


Triples 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 and Petra Tadić

Supported by the Croatian Science Foundation under the project

no. 6422. 

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 $\{a_1, a_2, \dots, a_m\}$ 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?

Conjecture 1: There does not exist a Diophantine quintuple.

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

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 2: 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. & Fuchs (2004): All Diophantine quadruples in $\mathbb{Z}[X]$ are regular.

D. & Jurasić (2010): In $\mathbb{Q}(\sqrt{-3})[X]$, the Diophantine quadruple

$$\left\{ \frac{\sqrt{-3}}{2}, -\frac{2\sqrt{-3}}{3}(X^2 - 1), \frac{-3 + \sqrt{-3}}{3}X^2 + \frac{2\sqrt{-3}}{3}, \frac{3 + \sqrt{-3}}{3}X^2 + \frac{2\sqrt{-3}}{3} \right\}$$

is not regular.

D. & Pethő (1998): $\{1, 3\}$ cannot be extended to a Diophantine quintuple

Fujita (2008): $\{k - 1, k + 1\}$ cannot be extended to a Diophantine quintuple

D. (2004): There does not exist a Diophantine sextuple. There are only finitely many Diophantine quintuples.

Fujita (2009): If $\{a, b, c, d, e\}$, with $a < b < c < d < e$, is a Diophantine quintuple, then $\{a, b, c, d\}$ is a regular Diophantine quadruple.

Cipu & Trudgian (2016): Number of Diophantine quintuples is less than $1.18 \cdot 10^{27}$.

He, Togbé & Ziegler (201?): There does not exist a Diophantine quintuple.

Fujita & Miyazaki (2017); 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.

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): $\left\{ \frac{11}{192}, \frac{35}{192}, \frac{155}{27}, \frac{512}{27}, \frac{1235}{48}, \frac{180873}{16} \right\}$

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.

Moreover, there are infinitely many rational Diophantine sextuples with positive elements, and also with any combination of signs.

By **DKMS (2017)**, there exist infinitely many triples, each of which can be extended to sextuples on infinitely many ways.

Piezas; D. & Kazalicki (2017): There are infinitely many sextuples $\{a, b, c, d, e, d\}$ with fixed products ab and cd .

Gibbs (2017): The quintuple

$$\left\{ \frac{243}{560}, \frac{147}{5040}, \frac{1100}{63}, \frac{7820}{567}, \frac{95}{112} \right\}$$

can be extended to two different sextuples, by $\frac{38269}{6480}$ and $\frac{196}{45}$.

Open question: Is there any rational Diophantine septuple?

Diophantine m -tuples of finite fields

Let p be a prime and $N^{(m)}(p)$ the number of Diophantine m -tuples with elements in \mathbb{F}_p (we consider 0 to be a square in \mathbb{F}_p).

Since half of the elements of \mathbb{F}_p^\times are squares, heuristically, one expects that a randomly chosen m -tuple of different elements in \mathbb{F}_p^\times will have the Diophantine property with probability $1/2^{\binom{m}{2}}$, i.e. we expect

$$N^{(m)}(p) = \frac{1}{2^{\binom{m}{2}}} \frac{p^m}{m!} + o(p^m).$$

This can be justified by using Weil's estimate for character sums.

D.& Kazalicki (201?): Let $m \geq 2$ be an integer. If $p > 2^{2m-2}m^2$ is a prime, then there exists a Diophantine m -tuple in \mathbb{F}_p .

Explicit formulas for $N^{(k)}(p)$ for $k = 2, 3, 4$:

$$N^{(2)}(p) = \begin{cases} \frac{(p-1)(p-2)}{4}, & \text{if } p \equiv 1 \pmod{4}, \\ \frac{p^2-3p+4}{4}, & \text{if } p \equiv 3 \pmod{4}. \end{cases}$$

$$N^{(3)}(p) = \begin{cases} \frac{(p-1)(p-3)(p-5)}{48}, & \text{if } p \equiv 1 \pmod{4}, \\ \frac{(p-3)(p^2-6p+17)}{48}, & \text{if } p \equiv 3 \pmod{4}. \end{cases}$$

The formula for $N^{(4)}(p)$ is given in terms of the Fourier coefficients of the certain modular forms.

Definition: For a nonzero integer n , a set of m distinct nonzero integers $\{a_1, a_2, \dots, a_m\}$ 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 a *$D(n)$ -set*. Note that a Diophantine m -tuple is a $D(1)$ -set.

A. Kihel & O. Kihel (2001): Is there any Diophantine m -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

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

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 is 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 for the following (a, b, c) ;

$(4, 12, 420)$, $(4, 420, 14280)$, $(12, 24, 2380)$, $(12, 420, 41184)$,
 $(24, 40, 7812)$, $(40, 60, 19404)$, $(60, 84, 40612)$, $(84, 112, 75660)$,
 $(112, 144, 129540)$, $(144, 180, 208012)$, $(180, 220, 317604)$,
 $(220, 264, 465612)$, $(264, 312, 660100)$, $(312, 364, 909900)$.

We will show that there are infinitely many such examples.

