Isogenies of elliptic curves over small degree number fields

Vukorepa, Borna

University of Zagreb

FACULTY OF SCIENCE

DEPARTMENT OF MATHEMATICS

Borna Vukorepa

Isogenies of elliptic curves over small degree number fields

DOCTORAL DISSERTATION

Zagreb, 2022.

University of Zagreb

FACULTY OF SCIENCE

DEPARTMENT OF MATHEMATICS

Borna Vukorepa

Isogenies of elliptic curves over small degree number fields

DOCTORAL DISSERTATION

Supervisor:

prof. dr. sc. Filip Najman

Zagreb, 2022.

Sveučilište u Zagrebu

PRIRODOSLOVNO–MATEMATIČKI FAKULTET

MATEMATIČKI ODSJEK

Borna Vukorepa

Izogenije eliptičkih krivulja nad poljima algebarskih brojeva malog stupnja

DOKTORSKI RAD

Mentor:

prof. dr. sc. Filip Najman

Zagreb, 2022.

ACKNOWLEDGEMENTS

The thesis author thanks his advisor, Filip Najman, for a very productive cooperation, steady guidance and all of the crucial advice he provided throughout the period of the creation of this thesis.

The author thanks Timo Keller, Nikola Adžaga, Philippe Michaud-Jacobs and Shiva Chidambaram for their cooperation and a lot of useful information on our joint project. I am thankful to Ivan Krijan and Tomislav Gužvić for our collaboration on our joint paper.

The author also thanks Maarten Derickx for several discussions which turned out to be very helpful.

I also give my thanks to Nikola Adžaga, Andrej Dujella and Matija Kazalicki for reading this thesis as well as for checking for all potential mistakes in it.

The author is grateful for the support and funding from the QuantiXLie Center of Excellence, a project co-financed by the Croatian Government and European Union through the European Regional Development Fund - the Competitiveness and Cohesion Operational Programme (Grant KK.01.1.1.01.0004).

SUMMARY

The main objects of interest in this thesis are elliptic curves and the objects related to them. We will mostly investigate the isogenies of elliptic curves over number fields of small degree, but we will also give some interesting results about the torsion of rational elliptic curves when the torsion is considered over some specific cyclotomic fields.

Let $E/\mathbb{Q}$ be an elliptic curve and $p \leq 11$ a prime. We give a complete classification of the possibilities for $E(\mathbb{Q}(\zeta_p))$ as well as for $E(\mathbb{Q}(\zeta_{16}))$ and $E(\mathbb{Q}(\zeta_{27}))$. Using the previous result of Gužvić and Krijan [41], we are able to give a complete classification for $E(\mathbb{Q}(\mu_{p^\infty}))_{tors}$. Here, the set μ_{p^∞} is the set of all complex numbers ω for which there exists non-negative integer k such that $\omega^{p^k} = 1$.

Moving on to the isogenies, we can ask ourselves which cyclic isogeny degrees are possible for a non-CM elliptic curve $E/\mathbb{Q}$ if the isogeny is defined over a low degree number field. Since the presence of a (cyclic) isogeny is invariant under quadratic twisting, we actually determine which cyclic isogeny degrees are possible for a non-CM elliptic curve defined over a quadratic field K, but which has a rational j-invariant.

Similarly, given a quadratic field K and an elliptic curve E/K, we can ask ourselves which cyclic isogeny degrees are possible for E. We use the fact that the pairs $(E/K, C)$, where C is a cyclic subgroup of E defined over K, are parametrized by K-rational points on the modular curve $X_0(n)$. Hence, we should look for quadratic points on curves $X_0(n)$. We are able to determine all the quadratic points on all bielliptic curves $X_0(n)$ for which this has not been done before. This covers the cases $n = 60, 62, 69, 79, 83, 89, 92, 94, 95, 101, 119, 131$. Our proof relies a lot on the relative symmetric Chabauty's method developed by Siksek [82] and used by Box [13] on a related problem. We also make some improvements to the method, both from the computational and algebraic perspective.

The `Magma` [12] code which verifies our computations can be found on the links given

at the beginning of each corresponding chapter.

SAŽETAK

Glavni objekti kojim se bavimo u ovoj disertaciji su eliptičke krivulje i objekti povezani s njima. Većinom ćemo proučavati izogenije eliptičkih krivulja nad poljima algebarskih brojeva malog stupnja, ali ćemo također dati i neke zanimljive rezultate vezane za torziju racinalnih eliptičkih krivulja, pri čemu torziju promatramo nad nekim specifičnim ciklotomskim poljima.

Neka je $E/\mathbb{Q}$ eliptička krivulja i $p \leq 11$ prost broj. Potpuno ćemo klasificirati mogućnosti za $E(\mathbb{Q}(\zeta_p))$ kao i za $E(\mathbb{Q}(\zeta_{16}))$ i $E(\mathbb{Q}(\zeta_{27}))$. Kombinirajući to s prethodnim rezultatom Gužvića i Krijana [41], možemo potpuno klasificirati mogućnosti za $E(\mathbb{Q}(\mu_{p^\infty}))_{tors}$. Pritom, skup μ_{p^∞} je skup svih kompleksnih brojeva ω za koje postoji nenegativan cijeli broj k za koji je $\omega^{p^k} = 1$.

Prebacujući se na izogenije, možemo se pitati koji stupnjevi cikličkih izogenija su mogući za eliptičku krivulju bez kompleksnog množenja (non-CM) $E/\mathbb{Q}$ ako je ta izogenija definirana nad poljem algebarskih brojeva malog stupnja. Kako je prisustvo (cikličke) izogenije invarijantno na kvadratni tvist, zapravo ćemo odrediti koji stupnjevi cikličkih izogenija su mogući za non-CM eliptičku krivulju definiranu nad kvadratnim poljem K s racionalnom j-invarijantom.

Slično, za neko kvadratno polje K i eliptičku krivulju E/K, možemo se pitati koje stupnjeve cikličkih izogenija može imati E. Koristimo činjenicu da su parovi $(E/K, C)$, gdje je C ciklička podgrupa od E definirana nad K, parametrizirani K-racionalnim točkama na modularnoj krivulji $X_0(n)$. Dakle, trebamo tražiti kvadratne točke na krivulji $X_0(n)$. Uspješno ćemo odrediti sve kvadratne točke na svim bieliptičkim $X_0(n)$ za koje to nije napravljeno ranije. To obuhvaća slučajeve $n = 60, 62, 69, 79, 83, 89, 92, 94, 95, 101, 119, 131$. Naš dokaz se značajno oslanja na relativnu simetričnu Chabautyjevu metodu koju je razvio Siksek [82], a koristio Box [13] na povezanom problemu. Također ćemo napraviti

neka poboljšanja te metode, gledano iz računske i algebarske perspektive.

`Magma` [12] kodovi koji provjeravaju naše izračune se mogu naći na poveznicama na početku svakog pripadnog poglavlja.

CONTENTS

1 Introduction **1**

1.1 Elliptic curves . . . 1

1.2 Galois representations . . . 8

1.3 Modular curves and Jacobians . . . 12

1.3.1 The modular curves X_0, X_1, X_H . . . 12

1.3.2 Modular forms . . . 15

1.3.3 Jacobians . . . 17

1.3.4 Hyperelliptic curves . . . 19

2 Known results **21**

2.1 Overview . . . 21

2.2 Auxiliary results . . . 24

3 Torsion groups of elliptic curves over $\mathbb{Q}(\mu_{p^\infty})$ **31**

3.1 Auxiliary results . . . 33

3.2 Torsion growth over $\mathbb{Q}(\zeta_{16})$ . . . 37

3.3 Torsion growth over $\mathbb{Q}(\zeta_{27})$ . . . 41

3.4 Torsion growth over $\mathbb{Q}(\zeta_5), \mathbb{Q}(\zeta_7)$ and $\mathbb{Q}(\zeta_{11})$ . . . 45

3.4.1 Proof of Proposition 3.0.6 . . . 45

3.4.2 Proof of Proposition 3.0.5 . . . 46

4 Isogenies over quadratic fields of elliptic curves with rational j-invariant **49**

4.1 Auxiliary results . . . 50

4.1.1 Case $37 \mid n$: . . . 52

4.1.2 Case 17 | n : . . . 52
4.1.3 Case 13 | n : . . . 52
4.1.4 Case 11 | n : . . . 53
4.1.5 Case 7 | n : . . . 53
4.1.6 Case 5 | n : . . . 53
4.1.7 Case 3 | n : . . . 54
4.1.8 Case 2 | n : . . . 54
4.2 Two diff. prime divs. of the isog. deg. . . . 55
4.3 Non-squarefree isogeny degrees . . . 60
4.4 Isogenies of prime power degree . . . 63
4.4.1 Isogenies of degree 5^k . . . 63
4.4.2 Isogenies of degree 3^k . . . 67
4.4.3 Isogenies of degree 2^k . . . 69
4.5 Isog. of remaining composite deg. . . . 70
4.5.1 Isogenies of degree $2^a \cdot 3^b$ . . . 70
4.5.2 Isogenies of degree $2^a \cdot 5^b$ . . . 70
4.5.3 Isogenies of degree $3^a \cdot 5^b$ . . . 71
4.5.4 Isogenies of degree $14, 30, 63$ . . . 72
4.6 Isogenies of degree 91 . . . 74

5 Quadratic points on bielliptic curves **78**
5.1 $\mathbb{Q}$-curves . . . 80
5.2 Results for $n \in \{62, 69, 92, 94\}$. . . . 84
5.3 Obtaining models for $X_0(n)$ and their quotients . . . 86
5.4 Determining the Mordell-Weil groups of $J_0(n)(\mathbb{Q})$ . . . 87
5.4.1 Determining the ranks . . . 87
5.4.2 Determining the torsion . . . 87
5.5 The Relative symmetric Chabauty method . . . 90
5.6 Methods and comps. for $n \in \{60, 79, 83, 89, 95, 101, 119, 131\}$ . . . 93
5.6.1 Description of the updated method . . . 93
5.6.2 Selecting G and I . . . 96

5.6.3 Quadratic points on $X_0(n)$ for $n \in \{79, 83, 101\}$ 96
5.6.4 Quadratic points on $X_0(89)$ 97
5.6.5 Quadratic points on $X_0(131)$ 97
5.7 Example of the sieving process for $N = 89$ 99
5.8 Final results and tables 100
5.8.1 $X_0(60)$ 101
5.8.2 $X_0(79)$ 102
5.8.3 $X_0(83)$ 103
5.8.4 $X_0(89)$ 104
5.8.5 $X_0(95)$ 105
5.8.6 $X_0(101)$ 107
5.8.7 $X_0(119)$ 108
5.8.8 $X_0(131)$ 110

Conclusion **112**

Bibliography **113**

Curriculum Vitae **124**

1. INTRODUCTION

In this chapter we will familiarize the reader with the basics of the theory of elliptic curves as well as with some of the objects and results which will be used throughout this dissertation.

1.1. ELLIPTIC CURVES

Definition 1.1.1. Let F be a field and let E be a smooth projective curve defined over F of genus 1 which contains a specified F-rational point O. Then we say that E is an elliptic curve over F.

One can use the Riemann-Roch theorem to get the following result which tells us something about the model of an elliptic curve:

Proposition 1.1.2 ([84, III.3., Proposition 3.1.])**.** Let F be a field and let E/F be an elliptic curve over F. Then E has a model of the form:

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

Notice that we will always be working with elliptic curves over number fields, which have characteristic 0, so the following holds:

Proposition 1.1.3. Let F be a field whose characteristic is not 2 or 3 and let E/F be an elliptic curve over F. Then E has a model of the form:

$$E : y^2 = x^3 + ax + b.$$

This model is called the short Weierstrass model of E.

Proof. The proof follows simply by completing a square on the left hand side and completing a cube on the right hand side of the model from Proposition 1.1.2. ■

Notice that one elliptic curve can be described by more than one short Weierstrass model. One can look at [84, Proposition 3.1], which gives us the relation between Weierstrass models of isomorphic elliptic curves. We state the result only for short Weierstrass models:

Proposition 1.1.4 ([84, III.3., Proposition 3.1]). Let K be a number field and E/K an elliptic curve. Then any two short Weierstrass models of E are related by a change of variables of the form:

$$x = u^2x', \quad y = u^3y', \quad u \in K^*.$$

Very often we will consider elliptic curves up to isomorphism over a certain field. The above proposition tells us when are two elliptic curves defined over K actually isomorphic over K. We now define the j-invariant of an elliptic curve.

Definition 1.1.5. Let F be a field and E/F an elliptic curve with the model:

$$E : y^2 = x^3 + ax + b.$$

The j-invariant of E is denoted by $j(E)$ and we have $j(E) = 1728\frac{4a^3}{4a^3+27b^2}$.

The number in the denominator is the discriminant of E (up to scalar -16):

Definition 1.1.6. Let F be a field and E/F an elliptic curve with the model:

$$E : y^2 = x^3 + ax + b.$$

The discriminant of E is denoted by $\Delta(E)$ and we have $\Delta(E) = -16(4a^3 + 27b^2)$.

The discriminant of E can be used to check the smoothness of E since E is smooth if and only if $\Delta(E) \neq 0$ (see, for example, [84, III.1., Proposition 1.4.]).

From now on we will be considering elliptic curves over number fields. Notice that if K is a number field and $j_0 \in K$, we can easily find an elliptic curve E/K with $j(E) = j_0$. If $j_0 \notin \{0, 1728\}$, we can take:

$$E : y^2 + xy = x^3 - \frac{36}{j_0 - 1728}x - \frac{1}{j_0 - 1728}.$$

If $j_0 = 0$ we can take $E : y^2 + y = x^3$ and for $j_0 = 1728$ we can take $E : y^2 = x^3 + x$.

The following well-known result tells us how j-invariant can be used to check whether two elliptic curves are isomorphic over a certain field:

Proposition 1.1.7 ([84, III.1., Proposition 1.4.]). Let K be a number field and E_1/K and E_2/K elliptic curves. Then $j(E_1) = j(E_2)$ if and only if E_1 and E_2 are isomorphic over $\overline{K}$. Moreover, if $j(E_1) = j(E_2)$ and $j(E_1) \notin \{0, 1728\}$, then E_1 and E_2 are isomorphic over a quadratic extension of K.

Now we will give some introductory results regarding points on elliptic curves. Let K be a number field. The set of K-rational points, denoted by $E(K)$, on some elliptic curve E/K can be naturally equipped with a binary operation such that $E(K)$ becomes an abelian group. One of the most important results about the group structure of points on elliptic curves is the Mordell-Weil theorem:

Theorem 1.1.8 (Mordell-Weil, [67], [96]). Let K be a number field and let E/K be an elliptic curve. Then $E(K)$ is a finitely generated abelian group.

Since we know how finitely generated abelian groups look like, we can conclude from Theorem 1.1.8 that:

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

The non-negative integer r is called the rank of E/K and $E(K)_{tors}$ is called the torsion subgroup of $E(K)$, that is, the group of K-rational points of E of finite order. It is natural to ask ourselves what values can r and $E(K)_{tors}$ take as E varies or even as K varies. Even when $K = \mathbb{Q}$, it is not known whether r is bounded or not. In 2006, Elkies found an elliptic curve $E/\mathbb{Q}$ with 28 independent points in $E(\mathbb{Q})$, which is the current record (see [32]). On the other hand, when $K = \mathbb{Q}$, we have a complete classification of the possibilities for $E(\mathbb{Q})_{tors}$ due to Mazur:

Theorem 1.1.9 (Mazur, [61]). Let $E/\mathbb{Q}$ be an elliptic curve. Then $E(\mathbb{Q})_{tors}$ is isomorphic to one of the following groups:

$$\mathbb{Z}/m\mathbb{Z}, \quad m = 1, 2, \ldots, 10, 12,$$
$$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2m\mathbb{Z}, \quad m = 1, 2, 3, 4.$$

It is also worth mentioning that we have a complete classification of $E(K)_{tors}$ for elliptic curves E/K when K runs through all quadratic fields due to Kamienny, Kenku and Momose:

Theorem 1.1.10 (Kamienny, Kenku, Momose [48], [52])**.** Let K be a quadratic field and E/K an elliptic curve. Then $E(K)_{tors}$ is isomorphic to one of the following groups:

$$\mathbb{Z}/m\mathbb{Z}, \quad m = 1,2,3,\ldots,16,18,$$
$$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2m\mathbb{Z}, \quad m = 1,2,\ldots,6,$$
$$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/3m\mathbb{Z}, \quad m = 1,2,$$
$$\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}.$$

Division polynomials are closely related to points of finite order on elliptic curves.

Definition 1.1.11. Let $E/\mathbb{Q}$ be an elliptic curve. Assume that E is given by a short Weierstrass model:

$$E: \quad y^2 = x^3 + ax + b.$$

Define the division polynomials $\psi_{E,m} \in \mathbb{Q}[x,y]$ by:

$$\begin{aligned}
&\psi_{E,0} = 0,\\
&\psi_{E,1} = 1,\\
&\psi_{E,2} = 2y,\\
&\psi_{E,3} = 3x^4 + 6ax^2 + 12bx - a^2,\\
&\psi_{E,4} = 4y(x^6 + 5ax^4 + 20bx^3 - 5a^2x^2 - 4abx - 8b^2 - a^3),\\
&\psi_{E,2m+1} = \psi_{E,m+2}\psi_{E,m}^3 - \psi_{E,m-1}\psi_{E,m+1}^3, \quad m \geq 2\\
&\psi_{E,2m} = (2y)^{-1} \cdot \psi_{E,m} \cdot (\psi_{E,m+2}\psi_{E,m-1}^2 - \psi_{E,m-2}\psi_{E,m+1}^2), \quad m \geq 3.
\end{aligned}$$

We now define the polynomials:

$$\phi_{E,m} = x\psi_{E,m}^2 - \psi_{E,m+1}\psi_{E,m-1},$$

$$\omega_{E,m} = (4y)^{-1}(\psi_{E,m+2}\psi_{E,m-1}^2 - \psi_{E,m-2}\psi_{E,m+1}^2).$$

By replacing y^2 with $x^3 + ax + b$, one can show that $\psi_{E,m} \in \mathbb{Q}[x]$ for odd m and $y^{-1}\psi_{E,m} \in \mathbb{Q}[x]$ for even m, see [95, Lemma 3.3.]. Similarly, we also have $\phi_{E,m} \in \mathbb{Q}[x]$,

see [95, Lemma 3.4.]. The following theorem connects points on E with division polynomials:

Theorem 1.1.12 ([95, Theorem 3.6.]). Let $P = (x, y)$ be a point on the elliptic curve

$$E: \quad y^2 = x^3 + ax + b$$

and let n be a positive integer. Then:

$$nP = \left(\frac{\phi_{E,n}(P)}{\psi^2_{E,n}(P)}, \frac{\omega_{E,n}(P)}{\psi^3_{E,n}(P)} \right).$$

If $n = p$ for prime $p \geq 3$, then $\psi_{E,p} \in \mathbb{Q}[x]$ and the roots of $\psi_{E,p}(x)$ are precisely the x-coordinates of points in $E[p]$. This gives us an easy way to check whether some $E/\mathbb{Q}$ has a point of order p defined over certain number field.

We will also be interested in the isogenies of the elliptic curves:

Definition 1.1.13. Let K be a number field and let E_1/K and E_2/K be elliptic curves. An isogeny from E_1 to E_2 is a nonconstant surjective morphism $\phi : E_1 \mapsto E_2$ satisfying $\phi(O_1) = O_2$, where O_1, O_2 are the neutral elements of E_1, E_2 respectively.

Definition 1.1.14. Let K be a number field and let E_1/K and E_2/K be elliptic curves. We say that E_1 and E_2 are isogenous if there is an isogeny from E_1 to E_2.

