Filomat 40:2 (2026), 557–566
https://doi.org/10.2298/FIL2602557C

Published by Faculty of Sciences and Mathematics,
University of Niš, Serbia
Available at: http://www.pmf.ni.ac.rs/filomat

p-Sylow subgroup growth of elliptic curves over Galois extension of prime degree q upon base change from quadratic cyclotomic number fields

Zakariae Cheddour[a,*], Abdelhakim Chillali[b], Ali Mouhib[b]

[a] *Department of Mathematics, University Abdelmalek Essaadi, Faculty of Sciences and Technology Al Hoceima, BP 34, Ajdir, 32003, Al Hoceima, Morocco*
[b] *Department of Mathematics, University of Sidi Mohamed Ben Abdellah-USMBA, FP Taza, Morocco*

Abstract. Let $L = \mathbb{Q}(i)$ or $\mathbb{Q}(\sqrt{-3})$ be a quadratic cyclotomic number field, and let K be a Galois extension of L of prime degree q. This paper examines the behavior of p-Sylow subgroups of elliptic curves defined over K, focusing on their growth under base change from L. The study uncovers distinctive patterns in subgroup growth, shaped by both the arithmetic nature of the base field and the intrinsic properties of the elliptic curves.

1. Introduction

Elliptic curves are central objects in number theory, algebraic geometry, and cryptography, known for their rich algebraic and geometric structures. Understanding their group-theoretic behavior over various fields and extensions remains a topic of significant interest across both pure and applied mathematics [1, 2, 4, 15]. In this paper, we investigate the growth of p-Sylow subgroups of elliptic curves over number fields of prime degree, focusing on base changes from quadratic cyclotomic fields.
The choice of these base fields is motivated by their deep connections to number theory and their prominent role in diverse mathematical applications. Our study primarily examines the growth patterns of the p-Sylow subgroups associated with elliptic curves over these extensions. These subgroups play a vital role in understanding the structure of finite groups, and analyzing their growth offers important insights into the algebraic and arithmetic behavior of elliptic curves.
Consider an elliptic curve E over a number field K with degree q. The classification of torsion subgroups of elliptic curves over number fields has been extensively studied. Numerous mathematicians have contributed to identifying these sets for fields of various degrees. In particular, Mazur established the complete

2020 *Mathematics Subject Classification*. Primary 14H52; Secondary 20D20, 14G32.
Keywords. Elliptic curves, p-Sylow subgroups, torsion subgroup, Galois group theory.
Received: 30 June 2024; Revised: 31 October 2025; Accepted: 18 November 2025
Communicated by Ljubica Velimirović
* Corresponding author: Zakariae Cheddour
Email addresses: z.cheddour@uae.ac.ma (Zakariae Cheddour), Abdelhakim.Chillali@usmba.ac.ma (Abdelhakim Chillali), Ali.Mouhib@usmba.ac.ma (Ali Mouhib)
ORCID iDs: https://orcid.org/0000-0001-5077-0693 (Zakariae Cheddour), https://orcid.org/0000-0002-2033-0280 (Abdelhakim Chillali), https://orcid.org/0000-0002-2040-9183 (Ali Mouhib)

classification of torsion subgroups of elliptic curves defined over $K = \mathbb{Q}$ [10].

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

Kenku, Momose, and Kamienny classify the different isomorphism types of $E(K)_{tors}$ in [9] and [8] respectively, for a quadratic number field K and E/K.

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

For $q = 3$, Jeon, Kim, and Schweizer in [6] found all the torsion structures that appear infinitely often as one runs through all elliptic curves over all cubic fields. A similar result was obtained for $q = 4$ by Jeon, Kim, and Park in [7], and for $q = 5, 6$ by Derickx and Sutherland in [3].
For elliptic curves defined over $\mathbb{Q}(i)$ or $\mathbb{Q}(\sqrt{-3})$, we do not have a precise description of the torsion subgroups that can appear over an extension of $\mathbb{Q}(i)$ or $\mathbb{Q}(\sqrt{-3})$ of degree q. In particular, Najman's paper, referenced as [11, 12], presents significant results concerning the structure of torsion subgroups of elliptic curves defined over cyclotomic quadratic number fields. Specifically, Najman establishes the following classifications:

- For $K = \mathbb{Q}(i)$,

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

- Similarly, for $K = \mathbb{Q}(\sqrt{-3})$,

$$\begin{aligned} &\mathbb{Z}/n\mathbb{Z} \quad \text{for} \quad 1 \leq n \leq 12, \quad n \neq 11, \\ &\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z} \quad \text{for} \quad 1 \leq n \leq 4, \\ &\mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3n\mathbb{Z} \quad \text{for} \quad 1 \leq n \leq 2. \end{aligned}$$

Further refinements were made by Newman [13, 14], whose work determined the sets of torsion structures that can arise as quadratic twists of a given torsion structure. He also studied the growth of the torsion part of an elliptic curve on $\mathbb{Q}(i)$ or $\mathbb{Q}(\sqrt{-3})$ that can appear over quadratic extension of the base fields.
Moreover, Ejder [5] determined the torsion subgroups of elliptic curves defined over $\mathbb{Q}(i)$ and $\mathbb{Q}(\sqrt{-3})$ in elementary abelian 2-extensions K of these fields. More precisely, the set of torsion subgroups is characterized by the following elements

- If $K = \mathbb{Q}(i)$, then $E(K)_{tors}$ is isomorphic to one of the following groups:

$$\begin{aligned} &\mathbb{Z}/n\mathbb{Z} \quad \text{for} \quad n \in \{1, 3, 5, 7, 9, 15\}, \\ &\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z} \quad \text{for} \quad n \in \{2, 3, 4, 5, 6, 8\}, \\ &\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4n\mathbb{Z} \quad \text{for} \quad 2 \leq n \leq 4, \\ &\mathbb{Z}/n\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z} \quad \text{for} \quad n \in \{2, 3, 4, 6, 8\}. \end{aligned}$$

- If $K = \mathbb{Q}(\sqrt{-3})$, then $E(K)_{tors}$ is either isomorphic to one of the groups listed above or

$$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/32\mathbb{Z}.$$

The main goal of this paper is to investigate the growth of the p-Sylow subgroups of elliptic curves over Galois extensions of prime degrees upon base change from quadratic cyclotomic number fields. This question naturally arises, given the significance of investigating elliptic curves over base changes in solving Diophantine equations.
In the following section, we present several auxiliary results, including a key step for constraining the full torsion subgroup, which is instrumental in studying the growth of p-Sylow subgroups of elliptic curves over Galois extensions of the base field with prime degree.

2. Auxiliary results

Before we begin our study, let's establish a few useful notations and abbreviations:

Notation 2.1.

- *L be a quadratic cyclotomic number field.*
- *K a Galois extension of prime degree q of L which means that $[K : L] = q$ and $\mathrm{Gal}(K/L) \simeq \mathbb{Z}/q\mathbb{Z}$, otherwise K is a degree q extension of L.*
- *E an elliptic curve defined over L.*
- *$E[n]$ the group of all points of $E(\bar{K})$ whose order is a divisor of n.*
- *$E(K)[n] = \{P = (x, y) \in E[n] \mid x, y \in K\}$.*
- *$\mathbb{Z}/n\mathbb{Z}$ a cyclic group of order n.*
- *For an odd positive integer m, we denote by ζ_m a m-th primitive root of unity.*
- *$E(K)\left[p^\infty\right]$ the p-Sylow subgroup of $E(K)$.*

Remark 2.2. *If $E(K)\left[p^\infty\right] \neq \{O\}$ we have that*

$$p \in S(q)$$

where $S(q)$ denotes the set of prime numbers p for which there exists a number field K of degree at most q, and an elliptic curve E/K containing a torsion subgroup of order multiple of p. Consequently, for primes not belonging to $S(q)$, we obtain

$$E(K)\left[p^\infty\right] = \{O\}.$$

To prove the main theorems 3.1, 3.2, 3.3, and 3.4, our approach began with the crucial step of constraining the full torsion subgroup, a crucial step that was rigorously established and supported by the proof of the following two lemmas.

