On the extensibility of $D(-1)$-pairs containing Fermat primes

M. Jukić Bokun[1] and I. Soldo[2]

[1] Mirela Jukić Bokun, Department of Mathematics, University of Osijek, Trg Ljudevita Gaja 6, 31000 Osijek, Croatia
e-mail: mirela@mathos.hr

[2] Ivan Soldo, Department of Mathematics, University of Osijek, Trg Ljudevita Gaja 6, 31000 Osijek, Croatia
e-mail: isoldo@mathos.hr

Abstract

In this paper, we study the extendibility of a $D(-1)$-pair $\{1, p\}$, where p is a Fermat prime, to a $D(-1)$-quadruple in $\mathbb{Z}[\sqrt{-t}], t > 0$.

Keywords: Diophantine quadruples, quadratic field, simultaneous Pellian equations, linear form in logarithms
Mathematics Subject Classification (2010): 11D09, 11R11, 11J86

1 Introduction

Let R be a commutative ring. A set of m distinct elements in R such that the product of any two distinct elements increased by $z \in R$ is a perfect square is called a $D(z)$-m-tuple in R. The most studied case is the ring of integers $\mathbb{Z}$ (for details see [6]). Recently, results on the extendibility of Diophantine m-tuples in rings of integers of the imaginary quadratic fields have been obtained. For example, such kind of problems in the ring of Gaussian integers were studied by Dujella [5], Franušić [10], Bayad et al. [3, 4]. To see different types of results for $z = -1$ in the ring of integers

Authors were supported by the Croatian Science Foundation under the project no. 6422.

$\mathbb{Z}[\sqrt{-t}]$, for certain $t > 0$, one can refer to [1, 9, 11, 19, 20, 21]. More recently, for odd prime p and positive integer i Dujella and authors in [7] obtained results about extendibility of a $D(-1)$-pair $\{1, 2p^i\}$ to a quadruple in $\mathbb{Z}[\sqrt{-t}], t > 0$. In this paper, we study the extendibility of another type of a $D(-1)$-pair in such rings.

If the set $\{1, N\}, N \in \mathbb{N}$ is a $D(-1)$-pair in $\mathbb{Z}[\sqrt{-t}], t > 0$, we can easily conclude that it should be a $D(-1)$-pair in $\mathbb{N}$. If we suppose that $N = p^k$, where p is a prime and $k \in \mathbb{N}$, it can be shown that $k = 1$ (for example, see [13]). In [20], it was shown that there does not exist a $D(-1)$-quadruple of the form $\{1, 2, c, d\}$ in $\mathbb{Z}[\sqrt{-t}], t > 1$. In Gaussian integers there exist infinitely many such quadruples (see [5]). Therefore, we will suppose that p is an odd prime. By [21, Theorem 2.2] and its proof it follows:

Lemma 1 *If $t > 0$, p prime and $\{1, p, c\}$ 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 only if $t | p - 1$ and the equation*

$$x^2 - py^2 = \frac{1-p}{t} \tag{1}$$

has an integer solution.

We can easily identify all divisors t of $p-1$ if we suppose that $p-1 = q^{2j}$, where q is a prime and $j \in \mathbb{N}$. This leads us to the form $p = 2^{2^n} + 1, n \in \mathbb{N}$. Therefore, we will consider Fermat primes greater than 3 as members of $D(-1)$-quadruple in the ring $\mathbb{Z}[\sqrt{-t}], t > 0$ (since 2 is not a square in $\mathbb{Z}[\sqrt{-t}]$ for any $t > 0$, we omitted the case $p = 3$). So far, the only known such primes are $p = 5, 17, 257, 65537$ ([17]) corresponding to $n = 1, 2, 3, 4$, respectively. The cases of $p = 5, 17$ are already solved in [20]. Whenever it was possible we proved some of our results on extendibility of a $D(-1)$-pair $\{1, p\}$ to a $D(-1)$-quadruple in $\mathbb{Z}[\sqrt{-t}], t > 0$ for arbitrary Fermat prime p.

2 Results

From [7, Proposition 2] immediately follows the next result:

Proposition 1 *Let $n \geq 1$ and let p be the n-th Fermat prime. There exist infinitely many $D(-1)$-quadruples of the form $\{1, p, -c, d\}$, $c, d > 0$ in $\mathbb{Z}[\sqrt{-t}], t \in \{1, 2^2, \ldots, 2^{2^n-2}, 2^{2^n}\}$.*

In proving of our results we will use the following lemma:

Lemma 2 *If a $D(-1)$-pair $\{1, a\}, a \in \mathbb{N}$ cannot be extended to $D(-1)$-quadruple in integers, then there does not exist $D(-1)$-quadruple of the form $\{1, a, b, c\}, b, c \in \mathbb{N}$ in the ring $\mathbb{Z}[\sqrt{-t}], t > 0$.*

Proof: If we suppose that a $D(-1)$-quadruple of the form $\{1, a, b, c\}$, $a, b, c \in \mathbb{N}$ does not exist in integers and it exists in $\mathbb{Z}[\sqrt{-t}], t > 0$, the only possibility is that at least one of terms $a-1, b-1, c-1, ab-1, ac-1, bc-1$ is equal to $-tu^2$, for some integer u. We obtain the contradiction with $a, b, c > 0$.

□

Suppose that there exists a $D(-1)$-quadruple of the form $\{1, p, c, d\}$, in $\mathbb{Z}[\sqrt{-t}], t > 0$.

For $t \nmid 2^{2^n}$, from Lemma 1 it follows that $c, d > 0$. Now, from Lemma 2 we conclude that such quadruple exists in integers which contradicts with [12, Corollarry 1.3].

Keeping in mind the statement of Proposition 1, it remains to consider the cases of $t \in \{2, 2^3, \ldots, 2^{2^n-3}, 2^{2^n-1}\}$. They all satisfy the condition $t \mid 2^{2^n}$, so by Lemma 1 we have to consider weather the equation (1) has an integer solution. We obtain equations

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

From [7, Proposition 1] it follows that (2) is not solvable for $l \leq \frac{2^{n-1}-1}{2}$, and the solution exists in the case of $l > \frac{2^{n-1}-1}{2}$.

If $n \geq 2$, then the equation (2) is not solvable for $l < \frac{2^{n-1}-1}{2}$, i.e. $l \in \{0, 1, \ldots, 2^{n-2} - 1\}$. We conclude that for $t \in \{2^{2^{n-1}+1}, 2^{2^{n-1}+3}, \ldots, 2^{2^n-1}\}$ we have $c, d > 0$ which is againt the contradiction with [12, Corollarry 1.3].

If $n = 1$ the only possibility is $l = 0$ and the equation (2) has no solutions. Therefore, in the same way as above we obtain the contradiction in the case of $t = 2$.

At this moment we can state the following result:

Proposition 2 *Let $n \geq 1$ and let p be the n-th Fermat prime. There does not exist $D(-1)$-quadruple of the form $\{1, p, c, d\}$ in $\mathbb{Z}[\sqrt{-t}], t > 0$ in the following cases:*

a) $t \nmid 2^{2^n}$;

b) $n = 1$ *and* $t = 2$;

c) $n \geq 2$ *and* $t \in \{2^{2^{n-1}+1}, 2^{2^{n-1}+3}, \ldots, 2^{2^n-1}\}$.