It can be shown that being isogenous is an equivalence relation. Also, isogenies are actually homomorphisms:

Theorem 1.1.15 ([84, Theorem 4.8.]). Let $\phi : E_1 \mapsto E_2$ be an isogeny of elliptic curves. Then $\phi(P+Q) = \phi(P) + \phi(Q)$ for all $P, Q \in E_1$.

To each isogeny $\phi : E_1 \mapsto E_2$ of elliptic curves we can associate its kernel $\ker(\phi) = \phi^{-1}(O_1)$. We can also assign a number $\deg(\phi)$ to an isogeny which we call the degree of ϕ and $\deg(\phi) = \#\ker(\phi)$ holds. We call an isogeny ϕ cyclic if $\ker(\phi)$ is cyclic.

Definition 1.1.16. Let $\phi : E_1 \mapsto E_2$ be an isogeny of elliptic curves which is cyclic and of degree n. Then we say that ϕ is a cyclic n-isogeny.

We now state an important result which gives the correspondence between the isogenies and the subgroups of points of an elliptic curve:

Proposition 1.1.17 ([84, Proposition 4.12.]). Let K be a number field and E/K an elliptic curve. Let G be a finite subgroup of E. There exist a unique elliptic curve E' and an isogeny $\phi : E \mapsto E'$ such that $\ker(\phi) = G$.

It is also worth mentioning that ϕ and E' from the above proposition will be defined over K if and only if the group $\mathrm{Gal}(\overline{K}/K)$ acts on G.

Definition 1.1.18. Let K be a number field and E/K an elliptic curve. If $\mathrm{End}(E)$ is strictly larger than $\mathbb{Z}$, we say that E has complex multiplication (CM) and that E is an elliptic curve with complex multiplication (CM curve).

Notice that we have $\mathbb{Z} \subseteq \mathrm{End}(E)$ since the map $[m] : E \mapsto E$ which multiplies a point on E by m is an endomorphism for all $m \in \mathbb{Z}$. Similar as with torsion, we have a result by Mazur which tells us which cyclic isogeny degrees are possible for elliptic curves over $\mathbb{Q}$:

Theorem 1.1.19 (Mazur, Kenku, [60], [51]). Let $E/\mathbb{Q}$ be an elliptic curve with a cyclic n-isogeny defined over $\mathbb{Q}$. Then $n \leq 19$ or $n \in \{21, 25, 27, 37, 43, 67, 163\}$. If E does not have complex multiplication, then $n \leq 18$ with $n \neq 14$ or $n \in \{21, 25, 37\}$.

Now we define quadratic twists of an elliptic curve:

Definition 1.1.20. Let K be a number field, $d \in K$ which is not a square and E/K an elliptic curve given by a short Weierstrass model:

$$E : \quad y^2 = x^3 + ax + b.$$

The elliptic curve E^d given by a model:

$$E^d : \quad dy^2 = x^3 + ax + b$$

is called the quadratic twist of E by d.

For an elliptic curve $E/\mathbb{Q}$ with $j(E) \notin \{0, 1728\}$, any elliptic curve $E_1/\mathbb{Q}$ satisfying $j(E_1) = j(E)$ is a quadratic twist of E (see [84, Section X.5.]). Now we can easily see from the formulas that define division polynomials that the division polynomials of E and E_1 are identical up to scalar. More formally, for every positive integer n, we have $\psi_{E,n} = \alpha \psi_{E_1,n}$ for some $\alpha \in \mathbb{Q}$. This means that just by knowing the j-invariant of an elliptic curve, we can say a lot about its torsion points.

Presence of a cyclic isogeny is invariant under quadratic twisting, unlike the presence of torsion:

Proposition 1.1.21. [83, Corollary 5.2.] Let K be a number field, $n \geq 1$ an integer and E/K an elliptic curve. If E has a K-rational cyclic n-isogeny, then so does any quadratic twist of E.

In some parts of this thesis, we will be mentioning $\mathbb{Q}$-curves. For more details about the theory of $\mathbb{Q}$-curves, see [24, 31].

Definition 1.1.22. Let K be a number field and E/K an elliptic curve. We say that E is a $\mathbb{Q}$-curve if E is isogenous to E^{σ} for all $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$.

1.2. GALOIS REPRESENTATIONS

We will now define Galois representations of elliptic curves and introduce some related objects, as well as state some important results about them. We will work with elliptic curves over $\mathbb{Q}$ here.

Definition 1.2.1. Let $E/\mathbb{Q}$ be an elliptic curve. For an integer $n \geq 1$, we define the set $E[n]$ as

$$E[n] = \ker[n] = \{P \in E(\overline{\mathbb{Q}}) : nP = O\}.$$

Proposition 1.2.2 ([84, Corollary 6.4.])**.** Let $E/\mathbb{Q}$ be an elliptic curve and $n \geq 1$ an integer. Then $E[n] \cong \mathbb{Z}/n\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z}$.

Because of the previous proposition, we can choose a basis $\{P,Q\}$ for $E[n]$ and then consider the action of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on P and Q. It is not hard to show that $E[n]$ is a $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-module, which means that $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ acts on $E[n]$. Therefore, given $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, we can find $a,b,c,d \in \mathbb{Z}/n\mathbb{Z}$ such that:

$$P^\sigma = aP + bQ,$$
$$Q^\sigma = cP + dQ.$$

Hence, we can assign a matrix $\begin{bmatrix} a & c \\ b & d \end{bmatrix}$ to each $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. Notice that such matrices actually correspond to automorphisms of $E[n]$. Now we are ready to define the mod n Galois representation of E.

Definition 1.2.3. Let $E/\mathbb{Q}$ be an elliptic curve. Let $n \geq 2$ be an integer and $\{P,Q\}$ a basis for $E[n]$. Consider the map:

$$\rho_{E,n} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \mapsto \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z}),$$

which satisfies $\rho_{E,n}(\sigma) = \begin{bmatrix} a & c \\ b & d \end{bmatrix}$, where $P^\sigma = aP + bQ$ and $Q^\sigma = cP + dQ$. We call $\rho_{E,n}$ the mod n Galois representation of E.

It is easy to check that $\rho_{E,n}$ is a homomorphism, see, for example [85, Section 6.3.].

Definition 1.2.4. Let $E/\mathbb{Q}$ be an elliptic curve and let $n \geq 2$ be an integer. Denote by $\mathbb{Q}(E[n])$ the smallest field containing all the coordinates of all points in $E[n]$. We call $\mathbb{Q}(E[n])$ the n-th division field of E.

Notice that $\ker(\rho_{E,n}) = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}(E[n]))$. Hence, it is enough to consider the action of $\mathrm{Gal}(\mathbb{Q}(E[n])/\mathbb{Q})$ on $E[n]$. It is not hard to see that $\rho_{E,n}$ is injective on $\mathrm{Gal}(\mathbb{Q}(E[n])/\mathbb{Q})$, which means that $Im(\rho_{E,n}) \cong \mathrm{Gal}(\mathbb{Q}(E[n])/\mathbb{Q})$. This is also directly obtained through the first isomorphism theorem. See [85, Theorem 6.7.] for a formal proof of this fact.

One of the main questions about Galois representations is classifying all the possible images of $\rho_{E,n}$ as $E/\mathbb{Q}$ varies. Notice that the image depends on the choice of basis for $E[n]$, so the image is always considered up to conjugation. To begin with, let's define several important specific subgroups of $\mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$.

Definition 1.2.5. Let p be a prime and $\delta \in \mathbb{Z}/p\mathbb{Z}$ a quadratic non-residue. Consider these subgroups of $\mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$:

$$B(p) = \left\{ \begin{bmatrix} a & b \\ 0 & c \end{bmatrix} : a,b,c \in \mathbb{Z}/p\mathbb{Z}, ac \neq 0 \right\},$$

$$C_s(p) = \left\{ \begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix} : a,b \in \mathbb{Z}/p\mathbb{Z}, ab \neq 0 \right\},$$

$$C_{ns}(p) = \left\{ \begin{bmatrix} a & \delta b \\ b & a \end{bmatrix} : a,b \in \mathbb{Z}/p\mathbb{Z}, (a,b) \neq (0,0) \right\},$$

$$N_s(p) = \left\{ \begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix}, \begin{bmatrix} 0 & a \\ b & 0 \end{bmatrix} : a,b \in \mathbb{Z}/p\mathbb{Z}, ab \neq 0 \right\},$$

$$N_{ns}(p) = \left\{ \begin{bmatrix} a & \delta b \\ b & a \end{bmatrix}, \begin{bmatrix} a & \delta b \\ -b & -a \end{bmatrix} : a,b \in \mathbb{Z}/p\mathbb{Z}, (a,b) \neq (0,0) \right\}.$$

The group $B(p)$ is called a Borel subgroup. The group $C_s(p)$ is called a split Cartan subgroup. The group $C_{ns}(p)$ is called a non-split Cartan subgroup. The group $N_s(p)$ is the normalizer of $C_s(p)$. The group $N_{ns}(p)$ is the normalizer of $C_{ns}(p)$.

Clearly, both split and non-split Cartan subgroups have index 2 in their normalizer. We now state Dickson's classification of subgroups of $\mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$:

Theorem 1.2.6 (Dickson, [30])**.** Let G be a subgroup of $\mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$ not containing $\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$. Then G is conjugate to a subgroup of one of $B(p)$, $N_s(p)$, $N_{ns}(p)$ or the image of G in $\mathrm{PGL}_2(\mathbb{Z}/p\mathbb{Z})$ is isomorphic to A_4, S_4 or A_5.

This is important because it can be shown that if $Im(\rho_{E,p})$ contains $\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$, then $\rho_{E,p}$ is surjective. Hence, if $\rho_{E,p}$ is not surjective, it is conjugate to a subgroup of one of the groups in Theorem 1.2.6. Serre [80] proved that, given a fixed non-CM $E/\mathbb{Q}$, $\rho_{E,p}$ is not surjective for only finitely many primes p. Serre [81, p. 399] also asked a question whether a stronger variant of that theorem holds uniformly for all non-CM $E/\mathbb{Q}$. The following was formally conjectured by Zywina [98] and Sutherland [90]:

Conjecture 1.2.7 (Serre's uniformity conjecture)**.** Let $E/\mathbb{Q}$ be a non-CM elliptic curve and $p > 37$ a prime. Then $\rho_{E,p}$ is surjective.

To prove the above conjecture, the only remaining thing to prove is that for $p > 37$ the image of $\rho_{E,p}$ can never be conjugate to a subgroup of $N_{ns}(p)$. All other cases have been handled. For small primes p, a lot is known about the possibilites for the image of $\rho_{E,p}$, see, for example [4], [5], [98].

Notice that the Galois representation is connected to the presence of an isogeny or a torsion point defined over certain field. For example, assume that $E/\mathbb{Q}$ has a rational point P of order $n \geq 2$. Then we can choose a basis for $E[n]$ which contains P. Since P is fixed by all elements in $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, we have:

$$\rho_{E,n}(\sigma) = \begin{bmatrix} 1 & * \\ 0 & * \end{bmatrix}, \forall \sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}).$$

Clearly, this works both ways since if $\rho_{E,n}(\sigma)$ is of the above form for all $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ for some basis $\{P,Q\}$ of $E[n]$, then P is fixed by all $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. Therefore, P is rational.

Similar conclusions can be reached if E has cyclic n-isogeny ϕ defined over $\mathbb{Q}$. Notice that $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ acts on $\ker(\phi)$. Let P be the generator of $\ker(\phi)$. Then we can choose a basis for $E[n]$ which contains P. We have that $P^\sigma = aP$ for all $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. Therefore, we have:

$$\rho_{E,n}(\sigma) = \begin{bmatrix} * & * \\ 0 & * \end{bmatrix}, \forall \sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}).$$

Again, this works both ways since if $\rho_{E,n}(\sigma)$ is of the above form for all $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ for some basis $\{P,Q\}$ of $E[n]$, then $\langle P \rangle$ is fixed by all $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. Therefore, it is a kernel of a cyclic rational n-isogeny by Theorem 1.1.17.

Notice that given a prime p, we can consider the representations ρ_{E,p^k} for any integer $k \geq 1$. We can select bases for all $E[p^k]$ which are compatible with respect to the multiplication by p map. They form a basis for the Tate module of E, an object which we now define:

Definition 1.2.8. Let $E/\mathbb{Q}$ be an elliptic curve and p a prime. Consider the inverse limit $T_p(E) = \varprojlim_n E[p^n]$ with respect to the map $[p]$ (multiplication by p). The module $T_p(E)$ is called the Tate module of E.

Notice that $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ acts naturally on $T_p(E)$. Similarly to mod n Galois representation of E, we can define the p-adic Galois representation of E:

Definition 1.2.9. Let $E/\mathbb{Q}$ be an elliptic curve and p a prime. Consider the representation:

$$\rho_{E,p^\infty} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \mapsto \mathrm{GL}_2(\mathbb{Z}_p),$$

induced by the action of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on $T_p(E)$. The homomorphism ρ_{E,p^∞} is called the p-adic Galois representation of E.

Naturally, as with mod p Galois representations, we can ask ourselves about the possible images of ρ_{E,p^∞}. For $p = 2$ the question was answered by Rouse and Zureick-Brown [79] and some additional progress was made by Rouse, Sutherland and Zureick-Brown [78]. Serre proved the following:

Theorem 1.2.10 (Serre's open image theorem, [80])**.** Let $E/\mathbb{Q}$ be a non-CM elliptic curve. Then ρ_{E,p^∞} is surjective for all but finitely many primes p. Additionally, ρ_{E,p^∞} is of finite index in $\mathrm{GL}_2(\mathbb{Z}_p)$ (it is open in the p-adic topology).

1.3. MODULAR CURVES AND JACOBIANS

In this section we will give a brief overview of modular curves related to our research. We will introduce some basic definitions and state the most important results which link the points on some specific modular curves to elliptic curves with a desired property. We will also mention Jacobians, a very important part of many of our methods.

1.3.1. The modular curves X_0, X_1, X_H

The goal of this part is to define the well-known modular curves $X_0(n)$, $X_1(n)$ and X_H. We begin by defining some important subgroups of $\mathrm{SL}_2(\mathbb{Z})$.

Definition 1.3.1. Let n be a positive integer. Consider the following subgroup of $\mathrm{SL}_2(\mathbb{Z})$:

$$\Gamma(n) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{SL}_2(\mathbb{Z}) : \begin{bmatrix} a & b \\ c & d \end{bmatrix} \equiv \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \pmod{n} \right\}.$$

Group $\Gamma(n)$ is called the main congruence subgroup of level n.

Definition 1.3.2. Let Γ be a subgroup of $\mathrm{SL}_2(\mathbb{Z})$. We say that Γ is a congruence subgroup if $\Gamma(n) \leq \Gamma$ for some positive integer n.

Here are two important examples of congruence subgroups:

$$\Gamma_0(n) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{SL}_2(\mathbb{Z}) : \begin{bmatrix} a & b \\ c & d \end{bmatrix} \equiv \begin{bmatrix} * & * \\ 0 & * \end{bmatrix} \pmod{n} \right\},$$

$$\Gamma_1(n) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{SL}_2(\mathbb{Z}) : \begin{bmatrix} a & b \\ c & d \end{bmatrix} \equiv \begin{bmatrix} 1 & * \\ 0 & 1 \end{bmatrix} \pmod{n} \right\}.$$

Definition 1.3.3. Let $\mathbb{H} = \{\tau \in \mathbb{C} : \mathrm{im}(\tau) > 0\}$. Let $\mathbb{H}^* = \mathbb{H} \cup \mathbb{Q} \cup \{\infty\}$. We call $\mathbb{H}$ the upper half-plane and $\mathbb{H}^*$ the extended upper half-plane.

It is easy to check that $\mathrm{SL}_2(\mathbb{Z})$ and, consequently, all its subgroups act on $\mathbb{H}$ and $\mathbb{H}^*$ via the following action:

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} (\tau) = \frac{a\tau + b}{c\tau + d}.$$

We can now give the definition of a modular curve.

Definition 1.3.4. Let Γ be a congruence subgroup of $\mathrm{SL}_2(\mathbb{Z})$. The modular curve corresponding to Γ, denoted by $Y(\Gamma)$, is the quotient space $Y(\Gamma) = \Gamma\backslash\mathbb{H} = \{\Gamma\tau : \tau \in \mathbb{H}\}$.

Also set $X(\Gamma) = \Gamma\backslash\mathbb{H}^* = \{\Gamma\tau : \tau \in \mathbb{H}^*\}$.

Definition 1.3.5. Let Γ be a congruence subgroup of $\mathrm{SL}_2(\mathbb{Z})$. The elements of the set $X(\Gamma) \setminus Y(\Gamma)$ are called cusps or cuspidal points.

Theorem 1.3.6 ([83, p. 13-14])**.** The modular curve $X(\mathrm{SL}_2(\mathbb{Z}))$ is isomorphic to $\mathbb{P}^1$ and is denoted by $X(1)$ and its non-cuspidal points correspond to isomorphism classes of elliptic curves $E/\mathbb{C}$.

Now we will consider what happens with $\Gamma_0(n)$ and $\Gamma_1(n)$. Set:

$$Y_0(n) = Y(\Gamma_0(n)), \quad Y_1(n) = Y(\Gamma_1(n)),$$
$$X_0(n) = X(\Gamma_0(n)), \quad X_1(n) = X(\Gamma_1(n)).$$

Theorem 1.3.7 ([83, p. 14-15])**.** All $X_0(n), X_1(n), Y_0(n), Y_1(n)$ are algebraic curves with models over $\mathbb{Q}$.

- For a number field K, pairs $(E/K, C)$, where E is an ellipic curve and C is a cyclic subgroup of E order n defined over K, are parametrized by non-cuspidal points on $X_0(n)(K)$, up to isomorphism over $\overline{K}$.
- For a number field K, pairs $(E/K, P)$, where E is an ellipic curve and $P \in E(K)$ is of order n, are parametrized by non-cuspidal points on $X_1(n)(K)$. This is up to isomorphism over K.

Notice that, by Proposition 1.1.17, C is a kernel of an isogeny defined over K, so by determining all the points on $X_0(n)(K)$ we can determine whether there exists an elliptic curve E/K with a K-rational cyclic n-isogeny. Similarly, by determining all the points on $X_1(n)(K)$ we can say something about the possibilities for $E(K)_{tors}$. Also, for positive integers m and n, one may consider the modular curves $X_1(m,mn)$ whose non-cuspidal K-rational points parametrize triples (E,P,Q) where E/K is an elliptic curve and P and Q are independent points of order m and mn on $E(K)$ respectively, see [28, p. 2]. This is important since there exist many different methods for determining points on modular

curves, many of which we will use in this thesis. This enables us to translate the problem of determining the possible torsion structures or cyclic isogeny degrees of elliptic curves into the problem of determining K-rational points on specific modular curves. Notice that we are only interested in non-cuspidal points so we will need some information about cusps:

Theorem 1.3.8 ([29, Section 3.8.])**.** Let n be a positive integer. The number of cusps of $X_0(n)$ is equal to the sum:

$$\sum_{d|n} \varphi(\gcd(d, \frac{n}{d})).$$

Theorem 1.3.9 ([74, Section 5.2.])**.** Let n be a positive integer. Assume d is the largest number such that $d^2 \mid n$. Then all cusps of $X_0(n)$ are defined over $\mathbb{Q}(\zeta_d)$.

For all of the curves $X_1(n)$ and $X_1(m,mn)$ that we will consider, it will be easy to determine whether certain points are cusps since there are simple equations which are satisifed by cuspidal points and no other points, see [77]. Models for many $X_1(n)$ and $X_1(m,mn)$ can also be found there and in [89]. For larger values of n, see [27,91].

