ON THE EXCEPTIONAL SET IN THE PROBLEM OF DIOPHANTUS AND DAVENPORT

Andrej Dujella

Department of Mathematics, University of Zagreb, 10000 Zagreb, CROATIA

The Greek mathematician Diophantus of Alexandria noted that the numbers x, $x+2$, $4x+4$ and $9x+6$, where $x=\frac{1}{16}$, have the following property: the product of any two of them increased by 1 is a square of a rational number (see [4]). Fermat first found a set of four positive integers with the above property, and it was $\{1,3,8,120\}$. Later, Davenport and Baker [3] showed that if d is a positive integer such that the set $\{1,3,8,d\}$ has the property of Diophantus, then d has to be 120.

In [2] and [5], the more general problem was considered. Let n be an integer. A set of positive integers $\{a_1,a_2,\dots,a_m\}$ is said to have *the property* $D(n)$ if for all $i,j\in\{1,2,\dots,m\}$, $i\neq j$, the following holds: $a_ia_j+n=b_{ij}^2$, where b_{ij} is an integer. Such a set is called *a Diophantine m-tuple*. If n is an integer of the form $4k+2$, $k\in\mathbf{Z}$, then there does not exist Diophantine quadruple with the property $D(n)$ (see [2, Theorem 1], [5, Theorem 4] or [8, p. 802]). If an integer n is not of the form $4k+2$ and $n\notin S=\{-4,-3,-1,3,5,8,12,20\}$, then there exists at least one Diophantine quadruple with the property $D(n)$, and if $n\notin S\cup T$, where $T=\{-15,-12,-7,7,13,15,21,24,28,32,48,60,84\}$, then there exist at least two distinct Diophantine quadruples with the property $D(n)$ (see [5, Theorems 5 and 6] and [6, p. 315]). For $n\in S$ the question of the existence of Diophantine quadruples with the property $D(n)$ is still unanswered. This question is at present far from being solved. Remark 3 from [5] reduces the problem to the elements of the set $S'=\{-3,-1,3,5,8,20\}$. Let us mention that in [2] and [11], it was proved that the Diophantine triples $\{1,2,5\}$ and $\{1,5,10\}$ with the property $D(-1)$ cannot be extended to the Diophantine quadruples with the same property.

Our hypothesis is that for $n\in S$ there does not exist a Diophantine quadruple with the property $D(n)$. In this paper we consider some consequences of this hypothesis to the problem of Diophantus for linear polynomials.

Definition 1 Let $k \neq 0$ and l be integers. A set of linear polynomials with integral coefficients $\{a_i x + b_i : i = 1, 2, \ldots, m\}$ is called *a linear Diophantine m-tuple with the property $D(kx + l)$* if

$$(a_i x + b_i)(a_j x + b_j) + kx + l$$

is a square of a polynomial with integral coefficients for all $i, j \in \{1, 2, \ldots, m\}$, $i \neq j$. We call a linear Diophantine m-tuple *canonical* if $\gcd(a_1, a_2, \ldots, a_m, k) = 1$.

Remark 1 If the set $\{a_i x + b_i : i = 1, \ldots, m\}$ is a linear Diophantine m-tuple with the property $D(kx + l)$, then the numbers $a_1, \ldots, a_m$ are all of the same sign. Therefore we may assume that $a_1, \ldots, a_m$ are positive. If the above m-tuple is canonical, then the numbers $a_1, \ldots, a_m$ are perfect squares. If $\gcd(a_1, \ldots, a_m, k) = e > 1$, then replacing ex by x we get a canonical linear Diophantine quadruple with the property $D(\frac{k}{e}x + l)$.

Some aspects of the problem of Diophantus for polynomials were considered in [1], [5], [7], [9] and [10]. In [5], it was proved that if $\{a_i x + b_i : i = 1, 2, 3, 4\}$ is a linear Diophantine quadruple with the property $D(kx + l)$, then k is even, and if the above quadruple is canonical and if $\gcd(k, l) = 1$, then l is a quadratic residue modulo k. It is not known whether the converse of this result is true. We will show that this question is connected with the our hypothesis about the elements of the exceptional set S.

The basic idea is to consider linear Diophantine quadruples which have two elements with equal constant terms.

