On Diophantine m-tuples and $D(n)$-sets

Nikola Adžaga, Andrej Dujella, Dijana Kreso and Petra Tadić

Abstract

For a nonzero integer n, a set of distinct nonzero integers $\{a_1, a_2, \ldots, a_m\}$ such that $a_i a_j + n$ is a perfect square for all $1 \leq i < j \leq m$, is called a Diophantine m-tuple with the property $D(n)$ or simply $D(n)$-set. Such sets have been studied since the ancient times. In this article, we give an overview of the results from the literature about $D(n)$-sets and summarize our recent findings about triples of integers which are $D(n)$-sets for several n's. Furthermore, we include some new observations and remarks about the ways to construct such triples.

Keywords: Diophantine m-tuples, elliptic curves.
2010 Mathematics Subject Classification: 11D09, 11G05.

1 Introduction

For a nonzero integer n, a set of distinct nonzero integers $\{a_1, a_2, \ldots, a_m\}$ such that $a_i a_j + n$ is a perfect square for all $1 \leq i < j \leq m$, is called a Diophantine m-tuple with the property $D(n)$ or $D(n)$-set. The $D(1)$-sets are called simply Diophantine m-tuples, and have been studied since the ancient times. In Section 2, we give an overview of the most significant results from the literature about $D(n)$-sets. In [20], A. Kihel and O. Kihel asked if there are Diophantine triples $\{a, b, c\}$ which are $D(n)$-sets for several distinct n's. They conjectured that there are no Diophantine triples which are also $D(n)$-sets for some $n \neq 1$. However, the conjecture does not hold, since, for example, $\{8, 21, 55\}$ is a $D(1)$ and $D(4321)$-triple (as noted in the MathSciNet review of [20]), while $\{1, 8, 120\}$ is a $D(1)$ and $D(721)$-triple, as observed by Zhang and Grossman [22]. In [1], we presented several infinite families of Diophantine triples which are also $D(n)$-sets for two additional n's. We further found examples of Diophantine triples which are $D(n)$-sets for three additional n's. In this article, in particular Section 3, we summarize our findings from [1] and add some new observations and remarks about the ways to construct such triples.

2 On Diophantine m-tuples

The problem of constructing $D(1)$-sets was first studied by Diophantus of Alexandria, who found a set of four rationals $\{\frac{1}{16}, \frac{33}{16}, \frac{17}{4}, \frac{105}{16}\}$ with the given property. Fermat found a first Diophantine quadruple – the set $\{1, 3, 8, 120\}$. Any Diophantine pair $\{a, b\}$ can be extended to a Diophantine triple, e.g. by adding $a + b + 2r$ to the set, where $ab + 1 = r^2$. Also, any Diophantine triple $\{a, b, c\}$ can be extended to a Diophantine quadruple. Namely, let $ab + 1 = r^2$, $bc + 1 = s^2$, $ca + 1 = t^2$, where r, s, t are positive integers. Then for $d_{\pm} = a + b + c + 2abc \pm 2rst$, both sets $\{a, b, c, d_+\}$

and $\{a, b, c, d_-\}$ are Diophantine quadruples provided $d_- \neq 0$. Such quadruples are said to be *regular*. In 2004, Dujella [9] showed that there are no Diophantine sextuples and that there are at most finitely many Diophantine quintuples. In 2016, He, Togbé and Ziegler announced a proof of a couple of decades old conjecture that there are no Diophantine quintuples [17]. (See also [3] for an analogous result concerning the conjecture of nonexistence of $D(4)$-quintuples.) A stronger and still open conjecture is that all Diophantine quadruples are regular. In that direction, Fujita and Miyazaki [15] recently proved that any fixed Diophantine triple can be extended to a Diophantine quadruple in at most 11 ways by joining a fourth element exceeding the maximal element in the triple, while Cipu, Fujita and Miyazaki [5] improved that result by replacing 11 by 8. In 1969, Baker and Davenport [2], using a then new technique of linear forms in logarithms, showed that the set $\{1, 3, 8\}$ can be extended to a Diophantine quintuple only by adding 120 to the set, which was the first result supporting the conjecture.

