Hacettepe Journal of
Mathematics & Statistics

Hacet. J. Math. Stat.
Volume 50 (3) (2021), 721 – 731
DOI : 10.15672/hujms.708945

Research Article

Elliptic curve involving subfamilies of rank at least 5 over $\mathbb{Q}(t)$ or $\mathbb{Q}(t,k)$

Ahmed El Amine Youmbai*[1,2], Muhammed Uludağ[3], Djilali Behloul[1,4]

[1] *LATN Laboratory, Faculty of Mathematics, USTHB, BP 32, El Alia, 16111 Bab Ezzouar, Algiers, Algeria*

[2] *Mathematics Department, Faculty of Exact Sciences, University of El Oued, PO Box 789, 39000, El Oued, Algeria*

[3] *Department of Mathematics, Galatasaray University, Çiragan Cad. No. 36, 34357 Beşiktaş, Istanbul, Turkey*

[4] *Computer Science Department, USTHB, BP 32, El Alia, 16111 Bab Ezzouar, Algiers, Algeria*

Abstract

Motivated by the work of Zargar and Zamani, we introduce a family of elliptic curves containing several one- (respectively two-) parameter subfamilies of high rank over the function field $\mathbb{Q}(t)$ (respectively $\mathbb{Q}(t,k)$). Following the approach of Moody, we construct two subfamilies of infinitely many elliptic curves of rank at least 5 over $\mathbb{Q}(t,k)$. Secondly, we deduce two other subfamilies of this family, induced by the edges of a rational cuboid containing five independent $\mathbb{Q}(t)$-rational points. Finally, we give a new subfamily induced by Diophantine triples with rank at least 5 over $\mathbb{Q}(t)$. By specialization, we obtain some specific examples of elliptic curves over $\mathbb{Q}$ with a high rank (8, 9, 10 and 11).

Mathematics Subject Classification (2020). 14H52, 11G05, 11D45

Keywords. elliptic curves, rank, rational cuboid, diophantine triples

1. Introduction

According to the fundamental theorem of Mordell on elliptic curves, the set of $\mathbb{Q}-$rational points $E(\mathbb{Q})$ of an elliptic curve E defined over $\mathbb{Q}$ is a finitely generated abelian group, under an operation known as chord-and-tangent addition, therefore, it can be written as a direct sum $E(\mathbb{Q}) \simeq T \oplus L$ where T is the torsion subgroup (set of elements of finite order) and L is a free part isomorphic to r copies of $\mathbb{Z}$. The nonnegative integer r (called the rank of the elliptic curve) never cease to intrigue number theorists and until today, there is no computational formula that gives its exact value. The question of whether elliptic curves of arbitrary high rank exist has been a topic of wide debate with initial conjectures by Neron and Honda [15] about the boundedness of the rank, a part of specialists (Cassels [5], Tate [26], Mestre [16], Silverman [24], Brumer [3]) believe that the rank is unbounded. Following recent studies [22], other specialists like Park, Poonen,

*Corresponding Author.
Email addresses: youmbai-amine@univ-eloued.dz (A.E.A Youmbai), muhammed.uludag@gmail.com (A. M. Uludag), dbehloul@yahoo.fr (D. Behloul)
Received: 25.03.2020; Accepted: 29.10.2020

Voight and Wood have predicted that it is bounded. It has become of interest to construct elliptic curves with exceptionally high ranks.

One of the most powerful tools to compute a lower bound of the rank of an elliptic curve over function field is the specialization theorem of Silverman [25], which states that if a set of N $\mathbb{Q}(t)-$rational points of an elliptic curve defined over the function field $\mathbb{Q}(t)$ are independent for a single value of t then they remain so for all except a finite number of values of t. (To our knowledge there is no way to determine these exceptional values in general).

To search for specific high-rank elliptic curves, one usually constructs infinite families of high generic rank and then try to find in these families curves having a particularly high rank using for example the sum of Mestre-Nagao [17] defined by

$$S(N,E) = \sum_{p\leq N:p \text{ prime}} \left(1 - \frac{p-1}{|E(\mathbb{F}_t)|}\right)\log p = \sum_{p\leq N:p \text{ prime}} \frac{-a_p+2}{p+1-a_p}\log p. \tag{1.1}$$

It is experimentally known ([16, 19, 20]) and strongly supported by the BSD conjecture (see [4]) that we can expect to find curves of high rank by looking at those which have a large $S(N,E)$. This method has been exploited in various constructions ([1, 9, 11, 19, 20]) successfully.

