The rank of certain subfamilies of the elliptic curve $Y^2 = X^3 - X + T^2$*

Petra Tadić†

Institute of Analysis and Computational Number Theory
Technische Universität Graz, Graz, Austria
tadic@math.tugraz.at

Submitted May 24, 2012 — Accepted October 13, 2012

Abstract

Let $E$ be the elliptic curve over $\mathbb{Q}(T)$ given by the equation

$$E : Y^2 = X^3 - X + T^2.$$ 

It is known that the torsion subgroup is trivial,

$$\text{rank}_{\mathbb{C}(T)}(E) = 2 \quad \text{and} \quad \text{rank}_{\mathbb{Q}(T)}(E) = 2.$$ 

We find a parametrization of rank $\geq 3$ over the function field $\mathbb{Q}(a, i, s, n, k, l)$ where $s^2 = i^3 + a^2$. From this we get families of rank $\geq 3$ and $\geq 4$ over fields of rational functions in four variables and a family of rank $\geq 5$ parametrized by an elliptic curve of positive rank. We also found a particular elliptic curve with rank $\geq 11$.

Keywords: parametrization, elliptic surface, elliptic curve, function field, rank, family of elliptic curves, torsion

MSC: 11G05

1. Introduction

Let $E$ be the elliptic curve over $\mathbb{Q}(T)$ given by the equation

$$Y^2 = X^3 - X + T^2.$$ 

*I would like to thank professor Andrej Dujella for his guidance and discussions on the topic of this paper.

†The author was supported by the Ministry of Science, Education and Sports, Republic of Croatia, grant 037-0372781-2821 and by the Austrian Science Fund (FWF): P 24574-N26.
In [2, Theorem 1], Brown and Myers proved that if \( t \geq 2 \) is an integer, the elliptic curve \( E_t : Y^2 = X^3 - X + t^2 \) has rank at least 2 over \( \mathbb{Q} \), with linearly independent points \((0, t)\) and \((-1, t)\). They also prove that there are infinitely many integer values of \( t \) for which the elliptic curve \( E_t \) over \( \mathbb{Q} \) has rank at least 3. In [5], Eikenberg showed that the torsion subgroup is trivial, the rank of the group \( E(\mathbb{Q}(T)) \) equals 2 as does the rank of \( E(\mathbb{C}(T)) \), both groups have as generators the points \((0, T)\) and \((1, T)\). These results follow also from the more general result by Shioda (see [14, Theorem A2]). Eikenberg gives quadratic polynomials \( T(n) \in \mathbb{Q}[n] \) for which \( E_{T(n)}(\mathbb{Q}(n)) \) has rank at least 3, [5, Theorem 4.2.1]. He also shows that there are infinitely values of \( t \) for which \( E_t \) has rank at least 5.

In this paper we find a subfamily of \( E \) for which the rank over the function field \( \mathbb{Q}(a, i, s, n, k, l) \) where \( s^2 = i^3 + a^2 \) is \( \geq 3 \) and three independent points are listed. From this we get families of rank \( \geq 3 \) and \( \geq 4 \) over fields of rational functions in four variables and a family of rank \( \geq 5 \) over an elliptic curve of positive rank. We also found a particular elliptic curve with rank \( \geq 11 \).

In [16], an elliptic curve \( Y^2 = X^3 - T^2X + 1 \) was analyzed in a similar way, and the results obtained contain some resemblances with the results of this paper.

2. Subfamilies of higher rank

We know that the elliptic curve \( E \) observed in this section and defined above, has rank 2 over \( \mathbb{Q}(T) \) and \( \mathbb{C}(T) \), with generators \((0, T)\) and \((-1, T)\). First we give two subfamilies which have generic rank \( \geq 3 \) and we give the third independent point. By observing \( T(n) \) which are polynomials in the variable \( n \) of degree 3 over \( \mathbb{Q} \) with an additional point with first coordinate \( X(n) \) which is a polynomial in the variable \( n \) of degree 2 over \( \mathbb{Q} \) on the elliptic curve \( Y^2 = X^3 - X + T(n)^2 \) over \( \mathbb{Q}(n) \) (see [13, Theorem 10.10]), we obtain the following.

Theorem 2.1.

