On elliptic curves induced by rational Diophantine quadruples

Andrej Dujella

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

Joint work with **Gökhan Soydan**

Supported by the QuantiXLie Center of Excellence

**Number Theory Conference in honour of Professors
Kálmán Győry, János Pintz and András Sárközy,
Debrecen, 2022**

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.

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

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

It is natural to assign the elliptic curve

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

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

- used in construction of families of rational Diophantine sextuples

- used for obtaining previous and current records for ranks of elliptic curves over $\mathbb{Q}$ and $\mathbb{Q}(t)$ with torsion groups $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/k\mathbb{Z}$ for $k = 2, 4, 6, 8$
(**D. (2000,2007), Aguirre, D., Peral (2012), D., Peral (2014,2019,2020,2021)**)

- integer points for parametric families of triples
(**D., Pethő (Publ. Math. Debrecen, 2000), D. (2000,2001), Najman (2009,2010)**)

Elliptic curves induced by Diophantine quadruples

Let $\{a, b, c, d\}$ be a rational Diophantine quadruple. To extend it to a rational Diophantine quintuple, we need to find an X such that $aX + 1$, $bX + 1$, $cX + 1$ and $dX + 1$ are squares of rational numbers. As before, we can multiply these four conditions and we obtain

$$Y^2 = (aX + 1)(bX + 1)(cX + 1)(dX + 1),$$

which is a genus 1 curve. By the substitution

$$y = \frac{Y(d-a)(d-b)(d-c)}{(dX+1)^2}, \qquad x = \frac{(aX+1)(d-b)(d-c)}{dX+1},$$

we obtain the following elliptic curve

$$E: \quad y^2 = x(x + (b-a)(d-c))(x + (c-a)(d-b)).$$

We say that this elliptic curve is induced by the rational Diophantine quadruple $\{a, b, c, d\}$.

Question: Which torsion groups are possible for elliptic curves induced by rational Diophantine quadruples?

D., Soydan (2022): All four torsion groups that are allowed by Mazur's theorem, $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/k\mathbb{Z}$ for $k = 2, 4, 6, 8$, are possible, and in fact they can be achieved for infinitely many rational Diophantine quadruples.

In each of four cases, we also found curves with moderately large rank.

There are three non-trivial rational 2-torsion points on E:

$A = (0,0), \quad B = (-(b-a)(d-c), 0), \quad C = (-(c-a)(d-b), 0),$
and another two obvious rational points:

$P = ((b-a)(c-a),\, (b-a)(c-a)(d-a)),$
$Q = ((ad+1)(bc+1),\, \sqrt{(ab+1)(ac+1)(ad+1)(bc+1)(bd+1)(cd+1)}).$

The points P and Q will play an important role in our constructions. In particular, we will be interested in question under which assumptions these points may have finite order.

Torsion $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$

- rank 8 examples (D. (2000))

- rank 9 examples based of new rational Diophantine sextuples found by Gibbs (2016), e.g.

$$\{a,b,c,d\} = \left\{\frac{8064}{597529}, \frac{1408}{75}, \frac{16225}{48}, \frac{3337875}{16}\right\}$$

- rank 10 examples within parametric families of rational Diophantine quadruples

A Diophantine triple $\{a, b, c\}$ is called regular if $c = a + b + 2r$, where $ab + 1 = r^2$. We consider rational Diophantine quadruples $\{a, b, c, d\}$ such that the triples $\{a, b, c\}$ and $\{b, c, d\}$ are both regular. This leads to

$$b = \frac{(t^2 - 2at - 4t + 3)(t^2 - 2at + 4t + 3)}{16t^2 a},$$
$$c = \frac{(t^2 + 2at + 4t + 3)(t^2 + 2at - 4t + 3)}{16t^2 a},$$
$$d = \frac{(t - 1)(t + 3)(t - 3)(t + 1)}{4t^2 a}.$$

We were able to find several curves with rank 9 within corresponding family of elliptic curves.

