جامعة سيدي محمد بن عبد الله بفاس
UNIVERSITÉ SIDI MOHAMED BEN ABDELLAH DE FES

كلية العلوم والتقنيات فاس
FACULTÉ DES SCIENCES ET TECHNIQUES DE FÈS

N° d'ordre : 68/2023

Centre des Etudes Doctorales : Sciences et Techniques et Sciences Médicales
Formation Doctorale : Sciences de l'Ingénieur, Sciences Physiques, Mathématiques et Informatique.
Discipline : Mathématiques
Spécialité* : Mathématiques fondamentales et appliquées
Laboratoire : Sciences de l'Ingénieur

** voir la liste des spécialités qui correspond à la formation doctorale sur le lien : https://fst-usmba.ac.ma/formations-doctorales/*

Thèse pour l'obtention de DOCTORAT

Sur des problèmes liés aux courbes elliptiques

Préparée par : Mr Cheddour Zakariae

Soutenue le 30/09/2023 devant le jury :

Nom et Prénom	Grade	Etablissement	Qualité
ZIANE M'hammed	PES	FS, Oujda	Président
TADMORI Abdelhamid	PH	FST, Alhoceima	Rapporteur & examinateur
BOUZKOURA Khadija	PH	FS, Ben M'sik, Casa	Rapporteur & examinateur
BOUA Abdelkarim	PH	FP, Taza	Rapporteur & examinateur
ABDELALIM Seddik	PH	FS, Ain Chock- Casa	Examinateur
LALAOUI RHALI Soumia	PES	FP, Taza	Examinateur
MOUHIB Ali	PES	FP, Taza	Directeur de thèse
CHILLALI Abdelhakim	PH	FP, Taza	Co-directeur de thèse

الملخص

هذه الأطروحة تستكشف المبادئ الأساسية للمنحنيات الإهليجية، و توسع قابليتها للاستخدام خارج مجموعة الأعداد النسبية، وتشمل حقول الأعداد الدورانية التربيعية التي تمتد من الحقول المحدودة إلى تمديدات الحقول المحدودة. تبدأ الدراسة بفحص المنحنيات الإهليجية في مجموعة الأعداد النسبية Q حيث توفر أساسًا قويًا في النظرية الأساسية. بناءً على هذه الأسس، تستكشف الأطروحة المنحنيات الإهليجية عبر حقول الأعداد الدورانية التربيعية، مقدمة منظورات وتحديات جديدة. بالإضافة إلى ذلك، توسع البحث نطاق المنحنيات الإهليجية من الحقول المحدودة F_q إلى تمديدات الحقول المحدودة $F_q[\alpha]$. من خلال دراسة هذه التمديدات، تسلط الأطروحة الضوء على العلاقات والخصائص المعقدة التي تظهر في هذه السياقات المزدوجة. وهكذا من خلال هذا البحث، تساهم الأطروحة في فهم أفضل للمنحنيات الإهليجية، وسلوكها، وتطبيقاتها في مجالات رياضية مختلفة مثل التشفير والترميز.

الكلمات المفتاحية:

المنحنى الإهليجية، المجموعات الفرعية الملتوية، حقول الأعداد الدورانية التربيعية، نظام التشفير، التشفير المنزلي الكامل، سلسلة فيبوناتشي، المصفوفات، مشكلة لوغاريتم المنفصل على المنحنى الإهليجي، حقول الأعداد المتعددة التربيعية الوهمية، المنحنيات البيضاوية مفرطة الانحدار، حلقة المجموعة، التشفير بالمفتاح العام، بروتوكول تبادل المفاتيح.

Résumé de la thèse

Cette thèse explore les principes fondamentaux des courbes elliptiques, puis étend leur applicabilité au-delà des nombres rationnels, englobant les corps de nombres cyclotomiques quadratiques et s'étendant des corps finis aux extensions de corps finis. L'étude commence par un examen des courbes elliptiques sur le corps des nombres rationnels Q, fournissant ainsi une base solide dans la théorie de base. En s'appuyant sur ces bases, la thèse se plonge dans l'exploration des courbes elliptiques sur les corps de nombres cyclotomiques quadratiques, introduisant de nouvelles perspectives et des défis. De plus, l'enquête élargit le champ d'application des courbes elliptiques des corps finis F_q aux extensions des corps finis $F_q[\alpha]$. En étudiant ces extensions, la thèse met en lumière les relations complexes et les propriétés qui émergent dans ces contextes augmentés. Grâce à cette recherche, la thèse contribue à une meilleure compréhension des courbes elliptiques, de leur comportement et de leurs applications dans divers domaines mathématiques et cryptographiques.

Mots clés :

Courbe elliptique, sous-groupes de torsion, corps de nombres quadratiques cyclotomiques, crypto système, cryptage entièrement homomorphe, suite de type k-Fibonacci, matrices, problème du logarithme discret sur les courbes elliptiques, corps de nombres multiquadratiques imaginaires, courbes hyper elliptiques, anneau de groupes, cryptographie à clé publique, Diffie-Hellman, protocole d'échange de clés.

Abstract

This thesis explores the fundamental principles of elliptic curves and then extends their applicability beyond the rational numbers, encompassing quadratic cyclotomic number fields and extending from finite fields to finite field extensions. The study begins with an examination of elliptic curves over the rational number field Q, providing a solid foundation in basic theory. Building on this groundwork, the thesis delves into the exploration of elliptic curves over quadratic cyclotomic number fields, introducing new perspectives and challenges. In addition, the investigation extends the scope of elliptic curves from finite fields F_q to extensions of finite fields $F_q[\alpha]$ By studying these extensions, the thesis sheds light on the complex relations and properties that emerge in these augmented contexts. Through this research, the thesis contributes to a better understanding of elliptic curves, their behavior, and applications in various mathematical and cryptographic domains.

Keywords :

Elliptic curve, torsion subgroups, quadratic cyclotomic number fields, cryptosystem, fully homomorphic encryption, k-Fibonacci-like sequence, matrices, elliptic curve discrete logarithm problem, imaginary multiquadratic number fields, hyper elliptic curves, Group ring, public key cryptography, Diffie-Hellman, key exchange protocol.

Publications

- Z. Cheddour, A. Chillali and A. Mouhib, The "Elliptic" matrices and a new kind of cryptography, Bol. Soc. Parana. Mat, V 41, p 1-12, (2022).

- Z. Cheddour, A. Chillali and A. Mouhib, Torsion section of elliptic curves over quadratic extensions of $\mathbb{Q}$, Italian Journal of Pure and Applied Mathematics, (2022).

- Z. Cheddour, A. Chillali and A. Mouhib, Elliptic curve and k-Fibonacci-like sequence, Scientific African, V 20, p 1-11, (2023).

- Z. Cheddour, A. Chillali and A. Mouhib, Elliptic curve over a finite ring, Annals of the University of Craiova, Mathematics and Computer Science Series, (2023).

- Z. Cheddour, A. Chillali and A. Mouhib, Torsion of elliptic curves over imaginary multiquadratic number fields of class number one.(preprint)

- Z. Cheddour, A. Chillali and A. Mouhib, Torsion of elliptic curves over quadratic cyclotomic fields in quadratic extensions of the base field.(preprint)

الملخص

هذه الأطروحة تستكشف المبادئ الأساسية للمنحنيات الإهليليجية، ثم توسع قابليتها للاستخدام خارج مجموعة الأعداد النسبية، وتشمل حقول الأعداد الدويرانية التربيعية وتمتد من الحقول المحدودة إلى تمديدات الحقول المحدودة. تبدأ الدراسة بفحص المنحنيات الإهليليجية في مجموعة الأعداد النسبية $\mathbb{Q}$ ، وتوفر أساسًا قويًا في النظرية الأساسية. بناءً على هذه الأسس، تستكشف الأطروحة المنحنيات الإهليليجية عبر حقول الأعداد االدويرانية التربيعية، مقدمة منظورات وتحديات جديدة. بالإضافة إلى ذلك، توسع البحث نطاق المنحنيات الإهليليجية من الحقول المحدودة $\mathbb{F}q$ إلى تمديدات الحقول المحدودة $\mathbb{F}q[\alpha]$. من خلال دراسة هذه التمديدات، تسلط الأطروحة الضوء على العلاقات والخصائص المعقدة التي تظهر في هذه السياقات المزدوجة. من خلال هذا البحث، تساهم الأطروحة في فهم أفضل للمنحنيات الإهليليجية، وسلوكها، وتطبيقاتها في مجالات رياضية وتشفيرية مختلفة.

Abstract

This thesis explores the fundamental principles of elliptic curves and then extends their applicability beyond the rational numbers, encompassing quadratic cyclotomic number fields and extending from finite fields to finite field extensions. The study begins with an examination of elliptic curves over the rational number field $\mathbb{Q}$, providing a solid foundation in basic theory. Building on this groundwork, the thesis delves into the exploration of elliptic curves over quadratic cyclotomic number fields, introducing new perspectives and challenges. In addition, the investigation extends the scope of elliptic curves from finite fields $\mathbb{F}_q$ to extensions of finite fields $\mathbb{F}_q[\alpha]$. By studying these extensions, the thesis sheds light on the complex relations and properties that emerge in these augmented contexts. Through this research, the thesis contributes to a better understanding of elliptic curves, their behavior, and their applications in various mathematical and cryptographic domains.

R*ésum*é

Cette thèse explore les principes fondamentaux des courbes elliptiques, puis étend leur applicabilité au-delà des nombres rationnels, englobant les corps de nombres cyclotomiques quadratiques et s'étendant des corps finis aux extensions de corps finis. L'étude commence par un examen des courbes elliptiques sur le corps des nombres rationnels $\mathbb{Q}$, fournissant ainsi une base solide dans la théorie de base. En s'appuyant sur ces bases, la thèse se plonge dans l'exploration des courbes elliptiques sur les corps de nombres cyclotomiques quadratiques, introduisant de nouvelles perspectives et des défis. De plus, l'enquête élargit le champ d'application des courbes elliptiques des corps finis $\mathbb{F}_q$ aux extensions des corps finis $\mathbb{F}_q[\alpha]$. En étudiant ces extensions, la thèse met en lumière les relations complexes et les propriétés qui émergent dans ces contextes augmentés. Grâce à cette recherche, la thèse contribue à une meilleure compréhension des courbes elliptiques, de leur comportement et de leurs applications dans divers domaines mathématiques et cryptographiques.

keywords
Elliptic curve, torsion subgroups, quadratic cyclotomic number fields, cryptosystem, fully homomorphic encryption, k-Fibonacci-like sequence, matrices, elliptic curve discrete logarithm problem, imaginary multiquadratic number fields, hyperelliptic curves, Group ring, elliptic curves, public key cryptography, Diffie-Hellman, key exchange protocol.

Contents

Introduction **12**

0.1 General introduction 12

0.2 Some key results 14

0.3 Presentation of the thesis 17

1 Basic theory **20**

1.1 Introduction 20

1.2 Weierstrass form 20

1.3 Elliptic curve and its quadratic twist 21

1.4 Torsion Points 22

1.5 The Group Law 24

1.6 Division polynomials 27

1.7 The Weil Pairing 29

1.8 The modular curve $X_1(n, m)$ 31

2 Torsion of elliptic curves over imaginary multiquadratic number fields of class number one **33**

2.1 Introduction 33

2.2 Imaginary biquadratic number fields of class number one 33

2.2.1 Odd torsion subgroup 34

2.2.2 The group $\mathbb{Z}/11\mathbb{Z}$ 35

2.2.3 The group $\mathbb{Z}/14\mathbb{Z}$ 37

2.2.4 The group $\mathbb{Z}/15\mathbb{Z}$ 38

2.2.5 The group $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/10\mathbb{Z}$ 40

2.2.6 The group $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/12\mathbb{Z}$ . . . 41
2.3 Imaginary triquadratic number fields of class number one . . . 43
2.4 The hyperelleptic curves $X_1(13)$, $X_1(16)$, and $X_1(18)$ . . . 44

3 Torsion of Elliptic curves over quadratic cyclotomic fields in quadratic extensions of the base field 48
3.1 Introduction . . . 48
3.2 Torsion of elliptic curves over $K(\sqrt{d})$ . . . 48
3.3 Biquadratic number field $\mathbb{Q}(\sqrt{e}, \sqrt{d})$ of class number . . . 51
3.4 On the number of $K(\sqrt{d})$ with proper extension of a fixed torsion subgroup over K . . . 58

4 Torsion subgroup of elliptic curves over quadratic extensions of $\mathbb{Q}$ 60
4.1 Introduction . . . 60
4.2 The ring $(\mathbb{Q}[\lambda], +, *)$ . . . 61
4.3 Elliptic curves over $\mathbb{Q}[\lambda]$ . . . 63
4.4 The torsion subgroup of elliptic curves over $\mathbb{Q}[\lambda]$ . . . 65
4.4.1 The group law $\star$ over $E_{a,b}$ . . . 67
4.5 Conclusion . . . 69

5 The "Elliptic" matrices and a new kind of cryptography. 70
5.1 Introduction . . . 70
5.2 Ring of "elliptic" matrices . . . 71
5.2.1 The ring $\aleph$ . . . 71
5.2.2 The "elliptic" matrices . . . 77
5.3 Encryption Schemes using the "elliptic" matrices . . . 78
5.3.1 Cryptographic Protocols . . . 78
5.3.1.1 Public-key encryption . . . 78
5.3.2 Security of this protocol . . . 80
5.3.3 Encryption of message . . . 80
5.3.4 Decryption of message . . . 81
5.4 Numerical example . . . 82

6 Elliptic curve and k-Fibonacci-like sequence **85**

6.1 Introduction . . . 85

6.2 The modified k-Fibonacci-like sequence . . . 86

6.2.1 Binet's formula . . . 87

6.2.2 The best candidate among the points of an elliptic curve . . . 88

6.3 Encryption Scheme . . . 91

6.3.1 Cryptographic Protocols . . . 91

6.3.1.1 Public-key encryption . . . 92

6.3.1.2 The secret k-Fibonacci-like sequence . . . 93

6.3.2 Encryption the message . . . 94

6.3.3 Decryption the message . . . 94

6.3.4 Security of this protocol . . . 94

6.3.4.1 Security . . . 94

6.3.4.2 Discussion and analysis . . . 95

6.4 Numerical example . . . 95

7 Elliptic curve over a finite ring **99**

7.1 Introduction . . . 99

7.2 The ring $(\mathbb{F}_q[\alpha], +, *)$ . . . 100

7.2.1 Inverse elements over $\mathbb{F}_q[\alpha]$ . . . 102

7.3 Elliptic curves over $\mathbb{F}_q[\alpha]$ . . . 103

7.3.1 The elliptic curves E_k . . . 103

7.3.2 The group law $\star$ over $E_{a,b}$ . . . 107

7.4 Applications . . . 108

7.5 Cramer-Shoup Elliptic curve cryptosystem . . . 108

7.5.1 Coding of the elements of G. . . . 108

7.5.2 Cramer-Shoup $E_{a,b}$ cryptosystem Key generation. . . . 109

7.5.2.1 Encryption of message . . . 109

7.5.2.2 Decryption of message . . . 109

7.5.3 Security of this protocol . . . 110

7.5.3.1 Security . . . 110

7.5.4 Discussion and analysis 110
7.5.5 Conclusion 111

Conclusions **112**

Tables **113**

Dedication

To my beloved mother and father, who have always been my unconditional support throughout this academic journey.

Acknowledgements

This research work was carried out within the Laboratory of Engineering Sciences (LSI), of the Polydisciplinary Faculty of Taza.

I would like to express my deepest gratitude to my thesis supervisor, **Ali Mouhib**, and my thesis co-supervisor, **Abdelhakim Chillali**. Their advice, support, and encouragement have been invaluable throughout my journey towards obtaining my Ph.D. They have been excellent mentors, providing me with invaluable ideas and knowledge, pushing me to think critically, and urging me to become a better researcher. They have also been a constant source of inspiration, always leading by example, demonstrating an unwavering commitment to excellence, and fostering an environment of intellectual curiosity and inquiry.

I would also like to thank the members of the jury for their interest in my work and for giving me the benefit of their expertise.

I express my sincere thanks to all the members of the jury for doing me the honor of evaluating my work and for having taken the time to read it carefully.

Abbreviations

$\mathbb{Z}/n\mathbb{Z} = \mathbb{Z}_n$ cyclic group of order n.
EC elliptic curve.
K number field.
$\mathbb{F}_q$ finite field.
$\mathbb{Q}$ rational field.
ζ_n the nth root of unity.
k-FlS k-Fibonacci-like sequence.
FS Fibonacci sequence.
ECC Elliptic Curve Cryptography.
DLP discrete logarithm problem.
ECDLP Elliptic curve discrete logarithm problem.
$E(K)$ the group of K-rational points on E.
$X_1(n, m)$ modular curves and $X_1^d(n, m)$ its d-quadratic twist.
$E(K)_{tors}$ The torsion of E over K.
$\mathbf{L_{d_1,d_2,...,d_n}} = \mathbb{Q}(\sqrt{d_1}, \sqrt{d_2}, ..., \sqrt{d_n})$ imaginary multiquadratic number field of class number one, with d_1, d_2, ..., d_n are free squares.
Ω_k the set of torsion subgroups (up to isomorphism) that appear as $E(K)_{tors}$ for some elliptic curves E/K when K ranges over all number fields of a fixed degree k over $\mathbb{Q}$.
$J(X_1)$ the Jacobian variety of X_1.
$\widehat{\mathbb{Q}[\lambda]}$ the set of integral elements of $\mathbb{Q}[\lambda]$ over $\mathbb{Z}$.
DDH Decisional Diffie-Hellman.
CDH Computational Diffie-Hellman Assumption.

Introduction

0.1 General introduction

The study of elliptic curves is a thriving research area in mathematics today, with some aspects of it dating back much earlier despite significant development in the last 30 years. Elliptic curves are widely used in number theory and related fields such as cryptography, and have been instrumental in solving various Diophantine problems, including the proof of Fermats Last Theorem by Wiles in 1994. By transforming Diophantine equations into elliptic curves, solutions to the original equation correspond to rational points on the curve. Additionally, certain Diophantine problems can be converted into elliptic curves over quadratic cyclotomic number fields. This raises the question of whether there are connections between elliptic curves over $\mathbb{Q}$ and those over quadratic cyclotomic number fields, and whether results from elliptic curves over $\mathbb{Q}$ can be extended to those over quadratic cyclotomic number fields.

A key problem in understanding elliptic curves is classifying their possible torsion structures, particularly when extending the base field. Another related problem is examining elliptic curves defined over cyclotomic quadratic number fields and extending the base field to a quadratic extension. How many cases of proper extension in the corresponding torsion groups can we expect to see?
Let K be a number field. Elliptic curves are typically represented by Weierstrass equations, which take the form

$$y^2 = x^3 + Ax + B$$

where $A, B \in K$. For the curve to have desirable geometric properties, such as no cusps or self-intersections, and to form an Abelian group noted by $E(K)$, the field must not be characteristic 2 or 3, and the curve must be non-singular. Non-singularity means that the discriminant $\Delta = -16\,(4A^3 + 27B^2)$ must be non-zero. Geometrically, these curves can be thought of as taking a variable squared and setting it equal to any cubic polynomial with distinct roots. The set $E(K)$ consists of all points over K that satisfy the equation, along with an additional point at infinity, denoted by O, which gives the projective closure of the curve and acts as the group identity. The group operation is

defined by taking the unique collinear point that intersects the curve and then invert it about the x-axis. When two points are equal, the tangent to that point is used to find the resulting point $P + Q = R$.
If the x-value of two points P and Q on the curve is the same and the negative of their y-values are equal, the resulting point R is the additional point O at infinity.
If P and Q are the same point, we obtain the resulting point R by using the tangent line to P and then inverting the intersection.

The fact that this operation forms an Abelian group can be attributed to the geometric properties of these curves. The symmetry about the x-axis provides inverses, commutativity comes from the adjoining line between two points, and so on. The only non-obvious property is associativity, which can be tediously demonstrated case by case. A geometrical proof can be found in W. Fulton's Algebraic Curves [42].
The group law can also be defined algebraically by the following, given an elliptic curve $y^2 = x^3 + Ax + B$ and points $P = (x_P, y_P)$ and $Q = (x_Q, y_Q)$

$$P + Q = R = (x_R, y_R)\,.$$

If $x_P = x_Q$ and $y_P = -y_Q$ then $R = I$. Otherwise

$$x_R = \lambda^2 - x_P - x_Q$$
$$y_R = \lambda\,(x_P - x_R) - y_P$$

where λ is defined by

$$\lambda = \begin{cases} (y_Q - y_P)\,(x_Q - x_P)^{-1}\,, x_P \neq x_Q, \\ (3x_P^2 + A)\,(2y_P)^{-1}\,, x_P = x_Q, y_P = y_Q. \end{cases}$$

The slope λ of the line is calculated using a simple method for P not equal to Q or $-$Q, and using the derivative in the other cases.

Elliptic curves over finite fields can generate finite Abelian groups. For instance, the curve $y^2 = x^3 + 3x + 2$ over $\mathbb{F}_5$ produces the group:

$$\{(2,1), (1,4), (1,1), (2,4), O\}.$$

Since the order of the group is 5, any non-identity element acts as a generator. Although the exact size of these groups is unknown, Hasse's theorem on elliptic curves provides a bound [88]: if N is the number of points satisfying an elliptic curve over $\mathbb{F}_q$, then

$$|N - (q+1)| \leq 2\sqrt{q}.$$

Schoof's algorithm provides a polynomial-time method for counting points on elliptic curves over finite fields using Hasse's bound, the Chinese remainder theorem, and division

polynomials. Details of the algorithm can be found in Schoof's paper "Counting Points on Elliptic Curves over Finite Fields" [87].

Elliptic curves over finite fields have applications in various algorithms such as cryptography and integer factorization. The groups described above can be used for public key cryptography that relies on their algebraic structure. Computing powers of an element is simple, but taking logarithms is difficult. Several algorithms have been developed for this purpose, including the Elliptic Curve Diffie-Hellman and Elliptic Curve Digital Signature Algorithm. These protocols have gained popularity because of the difficulty of the discrete logarithm problem in comparison to number fields, which allows the use of smaller key sizes than their integer counterparts. The choice of curve and base point is publicly announced, and the selection of these parameters depends on the desired key size.

This thesis is an investigation of those questions and problems. It covers the basic theory of elliptic curves and then extends these from $\mathbb{Q}$ to quadratic cyclotomic fields and from $\mathbb{F}_q$ to $\mathbb{F}_q[\alpha]$.

0.2 Some key results

Consider a number field K and an elliptic curve, E defined over K. The Mordell-Weil theorem [88] tells us that the group of K-rational points on E forms a finitely generated abelian group. In particular, if we denote by $E(K)$ the group of K-rational points on E, we have that

$$E(K) \cong \mathbb{Z}^r \oplus E(K)_{\text{tors}} ,$$

for some finite group $E(K)_{tors}$, called the torsion of E over K and $r = rank(E)$ called the rank of the elliptic curve E. Throughout this thesis, we denote by $\mathbf{L_{d_1,d_2,...,d_n}} = \mathbb{Q}(\sqrt{d_1}, \sqrt{d_2}, ..., \sqrt{d_n})$ an imaginary multiquadratic number field of class number one with $1 \leq n \leq 3$ and by Ω_k the set of torsion subgroups (up to isomorphism) that appear as $E(K)_{tors}$ for some elliptic curves E/K when K ranges over all number fields of a fixed degree k over $\mathbb{Q}$.
Classifying torsion subgroups of elliptic curves over number fields is equivalent to classifying points on the modular curves $X_1(n, m)$ defined over these number fields. Thus, the classification of Ω_k implies the determination of all these modular curves with K-rational points for any number field K of degree k over $\mathbb{Q}$. In particular, Kubert and Mazur determined Ω_1.

Theorem 0.2.1. *(Kubert, [64], Mazur, [69]) Let $E/\mathbb{Q}$ be an elliptic curve. Then $E(\mathbb{Q})_{tors}$ is isomorphic to one of the following 15 groups*

$$\mathbb{Z}/n\mathbb{Z} \text{ for } 1 \leq n \leq 12, \ n \neq 11,$$
$$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z} \text{ for } 1 \leq n \leq 4.$$

Note that, Ω_k has been determined just for some other values of k. In particular, the set Ω_2 has been classified in the following theorem by Kamienny, Kenku and Momose.

Theorem 0.2.2. *(Kamienny, [55], Kenku and Momose, [58]) Let K be a quadratic number field and E be an elliptic curve over K. Then $E(K)_{tors}$ is isomorphic to one of the following 26 groups*

$$\begin{aligned}
&\mathbb{Z}/n\mathbb{Z} \text{ for } 1 \leq n \leq 18,\ n \neq 17,\\
&\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z} \text{ for } 1 \leq n \leq 6,\\
&\mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3n\mathbb{Z} \text{ for } 1 \leq n \leq 2,\\
&\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}.
\end{aligned}$$

Remark 1. *The above result classifies the possible torsion structures as one varies over all quadratic number fields. Hence for a given quadratic number field K, it is in general still unknown which torsion structures occur over K. Najman answered this question in the following theorem for two imaginary quadratic number field of class number one $\mathbb{Q}(i)$ and $\mathbb{Q}(\sqrt{-3})$.*

Theorem 0.2.3. *(Najman, [74, 75]) Let E/K be an elliptic curve, so*

- *If $K = \mathbb{Q}(i)$. Then $E(K)_{tors}$ is either one of the groups from Mazur's Theorem or $\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$.*
- *If $K = \mathbb{Q}(\sqrt{-3})$. Then $E(K)_{tors}$ is either one of the groups from Mazur's Theorem, $\mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}$ or $\mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}$.*

For the rest of the list of imaginary quadratic number fields of class number one, the torsion set has been studied by Sarma and Saikia in [84].
Furthermore, for cubic fields, the set Ω_3 has been classified by Derickx,

Theorem 0.2.4. *(Derickx, [26]) Let $K/\mathbb{Q}$ be a cubic extension and E/K be an elliptic curve. Then $E(K)_{tors}$ is isomorphic to one of the following 26 groups:*

$$\begin{aligned}
&\mathbb{Z}/n\mathbb{Z} \text{ for } n = 1, \ldots, 16, 18, 20, 21,\\
&\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z} \text{ for } n = 1, \ldots, 7.
\end{aligned}$$

In the case of quartic number fields, Jeon, Kim and Park determined in the following theorem which $\mathbb{Z}/n\mathbb{Z} \oplus \mathbb{Z}/m\mathbb{Z}$ groups appear infinitely often as $E(K)_{tors}$ torsion groups when K varies over all quartic number fields and E varies over all elliptic curves.

Theorem 0.2.5. *(Jeon et al, [43]) If K varies over all quartic number fields and E varies over all elliptic curves defined over K, the group structures that appear infinitely often as*

$E(K)_{tors}$ *are exactly the following*

$$\begin{aligned}
&\mathbb{Z}/n\mathbb{Z} \text{ for } n = 1, \ldots, 18, 20, 21, 22, 24,\\
&\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z} \text{ for } n = 1, \ldots, 9,\\
&\mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3n\mathbb{Z} \text{ for } n_3 = 1, 2, 3,\\
&\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4n\mathbb{Z} \text{ for } n = 1, 2,\\
&\mathbb{Z}/5\mathbb{Z} \oplus \mathbb{Z}/5\mathbb{Z},\\
&\mathbb{Z}/6\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}.
\end{aligned}$$

The results of the previous theorems are all in the framework where the elliptic curves are defined over the number fields themselves. We do not have a precise description of the torsion subgroups of an elliptic curve on K, that can appear over an extension of K of degree k. Although Newman's [77] work provided the set of torsion structures that appear as the quadratic twist of a given torsion structure, he also studied the growth of the torsion part of an elliptic curve with full 2-torsion over quadratic cyclotomic fields. A very interesting result is given by Ejder [36], who established the set of torsion subgroups of elliptic curves over quadratic cyclotomic fields in elementary abelian 2-extensions.

In the context of imaginary multiquadratic number fields of class number one. Gauss showed that the class number of $\mathbf{L_d}$, denoted $h(d)$, is equal to 1 for $d \in \{-1, -2, -3, -7, -11, -19, -43, -67, -163\}$ [49]. He conjectured that his list was complete. This conjecture was proven to be true through a series of results, the most significant contributors being Heegner [47], Baker [4] and Stark [92]. This is the complete list of imaginary quadratic number fields of class number one on which Najman and then Sarma was studying elliptic curves. For the imaginary biquadratic number fields of class number one, Brown and Parry have determined a complete list [12]. There are exactly 47 such fields. These are the fields $\mathbf{L_{d_1,d_2}}$ with the following sets $\{d_1, d_2\}$.

$\{-1, 2\}$	$\{2, -3\}$	$\{-3, 5\}$	$\{-7, 5\}$	$\{-11, 17\}$
$\{-1, 3\}$	$\{2, -11\}$	$\{-3, -7\}$	$\{-7, -11\}$	$\{-11, -19\}$
$\{-1, 5\}$	$\{-2, -3\}$	$\{-3, -11\}$	$\{-7, 13\}$	$\{-11, -67\}$
$\{-1, 7\}$	$\{-2, 5\}$	$\{-3, 17\}$	$\{-7, -19\}$	$\{-11, -163\}$
$\{-1, 11\}$	$\{-2, -7\}$	$\{-3, -19\}$	$\{-7, -43\}$	$\{-19, -67\}$
$\{-1, 13\}$	$\{-2, -11\}$	$\{-3, 41\}$	$\{-7, 61\}$	$\{-19, -163\}$
$\{-1, 19\}$	$\{-2, -19\}$	$\{-3, -43\}$	$\{-7, -163\}$	$\{-43, -67\}$
$\{-1, 37\}$	$\{-2, 29\}$	$\{-3, -67\}$	$\{-43, -163\}$	
$\{-1, 43\}$	$\{-2, -43\}$	$\{-3, 89\}$	$\{-67, -163\}$	
$\{-1, 67\}$	$\{-2, -67\}$	$\{-3, -163\}$		
$\{-1, 163\}$				

For the imaginary triquadratic number fields of class number one Feaver [41] showed that

the complete list of these fields are the fields $\mathbf{L_{d_1,d_2,d_3}}$ with the following sets $\{d_1, d_2, d_3\}$.

{-1, 2, 3}	{-1, 3, 5}	{-1, 7, 5}	{-2,-3,-7}	{-3,-7, 5}
{-1, 2, 5}	{-1, 3, 7}	{-1, 7, 13}	{-2,-3, 5}	{-3,-11, 2}
{-1, 2, 11}	{-1, 3, 11}	{-1, 7, 19}	{-2,-7, 5}	{-3,-11,-19}
{-1, 3, 19}				{-3,-11, 17}

Furthermore, he proves that there are no imaginary multiquadratic number fields with $n \geq 4$ that have class number 1.

0.3 Presentation of the thesis

The first chapter of this thesis covers motivating examples, the formal definition of an elliptic curve over a field K, the use of projective space, and the concept of the point at infinity. We introduce the addition over elliptic curves, with geometric and algebraic interpretations. The fact that this addition forms an abelian group from the set of all points of the curve is deduced. This is crucial for the study of other algebraic properties in Chapters 2-7. The chapter explores various properties of elliptic curves, including their quadratic twist and torsion points. The concept of division polynomials is also discussed, which can be used to study the torsion points over the elliptic curve. In addition, the chapter covers Weil Pairing, which is a bilinear pairing on the torsion subgroup of an elliptic curve that has many important cryptographic applications. Finally, the chapter concludes with an introduction to the modular curve $X_1(n, m)$, which is a higher-dimensional generalization of elliptic curves and has been extensively studied in number theory.

In Chapter 2, we study the existence of elliptic curves over an imaginary multiquadratic number field K of class number one whose torsion contains a subgroup isomorphic to one of the following groups: $\mathbb{Z}/11\mathbb{Z}$, $\mathbb{Z}/14\mathbb{Z}$, $\mathbb{Z}/15\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/10\mathbb{Z}$, and $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/12\mathbb{Z}$ over K. We also show that there is no elliptic curve with a torsion group containing a subgroup isomorphic to one of the following groups: $\mathbb{Z}/13\mathbb{Z}$, $\mathbb{Z}/16\mathbb{Z}$ and $\mathbb{Z}/18\mathbb{Z}$ on K respectively, when the Jacobian variety of $X_1(13)$, $X_1(16)$ and $X_1(18)$ is of rank 0 on K respectively.

In Chapter 3, we study the possible torsion groups of an elliptic curve E/K where $K = \mathbb{Q}(i)$ or $\mathbb{Q}(\sqrt{-3})$, when we extend the base field to $K(\sqrt{d})$ where d be square-free. Moreover, we study these elliptic curves on biquadratic number fields $\mathbb{Q}(\sqrt{e}, \sqrt{d})$ of class number one where $e = -1, -3$, and we will give some results on the number of quadratic

extensions of K where the torsion grows.

In Chapter 4, we 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 being a square-free integer. Additionally, we study and determine all possible torsion sections of elliptic curves given by the Weierstrass equation $Y^{*2} * Z = X^{*3} + a * X * Z^2 + b * Z^3$ that can appear on $\mathbb{Q}[\lambda]$. In this context, $\mathbb{Q}[\lambda]$ is endowed with the usual addition and a new product law defined as follows: for $X = x_0 + x_1\lambda$ and $Y = y_0 + y_1\lambda$, where x_0, x_1, y_0 and y_1 are elements of $\mathbb{Q}$, we have the equations

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

and

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

In Chapter 5, attention is shifted to elliptic curves defined over a finite field, the main idea in this Chapter is the design of some public key exchange protocols over a noncommutative ring, in particular over the ring of "elliptic" matrix, whose security is based on $ECDLP$. In other words, we propose a new key exchange protocol based on matrices with the following form $M(B_1, B_2, B_3) = \begin{pmatrix} B_1 & B_2 \\ 0 & B_3 \end{pmatrix}$ called "elliptic" matrices, where B_1, B_2, B_3 are three-dimensional matrices constructed over an elliptic curve whose diagonal elements are in $\mathbb{F}_q$. In addition, we investigate the complexity and security of the key exchange protocol.

In Chapter 6, we introduce a modified k-Fibonacci-like sequence defined over an elliptic curve called the "Elliptic" k-Fibonacci-like sequence and prove Binet's formula for this sequence. We also give a new encryption scheme using this k-Fibonacci-like sequence. Note that as described in [8, 21, 13], Elliptic Curve Cryptography (ECC) is an approach to public-key cryptography that relies on the algebraic structure of elliptic curves over finite fields. Here we use an approach that blends ECC with a k-Fibonacci-like sequence. Thus we obtain a secure protocol based on ECDLP, which is the key factor for elliptic curve coding and adaptive coding.

In Chapter 7, we study elliptic curves defined on the ring $\mathbb{F}_q[\alpha]$, where α is a root of a monic polynomial $P(X)$ of minimal degree denoted by n on $\mathbb{F}_q$. The new advantage of this approach is to obtain a large number of points with a smaller prime p, because we will prove $\sharp E_{a,b}(\mathbb{F}_q[\alpha]) = \prod_{k=0}^{n-1} \sharp E_{\mathbb{F}_q}$ (Corollary 23), in order to reserve memory for the calculations. Moreover, the group law of $E_{a,b}$ is easy to calculate in the forward direction, but difficult in the reverse direction. Thus, in this chapter, we will define a non-standard

way of multiplying $*$ elements on $\mathbb{F}_q[\alpha]$, as follows, for $X = \sum_{k=0}^{n-1} x_k \alpha^k$, $Y = \sum_{k=0}^{n-1} y_k \alpha^k$, we have

$$X * Y = \sum_{k=0}^{n-1} A_k \alpha^k, \ \textit{such that } A_0 = x_0 y_0$$
$$\textit{and } A_k = P_k(X)\varphi_{k-1}(Y) + P_k(Y)\varphi_k(X)$$

where P_k and φ_k are a collection of maps from $\mathbb{F}_q[\alpha]$ to $\mathbb{F}_q$ defined as follows:

$$\begin{array}{ccc} \mathbb{F}_q[\alpha] & \xrightarrow{P_k} & \mathbb{F}_q \\ X & \longmapsto & x_k \end{array} \quad \textit{and} \quad \begin{array}{ccc} \mathbb{F}_q[\alpha] & \xrightarrow{\varphi_k} & \mathbb{F}_q \\ X & \longmapsto & \sum_{j=0}^{k} P_j(X) \end{array}$$

Another objective of this chapter is the application of these results in cryptography. We describe here one of the variants of the ElGamal public key encryption scheme [37], the Cramer-Shoup elliptic curve encryption scheme [24]. Since we are working in the ring $\mathbb{F}_q[\alpha]$, the new scheme that we will define on the elliptic curve $E_{a,b}$ has the advantage of having a low complexity cost compared to the elliptic curves over a field.

The thesis also includes Magma scripts used for computing various examples of elliptic curves.