For \( T_{\pm}^{(1)}(a, i, s, n, k, l) = an^3 + (3ak + sl)n^2 + \left(3ak^2 + 2slk - al^2 \pm \frac{s}{i} \right)n - sl^3 - akl^2 + slk^2 \pm \frac{a}{i}l + ak^3 \pm \frac{s}{i}k, \)

the elliptic curve \( Y^2 = X^3 - X + T_{\pm}^{(1)}(a, i, s, n, k, l)^2 \) has rank \( \geq 3 \) over the function field \( \mathbb{Q}(a, i, s, n, k, l) \) where \( s^2 = i^3 + a^2 \), with an additional independent point \( C_{\pm}^{(1)}(a, i, s, n, k, l) \) with first coordinate

\[ X_{C_{\pm}^{(1)}}(a, i, s, n, k, l) = i(n + k)^2 - il^2. \]

Proof. For

\[ Y_{C_{\pm}^{(1)}}(a, i, s, n, k, l) = sn^3 + (al + 3ks)n^2 + \frac{2aikl \pm a - il^2 + 3isk^2}{\pm}n + \frac{-iskl^2 \pm ak - al^3 + 3isk^3 + aik^3 \pm sl}{\pm}, \]

we have

\[ X_{C_{\pm}^{(1)}}(a, i, s, n, k, l)^3 - X_{C_{\pm}^{(1)}}(a, i, s, n, k, l) - T_{\pm}^{(1)}(a, i, s, n, k, l)^2 - Y_{C_{\pm}^{(1)}}(a, i, s, n, k, l)^2 \]
The rank of certain subfamilies of the elliptic curve $y^2 = x^3 - x + t^2$

$$= (-s^2 + i^3 + a^2)q_\pm(a, i, s, n, k, l) = 0,$$

where $q_\pm \in \mathbb{Q}(a, i, s, n, k, l)$. Here we work over the function field $\mathbb{Q}(a, i, s, n, k, l)$ where $s^2 = i^3 + a^2$.

For the positive case the specialization $(a, i, s, n, k, l) \mapsto (6, -3, 1, 1, 1)$ gives $T_+^{(1)}(6, -3, 1, 1, 1) = 41$, and on the curve $E_{T_+^{(1)}}(6, -3, 1, 1, 1)$: $Y^2 = X^3 - X + 41^2$ there are three corresponding points $(0, 41), (-1, 41), (-9, 31)$ which are independent points of $E_{41}(\mathbb{Q})$. This shows that the points from the claim of the theorem are independent elements of the group

$$E_{T_+^{(1)}}(a, i, s, n, k, l)(\{Q(a, i, s, n, k, l) : s^2 = i^3 + a^2\}).$$

The proof for $T_-^{(1)}$ is analogous, we used the same specialization. \(\square\)

Now we will construct two subfamilies of generic rank $\geq 4$ by intersecting the families we have obtained. We try to find the solution to the equation

$$T_\pm^{(1)}(a, i, s, n, k, l) = T_\pm^{(1)}\left(a, 2a - s, \frac{4a^2 - 4as + i^3}{i^3}, n, k, m\right),$$

where actually $(i_2, s_2) := \left(2a\frac{a - s}{i^2}, a\frac{4a^2 - 4as + i^3}{i^3}\right) = (i, s) + (0, a)$ on the elliptic curve $Y^2 = X^3 + a^2$. This gives a polynomial $P(n)$ in the variable $n$ of degree two. Now we choose

