Rational Diophantine m-tuples in the work of Andrej Dujella

Representation theory XIX, Dubrovnik
June 23, 2025

Matija Kazalicki
University of Zagreb



This work was supported by the Croatian Science Foundation

under the project number HRZZ IP-2022-10-5008.

Introduction

Diophantine m-tuples

A (rational) Diophantine m-tuple is a set of m positive integers (or rational numbers) with the property that the product of any two of its distinct elements is one less then a square.

Diophantus of Alexandria

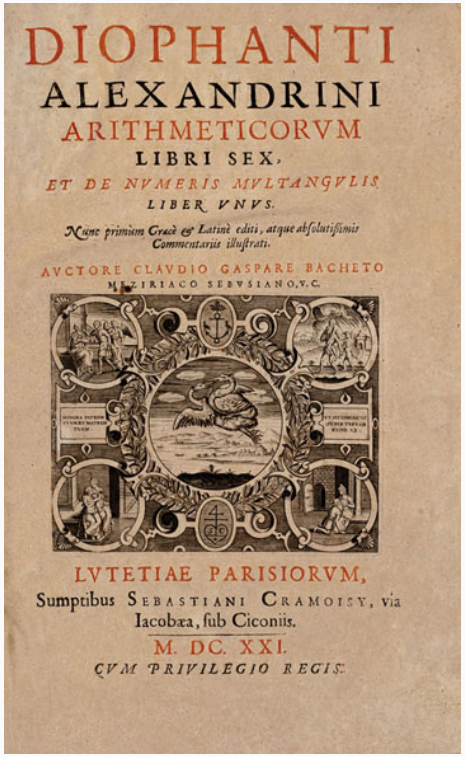

DIOPHANTI
ALEXANDRINI
ARITHMETICORVM
LIBRI SEX.
ET DE NVMERIS MVLTANGVLIS
LIBER VNVS.
Nunc primùm Græcè & Latinè editi, atque absolutissimis Commentariis illustrati.
AVCTORE CLAVDIO GASPARE BACHETO
MEZIRIACO SEBVSIANO, V.C.
LVTETIAE PARISIORVM,
Sumptibus SEBASTIANI CRAMOISY, via Iacobæa, sub Ciconiis.
M. DC. XXI.
CVM PRIVILEGIO REGIS.

Figure 1: Cover of the 1621 edition

Diophantus of Alexandria

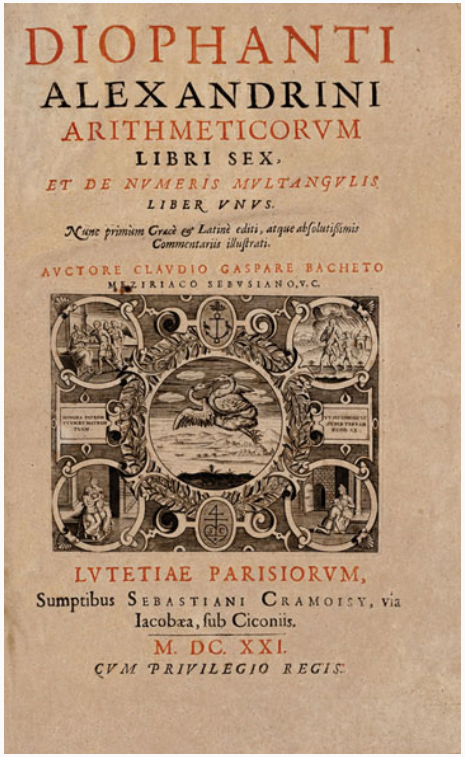

DIOPHANTI
ALEXANDRINI
ARITHMETICORVM
LIBRI SEX.
ET DE NVMERIS MVLTANGVLIS
LIBER VNVS.
Nunc primùm Græcè & Latinè editi, atque absolutissimis Commentariis illustrati.
AVCTORE CLAVDIO GASPARE BACHETO
MEZIRIACO SEBVSIANO, V.C.
LVTETIAE PARISIORVM,
Sumptibus SEBASTIANI CRAMOISY, via Iacobæa, sub Ciconiis.
M. DC. XXI.
CVM PRIVILEGIO REGIS.

Figure 1: Cover of the 1621 edition

Diophantus: $\{1/16, 33/16, 17/4, 105/16\}$

Fermat



Figure 2: Pierre de Fermat

Fermat



Figure 2: Pierre de Fermat

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

Fermat



Figure 2: Pierre de Fermat

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

$$1 \cdot 3 + 1 = 2^2 \quad 1 \cdot 8 + 1 = 3^2 \quad 1 \cdot 120 + 1 = 11^2$$
$$3 \cdot 8 + 1 = 5^2 \quad 3 \cdot 120 + 1 = 19^2 \quad 8 \cdot 120 + 1 = 31^2.$$

Euler



Figure 3: Leonhard Euler

Euler



Figure 3: Leonhard Euler

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

How big can these sets be (in integers)?

How big can these sets be (in integers)?

There are infinitely many Diophantine quadruples, e.g.

$$\{k, k+2, 4k+4, 16k^3+48k^2+44k+12\}$$

How big can these sets be (in integers)?