Chapter 1

Basic theory

1.1 Introduction

The study of elliptic curves in this thesis is related to several topics among which we mention, the division polynomials of the short Weierstrass form, the modular curve $X_1(n, m)$ and the Jacobian variety. Thus, in this section, we have some notions on these subjects.

1.2 Weierstrass form

For most situations in this thesis, we will refer to an elliptic curve, E by an equation of the form

$$y^2 = x^3 + Ax + B,$$

called the Weierstrass equation for E, where A and B are constants. In our case, they are elements of a field or ring, for example, a quadratic (multiquadratic) number field, one of the finite fields $\mathbb{F}_p$ for a prime number p, or one of the finite rings $\mathbb{F}_q[e]$, where e is the root of a monic polynomial of a minimal degree over $\mathbb{F}_q$. In fact, if $A, B \in K$, then we say that E is defined on K. Throughout this thesis, it will be implicitly assumed that E/K denotes an elliptic curve defined on K, with

$$4A^3 + 27B^2 \neq 0.$$

If we want to consider the set of points whose coordinates are in a certain field $K \subset L$, we write $E(L)$. By definition, this set always contains the point at infinity O:

$$E(L) = \{O\} \cup \left\{(x, y) \in L \times L \mid y^2 = x^3 + Ax + B\right\}.$$

For technical reasons, it makes sense to add a point at infinity to an elliptic curve. However, it is easier to think of it as a point (∞, ∞), usually denoted simply as O, located

at the top of the y-axis. For computational purposes, this will be a formal symbol that satisfies certain computational rules. For example, a line is said to pass through O if and only if the line is vertical. The point O may seem a bit artificial, but we will see that its inclusion has very useful consequences. Another convention regarding O. It's not only at the top of the y-axis, but also at the bottom of the y-axis. We imagine that the ends of the y-axis revolve and meet (perhaps somewhere behind the page) at the point O. That may seem a little strange. However, if we work with a field other than the real numbers, e.g. a finite field, there may not be a meaningful ordering of the elements and therefore no distinction between the top and bottom of the y-axis may make sense. In fact, in this situation, the ends of the y-axis have no meaning until we introduce projective coordinates (For more details, see Schmitt et al. [85]). Therefore, it's best to think of O as a formal symbol that satisfies certain properties.

We also mention here a more general equation called "The generalized Weierstrass equation" of the form,

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

where $a_1, \ldots, a_6$ are constants. This form is often used when working with fields of characteristic 2 or 3. If the characteristic of the field is not 2, then we have,

$$\left(y + \frac{a_1x}{2} + \frac{a_3}{2}\right)^2 = x^3 + \left(a_2 + \frac{a_1^2}{4}\right)x^2 + \left(a_4 + \frac{a_1a_3}{2}\right)x + \left(\frac{a_3^2}{4} + a_6\right)$$

which can be written as

$$y_1^2 = x^3 + a_2'x^2 + a_4'x + a_6'$$

with $y_1 = y + a_1x/2 + a_3/2$ and with some constants a_2', a_4', a_6'. If the characteristic is also not 3 , then we can let $x_1 = x + a_2'/3$ and obtain

$$y_1^2 = x_1^3 + Ax_1 + B$$

for some constants A, B.

For the majority of this thesis, we will develop the theory using the short Weierstrass equation.

1.3 Elliptic curve and its quadratic twist

It follows from the previous subsection that an elliptic curve over a number field K can be represented by a Weierstrass equation of the form

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, a_i \in K,$$

and can be reduced to the short form $y^2 = x^3 + Ax + B$ if $\mathrm{char}(K) \neq 2, 3$, by the following transformation

$$(x, y) \longrightarrow (\frac{1}{36}(x - 3a_1^2 - 12a_2), \frac{1}{216}(y - a_1 x - a_3)).$$

The d-quadratic twist of an elliptic curve in short Weierstrass form is defined by the equation

$$E^{(d)} : y^2 = x^3 + d^2 Ax + d^3 B.$$

And we have for a fixed quadratic number field $\mathbb{Q}(\sqrt{d})$ the following result.

Lemma 1. *(Silverman, [88]) Let E be a rational elliptic curve. So,*

(a) $rank(E(\mathbb{Q}(\sqrt{d}))) = rank(E(\mathbb{Q})) + rank(E^d(\mathbb{Q}))$.

(b) For odd number n, $E(\mathbb{Q}(\sqrt{d}))[n] \simeq E(\mathbb{Q})[n] \oplus E^d(\mathbb{Q})[n]$.

1.4 Torsion Points

Torsion points, i.e. those of finite order, play an important role in the study of elliptic curves. We will see this in Chapters 2 and 3 over some number fields and in Chapters 4, 5 and 6 for elliptic curves over finite fields, where all points are torsion points.
In this section we consider first the elementary cases of 2- and 3-torsion and then determine the general situation.

Let E/K be an elliptic curve and $\bar{K}$ = algebraic closure of K. Let n be a positive integer. We are interested in

$$E[n] = \{P \in E(\bar{K}) \mid nP = O\}.$$

We point out that $E[n]$ contains points over $\bar{K}$, not just over K. Since E can be put in the form $y^2 = x^3 + Ax + B$, it is easy to determine $E[2]$. Let

$$y^2 = (x - e_1)(x - e_2)(x - e_3),$$

with $e_1, e_2, e_3 \in \bar{K}$. A point P satisfies $2P = O$ if and only if the tangent line at P is vertical. It is easy to see that this means that $y = 0$, so

$$E[2] = \{O, (e_1, 0), (e_2, 0), (e_3, 0)\}.$$

As an abstract group, this is isomorphic to $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$.

We summarize the preceding discussion as follows.

Proposition 1.4.1. *Let E be an elliptic curve over a field K. If the characteristic of K is not 2 , then*

$$E[2] \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}.$$

Now let's look at $E[3]$. Assume first that the characteristic of K is not 2 or 3 , so that E can be given by the equation $y^2 = x^3 + Ax + B$. A point P satisfies $3P = O$ if and only if $2P = -P$. This means that the x-coordinate of $2P$ equals the x-coordinate of P (the y-coordinates therefore differ in sign, of course, if they were equal, then $2P = P$, hence $P = O$). In equations, this becomes

$$m^2 - 2x = x, \qquad \text{where } m = \frac{3x^2 + A}{2y}.$$

Using the fact that $y^2 = x^3 + Ax + B$, we find that

$$\left(3x^2 + A\right)^2 = 12x\left(x^3 + Ax + B\right).$$

This simplifies to

$$3x^4 + 6Ax^2 + 12Bx - A^2 = 0.$$

The discriminant of this polynomial is $-6912\left(4A^3 + 27B^2\right)^2$, which is nonzero. Therefore the polynomial has no multiple roots. There are 4 distinct values of x (in $\bar{K}$), and each x yields two values of y, so we have eight points of order 3. Since O is also in $E[3]$, we see that $E[3]$ is a group of order 9 in which every element is 3 -torsion. It follows that

$$E[3] \simeq \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}.$$

The general situation is given by the following.

Theorem 1.4.1. *Let E be an elliptic curve over a field K and let n be a positive integer. If the characteristic of K does not divide n, or is 0 , then*

$$E[n] \simeq \mathbb{Z}/n\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z}.$$

If the characteristic of K is $p > 0$ and $p \mid n$, write $n = p^r n'$ with $p \nmid n'$. Then

$$E[n] \simeq \mathbb{Z}/n'\mathbb{Z} \oplus \mathbb{Z}/n'\mathbb{Z} \quad \text{or} \quad \mathbb{Z}/n\mathbb{Z} \oplus \mathbb{Z}/n'\mathbb{Z}$$

Proof.
For more details, see Silverman [88]. □

Definition 1.4.1. *An elliptic curve, E in characteristic p is called ordinary if $E[p] \simeq \mathbb{Z}/p\mathbb{Z}$. It is called supersingular if $E[p] \simeq 0$. Note that the terms "supersingular" and "singular" (as applied to bad points on elliptic curves) are unrelated.*

Let n be a positive integer not divisible by the characteristic of K. Choose a basis $\{P_1, P_2\}$ for $E[n] \simeq \mathbb{Z}/n\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z}$. This means that every element of $E[n]$ is expressible in the form $m_1P_1 + m_2P$ with integers m_1, m_2. Note that m_1, m_2 are uniquely determined mod$n$. Let $\alpha : E(\bar{K}) \to E(\bar{K})$ be a homomorphism. Then α maps $E[n]$ into $E[n]$. Therefore, there are $a, b, c, d \in \mathbb{Z}/n\mathbb{Z}$ such that

$$\alpha(P_1) = aP_1 + cP_2, \quad \alpha(P_2) = bP_1 + dP_2.$$

Therefore each homomorphism $\alpha : E(\bar{K}) \to E(\bar{K})$ is represented by a 2×2 matrix

$$\alpha_n = \begin{pmatrix} a & b \\ c & d \end{pmatrix}.$$

Composition of homomorphisms corresponds to multiplication of the corresponding matrices.

In many cases, the homomorphism α will be taken to be an endomorphism, which means that it is given by rational functions (see Washington [100]). But α can also come from an automorphism of $\bar{K}$ that fixes K. This leads to the important subject of representations of Galois groups (that is, homomorphisms from Galois groups to groups of matrices).

Example 1.4.1. *Let E be the elliptic curve defined over $\mathbb{R}$ by $y^2 = x^3 - 5$, and let $n = 2$. Then*

$$E[2] = \left\{O, \left(5^{1/3}, 0\right), \left(\zeta 5^{1/3}, 0\right), \left(\zeta^2 5^{1/3}, 0\right)\right\},$$

where ζ is a nontrivial cube root of unity. Let

$$P_1 = \left(5^{1/3}, 0\right), \quad P_2 = \left(\zeta 5^{1/3}, 0\right).$$

Then $\{P_1, P_2\}$ is a basis for $E[2]$, and $P_3 = \left(\zeta^2 5^{1/3}, 0\right) = P_1 + P_2$.

Let $\alpha : E(\mathbb{C}) \to E(\mathbb{C})$ be complex conjugation: $\alpha(x, y) = (\bar{x}, \bar{y})$. It is easy to verify that α is a homomorphism. In fact, We have

$$\alpha(P_1) = 1 \cdot P_1 + 0 \cdot P_2, \quad \alpha(P_2) = P_3 = 1 \cdot P_1 + 1 \cdot P_2.$$

Therefore we obtain the matrix $\alpha_2 = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$. Note that $\alpha \circ \alpha$ is the identity, which corresponds to the fact that α_2^2 is the identity matrix mod 2 .

1.5 The Group Law

As we saw in the introduction, we could start with two points, or even one point, on an elliptic curve, and produce another point. We now examine this process in more detail. Start with two points

$$Q_1 = (x_1, y_1), \quad Q_2 = (x_2, y_2)$$

on an elliptic curve, E given by the equation $y^2 = x^3 + Ax + B$. Define a new point Q_3 as follows. Draw the line L through Q_1 and Q_2. We'll see below that L intersects E in a third point Q_3'. Reflect Q_3' across the x-axis (i.e., change the sign of the y-coordinate) to obtain Q_3. We define

$$Q_1 + Q_2 = Q_3.$$

Examples below will show that this is not the same as adding coordinates of the points. It might be better to denote this operation by $Q_1 +_E Q_2$, but we opt for the simpler notation since we will never be adding points by adding coordinates.

Assume first that $Q_1 \neq Q_2$ and that neither point is O. Draw the line L through Q_1 and Q_2. Its slope is

$$m = \frac{y_2 - y_1}{x_2 - x_1}.$$

If $x_1 = x_2$, then L is vertical. We'll treat this case later, so let's assume that $x_1 \neq x_2$. The equation of L is then

$$y = m(x - x_1) + y_1.$$

To find the intersection with E, substitute to get

$$(m(x - x_1) + y_1)^2 = x^3 + Ax + B.$$

This can be rearranged to the form

$$0 = x^3 - m^2x^2 + \cdots$$

The three roots of this cubic correspond to the three points of intersection of L with E. Generally, solving a cubic is not easy, but in the present case we already know two of the roots, namely x_1 and x_2, since Q_1 and Q_2 are points on both L and E. Therefore, we could factor the cubic to obtain the third value of x. But there is an easier way. If we have a cubic polynomial $x^3 + ax^2 + bx + c$ with roots r, s, t, then

$$x^3 + ax^2 + bx + c = (x - r)(x - s)(x - t) = x^3 - (r + s + t)x^2 + \cdots .$$

Therefore,

$$r + s + t = -a.$$

If we know two roots r, s, then we can recover the third as $t = -a - r - s$. In our case, we obtain

$$x = m^2 - x_1 - x_2$$

and

$$y = m(x - x_1) + y_1.$$

Now, reflect across the x-axis to obtain the point $Q_3 = (x_3, y_3)$:

$$x_3 = m^2 - x_1 - x_2, \quad y_3 = m(x_1 - x_3) - y_1.$$

In the case that $x_1 = x_2$ but $y_1 \neq y_2$, the line through Q_1 and Q_2 is a vertical line, which therefore intersects E in O. Reflecting O across the x-axis yields the same point O (this is why we put O at both the top and the bottom of the y-axis). Therefore, in this case $Q_1 + Q_2 = O$.

Now consider the case where $Q_1 = Q_2 = (x_1, y_1)$. When two points on a curve are very close to each other, the line through them approximates a tangent line. Therefore, when the two points coincide, we take the line L through them to be the tangent line. Implicit differentiation allows us to find the slope m of L :

$$2y\frac{dy}{dx} = 3x^2 + A, \quad \text{so} \quad m = \frac{dy}{dx} = \frac{3x_1^2 + A}{2y_1}.$$

If $y_1 = 0$ then the line is vertical and we set $Q_1 + Q_2 = O$, as before. (If $y_1 = 0$, then the numerator $3x_1^2 + A \neq 0$.) Therefore, assume that $y_1 \neq 0$. The equation of L is

$$y = m\,(x - x_1) + y_1,$$

as before. We obtain the cubic equation

$$0 = x^3 - m^2x^2 + \cdots$$

This time, we know only one root, namely x_1, but it is a double root since L is tangent to E at Q_1. Therefore, proceeding as before, we obtain

$$x_3 = m^2 - 2x_1, \quad y_3 = m\,(x_1 - x_3) - y_1.$$

Finally, suppose $Q_2 = O$. The line through Q_1 and O is a vertical line that intersects E in the point Q_1' that is the reflection of Q_1 across the x-axis. When we reflect Q_1' across the x-axis to get $Q_3 = Q_1 + Q_2$, we are back at Q_1. Therefore

$$Q_1 + O = Q_1$$

for all points Q_1 on E. Of course, we extend this to include $O + O = O$. Let's summarize the above discussion:

Let E be an elliptic curve defined by $y^2 = x^3 + Ax + B$. Let $Q_1 = (x_1, y_1)$ and $Q_2 = (x_2, y_2)$ be points on E with $Q_1, Q_2 \neq O$. Define $Q_1 + Q_2 = Q_3 = (x_3, y_3)$ as follows:

(a) If $x_1 \neq x_2$, then

$$x_3 = m^2 - x_1 - x_2, \quad y_3 = m\,(x_1 - x_3) - y_1, \quad \text{where } m = \frac{y_2 - y_1}{x_2 - x_1}.$$

(b) If $x_1 = x_2$ but $y_1 \neq y_2$, then $Q_1 + Q_2 = O$.

(c) If $Q_1 = Q_2$ and $y_1 \neq 0$, then

$$x_3 = m^2 - 2x_1, \quad y_3 = m\,(x_1 - x_3) - y_1, \qquad \text{where } m = \frac{3x_1^2 + A}{2y_1}.$$

(d) If $Q_1 = Q_2$ and $y_1 = 0$, then $Q_1 + Q_2 = O$. Moreover, define

$$Q + O = Q$$

for all points Q on E.

Note that when Q_1 and Q_2 have coordinates in a field L that contains A and B, then $Q_1 + Q_2$ also has coordinates in L. Therefore $E(L)$ is closed under the above addition of points.

Theorem 1.5.1. *The addition of points on an elliptic curve, E satisfies the following properties:*

(a) (Commutativity) $Q_1 + Q_2 = Q_2 + Q_1$ for all Q_1, Q_2 on E.

(b) (Existence of identity) $Q + O = Q$ for all points Q on E.

(c) (Existence of inverses) Given Q on E, there exists Q' on E with $Q + Q' = O$. This point Q' will usually be denoted $-Q$.

(d) (Associativity) $(Q_1 + Q_2) + Q_3 = Q_1 + (Q_2 + Q_3)$ for all Q_1, Q_2, Q_3 on E.

In other words, the points on E form an additive abelian group with O as the identity element.

Proof.
For more details, see [100]. □

1.6 Division polynomials

With the same notations as above, consider the n-division polynomials ψ_n [88] of an elliptic curve with the short Weierstrass form $y^2 = x^3 + Ax + B$, where is defined on

$\mathbb{Z}[x, y, A, B]$ by

$$\begin{aligned}
\psi_0 = 0, \quad \psi_1 = 1, \quad \psi_2 = 2y, \\
\psi_3 = 3x^4 + 6Ax^2 + 12Bx - A^2, \\
\psi_4 = 4y(x^6 + 5Ax^4 + 20Bx^3 - 5A^2x^2 - 4ABx - 8B^2 - A^3), \\
\psi_{2n+1} = \psi_{n+2}\psi_n^3 - \psi_{n-1}\psi_{n+1}^3 \quad \text{for } n \geq 2, \\
\psi_{2n} = (2y)^{-1}\psi_n \left[\psi_{n+2}\psi_{n-1}^2 - \psi_{n-2}\psi_{n+1}^2\right] \quad \text{for } n \geq 3.
\end{aligned}$$

And the polynomials ϕ_n and Ω_n defined as follows,

$$\begin{aligned}
\phi_n &= x\psi_n^2 - \psi_{n+1}\psi_{n-1}, \\
\Omega_n &= (4y)^{-1}(\psi_{n+2}\psi_{n-1}^2 - \psi_{n-2}\psi_{n+1}^2).
\end{aligned}$$

Lemma 2.

(a) *ψ_n is a polynomial in $\mathbb{Z}[x, y^2, A, B]$ when n is odd, and ψ_n is a polynomial in $2y\mathbb{Z}[x, y^2, A, B]$ when n is even.*

(b) *$\phi_n \in \mathbb{Z}[x, y^2, A, B]$ for all n. If n is odd, then $\omega_n \in y\mathbb{Z}[x, y^2, A, B]$. If n is even, then $\omega_n \in \mathbb{Z}[x, y^2, A, B]$.*

Proof.

(a) The lemma is true for $n \leq 4$. Assume, by induction, that it holds for all $n < 2m$. We may assume that $2m > 4$, so $m > 2$. Then $2m > m + 2$, so all polynomials appearing in the definition of ψ_{2m} satisfy the induction assumptions. If m is even, then $\psi_m, \psi_{m+2}, \psi_{m-2}$ are in $2y\mathbb{Z}[x, y^2, A, B]$, from which it follows that ψ_{2m} is in $2y\mathbb{Z}[x, y^2, A, B]$. If m is odd, then ψ_{m-1} and ψ_{m+1} are in $2y\mathbb{Z}[x, y^2, A, B]$, so again we find that ψ_{2m} is in $2y\mathbb{Z}[x, y^2, A, B]$. Therefore, the lemma holds for $n = 2m$. Similarly, it holds for $n = 2m + 1$.

(b) If n is odd, then ψ_{n+1} and ψ_{n-1} are in $y\mathbb{Z}[x, y^2, A, B]$, so their product is in $\mathbb{Z}[x, y^2, A, B]$. Therefore, $\phi_n \in \mathbb{Z}[x, y^2, A, B]$. If n is even, the proof is similar.

□

Therefore, we can establish a connection between the division polynomials and the torsion points according to the following theorem.

Theorem 1.6.1. *Consider the elliptic curve*

$$y^2 = x^3 + Ax + B,$$

defined over a number field K of characteristic not 2. Let $P = (x, y)$ be a point on the curve, and let n be a positive integer. Then,

$$nP = \left(\frac{\phi_n(x)}{\psi_n^2(x)}, \frac{\Omega_n(x,y)}{\psi_n^3(x,y)} \right).$$

The proof can be found in [100].

Lemma 3. *Let E be an elliptic curve. The endomorphism of E given by multiplication by n has degree n^2.*

Proof.
From [Lemma 3.5 [100]], we have that the maximum of the degrees of the numerator and denominator of $\phi_n(x)/\psi_n^2(x)$ is n^2. Therefore, the degree of the endomorphism is n^2 if this rational function is reduced, that is, if $\phi_n(x)$ and $\psi_n^2(x)$ have no common roots. For more details, see [100]. □

1.7 The Weil Pairing

The Weil pairing, which is a bilinear map on the n-torsion of an elliptic curve, is a powerful tool in the study of elliptic curves. Its applications are wide-ranging and significant. In particular, in chapters 2 and 3 of this study, the Weil pairing will be used to eliminate a specific structure that is related to the torsion group of an elliptic curve defined over number fields.

Let E be an elliptic curve over a field K and let n be an integer not divisible by the characteristic of K. Then $E[n] \simeq \mathbb{Z}/n\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z}$. Let

$$\mu_n = \left\{ x \in \bar{K} \mid x^n = 1 \right\}$$

be the group of nth roots of unity in $\bar{K}$. Since the characteristic of K does not divide n, the equation $x^n = 1$ has no multiple roots, hence has n roots in $\bar{K}$. Therefore, μ_n is a cyclic group of order n. Any generator ζ of μ_n is called a primitive nth root of unity. This is equivalent to saying that $\zeta^k = 1$ if and only if n divides k.

Theorem 1.7.1. *Let E be an elliptic curve defined over a field K and let n be a positive integer. Assume that the characteristic of K does not divide n. Then there is a pairing*

$$e_n : E[n] \times E[n] \to \mu_n,$$

called the Weil pairing, that satisfies the following properties:

(a) e_n *is bilinear in each variable. This means that*

$$e_n(S_1 + S_2, T) = e_n(S_1, T)\, e_n(S_2, T)$$

and

$$e_n(S, T_1 + T_2) = e_n(S, T_1)\, e_n(S, T_2)$$

for all $S, S_1, S_2, T, T_1, T_2 \in E[n]$.

(b) e_n *is nondegenerate in each variable. This means that if* $e_n(S, T) = 1$ *for all* $T \in E[n]$ *then* $S = O$ *and also that if* $e_n(S, T) = 1$ *for all* $S \in E[n]$ *then* $T = O$.

(c) $e_n(T, T) = 1$ *for all* $T \in E[n]$.

(d) $e_n(T, S) = e_n(S, T)^{-1}$ *for all* $S, T \in E[n]$.

(e) $e_n(\sigma S, \sigma T) = \sigma(e_n(S, T))$ *for all automorphisms* σ *of* $\bar{K}$ *such that* σ *is the identity map on the coefficients of* E *(if* E *is in Weierstrass form, this means that* $\sigma(A) = A$ *and* $\sigma(B) = B$*).*

(f) $e_n(\alpha(S), \alpha(T)) = e_n(S, T)^{\deg(\alpha)}$ *for all separable endomorphisms* α *of* E*. If the coefficients of* E *lie in a finite field* $\mathbb{F}_q$*, then the statement also holds when* α *is the Frobenius endomorphism* ϕ_q*. (Actually, the statement holds for all endomorphisms* α*, separable or not. For more details, see [38].)*

The proof can be found in [100].

Corollary 1. *Let* $\{T_1, T_2\}$ *be a basis of* $E[n]$*. Then* $e_n(T_1, T_2)$ *is a primitive* n*th root of unity.*

Proof.
Suppose $e_n(T_1, T_2) = \zeta$ with $\zeta^d = 1$. Then $e_n(T_1, dT_2) = 1$.
Also, $e_n(T_2, dT_2) = e_n(T_2, T_2)^d = 1$ (by (1) and (3)). Let $S \in E[n]$. Then $S = aT_1 + bT_2$ for some integers a, b. Therefore,

$$e_n(S, dT_2) = e_n(T_1, dT_2)^a\, e_n(T_2, dT_2)^b = 1.$$

Since this holds for all S, (2) implies that $dT_2 = O$. Since $dT_2 = O$ if and only if $n \mid d$, it follows that ζ is a primitive nth root of unity. □

Corollary 2. *If* $E[n] \subseteq E(K)$*, then* $\mu_n \subset K$.

Remark 2. *Recall that points in* $E[n]$ *are allowed to have coordinates in* $\bar{K}$*. The hypothesis of the corollary is that these points all have coordinates in* K

Proof.
Let σ be any automorphism of $\bar{K}$ such that σ is the identity on K. Let T_1, T_2 be a basis of $E[n]$. Since T_1, T_2 are assumed to have coordinates in K, we have $\sigma T_1 = T_1$ and $\sigma T_2 = T_2$. By (5),

$$\zeta = e_n(T_1, T_2) = e_n(\sigma T_1, \sigma T_2) = \sigma(e_n(T_1, T_2)) = \sigma(\zeta).$$

The fundamental theorem of Galois theory says that if an element $x \in \bar{K}$ is fixed by all such automorphisms σ, then $x \in K$. Therefore, $\zeta \in K$. Since ζ is a primitive nth root of unity by Corollary 1, it follows that $\mu_n \subset K$. (The fundamental theorem of Galois theory only implies that ζ lies in a purely inseparable extension of K. But an nth root of unity generates a separable extension of K when the characteristic does not divide n, so we conclude that $\zeta \in K$). □

Corollary 3. *Let E be an elliptic curve defined over $\mathbb{Q}$. Then $E[n] \nsubseteq E(\mathbb{Q})$ for $n \geq 3$.*

Proof.
If $E[n] \subseteq E(\mathbb{Q})$, then $\mu_n \subset \mathbb{Q}$, which is not the case when $n \geq 3$. □

Remark 3. *When $n = 2$, it is possible to have $E[2] \subseteq E(\mathbb{Q})$. For example, if E is given by $y^2 = x^3 - 4x$, then*

$$E[2] = \{O, (0,0), (2,0), (-2,0)\}.$$

If $n = 3, 4, 5, 6, 7, 8, 9, 10, 12$, there are elliptic curves defined over $\mathbb{Q}$ that have points of order n with rational coordinates. However, the corollary says that it is not possible for all points of order n to have rational coordinates for these n. For more details on the torsion subgroups of elliptic curves on $\mathbb{Q}$ see [50, 67, 76, 88, 100].

1.8 The modular curve $X_1(n, m)$

For positive integers n and m with $n \mid m$, consider the congruence subgroup $\Gamma_1(n, m)$ of SL $(2, \mathbb{Z})$ defined by

$$\Gamma_1(n,m) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix} \bmod (m), n \mid b \right\}.$$

When $n = 1$, we denote the subgroup $\Gamma_1(1, m)$ simply by $\Gamma_1(m)$. Such a subgroup acts on the upper half plane $\mathbb{H}$ by fractional linear transformations, as follows

$$\gamma(\tau) := \frac{a\tau + b}{c\tau + d}, \quad \tau \in \mathbb{H}, \quad \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_1(n, m).$$

Consider $Y_1(n, m)$ (respectively $Y_1(m)$) the set of orbits of this action by $\Gamma_1(n, m)$ (respectively $\Gamma_1(m)$). We can give it the structure of a non-compact Riemann surface. Also,

we can compactify it by adding cusps with appropriate local coordinate charts to obtain a compact Riemann surface denoted by $X_1(n,m)$ (respectively $X_1(m)$).
The curves $X_1(m)$ can be found in [3], and the curves $X_1(2,m)$ in [56]. In the table below, we listed some curves, and their cusps correspond to the torsion points that do not appear on the rational field.

Table 1.1: Modular curves and cusps.

X_1	**Modular curves.** **Cusps.**
$X_1(11)$	$y^2 - y = x^3 - x^2$ $x(x-1)(x^5 - 18x^4 + 35x^3 - 16x^2 - 2x + 1) = 0$
$X_1(13)$	$y^2 = x^6 - 2x^5 + x^4 - 2x^3 + 6x^2 - 4x + 1$ $x(x-1)(x^3 - 4x^2 + x + 1) = 0$
$X_1(14)$	$X_1(14) : y^2 + xy + y = x^3 - x$ $x(x-1)(x+1)(x^3 - 9x^2 - x + 1)(x^3 - 2x^2 - x + 1) = 0$
$X_1(15)$	$y^2 + xy + y = x^3 + x^2$ $x(x+1)(x^4 + 3x^3 + 4x^2 + 2x + 1)(x^4 - 7x^2 - 6x^2 + 2x + 1) = 0$
$X_1(16)$	$y^2 = x(x^2+1)(x^2 + 2x - 1)$ $x(x-1)(x+1)(x^2 - 2x - 1)(x^2 + 2x - 1) = 0$
$X_1(18)$	$y^2 = x^6 + 2x^5 + 5x^4 + 10x^3 + 10x^2 + 4x + 1$ $x(x+1)(x^2 + x + 1)(x^2 - 3x - 1) = 0$
$X_1(2,10)$	$y^2 = x^3 + x^2 - x$ $x(x-1)(x+1)(x^2 + x - 1)(x^2 - 4x - 1) = 0$
$X_1(2,12)$	$y^2 = x^3 - x^2 + x$ $x(x-1)(2x-1)(2x^2 - x + 1)(3x^2 - 3x - 1)(6x^2 - 6x - 1) = 0$

If $X_1(n,m)$ is a hyperelleptic curve, then the K-rational points of $X_1(n,m)$ do not form a group like an elliptic curve, but the K-rational points of its Jacobian $J(K)$ do [99]. Moreover, we have an injective morphism $X_1(n,m) \longrightarrow J$.

Chapter 2

Torsion of elliptic curves over imaginary multiquadratic number fields of class number one

2.1 Introduction

In this chapter [17], we will study the existence of elliptic curves whose torsion groups contain a subgroup isomorphic to one of the following groups: $\mathbb{Z}/11\mathbb{Z}$, $\mathbb{Z}/14\mathbb{Z}$, $\mathbb{Z}/15\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/10\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/12\mathbb{Z}$ over $\mathbf{L_{d_1,d_2,\ldots,d_n}}$. We also show that there are no elliptic curves with torsion group containing a subgroup isomorphic to one of the following groups: $\mathbb{Z}/13\mathbb{Z}$, $\mathbb{Z}/16\mathbb{Z}$ and $\mathbb{Z}/18\mathbb{Z}$ on $\mathbf{L_{d_1,d_2,\ldots,d_n}}$ respectively, when the Jacobian varieties of $X_1(13)$, $X_1(16)$ and $X_1(18)$ is of rank 0 on $\mathbf{L_{d_1,d_2,\ldots,d_n}}$ respectively.
The methods described in this chapter can be used to obtain results of this type, for example, we can use them to find all possible torsion subgroups of a multiquadratic number field. The problem is to determine whether there are any elliptic or hyperelliptic modular curves that have K-rational points that are not cusps.

2.2 Imaginary biquadratic number fields of class number one

To know if there exists a curve with a torsion subgroup $\mathbb{Z}/n\mathbb{Z} \oplus \mathbb{Z}/m\mathbb{Z}$ on $\mathbf{L_{d_1,d_2}}$, we need to determine if $X_1(n,m)$ has a $\mathbf{L_{d_1,d_2}}$-rational point which is not a cusp. In this

section, we will study the existence of elliptic curves whose torsion contains a subgroup isomorphic to one of the following groups: $\mathbb{Z}/11\mathbb{Z}$, $\mathbb{Z}/14\mathbb{Z}$, $\mathbb{Z}/15\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/10\mathbb{Z}$, and $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/12\mathbb{Z}$ over an imaginary biquadratic number field of class number one.

2.2.1 Odd torsion subgroup

In the following lemma, we generalize the result of E. Gonzalez-Jimenez and J. Tornero in [50] on $\mathbb{Q}$.
I would like to point out that the present study of elliptic curves does not involve the application of Lemma 4, Corollary 4 and Lemma 10. This is because, in general, these elliptic curves are not defined on a subfield of the multiquadratic number field. However, we use these mathematical principles specifically for certain modular curves. Specifically, we use them for $X_1(11)$, $X_1(14)$, $X_1(15)$, $X_1(2,10)$, and $X_1(2,12)$.

Lemma 4. *Let $E/\mathbf{L_{d_1}}$ be an elliptic curve. So, there exists a pair of homomorphisms*

$$E(\mathbf{L_{d_1,d_2}}) \xrightarrow{e_1} E(\mathbf{L_{d_1}}) \oplus E^{d_2}(\mathbf{L_{d_1}}) \xrightarrow{e_2} E(\mathbf{L_{d_1,d_2}})$$

such that $e_2 \circ e_1 = [2]$ and $e_1 \circ e_2 = [2] \oplus [2]$ Moreover, $ker(e_1) \subset E(\mathbf{L_{d_1,d_2}})[2]$, $ker(e_2) \subset E(\mathbf{L_{d_1}})[2] \oplus E^{d_2}(\mathbf{L_{d_1}})[2]$ and $coker(e_1)$, $coker(e_2)$ are groups where every non-zero element has order 2.

Proof.
We have $|Gal(\mathbf{L_{d_1,d_2}}/\mathbf{L_{d_1}})| = 2$, let σ be the non-trivial element of $Gal(\mathbf{L_{d_1,d_2}}/\mathbf{L_{d_1}})$ and $\alpha \in \mathbf{L_{d_1,d_2}}$. Set, for any $P = (x, y)$

$$\sigma P = (\sigma(x), \sigma(y)) \text{ and } e(P, \alpha) = (x, \alpha y).$$

Recall the canonical $\mathbf{L_{d_1,d_2}}$-isomorphisms between E and its d_2-twist E^{d_2}

$$E(\mathbf{L_{d_1,d_2}}) \overset{e(.,1/\sqrt{d_2})}{\longrightarrow} E^{d_2}(\mathbf{L_{d_1,d_2}}) \overset{e(.,-\sqrt{d_2})}{\longrightarrow} E(\mathbf{L_{d_1,d_2}})$$

Here we want to construct elements of $E(\mathbf{L_{d_1}})$ and $E^{d_2}(\mathbf{L_{d_1}})$ respectively, from an element P of $E(\mathbf{L_{d_1,d_2}})$.
So, let $P \in E(\mathbf{L_{d_1,d_2}})$. As $\sigma(P + \sigma P) = P + \sigma P$, we have $P + \sigma P \in E(\mathbf{L_{d_1}})$.
Consider now $P - \sigma P$. We have that, $\begin{cases} \sigma(P - \sigma P) = \mathcal{O}, \\ \sigma(P - \sigma P) = -(P - \sigma P) \neq \mathcal{O}. \end{cases}$
It follows that, if $\sigma(P - \sigma P) = \mathcal{O}$, we have $P = \sigma P$ and $P \in E(\mathbf{L_{d_1}})$.
On the other hand if $\sigma(P - \sigma P) = -(P - \sigma P) \neq \mathcal{O}$ we set

$$e(P - \sigma P, 1/\sqrt{d_2}) = (x_{P-\sigma P}, a) \in E^{d_2}(\mathbf{L_{d_1}}),$$

where $a \in \mathbf{L_{d_1}}$ and $a\sqrt{d_2} = y_{P-\sigma P}$.
So we define the homomorphism e_1 as follows

$$\begin{aligned} e_1 : E(\mathbf{L_{d_1,d_2}}) &\longrightarrow E(\mathbf{L_{d_1}}) \oplus E^{d_2}(\mathbf{L_{d_1}}) \\ P &\longmapsto (P + \sigma P, e(P - \sigma P, 1/\sqrt{d_2})) \end{aligned}$$

For e_2, let $M = (a, b) \in E^{d_2}(\mathbf{L_{d_1}})$. Clearly

$$e(M, \sqrt{d_2}) = (a, b\sqrt{d_2}) \in E(\mathbf{L_{d_1,d_2}})$$

and we define then

$$\begin{aligned} e_2 : E(\mathbf{L_{d_1}}) \oplus E^{d_2}(\mathbf{L_{d_1}}) &\longrightarrow E(\mathbf{L_{d_1,d_2}}) \\ (P, M) &\longmapsto P + e(M, \sqrt{d_2}) \end{aligned}$$

which is a homomorphism over $E(\mathbf{L_{d_1}}) \oplus E^{d_2}(\mathbf{L_{d_1}})$.
Since E^{d_2} is an abelian variety over $\mathbf{L_{d_1}}$ and is isomorphic to E over $\mathbf{L_{d_1,d_2}}$, then E^{d_2} is a $\mathbf{L_{d_1,d_2}}/\mathbf{L_{d_1}}$-form of E. Thus, with these applications, it turns out that the results can be deduced from Lemma 1.1 [67]. □

Corollary 4. *Let $E/\mathbf{L_{d_1}}$ be an elliptic curve. If n is an odd integer, then there exists an isomorphism*

$$E(\mathbf{L_{d_1,d_2}})[n] \simeq E(\mathbf{L_{d_1}})[n] \oplus E^{d_2}(\mathbf{L_{d_1}})[n].$$

2.2.2 The group $\mathbb{Z}/11\mathbb{Z}$

Lemma 5. *The fields over which $\mathbb{Z}/11\mathbb{Z}$ appears as a torsion subgroup are $\mathbf{L_{d_1,d_2}}$ with the following sets $\{d_1, d_2\}$.*

$\{-1, 2\}$	$\{2, -3\}$	$\{-3, -7\}$	$\{-7, 5\}$	$\{-11, 17\}$
$\{-1, 7\}$	$\{2, -11\}$	$\{-3, -11\}$	$\{-7, -11\}$	$\{-11, -19\}$
$\{-1, 11\}$	$\{-2, -3\}$	$\{-3, 17\}$	$\{-7, 13\}$	$\{-11, -67\}$
$\{-1, 13\}$	$\{-2, 5\}$	$\{-3, -19\}$	$\{-7, -19\}$	$\{-11, -163\}$
$\{-1, 19\}$	$\{-2, -7\}$	$\{-3, 41\}$	$\{-7, -43\}$	$\{-19, -67\}$
$\{-1, 43\}$	$\{-2, -11\}$	$\{-3, -43\}$	$\{-7, 61\}$	$\{-19, -163\}$
$\{-1, 163\}$	$\{-2, -19\}$		$\{-7, -163\}$	$\{-43, -67\}$
	$\{-2, 29\}$			$\{-43, -163\}$
	$\{-2, -43\}$			
	$\{-2, -67\}$			

Proof.
From [3, 83] we have that an elliptic curve with torsion $\mathbb{Z}/11\mathbb{Z}$ is induced by solutions of the equation

$$X_1(11) : y^2 - y = x^3 - x^2,$$

where the cusps are those points whose x-coordinates satisfy the equation

$$x(x-1)(x^5 - 18x^4 + 35x^3 - 16x^2 - 2x + 1) = 0.$$

We see that $X_1(11)$ is an elliptic curve. The equation for $X_1(11)$ can be reduced to the short Weierstrass form

$$y^2 = x^3 - 432x + 8208.$$

Using the 2-descent, we can calculate the rank of $X_1^d(11)$ over all imaginary biquadratic number fields of class number one. So, as shown in the Table 7.1, the rank of $X_1(11)$ is ≥ 1, with the following sets $\{d_1, d_2\}$.