In this work we use a simpler procedure: starting with a family of prescribed generic rank, we impose a given abscissa point by making the necessary parameter changes so that the point lies on the curve and we verify its independence from the generic points. This procedure can be repeated to increase the rank by 1 each time. There are some difficulties involved in the repetition of our procedure, which depend to the choice of the starting point. We thus have more complicated functions. In our case, 3 points are imposed and among the resulting curves, one of them seems to be useful for finding high rank elliptic curves over $\mathbb{Q}$.

2. The elliptic curve $E_{a,b,c}$

In [27], authors give some heuristics about the elliptic curve

$$E_{(r,s)} : (y-r)(y+r) = x(x-s)(x+s), \tag{2.1}$$

which contains several subfamilies of rank 4, 5 over $\mathbb{Q}(t)$ and 6 (parametrized by an elliptic curve of positive rank) and construct a new subfamily of such curves. In this note, we deal with a similar curve given by the equation

$$E_{(a,b,c)} : (y-h)(y+h) = (x-a^{\alpha})(x-b^{\beta})(x-c^{\gamma}), \tag{2.2}$$

where $a,b,c \in \mathbb{Q}(t)$ or $\mathbb{Q}(t,k)$, $h = a^l b^m c^n$ and (l,m, n,α, β and γ are positive integers). What makes the family $E_{(a,b,c)}$ interesting is that it has different sub-families of rank going up to 5 over $\mathbb{Q}(t)$ or $\mathbb{Q}(t,k)$. In [18] the authors construct two subfamilies of $E_{(a,b,c)}$ of rank ≥ 5 over $\mathbb{Q}(t)$. The first subfamily is given by the equation

$$y^2 = x(x-a^2)(x-b^2) + a^2b^2,$$

which corresponds to

$$E_{(a,b,0)} : (y-ab)(y+ab) = x(x-a^2)(x-b^2). \tag{2.3}$$

The second uses a new parametrization of the edge lengths of a rational cuboid to construct a subfamily of

$$y^2 = (x-c^2)(x-a^2)(x-b^2) + a^2b^2b^2$$

of rank ≥ 5, in term of our new elliptic curve, it corresponds to

$$E_{(a,b,c)} : (y-abc)(y+abc) = (x-a^2)(x-b^2)(x-c^2). \tag{2.4}$$

In the next section we construct two new high rank subfamilies of $E_{(a,b,c)}$ over $\mathbb{Q}(t,k)$

3. High rank subfamilies over $\mathbb{Q}(t,k)$

3.1. First high rank subfamily of $E_{(a,b,c)}$

We treat the case where

$$\begin{cases} h = a \\ c = 0 \end{cases} \tag{3.1}$$

Under these conditions, we are going to study the elliptic curve

$$E^1_{(a,b)} : (y-a)(y+a) = x(x-a)(x-b). \tag{3.2}$$

3.1.1. Generic rank. The curve (3.2) can be written as

$$E^1_{(a,b)} : y^2 = x(x-a)(x-b) + a^2.$$

Here, we are only interested in the case where the curve is not singular. We see the points $P_0 = (0,a)$, $P_1 = (a,a)$ and $P_2 = (b,a)$ are on $E_{(a,b)}$ and as they are collinear, only two of them can be independent which can be seen by using the specialization theorem [25]. When we specialize to $(a,b) = (2,3)$ we obtain a set of three points

$$P_0 = (0,2), P_1 = (2,2) \text{ and } P_2 = (3,2)$$

on the elliptic curve

$$E^1_{(2,3)} : y^2 = x(x-2)(x-3) + 4.$$

Using MAGMA [2], one can easily check that the associated height pairing matrix of $P_1 = (2,2)$ and $P_2 = (3,2)$ has non zero determinant $\simeq 0.445622526870092824595332301823$ showing that these two points are independent and so $E_{(2,3)}$ has rank ≥ 2.

3.1.2. Rank-3 family. In order to increase the rank, we will extract a subfamily which contains an additional point P_3 so that P_1, P_2 and P_3 are independent. To do this, we impose another point on $E_{(a,b)}$ with x-coordinate $a+b$ which implies that $a^2b + a^2 + ab^2$ is a perfect rational square, a simple calculation shows that

$$b = \frac{a(a+2r)}{(-a+r^2)}$$

is among a possible parametric solutions. Hence the point

$$P_3 = \left(ar\frac{(r-2)}{(-a+r^2)}, \frac{a(a+ar+r^2)}{(a-r^2)} \right)$$

is a rational point on the subfamily

$$F^1_{(a,r)} : y^2 = x^3 + \frac{ar(r+2)}{(a-r^2)}x^2 + \frac{a^2(a+2r)}{(-a+r^2)}x + a^2. \tag{3.3}$$

By specialization to $(a,r) = (5,4)$ the three points $P_1 = (5,5)$, $P_2 = (-45,5)$ and $P_3 = (-40,95)$ which are on the resulting elliptic curve $y^2 = x^3+40x^2-225x+25$ are independent since they have non-vanishing regulator $3.91899867632371445488440215771$ as calculated by MAGMA. Hence, the rank is ≥ 3.