There are infinitely many Diophantine quadruples, e.g.

$$\{k, k+2, 4k+4, 16k^3+48k^2+44k+12\}$$

Dujella (2004): There are no integer Diophantine sextuples, and there are at most finitely many integer Diophantine quintuples.

How big can these sets be (in integers)?

There are infinitely many Diophantine quadruples, e.g.

$$\{k, k+2, 4k+4, 16k^3+48k^2+44k+12\}$$

Dujella (2004): There are no integer Diophantine sextuples, and there are at most finitely many integer Diophantine quintuples.

He, Togbe, Ziegler (2018): There are no integer Diophantine quintuples.

How big can these sets be (in rationals)?

Gibbs (1999): the first rational Diophantine sextuple

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

Construction of Diophantine sextuples

Dujella, K., Mikić, Szikszai (2016): There are infinitely many rational Diophantine sextuples

Dujella, K., Mikić, Szikszai (2016): There are infinitely many rational Diophantine sextuples

More precisely, there are infinitely many rational Diophantine triples that can be extended to Diophantine sextuples in infinitely many ways.

Example of an infinity family

$$\{a, b, c, d, e, f\}$$

Example of an infinity family

$$\{a, b, c, d, e, f\}$$

$$\begin{aligned}
a &= \frac{18t(t-1)(t+1)}{(t^2-6t+1)(t^2+6t+1)}, \\
b &= \frac{(t-1)(t^2+6t+1)^2}{6t(t+1)(t^2-6t+1)}, \\
c &= \frac{(t+1)(t^2-6t+1)^2}{6t(t-1)(t^2+6t+1)}, \\
d &= d_1/d_2, \\
e &= e_1/e_2, \\
f &= f_1/f_2.
\end{aligned}$$

Example cont'd

$$
\begin{aligned}
d_1 &= 6(t+1)(t-1)(t^2+6t+1)(t^2-6t+1)(8t^6+27t^5+24t^4-54t^3+24t^2+27t+8)\\
&\quad\times(8t^6-27t^5+24t^4+54t^3+24t^2-27t+8)(t^8+22t^6-174t^4+22t^2+1),\\
d_2 &= t(37t^{12}-885t^{10}+9735t^8-13678t^6+9735t^4-885t^2+37)^2,\\
e_1 &= -2t(4t^6-111t^4+18t^2+25)(3t^7+14t^6-42t^5+30t^4+51t^3+18t^2-12t+2)\\
&\quad\times(3t^7-14t^6-42t^5-30t^4+51t^3-18t^2-12t-2)(t^2+3t-2)(t^2-3t-2)\\
&\quad\times(2t^2+3t-1)(2t^2-3t-1)(t^2+7)(7t^2+1),\\
e_2 &= 3(t+1)(t^2-6t+1)(t-1)(t^2+6t+1)\\
&\quad\times(16t^{14}+141t^{12}-1500t^{10}+7586t^8-2724t^6+165t^4+424t^2-12)^2,\\
f_1 &= 2t(25t^6+18t^4-111t^2+4)(2t^7-12t^6+18t^5+51t^4+30t^3-42t^2+14t+3)\\
&\quad\times(2t^7+12t^6+18t^5-51t^4+30t^3+42t^2+14t-3)(2t^2+3t-1)(2t^2-3t-1)\\
&\quad\times(t^2-3t-2)(t^2+3t-2)(t^2+7)(7t^2+1),\\
f_2 &= 3(t+1)(t^2-6t+1)(t-1)(t^2+6t+1)\\
&\quad\times(12t^{14}-424t^{12}-165t^{10}+2724t^8-7586t^6+1500t^4-141t^2-16)^2.
\end{aligned}
$$

Diophantine m-tuples and elliptic curves

To a Diophantine triple $\{a, b, c\}$ we associate the elliptic curve

$$y^2 = (ax + 1)(bx + 1)(cx + 1)$$

or equivalently

$$E_{abc} : y^2 = (x + ab)(x + ac)(x + bc),$$

with points $P = [0, abc]$ and $S = [1, \sqrt{(ab + 1)(ac + 1)(bc + 1)}]$.

Diophantine m-tuples and elliptic curves

To a Diophantine triple $\{a, b, c\}$ we associate the elliptic curve

$$y^2 = (ax + 1)(bx + 1)(cx + 1)$$

or equivalently

$$E_{abc} : y^2 = (x + ab)(x + ac)(x + bc),$$

with points $P = [0, abc]$ and $S = [1, \sqrt{(ab + 1)(ac + 1)(bc + 1)}]$.

Let $T \in E_{abc}(\mathbb{Q})$

$$\left\{a, b, c, \frac{x(T)}{abc}\right\} \text{ is a Diophantine quadruple } \iff T - P = 2E_{abc}(\mathbb{Q}).$$

Extending triples to sextuples

Idea: for a Diophantine triple $\{a, b, c\}$ and $T \in P + 2E_{abc}(\mathbb{Q})$ consider

$$\left\{a, b, c, \frac{x(T)}{abc}, \frac{x(T+S)}{abc}, \frac{x(T-S)}{abc}\right\}.$$

Extending triples to sextuples

Idea: for a Diophantine triple $\{a, b, c\}$ and $T \in P + 2E_{abc}(\mathbb{Q})$ consider

$$\left\{a, b, c, \frac{x(T)}{abc}, \frac{x(T+S)}{abc}, \frac{x(T-S)}{abc}\right\}.$$

One can show that if S is a point of order 3, then the set above in Diophantine sextuple.