This construction can be generalized for many more congruence subgroups. One can find a more detailed discussion in [83] and especially [29, Chapter 2]. Let n be a positive integer and let H be a subgroup of $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$. We can associate a congruence subgroup to H. Let:

$$H_0 = H \cap \mathrm{SL}_2(\mathbb{Z}/n\mathbb{Z}), \quad \Gamma_H = \{M \in \mathrm{SL}_2(\mathbb{Z}) : (M \mod n) \in H_0\}.$$

One can easily see that Γ_H is a congruence subgroup. We can define X_H and Y_H as:

$$Y_H = \Gamma_H \backslash \mathbb{H}, \quad X_H = \Gamma_H \backslash \mathbb{H}^*.$$

Theorem 1.3.10 ([83, Theorem 21., Theorem 22.])**.** Both X_H, and Y_H are algebraic curves with models over $\mathbb{Q}$ when the set of determinants of H is $(\mathbb{Z}/n\mathbb{Z})^\times$.

- For a number field K, elliptic curves E/K such that $\rho_{E,n}(\mathrm{Gal}(\overline{K}/K)) \subseteq H$ (up to conjugation) are parametrized by non-cuspidal points on $X_H(K)$, away from the j-invariants 0 and 1728.
- If $-I \notin H$, then the parametrization is up to K-isomorphism, otherwise it is up to $\overline{K}$-isomorphism.

Notice that if we have a congruence subgroup $\Gamma_H \leq \mathrm{SL}_2(\mathbb{Z})$, then we have a natural surjective morphism:

$$\Gamma_H \backslash \mathbb{H}^* \to \mathrm{SL}_2(\mathbb{Z}) \backslash \mathbb{H}^*, \quad \Gamma_H \cdot \tau \to \mathrm{SL}_2(\mathbb{Z}) \cdot \tau.$$

This induces a non-constant morphism of curves $j : X_H \mapsto X(1)$ defined over $\mathbb{Q}$ when the set of determinants of H is $(\mathbb{Z}/n\mathbb{Z})^*$, called the j-map (see [83, p. 17]). Poles of the j-map are the cusps of X_H:

Theorem 1.3.11 ([83, p. 17])**.** Let $H \leq \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$. The set of cusps of X_H is the set $j^{-1}(\infty)$.

1.3.2. Modular forms

Now we will give a very basic overview of modular forms.

Definition 1.3.12. A modular form of weight k and level n for the group $\Gamma_0(n)$ is a function $f : \mathbb{H}^* \to \mathbb{C}$ satisfying these conditions:

- f is holomorphic on $\mathbb{H}$.
- For any $z \in \mathbb{H}$ and any $\begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \Gamma_0(n)$ we have:

$$f\left(\frac{az+b}{cz+d}\right) = (cz+d)^k f(z).$$

- f is holomorphic at the cusps.

Definition 1.3.13. A cuspform of weight k and level n for the group $\Gamma_0(n)$ is a modular form of weight k and level n for the group $\Gamma_0(n)$ which vanishes at the cusps.

Cuspforms of weight k and level n for the group $\Gamma_0(n)$ form a $\mathbb{C}$-vector space which we denote by $S_k(n)$. For our purposes, the most important of them will be $S_2(n)$ since it is crucial in determining the model for $X_0(n)$. Most methods for determining those models are a variation of Galbraith's method [34, Chapter 3]. The curve $X_0(n)$ admits some specific automorphisms which are involutions. We now define Atkin-Lehner invlolutions.

Definition 1.3.14. Let n be a positive integer and d a positive divisor of n satisfying $\gcd(d, \frac{n}{d}) = 1$. Then there exist $x, y, z, t \in \mathbb{Z}$ for which the matrix $W_d = \begin{bmatrix} dx & y \\ nz & dt \end{bmatrix}$ has determinant d. The matrix W_d normalizes the group $\Gamma_0(n)$ and induces a linear operator w_d on the space of cuspforms $S_k(n)$ which is an involution and is called the Atkin-Lehner involution of $S_k(n)$. In turn, it also induces an automorphism on $X_0(n)$ which is an involution also denoted by w_d and called the Atkin-Lehner involution.

Definition 1.3.15. Let n be a positive integer. The degree 2 quotient curve $X_0(n)/\langle w_n \rangle$ is denoted by $X_0^+(n)$.

The modular interpretation of w_d will be useful to us. If a point $P \in X_0(n)(K)$ represents an elliptic curve E/K with a K-rational cyclic n-isogeny, then $w_d(P)$ represents an elliptic curve E'/K with a K-rational cyclic n-isogeny which is also d-isogenous to E via a cyclic d-isogeny. Therefore, the non-cuspidal points on $X_0^+(n)$ represent the unordered pairs $\{E, E'\}$ of elliptic curves which are n-isogenous (see [34, Section 7.2.]).

Definition 1.3.16. Let n be a positive integer. Let $\rho_n : X_0(n) \mapsto X_0^+(n)$ be the degree 2 quotient map. We say that a point $P \in X_0(n)$ is a pullback of a rational point on $X_0^+(n)$ if we have $\rho_n(P) \in X_0^+(n)(\mathbb{Q})$.

We now define Hecke operators.

Definition 1.3.17. Let M_m be the set of 2×2 integral matrices with determinant $m \geq 1$. Given a modular form f of weight k, the m-th Hecke operator acts by the formula:

$$T_m f(z) = m^{k-1} \cdot \sum_{\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in M_m / \mathrm{SL}_2(\mathbb{Z})} (cz+d)^{-k} f\Big(\frac{az+b}{cz+d}\Big).$$

One can see from the formula that T_m sends cuspforms to cuspforms (if the constant coefficient of f is 0, then so is of $T_m f$).

Definition 1.3.18. A cuspform f is called a Hecke eigenform if it is an eigenvector for all Hecke operators T_m. We denote by K_f the number field we get by adjoining the eigenvalues λ_m to $\mathbb{Q}$.

To each cuspform we can assign an L-function:

Definition 1.3.19. The L-function of a cusp form $f(z) = \sum_{n=1}^{\infty} a_n q^n$ of weight k is the complex function defined by the Dirichlet series:

$$L(f,s) = \sum_{n=1}^{\infty} a_n n^{-s}.$$

We can associate an abelian variety $\mathcal{A}_f/\mathbb{Q}$ to each eigenform f. Then we have the equality of L-functions:

$$L(\mathcal{A}_f,s) = \prod_{i=1}^{d} L(f_i,s),$$

where f_i are conjugates of f (see [83, p. 27]).

The space of differentials on a curve will be needed for some important computations later in the thesis so we give its definition here.

Definition 1.3.20. Let K be a number field and X/K a curve over K. The space of differentials on X, denoted by Ω_X, is the $\overline{K}$-vector space generated by the symbols of the form dx for $x \in \overline{K}(X)$ satisfying these relations:

- $d(x+y) = dx + dy$ for all $x, y \in \overline{K}(X)$.
- $d(xy) = ydx + xdy$ for all $x, y \in \overline{K}(X)$.
- $da = 0$ for all $a \in \overline{K}$.

1.3.3. Jacobians

Even though we will not explicitly define the Jacobian, we will define the basic elements and concepts needed for the work with Jacobians. We start by defining a divisor.

Definition 1.3.21. Let K be a number field and X/K a curve over K. A divisor D on X is a formal linear combination:

$$D = \sum_{i=1}^{n} a_i P_i, \quad a_i \in \mathbb{Z}, \quad P_i \in X(\overline{K}).$$

The degree of the divisor D is the integer $\sum_{i=1}^{n} a_i$. We say that D is K-rational if it is invariant under the action of $Gal(\overline{K}/K)$. We say that D is effective if we have $a_i \geq 0$ for all i and we write $D \geq 0$. Clearly, the K-rational divisors on X form an abelian group called the divisor group and denoted by $Div(X/K)$. The degree 0 subgroup of that group is the subgroup:

$$Div^0(X/K) = \{D \in Div(X/K) : deg(D) = 0\}.$$

Definition 1.3.22. Let K be a number field and X/K a curve over K. Let $K(X)$ be the function field of X and let $f \in K(X)^*$. For $P \in X(\overline{K})$ denote by $v_P(f)$ the order of vanishing of f at P. Set

$$div(f) = \sum_{P \in X(\overline{K})} v_P(f)P.$$

A divisor of the form $div(f)$ is called a principal divisor.

Definition 1.3.23. Let K be a number field and X/K a curve over K and D a divisor on X. We define the Riemann-Roch space of D as:

$$L(D) = \{f \in K(C)^* : div(f) + D \geq 0\} \cup \{0\}.$$

It is easy to show that $L(D)$ is a K-vector space and we denote its dimension by $l(D)$.

The group of principal divisors $Princ(X/K) = \{div(f) : f \in K(X)^*\}$ is a subgroup of $Div^0(X/K)$ (see [83, Lemma 2.1. p. 24]). We define the Picard group of X/K as

$$Pic^0(X/K) = \frac{Div^0(X/K)}{Princ(X/K)}.$$

If we have $D \in Div^0(X/K)$, we write $[D]$ for the corresponding class. Assume X/K is a curve of genus g. Then there is a g-dimensional abelian variety $J(X)$ such that we have an embedding of $X(K)$ into $J(X)(K)$. The Mordell-Weil theorem also holds for $J(X)(K)$ and it is a finitely generated abelian group (see [83, Theorem 34.]). By studying the points on $J(X)(K)$ we can usually say a lot about the points on $X(K)$. We also have the following result:

Theorem 1.3.24 ([76, Section 3.])**.** Let K be a number field and X/K a curve over K with $X(K) \neq \emptyset$. Then $J(X)(K) \cong Pic^0(X/K)$.

Proposition 1.3.25. Let K be a number field and X/K a curve of genus $g \geq 1$. Let D_1 be a K-rational divisor on X of degree 1. Then the map:

$$i : X(K) \mapsto J(X)(K), \quad i(P) = [P - D_1]$$

is injective.

Proof. Assume that we have $i(P) = i(Q)$, that is, $[P - D_1] = [Q - D_1]$. Hence, $P - D_1 + div(f) = Q - D_2$ so $div(f) = Q - P$. But then f is a degree 1 morphism, meaning that X is of genus 0, a contradiction. ■

1.3.4. Hyperelliptic curves

Lastly, we give a short summary of some of the basic properties of hyperelliptic curves.

Definition 1.3.26. Let K be a number field and X/K a curve over K. We say that X is hyperelliptic if there is a K-rational morphism $\phi : X \to \mathbb{P}^1$ of degree 2.

Definition 1.3.27. Let K be a number field and X/K a curve over K. We say that X is of gonality d over K if there is a nonconstant K-rational morphism $\phi : X \to \mathbb{P}^1$ of degree d, but not of any lower degree.

Proposition 1.3.28 ([21, Section 4.4.2.b])**.** Let K be a number field and X/K a hyperelliptic curve of genus g over K. Then X has a model of the form:

$$y^2 = f(x) = \prod_{i=1}^{d}(x - x_i),$$

with $f(x) \in K[x]$, $x_i \in \overline{K}$ pairwise different and $2g+1 \leq d \leq 2g+2$.

Clearly, given the above model, X has an involution mapping (x,y) to $(x,-y)$. This map is called the hyperelliptic involution. It gives rise to the morphism of degree 2 from Definition 1.3.27 which maps X to $\mathbb{P}^1$. The hyperelliptic curve X/K has infinitely many quadratic points since for any $x \in K$ we have $(x, \sqrt{f(x)}) \in X(\overline{K})$. Such points are often called obvious points. The elements of the Jacobian $J(X)$ can be represented in a convenient way via their Mumford representations:

Theorem 1.3.29 ([21, Theorem 4.145])**.** Let K be a number field and X/K a hyperelliptic curve of genus g with the model $y^2 = f(x)$ with $f \in K[x]$ of degree $2g+1$. Each nontrivial element $D \in J(X)$ can be represented via a unique pair of polynomials $u, v \in K[x]$ where:

- u is monic,
- $deg(v) < deg(u) \leq g$,
- $u \mid v^2 - f$

Notice that this covers only the situations when $deg(f) = 2g+1$, but the analogous representation exists when $deg(f) = 2g+2$, see `Magma` [12] documentation [11, p. 4157-4158]. See also [93, p. 6-7] for a simple algorithm which is used to reconstruct the points of $X(K)$ from the Mumford representations of points on $J(X)(K)$.

We have the similar notion of quadratic twists as with elliptic curves:

Definition 1.3.30. Let K be a number field and X/K a hyperelliptic curve over K with the model:

$$X: \quad y^2 = f(x), \quad f(x) \in K[x].$$

The hyperelliptic curve X^d given by the model:

$$X^d: \quad dy^2 = f(x).$$

is called the quadratic twist of X by d.

Proposition 1.3.31. Let K be a number field and X/K a non-hyperelliptic curve over K. Let D_2 be a K-rational divisor on X of degree 2. Then the map:

$$i: X^{(2)}(K) \mapsto J(X)(K), \quad i(\{P,Q\}) = [P+Q-D_2]$$

is injective.

Proof. Assume that we have $i(\{P,Q\}) = i(\{R,S\})$, that is, $[P+Q-D_2] = [R+S-D_2]$. Hence, $P+Q-D_2+div(f) = R+S-D_2$ so $div(f) = R+S-P-Q$. But then f is a K-rational morphism of degree 2, contradicting the fact that X is non-hyperelliptic. ■

We will also work with the symmetric square of a curve several times in this thesis.

Definition 1.3.32. Let K be a number field and X/K a curve over K. Denote by $X^{(2)}$ the algebraic variety whose points are unordered pairs $Q = \{Q_1, Q_2\}$, where Q_1 and Q_2 are points on X. We say that $X^{(2)}$ is the symmetric square of X.

Definition 1.3.33. Let K be a number field and X/K a curve over K. We say that a point $Q = \{Q_1, Q_2\}$ of $X^{(2)}$ is K-rational if $\{Q_1, Q_2\} = \{Q_1^\sigma, Q_2^\sigma\}$ for all $\sigma \in \mathrm{Gal}(\overline{K}/K)$. We denote the set of all K-rational points of $X^{(2)}$ with $X^{(2)}(K)$.

Definition 1.3.34. Let K be a number field and X/K a curve over K. Let $P = \{P_1, P_2\}$ and $Q = \{Q_1, Q_2\}$ be two points of $X^{(2)}(K)$. We say that they lie in the same residue class modulo prime $\mathfrak{p}$ if $\widetilde{P} = \widetilde{Q}$. Here, $\widetilde{P} = \{\widetilde{P_1}, \widetilde{P_2}\}$ denotes reduction modulo $\mathfrak{p}$.

2. KNOWN RESULTS

In this chapter we will give a brief overview of existing results related to our research as well as formally state some of the results which will be used in the later chapters.

2.1. OVERVIEW

An important problem in the theory of elliptic curves over number fields is to understand their possible torsion groups, parametrized by non-cuspidal points on the modular curves $X_1(m,n)$, and isogenies, parametrized by non-cuspidal points on $X_0(n)$.

After Mazur [61] determined the possible torsion groups over $\mathbb{Q}$, Kamienny, Kenku and Momose [48, 52] determined the possible torsion groups over quadratic fields. Following a pause of almost 3 decades, recent years have seen a number of advances in understanding torsion groups over number fields of degree d: Derickx, Etropolski, van Hoeij, Morrow and Zureick-Brown [25] determined the possible torsion groups over cubic fields and Derickx, Kamienny, Stein and Stoll [26] determined the primes dividing the order of all the possible torsion groups over number fields of degree $4 \leq d \leq 7$. Merel proved that the set of all possible torsion groups over all number fields of degree d is finite, for any positive integer d [63]. All the possible torsion groups over a fixed number field K, for many fixed number fields of degree 2, 3 and 4 have also been determined, see [16, 68, 93]. Gužvić has completely classified the possibilities for $E(K)_{tors}$, where K is a number field of prime degree and E/K an elliptic curve with rational j-invariant [43].

A similar problem that has been considered is classifying the possibilities for $E(K)_{tors}$ for an elliptic curve $E/\mathbb{Q}$. This has been done for quadratic and cubic fields by Najman [71], for quartic fields by Najman, González-Jiménez and Chou [18, 36] and for quintic fields by González-Jiménez [38]. Complete classification for sextic fields, with

the exception of the group $\mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/18\mathbb{Z}$, has been done by Gužvić [44]. Najman and González-Jiménez determined all the possibilities for $[\mathbb{Q}(P) : \mathbb{Q}]$ for a point P of prime order on an elliptic curve $E/\mathbb{Q}$, as well as all the possibilities for $E(K)_{tors}$, where K is a number field of prime degree $p \geq 7$ [36]. Torsion subgroups of elliptic curves $E/\mathbb{Q}$ over some infinite extensions of $\mathbb{Q}$ have also been handled, see [18, 19].

Unfortunately, much less is known about possible degrees of isogenies of elliptic curves over number fields. The only number field K over which the K-rational points on $X_0(n)$ are known for all n is $\mathbb{Q}$, by the results of Mazur [60] and Kenku (see [51] and the references therein) and accordingly, the only positive integer d such that we know all the possible n with $Y_0(n)$ having a rational point of degree d, is $d = 1$. Even the problem of finding all n such that $Y_0^+(n)(\mathbb{Q})$ contains points that are neither CM nor cusps (the set of such n has been conjectured by Elkies [31] to be finite), which can be considered a sub-problem of the case $d = 2$, is still open.

However, lately there has been a great deal of progress in our understanding of quadratic points on $Y_0(n)$. Momose [65, Theorem B] proved that for any fixed quadratic field K which is not imaginary of class number 1, $X_0(p)(K)$ has non-cuspidal points for only finitely many p. Assuming the Generalized Riemann Hypothesis, Banwait [6] explicitly found, for some specific fixed number fields K, all the primes p for which $X_0(p)(K)$ has non-cuspidal points. The Generalized Riemann Hypothesis was needed to get an explicit bound on Momose Type 2 primes (see [6, Proposition 5.3.] and [6, Chapter 1] for more details). Najman [72] determined all the prime degree isogenies of non-CM elliptic curves E with $j(E) \in \mathbb{Q}$ for number fields of degree $d \leq 7$ (and conditionally on Serre's uniformity conjecture for all d). This has been extended to all $d > 1.4 \times 10^7$ unconditionally by Le Fourn and Lemos [56, Theorem 1.3].

Note that the quadratic points when $Y_0(n)$ has genus $g < 2$ are not interesting in a sense. When $Y_0(n)$ has genus 0, the set $Y_0(n)(K)$ is infinite for any number field K, while the modular curves $Y_0(n)$ with genus 1 have infinitely many quadratic points, and moreover the points do not admit a nice geometric description.

On the other hand, for a hyperelliptic curve X of genus $g \geq 2$ with $J(X)$ having rank 0 over $\mathbb{Q}$ and with the hyperelliptic map $h : X \to \mathbb{P}^1$, all but finitely many quadratic points on X are pullbacks $h^{-1}(\mathbb{P}^1(\mathbb{Q}))$ of rational points. Since in the case of $X = X_0(n)$, the hy-

perelliptic involution is almost always an Atkin-Lehner involution w_d for some d dividing n, it follows that all the quadratic points in $h^{-1}(\mathbb{P}^1(\mathbb{Q}))$, and hence all but finitely many quadratic points on $X_0(n)$ correspond to $\mathbb{Q}$-curves of degree d. Using these observations, Bruin and Najman [15] described all the quadratic points on the hyperelliptic curves $X_0(n)$ such that $J(X)(\mathbb{Q})$ is finite; of the 19 values of n such that $X_0(n)$ is hyperelliptic, all but the peculiar case of $n = 37$ satisfy that $J(X)(\mathbb{Q})$ is finite.

