A Pellian equation with primes and applications to $D(-1)$-quadruples

Andrej Dujella[1], Mirela Jukić Bokun[2] and Ivan Soldo[2,*]

[1]Department of Mathematics, Faculty of Science, University of Zagreb, Bijenička cesta 30, 10 000 Zagreb, Croatia
e-mail: duje@math.hr

[2]Department of Mathematics, University of Osijek, Trg Ljudevita Gaja 6, 31 000 Osijek, Croatia
e-mail: mirela@mathos.hr, isoldo@mathos.hr

Abstract

In this paper, we prove that the equation $x^2-(p^{2k+2}+1)y^2=-p^{2l+1}$, $l\in\{0,1,\ldots,k\}, k\geq 0$, where p is an odd prime number, is not solvable in positive integers x and y. By combining that result with other known results on the existence of Diophantine quadruples, we are able to prove results on the extensibility of some $D(-1)$-pairs to quadruples in the ring $\mathbb{Z}[\sqrt{-t}], t>0$.

Keywords: Diophantine equation, quadratic field, Diophantine triple
Mathematics Subject Classification (2010): 11D09, 11R11

1 Introduction

Diophantus of Alexandria raised the problem of finding four positive rational numbers a_1, a_2, a_3, a_4 such that a_ia_j+1 is a square of a rational number for each i, j with $1\leq i<j\leq 4$ and gave a solution $\{\frac{1}{16}, \frac{33}{16}, \frac{17}{4}, \frac{105}{16}\}$. The first example of such a set in the ring of integers was found by Fermat and it was the set $\{1, 3, 8, 120\}$. Replacing "+1" by "$+n$" suggests the following general definition:

*Corresponding author

Authors were supported by the Croatian Science Foundation under the project no. 6422. A. D. acknowledges support from the QuantiXLie Center of Excellence, a project cofinanced by the Croatian Government and European Union through the European Regional Development Fund - the Competitiveness and Cohesion Operational Programme (Grant KK.01.1.1.01.0004).

Definition 1 *Let n be a non-zero element of a commutative ring R. A Diophantine m-tuple with the property $D(n)$, or simply a $D(n)$-m-tuple, is a set of m non-zero elements of R such that if a, b are any two distinct elements from this set, then $ab + n = k^2$, for some element k in R.*

Let p be an odd prime and k a non-negative integer. We consider the Pellian equation

$$x^2 - (p^{2k+2} + 1)y^2 = -p^{2l+1}, \quad l \in \{0, 1, \ldots, k\}. \tag{1}$$

The existence of positive solutions of the above equation is closely related to the existence of a Diophantine quadruple in a certain ring. More precisely, the entries in a Diophantine quadruple are severely restricted in that they appear as coefficients of three generalized Pell equations that must have at least one common solution in positive integers.

According to Definition 1, we will look at the case $n = -1$. Research on $D(-1)$-quadruples is quite active. It is conjectured that $D(-1)$-quadruples do not exist in integers (see [6]). Dujella, Filipin and Fuchs in [10] proved that there are at most finitely many $D(-1)$-quadruples, by giving an upper bound of 10^{903} for their number. There is a vast literature on improving that bound (e.g., see [14, 2, 13, 30]). At present, the best known bound for the number of $D(-1)$-quadruples is $3.677 \cdot 10^{58}$ due to Lapkova [23] (see also [21, 22]).

Concerning the imaginary quadratic fields, Dujella [5] and Franušić [17] considered the problem of existence of $D(-1)$-quadruples in Gaussian integers. Moreover, in [18] Franušić and Kreso showed that the Diophantine pair $\{1, 3\}$ cannot be extended to a Diophantine quintuple in the ring $\mathbb{Z}[\sqrt{-2}]$. Several authors contributed to the characterization of elements z in $\mathbb{Z}[\sqrt{-2}]$ for which a Diophantine quadruple with the property $D(z)$ exists (see [1, 12, 27]). The problem of Diophantus for integers of the quadratic field $\mathbb{Q}(\sqrt{-3})$ was studied in [19]. In [28, 29], Soldo studied the existence of $D(-1)$-quadruples of the form $\{1, b, c, d\}, b \in \{2, 5, 10, 17, 26, 37, 50\}$, in the ring $\mathbb{Z}[\sqrt{-t}], t > 0$.

