ON THE FAMILY OF ELLIPTIC CURVES $Y^2 = X^3 - T^2X + 1$

Petra Tadić
University of Zagreb, Croatia

Abstract. Let $E$ be the elliptic curve over $\mathbb{Q}(T)$ given by the equation
\[ E : Y^2 = X^3 - T^2X + 1. \]
We prove that the torsion subgroup of the group $E(\mathbb{C}(T))$ is trivial, rank $\mathbb{Q}(T)(E) = 3$ and rank $\mathbb{C}(T)(E) = 4$. We find a parametrization of $E$ of rank at least four over the function field $\mathbb{Q}(a, i, s, n, k)$ where $s^2 = i^3 - a^2 i$.
From this we get a family of rank $\geq 5$ over the field of rational functions in two variables and a family of rank $\geq 6$ over an elliptic curve of positive rank. We also found particular elliptic curves with rank $\geq 11$.

1. Introduction

Let $E$ be the elliptic curve over $\mathbb{Q}(T)$ given by the equation
\[ Y^2 = X^3 - T^2X + 1. \]
In [1, Theorem 3.11] it is proven that if $t \geq 2$ is an integer, the elliptic curve $E_t : Y^2 = X^3 - t^2X + 1$ has rank at least 2 over $\mathbb{Q}$, with independent points $(0, 1)$ and $(-1, t)$. It is proven that the rank of $E_t$ is at least 3, for integers $t \equiv 0 \pmod{4}$ and $t = 7$. Here the third independent point is $(-1, 1)$.
Additionally, the torsion subgroup of $E_t(\mathbb{Q})$ is trivial, for all integer values $t \geq 1$.

In this paper we prove that the rank of the elliptic curve $E$ over $\mathbb{Q}(T)$ is equal 3. We find the generators $(0, 1), (-1, T), (-T, 1)$ of the finitely generated Abelian group $E(\mathbb{Q}(T))$ and prove that its torsion subgroup is trivial. Since the rank of $E(\mathbb{Q}(T))$ is equal three, by the Silverman’s specialization theorem [12, p. 271, Theorem 11.4] we obtain that rank $E_t(\mathbb{Q}) \geq 3$, for all but finitely many rational values $t$. We also compute the rank of $E$ over $\mathbb{C}(T)$ and find the

2010 Mathematics Subject Classification. 11G05, 14H52.
Key words and phrases. Elliptic surface, elliptic curve, parametrization, function field, rank, family of elliptic curves, torsion.
generators. In addition we find parametrisations of $E$ for which the generic rank is $\geq 4$, $\geq 5$ and $\geq 6$. We also search for particular high rank curves in the family $E_t$. We find several curves with rank $\geq 9$ for integer values of the parameter $t$, and several curves with rank $\geq 11$ for rational values of the parameter $t$.

2. The rational elliptic surface $Y^2 = X^3 - T^2X + 1$

In this section we give results regarding the elliptic curve $Y^2 = X^3 - T^2X + 1$ over $\mathbb{Q}(T)$. We will find the torsion subgroup, calculate the rank over $\mathbb{Q}(T)$ and $\mathbb{C}(T)$, find the generators and find parametrizations of generic rank $\geq 4$ and $\geq 5$.

**Proposition 2.1.** Let $E$ be the elliptic curve over $\mathbb{Q}(T)$ given by the equation $E : Y^2 = X^3 - T^2X + 1$.

(i) The associated elliptic surface (denoted $\mathcal{E}$) is rational.

(ii) $\text{rank}_{\mathbb{C}(T)} E = 4$.

(iii) The generators of the group $E(\mathbb{C}(T))$ are the points

$$(0, 1), (-1, T), (-T, 1), \left(\frac{1 + \sqrt{-3}}{2}, \frac{1 - \sqrt{-3}}{2}T\right),$$

and the torsion subgroup of $E(\mathbb{C}(T))$ is trivial.

(iv) $\text{rank}_{\mathbb{Q}(T)} E = 3$, the generators over $\mathbb{Q}(T)$ are

$$(0, 1), (-1, T), (-T, 1),$$

and the torsion subgroup of $E(\mathbb{Q}(T))$ is trivial.

