Rational Diophantine sextuples with strong pair

Andrej Dujella

Department of Mathematics, Faculty of Science
University of Zagreb, Croatia
URL: `https://web.math.pmf.unizg.hr/~duje/`

Joint work with **Matija Kazalicki** *and* **Vinko Petričević**

Supported by the QuantiXLie Center of Excellence

8th Croatian Mathematical Congress, Osijek, 2024

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: $\{1, 3, 8, 120, \frac{777480}{8288641}\}$
(extension is unique – Stoll (2019))

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

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 Denton (1957), Gardner (1967), van Lint (1968))

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

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

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.

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

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.

If in addition, a rational Diophantine m-tuple has the property that the square of each element plus 1 is a square, we say that it is strong.

D. & Petričević (2008): There are infinitely many strong rational triples.

No example of a strong rational quadruple is known.

D., Gusić, Petričević & Tadić (2018) and **D., Paganin & Sadek (2020):** Generalizations to strong $D(-1)$ and strong $D(q)$-triples.

Theorem: There are infinitely many rational Diophantine sextuples that contain a strong Diophantine pair.

Example: The sextuple

$$\left\{\frac{30464}{2223}, \frac{22815}{5168}, \frac{361}{7956}, \frac{85524782446417734784}{49119640878715960913}, \right.$$

$$\frac{1109399105264038520087475}{5658475994988984144l728368},$$

$$\left.\frac{10415499568210504847837540 75}{2227035543179601212214436 8}\right\}.$$

contains a strong pair $\left\{\frac{30464}{2223}, \frac{22815}{5168}\right\}$.

Elliptic curves induced by Diophantine triples

Let $\{a, b, c\}$ be a rational Diophantine triple. To extend this triple to a quadruple, we consider the system

$$ax + 1 = \square, \qquad bx + 1 = \square, \qquad cx + 1 = \square. \tag{1}$$

It is natural to assign the elliptic curve

$$\mathcal{E}: \qquad y^2 = (ax + 1)(bx + 1)(cx + 1)$$

to the system (1). We say $\mathcal{E}$ is induced by the triple $\{a, b, c\}$.

Three rational points on the $\mathcal{E}$ of order 2:

$$A = [-1/a, 0], \quad B = [-1/b, 0], \quad C = [-1/c, 0]$$

and also other obvious rational points

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

The x-coordinate of a point $T \in \mathcal{E}(\mathbb{Q})$ satisfies (1) if and only if $T - P \in 2\mathcal{E}(\mathbb{Q})$.

It holds that $S \in 2\mathcal{E}(\mathbb{Q})$. Indeed, if $ab+1 = r^2$, $ac+1 = s^2$, $bc+1 = t^2$, then $S = [2]V$, where

$$V = \left[\frac{rs+rt+st+1}{abc}, \frac{(r+s)(r+t)(s+t)}{abc}\right].$$

This implies that if $x(T)$ satisfies system (1), then also the numbers $x(T \pm S)$ satisfy the system.

D. (1997,2001): $x(T)x(T \pm S)+1$ is always a perfect square.

Proposition (DKMS): Let Q, T and $[0, \alpha]$ be three rational points on an elliptic curve $\mathcal{E}$ over $\mathbb{Q}$ given by the equation $y^2 = f(x)$, where f is a monic polynomial of degree 3. Assume that $\mathcal{O} \notin \{Q, T, Q+T\}$. Then

$$x(Q)x(T)x(Q+T) + \alpha^2$$

is a perfect square.

$x \mapsto x/abc$, $y \mapsto y/abc$, applied to $\mathcal{E}$ leads to

$$E' : \qquad y^2 = (x+ab)(x+ac)(x+bc)$$

The points P and S become $P' = [0, abc]$ and $S' = [1, rst]$, respectively.

If we apply Proposition 1 with $Q = \pm S'$, since $x(S') = 1$, we get a simple proof of the fact that $x(T)x(T \pm S) + 1$ is a perfect square (after dividing $x(T')x(T' \pm S') + a^2b^2c^2 = \square$ by $a^2b^2c^2$).

Now we have a general construction which produces two rational Diophantine quintuples with four joint elements. So, the union of these two quintuples,

$$\{a, b, c, x(T-S), x(T), x(T+S)\},$$

is "almost" a rational Diophantine sextuple.

Assuming that $T, T \pm S \notin \{\mathcal{O}, \pm P\}$, the only missing condition is

$$x(T-S) \cdot x(T+S) + 1 = \square.$$

To construct examples satisfying this last condition, we will use the Proposition with $Q = [2]S'$. To get the desired conclusion, we need the condition $x([2]S') = 1$ to be satisfied. This leads to $[2]S' = -S'$, i.e. $[3]S' = \mathcal{O}$.