$\{-1,2\}$	$\{2,-3\}$	$\{-3,-7\}$	$\{-7,5\}$	$\{-11,17\}$
$\{-1,7\}$	$\{2,-11\}$	$\{-3,-11\}$	$\{-7,-11\}$	$\{-11,-19\}$
$\{-1,11\}$	$\{-2,-3\}$	$\{-3,17\}$	$\{-7,13\}$	$\{-11,-67\}$
$\{-1,13\}$	$\{-2,5\}$	$\{-3,-19\}$	$\{-7,-19\}$	$\{-11,-163\}$
$\{-1,19\}$	$\{-2,-7\}$	$\{-3,41\}$	$\{-7,-43\}$	$\{-19,-67\}$
$\{-1,43\}$	$\{-2,-11\}$	$\{-3,-43\}$	$\{-7,61\}$	$\{-19,-163\}$
$\{-1,163\}$	$\{-2,-19\}$		$\{-7,-163\}$	$\{-43,-67\}$
	$\{-2,29\}$			$\{-43,-163\}$
	$\{-2,-43\}$			
	$\{-2,-67\}$			

Hence, $\mathbb{Z}/11\mathbb{Z}$ appears as a torsion subgroup for infinitely many isomorphism classes of elliptic curves over $\mathbf{L_{d_1,d_2}}$ with the previous sets $\{d_1, d_2\}$.
Consider $\{d_1, d_2\}$ in the following cases $\{-1,3\}$, $\{-1,5\}$, $\{-1,37\}$, $\{-1,67\}$, $\{-3,5\}$, $\{-3,-67\}$, $\{-3,89\}$, $\{-3,-163\}$, and $\{-67,-163\}$. In this case, the rank of $X_1(11)$ over $\mathbf{L_{d_1,d_2}}$ is 0.
We then compute the torsion subgroup of $X_1(11)^d$ for $d = \pm 1, \pm 3, \pm 5, -15, \pm 37, \pm 67, 89, -163, 201, -267, 489, 10921$. So, we have $X_1(11)(\mathbb{Q}) \simeq \mathbb{Z}/5\mathbb{Z}$ and $X_1(11)^d \simeq \{O\}$ for the other values of d. Thus, the n-torsion of $X_1(11)(\mathbf{L_{d_1,d_2}})$ for an odd integer n, is determined by the above computation and the Lemma 4. On the other hand $f(x) = x^3 - 432x + 8208$ is irreducible on $\mathbb{Q}$, and thus on all biquadratic extensions of $\mathbb{Q}$. This confirms that $X_1(11)$ has no 2-torsion on $\mathbf{L_{d_1,d_2}}$. It follows that,

$$X_1(11)(\mathbf{L_{d_1,d_2}}) \cong \mathbb{Z}/5\mathbb{Z} \cong \{O, (0,0), (0,1), (1,0), (1,1)\}.$$

We see that all of these torsion points correspond to $x = 0$ or 1, and hence, are cusps of $X_1(11)$. Therefore, $\mathbb{Z}/11\mathbb{Z}$ cannot occur as torsion over the field $\mathbf{L_{d_1,d_2}}$ in the following

cases $\{-1,3\}$, $\{-1,5\}$, $\{-1,37\}$, $\{-1,67\}$, $\{-3,5\}$, $\{-3,-67\}$, $\{-3,89\}$, $\{-3,-163\}$, and $\{-67,-163\}$. □

Corollary 5. *$\mathbb{Z}/22\mathbb{Z}$ cannot occur as torsion over the field $\mathbf{L_{d_1,d_2}}$ in the following cases $\{-1,3\}$, $\{-1,5\}$, $\{-1,37\}$, $\{-1,67\}$, $\{-3,5\}$, $\{-3,-67\}$, $\{-3,89\}$, $\{-3,-163\}$, and $\{-67,-163\}$.*

2.2.3 The group $\mathbb{Z}/14\mathbb{Z}$

Lemma 6. *The fields over which $\mathbb{Z}/14\mathbb{Z}$ appears as a torsion subgroup are $\mathbf{L_{d_1,d_2}}$ with the following sets $\{d_1,d_2\}$.*

$\{-1,3\}$	$\{2,-3\}$	$\{-3,-11\}$	$\{-7,5\}$	$\{-11,17\}$
$\{-1,5\}$	$\{2,-11\}$	$\{-3,17\}$	$\{-7,-11\}$	$\{-11,-19\}$
$\{-1,7\}$	$\{-2,-3\}$	$\{-3,41\}$	$\{-7,13\}$	$\{-11,-67\}$
$\{-1,11\}$	$\{-2,5\}$	$\{-3,-43\}$	$\{-7,61\}$	$\{-11,-163\}$
$\{-1,13\}$	$\{-2,-7\}$	$\{-3,-67\}$	$\{-7,-43\}$	$\{-19,-67\}$
$\{-1,19\}$	$\{-2,-11\}$	$\{-3,89\}$	$\{-7,-163\}$	$\{-19,-163\}$
$\{-1,37\}$	$\{-2,-19\}$	$\{-3,-163\}$		$\{-43,-67\}$
$\{-1,43\}$	$\{-2,29\}$			$\{-43,-163\}$
$\{-1,67\}$	$\{-2,-43\}$			$\{-67,-163\}$
$\{-1,163\}$	$\{-2,-67\}$			

Proof.
From [3, 83] we have that an elliptic curve with torsion $\mathbb{Z}/14\mathbb{Z}$ is induced by solutions of the equation

$$X_1(14) : y^2 + xy + y = x^3 - x,$$

whose cusps satisfy the equation

$$x(x-1)(x+1)(x^3 - 9x^2 - x + 1)(x^3 - 2x^2 - x + 1) = 0.$$

We see that $X_1(14)$ is an elliptic curve, which can be reduced to the short Weierstrass form

$$y^2 = x^3 - 675x + 13662.$$

Using the 2-descent, we can calculate the rank of $X_1^d(14)$ over all imaginary biquadratic number fields of class number one. So, as shown in the Table 7.1, the rank of $X_1(14)$ is

≥ 1, with the following sets $\{d_1, d_2\}$.

$\{-1,3\}$	$\{2,-3\}$	$\{-3,-11\}$	$\{-7,5\}$	$\{-11,17\}$
$\{-1,5\}$	$\{2,-11\}$	$\{-3,17\}$	$\{-7,-11\}$	$\{-11,-19\}$
$\{-1,7\}$	$\{-2,-3\}$	$\{-3,41\}$	$\{-7,13\}$	$\{-11,-67\}$
$\{-1,11\}$	$\{-2,5\}$	$\{-3,-43\}$	$\{-7,61\}$	$\{-11,-163\}$
$\{-1,13\}$	$\{-2,-7\}$	$\{-3,-67\}$	$\{-7,-43\}$	$\{-19,-67\}$
$\{-1,19\}$	$\{-2,-11\}$	$\{-3,89\}$	$\{-7,-163\}$	$\{-19,-163\}$
$\{-1,37\}$	$\{-2,-19\}$	$\{-3,-163\}$		$\{-43,-67\}$
$\{-1,43\}$	$\{-2,29\}$			$\{-43,-163\}$
$\{-1,67\}$	$\{-2,-43\}$			$\{-67,-163\}$
$\{-1,163\}$	$\{-2,-67\}$			

Hence, $\mathbb{Z}/14\mathbb{Z}$ appears as a torsion subgroup for infinitely many isomorphism classes of elliptic curves over $\mathbf{L_{d_1,d_2}}$ with the previous sets $\{d_1, d_2\}$.
Consider $\{d_1, d_2\}$ in the following cases $\{-1,2\}$, $\{-3,5\}$, $\{-3,-7\}$, $\{-3,-19\}$, and $\{-7,-19\}$. In this case, the rank of $X_1(14)$ over $\mathbf{L_{d_1,d_2}}$ is 0. We then compute the torsion subgroup of $X_1^d(14)$ over $\mathbb{Q}$, for $d = -19,-15,-7,-3,\pm 2,\pm 1,\ 5, 21, 57, 133$. So, we have $X_1(14)(\mathbb{Q}) \simeq \mathbb{Z}/6\mathbb{Z}$ and $X_1(14)^d \simeq \mathbb{Z}/2\mathbb{Z}$ for the other values of d. Thus, the n-torsion of $X_1(14)(\mathbf{L_{d_1,d_2}})$ for an odd integer n is determined by the above computation and the Lemma 4. On the other hand, we have the following two equivalents.

- The 2-torsion is contained in $X_1(14)(\mathbb{Q}(\sqrt{d_1}, \sqrt{d_2}))$.
- The 2-division polynomial splits over $\mathbb{Q}(\sqrt{d_1}, \sqrt{d_2})$.

Moreover $x^3 - 675x + 13662$ splits only on $\mathbf{L_{-3,-7}}$. This allows us to see that

$$\begin{cases} X_1(14)(\mathbf{L_{-3,-7}}) \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}, \\ X_1(14)(\mathbf{L_{d_1,d_2}}) \cong \mathbb{Z}/6\mathbb{Z}, \qquad \text{for the other values of } \{d_1, d_2\}. \end{cases}$$

We have that all of these torsion points correspond to $x = -1$, 0 or 1 , and hence, are cusps of $X_1(14)$. Therefore, $\mathbb{Z}/14\mathbb{Z}$ cannot occur as torsion over the field $\mathbf{L_{d_1,d_2}}$ in the following cases $\{-1,2\}$, $\{-3,5\}$, $\{-3,-7\}$, $\{-3,-19\}$, and $\{-7,-19\}$. □

Corollary 6. *$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/14\mathbb{Z}$ cannot occur as torsion over the field $\mathbf{L_{d_1,d_2}}$ in the following cases $\{-1,2\}$, $\{-3,5\}$, $\{-3,-7\}$, $\{-3,-19\}$, and $\{-7,-19\}$. Otherwise it would induce a $\mathbf{L_{d_1,d_2}}$-rational cyclic subgroup of order 14.*

2.2.4 The group $\mathbb{Z}/15\mathbb{Z}$

Lemma 7. *The fields over which $\mathbb{Z}/15\mathbb{Z}$ appears as a torsion subgroup are $\mathbf{L_{d_1,d_2}}$ with the following sets $\{d_1, d_2\}$.*

$\{-1,3\}$	$\{2,-3\}$	$\{-3,-7\}$	$\{-7,5\}$	$\{-11,17\}$
$\{-1,7\}$	$\{2,-11\}$	$\{-3,-11\}$	$\{-7,-11\}$	$\{-11,-19\}$
$\{-1,11\}$	$\{-2,5\}$	$\{-3,17\}$	$\{-7,13\}$	$\{-11,-67\}$
$\{-1,13\}$	$\{-2,-7\}$	$\{-3,-19\}$	$\{-7,-19\}$	$\{-11,-163\}$
$\{-1,37\}$	$\{-2,-11\}$	$\{-3,41\}$	$\{-7,-43\}$	$\{-19,-67\}$
$\{-1,43\}$	$\{-2,29\}$	$\{-3,-43\}$	$\{-7,61\}$	$\{-19,-163\}$
$\{-1,67\}$	$\{-2,-43\}$	$\{-3,-67\}$	$\{-7,-163\}$	$\{-43,-67\}$
$\{-1,163\}$	$\{-2,-67\}$	$\{-3,89\}$		$\{-43,-163\}$
		$\{-3,-163\}$		$\{-67,-163\}$

Proof.
From [3, 83] we have that an elliptic curve with torsion $\mathbb{Z}/15\mathbb{Z}$ is induced by solutions of the equation

$$X_1(15) : y^2 + xy + y = x^3 + x^2,$$

whose cusps satisfy the equation

$$x(x+1)(x^4 + 3x^3 + 4x^2 + 2x + 1)(x^4 - 7x^3 - 6x^2 + 2x + 1) = 0.$$

We see that $X_1(15)$ is an elliptic curve, which can be reduced to the short Weierstrass form

$$y^2 = x^3 - 27x + 8694.$$

Using the 2-descent, we can calculate the rank of $X_1^d(15)$ over all imaginary biquadratic number fields of class number one. So, as shown in the Table 7.1, the rank of $X_1(15)$ is ≥ 1, with the following sets $\{d_1, d_2\}$.

$\{-1,3\}$	$\{2,-3\}$	$\{-3,-7\}$	$\{-7,5\}$	$\{-11,17\}$
$\{-1,7\}$	$\{2,-11\}$	$\{-3,-11\}$	$\{-7,-11\}$	$\{-11,-19\}$
$\{-1,11\}$	$\{-2,5\}$	$\{-3,17\}$	$\{-7,13\}$	$\{-11,-67\}$
$\{-1,13\}$	$\{-2,-7\}$	$\{-3,-19\}$	$\{-7,-19\}$	$\{-11,-163\}$
$\{-1,37\}$	$\{-2,-11\}$	$\{-3,41\}$	$\{-7,-43\}$	$\{-19,-67\}$
$\{-1,43\}$	$\{-2,29\}$	$\{-3,-43\}$	$\{-7,61\}$	$\{-19,-163\}$
$\{-1,67\}$	$\{-2,-43\}$	$\{-3,-67\}$	$\{-7,-163\}$	$\{-43,-67\}$
$\{-1,163\}$	$\{-2,-67\}$	$\{-3,89\}$		$\{-43,-163\}$
		$\{-3,-163\}$		$\{-67,-163\}$

Hence, $\mathbb{Z}/15\mathbb{Z}$ appears as a torsion subgroup for infinitely many isomorphism classes of elliptic curves over $\mathbf{L_{d_1,d_2}}$ with the previous sets $\{d_1, d_2\}$.
Consider $\{d_1, d_2\}$ in the following cases $\{-1,2\}$, $\{-1,5\}$, $\{-1,19\}$, $\{-2,-3\}$, $\{-2,19\}$,

and $\{-3,5\}$. In this cases, the rank of $X_1(15)$ over $\mathbf{L_{d_1,d_2}}$ is 0. We then compute the torsion subgroup of $X_1^d(15)$ over $\mathbb{Q}$, for $d = -38, \pm 19, -15, \pm 5, -3, \pm 2, \pm 1, 6$. So, we have $X_1^d(15)(\mathbb{Q}) \simeq \mathbb{Z}/4\mathbb{Z}$ for $d = -15$ or 1 and $X_1(15)^d \simeq \mathbb{Z}/2\mathbb{Z}$ for the other values of d. Thus, the n-torsion of $X_1(15)(\mathbf{L_{d_1,d_2}})$ for an odd integer n is determined by the above computation and the Lemma 4. For the 2-torsion, we find that the 2-division polynomial is splits only over $\mathbf{L_{-3,5}}$. This shows that

$$\begin{cases} X_1(15)(\mathbf{L_{-3,5}}) \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}, \\ X_1(15)(\mathbf{L_{d_1,d_2}}) \cong \mathbb{Z}/4\mathbb{Z}, & \text{for the other values of } \{d_1, d_2\}. \end{cases}$$

We have that all of these torsion points correspond to $x = 0$ or -1 , and hence, are cusps of $X_1(15)$. Therefore, $\mathbb{Z}/15\mathbb{Z}$ cannot occur as torsion over the fields $\mathbf{L_{d_1,d_2}}$ in the following cases $\{-1,2\}$, $\{-1,5\}$, $\{-1,19\}$, $\{-2,-3\}$, $\{-2,19\}$, and $\{-3,5\}$. □

2.2.5 The group $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/10\mathbb{Z}$

Lemma 8. *The fields over which $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/10\mathbb{Z}$ appears as a torsion subgroup are $\mathbf{L_{d_1,d_2}}$ are with the following sets $\{d_1, d_2\}$.*

$\{-1,2\}$	$\{2,-11\}$	$\{-3,5\}$	$\{-7,5\}$	$\{-11,17\}$
$\{-1,11\}$	$\{-2,-3\}$	$\{-7,-11\}$	$\{-7,13\}$	$\{-11,-19\}$
$\{-1,13\}$	$\{-2,5\}$	$\{-3,-11\}$	$\{-7,-19\}$	$\{-11,-67\}$
$\{-1,19\}$	$\{-2,-7\}$	$\{-3,17\}$	$\{-7,61\}$	$\{-11,-163\}$
$\{-1,37\}$	$\{-2,-11\}$	$\{-3,-19\}$		$\{-19,-67\}$
	$\{-2,-19\}$	$\{-3,41\}$		$\{-19,-163\}$
	$\{-2,29\}$	$\{-3,89\}$		
	$\{-2,-43\}$			
	$\{-2,-67\}$			

Proof.
From [3, 83] we have that an elliptic curve with torsion $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/10\mathbb{Z}$ is induced by solutions of the equation

$$X_1(2,10) : y^2 = x^3 + x^2 - x,$$

whose cusps satisfy the equation

$$x(x^2-1)(x^2+x-1)(x^2-4x-1) = 0.$$

We see that $X_1(2,10)$ is an elliptic curve. So, using 2-descent we compute the rank of $X_1^d(2,10)$ over all imaginary biquadratic number fields of class number one.

So, as shown in the Table 7.1, the rank of $X_1^d(2,10)$ is ≥ 1, with the following sets $\{d_1, d_2\}$.

$\{-1,2\}$	$\{2,-11\}$	$\{-3,5\}$	$\{-7,5\}$	$\{-11,17\}$
$\{-1,11\}$	$\{-2,-3\}$	$\{-7,-11\}$	$\{-7,13\}$	$\{-11,-19\}$
$\{-1,13\}$	$\{-2,5\}$	$\{-3,-11\}$	$\{-7,-19\}$	$\{-11,-67\}$
$\{-1,19\}$	$\{-2,-7\}$	$\{-3,17\}$	$\{-7,61\}$	$\{-11,-163\}$
$\{-1,37\}$	$\{-2,-11\}$	$\{-3,-19\}$		$\{-19,-67\}$
	$\{-2,-19\}$	$\{-3,41\}$		$\{-19,-163\}$
	$\{-2,29\}$	$\{-3,89\}$		
	$\{-2,-43\}$			
	$\{-2,-67\}$			

Hence, $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/10\mathbb{Z}$ appears as a torsion subgroup for infinitely many isomorphism classes of elliptic curves over $\mathbf{L_{d_1,d_2}}$ with the previous sets $\{d_1, d_2\}$.
Consider $\{d_1, d_2\}$ in the following cases $\{-1,3\}$, $\{-1,5\}$, $\{-1,7\}$, $\{-1,43\}$, $\{-1,67\}$, $\{-1,163\}$, $\{2,-3\}$, $\{-3,-7\}$, $\{-3,-43\}$, $\{-3,-67\}$, $\{-3,-163\}$, $\{-7,-43\}$, $\{-7,-163\}$, $\{-43,-67\}$, $\{-43,-163\}$, and $\{-67,-163\}$. In this cases, the rank of $X_1(2,10)$ over $\mathbf{L_{d_1,d_2}}$ is 0. We then compute the torsion subgroup of $X_1^d(2,10)$ over $\mathbb{Q}$, for $d = \pm 163, \pm 67, \pm 43, \pm 7, -6, \pm 5, \pm 3, \pm 1, 2, 18, 129, 201, 301, 489, 1141, 2881, 7009, 10921$. So, we have $X_1(2,10)(\mathbb{Q}) \simeq \mathbb{Z}/6\mathbb{Z}$ and $X_1(2,10)^d \simeq \mathbb{Z}/2\mathbb{Z}$ for the other values of d. Thus, the n-torsion of $X_1(2,10)(\mathbf{L_{d_1,d_2}})$ for an odd integer n is determined by the above computation and the Lemma 4. For the 2-torsion, we find that the 2-division polynomial splits only over $\mathbf{L_{-1,5}}$. This shows that

$$\begin{cases} X_1(2,10)(\mathbf{L_{-1,5}}) \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}, \\ X_1(2,10)(\mathbf{L_{d_1,d_2}}) \cong \mathbb{Z}/6\mathbb{Z}, \qquad \text{for the other values of } \{d_1, d_2\}. \end{cases}$$

We have that all of the points in $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}$ correspond to $x = -1$, 0 or 1 , hence they are cusps of $X_1(2,10)$. Therefore, $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/10\mathbb{Z}$ cannot occur as torsion over the field $\mathbf{L_{d_1,d_2}}$ with the previous sets $\{d_1, d_2\}$. □

2.2.6 The group $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/12\mathbb{Z}$

Lemma 9. *The fields over which $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/12\mathbb{Z}$ appears as a torsion subgroup are $\mathbf{L_{d_1,d_2}}$ are with the following sets $\{d_1, d_2\}$.*

$\{-1,5\}$	$\{2,-11\}$	$\{-3,5\}$	$\{-7,13\}$	$\{-11,17\}$
$\{-1,11\}$	$\{-2,-3\}$	$\{-3,-7\}$	$\{-7,-19\}$	$\{-11,-19\}$
$\{-1,13\}$	$\{-2,5\}$	$\{-3,17\}$	$\{-7,-43\}$	$\{-11,-67\}$
$\{-1,19\}$	$\{-2,29\}$	$\{-3,-19\}$	$\{-7,61\}$	$\{-11,-163\}$
$\{-1,37\}$	$\{-2,-43\}$	$\{-3,41\}$	$\{-7,-163\}$	$\{-19,-67\}$
$\{-1,43\}$	$\{-2,-11\}$	$\{-3,-43\}$		$\{-19,-163\}$
$\{-1,67\}$	$\{-2,-67\}$	$\{-3,-67\}$		$\{-43,-67\}$
$\{-1,163\}$		$\{-3,89\}$		$\{-43,-163\}$
		$\{-3,-163\}$		$\{-67,-163\}$

Proof.
From [3, 83] we have that an elliptic curve with torsion $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/12\mathbb{Z}$ is induced by solutions of the equation

$$X_1(2,12) : y^2 = x^3 - x^2 + x,$$

whose cusps satisfy the equation

$$x(x-1)(2x-1)(2x^2-x+1)(3x^2-3x-1)(6x^2-6x-1) = 0.$$

We have that $X_1(2,12)$ is an elliptic curve. So, in the same way in the proof of the previous lemma, we find that the rank of $X_1^d(2,12)$ is ≥ 1, with the following sets $\{d_1, d_2\}$.

$\{-1,5\}$	$\{2,-11\}$	$\{-3,5\}$	$\{-7,13\}$	$\{-11,17\}$
$\{-1,11\}$	$\{-2,-3\}$	$\{-3,-7\}$	$\{-7,-19\}$	$\{-11,-19\}$
$\{-1,13\}$	$\{-2,5\}$	$\{-3,17\}$	$\{-7,-43\}$	$\{-11,-67\}$
$\{-1,19\}$	$\{-2,29\}$	$\{-3,-19\}$	$\{-7,61\}$	$\{-11,-163\}$
$\{-1,37\}$	$\{-2,-43\}$	$\{-3,41\}$	$\{-7,-163\}$	$\{-19,-67\}$
$\{-1,43\}$	$\{-2,-11\}$	$\{-3,-43\}$		$\{-19,-163\}$
$\{-1,67\}$	$\{-2,-67\}$	$\{-3,-67\}$		$\{-43,-67\}$
$\{-1,163\}$		$\{-3,89\}$		$\{-43,-163\}$
		$\{-3,-163\}$		$\{-67,-163\}$

Hence, $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/12\mathbb{Z}$ appears as a torsion subgroup for infinitely many isomorphism classes of elliptic curves over $\mathbf{L_{d_1,d_2}}$ with the previous sets $\{d_1, d_2\}$.
Consider $\{d_1, d_2\}$ in the following cases $\{-1,2\}$, $\{-1,3\}$, $\{-1,7\}$, $\{2,-3\}$, $\{-2,-7\}$, $\{-2,-19\}$, $\{-3,-11\}$, $\{-7,5\}$, and $\{-7,-11\}$. In this case, the rank of $X_1(2,12)$ over $\mathbf{L_{d_1,d_2}}$ is 0. We then compute the torsion subgroup of $X_1^d(2,12)$ over $\mathbb{Q}$, for
$d = -35, -19, -11, \pm 7, -6, \pm 3, \pm 2, \pm 1, 5, 14, 28, 33, 77$.
So, we have $X_1(2,12)^d(\mathbb{Q}) \simeq \mathbb{Z}/4\mathbb{Z}$ for $d = \pm 1$ and $X_1(2,12)^d \simeq \mathbb{Z}/2\mathbb{Z}$ for the other

values of d. Thus, the n-torsion of $X_1(2,12)(\mathbf{L_{d_1,d_2}})$ for an odd integer n is determined by the above computation and the Lemma 4. For the 2-torsion, we find that the 2-division polynomial splits only over $\mathbf{L_{d_1,d_2}}$ in the following cases $\{-1,3\}$, $\{2,-3\}$, and $\{-3,-11\}$. This shows that

$$\begin{cases} X_1(2,12)(\mathbf{L_{d_1,d_2}}) \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}, & \text{for } \{-1,3\},\ \{2,-3\}, \text{ and } \{-3,-11\} \\ X_1(2,12)(\mathbf{L_{d_1,d_2}}) \cong \mathbb{Z}/4\mathbb{Z}, & \text{for the other values of } \{d_1,d_2\}. \end{cases}$$

We have that all the points in $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$ are cusps of $X_1(2,12)$.
Therefore, $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/12\mathbb{Z}$ cannot occur as torsion over the field $\mathbf{L_{d_1,d_2}}$ with the previous sets $\{d_1,d_2\}$. □

2.3 Imaginary triquadratic number fields of class number one

In this section, we will conduct our study on imaginary triquadratic fields of class number one. To do so, we use the following lemma. So, let $\mathbf{L_{d_1,d_2,d_3}}$ be an imaginary triquadratic fields of class number one with the following sets $\{d_1,d_2,d_3\}$

$\{-1,2,3\}$	$\{-1,3,5\}$	$\{-1,7,5\}$	$\{-2,-3,-7\}$	$\{-3,-7,5\}$
$\{-1,2,5\}$	$\{-1,3,7\}$	$\{-1,7,13\}$	$\{-2,-3,5\}$	$\{-3,-11,2\}$
$\{-1,2,11\}$	$\{-1,3,11\}$	$\{-1,7,19\}$	$\{-2,-7,5\}$	$\{-3,-11,-19\}$
$\{-1,3,19\}$				$\{-3,-11,17\}$

Lemma 10. *Let $E/\mathbf{L_{d_1,d_2}}$ be an elliptic curve. If n is an odd integer, then there exists an isomorphism*

$$E(\mathbf{L_{d_1,d_2,d_3}})[n] \simeq E(\mathbf{L_{d_1,d_2}})[n] \oplus E^{d_3}(\mathbf{L_{d_1,d_2}})[n].$$

Proof.
In the same way as we already do in the proof of the Lemma 4. □

Lemma 11. *For any imaginary triquadratic number fields of class number one with two exceptions, there exists an elliptic curve whose torsion is isomorphic to one of the following groups: $\mathbb{Z}/11\mathbb{Z}$, $\mathbb{Z}/14\mathbb{Z}$, $\mathbb{Z}/15\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/10\mathbb{Z}$ or $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/12\mathbb{Z}$.*

- $\mathbb{Z}/11\mathbb{Z}$ *cannot appear as torsion subgroups over* $\mathbf{L_{-1,3,5}}$.
- $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/10\mathbb{Z}$ *cannot appear as torsion subgroups over* $\mathbf{L_{-1,3,7}}$.

Proof.
From the results obtained in section 2, we can conclude that for any imaginary triquadratic number field of class number one except for the two following cases $\mathbf{L_{-1,3,5}}$ and $\mathbf{L_{-1,3,7}}$. There exists an elliptic curve whose torsion is isomorphic to one of the following groups: $\mathbb{Z}/11\mathbb{Z}$, $\mathbb{Z}/14\mathbb{Z}$, $\mathbb{Z}/15\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/10\mathbb{Z}$, and $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/12\mathbb{Z}$.
The first case
We have the rank of $X_1(11)$ over $\mathbf{L_{-1,3,5}}$ is 0, and the torsion subgroup of $X_1(11)^d$ for $d = -1, \pm 3, \pm 5, \pm 15$ is trivial, and $X_1(11)(\mathbb{Q}) \simeq \mathbb{Z}/5\mathbb{Z}$. Thus, the n-torsion of $X_1(11)(\mathbf{L_{-1,3,5}})$ for an odd integer n is determined by the above computation and the Lemma 10. On the other hand $f(x) = x^3 - 432x + 8208$ is irreducible on $\mathbb{Q}$, and thus on all imaginary multiquadratic extensions of $\mathbb{Q}$. This confirms that $X_1(11)$ has no 2-torsion on $\mathbf{L_{-1,3,5}}$. It follows that,

$$X_1(11)(\mathbf{L_{-1,3,5}}) \cong \mathbb{Z}/5\mathbb{Z} \cong \{O, (0,0), (0,1), (1,0), (1,1)\}.$$

We see that all of these torsion points correspond to $x = 0$ or 1, hence they are cusps of $X_1(11)$. Therefore, $\mathbb{Z}/11\mathbb{Z}$ cannot occur as torsion over the field $\mathbf{L_{-1,3,5}}$.
The second case
We have the rank of $X_1(2,10)$ over $\mathbf{L_{-1,3,7}}$ is 0, the torsion subgroup of $X_1(2,10)^d$ for $d = -1, \pm 3, \pm 7, \pm 21$ is trivial, and $X_1(2,10)(\mathbb{Q}) \simeq \mathbb{Z}/6\mathbb{Z}$. Thus, the n-torsion of $X_1(2,10)(\mathbf{L_{-1,3,7}})$ for an odd integer n is determined by the above computation and the Lemma 10.

On the other hand $f(x) = x^3 + x^2 - x$ is irreducible over $\mathbf{L_{-1,3,7}}$, This ensures that $X_1(2,10)$ does not have 2-torsion over $\mathbf{L_{-1,3,7}}$. As a result,

$$X_1(2,10)(\mathbf{L_{-1,3,7}}) \cong \mathbb{Z}/6\mathbb{Z}.$$

All of the points in $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}$ correspond to $x = -1$, 0 or 1, and hence, are cusps of $X_1(2,10)$. Therefore, $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/10\mathbb{Z}$ cannot occur as torsion over the field $\mathbf{L_{-1,3,7}}$. □

2.4 The hyperelleptic curves $X_1(13)$, $X_1(16)$, and $X_1(18)$

In this section, we study the hyperelliptic curves $X_1(13)$, $X_1(16)$, and $X_1(18)$ over imaginary multiquadratic number fields of class one. We focus on fields where the rank of their Jacobian variety is zero.

Theorem 2.4.1. *Let $\mathbf{L_{d_1,d_2,\ldots,d_n}}$ with $2 \leq n \leq 3$, be an imaginary multiquadratic number field of class number one.*

- *If $J_1(13)$ has rank 0 over $\mathbf{L_{d_1,d_2,\ldots,d_n}}$, then $\mathbb{Z}/13\mathbb{Z}$ cannot appear as torsion subgroups over any of these fields.*

- *If* $J_1(16)$ *has rank* 0 *over* $\mathbf{L_{d_1,d_2,\ldots,d_n}}$*, then* $\mathbb{Z}/16\mathbb{Z}$ *cannot appear as torsion subgroups over any of these fields.*

- *If* $J_1(18)$ *has rank* 0 *over* $\mathbf{L_{d_1,d_2,\ldots,d_n}}$*, then* $\mathbb{Z}/18\mathbb{Z}$ *cannot appear as torsion subgroups over any of these fields.*

Proof.

The case $\mathbb{Z}/13\mathbb{Z}$**.**
We have that $X_1(13)$ is a hyperelliptic curve. So we will study the torsion points of $J_1(13)$ over $\mathbf{L_{d_1,d_2,\ldots,d_n}}$.
Since the Jacobian is an abelian variety [99], it follows that for a prime p of good reduction over $\mathbb{Q}(\sqrt{d})$, we have

- If $d \equiv 1 \ mod\ 4$ and $(\frac{d}{p}) = 1$, then the prime-to-p part of $J_1(13)(\mathbb{Q}(\sqrt{d}))_{\text{tors}}$ injects into $J_1(13)(\mathbb{F}_p)$.

- If $d \equiv 1 \ mod\ 4$ and $(\frac{d}{p}) = -1$, then the prime-to-p part of $J_1(13)(\mathbb{Q}(\sqrt{d}))_{\text{tors}}$ injects into $J_1(13)(\mathbb{F}_p(\sqrt{d})) \simeq J_1(13)(\mathbb{F}_{p^2})$.

- If $d \equiv 2,\ 3 \ mod\ 4$ and $(\frac{4d}{p}) = 1$, then the prime-to-p part of $J_1(13)(\mathbb{Q}(\sqrt{d}))_{\text{tors}}$ injects into $J_1(13)(\mathbb{F}_p)$.

- If $d \equiv 2, 3 \ mod\ 4$ and $(\frac{4d}{p}) = -1$, then the prime-to-p part of $J_1(13)(\mathbb{Q}(\sqrt{d}))_{\text{tors}}$ injects into $J_1(13)(\mathbb{F}_p(\sqrt{d})) \simeq J_1(13)(\mathbb{F}_{p^2})$.

On the other hand, the discriminant of $X_1(13)$ is $-2^{12}.13^2$, so 2 and 13 are the only rational primes with bad reduction.
We will discuss the cardinal of the Jacobian variety of $X_1(13)$ on imaginary quadratic fields $\mathbb{Q}(\sqrt{d_1})$ in the following cases $d_1 = -1, -2, -3, -7, -11, -19 - 43, -67$. So, when $d_1 = -1$, we have 3 is inert and 5 splits into $\mathbb{Q}(i)$. Thus, the prime-to-3 part and the prime-to-5 part of $J_1(13)(\mathbb{Q}(i))_{\text{tors}}$ are injected respectively into $J_1(13)(\mathbb{F}_3(i)) \simeq J_1(13)(\mathbb{F}_9)$ and $J_1(13)(\mathbb{F}_5)$. We see that $\sharp J_1(\mathbb{Q}(i)) \leq 19$. Therefore, it follows that $J_1(\mathbb{Q}(i)) = J_1(\mathbb{Q}) \simeq \mathbb{Z}/19\mathbb{Z}$.
As $J_1^d(\mathbb{Q}(i)) \simeq \{O\}$ for $d = 2, 3,\ 5, 7, 11,\ 13, 19,\ 37, 43,\ 67, 163$ and $J_1(\mathbb{Q})$ is generated by the cusps of $X_1(13)$, we have for an odd number n, the n-part of $J_1(\mathbf{L_{-1,d}})$ for
$d = 2, 3,\ 5, 7, 11,\ 13, 19,\ 37, 43,\ 67, 163$ is generated by the cusps of $X_1(13)$.
On the other hand, we have the 2-division polynomial of $X_1(13)$ is irreducible over $\mathbf{L_{-1,d}}$

for $d = 2, 3, 5, 7, 11, 13, 19, 37, 43, 67, 163$.
Similarly for the other values of d_1. So, as a conclusion, $\mathbb{Z}/13\mathbb{Z}$ cannot appear as torsion subgroups over any of these fields.