Since all the hyperelliptic $X_0(n)$ have genus ≤ 5, the next natural step is finding all the (finitely many) quadratic points on the non-hyperelliptic modular curves $X_0(n)$ with $g(X_0(n)) \leq 5$ and $\mathrm{rk}(J_0(n)(\mathbb{Q})) = 0$, of which there are 15. This has been done by Ozman and Siksek [74] by using the fact that the Abel-Jacobi map $\iota : X^{(2)}(\mathbb{Q}) \to J(X)(\mathbb{Q})$ which sends $\{P,Q\}$ to $[P+Q-2P_0]$, for some fixed $P_0 \in X(\mathbb{Q})$, is injective, and hence all the quadratic points of X can be found by checking $J(X)(\mathbb{Q})$, which is, by assumption, finite.

Box [13] completed the description of quadratic points on $X_0(n)$ of genus $2 \leq g \leq 5$ by describing the quadratic points for the 8 values of n such that $\mathrm{rk}(J_0(n)(\mathbb{Q})) > 0$, including the hyperelliptic case of $n = 37$. Box, Gajović and Goodman [14] also determined all the cubic points on the modular curves $X_0(n)$ for $n \in \{53,57,61,65,67,73\}$ as well as all the quartic points on $X_0(65)$.

Similar computations were done with the curves $X_0(125)$ and $X_0(169)$ and all of the finitely many quadratic points on them have been found by Banwait, Najman and Padurariu [2]. Also, the authors completely classified all the possible cyclic isogeny degrees for the quadratic field $\mathbb{Q}(\sqrt{213})$ and several other quadratic fields, assuming the Generalized Riemann Hypothesis (for the same reason as [6]).

2.2. AUXILIARY RESULTS

In this section we will list some theorems and lemmas which are either well known or which we will be using in various parts of our thesis. The results mentioned here are also very useful to know outside of the scope of this thesis. First we will give some additional known results about torsion subgroups of elliptic curves which we will use several times.

Very often, the question of whether an elliptic curve can have a certain torsion subgroup over some number field can be reduced to the same question for a lower degree number field. Hence, these results are very useful:

Theorem 2.2.1 ([71, Theorem 2])**.** Let $E/\mathbb{Q}$ be an elliptic curve and K a quadratic field. Then $E(K)_{tors}$ is isomorphic to one of the following groups:

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

$\mathbb{Z}/15\mathbb{Z}$ is the only group which appears in only finitely many cases, and only over the extensions $\mathbb{Q}(\sqrt{5})$ and $\mathbb{Q}(\sqrt{-15})$.

Theorem 2.2.2 ([71, Theorem 1])**.** Let $E/\mathbb{Q}$ be an elliptic curve and K a cubic field. Then $E(K)_{tors}$ is isomorphic to one of the following groups:

$$\mathbb{Z}/m\mathbb{Z}, \quad m = 1,\dots,10,12,13,14,18,21,$$
$$\mathbb{Z}/2\mathbb{Z}\oplus\mathbb{Z}/2m\mathbb{Z}, \quad m = 1,2,3,4,7.$$

$\mathbb{Z}/21\mathbb{Z}$ is the only group which appears in only finitely many cases, and only over the extension $\mathbb{Q}(\zeta_9)^+$.

Theorem 2.2.3 ([17, 36])**.** Let $E/\mathbb{Q}$ be an elliptic curve and K a quartic field. Then

$E(K)_{tors}$ is isomorphic to one of the following groups:

$$\mathbb{Z}/m\mathbb{Z}, \quad m = 1,\dots,10,12,13,15,16,20,24,$$
$$\mathbb{Z}/2\mathbb{Z}\oplus\mathbb{Z}/2m\mathbb{Z}, \quad m = 1,\dots,6,8,$$
$$\mathbb{Z}/3\mathbb{Z}\oplus\mathbb{Z}/3m\mathbb{Z}, \quad m = 1,2,$$
$$\mathbb{Z}/4\mathbb{Z}\oplus\mathbb{Z}/4m\mathbb{Z}, \quad m = 1,2,$$
$$\mathbb{Z}/5\mathbb{Z}\oplus\mathbb{Z}/5\mathbb{Z},$$
$$\mathbb{Z}/6\mathbb{Z}\oplus\mathbb{Z}/6\mathbb{Z}.$$

We will also use the following result which considers possible torsion subgroups over $\mathbb{Q}^{ab}$, the maximal abelian extension of $\mathbb{Q}$ which can be realized by adjoining all roots of unity to $\mathbb{Q}$.

Theorem 2.2.4 ([18, Theorem 1.2.]). Let $E/\mathbb{Q}$ be an elliptic curve. Then $E(\mathbb{Q}^{ab})_{tors}$ is isomorphic to one of the following groups:

$$\mathbb{Z}/m\mathbb{Z}, \quad m = 1,3,5,7,9,11,13,15,17,19,21,25,27,37,43,67,163,$$
$$\mathbb{Z}/2\mathbb{Z}\oplus\mathbb{Z}/2m\mathbb{Z}, \quad m = 1,2,\dots,8,9,$$
$$\mathbb{Z}/3\mathbb{Z}\oplus\mathbb{Z}/3m\mathbb{Z}, \quad m = 1,3,$$
$$\mathbb{Z}/4\mathbb{Z}\oplus\mathbb{Z}/4m\mathbb{Z}, \quad m = 1,2,3,4,$$
$$\mathbb{Z}/5\mathbb{Z}\oplus\mathbb{Z}/5\mathbb{Z},$$
$$\mathbb{Z}/6\mathbb{Z}\oplus\mathbb{Z}/6\mathbb{Z},$$
$$\mathbb{Z}/8\mathbb{Z}\oplus\mathbb{Z}/8\mathbb{Z}.$$

We have another very useful result connecting the torsion subgroups of elliptic curves with the cyclotomic fields:

Theorem 2.2.5 ([84, Corollary 8.1.1.]). Let K be a number field and E/K an elliptic curve. Assume that $E[n] \subseteq E(K)$. Then $\mathbb{Q}(\zeta_n) \subseteq K$.

The following results about the 2-torsion of an elliptic curve are also useful:

Proposition 2.2.6 ([83, p. 6]). Let K be a number field and E/K an elliptic curve given in a short Weierstrass form. Let $P = (x,y)$ be a point of E of order 2. Then $y = 0$ and $[K(P) : K] \in \{1,2,3\}$.

Proposition 2.2.7 ([83, p. 6])**.** Let K be a number field and E/K an elliptic curve. Then $[K(E[2]):K] \in \{1,2,3,6\}$. When $[K(E[2]):K] = 6$, the Galois group of the corresponding extension is isomorphic to S_3, hence not commutative.

We will also be considering the torsion of certain Jacobians. For those computations, this result will be crucial:

Theorem 2.2.8 ([49, Appendix])**.** Let K be a number field and A/K an abelian variety. Let $\mathfrak{p}$ be a prime of good reduction for A. Let p be the rational prime below $\mathfrak{p}$ and let $e(\mathfrak{p}/p)$ be the ramification degree. Suppose $e(\mathfrak{p}/p) < p-1$. Then the reduction map $red_{\mathfrak{p}}$ is injective when restricted to the torsion subgroup $A(K)_{tors}$.

Remark 2.2.9. Notice that the condition $e(\mathfrak{p}/p) < p-1$ reduces to $p > 2$ when $K = \mathbb{Q}$.

Next we give some generally useful results about isogenies of elliptic curves. Some of these results are well-known while others are useful lemmas which will be used in the later chapters.

Lemma 2.2.10. Let K be a number field and E/K an elliptic curve with a cyclic n-isogeny and a cyclic m-isogeny both defined over K with $\gcd(m,n) = 1$. Then E also has a cyclic mn isogeny defined over K.

Proof. Let $\langle P \rangle$ be the kernel of the n-isogeny and let $\langle Q \rangle$ be the kernel of the m-isogeny. Consider the group $C = \langle P+Q \rangle$. Clearly, C has mn elements and we have $C = \{aP+bQ : 0 \le a < n, 0 \le b < m\}$. Because $\mathrm{Gal}(\overline{K}/K)$ acts on both $\langle P \rangle$ and $\langle Q \rangle$, it also acts on C. Therefore, C is the kernel of a cyclic mn-isogeny defined over K by Theorem 1.1.17. ■

The following result of Najman says a lot about the isogenies of prime degree and is the motivation for Chapter 4 of this thesis:

Theorem 2.2.11 ([72, Theorem 1.1.])**.** Let K be a number field of degree at most 7 and $E/\mathbb{Q}$ a non-CM elliptic curve with a cyclic p-isogeny defined over K with p prime. Then $p \in \{2,3,5,7,11,13,17,37\}$.

As we mentioned in Section 1.2, elliptic curves with a cyclic n-isogeny over $\mathbb{Q}$ have only upper-triangular matrices in its image of $\rho_{E,n}$ (up to conjugation). A more general version of that fact holds:

Lemma 2.2.12. Let $E/\mathbb{Q}$ be an elliptic curve and $n \geq 2$ an integer. Assume that the image of $\rho_{E,n}$ contains a subgroup $H \leq B(n)$, up to conjugation and that $[Im(\rho_{E,n}) : H] = d$. Then E has a cyclic n-isogeny defined over a field K such that $[K : \mathbb{Q}] = d$.

Proof. Select a basis $\{P, Q\}$ for $E[n]$ such that $H \leq Im(\rho_{E,n})$. Recall from Section 1.2 that $\rho_{E,n}$ is injective on $\mathrm{Gal}(\mathbb{Q}(E[n])/\mathbb{Q})$. Hence, a subgroup $S \leq \mathrm{Gal}(\mathbb{Q}(E[n])/\mathbb{Q})$ of index d is mapped to H via $\rho_{E,n}$. Because $H \leq B(n)$, we have that $P^\sigma \in \langle P \rangle$ for all $\sigma \in S$. Hence, the absolute Galois group of the fixed field K of S acts on $\langle P \rangle$, so $\langle P \rangle$ is the kernel of a cyclic isogeny defined over K by Theorem 1.1.17. By Galois theory, the field K satisfies $[K : \mathbb{Q}] = d$ and the proof is complete. ■

Remark 2.2.13. Notice that in the proof of the Lemma 2.2.12, the field K contains the smallest field over which the isogeny with kernel $\langle P \rangle$ is defined. By going through all possible bases for $E[n]$ and subgroups H of the image of $\rho_{E,n}$ satisfying $H \leq B(n)$ (up to conjugation), we can find the field with the smallest extension degree over which E has a cyclic n-isogeny.

Let $E/\mathbb{Q}$ be an elliptic curve, $n \geq 2$ an integer and $\{P, Q\}$ a basis for $E[n]$. Then any cyclic subgroup $G \leq E[n]$ of order n can be written as $G = \langle R \rangle$ with $R = kP + lQ$ of order n, where $k, l \in \mathbb{Z}/n\mathbb{Z}$. Hence, we can assign a column $\begin{bmatrix} k \\ l \end{bmatrix}$ to G (and R). Notice that there are $\phi(n)$ possibilities for the column since we have $\phi(n)$ options to select a generator of a group isomorphic to $\mathbb{Z}/n\mathbb{Z}$, but let's take any of them. Now we define the action of $Im(\rho_{E,n})$ on the set of cyclic subgroups $G \leq E[n]$ of order n. For such $G \leq E[n]$, an element $A_\sigma \in Im(\rho_{E,n})$ maps G to a subgroup G^{A_σ} represented by the column $A_\sigma \begin{bmatrix} k \\ l \end{bmatrix}$. We now must show that the action is well defined. First we will show that the subgroup G^{A_σ} really is cyclic of order n. Set $A_\sigma = \rho_{E,n}(\sigma) = \begin{bmatrix} a & c \\ b & d \end{bmatrix}$. That means that:

$$P^\sigma = aP + bQ,$$

$$Q^\sigma = cP + dQ.$$

We have $A_\sigma \begin{bmatrix} k \\ l \end{bmatrix} = \begin{bmatrix} ak + cl \\ bk + dl \end{bmatrix}$. Notice that for $R = kP + lQ$ (a generator for G) we have $R^\sigma = (ak + cl)P + (bk + dl)Q$ (a generator for G^{A_σ}). Because σ preserves the order of a

point, G^{A_σ} is cyclic of order n. It remains to prove that the action is not disrupted by using a different generator of G. Assume we take another generator for $G = \langle R \rangle$, it is of the form mR with $m \in (\mathbb{Z}/n\mathbb{Z})^\times$. From the above computation, we see that G^{A_σ} is generated by $(mR)^\sigma = mR^\sigma$. Clearly, we have $\langle mR^\sigma \rangle = \langle R^\sigma \rangle$, so the action is well defined. Notice that when $n = p$ for a prime number p, this action can be viewed as the action of $\mathrm{PGL}_2(\mathbb{Z}/p\mathbb{Z})$ on $\mathbb{P}^1(\mathbb{Z}/p\mathbb{Z})$.

We have now defined the action of $Im(\rho_{E,n})$ on the set of all cyclic subgroups of $E[n]$ of order n such that $A_\sigma = \rho_{E,n}(\sigma)$ sends G to G^σ for each $\sigma \in \mathrm{Gal}(\mathbb{Q}(E[n])/\mathbb{Q})$.

Lemma 2.2.14. Let $E/\mathbb{Q}$ be an elliptic curve and $n \geq 2$ an integer. Let $G \leq E[n]$ be cyclic of order n. Assume that the orbit length of G under the above action of $Im(\rho_{E,n})$ is d. Then a cyclic n-isogeny with kernel G is defined over a degree d number field and not over any number field of lower degree.

Proof. By the Orbit-Stabilizer theorem we have:

$$\#\mathrm{Stab}(G) = \frac{\#Im(\rho_{E,n})}{\#\mathrm{Orb}(G)}.$$

Hence, $[Im(\rho_{E,n}) : \mathrm{Stab}(G)] = d$. Since all A_σ such that $G^{A_\sigma} = G^\sigma = G$ form an index d subgroup of $Im(\rho_{E,n})$, then all the corresponding $\sigma \in \mathrm{Gal}(\mathbb{Q}(E[n])/\mathbb{Q})$ satisfying $G^\sigma = G$ form an index d subgroup H of $\mathrm{Gal}(\mathbb{Q}(E[n])/\mathbb{Q})$, due to $Im(\rho_{E,n})$ being injective on $\mathrm{Gal}(\mathbb{Q}(E[n])/\mathbb{Q})$. Let K be the fixed field of H. This shows that $\mathrm{Gal}(\overline{K}/K)$ acts on G, so the cyclic isogeny with kernel G is defined over K by Theorem 1.1.17. Notice that by Galois theory we have $[K : \mathbb{Q}] = d$. Also notice that this is the lowest possible field degree since H contains all $\sigma \in \mathrm{Gal}(\mathbb{Q}(E[n])/\mathbb{Q})$ which fix G. This completes the proof. ■

For an elliptic curve $E/\mathbb{Q}$ and a prime p, it will be useful for us to connect the image of $\rho_{E,p}$ with the degree of the field of definition of a point of order p. The following tables 2.1 and 2.2 give such correspondence. Groups labeled with `pB` correspond to various subgroups of $B(p)$. Groups labeled with `pCs` correspond to various subgroups of $C_s(p)$. Groups labeled with `pCn` correspond to various subgroups of $C_{ns}(p)$. Groups labeled with `pNs` correspond to various subgroups of $N_s(p)$. Groups labeled with `pNn` correspond to various subgroups of $N_{ns}(p)$. The number d_v gives the corresponding possibilities for $[\mathbb{Q}(P) : \mathbb{Q}]$, where $P \in E[p]$. The number d gives the corresponding value of $[\mathbb{Q}(E[p]) : \mathbb{Q}]$.

Note that Tables 2.1 and 2.2 are partially extracted from Table 3 of [90]. They can also be found in [36].

Sutherland	Zywina	d_v	d
2Cs	G_1	1	1
2B	G_2	1,2	2
2Cn	G_3	3	3
3Cs.1.1	$H_{1,1}$	1,2	2
3Cs	G_1	2,4	4
3B.1.1	$H_{3,1}$	1,6	6
3B.1.2	$H_{3,2}$	2,3	6
3Ns	G_2	4	8
3B	G_3	2,6	12
3Nn	G_4	8	16
5Cs.1.1	$H_{1,1}$	1,4	4
5Cs.1.3	$H_{1,2}$	2,4	4
5Cs.4.1	G_1	2,4,8	8
5Ns.2.1	G_3	8,16	16
5Cs	G_2	4,4	16
5B.1.1	$H_{6,1}$	1,20	20
5B.1.2	$H_{5,1}$	4,5	20
5B.1.4	$H_{6,2}$	2,20	20
5B.1.3	$H_{5,2}$	4,10	20
5Ns	G_4	8,16	32
5B.4.1	G_6	2,20	40
5B.4.2	G_5	4,10	40
5Nn	G_7	24	48
5B	G_8	4,20	80
5S4	G_9	24	96

Sutherland	Zywina	d_v	d
7Ns.2.1	$H_{1,1}$	6,9,18	18
7Ns.3.1	G_1	12,18	36
7B.1.1	$H_{3,1}$	1,42	42
7B.1.3	$H_{4,1}$	6,7	42
7B.1.2	$H_{5,2}$	3,42	42
7B.1.5	$H_{5,1}$	6,21	42
7B.1.6	$H_{3,2}$	2,21	42
7B.1.4	$H_{4,2}$	3,14	42
7Ns	G_2	12,36	72
7B.6.1	G_3	2,42	84
7B.6.3	G_4	6,14	84
7B.6.2	G_5	6,42	84
7Nn	G_6	48	96
7B.2.1	$H_{7,2}$	3,42	126
7B.2.3	$H_{7,1}$	6,21	126
7B	G_7	6,42	252
11B.1.4	$H_{1,1}$	5,110	110
11B.1.5	$H_{2,1}$	5,110	110
11B.1.6	$H_{2,2}$	10,55	110
11B.1.7	$H_{1,2}$	10,55	110
11B.10.4	G_1	10,110	220
11B.10.5	G_2	10,110	220
11Nn	G_3	120	240

Table 2.1: Possible images $G_E(p) \neq \mathrm{GL}_2(\mathbb{F}_p)$, for $p \leq 11$, for non-CM elliptic curves $E/\mathbb{Q}$.

Sutherland	Zywina	d_v	d	Sutherland	Zywina	d_v	d
13S4	G_7	$72, 96$	288	13B.4.1	G_5	$6, 156$	936
13B.3.1	$H_{5,1}$	$3, 156$	468	13B.4.2	G_4	$12, 78$	936
13B.3.2	$H_{4,1}$	$12, 39$	468	13B	G_6	$12, 156$	1872
13B.3.4	$H_{5,2}$	$6, 156$	468	17B.4.2	G_1	$8, 272$	1088
13B.3.7	$H_{4,2}$	$12, 78$	468	17B.4.6	G_2	$16, 136$	1088
13B.5.1	G_2	$4, 156$	624	37B.8.1	G_1	$12\ ,\ 1332$	15984
13B.5.2	G_1	$12, 52$	624	37B.8.2	G_2	$36\ ,\ 444$	15984
13B.5.4	G_3	$12, 156$	624				

Table 2.2: Known images $G_E(p) \neq \mathrm{GL}_2(\mathbb{F}_p)$, for $p = 13, 17$ or 37, for non-CM elliptic curves $E/\mathbb{Q}$.