On the other hand, it was known already to Euler that there are infinitely many rational Diophantine quintuples. In particular, the Fermat's set $\{1, 3, 8, 120\}$ can be extended to a rational Diophantine quintuple by adding 777480/8288641 to the set. Recently, Stoll [21] proved that the extension of Fermat's set to a rational Diophantine quintuple is unique. The first example of a rational Diophantine sextuple, the set $\{11/192, 35/192, 155/27, 512/27, 1235/48, 180873/16\}$, was found by Gibbs [16], while Dujella, Kazalicki, Mikić and Szikszai [13] recently proved that there are infinitely many rational Diophantine sextuples (see also [12]). It is not known whether there exists a rational Diophantine septuple.

There are also some results concerning $D(n)$-sets with $n \neq 1$. It is easy to show that there are no $D(n)$-quadruples if $n \equiv 2 \pmod 4$ (see e.g. [4]). On the other hand, it is known that if $n \not\equiv 2 \pmod 4$ and $n \notin \{-4, -3, -1, 3, 5, 8, 12, 20\}$, then there exists at least one $D(n)$-quadruple [6]. It is widely believed that there do not exist $D(-1)$-quadruples, and it is known that there do not exist $D(-1)$-quintuples and that there are only finitely many $D(-1)$-quadruples [10, 11]. Finally, let us mention that the size of a $D(n)$-set is ≤ 31 for $|n| \leq 400$; $< 15.476 \log |n|$ for $|n| > 400$, and $< 3 \cdot 2^{168}$ for n prime (see [7, 8, 14]).

3 Triples which are $D(n)$-sets for several n's

Let $\{a, b, c\}$ be a Diophantine triple. Then there exist integers r, s, t such that $bc + 1 = r^2$, $ca + 1 = s^2$, $ab + 1 = t^2$. This triple is said to *induce* the elliptic curve

$$E(\mathbb{Q}): \quad y^2 = (x + ab)(x + ac)(x + bc). \tag{3.1}$$

Note that for the Diophantine triple $\{a, b, c\}$ there are only finitely many n's such that $\{a, b, c\}$ is a $D(n)$-set, since there are only finitely many integer points on the induced elliptic curve (3.1). Of interest to us are integers n such that $\{a, b, c\}$ is a $D(n)$-set, that is integer solutions x of the system of equations

$$x + bc = \square, \quad x + ca = \square, \quad x + ab = \square, \tag{3.2}$$

whereby symbol $\square$ stands for a perfect square. According to [18, 4.1, p. 37] (see also [19, 4.2, p. 85]), for $T \in E(\mathbb{Q})$ we have that $x = x(T)$ is a rational solution of (3.2) if and only if $T \in 2E(\mathbb{Q})$. It follows that for any point $T \in 2E(\mathbb{Q}) \cap \mathbb{Z}^2$ we have that $\{a, b, c\}$ is a $D(x(T))$-set, provided $x(T)$ is nonzero. Note that $E(\mathbb{Q})$ has several obvious rational points:

$$A = (-bc, 0), \quad B = (-ca, 0), \quad C = (-ab, 0), \quad P = (0, abc), \quad S = (1, rst).$$

One easily sees that $2A = 2B = 2C = \mathcal{O}$. Since we are assuming that $\{a, b, c\}$ is a Diophantine triple it follows that $S \in 2E(\mathbb{Q}) \cap \mathbb{Z}^2$. In our search for Diophantine triples which are $D(n)$-sets for several n's, we are thus led to look for triples $\{a, b, c\}$ for which $2kP + \ell S \in \mathbb{Z}^2$ for some $k, \ell \in \mathbb{Z}$.

An elementary proof of the fact that for a fixed $D(1)$-set $\{a, b, c\}$ there are only finitely many n's such that $\{a, b, c\}$ is a $D(n)$-set follows from the following proposition, which is similar in flavor to Theorem 2.7 and Remark 2.8 from [20].

