ACTA ARITHMETICA
LXV.1 (1993)

Generalization of a problem of Diophantus

by

ANDREJ DUJELLA (Zagreb)

1. Introduction. The Greek mathematician Diophantus of Alexandria noted that the numbers $\frac{1}{16}$, $\frac{33}{16}$, $\frac{68}{16}$ and $\frac{105}{16}$ have the property that the product of any two of them when increased by 1 is a square of a rational number.

Let n be an integer. We say the set of natural numbers $\{a_1, \ldots, a_m\}$ has the *property of Diophantus of order* n, in brief $D(n)$, if for all $i, j = 1, \ldots, m$, $i \neq j$, the following holds: $a_i a_j + n = b_{ij}^2$, where b_{ij} is an integer. The first set of four natural numbers with property $D(1)$ was found by the French mathematician Pierre de Fermat (1601–1665). That set is $\{1, 3, 8, 120\}$. Davenport and Baker [3] show that one cannot add a fifth integer r to that set and maintain the same property unless $r = 0$. For the rational number $r = \frac{777480}{8288641}$ the product of any two different members of that set increased by 1 is the square of a rational number (see [1]).

In this paper we consider some problems of existence of sets of four natural numbers with property $D(n)$, for any integer n. We prove that, for all $e \in \mathbb{Z}$, there exist an infinite number of sets of four natural numbers with property $D(e^2)$. Indeed, we show how a set $\{a, b\}$ with property $D(e^2)$ can be extended to a set $\{a, b, c, d\}$ with the same property, if ab is not a perfect square. That construction is applied to the identities

$$(k-e)(k+e) + e^2 = k^2 ,$$
$$F_{2n} F_{2n+2m} + F_m^2 = F_{2n+m}^2 ,$$

and some formulas are obtained for sets of four numbers with the property of Diophantus. The general case is also considered: sets with property $D(n)$ when n need not be a perfect square. The main results are:

If n is an integer of the form $n = 4k+2$, $k \in \mathbb{Z}$, then there does not exist a set of four natural numbers with property $D(n)$.

If n is an integer which is not of the form $4k+2$ and $n \notin S = \{3, 5, 8, 12, 20, -1, -3, -4\}$ then there exists at least one set of four natural numbers with property $D(n)$.

2. Sets of four numbers with property $D(e^2)$**.** Let $a, b \in \mathbb{N}$, $a < b$, such that the set $\{a, b\}$ has property $D(e^2)$, i.e. $ab + e^2 = k^2$, $k \in \mathbb{N}$. Now we want to find a natural number x such that $\{a, b, x\}$ also has property $D(e^2)$. Thus, the following must hold:

$$ax + e^2 = y^2 , \qquad bx + e^2 = z^2 . \tag{1}$$

This implies

$$by^2 - az^2 = e^2(b - a) . \tag{2}$$

It is obvious that one solution of this Diophantine equation is $y = e$, $z = e$ and it is easy to verify that $y = k \pm a$, $z = k \pm b$ are also solutions of (2).

Now assume that ab is not a perfect square. Consider the Pellian equation $S^2 - abT^2 = 1$. Under the above assumption it has an infinite number of solutions in natural numbers. Let s and t be the least solutions of that equation in natural numbers. (You can see how to find the minimal solution of $S^2 - pT^2 = 1$ in [2].)

Let us now define two double sequences $y_{n,m}$ and $z_{n,m}$, $n, m \in \mathbb{Z}$, as follows:

$$y_{0,0} = e, \quad z_{0,0} = e, \quad y_{1,0} = k + a, \quad z_{1,0} = k + b ,$$
$$y_{-1,0} = k - a, \quad z_{-1,0} = k - b ,$$
$$y_{n+1,0} = \frac{2k}{e} y_{n,0} - y_{n-1,0}, \quad z_{n+1,0} = \frac{2k}{e} z_{n,0} - z_{n-1,0}, \quad n \in \mathbb{Z} ,$$
$$y_{n,1} = sy_{n,0} + atz_{n,0}, \quad z_{n,1} = bty_{n,0} + sz_{n,0}, \quad n \in \mathbb{Z} ,$$
$$y_{n,m+1} = 2sy_{n,m} - y_{n,m-1}, \quad z_{n,m+1} = 2sz_{n,m} - z_{n,m-1}, \quad n, m \in \mathbb{Z} .$$

THEOREM 1.

$$by_{n,m}^2 - az_{n,m}^2 = e^2(b - a), \quad \textit{for all } n, m \in \mathbb{Z} .$$

LEMMA 1.

$$by_{n,0}^2 - az_{n,0}^2 = e^2(b - a) , \tag{3}$$
$$by_{n,0}y_{n-1,0} - az_{n,0}z_{n-1,0} = ek(b - a), \quad \textit{for all } n \in \mathbb{Z} . \tag{4}$$

Proof. We prove the lemma by induction. Let $n \geq 0$. For $n = 0$ and $n = 1$ relation (3) is obviously valid. If $n = 0$ is substituted in (4), we obtain

$$by_{0,0}y_{0,-1} - az_{0,0}z_{0,-1} = be(k - a) - ae(k - b) = ek(b - a) ,$$

and if $n = 1$,

$$by_{1,0}y_{0,0} - az_{1,0}z_{0,0} = be(k + a) - ae(k + b) = ek(b - a) .$$

Assume that the assertion of the lemma is valid for all integers n, $0 \leq n < m$,

