Torsion of Elliptic Curves Over Quadratic Fields

Jody Ryker, Sophie De Arment

November 20, 2014

Abstract

By focusing on the family $E : y^2 = x^3 + a$, we present strategies for determining the structure of the torsion subgroup of the Mordell-Weil group of an elliptic curve, $E(K)$, over quadratic field $K$. Generalizations of the Nagell-Lutz theorem and Mazur’s theorem to curves defined over quadratic fields allows us to determine the full torsion subgroup of $E(K)$ as one of at most three possibilities when $a$ is a square.

1 Introduction

The structure of the torsion subgroup of an elliptic curve over $\mathbb{Q}$ is well understood. Mordell’s theorem states that the set of rational torsion points on $E$ is a finitely-generated abelian group. As a result, there are finitely many points of rational torsion on $E$. Further, Mazur’s Theorem describes the possible structures of $E(\mathbb{Q})_{\text{tors}}$. Finally, we can use Nagell-Lutz’s theorem to compute all the rational torsion points of a given elliptic curve [6]. So, the Mordell, Mazur, and Nagell-Lutz theorems provide a complete description of the torsion subgroup of any elliptic curve over $\mathbb{Q}$. We would like to have a similar description for the torsion subgroup of elliptic curves over quadratic fields. An extension of Mordell’s theorem, shows that $E(K)_{\text{tors}}$, where $K$ is a quadratic field, is also a finitely generated abelian group [6]. The following theorem of Kamienny, Kenku, and Momose lists the 26 possibilities for the structure of $E(K)_{\text{tors}}$.

**Theorem 1.** (Kamienny [7], Kenku and Momose [2]) Let $K$ be a quadratic field and $E$ an elliptic curve over $K$. Then the torsion subgroup $E(K)_{\text{tors}}$ of $E(K)$ is isomorphic to one of the following 26 groups:

$$\mathbb{Z}/m\mathbb{Z}, \text{ for } 1 \leq m \leq 18, m \neq 17,$$
\[
\begin{align*}
\mathbb{Z}/2\mathbb{Z} & \oplus \mathbb{Z}/2m\mathbb{Z}, \ for \ 1 \leq m \leq 6, \\
\mathbb{Z}/3\mathbb{Z} & \oplus \mathbb{Z}/2m\mathbb{Z}, \ for \ m = 1, 2 \\
\mathbb{Z}/4\mathbb{Z} & \oplus \mathbb{Z}/4\mathbb{Z}.
\end{align*}
\]

In this paper, we concentrate on more specifically characterizing \( E(K)_{\text{tors}} \) for families of curves. In particular, we can pare down the list of 26 possibilities to at most three for curves of the form \( y^2 = x^3 + a \), where \( a \) is a square. We also present strategies for describing \( E(K)_{\text{tors}} \) for other families of elliptic curves. We generalize Nagell-Lutz’s theorem to determine where 2-torsion occurs. We also describe a method for finding 3-torsion. Using this information, we can more specifically describe the possibilities for \( E(K)_{\text{tors}} \). Next, we compare curves with parameterizations given in Rabarison’s work ([4]) for curves having certain torsion structures. Finally, we consider torsion structures that we know only occur over quadratic cyclotomic fields ([3], [5]).

In Section 2, we will present methods for finding 2-torsion and 3-torsion points. In Section 3 we will prove our main result:

**Theorem 2.** Let \( E(K) : y^2 = x^3 + a \), where \( a \) is an integer and \( K \) is any quadratic field.

i. Suppose \( a \) is a sixth power integer.

If \( K \neq \mathbb{Q}(\sqrt{-3}) \), then \( E(K)_{\text{tors}} \) is isomorphic to \( \mathbb{Z}/6\mathbb{Z}, \mathbb{Z}/12\mathbb{Z}, \) or \( \mathbb{Z}/18\mathbb{Z} \).

If \( K = \mathbb{Q}(\sqrt{-3}) \), then \( E(K)_{\text{tors}} \) is isomorphic to \( \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z} \).

ii. Suppose \( a \) is a square but not a sixth power, and \( K \neq \mathbb{Q}(\sqrt{-3}) \). Then \( E(K)_{\text{tors}} \) is isomorphic to \( \mathbb{Z}/3\mathbb{Z}, \mathbb{Z}/9\mathbb{Z} \).