3.1.3. Rank-4 family. We continue the procedure by forcing another point of abscissa $\frac{(a-r^2)}{(a-2r)}$ to be on the curve. This holds when $\frac{(a-r^2)}{(a-2r)}$ is a perfect rational square, say t^2. A simple parametric solution is given by

$$a = r\frac{(-r+2t^2)}{(t-1)(t+1)}.$$

We arrange the curve with the new parameters to get the subfamily

$$G^1_{(t,r)} : y^2 = x^3 + \left(\frac{r(r-2t^2)}{(t^2)}\right)x^2 + \left(-\frac{r^2(r-2t^2)^2}{t^2(t-1)^2(t+1)^2}\right)x + \left(\frac{r(-r+2t^2)}{(t-1)(t+1)}\right)^2, \quad (3.4)$$

which contains the points

$$\begin{aligned} P_1 &= \left(\frac{r(-r+2t^2)}{(t-1)(t+1)}, \frac{r(-r+2t^2)}{(t-1)(t+1)}\right), \\ P_2 &= \left(\frac{r(r-2t^2}{t^2(t-1)(t+1)}, \frac{r(-r+2t^2)}{(t-1)(t+1)}\right), \\ P_3 &= \left(\frac{-r(r-2t^2)}{t^2}, \frac{r(r-2t^2)(r-t^2)}{t^2(t-1)(t+1)}\right), \\ P_4 &= \left(t^2, t(r-t^2)\right). \end{aligned}$$

Specialization to $(t,r) = (5,3)$ yield the elliptic curve

$$y^2 = x^3 - \frac{141}{25}x^2 - \frac{2209}{1600}x + \frac{2209}{64}.$$

The points in question $P_1 = (47/8, 47/8)$, $P_2 = (-47/200, 47/8)$, $P_3 = (141/25, 517/100)$ and $P_4 = (25, -110)$ have regulator 147.475251328688414759767293294, Consequently, the points are independent and the curve with two parameters $G^1_{(t,r)}$ is of rank ≥ 4.

3.1.4. Rank-5 family. We impose another point with x-coordinate $-\dfrac{r(r-2t^2)}{t^2(t-1)(t+1)}$ on the curve $G^1_{(t,r)}$. Hence we want $(-4rt^2 + 2r^2 + t^6)$ to be a perfect rational square, indeed, over $\mathbb{Q}(t)$ the conic section $2r^2 - (4t^2)r + (t^6) = k^2$ has a solution $(r,k) = (0, t^3)$, so a parametric solution can be given by

$$r = \frac{2t^2(kt-2)}{(k^2-2)}.$$

This gives a new subfamily $H^1_{(t,k)}$ with equation

$$y^2 = x^3 - \left(\frac{4kt^2(k-t)(kt-2)}{(k^2-2)^2}\right)x^2 - \left(\frac{16t^6k^2(k-t)^2(kt-2)^2}{(k^2-2)^4(t-1)^2(t+1)^2}\right) + \left(\frac{4t^4k(kt-2)}{(k^2-2)^2(t-1)(t+1)}\right). \quad (3.5)$$

This last subfamily contains the following five $\mathbb{Q}(t,k)$-rational points :

$$\begin{aligned} P_1 &= \left(\frac{4t^4k(k-t)(kt-2)}{(k^2-2)^2(t-1)(t+1)}, \frac{4t^4k(k-t)(kt-2)}{(k^2-2)^2(t-1)(t+1)}\right), \\ P_2 &= \left(\frac{-4kt^2(k-t)(kt-2)}{(k^2-2)^2(t-1)(t+1)}, \frac{4t^4k(k-t)(kt-2)}{(k^2-2)^2(t-1)(t+1)}\right), \\ P_3 &= \left(\frac{4kt^2(k-t)(kt-2)}{(k^2-2)^2}, \frac{4kt^2(k-t)(kt-2)(-2kt+k^2+2)}{(k^2-2)^3(t-1)(t+1)}\right), \\ P_4 &= \left(t^2, \frac{-t^3(-2kt+k^2+2)}{(k^2-2)}\right), \\ P_5 &= \left(\frac{4kt^2(k-t)(kt-2)}{(k^2-2)^2(t-1)(t+1)}, \frac{16k^2t^6(kt-2)^2(k-t)^2(-4k+2t+k^2t)^2}{(k^2-2)^6(t-1)^2(t+1)^2}\right). \end{aligned}$$