$m \geq 2$. Now we get

$$\begin{aligned}
&by_{m,0}y_{m-1,0} - az_{m,0}z_{m-1,0} \\
&\qquad = by_{m-1,0}\bigg(\frac{2k}{e}y_{m-1,0} - y_{m-2,0}\bigg) - az_{m-1,0}\bigg(\frac{2k}{e}z_{m-1,0} - z_{m-2,0}\bigg) \\
&\qquad = \frac{2k}{e}(by_{m-1,0}^2 - az_{m-1,0}^2) - (by_{m-1,0}y_{m-2,0} - az_{m-1,0}z_{m-2,0}) \\
&\qquad = \frac{2k}{e}e^2(b-a) - ek(b-a) = ek(b-a) \qquad \text{(by assumption)}\,.
\end{aligned}$$

Also

$$\begin{aligned}
&by_{m,0}^2 - az_{m,0}^2 \\
&\quad = b\bigg(\frac{2k}{e}y_{m-1,0} - y_{m-2,0}\bigg)^2 - a\bigg(\frac{2k}{e}z_{m-1,0} - z_{m-2,0}\bigg)^2 \\
&\quad = \frac{4k^2}{e^2}(by_{m-1,0}^2 - az_{m-1,0}^2) + (by_{m-2,0}^2 - az_{m-2,0}^2) \\
&\qquad - \frac{4k}{e}(by_{m-1,0}y_{m-2,0} - az_{m-1,0}z_{m-2,0}) \\
&\quad = 4k^2(b-a) + e^2(b-a) - 4k^2(b-a) = e^2(b-a) \qquad \text{(by assumption)}.
\end{aligned}$$

The assertion is thus proved for $n \geq 0$. For $n \leq 0$, the proof is completely analogous. ∎

LEMMA 2. *For $n \in \mathbb{Z}$ and $m \in \mathbb{N} \cup \{0\}$,*

$$y_{n,m+1} = sy_{n,m} + atz_{n,m}, \qquad z_{n,m+1} = bty_{n,m} + sz_{n,m}\,.$$

Proof. We proceed by induction on m. For $m = 0$, the assertion is a consequence of the definition of $y_{n,1}$ and $z_{n,1}$. Let n be a fixed integer. Assume that the assertion is valid for some $m \in \mathbb{N} \cup \{0\}$. Then

$$\begin{aligned}
y_{n,m+2} &= 2sy_{n,m+1} - y_{n,m} = sy_{n,m+1} + s^2y_{n,m} + astz_{n,m} - y_{n,m} \\
&= sy_{n,m+1} + abt^2y_{n,m} + astz_{n,m} = sy_{n,m+1} + astz_{n,m+1}\,.
\end{aligned}$$

Similarly

$$z_{n,m+2} = sz_{n,m+1} + bty_{n,m+1}\,. \;\blacksquare$$

Proof of Theorem 1. Let n be a fixed integer. We prove the theorem by induction on m, first for $m \geq 0$. For $m = 0$ the assertion follows from Lemma 1. Assume that the hypothesis of Theorem 1 is true for some $m \geq 0$.

Then, by Lemma 2,

$$\begin{aligned} by_{n,m+1}^2 - az_{n,m+1}^2 &= b(sy_{n,m} + atz_{n,m})^2 - a(bty_{n,m} + sz_{n,m})^2 \\ &= s^2(by_{n,m}^2 - az_{n,m}^2) - abt^2(by_{n,m}^2 - az_{n,m}^2) \\ &= (s^2 - abt^2)(by_{n,m}^2 - az_{n,m}^2) = e^2(b-a)\,. \end{aligned}$$

So, the theorem is proved in case $m \geq 0$. The proof in case $m \leq 0$ is analogous. We use the relations

$$y_{n,m-1} = sy_{n,m} - atz_{n,m}, \qquad z_{n,m-1} = sz_{n,m} - bty_{n,m}\,,$$

which easily follow from Lemma 2. ■

By Theorem 1, the numbers $x_{n,m} = (y_{n,m}^2 - e^2)/a$ satisfy (1) for all $n, m \in \mathbb{Z}$.

Theorem 2.

$$x_{n,m}x_{n+1,m} + e^2 = \left(\frac{y_{n+1,m}y_{n,m} + ek}{a}\right)^2, \qquad \textit{for all } n, m \in \mathbb{Z}\,.$$

Lemma 3. *For every integer m the following hold*:

$$\begin{aligned} y_{0,m}^2 - y_{1,m}y_{-1,m} &= a^2 + e^2 - k^2\,, \\ 2y_{0,m}y_{0,m-1} - y_{-1,m}y_{1,m-1} - y_{1,m}y_{-1,m-1} &= 2s(a^2 + e^2 - k^2)\,. \end{aligned}$$