Proposition 1. *Let $\{a, b, c\}$ be a Diophantine triple. For any n such that $\{a, b, c\}$ is a $D(n)$-set, there exists a divisor d of $P = b(c - a)$ such that*

$$n = \frac{1}{4}\left(d + \frac{P}{d}\right)^2 - bc. \tag{3.3}$$

Proof. Assume that $n + bc = r^2$, $n + ca = s^2$, $n + ab = t^2$ for integers r, s, t. Then $r^2 - t^2 = b(c - a)$. Letting $d = r - t$, we obtain $2r = d + b(c - a)/d$ which implies (3.3). □

Note that for n defined by (3.3) we have that $n + bc$ and $n + ab$ are always perfect squares since

$$n + bc = \frac{1}{4}\left(d + \frac{P}{d}\right)^2, \quad n + ab = \frac{1}{4}\left(d - \frac{P}{d}\right)^2.$$

It follows that for a given Diophantine triple $\{a, b, c\}$ we may search for n's such that $\{a, b, c\}$ is a $D(n)$-set by examining for which divisors d of $P = b(c - a)$ we have that $n + ca$ is a perfect square.

Through the elliptic curves approach described above and extensive computer search we found three infinite families of Diophantine triples which are $D(n)$-sets for two additional n's and the following examples of Diophantine triples which are $D(n)$-sets for three additional n's. The first six examples from the table were already presented in [1], while the last example is new.

$\{a, b, c\}$	n's
$\{4, 12, 420\}$	$1, 436, 3796, 40756$
$\{10, 44, 21252\}$	$1, 825841, 6921721, 112338361$
$\{4, 420, 14280\}$	$1, 14704, 950896, 47995504$
$\{40, 60, 19404\}$	$1, 19504, 3680161, 93158704$
$\{78, 308, 7304220\}$	$1, 242805865, 4770226465, 13336497750865$
$\{4, 485112, 16479540\}$	$1, 16964656, 2007609136, 63955397832496$
$\{15, 528, 32760\}$	$1, 66609, 5369841, 15984081$

It remains an open question if there exists an infinite family of Diophantine triples which are $D(n)$-sets for three additional n's, and if there are any Diophantine triples which are $D(n)$-sets for four additional n's. One should note that the size of a set N for which there exists a triple $\{a, b, c\}$

of nonzero integers which is a $D(n)$-set for all $n \in N$ can be arbitrarily large, see [1, Section 5]. In what follows we present our findings.

Let $\{a, b, c\}$ be a Diophantine triple and let $E(\mathbb{Q})$, P and S be defined as earlier in the section. Recall that if $2P \in E(\mathbb{Q}) \cap \mathbb{Z}^2$, then $\{a, b, c\}$ is a $D(x(2P))$-set provided $x(2P)$ is nonzero. Since

$$x_{2P} = \frac{1}{4}(a+b+c)^2 - ab - ac - bc,$$

it follows that $2P \in \mathbb{Z}^2$ when $a+b+c$ is an even number. One easily checks that $x(2P) = 0$ if and only if $c = a + b \pm 2\sqrt{ab}$, and hence for a Diophantine triple $\{a, b, c\}$ we have $x(2P) \neq 0$. One easily checks that $x(2P) = 1$ if and only if $c = a + b \pm 2\sqrt{ab+1}$.

Proposition 2. *Let $\{a, b, c\}$ be a Diophantine triple such that $c \neq a + b \pm 2\sqrt{ab+1}$. If $a+b+c$ is even, then $\{a, b, c\}$ is also a $D(n)$-set for some $n \neq 1$.*

A computer search showed that for the Diophantine triple $\{a, b, c\}$ with a, b, c in the range 1 to 10000, the corresponding points $S - 2P$ and $4P$ never have integer coordinates. On the other hand, the point $S + 2P = 2(R + P)$ has integer coordinates for triples $\{4, 12, 420\}, \{12, 24, 2380\}, \{24, 40, 7812\}$. These examples led us to the following construction of an infinite family of Diophantine triples which are $D(n)$-sets for two additional n's.

