ON THE RANK OF ELLIPTIC CURVES COMING FROM RATIONAL DIOPHANTINE TRIPLES

JULIÁN AGUIRRE, ANDREJ DUJELLA, AND JUAN CARLOS PERAL

Abstract. We construct a family of Diophantine triples $\{c_1(t), c_2(t), c_3(t)\}$ such that the elliptic curve over $\mathbb{Q}(t)$ induced by this triple, i.e.:

$$y^2 = (c_1(t)\, x + 1)(c_2(t)\, x + 1)(c_3(t)\, x + 1)$$

has torsion group isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ and rank 5. This represents an improvement of the result of A. Dujella, who showed a family of this kind with rank 4. By specialization we obtain two examples of elliptic curves over $\mathbb{Q}$ with torsion group $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ and rank equal to 11. This is also an improvement over the known results relating this kind of curves.

1. Diophantine triples and elliptic curves

Definition. A set $\{c_1, c_2, \ldots, c_m\}$ of non-zero integers (rationals) is called a (rational) $D(n)$-m-tuple if $c_i \cdot c_j + n$ is a perfect square for all $1 \leq i < j \leq m$. A $D(1)$-m-tuple is also called a Diophantine m-tuple.

The first rational Diophantine quadruple, the set $\{1/16, 33/16, 17/4, 105/16\}$, was found by Diophantus of Alexandria (for the history of the problem see e.g. [Di]). It is well-known that there exist infinitely many rational Diophantine quadruples and quintuples (see e.g. [D2]) and several examples of rational Diophantine sextuples were found recently by Gibbs [G1] and Dujella [D7]. Euler proved that there exist infinitely many integer Diophantine quadruples (the first such set $\{1, 3, 8, 120\}$ was found by Fermat). A famous conjecture is that there does not exist an integer Diophantine quintuple (see e.g. [Gu]). Baker and Davenport [BD] proved that Fermat's quadruple cannot be extended to a Diophantine quintuple. It is known that there does not exist a Diophantine sextuple and there are only finitely many (at most 10^{276}) Diophantine quintuples [D5, F].

Let $\{c_1, c_2, c_3, c_4\}$ be a rational Diophantine quadruple. Consider a subtriple $\{c_1, c_2, c_3\}$ and define the elliptic curve by the equation

$$y^2 = (c_1\, x + 1)(c_2\, x + 1)(c_3\, x + 1). \tag{E}$$

We say that E is the elliptic curve induced by the Diophantine triple $\{c_1, c_2, c_3\}$. Let

$$c_i c_j + 1 = t_{i,j}^2, \quad 1 \leq i < j \leq 4.$$

Then the curve E has three rational points of order 2:

$$T_1 = [\,-1/c_1, 0\,], \qquad T_2 = [\,-1/c_2, 0\,], \qquad T_3 = [\,-1/c_3, 0\,],$$

The first author supported by grant IT-305-07 of the Basque Government. The second author supported by the Ministry of Science, Education and Sports, Republic of Croatia, grant 037-0372781-2821. The last author supported by grant UPV/EHU 07/09: Topics in number theory.

and at least three other rational points:

$$\tag{1} \begin{cases} P_1 = [\,0, 1\,], \\ P_2 = [\,c_4, t_{1,4}\, t_{2,4}\, t_{3,4}\,], \\ P_3 = \Big[\, \dfrac{t_{1,2}\, t_{1,3} + t_{1,2}\, t_{2,3} + t_{1,3}\, t_{2,3} + 1}{c_1 c_2 c_3}, \\ \qquad \dfrac{(t_{1,2} + t_{1,3})(t_{1,2} + t_{2,3})(t_{1,3} + t_{2,3})}{c_1 c_2 c_3} \,\Big]. \end{cases}$$

We will first prove that there exists a bi-parametric set of diophantine quadruples such that these three points are of infinite order and independent, so the elliptic curve induced by these triples has generic rank greater or equal to 3.

In section 3 we show that adequate choices of the parameters induce subfamilies of curves with rank 4 and rank 5.

In the last section we show particular examples of curves having rank 10 and 11. We present also the results of computation on a large set of curves.

Both the families of rank 5 over $\mathbb{Q}(t)$ and the particular examples of curves with rank 11 represent improvements over the known results of curves induced by Diophantine triples. Namely, in [D3] a family of rank 4 over $\mathbb{Q}(t)$ was constructed using the formulas for the extension of a rational Diophantine quadruple to a quintuple in [D2], while in [D6] an example with rank 9 was obtained in the family of curves induced by Diophantine triples of the form $\{t-1, t+1, 16\,t^3-4\,t\}$ (of generic rank 2).

2. Construction of a curve of rank 3 over $\mathbb{Q}(t)$

In [D1] several families of $D(n)$-quadruples are described. We will use for our construction the one given by

$$\{a, a(k+1)^2 - 2\,k, a(2\,k+1)^2 - 8\,k - 4, a\,k^2 - 2\,k - 2\}.$$

For each a and k this quadruple is a $D(2\,a(2\,k{+}1){+}1)$-quadruple. Now we specialize to the following value of k:

$$k = \frac{-1 - 2\,a + n^2}{4\,a}.$$

The resulting quadruple is a $D(n^2)$-quadruple and once divided by n we get the following rational $D(1)$-quadruple:

$$\tag{2} \begin{cases} c_1(a,n) = \dfrac{a}{n}, \\ c_2(a,n) = \dfrac{((n-3)(n-1) + 2\,a)((n+1)(n+3) + 2\,a)}{16\,a\,n}, \\ c_3(a,n) = \dfrac{(n-3)(n-1)(n+1)(n+3)}{4\,a\,n}, \\ c_4(a,n) = \dfrac{((n-3)(n-1) - 2\,a)((n+1)(n+3) - 2\,a)}{16\,a\,n}. \end{cases}$$