Lemma 2.3. *Consider an elliptic curve E defined over $\mathbb{Q}(i)$. Thus, the elliptic curve E has a full n-torsion for $n \geq 2$ over K only when n equals 2, or 4.*

Proof. Assuming that $E(K)$ has a full n-torsion over K, according to Weil's pairing, this implies that the nth roots of unity are defined in K. Consequently, we derive

$$\mathbb{Q}\left(\zeta_{\mathrm{lcm}(4,n)}\right) \subseteq K.$$

Subsequently, we can write :

$$\left[K : \mathbb{Q}\left(\zeta_{\mathrm{lcm}\,(4,n)}\right)\right]\left[\mathbb{Q}\left(\zeta_{\mathrm{lcm}\,(4,n)}\right) : \mathbb{Q}\right] = [K : \mathbb{Q}] = 2q$$

and since $\left[\mathbb{Q}\left(\zeta_{lcm(4,n)}\right) : \mathbb{Q}\right] = \varphi(lcm(4, n))$ divides $2q$, the only possibilities for n are 2, or 4. □

Lemma 2.4. *Consider an elliptic curve E defined over* $\mathbb{Q}(\sqrt{-3})$. *Thus, the elliptic curve E has a full n-torsion for* $n \geq 2$ *over K only when n equals* 2, 3 *or* 6.

Proof. Following the same approach as in the previous proof, we obtain that

$$\mathbb{Q}\left(\zeta_{\text{lcm }(a,n)}\right) \subseteq K, \text{ where a } = 3 \text{ or } 6.$$

We can then write :

$$\left[K : \mathbb{Q}\left(\zeta_{\text{lcm }(a,n)}\right)\right]\left[\mathbb{Q}\left(\zeta_{\text{lcm }(a,n)}\right) : \mathbb{Q}\right] = [K : \mathbb{Q}] = 2q$$

and since $\left[\mathbb{Q}\left(\zeta_{lcm(a,n)}\right) : \mathbb{Q}\right] = \varphi(lcm(a,n))$ divides $2q$, the only possibilities for n are 2, 3 or 6. □

3. Main results

In this section, we present our main theorems 3.1, 3.2, 3.3, and 3.4, which investigate the growth of the p-Sylow subgroup of elliptic curves defined over a quadratic cyclotomic field L that can appear on K.

Theorem 3.1. *Consider a Galois extension* $K/\mathbb{Q}(i)$ *of prime degree* $q \geq 3$ *and E be an elliptic curve over* $\mathbb{Q}(i)$. *Then, if* $E(\mathbb{Q}(i))[2] = 0$ *it follows that*

$$E(K)\,[2^\infty] \text{ is either trivial, } \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \text{ or } \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}.$$

On the other hand, if $E(\mathbb{Q}(i))\,[2^\infty] \neq 0$ *then* $E(\mathbb{Q}(i))\,[2^\infty] = E(K)\,[2^\infty]$.

Theorem 3.2. *Consider a Galois extension* $K/\mathbb{Q}(\sqrt{-3})$ *of prime degree* $q \geq 3$ *and E be an elliptic curve over* $\mathbb{Q}(\sqrt{-3})$. *Then, if* $E(\mathbb{Q}(\sqrt{-3}))[2] = 0$ *it follows that*

$$E(K)\,[2^\infty] \text{ is either trivial or } \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}.$$

On the other hand, if $E(\mathbb{Q}(\sqrt{-3}))\,[2^\infty] \neq 0$ *then,* $E(\mathbb{Q}(\sqrt{-3}))\,[2^\infty] = E(K)\,[2^\infty]$.

Theorem 3.3. *Consider* K/L *a Galois extension of prime degree* $q \geq 3$ *and E be an elliptic curve over L. Then, if* $L = \mathbb{Q}(\sqrt{-3})$ *it follows that*

$$E(K)\,[3^\infty] \text{ is isomorphic to a subgroup of } \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/9\mathbb{Z}.$$

On the other hand, if $L = \mathbb{Q}(i)$ *then,*

$$E(K)\,[3^\infty] \text{ is isomorphic to a subgroup of } \mathbb{Z}/9\mathbb{Z}.$$

Theorem 3.4. *Consider* K/L *a Galois extension of prime degree* $q \geq 3$ *and E be an elliptic curve over L. Then,*

1. *If* $p = q$ *and* $E(L)[q] = 0$ *then* $E(K)[q] = 0$.
2. *If* $p \neq q$. *Then, the p-Sylow subgroup of* $E(K)$ *is either trivial or isomorphic to* $\mathbb{Z}/p\mathbb{Z}$.
3. *If q is coprime to* $p - 1$. *Then, the p-Sylow groups of* $E(L)$ *and* $E(K)$ *are equal.*

3.1. Proof of Theorems 3.1 and 3.2

To prove Theorems 3.1 and 3.2, we will rely on the following results. In these theorems, we focus on analysing the growth of 2-Sylow subgroups of elliptic curves over $\mathbb{Q}(i)$ and $\mathbb{Q}(\sqrt{-3})$.