The case $\mathbb{Z}/16\mathbb{Z}$.
Similarly, we will discuss the cardinal of the Jacobian variety of $X_1(16)$ on imaginary quadratic fields $\mathbb{Q}(\sqrt{d_1})$ in the following cases $d_1 = -1, -2, -3, -7, -11, -19 - 43, -67$. So, we will do this proof for $d_1 = -3$, and similarly for the other values.
Since the discriminant of $X_1(16)$ is -2^{19}, so 2 is the only rational prime with bad reduction. We have 5 is inert and 7 split into $\mathbb{Q}(\sqrt{-3})$. Thus, the prime-to-5 part and the prime-to-7 part of $J_1(16)(\mathbb{Q}(\sqrt{-3}))_{\text{tors}}$ are injected respectively into $J_1(16)(\mathbb{F}_5(\sqrt{-3})) \simeq J_1(16)(\mathbb{F}_{25})$ and $J_1(16)(\mathbb{F}_7)$. We see that $\sharp J_1(16)(\mathbb{Q}(\sqrt{-3})) \leq 40$. Therefore, it follows that $J_1(\mathbb{Q}(\sqrt{-3})) \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/10\mathbb{Z}$ or $J_1(\mathbb{Q}(\sqrt{-3})) \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/10\mathbb{Z}$.
As $J_1(16)(\mathbb{Q})$ is generated by the cusps of $X_1(16)$, and we have for an odd prime number p $J_1^d(16)(\mathbb{Q}(\sqrt{-3}))[p] \simeq \{O\}$ for $d = 2, -7, -11, -19, -43, -67, 89$, thus the p-part of $J_1(16)(\mathbf{L_{-3,d}})$ for $d = 2, -7, -11, -19, -43, -67, 89$ are generated by the cusps of $X_1(16)$. On the other hand, we have the 2-division polynomial of $X_1(16)$ is irreducible over $\mathbf{L_{-3,d}}$ for all d.
Note that when we take the field $\mathbf{L_{-1,2}}$, we have the 2-division polynomial of $X_1(16)$ which splits only on this one, but again all these points are cusps.
So, as a conclusion, $\mathbb{Z}_{16}$ cannot appear as torsion subgroups over any of these fields.

The case $\mathbb{Z}/18\mathbb{Z}$.
We have that $X_1(18)$ is a hyperelliptic curve, and according to [74] $\mathbb{Z}/18\mathbb{Z}$ does not appear on $\mathbb{Q}(i)$. So, we will study its Jacobian $J_1(18)$. We obtain via 2-descent that, $rank(J_1(18)(\mathbf{L_{-1,d}})) = 0$ for $d = 2, 3, 5, 7, 13, 19, 37, 163$. So we will study the torsion points of $J_1(18)$ over $\mathbf{L_{-1,d}}$ for $d = 2, 3, 5, 7, 13, 19, 37, 163$.
As the discriminant of $X_1(18)$ is $-2^{15}.3^4$, so 2 and 3 are the only rational primes with bad reduction, and we have 7 is inert and 5 splits into $\mathbb{Q}(i)$. Thus, the prime-to-7 part and the prime-to-5 part of $J_1(18)(\mathbb{Q}(i))_{\text{tors}}$ are injected respectively into $J_1(18)(\mathbb{F}_7(i)) \simeq J_1(18)(\mathbb{F}_{49})$ and $J_1(18)(\mathbb{F}_5) \simeq J_1(18)(\mathbb{F}_5)$. We see that $\sharp J_1(\mathbb{Q}(i)) \leq 21$. Therefore, it follows that $J_1(\mathbb{Q}(i)) = J_1(\mathbb{Q}) \simeq \mathbb{Z}/21\mathbb{Z}$.
As $J_1^d(\mathbb{Q}(i)) \simeq \{O\}$ for $d = 2, 5, 7, 13, 19, 37, 163$ and $J_1(\mathbb{Q})$ is generated by the cusps of $X_1(18)$, we have for an odd prime number p, the p-part of $J_1(\mathbf{L_d})$ for
$d = 2, 5, 7, 13, 19, 37, 163$ is generated by the cusps of $X_1(18)$.
If $d = 3$, $J_1^3(\mathbb{Q}(i)) \simeq \mathbb{Z}/3\mathbb{Z}$ and also generated by the cusps of $X_1(18)$.
On the other hand, we have that the 2-division polynomial of $X_1(18)$ is irreducible over $\mathbf{L_{-1,d}}$ for all d.
So, as a conclusion, $\mathbb{Z}/18\mathbb{Z}$ cannot appear as torsion subgroups over any of these fields. □

The proof for imaginary triquadratic number fields is based on the same proof principle

as for biquadratic number fields. In the same way, we have, $\mathbb{Z}/13\mathbb{Z}$, $\mathbb{Z}/16\mathbb{Z}$, and $\mathbb{Z}/18\mathbb{Z}$ cannot appear as torsion subgroups in any of these fields.

Corollary 7. *The groups* $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/16\mathbb{Z}$ *and* $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/18\mathbb{Z}$ *cannot appear as torsion subgroups over any of the fields* $\mathbf{L_{d_1,d_2,\ldots,d_n}}$ *mentioned in the above Proof. Otherwise it would induce a* $\mathbf{L_{d_1,d_2,\ldots,d_n}}$*-rational cyclic subgroup of order* 16 *(respectively of order* 18*).*

Remark 4. *From the results obtained in this section, we can conclude that* $\mathbb{Z}/13\mathbb{Z}$*,* $\mathbb{Z}/16\mathbb{Z}$*, and* $\mathbb{Z}/18\mathbb{Z}$ *cannot appear as torsion subgroups over any imaginary multiquadratic number field of class number one mentioned in the above Proof.*
Which ends the demonstration of the main result.

Chapter 3

Torsion of Elliptic curves over quadratic cyclotomic fields in quadratic extensions of the base field

3.1 Introduction

Throughout this chapter [18], we take K as the cyclotomic quadratic field, d be square-free and $K(\sqrt{d})$ be a quadratic extension of K. In this chapter, we will study the possible torsion groups of elliptic curves over K when we extend the base field to $K(\sqrt{d})$. Moreover, we will study these elliptic curves on biquadratic number fields $\mathbb{Q}(\sqrt{e}, \sqrt{d})$ of class number one, where $e = -1, -3$, and we will give some results on the number of $K(\sqrt{d})$ where the torsion grows.
Note that throughout this chapter we have E is an elliptic curve defined on cyclotomic quadratic number fields.

3.2 Torsion of elliptic curves over $K(\sqrt{d})$

The results of this section provide a nice framework for the torsion part of elliptic curves defined over a cyclotomic quadratic field K which can appear on quadratic extensions of the base field.

Theorem 3.2.1. *Let E/K be an elliptic curve and $K(\sqrt{d})$ be a quadratic extension of K.*

The torsion of $E(K(\sqrt{d}))$ is isomorphic to one of the following groups

1

$$\mathbb{Z}/m\mathbb{Z}, m = 1, \ldots, 10, 12, 15, 16,$$
$$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2m\mathbb{Z}, m = 1, .., 6, 8,$$
$$\mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3m\mathbb{Z}, m = 1, 2,$$
$$\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4m\mathbb{Z}, m = 1, 2,$$
$$\mathbb{Z}/6\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}.$$

Moreover,

2 if $K = \mathbb{Q}(i)$ and $d \neq \pm 3$. Then the following groups $\mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3m\mathbb{Z}, m = 1, 2$ and $\mathbb{Z}/6\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}$ cannot appear as torsion subgroups.

3 if $K = \mathbb{Q}(\sqrt{-3})$ and $d \neq -1, 3$. Then the following groups $\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4m\mathbb{Z}, m = 1, 2$ cannot appear as torsion subgroups.

The proof of the Theorem 3.2.1, can be deduced from the following Lemmas.

In the following Lemma, we extend the result of Enrique Gonzlez-Jimnez and Jos M. Tornero in [50] on the rationals to the cyclotomic quadratic field. Moreover, we will use this result to determine the odd torsion subgroup in a quadratic extension of K.

Lemma 12. *Let E be an elliptic curve defined over K. So, there exists a pair of homomorphisms*

$$E(K(\sqrt{d})) \xrightarrow{\chi_1} E(K) \oplus E^d(K) \xrightarrow{\chi_2} E(K(\sqrt{d}))$$

such that

$$\chi_2 \circ \chi_1 = [2],$$
$$\chi_1 \circ \chi_2 = [2] \oplus [2],$$
$$ker(\chi_1) \subset E(K(\sqrt{d}))[2],$$
$$ker(\chi_2) \subset E(K)[2] \oplus E^d(K)[2].$$

Moreover, each non-zero element of $coker(\chi_1)$ and $coker(\chi_2)$ is of order 2.

Proof.
In the same way as we already do in the proof of the Lemma 4. □

Corollary 8. *Let E be an elliptic curve defined over K. If n is an odd integer, then we have*

$$E(K(\sqrt{d}))[n] \simeq E(K)[n] \oplus E^d(K)[n]. \tag{3.1}$$

Remark 5. *Note that $\Omega_1 \subset \Omega_d$ for all $d > 1$. It remains for us to examine torsion structures other than those of Mazur.*

In the following Lemmas, we will exclude some structures.

Lemma 13. *Let E/K be an elliptic curve. Then the following cyclic groups $\mathbb{Z}/11\mathbb{Z}$, $\mathbb{Z}/13\mathbb{Z}$ and $\mathbb{Z}/17\mathbb{Z}$ cannot appear as torsion subgroups over $K(\sqrt{d})$.*

Proof.
By Lemma 12, for an odd number n, we have $E(K(\sqrt{d}))[n] \simeq E(K)[n] \oplus E^d(K)[n]$. The curve E^d is clearly defined on K, and by the classification of torsion subgroups of elliptic curves defined on K (Theorem 0.2.3), it follows that neither $E^d(K)$ nor $E(K)$ have points of order n=11, 13 or 17. Thus, $E(K(\sqrt{d}))$ has no points of order n=11, 13 or 17. □

Corollary 9. *$\mathbb{Z}/22\mathbb{Z}$ cannot occur as torsion over the field $K(\sqrt{d})$.*

Lemma 14. *Assume that $E/\mathbb{Q}(i)$, and $d \neq \pm 3$. Then the following groups $\mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}$, $\mathbb{Z}/5\mathbb{Z} \oplus \mathbb{Z}/5\mathbb{Z}$ and $\mathbb{Z}/6\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}$, cannot appear as torsion subgroups over $K(\sqrt{d})$.*

Proof.
By the existence of the Weil pairing, full n-torsion is defined over $K(\sqrt{d})$ only if the n-th roots of unity are in $K(\sqrt{d})$. Since for $d \neq \pm 3$, we have no primitive root of the unit for $n = 3, 5$ or 6 on $K(\sqrt{d})$, it follows that by Weil pairing, $E(K(\sqrt{d}))_{tors}$ cannot be isomorphic to any of the following subgroups, $\mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}$, $\mathbb{Z}/5\mathbb{Z} \oplus \mathbb{Z}/5\mathbb{Z}$ and $\mathbb{Z}/6\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}$. □

Corollary 10. *With the same notation as in the previous Lemma we have, $\mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}$ cannot occur as a torsion subgroup over the field $K(\sqrt{d})$.*

Remark 6. *Note that by the Theorem 0.2.3, we have $\mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}$ and $\mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}$ can appear as torsion subgroups on $\mathbb{Q}(i, \sqrt{3})$ of an elliptic curve defined on $\mathbb{Q}(i)$.*

Lemma 15. *Let E be an elliptic curve defined over $\mathbb{Q}(\sqrt{-3})$ and $d \neq -1, 3$. Then the following groups $\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$ and $\mathbb{Z}/5\mathbb{Z} \oplus \mathbb{Z}/5\mathbb{Z}$, cannot appear as torsion subgroups over $K(\sqrt{d})$.*

Proof.
Since $d \neq -1, 3$, we have no primitive root of the unit for $n = 4$ or 5 on $K(\sqrt{d})$, it follows that by Weil pairing, $E(K(\sqrt{d}))_{tors}$ cannot be isomorphic to any of the following subgroups, $\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$ and $\mathbb{Z}/5\mathbb{Z} \oplus \mathbb{Z}/5\mathbb{Z}$. □

Corollary 11. *With the same notation as above we have, $\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z}$ cannot occur as torsion subgroup over the field $K(\sqrt{d})$.*

Lemma 16. *Let E/K be an elliptic curve. Then $E(K(\sqrt{d}))_{tors}$ does not contain a point of order $2n$, for $n = 7$ or 9.*

Proof.
Note that for an elliptic curve $E : y^2 = f(t)$, the number of points of order 2 on $K(\sqrt{d})$, is equal to the number of roots of $f(t)$ on $K(\sqrt{d})$. So if $E(K)[2] = \{O\}$, then $E(K(\sqrt{d}))[2] = \{O\}$. Suppose that for n = 7 or 9, $E(K(\sqrt{d}))$ has a 2n-torsion. So, as mentioned above, $E(K)_{tors}$ and $E^d(K)_{tors}$ would have a point of order 2, and it follows from Lemma 12 that either $E(K)$ or $E^d(K)$ has an n-torsion point and thus also a 2n-torsion point, which is impossible by Theorem 0.2.3. □

Corollary 12. *With the same notation as above we have, $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/14\mathbb{Z}$ and $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/18\mathbb{Z}$ cannot occur as torsion subgroups over the field $K(\sqrt{d})$.*

Remark 7. *It can be seen from [56, 83] that there exist infinitely many elliptic curves defined over $\mathbb{Q}$, therefore also defined on K with torsion $\mathbb{Z}/16\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2m\mathbb{Z}$ for $m = 5, 6$, $\mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3m\mathbb{Z}$ for $m = 1, 2$ and $\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$.*

We now want to find an elliptic curve with a point of order 15 on $K(\sqrt{d})$. So, let E/K be an elliptic curve realizing a point of order 15 on a quadratic extension of K. By Lemma 12 this implies that (Suppose without loss of generality that),

$$E(K)_{\text{tors}} \simeq \mathbb{Z}/3\mathbb{Z} \text{ and } E^d(K)_{\text{tors}} \simeq \mathbb{Z}/5\mathbb{Z}$$

Moreover, all quadratic twists E^d of E have p-isogeny if E has one. That E must have a 15-isogeny. For example there is a family of twists of elliptic curves with a 15-isogeny, and with j-invariants 46969655/32768, which are the twists of the elliptic curve $50B2$. By the division polynomial method [76] we find that
• If $K = \mathbb{Q}(\sqrt{-3})$, $50B2$ has 15-torsion over $K(\sqrt{5})$.
• If $K = \mathbb{Q}(i)$, $50B2$ has 15-torsion over $K(\sqrt{15})$.

Note that $E(K(\sqrt{d}))_{tors}$ does not contain the subgroups $\mathbb{Z}/21\mathbb{Z}$, $\mathbb{Z}/24\mathbb{Z}$ and $\mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/9\mathbb{Z}$, the statement follows from Ejder's main result [36], which is the proof of the Theorem 3.2.1.

3.3 Biquadratic number field $\mathbb{Q}(\sqrt{e}, \sqrt{d})$ of class number

To know if there exists a curve with a torsion subgroup $\mathbb{Z}/n\mathbb{Z} \oplus \mathbb{Z}/m\mathbb{Z}$ on a fixed number field K, we need to determine if $X_1(n, m)$ has a K-rational point which is not a

cusp. In this section, from the following Lemmas, we will eliminate certain subgroups of $E(\mathbb{Q}(\sqrt{e},\sqrt{d}))$ where $e=-1,\ -3$.
The possible torsion structures of an elliptic curve E/K in a biquadratic number field of class number one is a subset of the list in Theorem 3.2.1. So, the main result of this section is given and proved as Lemmas.

Lemma 17. *The fields among $\mathbb{Q}(\sqrt{e},\sqrt{d})$, over which $\mathbb{Z}/15\mathbb{Z}$ can appears as torsion of elliptic curves are,*

(a) $\mathbb{Q}(i,\sqrt{d})$ *with* $d=3,7,11,13,37,43,67,163$.

(b) $\mathbb{Q}(\sqrt{-3},\sqrt{d})$ *for all* d.

Proof.
From [3, 83] we have that an elliptic curve with torsion $\mathbb{Z}/15\mathbb{Z}$ is induced by solutions of the equation

$$X_1(15): y^2+sy+y=s^3+s^2,$$

where the cusps satisfy

$$s(s+1)(s^4+3s^3+4s^2+2s+1)(s^4-7s^3-6s^2+2s+1)=0.$$

We see that $X_1(15)$ is an elliptic curve, which can be reduced to the short Weierstrass form

$$y^2=s^3-27s+8694.$$

First case $K=\mathbb{Q}(i)$
We compute using 2-descent the rank of $X_1^d(15)$ over $\mathbb{Q}(i,\sqrt{d})$ for $d=2,3,5,7,11,13,19,37,43,67,163$. As shown in the Table 3.1, we have for $d=2,5$ or 19, the rank

Table 3.1: Rank of $X_1^d(15)$.

d	2	3	5	7	11	13	19	37	43	67	163
rank over $\mathbb{Q}(i,\sqrt{d})$	0	1	0	2	2	2	0	2	2	2	2

of $X_1(15)$ over $\mathbb{Q}(i,\sqrt{d})$ is 0. We then compute the torsion subgroup of $X_1^d(15)$ over $\mathbb{Q}$ for $d=\pm1,\pm2,\pm5,\pm19$.

The n-torsion of $X_1(15)(\mathbb{Q}(i,\sqrt{d}))$ for an odd integer n and $d=2,5,19$ is determined by the Lemma 12, and the above computation in the Table 3.2. For the 2-torsion, we find that the 2-division polynomial is irreducible over $\mathbb{Q}(i,\sqrt{d})$ for $d=2,5,19$. This ensures that $X_1(15)$ does not have 2-torsion over $\mathbb{Q}(i,\sqrt{d})$ with $d=2,5,19$. As a result,

$$X_1(15)(\mathbb{Q}(i,\sqrt{d}))\cong\mathbb{Z}/4\mathbb{Z}\cong\{O,(0,0),(0,-1),(-1,0)\}.$$

Table 3.2: Torsion subgroup.

d	1	2	5	19
$(X_1(15)^d(\mathbb{Q}))_{tors}$	$\mathbb{Z}/4\mathbb{Z}$	$\mathbb{Z}/2\mathbb{Z}$	$\mathbb{Z}/2\mathbb{Z}$	$\mathbb{Z}/2\mathbb{Z}$
$(X_1(15)^{-d}(\mathbb{Q}))_{tors}$	$\mathbb{Z}/2\mathbb{Z}$	$\mathbb{Z}/2\mathbb{Z}$	$\mathbb{Z}/2\mathbb{Z}$	$\mathbb{Z}/2\mathbb{Z}$

So, all these torsion points have the first coordinate $s = 0$ or -1. It follows that they are all cusps of $X_1(15)$. Thus, $\mathbb{Z}/15\mathbb{Z}$ cannot occur as torsion over the fields $\mathbb{Q}(i, \sqrt{d})$ with $d = 2, 5$ or 19.

Second case $K = \mathbb{Q}(\sqrt{-3})$

We compute using 2-descent the rank of $X_1^d(15)$ over $\mathbb{Q}(\sqrt{-3}, \sqrt{d})$ for $d = 2, -7, -11, -19, -43, -67, 89$. As shown in the Table 3.3, we have for $d = 2, -7, -11, -19, -43, -67,$

Table 3.3: Rank of $X_1^d(15)$.

d	2	-7	-11	-19	-43	-67	89
rank over $\mathbb{Q}(\sqrt{-3}, \sqrt{d})$	1	1	2	1	1	1	1

89, the rank of $X_1(15)$ is ≥ 1. Hence, $\mathbb{Z}/15\mathbb{Z}$ appears as a torsion subgroup for infinitely many isomorphism classes of elliptic curves over $\mathbb{Q}(\sqrt{-3}, \sqrt{d})$ for all d. □

Lemma 18. *The fields among $\mathbb{Q}(\sqrt{e}, \sqrt{d})$, over which $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/10\mathbb{Z}$ can appears as torsion of elliptic curves are,*

(a) $\mathbb{Q}(i, \sqrt{d})$ with $d = 2, 3, 7, 11, 13, 19, 37, 43, 67, 163$.

(b) $\mathbb{Q}(\sqrt{-3}, \sqrt{d})$ with $d = -11, -19, 89$.

Proof.

From [3, 83] we have that an elliptic curve with torsion $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/10\mathbb{Z}$ is induced by solutions of the equation

$$X_1(2, 10) : y^2 = s^3 + s^2 - s,$$

where the cusps satisfy

$$s(s^2 - 1)(s^2 + s - 1)(s^2 - 4s - 1) = 0.$$

We see that $X_1(2, 10)$ is an elliptic curve.

First case $K = \mathbb{Q}(i)$

Using 2-descent we compute the rank of $X_1^d(2, 10)$ over $\mathbb{Q}(i, \sqrt{d})$ for $d = 2, 3, 5, 7, 11, 13, 19, 37, 43, 67, 163$.

Table 3.4: Rank of $X_1^d(2,10)$.

d	2	3	5	7	11	13	19	37	43	67	163
rank over $\mathbb{Q}(i,\sqrt{d})$	1	1	0	1	1	1	2	1	1	1	1

As shown in the Table 3.4, we have for $d = 5$, the rank of $X_1(2,10)$ over $\mathbb{Q}(i,\sqrt{5})$ is 0. We then compute the torsion subgroup of $X_1^d(2,10)$ over $\mathbb{Q}$, for $d = \pm 1, \pm 5$.

Table 3.5: Torsion subgroup.

d	1	5
$(X_1^d(2,10)(\mathbb{Q}))_{tors}$	$\mathbb{Z}/6\mathbb{Z}$	$\mathbb{Z}/2\mathbb{Z}$
$(X_1^{-d}(2,10)(\mathbb{Q}))_{tors}$	$\mathbb{Z}/2\mathbb{Z}$	$\mathbb{Z}/2\mathbb{Z}$

The n-torsion of $X_1(2,10)(\mathbb{Q}(i,\sqrt{5}))$ for an odd integer n is determined by the Lemma 12, and the above computation in the Table 3.5. For the 2-torsion, we find that the 2-division polynomial splits only over $\mathbb{Q}(i,\sqrt{5})$. This shows that

$$(X_1(2,10)(\mathbb{Q}(i,\sqrt{5})))_{tors} \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}.$$

So, all these torsion points have the first coordinate $s = -1$, 0 or 1. It follows that they are all cusps of $X_1(2,10)$. Thus, $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/10\mathbb{Z}$ cannot occur as torsion over the field $\mathbb{Q}(i,\sqrt{5})$.

Second case $K = \mathbb{Q}(\sqrt{-3})$ Calculate the rank of $X_1^d(2,10)$ over $\mathbb{Q}(\sqrt{-3},\sqrt{d})$ for $d = 2, -7, -11, -19, -43, -67, 89$.

Table 3.6: Rank of $X_1^d(2,10)$.

d	2	-7	-11	-19	-43	-67	89
rank over $\mathbb{Q}(\sqrt{-3},\sqrt{d})$	0	0	2	2	0	0	2

As shown in the Table 3.6, we have for $d = 2, -7, -43, -67$, the rank of $X_1(2,10)$ over $\mathbb{Q}(\sqrt{-3},\sqrt{d})$ is 0. We then compute the torsion subgroup of $X_1^d(2,10)$ and $X_1^{-3d}(2,10)$ over $\mathbb{Q}$, for $d = 2, -7, -43, -67$.

The n-torsion of $X_1(2,10)(\mathbb{Q}(\sqrt{-3},\sqrt{d}))$ for an odd integer n is determined by the Lemma 12, and the above computation in the Table 3.7. For the 2-torsion, we find that the 2-division polynomial is irreducible over $\mathbb{Q}(\sqrt{-3},\sqrt{d})$ for all d. This shows that

$$(X_1(2,10)(\mathbb{Q}(\sqrt{-3},\sqrt{d})))_{tors} \cong \mathbb{Z}/6\mathbb{Z} \; for \; d = 2, -7, -43, -67.$$

Table 3.7: Torsion subgroup.

d	2	-7	-43	-67
$(X_1^d(2,10)(\mathbb{Q}))_{tors}$	$\mathbb{Z}/6\mathbb{Z}$	$\mathbb{Z}/2\mathbb{Z}$	$\mathbb{Z}/2\mathbb{Z}$	$\mathbb{Z}/2\mathbb{Z}$
$(X_1^{-3d}(2,10)(\mathbb{Q}))_{tors}$	$\mathbb{Z}/2\mathbb{Z}$	$\mathbb{Z}/2\mathbb{Z}$	$\mathbb{Z}/2\mathbb{Z}$	$\mathbb{Z}/2\mathbb{Z}$

So, all these torsion points have the first coordinate $s = -1$, 0 or 1. It follows that they are all cusps of $X_1(2,10)$. Thus, $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/10\mathbb{Z}$ cannot occur as torsion over the field $\mathbb{Q}(\sqrt{-3}, \sqrt{d})$ for $d = 2, -7, -43, -67$. □

Lemma 19. *The fields among $\mathbb{Q}(\sqrt{e}, \sqrt{d})$, over which $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/12\mathbb{Z}$ can appears as torsion of elliptic curves are,*

(a) $\mathbb{Q}(i, \sqrt{d})$ with $d = 5, 7, 11, 19, 43, 67, 163$.

(b) $\mathbb{Q}(\sqrt{-3}, \sqrt{d})$ with $d = -7, -19, -43, -67, 89$.

Proof.
From [3, 83] we have that an elliptic curve with torsion $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/12\mathbb{Z}$ is induced by solutions of the equation

$$X_1(2,12) : y^2 = s^3 - s^2 + s,$$

where the cusps satisfy

$$s(s-1)(2s-1)(2s^2 - s + 1)(3s^2 - 3s - 1)(6s^2 - 6s - 1) = 0.$$

We have that $X_1(2,12)$ is an elliptic curve.
First case $K = \mathbb{Q}(i)$
We compute using 2-descent the rank of $X_1^d(2,12)$ over $\mathbb{Q}(i, \sqrt{d})$ for
$d = 2, 3, 5, 7, 11, 13, 19, 37, 43, 67, 163$.

Table 3.8: Rank of $X_1^d(2,12)$.

d	2	3	5	7	11	13	19	37	43	67	163
rank over $\mathbb{Q}(i, \sqrt{d})$	0	0	1	1	1	0	1	0	1	2	1

As shown in the Table 3.8, we have for $d = 2, 3, 13, 37$, the rank of $X_1(2,12)$ over $\mathbb{Q}(i, \sqrt{d})$ is 0. We then compute the torsion subgroup of $X_1^d(2,12)$ over $\mathbb{Q}$, for
$d = \pm 1, \pm 2, \pm 3, \pm 13, \pm 37$.

Table 3.9: Torsion subgroup.

d	1	2	3	13	37
$(X_1(2,12)^d(\mathbb{Q}))_{tors}$	$\mathbb{Z}/4\mathbb{Z}$	$\mathbb{Z}/2\mathbb{Z}$	$\mathbb{Z}/2\mathbb{Z}$	$\mathbb{Z}/2\mathbb{Z}$	$\mathbb{Z}/2\mathbb{Z}$
$(X_1(2,12)^{-d}(\mathbb{Q}))_{tors}$	$\mathbb{Z}/2\mathbb{Z}$	$\mathbb{Z}/2\mathbb{Z}$	$\mathbb{Z}/2\mathbb{Z}$	$\mathbb{Z}/2\mathbb{Z}$	$\mathbb{Z}/2\mathbb{Z}$

So, the n-torsion of $X_1(2,12)(\mathbb{Q}(i,\sqrt{d}))$ for an odd integer n and $d = 2, 3, 13, 37$ is determined by the Lemma 12, and the above computation in the Table 3.9. For the 2-torsion, we find that the 2-division polynomial splits only over $\mathbb{Q}(i,\sqrt{3})$. This shows that

$$(X_1(2,12)(\mathbb{Q}(i,\sqrt{3}))_{tors} \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z},$$
$$(X_1(2,12)(\mathbb{Q}(i,\sqrt{d})))_{tors} \cong \mathbb{Z}/4\mathbb{Z} \qquad for\ d = 2, 13, 37.$$

So, all these torsion points have the first coordinate $s = 0$ or 1. It follows that they are all cusps of $X_1(2,12)$. Thus, $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/12\mathbb{Z}$ cannot occur as torsion over the fields $\mathbb{Q}(i,\sqrt{d})$ with $d = 2, 3, 13, 37$.

Second case $K = \mathbb{Q}(\sqrt{-3})$

Calculate the rank of $X_1^d(2,12)$ over $\mathbb{Q}(\sqrt{-3},\sqrt{d})$ for $d = 2, -7, -11, -19, -43, -67, 89$.

Table 3.10: Rank of $X_1^d(2,12)$.

d	2	-7	-11	-19	-43	-67	89
rank over $\mathbb{Q}(\sqrt{-3},\sqrt{d})$	0	1	0	1	1	1	1

as shown in the Table 3.10, we have for $d = 2, -11$, the rank of $X_1(2,12)$ over $\mathbb{Q}(\sqrt{-3},\sqrt{d})$ is 0. We then compute the torsion subgroup of $X_1^d(2,12)$ and $X_1^{-3d}(2,12)$ over $\mathbb{Q}$, for $d = 2, -11$

Table 3.11: Torsion subgroup.

d	1	2	-11
$(X_1(2,12)^d(\mathbb{Q}))_{tors}$	$\mathbb{Z}/4\mathbb{Z}$	$\mathbb{Z}/2\mathbb{Z}$	$\mathbb{Z}/2\mathbb{Z}$
$(X_1(2,12)^{-3d}(\mathbb{Q}))_{tors}$	$\mathbb{Z}/2\mathbb{Z}$	$\mathbb{Z}/2\mathbb{Z}$	$\mathbb{Z}/2\mathbb{Z}$

So, the n-torsion of $X_1(2,12)(\mathbb{Q}(\sqrt{-3},\sqrt{d}))$ for an odd integer n and $d = 2, -11$ is determined by the Lemma 12, and the above computation in the Table 3.11. For the 2-torsion, we find that the 2-division polynomial splits over $\mathbb{Q}(\sqrt{-3},\sqrt{d})$ for all d. This shows that

$$(X_1(2,12)(\mathbb{Q}(\sqrt{-3},\sqrt{d})))_{tors} \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z} \quad for\ d = 2, -11.$$

So, all these torsion points have the first coordinate $s = 0$ or 1. It follows that they are all cusps of $X_1(2,12)$. Thus, $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/12\mathbb{Z}$ cannot occur as torsion over the fields $\mathbb{Q}(\sqrt{-3}, \sqrt{d})$ with $d = 2, -11$. □

Lemma 20. *The group $\mathbb{Z}/16\mathbb{Z}$ cannot appear as a torsion subgroup of elliptic curves over the following biquadratic number fields of class number one,*

(a) $\mathbb{Q}(i, \sqrt{d})$ *for* $d = 2, 3, 5, 7, 11, 13, 19, 37, 43, 67, 163$.

(b) $\mathbb{Q}(\sqrt{-3}, \sqrt{d})$ *for* $d = 2, -7, -11, -19, -43, -67, 89$.

Proof.
We have that $X_1(16)$ is a hyperelliptic curve, and according to [74] $\mathbb{Z}/16\mathbb{Z}$ does not appear on K. So, we will study its Jacobian $J_1(16)$ [99].
First case $K = \mathbb{Q}(i)$
We obtain via 2-descent that $rank(J_1(16)(\mathbb{Q}(i, \sqrt{d}))) = 0$ for $d = 2, 3, 5, 7, 11, 13, 19, 37, 43, 67, 163$. So we will study the torsion points of $J_1(16)$ over $\mathbb{Q}(i, \sqrt{d})$ for $d = 2, 3, 5, 7, 11, 13, 19, 37, 43, 67, 163$.
Since the discriminant of $X_1(16)$ is -2^{19}, so 2 is the only rational prime with bad reduction. We have 3 is inert and 5 splits into $\mathbb{Q}(i)$. Thus, the prime-to-3 part and the prime-to-5 part of $J_1(16)(\mathbb{Q}(i))_{\text{tors}}$ are injected respectively into $J_1(16)(\mathbb{F}_3(i)) \simeq J_1(16)(\mathbb{F}_9)$ and $J_1(16)(\mathbb{F}_5) \simeq J_1(16)(\mathbb{F}_5)$. We see that $\sharp J_1(16)(\mathbb{Q}(i)) \leq 40$. Therefore, it follows that $J_1(\mathbb{Q}(i)) \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/10\mathbb{Z}$ or $J_1(\mathbb{Q}(i)) \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/10\mathbb{Z}$.
As $J_1(16)(\mathbb{Q})$ is generated by the cusps of $X_1(16)$, and we have for an odd prime number p $J_1^d(16)(\mathbb{Q}(i))[p] \simeq \{O\}$ for $d = 2, 3, 5, 7, 11, 13, 19, 37, 43, 67, 163$, thus the p-part of $J_1(16)(\mathbb{Q}(i, \sqrt{d}))$ for $d = 2, 3, 5, 7, 11, 13, 19, 37, 43, 67, 163$ are generated by the cusps of $X_1(16)$.
On the other hand, we have the 2-division polynomial of $X_1(16)$ splits only over $\mathbb{Q}(i, \sqrt{2})$, but again all these points are cusps.
So, as a conclusion, $\mathbb{Z}/16\mathbb{Z}$ cannot appear as torsion.
Second case $K = \mathbb{Q}(\sqrt{-3})$
In the same way we obtain that $rank(J_1(16)(\mathbb{Q}(\sqrt{-3}, \sqrt{d}))) = 0$ for $d = 2, -7, -11, -19, -43, -67, 89$. So we will study the torsion points of $J_1(16)$ over $\mathbb{Q}(\sqrt{-3}, \sqrt{d})$ for $d = 2, -7, -11, -19, -43, -67, 89$.
Since the discriminant of $X_1(16)$ is -2^{19}, so 2 is the only rational primes with bad reduction. We have 5 is inert and 7 split into $\mathbb{Q}(\sqrt{-3})$. Thus, the prime-to-5 part and the prime-to-7 part of $J_1(16)(\mathbb{Q}(\sqrt{-3}))_{\text{tors}}$ are injected respectively into $J_1(16)(\mathbb{F}_5(\sqrt{-3})) \simeq J_1(16)(\mathbb{F}_{25})$ and $J_1(16)(\mathbb{F}_7)$. We see that $\sharp J_1(16)(\mathbb{Q}(\sqrt{-3})) \leq 40$. Therefore, it follows that $J_1(\mathbb{Q}(\sqrt{-3})) \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/10\mathbb{Z}$ or $J_1(\mathbb{Q}(\sqrt{-3})) \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/10\mathbb{Z}$.
As $J_1(16)(\mathbb{Q})$ is generated by the cusps of $X_1(16)$, and we have for an odd prime number

p $J_1^d(16)(\mathbb{Q}(\sqrt{-3}))[p] \simeq \{O\}$ for $d = 2, -7, -11, -19, -43, -67, 89$, thus the p-part of $J_1(16)(\mathbb{Q}(\sqrt{-3}, \sqrt{d}))$ for $d = 2, -7, -11, -19, -43, -67, 89$ are generated by the cusps of $X_1(16)$.
On the other hand, we have the 2-division polynomial of $X_1(16)$ is irreducible over $\mathbb{Q}(\sqrt{-3}, \sqrt{d})$ for all d.
So, as a conclusion, $\mathbb{Z}/16\mathbb{Z}$ cannot appear as torsion. □

Corollary 13. *The group $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/16\mathbb{Z}$ cannot appear as a torsion subgroup of elliptic curves over any fields among $\mathbb{Q}(\sqrt{e}, \sqrt{d})$ mentioned in the above Proof. Otherwise it would induce a $\mathbb{Q}(\sqrt{e}, \sqrt{d})$-rational cyclic subgroup of order 16.*

3.4 On the number of $K(\sqrt{d})$ with proper extension of a fixed torsion subgroup over K

Here we will consider the following problem, if we fix an elliptic curve defined over quadratic cyclotomic fields with a fixed torsion subgroup G and take a quadratic extension of K. How many proper extensions of G can we expect to see?

