# Torsion section of elliptic curves over quadratic extensions of $\mathbb{Q}$

**Zakariae Cheddour**
*zakariae.cheddour@usmba.ac.ma*

**Abdelhakim Chillali***
*abdelhakim.chillali@usmba.ac.ma*

**A. Mouhib**
*University of Sidi Mohamed Ben Abdellah-USMBA, LSI, FP*
*MPI Department*
*BP. 1223, Taza*
*Morocco*
*ali.mouhib@usmba.ac.ma*

**Abstract.** In this paper, we will study and determine all possible torsion sections of elliptic curves that can appear on quadratic extensions of the set of rational numbers endowed by the usual addition and a non-standard way of multiplication.
**Keywords:** elliptic curves, torsion section, quadratic extension.

## 1. Introduction

Let E be an elliptic curve over $\mathbb{Q}$. By the Mordell-Weil theorem, the group $E(\mathbb{Q})$ of rational points on E is a finitely generated abelian group. Therefore, it is the product of the torsion group and $r \geq 0$ copies of an infinite cyclic group:

$$E(\mathbb{Q}) \cong E(\mathbb{Q})_{tors} \times \mathbb{Z}^r.$$

By Mazur's theorem [5], we know that $E(\mathbb{Q})_{tors}$ is one of the following 15 groups:

$$\begin{cases} \mathbb{Z}/n\mathbb{Z}, & \text{with } 1 \leq n \leq 10 \text{ or } n = 12, \\ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2m\mathbb{Z}, & \text{with } 1 \leq m \leq 4. \end{cases}$$

Subsequently, S. Kamienny, F. Najman [3] and M. A. Kenku, F. Momose [4] have worked on the possible torsion groups which can appear on quadratic extensions of $\mathbb{Q}$. In [3, 4] we find that on a quadratic extension $K$ of $\mathbb{Q}$, we have that $E(K)_{tors}$ is isomorphic to one of the following groups 26 :

$$\begin{cases} \mathbb{Z}/m\mathbb{Z}, & \text{with } 1 \leq m \leq 18 \ , \ m \neq 17, \\ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2m\mathbb{Z}, & \text{with } 1 \leq m \leq 6, \\ \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3m\mathbb{Z}, & \text{with } 1 \leq m \leq 2, \\ \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}. \end{cases}$$

*. Corresponding author

Note that $E(K)_{tors}$ is finite over a quadratic numbers field because of S. Kamienny theorem [2]. In particular, F. Najman [6, 7] has classified all possible torsion subgroups on cyclotomic quadratic extensions. Similarly, K. Sarma and A. Saikia [8] determined the possible torsion subgroups on the other imaginary quadratic fields of class 1.

In this paper, we will define a non-standard way of multiplying elements in the quadratic extension of the set of rational numbers, denoted by $\mathbb{Q}[\lambda]$ with $\lambda = \sqrt{d}$ and $d$ is a square-free integer. Also, we will study and determine all possible torsion sections of elliptic curves given by a Weierstrass equation $Y^{*2} * Z = X^{*3} + a * X * Z^2 + b * Z^3$ that can appear on $\mathbb{Q}[\lambda]$, where $\mathbb{Q}[\lambda]$ endowed by the usual addition and the new product law defined as follows, so for $X = x_0 + x_1\lambda$ and $Y = y_0 + y_1\lambda$, where $x_0$, $x_1$, $y_0$ and $y_1 \in \mathbb{Q}$, we have

$$X + Y = (x_0 + y_0) + (x_1 + y_1)\lambda$$

and

$$X * Y = x_0y_0 + (x_0y_1 + y_0x_1 + x_1y_1)\lambda.$$

Note that, if $X$ and $Y$ are two elements of $\mathbb{Q}$, then the product law $*$ is the usual product law over $\mathbb{Q}$.

In a later work, we will use these results to study the classification of the torsion section of elliptic curves on imaginary (real) multiquadratic extensions of the set of rational numbers. Furthermore, we will use these results to give a new encryption scheme... In what follows, we will use the following notation:

- For $X \in \mathbb{Q}[\lambda]$, we have $X^{*n} = \underbrace{X * X * ... * X}_{n\ times}$,
- $\Im_{a,b}$ for an elliptic curve over the ring $(\mathbb{Q}[\lambda], +, *)$ given by a Weierstrass equation $Y^{*2} * Z = X^{*3} + a * X * Z^{*2} + b * Z^{*3}$, with $a, b \in \mathbb{Q}[\lambda]$ and such that the discriminant $D = 4a^{*3} + 27b^{*2}$ is invertible in $\mathbb{Q}[\lambda]$,
- $Tor(\Im_{a,b})$ for the torsion section of $\Im_{a,b}$.