Observe that until now we expressed all results for the case of $n = 1$.

For $n \geq 2$ and $l \in \{2^{n-2}, \ldots, 2^{n-1} - 1\}$, i.e., $t \in \{2, 2^3, \ldots, 2^{2^{n-1}-1}\}$ the integer solution of (2) exists. In that case at least one of c, d has to be negative integer (otherwise, we have the contradiction with [12, Corollarry 1.3]). Since $\mathbb{Z}[\sqrt{-2^{2l+1}}] \subseteq \mathbb{Z}[\sqrt{-2}]$, it is enough to prove the nonexistence of such $D(-1)$-quadruple in the ring $\mathbb{Z}[\sqrt{-2}]$. Therefore, if $\tilde{s}, \tilde{t}, x, y, z \in \mathbb{Z}$, we will consider the existence of $D(-1)$-quadruples of the form $\{1, p, -c, -d\}$ and $\{1, p, -c, d\}$, where $c, d > 0$, corresponding to the following systems, respectively:

(i) $-c-1 = -2\tilde{s}^2,\ -pc-1 = -2\tilde{t}^2,\ -d-1 = -2x^2,\ -pd-1 = -2y^2,\ cd-1 = z^2$,

(ii) $-c-1 = -2\tilde{s}^2,\ -pc-1 = -2\tilde{t}^2,\ d-1 = x^2,\ pd-1 = y^2,\ -cd-1 = -2z^2$.

In both cases the first two equations are equal and if we eliminate the variable c we obtain

$$\tilde{t}^2 - (2^{2^n} + 1)\tilde{s}^2 = -2^{2^n-1}. \tag{3}$$

Now we will analyze each of above cases.

Case (i)

According to [14] the primitive solutions to $x^2 - Dy^2 = N$, where $D > 0$ is not a perfect square, with $y > 0$ can be found by considering the continued fraction expansions of both $\omega_i = \frac{-u_i+\sqrt{D}}{Q_0}$ and $\omega_i' = \frac{u_i+\sqrt{D}}{Q_0}$, for $1 \leq i \leq r+2$, where $Q_0 = |N|$, and $u_1, \ldots u_{r+2}$ are solutions of equation $u^2 \equiv D \pmod{Q_0}$ in the range $0 \leq u \leq |N|/2$. To check the solvability, we have to consider only one of ω_i and ω_i'. This condition and [14, Theorem 2(a)] imply the next lemma.

Lemma 3 *For $1 \leq i \leq r+2$, let*

$$\omega_i = \frac{-u_i + \sqrt{D}}{Q_0} = \left[a_0, \ldots, a_t, \overline{a_{t+1}, \ldots, a_{t+l}}\right],$$

and let $(P_m + \sqrt{D})/Q_m$ be the m-th complete convergent of the simple continued fraction for ω_i. Then a necessary condition for $x^2 - Dy^2 = N, \gcd(x, y) = 1$, to be solvable is that for some $i \in \{1, \ldots, r+2\}$, we have $Q_m = 1$ for some m such that $t+1 \leq m \leq t+l$, where if l is even, then $(-1)^m N/|N| = 1$.

We can apply the above lemma to equation (3), for $n \geq 3$ (the case of $n = 2$ is covered by [20]). We have $D = 2^{2^n} + 1, N = -2^{2^n - 1}$. Therefore, $Q_0 = 2^{2^n - 1}$. Since the only solutions of equation $u^2 \equiv 2^{2^n} + 1 \equiv 1 \pmod{2^{2^n - 1}}$ such that $0 \leq u \leq 2^{2^n - 2}$ are 1 and $2^{2^n - 2} - 1$, according to Lemma 3 we have to find m-th complete convergents of

$$\omega_1 = \frac{-1 + \sqrt{2^{2^n} + 1}}{2^{2^n - 1}} \quad \text{and} \quad \omega_2 = \frac{-2^{2^n - 2} + 1 + \sqrt{2^{2^n} + 1}}{2^{2^n - 1}}.$$

It can be shown that

i	0	1	2	3	4
P_i	-1	1	$2^{2^{n-1}} - 1$	1	$2^{2^{n-1}} - 1$
Q_i	$2^{2^n - 1}$	2	$2^{2^{n-1}}$	$2^{2^{n-1}}$	2

and $\omega_1 = \left[0, 2^{2^{n-1} - 1}, \overline{1, 1, 2^{2^{n-1}} - 1}\right]$. In this case we have $l = 3, t = 1$ and the condition $Q_m = 1$ does not hold for $2 \leq m \leq 4$.
Similarly, in case of ω_2 we obtain

i	0	1	2	3	4
P_i	$-2^{2^n - 2} + 1$	$-2^{2^n - 2} - 1$	$2^{2^n - 3} + 2$	-5	$2^{2^{n-1}} - 3$
Q_i	$2^{2^n - 1}$	$-2^{2^n - 3} + 1$	$2^{2^n - 3} - 3$	8	$3 \cdot 2^{2^{n-1} - 2} - 1$

i	5	6	7	8
P_i	$2^{2^{n-1} - 1} + 1$	$2^{2^{n-1} - 1} - 1$	$2^{2^{n-1} - 2} + 2$	$2^{2^{n-1}} - 5$
Q_i	$2^{2^{n-1}}$	$3 \cdot 2^{2^{n-1} - 2} + 1$	$5 \cdot 2^{2^{n-1} - 2} - 3$	8

and $\omega_2 = \left[-1, 1, 1, 2^{2^{n-1} - 3} - 1, \overline{2, 1, 1, 1, 2^{2^{n-1} - 2} - 1}\right]$. Here we have $l = 5$, $t = 3$. The condition $Q_m = 1$ does not hold for $4 \leq m \leq 8$.

These considerations imply that the equation (3) has no primitive solutions. Thus, $\tilde{t}$ and $\tilde{s}$ are even numbers. Since $c + 1 = 2\tilde{s}^2$ it follows that $c \equiv 3 \pmod 4$. On the other hand,

$$z^2 = cd - 1 \equiv -1 \pmod c.$$

That implies that $\left(\frac{-1}{c}\right) = 1$, i.e., $c \equiv 1 \pmod 4$, which is a contradiction.