If \( K = \mathbb{Q}(\sqrt{-3}) \), then \( E(K)_{\text{tors}} \) is isomorphic to \( \mathbb{Z}/3\mathbb{Z}, \mathbb{Z}/9\mathbb{Z}, \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z} \).

We will also describe the torsion structure of a particular curve using Theorem 2.

**Corollary 3.** Let \( E(K) : y^2 = x^3 + 1 \), where \( K \) is any quadratic field. Then \( E(K)_{\text{tors}} \) is isomorphic to \( \mathbb{Z}/6\mathbb{Z}, \mathbb{Z}/18\mathbb{Z}, \) or \( \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z} \).

## 2 2-Torsion and 3-Torsion

Let \( E(K) : y^2 = x^3 + bx + a \) be an elliptic curve with \( a, b \in K \) with \( K \) quadratic. We will first consider over which quadratic fields 2-torsion and 3-torsion occur in order to more precisely describe \( E(K)_{\text{tors}} \).
Lemma 4. A non-trivial point \((x, y)\) on a curve \(E(K) : y^2 = x^3 + bx + a\), where \(a, b \in K\), is a point of order two if and only if \(x \in K\) satisfies \(x^3 + bx + a = 0\).

Proof. From Nagell-Lutz’s theorem we know that a point \((x, y) \neq O\) on \(E\) is a point of order two if and only if \(y = 0\). 

In other words, we factor \(x^3 + bx + a\) to identify the fields over which \(E\) has 2-torsion. In order for \(E(K)_{\text{tors}}\) to contain a 2-torsion point, there would necessarily be an element \(x \in K\) such that \(x\) satisfies \(x^3 + bx + a = 0\).

Lemma 5.

i. Let \(E(K) : y^2 = x^3 + bx + a\), where \(a, b \in K\). A point \((x, y) \in E(K)\) is a point of order three if and only if \(x \in K\) satisfies \(3x^4 + 6bx^2 + 12ax - b^2 = 0\).

ii. Let \(E(K) : y^2 = x^3 + a\), where \(a \in K\). A point \((x, y) \in E(K)\) is a point of order three if and only if \(x \in K\) satisfies \(3x^4 + 12ax = 0\). When \(a\) is a square, there will always be a point of order three on \(E(\mathbb{Q})\).

Proof. Proof:

i. First recall that points of order three are points of inflection of \(E\). We take the second derivative of \(E(K)\), and find that the \(x\)-coordinate a point of order three must be a root of
\[
3x^4 + 6bx^2 + 12ax - b^2 = 0.
\]

ii. If \(b = 0\), Equation (1) simplifies to
\[
3x^4 + 12ax = 0.
\]
The inflection points occur at
\[
x = 0, \quad x = -\sqrt[3]{4a}, \quad x = -\frac{\sqrt[4]{4a}(1 - \sqrt{3})}{2}, \quad \text{and} \quad x = -\frac{\sqrt[4]{4a}(1 + \sqrt{3})}{2}.
\]
Since \(x = 0\) results in a 3-torsion point, there will be a point of order three, namely \((0, \pm \sqrt{a})\). If \(a\) is a square, this point is in \(\mathbb{Q}\).
3 Torsion Over Quadratic Fields

Theorem 2. Let $E(K): y^2 = x^3 + a$, where $a$ is an integer and $K$ is any quadratic field.

i. Suppose $a$ is a sixth power integer.

If $K \neq \mathbb{Q} (\sqrt{-3})$, then $E(K)_{\text{tors}}$ is isomorphic to $\mathbb{Z}/6\mathbb{Z}, \mathbb{Z}/12\mathbb{Z}$, or $\mathbb{Z}/18\mathbb{Z}$.

If $K = \mathbb{Q} (\sqrt{-3})$, then $E(K)_{\text{tors}}$ is isomorphic to $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}$.

ii. Suppose $a$ is a square but not a sixth power, and $K \neq \mathbb{Q} (\sqrt{-3})$. Then $E(K)_{\text{tors}}$ is isomorphic to $\mathbb{Z}/3\mathbb{Z}$ or $\mathbb{Z}/9\mathbb{Z}$.

If $K = \mathbb{Q} (\sqrt{-3})$, then $E(K)_{\text{tors}}$ is isomorphic to $\mathbb{Z}/3\mathbb{Z}, \mathbb{Z}/9\mathbb{Z}$, or $\mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}$.