Lemma 1 *Let $\{a^2 x - \beta, b^2 x - \beta\}$ be a linear Diophantine pair with the property $D(kx + l)$. Then there exists an integer α such that $l = \alpha^2 - \beta^2$ and $k = \beta(a^2 + b^2) + 2\alpha ab$.*

Proof: Since $\beta^2 + l$ is a perfect square, we conclude that there exists an integer α such that $l = \alpha^2 - \beta^2$. From

$$(a^2 x - \beta)(b^2 x - \beta) + kx + l = (abx + \alpha)^2$$

it follows that $k = \beta(a^2 + b^2) + 2\alpha ab$. ■

Lemma 2 *Let $\{a^2 x - \beta, b^2 x - \beta, c(x)\}$ be a linear Diophantine triple with the property $D(kx + l)$. In the notation of Lemma 1, we have:*

$$\begin{aligned} c(x) \in \{ & (a+b)^2 x + 2\alpha - 2\beta,\ (a-b)^2 x - 2\alpha - 2\beta, \\ & [\frac{k}{\beta(a+b)}]^2 x + \frac{2k(\alpha - \beta)}{\beta(a+b)^2},\ [\frac{k}{\beta(a-b)}]^2 x - \frac{2k(\alpha + \beta)}{\beta(a-b)^2} \}\,. \end{aligned}$$

Proof: Write $c(x) = c^2x - \gamma$. Then there exists an integer δ such that

$$\beta\gamma + \alpha^2 - \beta^2 = \delta^2. \tag{1}$$

We conclude from $(a^2x - \beta)(c^2x - \gamma) + kx + l = (acx \pm \delta)^2$ and Lemma 1 that

$$\gamma a^2 - \beta c^2 + \beta(a^2 + b^2) + 2\alpha ab = \pm 2\delta ac\,. \tag{2}$$

Combining (2) with (1) we obtain

$$(\alpha a + \beta b)^2 = (\delta a \pm \beta c)^2$$

and finally

$$\alpha a + \beta b = \pm\delta a \pm \beta c\,. \tag{3}$$

In the same manner we can see that from $(b^2x - \beta)(c^2x - \gamma) + kx + l = (bcx \pm \delta)^2$ it follows that

$$\alpha b + \beta a = \pm\delta b \pm \beta c\,. \tag{4}$$

Solving the systems of the equations (3) and (4) we get

$$\begin{aligned}(|c|, |\delta|) \;\in\; & \{(|a+b|, |\alpha - \beta|),\, (|a-b|, |\alpha + \beta|),\\ & (|\frac{k}{\beta(a+b)}|, |\frac{(\alpha-\beta)(a-b)}{a+b}|),\, (|\frac{k}{\beta(a-b)}|, |\frac{(\alpha+\beta)(a+b)}{a-b}|)\}\,.\end{aligned}$$

From (1) we see that

$$\begin{aligned}c(x) \;\in\; & \{(a+b)^2x + 2\alpha - 2\beta,\, (a-b)^2x - 2\alpha - 2\beta,\\ & [\frac{k}{\beta(a+b)}]^2x + \frac{2k(\alpha-\beta)}{\beta(a+b)^2},\, [\frac{k}{\beta(a-b)}]^2x - \frac{2k(\alpha+\beta)}{\beta(a-b)^2}\}\,.\end{aligned}$$

■

Lemma 3 *Let* $\{a^2x - \beta, b^2x - \beta, c(x), d(x)\}$ *be a linear Diophantine quadruple with the property* $D(kx + l)$*, where* $\gcd(k, l) = 1$*. In the notation of Lemma 1, we have:*

$$\frac{a}{b} \in \{\frac{\beta}{\pm\beta - 2\alpha}, \frac{\pm\beta - 2\alpha}{\beta}, \frac{\beta}{2\alpha \pm 3\beta}, \frac{2\alpha \pm 3\beta}{\beta}, \frac{3\beta}{\pm\beta - 2\alpha}, \frac{\pm\beta - 2\alpha}{3\beta}\}\,.$$

Proof: Set $p_1(x) = (a+b)^2x + 2\alpha - 2\beta$, $p_2(x) = (a-b)^2x - 2\alpha - 2\beta$, $p_3(x) = [\frac{k}{\beta(a+b)}]^2x + \frac{2k(\alpha-\beta)}{\beta(a+b)^2}$, $p_4(x) = [\frac{k}{\beta(a-b)}]^2x - \frac{2k(\alpha+\beta)}{\beta(a-b)^2}$. According to Lemma 2, we have

$$\{c(x), d(x)\} \subseteq \{p_1(x), p_2(x), p_3(x), p_4(x)\}\,.$$

Thus we need to consider six cases. We can assume that $\gcd(a,b) = 1$, since otherwise we put $x' = e^2x$, where $e = \gcd(a,b)$.