Proof. We proceed by induction for $m \geq 0$. The proof for $m \leq 0$ is analogous. For $m = 0$ we get

$$y_{0,0}^2 - y_{1,0}y_{-1,0} = e^2 - (k+a)(k-a) = a^2 + e^2 - k^2$$

and

$$\begin{aligned} &2y_{0,0}y_{0,-1} - y_{-1,0}y_{1,-1} - y_{1,0}y_{-1,-1} \\ &\qquad = 2e(se - ate) - (k-a)[s(k+a) - at(k+b)] \\ &\qquad\quad - (k+a)[s(k-a) - at(k-b)] \\ &\qquad = 2se^2 - 2ate^2 - sk^2 + sa^2 + atk^2 + abtk - a^2tk - a^2bt \\ &\qquad\quad - sk^2 + sa^2 + atk^2 - abtk + a^2tk - a^2bt \\ &\qquad = 2s(e^2 - k^2 + a^2) + 2at(k^2 - e^2 - ab) \\ &\qquad = 2s(a^2 + e^2 - k^2)\,, \end{aligned}$$

and for $m = 1$,

$$\begin{aligned} &y_{0,1}^2 - y_{1,1}y_{-1,1} \\ &\qquad = (se + ate)^2 - [s(k+a) - at(k+b)][s(k-a) + at(k-b)] \end{aligned}$$

$$
\begin{aligned}
&= s^2e^2 + 2aste^2 + a^2t^2e^2 - s^2k^2 + s^2a^2 - a^2t^2k^2 - 2astk^2 + 2a^2bst \\
&= 2ast(e^2 - k^2 + ab) + (s^2 + a^2t^2)(e^2 - k^2) + s^2a^2 + a^2t^2b^2 \\
&= s^2a^2 + a^2t^2b^2 - s^2ab - a^3bt^2 = (a^2 - ab)(s^2 - abt^2) \\
&= a^2 + e^2 - k^2 \,.
\end{aligned}
$$

Now assume that the assertion of the lemma is true for all nonnegative integers which are less than or equal to m. Then

$$
\begin{aligned}
&2y_{0,m+1}y_{0,m} - y_{-1,m+1}y_{1,m} - y_{1,m+1}y_{-1,m} \\
&\qquad = 2y_{0,m}(2sy_{0,m} - y_{0,m-1}) - y_{1,m}(2sy_{-1,m} - y_{-1,m-1}) \\
&\qquad\quad - y_{-1,m}(2sy_{1,m} - y_{1,m-1}) \\
&\qquad = 4s(y_{0,m}^2 - y_{1,m}y_{-1,m}) \\
&\qquad\quad - (2y_{0,m}y_{0,m-1} - y_{1,m}y_{-1,m-1} - y_{-1,m}y_{1,m-1}) \\
&\qquad = 4s(a^2 + e^2 - k^2) - 2s(a^2 + e^2 - k^2) \\
&\qquad = 2s(a^2 + e^2 - k^2) \,.
\end{aligned}
$$

Also,

$$
\begin{aligned}
&y_{0,m+1}^2 - y_{1,m+1}y_{-1,m+1} \\
&\quad = (2sy_{0,m} - y_{0,m-1})^2 - (2sy_{1,m} - y_{1,m-1})(2sy_{-1,m} - y_{-1,m-1}) \\
&\quad = 4s^2(y_{0,m}^2 - y_{1,m}y_{-1,m}) + (y_{0,m-1}^2 - y_{1,m-1}y_{-1,m-1}) \\
&\qquad - 2s(2y_{0,m}y_{0,m-1} - y_{1,m}y_{-1,m-1} - y_{1,m-1}y_{-1,m}) \\
&\quad = (a^2 + e^2 - k^2)(4s^2 - 2s \cdot 2s + 1) \\
&\quad = a^2 + e^2 - k^2 \,,
\end{aligned}
$$

which completes the proof. ■

Proof of Theorem 2. By definition it follows by induction that

$$
y_{n+1,m} = \frac{2k}{e}y_{n,m} - y_{n-1,m}, \qquad \text{for } n, m \in \mathbb{Z} \,.
$$

Since

$$
\begin{aligned}
&y_{n+1,m}^2 - y_{n,m}y_{n+2,m} - (y_{n,m}^2 - y_{n-1,m}y_{n+1,m}) \\
&\qquad = y_{n+1,m}(y_{n+1,m} + y_{n-1,m}) - y_{n,m}(y_{n+2,m} + y_{n,m}) \\
&\qquad = \frac{2k}{e}y_{n+1,m}y_{n,m} - \frac{2k}{e}y_{n,m}y_{n+1,m} = 0 \,,
\end{aligned}
$$

we get

$$y_{n+1,m}^2 - y_{n,m}y_{n+2,m} = y_{0,m}^2 - y_{1,m}y_{-1,m} = a^2 + e^2 - k^2\,,$$

for $n, m \in \mathbb{Z}$. Therefore

$$\begin{aligned}
x_{n,m}x_{n+1,m} + e^2 &= [(y_{n,m}^2 - e^2)(y_{n+1,m} - e^2) + a^2e^2]/a^2 \\
&= [y_{n,m}^2 y_{n+1,m}^2 - e^2 y_{n,m}^2 - e^2 y_{n+1,m}^2 + e^2(a^2 + e^2)]/a^2 \\
&= [y_{n,m}^2 y_{n+1,m}^2 - e^2 y_{n,m}^2 - e^2 y_{n+1,m}^2 \\
&\quad + e^2(y_{n+1,m}^2 - y_{n,m}y_{n+2,m} + k^2)]/a^2 \\
&= [y_{n,m}^2 y_{n+1,m}^2 - e^2 y_{n,m}(y_{n,m} + y_{n+2,m}) + e^2k^2]/a^2 \\
&= (y_{n,m}^2 y_{n+1,m}^2 - 2eky_{n,m}y_{n+1,m} + e^2k^2)/a^2 \\
&= \left(\frac{y_{n,m}y_{n+1,m} - ek}{a}\right)^2 . \ \blacksquare
\end{aligned}$$