Specialization at $(t,k)=(11,17)$ shows that these points are

$$\begin{aligned} P_1 &= \left(\frac{9209189}{82369}, \frac{9209189}{82369}\right), \\ P_2 &= \left(\frac{-76109}{82369}, \frac{9209189}{82369}\right), \\ p_3 &= \left(\frac{9133080}{82369}, \frac{764362687}{23639903}\right), \\ P_4 &= \left(121, \frac{110473}{287}\right), \\ P_5 &= \left(\frac{76109}{82369}, \frac{2622944467}{23639903}\right), \end{aligned}$$

on the specialized curve

$$H^1_{(11,17)} : y^2 = x^3 - \frac{9133080}{82369}x^2 - \frac{700902165601}{6784652161}x + \frac{84809162037721}{6784652161}. \tag{3.6}$$

Magma computes the regulator of the set $S=\{P_1,P_2,P_3,P_4,P_5\}$ to be $R(S)\simeq 6915.28812722...$ which implies the independence of these points, and shows that the subfamily $H^1_{(t,k)}(\mathbb{Q}(t,k))$ is of rank at least 5.

3.2. Second high rank subfamily of $E_{(a,b,c)}$

The study of this curve is similar to the first family (3.2), so some details will be omitted. Consider the elliptic curve given by

$$E^2_{(a,b)} : (y-ab)(y+ab) = x(x-ab)(x-b),$$

which can be written as

$$E^2_{(a,b)} : y^2 = x(x-ab)(x-b) + (ab)^2. \tag{3.7}$$

In addition to the three clearly visible points $(0,ab)$, (b,ab) and (ab,ab), we start by imposing :

3.2.1. The first point with abscissa $ab+b$. This can be achieved when $b=\dfrac{-(a-r)(a+r)}{a(a+1)}$. The curve becomes

$$F^2_{(a,r)} : y^2 = x\left(x - \frac{-(a-r)(a+r)}{(a+1)}\right)\left(x - \frac{-(a-r)(a+r)}{a(a+1)}\right) + \left(\frac{-(a-r)(a+r)}{(a+1)}\right)^2. \tag{3.8}$$

3.2.2. The second point with abscissa $-a$. For that we need $a=-k^2$ and the equation will be of the form

$$G^2_{(k,r)} : y^2 = x^3 + \left(\frac{-(k^4-r^2)}{(k^2)}\right)x^2 + \left(\frac{-(r+k^2)^2(-r+k^2)^2}{k^2(k-1)^2(k+1)^2}\right)x + \left(\frac{(r+k^2)^2(-r+k^2)^2}{(k-1)^2(k+1)^2}\right). \tag{3.9}$$

3.2.3. The third point with abscissa $\dfrac{(r+k^2)(-r+k^2)}{(k-1)^2(k+1)^2}$. To force this point to be in the curve, it must be shown that the conic section

$$t^2 = (2k^4-5k^2+2)r^2 + k^2(k+k^2-1)^2(-k+k^2-1)^2$$

has a solution. Indeed, over $\mathbb{Q}(k)$ this last has the solution $(t,r)=(k(k+k^2-1)(-k+k^2-1),0)$. Therefore, a parametrized solution can be given by

$$r = \frac{2tk(-k+k^2-1)(k+k^2-1)}{(t^2+5k^2-2k^4-2)}.$$

Finally, we obtain an elliptic curve over $\mathbb{Q}(t,k)$ with equation

$$H^2_{(t,k)} : y^2 = x(x-ab)(x-b)+(ab)^2 \tag{3.10}$$

where

$$\begin{aligned}
ab &= \frac{k^2(kt-5k^2+2k^4+2)(-kt-5k^2+2k^4+2)(k-t)(k+t)}{(-5k^2+2k^4-t^2+2)^2(k-1)(k+1)},\\
b &= \frac{-(-kt-5k^2+2k^4+2)(kt-5k^2+2k^4+2)(k-t)(k+t)}{(-5k^2+2k^4-t^2+2)^2(k-1)(k+1)},\\
a &= -k^2.
\end{aligned}$$