Theorem 3.4.1. *Let E/K be an elliptic curve. Thus, for all but finitely many quadratic twists E^d, $E^d(K)$ has only elements of order at most two.*

Proof.
From Lemma 12, we have

$$E(K(\sqrt{d})) \xrightarrow{\chi_1} E(K) \times E^d(K) \xrightarrow{P_2} E^d(K), \tag{3.2}$$

where P_2 is the second projection map into $E^d(K)$.
So, consider the morphism ρ from $E(K(\sqrt{d}))$ into $E^d(K)$, given by the composition 3.2 Thus, $\rho(B) = \chi(B - \beta B, 1/\sqrt{d})$ and $ker(\rho) = E(K)$. So, now consider

$$0 \to E(K) \longrightarrow E(K(\sqrt{d})) \xrightarrow{\rho} E^d(K) \longrightarrow \text{coker}(\rho) \to 0$$

Thus,

$$E(K(\sqrt{d}))_{tors}/E(K)_{tors} \simeq Img(\rho)$$
$$E^d(K)_{tors}/Img(\rho) \simeq coker(\rho).$$

First, the Lemma 12 allows us to say that each non-zero element of $coker(\rho)$ is of order 2. On the other hand, from Theorem 3.2.1 if $B \in E(K(\sqrt{d}))_{tors}$ of order n, then $n \in A = \{1, ..., 10, 12, 15, 16\}$. Therefore, $x(B)$ the first coordinate of B is a root of n-th division polynomials $\psi_n(X)$ [88]. So, we look for irreducible quadratic and linear factors in $K[X]$.

Thus, if we consider their splitting fields, these extensions are the only quadratic extension of K where the torsion subgroup may grow and are finitely many. Therefore, implies that for almost all d, we have $E(K(\sqrt{d}))_{tors} = E(K)_{tors}$. Thus, $E^d(K)_{tors} \simeq coker(\rho)$. □

Corollary 14. *The number of quadratic extensions of K where the torsion subgroup G of an elliptic curve E/K may grow, is bounded by a constant that only depends on G.*

We could actually put an upper bound on the number of $K(\sqrt{d})$ where the torsion subgroup G of an elliptic curve E/K may grow, by considering the number of linear factors of $\psi_n(X)$, with $n \in A$ being a prime power. On the other hand, to reduce the number of the division polynomials that must be taken into account we use the Theorem 15 in Newman's paper [77].

Chapter 4

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

4.1 Introduction

In this chapter [14], 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 subgroups of elliptic curves given by the 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 is 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 what follows, we will use the following notation:

- For $X \in \mathbb{Q}[\lambda]$, we have $X^{*n} = \underbrace{X * X * ... * X}_{n \text{ times}}$.
- $E_{a,b}$ 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 $\mathbb{Q}[\lambda]$.

- $Tor(E_{a,b})$ for the torsion subgroup of $E_{a,b}$.

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

Theorem 4.1.1. *With the same notation as above, let $E_{a,b}$ be an elliptic curve defined over $\mathbb{Q}[\lambda]$. So,*

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

4.2 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 chapter. 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 21. *The set $\mathbb{Q}[\lambda]$ together with the addition " $+$ " and the 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 15. $\mathbb{Q}[\lambda]$ *is a vector space over* $\mathbb{Q}$ *of dimension 2, and* $(1, \lambda)$ *is its basis.*

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

Proposition 4.2.1. *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 exists 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 16. *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 4.2.2.

- $\mathbb{Q}[\lambda]$ *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 $I = \{b - b\lambda \mid b \in \mathbb{Q}\} \cup \lambda\mathbb{Q}$ 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 4.2.1. $\widehat{\mathbb{Q}[\lambda]} = \mathbb{Z}[\lambda]$.

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 $P(X) = X^{*n} + a_1 X^{*n-1} + ... + a_n$ 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 $f^n + Q_2(e, f) = 0$. Thus

- 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 $f \in \mathbb{Z}$.

□

4.3 Elliptic curves over $\mathbb{Q}[\lambda]$

Definition 4.3.1. *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 [101] for an introduction to affine group schemes.*

Proposition 4.3.1. *[97] Let R be a ring in which 6 is invertible and let a and, b be two elements of R such that $4a^3 + 27b^2$ is invertible in R, the elliptic curve E of the 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 8. *According to the previous Proposition we can consider the elliptic curve $E_{a,b}$ on the ring $\mathbb{Q}[\lambda]$ given 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 E_0 and E_1 two restrictions of $E_{a,b}$ over $\mathbb{Q}$, defined as follows,

$$E_0 = \{[X : Y : Z] \in P^2(\mathbb{Q}) | Y^2Z = X^3 + a_0XZ^2 + b_0Z^3\},$$

and

$$E_1 = \{[X : Y : Z] \in P^2(\mathbb{Q}) | Y^2Z = X^3 + (a_0 + a_1)XZ^2 + (b_0 + b_1)Z^3\},$$

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 $E_{a,b}$ is an elliptic curve over $\mathbb{Q}[\lambda]$, so we have the following Lemmas,

Lemma 22. *E_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 $b^{*2} = b_0^2 + Q_2\lambda$, then we have $\triangle = 4(a_0^3 + Q_1\lambda) + 27(b_0^2 + Q_2\lambda)$. Thus, $\triangle = 4a_0^3 + 27b_0^2 + [4Q_1 + 27Q_2]\lambda$ and since $\triangle$ is invertible it follows from the Proposition 4.2.1 that $4a_0^3 + 27b_0^2 \neq 0$. □

Lemma 23. *E_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 4.2.1 that $4[a_0 + a_1]^3 + 27[b_0 + b_1]^2 \neq 0$. □

Theorem 4.3.1. *E_i are elliptic curves over $\mathbb{Q}$ for $i = 0,\ 1$ if and only if $E_{a,b}$ is an elliptic curve over $\mathbb{Q}[\lambda]$.*

Proof.
Suppose that E_0 and E_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 4.2.1, 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 22 and 23. □

4.4 The torsion subgroup of elliptic curves over $\mathbb{Q}[\lambda]$

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

Theorem 4.4.1. *Let $E_{a,b}$ be an elliptic curve over $\mathbb{Q}[\lambda]$. So*

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

To prove this result we will define a relation between $E_{a,b}$ and $E_0\times E_1$.

Lemma 24. *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 exists $(U,V,W)\in(\mathbb{Q}[\lambda])^3$ 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 cases 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 25. *With the same notation as above, we have $[X:Y:Z]$ is in $E_{a,b}$ if and only if $[x_0:y_0:z_0]\in E_0$ and $[x_0+x_1:y_0+y_1:z_0+z_1]\in E_1$.*

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 shown 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

- $Y^{*2} * Z = y_0^2z_0 + ((y_0 + y_1)^2(z_0 + z_1) - y_0^2z_0)\lambda$,
- $X^{*3} = x_0^3 + ((x_0 + x_1)^3 - x_0^3)\lambda$,
- $a * X * Z^{*2} = a_0x_0z_0 + ((a_0 + a_1)(x_0 + x_1)(z_0 + z_1)^2 - a_0x_0z_0)\lambda$
- $b * Z^{*3} = b_0z_0^3 + ((b_0 + b_1)(z_0 + z_1)^3 - b_0z_0^3)\lambda$.

We deduce from the Proposition 4.2.1 that $Y^{*2} * Z = X^{*3} + a * X * Z^{*2} + b * Z^{*3}$ if and only if $y_0^2z_0 = x_0^3 + a_0x_0z_0^2 + b_0z_0^3$ 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 $E_{a,b}$ with the elliptic curves E_0 and E_1,

Theorem 4.4.2. *The mapping*

$$\begin{array}{ccc} E_{a,b} & \xrightarrow{\wp} & E_0 \times E_1 \\ [X : Y : Z] & \longmapsto & ([x_0 : y_0 : z_0], [x_0 + x_1 : y_0 + y_1 : z_0 + z_1]) \end{array}$$

is a bijection.

Proof.
• From Lemma 25 it follows that $\wp$ is well defined.
• $\wp$ is a surjective map:
Let $[x_0 : y_0 : z_0] \in E_0$ and $[x_1 : y_1 : z_1] \in E_1$ then

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

so we have:
$\wp([x_0 + (x_1 - x_0)\,\lambda : y_0 + (y_1 - y_0)\,\lambda : z_0 + (z_1 - z_0)\,\lambda])$
$= ([x_0 : y_0 : z_0], [x_0 + (x_1 - x_0) : y_0 + (y_1 - y_0) : z_0 + (z_1 - z_0)])$

$= ([x_0 : y_0 : z_0], [x_1 : y_1 : z_1])$,
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:
$\wp^{-1}([x_0 : y_0 : z_0], [x_1 : y_1 : z_1]) = [x_0 + (x_1 - x_0)\lambda : y_0 + (y_1 - y_0)\lambda : z_0 + (z_1 - z_0)\lambda]$
is the inverse of $\wp$. □

4.4.1 The group law $\star$ over $E_{a,b}$

To define the group law $\star$ over $E_{a,b}$, we use the explicit formulas in the article [10] [pages : 236-238], and since $\wp$ is a bijection we can define $\star$ as follows $P \star Q = \wp^{-1}(\wp(P) + \wp(Q))$ for $P, Q \in E_{a,b}$.

Corollary 17. *The mapping*

$$\begin{array}{ccc} (E_{a,b}, \star) & \xrightarrow{\wp} & (E_0 \times E_1, +) \\ [X : Y : Z] & \longmapsto & ([x_0 : y_0 : z_0], [x_0 + x_1 : y_0 + y_1 : z_0 + z_1]) \end{array}$$

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 $E_{a,b}$ 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 4.4.1. *Let $P = [X : Y : Z] \in E_{a,b}$ such that $X = x_0 + x_1\lambda$, $Y = y_0 + y_1\lambda$ and $Z = z_0 + z_1\lambda$, so $P \in Tor(E_{a,b})$ if and only if $P_0 \in Tor(E_0)$ and $P_1 \in Tor(E_1)$, 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 $P \in Tor(E_{a,b})$ then there exists 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 $P_0 \in Tor(E_0)$ and $P_1 \in Tor(E_1)$. On the other hand, if there exist integers m, n such that $mP_0 = O_0$ and $nP_1 = O_1$, we have $mnP = \wp^{-1}((P_0, P_1) + ... + (P_0, P_1) = \wp^{-1}((mnP_0, mnP_1)) = \wp^{-1}(O_0, O_1) = O$. □

Corollary 18. *With the same notation as above we have* $\wp(Tor(E_{a,b})) = Tor(E_0) \times Tor(E_1)$.

Proposition 4.4.2. *According to the above we have*

$$Tor(E_{a,b}) \simeq Tor(E_0) \times Tor(E_1).$$

Proof.
Put

$$\begin{array}{ccc} Tor(E_{a,b}) & \overset{\wp/_{Tor(E_{a,b})}}{\longrightarrow} & Tor(E_0) \times Tor(E_1) \\ P & \longmapsto & \wp(P) \end{array}$$

the $\wp$-restriction on the torsion subgroup of $E_{a,b}$. From the theorem 4.4.2 and the previous Lemmas we have $\wp/_{Tor(E_{a,b})}$ is an isomorphism of groups, hence the result. □

Proof. (Theorem 4.4.1.)
From the previous Proposition we have $Tor(E_{a,b}) \simeq Tor(E_0) \times Tor(E_1)$, and from the Mazur's Theorem 0.2.1 we deduce the result. □

Example 4.4.1. *Let* λ *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* $E_{a,b}$ *the elliptic curve defined by* $Y^{*2} * Z = X^{*3} + a * X * Z^{*2} + b * Z^{*3}$ *over* $\mathbb{Q}[\lambda]$. *We consider* E_0 *and* E_1 *two restriction of* $E_{a,b}$ *over* $\mathbb{Q}$, *defined as follows*

$$E_0 = \{[X : Y : Z] \in P^2(\mathbb{Q}) | Y^2Z = X^3 - 675XZ^2 + 13662Z^3\},$$

and

$$E_1 = \{[X : Y : Z] \in P^2(\mathbb{Q}) | Y^2Z = X^3 - 27XZ^2 + 8694Z^3\}.$$

So, using the magma calculator, we find that

	$\triangle$	j	$E_i(\mathbb{Q})_{tor}$	*Generator of* $E_i(\mathbb{Q})_{tor}$
E_0	-2.14	$-\frac{5^6}{2.14}$	$\mathbb{Z}_6$	$(1, -2)$
E_1	-15	$-\frac{1}{15}$	$\mathbb{Z}_4$	$(15, 108)$

Hence

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

4.5 Conclusion

In this chapter, we have studied an elliptic curve $E_{a,b}$ 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 subgroups of this elliptic curve,

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

Chapter 5

The "Elliptic" matrices and a new kind of cryptography.

5.1 Introduction

In the paper [79], Varadharajan proposed a non-commutative group as a platform group for DH-key exchange, which was later cryptographically analyzed using eigenvalues and Jordan form in the paper [71]. Subsequently, the use of non-commutative groups and rings in public-key cryptography has attracted much attention [11, 20, 23, 89, 103].
In [103], A.chillali et al introduce a new cryptographic method based on a non-commutative group matrix over a finite field $\mathbb{F}_{p^n}$, where p is a prime number. As described in [34, 35, 54, 71, 72], some properties of matrices such as determinant, eigenvalues, and Cayley-Hamilton theorem can be used to develop attacks against this protocol. Such attacks reduce DLP on the group of invertible matrices to DLP on finite fields or to a simple factorization problem. To avoid this reduction of DLP on the matrix group to that on finite fields, we will introduce a matrix group over an elliptic curve and its diagonal in $\mathbb{Z}/n\mathbb{Z}$, under a new matrix multiplication operation, and consequently, go from DLP to $(ECDLP)$ which is the fundamental factor of elliptic curves cryptography and matching-based cryptography. It has been a major investigation area in number theory and cryptography for many decades [2, 5, 6, 48, 46, 100]. Hence, the main idea of this chapter [13] is the design of some public key exchange protocols over a noncommutative ring, in particular over the ring of "elliptic" matrix, whose security is based on $ECDLP$. In other words, we propose a new key exchange protocol based on matrices with the following form $M(B_1, B_2, B_3) = \begin{pmatrix} B_1 & B_2 \\ 0 & B_3 \end{pmatrix}$ called "elliptic" matrices, where B_1, B_2, B_3

are three-dimensional matrices constructed over an elliptic curve whose diagonal elements are in $\mathbb{Z}/n\mathbb{Z}$. In addition, we investigate the complexity and security of the key exchange protocol.

The rest of the chapter is organized as follows. In Sec. 5.2, we define the non-commutative ring of elliptic matrices and give an example of matrix multiplication on this ring. In Sec. 5.3, a key exchange protocol is explained and the security and complexity of the protocol are provided. In Sec. 5.4, we propose a numerical Example.

5.2 Ring of "elliptic" matrices

Let E be an elliptic curve over a finite field K, P is a point of order n and G is the group generated by P. In this section, we present the theoretical concept for our encryption scheme by using the matrix-ring $\aleph$, with the following form, $\aleph = \left\{ \begin{pmatrix} a_1 & P_1 & P_2 \\ Q_3 & a_2 & P_3 \\ Q_2 & Q_1 & a_3 \end{pmatrix} \mid a_i \in \mathbb{Z}/n\mathbb{Z},\ Q_i, P_i \in G,\ i \in \{1,2,3\} \right\}$

5.2.1 The ring $\aleph$

In this subsection, we will define on $\aleph$ two internal laws called addition $+$ and multiplication $\star$ as follows, let $X = \begin{pmatrix} a_1 & P_1 & P_2 \\ Q_3 & a_2 & P_3 \\ Q_2 & Q_1 & a_3 \end{pmatrix}$ and $Y = \begin{pmatrix} b_1 & P_1' & P_2' \\ Q_3' & b_2 & P_3' \\ Q_2' & Q_1' & b_3 \end{pmatrix}$ be two elements in $\aleph$. So,

$$X + Y = \begin{pmatrix} a_1 + b_1 & P_1 + P_1' & P_2 + P_2' \\ Q_3 + Q_3' & a_2 + b_2 & P_3 + P_3' \\ Q_2 + Q_2' & Q_1 + Q_1' & a_3 + b_3 \end{pmatrix},$$

$$X \star Y = \begin{pmatrix} a_1 b_1 & b_2 P_1 + a_1 P_1' & b_3 P_2 + a_1 P_2 \\ b_1 Q_3 + a_2 Q_3' & a_2 b_2 & b_3 P_3 + a_2 P_3 \\ b_1 Q_2 + a_3 Q_2' & b_2 Q_1 + a_3 Q_1' & a_3 b_3 \end{pmatrix}.$$

Lemma 26. *The set $\aleph$ together with addition "$+$" and multiplication "$\star$" is a unitary non-commutative ring with identities,*

$$1_\aleph = \begin{pmatrix} 1 & [0:1:0] & [0:1:0] \\ [0:1:0] & 1 & [0:1:0] \\ [0:1:0] & [0:1:0] & 1 \end{pmatrix} \text{ and } 0_\aleph = \begin{pmatrix} 0 & [0:1:0] & [0:1:0] \\ [0:1:0] & 0 & [0:1:0] \\ [0:1:0] & [0:1:0] & 0 \end{pmatrix}.$$

Proof.

Let $X = \begin{pmatrix} a_1 & P_1 & P_2 \\ Q_3 & a_2 & P_3 \\ Q_2 & Q_1 & a_3 \end{pmatrix}, Y = \begin{pmatrix} b_1 & P'_1 & P'_2 \\ Q'_3 & b_2 & P'_3 \\ Q'_2 & Q'_1 & b_3 \end{pmatrix}$ *and* $Z = \begin{pmatrix} c_1 & P"_1 & P"_2 \\ Q"_3 & c_2 & P"_3 \\ Q"_2 & Q"_1 & c_3 \end{pmatrix}$ be elements in $\aleph$, then

- Associative laws,

  We start with the product law " $\star$ ",

$$(X \star Y) \star Z = \begin{pmatrix} a_1b_1 & b_2P_1 + a_1P'_1 & b_3P_2 + a_1P'_2 \\ b_1Q_3 + a_2Q'_3 & a_2b_2 & b_3P_3 + a_2P'_3 \\ b_1Q_2 + a_3Q'_2 & b_2Q_1 + a_3Q'_1 & a_3b_3 \end{pmatrix} \star \begin{pmatrix} c_1 & P"_1 & P"_2 \\ Q"_3 & c_2 & P"_3 \\ Q"_2 & Q"_1 & c_3 \end{pmatrix}$$

$$= \begin{pmatrix} a_1b_1c_1 & b_2c_2P_1 + a_1c_2P'_1 + a_1b_1P"_1 & b_3c_3P_2 + a_1c_3P'_2 + a_1b_1P"_2 \\ b_1c_1Q_3 + a_2c_1Q'_3 + a_2b_2Q"_3 & a_2b_2c_2 & b_3c_3P_3 + a_2c_3P'_3 + a_2b_2P"_3 \\ b_1c_1Q_2 + a_3c_1Q'_2 + a_3b_3Q"_2 & b_2c_2Q_1 + a_3c_2Q'_1 + a_3b_3Q"_1 & a_3b_3c_3 \end{pmatrix}$$

  and,

$$X \star (Y \star Z) = \begin{pmatrix} a_1 & P_1 & P_2 \\ Q_3 & a_2 & P_3 \\ Q_2 & Q_1 & a_3 \end{pmatrix} \star \begin{pmatrix} b_1c_1 & c_2P'_1 + b_1P"_1 & c_3P'_2 + b_1P'_2 \\ c_1Q'_3 + b_2Q"_3 & b_2c_2 & c_3P'_3 + b_2P'_3 \\ c_1Q'_2 + b_3Q"_2 & c_2Q'_1 + b_3Q"_1 & b_3c_3 \end{pmatrix}$$

$$= \begin{pmatrix} a_1b_1c_1 & b_2c_2P_1 + a_1c_2P'_1 + a_1b_1P"_1 & b_3c_3P_2 + a_1c_3P'_2 + a_1b_1P"_2 \\ b_1c_1Q_3 + a_2c_1Q'_3 + a_2b_2Q"_3 & a_2b_2c_2 & b_3c_3P_3 + a_2c_3P'_3 + a_2b_2P"_3 \\ b_1c_1Q_2 + a_3c_1Q'_2 + a_3b_3Q"_2 & b_2c_2Q_1 + a_3c_2Q'_1 + a_3b_3Q"_1 & a_3b_3c_3 \end{pmatrix}.$$

  Hence, $(X \star Y) \star Z = X \star (Y \star Z)$.

  On the other hand, in the same way, we find that $(X + Y) + Z = X + (Y + Z)$.

- Distributive laws, we shall prove that $(X+Y) \star Z = X \star Z + Y \star Z$ and $\star\, Z \star (X+Y) = Z \star X + Z \star Y$.

  So, for the first equality $(X + Y) \star Z = X \star Z + Y \star Z$, we have

$$(X + Y) \star Z = \begin{pmatrix} a_1 + b_1 & P_1 + P'_1 & P_2 + P'_2 \\ Q_3 + Q'_3 & a_2 + b_2 & P_3 + P'_3 \\ Q_2 + Q'_2 & Q_1 + Q'_1 & a_3 + b_3 \end{pmatrix} \star \begin{pmatrix} c_1 & P"_1 & P"_2 \\ Q"_3 & c_2 & P"_3 \\ Q"_2 & Q"_1 & c_3 \end{pmatrix}$$

$$= \begin{pmatrix} (a_1 + b_1)c_1 & c_2(P_1 + P'_1) + (a_1 + b_1)P"_1 & c_3(P_2 + P'_2) + (a_1 + b_1)P"_2 \\ c_1(Q_3 + Q'_3) + (a_2 + b_2)Q"_3 & (a_2 + b_2)c_2 & c_3(P_3 + P'_3) + (a_2 + b_2)P"_3 \\ c_1(Q_2 + Q'_2) + (a_3 + b_3)Q"_2 & c_2(Q_1 + Q'_1) + (a_3 + b_3)Q"_1 & (a_3 + b_3)c_3 \end{pmatrix},$$

and, $X \star Z + Y \star Z =$

$$\begin{pmatrix} a_1c_1 + b_1c_1 & c_2P_1 + c_2P_1' + (a_1+b_1)P"_1 & c_3P_2 + c_3P_2' + (a_1+b_1)P"_2 \\ c_1Q_3 + c_1Q_3' + (a_2+b_2)Q"_3 & a_2c_2 + b_2c_2 & c_3P_3 + c_3P_3' + (a_2+b_2)P"_3 \\ c_1Q_2 + c_1Q_2' + (a_3+b_3)Q"_2 & c_2Q_1 + c_2Q_1' + (a_3+b_3)Q"_1 & a_3c_3 + b_3c_3 \end{pmatrix}.$$

Hence, $(X+Y) \star Z = X \star Z + Y \star Z$.
Similarly for the second equality.

- Additive inverses, $\forall X = \begin{pmatrix} a_1 & P_1 & P_2 \\ Q_3 & a_2 & P_3 \\ Q_2 & Q_1 & a_3 \end{pmatrix} \in \aleph$, we have $X + (-X) = 0_\aleph$, with $(-X) = \begin{pmatrix} -a_1 & -P_1 & -P_2 \\ -Q_3 & -a_2 & -P_3 \\ -Q_2 & -Q_1 & -a_3 \end{pmatrix}$ is called the additive inverse of X.

□

The next proposition characterize the set of invertible elements in $\aleph$.

Proposition 5.2.1. *Let* $X = \begin{pmatrix} a_1 & P_1 & P_2 \\ Q_3 & a_2 & P_3 \\ Q_2 & Q_1 & a_3 \end{pmatrix} \in \aleph$, *$X$ is invertible if only if* $gcd(a_i, n) = 1$ *for all* $i \in \{1,2,3\}$, *in this case we have,*

$$X^{\star(-1)} = \begin{pmatrix} a_1^{-1} & -a_1^{-1}a_2^{-1}P_1 & -a_1^{-1}a_3^{-1}P_2 \\ -a_1^{-1}a_2^{-1}Q_3 & a_2^{-1} & -a_2^{-1}a_3^{-1}P_3 \\ -a_1^{-1}a_3^{-1}Q_2 & -a_2^{-1}a_3^{-1}Q_1 & a_3^{-1} \end{pmatrix} \in \aleph.$$

Proof.
Let $Y = \begin{pmatrix} b_1 & P_1' & P_2' \\ Q_3' & b_2 & P_3' \\ Q_2' & Q_1' & b_3 \end{pmatrix}$ the inverse of X, we have

$$X \star Y = Y \star X = 1_\aleph.$$

So,

$$X \star Y = \begin{pmatrix} a_1b_1 & b_2P_1 + a_1P_1' & b_3P_2 + a_1P_2' \\ b_1Q_3 + a_2Q_3' & a_2b_2 & b_3P_3 + a_2P_3' \\ b_1Q_2 + a_3Q_2' & b_2Q_1 + a_3Q_1' & a_3b_3 \end{pmatrix} = \begin{pmatrix} 1 & [0:1:0] & [0:1:0] \\ [0:1:0] & 1 & [0:1:0] \\ [0:1:0] & [0:1:0] & 1 \end{pmatrix},$$

and

$$Y \star X = \begin{pmatrix} a_1b_1 & b_1P_1 + a_2P_1' & b_1P_2 + a_3P_2' \\ b_2Q_3 + a_1Q_3' & a_2b_2 & b_2P_3 + a_3P_3' \\ b_3Q_2 + a_1Q_2' & b_3Q_1 + a_2Q_1' & a_3b_3 \end{pmatrix} = \begin{pmatrix} 1 & [0:1:0] & [0:1:0] \\ [0:1:0] & 1 & [0:1:0] \\ [0:1:0] & [0:1:0] & 1 \end{pmatrix}.$$

Thus, $a_i b_i \equiv 1 \pmod{n}$ for all $i \in \{1,2,3\}$ and

$$\begin{aligned}
b_2P_1 + a_1P_1' &= [0:1:0],\\
b_3P_2 + a_1P_2' &= [0:1:0],\\
b_3P_3 + a_2P_3' &= [0:1:0],\\
b_2Q_1 + a_3Q_1' &= [0:1:0],\\
b_1Q_2 + a_3Q_2' &= [0:1:0],\\
b_1Q_3 + a_2Q_3' &= [0:1:0].
\end{aligned}$$

Therefore, X is invertible if only if $gcd(a_i, n) = 1$ for all $i \in \{1,2,3\}$, in this case we have, $b_i = a_i^{-1}$ for all $i \in \{1,2,3\}$ and

$$\begin{aligned}
P_1' &= -a_1^{-1}a_2^{-1}P_1,\\
P_2' &= -a_1^{-1}a_3^{-1}P_2,\\
P_3' &= -a_2^{-1}a_3^{-1}P_3,\\
Q_1' &= -a_3^{-1}a_2^{-1}Q_1,\\
Q_2' &= -a_3^{-1}a_1^{-1}Q_2,\\
Q_3' &= -a_2^{-1}a_1^{-1}Q_3.
\end{aligned}$$

So,

$$X^{\star(-1)} = \begin{pmatrix} a_1^{-1} & -a_1^{-1}a_2^{-1}P_1 & -a_1^{-1}a_3^{-1}P_2 \\ -a_1^{-1}a_2^{-1}Q_3 & a_2^{-1} & -a_2^{-1}a_3^{-1}P_3 \\ -a_1^{-1}a_3^{-1}Q_2 & -a_2^{-1}a_3^{-1}Q_1 & a_3^{-1} \end{pmatrix} \in \aleph.$$

□

Lemma 27. *Let k be a positive integer. Then if $X = \begin{pmatrix} a_1 & P_1 & P_2 \\ Q_3 & a_2 & P_3 \\ Q_2 & Q_1 & a_3 \end{pmatrix}$ is an element of $\aleph$, the k-power of X can be given by $X^{\star k} = \begin{pmatrix} a_1^k & \lambda_{1,k}P_1 & \lambda_{2,k}P_2 \\ \lambda_{1,k}Q_3 & a_2^k & \lambda_{3,k}P_3 \\ \lambda_{2,k}Q_2 & \lambda_{3,k}Q_1 & a_3^k \end{pmatrix}$, where*

$$\lambda_{1,k} = \sum_{i+j=k-1} a_1^i a_2^j \tag{5.1}$$

$$\lambda_{2,k} = \sum_{i+j=k-1} a_1^i a_3^j \tag{5.2}$$

$$\lambda_{3,k} = \sum_{i+j=k-1} a_2^i a_3^j \tag{5.3}$$

Proof.
Using a Proof by induction on k. For $k = 1$, we have $\lambda_{i,1} = 1$ for all $i \in \{1,2,3\}$, then

$X^{\star 1} = X$.
Let $k \geq 1$. Assume the induction hypothesis, for a given value $k \geq 1$, the single case

$$\lambda_{1,k} = \sum_{i+j=k-1} a_1^i a_2^j \tag{5.4}$$

$$\lambda_{2,k} = \sum_{i+j=k-1} a_1^i a_3^j \tag{5.5}$$

$$\lambda_{3,k} = \sum_{i+j=k-1} a_2^i a_3^j \tag{5.6}$$

is true, and proof that we have,

$$\lambda_{1,k+1} = \sum_{i+j=k} a_1^i a_2^j \tag{5.7}$$

$$\lambda_{2,k+1} = \sum_{i+j=k} a_1^i a_3^j \tag{5.8}$$

$$\lambda_{3,k+1} = \sum_{i+j=k} a_2^i a_3^j \tag{5.9}$$

So, we have

$$X^{\star(k+1)} = \begin{pmatrix} a_1^k & \lambda_{1,k}P_1 & \lambda_{2,k}P_2 \\ \lambda_{1,k}Q_3 & a_2^k & \lambda_{3,k}P_3 \\ \lambda_{2,k}Q_2 & \lambda_{3,k}Q_1 & a_3^k \end{pmatrix} \star \begin{pmatrix} a_1 & P_1 & P_2 \\ Q_3 & a_2 & P_3 \\ Q_2 & Q_1 & a_3 \end{pmatrix}.$$

Then,

$$X^{\star(k+1)} = \begin{pmatrix} a_1^{k+1} & (a_1^k + a_2\lambda_{1,k})P_1 & (a_1^k + a_3\lambda_{2,k})P_2 \\ (a_2^k + a_1\lambda_{1,k})Q_3 & a_2^{k+1} & (a_2^k + a_3\lambda_{3,k})P_3 \\ (a_3^k + a_1\lambda_{2,k})Q_2 & (a_3^k + a_2\lambda_{3,k})Q_1 & a_3^{k+1} \end{pmatrix}.$$

Thus,

$$\begin{aligned} \lambda_{1,k+1} &= a_1^k + a_2\lambda_{1,k} = a_1^k + a_2 \sum_{i+j=k-1} a_1^i a_2^j \\ &= \sum_{i+j=k} a_1^i a_2^j \\ \lambda_{2,k+1} &= a_1^k + a_3\lambda_{2,k} = a_1^k + a_3 \sum_{i+j=k-1} a_1^i a_3^j \\ &= \sum_{i+j=k} a_1^i a_3^j \\ \lambda_{3,k+1} &= a_2^k + a_3\lambda_{3,k} = a_2^k + a_3 \sum_{i+j=k-1} a_2^i a_3^j \\ &= \sum_{i+j=k} a_2^i a_3^j \end{aligned}$$

We conclude that, $\forall k \geq 1$,

$$\lambda_{1,k} = \sum_{i+j=k-1} a_1^i a_2^j$$
$$\lambda_{2,k} = \sum_{i+j=k-1} a_1^i a_3^j$$
$$\lambda_{3,k} = \sum_{i+j=k-1} a_2^i a_3^j$$

Hence the result. □

We have $\star$ is a non-commutative law, so in the following proposition we will characterize the set of matrices in $\aleph$ that commute with such a matrix $X = \begin{pmatrix} a_1 & n_1P & n_2P \\ m_3P & a_2 & n_3P \\ m_2P & m_1P & a_3 \end{pmatrix}$.

Definition 5.2.1. *The centralizer of the matrix X over $\aleph$ is defined as follows*

$$\mathrm{C}_{\aleph}(X) = \{Y \in \aleph \mid X \star Y = Y \star X\}.$$

Proposition 5.2.2. *With the same notation as above, we have*

$$Y = \begin{pmatrix} b_1 & e_1P & e_2P \\ f_3P & b_2 & e_3P \\ f_2P & f_1P & b_3 \end{pmatrix} \in \mathrm{C}_{\aleph}(X)$$

such that

1 *If* $a_1 \equiv a_2 \pmod{n}$ *and* $a_2 - a_3 \neq 0$, *then* $\begin{cases} b_1 \equiv b_2 \pmod{n} \\ n_2f_2 \equiv m_2e_2 \pmod{n} \\ n_3f_1 \equiv m_1e_3 \pmod{n} \end{cases}$.

2 *If* $a_i \equiv a_j \pmod{n}$ *for* $i \neq j$, *then* $b_i \equiv b_j \pmod{n}$ *for* $i \neq j$.

3 *If* $a_i - a_j \neq 0$ *for* $i \neq j$, *then* $\begin{cases} n_1f_3 \equiv m_3e_1 \pmod{n} \\ n_2f_2 \equiv m_2e_2 \pmod{n} \\ n_3f_1 \equiv m_1e_3 \pmod{n} \end{cases}$.

Proof.

Since,

$$X \star Y = \begin{pmatrix} a_1b_1 & b_2n_1P + a_1e_1P & b_3n_2P + a_1e_2P \\ b_1m_3P + a_2f_3P & a_2b_2 & b_3n_3P + a_2e_3P \\ b_1m_2P + a_3f_2P & b_2m_1P + a_3f_1P & a_3b_3 \end{pmatrix},$$

and

$$Y \star X = \begin{pmatrix} a_1b_1 & b_1n_1P + a_2e_1P & b_1n_2P + a_3e_2P \\ b_2m_3P + a_1f_3P & a_2b_2 & b_2n_3P + a_3e_3P \\ b_3m_2P + a_1f_2P & b_3m_1P + a_2f_1P & a_3b_3 \end{pmatrix}.$$

Subsequently, we can determine the result through comparative calculations. □

5.2.2 The "elliptic" matrices

In the following, we present the theoretical concept for our encryption scheme by using the elliptic matrix $M(B_1, B_2, B_3) = \begin{pmatrix} B_1 & B_2 \\ 0 & B_3 \end{pmatrix}$ where $B_i \in \aleph$ for all $i \in \{1, 2, 3\}$.

Lemma 28. *With the same notations as above, we have the k-power of an elliptic matrix as follows,*

$$M(B_1, B_2, B_3)^{\star k} = \begin{pmatrix} B_1^{\star k} & T_k \\ 0 & B_3^{\star k} \end{pmatrix} \quad for\ all\ \ k \in \mathbb{N}^*$$

with $T_k = \sum_{i=0}^{k-1} B_1^{\star(k-1-i)} B_2 B_3^{\star i}$.

Proof.
Fix an arbitrary matrices B_1, B_2 and B_3 in $\aleph$, and let $M(B_1, B_2, B_3)^k$ be the statement. We induct on k. Then

$$\begin{aligned} M(B_1, B_2, B_3)^{\star 1} &= \begin{pmatrix} B_1^{\star 1} & T_1 \\ 0 & B_3^{\star 1} \end{pmatrix} \\ &= \begin{pmatrix} B_1 & B_2 \\ 0 & B_3 \end{pmatrix} \\ &= M(B_1, B_2, B_3) \end{aligned}$$

then our Lemma is true for $k = 1$.
We assume the recurrence hypothesis, $M(B_1, B_2, B_3)^{\star k} = \begin{pmatrix} B_1^{\star k} & T_k \\ 0 & B_3^{\star k} \end{pmatrix}$ for certain k.

So, We have

$$
\begin{aligned}
M(B_1,B_2,B_3)^{\star(k+1)} &= (M(B_1,B_2,B_3))^{\star k} \star M(B_1,B_2,B_3) \\
&= \begin{pmatrix} B_1^{\star k} & T_k \\ 0 & B_3^{\star k} \end{pmatrix} \star \begin{pmatrix} B_1 & B_2 \\ 0 & B_3 \end{pmatrix} \\
&= \begin{pmatrix} B_1^{\star k} \star B_1 & B_1^k B_2 + T_k \star B_3 \\ 0 & B_3^{\star k} \star B_3 \end{pmatrix} \\
&= \begin{pmatrix} B_1^{\star(k+1)} & B_1^k B_2 + (\sum_{i=0}^{k-1} B_1^{\star(k-1-i)} B_2 B_3^{\star i}) \star B_3 \\ 0 & B_3^{\star(k+1)} \end{pmatrix} \\
&= \begin{pmatrix} B_1^{\star(k+1)} & B_1^k B_2 + \sum_{i=0}^{k-1} B_1^{\star(k-1-i)} B_2 B_3^{\star(i+1)} \\ 0 & B_3^{\star(k+1)} \end{pmatrix} \\
&= \begin{pmatrix} B_1^{\star(k+1)} & B_1^k B_2 + \sum_{j=1}^{k} B_1^{\star(k-j)} B_2 B_3^{\star j} \\ 0 & B_3^{\star(k+1)} \end{pmatrix} \\
&= \begin{pmatrix} B_1^{\star(k+1)} & \sum_{j=0}^{k} B_1^{\star(k-j)} B_2 B_3^{\star j} \\ 0 & B_3^{\star(k+1)} \end{pmatrix} \\
&= \begin{pmatrix} B_1^{\star(k+1)} & T_{k+1} \\ 0 & B_3^{\star(k+1)} \end{pmatrix}
\end{aligned}
$$

Hence the result. □

5.3 Encryption Schemes using the "elliptic" matrices

In this section we will construct an encryption scheme using the matrix $M(B_1, B_2, B_3)$.