(v) For

$$T(a, i, s, n, k) = an^2 + \left(2ak + \frac{s}{i}\right)n + ak^2 + \frac{s}{i}k + \frac{a^3 - 2ai^2}{i^3 - a^2i},$$

the elliptic curve $Y^2 = X^3 - T(a, i, s, n, k)^2X + 1$ over the function field $\mathbb{Q}(a, i, s, n, k)$ where $s^2 = i^3 - a^2i$, has rank $\geq 4$, with an extra independent point with the first coordinate

$$X_C(a, i, s, n, k) = i(n + k)^2 + \frac{i^2}{a^2 - i^2}.$$

**Proof of Proposition 2.1.** The elliptic curve $E$ over $\mathbb{Q}(T)$ is written in short Weierstrass form

$$E : Y^2 = X^3 + A(T)X + B(T),$$
where we have
\[ A(T) = -T^2, \]
\[ B(T) = 1, \]
\[ \Delta(T) = 16(4T^6 - 27), \]
here \( \Delta \) is the discriminant.

(i) Since \( \deg(A) = 2 \) and \( \deg(B) = 0 \), from [11, Equation 10.14] we find that the associated elliptic surface \( E \) is rational.

(ii) For the proof we will use Shioda’s formula. Since from (i) we know that the associated elliptic surface \( E \) is rational, by [11, Lemma 10.1] we find that the rank of the Néron-Severi group (denoted \( NS(E, \mathbb{C}) \)) of \( E \) over \( \mathbb{C} \) is equal 10. From the discriminant \( \Delta(T) \), we see that the singular fibres are at \( \varphi_1, \ldots, \varphi_6 \) and \( \infty \), where the \( \varphi_i \) are the roots of the equation \( 4T^6 - 27 = 0 \).

We determine the numbers \( m_s \) (of irreducible components of the fibre over \( s \)) from Kodaira types of singular fibres [7, Section 4]:

<table>
<thead>
<tr>
<th>( s )</th>
<th>( \text{coefficients} )</th>
<th>( \text{Kodaira type} )</th>
<th>( m_s - 1 )</th>
</tr>
</thead>
<tbody>
<tr>
<td>( \varphi_i )</td>
<td>( 0 )</td>
<td>( 1 )</td>
<td>( I_1 )</td>
</tr>
<tr>
<td>( \infty )</td>
<td>( 2 )</td>
<td>( 6 )</td>
<td>( I_0 )</td>
</tr>
</tbody>
</table>

Now we compute \( \text{rank}_{\mathbb{C}(T)}(E) \) using Shioda’s formula [11, Corollary 5.3]
\[
\text{rank}_{\mathbb{C}(T)}(E) = \text{rank}NS(E, \mathbb{C}) - 2 - \sum_s (m_s - 1) = 10 - 2 - 6 \cdot 0 - 4 = 4.
\]

