There are infinitely many rational Diophantine sextuples

Andrej Dujella

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

Joint work with Matija Kazalicki, Miljen Mikić and Márton Szikszai

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

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

Euler: There are infinitely many Diophantine quadruples in integers. E.g. $\{k-1, k+1, 4k, 16k^3-4k\}$ for $k \geq 2$.

Conjecture: There does not exist a Diophantine quintuple in integers.

D. (2004): There does not exist a Diophantine sextuple in integers, and there are only finitely many quintuples.

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

Euler: There are infinitely many rational Diophantine quintuples. E.g. $\{1, 3, 8, 120, \frac{777480}{8288641}\}$. 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).

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?

$$e, f = \frac{(a+b+c+d)(abcd+1) + 2abc + 2abd + 2acd + 2bcd \pm 2\sqrt{A}}{(abcd-1)^2},$$

where

$$A = (ab+1)(ac+1)(ad+1)(bc+1)(bd+1)(cd+1).$$

Gibbs (1999): $\left\{\frac{5}{36}, \frac{5}{4}, \frac{32}{9}, \frac{189}{4}, \frac{665}{1521}, \frac{3213}{676}\right\}$

Dujella (2009): $\left\{\frac{5}{14}, \frac{7}{2}, \frac{48}{7}, \frac{1680}{361}, -\frac{2310}{19321}, \frac{93840}{71407}\right\}$

Dujella, Kazalicki, Mikić & Szikszai (2016): 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.

Open question:

Is there any rational Diophantine septuple?

Is there any rational Diophantine quintuple (quadruple) which can be extended to two different sextuples?

By DKMS (2016), there exist infinitely many triples, each of which can be extended to sextuples on infinitely many ways.

Herrmann, Pethő & Zimmer (1999): A rational Diophantine quadruple has only finitely many extensions to a rational Diophantine quintuple.

Piezas; D. & Kazalicki (2016): There are infinitely many sextuples $\{a, b, c, d, e, d\}$ with fixed products ab and cd.

Induced elliptic curves

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

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

to the system (1). We say the $\mathcal{E}$ 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. With $x(T) = d$, the numbers $x(T \pm S)$ are exactly e and f.

Proposition 1: Let Q, T and $[0, \alpha]$ be three rational points on an elliptic curve 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.

The transformation $x \mapsto x/abc$, $y \mapsto y/abc$, 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

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

To construct examples satisfying this last condition, we will use Proposition 1 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 1: For the point $S' = [1, rst]$ on E' it holds $[3]S' = \mathcal{O}$ if and only if

$$\begin{aligned} &-a^4b^2c^2 + 2a^3b^3c^2 + 2a^3b^2c^3 - a^2b^4c^2 + 2a^2b^3c^3 \\ &-a^2b^2c^4 + 12a^2b^2c^2 + 6a^2bc + 6ab^2c + 6abc^2 \\ &+4ab + 4ac + 4bc + 3 = 0. \end{aligned} \tag{3}$$

The polynomial in a, b, c on the left hand side of (3) is symmetric. Thus, by taking $\sigma_1 = a + b + c$, $\sigma_2 = ab + ac + bc$, $\sigma_3 = abc$, we get from (3) that

$$\sigma_2 = (\sigma_1^2\sigma_3^2 - 12\sigma_3^2 - 6\sigma_1\sigma_3 - 3)/(4 + 4\sigma_3^2). \tag{4}$$

Inserting (4) in $(ab+1)(ac+1)(bc+1) = (rst)^2$, we get $(2\sigma_3^2 + \sigma_1\sigma_3 - 1)^2/(4 + 4\sigma_3^2) = (rst)^2$, i.e. $1 + \sigma_3^2 = \square$.

The polynomial

$$X^3 - \sigma_1 X^2 + \sigma_2 X - \sigma_3$$

should have rational roots, so its discriminant has to be a perfect square. Inserting (4) in the expression for the discriminant, we get

$$(\sigma_1^3\sigma_3 - 9\sigma_1^2 - 27\sigma_1\sigma_3 - 54\sigma_3^2 - 27)(1+\sigma_3^2)(\sigma_1\sigma_3 + 2\sigma_3^2 - 1) = \square. \quad (5)$$

For a fixed σ_3, we may consider (5) as a quartic in σ_1. Since $1+\sigma_3^2$ has to be a perfect square, from (5) we get a quartic with a rational point (point at infinity), which therefore can be transformed into an elliptic curve.

