Uniqueness of the extension of the $D(4k^2)$-triple
\[\{k^2 - 4, k^2, 4k^2 - 4\}\]

Yasutsugu Fujita\(^1\) and Alain Togbé\(^2\)

\(^1\) Department of Mathematics, College of Industrial Technology
Nihon University, 2-11-1 Shin-ei, Narashino, Chiba, Japan
e-mail: fujita.yasutsugu@nihon-u.ac.jp

\(^2\) Mathematics Department, Purdue University North Central
1401 S, U.S. 421, Westville, IN 46391, USA
e-mail: atogbe@pnc.edu

Abstract: Let $n$ be a nonzero integer. A set of $m$ distinct positive integers is called a $D(n)$-$m$-tuple if the product of any two of them increased by $n$ is a perfect square. Let $k$ be an integer greater than two. In this paper, we show that if \(\{k^2 - 4, k^2, 4k^2 - 4, d\}\) is a $D(4k^2)$-quadruple, then $d = 4k^4 - 8k^2$.

Keywords: Diophantine tuples, Simultaneous Diophantine equations.
AMS Classification: 11D09, 11J68

1 Introduction

Let $n$ be a nonzero integer. A set of $m$ distinct positive integers \(\{a_1, \ldots, a_m\}\) is called a Diophantine $m$-tuple with the property $D(n)$ or a $D(n)$-$m$-tuple, if $a_ia_j + n$ is a perfect square for each $i, j$ with $1 \leq i < j \leq m$.

The first example of a $D(1)$-quadruple was found by Fermat, which was the set \(\{1, 3, 8, 120\}\). Baker and Davenport ([1]) showed that \(\{1, 3, 8, 120\}\) cannot be extended to a $D(1)$-quintuple. There are several generalizations of this result (see [17] and its references); for example, \(\{k - 1, k + 1\}\) cannot be extended to a $D(1)$-quintuple ([14]). A folklore conjecture says that there does not exist a $D(1)$-quintuple, and Dujella ([7]) showed that there does not exist a $D(1)$-sextuple and that there exist only finitely many $D(1)$-quintuples.

The $n = 4$ case can be considered in the same way as the $n = 1$ case (see [12] and its references) and it is conjectured that there does not exist a $D(4)$-quintuple. The following is a stronger version of this conjecture.

Conjecture 1.1. ([10, Conjecture 1]) If \(\{a, b, c, d\}\) is a $D(4)$-quadruple with $a < b < c < d$, then $d = a + b + c + (abc + rst)/2$, where $r, s, t$ are positive integers defined by $ab + 4 = r^2$, $ac + 4 = s^2$, $bc + 4 = t^2$. 

42
In general, if \( n \equiv 2 \) (mod 4), then there does not exist a \( D(n) \)-quadruple ([3, 16, 19]). Dujella ([4]) showed that if \( n \not\equiv 2 \) (mod 4) and if \( n \not\in S := \{-4, -3, -1, 3, 5, 8, 12, 20\} \), then there exists at least one \( D(n) \)-quadruple, and conjectured the following.

**Conjecture 1.2.** ([5]) *There does not exist a \( D(n) \)-quadruple for \( n \in S \).*

There are several results supporting Conjecture 1.2 for the \( n = -1 \) case (see [8] and its references), and the validity of Conjecture 1.2 for \( n = -1 \) implies the one for \( n = -4 \) ([4, Remark 3]). For \( n \not\in \{\pm 1, \pm 4\} \), it is not easy to show either nonexistence or uniqueness of extension of a \( D(n) \)-triple, unless an argument using congruences modulo a power of 2 works. This is why we have to know the fundamental solutions of at least two of the Pell equations

\[
ay^2 - bx^2 = 1, \quad az^2 - cx^2 = 1, \quad bz^2 - cy^2 = 1.
\]

The first author ([13]) showed that the \( D(4k) \)-triple \( \{1, 4k(k-1), 4k^2 + 1\} \) with \( |k| \) prime cannot be extended to a \( D(4k) \)-quadruple. Moreover, he ([15]) proved that the \( D(\mp k^2) \)-triple \( \{k^2, k^2 \pm 1, 4k^2 \pm 1\} \) cannot be extended to a \( D(\mp k^2) \)-quintuple. In either case, \( ab \) and \( ac \) are of Richaud-Degert type ([20]), which gives the fundamental solutions of the corresponding Pell equations.

