A NOTE ON DIOPHANTINE QUINTUPLES

ANDREJ DUJELLA

Introduction. Diophantus noted that the rational numbers 1/16, 33/16, 17/4 and 105/16 have the following property: the product of any two of them increased by 1 is a square of a rational number (see [2, 3]).

Let n be an integer. A set of positive integers $\{a_1, a_2, \ldots, a_m\}$ is said to have *the property* $D(n)$ if $a_i a_j + n$ is a perfect square for all $1 \leq i < j \leq m$. Such a set is called *a Diophantine* m*-tuple*. Fermat first found an example of a Diophantine quadruple with the property $D(1)$, and it was $\{1, 3, 8, 120\}$ (see [2]).

In 1985, Brown [1], Gupta and Singh [7] and Mohanty and Ramasamy [9] proved independently that if $n \equiv 2 \pmod 4$, then there does not exist a Diophantine quadruple with the property $D(n)$. If $n \not\equiv 2 \pmod 4$ and $n \notin \{-4, -3, -1, 3, 5, 8, 12, 20\}$, then there exists at least one Diophantine quadruple with the property $D(n)$ (see [4, Theorem 5].

In [5], the definition of Diophantine m-tuples is extended to the rational numbers. Namely, if q is a rational number, the set of non-zero rationals $\{a_1, a_2, \ldots, a_m\}$ is called *a rational Diophantine* m*-tuple with the property* $D(q)$ if $a_i a_j + q$ is a square of a rational number for all $1 \leq i < j \leq m$.

A direct consequence of [4, Theorem 5] is the following theorem.

Theorem 1 *For every rational number q there exist infinitely many distinct rational Diophantine quadruples with the property $D(q)$.*

Proof. The statement of the theorem is obviously true if $q = 0$. Let $q = \frac{m}{n}$, where $m \neq 0$ and $n > 0$ are integers. For a prime p define $k = 64p^2n^2q$. Then k is an integer, $k \equiv 0 \pmod 8$ and $|k| \geq 64$. Therefore, from the proof of [4, Theorem 5] we conclude that there exists a Diophantine quadruple of the form $\{1, a_2, a_3, a_4\}$ with the property $D(k)$. Now the set

$$D_p = \{\frac{1}{8pn}, \frac{a_2}{8pn}, \frac{a_3}{8pn}, \frac{a_4}{8pn}\}$$

is a rational Diophantine quadruple with the property $D(q)$. It suffices to show that $p \neq p'$ implies $D_p \neq D_{p'}$. Suppose that $D_p = D_{p'}$. Then from $\frac{1}{8pn} \cdot \frac{1}{8p'n} + \frac{m}{n} = \Box$ it follows that $\frac{1}{pp'} + 64mn = \Box$ and we obtain that pp' is a perfect square, a contradiction. ∎

Thus we came to the following open question: For which rational numbers q there exist infinitely many distinct Diophantine quintuples with the property $D(q)$?

We can easily give an affirmative answer for all rationals of the form $q = r^2$, $r \in \mathbf{Q}$. Namely, already Euler proved that an arbitrary Diophantine pair with the property $D(1)$ can be extended to the Diophantine quintuple (see [2]), and in [5] it is proved that the same is true for an arbitrary Diophantine quadruple with the property $D(1)$ (see also [6]).

The main result of the present paper is the following theorem which gives an affirmative answer to the above question for all rationals of the form $q = -3r^2$, $r \in \mathbf{Q}$.

Theorem 2 *There exist infinitely many distinct rational Diophantine quintuples with the property $D(-3)$.*

Proof. We will consider quintuples of the form $\{\alpha a^2, \beta b^2, C, D, E\}$ with the property $D(-\alpha\beta a^2 b^2)$, where $\alpha, \beta, a, b, C, D, E$ are integers. Furthermore, we will use the following simple and useful fact: If $AB + n = k^2$, then the set $\{A, B, A+B+2k\}$ has the property $D(n)$. Indeed, $A(A+B+2k)+n = (A+k)^2$, $B(A+B+2k)+n = (B+k)^2$.

Applying this construction to the identity

$$\alpha a^2 \cdot \beta b^2 - \alpha\beta a^2 b^2 = 0$$

we obtain $C = \alpha a^2 + \beta b^2$. The same construction applied to

$$\beta b^2 \cdot C - \alpha\beta a^2 b^2 = (\beta b^2)^2$$

gives $D = \alpha a^2 + 4\beta b^2$, and applied to

$$C \cdot D - \alpha\beta a^2 b^2 = (\alpha a^2 + 2\beta b^2)^2$$

gives $E = 4\alpha a^2 + 9\beta b^2$.

Hence, the set $\{\alpha a^2, \beta b^2, C, D, E\}$ will have the property $D(-\alpha\beta a^2 b^2)$ if and only if $\alpha a^2 \cdot D - \alpha\beta a^2 b^2$, $\alpha a^2 \cdot E - \alpha\beta a^2 b^2$ and $\beta b^2 \cdot E - \alpha\beta a^2 b^2$ are perfect squares. Remaining seven conditions are satisfied automatically. Hence, we have

$$\alpha a^2(\alpha a^2 + 3\beta b^2) = \square, \tag{1}$$

$$4\alpha a^2(\alpha a^2 + 2\beta b^2) = \square, \tag{2}$$

$$3\beta b^2(\alpha a^2 + 3\beta b^2) = \square. \tag{3}$$

Now (1) and (3) imply $3\alpha\beta = \square$, and we may assume that $\alpha = 1$ and $\beta = 3$. Thus our conditions (1)–(3) become