Theorem 3.5. *Consider a Galois extension K of degree q of* $\mathbb{Q}(i)$ *and E be an elliptic curve over* $\mathbb{Q}(i)$. *If* $E(\mathbb{Q}(i))[2] = 0$. *Then*

- $E(K)[2] \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$

- *If $E(K)$ has a point of order 4, then $E(K)[4] \simeq \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$.*
- *E cannot have points of order 8 over K.*

Proof. Under the assumption that $E/\mathbb{Q}(i)$ and $E(\mathbb{Q}(i))[2] = 0$, the elliptic curve E can be represented by the equation $y^2 = f(x) = x^3 + ax + b$, where the cubic polynomial $f(x)$ is irreducible on $\mathbb{Q}(i)$.

- Assume that $E(K)[2] \neq 0$. Since K is a Galois extension of $\mathbb{Q}(i)$ and f has a root on K, we can deduce that all roots of f are also elements of K. Consequently, this implies that
$$E(K)[2] \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}.$$
- Assume that $E(K)[4] \neq 0$. Since $\zeta_4 \in K$, it follows that
$$E(K)[4] \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z} \text{ or } \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}.$$
Assuming that
$$E(K)[4] \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}.$$
Let $C := \mathrm{Gal}(K/\mathbb{Q}(i))$, and consider the short exact sequence
$$0 \to E(K)[2] \to E(K)[4] \to E(K)[4]/E(K)[2] \to 0$$
Therefore, we have
$$\begin{aligned} 0 \to H^0(C, E(K)[2]) &\to H^0(C, E(K)[4]) \\ &\to H^0(C, E(K)[4]/E(K)[2]) \to H^1(C, E(K)[2]) \end{aligned}$$
Since $E(K)[2] \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ and $\sharp C = q$ (q is a prime number > 2) it follows that $H^1(C, E(K)[2]) = 0$, on the other hand the group $E(K)[4]/E(K)[2]$ is of order 2. Thus,
$$H^0(C, E(K)[4]) / H^0(C, E(K)[2]) \simeq H^0(C, E(K)[4]/E(K)[2]) \simeq \mathbb{Z}/2\mathbb{Z}$$
Consequently, we have that $H^0(C, E(K)[4]) \neq 0$. This leads to a contradiction, indicating that $E(\mathbb{Q}(i))$ possesses a 2-torsion point.
Therefore, the only possible 4-torsion structure over K must be
$$E(K)[4] \simeq \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}.$$
- Assume that $E(K)[8] \neq 0$. It follows that
$$E(K)[8] \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z}, \ \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z}, \text{ or } \mathbb{Z}/8\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z}.$$
Let $C := \mathrm{Gal}(K/\mathbb{Q}(i))$, and consider the short exact sequence
$$0 \to E(K)[2] \to E(K)[8] \to E(K)[8]/E(K)[2] \to 0$$
Therefore, we have
$$\begin{aligned} 0 \to H^0(C, E(K)[2]) &\to H^0(C, E(K)[8]) \\ &\to H^0(C, E(K)[8]/E(K)[2]) \to H^1(C, E(K)[2]) \end{aligned}$$
If $E(K)[8] \simeq \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z}$. Then $E(K)[8]/E(K)[2] \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$ and it follows from the previous proof that $H^0(C, E(K)[8]/E(K)[2]) \neq 0$, and since $H^1(C, E(K)[2]) = 0$ it follows that $H^0(C, E(K)[8]) \neq 0$. Consequently, it implies that $E(\mathbb{Q}(i))[2] \neq 0$, leading to a contradiction.
If $E(K)[8] \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z}$. Then $E(K)$ has a point of order 4. It follows from the second statement that $E(K)[4] \simeq \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$, which is a contradiction.
Note that Lemma 2.3 indicates that $E(K)[8]$ cannot be isomorphic to $\mathbb{Z}/8\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z}$.

□

Theorem 3.6. *Consider a Galois extension K of prime degree q of $\mathbb{Q}(\sqrt{-3})$, and E be an elliptic curve over $\mathbb{Q}(\sqrt{-3})$. If $E(\mathbb{Q}(\sqrt{-3}))[2] = 0$. Then*

- $E(K)[2] \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$.
- *E cannot have points of order 4 over K.*

Proof. Assume that $E/\mathbb{Q}(\sqrt{-3})$ and $E(\mathbb{Q}(\sqrt{-3}))[2] = 0$.