In the terminology of [G2], (2) is an irregular and twice semi-regular Diophantine quadruple. A Diophantine triple $\{a_1, a_2, a_3\}$ is regular if $(a_3 - a_2 - a_1)^2 = 4(a_1 a_2 + 1)$, while a Diophantine quadruple $\{a_1, a_2, a_3, a_4\}$ is regular if $(a_4 + a_3 - a_1 - a_2)^2 = 4(a_1 a_2 + 1)(a_3 a_4 + 1)$. It can be checked that (2) is irregular, but it contains two regular triples: $\{c_1, c_2, c_4\}$ and $\{c_2, c_3, c_4\}$.

Now we define the elliptic curve associated to the triple $\{c_1, c_2, c_3\}$ as explained above, i.e.:

$$y^2 = (c_1(a,n)x + 1)(c_2(a,n)x + 1)(c_3(a,n)x + 1).$$

Note that we choose an irregular triple which is a subtriple of an irregular quadruple. Otherwise, by [D4], the points P_1, P_2, P_3 would not be independent.

Besides the 2-torsion points, this curve has the points with x-coordinate given by

$$0, \quad c_4(a,n) \quad \text{and} \quad \frac{t_{1,2}\,t_{1,3}+t_{1,2}\,t_{2,3}+t_{1,3}\,t_{2,3}+1}{c_1(a,n)c_2(a,n)c_3(a,n)},$$

where as before $t_{i,j}=t_{i,j}(a,n)=\sqrt{c_i(a,n)c_j(a,n)+1}$, $1\le i<j\le 3$. In terms of a and n, the three rational points (1) are:

$$\begin{aligned}
P_1 &= [\,0,1\,],\\
P_2 &= \Big[\frac{(n^2+4\,n-2\,a+3)(n^2-4\,n-2\,a+3)}{16\,a\,n},\\
&\quad -\frac{(n^2-2\,a+3)(n^4-10\,n^2-4\,a^2+9)(n^4-2\,a\,n^2-10\,n^2-6\,a+9)}{512\,a^2\,n^3}\Big],\\
P_3 &= \Big[\frac{6\,n}{(n-3)(n+3)},\frac{(n^2+6\,a-9)(3\,n^2+2\,a-3)}{4\,a(n-3)(n+3)}\Big].
\end{aligned}$$

Theorem 1. *The curve $y^2=(c_1(a,n)x+1)(c_2(a,n)x+1)(c_3(a,n)x+1)$ has torsion group $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$ and rank 3 over $\mathbb{Q}(n,a)$. The points P_1, P_2 and P_3 are of infinite order and independent.*

Proof. Since the specialization map is always a homomorphism, see [Si], it is enough to prove that there exist values of a and n such that the specialized three points are $\mathbb{Q}$-independent. Consider for example $a=2$ and $n=5$. Then the specialized points are

$$Q_1=[0,1], \quad Q_2=[11/10,-1173/125], \quad Q_3=[15/8,133/8].$$

A calculation using J. Cremona's program `mwrank` [C] shows that the elliptic curve induced by the triple having these parameters has rank 3, and from obtained generators it is easy to check that the three points Q_1, Q_2 and Q_3 are independent. Thus, by the specialization theorem of Silverman, the proof is finished. □

The symbolic calculations in this and the next sections were carried out with *Mathematica*®[M].

3. Search for higher rank

3.1. **Change of variables.** Now we look for conditions on a and n such that there are new rational points on the curve. This task is made simpler by means of a change of variable. The coordinate transformation

$$x\mapsto c_1(a,n)c_2(a,n)c_3(a,n)\,x, \quad y\mapsto c_1(a,n)c_2(a,n)c_3(a,n)\,y$$

applied to the curve leads to

$$y^2=(x+c_1(a,n)c_2(a,n))(x+c_1(a,n)c_3(a,n))(x+c_2(a,n)c_3(a,n)).$$

Next, the change $x\mapsto x-c_1(a,n)c_2(a,n)$ transforms it into

$$\begin{aligned}
y^2 = x(x&+c_1(a,n)c_3(a,n)-c_1(a,n)c_2(a,n))\\
&\times(x+c_2(a,n)c_3(a,n)-c_1(a,n)c_2(a,n)).
\end{aligned}$$

From this point on, in order to avoid denominators, we will make, when necessary, the appropriate change of variables to write the curve as

$$y^2=x^3+A\,x^2+B\,x \tag{3}$$

where A and B are integers. This leads to the following values of the coefficients A and B:

$$\begin{aligned} A &= 81 + 108\,a + 108\,a^2 - 96\,a^3 - 32\,a^4 - 180\,n^2 - 84\,a\,n^2 - 120\,a^2\,n^2 \\ &\quad - 32\,a^3\,n^2 + 118\,n^4 - 28\,a\,n^4 + 12\,a^2\,n^4 - 20\,n^6 + 4\,a\,n^6 + n^8, \\ B &= 4\,a^2(9 + 2\,a - n^2)(3 + 2\,a - 4\,n + n^2)(3 + 2\,a + 4\,n + n^2) \\ &\quad \times (-3 + 2\,a + 3\,n^2)(-9 + 4\,a^2 + 10\,n^2 - n^4), \end{aligned}$$

and the corresponding value of the discriminant is

$$\begin{aligned} \Delta = 16(A^2 - 4\,B)B^2 &= 256(n-1)^2(n+3)^2(n-3)^2(n+1)^2a^4(6a - 9 + n^2)^2 \\ &\times (-2a - 1 + n^2)^2(-9 - 2a + n^2)^2(3 + 2a - 4n + n^2)^2 \\ &\times (3 + 2a + 4n + n^2)^2(-3 + 2a + 3n^2)^2(9 - 4a^2 - 10n^2 + n^4)^2. \end{aligned}$$