5.3.1 Cryptographic Protocols

This sub-section describes some public-key encryption and key establishment schemes. Surveys the state-of-the-art in algorithms for solving the following classical problem (ECDLP) find an integer a, if it exists, such that $Q = aP$, with P and Q being well-defined points of this elliptic curve, whose intractability is necessary for the security of our cryptographic schemes.

5.3.1.1 Public-key encryption

Key exchange protocol
Alice and **Bob** agree on a public prime number p and a point P over an elliptic curve

$E(\mathbb{F}_q)$ of order n, where q is a power of p.
First **Alice** chooses two matrices $(A, A_1) \in \aleph$ and publish the pair $(A, \mathrm{C}_\aleph(A_1))$, in the same way, **Bob** chooses two matrices $(B, B_2) \in \aleph$ and publish the pair $(B, \mathrm{C}_\aleph(B_2))$.

Alice chooses private keys: $k \in \mathbb{N}^*$ and $A_2 \in \mathrm{C}_\aleph(B_2)$. She calculated the matrix

$$(M(A_1, A+B, A_2))^{\star k} = \begin{pmatrix} A_1^{\star k} & T_k \\ 0 & A_2^{\star k} \end{pmatrix}$$

and send T_k to **Bob**.

In turn, **Bob** chooses private keys, $t \in \mathbb{N}^*$ and $B_1 \in \mathrm{C}_\aleph(A_1)$. He calculated the matrix

$$(M(B_1, A+B, B_2))^{\star t} = \begin{pmatrix} B_1^{\star t} & E_t \\ 0 & B_2^{\star t} \end{pmatrix}$$

and send E_t to **Alice**.

With their private keys k and t, **Alice** and **Bob** calculate separately the matrices:

$$\textbf{Alice}: M(A_1, E_t, A_2)^{\star k} = \begin{pmatrix} A_1^{\star k} & E_{t,k} \\ 0 & A_2^{\star k} \end{pmatrix} \tag{5.10}$$

$$\textbf{Bob}: M(B_1, T_k, B_2)^{\star t} = \begin{pmatrix} B_1^{\star t} & T_{k,t} \\ 0 & B_2^{\star t} \end{pmatrix} \tag{5.11}$$

Lemma 29. *With the same notation as above, we have $E_{t,k} = T_{k,t}$.*

Proof.
We have,

$$\begin{aligned} T_{k,t} &= \sum_{i=0}^{t-1} B_1^{t-i-1} T_k B_2^i \\ &= \sum_{i=0}^{t-1} B_1^{t-i-1} \left(\sum_{j=0}^{k-1} A_1^{k-1-j} (A+B) A_2^j \right) B_2^i \\ &= \sum_{i=0}^{t-1} \sum_{j=0}^{k-1} B_1^{t-i-1} A_1^{k-1-j} (A+B) A_2^j B_2^i \end{aligned}$$

and

$$\begin{aligned} E_{t,k} &= \sum_{j=0}^{k-1} A_1^{k-j-1} E_t A_2^j \\ &= \sum_{j=0}^{k-1} A_1^{k-j-1} \left(\sum_{i=0}^{t-1} B_1^{t-1-i} (A+B) B_2^i \right) A_2^j \\ &= \sum_{j=0}^{k-1} \sum_{i=0}^{t-1} A_1^{k-j-1} B_1^{t-1-i} (A+B) B_2^i A_2^j \end{aligned}$$

Or, $B_1 \in \mathrm{C}_{\aleph}(A_1)$ and $A_2 \in \mathrm{C}_{\aleph}(B_2)$, it follows that $T_{k,t} = E_{t,k}$. □

Corollary 19. *The secret key of **Alice** and **Bob** is the matrix* $\Phi = E_{t,k} = T_{k,t}$.

5.3.2 Security of this protocol

The set $\mathrm{C}_{\aleph}(B_2)$, $\mathrm{C}_{\aleph}(A_1)$ and the matrices A, B are public. If another person wants to compute the secret key Φ, it must solve the following equation:
$\sum_{i=0}^{k-1} A_1^{k-1-i}(A+B)A_2^i = T_k$ whose unknowns the matrices A_1, A_2 and the natural number k.
In other words, to find the key, it is necessary (not sufficient) to solve the following classical problem, find an integer a, if it exists, such that $Q = aP$ $(ECDLP)$.

Proposition 5.3.1. *The complexity to calculate the key* Φ *is* $\mathcal{O}\left(3^{tk}\right)$.

Proof.
The encryption scheme using a matrix over $\aleph$ of order 3, will use a key Φ of size $O(3)$, as described previously. Since

$$\Phi = \sum_{i=0}^{k-1} \sum_{j=0}^{t-1} A_1^{t-1-j} B_1^{k-1-i} (A+B) B_2^i A_2^j,$$

we have the complexity to calculate the key Φ is $\mathcal{O}\left(3^{tk}\right)$. □

5.3.3 Encryption of message

Let Φ be a secret key exchanged by **Alice** and **Bob**. If Φ is invertible, let ∇ be the message that **Alice** wants to send to **Bob**, ∇ is a matrix of the same size as Φ. The encryption message

$$\triangle = e_{\Phi}(\nabla) = \Phi \star \nabla \star \Phi^{-1}$$

Otherwise, we return to the key exchange protocol.

Lemma 30. *Let ∇_1, ∇_2 be two messages and for all invertible key not equal to the unit matrix, Φ, we have:*

$$e_\Phi(\nabla_1 + \nabla_2) = e_\Phi(\nabla_1) + e_\Phi(\nabla_2),$$
$$e_\Phi(\nabla_1 \star \nabla_2) = e_\Phi(\nabla_1) \star e_\Phi(\nabla_2).$$

Proof.
We have:

$$\begin{aligned} e_\Phi(\nabla_1 + \nabla_2) &= \Phi \star (\nabla_1 + \nabla_2) \star \Phi^{-1} \\ &= (\Phi \star \nabla_1 + \Phi \star \nabla_2) \star \Phi^{-1} \\ &= \Phi \star \nabla_1 \star \Phi^{-1} + \Phi \star \nabla_2 \star \Phi^{-1} \\ &= e_\Phi(\nabla_1) + e_\Phi(\nabla_2) \end{aligned}$$

and

$$\begin{aligned} e_\Phi(\nabla_1 \star \nabla_2) &= \Phi \star (\nabla_1 \star \nabla_2) \star \Phi^{-1} \\ &= \Phi \star \nabla_1 \star \Phi^{-1} \star \Phi \star \nabla_2 \star \Phi^{-1} \\ &= e_\Phi(\nabla_1) \star e_\Phi(\nabla_2). \end{aligned}$$

□

Remark 9. *This encryption message is a fully homomorphic encryption that allows calculations to be performed on the ciphertext, producing an encrypted result that, when decrypted, matches the result of the operations performed on the plaintext.*

5.3.4 Decryption of message

When **Bob** receives the encrypted message $\triangle$ sent by **Alice**, it uses a decryption function to decrypt it. This function noted d_Φ is defined as follows:

$$d_\Phi(\triangle) = \Phi^{-1} \star \nabla \star \Phi.$$

Lemma 31. *For all message ∇, we have $d_\Phi \circ e_\Phi(\nabla) = \nabla$.*

Proof.
We have:

$$\begin{aligned} d_\Phi \circ e_\Phi(\nabla) &= d_\Phi(e_\Phi(\nabla)) \\ &= \Phi^{-1} \star e_\Phi(\nabla) \star \Phi \\ &= \Phi^{-1} \star \Phi \star \nabla \star \Phi^{-1} \star \Phi \\ &= \nabla. \end{aligned}$$

□

Remark 10. *The security of this Cryptosystem is based on*
- *The difficulty in computing the key Φ whose complexity is $\mathcal{O}\left(3^{tk}\right)$.*
- *The $(ECDLP)$ problem.*

5.4 Numerical example

Alice and **Bob** choose a large prime number p, $r \in \mathbb{N}^*$ and a point P over an elliptic curve $E(\mathbb{F}_{p^r})$ of a large order $n > 10^{32}$.

First **Alice** chooses two matrices in $\aleph$,

$$A = \begin{pmatrix} 1 & P_{1,A} & P_{2,A} \\ Q_{3,A} & 2 & P_{3,A} \\ Q_{2,A} & Q_{1,A} & 3 \end{pmatrix}, \quad A_1 = \begin{pmatrix} 1 & P_{1,A_1} & P_{2,A_1} \\ Q_{3,A_1} & 2 & P_{3,A_1} \\ Q_{2,A_1} & Q_{1,A_1} & 3 \end{pmatrix}$$

and publish the pair $(A, \mathrm{C}_{\aleph}(A_1))$, in the same way, **Bob** chooses two matrices in $\aleph$,

$$B = \begin{pmatrix} 5 & P_{1,B} & P_{2,B} \\ Q_{3,B} & 2 & P_{3,B} \\ Q_{2,B} & Q_{1,B} & 3 \end{pmatrix}, \quad B_2 = \begin{pmatrix} 3 & P_{1,B_2} & P_{2,B_2} \\ Q_{3,B_2} & 4 & P_{3,B_2} \\ Q_{2,B_2} & Q_{1,B_2} & 2 \end{pmatrix}$$

and publish the pair $(B, \mathrm{C}_{\aleph}(B_2))$.

To simplify the verification of our method, we will give the points of the matrices A, B, A_1 *and* B_2 as a function of the point P.
So, consider

$$A = \begin{pmatrix} 1 & P & P \\ 2P & 2 & P \\ 2P & 2P & 3 \end{pmatrix}, \quad B = \begin{pmatrix} 5 & 2P & P \\ 2P & 2 & O \\ 2P & O & 3 \end{pmatrix}$$

$$A_1 = \begin{pmatrix} 1 & P & 2P \\ 3P & 2 & 3P \\ 2P & P & 3 \end{pmatrix}, \quad B_2 = \begin{pmatrix} 3 & P & P \\ P & 4 & 2P \\ P & 5P & 2 \end{pmatrix}.$$

Alice choose a private keys, $k = 19$, and a matrix

$$A_2 = \begin{pmatrix} 2 & P & P \\ P & 3 & 2P \\ P & 5P & 1 \end{pmatrix} \in \mathrm{C}_{\aleph}(B_2).$$

She calculated the matrix

$$(M(A_1, A + B, A_2))^{\star 19} = \begin{pmatrix} A_1^{\star 19} & T_{19} \\ 0 & A_2^{\star 19} \end{pmatrix}$$

where

$$T_{19} = \sum_{i=0}^{18} A_1^{\star(18-i)}(A+B)A_2^{\star i} \tag{5.12}$$

$$= \begin{pmatrix} 3145722 & 7549456659P & 3489929930P \\ 4727164798P & 4646948716 & 15096291883P \\ 15097864744P & 141216865400P & 3486784398 \end{pmatrix} \tag{5.13}$$

and send it to **Bob**.

In turn, **Bob** choose a private keys, $t = 28$, and a matrix $B_1 = \begin{pmatrix} 1 & 2P & 4P \\ 6P & 3 & 6P \\ 4P & 2P & 5 \end{pmatrix} \in$ $\mathrm{C}_{\aleph}(A_1)$. He calculated the matrix

$$(M(B_1, A+B, B_2))^{\star 28} = \begin{pmatrix} B_1^{\star 28} & E_{28} \\ 0 & B_2^{\star 28} \end{pmatrix}$$

where
$E_{28} = \sum_{i=0}^{27} B_1^{\star(27-i)}(A+B)B_2^{\star i}$
$= \begin{pmatrix} 68630377364880 & 408166228667740245P & 74505874596394420668P \\ 291776278982230708P & 288138868981891900 & 2238050763680817133 09P \\ 2235171662635347100 94P & 5942450994114700487 24P & 74505805968701410338 \end{pmatrix}$
and send it to **Alice**.
With their private keys k and t, **Alice** and **Bob** calculate separately the matrices:

$$\textbf{Alice}: M(A_1, E_{28}, A_2)^{\star 19} = \begin{pmatrix} A_1^{\star 19} & E_{28,19} \\ 0 & A_2^{\star 19} \end{pmatrix} \tag{5.14}$$

$$\textbf{Bob}: M(B_1, T_{19}, B_2)^{\star 28} = \begin{pmatrix} B_1^{\star 28} & T_{19,28} \\ 0 & B_2^{\star 28} \end{pmatrix} \tag{5.15}$$

where, $E_{28,19} = \begin{pmatrix} a_1 & a_2P & a_3P \\ a_4P & a_5 & a_6P \\ a_7P & a_8P & a_9 \end{pmatrix}$
with,
$a_1 = 35982014657500840560$
$a_2 = 40453307156505458267653465$
$a_3 = 43297613671329240254353821864$
$a_4 = 33476067133353887752848 6148$
$a_5 = 33474163681127369798895 0100$
$a_6 = 13022758229098180352065 7526727$
$a_7 = 30292683309740507666883 64256534$
$a_8 = 56388651240331160584423 40338994$

$a_9 = 432976136353472256478557177 54$ and, $T_{19,28} = \begin{pmatrix} b_1 & b_2P & b_3P \\ b_4P & b_5 & b_6P \\ b_7P & b_8P & b_9 \end{pmatrix}$

with,

$b_1 = 35982014657500840560$

$b_2 = 40453307156505458267653465$

$b_3 = 432976136713292402543538218 64$

$b_4 = 33476067133353887752848 6148$

$b_5 = 33474163681127369798895 0100$

$b_6 = 13022758229098180352065752 6727$

$b_7 = 30292683309740507668836425 6534$

$b_8 = 56388651240331160584423403 38994$

$b_9 = 432976136353472256478557177 54$. Hence, $E_{28,19} = T_{19,28}$.

Remark 11. *In this example, we have constructed a large private key* $\Phi = \begin{pmatrix} a_1 & a_2P & a_3P \\ a_4P & a_5 & a_6P \\ a_7P & a_8P & a_9 \end{pmatrix}$

where,

$a_1 = 35982014657500840560$

$a_2 = 40453307156505458267653465$

$a_3 = 432976136713292402543538218 64$

$a_4 = 33476067133353887752848 6148$

$a_5 = 33474163681127369798895 0100$

$a_6 = 13022758229098180352065752 6727$

$a_7 = 30292683309740507668836425 6534$

$a_8 = 56388651240331160584423403 38994$

$a_9 = 432976136353472256478557177 54$

from small private keys $k = 19$ *and* $l = 28$.

Chapter 6

Elliptic curve and k-Fibonacci-like sequence

6.1 Introduction

The Fibonacci sequence $\{F_n\}$ is defined by the recurrence relation

$$F_n = F_{n-1} + F_{n-2} \text{ for } n \geq 2,$$

with $F_0 = 0$ and $F_1 = 1$. Several authors have studied this sequence and have introduced new sequences associated with it, we mention some of them here. Falcon and Plaza [40] introduced and studied the k-Fibonacci sequence. Two years later the Fibonacci sequence was generalized by Edson and Yayenie [32], and proved some related identities. The study of recurrence sequences in algebraic structures began with the early work of Wall [98] studying regular Fibonacci sequence in cyclic groups. The theory has been extended to some specific linear recurrence sequences by several authors, see for example [28, 40, 57, 80, 81, 102]. Deveci and Shannon [30] extended the theory to the quaternions. They also introduce the complex-type k-Fibonacci sequence and give some applications in [31]. Thus, our goal in this chapter [15] is to extend the theory to a group generated by a point on an elliptic curve.
Furthermore, we introduce a modified k-Fibonacci-like sequence defined over an elliptic curve called "Elliptic" k-Fibonacci-like sequence and prove Binet's formula for this sequence. We also give a new encryption scheme using this k-Fibonacci-like sequence. Note that as described in [8, 21, 13], Elliptic Curve Cryptography (ECC) is an approach to public-key cryptography that relies on the algebraic structure of elliptic curves over finite fields. Here we use an approach that blends ECC with k-Fibonacci-like sequence. Thus

we obtain a secure protocol based on ECDLP, which is the key factor for elliptic curve coding and adaptive coding. Note that the theoretical properties of numbers as obtained from homogeneous linear reccurence relations in the context of this article have recently been studied by several authors, see for example [29, 59, 60, 61, 82, 90, 91, 96].

6.2 The modified k-Fibonacci-like sequence

In this section, we will define the k-Fibonacci-like sequence over elliptic curves. We will also introduce and prove Binet's formula for this sequence.

Definition 6.2.1. *(Falcon, [39]) Let k be a positive integer. Thus, the k-Fibonacci sequence $\{F_{k,n}\}$ is given by the following recurrence relation*

$$F_{k,n} = kF_{k,n-1} + F_{k,n-2} \text{ for } n \geq 2,$$

with $F_{k,0} = 0$ and $F_{k,1} = 1$.

A few k-Fibonacci numbers are

$$F_{k,2} = k,\ F_{k,3} = k^2 + 1,\ F_{k,4} = k^3 + 2k,\ F_{k,5} = k^4 + 3k^2 + 1, \ldots$$

In the following definition, we will define the modified k-Fibonacci-like sequence that we will call the "Elliptic" k-Fibonacci-like sequence.

Definition 6.2.2. *Let E be an elliptic curve over a finite field $\mathbb{F}_q$, Θ be a point over E of order n and G is the group generated by Θ. Thus, for $\chi, \psi \in G$ and $k \in \{0, 1, ..., q-1\}$, the "Elliptic" k-Fibonacci-like sequence $\{N_{k,n}\}$ is defined by the recurrence relation*

$$N_{k,n+1} = kN_{k,n} + N_{k,n-1} \text{ for } n \geq 2,$$

with $N_{k,0} = 2(k+1)\psi$ and $N_{k,1} = k\chi + k(k+1)\psi$.
The first few "Elliptic" k-Fibonacci-like points are

$$\begin{aligned} N_{k,2} &= k^2\chi + (k+1)(k^2+2)\psi, \\ N_{k,3} &= k(k^2+1)\chi + k(k+1)(k^2+3)\psi, \\ N_{k,4} &= k^2(k^2+2)\chi + (k+1)(k^4+4k^2+2)\psi. \end{aligned}$$

Example 6.2.1. • *Case $k = 1$. We obtain*

$$N_{1,0} = 4\psi,\ N_{1,1} = \chi + 2\psi,\ \text{and } N_{1,n} = N_{1,n-1} + N_{1,n-2} \text{ for } n \geq 2.$$

The first few "Elliptic" 1-Fibonacci-like points are

$$\begin{aligned} N_{1,2} &= \chi + 6\psi, \\ N_{1,3} &= 2\chi + 8\psi, \\ N_{1,4} &= 3\chi + 14\psi. \end{aligned}$$

- *Case $k = 2$. We obtain*

$$N_{2,0} = 6\psi,\ N_{2,1} = 2\chi + 6\psi,\ \textit{and}\ N_{2,n} = 2N_{2,n-1} + N_{2,n-2}\ \textit{for}\ n \geq 2.$$

The first few "Elliptic" 2-Fibonacci-like points are

$$\begin{aligned} N_{2,2} &= 4\chi + 18\psi, \\ N_{2,3} &= 10\chi + 42\psi, \\ N_{2,4} &= 24\chi + 102\psi. \end{aligned}$$

6.2.1 Binet's formula

Binet's formulas are well known in the study of sequences such as the Fibonacci sequence [33, 32, 39, 65, 66].

Theorem 6.2.1. *(Falcon, [39]) The nth k-Fibonacci number is given by*

$$F_{k,n} = \frac{\alpha^n - \beta^n}{\alpha - \beta},$$

where α, β are the roots of the characteristic equation $x^2 - kx - 1 = 0$, and $\alpha > \beta$.

In this section, we will introduce and prove Binet's formula for our sequence. Binet's formula for this sequence allows us to express it in terms of the roots α and β of the characteristic equation $x^2 - kx - 1 = 0$ $(\alpha > \beta)$. Note that the roots of the characteristic equation are

$$\alpha = \frac{k + \sqrt{k^2+4}}{2}\ \textit{and}\ \beta = \frac{k - \sqrt{k^2+4}}{2}.$$

Therefore, $\beta < 0 < \alpha$, $\alpha + \beta = k$ and $\alpha\beta = -1$. So, Binet's formula for the "Elliptic" k-Fibonacci-like sequence is as follows.

Theorem 6.2.2. *The nth "Elliptic" k-Fibonacci-like sequence $N_{k,n}$ can be written in the following form*

$$N_{k,n} = k\left(\frac{\alpha^n - \beta^n}{\alpha - \beta}\right)(\chi + (k+1)\psi) + 2(k+1)\left(\frac{\alpha^{n-1} - \beta^{n-1}}{\alpha - \beta}\right)\psi.$$

Proof.
We employ proof by induction on n to demonstrate our argument. For $n = 0$ or 1, we have $N_{k,0} = 2(k+1)\psi$ and $N_{k,1} = k\chi + k(k+1)\psi$.
Let $n \geq 2$. Assuming the induction hypothesis, for a given value $n \geq 2$, the single case

$$N_{k,n} = k\left(\frac{\alpha^n - \beta^n}{\alpha - \beta}\right)(\chi + (k+1)\psi) + 2(k+1)\left(\frac{\alpha^{n-1} - \beta^{n-1}}{\alpha - \beta}\right)\psi$$

is true, and shows that we have,

$$N_{k,n+1} = k\left(\frac{\alpha^{n+1}-\beta^{n+1}}{\alpha-\beta}\right)(\chi+(k+1)\psi)+2(k+1)\left(\frac{\alpha^{n}-\beta^{n}}{\alpha-\beta}\right)\psi.$$

So, we have

$$\begin{aligned}
N_{k,n+1} &= kN_{k,n}+N_{k,n-1}\\
&= k(kF_{k,n}(\chi+(k+1)\psi)+2(k+1)F_{k,n-1}\psi)+kF_{k,n-1}(\chi+(k+1)\psi)\\
&+2(k+1)F_{k,n-2}\psi\\
&= k(kF_{k,n}+F_{k,n-1})(\chi+(k+1)\psi)+2(k+1)(kF_{k,n-1}+F_{k,n-2})\psi\\
&= kF_{k,n+1}(\chi+(k+1)\psi)+2(k+1)F_{k,n}\psi.
\end{aligned}$$

Hence,

$$\begin{aligned}
N_{k,n} &= kF_{k,n}(\chi+(k+1)\psi)+2(k+1)F_{k,n-1}\psi\\
&= k\left(\frac{\alpha^{n}-\beta^{n}}{\alpha-\beta}\right)(\chi+(k+1)\psi)+2(k+1)\left(\frac{\alpha^{n-1}-\beta^{n-1}}{\alpha-\beta}\right)\psi.
\end{aligned}$$

□

For choosing the points ψ and χ on a well-defined elliptic curve. In the next section, we will present the theoretical concept for our study using an "Elliptic" matrix [13] of the form $M(B_1,B_2,B_3) = \begin{pmatrix} B_1 & B_2 \\ 0 & B_3 \end{pmatrix}$ such that $B_i \in \aleph = \left\{ \begin{pmatrix} a_1 & P \\ Q & a_2 \end{pmatrix} \mid a_1,\ a_2 \in \mathbb{Z}_n,\ Q,\ P \in G \right\}$ for all $i \in \{1,2,3\}$, where G is a finite subgroup over an elliptic curve E of order n.

6.2.2 The best candidate among the points of an elliptic curve

Let E be an elliptic curve over a finite field $\mathbb{F}_q$, Θ is a point of order n and G is the group generated by Θ. So, we will define on $\aleph$ two internal laws called addition $+$ and multiplication $\star$ as follows, let $X = \begin{pmatrix} a_1 & P \\ Q & a_2 \end{pmatrix}$ and $Y = \begin{pmatrix} b_1 & P' \\ Q' & b_2 \end{pmatrix}$ be two elements in $\aleph$. So,

$$X+Y = \begin{pmatrix} a_1+b_1 & P+P' \\ Q+Q' & a_2+b_2 \end{pmatrix},$$

$$X\star Y = \begin{pmatrix} a_1b_1 & b_2P+a_1P' \\ b_1Q+a_2Q' & a_2b_2 \end{pmatrix}.$$

For more details on these laws, see [13].

Lemma 32. *The set* $\aleph$ *together with addition* " $+$ " *and multiplication* " $\star$ " *is a unitary non-commutative ring with identities,*

$$1_{\aleph} = \begin{pmatrix} 1 & [0:1:0] \\ [0:1:0] & 1 \end{pmatrix} \text{ and } 0_{\aleph} = \begin{pmatrix} 0 & [0:1:0] \\ [0:1:0] & 0 \end{pmatrix}.$$

The next proposition characterize the set of invertible elements in $\aleph$.

Proposition 6.2.1. *Let* $X = \begin{pmatrix} a_1 & P \\ Q & a_2 \end{pmatrix} \in \aleph$, *$X$ is invertible if only if* $gcd(a_i, n) = 1$ *for all* $i \in \{1, 2\}$, *in this case we have,*

$$X^{\star(-1)} = \begin{pmatrix} a_1^{-1} & -a_1^{-1}a_2^{-1}P \\ -a_1^{-1}a_2^{-1}Q & a_2^{-1} \end{pmatrix} \in \aleph.$$

Proof.
Let $Y = \begin{pmatrix} b_1 & P' \\ Q' & b_2 \end{pmatrix}$ be the inverse of X, we have:

$$X \star Y = Y \star X = 1_{\aleph}.$$

So,

$$X \star Y = \begin{pmatrix} a_1b_1 & b_2P + a_1P' \\ b_1Q + a_2Q' & a_2b_2 \end{pmatrix} = \begin{pmatrix} 1 & [0:1:0] \\ [0:1:0] & 1 \end{pmatrix},$$

and

$$Y \star X = \begin{pmatrix} a_1b_1 & b_1P + a_2P' \\ b_2Q + a_1Q' & a_2b_2 \end{pmatrix} = \begin{pmatrix} 1 & [0:1:0] \\ [0:1:0] & 1 \end{pmatrix}.$$

Thus, $a_ib_i \equiv 1 \pmod{n}$ for all $i \in \{1, 2\}$ and

$$\begin{aligned} b_2P + a_1P' &= [0:1:0], \\ b_1P + a_2P' &= [0:1:0], \\ b_1Q + a_2Q' &= [0:1:0], \\ b_2Q + a_1Q' &= [0:1:0]. \end{aligned}$$

Therefore, X is invertible if and only if $gcd(a_i, n) = 1$ for all $i \in \{1, 2\}$, in this case we have, $b_i = a_i^{-1}$ for all $i \in \{1, 2\}$ and

$$\begin{aligned} P' &= -a_1^{-1}a_2^{-1}P, \\ Q' &= -a_2^{-1}a_1^{-1}Q. \end{aligned}$$

So,

$$X^{\star(-1)} = \begin{pmatrix} a_1^{-1} & -a_1^{-1}a_2^{-1}P \\ -a_1^{-1}a_2^{-1}Q & a_2^{-1} \end{pmatrix} \in \aleph.$$

□

Lemma 33. *Let k be a positive integer. Then if $X = \begin{pmatrix} a_1 & P \\ Q & a_2 \end{pmatrix}$ is an element of $\aleph$, the k-power of X can be given by $X^{\star k} = \begin{pmatrix} a_1^k & \lambda_k P \\ \lambda_k Q & a_2^k \end{pmatrix}$, where*

$$\lambda_k = \sum_{i+j=k-1} a_1^i a_2^j.$$

Proof.
Using a proof by induction on k. For $k = 1$, we have $\lambda_1 = 1$, then $X^{\star 1} = X$.
Let $k \geq 1$. Assuming the induction hypothesis, for a given value of $k \geq 1$, the single case

$$\lambda_k = \sum_{i+j=k-1} a_1^i a_2^j$$

is true, and proof that we have,

$$\lambda_{k+1} = \sum_{i+j=k} a_1^i a_2^j.$$

So, we have

$$X^{\star(k+1)} = \begin{pmatrix} a_1^k & \lambda_{1,k} P \\ \lambda_k Q & a_2^k \end{pmatrix} \star \begin{pmatrix} a_1 & P \\ Q & a_2 \end{pmatrix}.$$

Then,

$$X^{\star(k+1)} = \begin{pmatrix} a_1^{k+1} & (a_1^k + a_2\lambda_{1,k})P \\ (a_2^k + a_1\lambda_{1,k})Q & a_2^{k+1} \end{pmatrix}.$$

Thus,

$$\lambda_{k+1} = a_1^k + a_2\lambda_k = a_1^k + a_2 \sum_{i+j=k-1} a_1^i a_2^j.$$

Hence we have, for all $k \geq 1$,

$$\lambda_k = \sum_{i+j=k-1} a_1^i a_2^j.$$

Therefore, we can conclude the result. □

We have $\star$ is a non-commutative law, so in the following proposition we will characterize the set of matrices in $\aleph$ that commute with such a matrix $X = \begin{pmatrix} a_1 & sP \\ mP & a_2 \end{pmatrix}$.

Definition 6.2.3. *The centralizer of the matrix X over $\aleph$ is defined as follows*

$$\mathrm{C}_{\aleph}(X) = \{Y \in \aleph \mid X \star Y = Y \star X\}.$$

Proposition 6.2.2. *With the same notation as above, we have* $Y = \begin{pmatrix} b_1 & eP \\ fP & b_2 \end{pmatrix} \in \mathrm{C}_{\aleph}(X)$ *if and only if*

$$\begin{cases} b_1 \equiv b_2 \pmod{n}, & if\ a_1 \equiv a_2 \pmod{n}, \\ sf \equiv me \pmod{n}, & if\ a_1 - a_2 \neq 0. \end{cases}$$

Proof.
We have,

$$X \star Y = \begin{pmatrix} a_1 b_1 & b_2 sP + a_1 eP \\ b_1 mP + a_2 fP & a_2 b_2 \end{pmatrix},$$

and

$$Y \star X = \begin{pmatrix} a_1 b_1 & b_1 sP + a_2 eP \\ b_2 mP + a_1 fP & a_2 b_2 \end{pmatrix}.$$

Subsequently, we can determine the result through comparative calculations. □

In the following Lemma, we present the k-power of an elliptic matrix.

Lemma 34. *With the same notations as above, we have the k-power of an elliptic matrix as follows,*

$$M(B_1, B_2, B_3)^{\star k} = \begin{pmatrix} B_1^{\star k} & T_k \\ 0 & B_3^{\star k} \end{pmatrix} \quad for\ all\ k \in \mathbb{N}^*,$$

with $T_k = \sum_{i=0}^{k-1} B_1^{\star(k-1-i)} B_2 B_3^{\star i}$.

Proof.
The result is derived from [13]. □

6.3 Encryption Scheme

In this section we will construct an encryption scheme using the matrix $M(B_1, B_2, B_3)$ and the k-Fibonacci-like sequence $N_{k,n}$.

6.3.1 Cryptographic Protocols

This sub-section describes some public-key encryption and key establishment schemes.

6.3.1.1 Public-key encryption

Alice and **Bob** agree on public prime number p and a point P over an elliptic curve $E(\mathbb{F}_q)$ of order n, where q is a power of p.
First **Alice** and **Bob** choose an integer "e" such that $2^e \geq order(P)$. They create an encryption and decryption table of the alphabetical letters, as shown in Table 7.2.
In the next step **Alice** chooses two matrices $(A, A_1) \in \aleph$ and publishes the pair $(A, \mathrm{C}_\aleph(A_1))$, in the same way, **Bob** chooses two matrices $(B, B_2) \in \aleph$ and publishes the pair $(B, \mathrm{C}_\aleph(B_2))$.
Alice chooses private keys: $r \in \mathbb{N}^*$ and $A_2 \in \mathrm{C}_\aleph(B_2)$. She computed the matrix

$$(M(A_1, A+B, A_2))^{\star r} = \begin{pmatrix} A_1^{\star r} & T_r \\ 0 & A_2^{\star r} \end{pmatrix},$$

and send T_r to **Bob**.
In turn, **Bob** chooses private keys, $t \in \mathbb{N}^*$ and $B_1 \in \mathrm{C}_\aleph(A_1)$. He computed the matrix

$$(M(B_1, A+B, B_2))^{\star t} = \begin{pmatrix} B_1^{\star t} & E_t \\ 0 & B_2^{\star t} \end{pmatrix},$$

and sends E_t to **Alice**.
With their private keys r and t, **Alice** and **Bob** calculate the matrices separately:

$$\begin{aligned} \textbf{Alice}: M(A_1, E_t, A_2)^{\star r} &= \begin{pmatrix} A_1^{\star r} & E_{t,r} \\ 0 & A_2^{\star r} \end{pmatrix}. \\ \textbf{Bob}: M(B_1, T_r, B_2)^{\star t} &= \begin{pmatrix} B_1^{\star t} & T_{r,t} \\ 0 & B_2^{\star t} \end{pmatrix}. \end{aligned}$$

Lemma 35. *With the same notations as above, we have $E_{t,r} = T_{r,t}$.*

Proof.
We have,

$$\begin{aligned} T_{r,t} &= \sum_{i=0}^{t-1} B_1^{t-i-1} T_r B_2^i \\ &= \sum_{i=0}^{t-1} B_1^{t-i-1} \left(\sum_{j=0}^{r-1} A_1^{r-1-j} (A+B) A_2^j \right) B_2^i \\ &= \sum_{i=0}^{t-1} \sum_{j=0}^{r-1} B_1^{t-i-1} A_1^{r-1-j} (A+B) A_2^j B_2^i \end{aligned}$$

and

$$\begin{aligned} E_{t,r} &= \sum_{j=0}^{r-1} A_1^{r-j-1} E_t A_2^j \\ &= \sum_{j=0}^{r-1} A_1^{r-j-1} \left(\sum_{i=0}^{t-1} B_1^{t-1-i} (A+B) B_2^i \right) A_2^j \\ &= \sum_{j=0}^{r-1} \sum_{i=0}^{t-1} A_1^{r-j-1} B_1^{t-1-i} (A+B) B_2^i A_2^j. \end{aligned}$$

Or, $B_1 \in \mathrm{C}_{\aleph}(A_1)$ and $A_2 \in \mathrm{C}_{\aleph}(B_2)$, it follows that $T_{r,t} = E_{t,r}$. □

Corollary 20. *The secret key of **Alice** and **Bob** is the matrix* $\Phi = E_{t,r} = T_{r,t}$.

6.3.1.2 The secret k-Fibonacci-like sequence

In this section, we will define the k-Fibonacci-like sequence that we will use to complete our protocol. At this point, we have the secret matrix $\phi = \begin{pmatrix} a & \chi \\ \psi & b \end{pmatrix}$ exchanged between **Bob** and **Alice**. Then, the k-Fibonacci-like sequence is defined by

$$N_{k,0} = 2(k+1)\psi, \tag{6.1}$$

$$N_{k,1} = k\chi + k(k+1)\psi, \tag{6.2}$$

$$N_{k,n+1} = kN_{k,n} + N_{k,n-1} \ for \ n \geq 1, \tag{6.3}$$

where $k \in \mathbb{N}$ such that $a + b \equiv k \pmod{q}$. So we get the secret key between **Alice** and **Bob**, which is the "Elliptic" k-Fibonacci-like sequence.
Let $G =< \phi >= \{1_{\aleph}, \phi, 2\phi, 3\phi, ..., (m-1)\phi\}$ with $m = ord(G)$. For $l \leq m$, we code $l\phi = \begin{pmatrix} a_l & \chi_l \\ \psi_l & b_l \end{pmatrix}$ by the general term of the "Elliptic" k-Fibonacci-like sequence $(N_{k,n})_n$

$$l\phi \to N_{k,l-1} \, and \, 1_{\aleph} \to N_{k,m}.$$

Then we get

$$\phi \to N_{k,1}$$

$$2\phi \to N_{k,2}$$

$$...$$

$$...$$

$$...$$

$$i\phi \to N_{k,i}$$

$$...$$

$$...$$

6.3.2 Encryption the message

Let Φ be a secret key exchanged between **Alice** and **Bob**. If Φ is invertible, let ∇ be the message that **Alice** wants to send to **Bob**, ∇ is a matrix of the same size as Φ. The encryption message

$$\triangle = e_{\Phi}(\nabla) = \Phi \star \nabla \star \Phi^{-1}$$

Otherwise, we return to the key exchange protocol.