which contains five $\mathbb{Q}(t,k)$-rational points given by their abscissa

$$\begin{aligned}
x(P_1) &= 0,\\
x(P_2) &= \frac{(t+k)(-tk-5k^2+2k^4+2)(tk-5k^2+2k^4+2)(t-k)}{(t^2+5k^2-2k^4-2)^2(k-1)(k+1)},\\
x(p_3) &= \frac{(t+k)(tk+5k^2-2k^4-2)(tk-5k^2+2k^4+2)(t-k)}{(t^2+5k^2-2k^4-2)^2},\\
x(P_4) &= k^2,\\
x(P_5) &= \frac{k^2(t+k)(tk+5k^2-2k^4-2)(tk-5k^2+2k^4+2)(t-k)}{(t^2+5k^2-2k^4-2)^2}.
\end{aligned}$$

By specialization to $(t,k)=(2,3)$ we get the elliptic curve

$$H^2_{(2,3)} : y^2 = x^3 - \frac{2825}{529}x^2 - \frac{71825625}{17909824}x + \frac{646430625}{17909824}.$$

The above mentioned points are

$$\begin{aligned}
P_1 &= (0, 25425/4232),\\
P_2 &= (-2825/4232, 25425/4232),\\
P_3 &= (2825/529, 93225/24334),\\
P_4 &= (9, 396/23),\\
P_5 &= (25425/33856, 34400025/6229504).
\end{aligned}$$

Their regulator calculated by Magma equal to 493.274384561293540502319589793 which proves their independence.

4. Subfamilies of $E_{(a,b,c)}$ with rank at least 5 arising from a rational cuboid

Let S be a system of 3 Diophantine equations with 6 unknowns defined by

$$S = \begin{cases} x^2+y^2 = Z^2,\\ x^2+z^2 = Y^2,\\ y^2+y^2 = X^2. \end{cases} \tag{4.1}$$

Searching for a rational solution to system (4.1) is equivalent to looking for a rectangular parallelepiped (cuboid) whose edges and the diagonals of faces are all rational. Such system has infinity many parametric solutions that can be found in [6, 18, 23]. If $[a,b,c]$ are edges of a rational cuboid then both $[ka,kb,kc]$ and $[ab,bc,ac]$ constitute a cuboid as well. In [18], it was shown that if a,b and c are edge lengths of a rational cuboid, then the curve (2.4) has 5 independent rational points. In fact, from this construction, one can create other subfamilies of rank at least 5 in a very simple way.

4.1. First subfamily

Let
$$E^{Cub1}_{(a,b,c)}:(y-a^2b^2c^2)(y+a^2b^2c^2)=(x-a^2b^2)(x-a^2c^2)(x-b^2c^2)$$
which can be written as
$$E^{Cub1}_{(a,b,c)}:y^2=(x-a^2b^2)(x-a^2c^2)(x-b^2c^2)+a^4b^4c^4. \tag{4.2}$$
This curve has torsion subgroup isomorphic to $\mathbb{Z}/2\mathbb{Z}$ generated by $(0,0)$.
The three points
$$P_0=(b^2c^2,a^2b^2c^2),\ P_1=(a^2b^2,a^2b^2c^2)\ \text{and}\ P_2=(a^2c^2,a^2b^2c^2)$$
clearly lie on the curve, they are non-torsion and since they are collinear, at most two of them can be independent. By consideration of any parametrization of a rational cuboid with lengths a, b and c three other points will be on (4.2), namely
$$P_3=((ab)^2+(ac)^2,a^3bcA),$$
$$P_4=((ab)^2+(bc)^2,ab^3cC),$$
$$P_5=((ac)^2+(bc)^2,abc^3B),$$
where $A^2=b^2+c^2$, $B^2=a^2+c^2$ and $C^2=a^2+b^2$. Using one of the parametrizations in ([18], Section 3.1-(4))
$$\begin{array}{rcl} a&=&-2t^2(t^4-3)(3t^4-1),\\ b&=&-8t^2(t^8-1),\\ c&=&(t^4-1)(t^8-14t^4+1),\\ A&=&(t^4-1)(t^8+18t^4+1),\\ B&=&(t^4+1)^3,\\ C&=&2t^2(5t^8-6t^4+5),\end{array} \tag{4.3}$$
and by specialization to $t=2$, (4.2) becomes
$$E^{Cub1}_2:y^2=x^3-1613068785000000x^2+353648093980462850805350400000x.$$
The five points in the resulting curve are
$$\begin{array}{rcl} P_1&=&(1590899377766400,389810120037212160000),\\ P_2&=&(5854270593600,389810120037212160000),\\ P_3&=&(1596753648360000,385635237438477312000 0),\\ P_4&=&(1607214514406400,645882676895858688000 0),\\ P_5&=&(22169407233600,46015992586586880000),\end{array}$$

and have a non-zero regulator R =952846.119732081738743944356546 as calculated by Magma which confirms that the rank is at least 5.