Finally, the x-coordinates of the three infinite order points are

$$\begin{aligned} x_1 &= 4\,a^2(3 + 2\,a - 4\,n + n^2)(3 + 2\,a + 4\,n + n^2), \\ x_2 &= \frac{(3 + 2\,a - 4\,n + n^2)(3 + 2\,a + 4\,n + n^2)(9 - 6\,a - 10\,n^2 - 2\,a\,n^2 + n^4)^2}{16\,n^2}, \\ x_3 &= 2\,a(3 + 2\,a - 4\,n + n^2)(3 + 2\,a + 4\,n + n^2)(-3 + 2\,a + 3\,n^2). \end{aligned}$$

Remark. Considering a as a variable, for fixed n, formula (3) defines a K3 surface $\mathcal{E}$. Hence its Picard number satisfies rank $NS(\mathcal{E}, \mathbb{C}) \le 20$. We can estimate $\mathrm{rank}_{\mathbb{C}(a)}\mathcal{E}$ using Shioda's formula [Sh, Corollary 5.3]:

$$\mathrm{rank}_{\mathbb{C}(a)}\mathcal{E} = \mathrm{rank}\ NS(\mathcal{E}, \mathbb{C}) - 2 - \sum_s (m_s - 1).$$

Here the sum ranges over all singular fibres, with m_s the number of irreducible components of the fibre. The numbers m_s can be easily determined from Kodaira types of singular fibres (see [Mi, Section 4]). In our case, we have eight fibres of type I_2 and two fibres of type I_4 (we can read this from the factorization of the discriminant Δ), which gives $\mathrm{rank}_{\mathbb{C}(a)}\mathcal{E} \le 4$. It can be shown that for $n = -7/3$, $\mathrm{rank}_{\mathbb{C}(a)}\mathcal{E} \le 4$ (since the point with x-coordinate $x_4 = \frac{4}{9}x_3$ is also rational and independent of the three others) and hence rank $NS(\mathcal{E}, \mathbb{C}) = 20$.

3.2. **Construction of a curve of rank 4 over $\mathbb{Q}(t)$.** Now we look for those polynomial factors of B that can be conditioned in a simple way to yield a new point in the curve. We find that the factor

$$B_1 = (3 + 2\,a - 4\,n + n^2)(-3 + 2\,a + 3\,n^2)(-9 + 4\,a^2 + 10\,n^2 - n^4)$$

satisfies the equation of the curve (i.e. $B_1 + A + B/B_1$ is a perfect square) if

$$2(9 + 6\,a + 8\,a^2 - 18\,n - 4\,a\,n + 8\,n^2 - 2\,a\,n^2 + 2\,n^3 - n^4)$$

is a square. A solution in terms of a is given by

$$a = \frac{18 - m^2 - 36n + 16n^2 + 4n^3 - 2n^4}{4(-3 + 2m + 2n + n^2)}. \tag{4}$$

It will be shown later that this value of a followed either by the substitution $m = 18 - n - n^2$ or by $n = -7/3$ leads in both cases to families of curves of rank 5.

For a given by (4), the values of A and B in (3) are polynomials in m and n of degree 16 and 29 respectively, whose explicit expressions are too long to include here. The x-coordinates of the preceding points jointly with the new one became

$$\begin{aligned}
X_1 &= m(-12+m+16\,n-4\,n^2)(-18+m^2+36\,n-16\,n^2-4\,n^3+2\,n^4)^2\\
&\quad\times(-12\,m+m^2+48\,n-16\,m\,n-32\,n^2-4\,m\,n^2-16\,n^3),\\
X_2 &= \frac{1}{16\,n^2}\,m(12-m-16\,n+4\,n^2)\\
&\quad\times(12\,m-m^2-48\,n+16\,m\,n+32\,n^2+4\,m\,n^2+16\,n^3)\\
&\quad\times(-108+36\,m+3\,m^2+144\,n+12\,n^2-40\,m\,n^2+m^2n^2\\
&\qquad-16\,n^3-36\,n^4+4\,mn^4+4\,n^6)^2,\\
X_3 &= m(-12+m+16\,n-4\,n^2)(-18+m^2+36\,n-16\,n^2-4\,n^3+2\,n^4)\\
&\quad\times(-36+12\,m+m^2+48\,n+8\,n^2-12\,m\,n^2-16\,n^3-4\,n^4)\\
&\quad\times(-12\,m+m^2+48\,n-16\,m\,n-32\,n^2-4\,m\,n^2-16\,n^3),\\
X_4 &= -m(12-m-16\,n+4\,n^2)\\
&\quad\times(36-12\,m-m^2-48\,n-8\,n^2+12\,m\,n^2+16\,n^3+4\,n^4)\\
&\quad\times(-432\,m+180\,m^2-m^4+864\,n+288\,m\,n-72\,m^2n-2304\,n^2\\
&\qquad+624\,m\,n^2-128\,m^2n^2+1632\,n^3-320\,m\,n^3+8\,m^2n^3+256\,n^4\\
&\qquad-208\,m\,n^4+12\,m^2n^4-480\,n^5+32\,m\,n^5+16\,m\,n^6+32\,n^7).
\end{aligned}$$

It can be proved, by specialization that this is a family of rank ≥ 4 over $\mathbb{Q}(m,n)$.