(iii) The group \( E(\mathbb{C}(T)) \) is generated, by [11, Theorem 10.10], with the points of the form \( (a_2T^2 + a_1T + a_0, b_3T^3 + b_2T^2 + b_1T + b_0) \), \( a_i, \ b_i \in \mathbb{C} \). We list all such points
\[
(0, \pm 1) =: \pm P,
(\pm 1, \pm 2T) =: \pm Q,
(\pm T, \pm 1) =: \pm R,
(T, \pm 1) =: \mp P \mp R,
(T + 2, \pm 2T \pm 3) =: \mp Q \mp R,
(T^3 - 1, \pm T^3 \mp 2T) =: \pm P \pm Q \mp 2R,
(T^2 + 2T + 2, \pm T^3 \mp 3T^2 \mp 4T \mp 3) =: \mp P \mp Q,
(T^2 - 2T + 2, \pm T^3 \mp 3T^2 \mp 4T \mp 3) =: \pm P \mp Q,
\left( \frac{1 + \sqrt{-3}}{2}, \pm \frac{1 - \sqrt{-3}}{2} \right) =: \pm S,
\]
\[
\left( \frac{1 - \sqrt{-3}}{2}, \pm \frac{1 + \sqrt{-3}}{2} \right) = \pm P \pm Q \pm 2R \neq S, \\
(T - 1 - \sqrt{-3}, \pm (1 - \sqrt{-3})T + 3) = \pm R \neq S, \\
(T - 1 + \sqrt{-3}, \pm (1 + \sqrt{-3})T + 3) = \mp P \mp Q \mp R \neq S, \\
(-T - 1 - \sqrt{-3}, \pm (1 - \sqrt{-3})T + 3) = \pm P \pm R \neq S, \\
(-T - 1 + \sqrt{-3}, \pm (1 + \sqrt{-3})T + 3) = \mp Q \mp R \neq S, \\
\left( -\frac{1}{3} T^2 - 1, \pm \frac{\sqrt{-3}}{9} T^3 \right) = \pm P \pm Q \pm 2R \neq 2S, \\
\left( \frac{1}{6} (1 + \sqrt{-3})T^2 + \frac{1}{2} (1 - \sqrt{-3}), \pm \frac{\sqrt{-3}}{9} T^3 \right) = \pm Q \pm S, \\
\left( \frac{1}{6} (1 - \sqrt{-3})T^2 + \frac{1}{2} (1 + \sqrt{-3}), \pm \frac{\sqrt{-3}}{9} T^3 \right) = \pm P \pm 2Q \neq 2S, \\
\left( -\frac{1}{2} (1 - \sqrt{-3})T^2 + \frac{1}{2} (1 + \sqrt{-3}), \pm T^3 \pm (1 - \sqrt{-3})T \right) = \pm P \pm 2R \neq S, \\
\left( -\frac{1}{2} (1 + \sqrt{-3})T^2 + \frac{1}{2} (1 - \sqrt{-3}), \pm T^3 \pm (1 + \sqrt{-3})T \right) = \mp Q \neq S, \\
\left( -\frac{1}{2} (1 - \sqrt{-3})T^2 + 2T \cdot (1 + \sqrt{-3}), \pm T^3 \mp \frac{3}{2} (1 + \sqrt{-3})T^2 \neq 2(1 - \sqrt{-3})T + 3 \right) = \mp P \mp S, \\
\left( -\frac{1}{2} (1 - \sqrt{-3})T^2 - 2T \cdot (1 + \sqrt{-3}), \pm T^3 \mp \frac{3}{2} (1 + \sqrt{-3})T^2 \neq 2(1 - \sqrt{-3})T + 3 \right) = \pm P \mp S, \\
\left( -\frac{1}{2} (1 + \sqrt{-3})T^2 + 2T \cdot (1 - \sqrt{-3}), \pm T^3 \mp \frac{3}{2} (1 - \sqrt{-3})T^2 \neq 2(1 + \sqrt{-3})T + 3 \right) = \mp 2P \pm Q \mp 2R \neq S, \\
\left( -\frac{1}{2} (1 + \sqrt{-3})T^2 - 2T \cdot (1 - \sqrt{-3}), \pm T^3 \mp \frac{3}{2} (1 - \sqrt{-3})T^2 \neq 2(1 + \sqrt{-3})T + 3 \right) = \mp Q \mp 2R \neq S.
\]

We see that all of the listed points which generate \( E(\mathbb{C}(T)) \) can be written as a combination of the four points \( P, Q, R, S \), so the points \( P, Q, R, S \) generate the group \( E(\mathbb{C}(T)) \). From (ii) we conclude that \( P, Q, R, S \) are independent points of infinite order that generate the group \( E(\mathbb{C}(T)) \), and the torsion subgroup \( E(\mathbb{C}(T))_{\text{Tors}} \) is trivial.

(iv) Since the torsion subgroup of \( E(\mathbb{C}(T)) \) is trivial, we conclude that the torsion subgroup of \( E(\mathbb{Q}(T)) \) is trivial.

We have to prove that the generators of the group \( E(\mathbb{Q}(T)) \) are the three independent points \( P, Q, R \in E(\mathbb{Q}(T)) \) in (iii). So we have to prove that these
three points generate the subgroup $E(Q(T))$ of the group $E(C(T))$, where the later is generated by the four points $P, Q, R, S$ in (iii). It is obvious that the point $S \in E(C(T)) \backslash E(Q(T))$ will not give a point of the group $E(Q(T))$, by the action of the Galois group Gal($Q(\sqrt{-3})/Q$) and using that the torsion subgroup of $E(C(T))$ is trivial. Precisely, since $aP + bQ + cR + dS \in E(Q(T)) (a, b, c, d \in \mathbb{Z})$, would mean $0 = (aP + bQ + cR + dS)^\sigma - (aP + bQ + cR + dS) = dS^\sigma - dS = d(S^\sigma - S)$ for all $\sigma \in$ Gal($Q(\sqrt{-3})/Q(T)$). Since the torsion subgroup is trivial and $S = \left(\frac{1+i\sqrt{-3}}{2}, \frac{1-i\sqrt{-3}}{2}T\right)$, this would give $d = 0$.

Thus, it would mean that if $d \in \mathbb{Z}\setminus\{0\}$, then $aP + bQ + cR + dS \notin E(Q(T))$. So we conclude that the points $P, Q, R$ generate the subgroup $E(Q(T))$ of the group $E(Q(T))$.