3. TORSION GROUPS OF ELLIPTIC CURVES OVER $\mathbb{Q}(\mu_{p^\infty})$

In this chapter we will consider torsion subgroups of rational elliptic curves over some specific cyclotomic fields and over some infinite extensions of $\mathbb{Q}$. This work is also documented in the paper [42] written by T. Gužvić and the author of this thesis. This work is motivated by the work of M. Chou [18] where he determined all the possible torsion subgroups of rational elliptic curves over $\mathbb{Q}^{ab}$, which is the maximal abelian extension of $\mathbb{Q}$. It is also related to the work of Chou, Daniels, Krijan and Najman [19] where they determined all the possible torsion subgroups of rational elliptic curves over the $\mathbb{Z}_p$-extensions of $\mathbb{Q}$.

Definition 3.0.1. Let p be a prime number. Denote with μ_{p^∞} the set of all complex numbers ω for which there exists a non-negative integer k such that $\omega^{p^k} = 1$.

Notice that $\mathbb{Q}(\mu_{p^\infty})$ is the field $\mathbb{Q}$ extended with all p^n-th primitive roots of unity. In [41], the authors showed that the torsion subgroup of $E/\mathbb{Q}$ grows only over small subfields of $\mathbb{Q}(\mu_{p^\infty})$ for a prime number p. This will enable us to quickly reduce the problem from infinite to finite extensions. Recall that, by Mazur's theorem, $E(\mathbb{Q})_{tors}$ is isomorphic to one of the following groups:

$$\mathbb{Z}/m\mathbb{Z}, \quad m = 1,2,\ldots,10,12,$$
$$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2m\mathbb{Z}, \quad m = 1,2,3,4.$$

Our main results are the following:

Proposition 3.0.2. Let $E/\mathbb{Q}$ be an elliptic curve. Then $E(\mathbb{Q}(\mu_{2^\infty}))_{tors}$ is isomorphic to one of the groups from Mazur's theorem or to one of the following groups, with examples

of curves given by their LMFDB labels in the brackets:

$$\mathbb{Z}/4\mathbb{Z}\oplus\mathbb{Z}/4\mathbb{Z} \quad (15.a5),$$
$$\mathbb{Z}/2\mathbb{Z}\oplus\mathbb{Z}/10\mathbb{Z} \quad (2112.bd4).$$

Proposition 3.0.3. Let $E/\mathbb{Q}$ be an elliptic curve. Then $E(\mathbb{Q}(\mu_{3^\infty}))_{tors}$ is isomorphic to one of the groups from Mazur's theorem or to one of the following groups, with examples of curves given by their LMFDB labels in the brackets:

$$\mathbb{Z}/21\mathbb{Z} \quad (162.b4),$$
$$\mathbb{Z}/27\mathbb{Z} \quad (27.a2),$$
$$\mathbb{Z}/3\mathbb{Z}\oplus\mathbb{Z}/3\mathbb{Z} \quad (54.a3),$$
$$\mathbb{Z}/3\mathbb{Z}\oplus\mathbb{Z}/6\mathbb{Z} \quad (126.b6),$$
$$\mathbb{Z}/3\mathbb{Z}\oplus\mathbb{Z}/9\mathbb{Z} \quad (27.a3).$$

Proposition 3.0.4. Let $E/\mathbb{Q}$ be an elliptic curve. Then $E(\mathbb{Q}(\mu_{5^\infty}))_{tors}$ is isomorphic to one of the groups from Mazur's theorem or to one of the following groups, with examples of curves given by their LMFDB labels in the brackets:

$$\mathbb{Z}/15\mathbb{Z} \quad (50.a2),$$
$$\mathbb{Z}/16\mathbb{Z} \quad (15.a7),$$
$$\mathbb{Z}/5\mathbb{Z}\oplus\mathbb{Z}/5\mathbb{Z} \quad (550.j3).$$

Proposition 3.0.5. Let $E/\mathbb{Q}$ be an elliptic curve. Then $E(\mathbb{Q}(\mu_{7^\infty}))_{tors}$ is isomorphic to one of the groups from Mazur's theorem or to one of the following groups, with examples of curves given by their LMFDB labels in the brackets:

$$\mathbb{Z}/13\mathbb{Z} \quad (147b1),$$
$$\mathbb{Z}/14\mathbb{Z} \quad (49a4),$$
$$\mathbb{Z}/18\mathbb{Z} \quad (14a6),$$
$$\mathbb{Z}/2\mathbb{Z}\oplus\mathbb{Z}/14\mathbb{Z} \quad (49a1),$$
$$\mathbb{Z}/2\mathbb{Z}\oplus\mathbb{Z}/18\mathbb{Z} \quad (14a4).$$

Proposition 3.0.6. Let $E/\mathbb{Q}$ be an elliptic curve. Then $E(\mathbb{Q}(\mu_{11^\infty}))_{tors}$ is isomorphic to one of the groups from Mazur's theorem or to one of the following groups, with examples of curves given by their LMFDB labels in the brackets:

$$\mathbb{Z}/11\mathbb{Z} \quad (121b2),$$
$$\mathbb{Z}/25\mathbb{Z} \quad (11a3),$$
$$\mathbb{Z}/2\mathbb{Z}\oplus\mathbb{Z}/10\mathbb{Z} \quad (10230bg2).$$

The code that verifies all the computation related to this work can be found on:

`https://github.com/brutalni-vux/TorsionCyclotomic`.

3.1. Auxiliary results

We begin by stating a theorem which will reduce the cases of infinite extensions to the cases of finite ones.

Theorem 3.1.1 ([41, Theorem 1.3.])**.** Let $E/\mathbb{Q}$ be an elliptic curve. Then for a prime number $p \geq 5$ it holds that

$$E(\mathbb{Q}(\mu_{p^\infty}))_{tors} = E(\mathbb{Q}(\zeta_p))_{tors}.$$

Furthermore,

$$E(\mathbb{Q}(\mu_{3^\infty}))_{tors} = E(\mathbb{Q}(\zeta_{27}))_{tors} \quad \text{and} \quad E(\mathbb{Q}(\mu_{2^\infty}))_{tors} = E(\mathbb{Q}(\zeta_{16}))_{tors}.$$

Remark 3.1.2. This result is *the best possible*. For E with the LMFDB label 27.a2 we have:

$$E(\mathbb{Q}(\zeta_9))_{tors} \cong \mathbb{Z}/9\mathbb{Z} \subsetneq \mathbb{Z}/27\mathbb{Z} \cong E(\mathbb{Q}(\zeta_{27}))_{tors}.$$

For E with the LMFDB label 32.a2 we have:

$$E(\mathbb{Q}(\zeta_8))_{tors} \cong \mathbb{Z}/2\mathbb{Z}\oplus\mathbb{Z}/4\mathbb{Z} \subsetneq \mathbb{Z}/2\mathbb{Z}\oplus\mathbb{Z}/8\mathbb{Z} \cong E(\mathbb{Q}(\zeta_{16}))_{tors}.$$

Because of Theorem 3.1.1, we only need to work with several specific cyclotomic fields to prove our main results. Clearly, those are the fields $\mathbb{Q}(\zeta_{16})$, $\mathbb{Q}(\zeta_{27})$, $\mathbb{Q}(\zeta_5)$, $\mathbb{Q}(\zeta_7)$ and $\mathbb{Q}(\zeta_{11})$. It becomes natural to ask ourselves how the torsion group of $E/\mathbb{Q}$

grows when we consider the base change $E/\mathbb{Q}(\zeta_p)$. This becomes much harder as p grows because our methods sometimes rely on pure computation.

The following lemma is well-known:

Lemma 3.1.3 ([37, Theorem 3., Corollary 4.])**.** Let $E/\mathbb{Q}$ be an elliptic curve and L/K a quadratic extension of number fields with $L = K(\sqrt{d})$. Let $E(K)_{(2')}$ be the group of K-rational points of E of odd order. Then we have:

$$E(K(\sqrt{d}))_{(2')} \cong E(K)_{(2')} \oplus E^d(K)_{(2')}.$$

The similar holds for hyperelliptic Jacobians and their ranks:

Lemma 3.1.4 ([55, Corollary 1.3.])**.** Let K be a number field, X/K a hyperelliptic curve and L/K a quadratic extension of number fields with $L = K(\sqrt{d})$. Let $J(X)$ be the Jacobian of X and let $J^d(X)$ be the Jacobian of the quadratic twist X^d. Then we have:

$$\mathrm{rk}(J(X)(L)) = \mathrm{rk}(J(X)(K)) + \mathrm{rk}(J^d(X)(K)).$$

Since all cyclotomic extensions are Galois over $\mathbb{Q}$, the following result imposes restrictions on the possibilities for the torsion subgroup of $E/\mathbb{Q}$ over cyclotomic fields.

Lemma 3.1.5. Let $E/\mathbb{Q}$ be an elliptic curve, m, n positive integers and K a finite Galois extension of $\mathbb{Q}$. Let $E(K)[mn] \cong \mathbb{Z}/m\mathbb{Z} \oplus \mathbb{Z}/mn\mathbb{Z}$ and $P \in E(K)$ a point of order mn. Then we have:

$$[\mathbb{Q}(mP) : \mathbb{Q}] \mid \gcd(\varphi(n), [K : \mathbb{Q}]),$$

where φ is the Euler function.

Proof. Let $P \in E(K)$ be a point of order mn. Then we can take $Q \in E[mn]$ such that $\{P, Q\}$ is a basis for $E[mn]$. Consider the mod n Galois representation of E:

$$\rho_{E,n} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z}).$$

Take $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$. Then we have $P^\sigma = \alpha P + \beta Q$ for some $\alpha, \beta \in \mathbb{Z}/mn\mathbb{Z}$ because the action of σ preserves the order of a point. Now we have $P^\sigma - \alpha P = \beta Q$, so $\beta Q \in E(K)$. Clearly, P and βQ are independent (except if $\beta Q = O$). Hence, they generate a subgroup of $E(K)[mn]$ of order $mn \cdot ord(\beta Q)$. Since we have $E(K)[mn] \cong \mathbb{Z}/m\mathbb{Z} \oplus \mathbb{Z}/mn\mathbb{Z}$, we

can conclude that $ord(\beta Q) \mid m$. Therefore, $m\beta \equiv 0 \pmod{mn}$ since Q is of order mn. Multiplying the equality $P^\sigma - \alpha P = \beta Q$ by m gives us $(mP)^\sigma = \alpha(mP)$ so $(mP)^\sigma \in \langle mP \rangle$ for all $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$. We know that mP is of order n, so we have $(mP)^\sigma = g(mP)$ for some $g \in (\mathbb{Z}/n\mathbb{Z})^\times$ since the action of σ preserves the order of a point.

Since by considering the restriction map we get $\mathrm{Gal}(K/\mathbb{Q}) \cong \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})/\mathrm{Gal}(\overline{\mathbb{Q}}/K)$ from the first isomorphism theorem and Galois theory, we have $(mP)^\sigma \in \langle mP \rangle$ for all $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. Therefore, if we choose mP to be one of the elements of the basis for $E[n]$, for all $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ we have:

$$\rho_{E,n}(\sigma) = \begin{bmatrix} \phi(\sigma) & \tau(\sigma) \\ 0 & \psi(\sigma) \end{bmatrix}.$$

Notice that we have the homomorphisms $\phi, \psi : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to (\mathbb{Z}/n\mathbb{Z})^\times$ and the map $\tau : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathbb{Z}/n\mathbb{Z}$.

For a point $R \in E(K)[mn]$, denote by $\mathrm{Orb}(R)$ the orbit of R under the action of $\mathrm{Gal}(K/\mathbb{Q})$ on $E(K)[mn]$. Denote by $\mathrm{Stab}(R)$ the stabilizer of R under that same action. We know that $(mP)^\sigma = g(mP) \Leftrightarrow \phi(\sigma) = g$, for all $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. Therefore, we have:

$$\#Im(\phi) = \#\{(mP)^\sigma : \sigma \in \mathrm{Gal}(K/\mathbb{Q})\} = \#\mathrm{Orb}(mP).$$

It is clear that $\mathrm{Stab}(mP) = \mathrm{Gal}(K/\mathbb{Q}(mP))$, so by Orbit-Stabilizer theorem we have:

$$\#Im(\phi) = \frac{\#\mathrm{Gal}(K/\mathbb{Q})}{\#\mathrm{Gal}(K/\mathbb{Q}(mP))} = [\mathbb{Q}(mP) : \mathbb{Q}].$$

On the other hand, we have $Im(\phi) \leq (\mathbb{Z}/n\mathbb{Z})^\times$, so we have:

$$[\mathbb{Q}(mP) : \mathbb{Q}] \mid \varphi(n).$$

Since $[\mathbb{Q}(mP) : \mathbb{Q}] \mid [K : \mathbb{Q}]$ is obvious, the proof is complete. ■

The following useful lemma provides a connection between torsion and isogenies:

Lemma 3.1.6 ([18, Lemma 2.7.])**.** Let K be a Galois extension of $\mathbb{Q}$ and $E/\mathbb{Q}$ an elliptic curve. If $E(K)_{tors} \cong \mathbb{Z}/m\mathbb{Z} \oplus \mathbb{Z}/mn\mathbb{Z}$, then E has a cyclic n-isogeny over $\mathbb{Q}$.

When dealing with points whose order is a power of a prime, the following will be helpful:

Lemma 3.1.7 ([36, Proposition 4.6.])**.** Let K be a number field and E/K an elliptic curve. Let n be a positive integer, p a prime and $P \in E(\overline{K})$ a point of order p^{n+1}. Then $[K(P) : K(pP)]$ divides p^2 or $p(p-1)$.

One of the crucial results that we will use is the result of Chou mentioned in the beginning of this chapter and already stated in this thesis (see Theorem 2.2.4) but we state it again for easier reading:

Theorem 3.1.8 ([18, Theorem 1.2.])**.** Let $E/\mathbb{Q}$ be an elliptic curve. Then $E(\mathbb{Q}^{ab})_{tors}$ is isomorphic to one of the following groups:

$$\mathbb{Z}/m\mathbb{Z}, \quad m = 1,3,5,7,9,11,13,15,17,19,21,25,27,37,43,67,163$$

$$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2m\mathbb{Z}, \quad m = 1,2,\ldots,8,9$$

$$\mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3m\mathbb{Z}, \quad m = 1,3$$

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

$$\mathbb{Z}/5\mathbb{Z} \oplus \mathbb{Z}/5\mathbb{Z},$$

$$\mathbb{Z}/6\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z},$$

$$\mathbb{Z}/8\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z}.$$

This means that all of our candidates for the torsion subgroup are the subgroups of the groups in Theorem 3.1.8.

3.2. TORSION GROWTH OVER $\mathbb{Q}(\zeta_{16})$

In this section we prove Proposition 3.0.2. Assume that $E/\mathbb{Q}$ is an elliptic curve and that $E(\mathbb{Q}(\zeta_{16}))_{tors} \cong \mathbb{Z}/m\mathbb{Z} \oplus \mathbb{Z}/mn\mathbb{Z}$. By Theorem 2.2.5, we have $\mathbb{Q}(\zeta_m) \subseteq \mathbb{Q}(\zeta_{16})$. It follows that $m \in \{1,2,4,8,16\}$. The case $m = 16$ is impossible by Theorem 3.1.8. We first eliminate a certain amount of cyclic groups listed in Theorem 3.1.8.

Lemma 3.2.1. Let $E/\mathbb{Q}$ be an elliptic curve. Then $E(\mathbb{Q}(\zeta_{16}))_{tors}$ is not isomorphic to $\mathbb{Z}/n\mathbb{Z}$ if $n \in \{11,14,17,18,19,21,25,27,37,43,67,163\}$.

Proof. Lemma 3.1.5 gives us that if $P_n \in E(\mathbb{Q}(\zeta_{16}))$ is a point of order $n \in \{11,14,18,19,27,43,67,163\}$, we have $[\mathbb{Q}(P_n) : \mathbb{Q}] \mid 2$, which is impossible by Theorem 2.2.1. By the same lemma we get that if P_n is a point of order $n \in \{21,25,37\}$, then we have $[\mathbb{Q}(P_n) : \mathbb{Q}] \mid 4$, which is impossible by Theorem 2.2.3.

It remains to consider the case $n = 17$. By [36, Theorem 5.8.] we conclude that the point $P_{17} \in E(\mathbb{Q}(\zeta_{16}))$ of order 17 cannot be defined over some strictly smaller subfield of $\mathbb{Q}(\zeta_{16})$. That means that all $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta_{16})/\mathbb{Q})$ act differently on P_{17}. Since $\mathrm{Gal}(\mathbb{Q}(\zeta_{16})/\mathbb{Q})$ has four elements σ such that $\sigma^2 = id$, we have that $P_{17}^{\sigma^2} = k^2 P_{17} = P_{17}$ for four different $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta_{16})/\mathbb{Q})$. That means that we have $k^2 \equiv 1 \pmod{17}$ for four different $k \in \mathbb{Z}/17\mathbb{Z}$, a contradiction. ∎

After eliminating plenty of cyclic groups, we discuss the cases when E obtains the full 2-torsion over $\mathbb{Q}(\zeta_{16})$. This is done by the following lemmas:

Lemma 3.2.2. Let $E/\mathbb{Q}$ be an elliptic curve. Then $E(\mathbb{Q}(\zeta_{16}))_{tors}$ is not isomorphic to $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/14\mathbb{Z}$ or $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/18\mathbb{Z}$.

Proof. We will prove the result for $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/14\mathbb{Z}$ and the proof for the case $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/18\mathbb{Z}$ is identical. Let $P_{14} \in E(\mathbb{Q}(\zeta_{16}))$ be the point of order 14. From Lemma 3.1.5 we get that $[\mathbb{Q}(2P_{14}) : \mathbb{Q}] \mid 2$. By Proposition 2.2.7 we have $[\mathbb{Q}(E[2]) : \mathbb{Q}] \in \{1,2,3,6\}$. Since $E[2]$ is defined over $\mathbb{Q}(\zeta_{16})$, we have $[\mathbb{Q}(E[2]) : \mathbb{Q}] \in \{1,2\}$.

Let Q_2 be a point of order 2 different from $7P_{14}$. We now have $[\mathbb{Q}(2P_{14}, 7P_{14}, Q_2) : \mathbb{Q}] \mid 4$. Since $2P_{14}, 7P_{14}$ and Q_2 generate our torsion subgroup $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/14\mathbb{Z}$, we now know that this torsion subgroup appears over some strictly smaller subfield of $\mathbb{Q}(\zeta_{16})$. Now we get a contradiction by using Theorem 2.2.1 and Theorem 2.2.3. ∎

Lemma 3.2.3. Let $E/\mathbb{Q}$ be an elliptic curve. Then $E(\mathbb{Q}(\zeta_{16}))_{tors}$ is not isomorphic to any of the following groups:

$$\mathbb{Z}/15\mathbb{Z}, \quad \mathbb{Z}/2\mathbb{Z}\oplus\mathbb{Z}/12\mathbb{Z},$$
$$\mathbb{Z}/4\mathbb{Z}\oplus\mathbb{Z}/12\mathbb{Z}, \quad \mathbb{Z}/4\mathbb{Z}\oplus\mathbb{Z}/8\mathbb{Z},$$
$$\mathbb{Z}/4\mathbb{Z}\oplus\mathbb{Z}/16\mathbb{Z}, \quad \mathbb{Z}/8\mathbb{Z}\oplus\mathbb{Z}/8\mathbb{Z}.$$

Proof. Both $X_1(15)$ and $X_1(2,12)$ are elliptic curves whose models can be found in [77]. A computation in `Magma` shows that $X_1(15)(\mathbb{Q}(\zeta_{16})) = X_1(15)(\mathbb{Q})$. Therefore, since $\mathbb{Z}/15\mathbb{Z}$ is not a possible torsion subgroup over $\mathbb{Q}$ by Theorem 1.1.9, it also cannot appear over $\mathbb{Q}(\zeta_{16})$.

