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

Andrej Dujella

Department of Mathematics
Faculty of Science
University of Zagreb, Croatia
e-mail: `duje@math.hr`
URL: `http://web.math.hr/~duje/`

Joint work with Nikola Adžaga, Dijana Kreso, Vinko Petričević and Petra Tadić

Supported by the QuantiXLie Center of Excellence

Diophantus: Find four (positive rational) numbers such that the product of any two of them, increased by 1, is a perfect square:

$$\left\{\frac{1}{16}, \frac{33}{16}, \frac{17}{4}, \frac{105}{16}\right\}$$

Fermat: $\{1, 3, 8, 120\}$

Euler: $\{1, 3, 8, 120, \frac{777480}{8288641}\}$

$$ab + 1 = r^2 \mapsto \{a, b, a + b + 2r, 4r(a + r)(b + r)\}$$

Definition: A set $\{a_1, a_2, \ldots, a_m\}$ of m non-zero integers (rationals) is called *a (rational) Diophantine m-tuple* if $a_i \cdot a_j + 1$ is a perfect square for all $1 \leq i < j \leq m$.

Question: How large such sets can be?

Baker & Davenport (1969): $\{1, 3, 8, d\} \Rightarrow d = 120$ (problem raised by Gardner (1967), van Lint (1968))

He, Togbé & Ziegler (2019): There does not exist a Diophantine quintuple.

Arkin, Hoggatt & Strauss (1978): Let

$$ab + 1 = r^2, \quad ac + 1 = s^2, \quad bc + 1 = t^2$$

and define

$$d_{+,-} = a + b + c + 2abc \pm 2rst.$$

Then $\{a, b, c, d_{+,-}\}$ is a Diophantine quadruple (if $d_- \neq 0$).

Conjecture: If $\{a, b, c, d\}$ is a Diophantine quadruple, then $d = d_+$ or $d = d_-$, i.e. all Diophantine quadruples satisfy

$$(a - b - c + d)^2 = 4(ad + 1)(bc + 1).$$

Such quadruples are called *regular*.

D. & Pethő (1998): All quadruples containing $\{1, 3\}$ are regular.

Fujita (2008), Bugeaud, D. & Mignotte (2007): All quadruples containing $\{k-1, k+1\}$ are regular.

Cipu, Fujita & Miyazaki (2018): Any fixed Diophantine triple can be extended to a Diophantine quadruple in at most 8 ways by joining a fourth element exceeding the maximal element in the triple.

There is no known upper bound for the size of rational Diophantine tuples.

Euler: There are infinitely many rational Diophantine quintuples. Any pair $\{a, b\}$ such that $ab+1 = r^2$ can be extended to a quintuple.

Arkin, Hoggatt & Strauss (1979): Any rational Diophantine triple $\{a, b, c\}$ can be extended to a quintuple.

D. (1997): Any rational Diophantine quadruple $\{a, b, c, d\}$, such that $abcd \neq 1$, can be extended to a quintuple (in two different ways, unless the quadruple is "regular" (such as in the Euler and AHS construction), in which case one of the extensions is trivial extension by 0).

Gibbs (1999): $\{\frac{11}{192}, \frac{35}{192}, \frac{155}{27}, \frac{512}{27}, \frac{1235}{48}, \frac{180873}{16}\}$

Question: If $\{a, b, c, d, e\}$ and $\{a, b, c, d, f\}$ are two extensions from D. (1997) and $ef \neq 0$, is it possible that $ef + 1$ is a perfect square?

D., Kazalicki, Mikić & Szikszai (2017): There are infinitely many rational Diophantine sextuples.

D., Kazalicki, Petričević (2019): There are infinitely many sextuples such that denominators of all the elements (in the lowest terms) in the sextuples are perfect squares.

Open question: Is there any rational Diophantine septuple?

Definition: For a nonzero integer n, a set of m 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 *a $D(n)$-m-tuple* or simply *a $D(n)$-set*. Note that a Diophantine m-tuple is a $D(1)$-set.

A. Kihel & O. Kihel (2001): Is there any Diophantine triple (i.e. $D(1)$-set) which is also a $D(n)$-set for some $n \neq 1$?