(v) We look for parameters $T$ of the form $an^2 + bn + c \ (a, b, c \in \mathbb{Q})$ for which the curve

$$Y^2 = X^3 - T^2X + 1$$

has a point of the form $(i_2n^2 + i_1n + i_0, j_3n^3 + j_2n^2 + j_1n + j_0)$, for $i_0, i_1, i_2, j_0, j_1, j_2, j_3 \in \mathbb{Q}$. In other words we search for $a, b, c, i_0, i_1, i_2$ for which the polynomial

$$(i_2n^2 + i_1n + i_0)^3 - (an^2 + bn + c)^2(i_2n^2 + i_1n + i_0) + 1$$

is a square in the field $\mathbb{Q}(n)$. Such an observation leads to the listed subfamily. We have

$$Y_C(a, i, s, n, k) = sn^3 + (3sk - a)n^2 + \frac{3ik^2s^2 - a^2i - 2aisk - 2s^2}{i^8}n + \frac{ai^2 + a^2sk - 2isk^2 - 2s^2k^2 + s^3k^3}{i^8(i^2 - a^2)}.$$ 

And we have

$$X_C(a, i, s, n, k)^3 - T(a, i, s, n, k)^2X_C(a, i, s, n, k) + 1 - Y_C(a, i, s, n, k)^2 = (-s^2 - a^2i + i^3)q(a, i, s, n, k) = 0,$$

where $q \in \mathbb{Q}(a, i, s, n, k)$. This proves that the listed point is on the elliptic curve $Y^2 = X^3 - T(a, i, s, n, k)^2 + 1$ over $\mathbb{Q}(a, i, s, n, k)$ where $s^2 = i^2 - a^2i$.

For the specialization $(a, i, s, n, k) \mapsto (6, -3, 9, 1, 1)$ we have that on the curve $E_{T(6, -3, 9, 1, 1)} : Y^2 = X^3 - (\frac{27}{2})^2X + 1$ over $\mathbb{Q}$ the four corresponding points $(0, 1), (-1, \frac{5}{2}), (-\frac{5}{2}, 1), (\frac{15}{2}, \frac{15}{2})$ are independent, this shows that the points from the claim of the proposition are independent since the specialization map is a homomorphism.

**Remark 2.2.** Most of the technical claims in (i)-(iv) from the above proposition can be extracted from [5], but for the sake of completeness we have given proofs here.
From Proposition 2.1 (iv) and the Silverman’s specialization theorem [12, p. 271, Theorem 11.4] the rank of \( E_t(\mathbb{Q}) \) ≥ 3, for all but finitely many rational values \( t \).

From the subfamily in Proposition 2.1 (v) we get subfamilies of rank ≥ 5. We write the family in Proposition 2.1 (v) as

\[
T(a, i, s, n, k) = a \left( n + k + \frac{s}{2ai} \right)^2 + \frac{8a^2i^3 - 4a^4i - a^2s^2 + i^2s^2}{4ai^2(a^2 - i^2)}.
\]

Now we look at the solution of

\[
T(a, i, s, n, k) = T(a, i_2, s_2, n_2, k_2),
\]

where

\[
i_2 = \frac{a(i + a)}{i - a}, \quad s_2 = \frac{a^2s}{(i - a)^2}.
\]

Actually, \((i_2, s_2) = (i, -s) + (a, 0)\) on the curve \( Y^2 = X^3 - a^2X \) over \( \mathbb{Q}(a) \).

So we look for solutions of

\[
a \left( n + k + \frac{s}{2ai} \right)^2 + \frac{8a^2i^3 - 4a^4i - a^2s^2 + i^2s^2}{4ai^2(a^2 - i^2)} = a \left( n_2 + k_2 + \frac{s_2}{2ai_2} \right)^2 + \frac{8a^2i_2^3 - 4a^4i_2 - a^2s_2^2 + i_2^2s_2^2}{4ai_2^2(a^2 - i_2^2)},
\]

more precisely

\[
\left( n + k + \frac{s}{2ai} \right)^2 - \left( n_2 + k_2 + \frac{s_2}{2ai_2} \right)^2 = \frac{1}{a} \left( \frac{8a^2i_2^3 - 4a^4i_2 - a^2s_2^2 + i_2^2s_2^2}{4ai_2^2(a^2 - i_2^2)} - \frac{8a^2i^3 - 4a^4i - a^2s^2 + i^2s^2}{4ai^2(a^2 - i^2)} \right).
\]

This leads to the solution of the equation \( A^2 - B^2 = p \), which is

\[
(A, B) = \left( \frac{1}{2} \frac{u^2p - 2up + 2u + u^2 + p + 1}{u^2 - 1}, - \frac{1}{2} \frac{u^2p - u^2 - 2up - 2u + p - 1}{(u^2 - 1)} \right),
\]

where on the other hand \( A = n + k + \frac{s}{2ai} \) and \( B = n_2 + k_2 + \frac{s_2}{2ai_2} \) (coming from the squares in \( T(a, i, s, n, k) \) and \( T(a, i_2, s_2, n_2, k_2) \) respectively), and \( p \) is as below.