A computation in `Magma` shows that $X_1(2,12)(\mathbb{Q}(\zeta_{16})) = X_1(2,12)(\mathbb{Q}(i))$. It was proved in [69, Lemma 7] that $\mathbb{Z}/2\mathbb{Z}\oplus\mathbb{Z}/12\mathbb{Z}$ does not appear as a torsion subgroup of $E/\mathbb{Q}$ over $\mathbb{Q}(i)$. Therefore, it also cannot appear over $\mathbb{Q}(\zeta_{16})$. This also covers the case $\mathbb{Z}/4\mathbb{Z}\oplus\mathbb{Z}/12\mathbb{Z}$.

Now consider the modular curve $X_1(4,8)$ which is isomorphic (over $\mathbb{Q}(i)$) to the elliptic curve with LMFDB label 32.a3 by [70, Lemma 13.]. A computation in `Magma` shows that $X_1(4,8)(\mathbb{Q}(\zeta_{16})) = X_1(4,8)(\mathbb{Q}(\zeta_8))$, which contains only cusps, see [16, p. 12]. This also covers the cases $\mathbb{Z}/8\mathbb{Z}\oplus\mathbb{Z}/8\mathbb{Z}$ and $\mathbb{Z}/4\mathbb{Z}\oplus\mathbb{Z}/16\mathbb{Z}$. ■

The following lemma is a bit more complicated than the previous ones. The idea is to consider the modular curve $X_1(16)$, which is hyperelliptic of genus 2, and its Jacobian $J_1(16)$ over $\mathbb{Q}(\zeta_{16})$. The first goal is to show that $J_1(16)(\mathbb{Q}(\zeta_{16}))$ has rank 0. After that, we determine the torsion of $J_1(16)(\mathbb{Q}(\zeta_{16}))$ and consequently the points on $X_1(16)(\mathbb{Q}(\zeta_{16}))$, all of which turn out to be cusps.

Lemma 3.2.4. Let $E/\mathbb{Q}$ be an elliptic curve. Then $E(\mathbb{Q}(\zeta_{16}))_{tors}$ is not isomorphic to $\mathbb{Z}/16\mathbb{Z}$ or $\mathbb{Z}/2\mathbb{Z}\oplus\mathbb{Z}/16\mathbb{Z}$.

Proof. We consider the modular curve $X_1(16)(\mathbb{Q}(\zeta_{16}))$ with the model [77]:

$$y^2 = x(x^2+1)(x^2+2x-1)$$

and its Jacobian $J_1(16)(\mathbb{Q}(\zeta_{16}))$. We will demonstrate the use of standard methods for this type of problem by determining all the points on $X_1(16)(\mathbb{Q}(\zeta_{16}))$. A computation in

Magma shows that $\mathrm{rk}(J_1(16)(\mathbb{Q}(\zeta_{16}))) = 0$ with the help of Lemma 3.1.4:

$$\mathrm{rk}(J_1(16)(\mathbb{Q}(\zeta_8)(\sqrt{\zeta_8}))) = \mathrm{rk}(J_1(16)(\mathbb{Q}(\zeta_8))) + \mathrm{rk}(J_1^{\zeta_8}(16)(\mathbb{Q}(\zeta_8))) = 0.$$

Now we determine $J_1(16)(\mathbb{Q}(\zeta_{16}))_{tors}$. The rational prime $p = 17$ splits completely in $\mathbb{Q}(\zeta_{16})$ so by reducing modulo some prime $\mathfrak{p}$ of $\mathbb{Q}(\zeta_{16})$ that lies above p we get an injection due to Theorem 2.2.8:

$$red_{\mathfrak{p}} : J_1(16)(\mathbb{Q}(\zeta_{16}))_{tors} \to J_1(16)(\mathbb{F}_{17}).$$

A computation in Magma shows that $\#J_1(16)(\mathbb{F}_{17}) = 400$. Hence, $\#J_1(16)(\mathbb{Q}(\zeta_{16})) \leq 400$. By using the generators of the 2-torsion subgroup of $J_1(16)(\mathbb{Q}(\zeta_{16}))$ and some elements of $J_1(16)(\mathbb{Q}(\zeta_{16}))$ that we get from some known points on $X_1(16)(\mathbb{Q}(\zeta_{16}))$, we are able to generate a group with 400 elements. Therefore, we know exactly how $J_1(16)(\mathbb{Q}(\zeta_{16}))$ looks like:

$$J_1(16)(\mathbb{Q}(\zeta_{16})) \cong (\mathbb{Z}/2\mathbb{Z})^4 \oplus (\mathbb{Z}/5\mathbb{Z})^2.$$

Now we are able to determine all points on $X_1(16)(\mathbb{Q}(\zeta_{16}))$ by considering the Mumford representations of the elements of $J_1(16)(\mathbb{Q}(\zeta_{16}))$. We get that $\#X_1(16)(\mathbb{Q}(\zeta_{16})) = 14$ with all points being cusps. Therefore, we can conclude that there are no elliptic curves $E/\mathbb{Q}(\zeta_{16})$ (and consequently $E/\mathbb{Q}$) with a point of order 16 over $\mathbb{Q}(\zeta_{16})$. ■

We now do a similar procedure with $X_1(13)$.

Lemma 3.2.5. Let $E/\mathbb{Q}$ be an elliptic curve. Then $E(\mathbb{Q}(\zeta_{16}))_{tors}$ is not isomorphic to $\mathbb{Z}/13\mathbb{Z}$.

Proof. We consider the modular curve $X_1(13)(\mathbb{Q}(\zeta_{16}))$ and its Jacobian $J_1(13)(\mathbb{Q}(\zeta_{16}))$. The model for $X_1(13)$ can be found in [77]:

$$y^2 = x^6 + 4x^5 + 6x^4 + 2x^3 + x^2 + 2x + 1.$$

A computation in Magma shows that $\mathrm{rk}(J_1(13)(\mathbb{Q}(\zeta_{16}))) = 0$ with the help of Lemma 3.1.4:

$$\mathrm{rk}(J_1(13)(\mathbb{Q}(\zeta_{16}))) = \mathrm{rk}(J_1(13)(\mathbb{Q}(\zeta_8))) + \mathrm{rk}(J_1^{\zeta_8}(13)(\mathbb{Q}(\zeta_8))) = 0.$$

The next step is to determine $J_1(13)(\mathbb{Q}(\zeta_{16}))_{tors}$. We determine the 2-torsion subgroup, which turns out to be trivial. By using Theorem 2.2.8, we get that this reduction map is injective:

$$red_{\mathfrak{p}} : J_1(13)(\mathbb{Q}(\zeta_{16}))_{tors} \to J_1(13)(\mathbb{F}_{17}).$$

We also get that the rational prime $q = 41$ has inertia degree 2 in $\mathbb{Q}(\zeta_{16})$ so we have another injection:

$$red_{\mathfrak{q}} : J_1(13)(\mathbb{Q}(\zeta_{16}))_{tors} \to J_1(13)(\mathbb{F}_{41^2}).$$

We notice that $\gcd(\#J_1(13)(\mathbb{F}_{17}), \#J_1(13)(\mathbb{F}_{41^2})) = 76$, so $\#J_1(13)(\mathbb{Q}(\zeta_{16})) \mid 76$. Since the two torsion subgroup is trivial, we get that $\#J_1(13)(\mathbb{Q}(\zeta_{16})) \mid 19$. We can find a point of order 19 on our Jacobian. By checking the Mumford representations of all elements of $J_1(13)(\mathbb{Q}(\zeta_{16}))$, we find that all of the points on $J_1(13)(\mathbb{Q}(\zeta_{16}))$ come from cusps on $X_1(13)(\mathbb{Q}(\zeta_{16}))$ (and actually $X_1(13)(\mathbb{Q})$). Therefore, we can conclude that there are no elliptic curves $E/\mathbb{Q}(\zeta_{16})$ (and consequently $E/\mathbb{Q}$) such that $E(\mathbb{Q}(\zeta_{16}))_{tors} \cong \mathbb{Z}/13\mathbb{Z}$. ■

Now all the lemmas in this section give us the proof of Proposition 3.0.2.

3.3. TORSION GROWTH OVER $\mathbb{Q}(\zeta_{27})$

In this section we prove Proposition 3.0.3. Assume that $E/\mathbb{Q}$ is an elliptic curve and that $E(\mathbb{Q}(\zeta_{27}))_{tors} \cong \mathbb{Z}/m\mathbb{Z} \oplus \mathbb{Z}/mn\mathbb{Z}$. By Theorem 2.2.5 we have $\mathbb{Q}(\zeta_m) \subseteq \mathbb{Q}(\zeta_{27})$. By combining that with Theorem 3.1.8, it follows that $m \in \{1,2,3,6\}$. We first eliminate a certain amount of cyclic groups listed in Theorem 3.1.8 and one non-cyclic group.

Lemma 3.3.1. Let $E/\mathbb{Q}$ be an elliptic curve. Then $E(\mathbb{Q}(\zeta_{27}))_{tors}$ is not isomorphic to $\mathbb{Z}/n\mathbb{Z}$ if $n \in \{11,13,14,15,16,17,19,25,37,43,67,163\}$. Additionally, $E(\mathbb{Q}(\zeta_{27}))_{tors}$ is not isomorphic to $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/14\mathbb{Z}$.

Proof.

- If $n \in \{11,15,25\}$ and $P_n \in E(\mathbb{Q}(\zeta_{27}))$ is a point of order n, then by Lemma 3.1.5 we have $[\mathbb{Q}(P_n) : \mathbb{Q}] \mid 2$, which is impossible by Theorem 2.2.1.

- Assume $n = 13$ and let $P_{13} \in E(\mathbb{Q}(\zeta_{27}))$ be a point of order 13. By Lemma 3.1.5 we have $[\mathbb{Q}(P_{13}) : \mathbb{Q}] \mid 6$. Therefore, this torsion subgroup is defined over $\mathbb{Q}(\zeta_9)$. Theorem 2.2.1 tells us that this torsion subgroup cannot be defined over quadratic field. Therefore, it is defined over sextic or cubic field. Assume it is defined over sextic field (the entire $\mathbb{Q}(\zeta_9)$). Then we can use Lemma 3.1.3 to get:

$$\mathbb{Z}/13\mathbb{Z} \cong E(\mathbb{Q}(\zeta_9))_{(2')} \cong E(\mathbb{Q}(\zeta_9)^+)_{(2')} \oplus E^{-3}(\mathbb{Q}(\zeta_9)^+)_{(2')}.$$

  This means that either E or E^{-3} has torsion subgroup isomorphic to $\mathbb{Z}/13\mathbb{Z}$ defined over $\mathbb{Q}(\zeta_9)^+$. Now we will be finished if we prove that torsion subgroup $\mathbb{Z}/13\mathbb{Z}$ can't appear over $\mathbb{Q}(\zeta_9)^+$. To do this, we consider $X_1(13)(\mathbb{Q}(\zeta_9)^+)$. As before, we use `Magma` to determine that $X_1(13)(\mathbb{Q}(\zeta_9)^+) = X_1(13)(\mathbb{Q})$, which completes the proof.

- Now let $P_{14} \in E(\mathbb{Q}(\zeta_{27}))$ be a point of order 14 and assume that $E(\mathbb{Q}(\zeta_{27}))_{tors}$ is isomorphic to $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/14\mathbb{Z}$ or $\mathbb{Z}/14\mathbb{Z}$. By Lemma 3.1.5 it follows that $[\mathbb{Q}(2P_{14}) : \mathbb{Q}] \mid 6$, so $\mathbb{Q}(2P_{14})$ is contained in $\mathbb{Q}(\zeta_9)$. The point $7P_{14}$ of order 2 satisfies $[\mathbb{Q}(7P_{14}) : \mathbb{Q}] \in \{1,2,3\}$ by Proposition 2.2.6, which means that it is also contained in $\mathbb{Q}(\zeta_9)$. It follows that $P_{14} \in E(\mathbb{Q}(\zeta_9))$. Consider the modular curve $X_1(14)$. It is

an elliptic curve with the LMFDB label 14.a5. A computation in `Magma` [12] shows that $X_1(14)(\mathbb{Q}) = X_1(14)(\mathbb{Q}(\zeta_9))$, both only containing cuspidal points. Hence, there does not exist an elliptic curve over $\mathbb{Q}(\zeta_9)$ with a point of order 14 over $\mathbb{Q}(\zeta_9)$ and consequently over $\mathbb{Q}(\zeta_{27})$.

- Assume $n = 16$ and let $P_{16} \in E(\mathbb{Q}(\zeta_{27}))$ be a point of order 16. By Lemma 3.1.5 it follows that $[\mathbb{Q}(P_{16}) : \mathbb{Q}] \mid 2$, so $\mathbb{Q}(P_{16})$ is contained in $\mathbb{Q}(\sqrt{-3})$. Therefore, $E(\mathbb{Q}(\sqrt{-3}))_{tors} \cong \mathbb{Z}/16\mathbb{Z}$. That is impossible by [69, Lemma 12.].

- Assume that $n \in \{17, 37\}$ and that $P_n \in E(\mathbb{Q}(\zeta_{27}))$ is a point of order n. By [36, Theorem 5.8.] it follows that $[\mathbb{Q}(P_n) : \mathbb{Q}]$ is divisible by 4, but since $\mathbb{Q}(P_n) \subseteq \mathbb{Q}(\zeta_{27})$, this is impossible.

- Assume $n = 19$, then E has a $\mathbb{Q}$-rational 19-isogeny by Lemma 3.1.6. By [58, Table 4.] we have that $j(E) = -2^{15} \cdot 3^3$. The 19th division polynomial $\psi_{E,19}$ must have a root over $\mathbb{Q}(\zeta_{27})$. Using `Magma`, we check that this is not the case and therefore this is impossible.

- Assume that $n \in \{43, 67, 163\}$ and let $P_n \in E(\mathbb{Q}(\zeta_{27}))$ be a point of order n. By [58, Theorem 2.1] it follows that $[\mathbb{Q}(P_n) : \mathbb{Q}] \geq \frac{n-1}{2} > [\mathbb{Q}(\zeta_{27}) : \mathbb{Q}] = 18$, a contradiction.

■

We continue with examining the points of order 18.

Lemma 3.3.2. Let $E/\mathbb{Q}$ be an elliptic curve. Then $E(\mathbb{Q}(\zeta_{27}))_{tors}$ is not isomorphic to $\mathbb{Z}/18\mathbb{Z}$ or $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/18\mathbb{Z}$.

Proof. If $E(\mathbb{Q}(\zeta_{27}))_{tors} \cong \mathbb{Z}/18\mathbb{Z}$, then Lemma 3.1.5 directly gives us that this torsion subgroup is defined over a number field of degree 6 which can only be $\mathbb{Q}(\zeta_9)$.

If $E(\mathbb{Q}(\zeta_{27}))_{tors} \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/18\mathbb{Z}$, then Lemma 3.1.5 gives us that if $P_{18} \in E(\mathbb{Q}(\zeta_{27}))$ is a point of order 18, then $2P_{18}$ is defined over $\mathbb{Q}(\zeta_9)$. We know that $[\mathbb{Q}(E[2]) : \mathbb{Q}] \in \{1, 2, 3, 6\}$ by Proposition 2.2.7, but all unique subextensions of $\mathbb{Q}(\zeta_{27})$ of those degrees are contained in $\mathbb{Q}(\zeta_9)$, so again our torsion subgroup is defined over $\mathbb{Q}(\zeta_9)$ since $2P_{18}$ and $E[2]$ generate our torsion subgroup.

Now from Lemma 3.1.3 we get that

$$\mathbb{Z}/9\mathbb{Z} \cong E(\mathbb{Q}(\zeta_9))_{(2')} \cong E(\mathbb{Q}(\zeta_9)^+)_{(2')} \oplus E^{-3}(\mathbb{Q}(\zeta_9)^+)_{(2')}.$$

Therefore, one of $E(\mathbb{Q}(\zeta_9)^+)$ and $E^{-3}(\mathbb{Q}(\zeta_9)^+)$ has a point of order 9. Let $P_2 \in E(\mathbb{Q}(\zeta_9))$ be a point of order 2. If $[\mathbb{Q}(P_2) : \mathbb{Q}] \in \{1,3\}$, then P_2 is on $E(\mathbb{Q}(\zeta_9)^+)$ but also on $E^{-3}(\mathbb{Q}(\zeta_9)^+)$ because of Proposition 2.2.6. If $[\mathbb{Q}(P_2) : \mathbb{Q}] = 2$, then there is another point Q_2 of order 2 on E defined over $\mathbb{Q}$. In any case, both $E(\mathbb{Q}(\zeta_9)^+)$ and $E^{-3}(\mathbb{Q}(\zeta_9)^+)$ have a point of order 2. Finally, one of them has a point of order 18. However, it was proved in [54, Lemma 3.4.7.] that all the points on $X_1(18)(\mathbb{Q}(\zeta_9)^+)$ are cusps, which completes the proof. ■

Lemma 3.3.3. Let $E/\mathbb{Q}$ be an elliptic curve. Assume that $E(\mathbb{Q}(\zeta_{27}))_{tors} \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z}$. Then $n \in \{1,2,3,4\}$. Also, $E(\mathbb{Q}(\zeta_{27}))_{tors}$ is not isomorphic to $\mathbb{Z}/6\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}$.

Proof. From Theorem 3.1.8 it follows that $n \leq 9$. We have shown that $E(\mathbb{Q}(\zeta_{27}))$ cannot contain a point of order 18 in Lemma 3.3.2 so $n \leq 8$.

- Assume that $E(\mathbb{Q}(\zeta_{27}))_{tors} \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/10\mathbb{Z}$ and let $P_5 \in E(\mathbb{Q}(\zeta_{27}))$ be a point of order 5. It follows from Lemma 3.1.6 that E has a $\mathbb{Q}$-rational 5-isogeny. We have from Lemma 3.1.5 that $[\mathbb{Q}(P_5) : \mathbb{Q}] \mid 2$. Notice that P_5 and $E[2]$ generate our torsion subgroup $E(\mathbb{Q}(\zeta_{27}))_{tors}$. Now we will use Table 2.1 and analyze the possible images of $\rho_{E,2}$. Notice that Table 2.1 covers only non-CM curves, but for the mod 2 representation, the information is correct even if we include CM curves (see also [83, p. 6]). If $\rho_{E,2}$ is surjective, then $[\mathbb{Q}(E[2]) : \mathbb{Q}] = 6$ and the corresponding Galois group is not commutative by Proposition 2.2.7, which is a contradiction. If $Im(\rho_{E,2}) \subseteq B(2)$, then by Table 2.1 we see that $[\mathbb{Q}(E[2]) : \mathbb{Q}] \in \{1,2\}$. Therefore, $\mathbb{Q}(P_5)$ and $\mathbb{Q}(E[2])$ are two at most quadratic fields contained in $\mathbb{Q}(\zeta_{27})$. Since $\mathbb{Q}(\zeta_{27})$ has a unique quadratic subextension $F = \mathbb{Q}(\sqrt{-3})$ and no quartic subextensions, it follows that $E(\mathbb{Q}(\sqrt{-3}))_{tors} \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/10\mathbb{Z}$, which is impossible by [69, Theorem 2]. The only remaining option is $Im(\rho_{E,2}) = C_{ns}(2)$. It was proved in [45, Page 61] that an elliptic curve $E/\mathbb{Q}$ with a $\mathbb{Q}$-rational 5-isogeny and $Im(\rho_{E,2}) = C_{ns}(2)$ does not exist. Hence, this case is impossible.