- Assume that $E(K)[2] \neq 0$. Since K is a Galois extension of $\mathbb{Q}(\sqrt{-3})$ and f has a root on K, we can deduce that all roots of f are also elements of K. Consequently, this implies that

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

- Assume that $E(K)[4] \neq 0$. Since $\zeta_4 \notin K$, it follows that the possibility for $E(K)$ to have a 4 -torsion point is that

$$E(K)[4] \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}.$$

Let $C := \mathrm{Gal}(K/\mathbb{Q}(\sqrt{-3}))$, and consider the short exact sequence

$$0 \to E(K)[2] \to E(K)[4] \to E(K)[4]/E(K)[2] \to 0$$

it follows that

$$\begin{aligned} 0 \to H^0(C, E(K)[2]) &\to H^0(C, E(K)[4]) \\ &\to H^0(C, E(K)[4]/E(K)[2]) \to H^1(C, E(K)[2]) \end{aligned}$$

Since $E(K)[2] \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ and $\sharp C = q$ (q is a prime number > 2) it follows that $H^1(C, E(K)[2]) = 0$, on the other hand $E(K)[4]/E(K)[2]$ is a group of order 2, then

$$H^0(C, E(K)[4]/E(K)[2]) \simeq \mathbb{Z}/2\mathbb{Z}$$

Therefore, we can conclude that $H^0(C, E(K)[4]) \neq 0$. This leads to a contradiction, indicating that $E(\mathbb{Q}(\sqrt{-3}))$ possesses a 2 -torsion point.
This means that the elliptic curve E has no points of order 4 over K.

□

Theorem 3.7. *Consider a Galois extension K/L of prime degree q and E be an elliptic curve over L. If the torsion group of the elliptic curve E over L has a nontrivial 2-Sylow subgroup, then $E(K)$ has the same 2-Sylow subgroup as $E(L)$.*

Proof. If $E(L) \simeq \mathbb{Z}/2n\mathbb{Z}$ for $n = 1, 2$ or 4, then if the 2-Sylow group grows, we must find a K-rational point $P = (x, y)$ (but not L-rational).
Let $Q \in E(L)$ be a nontrivial torsion point of order 2 such that $2P = Q$, put $E : y^2 = f(x) = x^3 + ax + b$ where α, β and γ are roots of f on K.
Since $E(L) \neq 0$ we can consider that $\alpha \in L$ and $Q = (\alpha, 0)$. On the other hand, we have $(x_{2P}, y_{2P}) = \left(x_Q, y_Q\right)$, and then

$$\begin{aligned} x_{2P} &= m^2 - 2x = \alpha \\ y_{2P} &= m(x - x_{2P}) - y = 0. \\ m &= \frac{3x^2 + a}{2y}. \end{aligned}$$

It follows that $\left(3x^2+a\right)^2 = 4m^2y^2$ and then

$$x^4 - 4\alpha x^3 - 2ax^2 - 4(\alpha a + 2b)x + a^2 4\alpha b = 0.$$

The discriminant of this polynomial is

$$D = -4096\left(4a^3 + 27b^2\right)\left(\alpha^3 + a\alpha + b\right)^2 = 0.$$

Thus, the polynomial has a multiple root. This means that $\beta = \gamma \in K\backslash L$ and then $f(x) = (x-\alpha)\left(x^2+ex+f\right)$ where x^2+ex+f is irreducible over L. Which is a contradiction.
Consider $\mathrm{Gal}(K/L) \simeq \mathbb{Z}/q\mathbb{Z}$ and let T and Q be elements of $E(L)$ such that T is of order 4 and Q is of order 8 (if they exist) and

$$A = \{P \in E(K) \mid 2P = T\} \text{ and } B = \{P \in E(K) \mid 2P = Q\}$$

The action of the group $\mathrm{Gal}(K/L)$ is observed on both sets A, which consists of 4 elements, and B, which comprises 8 elements. Furthermore, according to the orbit stabilizer theorem, the orbits have length q. This implies that A and B are decomposed into sets of q elements each, which is impossible because q is a prime number > 2. □

4. Proof of Theorem 3.3

To prove Theorem 3.3, we will use several auxiliary results and focus on the growth of the 3-Sylow subgroups of elliptic curves over $\mathbb{Q}(i)$ and $\mathbb{Q}(\sqrt{-3})$.