Furthermore, the Padé approximation method (a theorem of Bennett ([2]) or of Rickert ([21])) can work for the \( D(\pm k^2) \)-triple. Since \( D(\pm 4) \)-tuples have similar properties to \( D(\pm 1) \)-tuples as mentioned above, it is natural to ask whether the same is valid for \( D(\pm 4k^2) \)-tuples and \( D(\pm k^2) \)-tuples. This leads us to consider the \( D(\mp 4k^2) \)-triple \( \{k^2, k^2 \pm 4, 4k^2 \pm 4\} \).

Suppose that \( \{k^2, k^2 \pm 4, 4k^2 \pm 4, d\} \) is a \( D(\mp 4k^2) \)-quadruple. If \( k \) is even, say \( k = 2k' \), this is equivalent to that \( \{(k')^2, (k')^2 \pm 4, 4(k')^2 \pm 1, d'\} \) is a \( D(\mp (k')^2) \)-quadruple with some integer \( d' \). It follows from Theorems 1.4 and 1.5 in [15] that we may assume that \( k \) is odd. Then, since \( -4k^2 \equiv 12 \) (mod 16), the set \( \{k^2, k^2 \pm 4, 4k^2 \pm 4, d\} \) cannot be a \( D(-4k^2) \)-quadruple by Remark 3 in [4], stating that if \( \{a_1, a_2, a_3, a_4\} \) is a \( D(16l + 12) \)-quadruple with some integer \( l \), then every \( a_i \) is even. Therefore, the \( D(4k^2) \)-quadruple \( \{k^2 - 4, k^2, 4k^2 - 4, d\} \) with \( k \) odd is only to be considered. Our theorem in this paper is the following.

**Theorem 1.3.** *Let \( k \) be an integer greater than two. If \( \{k^2 - 4, k^2, 4k^2 - 4, d\} \) is a \( D(4k^2) \)-quadruple, then \( d = 4k^4 - 8k^2 \).*

Since Theorem 1.3 with \( k \) even follows immediately from Theorem 1.4 in [15], we will assume that \( k \) is odd throughout this paper.

The quadruple in Theorem 1.3 can be interpreted as the quadruple \( \{k^2 - 4, k^2, x_{1,0}, x_{2,0}\} \) in [4], where \( x_{n,m} \) and \( y_{n,m} \) are double sequences satisfying \( x_{n,0} = (y_{n,0}^2 - 4k^2)/(k^2 - 4) \) and \( y_{0,0} = 2k, \ y_{1,0} = 2k^2 - 4, \ y_{n+1,0} = ky_{n,0} - y_{n-1,0} \). Another interpretation of the quadruple is to regard it as an analogue of the quadruple in Conjecture 1.1. More generally, if \( \{a, k^2b, c\} \) is a \( D(4k^2) \)-triple, then \( \{a, k^2b, c, d\} \) is a \( D(4k^2) \)-quadruple with \( d = a + k^2b + c + (abc + rst)/2 \), where \( r, s, t \) are positive integers defined by \( ab + 4 = r^2 \), \( ac + 4k^2 = s^2 \), \( bc + 4 = t^2 \). Thus, Theorem 1.3 gives an example for which an analogue of Conjecture 1.1 holds. Note that this analogy does not hold in general. Filipin ([11, Theorem 3.10]) showed that if \( \{1, 20, 33, d\} \) is a \( D(16) \)-quadruple, then \( d = 105 \) or 273.

The organization of this paper is as follows. In Section 1, we transform the problem into a system of Diophantine equations, whose solution can be expressed as the intersection of two
recurrence sequences. The congruence method due to Dujella then gives a lower bound for the number of terms. In Section 3, the lower bound and the theorem of Bennett together yield \( k \leq 511 \). Finally, in Section 4 using the reduction method ([1, 9]) we arrive at a contradiction for each \( k \) with \( k \leq 511 \).