Proof. Proof:

i. Let $E(K): y^2 = x^3 + b^6$, where $a = b^6$ and $b \in \mathbb{Z}$. Since 2-torsion occurs when $y = 0$, we will look for the roots of $x^3 + b^6$ (Lemma 4). These are

$$-b^{6/3} = -b^2$$

and

$$\frac{b^{6/3} + b^{6/3} \sqrt{-3}}{2} = \frac{b^2 \pm b^2 \sqrt{-3}}{2}.$$ 

There is exactly one rational root, $b^2$, so there is one point of order two over $\mathbb{Q}$ and at least one point of order two over every quadratic extension of $\mathbb{Q}$. There are two more points of order two over $\mathbb{Q}(\sqrt{-3})$.

Since there will be at least one rational point of order three, $\mathbb{Z}/3\mathbb{Z} \subseteq E(Q)_{\text{tors}}$ (Lemma 5). Further, since we also know that $\mathbb{Z}/2\mathbb{Z} \subseteq E(Q)_{\text{tors}}$, then $\mathbb{Z}/6\mathbb{Z} \subseteq E(Q)_{\text{tors}}$.

Let $K$ be any quadratic field. Then since $\mathbb{Z}/6\mathbb{Z} \subseteq E(Q)_{\text{tors}}$, $\mathbb{Z}/6\mathbb{Z} \subseteq E(K)_{\text{tors}}$. Using Kamienny, Kenku, and Momose’s work ([1], [2]) in Theorem 1, $E(K)_{\text{tors}}$ is one of the following:

- $\mathbb{Z}/6\mathbb{Z}$
- $\mathbb{Z}/12\mathbb{Z}$
- $\mathbb{Z}/18\mathbb{Z}$
- $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}$
- $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/12\mathbb{Z}$
\[ \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z} \]

If \( K \neq \mathbb{Q} (\sqrt{-3}) \), there are no further points of order two. Also, \( \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z} \) does not occur over any quadratic field other than \( \mathbb{Q} (\sqrt{-3}) \). Hence, this limits the above list to \( \mathbb{Z}/6\mathbb{Z}, \mathbb{Z}/12\mathbb{Z} \), or \( \mathbb{Z}/18\mathbb{Z} \).

If \( K = \mathbb{Q} (\sqrt{-3}) \), there will be three non-trivial points of order two (Lemma 4). Due to Najman’s work, it has already been shown that \( E(\mathbb{Q}(\sqrt{-3}))_{\text{tors}} \) cannot be \( \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/12\mathbb{Z} \). This leaves one possibility for the torsion subgroup of \( E(\mathbb{Q}(\sqrt{-3})) \): \( \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z} \).

ii. Now let \( a = b^2 \), where \( b \) is not a cube. We already know that there will be one point of order three (Lemma 5). Hence, \( \mathbb{Z}/3\mathbb{Z} \subseteq E(\mathbb{Q})_{\text{tors}} \subseteq E(K)_{\text{tors}} \). This shortens the list of 26 possibilities in Theorem 1 down to nine (1, 2):

\[ \mathbb{Z}/6\mathbb{Z} \]
\[ \mathbb{Z}/9\mathbb{Z} \]
\[ \mathbb{Z}/12\mathbb{Z} \]
\[ \mathbb{Z}/15\mathbb{Z} \]
\[ \mathbb{Z}/18\mathbb{Z} \]
\[ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z} \]
\[ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/12\mathbb{Z} \]
\[ \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z} \]
\[ \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z} \]

Next, we consider if and when 2-torsion will occur by finding the roots of \( y^2 = x^3 + b^2 \) (Lemma 4). The roots are:

\[ -b^{2/3} \]

and

\[ \frac{b^{2/3} \pm b^{2/3} \sqrt{-3}}{2} \]

Since \( b \) is not a cube, these roots are not contained in any quadratic field, thus eliminating the possibility of 2-torsion points on \( E(K) \). This now shortens the list for \( E(K)_{\text{tors}} \) to:
Finally, we know that $\mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}$ torsion does not occur over any quadratic field other than $\mathbb{Q}(\sqrt{-3})$ (3), and $\mathbb{Z}/15\mathbb{Z}$ torsion never occurs over $\mathbb{Q}(\sqrt{-3})$ (5).