Lemma 4.1. *Let $E/\mathbb{Q}(i)$ be an elliptic curve and K be a Galois extension of $\mathbb{Q}(i)$ of prime degree q. Suppose that $E(K)$ has a point of order 27, it follows that E has a 27-isogeny over $\mathbb{Q}(i)$.*

Proof. Assume that $E(K)$ has a point of order 27, and $\mathrm{Gal}(K/\mathbb{Q}(i)) =< \sigma >$. Put $E[27] =< P, Q >$ then $P^\sigma = \alpha P + \beta Q \in E(K)$, so

$$(27-\alpha)P + P^\sigma = \beta Q \in E(K).$$

- If $\beta = 0 \pmod{27}$, then $P^\sigma = \alpha P$ and the action of $\mathrm{Gal}(\overline{\mathbb{Q}(i)}/\mathbb{Q}(i))$ on $\langle P\rangle$ factors through $\mathrm{Gal}(K/\mathbb{Q}(i))$, it follows that

  $$P^\mu = \alpha P, \mu \in \mathrm{Gal}(\overline{\mathbb{Q}(i)}/\mathbb{Q}(i))$$

  which means that $E/\mathbb{Q}(i)$ has an 27-isogeny.

- If $\beta \neq 0 \pmod{27}$, then βQ is a point of order l with $l/27$ not contained in $\langle P\rangle$, from which it follows that $E(K)$ has full l-torsion. On the other hand, the Lemma 2.3 shows that the only possibilities for l are 2 or 4, which is a contradiction.

□

Theorem 4.2. *Consider a Galois extension K of $\mathbb{Q}(i)$ of prime degree q and E be an elliptic curve over $\mathbb{Q}(i)$. Then the 3-Sylow group of $E(K)$ is isomorphic to a subgroup of $\mathbb{Z}/9\mathbb{Z}$.*

Proof. By Lemma 2.3 we have that $E(K)$ cannot have full 3^n-torsion for $n \geq 1$. Suppose that $E(K)$ has a point of order 27, it follows from Lemma 4.1 that E has a 27-isogeny over $\mathbb{Q}(i)$. But there is only one family of twists of elliptic curves over $\mathbb{Q}(i)$ defined over $\mathbb{Q}$ with a 27-isogeny and torsion $\mathbb{Z}/3\mathbb{Z}$ (see, [13]), this with j-invariant -12288000 which are the twists of the elliptic curve 27a4. By the division polynomial method, we find that 27a4 has no 27-torsion over any Galois extension of prime degree $q = 3$,5, 7 or 11 of the base field $\mathbb{Q}(i)$.

We then look at a broader statement that extends these number fields. Consider $\mathrm{Gal}(K/\mathbb{Q}(i)) \simeq \mathbb{Z}/q\mathbb{Z}$. So, if $q \geq 11$, and suppose $\mathbb{Z}/27\mathbb{Z} \subset E(K)$ it follows from the Lemma 2.3 that

$$E(K)[27] \simeq \mathbb{Z}/27\mathbb{Z}.$$

Let P and Q be elements of $E(L)$ such that P is of order 3 and Q is of order 9 (if they exist) and

$$A = \{T \in E(K) \mid 3T = P\} \text{ and } B = \{T \in E(K) \mid 3T = Q\}.$$

The action of the group $\mathrm{Gal}(K/L)$ is observed on both sets A, which consists of 3 elements, and B, which comprises 9 elements. Furthermore, according to the orbit stabilizer theorem, the orbits have length q. This implies that A and B are decomposed into sets of q elements, which is impossible because q is a prime number > 11. □

Theorem 4.3. *Consider a Galois extension K of $\mathbb{Q}(\sqrt{-3})$ of prime degree q and E be an elliptic curve over $\mathbb{Q}(\sqrt{-3})$. Then the 3-Sylow group of $E(K)$ is isomorphic to a subgroup of $\mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/9\mathbb{Z}$.*

Proof. By Lemma 2.4 we have that $E(K)$ cannot have full 3^n-torsion for $n \geq 2$. Suppose that $E(K)$ has a point of order 27, and $\mathrm{Gal}(K/\mathbb{Q}(\sqrt{-3})) =< \sigma >$. Put $E[27] =< P, Q >$ then $P^\sigma = \alpha P + \beta Q \in E(K)$, so $(27 - \alpha)P + P^\sigma = \beta Q \in E(K)$.