The aim of the present paper is to obtain results about solvability of the equation (1) in positive integers. We use obtained results to prove statements on the extensibility of some $D(-1)$-pairs to quadruples in the ring $\mathbb{Z}[\sqrt{-t}], t > 0$.

2 Pellian equations

The goal of this section is to determine all solutions in positive integers of the equation (1), which is the crucial step in proving our results in the next section. For this purpose, we need the following result on Diophantine approximations.

Theorem 1 ([31, Theorem 1], [8, Theorem 1]) *Let α be a real number and let a and b be coprime non-zero integers, satisfying the inequality*

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

where c is a positive real number. Then $(a, b) = (rp_{m+1} \pm up_m, rq_{m+1} \pm uq_m)$, for some integer $m \geq -1$ and non-negative integers r and u such that $ru < 2c$. Here p_m/q_m denotes the m-th convergent of the continued fraction expansion of α.

If $\alpha = \frac{s+\sqrt{d}}{t}$ is a quadratic irrational, then the simple continued fraction expansion of α is periodic. This expansion can be obtained by using the following algorithm. Let $s_0 = s, t_0 = t$ and

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

(see [25, Chapter 7.7]). If $(s_j, t_j) = (s_k, t_k)$ for $j < k$, then

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

We will combine Theorem 1 with the following lemma:

Lemma 1 ([11, Lemma 1]) *Let α, β be positive integers such that $\alpha\beta$ is not a perfect square, and let p_n/q_n denote the n-th convergent of the continued fraction expansion of $\sqrt{\frac{\alpha}{\beta}}$. Let the sequences (s_n) and (t_n) be defined by (2) for the quadratic irrational $\frac{\sqrt{\alpha\beta}}{\beta}$. Then*

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

for any real numbers r, u.

The next lemma will be useful.

Lemma 2 ([16, Lemma 2.3.]) *Let N and K be integers with $1 < |N| \leq K$. Then the Pellian equation*

$$X^2 - (K^2 + 1)Y^2 = N$$

has no primitive solution.

The solution (X_0, Y_0) is called primitive if $\gcd(X_0, Y_0) = 1$. Now we formulate the main result of this section.

Theorem 2 *Let p be an odd prime and let k be a non-negative integer. The equation*

$$x^2 - (p^{2k+2} + 1)y^2 = -p^{2l+1}, \quad l \in \{0, 1, \ldots, k\} \tag{3}$$

has no solutions in positive integers x and y.

In proving Theorem 2, we will apply the following technical lemma.

Lemma 3 *If (x, y) is a positive solution of the equation*

$$x^2 - (p^{2k+2} + 1)y^2 = -p^{2k+1}, \tag{4}$$

and $y \geq p^{\frac{2k+1}{2}}$, then the inequality

$$\sqrt{p^{2k+2} + 1} + \frac{x}{y} > 2p^{k+1}$$

holds.

Proof: From (4) we have

$$\frac{x^2}{y^2} = p^{2k+2} - \frac{p^{2k+1}}{y^2} + 1. \tag{5}$$

Thus we have to consider when the inequality

$$p^{2k+2} - \frac{p^{2k+1}}{y^2} + 1 > \left(2p^{k+1} - \sqrt{p^{2k+2} + 1}\right)^2$$

is satisfied. This inequality is equivalent to

$$\frac{p^k}{y^2} < 4\left(\sqrt{p^{2k+2} + 1} - p^{k+1}\right). \tag{6}$$

For $x > 1$, the inequality $(1 + \frac{1}{x})^{\frac{1}{2}} > 1 + \frac{1}{2x} - \frac{1}{8x^2}$ holds. Thus we have

$$\begin{aligned} & 4\left(\sqrt{p^{2k+2} + 1} - p^{k+1}\right) \\ & \quad = 4p^{k+1}\left(\left(1 + \frac{1}{p^{2k+2}}\right)^{\frac{1}{2}} - 1\right) \\ & \quad > 4p^{k+1}\left(\frac{1}{2p^{2k+2}} - \frac{1}{8p^{4k+4}}\right) \\ & \quad > 4p^{k+1} \cdot \frac{1}{4p^{2k+2}} \\ & \quad = \frac{1}{p^{k+1}}. \end{aligned}$$

