt{p^2q^2+1}-pq).$$

Therefore, for

$$\frac{q}{y^2}<\frac{1}{pq},$$

i.e., $y>q\sqrt{p}$ inequality (2.6), but also inequality (2.5) holds. Combining that with (2.4) we obtain

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

According to Theorem 2.2 we have

$$(x, y)=(rp_{m+1}\pm up_m, rq_{m+1}\pm uq_m), \tag{2.7}$$

for some $m \geq -1$ and nonnegative integers r and u such that

$$ru<q. \tag{2.8}$$

Terms p_m/q_m are convergents of the continued fraction expansion of $\sqrt{p^2q^2+1}$. Since $\sqrt{p^2q^2+1} = [pq, \overline{2pq}]$, by Lemma 2.1, we have

$$(p^2q^2+1)(rq_{n+1} \pm uq_n)^2 - (rp_{n+1} \pm up_n)^2 = \pm(u^2t_1 \pm 2rus_2 - r^2t_2). \tag{2.9}$$

Since

$$s_2 = s_3 = pq, \quad t_1 = t_2 = t_3 = 1.$$

from (1.2), (2.7) and (2.9) we get equations of the form

$$u^2 - r^2 \pm 2rupq = pq^2, \tag{2.10}$$

and have to consider their solubility.

It is easy to see that cases $r = 0$ or $u = 0$ or $u = r$ are not possible. Suppose that $0 \neq r \neq u \neq 0$. We will base our observation on the inequality $ur \geq u + r - 1$ and inequality (2.8), i.e., $ur < q$.

From (2.10) it follows that $pq | u^2 - r^2$.

If pq divide $u - r$ or $u + r$ then $u + r \geq pq$ implies $ur > q$ which is not possible. Suppose that pq does not divide $u - r$ or $u + r$. Then $p | u - r, q | u + r$ or $p | u + r, q | u - r$. In each case it follows that $u + r \geq q$ and we get

$$q > ur \geq u + r - 1 \geq q - 1.$$

So, the only possibility is $ur = q - 1, u + r = q$. This imply that $u_1 = q - 1, r_1 = 1$ or $u_2 = 1, r_2 = q - 1$. These cases in combination with (2.10) implies that $q = 2$ and $p = \pm 1$ for "+" sign and $q = \frac{2+2p}{1+3p}$ or $q = \frac{2p-2}{3p-1}$ for "-" sign. Niether of these cases are not possible.

We conclude that all positive solutions of equation (1.2) must satsify $y < q\sqrt{p}$. Since the set of positive solutions of soluble Pellian equation is unbounded this is a contradiction. In that way we complete the proof of the theorem.

□

Let us mention that in combination with Theorem 2.1 and it's corollary, the above result will be the crucial one to finish the proof of the main result of the next section.

3. $D(-1)$-quadruples in the ring $\mathbb{Z}[\sqrt{-t}]$, with $t > 0$

In this section, we present the results on extensibility of certain Diophantine pairs to quadruples in the ring $\mathbb{Z}[\sqrt{-t}], t > 0$.

By [16, Theorem 2.2] and its proof it follows:

Lemma 3.1. *If $t > 0$, b is a prime or twice prime or twice prime square and $\{1, b, c\}$ is a $D(-1)$-triple in the ring $\mathbb{Z}[\sqrt{-t}]$, then $c \in \mathbb{Z}$. Moreover, for every t there exists $c > 0$, while the case of $c < 0$ is possible if and only if $t | b - 1$ and equation*

$$x^2 - by^2 = \frac{1-b}{t}$$

has an integer solution.

We consider the extendibility of a $D(-1)$-pair $\{1, b\}$, where b is a prime, twice prime and twice prime squared in the ring $\mathbb{Z}[\sqrt{-t}]$ with $t > 0$. Since $b - 1$ has to be a square, we will observe the case of $b - 1 = P^2Q^2$, with different primes P and Q.

To prove our results we recall the following lemmas:

Lemma 3.2 ([7, Proposition 2])**.** *Let $m, n > 0$ and $b = n^2 + 1$. If $m | n$ and $t \in \{1, m^2, n^2\}$, then there exist infinitely many $D(-1)$-quadruples of the form $\{1, b, -c, d\}$, $c, d > 0$ in $\mathbb{Z}[\sqrt{-t}]$.*

Lemma 3.3 ([8, Corollary 1.3])**.** *Let r be a positive integer and let $b = r^2 + 1$. Assume that one of the following holds for any odd prime p and a positive integer k:*

$$b = p, \quad b = 2p^k, \quad r = p^k, \quad r = 2p^k.$$

Then the system of Diophantine equations

$$\begin{aligned} y^2 - bx^2 &= r^2, \\ z^2 - cx^2 &= s^2 \end{aligned}$$

has only the trivial solutions $(x, y, z) = (0, \pm r, \pm s)$, where s is such that (t, s) is a positive solution of $t^2 - bs^2 = r^2$ and $c = s^2 + 1$. Furthermore, the $D(-1)$-pair $\{1, b\}$ cannot be extended to a $D(-1)$-quadruple.