- If $\beta = 0 \pmod{27}$, then $P^\sigma = \alpha P$ and the action of $\mathrm{Gal}(\overline{\mathbb{Q}(\sqrt{-3})}/\mathbb{Q}(\sqrt{-3}))$ on $\langle P \rangle$ factors through $\mathrm{Gal}(K/\mathbb{Q}(\sqrt{-3}))$, it follows that

  $$P^\mu = \alpha P, \mu \in Gal(\overline{\mathbb{Q}(\sqrt{-3})}/\mathbb{Q}(\sqrt{-3}))$$

  which means that $E/\mathbb{Q}(\sqrt{-3})$ has an 27-isogeny over $\mathbb{Q}(\sqrt{-3})$. But according to (See, [13]), that's impossible.

- If $\beta \neq 0 \pmod{27}$, then βQ is a point of order l with $l/27$ not contained in $\langle P \rangle$, from which it follows that $E(K)$ has full l-torsion. Since $L = \mathbb{Q}(\sqrt{-3})$ then $l = 3$ and then,

  $$E[27] = \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/9\mathbb{Z}.$$

□

5. Proof of the Theorem 3.4

Consider K/L a Galois extension of prime degree $q \geq 3$ and E be an elliptic curve over L. We now turn our attention to the behavior of the p-sylow subgroup when $p = q$, $p \neq q$ or q is coprime to $p - 1$.

Proof. First note that for a positive integer n, $E(K)$ cannot have full p^n-torsion for a prime number p by Lemmas 2.3 and 2.4. Thus, $E(K)[p^n]$ is either trivial or a subgroup of $\mathbb{Z}/p^n\mathbb{Z}$.
Let $C := \mathrm{Gal}(K/L) \simeq \mathbb{Z}/q\mathbb{Z}$.

1. Suppose that $p = q$. then, $E(K)[q]$ is $\mathbb{F}_q$-linear representation of C and we denote this linear representation by ρ. Suppose that $E(K)[q] \neq 0$ and let x be a nonzero element of $E(K)[q]$, and M be the subgroup of $E(K)[q]$ generated by the $\rho(s)x, s \in C$. We apply Lemma 3 in [16] to M, observing that M is finite and of order a power of q. Therefore $H^0(C, \mathrm{M}) \neq \{0\}$, which proves that

   $$H^0(C, E(K)[q]) = E(L)[q] \neq \{0\}.$$

2. Suppose that $p \neq q$. then, if $E(L)[p] \simeq \mathbb{Z}/p\mathbb{Z}$ and $\mathbb{Z}/p^2\mathbb{Z} \subset E(K)$. Then there is a no L-rational point $Q \in E(K)\left[p^2\right]$ such that, $pQ = P$ and $P \in E(L)[p]$. If we consider all these points together and denote them by X. The orbit of a point $Q \in X$ under the action of C is of length q. This means that X can be partitioned into sets of size q. Consequently, the order of X must be a multiple of q. Thus, since the order of C is coprime to p and by the Orbit stabilizer theorem we have that $E(K)\left[p^2\right] = 0$, and then $E(K)\left[p^\infty\right]$ is either trivial or isomorphic to $\mathbb{Z}/p\mathbb{Z}$.

3. First, suppose $E(L)[p] \simeq \mathbb{Z}/p\mathbb{Z}$. Then
$$E(K)[p] \simeq \mathbb{Z}/p\mathbb{Z}$$
and we have that $E(K)\left[p^2\right] = 0$. Consequently, $E(L)\left[p^\infty\right]$ and $E(K)\left[p^\infty\right]$ are equal and all isomorphic to $\mathbb{Z}/p\mathbb{Z}$.
Suppose $E(L)[p] = 0$ and $E(K)[p] \neq 0$. Let $P \in E(K)[p]$. Since $E(L)[p] = 0$ it follows that $P^\alpha \neq P$, and that C acts on $\langle P \rangle$. On the other hand, we have that
$$\mathbb{Z}/q\mathbb{Z} \simeq C \to \mathrm{Aut}(\langle P \rangle) \simeq \mathrm{Aut}\left(\mathbb{Z}/p\mathbb{Z}\right) \simeq \left(\mathbb{Z}/p\mathbb{Z}\right)^\times$$
is a homomorphism. So either C acts trivially on P, or q divides $p-1$, and this contradicts the statement.