Now we consider the problem of existence of natural numbers in the sequence $x_{n,m}$. We have

$$\begin{aligned}
(5) \qquad x_{n,m+1} - x_{n,m} &= \frac{y_{n,m+1}^2 - e^2}{a} - \frac{y_{n,m} - e^2}{a} \\
&= [(sy_{n,m} + atz_{n,m})^2 - y_{n,m}^2]/a \\
&= [(s^2 - 1)y_{n,m}^2 + 2asty_{n,m}z_{n,m} + a^2t^2z_{n,m}^2]/a \\
&= bt^2y_{n,m}^2 + 2sty_{n,m}z_{n,m} + at^2z_{n,m}^2 \,.
\end{aligned}$$

Since $y_{i,m}$ and $z_{i,m}$, for $i = -1, 0, 1$, are integers by definition and $x_{-1,0} = a + b - 2k \in \mathbb{Z}$, $x_{0,0} = 0 \in \mathbb{Z}$, $x_{1,0} = a + b + 2k \in \mathbb{Z}$, we conclude from (5) that $x_{-1,m}$, $x_{0,m}$ and $x_{1,m}$ are integers for all $m \in \mathbb{Z}$. Furthermore,

$$\begin{aligned}
(6) \qquad & x_{n,m+3} - x_{n,m} \\
&= \frac{1}{a}(y_{n,m+3} + y_{n,m})(y_{n,m+3} - y_{n,m}) \\
&= \frac{1}{a}(2s - 1)(y_{n,m+2} + y_{n,m+1})(2s + 1)(y_{n,m+2} - y_{n,m+1}) \\
&= (4s^2 - 1)(x_{n,m+2} - x_{n,m+1})\,.
\end{aligned}$$

Since $y_{0,1} = e(s+at) > e$ and $y_{0,-1} = e(s-at) > e$, we see that $x_{0,1} > 0$ and $x_{0,-1} > 0$. From this fact, relation (6) and $s \geq 2$, we deduce by induction that $x_{0,m+1} \geq (4s^2 - 3)x_{0,m}$ for $m > 0$, and $x_{0,m-1} \geq (4s^2 - 3)x_{0,m}$ for $m < 0$. Therefore $x_{0,m} > 0$ for $m \neq 0$. Likewise, using the inequalities $tk \geq s$, $(a + b)t \geq 2s$, and $s(k + a) \geq at(k + b)$, we obtain $x_{-1,m} > 0$ for $m \notin \{0, 1\}$ and $x_{1,m} > 0$ for $m \neq -1$. Hence, it follows from Theorem 2 that the sets $\{a, b, x_{1,m}, x_{0,m}\}$, $m \in \mathbb{Z} \setminus \{0, 1\}$, and $\{a, b, x_{0,m}, x_{-1,m}\}$, $m \in \mathbb{Z} \setminus \{-1, 0\}$, have property $D(e^2)$.

Remark 1. Let s' and t' be the least solutions of the equation $S^2 - abT^2 = 4$ in natural numbers. If we define

$$\begin{aligned} y'_{n,0} &= y_{n,0}, \quad & z'_{n,0} &= z_{n,0}\,, \\ y'_{n,1} &= (s'y_{n,0} + at'z_{n,0})/2, \quad & z'_{n,1} &= (bt'y_{n,0} + s'z_{n,0})/2\,, \\ y'_{n,m+1} &= s'y'_{n,m} - y'_{n,m-1}, \quad & z'_{n,m+1} &= s'z'_{n,m} - z'_{n,m-1}\,, \end{aligned}$$

then the assertions of Theorems 1 and 2 hold for the sequences $y'_{n,m}$, $z'_{n,m}$. If t' is even, the sequences $y'_{n,m}$, $z'_{n,m}$ are identical to $y_{n,m}$, $z_{n,m}$. Otherwise, these modified sequences give us some solutions which cannot be obtained by means of $y_{n,m}$, $z_{n,m}$.

Remark 2. If ab is a perfect square then there exist natural numbers p, q, r such that $a = pq^2$, $b = pr^2$. So, equation (2) can be represented in the form

$$(qy)^2 - (rz)^2 = e^2(q^2 - r^2)\,.$$

It is obvious that this equation has at most a finite number of integer solutions, which means that there exist only finitely many sets $\{a, b, c, d\}$ with property $D(e^2)$. For some values of a, b and e (e.g. $a = 2$, $b = 8$, $e = 3$) that set does not exist at all, unless we allow 0 to be a member of the set.