Now we are able to state the following result:

Proposition 3 *Let $n \geq 2$ and let p be the n-th Fermat prime. There does not exist a $D(-1)$-quadruple of the form $\{1, p, c, d\}$, $cd > 0$ in $\mathbb{Z}[\sqrt{-t}], t \in \{2, 2^3, \dots, 2^{2^{n-1}-1}\}$.*

Case (ii)

To completely solve this case we have to involve the results containing different kind of bounds obtained by considering element c which is generated by solutions of (3). Thus, it was too complicate to obtain some general result and in what follows we will restrict ourself into the cases of $n = 3, 4$, i.e., $p = 257, 65537$. For all calculations we used *Wolfram Mathematica 11.*

By using [16, Theorem 108a] all solutions in positive integers of Pellian equation (3) are given by

$$\begin{aligned} \tilde{t} + \tilde{s}\sqrt{2^{2^n}+1} =& 2^{2^{n-2}-1}\left(2^{2^{n-1}} - 1 + \sqrt{2^{2^n}+1}\right) \\ & \times \left(2^{2^n+1} + 1 + 2^{2^{n-1}+1}\sqrt{2^{2^n}+1}\right)^N, \\ \tilde{t} + \tilde{s}\sqrt{2^{2^n}+1} =& -2^{2^{n-2}-1}\left(2^{2^{n-1}} - 1 - \sqrt{2^{2^n}+1}\right) \\ & \times \left(2^{2^n+1} + 1 + 2^{2^{n-1}+1}\sqrt{2^{2^n}+1}\right)^N, \end{aligned} \tag{4}$$

where $N \geq 0$, respectively. Thus we have two sequences of solutions determined by

$$\begin{aligned} \tilde{t}_0 &= 2^{2^{n-2}-1}(2^{2^{n-1}} - 1), \quad \tilde{s}_0 = 2^{2^{n-2}-1}, \\ \tilde{t}_1 &= 2^{2^{n-2}-1}(-2^{2^n+1} + 2^{3\cdot 2^{n-1}+2} + 3\cdot 2^{2^{n-1}} - 1), \\ \tilde{s}_1 &= 2^{2^{n-2}-1}(2^{2^n+2} - 2^{2^{n-1}+1} + 1), \\ \tilde{t}_{N+2} &= 2(2^{2^n+1}+1)\tilde{t}_{N+1} - \tilde{t}_N, \quad \tilde{s}_{N+2} = 2(2^{2^n+1}+1)\tilde{s}_{N+1} - \tilde{s}_N, \end{aligned} \tag{5}$$

$$\begin{aligned} \tilde{t}_0' &= -2^{2^{n-2}-1}(2^{2^{n-1}} - 1), \quad \tilde{s}_0' = 2^{2^{n-2}-1}, \\ \tilde{t}_1' &= 2^{2^{n-2}-1}(2^{2^n+1} + 2^{2^{n-1}} + 1), \\ \tilde{s}_1' &= 2^{2^{n-2}-1}(2^{2^{n-1}+1} + 1), \\ \tilde{t}_{N+2}' &= 2(2^{2^n+1}+1)\tilde{t}_{N+1} - \tilde{t}_N, \quad \tilde{s}_{N+2}' = 2(2^{2^n+1}+1)\tilde{s}_{N+1} - \tilde{s}_N. \end{aligned} \tag{6}$$

Let $(\tilde{t_k}, \tilde{s_k}), k = 0, 1, 2, \dots$ denote all positive solutions of Pellian equation (3) given by (5) and (6), respectively. Then there exists an integer k such that

$$c = c_k = 2\tilde{s_k}^2 - 1. \tag{7}$$

Eliminating d, from

$$\begin{aligned} d-1 &= x^2, \\ (2^{2^n}+1)d-1 &= y^2, \\ -cd-1 &= -2z^2 \end{aligned}$$

we obtain the system of simultaneous Pellian equations

$$2z^2 - cx^2 = c+1, \tag{8}$$
$$(2^{2^n+1}+2)z^2 - cy^2 = c+(2^{2^n}+1). \tag{9}$$

Now we have to solve the above system depending on c defined by (7). In dependence on whether or not the non-trivial solution of the above system exists, we will be able to conclude something about the existence of $D(-1)$-quadruples determined by (ii). We state the following result:

Proposition 4 *Let $n = 3, 4$ and let p be the n-th Fermat prime. Let k be a nonnegative integer and $c = c_k$ be defined by* (7). *There does not exist a $D(-1)$-quadruple of the form $\{1, p, -c, d\}$, $c, d > 0$ in $\mathbb{Z}[\sqrt{-t}], t \in \{2, 2^3, \dots, 2^{2^{n-1}-1}\}$.*

The proof of Proposition 4 is divided into several parts, where we use the standard methods when considering the extension of a Diophantine triple. The problem of solving the system of simultaneous Pellian equations reduces to finding intersection of binary recursive sequences v_M and w_N. By using the congruence method together with the result on linear forms in logarithms due to Matveev ([15]) we will obtain an upper bound of extension element and indices M, N of the recurring sequences. The reduction method ([8, Lemma 5a]), based on the Baker-Davenport lemma ([2, Lemma]), will complete the proof of Proposition 4. Although the strategy of the proof is similar as the proof of results in [20, 21], for the convenience of the reader we will write the basic steps. This is more technically challenging and really a laborious work.

Positive solutions of Pellian equations (8) and (9) respectively have the forms:

$$z\sqrt{2}+x\sqrt{c} = \left(z_0^{(i)}\sqrt{2}+x_0^{(i)}\sqrt{c}\right)\left(2c+1+2\tilde{s}\sqrt{2c}\right)^M, \tag{10}$$

$$\begin{aligned} z\sqrt{2^{2^n+1}+2}+y\sqrt{c} &= \left(z_1^{(j)}\sqrt{2^{2^n+1}+2}+y_1^{(j)}\sqrt{c}\right) \\ &\times\left((2^{2^n+1}+2)c+1+2\tilde{t}\sqrt{(2^{2^n+1}+2)c}\right)^N, \end{aligned} \tag{11}$$

where M, N are non-negative integers and $\{(z_0^{(i)}, x_0^{(i)}) : i = 1, \dots, i_0\}$, $\{(z_1^{(j)}, y_1^{(j)}) : j = 1, \dots, j_0\}$ are finite sets of fundamental solutions of (8) and (9), respectively, satisfying

$$\begin{aligned} |z_0^{(i)}| &\leq c, \\ |z_1^{(j)}| &< c + 2^{2^n-2} + 1 \leq c + 2^{2^n-2}. \end{aligned}$$

For simplicity, from now we will omit the superscripts (i) and (j). The problem of solving the system of simultaneous Pellian equations (8) and (9) consists in solving a finite number of Diophantine equations of the form $v_M = w_N$, where sequences (v_M) and (w_N) are given by

$$\begin{aligned} v_0 = z_0, \quad v_1 = (2c+1)z_0 + 2c\tilde{s}x_0, \\ v_{M+2} = (4c+2)v_{M+1} - v_M, \end{aligned} \tag{12}$$

$$\begin{aligned} w_0 = z_1, \quad w_1 = ((2^{2^n+1}+2)c+1)z_1 + 2c\tilde{t}y_1, \\ w_{N+2} = ((2^{2^n+2}+4)c+2)w_{N+1} - w_N. \end{aligned} \tag{13}$$

Congruences

From (12) and (13), we get by induction

$$\begin{aligned} v_M &\equiv z_0 \pmod{2c}, \\ w_N &\equiv z_1 \pmod{2c}. \end{aligned}$$

So if the equation $v_M = w_N$ has a solution in integers M and N, then we have

$$z_0 = z_1, \tag{14}$$

$$z_1 = z_0 - 2c, \quad z_0 > 0, \tag{15}$$

$$z_1 = z_0 + 2c, \quad z_0 < 0. \tag{16}$$

Observing the cases (15) and (16) from (8) we obtain the condition

$$c | 2i^2 - 1, \quad i \in \{0, 1, \dots, 2^{2^n-2}\}. \tag{17}$$

If $p = 257$, i.e., $n = 3$, from (7) we obtain that $c = c_0 = 7$. In that case, it can be seen that the condition (17) is satisfied for some i. Therefore, including the possibility (14), we have some new possibilities for z_0 and z_1 determined by (15) and (16). Inserting that solutions into (8) and (9) it is easy to see that at least one equation has no corresponding integer solutions

x_0, y_1. So in case of $c = 7$ we will omit possibilities (15) and (16). Thus, we will assume that $c > 7$ is the minimal positive integer such that the system of equations (8) and (9) has a solution. Then form (5), (6) and (7) we obtain that $c \geq c_1 = 8711$ is the minimal positive integer such that the $D(-1)$-triple of the form $\{1, 257, -c\}$ can be extended. In that case the condition (17) is not satisfied, and we have only (14).