We first note that all the examples above satisfy an additional condition that $x(S + 2P) = a + b + c$. A straightforward calculation shows that the condition $x(S + 2P) = a + b + c$ is equivalent to $q_1q_2q_3 = 0$, where

$$\begin{aligned} q_1 &= -4 + a^2 - 2ab + b^2 - 2ac - 2bc + c^2, \\ q_2 &= a^2 - 4a - 2ac - 4c + c^2 - 2ab - 4b - 8abc - 2bc + b^2, \\ q_3 &= -4a - 4b - 4c - 2ab - 2ac - 2bc - 4abc + a^2 + b^2 + c^2 \\ &\quad - 2a^2b - 2a^2c - 2ab^2 - 2ac^2 - 2b^2c - 2bc^2 - 2a^2b^2 \\ &\quad + 2a^3 + 2b^3 + 2c^3 + a^4 + b^4 + c^4 - 2a^2c^2 - 2b^2c^2. \end{aligned}$$

The condition $q_1 = 0$ is equivalent to $c = a + b \pm 2\sqrt{ab + 1}$, but in that case $x(2P) = 1$, so in this way we do not get a Diophantine triple which is also a $D(n)$ -set for two distinct n 's with $n \neq 1$. The equation $q_3 = 0$ has no solutions in Diophantine triples $\{a, b, c\}$.

Thus, the only interesting condition for us is $q_2 = 0$. It 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 $n \neq 1$.

Explicit infinite families of Diophantine triples $\{a, b, c\}$ satisfying the conditions of the theorem

Corollary: 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

$$n_1 = 1,$$

$$n_2 = 32i^4 + 128i^3 + 172i^2 + 88i + 16,$$

$$n_3 = 256i^8 + 2048i^7 + 6720i^6 + 11648i^5 + 11456i^4 + 6400i^3 \\ + 1932i^2 + 280i + 16.$$

Corollary: Let the sequence $(b_i)_{i \geq 0}$ be defined by

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

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

$$n_1 = 1,$$

$$n_2 = 4 + b_i + b_{i+1},$$

$$n_3 = \frac{1}{4}(4 + b_i + b_{i+1})^2 - 4b_i - 4b_{i+1} - b_i b_{i+1}.$$

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

Question: Are there infinitely many such triples?

A modification of the problem

So far we were interested in the maximum size of a set N of nonzero integers containing 1 for which there exists a triple of nonzero integers $\{a, b, c\}$ which is a $D(n)$ -set for all $n \in N$. If we omit the condition $1 \in N$, then 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. Indeed, take any triple $\{a, b, c\}$ such that the induced elliptic curve $E(\mathbb{Q})$ has positive rank. Then there are infinitely many rational points on E . For an arbitrary large positive integer m we may choose m distinct rational points $R_1, \dots, R_m \in 2E(\mathbb{Q})$, so that we have

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

We do so by taking points of the form $2m_1P_1 + 2m_2P_2 + \dots + 2m_rP_r$, where P_1, \dots, P_r are the generators of $E(\mathbb{Q})$. We then let $z \in \mathbb{Z} \setminus \{0\}$ be such that $z^2x(R_i) \in \mathbb{Z}$ for all $i = 1, 2, \dots, m$. Then the triple $\{az, bz, cz\}$ is a $D(n)$ -set for $n = x(R_i)z^2$ for all $i = 1, 2, \dots, m$.

Question: 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 we have found examples of Diophantine triples $\{a, b, c\}$ which are also $D(n)$ -sets for three distinct n 's greater than 1.

We can show that $|n_1(5)| \leq 36$. To that end we consider the Diophantine triple $\{1, 8, 120\}$, whose induced elliptic curve $E(\mathbb{Q})$ has rank 3. Following the procedure described above we find points $R_1, \dots, R_5 \in 2E(\mathbb{Q})$ such that

$$\begin{aligned}x(R_1) &= 1, & x(R_2) &= 721, & x(R_3) &= 12289/4, \\x(R_4) &= 769/9, & x(R_5) &= 1921/36.\end{aligned}$$

We then let $z = 6$. It follows that the triple $\{az, bz, cz\} = \{6, 48, 720\}$ is a $D(n)$ -set for

$$n = 36, 1921, 3076, 25956, 110601.$$

(We choose $R_2, \dots, R_5 \in 2E(\mathbb{Q})$ so that their x -coordinates have relatively small denominators. We obtained the n 's using $n = x(R_i)z^2$, $i = 1, 2, \dots, 5$).

k	$ n_1(k) \leq$	rank	$\{a, b, c\}$
5	36	3	$\{6, 48, 720\}$
6	215	3	$\{28, 168, 1848\}$
7	900	4	$\{380, 1400, 3240\}$
8	7740	3	$\{168, 1008, 11088\}$
9	32400	4	$\{2280, 8400, 19440\}$
10	129600	4	$\{4560, 16800, 38880\}$
11	215991	5	$\{9120, 22770, 30960\}$
12	863964	5	$\{18240, 45540, 61920\}$
13	4932144	5	$\{37128, 118440, 182280\}$
14	7706475	5	$\{46410, 148050, 227850\}$
15	30825900	5	$\{92820, 296100, 455700\}$
16	123303600	5	$\{185640, 592200, 911400\}$
17	371289600	5	$\{59400, 108360, 223200\}$
18	4438929600	5	$\{1113840, 3553200, 5468400\}$
19	18193190400	5	$\{415800, 758520, 1562400\}$
20	18193190400	5	$\{415800, 758520, 1562400\}$