First, suppose that b is a prime. It is obvious that $b \neq 2$. If $P = Q = 2$, than $b = 17$. In [15], we have already considered the extensions of the $D(-1)$-pair $\{1, 17\}$ in the ring $\mathbb{Z}[\sqrt{-t}]$ with $t > 0$. Thus, b is an odd prime of the form $b = P^2Q^2 + 1$, with $Q = 2$ and some odd prime P.

Next, we will observe the case of $b = 2p$ or $b = 2p^2$, with prime p, where $b = P^2Q^2 + 1$ and P, Q are different odd primes.
We are able to prove the next theorem:

Theorem 3.1. *Set*

$$\begin{aligned} S_1 &= \left\{ b = P^2Q^2 + 1 : Q = 2 \text{ and } b, P \text{ are odd primes} \right\}, \\ S_2 &= \left\{ b = P^2Q^2 + 1 : P, Q \text{ are different odd primes and } b = 2p \text{ or } b = 2p^2 \right. \\ &\qquad \left. \text{with prime } p \right\}. \end{aligned}$$

(a) *Let $b \in S_1 \cup S_2$.*
 (i) *If $t \in \{1, P^2, Q^2, P^2Q^2\}$, then there exist infinitely many $D(-1)$-quadruples of the form $\{1, b, -c, d\}$, $c, d > 0$ in $\mathbb{Z}[\sqrt{-t}]$.*
 (ii) *If $t \nmid P^2Q^2$, then there does not exists a $D(-1)$-quadruple of the form $\{1, b, c, d\}$ in $\mathbb{Z}[\sqrt{-t}], t > 0$.*

(b) *If $b \in S_1$ and $t \in \{2, 2P, 4P, 2P^2\}$, then there does not exists a $D(-1)$-quadruple of the form $\{1, b, c, d\}$ in $\mathbb{Z}[\sqrt{-t}]$.*
(c) *Let $b \in S_2$. If $t \in \{P, Q, PQ, PQ^2, P^2Q\}$, then there does not exists a $D(-1)$-quadruple of the form $\{1, b, c, d\}$ in $\mathbb{Z}[\sqrt{-t}]$.*

Proof. (a):
(i) It follows from Lemma 3.2.
(ii) Let $t \nmid P^2Q^2$. If there exists a $D(-1)$-quadruple of the form $\{1, b, c, d\}$ in $\mathbb{Z}[\sqrt{-t}]$, then from Lemma 3.1 we have $c, d > 0$. This leads to the contradiction with Lemma 3.3. Thus we obtain that at least one of the product of any two distinct elements from $\{1, b, c, d\}$ decreased by 1 is a square in $\mathbb{Z}[\sqrt{-t}] \setminus \mathbb{Z}$. This contradicts with $c, d \in \mathbb{N}$.
(b): Let $b \in S_1$ and $t \in \{2, 2P, 4P, 2P^2\}$. From Lemma 3.1 we have to consider the solubility of equations

$$x^2 - (4P^2 + 1)y^2 = -2P^2, \tag{3.1}$$
$$x^2 - (4P^2 + 1)y^2 = -2P, \tag{3.2}$$
$$x^2 - (4P^2 + 1)y^2 = -P, \tag{3.3}$$
$$x^2 - (4P^2 + 1)y^2 = -2. \tag{3.4}$$

Equations (3.1) and (3.4) have no solutions modulo 4. By Corollary 2.1.1, equations (3.2), (3.3) are solvable only if their right-hand side ($2P$, P, respectively) is a square, which is not possible. This implies that $c, d > 0$ and the proof follows in the same way as in the part (ii).

(c): Let $b \in S_2$ and $t \in \{P, Q, PQ, PQ^2, P^2Q\}$. Since $\mathbb{Z}[P\sqrt{-Q}]$ is a subring of $\mathbb{Z}[\sqrt{-Q}]$, and by the symmetry of P and Q, from Lemma 3.1 we obtain equations

$$x^2 - (P^2Q^2 + 1)y^2 = -PQ, \tag{3.5}$$

$$x^2 - (P^2Q^2 + 1)y^2 = -PQ^2. \tag{3.6}$$

By Theorem 2.3 equation (3.6) is not solvable. By Corollary 2.1.1, equation (3.5) is solvable only in the case of PQ is a square. That is not possible. Now, the proof follows in the same way as previous cases. □