By the same argumentation, in case of $p = 65537$, i.e., $n = 4$, possibilities (15) and (16) will be omitted for $c = c_0 = 127$ and $c = c_1 = 33685631$. Similarly, we will assume that $c \geq c_2 = 8761833816191$ is the minimal positive integer such that the $D(-1)$-triple of the form $\{1, 65537, -c\}$ can be extended and also conclude that if the equation $v_M = w_N$ has a solution, then we have (14).

Besides that, we are obliged to say since the case (14) can also appear for all above omitted c's, in all further results that might be necessary for the reduction method, we will also include those c and use the reduction method as well.

Let $d_0 = (2z_0^2 - 1)/c$. Then

$$\begin{aligned} d_0 - 1 &= x_0^2, \\ (2^{2^n} + 1)d_0 - 1 &= y_1^2, \\ -cd_0 - 1 &= -2z_0^2, \end{aligned}$$

so $\{1, 2^{2^n} + 1, -c, d_0\}$ is a $D(-1)$-quadruple. Moreover,

$$0 < d_0 \leq c + 2.$$

If $d_0 = c + 2$, then $(c + 1)^2 = 2z_0^2$, i.e. $c = -1$ and $z_0 = 0$. This is not possible.

If $d_0 = c + 1$, we obtain $c(c + 1) + 1 = 2z_0^2$. Since $c(c + 1) + 1$ is an odd number, we have a contradiction. Therefore, $d_0 \leq c$.

Let $d_0 > 1$. Now, we will consider the extensibility of $D(-1)$-triple $\{1, 2^{2^n} + 1, d\}, d = d_0$ to $D(-1)$-quadruple $\{1, 2^{2^n} + 1, d, e\}$ with properties

$$\begin{aligned} d - 1 &= \hat{s}^2, \\ (2^{2^n} + 1)d - 1 &= \hat{t}^2, \end{aligned} \tag{18}$$

and

$$\begin{aligned} e - 1 &= -2\hat{x}^2, \\ (2^{2^n} + 1)e - 1 &= -2\hat{y}^2, \\ ed - 1 &= -2\hat{z}^2. \end{aligned} \tag{19}$$

From (19) it follows

$$
\begin{aligned}
2\hat{z}^2 - 2d\hat{x}^2 &= 1-d, && (20)\\
(2^{2^n+1}+2)\hat{z}^2 - 2d\hat{y}^2 &= 2^{2^n}+1-d. && (21)
\end{aligned}
$$

If $d < 2^{2^n}+1$, then from (18) in cases of $n = 3, 4$ we obtain $d = 226$ and $d = 50626$, respectively. In both cases the equation (20) is not solvable modulo 4. Therefore, we can assume that $d > 2^{2^n}+1$.

If $(\hat{z}, \hat{x})$ and $(\hat{z}, \hat{y})$ are positive solutions of Pellian equations (20) and (21), respectively, then there exist $i \in \{1, \dots, i_0\}$, $j \in \{1, \dots, j_0\}$, and integers $M, N \geq 0$ such that

$$
\begin{aligned}
\hat{z}\sqrt{2} + \hat{x}\sqrt{2d} &= \left(\hat{z_0}^{(i)}\sqrt{2} + \hat{x_0}^{(i)}\sqrt{2d}\right)\left(2d-1+\hat{s}\sqrt{4d}\right)^M, && (22)\\
\hat{z}\sqrt{2^{2^n+1}+2} + \hat{y}\sqrt{2d} &= \left(\hat{z_1}^{(j)}\sqrt{2^{2^n+1}+2} + \hat{y_1}^{(j)}\sqrt{2d}\right)\\
&\quad \times \left((2^{2^n+1}+2)d+1+\hat{t}\sqrt{(2^{2^n+2}+4)d}\right)^N. && (23)
\end{aligned}
$$

We have

$$
\begin{aligned}
|\hat{z_0}^{(i)}| &< d,\\
|\hat{z_1}^{(j)}| &< d.
\end{aligned}
$$

Similarly, from (22) and (23), we conclude that $\hat{z} = \hat{v_M}^{(i)} = \hat{w_N}^{(j)}$, for some indices i, j and non-negative integers M, N, where

$$
\begin{aligned}
&\hat{v_0}^{(i)} = \hat{z_0}^{(i)}, \quad \hat{v_1}^{(i)} = (2d-1)\hat{z_0}^{(i)} + 2d\hat{s}\hat{x_0}^{(i)},\\
&\hat{v}_{M+2}^{(i)} = (4d-2)\hat{v}_{M+1}^{(i)} - \hat{v_M}^{(i)}, && (24)
\end{aligned}
$$

$$
\begin{aligned}
&\hat{w_0}^{(j)} = \hat{z_1}^{(j)}, \quad \hat{w_1}^{(j)} = ((2^{2^n+1}+2)d-1)\hat{z_1}^{(j)} + 2d\hat{t}\hat{y_1}^{(j)},\\
&\hat{w}_{N+2}^{(j)} = ((2^{2^n+2}+4)d-2)\hat{w}_{N+1}^{(j)} - \hat{w_N}^{(j)}. && (25)
\end{aligned}
$$

From now we will also omit the superscripts (i) and (j). Similarly, from (24) and (25) it follows by induction that

$$
\begin{aligned}
\hat{v_M} &\equiv (-1)^M \hat{z_0} \pmod{2d},\\
\hat{w_N} &\equiv (-1)^N \hat{z_1} \pmod{2d}.
\end{aligned}
$$

So, if $\hat{v_M} = \hat{w_N}$ has a solution, we must have $|\hat{z_0}| = |\hat{z_1}|$.

Suppose now that $e_0 = (2\hat{z_0}^2 - 1)/d$. Then

$$\begin{aligned}
-e_0 - 1 &= -2\hat{x_0}^2, \\
-(2^{2^n}+1)e_0 - 1 &= -2\hat{y_1}^2, \\
-e_0 d - 1 &= -2\hat{z_0}^2,
\end{aligned}$$

so $\{1, 2^{2^n}+1, d, -e_0\}$ is a $D(-1)$-quadruple with $0 < e_0 < d$.

Thus, by assumption that $D(-1)$-triple $\{1, 2^{2^n}+1, d_0\}$, $d_0 > 1$ can be extended to $D(-1)$-quadruple $\{1, 2^{2^n}+1, d_0, -c\}$, we conclude that there exists positive integer $e_0 < d_0 \le c$ such that $\{1, 2^{2^n}+1, d_0, -e_0\}$ is a $D(-1)$-quadruple. But, this is a contradiction with the minimality of c. Therefore, $d_0 = 1$ which implies that $z_0 = z_1 = \pm\tilde{s}$, $x_0 = 0$, $y_1 = 2^{2^{n-1}}$.