Example 1.

$$1 \cdot 7 + 3^2 = 4^2\,.$$

In this case, $x_{-2,m}, x_{-1,m}, x_{0,m}, x_{1,m} \in \mathbb{Z}$ and the following sets have property $D(9)$:

$$\{1, 7, 40, 216\}, \qquad \{1, 7, 216, 1080\},$$
$$\{1, 7, 1080, 5320\}, \qquad \{1, 7, 11440, 56160\}, \quad \ldots$$

Example 2.

$$1 \cdot 13 + 6^2 = 7^2\,.$$

Also, $x_{-2,m}, x_{-1,m}, x_{0,m}, x_{1,m} \in \mathbb{Z}$ and the least solution obtained by our construction is $\{1, 13, 2534428, 79188560\}$. The least solution of the equation $S^2 - 13T^2 = 1$ is $649^2 - 13 \cdot 180^2 = 1$. If Remark 1 and the equality $11^2 - 13 \cdot 3^2 = 4$ are used, then we get some other sets with property $D(36)$, e.g.

$$\{1, 13, 160, 540\}, \qquad \{1, 13, 540, 1728\},$$
$$\{1, 13, 1728, 5440\}, \qquad \{1, 13, 21280, 66528\}, \quad \ldots$$

3. Cases $e = 1$ and $e = 2$. If $e = 1$ then all the $x_{n,m}$ are integers. Indeed, $x_{0,0} = 0 \in \mathbb{Z}$, $x_{1,0} = a + b + 2k \in \mathbb{Z}$, $x_{-1,0} = a + b - 2k \in \mathbb{Z}$ and

$$x_{n+3,0} = (4k^2 - 1)(x_{n+2,0} - x_{n+1,0}) + x_{n,0}$$

(see the proof of relation (6)). Hence, $x_{n,0} \in \mathbb{Z}$ for all $n \in \mathbb{Z}$. In fact, $x_{n,0} \in \mathbb{N}$ for $n \in \mathbb{Z} \setminus \{0, -1\}$. Note that in this case $s = k$ and $t = 1$. The relation

$x_{n,m} = x_{n+m,0}$, $n, m \in \mathbb{Z}$, which is easy to prove by induction, implies that $x_{n,m} \in \mathbb{Z}$ for all $n, m \in \mathbb{Z}$.

Example 3.

$$1 \cdot 3 + 1^2 = 2^2 \,.$$

We have $a = 1$, $b = 3$, $k = 2$; $x_{0,0} = 0$, $x_{1,0} = 8$, $x_{-1,0} = 0$ and $x_{n+3,0} = 15(x_{n+2,0} - x_{n+1,0}) + x_{n,0}$. Thus, $x_{2,0} = 120$, $x_{3,0} = 1680$, $x_{4,0} = 23408, \ldots$ Hence, the sets $\{1, 3, 8, 120\}$, $\{1, 3, 120, 1680\}$ and $\{1, 3, 1680, 23408\}$ have property $D(1)$.

If $e = 2$ then all the $x_{n,m}$ are also integers. This follows from the relation

$$x_{n+3,0} = (k^2 - 1)(x_{n+2,0} - x_{n+1,0}) + x_{n,0} \,.$$

We are also able to obtain $y'_{n,m} = y_{n+m,0}$ by applying the construction from Remark 1. Consequently, we see that the use of double sequences was unnecessary in the cases $e = 1$ and $e = 2$.

Example 4.

$$1 \cdot 5 + 2^2 = 3^2 \,.$$

By the above construction, we obtain the following sequence of sets with property $D(4)$:

$$\{1, 5, 12, 96\}, \quad \{1, 5, 96, 672\}, \quad \{1, 5, 672, 4620\}, \quad \ldots$$

4. Connection with polynomials and with Fibonacci numbers. We will now apply our construction to the identity

$$(k - e)(k + e) + e^2 = k^2 \,.$$

We have $a = k - e$, $b = k + e$; $x_{0,0} = 0$, $x_{-1,0} = 0$, $x_{1,0} = 4k$.

For $e = 1$ we obtain a sequence of solutions:

$$\{k-1, k+1, 4k, 16k^3 - 4k\}, \quad \{k-1, k+1, 16k^3 - 4k, 64k^5 - 48k^3 + 8k\}, \quad \ldots$$

Jones (in [6]) showed that there is no set of five polynomials with the above property. But there are some other sets of four polynomials with property $D(1)$, e.g. $\{k + 1, 4k + 8, 9k + 15, 144k^3 + 672k^2 + 1036k + 528\}$.

For $e = 2$ we also obtain a sequence of solutions:

$$\{k - 2, k + 2, 4k, 4k^3 - 4k\}, \quad \{k - 2, k + 2, 4k^3 - 4k, 4k^5 - 12k^3 + 8k\}, \quad \ldots$$

Moreover, $\{k - 4, k + 4, 4k, k^3 - 4k\}$ has property $D(16)$ for all $k \geq 5$.