Lemma (DKMS): For the point $S' = [1, rst]$ on E' it holds $[3]S' = \mathcal{O}$ if and only if $S(a,b,c) = 0$, where

$$S(a,b,c) = 3 + 4(ab + ac + bc) + 6abc(a + b + c)$$
$$+ 12(abc)^2 - (abc)^2(a^2 + b^2 + c^2 - 2ab - 2ac - 2bc).$$

Thus we are led to the following question.

Question: Are there infinitely many rational Diophantine triples $\{a,b,c\}$ for which a^2+1 and b^2+1 are perfect squares and $S(a,b,c) = 0$?

Definition: A quadruple (a, b, c, d) is called regular if $r_4(a, b, c, d) = 0$, where

$$r_4(a, b, c, d) = (a + b - c - d)^2 - 4(ab + 1)(cd + 1).$$

A quintuple (a, b, c, d, e) is called regular if $r_5(a, b, c, d, e) = 0$, where

$$r_5(a, b, c, d, e) = (abcde + 2abc + a + b + c - d - e)^2 - 4(ab + 1)(ac + 1)(bc + 1)(de + 1).$$

Note that polynomials r_4 and r_5 are symmetric.

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

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

We noticed that for the first triple $\{a, b, c\}$ the (improper) quintuple $\{a, a, b, b, c\}$ is regular, i.e. $r_5(a, a, b, b, c) = 0$. Similarly, for the second and third triple the (improper) quadruple $\{a, b, b, c\}$ is regular, i.e. $r_4(a, b, b, c) = 0$. Furthermore, the elliptic curves associated to these Diophantine triples are isomorphic to each other.

These regularity conditions can be restated in the context of the arithmetic of the elliptic curve E induced by the triple $\{a, b, c\}$ and the points A, B, C, P and S.

Proposition: Let $\{a, b, c\}$ be a rational Diophantine triple containing a strong pair $\{a, b\}$. We have that

a) $r_4(a, a, b, c) = 0$ if and only if $A = \pm P \pm S$ for some choice of signs,

b) $r_5(a, a, b, b, c) = 0$ if and only if $A \pm B \pm S = \mathcal{O}$ for some choice of signs.

Set $a = \frac{2u}{u^2-1}$ and $b = \frac{2v}{v^2-1}$ to ensure that a^2+1 and b^2+1 are perfect squares. If we substitute these values in

$$r_5(a,a,b,b,c) = (abc)^2 - 2ac^2b - 4ac + c^2 - 4cb - 4$$

the resulting expression factors as $r_5(a,a,b,b,c) = q_1 q_2$ where

$$\begin{aligned} q_2 \; &= cv^2 - 2ucv^2 + 2cv + u^2v^2c - 2cvu^2 + cu^2 \\ &\quad + 2uc + c - 2 + 2v^2 - 2u^2v^2 + 2u^2. \end{aligned}$$

Solving for c in $q_2 = 0$ we obtain two solutions, one of which is

$$c = \frac{2(u^2v^2 - u^2 - v^2 + 1)}{(uv - u - v - 1)^2}.$$

If we substitute all this in $S(a,b,c)=0$, the expression factors as $s_1 s_2 s_3$, where

$$s_2 = 3u^4v^4 - 8u^4v^3 + 6u^4v^2 - u^4 - 8u^3v^4 + 4u^3v^3 - 8u^3v^2 + 12u^3v + 6u^2v^4 - 8u^2v^3 + 4u^2v^2 + 8u^2v + 6u^2 + 12uv^3 + 8uv^2 + 4uv + 8u - v^4 + 6v^2 + 8v + 3.$$

We claim that if u and v are rationals such that $s_2(u,v) = 0$, then the triple

$$\left\{\frac{2u}{(u-1)(u+1)}, \frac{2v}{(v-1)(v+1)}, \frac{2(v-1)(v+1)(u-1)(u+1)}{(-v+uv-u-1)^2}\right\}$$

has the following properties:

- it is a rational Diophantine triple,
- it contains a strong pair,
- it can be extended to infinitely many rational Diophantine sextuples.

All properties follow directly from the construction, except the condition that $ab+1$ is a perfect square.

Let $t(u,v)$ denote the product of the denominator and numerator of $ab+1$. It is straightforward to verify that

$$s_2(u,v)+t(u,v)=(uv+1)^2(uv-u-v-1)^2,$$

hence $t(u,v)$ is a perfect square (as is $ab+1$) whenever $s_2(u,v)=0$.

It remains to show that the curve C defined by the equation $s_2(u, v) = 0$ has infinitely many rational points.

Using `Magma`, we find the curve C is a genus 1 curve birationally equivalent to the elliptic curve

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

The torsion subgroup of Mordell-Weil group of E over $\mathbb{Q}$ is generated by the point $[-1, 10]$ of order 6, while the free part of the group is generated by the point $[11/4, -25/8]$ (it has rank 1). In particular, E (and thus also C) has infinitely many rational points.

Thank you very much
for your attention!