In this article, we study the mentioned elliptic curve, and we prove the following theorem,

**Theorem 1.1.** *With the same notation as above, let $\Im_{a,b}$ be an elliptic curve defined over $\mathbb{Q}[\lambda]$. So,*

$$Tor(\Im_{a,b}, \mathbb{Q}[\lambda]) \simeq \begin{cases} \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}, & n, m = 1, 2, ..., 10, 12, \\ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}, & 1 \leq n \leq 4, m = 1, 2, ..., 10, 12, \\ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2n\mathbb{Z} \times \mathbb{Z}/2m\mathbb{Z}, & 1 \leq n, m \leq 4. \end{cases}$$

## 2. The ring $(\mathbb{Q}[\lambda], +, *)$

In this section, we will give some results concerning the ring $\mathbb{Q}[\lambda]$, which are useful for the rest of this article. So, let $X$, $Y$ and $Z$ be elements of $\mathbb{Q}[\lambda]$ where $X = x_0 + x_1\lambda$, $Y = y_0 + y_1\lambda$ and $Z = z_0 + z_1\lambda$.

**Lemma 2.1.** *The set $\mathbb{Q}[\lambda]$ together with addition "$+$" and multiplication "$*$" is a finitely generated unitary commutative ring.*

**Proof.** By construction we have * is a commutative law.

We shall prove that $X * (Y * Z) = (X * Y) * Z$ so,

$$\begin{aligned} X * (Y * Z) &= X * (y_0z_0 + (y_0z_1 + z_0y_1 + y_1z_1)\lambda) \\ &= x_0y_0z_0 + (x_0[y_0z_1 + z_0y_1 + y_1z_1] + x_1y_0z_0 \\ &+ x_1[y_0z_1 + z_0y_1 + y_1z_1])\lambda \\ &= x_0y_0z_0 + (x_0y_0z_1 + x_0z_0y_1 + x_0y_1z_1 + x_1y_0z_0 + x_1y_0z_1 \\ &+ x_1z_0y_1 + x_1y_1z_1)\lambda \end{aligned}$$

on the other hand we have

$$\begin{aligned} (X * Y) * Z &= (x_0y_0 + (x_0y_1 + y_0x_1 + x_1y_1)\lambda) * Z \\ &= x_0y_0z_0 + (x_0y_0z_1 + [x_0y_1 + y_0x_1 + x_1y_1]z_0 \\ &+ [x_0y_1 + y_0x_1 + x_1y_1]z_1)\lambda \\ &= x_0y_0z_0 + (x_0y_0z_1 + x_0z_0y_1 + x_0y_1z_1 + x_1y_0z_0 + x_1y_0z_1 \\ &+ x_1z_0y_1 + x_1y_1z_1)\lambda \end{aligned}$$

hence $*$ is associative.

$*$ is distributive with respect to the law $+$

$$\begin{aligned} X * (Y + Z) &= X * (y_0 + z_0 + (y_1 + z_1)\lambda) \\ &= x_0(y_0 + z_0) + (x_0[y_1 + z_1] + x_1[y_0 + z_0] + x_1[y_1 + z_1])\lambda \\ &= x_0y_0 + x_0z_0 + (x_0y_1 + x_0z_1 + x_1y_0 + x_1z_0 + x_1y_1 + x_1z_1)\lambda \\ &= [x_0y_0 + (x_0y_1 + x_1y_0 + x_1y_1)t] + [x_0z_0 + (x_0z_1 + x_1z_0 + x_1z_1)\lambda] \\ &= X * Y + X * Z. \end{aligned}$$

□

**Corollary 2.1.** *$\mathbb{Q}[\lambda]$ is a vector space over $\mathbb{Q}$ of dimension 2, and $(1, \lambda)$ is its basis.*

The next proposition characterize the set $\mathbb{Q}[\lambda]^\times$ of invertible elements in $\mathbb{Q}[\lambda]$.

**Proposition 2.1.** *Let $X = x_0 + x_1\lambda \in \mathbb{Q}[\lambda]$, then $X \in \mathbb{Q}[\lambda]^\times$ if and only if $x_0 \neq 0$ and $x_0 + x_1 \neq 0$. The inverse is given by: $X^{-1} = x_0^{-1} - x_1x_0^{-1}(x_0 + x_1)^{-1}\lambda$.*