Consider now the Fibonacci numbers F_n, i.e. $F_1 = 1$, $F_2 = 1$, $F_{n+2} = F_{n+1} + F_n$, $n \in \mathbb{N}$. The following relation is valid:

$$F_{2n}F_{2n+2m} + F_m^2 = F_{2n+m}^2$$

(see [8], p. 28). By applying our construction to this identity, we get $e = F_m$, $a = F_{2n}$, $b = F_{2n+2m}$, $k = F_{2n+m}$. By taking $m = 1, 2, 3, 4, 6$ and using the properties of Fibonacci and Lucas numbers ($L_n = F_{n-1} + F_{n+1}$), we obtain

Theorem 3. *For all natural numbers n, the sets $\{F_{2n}, F_{2n+2}, F_{2n+4}, 4F_{2n+1}F_{2n+2}F_{2n+3}\}$ and $\{F_{2n}, F_{2n+4}, 5F_{2n+2}, 4L_{2n+1}F_{2n+2}L_{2n+3}\}$ have property $D(1)$, the sets $\{F_{2n}, F_{2n+6}, 4F_{2n+2}, 4F_{2n+1}F_{2n+3}F_{2n+4}\}$ and $\{F_{2n}, F_{2n+6}, 4F_{2n+4}, 4F_{2n+2}F_{2n+3}F_{2n+5}\}$ have property $D(4)$, the set $\{F_{2n}, F_{2n+8}, 9F_{2n+4}, 4F_{2n+2}F_{2n+4}F_{2n+6}\}$ has property $D(9)$ and $\{F_{2n}, F_{2n+12}, 16F_{2n+6}, F_{2n+3}F_{2n+6}F_{2n+9}\}$ has property $D(64)$.*

The assertions of Theorem 3 can also be proved directly, e.g.

$$F_{2n+4} \cdot 4F_{2n+1}F_{2n+2}F_{2n+3} + 1 = (2F_{2n+2}F_{2n+3} + 1)^2$$

or

$$5F_{2n+2} \cdot 4L_{2n+1}F_{2n+2}L_{2n+3} + 1 = (10F_{2n+2}^2 - 1)^2$$

(see [4]).

5. General case. Consider now the problem of existence of sets of four natural numbers with property $D(n)$ in the general case, i.e. in the case where n need not be a perfect square.

First we prove

Theorem 4. *If n is an integer of the form $n = 4k + 2$, $k \in \mathbb{Z}$, then there is no set of four natural numbers with property $D(n)$.*

Proof. Let $n = 4k + 2$, $k \in \mathbb{Z}$, and suppose that $\{a_1, a_2, a_3, a_4\}$, $a_i \in \mathbb{N}$, has property $D(n)$. This means that $a_ia_j + (4k+2) = b_{ij}^2$, for $i, j = 1, 2, 3, 4$, $i \neq j$, $b_{ij} \in \mathbb{Z}$. Observe that the square of an integer is 0 or 1 $\pmod 4$. This implies that $a_ia_j \equiv 2$ or $3 \pmod 4$. This, first of all, means that none of the a_i is divisible by 4. Hence, for some two of them, say a_s and a_t, we have $a_s \equiv a_t \pmod 4$ so that $a_sa_t \equiv a_t^2 \pmod 4$. This leads to a contradiction because the left side of this congruence is 2 or 3 $\pmod 4$ while the right side is 0 or 1. ■

What can we get if $n \neq 4k + 2$? It is known that every integer which is not of the form $4k + 2$ can be represented as the difference of two squares. Hence, $n = k^2 - a^2$. Now, the four numbers a, a, $2a + 2k$, $5a + 4k$ have the property that the product of any two of them increased by n is a perfect square. In fact,

$$\begin{aligned} a \cdot a + n &= k^2\,, \\ a(2a + 2k) + n &= (a + k)^2\,, \\ a(5a + 4k) + n &= (2a + k)^2\,, \\ (2a + 2k)(5a + 4k) + n &= (3a + 3k)^2\,. \end{aligned}$$

The numbers a, a, $(s^2+1)a+2sk$, $(s^2+2s+2)a+2(s+1)k$ have the same property for every integer s. Note that in any of these quadruples we have two equal numbers, so they are not solutions of our problem.

There remains the following question: for which integers n do there exist four distinct natural numbers such that the product of any two of them increased by n gives the square of an integer? Until now, we proved that there are an infinite number of solutions when n is a perfect square and that no solution exists in the case that $n=4k+2$, $k\in\mathbb{Z}$. If n is not of the form $4k+2$, then necessarily n can be represented in one of the forms

$$4k+3,\ 8k+1,\ 8k+5,\ 8k,\ 16k+4,\ 16k+12\,.$$

For all of these cases, we will give formulas for a set of four numbers which has the property of Diophantus:

$$n=4k+3:\quad \{1,9k^2+8k+1,9k^2+14k+6,36k^2+44k+13\}, \tag{7}$$

$$n=8k+1:\quad \{4,9k^2-5k,9k^2+7k+2,36k^2+4k\}, \tag{8}$$

$$n=8k+5:\quad \{2,18k^2+14k+2,18k^2+26k+10,72k^2+80k+22\}, \tag{9}$$

$$n=8k:\quad \{1,9k^2-8k,9k^2-2k+1,36k^2-20k+1\}, \tag{10}$$

$$n=16k+4:\quad \{4,9k^2-4k-1,9k^2+8k+3,36k^2+8k\}, \tag{11}$$

$$n=16k+12:\quad \{2,18k^2+16k+2,18k^2+28k+12,72k^2+88k+26\}. \tag{12}$$

Our problem is almost completely solved by these formulas. The solution is incomplete because from (7)–(12) we can get sets with nonpositive or equal members for small values of k. More precisely, this happens for $k=0$, $k=-1$ in (7), (9) and (12), for $k=0$, $k=1$, $k=-1$ in (8) and (11), and for $k=0$, $k=1$ in (10). In this way, there still remain 14 values of n for which we do not know whether a solution exists (a set of four natural numbers with property $D(n)$). However, among these numbers there are 0, 1, 4 and 9 for which we gave an affirmative answer to our question earlier. Moreover, the set $\{1,8,11,16\}$ has property $D(-7)$ and $\{1,12,28,76\}$ has property $D(-12)$. Consequently, we have proved

