ROCKY MOUNTAIN
JOURNAL OF MATHEMATICS
Volume 42, Number 6, 2012

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

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., [**3**]). It is well known that there exist infinitely many rational Diophantine quadruples and quintuples (see, e.g., [**5**]) and several examples of rational Diophantine sextuples were found recently by Gibbs [**13**] and Dujella [**10**]. 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., [**15**]).

The first author was supported by grant IT-305-07 of the Basque Government. The second author was supported by the Ministry of Science, Education and Sports, Republic of Croatia, grant # 037-0372781-2821. The third author was supported by grant # UPV/EHU 07/09: Topics in number theory.
Received by the editors on February 22, 2010, and in revised form on March 31, 2010.

DOI:10.1216/RMJ-2012-42-6-1759

Baker and Davenport [**1**] 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 [**8, 12**].

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

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

Then curve (E) has three rational points of order 2:

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

and at least three other rational points:

$$\begin{cases} P_1 = [0, 1], \\ P_2 = [c_4, t_{1,4}\,t_{2,4}\,t_{3,4}], \\ P_3 = [(t_{1,2}\,t_{1,3} + t_{1,2}\,t_{2,3} + t_{1,3}\,t_{2,3} + 1)/c_1c_2c_3, \\ \qquad ((t_{1,2} + t_{1,3})(t_{1,2} + t_{2,3})(t_{1,3} + t_{2,3}))/c_1c_2c_3]. \end{cases} \tag{1}$$

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 ranks 10 and 11. We also present the results of computation on a large set of curves.

Both the families of rank 5 over $\mathbf{Q}(t)$ and the particular examples of curves with rank 11 represent improvements over the known results of curves induced by Diophantine triples. Namely, in [**6**] a family of rank ≥ 4 over $\mathbf{Q}(t)$ was constructed using the formulas for the extension

of a rational Diophantine quadruple to a quintuple in [**5**], while in [**9**] 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 at least 3 over $\mathbf{Q}(t)$. In [**4**] 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:

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

In the terminology of [**14**], (2) is an irregular and twice semi-regular Diophantine quadruple. A Diophantine triple $\{a_1,a_2,a_3\}$ is regular if $(a_3-a_2-a_1)^2=4(a_1a_2+1)$, while a Diophantine quadruple $\{a_1,a_2,a_3,a_4\}$ is regular if $(a_4+a_3-a_1-a_2)^2=4(a_1a_2+1)(a_3a_4+1)$. It may 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 [**7**], 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

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

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:

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

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* $\mathbf{Z}/2\mathbf{Z}\times\mathbf{Z}/2\mathbf{Z}$ *and rank* ≥ 3 *over* $\mathbf{Q}(n,a)$. *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 [**22**, Section III.11], it is enough to prove that there exist values of a and n such that the specialized three points are $\mathbf{Q}$-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 Cremona's program `mwrank` [**2**] 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. □

The symbolic calculations in this and the next sections were carried out with *Mathematica*® [**23**].

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

$$x\longmapsto c_1(a,n)c_2(a,n)c_3(a,n)\,x,\qquad y\longmapsto c_1(a,n)c_2(a,n)c_3(a,n)\,y$$

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

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

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

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

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

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

Remark. Considering a as a variable, for fixed n, formula (3) defines a K3 surface $\mathcal{E}$. Hence, its Picard number satisfies $\operatorname{rank} NS(\mathcal{E}, \mathbf{C}) \leq 20$. We can estimate $\operatorname{rank}_{\mathbf{C}(a)}\mathcal{E}$ using Shioda's formula [**21**, Corollary 5.3]:

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

Here the sum ranges over all singular fibers, with m_s the number of irreducible components of the fiber. The numbers m_s can easily be determined from Kodaira types of singular fibers (see [**18**, Section 4]). In our case, we have eight fibers of type I_2 and two fibers of type I_4 (we can read this from the factorization of the discriminant Δ), which gives $\operatorname{rank}_{\mathbf{C}(a)}\mathcal{E} \leq 4$. It can be shown that, for $n = -7/3$, $\operatorname{rank}_{\mathbf{C}(a)}\mathcal{E} \geq 4$ (since the point with x-coordinate $x_4 = (4/9)x_3$ is also rational and independent of the three others), and hence, $\operatorname{rank} NS(\mathcal{E}, \mathbf{C}) = 20$.