$$a^2 + 9b^2 = c^2 \quad \text{and} \quad a^2 + 6b^2 = d^2,$$

or

$$c^2 - 9b^2 = a^2 \quad \text{and} \quad c^2 - 3b^2 = d^2. \tag{4}$$

It is natural to assign to the system (4) the single condition

$$(c^2 - 9b^2)(c^2 - 3b^2) = (ad)^2,$$

which under substitution

$$x = 36(\frac{c}{b} - 3)^{-1}, \quad y = \frac{ad}{36b}x^2 \tag{5}$$

gives the elliptic curve

$$E: \qquad y^2 = x^3 + 42x^2 + 432x + 1296.$$

It is easy to verify, using the program package SIMATH (see [10]), that $E(\mathbf{Q})_{\mathrm{tors}} \simeq \mathbf{Z}/4\mathbf{Z}$, $E(\mathbf{Q})_{\mathrm{tors}} = < A >$, $\operatorname{rank}(E(\mathbf{Q})) = 1$, $E(\mathbf{Q})/E(\mathbf{Q})_{\mathrm{tors}} = < P >$, where $A = (0, -36)$ and $P = (-8, 4)$.

We are left with the task of determining points on $E(\mathbf{Q})$ which gives the solutions of system (4). Note that $x + 6 = \frac{6(c+3b)}{c-3b} = 6(c^2 - 9b^2)(c - 3b)^{-2}$. By [8, 4.6, p.89], the function $\varphi : E(\mathbf{Q}) \to \mathbf{Q}^*/\mathbf{Q}^{*2}$ defined by

$$\varphi(X) = \begin{cases} (x+6)\mathbf{Q}^{*2} & \text{if } X = (x, y) \neq \mathcal{O}, (-6, 0) \\ \mathbf{Q}^{*2} & \text{if } X = \mathcal{O}, (-6, 0) \end{cases}$$

is a group homomorphism. This implies that if $X \in 2E(\mathbf{Q})$ then $x + 6 = \square$, if $X \pm A \in 2E(\mathbf{Q})$ then $x + 6 = 6\square$, if $X - P \in 2E(\mathbf{Q})$ then $x + 6 = -2\square$ and if $X - P \pm A \in 2E(\mathbf{Q})$ then $x + 6 = -3\square$.

Therefore, x-coordinates of all points on E of the form $A+2nP$, where n is a positive integer, induce, by (5), infinitely many distinct solutions (a,b,c,d) of the system (4). (Note that the points $A+2nP$ and $-A+2nP$ induce the same solution.) Accordingly we obtain infinitely many Diophantine quintuples

$$\{\frac{a}{b}, \frac{3b}{a}, \frac{a}{b}+\frac{3b}{a}, \frac{a}{b}+\frac{12b}{a}, \frac{4a}{b}+\frac{27b}{a}\}$$

with the property $D(-3)$. ∎

In the following table we give some examples of Diophantine quintuples with the property $D(-3)$.

point on E	Diophantine quintuple with the property $D(-3)$
$A+2P$	$\{\frac{5}{4}, \frac{12}{5}, \frac{73}{20}, \frac{217}{20}, \frac{133}{5}\}$
$A+4P$	$\{\frac{13199}{5720}, \frac{17160}{13199}, \frac{272368801}{75498280}, \frac{566834401}{75498280}, \frac{395062801}{18874570}\}$
$A+6P$	$\{\frac{478267515}{492364404}, \frac{1477093212}{4782871515}, \frac{23601214939371220873}{2354817210010752060}, \frac{25783019296307697817}{2354817210010752060}, \frac{24510300088094752933}{588704320502688015}\}$
$A+8P$	$\{\frac{27456280948852799}{62923528228692560}, \frac{188770584686077680}{27456280948852799}, \frac{126319585777835455287880151681952 01}{17276460693400528440272476664754 40}, \frac{48266292220507170645420838162377601}{17276460693400528440272476664754 40}, \frac{274795975955850559940516914157712 01}{43191151733501321100681191661886 0}\}$

References

[1] E. Brown, *Sets in which $xy+k$ is always a square*, Math. Comp. **45** (1985), 613–620.

[2] L. E. Dickson, *History of the Theory of Numbers, Vol. 2*, Chelsea, New York, 1966, pp. 513–520.

[3] Diophantus of Alexandria, *Arithmetics and the Book of Polygonal Numbers*, (I. G. Bashmakova, Ed.), Nauka, Moscow, 1974 (in Russian), pp. 103–104, 232.

[4] A. Dujella, *Generalization of a problem of Diophantus*, Acta Arith. **65** (1993), 15–27.

[5] A. Dujella, *On Diophantine quintuples*, Acta Arith. **81** (1997), 69–79.

[6] A. Dujella, *The problem of Diophantus and Davenport*, Mathematical Communications **2** (1997), 153–160.

[7] H. Gupta and K. Singh, *On k-triad sequences*, Internat. J. Math. Math. Sci. **5** (1985), 799–804.

[8] A. Knapp, *Elliptic Curves*, Princeton Univ. Press, 1992.

[9] S. P. Mohanty and A. M. S. Ramasamy, *On $P_{r,k}$ sequences*, Fibonacci Quart. **23** (1985), 36–44.

[10] SIMATH manual, Saarbrücken, 1997.

Department of Mathematics, University of Zagreb, Bijenička cesta 30, 10000 Zagreb, Croatia

E-mail address: duje@math.hr