$$k_2 := \frac{1 - 4a^3m + 4as^2ms - am^3 + 3aki^3 + sl^3}{i^3a}$$

so that the coefficient of the polynomial $P(n)$ of the term $n^2$ is zero. Now that we have $P(n)$ a linear polynomial in $n$ we can choose $n_\pm(a, i, s, k, l, m) := (256a^{10}m^3 - 1024a^9m^3s + (-288m^2ki^3 + 192m^3i^3 + 1536m^3s^2)a^8 + (864m^2ski^3 - 96m^3sl^3 - 1024m^3s^3 - 576m^3s^3)k^2 + (256m^3s^4 - 144m^3s^2k^4 + 144m^3s^2k + 888m^2s^2l^3 + 864m^3s^2ki^3)k^6 + (288m^2s^2ki^3 - 48m^2s^2sl - 288m^2s^2l^3)a^5 + (96m^2s^4l^3 - 108m^4k^4 + 114i^5s^2m - 32m^3i^9 + 54i^9 - 72i^8m + 54k^2i^8 + 96m^2s^2l - 144m^2s^2l^3k - 96m^3s^2l^3 - 72m^2l^9k)a^4 + (72m^2i^9ks - 54k^2i^9s + 54s^3l^3i^9 + 72i^8s + 90i^8m + 32m^3i^9s + 162ski^8 - 24m^2i^9l - 48m^2s^3l^6)a^3 + (\pm 54s^2ki^8 \pm 18i^11m + 36i^8s^2l - 54s^2t^9 \pm 27i^11k + 18k^9s^2t^2 + 24m^2s^2l^2) \pm \pm (2s^3l^3i^9 - 18ki^9s^3l^2i^9 + 9i^11s^a - 2s^4t^9) / (9a^3(32a^7m^2 - 96a^6m^2s + (16m^2i^3 + 96m^2s^2)k^2 + (-32m^2i^3s^2 - 32m^2i^3s^2)k^4 + (\pm 12i^5 + 16m^2s^2l^3 - 6l^2i^6 + 3i^6s^2 - 18i^6s^2m \pm 18i^6s^2m + 3i^6s^2m + 2s^4i^6t^6) a + 2s^4i^6t^6)) \text{ such that }$

$T_\pm^{(1)}(a, i, s, n_\pm(a, i, s, k, l, m), k, l) =$

$$= T_\pm^{(1)}\left(a, 2a - s, \frac{4a^2 - 4as + i^3}{i^3}, n_\pm(a, i, s, k, l, m), \frac{1 - 4a^3m + 4as^2ms - am^3 + 3aki^3 + sl^3}{i^3a}, m\right).$$
Proposition 2.2. Let
\[ S^{(1)}_{\pm}(a, i, s, k, l, m) := T^{(1)}_{\pm}(a, i, s, n_{\pm}(a, i, s, k, l, m), k, l), \]
where \( n_{\pm} \) is given above and \( T^{(1)}_{\pm} \) is as in Theorem 2.1. The elliptic curve
\[ Y^2 = X^3 - X + S^{(1)}_{\pm}(a, i, s, k, l, m)^2 \]
over the function field \( \mathbb{Q}(a, i, s, k, l, m) \) where \( s^2 = i^3 + a^2 \) has rank \( \geq 4 \) with four independent points, the two generators \( (0, S^{(1)}_{\pm}(a, i, s, k, l, m)), (-1, S^{(1)}_{\pm}(a, i, s, k, l, m)) \) mentioned in the introduction, and two additional points
\[ A^{(1)}(a, i, s, k, l, m) := C^{(1)}_{\pm}(a, i, s, n_{\pm}(a, i, s, k, l, m), k, l) \]
and
\[ B^{(1)}_{\pm}(a, i, s, k, l, m) := \]
\[ c^{(1)}_{\pm} \left( a, 2a - s, \frac{4a^2 - 4as + i^3}{i^3}, n_{\pm}(a, i, s, k, l, m), \frac{1}{3} \frac{-4a^3m + 4a^2ms - ami^3 + 3aki^3 + sli^3}{i^3a}, m \right) \]
(notation for \( C^{(1)}_{\pm} \) from Theorem 2.1).

Proof. With the specialization \( (a, i, s, k, l, m) \mapsto (6, -3, 3, 1, 1, 1) \) we prove that the above listed four points on the elliptic curve (over \( \mathbb{Q}(a, i, s, k, l, m) \) where \( s^2 = i^3 + a^2 \)) are independent, since the specialization gives the elliptic curve
\[ E_{S^{(1)}_{\pm}(6, -3, 3, 1, 1, 1)}: Y^2 = X^3 - X + \left( -\frac{5647}{13122} \right)^2 \]
with the corresponding four independent points with first coordinates 0, −1, \(-\frac{805}{972}, \frac{7084}{729}\).

