TORSION GROUPS OF ELLIPTIC CURVES OVER QUADRATIC FIELDS $\mathbb{Q}(\sqrt{d})$, $0 < d < 100$

ANTONELA TRBOVIĆ

Abstract. We prove results towards classifying the possible torsion subgroups of elliptic curves over quadratic fields $\mathbb{Q}(\sqrt{d})$, where $0 < d < 100$ is a square-free integer, and obtain a complete classification for 49 out of 60 such fields. Over the remaining 11 quadratic fields, we cannot rule out the possibility of the group $\mathbb{Z}/16\mathbb{Z}$ appearing as a torsion group of an elliptic curve.

1. Introduction

For an elliptic curve $E$ defined over a number field $K$, let $E(K)$ be the set of all $K$–rational points on $E$. By the Mordell-Weil theorem and the structure theorem for finitely generated abelian groups, we know that $E(K)$ is isomorphic to $E(K)_{\text{tors}} \oplus \mathbb{Z}^r$, where $r$ is a non-negative integer and $E(K)_{\text{tors}}$ is the torsion subgroup.

In the case of $K = \mathbb{Q}$, Mazur’s theorem [9] gives us all possible torsion subgroups of $E(\mathbb{Q})$:

$$\mathbb{Z}/n\mathbb{Z}, \ n = 1, ..., 10, 12,$$

$$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z}, \ n = 1, 2, 3, 4.$$  

We also have a similar result by Kamienny, Kenku and Momose [5, 7] concerning possible torsion subgroups of elliptic curves defined over any quadratic field, which are the following 26 groups:

$$\mathbb{Z}/n\mathbb{Z}, \ n = 1, ..., 16, 18,$$

$$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z}, \ n = 1, ..., 6,$$

$$\mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3n\mathbb{Z}, \ n = 1, 2,$$

$$\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}.$$  

While this theorem settles the question on what are the possibilities for the torsion subgroup over all quadratic fields, we are interested in what happens when we fix a quadratic field. In order to see what happens over a fixed field, one would have to go through each of the 26 groups mentioned above and check whether that is a possible torsion subgroup or not.

We are going to see why every group mentioned in Mazur’s theorem has to appear as a possible torsion subgroup over all quadratic fields, and what happens with the groups $\mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3n\mathbb{Z}, n = 1, 2, \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$. For the rest of the groups we will follow the methods described in [6].

2000 Mathematics Subject Classification. Primary 11G05.

Key words and phrases. torsion groups, elliptic curves, quadratic fields.

The author was supported by the QuantiXLie Centre of Excellence, a project co-financed by the Croatian Government and European Union through the European Regional Development Fund - the Competitiveness and Cohesion Operational Programme (Grant KK.01.1.1.01.0004).
From now on, let $K$ be a fixed quadratic field. Let $Y_1(m, n)$ be the affine modular curve whose every $K$–rational point corresponds to an isomorphism class of an elliptic curve together with an $m$–torsion point $P_m \in E(K)$ and an $n$–torsion point $P_n \in E(K)$ such that $P_m$ and $P_n$ generate a subgroup isomorphic to $\mathbb{Z}/m\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z}$, and let $X_1(m, n)$ be its compactification (the same curve with adjoined cusps). We denote $X_1(1, n)$ by $X_1(n)$.

More precisely, what we need to do in order to determine whether an elliptic curve with torsion $\mathbb{Z}/n\mathbb{Z} \oplus \mathbb{Z}/m\mathbb{Z}$ over $K$ exists, for the rest of the 26 groups, is to determine whether there are $K$–rational points on $X_1(m, n)$ that are not cusps. These modular curves are either elliptic or hyperelliptic.

If the modular curve $X_1(m, n)$ is elliptic, we compute its rank. If the rank is positive, there are infinitely many elliptic curves over $K$ with the given torsion subgroup, as the number of cusps is finite. If the rank is 0, we have to compute the torsion subgroup and check whether any torsion point corresponds to a $K$–rational point on the modular curve that is not a cusp.

If the modular curve $X_1(m, n)$ is hyperelliptic, we compute the rank of the Jacobian of the curve. If the rank is 0, we also have to check whether any torsion point arises from a $K$–rational point on the modular curve that is not a cusp.

If the rank is positive, the problem becomes more difficult. More about this can be found in [6].

2. Groups from Mazur’s theorem and

$\mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3n\mathbb{Z}, \ n = 1, 2, \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$

In this section, we are going to show that every group mentioned in Mazur’s theorem has to appear as a possible torsion group over any quadratic field $K$.

Let $E$ be an elliptic curve and denote by $\rho_{E,n} : \text{Gal}(K/\mathbb{Q}) \to \text{GL}_2(\mathbb{Z}/n\mathbb{Z})$ the mod $n$ Galois representation attached to $E$.

If $P, P'$ is a basis for $E[n]$, the subgroup of $E$ of points of order $n$, and if $P$ is a point of order $n$ in $E(\mathbb{Q})$, then $\rho_{E,n}(\sigma) = \begin{bmatrix} 1 & b \\ 0 & d \end{bmatrix}, \ b, d \in \mathbb{Z}/n\mathbb{Z}$ for every $\sigma \in \text{Gal}(K/\mathbb{Q})$, with respect to the basis $\{P, P'\}$.