From (10) and (11) it follows that we have to consider v_M and w_N of the form

$$v_M = \frac{\tilde{s}}{2}\Big(\Big(2c+1+2\tilde{s}\sqrt{2c}\Big)^M + \Big(2c+1-2\tilde{s}\sqrt{2c}\Big)^M \Big), \tag{26}$$

$$\begin{aligned}
w_N =& \frac{\Big(\tilde{s}\sqrt{2^{2^n+1}+2} \pm 2^{2^{n-1}}\sqrt{c}\Big)\Big((2^{2^n+1}+2)c+1+2\tilde{t}\sqrt{(2^{2^n+1}+2)c}\Big)^N}{2\sqrt{2^{2^n+1}+2}} \\
&+\frac{\Big(\tilde{s}\sqrt{2^{2^n+1}+2} \mp 2^{2^{n-1}}\sqrt{c}\Big)\Big((2^{2^n+1}+2)c+1-2\tilde{t}\sqrt{(2^{2^n+1}+2)c}\Big)^N}{2\sqrt{2^{2^n+1}+2}}.
\end{aligned} \tag{27}$$

From (12) and (13) we get by induction:

Lemma 4

$$\begin{aligned}
v_M &\equiv z_0 + 2cM^2 z_0 + 2cM\tilde{s}x_0 \pmod{8c^2}, \\
w_N &\equiv z_1 + (2^{2^n+1}+2)cN^2 z_1 + 2cN\tilde{t}y_1 \pmod{8c^2}.
\end{aligned}$$

Now we are going to obtain an unconditional relationship between M and N.

For $l > 0$ holds $v_l < w_l$, and $v_M = w_N, N \neq 0$ implies that $M > N$. Now we will estimate v_M and w_N. From (26) and (27) we have

$$\begin{aligned}
v_M &> \frac{\tilde{s}}{2}(2c+1+2\tilde{s}\sqrt{2c})^M \ge \frac{1}{2}(2c+1+2\tilde{s}\sqrt{2c})^M, \\
w_N &< \frac{\tilde{s}\sqrt{2^{2^n+1}+2}+2^{2^{n-1}}\sqrt{c}}{\sqrt{2^{2^n+1}+2}}\Big((2^{2^n+1}+2)c+1+2\tilde{t}\sqrt{(2^{2^n+1}+2)c}\Big)^N.
\end{aligned}$$

Since $\tilde{s} < \sqrt{c}$ and $\tilde{t} > 2^{2^{n-1}-1}\sqrt{2c}$ it follows that

$$\frac{\tilde{s}\sqrt{2^{2^n+1}+2}+2^{2^{n-1}}\sqrt{c}}{\sqrt{2^{2^n+1}+2}} < 2\sqrt{c}, \tag{28}$$

$$\frac{1}{2}\left((2^{2^n+1}+2)c+1+2\tilde{t}\sqrt{(2^{2^n+1}+2)c}\right)^{\frac{1}{2}} > 2^{2^{n-1}}\sqrt{c}, \tag{29}$$

and we obtain

$$w_N < \frac{1}{2}\left((2^{2^n+1}+2)c+1+2\tilde{t}\sqrt{(2^{2^n+1}+2)c}\right)^{N+\frac{1}{2}}.$$

Thus $v_M = w_N$ implies

$$\frac{2M}{2N+1} < \frac{\log\left((2^{2^n+1}+2)c+1+2\tilde{t}\sqrt{(2^{2^n+1}+2)c}\right)}{\log\left(2c+1+2\tilde{s}\sqrt{2c}\right)}. \tag{30}$$

By using (30), in cases of $n = 3, 4$ we can easily prove the next lemma:

Lemma 5 *Suppose that $N \neq 0, v_M = w_N$, and $c = c_k$ is defined by* (7)*.*

1° *Let $n = 3$.*

- (*i*) *If $c = c_0 = 7$, then $N < M < 3.94N$.*
- (*ii*) *If $c \geq c_1 = 8711$, then $N < M < 2.32N$.*

2° *Let $n = 4$.*

- (*i*) *If $c = c_0 = 127$, then $N < M < 4.18N$.*
- (*ii*) *If $c \geq c_1 = 33685631$, then $N < M < 2.5N$.*

Now we will determine the lover bound for M and N in terms of c.

Lemma 6 *If $v_M = w_N$, $N \neq 0$, $c = c_k > c_0 = 7$ in case of $n = 3$, and $c = c_k > c_1 = 33685631$ in case of $n = 4$, defined by* (7)*, then $M > N > \sqrt[5]{c}/2^{2^{n-1}}$.*

Proof: Let $c = c_k$ be defined by (7). Since $v_M = w_N$, $z_0 = z_1 = \pm\tilde{s}$, $x_0 = 0$, and $y_1 = 2^{2^{n-1}}$, Lemma 4 implies

$$\begin{aligned} M^2\tilde{s} &\equiv (2^{2^n}+1)N^2\tilde{s} \pm 2^{2^{n-1}}N\tilde{t} \pmod{4c}, \\ \tilde{s}(M^2-(2^{2^n}+1)N^2) &\equiv \pm 2^{2^{n-1}}N\tilde{t} \pmod{4c}, \\ 2\tilde{s}^2(M^2-(2^{2^n}+1)N^2)^2 &\equiv 2^{2^n+1}N^2\tilde{t}^2 \pmod{4c}. \end{aligned} \tag{31}$$

Since $c+1=2\tilde{s}^2, (2^{2^n}+1)c+1=2\tilde{t}^2$ we have

$$(c+1)(M^2-(2^{2^n}+1)N^2)^2 \equiv 2^{2^n}N^2((2^{2^n}+1)c+1) \pmod{4c},$$

which implies

$$(M^2-(2^{2^n}+1)N^2)^2 \equiv 2^{2^n}N^2 \pmod{c}. \tag{32}$$

Assume that $N \leq \sqrt[5]{c}/2^{2^{n-1}}$. Since $N<M$ by Lemma 5, we have

$$|\tilde{s}(M^2-(2^{2^n}+1)N^2)| < \sqrt{\frac{c+1}{2}} \cdot 2^{2^n}N^2 \leq \sqrt{\frac{c+1}{2}} \cdot \sqrt[5]{c^2} < c,$$

and

$$(M^2-(2^{2^n}+1)N^2)^2 < (2^{2^n}N^2)^2 = 2^{2^{n+1}}N^4 \leq \sqrt[5]{c^4} < c.$$

On the other hand, if $n=3, c>c_0=7$, and if $n=4, c>c_1=33685631$, it holds

$$\sqrt{\frac{(2^{2^n}+1)c+1}{2}} < \sqrt[5]{c^4},$$

and we have

$$2^{2^{n-1}}\tilde{t}N \leq 2^{2^{n-1}} \cdot \sqrt{\frac{(2^{2^n}+1)c+1}{2}} \cdot \frac{\sqrt[5]{c}}{2^{2^{n-1}}} < c, \qquad 2^{2^n}N^2 \leq \sqrt[5]{c^2} < c.$$

It follows from (31) and (32) that

$$\tilde{s}(M^2-(2^{2^n}+1)N^2) = -2^{2^{n-1}}\tilde{t}N, \qquad (M^2-(2^{2^n}+1)N^2)^2 = 2^{2^n}N^2.$$

Hence we have

$$\tilde{s}^2(M^2-(2^{2^n}+1)N^2)^2 = 2^{2^n}\tilde{t}^2N^2 = \tilde{t}^2(M^2-(2^{2^n}+1)N^2)^2,$$

which together with $N \neq 0$ implies $\tilde{s}^2=\tilde{t}^2$. This is not possible.