**Proof.** Let X be an invertible element of $\mathbb{Q}[\lambda]$, then there exist Y in $\mathbb{Q}[\lambda]$ such that $X * Y = 1$ so, $x_0y_0 = 1$ and $x_0y_1 + y_0x_1 + x_1y_1 = 0$, then we have $y_0 = x_0^{-1}$ and $y_1 = -(x_0 + x_1)^{-1}x_0^{-1}x_1$. So,

$$Y = X^{-1} = x_0^{-1} - (x_0 + x_1)^{-1}x_0^{-1}x_1\lambda.$$

Hence, $X$ is invertible if and only if $x_0 \neq 0$ and $x_0 + x_1 \neq 0$. □

**Corollary 2.2.** *The non invertible elements of* $\mathbb{Q}[\lambda]$ *are those elements of the form* $a\lambda$ *and* $b - b\lambda$*, where* $a, b \in \mathbb{Q}$*.*

**Proposition 2.2.**

- $\mathbb{Q}[\lambda]$ *is not a local ring,*
- $\mathbb{Q}[\lambda]$ *is not an integral domain.*

**Proof.** We use the fact that a ring R is a local ring if and only if all elements of R that are not units form an ideal. So, put $I = \{b - b\lambda \,|\, b \in \mathbb{Q}\} \cup \lambda\mathbb{Q}$ the set of non-invertible elements of $\mathbb{Q}[\lambda]$. We shall prove that $I$ is not an ideal, this turns out to prove that $\{b - b\lambda | b \in \mathbb{Q}\} \cap \lambda\mathbb{Q} = \{0\}$. So, let $X \in \{b - b\lambda | b \in \mathbb{Q}\} \cap \lambda\mathbb{Q}$ then $X = b - b\lambda = a\lambda$ where $a, b \in \mathbb{Q}$, it follows that $X = 0$.

For the 2nd point it is enough to take $X = \lambda$ and $Y = 1 - \lambda$, for which we have $X * Y = 0$. □

In what follows, we denote by $\widehat{\mathbb{Q}[\lambda]}$, the set of integral elements of $\mathbb{Q}[\lambda]$ over $\mathbb{Z}$. That is, $b \in \widehat{\mathbb{Q}[\lambda]}$ if and only if b is a root of a monic polynomial over $\mathbb{Z}$.

The following theorem characterizes the set $\widehat{\mathbb{Q}[\lambda]}$,

**Theorem 2.1.** $\widehat{\mathbb{Q}[\lambda]} = \mathbb{Z}[\lambda]$.

**Proof.** Let $A = e + f\lambda \in \mathbb{Z}[\lambda]$, then $A^{*2} = e^2 + (2ef + f^2)\lambda$, it follows that $A^{*2} = e^2 + 2e(A - e) + f(A - e)$, then A is a root of $P(X) = X^{*2} - e^2 - 2e(X - e) - f(X - e)$ over $\mathbb{Z}$. So, we have A is an integral element over $\mathbb{Z}$, then $\mathbb{Z}[\lambda] \subset \widehat{\mathbb{Q}[\lambda]}$.

On the other hand, let $A = e + f\lambda \in \widehat{\mathbb{Q}[\lambda]}$, so there exists a monic polynomial $P(X) = X^{*n} + a_1X^{*n-1} + ... + a_n$ over $\mathbb{Z}[X]$ such that $P(A) = 0$, then $P(e + f\lambda) = (e + f\lambda)^{*n} + a_1(e + f\lambda)^{*n-1} + ... + a_n = 0$. Since $\lambda^{*m} = \lambda$ for all $m \in \mathbb{N} - \{0\}$ it follows that $P(e + f\lambda) = e^n + Q_1(e) + \lambda(f^n + Q_2(e, f)) = 0$ with $Q_1$, $Q_2$ are two polynomials respectively belonging in $\mathbb{Z}[X]$ and $\mathbb{Z}[X, Y]$ such that $deg(Q_1(X)) < n$ and $deg(Q_2(e, Y)) < n$. So, $e^n + Q_1(e) = 0$ and $f^n + Q_2(e, f) = 0$ then:

- we have $T_1(X) = X^n + Q_1(X)$ is a monic polynomial over $\mathbb{Z}[X]$ and since $T_1(e) = 0$ it follows that e is an integral element over $\mathbb{Z}$. Hence, $e \in \mathbb{Z}$.
- on the other hand, since $e \in \mathbb{Z}$ we have $T_2(X) = X^n + Q_2(e, X)$ is a monic polynomial over $\mathbb{Z}[X]$ and since $T_2(f) = 0$ it follows that f is an integral element over $\mathbb{Z}$. Hence, $f \in \mathbb{Z}$. □

## 3. Elliptic curves over $\mathbb{Q}[\lambda]$

**Definition 3.1.** *An elliptic curve over a commutative ring $R$ is a group scheme (a group object in the category of schemes) over $Spec(R)$ (the prime spectrum of $R$) that is a relative 1-dimensional, smooth, proper curve over $R$. For more background information about group schemes, consult [10] for an introduction to affine group schemes.*