To increase the rank, we choose a such that a^2+1 is a perfect square, i.e

$$a = \frac{v^2-1}{2v}.$$

We used the standard sieving methods based on Mestre-Nagao sums and computing Selmer rank as an upper bound for the rank. We found two curves with rank 10, corresponding to $t = \frac{142}{53}$, $v = \frac{142}{23}$,

$$\{a,b,c,d\} = \left\{\frac{19635}{6532}, -\frac{46592463}{201832268}, \frac{84196064}{50458067}, -\frac{1144273}{8775316}\right\}$$

and $t = \frac{59}{4}$, $v = \frac{59}{34}$,

$$\{a,b,c,d\} = \left\{\frac{2325}{4012}, \frac{187020623}{9949760}, \frac{261411943}{9949760}, \frac{13104399}{146320}\right\}.$$

Torsion $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$

Consider the curve

$$E: \qquad y^2 = x(x+p_1)(x+p_2),$$

where $p_1 = (b-a)(d-c)$, $p_2 = (c-a)(d-b)$.

By the 2-descent, the point Q with $x(Q) = (ad+1)(bc+1)$ is in $2E(\mathbb{Q})$, because $x_1 = (ad+1)(bc+1)$, $x_1+p_1 = (ac+1)(bd+1)$ and $x_1+p_2 = (ab+1)(cd+1)$ are perfect squares. The point Q is of order 2 if say $ad+1=0$, i.e. if $d = -1/a$. So the point R such that $2R = Q$ is of order 4 and $E(\mathbb{Q})$ has a subgroup $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$.

Thus we need to find rational Diophantine quadruples which contain a subtriple of the form $\{a, -1/a, b\}$. We use the following two-parametric solution given in D. (2007):

$$a = \frac{ut+1}{t-u}, \qquad b = \frac{4tu}{(tu+1)(t-u)}.$$

To find the fourth element c of the quadruple, we may take c such that $\{a, b, c, d\}$ is a regular quadruple,

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

In that way, we get

$$c = \frac{(u-1)(u+1)(t-1)(t+1)}{(ut+1)(t-u)}.$$

Hence, we showed that there are infinitely many rational Diophantine quadruples which induces curves with torsion group $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$.

Other possibility it is take c to be $\frac{8(d-a-b)(a+d-b)(b+d-a)}{(a^2+b^2+d^2-2ab-2ad-2bd)^2}$ so we get another two-parametric family of quadruple with the same property.

Within this family of quadruples, we were able to find examples of curves with rank equal to 6, e.g. for $(t, u) = (3, 1/12)$, corresponding to the quadruple

$$\left\{\frac{3}{7}, \frac{48}{175}, -\frac{625153729200}{363378690481}, -\frac{7}{3}\right\}.$$

Torsion $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$

To achieve the torsion group $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$, we will find quadruples for which the condition $3Q = \mathcal{O}$ is satisfied, since then the point R such that $2R = Q$ will be a point of order 6.

To simplify the condition $3Q = \mathcal{O}$, we assume that $\{a, b, c, d\}$ is a regular quadruple.

Then we may take $R = \pm P$.

We use the parametrization of Diophantine triples $\{a, b, c\}$, due to Lasić (an appendix of Kazalicki, Naskrecki (2022)):

$$a = \frac{2t_1(1 + t_1t_2(1 + t_2t_3))}{(-1 + t_1t_2t_3)(1 + t_1t_2t_3)},$$
$$b = \frac{2t_2(1 + t_2t_3(1 + t_3t_1))}{(-1 + t_1t_2t_3)(1 + t_1t_2t_3)},$$
$$c = \frac{2t_3(1 + t_3t_1(1 + t_1t_2))}{(-1 + t_1t_2t_3)(1 + t_1t_2t_3)},$$

followed by the substitutions

$$t_1 = \frac{k}{t_2t_3}, \quad t_2 = m - \frac{1}{t_3}.$$

The regularity equation $(a+b-c-d)^2 = 4(ab+1)(cd+1)$, gives as one solution for d:

$$d = \frac{-2(1 - t_1 + t_3t_1)(-t_3 + t_2t_3 + 1)(-t_2 + 1 + t_1t_2)(-1 + t_1t_2t_3)}{(1 + t_1t_2t_3)^3}.$$

Now the condition $3Q = \mathcal{O}$ become a complicated algebraic equation in terms of t_3, k and m. It simplifies if we take (motivated by experimental data)

$$2 + t_3 k = \frac{3}{k^2 + 2},$$

i.e.