**Proposition 2.3.** Let

\[
T(a, i, s, u) = a \left( \frac{1}{2} \frac{u^2p - 2up + 2u + u^2 + p + 1}{u^2 - 1} \right)^2 + \frac{8a^2i^3 - 4a^4i - a^2s^2 + i^2s^2}{4ai^2(a^2 - i^2)},
\]

where

\[
i_2(a, i) = \frac{a(i + a)}{i - a}, \quad s_2(a, i, s) = \frac{a^2s}{(i - a)^2}.
\]
The elliptic curve \( Y^2 = X^3 - T(a, i, s, u)^2X + 1 \) over the function field \( \mathbb{Q}(a, i, s, u) \) where \( s^2 = i^3 - a^2i \) has rank \( \geq 5 \) with five independent points: the three generators \( (0, 1), (-1, T), (-T, 1) \) provided in Proposition 2.1 (iv) and two additional points \( C(a, i, s, u) \) and \( D(a, i, s, u) \) (notion from Proposition 2.1 (v)) where the first coordinates are

\[
X_C(a, i, s, u) = \frac{i}{4} \left( \frac{u^2p - 2up + 2u + u^2 + p + 1}{u^2 - 1} - \frac{s}{ia} \right)^2 + \frac{i^2}{a^2 - i^2}, \\
X_D(a, i, s, u) = \frac{a(i + a)}{i - a} \left( \frac{1}{2} \frac{u^2p - u^2 - 2up - 2u + p - 1}{u^2 - 1} + \frac{s}{i^2 - a^2} \right)^2 - \frac{(i + a)^2}{4ai}.
\]

**Proof of Proposition 2.3.** For the second coordinate of \( C \) and \( D \) we can take the second coordinate from the proof of Proposition 2.1 (v), specifically \( Y(a, i, s, u, 0, A - \frac{ax}{2a}) \) and \( Y(a, i, s_2, 0, B - \frac{ax}{r - a}) \), respectively.

With the specialisation \( (a, i, s, u) \mapsto (6, -2, 8, 3) \) we prove that the above listed five points on the elliptic curve (over \( \mathbb{Q}(a, i, s, u) \) where \( s^2 = i^3 - a^2i \)) are independent, since the specialization gives the elliptic curve

\[
E_{T(6,-2,8,3)} : Y^2 = X^3 - \left( \frac{239}{32} \right)^2 X + 1
\]

with the corresponding five independent points \( (0, 1), (-1, \frac{239}{32}), (-\frac{239}{32}, 1), (-\frac{225}{256}, \frac{2053}{1728}), (-\frac{299}{64}, \frac{640}{512}) \).

**Remark 2.4.** The variety \( s^2 = i^3 - a^2i \) from Proposition 2.1 (v) can be considered as an elliptic curve over the field \( \mathbb{Q}(a) \). In fact, it is the well-known “congruent number” elliptic curve. The torsion subgroup of this elliptic curve is equal \( \{O, (0, 0), (a, 0), (-a, 0)\} \). Nontrivial points on this variety \( s^2 = i^3 - a^2i \) can easily be obtained, for example \( (a, i, s) = (6, -2, 8) \) is a point on the variety. We also have
parametrisations of this variety (see e.g. [3]), for example:

\[
\begin{align*}
    a(t) &= t(t^2 - 1), \\
    i(t) &= -t^2 + 1, \\
    s(t) &= (t^2 - 1)^2.
\end{align*}
\]

For this parametrisation we get that Proposition 2.1 (v) and Proposition 2.3 transform into:

**Corollary 2.5.** (i) Let

\[
T(t, n, k) = (t^3 - t)n^2 + (t^2 - 1)(2tk - 1)n + (t^3 - t)k^2 - (t^2 - 1)k + \frac{(t^3 - 2t)}{(t^2 - 1)},
\]

and

\[
X_C(t, n, k) = -(t^2 - 1)n^2 - 2(t^2 - 1)kn - (t^2 - 1)k^2 + \frac{1}{t^2 - 1}.
\]

The elliptic curve

\[
Y^2 = X^3 - T(t, n, k)^2 X + 1
\]

over \(\mathbb{Q}(t, n, k)\) has rank \(\geq 4\) with four independent points with first coordinates 0, −1, −\(T(t, n, k)\), \(X_C(t, n, k)\).