**Proposition 3.1** ([9])**.** *let $R$ be a ring in which 6 is invertible, let $a$ and $b$ be two elements of $R$ such that $4a^3 + 27b^2$ is invertible in $R$, the elliptic curve $E$ of equation*

$$Y^2Z = X^3 + aXZ^2 + bZ^3$$

*has a unique group scheme structure on $Spec(R)$ whose neutral element is $O = [0 : 1 : 0]$.*

**Remark 1.** According to the previous proposition we can consider the elliptic curve $\Im_{a,b}$ on the ring $\mathbb{Q}[\lambda]$ giving by the weirstrass equation $Y^{*2} = X^{*3} + a * X + b$, where $(a = a_0 + a_1\lambda\ ,\ b = b_0 + b_1\lambda) \in (\mathbb{Q}[\lambda])^2$ and $4a^{*3} + 27b^{*2}$ is invertible in $\mathbb{Q}[\lambda]$.

In what follows, we consider $\Im_0$ and $\Im_1$ two restriction of $\Im_{a,b}$ over $\mathbb{Q}$, defined as follows

$$\Im_0 = \{[X : Y : Z] \in P^2(\mathbb{Q}) | Y^2Z = X^3 + a_0XZ^2 + b_0Z^3\}$$

and

$$\Im_1 = \{[X : Y : Z] \in P^2(\mathbb{Q}) | Y^2Z = X^3 + (a_0 + a_1)XZ^2 + (b_0 + b_1)Z^3\}$$

such that $4a_0^3 + 27b_0^2 \neq 0$ and $4(a_0 + a_1)^3 + 27(b_0 + b_1)^2 \neq 0$. Suppose that we have $\Im_{a,b}$ is an elliptic curve over $\mathbb{Q}[\lambda]$, so we have the following lemmas,

**Lemma 3.1.** *$\Im_0$ is an elliptic curve over $\mathbb{Q}$.*

**Proof.** To prove this result we shall prove that $4a_0^3 + 27b_0^2 \neq 0$ if $\triangle = 4a^{*3} + 27b^{*2}$ is invertible in $\mathbb{Q}[\lambda]$. So, $\triangle = 4a^{*3} + 27b^{*2}$, where $a^{*3} = a_0^3 + [(a_0 + a_1)^3 - a_0^3]\lambda$ and $b^{*2} = b_0^2 + [b_1^2 + 2b_0b_1]\lambda$ to simplify the notation put, $a^{*3} = a_0^3 + Q_1\lambda$ and $b^{*2} = b_0^2 + Q_2\lambda$, so we have $\triangle = 4(a_0^3 + Q_1\lambda) + 27(b_0^2 + Q_2\lambda)$ then $\triangle = 4a_0^3 + 27b_0^2 + [4Q_1 + 27Q_2]\lambda$ and since $\triangle$ is invertible it follows from the Proposition 2.1 that $4a_0^3 + 27b_0^2 \neq 0$. □

**Lemma 3.2.** *$\Im_1$ is an elliptic curve over $\mathbb{Q}$.*

**Proof.** To prove this result we shall prove that $4[a_0 + a_1]^3 + 27[b_0 + b_1]^2 \neq 0$ if $\triangle = 4a^{*3} + 27b^{*2}$ is invertible in $\mathbb{Q}[\lambda]$. From above we have $\triangle = 4a_0^3 + 27b_0^2 + [4[a_0 + a_1]^3 - 4a_0^3 + 27[b_0 + b_1]^2 - 27b_0^2]\lambda$ and since $\triangle$ is invertible it follows from the Proposition 2.1 that $4[a_0 + a_1]^3 + 27[b_0 + b_1]^2 \neq 0$. □

**Theorem 3.1.** *$\Im_i$ are elliptic curves over $\mathbb{Q}$ for $i = 0, 1$ if and only if $\Im_{a,b}$ is an elliptic curve over $\mathbb{Q}[\lambda]$.*

**Proof.** Suppose that $\Im_0$ and $\Im_1$ are elliptic curves, then we have $4a_0^3+27b_0^2 \neq 0$ and $4[a_0+a_1]^3+27[b_0+b_1]^2 \neq 0$, and from the Proposition 2.1, it follows that $\triangle = 4a_0^3+27b_0^2+[4[a_0+a_1]^3-4a_0^3+27[b_0+b_1]^2-27b_0^2]\lambda$ is invertible over $\mathbb{Q}[\lambda]$.