□

Linear forms in logarithms

In order to successfully solve the equation $v_M = w_N$, it is necessary to determine an explicit upper bound for index M or N. For this purpose, we use Baker's theory on linear forms in logarithms on algebraic numbers. In that way we will obtain an upper bound for N. We will use the following lemma:

Lemma 7 ([18, Lemma B2]) *If $a \in (0,1)$ and $0<|X|<a$, then*

$$|\log(X+1)| < \frac{-\log(1-a)}{a}|X|.$$

First, let us prove the following result:

Lemma 8 *Assume that* $c = c_k$ *is defined by* (7). *If* $v_M = w_N$ *and* $N \neq 0$, *then*

$$0 < N \log\left((2^{2^n+1}+2)c+1+2\tilde{t}\sqrt{(2^{2^n+1}+2)c}\right) - M\log\left(2c+1+2\tilde{s}\sqrt{2c}\right) + \log\frac{\tilde{s}\sqrt{2^{2^n+1}+2} \pm 2^{2^{n-1}}\sqrt{c}}{\tilde{s}\sqrt{2^{2^n+1}+2}} < K, \tag{33}$$

where

$$K = \begin{cases} 7.57\cdot(1028c)^{-N}, & \text{if } n=3; \\ 31.88\cdot(262148c)^{-N}, & \text{if } n=4. \end{cases}$$

Proof: Set

$$\begin{aligned} P =& \tilde{s}(2c+1+2\tilde{s}\sqrt{2c})^M, \\ Q =& \frac{1}{\sqrt{2^{2^n+1}+2}}\left(\tilde{s}\sqrt{2^{2^n+1}+2} \pm 2^{2^{n-1}}\sqrt{c}\right) \\ & \times \left((2^{2^n+1}+2)c+1+2\tilde{t}\sqrt{(2^{2^n+1}+2)c}\right)^N. \end{aligned} \tag{34}$$

Therefore,

$$\begin{aligned} P^{-1} =& \frac{1}{\tilde{s}}(2c+1-2\tilde{s}\sqrt{2c})^M, \\ Q^{-1} =& \frac{\sqrt{2^{2^n+1}+2}}{c+2^{2^n}+1}\left(\tilde{s}\sqrt{2^{2^n+1}+2} \mp 2^{2^{n-1}}\sqrt{c}\right) \\ & \times \left((2^{2^n+1}+2)c+1-2\tilde{t}\sqrt{(2^{2^n+1}+2)c}\right)^N. \end{aligned}$$

If $v_M = w_N$, then from (26) and (27) we obtain

$$P + \tilde{s}^2 P^{-1} = Q + \frac{c+2^{2^n}+1}{2^{2^n+1}+2}Q^{-1}. \tag{35}$$

We conclude that $P > 1$. Since

$$\begin{aligned} Q \geq& \frac{1}{\sqrt{2^{2^n+1}+2}}\left(\tilde{s}\sqrt{2^{2^n+1}+2} - 2^{2^{n-1}}\sqrt{c}\right) \\ & \times \left((2^{2^n+1}+2)c+1+2\tilde{t}\sqrt{(2^{2^n+1}+2)c}\right), \end{aligned}$$

it isn't hard to conclude that $Q > 1$. Furthermore,

$$\begin{aligned} P - Q =& \frac{c + 2^{2^n} + 1}{2^{2^n+1} + 2} Q^{-1} - \frac{c+1}{2} P^{-1} \\ <& \frac{c+1}{2}(P-Q)P^{-1}Q^{-1}, \qquad (36) \\ P - \frac{c+1}{2} =& \frac{c+1}{2}\left(\frac{(2c+1+2\tilde{s}\sqrt{2c})^M}{\tilde{s}} - 1\right) > 0. \end{aligned}$$

We obtain

$$P \quad > \quad \frac{c+1}{2}. \qquad (37)$$

If we suppose that $P > Q$, from (36) we conclude that $PQ < (c+1)/2$. Since $Q > 1$, by using (37) we obtain a contradiction. Therefore, $Q > P$.

Now, if we consider (35), we conclude that

$$P > Q - \frac{c+1}{2} P^{-1} > Q - 1. \qquad (38)$$

Since $Q > 1$, from (38) we obtain

$$\frac{Q-P}{Q} < Q^{-1}. \qquad (39)$$

On the other hand,

$$\begin{aligned} Q^{-1} \leq& \frac{\sqrt{2^{2^n+1}+2}}{c + 2^{2^n} + 1}\left(\tilde{s}\sqrt{2^{2^n+1}+2} + 2^{2^{n-1}}\sqrt{c}\right) \\ & \times \left((2^{2^n+1}+2)c + 1 + 2\tilde{t}\sqrt{(2^{2^n+1}+2)c}\right)^{-N}. \end{aligned}$$

Since c is defined by (7), we obtain that

$$\frac{\sqrt{2^{2^n+1}+2}}{c + 2^{2^n} + 1}\left(\tilde{s}\sqrt{2^{2^n+1}+2} + 2^{2^{n-1}}\sqrt{c}\right) < \begin{cases} 7.557, & \text{if } n = 3; \\ 31.876, & \text{if } n = 4. \end{cases}$$

Furthermore, from $2\tilde{t}\sqrt{(2^{2^n+1}+2)c} > (2^{2^n+1}+2)c$ we conclude that

$$\left((2^{2^n+1}+2)c + 1 + 2\tilde{t}\sqrt{(2^{2^n+1}+2)c}\right)^{-N} < \left((2^{2^n+2}+4)c\right)^{-N}.$$

Therefore,

$$Q^{-1} < \begin{cases} 7.557 \cdot (1028c)^{-N}, & \text{if } n = 3; \\ 31.876 \cdot (262148c)^{-N}, & \text{if } n = 4. \end{cases} \tag{40}$$

Now we are ready to bound linear form $\log \frac{Q}{P}$ in logarithms.

By Lemma 7 for $|X| = Q^{-1}$, it follows from (39) and (40) that

$$0 < \log \frac{Q}{P} = -\log\left(1 - \frac{Q-P}{Q}\right) < -\log(1 - Q^{-1}) < K, \quad \text{where}$$
$$K = \begin{cases} 7.57 \cdot (1028c)^{-N}, & \text{if } n = 3; \\ 31.88 \cdot (262148c)^{-N}, & \text{if } n = 4. \end{cases} \tag{41}$$

Since

$$\log \frac{Q}{P} = N \log\left((2^{2^n+1} + 2)c + 1 + 2\tilde{t}\sqrt{(2^{2^n+1} + 2)c}\right) - M \log\left(2c + 1 + 2\tilde{s}\sqrt{2c}\right)$$
$$+ \log \frac{\tilde{s}\sqrt{2^{2^n+1} + 2} \pm 2^{2^{n-1}}\sqrt{c}}{\tilde{s}\sqrt{2^{2^n+1} + 2}},$$

the statement of the lemma follows from (41).