2 A lower bound for solutions

Let \( k \) be an odd integer greater than two. Suppose that \( \{k^2 - 4, k^2, 4k^2 - 4, d\} \) is a \( D(4k^2) \)-quadruple. Then, there exist positive integers \( x, y', z' \) such that

\[
(k^2 - 4)d + 4k^2 = x^2, \quad k^2d + 4k^2 = (y')^2, \quad (4k^2 - 4)d + 4k^2 = (z')^2. \tag{2.1}
\]

Clearly we have \( y' \equiv 0 \pmod{k} \) and \( z' \equiv 0 \pmod{2} \), which enable us to write \( y' = ky \) and \( z' = 2z \) with positive integers \( y \) and \( z \). Eliminating \( d \) from (2.1), we obtain the system of Diophantine equations

\[
x^2 - (k^2 - 4)y^2 = 16, \tag{2.2}
\]
\[
z^2 - (k^2 - 1)y^2 = 4 - 3k^2. \tag{2.3}
\]

Since \( k \) is odd, \( k^2 - 4 \equiv 5 \pmod{8} \). Hence, (2.2) implies that both \( x \) and \( y \) are even, say \( x = 2X \) and \( y = 2Y \). Then, (2.2) can be rewritten as \( X^2 - (k^2 - 4)Y^2 = 4 \). The positive solutions of this Pell equation have the form

\[
\frac{X + Y\sqrt{k^2 - 4}}{2} = \left( \frac{k + \sqrt{k^2 - 4}}{2} \right)^m
\]

and hence, the positive solutions of (2.2) have the form

\[
x + y\sqrt{k^2 - 4} = 4 \left( \frac{k + \sqrt{k^2 - 4}}{2} \right)^m \text{ with nonnegative integers } m. \tag{2.4}
\]

The positive solutions of (2.3) can be expressed as follows.

**Lemma 2.1.** Let \((z, y)\) be a positive solution of the Diophantine equation (2.3). Then, there exist a nonnegative integer \( n \) and a solution \((z_0, y_0)\) of (2.3) such that

\[
z + y\sqrt{k^2 - 1} = (z_0 + y_0\sqrt{k^2 - 1})(k + \sqrt{k^2 - 1})^n \tag{2.5}
\]

with

\[
|z_0| < \sqrt{\frac{3}{2} k^3}, \quad 0 < y_0 < \sqrt{2k}. \tag{2.6}
\]

**Proof.** We omit the proof, since it proceeds along the same lines as the proof of Lemma 1 in [6] or Lemma 3.1 in [15].

**Lemma 2.2.** If \( v_m = w_n \) has a solution, then \( m \) is odd, \( n \) is even and \( z_0 = \pm k, y_0 = 2 \).
Proof. By (2.4) and (2.5), we may write $y = v_m = w_n$, where
\[
v_0 = 0, \ v_1 = 2, \ v_{m+2} = kv_{m+1} - v_m
\]
and
\[
w_0 = y_0, \ w_1 = ky_0 + z_0, \ w_{n+2} = 2kw_{n+1} - w_n.
\]
Hence,
\[(v_m \pmod{2k})_{m \geq 0} = (0, 2, 0, -2, 0, 2, \ldots)\]
and
\[(w_n \pmod{2k})_{n \geq 0} = (y_0, ky_0 + z_0, -y_0, -ky_0 - z_0, y_0, \ldots).\]
Suppose that $v_m \equiv 0 \pmod{2k}$. Then either $y_0 \equiv 0 \pmod{2k}$ or $ky_0 + z_0 \equiv 0 \pmod{2k}$. By
(2.6), we must have $ky_0 + z_0 \equiv 0 \pmod{2k}$. Then, $z_0 \equiv 0 \pmod{k}$ implies $y_0^2 \equiv 4 \pmod{k^2}$.
It follows from (2.6) that $y_0^2 = 4$, which implies that $z_0$ is even. This contradicts (2.3). Hence, $m$
is odd and $v_m \equiv \pm 2 \pmod{2k}$. Then, either $y_0 \equiv \pm 2 \pmod{2k}$ or $ky_0 + z_0 \equiv \pm 2 \pmod{2k}$.
If $ky_0 + z_0 \equiv \pm 2 \pmod{2k}$, then $z_0 \equiv \pm 2 \pmod{k}$, say $z_0 = \alpha k \pm 2$, where $\alpha$ is an integer
with $|\alpha| < \sqrt{3k/2} + 2/k$ by (2.6). Thus, $y_0^2 \equiv \pm 4\alpha k \pmod{k^2}$ and by (2.6) we have $k^2 - 4|\alpha|k$.
If $k \geq 29$, then $y_0^2 = k^2 - 4|\alpha|k > 2k$, which contradicts (2.6). The only odd integers $k$ with
$3 \leq k \leq 27$ such that $(z_0, y_0)$ with $y_0$ odd is a solution of (2.3) satisfying (2.6) are 7 and 19, and
then $(z_0, y_0) = (17, 3)$ and $(89, 5)$, respectively (note that $y_0$ must be odd, since $y_0$ and $z_0$ now
have the same parity and $z_0$ is odd). However, in either case $z_0 \pm 2 \not\equiv 0 \pmod{k}$, that is, $z_0$ is
not of the form $\alpha k \pm 2$. Therefore, $n$ is even and $y_0 \equiv \pm 2 \pmod{2k}$. It follows from (2.6) that
$y_0 = 2$ and $z_0 = \pm k$.