$\{8, 21, 55\}$ is a $D(1)$ and $D(4321)$-triple (D. (2002))

$\{1, 8, 120\}$ is a $D(1)$ and $D(721)$-triple (Zhang & Grossman (2015))

Question: For how many different n's with $n \neq 1$ can a $D(1)$-set also be a $D(n)$-set.

Adžaga, D., Kreso & Tadić (2017): There exist infinitely many Diophantine triples (i.e. $D(1)$-sets) which are also $D(n)$-sets for two distinct n's with $n \neq 1$.

There exist examples of Diophantine triples which are also $D(n)$-sets for three distinct n's with $n \neq 1$.

Main tool: elliptic curves induced by Diophantine triples.

Elliptic curves induced by Diophantine triples

Let $\{a, b, c\}$ be a Diophantine triple and let $ab + 1 = r^2$, $ac + 1 = s^2$, $bc + 1 = t^2$. We are interested in integer solutions x of the system of equations

$$x + ab = \square, \quad x + ac = \square, \quad x + bc = \square. \qquad (*)$$

Consider the corresponding elliptic curve

$$E: \quad y^2 = (x + ab)(x + ac)(x + bc).$$

Since E has only finitely many integer points, there are only finitely many n's such that $\{a, b, c\}$ is a $D(n)$-set.

E has several obvious rational points:

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

Proposition: For $T \in E(\mathbb{Q})$ we have that $x = x(T)$ is a rational solution of the system (*) if and only if $T \in 2E(\mathbb{Q})$.

Hence, we are interested in points in $2E(\mathbb{Q}) \cap \mathbb{Z}^2$. One such point in the point S, which corresponds to $x = 1$. Indeed, $S = 2R$, where

$$R = (rs + rt + st + 1, (r + s)(r + t)(s + t)) \in E(\mathbb{Q}) \cap \mathbb{Z}^2.$$

A, B, C are points of order 2. In general, we may expect that the points P and S are two independent points of infinite order. However, if $c = a + b \pm 2r$, where $ab + 1 = r^2$ (such triples are called *regular*), then $2P = \pm S$.

We want to find triples $\{a, b, c\}$ for which $2kP + \ell S \in \mathbb{Z}^2$ for some $k, \ell \in \mathbb{Z}$. We have

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

Lemma: Let a, b, c be nonzero integers such that $a + b + c$ is even. Then $\{a, b, c\}$ is a $D(n)$-set for

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

provided $n \neq 0$. Furthermore, $n = 0$ is equivalent to $c = a+b\pm 2\sqrt{ab}$ (and thus impossible if $\{a, b, c\}$ is a $D(1)$-triple), while $n = 1$ is equivalent to $c = a+b\pm 2\sqrt{ab + 1}$.

Corollary: Any Diophantine triple $\{a, b, c\}$ such that $a + b + c$ is even and $c \neq a + b \pm 2\sqrt{ab + 1}$ is also a $D(n)$-set for some $n \neq 1$.

A computer search, $\{a, b, c\}$ is a $D(1)$-set, $a, b \leq 1000$, $c \leq 1000000$: the points $S - 2P$ and $4P$ never have integer coordinates, while the point $S + 2P = 2(R + P)$ has integer coordinates in 14 cases, which all satisfy an additional condition that $x(S + 2P) = a + b + c$.

The condition $x(S+2P)=a+b+c$ leads to

$a^2-4a-2ac-4c+c^2-2ab-4b-8abc-2bc+b^2=0.$

This condition is is equivalent to

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

and this is exactly the condition that $\{2,a,b,c\}$ is a regular Diophantine quadruple.

It can be verified that for such triples $n_2=x(S+2P)$ and $n_3=x(2P)$ satisfy $n_2\neq n_3$, $n_1\neq 1$, $n_3\neq 1$.

Theorem: 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 $n\neq 1$.

Corollary: Let k be a positive integer and let

$$a = 2k(k+1),$$
$$b = 2(k+1)(k+2),$$
$$c = 4(2k+1)(2k+3)(2k^2+4k+1).$$

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

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

Triples $\{a, b, c\}$ which are $D(n)$-sets for $n_1 = 1 < n_2 < n_3 < n_4$:

$\{a, b, c\}$	n_2, n_3, n_4
$\{4, 12, 420\}$	$436, 3796, 40756$
$\{10, 44, 21252\}$	$825841, 6921721, 112338361$
$\{4, 420, 14280\}$	$14704, 950896, 47995504$
$\{40, 60, 19404\}$	$19504, 3680161, 93158704$
$\{78, 308, 7304220\}$	$242805865, 4770226465, 13336497750865$
$\{4, 485112, 16479540\}$	$16964656, 2007609136, 63955397832496$
$\{15, 528, 32760\}$	$66609, 5369841, 15984081$

Open question: Are there infinitely many such triples?