We define a subgroup of $\text{GL}_2(\mathbb{Z}/n\mathbb{Z})$,

$$\Gamma_1(n) = \left\{ \begin{bmatrix} 1 & b \\ 0 & d \end{bmatrix} : b \in \mathbb{Z}/n\mathbb{Z}, d \in (\mathbb{Z}/n\mathbb{Z})^\times \right\},$$

which corresponds to $X_1(n)$, i.e. the mod $n$ representations of elliptic curves parameterized by the points on $X_1(n)$ are elements in $G(n)$, with an appropriate choice of basis. Similarly, we define a subgroup

$$\Gamma_1(2, 2n) = \left\{ \begin{bmatrix} 1 & b \\ 0 & d \end{bmatrix} : b \in 2\mathbb{Z}/2n\mathbb{Z}, d \in (\mathbb{Z}/2n\mathbb{Z})^\times \right\},$$

which corresponds to $X_1(2, 2n)$, in the sense described above.

For any of the groups $\mathbb{Z}/n\mathbb{Z}$ or $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z}$ appearing in Mazur’s theorem, we have that the corresponding modular curve $X_1(n)$ or $X_1(2, 2n)$, respectively, is of genus 0. Now, with $X_G = X_1(n)$ or $X_G = X_1(2, 2n)$ in [13 Lemma 3.5], using the same arguments as in the proof of the lemma, but taking the base field to be a quadratic field $K$ instead of $\mathbb{Q}$, we have that there are infinitely many elliptic curves $E$ over $K$ such that $\rho_{E,n}(\text{Gal}(K/\mathbb{Q}))$ is conjugate (not just contained) in $\text{GL}_2(\mathbb{Z}/n\mathbb{Z})$ to $\Gamma_1(n)$ or $\Gamma_1(2, 2n)$, respectively, proving our claim.
Now, we will focus on the groups
\[ \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3n\mathbb{Z}, \quad n = 1, 2, \]
\[ \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4n\mathbb{Z}. \]
From the properties of the Weil pairing, we know that
\[ \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \subset E(K) \text{ only if } \mathbb{Q}(\zeta_n) \subset K. \]
Hence, \[ \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3n\mathbb{Z} \subset E(K), \quad n = 1, 2, \]
\[ \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4n\mathbb{Z} \subset E(K) \text{ only if } K \supset \mathbb{Q}(\zeta_3) = \mathbb{Q}(\sqrt{-3}) \text{ and } \mathbb{Q}(\sqrt{-17}) \text{, respectively.} \]

3. Torsion over \( \mathbb{Q}(\sqrt{17}) \)

We will now demonstrate how to carry out the mentioned methods over the quadratic field \( \mathbb{Q}(\sqrt{17}) \). We chose \( \mathbb{Q}(\sqrt{17}) \) because \( 17 \equiv 1 \pmod{8} \), and the significance of this relation will be clear later on.

As stated above, all groups from Mazur’s theorem are possible torsion subgroups over \( \mathbb{Q}(\sqrt{17}) \), and the groups \( \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3n\mathbb{Z}, \quad n = 1, 2, \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4n\mathbb{Z} \) are not.

For the rest of the groups we will follow the methods from [6] described above.

The equations for \( X_1(m, n) \) can be found in [1, 12].

All computations in the following propositions will be done in Magma [2]. Computations for this paper can be found [here].

**Proposition 3.1.** There are infinitely many elliptic curves with torsion \( \mathbb{Z}/11\mathbb{Z} \) over \( \mathbb{Q}(\sqrt{17}) \).

**Proof.** To show this, we have to prove that the modular curve \( X_1(11) \) defined over \( \mathbb{Q}(\sqrt{17}) \) has infinitely many points. It will suffice to see that the rank is positive, since the number of cusps on \( X_1(11) \) is finite. For the modular curve
\[ X_1(11) : \quad y^2 - y = x^3 - x^2, \]
we compute
\[ \text{rank}(X_1(11)(\mathbb{Q}(\sqrt{17}))) = 1 \]
in Magma. Now we can conclude that there are infinitely many elliptic curves with torsion \( \mathbb{Z}/11\mathbb{Z} \) over \( \mathbb{Q}(\sqrt{17}) \).

We can also compute a generator of the group \( X_1(11)(\mathbb{Q}(\sqrt{17})) \) (modulo the torsion subgroup), which is
\[ \left( \frac{1}{8}(-\sqrt{17} + 1), \frac{1}{16}(\sqrt{17} + 7) \right). \]

**Proposition 3.2.** There are infinitely many elliptic curves with torsion \( \mathbb{Z}/14\mathbb{Z} \) over \( \mathbb{Q}(\sqrt{17}) \).

**Proof.** For the modular curve
\[ X_1(14) : \quad y^2 + xy + y = x^3 - x \]
we compute
\[ \text{rank}(X_1(14)(\mathbb{Q}(\sqrt{17}))) = 1. \]
Using similar reasoning to the one in Proposition 3.1 we conclude that there are infinitely many elliptic curves with torsion \( \mathbb{Z}/14\mathbb{Z} \) over \( \mathbb{Q}(\sqrt{17}) \).
Also, one point of infinite order is given by
\[
\left(\frac{1}{2}(\sqrt{17} + 3), -\sqrt{17} - 5\right).
\]

Proposition 3.3. \(\mathbb{Z}/15\mathbb{Z}\) cannot be a torsion group of an elliptic curve over \(\mathbb{Q}(\sqrt{17})\).