Now one can easily obtain the following three lemmas in the same ways as Lemmas 4.2 to 4.4 in [15].

Lemma 2.3. If $v_m = w_n$ has a solution with $n \geq 2$ in the case of $z_0 = k$ or with $n \geq 6$ in the
case of $z_0 = -k$, then $n \geq 2k^2 - 6$.

Lemma 2.4. If $y = w_n$, then $\log y > (n - 1) \log(1.942k)$.

Lemma 2.5. If $v_m = w_n$ has a solution with $n \neq 0$, then $m > n$. Moreover, if $k \geq 5$, then
$m \leq 2n$; if $k = 3$, then $m \leq 3n$.

3 Application of a theorem of Bennett

Let $\theta_1 = \sqrt{1 - 4/k^2}$ and $\theta_2 = \sqrt{1 - 1/k^2}$. Then, a theorem ([2, Theorem 3.2]) of Bennett can
be applied if $k^2 \geq \max\{4^9, 1^9\}$, that is, $k > 512$.

Theorem 3.1. If $k > 512$, then the numbers $\theta_1$ and $\theta_2$ satisfy
\[
\max\left\{\frac{\theta_1 - p_1}{q}, \frac{\theta_2 - p_2}{q}\right\} > (2680k^2)^{-1}q^{-\lambda}
\]
for all integers $p_1, p_2, q$ with $q > 0$, where
\[
\lambda = 1 + \frac{\log(660k^2)}{\log(0.0116k^4)} < 2.
\]
The following lemma is similar to Lemma 3.6 in [15].

**Lemma 3.2.** All positive solutions of the system of Diophantine equations (2.2) and (2.3) satisfy
\[
\max \left\{ \left| \frac{\theta_1 - x}{ky} \right|, \left| \frac{\theta_2 - z}{ky} \right| \right\} < \frac{2.2}{y^2}.
\]

Combining Theorem 3.1 and Lemma 3.2, one can bound \( \log y \) above in terms of \( k \).

**Lemma 3.3.** Suppose that \( \{k^2 - 4, k^4, 4k^2 - 4, d\} \) is a \( D(4k^2) \)-quadruple with \( k > 512 \). Then,
\[
\log y < \frac{8\log(8.77k)\log(0.329k)}{\log(0.00419k)}.
\]

**Proof.** Applying Theorem 3.1 with \( p_1 = x, p_2 = z, q = ky \), we see from Lemma 3.2 that
\[
(2680k^2)^{-1}(ky)^{-\lambda} < \frac{2.2}{y^2}.
\]
Noting \( \lambda < 2 \), one can easily see that the desired inequality holds. \( \square \)

**Proposition 3.4.** Suppose that \( \{k^2 - 4, k^2, 4k^2 - 4, d\} \) is a \( D(4k^2) \)-quadruple with \( d \neq 4k^4 - 8k^2 \). Then, \( k \leq 511 \).