To show the opposite direction, we use the lemmas 3.1 and 3.2. □

## 4. The torsion section of elliptic curves over $\mathbb{Q}[\lambda]$

In this section we will give the possible structure of the torsion section of an elliptic curve defined over the ring $\mathbb{Q}[\lambda]$.

**Theorem 4.1.** *Let $\Im_{a,b}$ be an elliptic curve over $\mathbb{Q}[\lambda]$. So,*

$$Tor(\Im_{a,b},\mathbb{Q}[\lambda]) \simeq \begin{cases} \mathbb{Z}/n\mathbb{Z}\times\mathbb{Z}/m\mathbb{Z}, & n,m=1,2,...,10,12,\\ \mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2n\mathbb{Z}\times\mathbb{Z}/m\mathbb{Z}, & 1\leq n\leq 4, m=1,2,...,10,12,\\ \mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2n\mathbb{Z}\times\mathbb{Z}/2m\mathbb{Z}, & 1\leq n,m\leq 4. \end{cases}$$

To prove this result we will define a relation between $\Im_{a,b}$ and $\Im_0\times\Im_1$.

**Lemma 4.1.** *Let $X = x_0+x_1\lambda$, $Y = y_0+y_1\lambda$, $Z = z_0+z_1\lambda$, $a = a_0+a_1\lambda$ and $b = b_0+b_1\lambda$ be elements of $\mathbb{Q}[\lambda]$, then we have $[X:Y:Z]$ is in $P^2(\mathbb{Q}[\lambda])$, if and only if $[x_0:y_0:z_0] \in P^2(\mathbb{Q})$, and $[x_0+x_1:y_0+y_1:z_0+z_1] \in P^2(\mathbb{Q})$.*

**Proof.** Suppose that $[X:Y:Z] \in P^2(\mathbb{Q}[\lambda])$, then there exist $(U,V,W) \in (\mathbb{Q}[\lambda])^3$ such that $U*X+V*Y+W*Z = 1$. So, $[u_0x_0+(u_0x_1+u_1x_0+u_1x_1)\lambda]+[v_0y_0+(v_0y_1+v_1y_0+v_1y_1)\lambda]+[w_0z_0+(w_0z_1+w_1z_0+w_1z_1)\lambda] = 1$ , then $u_0x_0+v_0y_0+w_0z_0 = 1$ and $u_0x_1+u_1x_0+u_1x_1+v_0y_1+v_1y_0+v_1y_1+w_0z_1+w_1z_0+w_1z_1 = 0$.

It follows that $(u_0+u_1)(x_0+x_1)+(v_0+v_1)(y_0+y_1)+(w_0+w_1)(z_0+z_1)-(u_0x_0+v_0y_0+w_0z_0) = 0$, since $u_0x_0+v_0y_0+w_0z_0 = 1$ we have

$$\begin{cases} u_0x_0+v_0y_0+w_0z_0 = 1,\\ (u_0+u_1)(x_0+x_1)+(v_0+v_1)(y_0+y_1)+(w_0+w_1)(z_0+z_1) = 1. \end{cases}$$

So, $(x_0,y_0,z_0) \neq (0,0,0)$ and $(x_0+x_1,y_0+y_1,z_0+z_1) \neq (0,0,0)$, which proves that $[x_0:y_0:z_0]$ and $[x_0+x_1:y_0+y_1:z_0+z_1]$ are in $P^2(\mathbb{Q})$.

Conversely, let $[x_0:y_0:z_0]$, $[x_0+x_1:y_0+y_1:z_0+z_1] \in P^2(\mathbb{Q})$. Suppose that $y_0 \neq 0$, then we distinguish between two case of $y_0+y_1$:

- $y_0+y_1 \neq 0$ : then $Y$ is invertible in $\mathbb{Q}[\lambda]$, so $[X:Y:Z] \in \mathrm{P}^2(\mathbb{Q}[\lambda])$.
- $y_0+y_1 = 0$ : then $x_0+x_1 \neq 0$ or $z_0+z_1 \neq 0$. So, without loss of generality, suppose that $x_0+x_1 \neq 0$ then $Y+\lambda*X \in (\mathbb{Q}[\lambda])^\times$. Hence, $[X:Y:Z] \in P^2(\mathbb{Q}[\lambda])$.

We follow the same proof if $x_0 \neq 0$ or $z_0 \neq 0$. □

**Lemma 4.2.** *With the same notation as above, we have* $[X : Y : Z]$ *is in* $\Im_{a,b}$ *if and only if* $[x_0 : y_0 : z_0] \in \Im_0$ *and* $[x_0 + x_1 : y_0 + y_1 : z_0 + z_1] \in \Im_1$.