Proof. For the modular curve
\[
X_1(15) : \ y^2 + xy + y = x^3 + x^2,
\]
we compute
\[
\text{rank}(X_1(15)(\mathbb{Q}(\sqrt{17}))) = 0.
\]
Hence, we only have to show that
\[
Y_1(15)(\mathbb{Q}(\sqrt{17})) = \emptyset,
\]
i.e. that there are only cusps in \(X_1(15)(\mathbb{Q}(\sqrt{17}))\).

The \(x\)-coordinates of the cusps on \(X_1(15)\) satisfy the equation
\[
x(x + 1)(x^4 + 3x^3 + 4x^2 + 2x + 1)(x^4 - 7x^3 - 6x^2 + 2x + 1) = 0.
\]
So, the set of all cusps is
\[
X_1(15)(\mathbb{Q}(\sqrt{17})) \setminus Y_1(15)(\mathbb{Q}(\sqrt{17})) = \{O, (0, 0), (0, -1), (-1, 0)\}.
\]
We compute
\[
X_1(15)(\mathbb{Q}(\sqrt{17})) \cong \mathbb{Z}/4\mathbb{Z},
\]
so now it is obvious that all points on the modular curve \(X_1(15)\) defined over \(\mathbb{Q}(\sqrt{17})\) are cusps. Therefore, \(Y_1(15)(\mathbb{Q}(\sqrt{17})) = \emptyset\), so there are no elliptic curves with torsion \(\mathbb{Z}/15\mathbb{Z}\) over \(\mathbb{Q}(\sqrt{17})\). \(\square\)

Proposition 3.4. There are infinitely many elliptic curves with torsion \(\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/10\mathbb{Z}\) over \(\mathbb{Q}(\sqrt{17})\).

Proof. For the modular curve
\[
X_1(2, 10) : \ y^2 = x^3 + x^2 - x,
\]
we compute
\[
\text{rank}(X_1(2, 10)(\mathbb{Q}(\sqrt{17}))) = 1.
\]
One point of infinite order is
\[
\left(\sqrt{17} + 4, 3\sqrt{17} + 12\right).
\]
\(\square\)

Proposition 3.5. There are infinitely many elliptic curves with torsion \(\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/12\mathbb{Z}\) over \(\mathbb{Q}(\sqrt{17})\).

Proof. For the modular curve
\[
X_1(2, 12) : \ y^2 = x^3 - x^2 + x,
\]
we compute
\[
\text{rank}(X_1(2, 12)(\mathbb{Q}(\sqrt{17}))) = 1.
\]
A point of infinite order is 
\[ \left( \frac{1}{2}(-\sqrt{17} + 9), \frac{1}{2}(-3\sqrt{17} + 19) \right). \]

Now we have determined whether \( \mathbb{Z}/n\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z} \) is a possible torsion of an elliptic curve over \( \mathbb{Q}(\sqrt{d}) \), for all modular functions \( X_1(m, n) \) that are elliptic curves. To determine if the \( \mathbb{Z}/n\mathbb{Z}, n = 13, 16, 18, \) are possible torsion groups is somewhat more difficult, since corresponding modular curves are hyperelliptic curves.

The groups \( \mathbb{Z}/n\mathbb{Z}, n = 13, 18, \) are generally easier to deal with over quadratic fields, since we have the two following results that can be found in [3, 8].

**Theorem 3.6.** If \( X_1(13) \) has a point defined over \( \mathbb{Q}(\sqrt{d}) \), then:
 1. \( d > 0 \),
 2. \( d \equiv 1 \pmod{8} \).

**Theorem 3.7.** If \( X_1(18) \) has a point defined over \( \mathbb{Q}(\sqrt{d}) \), \( d \neq -3 \), then:
 1. \( d > 0 \),
 2. \( d \equiv 1 \pmod{8} \),
 3. \( d \not\equiv 2 \pmod{3} \).

Now it becomes clear why we chose the field \( \mathbb{Q}(\sqrt{17}) \), as we did not want to rule out the existence of the groups \( \mathbb{Z}/n\mathbb{Z}, n = 13, 18, \) as possible torsion subgroups.

**Proposition 3.8.** \( \mathbb{Z}/13\mathbb{Z} \) is a possible torsion over \( \mathbb{Q}(\sqrt{17}) \).

**Proof.** Let \( J_1(13) \) be the Jacobian of the hyperelliptic curve \( X_1(13) : y^2 = x^6 - 2x^5 + x^4 - 2x^3 + 6x^2 - 4x + 1 \) and let \( J_1^{17}(13) \) be its quadratic twist by 17, which becomes isomorphic to \( J_1(13) \) over \( \mathbb{Q}(\sqrt{17}) \). We compute

\[
\text{rank}(J_1(13)(\mathbb{Q})) = 0, \\
\text{rank}(J_1^{17}(13)(\mathbb{Q})) = 2.
\]

Now, we have

\[
\text{rank}(J_1(13)(\mathbb{Q}(\sqrt{17}))) = \text{rank}(J_1(13)(\mathbb{Q})) + \text{rank}(J_1^{17}(13)(\mathbb{Q})) = 2.
\]

By searching for points on \( X_1(13)(\mathbb{Q}(\sqrt{17})) \) in Magma, we find a point \( \left( \frac{1}{2}, \frac{1}{8}\sqrt{17} \right) \) on the curve.