□

Let

$$\Lambda = N \log\left((2^{2^n+1} + 2)c + 1 + 2\tilde{t}\sqrt{(2^{2^n+1} + 2)c}\right) - M \log\left(2c + 1 + 2\tilde{s}\sqrt{2c}\right)$$
$$+ \log \frac{\tilde{s}\sqrt{2^{2^n+1} + 2} \pm 2^{2^{n-1}}\sqrt{c}}{\tilde{s}\sqrt{2^{2^n+1} + 2}}.$$

From Lema 8 we obtain an upper bound for $\log \Lambda$. To obtain the lover bound for $\log \Lambda$ we recall the following theorem of E. M. Matveev [15]:

Theorem 1 (Matveev, [15]) *Let $\lambda_1, \lambda_2, \lambda_3$ be $\mathbb{Q}$-linearly independent logarithms of non-zero algebraic numbers and let b_1, b_2, b_3 be rational integers with $b_1 \neq 0$. Define $\alpha_j = \exp(\lambda_j)$ for $j = 1, 2, 3$ and*

$$\Lambda = b_1\lambda_1 + b_2\lambda_2 + b_3\lambda_3.$$

Let D be the degree of the number field $\mathbb{Q}(\alpha_1, \alpha_2, \alpha_3)$ over $\mathbb{Q}$. Put

$$\chi = [\mathbb{R}(\alpha_1, \alpha_2, \alpha_3) : \mathbb{R}].$$

Let A_1, A_2, A_3 *be positive real numbers, which satisfy*

$$A_j \geq \max\{Dh(\alpha_j), |\lambda_j|, 0.16\}, \quad 1 \leq j \leq 3,$$

where $h(\alpha_j)$ *is the absolute logarithmic height of* $\alpha_j, 1 \leq j \leq 3$*. Assume that*

$$B \geq \max\{1, \max\{|b_j| A_j / A_1 : 1 \leq j \leq 3\}\}.$$

Define also

$$C_1 = \frac{5 \cdot 16^5}{6\chi} e^3 (7 + 2\chi) \left(\frac{3e}{2}\right)^{\chi} \left(20.2 + \log(3^{5.5} D^2 \log(eD))\right).$$

Then

$$\log|\Lambda| > -C_1 D^2 A_1 A_2 A_3 \log\left(1.5eDB \log(eD)\right).$$

In our case, $b_1 = N, b_2 = -M, b_3 = 1, D = 4, \chi = 1$, and

$$\alpha_1 = (2^{2^n+1} + 2)c + 1 + 2\tilde{t}\sqrt{(2^{2^n+1} + 2)c},$$
$$\alpha_2 = 2c + 1 + 2\tilde{s}\sqrt{2c},$$
$$\alpha_3 = \frac{\tilde{s}\sqrt{2^{2^n+1} + 2} \pm 2^{2^{n-1}}\sqrt{c}}{\tilde{s}\sqrt{2^{2^n+1} + 2}}.$$

Minimal polynomials of α_1, α_2 are

$$P_{\alpha_1}(x) = x^2 - ((2^{2^n+2} + 4)c + 2)x + 1,$$
$$P_{\alpha_2}(x) = x^2 - (4c + 2)x + 1.$$

Therefore, the corresponding absolute logarithmic heights are

$$h(\alpha_1) = \frac{1}{2} \log \alpha_1,$$
$$h(\alpha_2) = \frac{1}{2} \log \alpha_2.$$

Note that α_3 is the root of the polynomial

$$P'_{\alpha_3}(x) = \frac{(2^{2^n} + 1)c + 2^{2^n} + 1}{2^{2^{n-1}-1}} x^2 - \frac{(2^{2^n+1} + 2)c + 2^{2^n+1} + 2}{2^{2^{n-1}-1}} x + \frac{2^{2^n} + 1 + c}{2^{2^{n-1}-1}}.$$

From (4) we conclude that $2^{2^{n-1}-2} | \tilde{s_k}^2$. Thus from (7) it follows that $c \equiv -1 \pmod{2^{2^{n-1}-1}}$. Therefore, P'_{α_3} is the polynomial with integer coefficients.

In this case we conclude that

$$h(\alpha_3) \le \frac{1}{2}\log\left(\frac{(2^{2^n}+1)c + 2^{2^n}+1}{2^{2^{n-1}-1}}\left(1 + \frac{2^{2^{n-1}-1}\sqrt{(2^{2^n+1}+2)c}}{(2^{2^n}+1)\tilde{s}}\right)\right)$$
$$= \frac{1}{2}\log\left(\frac{(2^{2^n}+1)\tilde{s}^2}{2^{2^{n-1}-2}} + 2\tilde{s}\sqrt{(2^{2^n+1}+2)c}\right).$$

Let $n = 3$. Since $\tilde{s} < \sqrt{c}$ and $\tilde{t} < 12\sqrt{c}$ it is easy to see that one can choose

$$A_1 = 2\log(1060c),$$
$$A_2 = 2\log(6c),$$
$$A_3 = 2\log(111c).$$

Therefore, by using Lemma 5 we take

$$B = \begin{cases} 1.66N, & \text{if } c = 7; \\ \dfrac{2.32 \cdot \log(6c) \cdot N}{\log(1060c)}, & \text{if } c > 7. \end{cases} \tag{42}$$

Now from Theorem 1 in combining with Lemma 8 we obtain

$$\begin{aligned} &2.464{\cdot}10^{12} \cdot \log(1060c) \cdot \log(6c) \cdot \log(111c)\log\left(6Be\log(4e)\right) \\ &\quad > N\log(1028c) - 2.03. \end{aligned} \tag{43}$$

Similarly, in case of $n = 4$ we obtain

$$\begin{aligned} &2.464{\cdot}10^{12} \cdot \log(262859c) \cdot \log(6c) \cdot \log(1750c)\log\left(6Be\log(4e)\right) \\ &\quad > N\log(262148c) - 3.47, \end{aligned} \tag{44}$$

where

$$B = \begin{cases} 1.61N, & \text{if } c = 127; \\ \dfrac{2.5 \cdot \log(6c) \cdot N}{\log(262859c)}, & \text{if } c > 127. \end{cases} \tag{45}$$

Now we are ready to prove the following result:

Proposition 5

1° *If* $n = 3$ *and* $c = c_k > c_0 = 7$ *defined by* (7) *is minimal for which the system of equations* (8) *and* (9) *has a nontrivial solution, then* $c < 1.156 \cdot 10^{100}$.

2° *If* $n = 4$ *and* $c = c_k > c_1 = 33685631$ *defined by* (7) *is minimal for which the system of equations* (8) *and* (9) *has a nontrivial solution, then* $c < 2.385 \cdot 10^{106}$.

Proof: 1°: Let $n = 3$ and $c = c_k > 7$ be defined by (7). From Lema 6 we have $N > \sqrt[5]{c}/16$. Then from (42) we obtain

$$B > \frac{2.32 \cdot \log(6c) \cdot \sqrt[5]{c}}{16 \cdot \log(1060c)}.$$

Thus we take

$$B = \frac{0.15 \cdot \log(6c) \cdot \sqrt[5]{c}}{\log(1060c)}.$$

Now from (43) we obtain

$$2.464{\cdot}10^{12} \cdot \log(1060c) \cdot \log(6c) \cdot \log(111c) \log\left(6Be\log(4e)\right) > \frac{\sqrt[5]{c}}{16} \log(1028c) - 2.03,$$

and it follows that $c < 1.156 \cdot 10^{100}$.