3.3. **Construction of curves of rank 5 over $\mathbb{Q}(t)$.** As was mentioned before, the substitution $m = 18-n-2\,n^2$ gives an additional point on the cubic and a subfamily of rank 5. We also have observed experimentally that in the subfamily obtained by letting $n=-7/3$ there were many curves of high rank. In fact this choice for n gives a new point on the cubic and a family of rank 5 with smaller coefficients. We provide here a unified derivation of these two rank 5 families.

We impose on m and n the condition that

$$\begin{aligned}
&(-12\,m+m^2+48\,n-16\,m\,n-32\,n^2-4\,m\,n^2-16\,n^3)\\
&\quad\times(-36+12\,m+m^2+48\,n+8\,n^2-12\,m\,n^2-16\,n^3-4\,n^4)\\
&\quad\times(432\,m-180\,m^2+m^4-864\,n-288\,m\,n+72\,m^2n+2304\,n^2\\
&\qquad-624\,m\,n^2+128\,m^2n^2-1632\,n^3+320\,m\,n^3-8\,m^2n^3-256\,n^4\\
&\qquad+208\,m\,n^4-12\,m^2n^4+480\,n^5-32\,m\,n^5-16\,m\,n^6-32\,n^7)
\end{aligned}$$

becomes the x-coordinate of a new point in the cubic. This is equivalent to forcing

$$\begin{aligned}
H &= 324-108m+45m^2-6m^3+m^4-864n-432mn+216m^2n-4m^3n\\
&\quad+1584n^2+84mn^2+22m^2n^2+2m^3n^2-1632n^3+480mn^3-24m^2n^3\\
&\quad+216n^4+28mn^4-3m^2n^4+480n^5-48mn^5-80n^6-4mn^6-32n^7+4n^8
\end{aligned}$$

to be a perfect square. Now from the identity

$$\begin{aligned}
(5)\quad H-(m^2+(-3-2\,n+n^2)m+(-2(-9-51\,n-6n^2+5\,n^3+n^4)))^2&\\
=-12n(n-3)(1+n)^2(7+3\,n)(-18+m+n+2\,n^2)&,
\end{aligned}$$

we see that in order for H to be a perfect square, it is enough that the right hand side of (5) vanishes. For $n=3$, $n=0$ and $n=-1$ we get singular curves, but the other two solutions, $n=-7/3$ and $m=18-n-2n^2$ give families of rank 5.

If we take $n = -7/3$, then A and B are

$$\begin{aligned} A = -2(&167772160000000 + 1323093196800000\,m - 32195543040000\,m^2 \\ &- 14929920000000\,m^3 - 1863701913600\,m^4 + 285400350720\,m^5 \\ &+ 5952139200\,m^6 - 2908045152\,m^7 + 43046721\,m^8), \\ B = 81\,&m(-640 + 9\,m)(-160 + 9\,m)(-80 + 9\,m)^2(32 + 9\,m) \\ &\times (80 + 9\,m)^2(-2240 + 96\,m + 27\,m^2)(3200 + 240\,m + 27\,m^2) \\ &\times (-1600 - 4320\,m + 81\,m^2)(4480 - 720\,m + 81\,m^2). \end{aligned}$$

Note that for $n = -7/3$ the coefficient B has 10 irreducible factors, compared with 7 factors for general n and m.

The quadruple is now

$$\left\{ \begin{aligned} q_1 &= \frac{(-80 + 9\,m)(80 + 9\,m)}{168(-10 + 9\,m)}, \\ q_2 &= \frac{9\,m(-640 + 9\,m)(-2240 + 96\,m + 27\,m^2)}{224(-80 + 9\,m)(-10 + 9\,m)(80 + 9\,m)}, \\ q_3 &= -\frac{2560(-10 + 9\,m)}{21(-80 + 9\,m)(80 + 9\,m)}, \\ q_4 &= \frac{(-6080 - 288\,m + 81\,m^2)(-12800 + 5760\,m + 81\,m^2)}{(672(-80 + 9\,m)(-10 + 9\,m)(80 + 9\,m)}. \end{aligned} \right. \tag{6}$$

The four old points of infinite order and the new fifth independent point, have the following x-coordinate:

$$\left\{ \begin{aligned} X_1 &= 27m(-640 + 9\,m)(-80 + 9\,m)^2(80 + 9\,m)^2(-2240 + 96m + 27\,m^2), \\ X_2 &= \frac{3}{49}\,m(-640 + 9\,m)(-2240 + 96\,m + 27\,m^2) \\ &\quad \times (-108800 - 11520\,m + 1539\,m^2)^2, \\ X_3 &= 27\,m(-640 + 9\,m)(-80 + 9\,m)(80 + 9\,m)(-2240 + 96\,m + 27\,m^2) \\ &\quad \times (-1600 - 4320\,m + 81\,m^2), \\ X_4 &= 27\,m(-640 + 9\,m)(3200 + 240\,m + 27\,m^2)(-1600 - 4320\,m + 81\,m^2) \\ &\quad \times (4480 - 720\,m + 81\,m^2), \\ X_5 &= 9(-2240 + 96\,m + 27\,m^2)(3200 + 240\,m + 27\,m^2) \\ &\quad \times (4480 - 720m + 81m^2)(-1600 - 4320\,m + 81\,m^2). \end{aligned} \right. \tag{7}$$