Since the \( x \)-coordinates of the cusps on the \( X_1(13) \) are the solutions of the equation

\[
x(x - 1)(x^3 - 4x^2 + x + 1) = 0,
\]

the cusps are

\[
X_1(13)(\mathbb{Q}(\sqrt{17})) \setminus Y_1(13)(\mathbb{Q}(\sqrt{17})) = \{ \infty_+, \infty_-, (0, \pm 1), (1, \pm 1) \}.
\]

We conclude that the point mentioned above is not a cusp and so the elliptic curve over \( \mathbb{Q}(\sqrt{17}) \) with a torsion subgroup \( \mathbb{Z}/13\mathbb{Z} \) exists.

Unlike in previous propositions, we do not have infinitely many elliptic curves with torsion \( \mathbb{Z}/13\mathbb{Z} \), since by Falting’s theorem the modular curve \( X_1(13) \) can only have finitely many points over a number field.
Proposition 3.9. \( \mathbb{Z}/16\mathbb{Z} \) cannot be a torsion group of an elliptic curve over \( \mathbb{Q}(\sqrt{17}) \).

Proof. Let \( J_1(16) \) be the Jacobian of the hyperelliptic curve

\[
X_1(16) : \quad y^2 = x(x^2 + 1)(x^2 + 2x - 1)
\]

and let \( J_1^{17}(16) \) be its quadratic twist.

We compute

\[
\text{rank}(J_1(16)(\mathbb{Q}(\sqrt{17}))) = \text{rank}(J_1(16)(\mathbb{Q})) + \text{rank}(J_1^{17}(16)(\mathbb{Q})) = 0.
\]

Since the rank is zero, we need to find the cusps in \( X_1(16)(\mathbb{Q}(\sqrt{17})) \) and the torsion subgroup of \( J_1(16)(\mathbb{Q}(\sqrt{17})) \) in order to determine if there exists a point on the Jacobian that arises from a point on the modular curve that is not a cusp.

As the \( x \)-coordinates of the cusps satisfy

\[
x(x-1)(x+1)(x^2 - 2x - 1)(x^2 + 2x - 1) = 0,
\]

the cusps on \( X_1(16)(\mathbb{Q}(\sqrt{17})) \) are

\[
X_1(16)(\mathbb{Q}(\sqrt{17})) \setminus Y_1(16)(\mathbb{Q}(\sqrt{17})) = \{ \infty, (0,0), (1,\pm2), (-1,\pm2) \}.
\]

We also compute

\[
\begin{align*}
J_1(16)(\mathbb{Q})_{\text{tors}} &\cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/10\mathbb{Z}, \\
J_1^{17}(16)(\mathbb{Q})_{\text{tors}} &\cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}.
\end{align*}
\]

The set of points of odd order on the Jacobian \( J_1(16) \) defined over \( \mathbb{Q}(\sqrt{17}) \) is

\[
J_1(16)(\mathbb{Q}(\sqrt{17}))_{(2')} \cong J_1(16)(\mathbb{Q})_{(2')} \oplus J_1^{17}(16)(\mathbb{Q})_{(2')} \cong \mathbb{Z}/5\mathbb{Z},
\]

and the \( 2 \)-torsion subgroup is

\[
J_1(16)(\mathbb{Q}(\sqrt{17}))_{\text{tors}} \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}.
\]

Thus, \( J_1(16)(\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/10\mathbb{Z} \) and \( J_1(16)(\mathbb{Q}) \cong J_1(16)(\mathbb{Q})_{\text{tors}} \).

In Magma, we find 20 divisor classes in Mumford representation \[4\].

\[
(1,0,0), \quad (x^2 + 2x + 1, 2x, 2), \quad (x^2 + 2x + 1, -2x, 2), \quad (x^2 - 2x + 1, 4x - 2, 2),
\]

\[
(x^2 - 2x + 1, -4x + 2, 2), \quad (x + 1, 2, 1), \quad (x + 1, -2, 1), \quad (x, 0, 1),
\]

\[
(x - 1, 2, 1), \quad (x - 1, -2, 1), \quad (x^2 + 2x - 1, 0, 2), \quad (x^2 + x, 2x, 2), \quad (x^2 + x, -2x, 2),
\]

\[
(x^2 - 1, 2x, 2), \quad (x^2 - 1, -2x, 2), \quad (x^2 - 1, -2, 2), \quad (x^2 + 1, 0, 2), \quad (x^2 - x, 2x, 2), \quad (x^2 - x, -2x, 2).
\]

The first divisor class represents the point at infinity, and for the rest of the divisor classes in Mumford representation, we follow the methods described in \[2\] in order to retrieve the point on the Jacobian from its Mumford representation.

For a triple \( (a(x), b(x), d) \) in Mumford representation we define \( A(x, z) \) as the homogenisation of the polynomial \( a(x) \) of degree \( d \) and \( B(x, z) \) as the homogenisation of the polynomial \( b(x) \) of degree \( g + 1 \), where \( g \) is a genus of \( X_1(16) \), in this case \( g = 2 \).

Now, by solving the equations

\[
A(x, z) = 0, \quad y = B(x, z),
\]

we get the points \( P_i = (x_i : y_i : 1), \quad i = 1, ..., d \), in projective coordinates. Note that the number of points is exactly \( d \), as the polynomial \( A(x, z) \) is of degree \( d \).

The point on the Jacobian represented by \( (a(x), b(x), d) \) is then the divisor class

\[
[P_1 + ... + P_d - d\infty],
\]
if there is a single point $\infty$ at infinity, or
\[
P_1 + \ldots + P_d - \frac{d}{2} (\infty_+ + \infty_-),
\]
if there are two points $\infty_+$ and $\infty_-$ at infinity.