(ii) Let

\[
T(t, u) = (t^8 - 2t^7 + 4t^5 - 3t^4 - 2t^3 - 2t^2 + 8t)u^4 + (4t^8 - 8t^7 - 4t^6 + 16t^5 - 8t^4 + 8t^3 - 4t^2 - 16t - 4)u^3 + (6t^8 - 12t^7 - 8t^6 + 24t^5 + 6t^4 - 44t^3 + 28t^2 + 16t + 8)u^2 + (4t^8 - 8t^7 - 4t^6 + 16t^5 - 8t^4 + 8t^3 - 4t^2 - 16t - 4)u + t^8 - 2t^7 + 4t^5 - 3t^4 - 2t^3 - 2t^2 + 8t)/(4t(u^2 - 1)^2(t + 1)(t - 1)^3),
\]

and

\[
X_C(t, u) = -((t^4 - 5t^2 + 4t + 2)u^2 + (2t^4 - 2t^3 - 2t - 2)u + t^4 - 2t^3 + t^2 + 2t)((t^4 - t^2 + 2)u^2 + (2t^4 - 2t^3 - 2t - 2)u + t^4 - 2t^3 + 6t)/(4t^2(u^2 - 1)^2(t + 1)(t - 1)^3),
\]

\[
X_D(t, u) = -(2t^4 - 2t^3 + 3t^2 - 2t - 2)u^2 + (2t^4 - 2t^3 - 4t^2 + 6t + 2)u + t^4 - 2t^3 - t^2 + 2t - 1)/(4t(u^2 - 1)^2(t^2 - 1)^2).
\]

The elliptic curve

\[
Y^2 = X^3 - T(t, u)^2 X + 1
\]

over \(\mathbb{Q}(t, u)\) has rank \(\geq 5\) with five independent points with first coordinates 0, −1, −\(T(t, u)\), \(X_C(t, u)\), \(X_D(t, u)\).

**Proof of Corollary 2.5.** (i) For the specialization \((t, n, k) \mapsto (2, 1, 1)\) the elliptic curve \(E_{T(2,1,1)} : Y^2 = X^3 - \left(\frac{25}{4}\right)^2 X + 1\) is a curve over \(\mathbb{Q}\) for which the four listed points are \((0, 1), (-1, \frac{58}{3}), (-\frac{25}{3}, 1), (-\frac{25}{3}, \frac{158}{3})\) and are independent. This proves that for the elliptic curve \(Y^2 = X^3 - T(t, n, k)^2 X + 1\) over \(\mathbb{Q}(t, n, k)\) the four points from the claim of the corollary are independent.
(ii) The specialization \((t, u) \mapsto (2, 2)\) gives the elliptic curve \(E_{T(2,2)} : Y^2 = X^3 - \left(\frac{404}{72}\right)^2 X + 1\) over \(\mathbb{Q}\) for which the five listed points \((0, 1), (\frac{-404}{72}, \frac{2902}{81}), (\frac{-128}{72}, \frac{24949}{729})\) are independent. This proves that for the elliptic curve \(Y^2 = X^3 - T(t, u)^2 X + 1\) over \(\mathbb{Q}(t, u)\) the five points from the claim of the corollary are independent.

3. A SUBFAMILY OF HIGHER RANK

- In [5], rational functions
  \[
  M_1(m) = \frac{2}{75}m^2 + m + 8,
  \]
  \[
  M_2(m) = \frac{1830m^4 - 64641m^3 + 907768m^2 - 5882331m + 15154230}{30(m^2 - 91)^2}
  \]
  are given such that the rank of \(E_{M(m)}\) over \(\mathbb{Q}(m)\) is \(\geq 4\) and \(\geq 5\), respectively.

- The first rational function \(M_1(m)\) is equal \(T \left(6, 18, 72, m, \frac{16}{3}m^2 + \frac{8}{3}m + 12, \frac{4}{25}m^3 + \frac{12}{15}m^2 + \frac{32}{15}m + 31\right)\) from Proposition 2.1 (v) and the fourth listed point \((\frac{16}{3}m^2 + \frac{8}{3}m + 12, \frac{4}{25}m^3 + \frac{12}{15}m^2 + \frac{32}{15}m + 31)\) from [5, Proposition 5.2.1.] is equal \(-\left(0, 1\right) - \left(-T, 1\right) - \left(\frac{5}{3}m^2 + \frac{19}{3}m + 44, \frac{1}{375}(8m^3 + 580m^2 + 13800m + 107625)\right)\), where the last point is the fourth independent point from Proposition 2.1 (v).