$$t_3 = \frac{-(2k^2 + 1)}{k(k^2 + 2)}.$$

This gives as one possibility of m:

$$m = \frac{3k(-2 + k - 2k^2 + k^3)}{2(2k^2 + 1)(k^2 - k + 1)}.$$

Finally, we can express a, b, c, d in terms of k:

$$a = \frac{-2k(k^2+2)(3k^3-2k^2+2k-2)}{(1+k)(k-1)(2k^2+1)(2k^2+k+2)},$$
$$b = \frac{-k(1+k)(k-1)(2k^2+k+2)(4k^2-k+4)}{2(k^2+2)(k^2-k+1)^2(2k^2+1)},$$
$$c = \frac{2(2k^2+1)(2k^3-2k^2+2k-3)}{(1+k)(k-1)(2k^2+k+2)(k^2+2)},$$
$$d = \frac{(2k^2+1)(1+k)(k^2+2)(k-1)}{2(k^2-k+1)^2(2k^2+k+2)}.$$

Hence, we obtained an infinite family of quadruples which induces curves with torsion group $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$.

For $k = 23$, we get the curve with rank 3, corresponding to the quadruple

$$\left\{-\frac{16051953}{11214104}, -\frac{170244712}{1784519841}, \frac{914623}{5622936}, \frac{5498328}{10310521}\right\}.$$

Torsion $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$

We start with the quadruple $\{a, b, c, d\}$, which gave us torsion group $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$:

$$a = \frac{ut+1}{t-u}, \quad b = \frac{4ut}{(ut+1)(t-u)},$$
$$c = \frac{(u-1)(u+1)(t-1)(t+1)}{(ut+1)(t-u)}, \quad d = -\frac{t-u}{ut+1}.$$

The point $Q = (0, 0)$ of order 2 is in $2E(\mathbb{Q})$, so there is point R such that $2R = Q$. To get the torsion group $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$, we just have to force the point R to be in $2E(\mathbb{Q})$, i.e. $R = 2S$, for a point S in $E(\mathbb{Q})$. Then the point S will be of order 8.

The point R has coordinates:

$$\left(\frac{(u+t)^2(ut-1)^2}{(ut+1)^2(t-u)^2}, \frac{(u^2+1)(t^2+1)(u+t)^2(ut-1)^2}{(ut+1)^3(t-u)^3}\right).$$

We want that for $x_1 = \frac{(u+t)^2(ut-1)^2}{(ut+1)^2(t-u)^2}$, x_1+p_1 and x_1+p_2 are squares. But x_1 is already a square, while $x_1+p_1 = \square$ and $x_1+p_2 = \square$ both lead to the same condition: $(u^2+1)(t^2+1)$ is a square. Put

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

and we get

$$t = -\frac{-2u^2v-2v+v^2u+u^3+u}{u^2+1-v^2},$$

and finally,

$$\begin{aligned}
a &= \frac{(u-v+1)(u-v-1)}{2(u-v)},\\
b &= -\frac{2(u^2+1-v^2)u(-2u^2v-2v+v^2u+u^3+u)}{(u^2+1)^2(u-v)(u-v+1)(u-v-1)},\\
c &= \frac{(-2u^2v-2v+v^2u+u^3+u-u^2-1+v^2)}{2(u^2+1)^2(u-v)(u-v+1)(u-v-1)}\times\\
&\quad\times(-2u^2v-2v+v^2u+u^3+u+u^2+1-v^2)(u+1)(u-1),\\
d &= -\frac{2(u-v)}{(u-v+1)(u-v-1)}.
\end{aligned}$$

Hence, we obtained infinitely many quadruples which induces curves with torsion group $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/8\mathbb{Z}$.

It fact, it can be shown that every curve with torsion group $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$ can be obtained from a rational Diophantine quadruple.

For example, the quadruple

$$\left\{\frac{1804}{1197}, -\frac{226796}{539847}, \frac{303199}{239932}, -\frac{1197}{1804}\right\},$$

obtained for $(u, v) = (2, -25/19)$, gives the curve with torsion $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$ and rank 3 (equivalent to the curve found by Connell and D. in 2000, what is the largest known rank for curves with this torsion group.

Thank you very much
for your attention!