For example, for the point $(x^2 + 2x + 1, 2x, 2)$ on $J_1(16)(\mathbb{Q}(\sqrt{17}))$ in Mumford representation we have
\[
A(x, z) = x^2 + 2xz + z^2,
B(x, z) = 2xz^2,
\]
and $P_1 = P_2 = (-1 : -2 : 1)$, so we conclude that the point $(x^2 + 2x + 1, 2x, 2)$ represents the divisor class $[(x^2 + 2x + 1, 2x, 2) - 2\infty]$ on the Jacobian $J_1(16)(\mathbb{Q}(\sqrt{17}))$.

By doing so for every divisor class in Mumford representation, one can check that all divisor points correspond to the cusps in $X_1(16)(\mathbb{Q}(\sqrt{17}))$, so we conclude that $\mathbb{Z}/16\mathbb{Z}$ cannot be a torsion group of an elliptic curve over $\mathbb{Q}(\sqrt{17})$.

**Proposition 3.10.** $\mathbb{Z}/18\mathbb{Z}$ cannot be a torsion group of an elliptic curve over $\mathbb{Q}(\sqrt{17})$.

**Proof.** Let $J_1(18)$ be the Jacobian of the hyperelliptic curve
\[
X_1(18) : y^2 = x^6 + 2x^5 + 5x^4 + 10x^3 + 10x^2 + 4x + 1
\]
and let $J_1^2(18)$ be its quadratic twist. We compute
\[
\text{rank}(J_1(18)(\mathbb{Q}(\sqrt{17}))) = \text{rank}(J_1(18)(\mathbb{Q})) + \text{rank}(J_1^2(18)(\mathbb{Q})) = 0.
\]
The $x-$coordinates of the cusps in $X_1(18)$ satisfy the equation
\[
x(x + 1)(x^2 + x + 1)(x^2 - 3x - 1) = 0,
\]
so the cusps are
\[
X_1(18)(\mathbb{Q}(\sqrt{17})) \setminus Y_1(18)(\mathbb{Q}(\sqrt{17})) = \{ \infty_+, \infty_-, (0, \pm 1), (-1, \pm 1) \}.
\]
On the other hand, we compute
\[
J_1(18)(\mathbb{Q})_{\text{tors}} \cong \mathbb{Z}/21\mathbb{Z},
\]
\[
J_1^2(18)(\mathbb{Q})_{\text{tors}} \cong \{ O \}.
\]
The set of points of odd order is
\[
J_1(18)(\mathbb{Q}(\sqrt{17}))_{(2')} \cong J_1(18)(\mathbb{Q})_{(2')} \oplus J_1^2(18)(\mathbb{Q})_{(2')} \cong \mathbb{Z}/21\mathbb{Z}.
\]
As the polynomial
\[
f(x) = x^6 + 2x^5 + 5x^4 + 10x^3 + 10x^2 + 4x + 1
\]
has no zeros defined over $\mathbb{Q}(\sqrt{17})$, we conclude that $J_1(18)(\mathbb{Q}(\sqrt{17}))$ has no points of order 2, and
\[
J_1(18)(\mathbb{Q}(\sqrt{17}))_{\text{tors}} \cong \mathbb{Z}/21\mathbb{Z}.
\]
The elements of $J_1(18)(\mathbb{Q}(\sqrt{17}))_{\text{tors}}$ in Mumford representation are
\[
(1, 0, 0), (1, x^3 + x^2, 2), (1, -x^3 - x^2, 2), (x^2 + 2x + 1, x, 2), (x^2 + 2x + 1, -x, 2),
(x^2, 2x + 1, 2), (x^2, -2x - 1, 2), (x + 1, x^3, 2), (x + 1, -x^3, 2),
(x + 1, x^3 + 2, 2), (x + 1, -x^3 - 2, 2), (x, x^4 - 1, 2), (x, -x^3 + 1, 2), (x, x^3 + 1, 2),
(x, -x^3 - 1, 2), (x^2, x, -2x - 1, 2), (x^2, x, 2x + 1, 2), (x^2 + x, -2x - 1, 2), (x^2 + x, 1, 2),
\]
(x^2 + x, −1, 2), (x^2 + x + 1, x − 1, 2), (x^2 + x + 1, −x + 1, 2),
and one can easily conclude that all of the points correspond to the cusps, so we obtain our result.

We proved the following theorem:

**Theorem 3.11.** The possible torsion subgroups of elliptic curves defined over \( \mathbb{Q}(\sqrt{17}) \) are the following:

\[
\mathbb{Z}/n\mathbb{Z}, \quad n = 1, \ldots, 14,
\]

\[
\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z}, \quad n = 1, \ldots, 6.
\]

**Remark 3.12.** In [8, Theorem 2.7.7, 2.7.8] Krumm found a list of possible quadratic fields \( \mathbb{Q}(\sqrt{d}) \) over which torsion subgroups \( \mathbb{Z}/13\mathbb{Z} \) and \( \mathbb{Z}/18\mathbb{Z} \) may appear, for \( 0 < d < 1000 \).

In our case, for \( 0 < d < 100 \), there are only two such fields, \( \mathbb{Q}(\sqrt{17}) \), over which \( \mathbb{Z}/13\mathbb{Z} \) appears, and \( \mathbb{Q}(\sqrt{33}) \), over which \( \mathbb{Z}/18\mathbb{Z} \) appears.