2°: Similarly, in case of $n = 4$ and $c = c_k > c_1 = 33685631$ defined by (7), from (44) and (45) we obtain the inequality

$$2.464{\cdot}10^{12} \cdot \log(262859c) \cdot \log(6c) \cdot \log(1750c) \log\left(6Be\log(4e)\right) > \frac{\sqrt[5]{c}}{256} \log(262148c) - 3.47,$$

where

$$B = \frac{0.01 \cdot \log(6c) \cdot \sqrt[5]{c}}{\log(262859c)}.$$

It follows that $c < 2.385 \cdot 10^{106}$. □

Now we determine all c defined by (7) which satisfy the Proposition 5. In case of $n = 3$ we obtain $c \in \{c_0, \ldots, c_{32}\}$, while for $n = 4$ it follows that $c \in \{c_0, \ldots, c_{19}\}$. To complete the proof of Proposition 4 in cases of $n = 3, 4$, we have to check if there is any nontrivial solution of the system of equations (8) and (9) for every such c. In the each case of c we use relations (42) – (45) to find an explicit upper bound for N. To obtain much better bound for N we use the reduction method of Dujella and Pethő [8].

Lemma 9 ([8, Lemma 5a]) *Suppose that* $\tilde{N}$ *is a positive integer. Let* p/q *be the convergent of the continued fraction expansion of* κ *such that* $q > 6\tilde{N}$

and let $\varepsilon = ||\mu q|| - \tilde{N} \cdot ||\kappa q||$, *where* $||\cdot||$ *denotes the distance from the nearest integer.*

If $\varepsilon > 0$, *then there is no solution of the inequality*

$$0 < N\kappa - M + \mu < A \cdot \tilde{B}^{-N}, \tag{46}$$

in integers M *and* N *with*

$$\frac{\log \frac{Aq}{\varepsilon}}{\log \tilde{B}} \le N \le \tilde{N}.$$

From (33) dividing by $\log(2c + 1 + 2\tilde{s}\sqrt{2c})$ we have

$$\kappa = \frac{\log\left((2^{2^n+1}+2)c+1+2\tilde{t}\sqrt{(2^{2^n+1}+2)c}\right)}{\log(2c+1+2\tilde{s}\sqrt{2c})}, \mu_{\pm} = \frac{\log \frac{\tilde{s}\sqrt{2^{2^n+1}+2} \pm 2^{2^{n-1}}\sqrt{c}}{\tilde{s}\sqrt{2^{2^n+1}+2}}}{\log(2c+1+2\tilde{s}\sqrt{2c})},$$

$$A \cdot \tilde{B}^{-N} = \frac{K}{\log(2c+1+2\tilde{s}\sqrt{2c})}.$$

We apply Lemma 9 with $\tilde{N}$ the upper bound for N in the each case of c. Once we get the sufficiently small an upper bound for N, by using Lemma 5 we find the corresponding M. For the convenience of the reader we will list one step in the each case of n.

• $n = 3, c = c_0 = 7, \tilde{s} = 2, \tilde{t} = 30$;
We obtain $\tilde{N} = 3 \cdot 10^{15}$. In the first step of reduction we obtain $N \le 4$. Therefore, $N = 1, M = 2, 3$; $N = 2, M = 3, \dots, 7$; $N = 3, M = 4, \dots, 11$; $N = 4, M = 5, \dots, 15$.

• $n = 4, c = c_0 = 127, \tilde{s} = 8, \tilde{t} = 2040$;
It follows $\tilde{N} = 9 \cdot 10^{15}$ and from the first step of reduction we have $N \le 2$. Thus, $N = 1, M = 2, 3, 4$; $N = 2, M = 3, \dots, 8$.

For determined indices M and N it is easy to check that in the each case there are no solutions of the equation $v_M = w_N$. This completes the proof of Proposition 4.

Note that we have just proved that for such c's the system of simultaneous Pellian equations (8) and (9) has only a trivial solution. Namely, if k is a nonnegative integer and $c = c_k$ is defined by (7), all solutions of the system of simultaneous Pellian equations (8) and (9) are given by

$$(x, y, z) = \left(0, 2^{2^{n-1}}, \pm\sqrt{\frac{c+1}{2}}\right).$$

All previously shown we can write in the form of the following result:

Proposition 6 *Let $n = 3, 4$ and let p be the n-th Fermat prime. There does not exist a $D(-1)$-quadruple of the form $\{1, p, c, d\}$ in $\mathbb{Z}[\sqrt{-t}]$, $t \in \{2, 2^3, \ldots, 2^{2^{n-1}-1}\}$.*

Although in Propositions 1, 2 and 3 we presented results on Fermat primes $2^{2^n} + 1$ for arbitrary $n \geq 1$ as members of $D(-1)$-quadruple in $\mathbb{Z}[\sqrt{-t}]$ depending on $t > 0$, we can summarize all previously known and just obtained results for so far known Fermat primes in the form of the following theorem:

Theorem 2 *Let $n \in \{1, 2, 3, 4\}$ and let p be the n-th Fermat prime. Let $t > 0$. If $t \in \{1, 2^2, \ldots, 2^{2^n-2}, 2^{2^n}\}$, then there exist infinitely many $D(-1)$-quadruples of the form $\{1, p, c, d\}$ in $\mathbb{Z}[\sqrt{-t}]$. In all other cases of t, in $\mathbb{Z}[\sqrt{-t}]$ does not exist $D(-1)$-quadruple of the previous form.*

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, 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] A. Bayad, A. Filipin, A. Togbe, *Extension of a parametric family of Diophantine triples in Gaussian integers*, Acta Math. Hung. **148** (2016), 312–327.

[4] 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.

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

[6] A. Dujella, *Diophantine m-tuples page*
`http://web.math.pmf.unizg.hr/~duje/dtuples.html`.

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

[8] A. Dujella, A. Pethö, *Generalization of a theorem of Baker and Davenport*, Quart. J. Math. Oxford Ser. **49** (1998), 291–306.

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

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

[11] 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.

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

[13] V. A. Lebesgue, *Sur l'impossbilité en nombres entiers de l'équation* $x^m = y^2 + 1$, Nouv. Ann. Math. **9** (1850), 178–181.

[14] K. Matthews, *The Diophantine equation* $x^2 - Dy^2 = N, D > 0$, Expo. Math. **18** (2000), 323–332.

[15] E. M. Matveev, *An explicit lower bound for a homogeneous rational linear form in logarithms of algebraic numbers. II*, Izv. Ross. Akad. Nauk Ser. Mat. **64** (2000), 125–180. English translation in Izv. Math. **64** (2000), 1217–1269.

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

[17] N. J. A. Sloane, *The on-line encyclopedia of integer sequences*, available at `https://oeis.org/A019434`.

[18] N. P. Smart, *The algorithmic resolution of diophantine equations*, Cambridge University Press, Cambridge, 1998.

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

[20] 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.

[21] 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.