4.2. Second subfamily

Other new subfamily can be given by considering the elliptic curve defined by
$$E^{Cub2}_{(a,b)}:y^2=(x-a^2)(x-b^2)(x-a^2b^2)+a^4b^4. \tag{4.4}$$
In addition to the three obvious points
$$P_0=(a^2b^2,a^2b^2),P_1=(a^2,a^2b^2)\ \text{and}\ P_2=(b^2,a^2b^2),$$

three other points can be imposed in the curve as follows: let $f(x)$ be the second member of (4.4), then

$$\begin{aligned} f(a^2+b^2) &= a^2b^2(a^2+b^2), \\ f(a^2+a^2b^2) &= a^6b^2(b^2+1), \\ f(b^2+a^2b^2) &= a^2b^6(a^2+1). \end{aligned} \tag{4.5}$$

From (4.5) we see that if 1, a and b are edge lengths of a rational cuboid, than, the points of abscissa (a^2+b^2), $(a^2+a^2b^2)$ and $(b^2+a^2b^2)$ are in the curve. Multiplication by $1/c$ on (4.3) yield a parametrization for the cuboid with lengths 1, a and b

$$\begin{aligned} a &= \frac{(t^4-1)(t^8-14t^4+1)}{-2t^2(t^4-3)(3t^4-1)}, \\ b &= \frac{-8t^2(t^8-1)}{-2t^2(t^4-3)(3t^4-1)}, \\ c &= 1. \end{aligned} \tag{4.6}$$

Now, let's show that the five points with abscissa a^2, b^2, (a^2+b^2), $(a^2+a^2b^2)$ and $(b^2+a^2b^2)$ are independent by specialization to $t=2$ in (4.6), the resulting curve is

$$E_2^{Cub2}: y^2 = x^3 - \frac{25204199765625}{8919588418624} + \frac{1445469627586730625}{1331947867211652121 6}x$$

and the points are

$$\begin{aligned} P_{a^2} &= (245025/23892544, 15932750625/557474276164), \\ P_{b^2} &= (1040400/373321, 15932750625/557474276164), \\ P_{a^2+b^2} &= (66830625/23892544, 1031889375/3649586096), \\ P_{a^2+a^2b^2} &= (346396988025/8919588418624, 36773725663125/10899737047558528), \\ P_{b^2+a^2b^2} &= (1569545424225/557474276164, 40324826210625/85154195684051), \end{aligned}$$

and have non zero regulator equal to 952846.119732081738743944356548, hence the points are independent and (4.4) is of rank at least 5 over $\mathbb{Q}(t)$.

5. High rank subfamily of $E_{(a,b,c)}$ induced by rational diophantine triples

In this section we introduce a new subfamily of (2.2) arising from Diophantine triples. A set of m non zero rationals $\{a_1, a_2, ..., a_m\}$ is called a *rational Diophantine m-tuple* if a_ia_j+1 is a perfect rational square for all $1 \leq i < j \leq m$. Rational Diophantine m-tuples have been thoroughly studied by A. Dujella, ([7, 8, 10, 12–14]). Here, we will use triples with this property to impose 3 points on the curve

$$E_{(a,b)}^{Dio}: y^2 = (x-1)(x-a^2)(x-a^2b^2) + a^4b^2. \tag{5.1}$$

The points

$$Q_0 = (a^2b^2, a^2b), Q_1 = (1, a^2b) \text{ and } Q_2 = (a^2, a^2b)$$

lie in the curve. Noting that if the images by $g(x)$ (second member of (5.1))

$$\begin{aligned} g(a^2+a^2b^2) &= a^6b^2(b^2+1), \\ g(a^2+1) &= a^2(a^2+1), \\ g(a^2b^2+1) &= a^2b^2(a^2b^2+1) \end{aligned} \tag{5.2}$$

are perfect squares then, the points of abscissa a^2+1, a^2b^2+1 and $a^2b^2+a^2$ will also be in the curve, to realize this, we have to solve the system of Diophantine equations with 5 unknowns

$$S' = \begin{cases} a^2+1 = A^2, \\ b^2+1 = B^2, \\ a^2b^2+1 = C^2. \end{cases} \tag{5.3}$$