Proposition 3. *Let i be a positive integer and let*

$$a = 2(i+1)i, \quad b = 2(i+2)(i+1), \quad c = 4(2i^2+4i+1)(2i+3)(2i+1).$$

Then $\{a, b, c\}$ is a $D(n)$-set for $n = n_1, n_2, n_3$, where

$$\begin{aligned}
n_1 &= 1,\\
n_2 &= 32i^4 + 128i^3 + 172i^2 + 88i + 16,\\
n_3 &= 256i^8 + 2048i^7 + 6720i^6 + 11648i^5 + 11456i^4 + 6400i^3 + 1932i^2 + 280i + 16.
\end{aligned}$$

In Proposition 3 we have $n_1 = x(S), n_2 = x(2P), n_3 = x(S + 2P)$. The proposition can be also easily verified through direct computation.

We now explain how we found another infinite family of Diophantine triples which are $D(n)$-sets for two additional n's. By extending our search, we found several other Diophantine triples $\{a, b, c\}$ such that the corresponding point $S + 2P$ has integer coordinates. In particular, $\{4, 12, 420\}$ and $\{4, 420, 14280\}$ are two such triples, which are moreover $D(n)$-sets for three additional n's. In our search for an infinite family of Diophantine triples which are $D(n)$-sets for three additional n's, we looked into these two triples more closely. Using the Online Encyclopedia of Integer Sequences we found that $12, 420, 14280$ are consecutive elements of a recursively defined sequence

$$b_0 = 0, \quad b_1 = 12, \quad b_2 = 420, \quad b_{i+3} = 35b_{i+2} - 35b_{i+1} + b_i, \quad i \geq 3, \tag{3.4}$$

which is a sequence of integers that are simultaneously of shape $2p(p+1)$ and $q(q+1)$ for some positive integers p and q. Furthermore, we have that $b_ib_{i+1} + 1$ is always a square since $b_ib_{i+1} = 4t_i(t_i - 1)$, where t_i's are integers which are at the same time squares and triangular numbers, see [23, 24].

Let $a = 4$ and let b and c be consecutive elements of the sequence $(b_i)_{i\geq 1}$, so that $\{a, b, c\}$ is a Diophantine triple. We now show that this Diophantine triple is such that the corresponding points $S, 2P, 2P + S$ have integer coordinates. Indeed, since a, b, c are all even, the sum $a + b + c$ is an even integer, and thus $2P$ has integer coordinates. Also, $x(2P) \neq 1$. See Proposition 2. We claim that the x-coordinate of the point $S + 2P = 2(R + P)$ is also an integer, and moreover that $x := x(S + 2P) = a + b + c$. (One easily checks that $x(2P) \neq a + b + c$.) Since

$$\begin{aligned} x_{S+2P} &= -\frac{1}{4}(a+b+c)^2 - 1 + \\ &+ \frac{1}{4}\left(\frac{8abc + ((a+b+c)^2 - 4ab - 4ac - 4bc)(a+b+c) + 8\sqrt{ab+1}\sqrt{ac+1}\sqrt{bc+1}}{((a+b+c)^2 - 4ab - 4ac - 4bc - 4)^2}\right)^2 \end{aligned}$$

one can show that the latter statement holds if

$$c = 2 + a + b + 4ab \pm 2\sqrt{(2a+1)(2b+1)(ab+1)}. \tag{3.5}$$

Setting $a = 4$, we see that (3.5) holds if and only if $b^2 + c^2 - 12b - 12c - 34bc = 0$. One easily shows by induction that $b_n^2 + b_{n+1}^2 - 12b_n - 12b_{n+1} - 34b_nb_{n+1} = 0$ for all $n \geq 0$ by first showing, also by induction, that $b_{n+2} = 34b_{n+1} - b_n + 12$ for all $n \geq 0$. We get the following proposition.