The proof for \( S^{(1)}_{-\pm} \) is analogous, by picking an adequate specialization. \( \square \)

Remark 2.3. The variety (from Theorem 2.1)
\[ s^2 = i^3 + a^2 \]
can be observed as an elliptic curve \( Y^2 = X^3 + T^2 \) over the field \( \mathbb{Q}(T) \). In [12, Corollary 8] it is shown that the torsion subgroup of \( s^2 = i^3 + a^2 \) over \( \mathbb{Q}(a) \) is equal \( \{O, (0, a), (0, -a)\} \). This elliptic curve has rank 0 over \( \mathbb{Q}(a) \). For more details see [6, p. 112]. Points on the variety \( s^2 = i^3 + a^2 \) from Theorem 2.1 can easily be obtained, for example \( (a, i, s) = (6, -3, 3) \) is a point on the variety. For \( a = 0 \) we have \( i = u^2 \) and \( s = u^3 \), in this case \( T^{(1)}_{\pm}(0, u^2, u^3, n, k, l) \) in Theorem 2.1 is a quadratic polynomial in \( n \). We also have parametrizations of this variety [3, Section 14.2]:
\[ \begin{aligned}
& a(t) = 2t^3 - 1, \\
& i(t) = 2t, \\
& s(t) = 2t^3 + 1,
\end{aligned} \]
For this parametrization Theorem 2.1 and Proposition 2.2 transform into:
Corollary 2.4.

(i) Let 
\[ T(2)_{\pm}(t, n, k, l) := T(1)_{\pm}(2t^3 - 1, 2t, 2t^3 + 1, n, k, l) \]
are independent. The proof for \( S(2)_{\pm} \) is analogous, by picking an adequate specialization.

(ii) Let 
\[ S(2)_{\pm}(t, k, l, m) := S(1)_{\pm}(2t^3 - 1, 2t, 2t^3 + 1, k, l, m). \]

The elliptic curve \( Y^2 = X^3 - X + T(2)_{\pm}(t, n, k, l) \) over \( \mathbb{Q}(t, n, k, l) \) has rank \( \geq 3 \) and three independent points have first coordinates \( (0, T(2)_{\pm}(t, n, k, l)), \) \( (-1, S(2)_{\pm}(t, n, k, l)), \) \( C(1)(2t^3 - 1, 2t, 2t^3 + 1, n, k, l). \) Notation for \( T(1)_{\pm} \) and \( C(1) \) as in Theorem 2.1.

Proof.

(i) For the specialization \( (t, n, k, l) \mapsto (1, 2, 1, 1) \) on the curve
\[ E_{T(2)_{\pm}(1, 2, 1, 1)} : Y^2 = X^3 - X + 53^2 \]
the corresponding points with first coordinates 0, -1, 16 are independent, so the claim of the corollary is true. The proof for \( T(2)_{\pm} \) is analogous, by picking an adequate specialization.

(ii) The specialization \( (t, k, l, m) \mapsto (2, 1, 1, 1) \) gives the elliptic curve
\[ E_{S(2)_{\pm}(2, 1, 1, 1)} : Y^2 = X^3 - X + \left( -\frac{49050562229}{10497600} \right)^2 \]
over \( \mathbb{Q} \) for which the four listed points with first coordinates 0, -1, \( \frac{14863849}{72900}, \) \( -\frac{48719569}{311040} \) are independent. This proves that for the elliptic curve \( Y^2 = X^3 - X + S(2)_{\pm}(t, k, l, m) \) over the field \( \mathbb{Q}(t, k, l, m) \) the corresponding four points the two generators mentioned in the introduction and the points \( A(1)_{\pm}(2t^3 - 1, 2t, 2t^3 + 1, k, l, m) \) and \( B(1)_{\pm}(2t^3 - 1, 2t, 2t^3 + 1, k, l, m) \) (from Proposition 2.2) are independent. The proof for \( S(2)_{\pm} \) is analogous, by picking an adequate specialization. \( \square \)
3. Subfamily of generic rank $\geq 5$

Remark 3.1.

- In [5, Theorem 3.5.1.] a rational function is given

$$M(m) = \frac{1017m^4 - 8487m^3 + 19298m^2 - 14145m + 2825}{(3m^2 - 5)^2},$$

with the property that the rank of $E_{M(m)}$ over $\mathbb{Q}(m)$ is $\geq 4$.