Question: Is there any set of four distinct nonzero integers which is a $D(n_i)$-quadruple for two distinct (nonzero) integers n_1 and n_2.

If $\{a, b, c, d\}$ is $D(n_1)$ and $D(n_2)$-quadruple and u is a nonzero rational such that au, bu, cu, du, n_1u^2 and n_2u^2 are integers, then $\{au, bu, cu, du\}$ is a $D(n_1u^2)$ and $D(n_2u^2)$-quadruples. We will say that these two quadruples are equivalent.

D. & Petričević (2019): There are infinitely many nonequivalent sets of four distinct nonzero integers $\{a, b, c, d\}$ with the property that there exist two distinct nonzero integers n_1 and n_2 such that $\{a, b, c, d\}$ a $D(n_1)$-quadruple and a $D(n_2)$-quadruple.

Experimentally: many solutions in which $a/b = -1/7$ and quadruples contain regular triples. If $cd + n_1 = r^2$, $cd + n_2 = s^2$, $c + d - 2r = 7$ and $c + d - 2s = -1$, then $\{7, c, d\}$ is a $D(n_1)$-triple and $\{-1, c, d\}$ is a $D(n_2)$-triple. The remaining six conditions from the definition of $D(n_i)$-quadruples can be satisfied parametrically.

The set

$$\{-(-v^2 + 7w^2)^2, 7(-v^2 + 7w^2)^2,$$
$$-(-2v^2 + vw + 7w^2)(2v^2 - 3vw + 7w^2),$$
$$(v^2 - 3vw + 14w^2)(-v^2 - vw + 14w^2)\}$$

is a $D(n_1)$-quadruple and a $D(n_2)$-quadruple for

$$n_1 = 4(-v^2 + 7w^2)^2(2v^4 - v^3w - 20v^2w^2 - 7vw^3 + 98w^4),$$
$$n_2 = 4(-v^2 + 7w^2)^2(2v^2 - 7vw + 14w^2)(v^2 + 7w^2).$$

By taking v and w to be solutions of the Pellian equation

$$v^2 - 7w^2 = 2,$$

and dividing elements of the quadruple by the common factor 4, we obtain quadruples of the form $\{-1, 7, c, d\}$ which are $D(n)$-quadruples for two distinct n's. Here are few examples:

$\{a, b, c, d\}$	$\{n_1, n_2\}$
-1, 7, 119, 64	128, 848
-1, 7, 1191959, 1185664	1585088, 11095568
-1, 7, 5840864, 5826919	7778528, 54449648
-1, 7, 76695715424, 76694116519	102259887968, 715819215728
-1, 7, 376369378007, 376365836032	501823476032, 3512764332176

D. & Petričević (2019): There are infinitely many nonequivalent sets of four distinct nonzero integers $\{a,b,c,d\}$ with the property that a,b,c,d are perfect squares (so that $\{a,b,c,d\}$ is a $D(0)$-quadruple) and there exist $n_2 \neq 0$ such that $\{a,b,c,d\}$ a $D(n_2)$-quadruple.

$\{4r^4(r+2)^2, (r^3-4r+1)^2, (r^3+4r^2-1)^2, 4(2r-1)^2\}$

is a $D(0)$-quadruple and a $D(16r^{10}+96r^9+112r^8-192r^7-256r^6+192r^5+112r^4-96r^3+16r^2)$-quadruple.

Sketch of the proof: the set

$$\{a, ak^2-2k-2, a(k+1)^2-2k, a(2k+1)^2-8k-4\}$$

is a $D(2a(2k+1)+1)$-quadruple (D. (1996)). Find rationals a and k such that ab, ac and ad are perfect squares. This leads to an elliptic curve over $\mathbb{Q}(r)$ with rank equal to 2, where $ab=(ak+r)^2$.