THEOREM 5. *If an integer n does not have the form $4k+2$ and $n\notin S=\{3,5,8,12,20,-1,-3,-4\}$ then there exists a set of four natural numbers with property $D(n)$.*

If $n\in S$ then the question of existence of a set with the given property is still unanswered.

Remark 3. Note that the set in (12) is obtained from the set in (7) by multiplication by 2. We will show that every set of four numbers with property $D(16k+12)$ can be obtained from some set of four numbers with property $D(4k+3)$ by multiplying its members by 2. It is sufficient to prove that if $\{a_1, a_2, a_3, a_4\}$ has property $D(16k+12)$ then all the a_i are even. Suppose that a_1 is odd. It is easy to see that the square of an integer is 0, 1, 4 or 9 $\pmod{16}$. Therefore, $a_i a_j \equiv 4, 5, 8$ or $13 \pmod{16}$, for $i, j = 1, 2, 3, 4$, $i \neq j$. This implies that if some a_i, $i = 2, 3, 4$, is even then it is divisible by 4. Since $a_i a_j$ cannot be divisible by 16, we conclude that there must be at most one even number, i.e. at least three odd numbers, among the a_i, $i = 1, 2, 3, 4$. Let a_1, a_2, a_3 be odd. We have

$$a_1a_2 \equiv 5 \pmod{8}, \quad a_1a_3 \equiv 5 \pmod{8}, \quad a_2a_3 \equiv 5 \pmod{8}.$$

By multiplying these congruences, we obtain

$$(a_1a_2a_3)^2 \equiv 5^3 = 125 \equiv 5 \pmod{8},$$

which is impossible, since the square of an integer is 0, 1 or 4 $\pmod{8}$.

Formulas (7)–(12) are consequences of two more general formulas: the set

$$\{m, (3k+1)^2m + 2k, (3k+2)^2m + 2k + 2, 9(2k+1)^2m + 8k + 4\} \tag{13}$$

has property $D(2(2k+1)m+1)$, and

$$\{4m, (3k-1)^2m + k - 1, (3k+1)^2m + k + 1, 36k^2m + 4k\} \tag{14}$$

has property $D(8km+1)$.

Similarly, since

$$\{m, k^2m - 2k - 2, (k+1)^2m - 2k, (2k+1)^2m - 8k - 4\} \tag{15}$$

has property $D(2(2k+1)m+1)$ and

$$\{4m, (k-1)^2m - k - 3, (k+1)^2m + k + 3, 4k^2m + 4k\} \tag{16}$$

has property $D(8km+9)$, we obtain the following sets with the property of Diophantus:

$$n = 4k+3: \quad \{1, k^2 - 2k - 2, k^2 + 1, 4k^2 - 4k - 3\}, \tag{17}$$

$$n = 8k+1: \quad \{4, k^2 - 3k, k^2 + k + 2, 4k^2 - 4k\}, \tag{18}$$

$$n = 8k+5: \quad \{2, 2k^2 - 2k - 2, 2k^2 + 2k + 2, 8k^2 - 2\}, \tag{19}$$

$$n = 8k: \quad \{1, k^2 - 6k + 1, k^2 - 4k + 4, 4k^2 - 20k + 9\}, \tag{20}$$

$$n = 16k+4: \quad \{4, k^2 - 4k - 1, k^2 + 3, 4k^2 - 8k\}, \tag{21}$$

$$n = 16k+12: \quad \{2, 2k^2 - 4k - 4, 2k^2 + 2, 8k^2 - 8k - 6\}. \tag{22}$$

It is obvious that for many integers n there exist more than one set with property $D(n)$. Indeed, formulas (7)–(12) and (17)–(22) together with the fact that $\{2, 7, 19, 35\}$, $\{1, 8, 19, 208\}$, $\{12, 76, 150, 440\}$ and $\{1, 24, 41, 129\}$ have properties $D(11)$, $D(17)$, $D(33)$ and $D(40)$ respectively, yield

Theorem 6. *If an integer n is not of the form $4k+2$ and $n \notin S \cup T$, where $T = \{7, 13, 15, 21, 24, 28, 32, 48, 52, 60, 84, -7, -12, -15\}$ then there exist at least two different sets of four natural numbers with property $D(n)$.*

6. Some other formulas for sets with the property of Diophantus. If we take some concrete values for m or k in (13)–(16) we obtain formulas for sets with property $D(n)$, where n is a member of one arithmetic progression. In the first case, one member of the set is constant and the other three are polynomials of degree two. In the second case, all members of the set are polynomials of degree one.

For example ($m = 5$ in (15) and $k = 2$ in (14)): the set $\{5, 5k^2 - 2k - 2, 5k^2 + 8k + 5, 20k^2 + 12k + 1\}$ has property $D(20k + 11)$ and $\{4m, 25m + 1, 49m + 3, 144m + 8\}$ has property $D(16m + 1)$.