Question

Describe rational Diophantine triples $\{a, b, c\}$ for which
$S = [1, \sqrt{(ab+1)(ac+1)(bc+1)}] \in E_{abc}$ is a point of order 3?

Parametrisation

Over $\mathbb{Q}(t)$ such triples are (essentially) parametrized by rational points on the elliptic curve:

$$E : y^2 = x^3 + 3(t^2 - 3t + 1)(t^2 + 3t + 1)x^2 + 3(t^2 + 1)^2(t^4 - 178t^2 + 1)x + (t^2 + 1)^2(t^4 + 110t^2 + 1)^2.$$

Parametrisation

Over $\mathbb{Q}(t)$ such triples are (essentially) parametrized by rational points on the elliptic curve:

$$E : y^2 = x^3 + 3(t^2 - 3t + 1)(t^2 + 3t + 1)x^2 + 3(t^2 + 1)^2(t^4 - 178t^2 + 1)x + (t^2 + 1)^2(t^4 + 110t^2 + 1)^2.$$

$$P = [-(t^2 + 1)(t^2 + 18t + 1), 27t(t + 1)^2(t^2 + 1)] \in E(\mathbb{Q}(t))$$

is the point of infinite order, hence by taking multiples of P we obtain an infinite number of parametric families of Diophantine triples which can be extended to Diophantine sextuples parametrically in an infinite number of ways.

Parametrisation

Over $\mathbb{Q}(t)$ such triples are (essentially) parametrized by rational points on the elliptic curve:

$$E : y^2 = x^3 + 3(t^2 - 3t + 1)(t^2 + 3t + 1)x^2 + 3(t^2 + 1)^2(t^4 - 178t^2 + 1)x + (t^2 + 1)^2(t^4 + 110t^2 + 1)^2.$$

$$P = [-(t^2 + 1)(t^2 + 18t + 1), 27t(t + 1)^2(t^2 + 1)] \in E(\mathbb{Q}(t))$$

is the point of infinite order, hence by taking multiples of P we obtain an infinite number of parametric families of Diophantine triples which can be extended to Diophantine sextuples parametrically in an infinite number of ways.

The family from the introduction corresponds to the point $3P$.

Extending quadruples to sextuples

Proposition (T. Piezas)

Let $\{a, b, c, d\}$ *be a rational Diophantine quadruple, and* x_1 *and* x_2 *the roots of*

$$(abcdx+2abc+a+b+c-d-x)^2 = 4(ab+1)(ac+1)(bc+1)(dx+1).$$

If $x_1x_2 \neq 0$ *and*

$$(abcd-3)^2 = 4(ab+cd+3), \qquad (*)$$

then $\{a, b, c, d, x_1, x_2\}$ *is a Diophantine sextuple.*

Extending quadruples to sextuples

Proposition (T. Piezas)

Let $\{a, b, c, d\}$ *be a rational Diophantine quadruple, and* x_1 *and* x_2 *the roots of*

$$(abcdx+2abc+a+b+c-d-x)^2 = 4(ab+1)(ac+1)(bc+1)(dx+1).$$

If $x_1x_2 \neq 0$ *and*

$$(abcd - 3)^2 = 4(ab + cd + 3), \qquad (*)$$

then $\{a, b, c, d, x_1, x_2\}$ *is a Diophantine sextuple.*

We will reformulate this proposition geometrically.

Correspondence, Dujella, K.

Let $\{a, b, c, d\}$ be a Diophantine quadruple with elements in $\mathbb{Q}$, and let

$$ab + 1 = t_{12}^2 \quad ac + 1 = t_{13}^2 \quad ad + 1 = t_{14}^2$$
$$bc + 1 = t_{23}^2 \quad bd + 1 = t_{24}^2 \quad cd + 1 = t_{34}^2.$$

Correspondence, Dujella, K.

Let $\{a, b, c, d\}$ be a Diophantine quadruple with elements in $\mathbb{Q}$, and let

$$ab + 1 = t_{12}^2 \quad ac + 1 = t_{13}^2 \quad ad + 1 = t_{14}^2$$
$$bc + 1 = t_{23}^2 \quad bd + 1 = t_{24}^2 \quad cd + 1 = t_{34}^2.$$

It follows that $(t_{12}, t_{34}, t_{13}, t_{24}, t_{14}, t_{23}, m' = abcd) \in \mathbb{Q}^7$ defines a point on an algebraic variety $\mathcal{C}$ over $\mathbb{Q}$ defined by the following equations:

$$(t_{12}^2 - 1)(t_{34}^2 - 1) = m'$$
$$(t_{13}^2 - 1)(t_{24}^2 - 1) = m'$$
$$(t_{14}^2 - 1)(t_{23}^2 - 1) = m'.$$

Correspondence cont'd.

The condition $(abcd-3)^2 = 4(ab+cd+3)$ is equivalent to

$$t_{12}t_{34} = \pm t_{12} \pm t_{34}, \text{ or } t_{34} = \pm t_{12}/(t_{12} \pm 1).$$

If we set $t_{12} = t$, $t_{34} = t/(t-1)$ and
$m' = (t^2-1)\frac{t^2}{(t-1)^2-1} = \frac{2t^2+t-1}{t-1}$, the condition (*) is satisfied.