- The second rational function \(M_2(m)\) is equal
  \[
  T \left(120, 180, 1800, \frac{1}{120} \frac{16m^2 - 743m + 6461}{m^2 - 91}, \frac{5}{12}\right)
  \]
  and it has two extra points \(R_4\) with first coordinate
  \[
  \frac{1}{2} \frac{1130m^4 - 4785m^3 + 70188m^2 - 469539m + 1222158}{(m^2 - 91)^2}
  \]
  and \(R_5\) with first coordinate
  \[
  - \frac{1}{150} \frac{(57m^2 - 743m + 2730)(42m^2 - 743m + 4095)}{(m^2 - 91)^2}
  \]
  The fifth point \(R_5\) in [5] is equal \(0, 1) + (T, 1) + (T, 1) - C\), where \(C\) is the fourth independent point from Proposition 2.1 (v).

- In [5] an elliptic surface over a curve is found for which the Mordell-Weil group has rank \(\geq 6\). Here we give a new example of an infinite family of curves with rank \(\geq 6\).

**COROLLARY 3.1.** The elliptic curve given by the equation
\[
Y^2 = X^3 - \left(210n^2 + 187n + \frac{275}{7}\right)^2 X + 1
\]
over the function field $\mathbb{Q}(m, n)$ where
\[
(m^2 - 91)(420n + 187))^2 = 53209m^4 - 1809948m^3 + 25059146m^2
- 164705268m + 440623729,
\]
has rank at least six with six independent points with first coordinates $0, -1$,
\[
- \left(210n^2 + 187n + \frac{275}{7}\right),
\]
\[
\frac{1}{2} \left(1130m^4 - 4785m^3 + 70188m^2 - 469539m + 1222158
- 164705268m + 440623729\right),
\]
\[
- \frac{1}{150} \left(57m^2 - 743m + 2730(42m^2 - 743m + 4095)\right)
- 294n^2 + 245n + 49.
\]

**Proof of Corollary 3.1.** Here we will intersect $M_2(m)$ with $T(210, 294, 3528, n, \frac{5}{12})$ from Proposition 2.1 (v), to get a subfamily of higher rank:
\[
M_2(m) = T(210, 294, 3528, n, \frac{5}{12}) = 210n^2 + 187n + \frac{275}{7}
\]
gives
\[
(m^2 - 91)(420n + 187))^2 = 53209m^4 - 1809948m^3 + 25059146m^2
- 164705268m + 440623729,
\]
so $(m, n)$ on (3.1) give six points listed in the claim of the corollary (where the fourth and fifth come from [5] and the last is from Proposition 2.1 (v)).

The curve
\[
V^2 = 53209U^4 - 1809948U^3 + 25059146U^2 - 164705268U + 440623729
\]
has a rational point $(\frac{71}{12}, \frac{464490}{81})$, so it transforms into the elliptic curve
\[
Y^2 = X^3 - X^2 - 312055478905X - 66993477540839303.
\]
of rank 1 generated by the point $(\frac{21246300582064}{12649337}, \frac{25760668421579637}{12649334})$, which corresponds to $(m, n) = (\frac{819}{71}, \frac{3911}{4893})$.

The specialization $(m, n) \mapsto (\frac{819}{71}, \frac{3911}{4893})$ gives the elliptic curve
\[
E_T(210, 294, 3528, -\frac{3911}{4893}, \frac{5}{12}) = E_M(\frac{819}{71}) : Y^2 = X^3 - \left(\frac{1301974}{54289}\right)X + 1
\]
with corresponding six independent points with first coordinates $0, -1$, $-397026, 2226040, -497026, 2226040$. It proves that the six points from the claim of the corollary are independent.
Remark 3.2. Points \((m, n)\) in the above corollary can be obtained by the transformation

\[
m = \frac{1730382402X + 2460079Y + 533615416078542}{50252248X + 311841Y + 1306602990688},
\]

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

\[Y^2 = X^3 - 3X^2 - 312055478905X - 66993477540839303.\]

This elliptic curve has rank 1 with generator \((21246300582064, 12649337, 25760668421579637, 1264933)\) and torsion subgroup of order four generated by \((644929, 0)\) and \((-312181, 0)\).

The value \(n\) can be obtained from (3.1).