Since $y \geq p^{\frac{2k+1}{2}}$, i.e.

$$\frac{1}{p^{k+1}} \geq \frac{p^k}{y^2},$$

we conclude that the inequality (6) holds. $\square$

Proof of Theorem 2:
Case 1. Let $2l + 1 \leq k + 1$, i.e., $l \leq \frac{k}{2}$.

By Lemma 2, we know that the equation (3) has no primitive solutions. Assume that there exists a non-primitive solution (x, y). Then $p|x$ and $p|y$, so there exist $0 < i \leq l, x_1, y_1 \geq 0, \gcd(x_1, y_1) = 1$ such that $x = p^i x_1, y = p^i y_1$. After dividing equation (3) by p^{2i}, we obtain

$$x_1^2 - (p^{2k+2} + 1)y_1^2 = -p^{2l-2i+1}, \quad 0 < 2l - 2i + 1 \leq k + 1.$$

But such x_1, y_1 do not exist according to Lemma 2, so we obtained a contradiction.
Case 2. Let $2l + 1 = 2k + 1$, i.e., $l = k$.

Let us suppose that there exists a solution (x, y) of the equation (1) such that $y \geq p^{\frac{2k+1}{2}}$. Then by applying (5) we obtain

$$\begin{aligned} |\sqrt{p^{2k+2}+1} - \frac{x}{y}| &= |p^{2k+2} - \frac{x^2}{y^2} + 1| \cdot |\sqrt{p^{2k+2}+1} + \frac{x}{y}|^{-1} \\ &= \frac{p^{2k+1}}{y^2} \cdot |\sqrt{p^{2k+2}+1} + \frac{x}{y}|^{-1}. \end{aligned}$$

Lemma 3 implies

$$|\sqrt{p^{2k+2}+1} - \frac{x}{y}| < \frac{p^k}{2y^2}. \tag{7}$$

Assume that $x = p^t x_1, y = p^t y_1$, where t, x_1, y_1 are non-negative integers and $\gcd(x_1, y_1) = 1$. Now the equation (1) is equivalent to

$$x_1^2 - (p^{2k+2} + 1)y_1^2 = -p^{2k-2t+1}. \tag{8}$$

Since $y \geq y_1$, from (7) we obtain

$$|\sqrt{p^{2k+2}+1} - \frac{x_1}{y_1}| < \frac{p^k}{2y_1^2}.$$

Now, Theorem 1 implies that

$$(x_1, y_1) = (rp_{m+1} \pm up_m, rq_{m+1} \pm uq_m), \tag{9}$$

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

$$ru < p^k. \tag{10}$$

Since x_1 and y_1 are coprime, we have $\gcd(r, u) = 1$.

The terms p_m/q_m are convergents of the continued fraction expansion of $\sqrt{p^{2k+2}+1}$. Since

$$\sqrt{p^{2k+2}+1} = [p^{k+1}, \overline{2p^{k+1}}]$$

implies that the period of that continued fraction expansion (and also of the corresponding sequences (s_n) and (t_n)) is equal to 1. Therefore, we apply Lemma 1 for $m = 0$. We obtain

$$(p^{2k+2} + 1)(rq_1 \pm uq_0)^2 - (rp_1 \pm up_0)^2 = u^2 t_1 \pm 2rus_2 - r^2 t_2, \tag{11}$$

where

$$s_2 = p^{k+1}, \quad t_1 = t_2 = 1, \quad p_0 = p^{k+1}, p_1 = 2p^{2k+2} + 1, \quad q_0 = 1, q_1 = 2p^{k+1}.$$

Since the observation is similar in both signs, we shall focus on the positive sign. By comparing (8) and (11), we obtain the equation

$$u^2 - r^2 + 2rup^{k+1} = p^{2k-2t+1}. \tag{12}$$

Now, we consider the solvability of (12).