In this paper we were able to eliminate the rest of the fields for \( 0 < d < 100 \) using only conditions from 3.6 and 3.7 and methods described in 3.8 and 3.10.

4. Torsion over \( \mathbb{Q}(\sqrt{d}) \), \( 0 < d < 100 \)

For every quadratic field \( \mathbb{Q}(\sqrt{d}) \), where \( d \) is a non-negative squarefree integer \( d \neq 1, 0 < d < 100 \), we found the torsion subgroups appearing by methods similar to the ones described in Theorem 3.11.

Since we know that the groups from the Mazur’s theorem appear as torsion subgroups, and the groups \( \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3n\mathbb{Z}, \quad n = 1, 2, \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z} \) do not appear as torsion subgroups of elliptic curves over mentioned fields, we give a list of possible torsion subgroups within the groups

\[
\mathbb{Z}/n\mathbb{Z}, \quad n = 11, 13, 14, 15, 16, 18,
\]

\[
\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z}, \quad n = 5, 6,
\]

i.e. the rest of the possible 26 torsion subgroups over quadratic fields.

Note that the groups mentioned above appear as a torsion subgroup 37, 1, 38, 37, 6-17, 1, 35, 36 times, respectively, over all \( \mathbb{Q}(\sqrt{d}) \), where \( 0 < d < 100 \).

We were unable to determine how many times exactly does the group \( \mathbb{Z}/16\mathbb{Z} \) appear as a torsion subgroup because of the following problem: computing (in Magma) the rank of the Jacobian of the modular curve \( X_1(16) \) defined over the problematic quadratic fields listed in the table did not give a result, only the lower and the upper bound that were not the same. That was a problem since it is important to know the mentioned rank in order to know which method to use for determining whether that is a possible torsion subgroup or not.

Also, searching for the points on the modular curve \( X_1(16) \) over the same fields did not yield a result.
Table 1. List of all possible torsion groups over quadratic fields $\mathbb{Q}(\sqrt{\varnothing})$, for $0 < \varnothing < 1009$, without the groups from the Mazur's theorem.

| Fields $\mathbb{Q}(\sqrt{\varnothing})$ | Possible torsion subgroups over a given field |
|----------------------------------------|-----------------------------------------------|
| $\mathbb{Q}(\sqrt{2})$                | $\mathbb{Z}/n\mathbb{Z}$, $n = 11$           |
| $\mathbb{Q}(\sqrt{3})$                | $\mathbb{Z}/n\mathbb{Z}$, $n = 14, 15$       |
|                                        | $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z}$, $n = 6$ |
| $\mathbb{Q}(\sqrt{5})$                | $\mathbb{Z}/n\mathbb{Z}$, $n = 15$           |
| $\mathbb{Q}(\sqrt{6})$                | $\mathbb{Z}/n\mathbb{Z}$, $n = 11, 14$       |
|                                        | $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z}$, $n = 5, 6$ |
| $\mathbb{Q}(\sqrt{7})$                | $\mathbb{Z}/n\mathbb{Z}$, $n = 11, 14, 15$   |
|                                        | $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z}$, $n = 6$ |
| $\mathbb{Q}(\sqrt{10})$               | $\mathbb{Z}/n\mathbb{Z}$, $n = 11, 14, 15, 16$ |
|                                        | $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z}$, $n = 5, 6$ |
| $\mathbb{Q}(\sqrt{11})$               | $\mathbb{Z}/n\mathbb{Z}$, $n = 11, 15$       |
| $\mathbb{Q}(\sqrt{13})$               | $\mathbb{Z}/n\mathbb{Z}$, $n = 11, 15$       |
|                                        | $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z}$, $n = 5, 6$ |
| $\mathbb{Q}(\sqrt{14})$               | $\mathbb{Z}/n\mathbb{Z}$, $n = 14, 15$       |
|                                        | $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z}$, $n = 5$ |
| $\mathbb{Q}(\sqrt{15})$               | $\mathbb{Z}/n\mathbb{Z}$, $n = 15, 16$       |
|                                        | $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z}$, $n = 5$ |
| $\mathbb{Q}(\sqrt{17})$               | $\mathbb{Z}/n\mathbb{Z}$, $n = 11, 13, 14$   |
|                                        | $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z}$, $n = 5, 6$ |
| $\mathbb{Q}(\sqrt{19})$               | $\mathbb{Z}/n\mathbb{Z}$, $n = 11, 14$       |
|                                        | $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z}$, $n = 5$ |
| $\mathbb{Q}(\sqrt{21})$               | $\mathbb{Z}/n\mathbb{Z}$, $n = 11$           |
|                                        | $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z}$, $n = 6$ |
| $\mathbb{Q}(\sqrt{22})$               | $\mathbb{Z}/n\mathbb{Z}$, $n = 11, 14, 15$   |
|                                        | $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z}$, $n = 6$ |
| $\mathbb{Q}(\sqrt{23})$               | $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z}$, $n = 6$ |
| $\mathbb{Q}(\sqrt{26})$               | $\mathbb{Z}/n\mathbb{Z}$, $n = 14, 15$, maybe $\mathbb{Z}/16\mathbb{Z}$ |
|                                        | $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z}$, $n = 5$ |
| $\mathbb{Q}(\sqrt{29})$               | $\mathbb{Z}/n\mathbb{Z}$, $n = 11, 14, 15$   |
|                                        | $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z}$, $n = 5$ |
| $\mathbb{Q}(\sqrt{30})$               | $\mathbb{Z}/n\mathbb{Z}$, $n = 11, 15$       |
|                                        | $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z}$, $n = 5, 6$ |
| $\mathbb{Q}(\sqrt{31})$               | $\mathbb{Z}/n\mathbb{Z}$, $n = 14$, maybe $\mathbb{Z}/16\mathbb{Z}$ |
|                                        | $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z}$, $n = 5$ |
| $\mathbb{Q}(\sqrt{33})$               | $\mathbb{Z}/n\mathbb{Z}$, $n = 11, 14, 15, 18$ |
|                                        | $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z}$, $n = 5$ |
| $\mathbb{Q}(\sqrt{34})$               | $\mathbb{Z}/n\mathbb{Z}$, $n = 14, 15$       |
|                                        | $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z}$, $n = 5, 6$ |
### Possible torsion subgroups over a given field