- Assume that $E(\mathbb{Q}(\zeta_{27}))_{tors} \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/12\mathbb{Z}$ and let $P_{12} \in E(\mathbb{Q}(\zeta_{27}))$ be the point of order 12. We have by Lemma 3.1.5 that $[\mathbb{Q}(2P_{12}) : \mathbb{Q}] \mid 2$. We also have by Lemma 3.1.7 that $[\mathbb{Q}(3P_{12}) : \mathbb{Q}(6P_{12})] \mid 4$. Since $[\mathbb{Q}(6P_{12}) : \mathbb{Q}] \mid 2$, we have $[\mathbb{Q}(3P_{12}) : \mathbb{Q}] \mid 8$. Since $\mathbb{Q}(\zeta_{27})$ has a unique quadratic subfield and no quartic subfields, we conclude that $[\mathbb{Q}(P_{12}) : \mathbb{Q}] \mid 2$. We know that $[\mathbb{Q}(6P_{12}) : \mathbb{Q}] \mid 2$, so E has a point of order 2 defined over at most a quadratic field. Hence, $[\mathbb{Q}(E[2]) : \mathbb{Q}] \in \{1,2\}$ (see [83, p. 6]). Now we can conclude that $E(\mathbb{Q}(\sqrt{-3}))_{tors} \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/12\mathbb{Z}$, which is impossible by [69, Theorem 2].

- Assume that $E(\mathbb{Q}(\zeta_{27}))_{tors} \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/16\mathbb{Z}$ and let $P_{16} \in E(\mathbb{Q}(\zeta_{27}))$ be the point of order 16. We have by Lemma 3.1.5 that $[\mathbb{Q}(2P_{16}) : \mathbb{Q}] \mid 2$. We also have by Lemma 3.1.7 that $[\mathbb{Q}(P_{16}) : \mathbb{Q}(2P_{16})] \mid 4$. Since $\mathbb{Q}(\zeta_{27})$ has a unique quadratic subfield and no quartic subfields, we conclude that $[\mathbb{Q}(P_{16}) : \mathbb{Q}] \mid 2$. We know that $[\mathbb{Q}(8P_{16}) : \mathbb{Q}] \mid 2$, so E has a point of order 2 defined over at most a quadratic field. Hence, $[\mathbb{Q}(E[2]) : \mathbb{Q}] \in \{1,2\}$ (see [83, p. 6]). Now we can conclude that $E(\mathbb{Q}(\sqrt{-3}))_{tors} \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/16\mathbb{Z}$, which is impossible by Theorem 2.2.1.

- Assume that $E(\mathbb{Q}(\zeta_{27}))_{tors} \cong \mathbb{Z}/6\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}$. We can use [39, Theorem 1.1.] which tells us that $\mathrm{Gal}(\mathbb{Q}(E[6])/\mathbb{Q})$ is isomorphic to $(\mathbb{Z}/2\mathbb{Z})^2$ or to $(\mathbb{Z}/2\mathbb{Z})^3$. Since $\mathrm{Gal}(\mathbb{Q}(\zeta_{27})/\mathbb{Q})$ is cyclic, this is impossible.

■

Now all the lemmas in this section give us the proof of Proposition 3.0.3.

3.4. Torsion growth over $\mathbb{Q}(\zeta_5), \mathbb{Q}(\zeta_7)$ and $\mathbb{Q}(\zeta_{11})$

Notice that Proposition 3.0.4 follows directly from [16, Threorem 6], which eliminates all the candidate subgroups for which we did not find an example except $\mathbb{Z}/17\mathbb{Z}$, which we can exclude by using Theorem 2.2.3.

3.4.1. Proof of Proposition 3.0.6

Now we prove Proposition 3.0.6. If $E/\mathbb{Q}$ is an elliptic curve with $E(\mathbb{Q}(\zeta_{11}))_{tors} \cong \mathbb{Z}/m\mathbb{Z} \oplus \mathbb{Z}/mn\mathbb{Z}$, then $\mathbb{Q}(\zeta_m) \subseteq \mathbb{Q}(\zeta_{11})$ by Theorem 2.2.5, which means $m \in \{1,2,11\}$. By applying Theorem 3.1.8, we eliminate the possibility $m = 11$. Now we eliminate a lot of cyclic groups.

Lemma 3.4.1. Let $E/\mathbb{Q}$ be an elliptic curve. Then $E(\mathbb{Q}(\zeta_{11}))_{tors}$ is not isomorphic to $\mathbb{Z}/n\mathbb{Z}$ if $n \in \{13,14,15,17,18,19,21,27,37,43,67,163\}$.

Proof. Assume that $E(\mathbb{Q}(\zeta_{11}))_{tors} \cong \mathbb{Z}/n\mathbb{Z}$ for some n from the statement and let $P_n \in E(\mathbb{Q}(\zeta_{11}))$ be a point of order n. By Lemma 3.1.5 we have $[\mathbb{Q}(P_n) : \mathbb{Q}] \mid 2$, so our torsion subgroup is defined over $\mathbb{Q}(\sqrt{-11})$, but this is impossible by Theorem 2.2.1. ■

Next we eliminate most of the remaining candidates for $E(\mathbb{Q}(\zeta_{11}))_{tors}$.

Lemma 3.4.2. Let $E/\mathbb{Q}$ be an elliptic curve. Then $E(\mathbb{Q}(\zeta_{11}))_{tors}$ is not isomorphic to $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z}$ if $n \in \{7,8,9\}$.

Proof. Assume that $E(\mathbb{Q}(\zeta_{11}))_{tors} \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z}$ for $n \in \{7,9\}$ and let $P_n \in E(\mathbb{Q}(\zeta_{11}))$ be a point of order n. By Lemma 3.1.5 we have $[\mathbb{Q}(2P_n) : \mathbb{Q}] \mid 2$. We also have $[\mathbb{Q}(E[2]) : \mathbb{Q}] \in \{1,2\}$ by Proposition 2.2.7. Since $E[2]$ and $2P_n$ generate our torsion subgroup and $\mathbb{Q}(\zeta_{11})$ has one quadratic and no quartic subfields, we conclude that $E(\mathbb{Q}(\sqrt{-11}))_{tors} \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z}$, but that is impossible by Theorem 2.2.1.

Assume that $E(\mathbb{Q}(\zeta_{11}))_{tors} \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/16\mathbb{Z}$ and let $P_{16} \in E(\mathbb{Q}(\zeta_{11}))$ be a point of order 16. By Lemma 3.1.5 we have $[\mathbb{Q}(2P_{16}) : \mathbb{Q}] \mid 2$. By Lemma 3.1.7 we have $[\mathbb{Q}(P_{16}) : \mathbb{Q}(2P_{16})] \mid 4$. We also have $[\mathbb{Q}(E[2]) : \mathbb{Q}] \in \{1,2\}$ by Proposition 2.2.7. Since $E[2]$ and P_{16}

generate our torsion subgroup and $\mathbb{Q}(\zeta_{11})$ has only one quadratic and no quartic subfields, we conclude that $E(\mathbb{Q}(\sqrt{-11}))_{tors} \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/16\mathbb{Z}$, but that is impossible by Theorem 2.2.1. ■

There are only two groups left to eliminate for which we use the already described computational methods in `Magma` [12].

Lemma 3.4.3. Let $E/\mathbb{Q}$ be an elliptic curve. Then $E(\mathbb{Q}(\zeta_{11}))_{tors}$ is not isomorphic to $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/12\mathbb{Z}$ or $\mathbb{Z}/16\mathbb{Z}$.

Proof. Assume that $E(\mathbb{Q}(\zeta_{11}))_{tors} \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/12\mathbb{Z}$ and let $P_{12} \in E(\mathbb{Q}(\zeta_{11}))$ be a point of order 12. By Lemma 3.1.5 we have $[\mathbb{Q}(2P_{12}) : \mathbb{Q}] \mid 2$. By Lemma 3.1.7 we have $[\mathbb{Q}(3P_{12}) : \mathbb{Q}(6P_{12})] \mid 4$. We also have $[\mathbb{Q}(E[2]) : \mathbb{Q}] \in \{1,2\}$ by Proposition 2.2.7. Since $E[2]$, $2P_{12}$ and $3P_{12}$ generate our torsion subgroup and $\mathbb{Q}(\zeta_{11})$ has only one quadratic and no quartic subfields, we conclude that $E(\mathbb{Q}(\sqrt{-11}))_{tors} \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/12\mathbb{Z}$. Hence, E comes from a non-cuspidal point on $X_1(2,12)(\mathbb{Q}(\sqrt{-11}))$ which is an elliptic curve. A simple computation in `Magma` like before shows that $X_1(2,12)(\mathbb{Q}(\sqrt{-11})) = X_1(2,12)(\mathbb{Q})$ and $X_1(2,12)(\mathbb{Q})$ consists only of cusps. Hence, this is impossible.

Assume that $E(\mathbb{Q}(\zeta_{11}))_{tors} \cong \mathbb{Z}/16\mathbb{Z}$ and let $P_{16} \in E(\mathbb{Q}(\zeta_{11}))$ be a point of order 16. By Lemma 3.1.5 we have $[\mathbb{Q}(P_{16}) : \mathbb{Q}] \mid 2$. We conclude that $E(\mathbb{Q}(\sqrt{-11}))_{tors} \cong \mathbb{Z}/16\mathbb{Z}$. Hence, E comes from a non-cuspidal point on $X_1(16)(\mathbb{Q}(\sqrt{-11}))$. A simple computation in `Magma` like before shows that $X_1(16)(\mathbb{Q}(\sqrt{-11})) = X_1(16)(\mathbb{Q})$ and $X_1(16)(\mathbb{Q})$ consists only of cusps. Hence, this is impossible. ■

With that, the proof of Proposition 3.0.6 is complete.

3.4.2. Proof of Proposition 3.0.5

Now we prove Proposition 3.0.5. If $E/\mathbb{Q}$ is an elliptic curve and if $E(\mathbb{Q}(\zeta_7))_{tors} \cong \mathbb{Z}/m\mathbb{Z} \oplus \mathbb{Z}/mn\mathbb{Z}$, then $\mathbb{Q}(\zeta_m) \subseteq \mathbb{Q}(\zeta_7)$ by Theorem 2.2.5, which means $m \in \{1,2,7\}$. By applying Theorem 3.1.8, we eliminate the possibility $m = 7$. Now we eliminate a lot of cyclic groups.

Lemma 3.4.4. Let $E/\mathbb{Q}$ be an elliptic curve. Then $E(\mathbb{Q}(\zeta_7))_{tors}$ is not isomorphic to $\mathbb{Z}/n\mathbb{Z}$ if $n \in \{11, 15, 16, 17, 19, 21, 25, 27, 37, 43, 67, 163\}$.

Proof.

- Assume that $E(\mathbb{Q}(\zeta_7))_{tors} \cong \mathbb{Z}/n\mathbb{Z}$ for $n \in \{11, 15, 17, 25\}$ and let $P_n \in E(\mathbb{Q}(\zeta_7))$ be a point of order n. By Lemma 3.1.5 we have $[\mathbb{Q}(P_n) : \mathbb{Q}] \mid 2$ and now we get a contradiction from Theorem 2.2.1.

- Assume that $E(\mathbb{Q}(\zeta_7))_{tors} \cong \mathbb{Z}/n\mathbb{Z}$ for $n \in \{19, 37, 43, 67, 163\}$. From [36, Theorem 5.8.], we get that a point of order n can't be defined over the field $\mathbb{Q}(\zeta_7)$ (a degree 6 extension).

- Assume that $E(\mathbb{Q}(\zeta_7))_{tors} \cong \mathbb{Z}/27\mathbb{Z}$. This is impossible by [44, Theorem 1.1.].

- Assume that $E(\mathbb{Q}(\zeta_7))_{tors} \cong \mathbb{Z}/16\mathbb{Z}$ and let $P_{16} \in E(\mathbb{Q}(\zeta_7))$ be a point of order 16. By Lemma 3.1.5 we have $[\mathbb{Q}(P_{16}) : \mathbb{Q}] \mid 2$. That means that $P_{16} \in E(\mathbb{Q}(\sqrt{-7}))$. We can use similar methods in `Magma` as before to consider $X_1(16)(\mathbb{Q}(\sqrt{-7}))$ and show that it consists of cusps and therefore prove that $E/\mathbb{Q}$ can't have a point of order 16 defined over $\mathbb{Q}(\sqrt{-7})$.

- Assume that $E(\mathbb{Q}(\zeta_7))_{tors} \cong \mathbb{Z}/21\mathbb{Z}$. We conclude from Lemma 3.1.6 that E has a $\mathbb{Q}$-rational 21-isogeny. There are 4 elliptic curves (up to $\overline{\mathbb{Q}}$-isomorphism) with a rational 21-isogeny (see [9, p.78-80]). Therefore, we can use the division polynomial method. We will consider the seventh division polynomials $\psi_{E,7}$. We can use `Magma` [12] to factor those polynomials in the field $\mathbb{Q}(\zeta_7)$ and see that they have no zeroes there. Hence, the elliptic curves of interest can't have a point of order 7 defined over $\mathbb{Q}(\zeta_7)$ so this case is impossible.

■

It remains to eliminate only three non-cyclic groups.

Lemma 3.4.5. Let $E/\mathbb{Q}$ be an elliptic curve. Then $E(\mathbb{Q}(\zeta_7))_{tors}$ is not isomorphic to $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z}$ if $n \in \{5, 6, 8\}$.

Proof. Assume that $E(\mathbb{Q}(\zeta_7))_{tors} \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/16\mathbb{Z}$ and let $P_{16} \in E(\mathbb{Q}(\zeta_7))$ be a point of order 16. By Lemma 3.1.5 we have $[\mathbb{Q}(2P_{16}) : \mathbb{Q}] \mid 2$. By Lemma 3.1.7 we have $[\mathbb{Q}(P_{16}) : \mathbb{Q}(2P_{16})] \mid 4$. That means that $P_{16} \in E(\mathbb{Q}(\sqrt{-7}))$, which was shown to be impossible in the proof of Lemma 3.4.4.

Assume that $E(\mathbb{Q}(\zeta_7))_{tors} \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/12\mathbb{Z}$, then we can consider the elliptic curve $X_1(2,12)(\mathbb{Q}(\zeta_7))$ and use `Magma` like several times before to show that $X_1(2,12)(\mathbb{Q}(\zeta_7)) = X_1(2,12)(\mathbb{Q})$, which completes the proof since torsion subgroup $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/12\mathbb{Z}$ does not appear over $\mathbb{Q}$.

Assume that $E(\mathbb{Q}(\zeta_7))_{tors} \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/10\mathbb{Z}$ and let $P_5 \in E(\mathbb{Q}(\zeta_7))$ be the point of order 5. The proof in this case will be very similar to the proof of the same case in Lemma 3.3.3. It follows from Lemma 3.1.6 that E has a $\mathbb{Q}$-rational 5-isogeny. We have from Lemma 3.1.5 that $[\mathbb{Q}(P_5) : \mathbb{Q}] \mid 2$. Notice that P_5 and $E[2]$ generate our torsion subgroup $E(\mathbb{Q}(\zeta_7))_{tors}$. If $\rho_{E,2}$ is surjective, then $[\mathbb{Q}(E[2]) : \mathbb{Q}] = 6$ and the corresponding Galois group is not commutative by Proposition 2.2.7, which is a contradiction. If $Im(\rho_{E,2}) \subseteq B(2)$, then by Table 2.1 we see that $[\mathbb{Q}(E[2]) : \mathbb{Q}] \in \{1,2\}$. Hence, it follows that $E(\mathbb{Q}(\sqrt{-7}))_{tors} \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/10\mathbb{Z}$. This is impossible since we can easily use `Magma` to show that $X_1(2,10)(\mathbb{Q}) = X_1(2,10)(\mathbb{Q}(\sqrt{-7}))$ and they contain only cusps. The only remaining option is $Im(\rho_{E,2}) = C_{ns}(2)$. It was proved in [45, Page 61] that an elliptic curve $E/\mathbb{Q}$ with a $\mathbb{Q}$-rational 5-isogeny and $Im(\rho_{E,2}) = C_{ns}(2)$ does not exist. Hence, this case is impossible. ■

With that, the proof of Proposition 3.0.5 is complete.

4. ISOGENIES OVER QUADRATIC FIELDS OF ELLIPTIC CURVES WITH RATIONAL j-INVARIANT

In this chapter we determine the possible degrees of cyclic isogenies defined over quadratic fields for non-CM elliptic curves with rational j-invariant. This work is also documented in the paper [94] written by the author of this thesis. This work is motivated by the work of Najman [72] where Najman determined all the possible prime isogeny degrees of elliptic curves defined over number fields with rational j-invariants. His work covered the fields of degree up to 7 (and of any degree, assuming Serre's uniformity conjecture). The next natural step is to consider cyclic isogenies of composite degree. We will only cover quadratic fields, but it will be clear from the proofs that most of the techniques we will use could be adapted to extensions of higher degrees with some additional work. Our main result is the following:

Theorem 4.0.1. Let E be a non-CM elliptic curve with $j(E) \in \mathbb{Q}$. Assume E has a cyclic n-isogeny defined over a quadratic extension of $\mathbb{Q}$. Then $n \leq 18$ with $n \neq 14$ or $n \in \{20, 21, 24, 25, 32, 36, 37\}$.

The only new degrees not already arising for isogenies over $\mathbb{Q}$ are $20, 24, 32, 36$ for which we can respectively find examples by simply using LMFDB: 2178.5-c7, 90.1-f3, 45.1-a3, 28.2-a11. Performing the following steps will give us the proof of Theorem 4.0.1:

1. Show that if $p < q$ are primes dividing n, then $q \leq 5$ or $(p,q) \in \{(2,7),(3,7),(7,13)\}$.
2. Show that if p is a prime and $p^2 \mid n$, then $p \in \{2,3,5\}$.

3. Show that if $5^k \mid n$ or $3^k \mid n$, then $k \leq 2$.
4. Show that if $2^k \mid n$, then $k \leq 5$.
5. Show that if $n = 2^a 3^b$, then $n \in \{2,4,6,8,9,12,16,18,24,32,36\}$.
6. Show that if $n = 2^a 5^b$, then $n \in \{2,4,5,8,10,16,20,25,32\}$.
7. Show that if $n = 3^a 5^b$, then $n \in \{3,5,9,15,25\}$.
8. Show that $n \in \{14,30,63\}$ is impossible.
9. Show that $n = 91$ is impossible.

Notice that these steps are really sufficient. Assume we have completed them. If n has at least two prime divisors, then all prime divisors of n are in the set $\{2,3,5,7\}$. Notice that the pair $(p,q) = (7,13)$ is eliminated by eliminating $n = 91$. Notice that the pairs $(2,7)$ and $(5,7)$ are also impossible. Because of that, if n had at least three prime divisors, the only possible triplet would be 2, 3 and 5. However, $n = 30$ is impossible so n has only two prime divisors. If they correspond to pairs $(2,3)$, $(2,5)$ or $(3,5)$, those cases are handled. If they are $(3,7)$, then the prime 7 can appear only once in the factorization because $7^2 \nmid n$. Also, the prime 3 can only appear once because we have eliminated $n = 63$.

Now consider the case when n has only one prime divisor. If that prime is at least $p = 7$, then $n = p$, hence $n \in \{2,3,5,7,11,13,17,37\}$ by Theorem 2.2.11. Otherwise, $n \in \{2,3,4,5,8,9,16,25,32\}$. Therefore, the steps mentioned above really prove Theorem 4.0.1.

Some of these steps will be easy or will follow from some known results, others will be more involved. The code that verifies all the computation related to this work can be found on:

`https://github.com/brutalni-vux/IsogeniesQuadratic_PhD`.