4. Specializations with high rank

The highest rank found of the elliptic curve \(E_t : Y^2 = X^3 - t^2X + 1\) over \(\mathbb{Q}\) is \(\geq 11\) and is obtained for \(t = \frac{23687}{3465}, \frac{86444}{833}, \frac{72269}{123}\). For example, for \(t = \frac{72269}{123}\) we get the elliptic curve

\[Y^2 = X^3 - \left(\frac{72269}{123}\right)^2 X + 1\]

and eleven independent points

\[
\begin{align*}
&(-1, \frac{72269}{123}), \left(-\frac{601}{123}, \frac{159743}{123}\right), \left(-\frac{793}{123}, \frac{543577}{123}\right), \left(-\frac{793}{123}, \frac{61163}{41}\right), \left(-\frac{7025}{123}, \frac{543577}{123}\right), \\
&\left(\frac{72269}{123}, 1\right), \left(\frac{72515}{123}, 144907\right), \left(\frac{1889}{123}, \frac{698807}{41}\right), \left(\frac{254568}{123}, 354287\right), \\
&\left(\frac{226895}{369}, \frac{4977013}{1107}\right), \left(-\frac{1133}{5043}, \frac{57582829}{206763}\right), \left(-\frac{328949}{5043}, \frac{975094283}{206763}\right).
\end{align*}
\]

The rank is actually equal 11 with the assumption of the Birch-Swinnerton-Dyer conjecture and the Generalized Riemann hypothesis. This was proved using the commands \texttt{Roha} which gives that the rank is odd and \texttt{Mest} which gives rank \(< 12.85\) (both in Apecs [2]), where the later uses the Birch-Swinnerton-Dyer conjecture and the Generalized Riemann hypothesis. The same holds for \(t = \frac{86444}{833}, \frac{23687}{3465}\).

This curve is found using the sieve method ([4, 6, 8]) which states that one may expect that high rank curves have large Mestre-Nagao sum, which is given by the formula

\[
S(N, E) = \sum_{p \leq n, p \text{ prime}} \frac{2 - a_p}{p + 1 - a_p} \log(p),
\]

where \(a_p = a_p(E) = p + 1 - \#E(\mathbb{F}_p)\). This expectation has been experimentally verified, and it is related to the Birch and Swinnerton-Dyer conjecture. Provided \(N\) is not too large, \(S(N, E)\) can be calculated using Pari ([9]). Here we observed \(t = \frac{72269}{123}\) (1 \(\leq t_2 \leq 10000, 1 \leq t_1 \leq 90000\), and elliptic curves \(E_t\)
with \( S(523, E_t) > 23 \) for which \( S(1979, E_t) \geq 47 \). The lower bound for the rank was calculated using the command \texttt{Seek1} in Apecs \cite{2}. We also observed integers \( 1 \leq t \leq 21819 \), and elliptic curves \( E_t \) with \( S(523, E_t) > 23 \) for which \( S(1979, E_t) \geq 34 \). Here is a list of values \( t \) we obtained for which the rank is \( \geq 8 \):

\[
\begin{array}{c|c}
\text{rank} & t \\
\hline
\geq 8 & 3665, 6355, 21507, 833, 3778, 4972, 5476, 5846, 5901, 6569, 7324, 7609, 8255, 8617, 8627, 8951, 9598, 10804, 12755, 13143, 14137, 14358, 14401, 15052, 17671, 19406, 19489, 19744, 21168 \\
\hline
\geq 9 & 1663, 1187, 1609, 3317, 2647, 4639, 3104, 9127, 28793, 12589, 32333, 34859, 59073, 30725, 39049, 18907, 48808, 11416, 16228, 20529 \\
\hline
\geq 10 & 317, 5441, 24733, 4951, 1381, 49049, 55717, 151241, 56633, 14173, 10343 \\
\hline
\geq 11 & 20798, 3465, 8644, 72269 \\
\end{array}
\]

For the integer values \( t \) in the above table the exact value of the rank was calculated using \texttt{mwrank} and it is equal to the lower bound in the table.

In \cite{5} the highest rank is obtained for \( t = 347, 443 \) and is equal 7.

Acknowledgements.

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

References

\begin{enumerate}
\item E. V. Eikenberg, Rational points on some families of elliptic curves, University of Maryland, 2004, PhD thesis.
\end{enumerate}


P. Tadić
Martićevu 23, 10000 Zagreb
Croatia
\textit{E-mail}: petra.tadic.zg@gmail.com

\textit{Received}: 31.3.2011.
\textit{Revised}: 10.5.2011.