If $r = 0$, then $u^2 = p^{2k-2t+1}$, and so p has to be a square, which is not possible.

If $u = 0$, we obtain $-r^2 = p^{2k-2t+1}$, and that is not possible, either.

If $r = u$, we have $p^{k-2t} = 2r^2$. Since p is an odd prime, that is not possible.

Let $0 \neq r \neq u \neq 0$. If $t < \frac{k}{2}$, then from (12) we conclude that $p^{k+1} | u^2 - r^2$. If $p | u + r$ and $p | u - r$, then $p | 2 \gcd(r, u)$, i.e., $p | 2$ which is not possible. Therefore, p^{k+1} divides exactly one of the numbers $u + r$ and $u - r$. In both cases, it follows that $u + r \geq p^{k+1}$. That implies

$$ur \geq u + r - 1 > p^k,$$

which contradicts (10).

Now, let us suppose that $t \geq \frac{k}{2}$. Since the equation (1) is equivalent to (8) and $0 < 2k - 2t + 1 \leq k + 1$, by Case 1 it has no solutions.

It remains to consider the case $y < p^{\frac{2k+1}{2}}$. Assume that there exists a solution of the equation (1) with this property. In that case we can generate an increasing sequence of infinitely many solutions of the equation (1). Therefore, a solution (x, y) such that $y \geq p^{\frac{2k+1}{2}}$ will appear. This contradicts with the first part of the proof of this case.

Case 3. Let $k + 1 < 2l + 1 < 2k + 1$, i.e., $\frac{k}{2} < l < k$.

In this case, if we suppose that the equation (3) has a solution, then multiplying (3) by p^{2k-2l} we obtain the solution of the equation

$$x^2 - (p^{2k+2} + 1)y^2 = -p^{2k+1},$$

which is not solvable by Case 2. That is the contradiction, and this completes the proof of Theorem 2. $\square$

Proposition 1 *Let $p = 2$.*

i) If $k \equiv 0 \pmod 2$, then the equation (3) has no solutions.

ii) If $k \equiv 1 \pmod 2$, then in case of $l > \frac{k}{2}$ the equation (3) has a solution, and in case of $l \leq \frac{k}{2}$ it has no solutions.

Proof: i) If $k \equiv 0 \pmod 2$, then the equation (3) is not solvable modulo 5.

ii) Let $k \equiv 1 \pmod 2$. If $l > \frac{k}{2}$, the equation (3) has the solution of the form

$$(x, y) = (2^{\frac{2l-k-1}{2}}(2^{k+1} - 1), 2^{\frac{2l-k-1}{2}}),$$

and therefore infinitely many solutions.

If $l \leq \frac{k}{2}$, then $2l + 1 \leq k + 1$ and we can proceed as in Case 1 of Theorem 2 and conclude that the equation (3) has no solutions. $\square$

3 Application to $D(-1)$-triples

By using results from the previous section and known results on Diophantine m-tuples, in this section we present the results on extensibility of certain Diophantine pairs to quadruples, in the ring $\mathbb{Z}[\sqrt{-t}], t > 0$.

The following result is proved in [29]:

Theorem 3 ([29, Theorem 2.2]) *Let $t > 0$ and let $\{1, b, c\}$ be a $D(-1)$-triple in the ring $\mathbb{Z}[\sqrt{-t}]$.*

(i) If b is a prime, then $c \in \mathbb{Z}$.

(ii) If $b = 2b_1$, where b_1 is a prime, then $c \in \mathbb{Z}$.

(iii) If $b = 2b_2^2$, where b_2 is a prime, then $c \in \mathbb{Z}$.

Remark 1 *In the proof of [29, Theorem 2.2] it was shown that for every t there exists such $c > 0$, while the case $c < 0$ is possible only if $t|b-1$ and the equation*

$$x^2 - by^2 = \frac{1-b}{t} \tag{13}$$

has an integer solution.