**Proof.** If \( n = 0 \), then \( d = 0 \), which cannot be an element in a \( D(4k^2) \)-quadruple. If \( n = 2 \) with \( z_0 = -k \), then \( d = 4k^4 - 8k^2 \). Denoting \( w_4 \) with \( z_0 = -k \) by \( w_4^- \), we easily see that
\[
v_5 < w_4^- < v_7;
\]
indeed, \( w_4^- = 8k^4 - 12k^2 + 2 \), \( v_5 = 2k^4 - 6k^2 + 2 \), \( v_7 = 2k^6 - 10k^4 + 12k^2 - 2 \). Since \( m \) is odd and \( n \) is even by Lemma 2.2, we may apply Lemma 2.3. Suppose that \( k \geq 513 \). Then, Lemmas 2.3, 2.4 and 3.3 together imply that
\[
\frac{2k^2 - 7}{8} < \frac{\log(8.77k)\log(0.329k)}{\log(1.942k)\log(0.00419k)} =: f(k).
\]
Since \( f(k) \) is a decreasing function for \( k \geq 513 \), we have \( f(k) \leq f(513) < 9 \), which contradicts (3.1). \( \square \)

### 4 The reduction method

By the standard method (see, e.g., [15, Lemma 3.9]), the following estimate on the linear form in three logarithms is obtained.

**Lemma 4.1.** If \( v_m = w_n \) has a solution with \( n \neq 0 \), then
\[
0 < m \log \alpha_1 - n \log \alpha_2 + \log \alpha_3 < 10\alpha_2^{-m'}, \tag{4.1}
\]
where
\[
\alpha_1 = \frac{k + \sqrt{k^2 - 4}}{2}, \quad \alpha_2 = k + \sqrt{k^2 - 1}, \quad \alpha_3 = \frac{4\sqrt{k^2 - 1}}{\sqrt{k^2 - 4(2\sqrt{k^2 - 1} \pm k)}},
\]
and \( m' = m \) if \( k \geq 5 \); \( m' = 2m/3 \) if \( k = 3 \).
The following theorem of Matveev gives an upper bound for $m$.

**Theorem 4.2.** ([18]) Let $\Lambda$ be a linear form in logarithms of $l$ multiplicatively independent totally real algebraic numbers $\alpha_1, \ldots, \alpha_l$ with rational integer coefficients $b_1, \ldots, b_l$ ($b_i \neq 0$). Let $h(\alpha_j)$ denote the absolute logarithmic height of $\alpha_j$ for $1 \leq j \leq l$. Define the numbers $D, A_j (1 \leq j \leq l)$ and $B$ by $D = [\mathbb{Q}(\alpha_1, \ldots, \alpha_l) : \mathbb{Q}], A_j = \max\{ Dh(\alpha_j), |\log \alpha_j|\}, B = \max\{1, \max\{|b_j|A_j/A_i; 1 \leq j \leq l\}\}$. Then,

$$\log |\Lambda| > -C(l)C_0W_0D^2\Omega,$$

where

$$C(l) = \frac{8}{(l-1)!}(l+2)(2l+3)(4e(l+1))^{l+1},$$

$$C_0 = \log(e^{4.4l^7}l^{5.5}D^2\log(eD)),$$

$$W_0 = \log(1.5eBD\log(eD)), \quad \Omega = A_1 \cdots A_l.$$

**Proposition 4.3.** Suppose that $\{k^2 - 4, k^2, 4k^2 - 4, d\}$ is a $D(4k^2)$-quadruple. Then $m < 10^{17}$.

**Proof.** We apply Theorem 4.2 with $l = 3$, $D = 4$, $b_1 = m$, $b_2 = -n$, $b_3 = 1$. We have $A_1 = 2\log \alpha_1 < 2\log k$ and $A_2 = 2\log \alpha_2 < 2\log(2k)$. Since the minimal polynomial of $\alpha_3$ over $\mathbb{Z}$ is

$$(k^2 - 4)^2(3k^2 - 4)^2X^4 - 32(k^2 - 1)(k^2 - 4)(5k^2 - 4)X^2 + 256(k^2 - 1)^2$$