This problem is equivalent to finding a rational Diophantine triples of the form $\{1, a^2, b^2\}$. There are several rational parametric solutions for this and we will give two of them which were communicated to us by A. Dujella. For $t \notin \left\{0, \pm 1, -\frac{1}{3}, \frac{1}{2}, -2, 3\right\}$

$$\begin{aligned} a &= \frac{4(t^2+1)(t^2-t-1)}{(t-1)(t-3)(3t+1)(t+1)}, \\ b &= \frac{(t^2+1)(t^2+4t-1)}{2t(t+2)(2t-1)}. \end{aligned} \tag{5.4}$$

For the second rational parametric solutions $(t \neq \pm 2)$

$$\begin{aligned} a &= \frac{(3t^2-4)(t^2-12)}{4(t-2)(t+2)(t^2+4)}, \\ b &= \frac{16t(t^2+4)}{(t^2-8t+4)(t^2+8t+4)}. \end{aligned} \tag{5.5}$$

Replacing a and b from (5.4) or (5.5) in (5.1), we get a subfamily of infinitely many elliptic curves F_t^{Dio} which contains the above mentioned points. Let us now show that the resulting subfamily has a rank greater than or equal to 5 over $\mathbb{Q}(t)$ by proving the independence of the five $\mathbb{Q}(t)$-rational points of abscissa

$$\begin{aligned} x(Q_1) &= 1, \\ x(Q_2) &= a^2, \\ x(Q_3) &= a^2+1, \\ x(Q_4) &= a^2b^2+1, \\ x(Q_5) &= a^2b^2+a^2. \end{aligned}$$

By specializing to $t=5$ in (5.4) this gives

$$a = 247/96, \ b = 572/315.$$

For these values, the resulting elliptic curve is

$$F_5^{Dio}(\mathbb{Q}) : y^2 = x^3 - \frac{26929244281}{914457600}x^2 + \frac{3643908031465}{21069103104}x,$$

and the points are

$$\begin{aligned} Q_1 &= \left(1, \frac{8724287}{725760}\right), \\ Q_2 &= \left(\frac{61009}{9216}, \frac{8724287}{725760}\right), \\ Q_3 &= \left(\frac{70225}{9216}, \frac{65455}{9216}\right), \\ Q_4 &= \left(\frac{1304726641}{57153600}, \frac{1275829841}{57153600}\right), \\ Q_5 &= \left(\frac{26014786681}{914457600}, \frac{1407148974517}{21946982400}\right) \end{aligned}$$

and have non zero regulator equal to 798694.261749649017692248307870. Therefore, the points are independent and the rank of F_t^{Dio} is at least 5 aver $\mathbb{Q}(t)$.

6. Numerical results

In this section, we try to find curves from our families of large rank by calculating $S(10^5, E)$ using Pari-Gp [21] and choosing the best candidates. To go further in the calculation, we choose the curve (3.5) because these coefficients increase in very small ways compared to the other curves obtained in this work. So, for the curve (3.5) let us put $t = 1/k$ which gives a curve defined over $\mathbb{Q}(k)$, this choice is justified by looking at the size of the coefficients of the obtained curve

$$H^1_{(\frac{1}{k},k)} : y^2 = x^3 + \left(\frac{4(k-1)(k+1)}{k^2(k^2-2)^2}\right)x^2 + \left(\frac{-16}{k^2(k^2-2)^4}\right)x + \left(\frac{4}{k^2(k^2-2)^2}\right) \tag{6.1}$$

written under its integral model

$$I^1_{(k)} : y^2 = x^3 + (4k^2-4)x^2 - 16k^2x + 16k^2(k^2-2)^2. \tag{6.2}$$

By using Magma and Pari-Gp we calculated $S(10^5, E)$ for $k \leq 100000$ and found several elliptic curves of rank 7, 8 and 9, two of rank 10 and only one of rank 11, the results are listed in the following table

Table 1. High Rank Curves

rank	k
7	23, 38, 941, ...
8	82, 138, 502, ...
9	123, 309, 652, 707, 749, 901, 996, 1044, ...
10	5394, 24862
11	30422

Acknowledgment. We would like to express our deep gratitude to the referee for the many comments, corrections and suggestions that helped to considerably improve the manuscript. Special thanks to Prof. Andrej Dujella for his help and clarifications on diophantine triples.