Lemma 36. *Let ∇_1, ∇_2 be two messages and for all invertible key not equal to unit matrix, Φ, we have:*

$$e_{\Phi}(\nabla_1 + \nabla_2) = e_{\Phi}(\nabla_1) + e_{\Phi}(\nabla_2)$$
$$e_{\Phi}(\nabla_1 \star \nabla_2) = e_{\Phi}(\nabla_1) \star e_{\Phi}(\nabla_2)$$

Remark 12. *This encryption message is a fully homomorphic encryption that allows calculations to be performed on the ciphertext, producing an encrypted result that, when decrypted, matches the result of the operations performed on the plaintext.*

6.3.3 Decryption the message

When **Bob** receives the encrypted message $\triangle$ sent by **Alice**, it uses a decryption function to decrypt it. This function noted d_{Φ} is defined as follows:

$$d_{\Phi}(\triangle) = \Phi^{-1} \star \nabla \star \Phi.$$

Lemma 37. *For all message ∇, we have $d_{\Phi} \circ e_{\Phi}(\nabla) = \nabla$.*

6.3.4 Security of this protocol

In this section, we discuss the security and compare it to other schemes.

6.3.4.1 Security

Our system is secure for the following reasons:
• Our cryptosystem is directly based on the difficulty of solving the ECDLP over $(G, +)$ of base P. In our system, we have $\mathrm{C}_{\aleph}(B_2)$, $\mathrm{C}_{\aleph}(A_1)$ and the matrices A, B are the public equations. The matrices A_1, A_2 and the secret integer k are all private.
• The complexity to calculate the key Φ is $\mathcal{O}(2^{tr})$.

6.3.4.2 Discussion and analysis

Since, ECLDP is hard to solve compared to DLP on fields, we can say that our cryptosystem over elliptic curves is more secure than the cryptosystem over finite fields. Moreover, we have sub-exponential algorithms that do DLP resolution over fields. However, the cryptographic primitive used in our scheme is based on the difficulty of DLP. Therefore, to ensure a sufficient level of security, it is necessary to work on large fields, which means that we will increase the transmission costs, the implementation and the computation time.
On the other hand, our cryptosystem is preferable to the one over fields, due to the fact that the ECDLP is an exponential problem. So, to ensure a maximum security of the cryptographic system, it is necessary to choose well the elliptic curve on which we are going to work. In addition, solving the ECLDP is more difficult than the IFP (Integer Factorization Problem). Thus, our cryptosystem over elliptic curve is more secure than the RSA cryptosystem. Moreover, ECLDP gives a higher level of security with small keys (in the sense of sizes) than in the RSA or DSA cryptosystem.

Digital Signature Algorithm[78]. The following table shows the length of the key to achieve an appropriate security level of k-bit.

security level	symmetric algorithms	elliptic curve algorithms	asymmetric algorithms like: RSA, DSA and El Gamal
128	80	160	1024
1024	128	256	2048

We conclude that, the memory consumption in our cryptosystem over elliptic curve is much lower than in the Cramer-Shoup signature scheme based on strong RSA [25].

6.4 Numerical example

Alice and **Bob** choose a prime number $p = 107099$ and a point $P = (33768, 33994)$ over the elliptic curve E given by the Weierstrass equation:

$$y^2 = x^3 + 2x + 10 \pmod{107099}.$$

The order of the point P is 107263.
So, to encrypt the message: " **a new encryption scheme**", we follow the following steps:

Step 1. **Alice** and **Bob** choose an integer "$e = 17$" such that $2^e \geq order(P) = 107263$.
Step 2. They build an encryption and decryption table of the alphabetical letters, as shown in Table 7.2.
First **Alice** chooses two matrices in $\aleph$,

$$A = \begin{pmatrix} 1 & P_A \\ Q_A & 2 \end{pmatrix}, \quad A_1 = \begin{pmatrix} 1 & P_{A_1} \\ Q_{A_1} & 2 \end{pmatrix}$$

and publish the pair $(A, \mathrm{C}_\aleph(A_1))$, in the same way, **Bob** chooses two matrices in $\aleph$,

$$B = \begin{pmatrix} 5 & P_B \\ Q_B & 2 \end{pmatrix}, \quad B_2 = \begin{pmatrix} 3 & P_{B_2} \\ Q_{3,B_2} & 4 \end{pmatrix}$$

and publish the pair $(B, \mathrm{C}_\aleph(B_2))$.

To simplify the verification of our method, we will give the points of the matrices A, B, A_1 *and* B_2 as a function of the point P.
So, consider

$$A = \begin{pmatrix} 1 & P \\ 2P & 2 \end{pmatrix}, \quad B = \begin{pmatrix} 5 & 2P \\ 2P & 2 \end{pmatrix}$$

$$A_1 = \begin{pmatrix} 1 & P \\ 3P & 2 \end{pmatrix}, \quad B_2 = \begin{pmatrix} 3 & P \\ P & 4 \end{pmatrix}$$

Alice choose a private keys, $r = 56$, and a matrix

$$A_2 = \begin{pmatrix} 2 & P \\ P & 3 \end{pmatrix} \in \mathrm{C}_\aleph(B_2).$$

She calculated the matrix

$$(M(A_1, A + B, A_2))^{\star 56} = \begin{pmatrix} A_1^{\star 56} & T_{56} \\ 0 & A_2^{\star 56} \end{pmatrix},$$

where

$$T_{56} = \sum_{i=0}^{18} A_1^{\star(18-i)}(A + B)A_2^{\star i} \tag{6.4}$$

$$= \begin{pmatrix} 432345564227567610 & 340175961395726755150854553 0P \\ 209339056684120247513531125 4P & 209339053182121177270233434 0 \end{pmatrix} \tag{6.5}$$

$$= \begin{pmatrix} 7666 & 78505P \\ 97693P & 12558 \end{pmatrix} \tag{6.6}$$

and send it to **Bob**.
In turn, **Bob** chooses a private keys, $t = 34$, and a matrix $B_1 = \begin{pmatrix} 1 & 2P \\ 6P & 3 \end{pmatrix} \in \mathrm{C}_{\aleph}(A_1)$.
He calculates the matrix

$$(M(B_1, A+B, B_2))^{\star 34} = \begin{pmatrix} B_1^{\star 34} & E_{34} \\ 0 & B_2^{\star 34} \end{pmatrix}$$

Where

$$E_{34} = \sum_{i=0}^{27} B_1^{\star(27-i)}(A+B)B_2^{\star i} \tag{6.7}$$

$$= \begin{pmatrix} 50031545098999704 & 16723880557444350138 69P \\ 11837769624220476181 12P & 11805249119906126371 48 \end{pmatrix} \tag{6.8}$$

$$= \begin{pmatrix} 64291 & 55199P \\ 15035P & 19173 \end{pmatrix} \tag{6.9}$$

and send it to **Alice**.

With their private keys k and t, **Alice** and **Bob** calculate separately the matrices:

$$\textbf{Alice}: M(A_1, E_{34}, A_2)^{\star 56} = \begin{pmatrix} A_1^{\star 56} & E_{34,56} \\ 0 & A_2^{\star 56} \end{pmatrix} \tag{6.10}$$

$$\textbf{Bob}: M(B_1, T_{56}, B_2)^{\star 34} = \begin{pmatrix} B_1^{\star 34} & T_{56,34} \\ 0 & B_2^{\star 34} \end{pmatrix}, \tag{6.11}$$

where, $E_{34,56} = \begin{pmatrix} a_1 & a_2P \\ a_3P & a_4 \end{pmatrix}$
with,
$a_1 = 4632654778292424869085 \equiv 14764 \pmod{107263}$,
$a_2 = 3628447641322223205703695678 2040 \equiv 37870 \pmod{107263}$,
$a_3 = 1003414453354817929558140149 4830 \equiv 69021 \pmod{107263}$,
$a_4 = 1003414416665202332950546407 5205 \equiv 72722 \pmod{107263}$,
and, $T_{56,34} = \begin{pmatrix} b_1 & b_2P \\ b_3P & b_4 \end{pmatrix}$
with,
$b_1 = 63923637454821955144 \equiv 14764 \pmod{107263}$,
$b_2 = 1094843495221297340892 5707 \equiv 37870 \pmod{107263}$,
$b_3 = 3726504198754437752991720 \equiv 69021 \pmod{107263}$,
$b_4 = 3706257961194528374326146 \equiv 72722 \pmod{107263}$,

Hence, $E_{34,56} = T_{56,34}$.
So,

$$\phi = \begin{pmatrix} a & \chi \\ \psi & b \end{pmatrix} \tag{6.12}$$

$$= \begin{pmatrix} 14764 & 37870P \\ 69021P & 72722 \end{pmatrix} \tag{6.13}$$

with, $37870P = (74423, 106580)$ and $69021P = (22314, 92350)$.

Step 3.Then from the Table 7.2, the message "**a new encryption scheme**" is converted into the following binary code
01000001011100010010100100100011000101010010101110000011101001000110
10100001101001011001101111111110000000101000111010010101101011100110
11000010011001010101101110110011000101010010101110000011101001000110
00001010001110100101011010111001101010000110100101100110111111111000
10011101001100101100011110111100000001101101100010101011111000110010
01100101001000010100110011010001011001010100110111010000000010101110
00011001100011000110011110010101101011101011011100001100011010100001
10100001101001011001101111111110001010000110100101100110111111111000
01010100101011100000111010010001100001100011001011100111011101000011
10011101001100101100011110111100000110100000111010010010111000100100
00001010001110100101011010111001101100000010110101010101010000001011
00001010001110100101011010111001 10

Chapter 7

Elliptic curve over a finite ring

7.1 Introduction

Let $\mathbb{F}_q$ be a finite field, where q is a power of a prime p such that $p \geq 5$. An elliptic curve $E_{a,b}$ over $\mathbb{F}_q$ is given by the Weierstrass equation $Y^2Z = X^3 + aXZ^2 + bZ^3$, where the coefficients a, b are in $\mathbb{F}_q$.
It is well known that elliptic curves are a versatile cryptographic tool [5, 7, 13, 22, 73, 70, 78, 94], and in particular, that their group structure plays a crucial role in such applications, see [52, 53, 68, 86].
In this chapter [16], we'll follow the series of works that study elliptic curves over finite rings. This study was introduced by M. Virat over the ring $\mathbb{F}_q[e]$, $e^2 = 0$, where q is a prime ≥ 5 [97]. Then A. Chillali develops and generalizes this work to the ring $\mathbb{F}_q[e]$, $e^n = 0$ [19]. In addition, elliptic curves on a local ring of characteristic 3 have been studied by Hassib et al [45]. For the characteristic 2, the study is done by Tadmori et al in [95]. Also, he studied in [94] such curves over a non-local ring. In the same context of a nonlocal ring, Boulbot et al have studied this kind of curve over $\mathbb{F}_q[e]$, $e^3 = e^2$ [7], and over $\mathbb{F}_q[e]$, $e^2 = e$ [9]. In this chapter, we study elliptic curves defined on the ring $\mathbb{F}_q[\alpha]$, where α is a root of a monic polynomial $P(X)$ of minimal degree denoted by n on $\mathbb{F}_q$. The new advantage of this approach is to obtain a large number of points with a smaller prime p, because we will prove $\sharp E_{a,b}(\mathbb{F}_q[\alpha]) = \prod_{k=0}^{n-1} \sharp E_k$ (Corollary 23), in order to reserve memory for the calculations. Moreover, the group law of $E_{a,b}$ is easy to calculate in the forward direction, but difficult in the reverse direction. Thus, in this chapter, we will define a non-standard way of multiplying $*$ elements on $\mathbb{F}_q[\alpha]$, as follows, for $X = \sum_{k=0}^{n-1} x_k\alpha^k$,

$Y = \sum_{k=0}^{n-1} y_k \alpha^k$, we have

$$X * Y = \sum_{k=0}^{n-1} A_k \alpha^k, \; such\, that\, A_0 = x_0 y_0, \; A_k = P_k(X)\varphi_{k-1}(Y) + P_k(Y)\varphi_k(X)$$

where P_k and φ_k are a collection of maps from $\mathbb{F}_q[\alpha]$ to $\mathbb{F}_q$ defined as follows:

$$\begin{array}{ccc} \mathbb{F}_q[\alpha] & \xrightarrow{P_k} & \mathbb{F}_q \\ X & \longmapsto & x_k \end{array} \quad and \quad \begin{array}{ccc} \mathbb{F}_q[\alpha] & \xrightarrow{\varphi_k} & \mathbb{F}_q \\ X & \longmapsto & \sum_{j=0}^{k} P_j(X) \end{array}$$

In the rest of this chapter, we will use the following notation:

- For $X \in \mathbb{F}_q[\alpha]$, we have $X^{*n} = \underbrace{X * X * ... * X}_{n\ times}$.
- $E_{a,b}$ for an elliptic curve over the ring $(\mathbb{F}_q[\alpha], +, *)$ given by a Weierstrass equation $Y^{*2} * Z = X^{*3} + aX * Z^{*2} + bZ^{*3}$, such that the discriminant $D = 4a^{*3} + 27b^{*2}$ is invertible in $\mathbb{F}_q[\alpha]$.

Another objective of this chapter is the application of these results in cryptography. We describe here one of the variants of the ElGamal public key encryption scheme [37], the Cramer-Shoup elliptic curve encryption scheme [24]. In the same context of Cramer-Shoup encryption, the second author et al presents a new variant of the Cramer-Shoup public key encryption system on a twisted Hessian curve over the ring $\mathbb{F}_q[\epsilon]$, $\epsilon^4 = 0$ [53]. Since we are working in the ring $\mathbb{F}_q[\alpha]$, the new scheme that we will define on the elliptic curve $E_{a,b}$ has the advantage of having a low complexity cost compared to the elliptic curves over a field.

7.2 The ring $(\mathbb{F}_q[\alpha], +, *)$

In this section we will give some results concerning the ring $(\mathbb{F}_q[\alpha], +, *)$, which are useful for the rest of this chapter. We keep the same notation as above. So, let $\mathbb{F}_q[\alpha]$ be the set endowed by the usual addition $X + Y = \sum_{k=0}^{n-1}(x_k + y_k)\alpha^k$, and by the product law *, $X * Y = \sum_{k=0}^{n-1} A_k \alpha^k$ where $A_0 = x_0 y_0$, and $A_k = P_k(X)\varphi_{k-1}(Y) + P_k(Y)\varphi_k(X)$.
We then have the following results.

Lemma 38. *φ_k is a surjective morphism.*

Proof.
First we will prove that for each $k \in \{0, ..., n-1\}$, φ_k is a morphism:
Let $X = \sum_{k=0}^{n-1} x_k \alpha^k$ and $Y = \sum_{k=0}^{n-1} y_k \alpha^k$ be two elements of $\mathbb{F}_q[\alpha]$.

- $\varphi_k(X+Y) = \sum_{j=0}^{k} P_j(X+Y) = \sum_{j=0}^{k}(P_j(X)+P_j(Y)) = \sum_{j=0}^{k} P_j(X) + \sum_{j=0}^{k} P_j(Y) = \varphi_k(X)+\varphi_k(Y)$.
- For $k=0$, $\varphi_0(X*Y) = A_0 = x_0y_0 = \varphi_0(X)\varphi_0(Y)$. Suppose that for $k \in \{0,...,n-1\}$ $\varphi_{k-1}(X*Y) = \varphi_{k-1}(X)\varphi_{k-1}(Y)$, then we obtain

$$\varphi_k(X*Y) = \varphi_{k-1}(X*Y) + A_k = \varphi_{k-1}(X)\varphi_{k-1}(Y) + x_k\varphi_{k-1}(Y) + y_k\varphi_k(X).$$

On the other hand, for any element s in $\mathbb{F}_q$, we put X=s then we have $\varphi_k(X) = s$ for all $k \in \{0,...,n-1\}$, hence φ_k is surjective. □

Lemma 39. *The product law $*$ is well defined.*

Proof.
We will show respectively, that $*$ is commutative, associative and distributive with respect to the law $+$.
Let X,Y and Z be elements of $\mathbb{F}_q[\alpha]$:

- Put $X*Y = \sum_{k=0}^{n-1} A_k\alpha^k$ and $Y*X = \sum_{k=0}^{n-1} B_k\alpha^k$, we shall prove that $X*Y = Y*X$ this turns out to prove that $A_k = B_k$ for all $k \in \{0,...,n-1\}$.
  This follows immediately that:

$$\begin{aligned} A_k &= P_k(X)\varphi_{k-1}(Y) + P_k(Y)\varphi_k(X) \\ &= P_k(X)\varphi_{k-1}(Y) + P_k(Y)\varphi_{k-1}(X) + P_k(Y)P_k(X) = B_k. \end{aligned}$$

- We shall prove that $X*(Y*Z) = (X*Y)*Z$. Put $X*(Y*Z) = \sum_{k=0}^{n-1} C_k\alpha^k$ and $(X*Y)*Z = \sum_{k=0}^{n-1} D_k\alpha^k$.
  We have $C_k = \varphi_k(X*(Y*Z)) - \varphi_{k-1}(X*(Y*Z))$ and $D_k = \varphi_k((X*Y)*Z) - \varphi_{k-1}((X*Y)*Z)$.
  Thus, we obtains:

$$\begin{aligned} C_k &= \varphi_k(X*(Y*Z)) - \varphi_{k-1}(X*(Y*Z)) = \varphi_k(X)\varphi_k(Y*Z) - \varphi_{k-1}(X)\varphi_{k-1}(Y*Z) \\ &= \varphi_k(X)\varphi_k(Y)\varphi_k(Z) - \varphi_{k-1}(X)\varphi_{k-1}(Y)\varphi_{k-1}(Z) \\ &= \varphi_k(X*Y)\varphi_k(Z) - \varphi_{k-1}(X*Y)\varphi_k(Z) \\ &= \varphi_k((X*Y)*Z) - \varphi_{k-1}((X*Y)*Z) \\ &= D_k. \end{aligned}$$

- Put $X*Y = \sum_{k=0}^{n-1} B_k\alpha^k$ and $X*Z = \sum_{k=0}^{n-1} C_k\alpha^k$, where $B_k = P_k(X)\varphi_{k-1}(Y) + P_k(Y)\varphi_k(X)$ and $C_k = P_k(X)\varphi_{k-1}(Z) + P_k(Z)\varphi_k(X)$.

So from the definition of $*$ it follows that, $X * (Y + Z) = \sum_{k=0}^{n-1} A_k \alpha^k$,
where $A_k = P_k(X)\varphi_{k-1}(Y + Z) + P_k(Y + Z)\varphi_k(X)$, then

$$\begin{aligned} A_k &= P_k(X)(\varphi_{k-1}(Y) + \varphi_{k-1}(Z)) + (P_k(Y) + P_k(Z))\varphi_k(X) \\ &= P_k(X)\varphi_{k-1}(Y) + P_k(X)\varphi_{k-1}(Z) + P_k(Y)\varphi_k(X) + P_k(Z)\varphi_k(X). \end{aligned}$$

So $A_k = B_k + C_k$.

□

Corollary 21.
- *The set $\mathbb{F}_q[\alpha]$ endowed by the laws " + " and " $*$ " is a finite unitary commutative ring.*
- *$\mathbb{F}_q[\alpha]$ is a vector space over $\mathbb{F}_q$ of dimension n, and $(1, \alpha, ..., \alpha^{n-1})$ is its basis.*

7.2.1 Inverse elements over $\mathbb{F}_q[\alpha]$

The next proposition characterize the set $(\mathbb{F}_q[\alpha])^\times$ of invertible elements in $\mathbb{F}_q[\alpha]$.

Proposition 7.2.1. *Let $X = \sum_{k=0}^{n-1} x_k \alpha^k \in \mathbb{F}_q[\alpha]$, then $X \in \mathbb{F}_q[\alpha]^\times$ if and only if $\varphi_k(X) \neq 0$ for all $k \in \{0, 1, ..., n-1\}$. The inverse is given by:*

$$X^{-1} = \varphi_0(X)^{-1} - \sum_{k=1}^{n-1} x_k \varphi_{k-1}(X)^{-1} \varphi_k(X)^{-1} \alpha^k.$$

Proof.
Let X be an invertible element of $\mathbb{F}_q[\alpha]$, then there exists Y in $\mathbb{F}_q[\alpha]$ such that
$X * Y = \sum_{k=0}^{n-1} A_k \alpha^k = 1$ so for each k such that $1 \leq k \leq n-1$, $A_0 = 1$ and $A_k = 0$, then we have $y_0 = x_0^{-1}$ and $A_k = \varphi_k(X * Y) - \varphi_{k-1}(X * Y) = 0$.
It follows that $\varphi_k(X)\varphi_k(Y) - \varphi_{k-1}(X)\varphi_{k-1}(Y) = 0$, then $(\varphi_{k-1}(X) + x_k)(\varphi_{k-1}(Y) + y_k) - \varphi_{k-1}(X)\varphi_{k-1}(Y) = 0$.
Therefore $y_k\varphi_{k-1}(X) + x_k\varphi_{k-1}(Y) + x_k y_k = 0$, so $y_k[\varphi_{k-1}(X) + x_k] = -x_k\varphi_{k-1}(Y)$.
We get that

$$\begin{cases} y_0 = x_0^{-1}, \\ y_k = -x_k \varphi_k(X)^{-1} \varphi_{k-1}(X)^{-1} \quad 1 \leq k \leq n-1. \end{cases}$$

Then we have

$$Y = X^{-1} = \varphi_0(X)^{-1} - \sum_{k=1}^{n-1} x_k \varphi_{k-1}(X)^{-1} \varphi_k(X)^{-1} \alpha^k.$$

From the above, it follows that X is invertible in $\mathbb{F}_q[\alpha]$ if and only if $\varphi_k(X) \neq 0$ *for all k in* $\{0, 1, ..., n-1\}$.

□

In the following proposition, we prove that $\mathbb{F}_q[\alpha]$ endowed by the law " $+$ " and " $*$ " is a non local ring.

Proposition 7.2.2. $(\mathbb{F}_q[\alpha], +, *)$ *is a non local ring.*

Proof.
Consider $I = \cup_{k=0}^{n-1} I_k$ the set of non invertible elements of $\mathbb{F}_q[\alpha]$ with

$$I_k = \{X \in \mathbb{F}_q[\alpha]/\varphi_k(X) = 0\}.$$

We shall prove that the set of non invertible elements over $\mathbb{F}_q[\alpha]$ is not an ideal, so for $a \in \mathbb{F}_q$ let $X = a - a\alpha$, $Y = a\alpha$ two elements of I, then $X + Y = a \in \mathbb{F}_q$, hence the result. □

7.3 Elliptic curves over $\mathbb{F}_q[\alpha]$

In most situations in this chapter, we'll refer to an elliptic curve E, by an equation of the form

$$y^2 = x^3 + ax + b,$$

called the Weierstrass equation for E, where a and b are constants. In our case, they are elements of a finite field $\mathbb{F}_q$ or of the ring $\mathbb{F}_q[\alpha]$.
In what follows, we study the elliptic curve $E_{a,b}$ over $\mathbb{F}_q[\alpha]$. For this purpose, we define restrictions E_k of $E_{a,b}$ on the finite field $\mathbb{F}_q$.

7.3.1 The elliptic curves E_k

In what follows, we will use the following notation, for $a = \sum_{k=0}^{n-1} a_k\alpha^k$ and $b = \sum_{k=0}^{n-1} b_k\alpha^k$ in $\mathbb{F}_q[\alpha]$ we put

$$for\, k \in \{0, 1, ..., n-1\},\ E_k = \{[X : Y : Z] \in P^2(\mathbb{F}_q)/Y^2Z = X^3 + \varphi_k(a)XZ^2 + \varphi_k(b)Z^3\}$$

and $D_k = 4\varphi_k(a)^3 + 27\varphi_k(b)^2$ is its discriminant.
The following theorem gives a link between $E_{a,b}(\mathbb{F}_q[\alpha])$ and E_k.

Theorem 7.3.1. *Let $\mathbb{F}_q$ be a finite field where $q = p^d$, d is a positive integer, $p \geq 5$ is a prime number, and α be a root of a monic polynomial $P(X)$ of a minimal degree over $\mathbb{F}_q$ denoted by n. Then there exist elliptic curves E_k defined over $\mathbb{F}_q$, for $k \in \{0, ..., n-1\}$, such that*

$$E_{a,b}(\mathbb{F}_q[\alpha]) \simeq \prod_{k=0}^{n-1} E_k.$$

Lemma 40. *D is invertible in $\mathbb{F}_q[\alpha]$ if and only if $D_k \neq 0$ for all $k \in \{0, 1, ..., n-1\}$.*

Proof.
We have $D = 4a^{*3} + 27b^{*2} \in \mathbb{F}_q[\alpha]$ such that $a = \sum_{k=0}^{n-1} a_k\alpha^k$, $b = \sum_{k=0}^{n-1} b_k\alpha^k$ and $D = \sum_{k=0}^{n-1} A_k\alpha^k$. Since $\sum_{j=0}^{k} A_j = \varphi_k(D) = \varphi_k(4a^{*3} + 27b^{*2}) = D_k$, we have $A_k = \varphi_k(D) - \varphi_{k-1}(D) = D_k - D_{k-1}$, so $D = \sum_{k=0}^{n-1} A_k\alpha^k = D_0 + \sum_{k=1}^{n-1}(D_k - D_{k-1})\alpha^k$. From the proof of the proposition 7.2.1 we deduce that, D is invertible in $\mathbb{F}_q[\alpha]$ if and only if $D_k \neq 0$ for all $k \in \{0, 1, ..., n-1\}$. □

Corollary 22. *$E_{a,b}(\mathbb{F}_q[\alpha])$ is an elliptic curve over $\mathbb{F}_q[\alpha]$, if and only if E_k is an elliptic curves over $\mathbb{F}_q$ for all $k \in \{0, ..., n-1\}$.*

The following theorem gives a relation between the elements of $E_{a,b}(\mathbb{F}_q[\alpha])$ and the elements of E_k for all $k \in \{0, ..., n-1\}$.

Theorem 7.3.2. *Let X, Y and Z be elements of $\mathbb{F}_q[\alpha]$, then the following statements are equivalent:*

- $[X : Y : Z] \in E_{a,b}(\mathbb{F}_q[\alpha])$.
- $[\varphi_k(X) : \varphi_k(Y) : \varphi_k(Z)] \in E_k$, *for all* $k \in \{0, 1, ..., n-1\}$.

Proof.
Let $[X : Y : Z]$ in $E_{a,b}(\mathbb{F}_q[\alpha]) \subset P^2(\mathbb{F}_q[\alpha])$, then there exist U, V and W in $\mathbb{F}_q[\alpha]$ such that,
$U * X + V * Y + W * Z = 1$. So, $\varphi_k(U * X + V * Y + W * Z) = 1$ for all $k \in \{0, 1, ..., n-1\}$, and then $\varphi_k(U)\varphi_k(X) + \varphi_k(V)\varphi_k(Y) + \varphi_k(W)\varphi_k(Z) = 1$, for all $k \in \{0, 1, ..., n-1\}$ and $[\varphi_k(U) : \varphi_k(V) : \varphi_k(W)]$ belong in $P^2(\mathbb{F}_q)$.
We deduce that $(\varphi_k(X), \varphi_k(Y), \varphi_k(Z)) \neq (0, 0, 0)$ and we have $[\varphi_k(X) : \varphi_k(Y) : \varphi_k(Z)] \in E_k$.
Reciprocally, let $[x_k : y_k : z_k]$ in E_k, and put $X = x_0 + \sum_{k=1}^{n-1}(x_k - x_{k-1})\alpha^k$,
$Y = y_0 + \sum_{k=1}^{n-1}(y_k - y_{k-1})\alpha^k$, $Z = z_0 + \sum_{k=1}^{n-1}(z_k - z_{k-1})\alpha^k$.
If X is invertible then $[X : Y : Z] \in P^2(\mathbb{F}_q[\alpha])$. Suppose next, that X is not invertible then there exists $l \in \{0, 1, ..., n-1\}$ such that $\varphi_l(X) = 0$.
Consider the set $I_X = \{l \mid \varphi_l(X) = 0, l \in \{0, 1, ..., n-1\}\}$ and $k = min\, I_X$, then $\varphi_k(X) = 0$. It follows that $\varphi_k(Y) \neq 0$ or $\varphi_k(Z) \neq 0$, because $[\varphi_k(X) : \varphi_k(Y) : \varphi_k(Z)] \in E_k$.
Without loss of generality, suppose that $\varphi_k(Y) \neq 0$, and put $T = X + \alpha^k * Y$.
If $k = n-1$, then $\varphi_{n-1}(Y) \neq 0$, thus $T = X + \alpha^{n-1} * Y \in (\mathbb{F}_q[\alpha])^\times$. On the other hand we will distinguish between two cases:
If $\varphi_j(X) \neq -\varphi_j(Y)$, for $k < j \leq n-1$, then we have $T = X + \alpha^k * Y \in (\mathbb{F}_q[\alpha])^\times$.

If there exists $k < j \leq n-1$, such that $\varphi_j(X) = -\varphi_j(Y)$ then $\varphi_j(T) = 0$. Suppose that $j = min\, I_T$ then we have $\varphi_j(X) \neq 0$ or $\varphi_j(Y) \neq 0$ or $\varphi_j(Z) \neq 0$ and we apply the above reasoning to T.
So on until we find an invertible element write in the form of linear combine of X, Y and Z. □

Proposition 7.3.1. *For $i \in \{0, 1, ..., n-1\}$, the mappings $\tilde{\varphi}_i$ is well defined, and given by:*

$$\begin{array}{ccc} E_{a,b}(\mathbb{F}_q[\alpha]) & \xrightarrow{\tilde{\varphi}_i} & E_i \\ [X:Y:Z] & \longmapsto & [\varphi_i(X):\varphi_i(Y):\varphi_i(Z)] \end{array}$$

Proof.
According to the previous theorem, we have

$$[\varphi_i(X):\varphi_i(Y):\varphi_i(Z)] \in E_i, \ for\ all\ i \in \{0, ..., n-1\}.$$

If $[X:Y:Z] = [A:B:C]$, then there exists $U \in (\mathbb{F}_q[\alpha])^{\times}$ such that: $X = U * A$, $Y = U * B$ and $Z = U * C$, then:

$$\begin{aligned} \widetilde{\varphi}_i([X:Y:Z]) &= [\varphi_i(X):\varphi_i(Y):\varphi_i(Z)] \\ &= \underbrace{[\varphi_i(U)\varphi_i(A):\varphi_i(U)\varphi_i(B):\varphi_i(U)\varphi_i(C)]}_{\varphi_i(U)\in \mathbb{F}_q^*} \\ &= [\varphi_i(A):\varphi_i(B):\varphi_i(C)] \\ &= \widetilde{\varphi}_i([A:B:C]). \end{aligned}$$

It remains to check that this map is well defined in terms of Weierstrass equation.
Let X, Y, Z, a and b in $\mathbb{F}_q[\alpha]$, so we have $Y^{*2} * Z = \sum_{k=0}^{n-1} A_k \alpha^k$, $X^{*3} = \sum_{k=0}^{n-1} B_k \alpha^k$, $a * X * Z^{*2} = \sum_{k=0}^{n-1} C_k \alpha^k$ and $b * Z^{*3} = \sum_{k=0}^{n-1} T_k \alpha^k$, such that
$A_k = \varphi_k(Y)^2\varphi_k(Z) - \varphi_{k-1}(Y)^2\varphi_{k-1}(Z)$, $B_k = \varphi_k(X)^3 - \varphi_{k-1}(X)^3$, $C_k = \varphi_k(a)\varphi_k(X)\varphi_k(Z)^2 - \varphi_{k-1}(a)\varphi_{k-1}(X)\varphi_{k-1}(Z)^2$ and $T_k = \varphi_k(b)\varphi_k(Z)^3 - \varphi_{k-1}(b)\varphi_{k-1}(Z)^3$.
We deduce that $Y^{*2} * Z = X^{*3} + a * X * Z^{*2} + b * Z^{*3}$ if and only if $A_k = B_k + C_k + T_k$ for all $k \in \{0, 1, ...n-1\}$ hence the result. □

Proof. (Theorem 7.3.1)
To prove the isomorphism of the theorem, we will first prove that the curve $E_{a,b}(\mathbb{F}_q[\alpha])$ is in bijection with $\prod_{k=0}^{n-1} E_k$. So we consider the mapping $\tilde{\varphi}$ defined by

$$\begin{array}{ccc} E_{a,b}(\mathbb{F}_q[\alpha]) & \xrightarrow{\tilde{\varphi}} & \prod_{k=0}^{n-1} E_k \\ [X:Y:Z] & \longmapsto & \prod_{k=0}^{n-1} [\varphi_k(X):\varphi_k(Y):\varphi_k(Z)] \end{array}$$

- As $\tilde{\varphi}_k$ are well defined, then $\tilde{\varphi}$ is well defined.

- $\tilde{\varphi}$ is a surjective map:
  Let $[x_k : y_k : z_k] \in E_k$, then

$$[X : Y : Z] \in E_{a,b}(\mathbb{F}_q[\alpha])$$

  where $X = x_0 + \sum_{k=1}^{n-1}(x_k - x_{k-1})\,\alpha^k$, $Y = y_0 + \sum_{k=1}^{n-1}(y_k - y_{k-1})\,\alpha^k$ and $Z = z_0 + \sum_{k=1}^{n-1}(z_k - z_{k-1})\,\alpha^k$.
  So we have:
  $\tilde{\varphi}\left(\left[x_0 + \sum_{k=1}^{n-1}(x_k - x_{k-1})\,\alpha^k : y_0 + \sum_{k=1}^{n-1}(y_k - y_{k-1})\,\alpha^k : z_0 + \sum_{k=1}^{n-1}(z_k - z_{k-1})\,\alpha^k\right]\right)$
  $= \prod_{k=0}^{n-1}[\varphi_k(x_0 + \sum_{k=1}^{n-1}(x_k - x_{k-1})\,\alpha^k) : \varphi_k(y_0 + \sum_{k=1}^{n-1}(y_k - y_{k-1})\,\alpha^k) :$
  $\varphi_k(z_0 + \sum_{k=1}^{n-1}(z_k - z_{k-1})\,\alpha^k)]$
  $= \prod_{k=0}^{n-1}([x_k : y_k : z_k])$

  hence $\tilde{\varphi}$ is a surjective mapping.

- It's remains to show that $\tilde{\varphi}$ is injective, for that lets $[X : Y : Z]$ and $[X' : Y' : Z']$ in $E_{a,b}(\mathbb{F}_q[\alpha])$, where $X = \sum_{k=0}^{n-1} x_k\alpha^k$, $Y = \sum_{k=0}^{n-1} y_k\alpha^k$, $Z = \sum_{k=0}^{n-1} z_k\alpha^k$, $X' = \sum_{k=0}^{n-1} x'_k\alpha^k$, $Y' = \sum_{k=0}^{n-1} y'_k\alpha^k$ and $Z' = \sum_{k=0}^{n-1} z'_k\alpha^k$. Suppose that $[\varphi_k(X) : \varphi_k(Y) : \varphi_k(Z)] = [\varphi_k(X') : \varphi_k(Y') : \varphi_k(Z')]$, then there exist $\beta_k \in (\mathbb{F}_q)^\times$ for all $k \in \{0, 1, ..., n-1\}$

$$\text{such that } \begin{cases} \varphi_k(X) = \beta_k\varphi_k(X') \\ \varphi_k(Y) = \beta_k\varphi_k(Y') \\ \varphi_k(Z) = \beta_k\varphi_k(Z') \end{cases}$$

$$so \begin{cases} x_k = \beta_k\varphi_k(X') - \beta_{k-1}\varphi_{k-1}(X') \\ y_k = \beta_k\varphi_k(Y') - \beta_{k-1}\varphi_{k-1}(Y') \\ z_k = \beta_k\varphi_k(Z') - \beta_{k-1}\varphi_{k-1}(Z') \end{cases}$$

$$then\ we\ have \begin{cases} x_k = \beta_k x'_k + (\beta_k - \beta_{k-1})\varphi_{k-1}(X') \\ y_k = \beta_k y'_k + (\beta_k - \beta_{k-1})\varphi_{k-1}(Y') \\ z_k = \beta_k z'_k + (\beta_k - \beta_{k-1})\varphi_{k-1}(Z') \end{cases}.$$

  Consider $\beta = \beta_0 + \sum_{k=1}^{n-1}(\beta_k - \beta_{k-1})\alpha$, it follows that

$$\begin{cases} x_k = P_k(X')\varphi_k(\beta) + P_k(\beta)\varphi_k(X') \\ y_k = P_k(Y')\varphi_k(\beta) + P_k(\beta)\varphi_k(Y') \\ z_k = P_k(Z')\varphi_k(\beta) + P_k(\beta)\varphi_k(Z') \end{cases}$$

  finally we have $X = \beta * X'$, $Y = \beta * Y'$, $Z = \beta * Z'$ and $\beta \in (\mathbb{F}_q[\alpha])^\times$ then $[X : Y : Z] = [X' : Y' : Z']$.
  Hence $\tilde{\varphi}$ is a bijection.