**Proof.** From the previous lemma we have $[X : Y : Z]$ is in $P^2(\mathbb{Q}[\lambda])$, if and only if $[x_0 : y_0 : z_0] \in P^2(\mathbb{Q})$, and $[x_0 + x_1 : y_0 + y_1 : z_0 + z_1] \in P^2(\mathbb{Q})$.

On the other hand, it remains to show that $[X : Y : Z]$ is a solution of $Y^{*2} * Z = X^{*3} + a * X * Z^{*2} + b * Z^{*3}$ if and only if $[x_0 : y_0 : z_0]$ is a solution of $Y^2Z = X^3 + a_0XZ^2 + b_0Z^3$ and $[x_0 + x_1 : y_0 + y_1 : z_0 + z_1]$ is a solution of $Y^2Z = X^3 + (a_0 + a_1)XZ^2 + (b_0 + b_1)Z^3$.

So, with the same notation as above, we have:

- $Y^{*2} * Z = y_0^2 z_0 + ((y_0 + y_1)^2(z_0 + z_1) - y_0^2 z_0)\lambda$,
- $X^{*3} = x_0^3 + ((x_0 + x_1)^3 - x_0^3)\lambda$,
- $a * X * Z^{*2} = a_0 x_0 z_0 + ((a_0 + a_1)(x_0 + x_1)(z_0 + z_1)^2 - a_0 x_0 z_0)\lambda$
- $b * Z^{*3} = b_0 z_0^3 + ((b_0 + b_1)(z_0 + z_1)^3 - b_0 z_0^3)\lambda$.

We deduce from the Proposition 2.1 that $Y^{*2} * Z = X^{*3} + a * X * Z^{*2} + b * Z^{*3}$ if and only if $y_0^2 z_0 = x_0^3 + a_0 x_0 z_0^2 + b_0 z_0^3$ and $(y_0 + y_1)^2(z_0 + z_1) = (x_0 + x_1)^3 + (a_0 + a_1)(x_0 + x_1)(z_0 + z_1)^2 + (b_0 + b_1)(z_0 + z_1)^3$, hence the result. □

In the following theorem, we will define a bijective application that allows us to connect the curve $\Im_{a,b}$ with the elliptic curves $\Im_0$ and $\Im_1$,

**Theorem 4.2.** *The mapping*

$$\begin{array}{ccc} \Im_{a,b} & \xrightarrow{\wp} & \Im_0 \times \Im_1 \\ [X : Y : Z] & \longmapsto & ([x_0 : y_0 : z_0], [x_0 + x_1 : y_0 + y_1 : z_0 + z_1]) \end{array}$$

*is a bijection.*

**Proof.** From lemma 4.2 it follows that $\wp$ is well defined.

$\wp$ is a surjective map:

Let $[x_0 : y_0 : z_0] \in \Im_0$ and $[x_1 : y_1 : z_1] \in \Im_1$ then

$$[x_0 + (x_1 - x_0)\,\lambda : y_0 + (y_1 - y_0)\,\lambda : z_0 + (z_1 - z_0)\,\lambda] \in \Im_{a,b}$$

so, we have:

$$\begin{aligned} &\wp\left([x_0 + (x_1 - x_0)\,\lambda : y_0 + (y_1 - y_0)\,\lambda : z_0 + (z_1 - z_0)\,\lambda]\right) \\ &= ([x_0 : y_0 : z_0], [x_0 + (x_1 - x_0) : y_0 + (y_1 - y_0) : z_0 + (z_1 - z_0)]) \\ &= ([x_0 : y_0 : z_0], [x_1 : y_1 : z_1]), \end{aligned}$$

hence $\wp$ is a surjective mapping.

$\wp$ is injective, for that lets $[X : Y : Z]$ and $[X' : Y' : Z']$ in $E_{a,b}$, where $X = x_0+x_1\lambda$, $Y = y_0+y_1\lambda$, $Z = z_0+z_1\lambda$, $X' = x'_0+x'_1\lambda$, $Y' = y'_0+y'_1\lambda$ and $Z' = z'_0 + z'_1\lambda$. So, if $[x_0 : y_0 : z_0] = [x'_0 : y'_0 : z'_0]$ and $[x_0 + x_1 : y_0 + y_1 : z_0 + z_1] = [x'_0 + x'_1 : y'_0 + y'_1 : z'_0 + z'_1]$ then there exist $\beta_0$, $\beta 1 \in \mathbb{Q}^\times$ such that $x_0 = \beta_0 x'_0$, $y_0 = \beta_0 y'_0$, $z_0 = \beta_0 z'$ and $x_0 + x_1 = \beta_1(x'_0 + x'_1)$, $y_0 + y_1 = \beta_1(y'_0 + y'_1)$, $z_0 + z_1 = \beta_1(z'_0 + z'_1)$. Consider $\beta = \beta_0 + (\beta_1 - \beta_0)\lambda$, it follows that

$$\begin{cases} x_0 = \beta_0 x'_0, \\ y_0 = \beta_0 y'_0, \\ z_0 = \beta_0 z'_0 \end{cases}$$

and

$$\begin{cases} x_1 = \beta_1 x'_1 + x'_0(\beta_1 - \beta_0), \\ y_1 = \beta_1 y'_1 + y'_0(\beta_1 - \beta_0), \\ z_1 = \beta_1 z'_1 + z'_0(\beta_1 - \beta_0). \end{cases}$$