Let p be an odd prime and $b = 2p^k, k \in \mathbb{N}$. We consider the extensibility of $D(-1)$-triples of the form $\{1, b, c\}$ to quadruples in the ring $\mathbb{Z}[\sqrt{-t}], t > 0$. The complexity of the problem depends on the number of divisors t of $b-1$. As b grows, we can expect the larger set of t's, and for each t we have to consider whether there exists a solution of the equation (13). If it is true, then the problem is reduced to solving the systems of simultaneous Pellian equations. A variety of different methods have been used to study such problems, including linear forms in logarithms, elliptic curves, theory around Pell's equation, elementary methods, separating the problem into several subproblems depending on the size of parameters, etc. A survey on that subject is given in [9].

Therefore, since $b - 1 = 2p^k - 1$ has to be a square, to reduce the number of t's, we consider the equation of the form

$$2p^k - 1 = q^{2j}, \quad j > 0, \tag{14}$$

where q is an odd prime. According to [20, Lemma 2.9] (see also [4, 3]), if $k > 1$ the equation (14) has solutions only for $(k, j) \in \{(2, 1), (4, 1)\}$. If $(k, j) = (2, 1)$, we obtain the Pellian equation in primes. So far known prime solutions are $(p, q) \in \{(5, 7), (29, 41), (44560482149, 63018038201),$
$(1355877461004671178 0701, 1917500294268803292 8599)\}$ (see [26]). If $(k, j) = (4, 1)$, the only solution is $(p, q) = (13, 239)$.

Let $k = 1$. Suppose that $j = mn$, where n is an odd number. Then we have

$$2p = q^{2j} + 1 = q^{2mn} + 1 = (q^{2m} + 1)((q^{2m})^{n-1} - (q^{2m})^{n-2} + \cdots - q^{2m} + 1).$$

Since p is an odd prime, we conclude that $q^{2m}+1=2p=q^{2mn}+1$. This implies that $n=1$. This means that the only possibility for $2p=q^{2j}+1$ is that j is a non-negative power of 2.

Note that in all possible cases of k, i.e., $k=1,2,4$, the equation (14) can be written in the form $2p^k=q^{2^l}+1, l>0$.

By following the same steps as in the proof of Theorem 3(ii), (iii), we can prove more general result:

Theorem 4 *Let k,t be positive integers and let $\{1,b,c\}$ be a $D(-1)$-triple in the ring $\mathbb{Z}[\sqrt{-t}]$. If $b=2p^k$, where p is an odd prime, then $c\in\mathbb{Z}$.*

Remark 2 *Remark 1 is also valid in the case of Theorem 4.*

In proving results of this section we will use the following result of Filipin, Fujita and Mignotte from [15] on $D(-1)$-quadruples in integers.

Lemma 4 ([15, 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

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

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 we prove the following result.

Theorem 5 *If p is an odd prime and k,t positive integers with $t\equiv 0 \pmod 2$, then there does not exist a $D(-1)$-quadruple in $\mathbb{Z}[\sqrt{-t}]$ of the form $\{1,2p^k,c,d\}$.*

Proof: Let $t\equiv 0 \pmod 2$. We have that $t\nmid 2p^k-1$. Therefore, if we suppose that $\{1,2p^k,c,d\}$ is a $D(-1)$-quadruple in $\mathbb{Z}[\sqrt{-t}]$, then according to Remarks 1 and 2 we obtain $c,d\in\mathbb{N}$. This means that there exist integers x_1,y_1,u_1,v_1,w_1, such that

$$c-1=x_1^2, d-1=y_1^2, 2p^kc-1=u_1^2, 2p^kd-1=v_1^2, cd-1=w_1^2,$$

or at least one of $c-1, d-1, 2p^kc-1, 2p^kd-1, cd-1$ is equal to $-tw_2^2$, for an integer w_2.

The first possibility contradicts with Lemma 4, i.e., a $D(-1)$-pair $\{1,2p^k\}$ cannot be extended to a $D(-1)$-quadruple in integers, while the second one contradicts to $c,d\in\mathbb{N}$.