Correspondence cont'd.

Denote by $\mathcal{D} : (x^2 - 1)(y^2 - 1) = m' = \frac{2t^2+t-1}{t-1}$.

Correspondence cont'd.

Denote by $\mathcal{D} : (x^2 - 1)(y^2 - 1) = m' = \frac{2t^2+t-1}{t-1}$.

The curve $\mathcal{D}$ is birationally equivalent to the elliptic curve

$$E : S^2 = T^3 - 2 \cdot \frac{2t^2 - t + 1}{t - 1} T^2 + \frac{(2t - 1)^2(t + 1)^2}{(t - 1)^2} T.$$

Correspondence cont'd.

Denote by $\mathcal{D} : (x^2-1)(y^2-1) = m' = \frac{2t^2+t-1}{t-1}$.

The curve $\mathcal{D}$ is birationally equivalent to the elliptic curve

$$E : S^2 = T^3 - 2 \cdot \frac{2t^2-t+1}{t-1} T^2 + \frac{(2t-1)^2(t+1)^2}{(t-1)^2} T.$$

with point $P = \left[\frac{(2t-1)^2(t+1)}{t-1}, \frac{2t(2t-1)^2(t+1)}{t-1} \right] \in E(\mathbb{Q}(t))$ of infinite order.

Any point on $\mathcal{C}$ corresponds to the three points $Q_1 = (t_{12}, t_{34})$, $Q_2 = (t_{13}, t_{24})$ and $Q_3 = (t_{14}, t_{23})$ on $\mathcal{D}$. When do three points $Q_1 = (t, \frac{t}{t-1}), Q_2, Q_3$ determine a rational Diophantine quadruple?

Correspondence cont'd.

Denote by $\mathcal{D} : (x^2-1)(y^2-1) = m' = \frac{2t^2+t-1}{t-1}$.

The curve $\mathcal{D}$ is birationally equivalent to the elliptic curve

$$E : S^2 = T^3 - 2 \cdot \frac{2t^2-t+1}{t-1} T^2 + \frac{(2t-1)^2(t+1)^2}{(t-1)^2} T.$$

with point $P = \left[\frac{(2t-1)^2(t+1)}{t-1}, \frac{2t(2t-1)^2(t+1)}{t-1} \right] \in E(\mathbb{Q}(t))$ of infinite order.

Any point on $\mathcal{C}$ corresponds to the three points $Q_1 = (t_{12}, t_{34})$, $Q_2 = (t_{13}, t_{24})$ and $Q_3 = (t_{14}, t_{23})$ on $\mathcal{D}$. When do three points $Q_1 = (t, \frac{t}{t-1}), Q_2, Q_3$ determine a rational Diophantine quadruple?

When are the elements rational?

It is enough to prove that one element is rational.

Proposition
Let $Q_2, Q_3 \in E(\mathbb{Q}(t))$.

a) *If* $Q_2 + Q_3 \equiv \mathcal{O} \bmod 2E(\mathbb{Q}(t))$ *then*
$a^2 \equiv (2t-1) \bmod \mathbb{Q}(t)^{\times 2}$.

b) *If* $Q_2 + Q_3 \equiv R \bmod 2E(\mathbb{Q}(t))$ *then*
$a^2 \equiv (t-1)(t+1) \bmod \mathbb{Q}(t)^{\times 2}$.

c) *If* $Q_2 + Q_3 \equiv P \bmod 2E(\mathbb{Q}(t))$ *then*
$a^2 \equiv (t-1)(t+1)(2t-1) \bmod \mathbb{Q}(t)^{\times 2}$.

d) *If* $Q_2 + Q_3 \equiv P + R \bmod 2E(\mathbb{Q}(t))$ *then* $a^2 \equiv 1 \bmod \mathbb{Q}(t)^{\times 2}$.

Example

When we apply our proposition, we obtain a very simple family of sextuples first found by Piezas

Example

When we apply our proposition, we obtain a very simple family of sextuples first found by Piezas

$$
\begin{aligned}
a &= \frac{(t^2-2t-1)\cdot(t^2+2t+3)\cdot(3t^2-2t+1)}{4t\cdot(t^2-1)\cdot(t^2+2t-1)},\\
b &= \frac{4t\cdot(t^2-1)\cdot(t^2-2t-1)}{(t^2+2t-1)^3},\\
c &= \frac{4t\cdot(t^2-1)\cdot(t^2+2t-1)}{(t^2-2t-1)^3},\\
d &= \frac{(t^2+2t-1)\cdot(t^2-2t+3)\cdot(3t^2+2t+1)}{4t\cdot(t^2-1)\cdot(t^2-2t-1)},\\
e &= \frac{-t\cdot(t^2+4t+1)\cdot(t^2-4t+1)}{(t-1)\cdot(t+1)\cdot(t^2+2t-1)\cdot(t^2-2t-1)},\\
f &= \frac{(t-1)\cdot(t+1)\cdot(3t^2-1)\cdot(t^2-3)}{4t\cdot(t^2+2t-1)\cdot(t^2-2t-1)}.
\end{aligned}
$$

Diophantine m-tuples with the strong elements

Strong Diophantine m-tuples

If a rational Diophantine m-tuples has additional property that the square of each element plus 1 is a square, we say that it is **strong**.