So, we have $X = \beta * X'$, $Y = \beta * Y'$, $Z = \beta * Z'$ and $\beta \in \mathbb{Q}[\lambda]^\times$ then $[X : Y : Z] = [X' : Y' : Z']$. Hence, $\wp$ is a bijection. We can show that the mapping $\wp^{-1}$ defined by:

$$\begin{aligned} &\wp^{-1}([x_0 : y_0 : z_0], [x_1 : y_1 : z_1]) \\ &= [x_0 + (x_1 - x_0)\lambda : y_0 + (y_1 - y_0)\lambda : z_0 + (z_1 - z_0)\lambda] \end{aligned}$$

is the inverse of $\wp$. □

### 4.1 The group law $\star$ over $\Im_{a,b}$

To define the group law $\star$ over $\Im_{a,b}$, we use the explicit formulas in the article [1] [pages : 236-238], and since $\wp$ is bijection we can define $\star$ as follows $P \star Q = \wp^{-1}(\wp(P) + \wp(Q))$ for $P$, $Q \in \Im_{a,b}$.

**Corollary 4.1.** *The mapping*

$$\begin{array}{ccc} (\Im_{a,b}, \star) & \xrightarrow{\wp} & (\Im_0 \times \Im_1, +) \\ [X : Y : Z] & \longmapsto & ([x_0 : y_0 : z_0], [x_0 + x_1 : y_0 + y_1 : z_0 + z_1]) \end{array}$$

*is an isomorphism of groups.*

**Proof.** From the previous theorem we have $\wp$ is a bijection and according to the construction of the group law over $\Im_{a,b}$ we have $\wp([X : Y : Z] \star [X' : Y' : Z']) = \wp([X : Y : Z]) + \wp([X' : Y' : Z'])$. So, $\wp$ is an isomorphism of groups. □

**Proposition 4.1.** *Let $P = [X : Y : Z] \in \Im_{a,b}$ such that $X = x_0 + x_1\lambda$, $Y = y_0 + y_1\lambda$ and $Z = z_0 + z_1\lambda$, so $P \in Tor(\Im_{a,b})$ if and only if $P_0 \in Tor(\Im_0)$ and $P_1 \in Tor(\Im_1)$, where $P_0 = [x_0 : y_0 : z_0]$ and $P_1 = [x_0+x_1 : y_0+y_1 : z_0+z_1]$.*

**Proof.** Let $P \in Tor(\Im_{a,b})$ then there exist an integer $m$ such that $mP = P\star...\star P = O$, so $\wp^{-1}(\wp(P)+...+\wp(P)) = O$ we obtain $(P_0,P_1)+...+(P_0,P_1) = \wp(O) = (O_0,O_1)$, then $mP_0 = O_0$ and $mP_1 = O_1$, hence $P_0 \in Tor(\Im_0)$ and $P_1 \in Tor(\Im_1)$. On the other hand, if there exist an integers $m$, $n$ such that $mP_0 = O_0$ and $nP_1 = O_1$, we have $mnP = \wp^{-1}((P_0,P_1)+...+(P_0,P_1) = \wp^{-1}((mnP_0,mnP_1)) = \wp^{-1}(O_0\times O_1) = O$. □

**Corollary 4.2.** *With the same notation as above we have* $\wp(Tor(\Im_{a,b})) = Tor(\Im_0)\times Tor(\Im_1)$.

**Proposition 4.2.** *According to the above we have* $Tor(\Im_{a,b}) \simeq Tor(\Im_0)\times Tor(\Im_1)$.

**Proof.** Put

$$\begin{array}{ccc} Tor(\Im_{a,b}) & \overset{\wp/_{Tor(\Im_{a,b})}}{\longrightarrow} & Tor(\Im_0)\times Tor(\Im_1) \\ P & \longmapsto & \wp(P). \end{array}$$

the $\wp$-restriction on the torsion section of $\Im_{a,b}$. From the theorem 4.2 and the previous lemmas we have $\wp/_{Tor(\Im_{a,b})}$ is an isomorphism of groups, hence the result. □