3.2. Construction of a curve of rank at least 4 over $\mathbf{Q}(t)$. 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 degrees 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 become

$$\begin{aligned} X_1 &= m(-12 + m + 16\,n - 4\,n^2) \\ &\quad \times (-18 + m^2 + 36\,n - 16\,n^2 - 4\,n^3 + 2\,n^4)^2 \\ &\quad \times (-12\,m + m^2 + 48\,n - 16\,m\,n - 32\,n^2 - 4\,m\,n^2 - 16\,n^3), \\ X_2 &= \frac{1}{16\,n^2}\,m(12 - m - 16\,n + 4\,n^2) \end{aligned}$$

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

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

3.3. Construction of curves of rank 5 over $\mathbf{Q}(t)$. 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

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

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

to forcing

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

to be a perfect square. Now, from the identity

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

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

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

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

$$
(6)\quad \begin{cases} q_1 = [(-80+9\,m)(80+9\,m)]/168(-10+9\,m), \\ q_2 = [9\,m(-640+9\,m)(-2240+96\,m+27\,m^2)]/ \\ \qquad\qquad [224(-80+9\,m)(-10+9\,m)(80+9\,m)], \\ q_3 = -[2560(-10+9\,m)]/[21(-80+9\,m)(80+9\,m)], \\ q_4 = [(-6080-288\,m+81\,m^2)(-12800+5760\,m+81\,m^2)]/ \\ \qquad\qquad [(672(-80+9\,m)(-10+9\,m)(80+9\,m)]. \end{cases}
$$

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

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

Theorem 2. *The elliptic curve induced by the first three components of the Diophantine quadruple* (6) *has torsion* $\mathbf{Z}/2\mathbf{Z}\times\mathbf{Z}/2\mathbf{Z}$ *and rank* ≥ 5 *over* $\mathbf{Q}(m)$. *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 exists a rational value such that the specialized five points are $\mathbf{Q}$-independent. For $m=16$, we get the curve given by

$$
\begin{aligned} y^2 = x^3 &+ 733622402025521152\,x^2 \\ &- 22059123095111248243290996656308224\,x \end{aligned}
$$

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

$$\begin{aligned}
Q_1 &= [-273384014239236096, -2010678624124814679972249 60\,], \\
Q_2 &= [-1503650823215775744/49, \\
&\qquad -125505240370913008443142963 20/343], \\
Q_3 &= [953182656789479424, 122944396747983696124968 9600], \\
Q_4 &= [2046570199951343616, 340581135727751780375514 3168], \\
Q_5 &= [-533648681170108416, -262145992018866595147284480].
\end{aligned}$$

These five points are of infinite order and independent over **Q**, since the determinant of their height matrix is $\approx 4075.770347 \neq 0$ (calculated in `PARI/GP` [**20**]), so the curve has rank at least 5 over $\mathbf{Q}(m)$. □

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 at least 6. The condition for the divisor of B given by:

$$\begin{aligned}
27(80+9m)(-80+9m)^2(-160+9m)(-2240+96m+27m^2) \\
\times (3200+240m+27m^2)
\end{aligned}$$

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 a similar property. For example, the five divisors:

$$\begin{aligned}
&9m(-640+9m)(-160+9m)(-80+9m) \\
&\quad \times (-1600-4320m+81m^2)(4480-720m+81m^2),
\end{aligned}$$

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

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 $d \in \mathbf{Z}$ is such that $d^2 \mid A$ and $d^4 \mid B$, then $d = \pm 1$.

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

(1) Compute

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

(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 $D = \max\{d \in \mathbf{Z} : d^2 \mid a_2,\ d^4 \mid b_2\}$.

(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 formulae [**17**], 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 upon the above-mentioned conjectures.

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 high rank curves satisfy $9 \mid s$.

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						

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						

Here we report results on the search of 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 $-20\,000 \le r \le -10$ and $9 \le s \le 18\,000$, for a total of 1 013 908 different curves. Running *mwrank* on the 58 260 curves in this restricted family with $10^{10} < A \le 10^{21}$, after the above-mentioned refinements, gives the results which are presented in Table 2.

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.

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

TABLE 3. Curves with rank 10.