Strong Diophantine m-tuples

If a rational Diophantine m-tuples has additional property that the square of each element plus 1 is a square, we say that it is **strong**.

- Dujella and Petričević proved that there are infinitely many strong rational triples, and no example of a strong rational quadruple is known.

Strong Diophantine m-tuples

If a rational Diophantine m-tuples has additional property that the square of each element plus 1 is a square, we say that it is **strong**.

- Dujella and Petričević proved that there are infinitely many strong rational triples, and no example of a strong rational quadruple is known.
- Dujella, K. and Petričević showed that there are infinitely many rational Diophantine sextuples containing a strong pair.

Result

Denote by C an affine curve given by the equation $p(u, v) = 0$ where

$$\begin{aligned} p(u,v) = {} & 3u^4v^4 - 8u^4v^3 + 6u^4v^2 - u^4 \\ & - 8u^3v^4 + 4u^3v^3 - 8u^3v^2 + 12u^3v + 6u^2v^4 \\ & - 8u^2v^3 + 4u^2v^2 + 8u^2v + 6u^2 + 12uv^3 + 8uv^2 \\ & + 4uv + 8u - v^4 + 6v^2 + 8v + 3. \end{aligned}$$

Result

Denote by C an affine curve given by the equation $p(u, v) = 0$ where

$$\begin{aligned} p(u,v) = {} & 3u^4v^4 - 8u^4v^3 + 6u^4v^2 - u^4 \\ & - 8u^3v^4 + 4u^3v^3 - 8u^3v^2 + 12u^3v + 6u^2v^4 \\ & - 8u^2v^3 + 4u^2v^2 + 8u^2v + 6u^2 + 12uv^3 + 8uv^2 \\ & + 4uv + 8u - v^4 + 6v^2 + 8v + 3. \end{aligned}$$

The curve C is birationally equivalent to the elliptic curve

$$E: \quad y^2 + xy + y = x^3 - 33x + 68$$

of rank 1.

Triples parametrised by rational points on elliptic curve

For $(u, v) \in C(\mathbb{Q})$

$$\mathcal{F}_1(u, v) = \left[\frac{2u}{(u-1)(u+1)}, \quad \frac{2v}{(v-1)(v+1)}, \quad \frac{2(v-1)(v+1)(u-1)(u+1)}{(-v+uv-u-1)^2}\right]$$

is a rational Diophantine triple whose first two elements form a strong Diophantine pair.

Triples parametrised by rational points on elliptic curve

For $(u, v) \in C(\mathbb{Q})$

$$\mathcal{F}_1(u, v) = \left[\frac{2u}{(u-1)(u+1)}, \quad \frac{2v}{(v-1)(v+1)}, \quad \frac{2(v-1)(v+1)(u-1)(u+1)}{(-v+uv-u-1)^2}\right]$$

is a rational Diophantine triple whose first two elements form a strong Diophantine pair.

It can be extended to a rational Diophantine sextuple in infinitely many ways (since point S on the corresponding elliptic curve $E_{a,b,c}$ has order 3).

Observation of regularity

Our key insight came from examining numerical examples of special Diophantine triples

$$\{30464/2223,\ 22815/5168,\ 361/7956\},$$
$$\{30464/2223,\ 4807/31824,\ 10881/1292\},$$
$$\{-22815/5168,\ 4807/31824,\ -8092/2223\}.$$

Observation of regularity

Our key insight came from examining numerical examples of special Diophantine triples

$$\{30464/2223,\ 22815/5168,\ 361/7956\},$$
$$\{30464/2223,\ 4807/31824,\ 10881/1292\},$$
$$\{\text{-}22815/5168,\ 4807/31824,\ \text{-}8092/2223\}.$$

For the first triple $\{a, b, c\}$ the (improper) quintuple $\{a, a, b, b, c\}$ is regular. Similarly, for the second and third triple the (improper) quadruple $\{a, b, b, c\}$ is regular. Furthermore, the elliptic curves associated to these Diophantine triples are isomorphic to each other.

D(q)-m-tuples

For a rational number q, we say that the set of m rational numbers is a rational $D(q) - m - tuple$ if the product of any two of its distinct elements is q less then a square.

m-tuples that have $D(n)$-property for more than one n

Adžaga, Dujella, Kreso and Tadić presented several families of Diophantine triples which have $D(n)$-property for two distinct n's with $n \neq 1$ as well as some Diophantine triples which are $D(n)$-sets for three distinct n's with $n \neq 1$.

m-tuples that have $D(n)$-property for more than one n

Adžaga, Dujella, Kreso and Tadić presented several families of Diophantine triples which have $D(n)$-property for two distinct n's with $n \neq 1$ as well as some Diophantine triples which are $D(n)$-sets for three distinct n's with $n \neq 1$.

Dujella and Petričević proved that there are infinitely many integer quadruples which are simultaneously $D(n_1)$ and $D(n_2)$-quadruples with $n_1 \neq n_2$ as well as $D(0)$-quadruples (since the elements of their quadruples are squares).