$\square$

In what follows, our main goal is to obtain some results for odd t's. Thus, let us consider the case of $t\equiv 1 \pmod 2$. We have the following result:

Theorem 6 *Let $k \in \{1,2,4\}$ and let $2p^k = q^{2^l} + 1, l > 0$, where p and q are odd primes.*

(i) If $t \in \{1, q^2, \dots, q^{2^l-2}, q^{2^l}\}$, then there exist infinitely many $D(-1)$-quadruples of the form $\{1, 2p^k, -c, d\}$, $c, d > 0$ in $\mathbb{Z}[\sqrt{-t}]$.

(ii) If $t \in \{q, q^3, \dots, q^{2^l-3}, q^{2^l-1}\}$, then there does not exist a $D(-1)$-quadruple of the form $\{1, 2p^k, c, d\}$ in $\mathbb{Z}[\sqrt{-t}]$.

Before we prove Theorem 6, we recall the following result.

Lemma 5 ([7, Lemma 3]) *If $\{a,b,c\}$ is a Diophantine triple with the property $D(l)$ and $ab+l = r^2$, $ac+l = s^2$, $bc+l = t^2$, then there exist integers e, x, y, z such that*

$$ae + l^2 = x^2, be + l^2 = y^2, ce + l^2 = z^2$$

and

$$c = a + b + \frac{e}{l} + \frac{2}{l^2}(abe + rxy).$$

Moreover, $e = l(a+b+c) + 2abc - 2rst$, $x = at - rs$, $y = bs - rt$, $z = cr - st$.

To prove the next proposition, which will be used in proving Theorem 6, we will use Lemma 5 for $l = -1$.

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

Proof: Since $\mathbb{Z}[ni]$ is a subring of $\mathbb{Z}[mi]$, it suffices to prove the statement for $t = n^2$. Thus, suppose that there exist $x, y \in \mathbb{Z}$ such that

$$\begin{aligned} -c - 1 &= -n^2x^2 = (nxi)^2, \\ -bc - 1 &= -n^2y^2 = (nyi)^2. \end{aligned}$$

Eliminating c, we obtain the Pellian equation

$$y^2 - (n^2+1)x^2 = -1. \tag{15}$$

All positive solutions of the equation (15) are given by

$$\begin{aligned} x = x_j &= \frac{\sqrt{n^2+1}}{2(n^2+1)}\left((n+\sqrt{n^2+1})^{2j-1} - (n-\sqrt{n^2+1})^{2j-1}\right), \\ y = y_j &= \frac{1}{2}\left((n+\sqrt{n^2+1})^{2j-1} + (n-\sqrt{n^2+1})^{2j-1}\right), \quad j \in \mathbb{N}. \end{aligned}$$

Therefore, for any $j \in \mathbb{N}$ and $c = c_j = n^2x_j^2 - 1$, the set $\{1, b, -c\}$ is a $D(-1)$-triple in $\mathbb{Z}[\sqrt{-t}]$. If we apply Lemma 5 on that triple, we obtain positive integers

$$d_\pm = \pm 2n^3x_jy_j + (2n^2+1)c + n^2 + 2,$$

such that

$$\begin{aligned} d_\pm - 1 &= \left(n^2x_j \pm ny_j\right)^2, \\ bd_\pm - 1 &= \left(n(n^2+1)x_j \pm n^2y_j\right)^2, \\ -cd_\pm - 1 &= \left(nci \pm n^2x_jy_ji\right)^2. \end{aligned}$$

Thus the sets $\{1, b, -c, d_+\}, \{1, b, -c, d_-\}$ are $D(-1)$-quadruples in $\mathbb{Z}[\sqrt{-t}]$, except for the case $j = 1$, where $d_- = 1$.

$\square$

Now, we are able to prove Theorem 6.

Proof of Theorem 6:
Let $l \geq 0$.