We can show that the mapping $\tilde{\varphi}^{-1}$ defined by:
$\tilde{\varphi}^{-1}(\prod_{k=0}^{n-1}[x_k : y_k : z_k]) = [x_0 + \sum_{k=1}^{n-1}(x_k - x_{k-1})\,\alpha^k : y_0 + \sum_{k=1}^{n-1}(y_k - y_{k-1})\,\alpha^k :$
$z_0 + \sum_{k=1}^{n-1}(z_k - z_{k-1})\,\alpha^k]$

is the inverse of $\tilde{\varphi}$. □

Corollary 23. *With the same notation as above, we have*

$$\sharp E_{a,b}(\mathbb{F}_q[\alpha]) = \prod_{k=0}^{n-1} \sharp E_k.$$

Example 7.3.1. *Lets* $a = 2 + 3\alpha + \alpha^2 - 5\alpha^3$, $b = 1 + 2\alpha^2 - 6\alpha^7 + \alpha^{12}$ *and* α *be a root of a monic polynomial of a minimal degree over* $\mathbb{F}_{691}$, *such that* $d^\circ P(X) = 13$. *So, we have* $card(E_0) = 726$, $card(E_1) = 714$, $card(E_2) = 678$, $card(E_3) = 652$, $card(E_4) = 652$, $card(E_5) = 652$, $card(E_6) = 652$, $card(E_7) = 732$, $card(E_8) = 732$, $card(E_9) = 732$, $card(E_{10}) = 732$, $card(E_{11}) = 732$ *and* $card(E_{12}) = 684$.
In view of $\sharp E_{a,b} = \prod_{k=0}^{12} \sharp E_k$, *we obtain*

$$\sharp E_{a,b} = 912990831561236121689283987194354073 6.$$

To complete the proof of the Theorem 7.3.1, we will define the group law on $E_{a,b}$, in the following subsection.

7.3.2 The group law $\star$ over $E_{a,b}$

To define the group law $\star$ over $E_{a,b}$, we use the explicit formulas in the article [10] [pages : 236-238], and since $\tilde{\varphi}$ is bijection we can define $\star$ as follows $P \star Q = \tilde{\varphi}^{-1}(\tilde{\varphi}(P) + \tilde{\varphi}(Q))$ for P, $Q \in E_{a,b}$.

Lemma 41. *The mapping*

$$\begin{array}{ccc} (E_{a,b}(\mathbb{F}_q[\alpha]), \star) & \xrightarrow{\tilde{\varphi}} & (\prod_{k=0}^{n-1} E_k, +) \\ [X : Y : Z] & \longmapsto & \prod_{k=0}^{n-1}[\varphi_k(X) : \varphi_k(Y) : \varphi_k(Z)] \end{array}$$

is an isomorphism of groups.

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

Which ends the demonstration of Theorem 7.3.1.

7.4 Applications

In cryptography applications, we have:

- If $\sharp E_{a,b}(\mathbb{F}_q[\alpha]) := n$ is an odd number, then $n = \prod_{k=0}^{n-1} n_k$ is the factorization of n, where $n_k := \sharp E_k$, hence the cardinal of $E_{a,b}(\mathbb{F}_q[\alpha])$ is not a prime number.

- **The discrete logarithm problem** [1, 78] in $E_{a,b}(\mathbb{F}_q[\alpha])$ is equivalent to the discrete logarithm problem in $\prod_{k=0}^{n-1} E_k$.

7.5 Cramer-Shoup Elliptic curve cryptosystem

The Cramer-Shoup cryptosystem for $E_{a,b}$ essentially consists in mapping the operations usually performed in the multiplicative group $\mathbb{Z}/p\mathbb{Z}$ to the set of points of the elliptic curve $E_{a,b}$, endowed with an additive group law.
Alice and **Bob** want to communicate in a secure way, for that they choose the initialization parameters of the Cramer-Shoup elliptic curve cryptosystem,

- A large prime number p, $m, n \in \mathbb{N}^*$.

- A finite ring $\mathbb{F}_q[\alpha]$.

- An elliptic curve $E_{a,b}$ such that $4a^3 + 27b^2$ is invertible in $\mathbb{F}_q[\alpha]$.

- A point $P \in E_{a,b}$ of large order τ and the cyclic group $G = \langle P \rangle$.

7.5.1 Coding of the elements of G.

Let for example $P = [2 + 8\alpha : 10 + 4\alpha : 1] \in E_{1+2\alpha,2}(\mathbb{F}_{11}[\alpha])$, P is of order $\tau = 104$.
We will use the subgroup $G =< P >$ of $E_{1+2\alpha,2}(\mathbb{F}_{11}[\alpha])$ to encrypt message. Thus, for each element $Q = m \cdot P \in G$, where $m \in \{1, 2, \ldots \tau\}$, we will give a code.
Let $Q = [\sum_{k=0}^{n} x_k \alpha^k : \sum_{k=0}^{n} y_k \alpha^k : \sum_{k=0}^{n} z_k \alpha^k]$ where, x_k, y_k and z_k are elements of $\mathbb{F}_q$, for $i \in \{0, ..., n\}$.
Thus, we code Q as follows:

$$Q = \underbrace{x_0 ... x_n y_0 ... y_n z_0 ... z_n}_{3\times(n+1)}.$$

We also attach any element $Q \in G$ with a letter of the alphabet or a punctuation sign.

7.5.2 Cramer-Shoup $E_{a,b}$ cryptosystem Key generation.

The generation of a public key in $E_{a,b}$ is as follows:

- **Alice** chooses five random integers $(c_1,\ c_2,\ s_1,\ s_2,\ x_1,\ x_2) \in (\mathbb{F}_\tau)^5$.
- **Alice** computes $E_1 = c_1 P,\ E_2 = c_2 P,\ E_3 = s_1 P + s_2 E_1,\ E_4 = x_1 P + x_2 E_1$.

Then, the public key is $\{P,\ E_1,\ E_2,\ E_3,\ E_4\}$ and the private key is $(c_1,\ c_2,\ s_1,\ s_2,\ x_1,\ x_2)$.

7.5.2.1 Encryption of message .

To encrypt a message P_m to **Alice** under her public key $\{P,\ E_1,\ E_2,\ E_3,\ E_4\}$, we use the following statement:

- **Bob** converts the plaintext message P_m to a point $P_m = (X_m, Y_m, Z_m)$ on the elliptic curve $E_{a,b}$ with $X_m \neq 0, Y_m \neq 1, Z_m \neq 0$.
- **Bob** chooses a random $k \in \mathbb{F}_\tau$, and calculates: $W_1 = kP$, $W_2 = kE_1$, $u = kE_2 + P_m$, $\delta = \mathbb{H}(W_1, W_2, u)$ (where $\mathbb{H}()$ is a collision-resistant hash function), $R = kE_3 + k\delta E_4$.
- **Bob** sends the ciphertext (W_1, W_2, u, R) to **Alice**.

7.5.2.2 Decryption of message .

To decrypt this message, with **Alice**'s secret key $(c_1,\ c_2,\ s_1,\ s_2,\ x_1,\ x_2)$:

- **Alice** computes $\delta = \mathbb{H}(W_1, W_2, u)$, and verifies that

  $$s_1 W_1 + s_2 W_2 + \delta (x_1 W_1 + x_2 W_2) = R.$$

  If this test fails, further decryption is aborted and the output is rejected.
- Otherwise, **Alice** computes $P_m = u - c_2 W_1$. The decryption stage correctly decrypts any properly-formed ciphertext, since

  $$u - c_2 W_1 = kE_2 + P_m - c_2 kP = kc_2 P + P_m - wkP = P_m.$$

7.5.3 Security of this protocol

In this section, we discuss the security and compare it to other schemes.

7.5.3.1 Security

Our system is secure for the following reasons:
• Cramer-Shoup $E_{a,b}$ cryptosystem is directly based on the difficulty of solving the ECDLP over $(G,+)$ of base P. In our system, we have $V_1 = kP$, $V_2 = kQ$, $u = kT + P_m$, $R = kE + k\delta K$ are the public equations. The point $P_m = (X_m, Y_m, Z_m)$ over $E_{a,b}$, the secret integer k and the collision-resistant hash function $\mathbb{H}$ are all private.
• The security analysis of the Cramer-Shoup cryptosystem over $E_{a,b}$ relies on the difficulty of the decisional Diffie-Hellman (DDH) problem, which states that the tuple (nP, mP, nmP) (where P is a base point) is indistinguishable from (nP, mP, eP), where n, m, and e are integers randomly selected.

Remark 13. *If we assume that we have the following two conditions*
• *The hash function $\mathbb{H}$ is chosen in a universal one-way family.*
• *The Diffie-Hellman decision problem is difficult in the group G.*
Then we have the following Lemma.

Lemma 42. *The above cryptosystem is secure against adaptive chosen ciphertext attack.*

Proof.
Since we assume that: the hash function $\mathbb{H}$ is chosen in a universal one-way family, and The Diffie-Hellman decision problem is hard in the group G. which feels the same conditions in Theorem 1 [Section 4] [24]. Hence the result. □

7.5.4 Discussion and analysis

The $E_{a,b}$ version of the Cramer-Shoup cipher is the analog of the Cramer-Shoup cipher [24]. where,
• Multiplication operations replaced by additions.
• Exponentiation operations replaced by multiplication.
Since, ECLDP is hard to solve compared to DLP on fields, we can say that Cramer-Shoup encryption at $E_{a,b}$ is more secure than the original Cramer-Shoup encryption. Moreover, we have sub-exponential algorithms that do DPL resolution over fields. However, the cryptographic primitive used in our scheme is based on the difficulty of DLP. Therefore, to ensure a sufficient level of security, it is necessary to work on large fields, which means that we will increase the transmission costs, the implementation and the computation time.

On the other hand, the Cramer-Shoup encryption over $E_{a,b}$ is preferable to the one over fields, due to the fact that the ECDLP is an exponential problem. In the same context we cite two of the best algorithms in exponential time for solving the ECDLP [62, 63, 78, 93] over an elliptic curve defined over finite fields. The Shanks Baby-Steps Giant-Steps algorithm and Pollard's p-method algorithm.
So, to ensure a maximum security of the cryptographic system, it is necessary to choose well the elliptic curve on which we are going to work. For this reason our elliptic curve $E_{a,b}$ on the ring $\mathbb{F}_q[\alpha]$ verifies this condition because it increases the ECDLP resolution time since it has been shown that $\sharp\left(E_{a,b}(\mathbb{F}_q[\alpha])\right) = \prod_{k=0}^{n-1} \sharp E_k$. Therefore, we can say that the time needed to solve the ECLDP on $E_{a,b}$ is larger than the one for the elliptic curve on a finite field.
The Cramer-Shoup cryptosystem is a more secure extension of ElGamal cryptosystem. such as the 1st is based on (DDH-A)(Decisional Diffie-Hellman) on the other hand ElGamal cryptosystem is based on (CDH-A)(Computational Diffie-Hellman Assumption). Therefore, we have Cramer-Shoup on $E_{a,b}$ is more secure than ElGamal encryption scheme. On the other hand, among the inconviniant of Cramer-Shoup cryptosystem on $E_{a,b}$ is that the cipher text is longer than the plaintext.
Solving the ECLDP is more difficult than the IFP (Integer Factorization Problem). Thus, the Cramer-Shoup cryptosystem on $E_{a,b}$ is more secure than the RSA cryptosystem. Moreover, ECLDP gives a higher level of security with small keys (in the sense of sizes) than in the RSA or DSA cryptosystem.
Digital Signature Algorithm [25, 86]. The following table shows the length of the key to achieve an appropriate security level of k-bit.

security level	symmetric algorithms	elliptic curve algorithms	asymmetric algorithms like: RSA, DSA and El Gamal
128	80	160	1024
1024	128	256	2048

We conclude that:
• The memory consumption in the Cramer-Shoup cryptosystem over $E_{a,b}$ is much lower than in the Cramer-Shoup signature scheme based on strong RSA [25].
• The size of the message encrypted in the Cramer-Shoup cryptosystem over $E_{a,b}$ is larger than in the RSA-based encryption.

7.5.5 Conclusion

In this chapter, we have extended the results for elliptic curves on $\mathbb{F}_q[\alpha]$ and related to elliptic curves over $\mathbb{F}_q$ by the Theorem 7.3.1. Moreover, we prove that the discrete logarithm problem in $E_{a,b}$ is equivalent to that in E_k. We also introduce the Cramer-Shoup

cryptosystem on $E_{a,b}$ which proves to be more secure than his original cryptosystem [24] and his cryptosystem on elliptic curve [51, 27]. In other respects, it works with smaller key sizes than RSA, but results in a higher ciphertext expansion rate.

Conclusions

In conclusion, this thesis delves into the exploration of elliptic curves and their applications in various mathematical and cryptographic domains. The study begins with a solid foundation in basic theory, focusing on elliptic curves over the rational number field $\mathbb{Q}$. The investigation then extends to quadratic cyclotomic fields and finite field extensions, providing new perspectives and challenges.

Throughout the thesis, several key topics are covered. The first chapter establishes the formal definition of an elliptic curve, introduces addition operations, and explores various properties, including quadratic twists, torsion points, division polynomials, and the Weil Pairing. Additionally, the chapter introduces the modular curve $X_1(n, m)$, which is a higher-dimensional generalization of elliptic curves.

Subsequent chapters delve into specific research areas. Chapter 2 focuses on the existence and non-existence of elliptic curves with specific torsion groups over a given field. Chapter 3 investigates possible torsion groups of elliptic curves defined over specific base fields and extended to biquadratic number fields. Chapter 4 determines all possible torsion sections of elliptic curves on quadratic extensions of the rational field with non-standard multiplication.

Chapter 5 shifts attention to elliptic curves defined over finite fields and explores the design of public key exchange protocols within a noncommutative ring. The complexity and security of the key exchange protocol are also investigated. Chapter 6 introduces a modified k-Fibonacci-like sequence defined over an elliptic curve, known as "Elliptic" k-FlS, and provides Binet's formula for this sequence. An encryption scheme using this sequence is also presented.

Finally, Chapter 7 focuses on elliptic curves defined on the ring $\mathbb{F}_q[\alpha]$, where α is a root of a monic polynomial $P(X)$ of minimal degree over $\mathbb{F}_q$. The chapter explores the application of these results in cryptography.

Overall, this thesis contributes to a better understanding of elliptic curves, their behavior, and their wide-ranging applications, providing valuable insights into mathematical and cryptographic domains.

Tables

Table 7.1: Rank of $X_1(11)$, $X_1(14)$, $X_1(15)$, $X_1(2,10)$, and $X_1(2,12)$.

d	$X_1(11)$	$X_1(14)$	$X_1(15)$	$X_1(2,10)$	$X_1(2,12)$
$\{-1,2\}$	2	0	0	1	0
$\{-1,3\}$	0	1	1	0	0
$\{-1,5\}$	0	1	0	0	1
$\{-1,7\}$	2	1	2	0	0
$\{-1,11\}$	1	1	2	2	1
$\{-1,13\}$	2	1	2	2	1
$\{-1,19\}$	2	1	0	2	1
$\{-1,37\}$	0	1	2	2	1
$\{-1,43\}$	2	1	2	0	1
$\{-1,67\}$	0	1	2	0	1
$\{-1,163\}$	2	1	2	0	1
$\{2,-3\}$	2	1	1	0	0
$\{2,-11\}$	1	1	2	2	1
$\{-2,-3\}$	2	1	0	2	1
$\{-2,5\}$	2	1	1	1	1
$\{-2,-7\}$	2	1	1	2	0
$\{-2,-11\}$	2	3	3	2	1
$\{-2,19\}$	2	2	0	3	0
$\{-2,29\}$	2	1	2	2	1
$\{-2,-43\}$	4	1	2	2	1

d	$X_1(11)$	$X_1(14)$	$X_1(15)$	$X_1(2,10)$	$X_1(2,12)$
$\{-2,-67\}$	2	1	2	2	3
$\{-3,5\}$	0	0	0	1	1
$\{-3,-7\}$	2	0	1	0	1
$\{-3,-11\}$	1	2	2	2	0
$\{-3,17\}$	2	2	1	2	1
$\{-3,-19\}$	2	0	1	2	1
$\{-3,41\}$	2	2	1	2	1
$\{-3,-43\}$	2	2	1	0	1
$\{-3,-67\}$	0	2	1	0	1
$\{-3,89\}$	0	2	1	2	1
$\{-3,-163\}$	0	2	1	0	1
$\{-7,5\}$	2	1	1	1	0
$\{-7,-11\}$	2	1	2	2	0
$\{-7,13\}$	2	1	2	2	2
$\{-7,-19\}$	2	0	2	2	2
$\{-7,-43\}$	2	1	2	0	2
$\{-7,61\}$	2	1	2	2	2
$\{-7,-163\}$	2	1	2	0	2
$\{-11,17\}$	1	2	2	2	2
$\{-11,-19\}$	2	2	2	2	2
$\{-11,-67\}$	1	2	4	2	2
$\{-11,-163\}$	1	4	2	2	2
$\{-19,-67\}$	2	2	2	2	2
$\{-19,-163\}$	2	2	2	2	2
$\{-43,-67\}$	2	2	2	0	2
$\{-43,-163\}$	2	4	2	0	2
$\{-67,-163\}$	0	2	2	0	2

Table 7.2: Table of codes.

m	mχ **and** mψ	$F_{k,m}$	**Code**	**Symbol**
1	(74423,106580) (22314,92350)	(33506,42124)	0100000101110001001010010010001100	a
2	(62134,63396) (95705,34759)	(101733,8958)	1100011010110010100010001011111110	b
3	(90598,58866) (98732,56731)	(80485,73456)	1001110100110010110001111011110000	c
4	(104397,78748) (82869,85948)	(10352,83747)	0001010000111000010100011100100011	d
5	(23890,16576) (100667,84724)	(5236,88806)	0000101000111010010101101011100110	e
6	(59807,56935) (55826,61230)	(33135,11702)	0100000010110111100010110110110110	f
7	(27998,10902) (74475,25297)	(859,4901)	0000000110101101100001001100100101	g
8	(50593,62584) (45472,35470)	(53364,77348)	0110100000111010010010111000100100	h
9	(46329,40091) (93906,50481)	(13080,106070)	0001100110001100011001111001010110	i
10	(56326,32419) (106156,86811)	(70976,69326)	1000101010100000010000111011001110	j
11	(17405,66933) (40859,9752)	(75269,66387)	1001001100000010110000001101010011	k
12	(72335,44966) (97234,99444)	(76759,96855)	1001010111101011110111101001010111	l
13	(8179,23813) (34573,38882)	(98666,87051)	1100000010110101010101010000001011	m
14	(85243,64015) (19489,31677)	(82763,28664)	1010000110100101100110111111111000	n
15	(88975,48659) (94653,88562)	(95672,50849)	1011101011011100001100011010100001	o
16	(54587,70498) (59217,23779)	(76398,65710)	1001010100110111010000000010101110	p
17	(82876,46748) (2794,86143)	(96825,47796)	1011110100011100101011101010110100	q
18	(61152,92731) (41075,9952)	(14021,48690)	0001101101100010101011111000110010	r
19	(105388,85731) (88322,24831)	(12695,30531)	0001100011001011100111011101000011	s
20	(79291,92606) (27724,98381)	(38358,9284)	0100101011101011000010010001000100	t
21	(12813,60829) (84966,101258)	(28347,88148)	0011011101011101110101100001010100	u

22	(49174,2040) (60765,68770)	(96402,72483)	10111100010010010100011101100100011	v
23	(85160,16169) (17354,13320)	(99530,93900)	11000010011001010101101110110011100	w
24	(29077,83287) (55139,55946)	(6165,70870)	00001100000010101100010100110101110	x
25	(70472,38767) (52917,27928)	(51778,78661)	01100101001000010100110011010001 01	y
26	(16977,52908) (105225,16336)	(99214,10194)	11000001110001110000100111110100 10	z
27	(83705,25047) (105532,37028)	(488,54677)	00000000111101000011010101100101 01	0
28	(52251,9320) (5377,30467)	(40819,95052)	01001111101110011101110011010011 00	1
29	(54200,68826) (91864,30287)	(91879,35667)	10110011011100111010001011010100 11	2
30	(56752,103028) (2165,24122)	(11946,103115)	00010111010101010110010010110010 11	3
31	(97171,5480) (30568,42919)	(45581,72176)	01011001000001101100011001111100 00	4
32	(79702,70986) (75931,87822)	(49349,49850)	01100000011000101011000010101110 10	5
33	(51009,42422) (59549,80984)	(59908,67695)	01110101000000100100001000011011 11	6
34	(11080,57201) (17077,91682)	(37894,79969)	01001010000000110100111000011000 01	7
35	(46477,5525) (88074,97386)	(51940,104526)	01100101011100100110011000010011 10	8
36	(96238,26223) (100753,69451)	(18707,68219)	00100100100010011100001010011110 11	9
37	(45707,63125) (69729,55545)	(34968,38365)	01000100010011000010010101110111 01	+
38	(98379,39411) (10309,57698)	(71775,32626)	10001100001011111001111111011100 10	,
39	(68014,52877) (104139,53114)	(53652,88638)	01101000110010100101011010001111 10	=
40	(106597,48527) (260,38867)	(43356,14918)	01010100101011100000111010010001 10	space
⋮ ⋮	⋮ ⋮	⋮ ⋮	⋮ ⋮	⋮ ⋮

Bibliography

[1] A. Amadori, F. Pintore and M. Sala, (2018), On the discrete logarithm problem for prime-field elliptic curves, Finite Fields and Their Applicationsx, 168-182.

[2] R. Avanzi, H. Cohen, C. Doche, G. Frey, T. Lange, K. Nguyen and F. Vercauteren, (2006), Handbook of elliptic and hyperelliptic cryptography. Chapman and Hall/CRC.

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

[4] A. Baker, (1966), Linear forms in the logarithms of algebraic numbers, Mathematika 13, 204-216.

[5] I. F. Blake, G. Seroussi and N. P. Smart, (1999), Elliptic Curves in Cryptography. Cambridge.

[6] I. F. Blake, G. Seroussi and N. P. Smart, (2005), Advances in Elliptic Curve Cryptography. Cambridge.

[7] A. Boulbot, A. Chillali, A. Mouhib,(2016), Elliptic curves over the ring $\mathbb{F}_q[e]$, $e^3 = e^2$. Gulf J. Math, 123-129.

[8] A. Boulbot, A. Chillali and A. Mouhib, (2019), Elliptic curves over the ring R, Bol. Soc.Parana. Mat 38(3), 193-201.

[9] A. Boulbot, A. Chillali, A. Mouhib,(2020), Elliptic Curves Over the Ring $\mathbb{R}^*$, Boletim da Sociedade Paranaense de Matematica, 193-201.

[10] W. Bosma, H. W. Lenstra, (1995), Complete System of Two Addition Laws for Elliptic Curves, Journal of Number Theory, 229-240.

[11] C. Boyd and A. Mathuria, (2003), Protocols for Authentication and Key Establishment, Information Security and Cryptography Series, Springer-Verlag, Heidelberg.

[12] E. Brown and C. Parry, (1974), The imaginary bicyclic biquadratic fields with class-number 1, J. Reine Angew 266, 118-120.

[13] Z. Cheddour, A. Chillali and A. Mouhib, (2022), The "Elliptic" matrices and a new kind of cryptography, Bol. Soc. Parana. Mat, V 41 p 1-12.

[14] Z. Cheddour, A. Chillali and A. Mouhib, (2022), Torsion section of elliptic curves over quadratic extensions of $\mathbb{Q}$, Italian Journal of Pure and Applied Mathematics.

[15] Z. Cheddour, A. Chillali and A. Mouhib, (2023), Elliptic curve and k-Fibonacci-like sequence, Scientific African, V 20 p 1-11.

[16] Z. Cheddour, A. Chillali and A. Mouhib, (2023), Elliptic curve over a finite ring, Annals of the University of Craiova, Mathematics and Computer Science Series.

[17] Z. Cheddour, A. Chillali and A. Mouhib, Torsion of elliptic curves over imaginary multiquadratic number fields of class number one, (preprint).

[18] Z. Cheddour, A. Chillali and A. Mouhib, Torsion of elliptic curves over quadratic cyclotomic fields in quadratic extensions of the base field, (preprint).

[19] A. Chillali, Ellipic cuvre over ring, International Mathematical Forum, 1501-1505.

[20] A. Chillali, (2011), Cryptography over elliptic curve of the ring $\mathbb{F}_q[e], e^4 = 0$, World Acad. of Sci. Eng. and Technol 78, 848-850.

[21] A. Chillali and M. Sahmoudi, (2020), SCC-Cryptosystem on an algebraic closure ring,J. Discrete Mathematical Sciences and Cryptography, 23(8) 1475-1485.

[22] M. Ciet, J. J. Quisquater and F. Sica, (2011), Compact elliptic curve representations, J. Math. Cryptol, 89-100.

[23] J. J. Climent, P. R. Navarro and L. Tortosa, (2012), Key exchange protocols over non-commutative rings. The case of End $(\mathbb{Z}_p \times \mathbb{Z}_{p^2})$, Int. J. Comput. Math 89(1314), 1753-1763.

[24] R. Cramer and V. Shoup, (1998), A practical public key cryptosystem provably secure against adaptive chosen ciphertext attack. In: Krawczyk, H. (eds) Advances in Cryptology CRYPTO '98. CRYPTO 1998. Lecture Notes in Computer Science, vol 1462. Springer, Berlin, Heidelberg.

[25] R. Cramer and V. Shoup, (2000), Signature Schemes Based on the Strong RSA Assumption. ACM Trans. Inf. Syst. Security (ACM TISSEC), 161-185.

[26] M. Derickx, A. Etropolski, M. V. Hoeij, J. S. Morrow and B. D. Zureick, (2021), Sporadic cubic torsion, Algebra and Number Theory, 1837-1864.

[27] T. V. Deursen, S. Radomirovic, (2011), Insider Attacks and Privacy of RFID Protocols, EuroPKI.

[28] O. Deveci, E. Karaduman and C. M. Campbell, (2011), On the k-Fibonacci sequences in finite binary polyhedral groups, Algebra Colloq 18(01), 945-954.

[29] O. Deveci, E. Karaduman and C. M. Campbell, (2017), The Fibonacci-circulant sequences and their applications, Iran. J. Sci. Technol. Trans. Sci 41(4), 1033-1038.

[30] O. Deveci, A. G. Shannon, (2018), The quaternion-Pell sequence, Commun. Algebra 46(12), 5403-5409.

[31] O. Deveci, A. G. Shannon, (2018), The complex-type k-Fibonacci sequences and their applications, Commun. Algebra.

[32] M. Edson and O. Yayenie, (2009), A new generalization of Fibonacci sequences and extended Binet's formula, Integers, 639-654.

[33] M. Edson, S. Lewis, and O. Yayenie,(2011), The k-periodic Fibonacci sequence and an extended Binets formula, Integers, 12 pp.

[34] M. Eftekhari, (2012), A Diffie-Hellman key exchange protocol using matrices over non-commutative rings, Groups Complex. Cryptol 4(1), 167-176.

[35] M. Eftekhari, (2017), Cryptanalysis of some protocols using matrices over group rings, in Int. Conf. on Cryptology in Africa: Progress in Cryptology - AFRICACRYPT 2017, Lecture Notes in Computer Science, Vol. 10239.

[36] $\ddot{O}$. Ejder, (2018), Torsion subgroups of elliptic curves over quadratic cyclotomic fields in elementary abelian 2-extensions, J. Number Theory, 266-301.

[37] T. ElGamal, (1984), A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms, Advances in Cryptology, CRYPTO 1984, Lecture Notes in Computer Science, vol 196. Springer, Berlin Heidelberg.

[38] A. Enge, (1999), Elliptic curves and their applications to cryptography: An introduction, Kluwer Academic Publishers, Dordrecht.

[39] S. Falcon, A. Plaza, (2007), The k-Fibonacci sequence and the Pascal 2-triangle, Chaos Solitons Fractals, 38-49.

[40] S. Falcon, A. Plaza, (2009), k-Fibonacci sequences modulo m. Chaos Solitons Fract 41(1), 497-504.

[41] A. Feaver, (2017), Imaginary multiquadratic fields of class number 1. J. Number Theory, 93-117.

[42] W. Fulton, (2008), Algebraic Curves: An Introduction to Algebraic Geometry.

[43] D. Jeon, C. H. Kim and E. Park, (2006), On the torsion of elliptic curves over quartic number fields, J. Lond. Math. Soc, 1-12.

[44] D. Jeon, C. H. Kim and Y. Lee, (2011), Families of elliptic curves over quartic number fields with prescribed torsion subgroups, Math. Comp 80, 2395-2410.

[45] M. H. Hassib, A. Chillali and M. A. Elomary, (2015), Elliptic curve over a chain ring of characteristic 3, International Workshop of Algebra and Applications, FST Fez, Morocco, Journal of Taibah University for Science.

[46] D. Hankerson, A. Menezes and S. Vanstone, (2004), Guide to elliptic curve cryptography. Springer.

[47] K. Heegner, (1952), Diophantische Analysis und Modulfunktionen, Mathematische Zeitschrift, 227-253.

[48] S. D. Galbraith, (2012), Mathematics of public key cryptography. Cambridge University Press.

[49] C. F. Gauss, (1801), Disquisitiones Arithmeticae, Springer New York, NY, XX, 472.

[50] E. Gonzlez-Jimnz and M. T. Jos, (2014), Torsion of rational elliptic curves over quadratic fields, RACSAM, 923-934.

[51] M. Gotaishi and S. Tsujii, (2018), Organizational Cryptography for Access Control. IACR Cryptol. ePrint Arch.

[52] A. Grini, A. Chillali and H. Mouanis, (2021), Cryptography over twisted Hessian curves of the ring $\mathbb{F}_q[e]$, $e^2 = 0$, Adv. Math. Sci. J, 235-243.

[53] A. Grini, A. Chillali and H. Mouanis, (2022), A new cryptosystem based on a twisted Hessian curve $H^4_{a,d}$, Journal of Applied Mathematics and Computing, 235-243.

[54] D. Kahrobaei, C. Koupparis and V. Shpilrain, (2013), Public key exchange using matrices over group rings, Groups Complex. Cryptol 5(1), 97-115.

[55] S. Kamienny,(1992), Torsion points on elliptic curves and q-coefficients of modular forms, Invent. Math 109(2), 221-229.

[56] S. Kamienny, F. Najman, (2012), Torsion groups of elliptic curves over quadratic fields, Acta Arithmetica, 291-305.

[57] E. Karaduman, H. Aydin, (2009), k-Fibonacci sequences in some special groups of finite order, Math. Comput. Modell, 53-58.

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

[59] E. Kilic, (2008), The Binet formula, sums and representations of generalized Fibonacci p-numbers, Eur. J. Combin 29(3), 701-711.

[60] E. Kilic, D. Tasci, (2006), On the generalized order-k Fibonacci and Lucas numbers, Rocky Mt. J. Math 36(6), 1915-1926.

[61] E. Kilic, D. Tasci, (2007), On the permanents of some tridiagonal matrices with applications to theFibonacci and Lucas numbers, Rocky Mt. J. Math 37(6), 1953-1969.

[62] N. Koblitz, (1987), Elliptic curve cryptosystems, Mathematics of Computation, 203-209.

[63] N. Koblitz, A. Menezes and S. Vanstone, (2000), The State of Elliptic Curve Cryptography, Designs. Codes and Cryptography, 173-193.

[64] D. S. Kubert, (1976), Universal bounds on the torsion of elliptic curves, Proc. Lond. Math. Soc, 193-237.

[65] Y. Kwon, (2016), A note on the modified k-Fibonacci-Like sequence, Commun. Korean Math. Soc, 16 pp.

[66] S. Lagheliel, A. Chillali and A. Ait-Mokhtar, (2022), New encryption scheme using k-Fibonacci-like sequence, Asian-European Journal of Mathematics.

[67] M. Laska and M. Lorenz, (1985), Rational points on elliptic curves over $\mathbb{Q}$ in elementary abelian 2-extensions of $\mathbb{Q}$, J. Reine Angew. Math, 163-172.

[68] H. W. Lenstra, (1986), Elliptic Curves and Number-Theoretic Algorithms, Processing of the International Congress of Mathematicians, Berkely, California,USA, 156-163.

[69] B. Mazur, (1978), Rational isogenies of prime degree, with an appendix by D. Goldfeld, Invent. Math, 129-162.

[70] A. J. Menezes, T. Okamoto, and S. Vanstone, (1993), Reducing elliptic curve logarithms to a finite field. IEEE Trans Inform. Theory, 1639-1646.

[71] A. J. Menezes and Y. H. Wu, (1997), The discrete logarithm problem in $GL(n, q)$, ARS Combinatoria 47, 23-32.

[72] G. Micheli, (2015), Cryptanalysis of a non-commutative key exchange protocol, Adv. Math. of Comm 9(2), 247-253.

[73] V. Miller, (1986), Use of elliptic curves in cryptography, Advances in Cryptology-Crypto'85, Lecture Notes in Comput. Sci. 218, Springer, Berlin, 417-426.

[74] F. Najman, (2010), Complete classification of torsion of elliptic curves over quadratic cyclotomic fields, J. Number Theory, 1964-1968.

[75] F. Najman, (2011), Torsion of elliptic curves over quadratic cyclotomic fields, Math. J. Okayama U, 75-82.

[76] F. Najman, (2016), Torsion of rational elliptic curves over cubic fields and sporadic points on X1. n/, Math. Res. Lett, 245-272.

[77] B. Newman, (2017), Growth of torsion of elliptic curves with full 2-torsion over quadratic cyclotomic fields, J. Number Theory, 570-601.

[78] A. Odlyzko, (2000), Discrete logarithms: The past and the future, Designs, Codes and Cryptography, 129-145.

[79] R. Odoni, V. Varadharajan and P. Sanders, (1984), Public key distribution in matrix rings, Electron. Lett 20(9), 386-387.

[80] E. Ozkan, (2014), Truncated Lucas sequences and its period, Appl. Math. Comput, 285-291.

[81] E. Ozkan, H. Aydin and R. Dikici, (2003), 3-step Fibonacci series modulo m, Appl. Math. Comput 143(1), 165-172.

[82] N. Y. Ozgur, (2005), On the sequences related to Fibonacci and Lucas numbers, J. Korean Math. Soc 42(1), 135-151.

[83] F. P. Rabarison, (2010), Structure de torsion des courbes elliptiques sur les corps quadratiques, Acta Arith, 17-52.

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

[85] S. Schmitt and H. G. Zimmer, (2003), Elliptic Curves, A Computational Approach, Walter de Gruyter, 367 pages.

[86] R. Schoof, (1995), Elliptic Curves Over finite Fields and the Computation of Square Roots mod p, Mathematics of Computation, 483-494.

[87] R. Schoof, (1995), Counting points on elliptic curves over finite fields, Journal de Thorie des Nombres de Bordeaux.

[88] J. H. Silverman, (1986), The arithmetic of elliptic curves, Graduate Texts in Mathematics, Springer-Verlag, New York.

[89] A.P. Stakhov, (2007), The golden matrices and a new kind of cryptography, Chaos, Solitons and Fractals 32, 1138-1146.

[90] A. P. Stakhov and B. Rozin, (2006), Theory of Binet formulas for Fibonacci and Lucas p-numbers, Chaos Solitons Fract 27(5), 1162-1177.

[91] A. P. Stakhov and B. Rozin, (2006), The continuous functions for the Fibonacci and Lucas p-numbers, Chaos Solitons Fract 28(4), 1014-1025.

[92] HM. Stark, (1967), A complete determination of the complex quadratic fields of class-number one, Michigan Mathematical Journal, 1-27.

[93] D. R. Stinson, (2006), Cryptography Theory And Practice, 3rd edn. Chapman Hall/CRC, New York.

[94] A. Tadmori, A. Chillali and M. Ziane, (2015), Cryptography over the elliptic curve $E_{a,b}$, J. Taibah Univ. Sci, 326-331.

[95] A. Tadmori, A. Chillali and M. Ziane, (2021), Elliptic Curves Over a non-local ring $\mathbb{F}_{2^d}[\epsilon]$, $\epsilon^2 = \epsilon$, Asian-European Journal of Mathematics.

[96] D. Tasci, M. C. Firengiz, (2010), Incomplete Fibonacci and Lucas p-numbers, Math. Comput. Modell 52(9-10), 1763-1770.

[97] M. Virat, (2009), Courbe elliptique sur un anneau et applications cryptographiques, Nice-Sophia Antipolis, (Thse du Doctoral).

[98] D. D. Wall, (1960), Fibonacci series modulo m, Am. Math. Mon 67(6), 525-532.

[99] P. V. Wamelen, (1998), equations for the Jacobian of a hyperelliptic curve, Transactions of the American mathematical society, 3083-3106.

[100] L. C. Washington, (2008), Elliptic Curves, Number Theory and Cryptography, 2nd edn. CRC Press.

[101] W. C. Waterhouse, (1979), Introduction to affine group schemes, Graduate texts in mathematics, New York-Berlin: Springer-Verlag, vol 66.

[102] O. Yayenie, (2011), A note on generalized Fibonacci sequences, Appl. Math. Comput, 5603-5611.

[103] M. Zeriouh, A. Chillali and A. Boua, (2019), Cryptography Based on the Matrices, Bol. Soc. Paran. Mat, 75-83.