Case 1. $\{c(x), d(x)\} = \{p_1(x), p_2(x)\}$

If y is an integer such that $(2\alpha - 2\beta)(-2\alpha - 2\beta) + l = y^2$, then

$$y^2 = -3l\,. \tag{5}$$

From $p_1(x) \cdot p_2(x) + kx + l = [(a^2-b^2)x + y]^2$ it follows that

$$(2\alpha - 2\beta)(a-b)^2 - (2\alpha + 2\beta)(a+b)^2 + \beta(a^2+b^2) + 2\alpha ab = 2y(a^2-b^2)\,.$$

This gives

$$-3k = 2y(a^2-b^2)\,. \tag{6}$$

Therefore $|y| = 3$, by (5), (6) and $\gcd(k,l) = 1$. We conclude that $l = -3$ and that $|\alpha| = 1$, $|\beta| = 2$. Combining $k = \pm 2(a^2+b^2) \pm 2ab$ with (6) we get $\frac{a}{b} \in \{\pm\frac{1}{2}, \pm 2\}$. It is easily seen that in all of these four cases the intersection

$$\{c(x), d(x)\} \cap \{a^2x - \beta, b^2x - \beta\}$$

is nonempty, which contradicts our assumption that $\{a^2x - \beta, b^2x - \beta, c(x), d(x)\}$ is a quadruple. Therefore the first case is impossible.

Case 2. $\{c(x), d(x)\} = \{p_1(x), p_3(x)\}$

We have:

$$\frac{a}{b} \in \{\frac{\beta}{\beta - 2\alpha}, \frac{\beta - 2\alpha}{\beta}, \frac{\beta}{2\alpha - 3\beta}, \frac{2\alpha - 3\beta}{\beta}\}\,.$$

Case 3. $\{c(x), d(x)\} = \{p_2(x), p_4(x)\}$

We have:

$$\frac{a}{b} \in \{\frac{\beta}{-\beta - 2\alpha}, \frac{-\beta - 2\alpha}{\beta}, \frac{\beta}{2\alpha + 3\beta}, \frac{2\alpha + 3\beta}{\beta}\}\,.$$

Case 4. $\{c(x), d(x)\} = \{p_1(x), p_4(x)\}$

We have:

$$\frac{a}{b} \in \{\frac{\beta}{-\beta - 2\alpha}, \frac{3\beta}{\beta - 2\alpha}, \frac{-\beta - 2\alpha}{\beta}, \frac{\beta - 2\alpha}{3\beta}\}\,.$$

Case 5. $\{c(x),d(x)\}=\{p_2(x),p_3(x)\}$

We have:
$$\frac{a}{b}\in\{\frac{\beta}{\beta-2\alpha},\frac{3\beta}{-\beta-2\alpha},\frac{\beta-2\alpha}{\beta},\frac{-\beta-2\alpha}{3\beta}\}\,.$$

Case 6. $\{c(x),d(x)\}=\{p_3(x),p_4(x)\}$

We have:
$$\frac{a}{b}\in\{\frac{-\beta-2\alpha}{\beta},\frac{\beta}{\beta-2\alpha},\frac{\beta-2\alpha}{\beta},\frac{\beta}{-\beta-2\alpha}\}\,.$$

We give the proof only for the case 6, which is the most involved; the proofs of the other cases are similar in spirit.