More formulas of this type can also be obtained by using the fact that the set

$$\{m, k^2m + 2k - 2, (k + 1)^2m + 2k + 4, (2k + 1)^2m + 8k + 4\} \tag{23}$$

has property $D(2(2k + 1) + 9)$.

There are also formulas for sets of four polynomials of degree one which are not consequences of (13)–(16) and (23). For example:

$$\begin{aligned}
n = 16k + 9: &\quad \{k, 16k + 8, 25k + 14, 36k + 20\}\,,\\
n = 10k + 9: &\quad \{k, 9k + 8, 16k + 14, 25k + 20\}\,,\\
n = 14k + 11: &\quad \{4k + 2, 9k + 7, 25k + 19, 49k + 35\}\,,\\
n = 22k + 5: &\quad \{9k + 2, 16k + 2, 49k + 10, 121k + 22\}\,,\\
n = 34k + 19: &\quad \{9k + 5, 49k + 25, 100k + 54, 289k + 153\}\,.
\end{aligned}$$

For more formulas see [5].

The question is which arithmetic progression $ak + b$ allows formulas of this type. Assume $\{a_ik + b_i : i = 1, 2, 3, 4\}$ has property $D(ak + b)$. Without losing generality, we can suppose that $\gcd(a_1, a_2, a_3, a_4, a) = 1$ (otherwise we put $m = kd$, where $\gcd(a_1, a_2, a_3, a_4, a) = d$). We will also suppose that $\gcd(a, b) = 1$. Now we will prove that a is even and b is a quadratic residue modulo a.

Suppose that a is odd. From

$$(a_ik + b_i)(a_jk + b_j) + ak + b = (c_{ij}k + d_{ij})^2$$

it follows that $a_ib_j + b_ia_j \equiv 1 \pmod 2$, $i, j = 1, 2, 3, 4$, $i \neq j$. This implies that at most one a_i is even. So we can suppose that a_1, a_2, a_3 are odd. Hence,

$$b_1 + b_2 \equiv 1 \pmod 2, \qquad b_2 + b_3 \equiv 1 \pmod 2, \qquad b_3 + b_1 \equiv 1 \pmod 2$$

and $2(b_1 + b_2 + b_3) \equiv 3 \pmod 2$. Contradiction.

Let $j \in \{1,2,3,4\}$. The set $\{a_j a_i k + a_j b_i : i = 1,2,3,4\}$ has property $D(a_j^2 ak + a_j^2 b)$ and so $\{a_i k + a_j b_i : i = 1,2,3,4\}$ has property $D(a_j ak + a_j^2 b)$. For $k = -b_j$ we obtain

$$-a_j b_j a + a_j^2 b = x_j^2, \qquad x_j \in \mathbb{Z}\,.$$

Let $a = 2^\alpha p_1^{\alpha_1} p_2^{\alpha_2} \dots p_s^{\alpha_s}$. For $m \in \{1,\dots,s\}$ there exists $n \in \{1,2,3,4\}$ such that $\gcd(p_m, a_n) = 1$. Now we have $a_n^2 b \equiv x_n^2 \pmod{p_m}$ and $\left(\frac{b}{p_m}\right) = 1$ (Legendre's symbol). If $\alpha \ge 2$ then there exists $t \in \{1,2,3,4\}$ such that a_t is odd. This implies that $b \equiv 1 \pmod 4$. If $\alpha \ge 3$ that implies $b \equiv 1 \pmod 8$. Hence, we conclude (see [9], p. 94) that b is a quadratic residue modulo a.

References

[1] J. Arkin and G. E. Bergum, *More on the problem of Diophantus*, in: Applications of Fibonacci Numbers, A. N. Philippou, A. F. Horadam and G. E. Bergum (eds.), Kluwer, Dordrecht, 1988, 177–181.

[2] A. H. Beiler, *Recreations in the Theory of Numbers*, Dover, New York, 1966.

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

[4] A. Dujella, *One Diofant's problem and Fibonacci's numbers*, Matematika 19 (3) (1990), 45–52 (in Croatian).

[5] —, *Generalization of a Diophantine problem*, Matematika 20 (1) (1991), 22–29 (in Croatian).

[6] B. W. Jones, *A variation on a problem of Davenport and Diophantus*, Quart. J. Math. Oxford Ser. (2) 27 (1976), 349–353.

[7] C. Long and G. E. Bergum, *On a problem of Diophantus*, in: Applications of Fibonacci Numbers, A. N. Philippou, A. F. Horadam and G. E. Bergum (eds.), Kluwer, Dordrecht, 1988, 183–191.

[8] S. Vajda, *Fibonacci & Lucas Numbers, and the Golden Section: Theory and Applications*, Horwood, Chichester, 1989.

[9] I. M. Vinogradov, *Elements of Number Theory*, Dover, New York, 1954.

DEPARTMENT OF MATHEMATICS
UNIVERSITY OF ZAGREB
BIJENIČKA CESTA 30
41000 ZAGREB, CROATIA
E-mail: DUJE@MATH.HR

Received on 18.12.1991
and in revised form on 10.3.1993 (2206)