**Proof of Theorem 4.1.** *From the previous proposition we have* $Tor(\Im_{a,b}) \simeq Tor(\Im_0)\times Tor(\Im_1)$, *and from the Mazur's theorem [6] we deduce the result.* □

**Example 1.** Let $\lambda$ be a root of the polynomial $P(X) = X^2+2$, let $a = -676+648\lambda$ and $b = 13662-4968\lambda$ two elements in $\mathbb{Q}[\lambda]$. So, let $\Im_{a,b}$ the Elliptic curve defined by $Y^{*2}*Z = X^{*3}+a*X*Z^{*2}+b*Z^{*3}$ over $\mathbb{Q}[\lambda]$. We consider $\Im_0$ and $\Im_1$ two restriction of $\Im_{a,b}$ over $\mathbb{Q}$, defined as follows $\Im_0 = \{[X:Y:Z] \in P^2(\mathbb{Q}) | Y^2Z = X^3-675XZ^2+13662Z^3\}$ and $\Im_1 = \{[X:Y:Z] \in P^2(\mathbb{Q}) | Y^2Z = X^3-27XZ^2+8694Z^3\}$. So, using the magma calculator, we find that

| | $\triangle$ | j | $\Im_i(\mathbb{Q})_{tor}$ | Generator of $\Im_i(\mathbb{Q})_{tor}$ |
|---|---|---|---|---|
| $\Im_0$ | $-2.14$ | $-\frac{5^6}{2.14}$ | $\mathbb{Z}_6$ | $(1,-2)$ |
| $\Im_1$ | $-15$ | $-\frac{1}{15}$ | $\mathbb{Z}_4$ | $(15,108)$ |

Hence,

| | $\triangle$ | j | $\Im_{a,b}(\mathbb{Q}[\lambda])_{tor}$ | Generator of $\Im_{a,b}(\mathbb{Q}[\lambda])_{tor}$ |
|---|---|---|---|---|
| $\Im_{a,b}$ | $-2.14+13\lambda$ | $\frac{-5^7.3+23.10189\lambda}{2^2.3.5.7}$ | $\mathbb{Z}_4\times\mathbb{Z}_6$ | $(1+14\lambda,-2+110\lambda)$ |

## 5. Conclusion

In this paper, we have study an elliptic curve $\Im_{a,b}$ given by a Weierstrass equation $Y^{*2}*Z = X^{*3}+a*X*Z^2+b*Z^3$ over $(\mathbb{Q}[\lambda],+,*)$ and determine all possible torsion sections of this elliptic curve. So,

$$Tor(\Im_{a,b},\mathbb{Q}[\lambda]) \simeq \begin{cases} \mathbb{Z}/n\mathbb{Z}\times\mathbb{Z}/m\mathbb{Z}, & n,m = 1,2,...,10,12, \\ \mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2n\mathbb{Z}\times\mathbb{Z}/m\mathbb{Z}, & 1\leq n\leq 4, m=1,2,...,10,12, \\ \mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2n\mathbb{Z}\times\mathbb{Z}/2m\mathbb{Z}, & 1\leq n,m\leq 4. \end{cases}$$

In later work we will explain how our methods and results can be used to give a new encryption scheme. We expect that these methods and results can be used in many other settings.

**Acknowledgments**

We thank the referee by your suggestions.

**References**

[1] W. Bosma, H. W. Lenstra, *Complete system of two addition laws for elliptic curves*, Journal of Number Theory, 53 (1995), 229-240.

[2] S. Kamienny, *Torsion points on elliptic curves and q-coefficients of modular forms*, Invent. Math., 109 (1991), 221-229.

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

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

[5] B. Mazur, *Modular curves and Eisenstein ideal*, IHES Publ. Math., 47 (1977), 33-186.

[6] F. Najmam, *Torsion of elliptic curves over quadratic cyclotomic field*, Math. J. Okayama Univ., 53 (2011), 75-82.

[7] F. Najmam, *Complete classification of torsion of elliptic curves over quadratic cyclotomic field*, J. Num. Th., 130 (2010), 1964-1968.

[8] N. K. Sarma, A. Saikia, *Torsion of elliptic curves over quadratic fields of class number 1*, Rocky Mountain Journal of Mathematics, 48 (2018).

[9] M. Virat, *Courbe elliptique sur un annean et applications cryptographiques*, Nice-Sophia Antipolis, (Thèse du Doctoral), 2009.

[10] W. C. Waterhouse, *Introduction to affine group schemes*, Graduate Texts in Mathematics, New York-Berlin: Springer-Verlag, 66 (1979).

Accepted: May 16, 2022