$D(0)$ and $D(1)$ rational Diophantine quintuples

Note that if $\{a, b, c, d, e\}$ is a $D(n_1)$-quintuple, and u a nonzero rational, then $\{ua, ub, uc, ud, ue\}$ is a $D(n_1u^2)$-quintuple - we say that these two quintuples are equivalent.

$D(0)$ and $D(1)$ rational Diophantine quintuples

Note that if $\{a, b, c, d, e\}$ is a $D(n_1)$-quintuple, and u a nonzero rational, then $\{ua, ub, uc, ud, ue\}$ is a $D(n_1u^2)$-quintuple - we say that these two quintuples are equivalent.

Theorem
Dujella, K., Petričević There are infinitely many nonequivalent quintuples that have $D(n_1)$-property for some $n_1 \in \mathbb{N}$ such that all the elements in the quintuple are perfect squares.

$D(0)$ and $D(1)$ rational Diophantine quintuples

Note that if $\{a, b, c, d, e\}$ is a $D(n_1)$-quintuple, and u a nonzero rational, then $\{ua, ub, uc, ud, ue\}$ is a $D(n_1u^2)$-quintuple - we say that these two quintuples are equivalent.

Theorem
Dujella, K., Petričević There are infinitely many nonequivalent quintuples that have $D(n_1)$-property for some $n_1 \in \mathbb{N}$ such that all the elements in the quintuple are perfect squares.

The theorem will follow if we prove that there are infinitely many rational Diophantine quintuples with the property that the product of any two of its elements is a perfect square (i.e. the quintuple has the $D(0)$ property).

Experimental search

Our starting point was the experimental discovery of an rational Diophantine quintuple

$$\left\{\frac{225^2}{480480}, \frac{2548^2}{480480}, \frac{286^2}{480480}, \frac{1408^2}{480480}, \frac{819^2}{480480}\right\}$$

which by clearing denominators gives Diophantine $D(480480^2)$-quintuple with square elements.

Exotic quintuples

A Diophantine quadruple $\{a, b, c, d\}$ is called *regular* if

$$(a + b - c - d)^2 = 4(ab + 1)(cd + 1).$$

Exotic quintuples

A Diophantine quadruple $\{a, b, c, d\}$ is called *regular* if

$$(a + b - c - d)^2 = 4(ab + 1)(cd + 1).$$

This quintuple $\{a, b, c, d, e\}$ has the following properties

i) $abcd = 1$,

ii) quadruples $\{a, b, d, e\}$ and $\{a, c, d, e\}$ are regular,

iii) $D(0)$-property.

Exotic quintuples

A Diophantine quadruple $\{a, b, c, d\}$ is called *regular* if

$$(a + b - c - d)^2 = 4(ab + 1)(cd + 1).$$

This quintuple $\{a, b, c, d, e\}$ has the following properties

i) $abcd = 1$,

ii) quadruples $\{a, b, d, e\}$ and $\{a, c, d, e\}$ are regular,

iii) $D(0)$-property.

We call such Diophantine quintuples *exotic*.

Diophantine quadruples with $abcd = 1$

Proposition
Let $\{a, b, c, d\}$ be a rational Diophantine quadruple with $abcd = 1$. Then the product of any two elements of the quadruple is a perfect square. We have a rational parametrization of such quadruples.

Parametrization of exotic quintuples

Denote by S the affine surface defined over $\mathbb{Q}$ by

$$(1+r-2r^2t-t^2+rt^2)(-1+r+2r^2t+t^2+rt^2)(-r-r^2-2t-rt^2+r^2t^2)(r-r^2-2t+rt^2+r^2t^2)=y^2.$$

Parametrization of exotic quintuples

Denote by S the affine surface defined over $\mathbb{Q}$ by

$$(1+r-2r^2t-t^2+rt^2)(-1+r+2r^2t+t^2+rt^2)(-r-r^2-2t-rt^2+r^2t^2)(r-r^2-2t+rt^2+r^2t^2)=y^2.$$

Proposition
All exotic quintuples $\{a,b,c,d,e\}$ are parametrized by rational points on S.

Finding low genus curves on S

To show that there are infinitely many exotic quintuples we are led to search for low genus (0 or 1) curves on S.

Finding low genus curves on S

To show that there are infinitely many exotic quintuples we are led to search for low genus (0 or 1) curves on S.

Results

Denote by $\pi : S \to \mathbb{A}^2$ the projection $\pi(r, t, y) = (r, t)$. Let D_1, D_2 and D_3 be plane genus zero curves in $\mathbb{A}^2$ defined by

$$D_1 : r^2t^2 - 4r^2t - 3r^2 - 2rt^2 - 2r - 3t^2 - 4t + 1 = 0,$$
$$D_2 : r^2t - r^2 + 2rt^2 + 2r - t - 1 = 0,$$
$$D_3 : r^2t^2 + 3r^2 - t^2 + 2t - 1 = 0,$$

and let $\widetilde{D_i} = \pi^{-1}(D_i)$ be pullbacks of these curves to S via π.