Let y be an integer such that
$$\frac{4k^2(\beta^2-\alpha^2)}{\beta^2(a^2-b^2)^2}+l=\frac{y^2}{\beta^2(a^2-b^2)^2}\,. \tag{7}$$

From $p_3(x)\cdot p_4(x)+kx+l=[\frac{k^2}{\beta^2(a^2-b^2)}x+\frac{y}{\beta(a^2-b^2)}]^2$ it follows that
$$\beta^3(a^2-b^2)^2-4\beta k^2=2ky\,. \tag{8}$$

Combining (8) with (7) we have
$$[4k^2-\beta^2(a^2-b^2)^2]\cdot[4k^2\alpha^2-\beta^4(a^2-b^2)^2]=0\,.$$

Let $4k^2=\beta^2(a^2-b^2)^2$. We can assume that $2k=\beta(a^2-b^2)$. We conclude that $2\beta(a^2+b^2)+4\alpha ab=\beta(a^2-b^2)$, and hence that
$$\beta a^2+4\alpha ab+3\beta b^2=0\,. \tag{9}$$

From this we have $\frac{a}{b}=\frac{-2\alpha\pm z}{\beta}$, where $z^2=4\alpha^2-3\beta^2$. Write $\frac{a_1}{b_1}=\frac{-2\alpha+z}{\beta}$, $\frac{a_2}{b_2}=\frac{-2\alpha-z}{\beta}$, where $\gcd(a_1,b_1)=\gcd(a_2,b_2)=1$, and $2k_i=\beta(a_i^2-b_i^2)$, $i=1,2$. We claim that $\gcd(k_i,l)>1$ for $i=1,2$. Suppose, contrary to our claim, that $\gcd(k_i,l)=1$ for some $i\in\{1,2\}$. We have
$$\begin{aligned}4k_1k_2&=\beta^2(a_1^2-b_1^2)(a_2^2-b_2^2)\\&=\beta^2\cdot\frac{b_1^2b_2^2}{\beta^4}\cdot[(-2\alpha+z)^2-\beta^2]\cdot[(-2\alpha-z)^2-\beta^2]\\&=\frac{b_1^2b_2^2}{\beta^2}\cdot[(2\alpha+\beta)^2-z^2]\cdot[(2\alpha-\beta)^2-z^2]\\&=\frac{b_1^2b_2^2}{\beta^2}\cdot16\beta^2(\beta^2-\alpha^2)=-16lb_1^2b_2^2\,.\end{aligned}$$

We conclude from $(-2\alpha+z)(-2\alpha-z) = 3\beta^2$ that $b_1b_2|\beta$, and hence that $k_1k_2|4\beta^2 l$. Set $c_i = a_i^2 - b_i^2$. Since $\gcd(k_i, l) = 1$ and the integer $2k_i = \beta c_i$ divides $8\beta^2$, we have $8\beta \equiv 0 \pmod{c_i}$. From (9) it follows that $8\alpha a_i b_i = -8\beta b_i - 2\beta c_i \equiv 0 \pmod{c_i}$. We conclude from $\gcd(a_i, b_i) = 1$ that $\gcd(a_i, b_i, c_i) = 1$, and hence that $8\alpha \equiv 0 \pmod{c_i}$. Thus we have $2k \equiv 0 \pmod{c_i}$, $8l \equiv 0 \pmod{c_i}$ and $\gcd(k, l) = 1$, which implies $c_i|8$, i.e. $c_i \in \{\pm 1, \pm 2, \pm 4, \pm 8\}$. Since $a_i \neq 0$ and $b_i \neq 0$, it follows that $c_i = \pm 8$. Hence α and β are odd and l is even, which contradicts the fact that k is even and $\gcd(k, l) = 1$.

Let $4k^2\alpha^2 = \beta^4(a^2 - b^2)^2$. We have

$$\begin{aligned}&[2k\alpha + \beta^2(a^2 - b^2)] \cdot [2k\alpha - \beta^2(a^2 - b^2)] \\ &\quad = [\beta a + (2\alpha + \beta)b] \cdot [(2\alpha - \beta)a + \beta b] \cdot [\beta a + (2\alpha - \beta)b] \cdot [(2\alpha + \beta) + \beta b] = 0\,.\end{aligned}$$

Hence

$$\frac{a}{b} \in \{\frac{-\beta - 2\alpha}{\beta}, \frac{\beta}{\beta - 2\alpha}, \frac{\beta - 2\alpha}{\beta}, \frac{\beta}{-\beta - 2\alpha}\}\,.$$

■

Theorem 1 *Let* $l \in \{-3, -1, 3, 5\}$. *Write* $e(-3) = 21$, $e(-1) = 5$, $e(3) = 39$ *and* $e(5) = 55$. *Suppose that there does not exist a Diophantine quadruple with the property* $D(l)$. *Then there does not exist a Diophantine quadruple with the property* $D(kx + l)$, *provided* $\gcd(k, e(l)) = 1$.