References

[1] J. Aguirre, A. Dujella, M.J. Bokun and J.C. Peral, *High rank elliptic curves with prescribed torsion group over quadratic fields*, Period. Math. Hungar. **68** (2), 222–230, 2014.

[2] W. Bosma, J.J. Cannon, C. Fieker and A. Steel (eds.), *Handbook of Magma Functions*, Edition 2.20-9, 2014.

[3] A. Brumer, *The average rank of elliptic curves I*, Invent. Math. **109** (1), 445–472, 1992.

[4] G. Campbell, *Finding elliptic curves and families of elliptic curves over $\mathbb{Q}$ of large rank*, PhD Thesis, Rutgers University, 1999.

[5] J.W.S. Cassels, *Diophantine equations with special reference to elliptic curves*, J. London. Math. Soc. **1** (1), 193-291, 1966.

[6] L.E. Dickson, *History of the Theory of Numbers*, Vol. II, Diophantine analysis, Dover Publications, New York, 2005.

[7] A. Dujella, `https://web.math.pmf.unizg.hr/~duje/index.html`.

[8] A. Dujella, *On the size of Diophantine m-tuples*, Math. Proc. Cambridge Philos. Soc. **132**, 23–33, 2002.

[9] A. Dujella, *An example of elliptic curve over $\mathbb{Q}$ with rank equal to 15*, Proc. Japan Acad. Ser. A Math. Sci. **78** (7), 109–111, 2002.

[10] A. Dujella, *On the number of Diophantine m-tuples*, Ramanujan J. **15**, 37–46, 2008.

[11] A. Dujella and J.C. Peral, *High rank elliptic curves with torsion $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/4\mathbb{Z}$ induced by Diophantine triples*, LMS J. Comput. Math. **17**, 282–288, 2014.

[12] A. Dujella and V. Petricevic, *Strong Diophantine triples*, Exp. Math. **17**, 83–89, 2008.

[13] A. Filipin and A. Togbé, *On the family of Diophantine triples* $\{k+2, 4k, 9k+6\}$, Acta Math. Acad. Paedagog. Nyhàzi. (N.S.)ü **25** (2), 145–153,2009.

[14] B. He and A. Togbé, *On the family of Diophantine triples* $\{k+1, 4k, 9k+3\}$, Period. Math. Hungar. **58** (1), 59–70, 2009.

[15] T. Honda, *Isogenies, rational points and section points of group varieties*, Jpn. J. Math. **30**, 84–101, 1960.

[16] J.F. Mestre, *Construction de courbes elliptiques sur $\mathbb{Q}$ de rang* ≥ 12, C. R. Acad. Sci. Paris, Série I, **295**, 643644, 1982.

[17] J.F. Mestre, *Courbes elliptiques de rang* ≥ 11 *sur* $\mathbb{Q}(T)$, C. R. Acad. Sci. Paris, Série I, **313**, 139-142, 1991.

[18] D. Moody, M. Sadek and A.S. Zargar, *Families of elliptic curves of rank* ≥ 5 *over* $\mathbb{Q}(t)$, Rocky Mountain J. Math. **49** (7), 2253–2266, 2019.

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

[20] K. Nagao, *An example of elliptic curve over $\mathbb{Q}$ with rank* ≥ 21, Proc. Japan Acad. Ser. A Math. Sci. **70**, 104-105, 1994.

[21] The PARI Group, PARI/GP version `2.9.1`, Univ. Bordeaux, 2016, http://pari.math.u-bordeaux.fr/.

[22] J. Park, B. Poonen, J. Voight and M.M. Wood, *A heuristic for boundedness of ranks of elliptic curves*, J. Eur. Math. Soc. **21**, 2859–2903, 2019, doi: 10.4171/JEMS/893.

[23] N. Saunderson, *The Elements of Algebra*, Book 6, Cambridge University Press, Cambridge, 1740.

[24] J.H. Silverman, *The Arithmetic of Elliptic Curves, 2nd Edition*, Vol. 106, Springer Science and Business Media, 2009.

[25] J.H. Silverman, *Advanced Topics in the Arithmetic of Elliptic Curves*, Vol. 151, Springer Science and Business Media, 2013.

[26] J.T. Tate, *The arithmetic of elliptic curves*, Invent. Math. **23** (3-4), 179–206, 1974.

[27] A.S. Zargar and N. Zamani, *A Family of Elliptic Curves of Rank* ≥ 5 *over* $\mathbb{Q}(m)$, Notes Number Theory Discrete Math. **25** (4), 24–29, 2019.