Proposition 4. *Let the sequence $(b_i)_{i\geq 0}$ be defined by (3.4). Then for all positive integers i the triple $\{4, b_i, b_{i+1}\}$ is a $D(n)$-set for $n = n_1, n_2, n_3$, where*

$$n_1 = 1, \quad n_2 = \frac{1}{4}(4 + b_i + b_{i+1})^2 - 4b_i - 4b_{i+1} - b_ib_{i+1}, \quad n_3 = 4 + b_i + b_{i+1}.$$

The above proof of Proposition 4 led us to the following general result, which is the main result of our paper [1].

Theorem 5. *Let $\{2, a, b, c\}$ be a regular Diophantine quadruple. Then the Diophantine triple $\{a, b, c\}$ is also a $D(n)$-set for two distinct n's with $n \neq 1$.*

For the sake of brevity we omit a formal proof of Theorem 5. The key observation is that, as a step in the proof of Proposition 4, we showed that if $\{2, a, b, c\}$ is a regular Diophantine quadruple, which is equivalent to (3.5), then $x(S + 2P) = a + b + c$. The two additional n's in Theorem 5 are thus $n_2 = x_{2P}$ and $n_3 = x_{S+2P}$. The technical details (proofs that $1, n_2, n_3$ are all distinct and that n_2 is an integer) can be found in [1]. Note that the triples $\{a, b, c\}$ from Propositions 3 and 4 are such that $\{2, a, b, c\}$ is a regular Diophantine quadruple, so that Propositions 3 and 4 follow from Theorem 5. Another family of Diophantine triples of type $\{2, a, b\}$ can be obtained by taking $a = 2(i + 1)i$, $b = 4(2i^2 + 4i + 1)(2i + 3)(2i + 1)$. If we compute c using the regularity condition (3.5) we obtain the following corollary.

Corollary 6. *Let i be a positive integer and let*

$$a = 2(i+1)i, \quad b = 4(2i^2+4i+1)(2i+3)(2i+1), \quad c = 2(4i+1)(4i+3)(4i^2+9i+4)(4i^2+7i+1).$$

Then $\{a,b,c\}$ *is a* $D(n)$*-set for* $n = n_1, n_2, n_3$*, where*

$$\begin{aligned}
&n_1 = 1,\\
&n_2 = 512i^6 + 2560i^5 + 4832i^4 + 4352i^3 + 1980i^2 + 432i + 36,\\
&n_3 = 65536i^{12} + 655360i^{11} + 2859008i^{10} + 7151616i^9 + 11346176i^8 + 11932672i^7 + 8450112i^6\\
&\quad + 4012672i^5 + 1249280i^4 + 243840i^3 + 27612i^2 + 1584i + 36.
\end{aligned}$$

This summarizes our results from [1] about Diophantine triples which are $D(n)$-sets for several n's. Since the size of a set N for which there exists a triple $\{a,b,c\}$ of nonzero integers which is a $D(n)$-set for all $n \in N$ can be arbitrarily large, we may consider the following modification of the problem.

Question 1. *For a given positive integer* k*, what can be said about the smallest in absolute value nonzero integer* $n_1(k)$ *for which there exists a triple* $\{a,b,c\}$ *of nonzero integers and a set* N *of integers of size* k *containing* $n_1(k)$ *such that* $\{a,b,c\}$ *is a* $D(n)$*-set for all* $n \in N$*?*

Note that if $k \leq 4$, then $n_1(k) = 1$ since there are examples of Diophantine triples $\{a,b,c\}$ which are also $D(n)$-sets for three additional n's. We suspect that $|n_1(5)| > 1$ based on our exhaustive but unsuccessful computer search. In [1], we showed that $|n_1(5)| \leq 36$, and gave upper bounds for $|n_1(k)|$, $k \leq 20$. These results were obtained by searching for the triples of nonzero integers $\{a,b,c\}$ (which are not necessarily $D(1)$-triples) whose induced elliptic curve has relatively large rank r (say $r \geq 5$), see [1, Section 4] for details.