Proof: Let $l \in \{-3, -1, 3, 5\}$ and let k be an integer such that $\gcd(k, l) = 1$. Suppose that $\{a_i x + b_i : i = 1, 2, 3, 4\}$ is a canonical linear Diophantine quadruple with the property $D(kx + l)$. Then the set $\{b_1, b_2, b_3, b_4\}$ has the property that the number $b_i b_j + l$ is a perfect square for all $i, j \in \{1, 2, 3, 4\}$, $i \neq j$. Since, by assumption of the theorem, this set is not a Diophantine quadruple with the property $D(l)$, we conclude that there exist indices $i, j \in \{1, 2, 3, 4\}$, $i \neq j$, such that $b_i = b_j$. Without loss of generality we can assume that $b_1 = b_2 = \beta$.

The integers l have the unique representation as a difference of the squares of two integers:

$$-3 = 1^2 - 2^2,\ \ -1 = 0^2 - 1^2,\ \ 3 = 2^2 - 1^2,\ \ 5 = 3^2 - 2^2.$$

From Lemma 3 by an easy computation we conclude that for $l \in \{-3, -1, 3, 5\}$ there is one and only one canonical linear Diophantine quadruple with the property $D(kx + l)$, such that $\gcd(k, l) = 1$. These quadruples are

$$\{4x - 2, 9x - 2, 25x - 6, 49x - 14\}, \tag{10}$$

$$\{x-1, 9x-1, 16x-2, 25x-5\}, \tag{11}$$

$$\{9x+1, 25x+1, 64x+6, 169x+13\}, \tag{12}$$

$$\{9x+2, 16x+2, 49x+10, 121x+22\} \tag{13}$$

with the properties $D(14x-3)$, $D(10x-1)$, $D(26x+3)$ and $D(22x+5)$ respectively. This proves the theorem. ■

Remark 2 The sets (10) – (13) are the special cases of the following more general formula from [7]: the set

$$\begin{gathered}\{9m+4(3k-1),\ (3k-2)^2m+2(k-1)(6k^2-4k+1),\\ (3k+1)^2m+2k(6k^2+2k-1),\ (6k-1)^2m+4k(2k-1)(6k-1)\}\end{gathered} \tag{14}$$

has the property $D(2m(6k-1)+(4k-1)^2)$. The sets (10) – (13) can be obtained from (14) for $k=-1$, $m=-x+2$; $k=1$, $m=x-1$; $k=-2$, $m=-x+3$ and $k=2$, $m=x-2$ respectively.

References

[1] J. Arkin & G. E. Bergum. "More on the problem of Diophantus." In *Application of Fibonacci Numbers* **2**:177-181. Ed. A. N. Philippou, A. F. Horadam & G. E. Bergum. Dordrecht: Kluwer, 1988.

[2] E. Brown. "Sets in which $xy+k$ is always a square." *Mathematics of Computation* **45** (1985):613-620.

[3] H. Davenport & 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] Diofant Aleksandriĭskiĭ. *Arifmetika i kniga o mnogougol'nyh chislakh.* Moscow: Nauka, 1974.

[5] A. Dujella. "Generalization of a problem of Diophantus." *Acta Arithmetica* **65** (1993):15-27.

[6] A. Dujella. "Diophantine quadruples for squares of Fibonacci and Lucas numbers." *Portugaliae Mathematica* **52** (1995):305-318.

[7] A. Dujella. "Some polynomial formulas for Diophantine quadruples." *Grazer Mathematishe Berichte* (to appear).

[8] H. Gupta & K. Singh. "On k-triad sequences." *Internat. J. Math. Math. Sci.* **8** (1985):799-804.

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

[10] B. W. Jones. "A second variation on a problem of Diophantus and Davenport." *The Fibonacci Quarterly* **16** (1978):155-165.

[11] S. P. Mohanty & M. S. Ramasamy. "The simultaneous Diophantine equations $5y^2-20=x^2$ and $2y^2+1=z^2$." *Journal of Number Theory* **18** (1984):356-359.

AMS Classification Numbers: 11D09, 11C08