Remark 3. One can note that in the case of $b \in S_1$ there also appear the possibility $t = P$. This leads us to observe equation

$$x^2 - (4P^2 + 1)y^2 = -4P. \tag{3.7}$$

According to Corollary 2.1.2, the only fundamental solutions of (3.7) are $(\pm(2P - 1), 1)$. So, all solutions of (3.7) are given by

$$x + y\sqrt{4P^2 + 1} = (\pm(2P - 1) + \sqrt{4P^2 + 1})(8P^2 + 1 + 4P\sqrt{4P^2 + 1})^n,$$

where n is a non-negative integer. Now, if we consider the existence of the $D(-1)$-quadruple $\{1, 4P^2 + 1, c, d\}$ in the ring $\mathbb{Z}[\sqrt{-P}]$, then according to Lemma 3.1 it follows that $c = 1 - Py^2$ and $d \in \mathbb{Z}$ (i.e., d can be positive or negative integer). Thus in both cases we have to solve the systems of simultaneous pellian equations depending on P and corresponding solution y. In [9], we solved the case of $y = 1$, i.e., proved that the $D(-1)$-triple $\{1, 4P^2 + 1, 1 - P\}$ cannot be extended to a $D(-1)$-quadruple in the ring $\mathbb{Z}[\sqrt{-P}]$. The general case may be considered in some future work.

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. Bayad, A. Dossavi-Yovo, A. Filipin, A. Togbe, *On the extensibility of* $D(4)$*-triple* $\{k-2, k+2, 4k\}$ *over Gaussian integers*, Notes Number Theory Discrete Math. **23** (2017), 1–26.

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

[4] A. Dujella, *Continued fractions and RSA with small secret exponents*, Tatra Mt. Math. Publ. **29** (2004), 101–112.

[5] A. Dujella, B. Jadrijević, *A family of quartic Thue inequalities*, Acta Arith. **111** (2004), 61–76.

[6] A. Dujella, I. Soldo, *Diophantine quadruples in* $\mathbb{Z}[\sqrt{-2}]$, An. Ştiinţ. Univ. "Ovidius" Constanţa Ser. Mat. **18** (2010), 81–98.

[7] A. Dujella, M. Jukić Bokun, I. Soldo, *A Pellian equation with primes and applications to D(-1)-quadruples* Bull. Malays. Math. Sci. Soc. **42** (2019), 2915–2926.

[8] A. Filipin, Y. Fujita, M. Mignotte, *The non-extendibility of some parametric families of* $D(-1)$*-triples*, Quart. J. Math. **63** (2012), 605–621.

[9] A. Filipin, M. Jukić Bokun, I. Soldo, *On* $D(-1)$*-triples* $\{1, 4p^2 + 1, 1 - p\}$ *in the ring* $\mathbb{Z}[\sqrt{-p}]$ *with a prime* p, preprint.

[10] Z. Franušić, D. Kreso, *Nonextensibility of the pair* $\{1, 3\}$ *to a Diophantine quintuple in* $\mathbb{Z}[\sqrt{-2}]$, J. Comb. Number Theory **3** (2011), 1–15.

[11] M. Jukić Bokun, I. Soldo, *On the extensibility of D(-1)-pairs containing Fermat primes*, Acta Math. Hungar. **159** (2019), 89–108.

[12] T. Nagell, *Introduction to Number Theory*, Wiley, New York, 1951.

[13] I. Niven, H. S. Zuckerman, H. L. Montgomery, *An Introduction to the Theory of Numbers*, John Wiley & Sons, New York, 1991.

[14] I. Soldo, *On the existence of Diophantine quadruples in* $\mathbb{Z}[\sqrt{-2}]$, Miskolc Math. Notes **14** (2013), 261–273.

[15] I. Soldo, *On the extensibility of $D(-1)$-triples $\{1, b, c\}$ in the ring $\mathbb{Z}[\sqrt{-t}], t > 0$*, Studia Sci. Math. Hungar. **50** (2013), 296–330.
[16] I. Soldo, *$D(-1)$-triples of the form $\{1, b, c\}$ in the ring $\mathbb{Z}[\sqrt{-t}], t > 0$*, Bull. Malays. Math. Sci. Soc. **39** (2016), 1201–1224.
[17] R. T. Worley, *Estimating $|\alpha - p/q|$*, J. Austral. Math. Soc. Ser. A **31** (1981), 202–206.

* Department of Mathematics
University of Osijek
Trg Ljudevita Gaja 6
HR-31000 Osijek
CROATIA
Email address: mirela@mathos.hr

** Department of Mathematics
University of Osijek
Trg Ljudevita Gaja 6
HR-31000 Osijek
CROATIA
Email address: isoldo@mathos.hr