- We have two additional points coming from [5, Theorem 3.5.1.], $R_3$ with first coordinate

$$\frac{69m^2 - 414m + 295}{3m^2 - 5}$$

and the point $R_4$ with first coordinate

$$\frac{357m^2 - 410m + 95}{3m^2 - 5}.$$

- This rational function $M(m)$ is equal $T_+^{(1)}(0, 9, 27, n, -\frac{1}{3} \frac{9nm^2 - 20m^2 + 69m - 15n - 35}{3m^2 - 5}, 1)$ in Theorem 2.1. The third point $R_3$ in [5] is equal $(0, T_+^{(1)}) + (-1, T_+^{(1)}) - C_+^{(1)}$, where $C_+^{(1)}$ is the third independent point in Theorem 2.1.

- The rational function $M(m)$ is also equal

$$T_+^{(1)}(0, 25, 125, n, -\frac{1}{25} \frac{75nm^2 - 102m^2 + 205m - 125n - 175}{3m^2 - 5}, 1).$$

The fourth point $R_4$ in [5] is equal $(-1, T_+^{(1)}) - C_+^{(1)}$, where $C_+^{(1)}$ is the third independent point in Theorem 2.1.

- In [5] an elliptic surface over a curve is found for which the Mordell-Weil group has rank $\geq 5$. Here we give another example of an infinite family of elliptic curves of generic rank $\geq 5$.

Theorem 3.2. The elliptic curve

$$Y^2 = X^3 - X + \left( \frac{3723875}{729} n^2 + \frac{155}{9} n - \frac{3723875}{729} \right)^2$$

over the function field $\mathbb{Q}(m, n)$ where $((3m^2 - 5) \left( \frac{48050}{81} n + 1 \right))^2 = \frac{2257735321}{729} m^4 + \frac{584660m^3}{2187} - \frac{2599552790}{3} m^2 + \frac{2923300}{3} m + \frac{5644383025}{6561}$, has rank $\geq 5$ with five independent points with first coordinates

$$0, -1, \frac{69m^2 - 414m + 295}{3m^2 - 5}, \frac{357m^2 - 410m + 95}{3m^2 - 5}, \frac{24025}{81} n^2 - \frac{24025}{81}. $$
The rank of certain subfamilies of the elliptic curve $y^2 = x^3 - x + t^2$

Proof. Here we will intersect $M(m)$ with $T^{(1)}_+(0, u^2, u^3, n, k, l)$ from Theorem 2.1 to obtain a subfamily of higher rank:

$$M(m) = T^{(1)}_+(0, u^2, u^3, n, k, l) = u^3l(n+k+\frac{1}{2u^2l})^2 - \frac{1}{4}(2u^2l^2 - 2ul + 1)(2u^2l^2 + 2ul + 1)ul.$$  

This gives $(2u^2l(3m^2 - 5)(n+k+\frac{1}{2u^2l}))^2 = (9 + 36(ul)^4 + 4068(ul)m^4 - 33948(ul)m^3 + (-30 + 77192ul - 120(ul)^4)m^2 - 56580(ul)m + 25 + 100(ul)^4 + 11300(ul))$.

So, the point $m = 1$ will be the solution of the above equation if $c = ul$ is the first coordinate on

$$\square = 16c^4 + 2032c + 4.$$  

The corresponding elliptic curve is of rank five and from one of the generators of the free part we get $c = ul = -\frac{155}{9}$ (chosen such that the specialization $m = 1$ gives the independence of points). So we take $k = 0, l = 1$ and we look at the intersection

$$M(m) = T^{(1)}_+(0, \left(-\frac{155}{9}\right)^2, \left(-\frac{155}{9}\right)^3, n, 0, 1) = \left(-\frac{3723875}{729}n^2 - \frac{155}{9}n + \frac{3723875}{729}\right),$$  

and we get that $(m, n)$ lies on

$$\left(3m^2 - 5\right)\left(\frac{48050}{81}n + 1\right)^2 = \frac{2257735321}{729}m^4 + 584660m^3$$  

$$- \frac{25995527290}{2187}m^2 + \frac{2923300}{3}m + \frac{56443383025}{6561}. \quad (3.1)$$  

So $(m, n)$ on (3.1) gives five points from the claim of the theorem (where the third and fourth point are from [5] and the last point is from Theorem 2.1).