A	B	r	s
747855613433348693	37971496662597382325245674854656	-11860	477
2748683743713727033	91231763432620387333978420798833 5616	-48	25
3351364638294432929	-879023248685765513449090903732438 4000	-560	2547
4552418484376711606	285501503227662055364615378373352 8409	-412	261
5631826628732300518	404606721473136335641039021507632 7081	-152	243
7164838580600101729	180129922100997806258324399718400 00	-406	9
9698787151884024353	932180175724304941497114123304 96	-3530	9
28429980819035946214	835460633561009556764886504788 3891625	-120	319
48386624390778183446	340722320204726405618912807689617461625	-1880	2331
63788123186512356001	110531778085880797908979968522485760000 00	-11	135
158812592576004664822	-446034933028279812350817874330611762927079	-6740	639
491529834940711863545	-767664748782824827328732037300680046080 0	-25840	2691
778121977076533994270	836550629932636415433862219026485201586 25	-3560	5031
1056137838517295947582	345129671483519623388707144255902555516 81	-70	177
1091379930771597822721	-992304430068942204027385315580107223040 00	38960	3393
1202915055786699743638	535384460107862619444176358949623452025	7840	2511
2345704511683192121806	-902100762412601807926883761033156636575937 5	-14860	2421
309686433461043925202 2	-858506739076820940781279898390463769667879	-5	26
368084600610502538024 3	382354925380554520634708065792580377290 0	10328	2907
488568780887367178737 69	311875551274550630964340541678978678630400 0	-8720	13509
5023109290447026238846	172307028715490007483528343434465191184652 9	-655	243
704713396471702705511 0	608483091352335992984516057996786867494042 5	-2780	4653
15589866837195270063049	-148086935778195797958695366995638434313666 56	-19120	2727
221394109008347850591 95	673332329300790708716342654751864526363542 00	-12160	7659
231819314987640734437 10	-129678002836860809325881857439654807419989 75	-15830	2007
232572115330696606620 25	-271320668811717174784832334274232989744896 00	-6736	927
408859600716235334020 94	-220893566183419511743172152334517081828022191	9598	171
807719285196880443283 45	773246135432407989039601133768717369344 00	-4010	339
966148184718359960068 45	169674207344719455092048156293205053190400	1528	1899
162148129016051669054785	-700643054670341159978745564045962362178355200	-18800	2403
251653795575144603139313	950050430242553244529811771910922421322267033 6	-7088	6057
303232848545484408282614	-513768013664529351311483890599036231021533437 5	10060	2313
792730824646378117452517	107891184684808592438523258292998789909817600	2372	1089
845779368201476985117505	139520802452557257825506680208452597003823 6400	-3400	299
988206562952637534705025	403640866105661266338265292245730644252164096 00	-10640	3501
120498459590156542625389 3	420361950788928178283791597629917345020422400	4780	1887
125456378253210691782576 1	326334421011475076633583096252694675460000 00	-97	5
203035254887615830326385 4	527855941658733788306437169014252525293116542929	-181	288
280824775877573984653204 6	-194538960009787391836257024519082934757721537 5	-590	67
167302313961870185994776 14	275096410489343497481615456639226295591913847804625	-4495	1971
923963006353643178248840 62	517416068178189153899285426436670772369894021025	8656	4779
241356562285348827406451894	239196310124712567231437666988573024891642683265625	-44512	3285
475668889686708922071772558	237299543025483671693929700036501768931787510065841	-6480	379
106510618713441038500463020 6	165031175519231666816637006489377599410518421854950209	6379	153
129555033735159946673547927 8	-119102899310595478945546030162337788732731045444638967 9	-5251	504
152615892608424256252396884 46	307623486428217530930089716473838631146755589374112673 29	-5690	3339
749732252183441108877451230 37	102057068281404548823715018616769051480908329932871936	9380	5949
145180882575715752344574776750	720451339578645320820550792176352548127962373309799630 25	-8503	2421
644532051041139515872833852058	127488768327500156515120136574251728137499879774432346484 1	10880	30411

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*

$$y^2 = x^3 + 1787870057062165563398\,x^2 - 3010692612259710272238718021451023106733 99\,x,$$

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

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

Proof. The minimal Weierstrass equation for this curve is

$$y^2 + xy = x^3 + x^2 - 85410148429528838113064973147497868527637\,x + 941795940891009199205661922839723393804231554271643982191362 9$$

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

$$[18773016241328080 9858, -93865081206640404929],$$
$$\left[\frac{595956685687388521131}{4}, -\frac{595956685687388521131}{8}\right],$$
$$[-336719333835127940142,\ 168359666917563970071].$$