| Field       | Possible torsion subgroups over a given field |
|-------------|-----------------------------------------------|
| \( \mathbb{Q}(\sqrt{35}) \) | \( \mathbb{Z}/n\mathbb{Z}, \ n = 11, 14 \)  
            | \( \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z}, \ n = 5, 6 \) |
| \( \mathbb{Q}(\sqrt{37}) \) | \( \mathbb{Z}/n\mathbb{Z}, \ n = 14, 15 \)  
            | \( \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z}, \ n = 5, 6 \) |
| \( \mathbb{Q}(\sqrt{38}) \) | \( \mathbb{Z}/n\mathbb{Z}, \ n = 14, 15 \)  |
| \( \mathbb{Q}(\sqrt{39}) \) | \( \mathbb{Z}/n\mathbb{Z}, \ n = 11 \)  
            | \( \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z}, \ n = 5, 6 \) |
| \( \mathbb{Q}(\sqrt{41}) \) | \( \mathbb{Z}/n\mathbb{Z}, \ n = 11, 14, 15, 16 \)  
            | \( \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z}, \ n = 6 \) |
| \( \mathbb{Q}(\sqrt{42}) \) | \( \mathbb{Z}/n\mathbb{Z}, \ n = 14, 15 \)  
            | \( \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z}, \ n = 6 \) |
| \( \mathbb{Q}(\sqrt{43}) \) | \( \mathbb{Z}/n\mathbb{Z}, \ n = 11, 15 \)  |
| \( \mathbb{Q}(\sqrt{46}) \) | \( \mathbb{Z}/n\mathbb{Z}, \ n = 11 \)  
            | \( \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z}, \ n = 5, 6 \) |
| \( \mathbb{Q}(\sqrt{47}) \) | \( \mathbb{Z}/n\mathbb{Z}, \ n = 14 \)  
            | \( \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z}, \ n = 6 \) |
| \( \mathbb{Q}(\sqrt{51}) \) | \( \mathbb{Z}/n\mathbb{Z}, \ n = 11, 14, 16 \)  
            | \( \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z}, \ n = 5 \) |
| \( \mathbb{Q}(\sqrt{53}) \) | \( \mathbb{Z}/n\mathbb{Z}, \ n = 11 \)  
            | \( \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z}, \ n = 5 \) |
| \( \mathbb{Q}(\sqrt{55}) \) | \( \mathbb{Z}/n\mathbb{Z}, \ n = 11, 14, 15 \)  
            | \( \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z}, \ n = 5, 6 \) |
| \( \mathbb{Q}(\sqrt{57}) \) | \( \mathbb{Z}/n\mathbb{Z}, \ n = 11, 15 \)  
            | \( \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z}, \ n = 5 \) |
| \( \mathbb{Q}(\sqrt{58}) \) | \( \mathbb{Z}/n\mathbb{Z}, \ n = 11, 15 \)  
            | \( \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z}, \ n = 6 \) |
| \( \mathbb{Q}(\sqrt{59}) \) | \( \mathbb{Z}/n\mathbb{Z}, \ n = 14, 15 \)  
            | \( \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z}, \ n = 5, 6 \) |
| \( \mathbb{Q}(\sqrt{61}) \) | \( \mathbb{Z}/n\mathbb{Z}, \ n = 11 \)  
            | \( \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z}, \ n = 6 \) |
| \( \mathbb{Q}(\sqrt{62}) \) | \( \mathbb{Z}/n\mathbb{Z}, \ n = 11, 14 \)  
            | \( \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z}, \ n = 6 \) |
| \( \mathbb{Q}(\sqrt{65}) \) | \( \mathbb{Z}/n\mathbb{Z}, \ n = 11 \)  
            | \( \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z}, \ n = 6 \) |
| \( \mathbb{Q}(\sqrt{66}) \) | \( \mathbb{Z}/n\mathbb{Z}, \ n = 11, 14 \)  
            | \( \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z}, \ n = 5, 6 \) |
| \( \mathbb{Q}(\sqrt{67}) \) | \( \mathbb{Z}/n\mathbb{Z}, \ n = 15 \)  |
| \( \mathbb{Q}(\sqrt{69}) \) | \( \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z}, \ n = 6 \) |
| \( \mathbb{Q}(\sqrt{70}) \) | \( \mathbb{Z}/n\mathbb{Z}, \ n = 14, 15 \)  
            | \( \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z}, \ n = 5, 6 \) |
| Fields       | Possible torsion subgroups over a given field                                      |
|-------------|----------------------------------------------------------------------------------|
| \( \mathbb{Q}(\sqrt{73}) \) | \( \mathbb{Z}/n\mathbb{Z}, \ n = 11, 14, 15 \)                                    |
|             | \( \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z}, \ n = 5, 6 \)         |
| \( \mathbb{Q}(\sqrt{74}) \) | \( \mathbb{Z}/n\mathbb{Z}, \ n = 11, 15, \) maybe \( \mathbb{Z}/16\mathbb{Z} \) | |
|             | \( \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z}, \ n = 5 \)         |
| \( \mathbb{Q}(\sqrt{77}) \) | \( \mathbb{Z}/n\mathbb{Z}, \ n = 11 \)                                          |
|             | \( \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z}, \ n = 5 \)         |
| \( \mathbb{Q}(\sqrt{78}) \) | \( \mathbb{Z}/n\mathbb{Z}, \ n = 15, \) maybe \( \mathbb{Z}/16\mathbb{Z} \) | |
|             | \( \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z}, \ n = 6 \)         |
| \( \mathbb{Q}(\sqrt{79}) \) | \( \mathbb{Z}/n\mathbb{Z}, \ n = 11, 14, \) maybe \( \mathbb{Z}/16\mathbb{Z} \) | |
|             | \( \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z}, \ n = 5 \)         |
| \( \mathbb{Q}(\sqrt{82}) \) | \( \mathbb{Z}/n\mathbb{Z}, \ n = 14, 15, \) maybe \( \mathbb{Z}/16\mathbb{Z} \) | |
|             | \( \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z}, \ n = 6 \)         |
| \( \mathbb{Q}(\sqrt{83}) \) | \( \mathbb{Z}/n\mathbb{Z}, \ n = 11, 14 \)                                          |
|             | \( \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z}, \ n = 6 \)         |
| \( \mathbb{Q}(\sqrt{85}) \) | \( \mathbb{Z}/n\mathbb{Z}, \ n = 11, 14, 15 \)                                    |
|             | \( \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z}, \ n = 6 \)         |
| \( \mathbb{Q}(\sqrt{86}) \) | \( \mathbb{Z}/n\mathbb{Z}, \ n = 11, 15 \)                                          |
|             | \( \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z}, \ n = 5 \)         |
| \( \mathbb{Q}(\sqrt{87}) \) | \( \mathbb{Z}/n\mathbb{Z}, \ n = 11, 14, 15, \) maybe \( \mathbb{Z}/16\mathbb{Z} \) | |
| \( \mathbb{Q}(\sqrt{89}) \) | \( \mathbb{Z}/n\mathbb{Z}, \ n = 14, 15, \) maybe \( \mathbb{Z}/16\mathbb{Z} \) | |
|             | \( \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z}, \ n = 5, 6 \)       |
| \( \mathbb{Q}(\sqrt{91}) \) | \( \mathbb{Z}/n\mathbb{Z}, \ n = 11 \)                                          |
|             | \( \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z}, \ n = 5, 6 \)       |
| \( \mathbb{Q}(\sqrt{97}) \) | \( \mathbb{Z}/n\mathbb{Z}, \ n = 14, 15 \)                                          |
|             | \( \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z}, \ n = 5 \)         |
References