up to a multiple of a constant, and $\gcd((k^2 - 4)(3k^2 - 4), 16(k^2 - 1))$ divides 3, the leading coefficient $a_0$ of the minimal polynomial of $\alpha_3$ over $\mathbb{Z}$ satisfies

$$\frac{(k^2 - 4)^2(3k^2 - 4)^2}{9} \leq a_0 \leq (k^2 - 4)^2(3k^2 - 4)^2.$$

Since $\alpha_3$ with the minus sign is less than 1.91 and $\alpha_3$ with the plus sign is less than 1, we have

$$A_3 = 4h(\alpha_3) < \log(1.91^2(k^2 - 4)^2(3k^2 - 4)^2) < 8\log(1.55k),$$

$$A_3 > \log\left(\frac{(k^2 - 4)^2(3k^2 - 4)^2}{9}\right) > 8\log(0.829k).$$

Hence, we obtain the following:

$$B < \max\left\{\frac{2m\log k}{8\log(0.829k)}, \frac{2n\log(2k)}{8\log(0.829k)}\right\} < \frac{m\log(2k)}{4\log(0.829k)} < 0.5m,$$

$$C(3) = \frac{8}{2!} \cdot 5 \cdot 9(16e)^4 < 6.45 \cdot 10^8,$$

$$C_0 = \log\left(e^{4.4+7}3^{5.5}16\log(4e)\right) < 29.9,$$

$$W_0 = \log(1.5eBD\log(4e)) < \log(20m),$$

$$\Omega = A_1A_2A_3 < 32\log(k)\log(2k)\log(1.55k) < 73.1(\log k)^3.$$
Assume that \( m \geq 10 \). Since \( \log(10\alpha_1^{-m'}) < -m' \log k \), we see from Lemma 4.1 that

\[
2.3 \cdot 10^{13} (\log k)^2 > \frac{m'}{\log(20m)} =: F(m).
\]

By Proposition 3.4, we have \( F(m) < 2.3 \cdot 10^{13} (\log(511))^2 < 9 \cdot 10^{14} \). Since \( F(m) \) is increasing and \( F(10^{17}) > 10^{15} \), we obtain \( m < 10^{17} \).

\[ \square \]

**Proof of Theorem 1.3.** Dividing (4.1) by \( \log \alpha_2 \), we have

\[
0 < m\kappa - n + \mu < AB^{-m},
\]

where

\[
\kappa = \frac{\log \alpha_1}{\log \alpha_2}, \quad \mu = \frac{\log \alpha_3}{\log \alpha_2}, \quad A = \frac{10}{\log \alpha_2}, \quad B = \alpha_2 \ (k \geq 5) \text{ or } \alpha_2^{2/3} \ (k = 3).
\]

**Lemma 4.4.** ([9, Lemma 5 a]) Let \( M \) be a positive integer and \( p/q \) a convergent of the continued fraction expansion of \( \kappa \) such that \( q > 6M \). Put \( \epsilon = ||\mu q|| - M||\kappa q|| \), where \( || \cdot || \) denotes the distance from the nearest integer. If \( \epsilon > 0 \), then the inequality (4.2) has no solution in the range

\[
\frac{\log(Aq/\epsilon)}{\log B} \leq m \leq M.
\]

As seen at the beginning in the proof of Proposition 3.4, we may assume that \( n \geq 4 \) for \( z_0 = k \) and \( n \geq 6 \) for \( z_0 = -k \). We can thus use Lemma 2.3, which implies \( n \geq 2k^2 - 6 \). We apply Lemma 4.4 with \( M = 10^{17} \) for odd \( k \) with \( 3 \leq k \leq 511 \) and for each sign of \( \alpha_3 \). For \( 5 \leq k \leq 511 \), the second convergent is needed in 2 cases and the third convergent is needed in 2 cases. In any case, the first step of reduction gives \( m \leq 21 \), which contradicts Lemma 2.3 with \( k \geq 5 \). For \( k = 3 \), the first step of reduction gives \( m \leq 40 \) and the second step gives \( m \leq 10 \) (the second convergent is needed only in the first step for the minus sign of \( \alpha_3 \)). This contradicts Lemma 2.3 with \( k = 3 \), and completes the proof of Theorem 1.3.

\[ \square \]

**References**