(i) Suppose that $t \in \{1, q^2, \dots, q^{2^l-2}, q^{2^l}\}$. By Proposition 2 there exist infinitely many $D(-1)$-quadruples of the form $\{1, 2p^k, -c, d\}$, $c, d > 0$ in $\mathbb{Z}[\sqrt{-t}]$.

(ii) Let us assume that $t \in \{q, q^3, \dots, q^{2^l-3}, q^{2^l-1}\}$. In this case, the equation (13) is equivalent to

$$x^2 - (q^{2^l} + 1)y^2 = -q^s, \tag{16}$$

where s is an odd integer and $0 < s \leq 2^l - 1$. Theorem 2 implies that the equation (16) has no integer solutions. Therefore, if $\{1, 2p^k, c, d\}$ is $D(-1)$-quadruple in $\mathbb{Z}[\sqrt{-t}]$, then $c, d > 0$. By the same arguments as in Theorem 5 we conclude that such a quadruple does not exist.

$\square$

Acknowledgement

Authors are deeply grateful to the anonymous referees for their helpful comments, insights and suggestions that lead to an improved version of the paper.

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] N. C. Bonciocat, M. Cipu, M. Mignotte, *On* $D(-1)$*-quadruples*, Publ. Mat. **56** (2012), 279-304.

[3] Y. Bugeaud, M. Mignotte, *On integers with identical digits*, Mathematika **46** (1999), 411–417.

[4] P. Crescenzo, *A diophantine equation which arises in the theory of finite groups*, Adv. Math. **17** (1975), 25–29.

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

[6] A. Dujella, *On the exceptional set in the problem of Diophantus and Davenport*, Applications of Fibonacci Numbers **7** (1998), 69–76.

[7] A. Dujella, *On the size of Diophantine m-tuples*, Math. Proc. Cambridge Philos. Soc. **132** (2002), 23–33.

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

[9] A. Dujella, *What is ... a Diophantine m-tuple?*, Notices Amer. Math. Soc. **63** (2016), 772–774.

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

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

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

[13] C. Elsholtz, A. Filipin, Y. Fujita, *On Diophantine quintuples and $D(-1)$-quadruples*, Monatsh. Math. **175** (2014), 227–239.

[14] A. Filipin, Y. Fujita, *The number of $D(-1)$-quadruples*, Math. Commun. **15** (2010), 381–391.

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

[16] Y. Fujita, *The non-extensibility of $D(4k)$-triples* $\{1, 4k(k-1), 4k^2+1\}$, with $|k|$ prime, Glas. Mat. Ser. III **41** (2006), 205–216.

[17] Z. Franušić, *On the extensibility of Diophantine triples $\{k-1, k+1, 4k\}$ for Gaussian integers*, Glas. Mat. Ser. III **43** (2008), 265–291.

[18] 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.

[19] Z. Franušić, I. Soldo, *The problem of Diophantus for integers of* $\mathbb{Q}(\sqrt{-3})$, Rad Hrvat. Akad. Znan. Umjet. Mat. Znan. **18** (2014), 15–25.

[20] A. Khosravi, B. Khosravi, *A new characterization of some alternating and symmetric groups (II)*, Houston J. Math. **30** (2004), 953–967.

[21] K. Lapkova, *Explicit upper bound for an average number of divisors of quadratic polynomials*, Arch. Math. (Basel) **106** (2016), 247–256.

[22] K. Lapkova, *Explicit upper bound for the average number of divisors of irreducible quadratic polynomials*, Monatsh. Math. (2017), doi:10.1007/s00605-017-1061-y.

[23] K. Lapkova, *Explicit upper bound for the average number of divisors of irreducible quadratic polynomials*, arXiv:1704.02498v3 [math. NT].

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

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

[26] N. J. A. Sloane, *The on-line encyclopedia of integer sequences*, availabe at `https://oeis.org/A118612`.

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

[28] 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.

[29] 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.

[30] T. Trudgian, *Bounds on the number of Diophantine quintuples*, J. Number Theory **157** (2015), 233–249.

[31] R. T. Worley, *Estimating* $|\alpha - p/q|$, J. Austral. Math. Soc. Ser. A **31** (1981), 202–206.