[1] H. Baaziz, *Equations for the modular curve $X_1(N)$ and models of elliptic curves with torsion points*, Math. Comp. 79 (2010), 2371–2386. 3

[2] W. Bosma, J. Cannon, C. Playoust *The Magma algebra system. I. The user language*, J. Symbolic Comput. 24 (1997), 235–265. 3, 6

[3] J. Bosman, P. Bruin, A. Dujella, F. Najman, *Ranks of elliptic curves with prescribed torsion over number fields*, Int. Math. Res. Not. IMRN 2014 (2014), 2885–2923. 3

[4] H. Cohen, G. Frey, *Handbook of Elliptic and Hyperelliptic Curve Cryptography*, Chapman & Hall/CRC, 2006. 4

[5] S. Kamienny, *Torsion points on elliptic curves and $q$-coefficients of modular forms*, Invent. Math. 109 (1992), 221–229. 1

[6] S. Kamienny, F. Najman, *Torsion groups of elliptic curves over quadratic fields*, Acta. Arith. 152 (2012), 291–305. 1

[7] M. A. Kenku, F. Momose, *Torsion points on elliptic curves defined over quadratic fields*, Nagoya Math. J. 109, (1988), 125–149. 1

[8] D. Krumm, *Quadratic Points on Modular Curves*, Doctoral thesis, Athens, Georgia, 2013. 8

[9] B. Mazur, *Modular curves and the Eisenstein ideal*, Inst. Hautes Etudes Sci. Publ. Math. 47 (1978), 33–186. 1

[10] F. Najman, *Complete classification of torsion of elliptic curves over quadratic cyclotomic fields*, J. Number Theory 130 (2010), 1964–1968. 3

[11] F. Najman, *Torsion of elliptic curves over quadratic cyclotomic fields*, Math. J. Okayama Univ. 53 (2011), 75–82. 1

[12] F. P. Rabarison, *Structure de torsion des courbes elliptiques sur les corps quadratiques*, Acta Arith. 144 (2010), 17–52. 3

[13] D. J. Zywina, *On the possible images of the mod $l$ representations associated to elliptic curves over $Q$*, preprint. 2

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

E-mail address: antonela.trbovic@gmail.com