Theorem 2. *The elliptic curve induced by the first three components of the Diophantine quadruple* (6) *has torsion* $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$ *and rank* 5 *over* $\mathbb{Q}(m)$*. The points with* x*-coordinate given in* (7) *are of infinite order and independent.*

Proof. As before, we use that the specialization map is a homomorphism, so that it is enough to prove that there exist a rational value such that the specialized five points are $\mathbb{Q}$-independent. For $m = 16$ we get the curve given by

$$y^2 = x^3 + 733622402025521152\,x^2 - 2205912309511248243290996656308224\,x$$

whose rank calculated with `mwrank` is exactly 5. So it is enough to show that the corresponding points are $\mathbb{Q}$-independent. The points are:

$$\begin{aligned}
Q_1 &= [-273384014239236096, -2010678624124814679972249600],\\
Q_2 &= [-15036508232157757744/49, -125505240370913008443142963 20/343],\\
Q_3 &= [953182656789479424, 1229443967479836961249689600],\\
Q_4 &= [2046570199951343616, 3405811357277517803755143168],\\
Q_5 &= [-533648681170108416, -2621459920188665951472844 80].
\end{aligned}$$

These five points are of infinite order and independent over $\mathbb{Q}$, since the determinant of their height matrix is $\approx 4075.770347 \neq 0$ (calculated in `PARI/GP` [P]), so the curve has rank at least 5 over $\mathbb{Q}(m)$. $\square$

Remark. A similar argument yields other pairs of substitutions, like $n = 9/7$, $m = (15 - 16\,n + 3\,n^2)/2$ and $n = -9/7$, $m = (15 - 2\,n + 3\,n^2)/2$, that produce families of rank ≥ 5.

3.4. **Families of rank 6.** The condition for the divisor of B given by:

$$27(80+9m)(-80+9m)^2(-160+9m)(-2240+96m+27m^2)(3200+240m+27m^2)$$

to be the x-coordinate of a new point on the curve gives the quartic equation

$$y^2 = (81m^2 + 1728m + 11840)(27m^2 - 480m + 5120)$$

which is birationally equivalent to an elliptic curve of rank 3. So the points on this elliptic curve give a parametrization for an infinite family of curves with rank 6.

There are other divisors of B with the similar property. For example, the five divisors:

$$\begin{aligned}
&9m(-640+9m)(-160+9m)(-80+9m)(-1600-4320m+81m^2)\\
&\qquad \times (4480-720m+81m^2),\\
&3(-80+9m)^2(80+9m)^2(3200+240m+27m^2)(4480-720m+81m^2),\\
&3(-160+9m)(-80+9m)^2(80+9m)(-2240+96m+27m^2)\\
&\qquad \times (4480-720m+81m^2),\\
&3(-640+9m)(-80+9m)^2(32+9m)(80+9m)^2(-2240+96m+27m^2),\\
&3(-640+9m)(-160+9m)(32+9m)(80+9m)(-2240+96m+27m^2)\\
&\qquad \times (-1600-4320m+81m^2)
\end{aligned}$$

are the x-coordinate of a new point on the cubic provided that the corresponding values of m satisfy a quartic equation equivalent in all five cases to an elliptic curve of rank 2.

4. The case $n = -7/3$

4.1. **Search results.** We have run a search for elliptic curves of high rank corresponding to $n = -7/3$. We write $m = r/s$. Hence, we are considering the family of elliptic curves (3) where the coefficients A and B are integers verifying:

(1) $A > 0$;
(2) If $d \in \mathbb{Z}$ is such that $d^2 \mid A$ and $d^4 \mid B$, then $d = \pm 1$.

They depend on two parameters $r, s \in \mathbb{Z}$ and are computed by the following algorithm:

(1) Compute

$$\begin{aligned} a_1 &= -2(43046721\, r^8 - 2908045152\, r^7 s + 5952139200\, r^6 s^2 + 285400350720\, r^5 s^3 \\ &\quad - 1863701913600\, r^4 s^4 - 14929920000000\, r^3 s^5 - 32195543040000\, r^2 s^6 \\ &\quad + 1323093196800000\, r\, s^7 + 167772160000000\, s^8), \\ b_1 &= 81\, r(9\, r - 640\, s)(9\, r - 160\, s)(9\, r - 80\, s)^2(9\, r + 32\, s)(9\, r + 80\, s)^2 \\ &\quad \times (27\, r^2 + 96\, r\, s - 2240\, s^2)(81\, r^2 - 4320\, r\, s - 1600\, s^2) \\ &\quad \times (27\, r^2 + 240\, r\, s + 3200\, s^2)(81\, r^2 - 720\, r\, s + 4480\, s^2). \end{aligned}$$

(2) If $a_1 < 0$, let $a_2 = -2\, a_1$ and $b_2 = a_1^2 - 4\, b_1$; otherwise $a_2 = a_1$ and $b_2 = b_1$.
(3) Compute $D = \max\{\, d \in \mathbb{Z} : d^2 \mid a_2,\ d^4 \mid b_2 \,\}$.
(4) Let $A = a_2/D$, $B = b_2/D$.