Below are examples of curves of the form $y^2 = x^3 + a$.

\[
E : y^2 = x^3 + 1, \quad E(\mathbb{Q}(\sqrt{-3})) \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}
\]
\[
E : y^2 = x^3 + 4^2, \quad E(\mathbb{Q}(\sqrt{-3})) \cong \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}
\]

**Corollary 3.** Let $E(K) : y^2 = x^3 + 1$, where $K$ is any quadratic field. Then $E(K)_{\text{tors}}$ is isomorphic to $\mathbb{Z}/6\mathbb{Z}$, $\mathbb{Z}/18\mathbb{Z}$, or $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}$.

**Proof:** From Theorem 2 we know that $E(K)_{\text{tors}}$ is isomorphic to $\mathbb{Z}/6\mathbb{Z}$, $\mathbb{Z}/12\mathbb{Z}$, $\mathbb{Z}/18\mathbb{Z}$, or $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}$. We will compare the curve $y^2 = x^3 + 1$ with the parameterization given for a curve $E(K)$ with $\mathbb{Z}/12\mathbb{Z} \subseteq E(K)_{\text{tors}}$ in Rabarison’s paper [4]. First, we convert $y^2 = x^3 + 1$ from Weierstrass form to Tate Normal form:

\[
y^2 + \frac{4}{3}xy + \frac{2}{9}y = x^3 + \frac{2}{9}x^2
\]

Below is the parameterization of [4]:

\[
y^2 + (6t^4 - 8t^3 + 2t^2 + 2t - 1)xy + (-12t^6 + 30t^5 - 34t^4 + 21t^3 - 7t^2 + t)(t - 1)y =
\]
\[
x^3 + (-12t^6 + 30t^5 - 34t^4 + 21t^3 - 7t^2 + t)(t - 1)^2x^2
\]
The parameterization is centered at a point of order 12. We transform the curve so it is centered at a point of order six, as $y^2 + \frac{2}{9}xy + \frac{2}{9}y = x^3 + \frac{2}{9}x^2$ is. Next, we compare coefficients:

$$\frac{-10t^4 + 20t^3 - 16t^2 + 6t - 1}{(3t^2 - 3t + 1)^2} = \frac{4}{3}$$

$$\frac{t^2(t-1)^2(2t-1)^2(2t^2-2t+1)}{(3t^2-3t+1)^4} = \frac{2}{9}$$

This system is inconsistent. Hence, $\mathbb{Z}/12\mathbb{Z} \not\sim E(K)_{\text{tors}}$.

We believe that $E(K)_{\text{tors}} \not\sim \mathbb{Z}/18\mathbb{Z}$ for all $K$. However, we were unable to prove this. We attempted to compare the curve $y^2 = x^3 + 1$ to parameterizations for a curve with $\mathbb{Z}/18\mathbb{Z} \subseteq E(K)_{\text{tors}}$. We obtained a system of equations that Mathematica was unable to solve. We checked the torsion structure of $E(\mathbb{Q}(\sqrt{d}))$ for $-9000 \leq d \leq 3814$, and determined that $E(\mathbb{Q}(\sqrt{d})) \not\sim \mathbb{Z}/18\mathbb{Z}$ for such $d$.

References

[1] S. Kamienny. Torsion points on elliptic curves and q-coefficients of modular forms. *Inventiones mathematicae*, 109(1):221–229, 1992.

[2] M. A. Kenku and F. Momose. Torsion points on elliptic curves defined over quadratic fields. *Nagoya Mathematical Journal*, 109:125–149, 1988.

[3] Filip Najman. Complete classification of torsion of elliptic curves over quadratic cyclotomic fields. *Journal of Number Theory*, 130(9):1964–1968, 2010.

[4] F. P. Rabarison. *Torsion et rang des courbes elliptiques définies sur les corps de nombres algébriques*. PhD thesis, l’Université de Caen, 2008.

[5] F. P. Rabarison. Structure de torsion des courbes elliptiques sur les corps quadratiques. (french) [torsion structure of elliptic curves over quadratic fields]. *Acta Arith.*, 144(1):17–52, 2010.

[6] John Tate and Joseph H. Silverman. *Rational Points on Elliptic Curves*. Springer New York, 1992.