For the specialization $(m, n) \mapsto (1, -\frac{4753}{4805})$ we get the elliptic curve

$$E_{M_2(1)} = E_{T^{(1)}_+(0, \left(-\frac{155}{9}\right)^2, \left(-\frac{155}{9}\right)^3, -\frac{4753}{4805}, 0, 1)} = E_{127} : Y^2 = X^3 - X + 127^2,$$

with corresponding five independent points with first coordinates $0, -1, -25, -21, -\frac{6136}{961}$. So the five points from the claim of the theorem are independent. \hfill \Box

Remark 3.3. Points $(m, n)$ in the above theorem can be obtained with the transformation

$$m = \frac{11602011740X - 139896435555764171800 + 47449Y}{47449Y + 7099196538X - 80704505760225548460},$$  

where $(X, Y)$ is a point on the curve

$$Y^2 = X^3 - 411900623573078732700X + 3213758699878398237969890146000.$$  

The value of $n$ can be obtained from (3.1). This curve is of positive rank by [7], so the subfamily of elliptic curves from Theorem 3.2 is infinite.
4. Specializations of high rank

The highest rank found for the elliptic curve $E_t : Y^2 = X^3 - X + t^2$ over $\mathbb{Q}$ is $\geq 11$ and is obtained for $t = 1118245045$. In this case we get the elliptic curve $E_{1118245045} : Y^2 = X^3 - X + 1118245045^2$ and eleven independent points

$$(1, 1118245045), (-1, 1118245045), (-149499, 1116750055), (-187723, 1115283209)$$

$$(208403, 1122284857), (-357751, 1097581405), (-369623, 1095433091),$$

$$(-398399, 1089604235), (402083, 1146942473), (506597, 1174940551),$$

$$(919987, 1424474279).$$

This was found using the sieve method explained in [4, 8, 10]. Here we observed $t = \frac{1}{t}$ (1 $\leq t_2 \leq 10000$, 1 $\leq t_1 \leq 100000$), and elliptic curves $E_t$ with $S(523, E_t) > 23$ for which $S(1979, E_t) > 43.5$. The lower bound was found using the command $\text{Seek1}$ in Apecs [1]. In addition we observed integers $1 \leq t \leq 1130000000$, and elliptic curves $E_t$ with $S(523, E_t) > 23$ for which $S(1979, E_t) > 41.5$ for the remaining ones. Here is the list of values $t$ which we obtained with rank $\geq 8$:

<table>
<thead>
<tr>
<th>rank</th>
<th>$t$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\geq 8$</td>
<td>1507, 7247, 23618, 14089, 32971, 22009, 21581, 18353, 6882, 88745, 74227, 47059, 6011, 19489, 35704, 11569, 29686, 78560, 2011060, 14083286, 14083286, 21171559, 35498230, 38998023, 45321449, 58235977, 67199043, 67292109, 83402041, 86010677, 96384349, 101940616, 122421035, 159056061, 171981307, 200300248, 217135540, 230684707, 266349308, 307253369, 329132909, 331903387, 342825543, 349640440, 391942721, 42378655, 436687265, 484259053, 484594343, 566328793, 586597025, 594744835, 594782908, 594869501, 598442638, 620093242, 631151494, 747946597, 781809427, 787815289, 836422595, 851738165, 919540903, 1015597721, 1029670387, 1111072411</td>
</tr>
<tr>
<td>$\geq 9$</td>
<td>20155, 20719, 36749, 51691, 83351, 70312, 423515, 829999, 1741033, 2650019, 7039799, 11106651, 1741033, 2650019, 7039799, 11106651, 53958107, 7080869, 76778473, 97399947, 101479426, 154523221, 197903551, 281137843, 300361741, 304534681, 352968853, 355308367, 599768545, 863224739, 911227325, 1040969455</td>
</tr>
<tr>
<td>$\geq 10$</td>
<td>765617, 17708315, 64232534, 77799653, 236075608, 269371865, 337557943, 450112831, 808983247</td>
</tr>
<tr>
<td>$\geq 11$</td>
<td>1118245045</td>
</tr>
</tbody>
</table>

The greatest rank obtained in [5] was rank 6 for $t = 337$, while the greatest rank obtained in [2] was rank 10 for $t = 765617$.

References


The rank of certain subfamilies of the elliptic curve $y^2 = x^3 - X + T^2$