The unrestricted family. We have computed all such curves for $-1\,000 \le r \le -1$ and $1 \le s \le 1\,000$, obtaining a total of 608 381 different curves. We have found that:

- 93.60% of the values of A are square-free;
- 10.97% of the values of B are perfect squares (they correspond to the case $a_1 < 0$, since $a_1^2 - 4b_1$ is always a perfect square);
- the possible values of $\gcd(A, B)$ are $\{\, 1, 5, 7, 25, 35, 175 \,\}$.

We were running `mwrank` (with the default options, except the precision) on the 23 154 curves among them with $10^{15} \le A < 10^{22}$. We have refined the obtained results by using `mwrank` with increased height bound for quartic point search. Also, we have used the data which conditionally give information of the rank (like root-number which conjecturally determines the parity of the rank, and Mestre's formulas [M2] which give upper bounds for the rank assuming the Birch and Swinnerton-Dyer conjecture and GRH). The refined results on rank distribution are given in Table 1. The results in the first column are unconditional, while the results in the last three columns are conditional and depend on the above mentioned conjectures.

Table 1. Number of curves with rank R.

$R = 5$	4877	$R = 5^*$	15	$R = 5$ or 7	2404	$R = 5$ or 7 or 9	27
$R = 6$	6153	$R = 6^*$	3758	$R = 6$ or 8	967		
$R = 7$	3342	$R = 7^*$	616	$R = 7$ or 9	131		
$R = 8$	762	$R = 8^*$	16	$R = 8$ or 10	1		
$R = 9$	76						
$R = 10$	9						

A restricted family. A detailed analysis of the results suggests that curves of high rank can be found for pairs (r, s) satisfying some divisibility properties, in particular, the most of high rank curves satisfy $9 \mid s$.

Here we report results on the search on pairs (r, s) such that $r\,s < 0$, $10 \mid r$, $9 \mid s$ and $\gcd(r, s) = 1$. We have computed all such pairs with $-20\,000 \leq r \leq -10$ and $9 \leq s \leq 18\,000$, for a total of 1 013 908 different curves. Running `mwrank` on the 58 260 curves in this restricted family with $10^{10} < A \leq 10^{21}$, after above mentioned refinements, gives the results which are presented in Table 2.

Table 2. Number of curves with rank R in the restricted family.

$R = 5$	12733	$R = 5^*$	94	$R = 5$ or 7	5975	$R = 5$ or 7 or 9	20
$R = 6$	15889	$R = 6^*$	9052	$R = 6$ or 8	2310		
$R = 7$	8544	$R = 7^*$	1392	$R = 7$ or 9	212		
$R = 8$	1794	$R = 8^*$	37				
$R = 9$	202						
$R = 10$	6						

Results. Apart from the two described systematic searches, we performed several similar searches for r and s satisfying some congruence properties and sieving for curves with large Selmer rank. All searches combined produced

- over 450 curves of rank 9;
- 49 curves of rank 10, given in table 3;
- 2 curves of rank 11 (see Subsection 4.2).

Among the curves of rank at least 9 we find that:

- 92.1% of the values of A are square-free;
- The values of A have few divisors; 89.1% of them have less than 32 divisors; in particular, $(r, s) = (-97, 5)$, $(-406, 9)$, $(-3530, 9)$, and $(-7088, 6057)$ yield curves with rank 10 and prime A;
- 26.7% of the values of B are perfect squares.

Table 3. Curves with rank 10.

A	B	r	s
747855613433348693	37971496662597382325245674854656	-11860	477
2748683743713727033	912317634326203873339784207988335616	-48	25
3351364638294432929	-8790232486857655134490909037324384000	-560	2547
4552418484376711606	2855015032276620553646153783733528409	-412	261
5631826628732300518	4046067214731363356410390215076327081	-152	243
7164838580600101729	18012992210099780625832439971840000	-406	9
9698787151884024353	93218017572430494149711412330496	-3530	9
28429980819035946214	8354606335610095567648865047883891625	-120	319
48386624390778183446	340722320204726405618912807689617461625	-1880	2331
63788123186512356001	11053177808588079790897996852248576000000	-11	135
158812592576004664822	-44603493302827981235081787433061762927079	-6740	639
491529834940711863545	-7676647487828248273287320373006800460800	-25840	2691
778121977076533994270	83655062993263641543386221902648520158625	-3560	5031
1056137838517295947582	34512967148351962338870714425590255551681	-70	177
1091379930771597822721	-99230443006894220402738531558010722304000	38960	3393
1202915055786699743638	535384460107862619444176358949623452025	7840	2511
2345704511683192121806	-9021007624126018079268837610331566365759375	-14860	2421
3096864334610439252022	-858506739076820940781279898390463769667879	-5	26
3680846006105025380243	3823549253805545206347080657925803772900	10328	2907
4885687808873671787369	3118755512745506309643405416789786786304000	-8720	13509
5023109290447026238846	1723070287154900074835283434344651911846529	-655	243
7047313964717027055110	6084830913523359929845160579967868674940425	-2780	4653
15589866837195270063049	-14808693577819579795869536699563843431366656	-19120	2727
22139410900834785059195	67333232930079070871634265475186452636354200	-12160	7659
23181931498764073443710	-12967800283686080932588185743965480741998975	-15830	2007
23257211533069660662025	-27132066881171717478483233427423298974489600	-6736	927
40885960071623533402094	-220893566183419511743172152334517081828022191	9598	171
80771928519688044328345	77324613543240798903960113376871736934400	-4010	339
96614818471635996006845	169674207344719455092048156293205053190400	1528	1899
162148129016051669054785	-700643054670341159978745564045962362178355200	-18800	2403
251653795575144603139313	9500504302425532445298117719109224213222670336	-7088	6057
303232848545484408282614	-5137680136645293513114838905990362310215334375	10060	2313
792730824646378117452517	107891184684808592438523258292998789909817600	2372	1089
845779368201476985117505	13952080245255725782550668020845259700382736400	-3400	299
988206562952637534705025	40364086610566126633826529224573064425216409600	-10640	3501
1204984595901565426253893	420361950788928178283791597629917345020422400	4780	1887
1254563782532106917825761	326334421011475076633583096252694675456000000	-97	5
2030352548876158303263854	527855941658733788306437169014252525293116542929	-181	288
2808247758775739846532046	-1945389600097873918362570245190829347577215375	-590	67
16730231396187018599477614	27509641048934349748161545663922629551913847804625	-4495	1971
92396300635364317824884062	517416068178189153899285426436670772369894021025	8656	4779
241356562285348827406451894	239196310124712567231437666988573024891642683265625	-44512	3285
475668889686708922071772558	237299543025483671693929700036501768931787510065841	-6480	379
1065106187134410385004630206	165031175519231666816637006489377599410518421854950209	6379	153
1295550337351599466735479278	-1191028993105954789455460301623377887327310454446389679	-5251	504
15261589260842425625239688446	30762348642821753093008971647383863114675558937411267329	-5690	3339
74973225218344110887745123037	102057068281404548823715018616769051480908329932871936	9380	5949
145180882575715752344574776750	72045133957864532082055079217635254812796237330979963025	-8503	2421
644532051041139515872833852058	1274887683275001565151201365742517281374998797744323464841	10880	30411