Acknowledgements. N.A., A.D. and P.T. were supported by the Croatian Science Foundation under the project no. 6422. A.D. acknowledges support from the QuantiXLie Center of Excellence, a project co-financed by the Croatian Government and European Union through the European Regional Development Fund - the Competitiveness and Cohesion Operational Programme (Grant KK.01.1.1.01.0004). D.K. acknowledges support of the Austrian Science Fund (FWF): J-3955.

References

[1] N. Adžaga, A. Dujella, D. Kreso, P. Tadić, *Triples which are* $D(n)$*-sets for several* n*'s*, J. Number Theory **184** (2018), 330–341.

[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] M. Bliznac Trebješanin, A. Filipin, *Nonexistence of* $D(4)$*-quintuples*, preprint, `arXiv:1704.01874`.

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

[5] M. Cipu, Y. Fujita, T. Miyazaki, *On the number of extensions of a Diophantine triple*, Int. J. Number Theory, to appear.

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

[7] A. Dujella, *On the size of Diophantine m-tuples*, Math. Proc. Cambridge Philos. Soc. **132** (2002), 23–33.

[8] A. Dujella, *Bounds for the size of sets with the property $D(n)$*, Glas. Mat. Ser. III **39** (2004), 199–205.

[9] A. Dujella, *There are only finitely many Diophantine quintuples*, J. Reine Angew. Math. **566** (2004), 183–214.

[10] A. Dujella, A. Filipin, C. Fuchs, *Effective solution of the $D(-1)$-quadruple conjecture*, Acta Arith. **128** (2007), 319–338.

[11] A. Dujella, C. Fuchs, *Complete solution of a problem of Diophantus and Euler*, J. London Math. Soc. (2) **71** (2005), 33–52.

[12] A. Dujella, M. Kazalicki, *More on Diophantine sextuples*, in: Number Theory - Diophantine problems, uniform distribution and applications, Festschrift in honour of Robert F. Tichy's 60th birthday (C. Elsholtz, P. Grabner, Eds.), Springer-Verlag, Berlin, 2017, pp. 227–235.

[13] A. Dujella, M. Kazalicki, M. Mikić, M. Szikszai, *There are infinitely many rational Diophantine sextuples*, Int. Math. Res. Not. IMRN **2017 (2)** (2017), 490–508.

[14] A. Dujella, F. Luca, *Diophantine m-tuples for primes*, Int. Math. Res. Not. **47** (2005), 2913–2940.

[15] Y. Fujita, T. Miyazaki, *The regularity of Diophantine quadruples*, Trans. Amer. Math. Soc., to appear.

[16] P. Gibbs, *Some rational Diophantine sextuples*, Glas. Mat. Ser. III **41** (2006), 195–203.

[17] B. He, A. Togbe, V. Ziegler, *There is no Diophantine quintuple*, preprint, `arXiv:1610.04020`.

[18] D. Husemöller, Elliptic Curves, Springer–Verlag, 1987.

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

[20] A. Kihel, O. Kihel, *On the intersection and the extendibility of P_t-sets*, Far East J. Math. Sci. **3** (2001), 637–643.

[21] M. Stoll, *Diagonal genus 5 curves, elliptic curves over $\mathbb{Q}(t)$, and rational diophantine quintuples*, preprint, `arXiv:1711.00500`.

[22] Y. Zhang, G. Grossman, *On Diophantine triples and quadruples*, Notes Number Theory Discrete Math. **21** (2015), 6–16.

[23] `http://oeis.org/A098602`

[24] `http://oeis.org/A001110`

Nikola Adžaga
Faculty of Civil Engineering
University of Zagreb
10000 Zagreb, Croatia
E-mail address: `nadzaga@grad.hr`

Andrej Dujella
Department of Mathematics
Faculty of Science
University of Zagreb
10000 Zagreb, Croatia
E-mail address: `duje@math.hr`

Dijana Kreso
Department of Mathematics
University of British Columbia
Vancouver BC, Canada
E-mail address: `kreso@math.ubc.ca`

Petra Tadić
Department of Economics and Tourism
Juraj Dobrila University of Pula
52100 Pula, Croatia
E-mail address: `ptadic@unipu.hr`