□

6. Conclusion

This paper delves into the behavior of p-Sylow subgroups of elliptic curves over a Galois extension K of prime degree q, with a focus on base changes from the quadratic cyclotomic number field L. The investigation reveals distinct patterns in subgroup growth contingent upon the base field and properties of the elliptic curves. Specifically, the Theorems 3.1 and 3.2 outline the conditions over the 2-Sylow subgroup. More precisely, if $E(L)\left[2^\infty\right] \neq 0$ then $E(L)\left[2^\infty\right] = E(K)\left[2^\infty\right]$. On the other hand, if $E(L)[2] = 0$ it follows that $E(K)\left[2^\infty\right]$ is either trivial, $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ or $\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$, and $E(K)\left[2^\infty\right]$ is either trivial or $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$.
For the 3-Sylow we prove in the Theorem 3.3 that $E(K)\left[3^\infty\right]$ is isomorphic to a subgroup of $\mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/9\mathbb{Z}$, and $E(K)\left[3^\infty\right]$ is isomorphic to a subgroup of $\mathbb{Z}/9\mathbb{Z}$.
Moreover, in Theorem 3.4 we provide the conditions over p-Sylow subgroups for $p > 3$. More presisly we have that, if $E(L)[q] = 0$ then $E(K)[q] = 0$ and if $p \neq q$, then the p-Sylow group of $E(K)$ is either trivial or isomorphic to $\mathbb{Z}/p\mathbb{Z}$. Moreover, if q is coprime to $p-1$, then the p-Sylow groups of $E(L)$ and $E(K)$ are equal. These results provide a deeper understanding of the interplay between elliptic curves and their behavior over different field extensions.

Acknowledgments

The authors are thankful to the anonymous referees for their helpful comments.

Funding

This research received no external funding.

Data availability

Not applicable.

Conflicts of interest

The authors declare no conflict of interest.

References

[1] Z. Cheddour, A. Chillali and A. Mouhib, *Elliptic curves over imaginary biquadratic number fields of class number one*, Gulf Journal of Mathematics **19(1)** (2025), 75-92.
[2] Z. Cheddour, A. Chillali, and A. Mouhib, *Torsion section of elliptic curves over quadratic extensions of* $\mathbb{Q}$, Italian J. Pure Appl. Math. **50** (2023), 191–200.
[3] M. Derickx and A. V. Sutherland, *Torsion subgroups of elliptic curves over quintic and sextic number fields*, Proc. Amer. Math. Soc. **145** (2017), 4233–4245.
[4] M. Derickx, S. Kamienny, W. Stein, and M. Stoll, *Torsion points on elliptic curves over number fields of small degree*, Algebra Number Theory **17**(2) (2023).
[5] Ö. Ejder, *Torsion subgroups of elliptic curves over quadratic cyclotomic fields in elementary abelian 2-extensions*, J. Number Theory (2018).
[6] D. Jeon, C. H. Kim, and A. Schweizer, *On the torsion of elliptic curves over cubic number fields*, Acta Arith. **113**(3) (2004).
[7] D. Jeon, C. H. Kim, and E. Park, *On the torsion of elliptic curves over quartic number fields*, J. Lond. Math. Soc. (2006), 1–12.
[8] S. Kamienny, *Torsion points on elliptic curves and q-coefficients of modular forms*, Invent. Math. **109**(2) (1992), 221–229.
[9] M. A. Kenku and F. Momose, *Torsion points on elliptic curves defined over quadratic fields*, Nagoya Math. J. (1988), 125–149.
[10] B. Mazur, *Rational isogenies of prime degree*, with an appendix by D. Goldfeld, Invent. Math. (1978), 129–162.
[11] F. Najman, *Complete classification of torsion of elliptic curves over quadratic cyclotomic fields*, J. Number Theory (2010), 1964–1968.
[12] F. Najman, *Torsion of elliptic curves over quadratic cyclotomic fields*, Math. J. Okayama Univ. (2011), 75–82.
[13] B. Newman, *Growth of torsion of elliptic curves with odd-order torsion over quadratic cyclotomic fields*, arXiv:1604.01153v2 [math.NT] (2016).
[14] B. Newman, *Growth of torsion of elliptic curves with full 2-torsion over quadratic cyclotomic fields*, J. Number Theory (2017).
[15] F. P. Rabarison, *Structure de torsion des courbes elliptiques sur les corps quadratiques*, Acta Arith. (2010), 17–52.
[16] J. P. Serre, *Linear Representations of Finite Groups*, Graduate Texts in Mathematics, Springer-Verlag, New York, 42, 1977.