4.2. **Examples of curves of rank** 11**.** Here we give some details on two curves with rank equal to 11. It can be mentioned that at present there are only few curves known with torsion group $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ and rank ≥ 11 (due to Elkies, Eroshkin, Dujella and Kulesz; the record is a curve with rank 15 found by Elkies in 2009; see [D8] for details).

The first example with rank equal to 11 is found in the above described restricted family satisfying $10 \mid r$, $9 \mid s$. We have considered 27599 curves with $10^{21} < A <$

10^{22} in this family and searched for those with Selmer rank 11. We have found two such curves, and found by `mwrank` that one of them has rank equal to 11. The details are given in the next theorem.

Theorem 3. *The curve*

$$\begin{aligned} y^2 = x^3 &+ 178787005706216556339 8\,x^2 \\ &- 3010692612259710272238718021451023106733 99\,x, \end{aligned}$$

corresponding to the values of the parameters $r = -15580$ *and* $s = 2853$, *has rank* 11. *The curve is induced by the rational Diophantine triple*

$$\Big\{ \frac{333661}{832125}, -\frac{1395935438579}{1110590638500}, -\frac{12680000}{7006881} \Big\}.$$

Proof. The minimal Weierstrass equation for this curve is

$$\begin{aligned} y^2 + xy = x^3 + x^2 &- 854101484295288381130649731474978685276 37\,x \\ &+ 941795940891009199205661922839723393804231554271643982191362 9 \end{aligned}$$

Torsion points are $\mathcal{O}$ and:

$$\begin{gathered} [\,187730162413280809858, -93865081206640404929\,], \\ \Big[\,\frac{595956685687388521131}{4}, -\frac{595956685687388521131}{8}\,\Big], \\ [-336719333835127940142, 168359666917563970071\,]. \end{gathered}$$

Independent points of infinite order are:

$$\begin{aligned}
Q_1 &= [-882915776561947416 42, -40336940587656217288662615799 29], \\
Q_2 &= [132528792265728660983, 65297434667548817582215882007 1], \\
Q_3 &= [189017660415735476733, 16460466866858348524733070444 6], \\
Q_4 &= [231479176857636247358, 14319730632233113024103254075 71], \\
Q_5 &= [-180297353866722177267, -43538755832892140264585852115 54], \\
Q_6 &= [909604797725054454039, 26159474457841141855998719225 058], \\
Q_7 &= \Big[\frac{7560473504917895649 87}{4}, \frac{13137533944056463024371529953 93}{8}\Big], \\
Q_8 &= [556305932619791723 58, 21997058161406709692960271700 71], \\
Q_9 &= \Big[-\frac{12732086826508795886 93}{4}, -\frac{16694920515417325034029558911 307}{8}\Big], \\
Q_{10} &= [108052480827435686191 3, 34331901735067855866097775725 846], \\
Q_{11} &= \Big[\frac{204885642862796148902747}{2209}, \frac{157250952026186871978974423595399558}{103823}\Big],
\end{aligned}$$

so that its rank is at least 11. `mwrank` (which uses 2-descent, via 2-isogeny if possible, to unconditionally determine the rank) establishes that in fact it is exactly 11. ☐

The second example with rank 11 is found in the family satisfying similar congruence conditions: $16 \mid r$, $9 \mid s$ and $\gcd(2\,r, 3\,s) = 1$. Within this family, we have searched for curves with

(1) relatively large Mestre-Nagao sums $S(N,E) = \sum_{p=2}^{N} \dfrac{-a_p + 2}{p + 1 - a_p} \log p$, where $a_p = a_p(E) = p + 1 - \#E(\mathbb{F}_p)$, since it is experimentally known [M1, N] that we may expect that high rank curves have large $S(N,E)$ (we take e.g. $S(523,E) > 23$ and $S(1979,E) > 38$);
(2) root-number of E equal to -1 (conjecturally this implies that rank is odd);
(3) Selmer rank ≥ 11 (as implemented in `mwrank` with option `-s`).