Results

Denote by $\pi : S \to \mathbb{A}^2$ the projection $\pi(r, t, y) = (r, t)$. Let D_1, D_2 and D_3 be plane genus zero curves in $\mathbb{A}^2$ defined by

$$D_1 : r^2t^2 - 4r^2t - 3r^2 - 2rt^2 - 2r - 3t^2 - 4t + 1 = 0,$$
$$D_2 : r^2t - r^2 + 2rt^2 + 2r - t - 1 = 0,$$
$$D_3 : r^2t^2 + 3r^2 - t^2 + 2t - 1 = 0,$$

and let $\widetilde{D_i} = \pi^{-1}(D_i)$ be pullbacks of these curves to S via π.

Proposition
The curves $\widetilde{D_1}, \widetilde{D_2}$ and $\widetilde{D_3}$ are genus one curves defined over $\mathbb{Q}$ birationally equivalent to elliptic curves with positive Mordell-Weil rank. In particular, there are infinitely many exotic quintuples.

Example

Consider the following parametrization of D_3

$$(r, t) = \left(-\frac{2u+1}{u^2+u+1}, \frac{u^2+4u+1}{(u-1)(u+1)} \right).$$

Example

Consider the following parametrization of D_3

$$(r,t) = \left(-\frac{2u+1}{u^2+u+1}, \frac{u^2+4u+1}{(u-1)(u+1)} \right).$$

It defines a curve birational to $\widetilde{D_3}$ given by the quartic

$$-48\left(u^2-3u-1\right)\left(u^2+5u+3\right) = v^2.$$

The point $(u,v) = (3,36)$ of this quartic corresponds to $(r,t) = (-\frac{7}{13}, \frac{11}{4})$ which in turn is mapped by p to our original exotic Diophantine quintuple

$$\left\{ \frac{225^2}{480480}, \frac{2548^2}{480480}, \frac{286^2}{480480}, \frac{1408^2}{480480}, \frac{819^2}{480480} \right\}.$$

Rational Diophantine sextuples with square denominators

Main result

Theorem (Dujella, K., Petričević)
There are infinitely many rational Diophantine sextuples such that the denominators of all elements (in lowest terms) in the sextuples are perfect squares.

An example

Let $C : t^4 - 1 = -6s^2$ be a curve birationally equivalent to the elliptic curve $E' : y^2 = x^3 + 9x$. Denote by $T = [4, 10]$ the point of infinite order in Mordell-Weil group $E'(\mathbb{Q})$. For $k \in \mathbb{N}$ denote by t_k the t-coordinate of the point on C that corresponds to the point $[k]T$ on $E'(\mathbb{Q})$.

An example

Let $C : t^4 - 1 = -6s^2$ be a curve birationally equivalent to the elliptic curve $E' : y^2 = x^3 + 9x$. Denote by $T = [4, 10]$ the point of infinite order in Mordell-Weil group $E'(\mathbb{Q})$. For $k \in \mathbb{N}$ denote by t_k the t-coordinate of the point on C that corresponds to the point $[k]T$ on $E'(\mathbb{Q})$.

Denote by $\mathcal{F}(t)$ the family of Diophantine sextuples

$$\left\{ -\frac{9\left(t^2+1\right)}{8(t-1)(t+1)}, \frac{\left(t^2-7\right)\left(t^2+1\right)\left(7t^2-1\right)}{8(t-1)^3(t+1)^3}, \frac{8(t-1)^3(t+1)^3}{9\left(t^2+1\right)^3}, -\frac{2\left(t^2+5\right)\left(5t^2+1\right)}{9(t-1)(t+1)\left(t^2+1\right)}, \right.$$
$$-\frac{2t\left(t^2-4t-3\right)\left(3t^2-4t-1\right)\left(t^3+8t^2+5t+4\right)\left(4t^3-5t^2+8t-1\right)}{(t-1)(t+1)\left(t^2+1\right)\left(t^4+34t^2+1\right)^2},$$
$$\left. \frac{2t\left(t^2+4t-3\right)\left(3t^2+4t-1\right)\left(t^3-8t^2+5t-4\right)\left(4t^3+5t^2+8t+1\right)}{(t-1)(t+1)\left(t^2+1\right)\left(t^4+34t^2+1\right)^2} \right\} .$$

An example

Let $C : t^4 - 1 = -6s^2$ be a curve birationally equivalent to the elliptic curve $E' : y^2 = x^3 + 9x$. Denote by $T = [4, 10]$ the point of infinite order in Mordell-Weil group $E'(\mathbb{Q})$. For $k \in \mathbb{N}$ denote by t_k the t-coordinate of the point on C that corresponds to the point $[k]T$ on $E'(\mathbb{Q})$.

Denote by $\mathcal{F}(t)$ the family of Diophantine sextuples

$$\left\{ -\frac{9\left(t^2+1\right)}{8(t-1)(t+1)}, \frac{\left(t^2-7\right)\left(t^2+1\right)\left(7t^2-1\right)}{8(t-1)^3(t+1)^3}, \frac{8(t-1)^3(t+1)^3}{9\left(t^2+1\right)^3}, -\frac{2\left(t^2+5\right)\left(5t^2+1\right)}{9(t-1)(t+1)\left(t^2+1\right)}, \right.$$
$$-\frac{2t\left(t^2-4t-3\right)\left(3t^2-4t-1\right)\left(t^3+8t^2+5t+4\right)\left(4t^3-5t^2+8t-1\right)}{(t-1)(t+1)\left(t^2+1\right)\left(t^4+34t^2+1\right)^2},$$
$$\left. \frac{2t\left(t^2+4t-3\right)\left(3t^2+4t-1\right)\left(t^3-8t^2+5t-4\right)\left(4t^3+5t^2+8t+1\right)}{(t-1)(t+1)\left(t^2+1\right)\left(t^4+34t^2+1\right)^2} \right\}.$$

For every $k \equiv 1, 2 \pmod 3$ the denominators of all the elements of $\mathcal{F}(t_k)$ are perfect squares.