Let us take $\sigma_3 = \frac{t^2-1}{2t}$. Then we get the quartic over $\mathbb{Q}(t)$ which is birationally equivalent to the following elliptic curve over $\mathbb{Q}(t)$

$$E: \quad y^2 = x^3 + (3t^4 - 21t^2 + 3)x^2 + (3t^8 + 12t^6 + 18t^4 + 12t^2 + 3)x + (t^2+1)^6. \quad (6)$$

This elliptic curve has positive rank, since the point $R = [0, (t^2+1)^3]$ is of infinite order.

By taking multiples $[m]R$ of the point R, transforming these coordinates back to the quartic and computing corresponding triples $\{a, b, c\}$, we may expect to get infinitely many parametric families of rational triples for which the corresponding point S' on E' satisfies $[3]S' = \mathcal{O}$.

In particular, if we take the point $[2]R$, we get the following family of rational Diophantine triples

$$a = \frac{18t(t-1)(t+1)}{(t^2-6t+1)(t^2+6t+1)},$$
$$b = \frac{(t-1)(t^2+6t+1)^2}{6t(t+1)(t^2-6t+1)},$$
$$c = \frac{(t+1)(t^2-6t+1)^2}{6t(t-1)(t^2+6t+1)}.$$

Consider now the elliptic curve over $\mathbb{Q}(t)$ induced by the triple $\{a, b, c\}$. It has positive rank since the point $P = [0, 1]$ is of infinite order. Thus, the above described construction produces infinitely many rational Diophantine sextuples containing the triple $\{a, b, c\}$. One such sextuple $\{a, b, c, d, e, f\}$ is obtained by taking x-coordinates of points $[3]P$, $[3]P + S$, $[3]P - S$.

We get $d = d_1/d_2$, $e = e_1/e_2$, $f = f_1/f_2$, where

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

These formulas produce infinitely many rational Diophantine sextuples. Moreover, by choosing the rational parameter t from the appropriate interval, we get infinitely many sextuples for each combination of signs. E.g., for $5.83 < t < 6.86$ all elements are positive. As a specific example, let us take $t = 6$, for which we get a sextuple with all positive elements:

$$\left\{\frac{3780}{73}, \frac{26645}{252}, \frac{7}{13140}, \frac{791361752602550684660}{1827893092234556692801},\right.$$
$$\frac{9510485270981580922898 1184}{3510419116546513356332669 55},$$
$$\left.\frac{3210891270762333567521084544}{21712719223923581005355}\right\}.$$

The construction of the above parametric family of rational Diophantine sextuples relies on the fact that the cubic polynomial corresponding to the point $[2]R$ has rational roots.

Is the same true for all multiples $[m]R$ of R? YES!

Is the same true for all other points on the curve (6) (in the case when the rank is > 1)? NO!

For example for $t = 31$ (when the rank of (6) is 2) and point $[x, y] = [-150072, 682327360]$ (which is not a multiple of R) the polynomial $X^3 - \sigma_1 X^2 + \sigma_2 X - \sigma_3$ has no rational roots.

Curves with high rank and/or large torsion

Our parametric formula for the rational Diophantine sextuples $\{a, b, c, d, e, f\}$ can be used to obtain an elliptic curve over $\mathbb{Q}(t)$ with reasonably high rank. The curve

$$y^2 = (dx + 1)(ex + 1)(fx + 1).$$

has rank ≥ 5 over $\mathbb{Q}(t)$ and torsion group $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

The curve

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

has subfamilies with rank 2 over $\mathbb{Q}(t)$ and particular examples with rank 6 over $\mathbb{Q}$ and torsion group $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$ (D. & Peral (2016)), and also subfamily with torsion group $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/12\mathbb{Z}$ over certain quadratic fields (D. & Jukić Bokun & Soldo (2016)).