Independent points of infinite order are:

$$Q_1 = [-88291577656194741642, -4033694058765621728866261579929],$$
$$Q_2 = [132528792265728660983, 65297434667548817582215882 0071],$$
$$Q_3 = [189017660415735476733, 16460466866858348524733070 4446],$$
$$Q_4 = [231479176857636247358, 14319730632233113024103254 07571],$$

$$Q_5 = [-180297353866722177267, -435387558328921402645858521155 4],$$
$$Q_6 = [909604797725054454039, 26159474457841141855998719225058],$$
$$Q_7 = \left[\frac{756047350491789564987}{4}, \frac{131375339440564630243715299539 3}{8}\right],$$
$$Q_8 = [55630593261979172358, 219970581614067096929602717007 1],$$
$$Q_9 = \left[-\frac{1273208682650879588693}{4}, -\frac{166949205154173250340295589113 07}{8}\right],$$
$$Q_{10} = [1080524808274356861913, 343319017350678558660977757258 46],$$
$$Q_{11} = \left[\frac{204885642862796148902747}{2209}, \frac{157250952026186871978974423595399558}{103823}\right],$$

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 $S(N,E) = \sum_{p=2}^{N}(-a_p + 2)/(p + 1 - a_p)\log p$, where $a_p = a_p(E) = p + 1 - \#E(\mathbf{F}_p)$, since it is experimentally known [**16, 19**] 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

$$y^2 = x^3 + 188242741159406162972959111 3\,x^2 + 39853608724679710582849269760044810580213942846095 36\,x,$$

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 $9 \leq$ rank ≤ 11 (corresponding to the parameters $(r,s) = (14920, 128853), (-25936, 14319)$).

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

REFERENCES

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

2. J. Cremona, *Algorithms for modular elliptic curves*, Cambridge University Press, Cambridge, 1997.

3. L.E. Dickson, *History of the theory of numbers*, Vol. 2, Chelsea, New York, 1966.

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

5. ———, *On Diophantine quintuples*, Acta Arith. **81** (1997), 69–79.

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

7. ———, *Diophantine* m*-tuples and elliptic curves*, J. Theor. Nombres Bordeaux **13** (2001), 111–124.

8. ———, *There are only finitely many Diophantine quintuples*, J. reine angew. Math. **566** (2004), 183–214.

9. ———, *On Mordell-Weil groups of elliptic curves induced by Diophantine triples*, Glas. Mat. **42** (2007), 3–18.

10. ———, *Rational Diophantine sextuples with mixed signs*, Proc. Japan Acad. Sci. **85** (2009), 27–30.

11. ———, *High rank elliptic curves with prescribed torsion*, `http://web.math.hr/~duje/tors/tors.html`.

12. Y. Fujita, *The number of Diophantine quintuples*, Glas. Mat. **45** (2010).

13. P. Gibbs, *Some rational Diophantine sextuples*, Glas. Mat. **41** (2006), 195–203.

14. ———, *Adjugates of Diophantine quadruples*, Integers **10** (2010), 201–209.

15. R.K. Guy, *Unsolved problems in number theory*, 3rd edition, Springer-Verlag, New York, 2004.

16. J.-F. Mestre, *Construction de courbes elliptiques sur* $\mathbf{Q}$ *de rank* ≥ 12, C.R. Acad. Sci. **295** (1982), 643–644.

17. ———, *Formules explicites et minorations de conducteurs de variétés algébriques*, Compos. Math. **58** (1986), 209–232.

18. R. Miranda, *An overview of algebraic surfaces*, in *Algebraic geometry*, Dekker, New York, 1997.

19. K. Nagao, *An example of elliptic curve over* $\mathbf{Q}$ *with rank* ≥ 20, Proc. Japan Acad. Sci. **69** (1993), 291–293.

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

21. T. Shioda, *On the Mordell-Weil lattices*, Comment. Math. Univ. St. Paul. **39** (1990), 211–240.

22. J.H. Silverman, *Advanced topics in the arithmetic of elliptic curves*, Springer-Verlag, New York, 1994.

23. Wolfram Research, Inc., `Mathematica`, Version 7.0, Champaign, IL, 2008.

Departamento de Matemáticas, Universidad del País Vasco, Aptdo. 644, 48080 Bilbao, Spain
Email address: julian.aguirre@ehu.es

Department of Mathematics, University of Zagreb, Bijenička cesta 30, 10000 Zagreb, Croatia
Email address: duje@math.hr

Departamento de Matemáticas, Universidad del País Vasco, Aptdo. 644, 48080 Bilbao, Spain
Email address: juancarlos.peral@ehu.es