Numerical experiment

Our starting point is an example of a Diophantine sextuple with square denominators

$$\mathcal{L} = \left\{ \frac{75}{8^2}, -\frac{3325}{64^2}, -\frac{12288}{125^2}, \frac{123}{10^2}, \frac{3498523}{2260^2}, \frac{698523}{2260^2} \right\},$$

which we have discovered (together with seventeen other examples) by a numerical search.

A pattern

The sextuple $\mathcal{L} = \{a, b, c, d, e, f\}$ has the following structure:

A pattern

The sextuple $\mathcal{L} = \{a, b, c, d, e, f\}$ has the following structure:

- Diophantine quintuples $\{a, b, c, d, e\}$ and $\{a, b, c, d, f\}$ are regular, i.e. e and f are roots of the

  $$(abcdx+2abc+a+b+c-d-x)^2 = 4(ab+1)(ac+1)(bc+1)(dx+1),$$

- Diophantine quadruple $\{a, b, c, d\}$ has the property that

  $$(abcd - 3)^2 = 4(ab + cd + 3).$$

A pattern

The sextuple $\mathcal{L} = \{a, b, c, d, e, f\}$ has the following structure:

- Diophantine quintuples $\{a, b, c, d, e\}$ and $\{a, b, c, d, f\}$ are regular, i.e. e and f are roots of the

  $$(abcdx+2abc+a+b+c-d-x)^2 = 4(ab+1)(ac+1)(bc+1)(dx+1),$$

- Diophantine quadruple $\{a, b, c, d\}$ has the property that

  $$(abcd - 3)^2 = 4(ab + cd + 3).$$

Such sextuples have been described in the paper Dujella, K.: More on Diophantine sextuples. Using that work we want to construct a family that contains quadruple $\mathcal{L}$.

Parametrization

Denote by $\mathcal{D} : (x^2-1)(y^2-1) = \frac{2t^2+t-1}{t-1}$ a genus one curve over $\mathbb{Q}(t)$ birationally equivalent to the elliptic curve

$$E : S^2 = T^3 - 2 \cdot \frac{2t^2-t+1}{t-1} T^2 + \frac{(2t-1)^2(t+1)^2}{(t-1)^2} T.$$

Parametrization

Denote by $\mathcal{D} : (x^2-1)(y^2-1) = \frac{2t^2+t-1}{t-1}$ a genus one curve over $\mathbb{Q}(t)$ birationally equivalent to the elliptic curve

$$E : S^2 = T^3 - 2 \cdot \frac{2t^2-t+1}{t-1} T^2 + \frac{(2t-1)^2(t+1)^2}{(t-1)^2} T.$$

Denote by

- $P = \left[\frac{(2t-1)^2(t+1)}{t-1}, \frac{2t(2t-1)^2(t+1)}{t-1} \right] \in E(\mathbb{Q}(t))$ a point of infinite order,
- $R = \left[\frac{(t+1)(2t-1)}{(t-1)}, \frac{2(t+1)(2t-1)}{t-1} \right]$ a point of order 4.

Looking for a specialization

One can check that the quadruple $\{a, b, c, d\}$ from $\mathcal{L}$ corresponds to $t_0 = 113/625$.

Looking for a specialization

One can check that the quadruple $\{a, b, c, d\}$ from $\mathcal{L}$ corresponds to $t_0 = 113/625$.

Inspired by the fact that $\frac{1-t_0}{2} = (16/25)^2$ is a square, we restrict to the subfamily $t := 1 - 2t^2$.

Looking for a specialization

One can check that the quadruple $\{a, b, c, d\}$ from $\mathcal{L}$ corresponds to $t_0 = 113/625$.

Inspired by the fact that $\frac{1-t_0}{2} = (16/25)^2$ is a square, we restrict to the subfamily $t := 1 - 2t^2$.

If we further specialize $t := \frac{3t^2+3}{4t^2-4}$ and denote the resulting elliptic curve also by E, then we obtain another point of infinite order in $E(\mathbb{Q}(t))$.

Another point

$$Q = \left[-\frac{\left(t^2+5\right)^2\left(5t^2+1\right)^2}{36(t-1)^2(t+1)^2\left(t^2+1\right)^2}, \frac{t\left(t^2+5\right)^2\left(5t^2+1\right)^2}{9(t-1)^2(t+1)^2\left(t^2+1\right)^3} \right].$$

One can obtain the family $\mathcal{F}$ from the points $(P, Q, P+R)$, and we get $\mathcal{L}$ if we specialize to $t = -1/7$, i.e. $\mathcal{L} = \mathcal{F}(-1/7)$.

p-adic analysis

From some elementary p-analysis of denominators of $\mathcal{F}(t_k)$, it follows that all the denominators are perfect squares.

Thank you for your attention!