We perform the search in various ranges of parameters r and s. Only few curves pass all the tests, and for them we try to compute the exact value of the rank using `mwrank`. In that way, we find the curve

$$\begin{aligned} y^2 = x^3 &+ 18824274115940616297295911113\,x^2 \\ &+ 3985360872467971058284926976004481058021394284609536\,x, \end{aligned}$$

which has rank 11. It corresponds to the values of the parameters $r = -10768$ and $s = 29205$, and is induced by the rational Diophantine triple

$$\left\{ \frac{795025}{3128544}, -\frac{22247424}{7791245}, \frac{24807390285149}{97501011189120} \right\}.$$

Finally, let us mention that we also found two curves for which `mwrank` gives $9 \le \mathrm{rank} \le 11$ (corresponding to the parameters $(r, s) = (14920, 128853), (-25936, 14319)$).

Acknowledgement: The authors would like to thank the referee for useful comments on the first version of the manuscript.

References

[BD] A. Baker and H. Davenport, *The equations* $3x^2 - 2 = y^2$ *and* $8x^2 - 7 = z^2$, Quart. J. Math. Oxford Ser. (2) **20** (1969), 129–137.

[C] J. Cremona, Algorithms for Modular Elliptic Curves. Cambridge University Press, Cambridge, 1997.

[Di] L. E. Dickson, History of the Theory of Numbers, Vol. 2, Chelsea, New York, 1966, pp. 513–520.

[D1] A. Dujella, *Some polynomial formulas for Diophantine quadruples*, Grazer Math. Ber. **328** (1996), 25–30.

[D2] A. Dujella, *On Diophantine quintuples*, Acta Arith. **81** (1997), 69–79.

[D3] A. Dujella, *Diophantine triples and construction of high-rank elliptic curves over* $\mathbb{Q}$ *with three non-trivial* 2*-torsion points*, Rocky Mountain J. Math. **30** (2000), 157–164.

[D4] A. Dujella, *Diophantine* m*-tuples and elliptic curves*, J.Theor. Nombres Bordeaux **13** (2001), 111–124.

[D5] A. Dujella, *There are only finitely many Diophantine quintuples*, J. Reine Angew. Math. **566** (2004), 183–214.

[D6] A. Dujella, *On Mordell-Weil groups of elliptic curves induced by Diophantine triples*, Glas. Mat. Ser. III **42** (2007), 3–18.

[D7] A. Dujella, *Rational Diophantine sextuples with mixed signs*, Proc. Japan Acad. Ser. A Math. Sci. **85** (2009), 27–30.

[D8] A. Dujella, *High rank elliptic curves with prescribed torsion*, `http://web.math.hr/~duje/tors/tors.html`

[F] Y. Fujita, *The number of Diophantine quintuples*, Glas. Mat. Ser. III **45** (2010), to appear.

[G1] P. Gibbs, *Some rational Diophantine sextuples*, Glas. Mat. Ser. III **41** (2006), 195–203.

[G2] P. Gibbs, *Adjugates of Diophantine quadruples*, Integers, to appear.

[Gu] R. K.Guy, Unsolved Problems in Number Theory, 3rd edition, Springer-Verlag, New York, 2004, Section D29, p. 310.

[M] Wolfram Research, Inc., Mathematica, Version 7.0, Champaign, IL (2008).

[M1] J.-F. Mestre, *Construction de courbes elliptiques sur* $\mathbb{Q}$ *de rank* ≥ 12, C. R. Acad. Sci. Paris Ser. I **295** (1982) 643–644.

[M2] J.-F. Mestre, *Formules explicites et minorations de conducteurs de variétés algébriques*, Compositio Math. **58** (1986), 209–232.

[Mi] R. Miranda, An overview of algebraic surfaces, in Algebraic Geometry (Ankara, 1995), Lecture Notes in Pure and Appl. Math. **193**, Dekker, New York, 1997, pp. 157–217.

[N] K. Nagao, *An example of elliptic curve over* $\mathbb{Q}$ *with rank* ≥ 20, Proc. Japan Acad. Ser. A Math. Sci. **69** (1993) 291–293.

[P] PARI/GP, version 2.4.0, Bordeaux, 2008, `http://pari.math.u-bordeaux.fr`.

[Sh] T. Shioda, *On the Mordell - Weil lattices*, Comment. Math. Univ. St. Pauli **39** (1990), 211–240.

[Si] J. H. Silverman, Advanced Topics in the Arithmetic of Elliptic Curves, Springer-Verlag, New York, 1994.

Departamento de Matemáticas, Universidad del País Vasco, Aptdo. 644, 48080 Bilbao, Spain

E-mail address, J. Aguirre: julian.aguirre@ehu.es

Department of Mathematics, University of Zagreb, Bijenička cesta 30, 10000 Zagreb, Croatia

E-mail address, A. Dujella: duje@math.hr

Departamento de Matemáticas, Universidad del País Vasco, Aptdo. 644, 48080 Bilbao, Spain

E-mail address, J. C. Peral: juancarlos.peral@ehu.es