4.1. Auxiliary results

Notice that it is enough to consider non-CM elliptic curves defined over $\mathbb{Q}$. Presence of a cyclic n-isogeny is invariant under quadratic twisting by Proposition 1.1.21. Hence, for

E/K (with K being a number field) with a K-rational cyclic n-isogeny we can descend from E/K to $E'/\mathbb{Q}$ via a quadratic twist and isomorphism over K with E' having a K-rational cyclic n-isogeny.

Definition 4.1.1. Let $E/\mathbb{Q}$ be an elliptic curve and C a finite cyclic subgroup of $E(\overline{\mathbb{Q}})$. The field $\mathbb{Q}(C)$ is defined as the smallest field whose absolute Galois group acts on C.

Notice that, by Theorem 1.1.17 and the comment after it, $\mathbb{Q}(C)$ is the field of definition of the unique cyclic isogeny with kernel C. In the remaining part of this section, we list several lemmas which we will use frequently.

Lemma 4.1.2 ([72, Proposition 3.1.]). Let $E/\mathbb{Q}$ be an elliptic curve and p a prime such that $\rho_{E,p}$ is surjective, and C a subgroup of $E[p]$ of order p. Then $[\mathbb{Q}(C):\mathbb{Q}] = p+1$.

Lemma 4.1.3 ([72, Lemma 3.2.]). Let $E/\mathbb{Q}$ be an elliptic curve over a number field and $P \in E[p]$. Let $C = \langle P \rangle$. Then $[\mathbb{Q}(P):\mathbb{Q}(C)]$ divides $p-1$.

Lemma 4.1.4 ([72, Proposition 3.3.]). Let $E/\mathbb{Q}$ be an elliptic curve and p a prime such that the image of $\rho_{E,p}$ is contained in the normalizer of the non-split Cartan subgroup and let $\langle P \rangle = C \subseteq E[p]$ a cyclic subgroup of order p. Then:

- If $p \equiv 1 \pmod 3$, then $[\mathbb{Q}(C):\mathbb{Q}] = p+1$.
- If $p \equiv 2 \pmod 3$, then $[\mathbb{Q}(C):\mathbb{Q}] \geq (p+1)/3$.

Definition 4.1.5. We say that the p-adic Galois representation $\rho_{E,p^\infty} : Gal(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{Z}_p)$ of E is defined modulo p^n if the image $\rho_{E,p^\infty}(Gal(\overline{\mathbb{Q}}/\mathbb{Q}))$ contains the kernel of the reduction map $\mathrm{GL}_2(\mathbb{Z}_p) \to \mathrm{GL}_2(\mathbb{Z}_p/p^n\mathbb{Z}_p)$. We also say that ρ_{E,p^∞} is of level p^n if n is the smallest integer such that ρ_{E,p^∞} is defined modulo p^n.

Notice that being defined modulo p^n is invariant under conjugation.

Lemma 4.1.6 ([24, Proposition 3.7.]). Let $E/\mathbb{Q}$ be an elliptic curve such that its p-adic representation is defined modulo p^{n-1} for some $n \geq 1$. Then for any cyclic subgroup C of $E(\overline{\mathbb{Q}})$ of order p^n, we have $[\mathbb{Q}(C):\mathbb{Q}(pC)] = p$.

First we will draw several conclusions from some known results. Assume a non-CM $E/\mathbb{Q}$ has a cyclic n-isogeny defined over a quadratic number field K and $p \mid n$. Then E has

a p-isogeny defined over K. Theorem 2.2.11 gives us that $p \in \{2,3,5,7,11,13,17,37\}$. We will first observe what happens when each of these possibilities for p divides n and give out some easy bounds for the degree of a p-isogeny which will follow easily from already mentioned lemmas.

4.1.1. Case $37 \mid n$:

We know from [98, Theorem 1.11] that $\rho_{E,37}$ is surjective, conjugate to a subgroup of $N_{ns}(37)$, or $j(E) \in \{-7\cdot 11^3, -7\cdot 137^3\cdot 2083^3\}$. Let C be the kernel of a 37-isogeny. If $\rho_{E,37}$ is surjective or conjugate to a subgroup of $N_{ns}(37)$, we have from Lemmas 4.1.2 and 4.1.4 respectively that $[\mathbb{Q}(C):\mathbb{Q}] \geq 38$. Otherwise, $j(E) \in \{-7\cdot 11^3, -7\cdot 137^3\cdot 2083^3\}$ and there is a 37-isogeny defined over $\mathbb{Q}$.

4.1.2. Case $17 \mid n$:

We know from [98, Theorem 1.11] that $\rho_{E,17}$ is surjective, conjugate to a subgroup of $N_{ns}(17)$, or $j(E) \in \{-17\cdot 373^3/2^{17}, -17^2\cdot 101^3/2\}$. Let C be the kernel of a 17-isogeny. If $\rho_{E,17}$ is surjective or conjugate to a subgroup of $N_{ns}(17)$, we have from Lemmas 4.1.2 and 4.1.4 respectively that $[\mathbb{Q}(C):\mathbb{Q}] \geq 6$. Otherwise, $j(E) \in \{-17\cdot 373^3/2^{17}, -17^2\cdot 101^3/2\}$ and there is a 17-isogeny defined over $\mathbb{Q}$.

4.1.3. Case $13 \mid n$:

We can use [98, Theorem 1.8] which tells us that the image of $\rho_{E,13}$ is surjective or conjugate to a subgroup of $B(13)$, $N_s(13)$, $N_{ns}(13)$ or to a subgroup of G_7, a group whose image in $\mathrm{PGL}_2(\mathbb{F}_{13})$ is isomorphic to S_4. Let C be the kernel of a 13-isogeny. If $\rho_{E,13}$ is surjective, we have $[\mathbb{Q}(C):\mathbb{Q}] = 14$ by Lemma 4.1.2. The possibilities $N_{ns}(13)$ and $N_s(13)$ for a non-CM $E/\mathbb{Q}$ have been eliminated by [4, Thoerem 1.1., Corollary 1.3.]. It was proved by [5, Section 5.1.] that the image of $\rho_{E,13}$ is conjugate to a subgroup of G_7 for only three possible j-invariants of E. Also, by [98, Theorem 1.8.], the image is exactly G_7 in those cases. If the image of $\rho_{E,13}$ is G_7, we can use Table 2.2 to see that if the image of $\rho_{E,13}$ is conjugate to G_7, then $[\mathbb{Q}(P):\mathbb{Q}] \geq 72$ for any P of order 13. By putting $C = \langle P\rangle$, we can use Lemma 4.1.3 to get: $[\mathbb{Q}(C):\mathbb{Q}] = \frac{[\mathbb{Q}(P):\mathbb{Q}]}{[\mathbb{Q}(P):\mathbb{Q}(C)]} \geq 6$. Otherwise,

the image of $\rho_{E,13}$ is conjugate to a subgroup of $B(13)$, so there is a 13-isogeny is defined over $\mathbb{Q}$. By [58, Table 3], we know that $j(E) = \frac{(h^2+5h+13)(h^4+7h^3+20h^2+19h+1)^3}{h}$ for some $h \in \mathbb{Q}$.

4.1.4. Case 11 | n :

We can use [98, Theorem 1.6] which tells us that the image of $\rho_{E,11}$ is surjective, conjugate to a subgroup of $B(11)$ or to a subgroup of $N_{ns}(11)$. Let C be the kernel of an 11-isogeny. If $\rho_{E,11}$ is surjective, we have $[\mathbb{Q}(C):\mathbb{Q}] = 12$ by Lemma 4.1.2. If the image of $\rho_{E,11}$ is conjugate to a subgroup of $N_{ns}(11)$, we can use Table 2.1 to see that in that case we have $[\mathbb{Q}(P):\mathbb{Q}] = 120$ for any P of order 11. By putting $C = \langle P \rangle$, we can use Lemma 4.1.3 to get: $[\mathbb{Q}(C):\mathbb{Q}] = \frac{[\mathbb{Q}(P):\mathbb{Q}]}{[\mathbb{Q}(P):\mathbb{Q}(C)]} \geq 12$. Otherwise, there is an 11-isogeny is defined over $\mathbb{Q}$, so by [58, Table 4], we know that $j(E) \in \{-11 \cdot 131^3, -11^2\}$.

4.1.5. Case 7 | n :

We can use [98, Theorem 1.5] which tells us that the image of $\rho_{E,7}$ is surjective, conjugate to a subgroup of $B(7)$, $N_{ns}(7)$ or $N_s(7)$. Let C be the kernel of a 7-isogeny. If the image of $\rho_{E,7}$ is surjective or conjugate to a subgroup of $N_{ns}(7)$, we can use Lemmas 4.1.2 and 4.1.4 respectively to get that $[\mathbb{Q}(C):\mathbb{Q}] \geq 8$. If the image of $\rho_{E,7}$ is conjugate to a subgroup of $N_s(7)$, then E has a cyclic 7-isogeny defined over a quadratic extension of $\mathbb{Q}$ by Lemma 2.2.12 since a split-Cartan subgroup has index 2 in its normalizer. Otherwise, there is a 7-isogeny defined over $\mathbb{Q}$, so by [58, Table 3], we know that $j(E) = \frac{(h^2+13h+49)(h^2+5h+1)^3}{h}$ for some $h \in \mathbb{Q}$.

4.1.6. Case 5 | n :

We can use [98, Theorem 1.4] which tells us that the image of $\rho_{E,5}$ is surjective, conjugate to a subgroup of $B(5)$, $N_{ns}(5)$, $N_s(5)$ or to a group G_9 which is a unique maximal subgroup of $\mathrm{GL}_2(\mathbb{F}_5)$ containing $N_s(5)$. Let C be the kernel of a 5-isogeny. If the image of $\rho_{E,5}$ is surjective, we can use Lemma 4.1.2 to get that $[\mathbb{Q}(C):\mathbb{Q}] = 6$. If $\rho_{E,5}$ is conjugate to a subgroup of $N_{ns}(5)$ or to G_9, we can use Table 2.1 to see that in those cases we have $[\mathbb{Q}(P):\mathbb{Q}] = 24$ for any P of order 5. By putting $C = \langle P \rangle$, we can use Lemma 4.1.3 to

get: $[\mathbb{Q}(C):\mathbb{Q}] = \frac{[\mathbb{Q}(P):\mathbb{Q}]}{[\mathbb{Q}(P):\mathbb{Q}(C)]} \geq 6$. If $\rho_{E,5}$ is conjugate to a subgroup of $N_s(5)$, then E has a cyclic 5-isogeny defined over a quadratic extension of $\mathbb{Q}$ by Lemma 2.2.12 since a split-Cartan subgroup has index 2 in its normalizer. Otherwise, E has a 5-isogeny defined over $\mathbb{Q}$. Hence, by [58, Table 3], we know that $j(E) = \frac{(h^2+10h+5)^3}{h}$ for some $h \in \mathbb{Q}$.

4.1.7. Case $3 \mid n$:

We can use [98, Theorem 1.2] which tells us that the image of $\rho_{E,3}$ is surjective or conjugate to a subgroup of $B(3)$, $N_{ns}(3)$ or $N_s(3)$. Let C be the kernel of a 3-isogeny. If the image of $\rho_{E,3}$ is surjective, we can use Lemma 4.1.2 to get that $[\mathbb{Q}(C):\mathbb{Q}] = 4$. If $\rho_{E,3}$ is conjugate to a subgroup of $N_{ns}(3)$, we can use Table 2.1 to see that in those cases we have $[\mathbb{Q}(P):\mathbb{Q}] = 8$ for any P of order 3. By putting $C = \langle P \rangle$, we can use Lemma 4.1.3 to get: $[\mathbb{Q}(C):\mathbb{Q}] = \frac{[\mathbb{Q}(P):\mathbb{Q}]}{[\mathbb{Q}(P):\mathbb{Q}(C)]} \geq 4$. We can also see from [98, Theorem 1.2] that if $\rho_{E,3}$ is not surjective, then either E has a 3-isogeny defined over $\mathbb{Q}$, or $j(E) = h^3$ for $h \in \mathbb{Q}$.

4.1.8. Case $2 \mid n$:

We can use [98, Theorem 1.1] to see that either $\rho_{E,2}$ is surjective, E has a 2-isogeny over $\mathbb{Q}$ or that $j(E) = h^2 + 1728$ for some $h \in \mathbb{Q}$. Notice that if $\rho_{E,2}$ is surjective, we can again use Lemma 4.1.2 to get that $[\mathbb{Q}(C):\mathbb{Q}] = 3$ for C a cyclic subgroup of $E[2]$ of order 2. Also notice that $[\mathbb{Q}(C):\mathbb{Q}] = 3$ when E does not have a 2-isogeny over $\mathbb{Q}$ by [98, Theorem 1.1].

4.2. TWO DIFFERENT PRIME DIVISORS OF THE ISOGENY DEGREE

In this section we will consider a situation when $E/\mathbb{Q}$ without CM has a cyclic n-isogeny defined over a quadratic extension of $\mathbb{Q}$ and n has at least two different prime divisors $p < q$. It is known that if we only consider the isogenies defined over $\mathbb{Q}$, then $(p,q) \in \{(2,3),(2,5),(3,5),(3,7)\}$. Notice that in the statement of the following lemma, we allow pairs $(2,7)$ and $(7,13)$ to potentially occur, but we will eliminate them in the later chapters.

Lemma 4.2.1. Let $E/\mathbb{Q}$ be a non-CM elliptic curve with a cyclic n-isogeny defined over a quadratic number field K. Assume that n has at least two different prime divisors p and q with $p < q$. Then all possible pairs (p,q) are the same ones as for $\mathbb{Q}$-rational isogenies plus the pairs $(2,7)$ and $(7,13)$.

Proof. Clearly, E has a p-isogeny and a q-isogeny over K. We will constantly be using the conclusions from Section 4.1.

Case $q = 37$: We know from Subsection 4.1.1 that $j(E) \in \{-7\cdot 11^3, -7\cdot 137^3\cdot 2083^3\}$ and there is a 37-isogeny defined over $\mathbb{Q}$. If $p = 17$, then we see from Subsection 4.1.2 that $j(E) \in \{-17\cdot 373^3/2^{17}, -17^2\cdot 101^3/2\}$, so this is impossible. If $p = 13$, then we see from Subsection 4.1.3 that we must have a 13-isogeny defined over $\mathbb{Q}$, so we have a 481-isogeny over $\mathbb{Q}$ by Lemma 2.2.10, but that is impossible. If $p = 11$, then we see from Subsection 4.1.4 that we must have a 11-isogeny defined over $\mathbb{Q}$, so we have a 143-isogeny over $\mathbb{Q}$ by Lemma 2.2.10, but that is impossible.

If $p = 7$, we see from Subsection 4.1.5 that either E has a 7-isogeny defined over $\mathbb{Q}$ or over a quadratic extension. From Subsection 4.1.5 we see that $j(E) = \frac{(h^2+13h+49)(h^2+5h+1)^3}{h}$ for some h in some (at most) quadratic extension of $\mathbb{Q}$. We match the above formula for j-invariant with the two possible j-invariants that allow a rational 37-isogeny and in both cases we get a polynomial over $\mathbb{Q}$ with no quadratic roots, so h can't be from a quadratic extension and this is impossible.

If $p = 5$, we can do the analogous computation as for $p = 7$. We have $j(E) = \frac{(h^2+10h+5)^3}{h}$ for some h inside some (at most) quadratic extension of $\mathbb{Q}$. We match the

j-invariants like before and again we always get a polynomial over $\mathbb{Q}$ with no quadratic roots, so h can't be from a quadratic extension of $\mathbb{Q}$.

If $p = 3$, then we see from Subsection 4.1.7 that either E has a 3-isogeny defined over $\mathbb{Q}$ or $j(E) = h^3$. If E had a 3-isogeny defined over $\mathbb{Q}$, it would have a 111-isogeny over $\mathbb{Q}$ by Lemma 2.2.10, which is impossible. The remaining option is that $j(E) = h^3$ for some $h \in \mathbb{Q}$, which can't match the j-invariants allowing a rational 37-isogeny.

If $p = 2$, then we see from Subsection 4.1.8 that either E has a 2-isogeny defined over $\mathbb{Q}$ or $j(E) = h^2 + 1728$. If E had a 2-isogeny defined over $\mathbb{Q}$, it would have a 74-isogeny over $\mathbb{Q}$ by Lemma 2.2.10, which is impossible. The remaining option is that $j(E) = h^2 + 1728$ for some $h \in \mathbb{Q}$, which can't match the j-invariants allowing a rational 37-isogeny.

Case $q = 17$: We know from Subsection 4.1.2 that $j(E) \in \{-17 \cdot 373^3/2^{17}, -17^2 \cdot 101^3/2\}$ and there is a 17-isogeny defined over $\mathbb{Q}$. If $p = 13$, then we see from Subsection 4.1.3 that we must have a 13-isogeny defined over $\mathbb{Q}$, so we have a 221-isogeny over $\mathbb{Q}$ by Lemma 2.2.10, but that is impossible. If $p = 11$, then we see from Subsection 4.1.3 that we must have a 11-isogeny defined over $\mathbb{Q}$, so we have a 187-isogeny over $\mathbb{Q}$ by Lemma 2.2.10, but that is impossible.

If $p = 7$, we see from Subsection 4.1.5 that either E has a 7-isogeny defined over $\mathbb{Q}$ or over a quadratic extension. That means that, by [58, Table 3], $j(E) = \frac{(h^2+13h+49)(h^2+5h+1)^3}{h}$ for some h in some (at most) quadratic extension of $\mathbb{Q}$. We match the above formula for j-invariant with the two possible j-invariants that allow a $\mathbb{Q}$-rational 17-isogeny and in both cases we get a polynomial over $\mathbb{Q}$ with no quadratic roots, so h can't be from a quadratic extension.

If $p = 5$, we can do the analogous computation as for $p = 7$. We have $j(E) = \frac{(h^2+10h+5)^3}{h}$ for some h inside some (at most) quadratic extension of $\mathbb{Q}$. We match the j-invariants like before and again we always get a polynomial over $\mathbb{Q}$ with no quadratic roots, so h can't be from a quadratic extension of $\mathbb{Q}$.

If $p = 3$, then we see from Subsection 4.1.7 that either E has a 3-isogeny defined over $\mathbb{Q}$ or $j(E) = h^3$. If E had a 3-isogeny defined over $\mathbb{Q}$, it would have a 51-isogeny over $\mathbb{Q}$, which is impossible. The remaining option is that $j(E) = h^3$ for some $h \in \mathbb{Q}$, which can't match the j-invariants allowing a rational 17-isogeny.

If $p = 2$, then we see from Subsection 4.1.8 that either E has a 2-isogeny defined over $\mathbb{Q}$ or $j(E) = h^2 + 1728$. If E had a 2-isogeny defined over $\mathbb{Q}$, it would have a 34-isogeny over $\mathbb{Q}$ by Lemma 2.2.10, which is impossible. The remaining option is that $j(E) = h^2 + 1728$ for some $h \in \mathbb{Q}$, which can't match the j-invariants allowing a rational 17-isogeny.

Case $q = 13$: We know from Subsection 4.1.3 that the 13-isogeny is defined over $\mathbb{Q}$ and that

$$j(E) = \frac{(h^2+5h+13)(h^4+7h^3+20h^2+19h+1)^3}{h}$$

for some $h \in \mathbb{Q}$. If $p = 11$, then we know from Subsection 4.1.4 that the 11-isogeny must be defined over $\mathbb{Q}$, so E has a 143-isogeny over $\mathbb{Q}$, a contradiction. If $p = 7$, then that case is more difficult and we will solve it in the later chapter, see Section 4.6.

If $p = 5$, then E has a 65-isogeny defined over a quadratic extension of $\mathbb{Q}$. We can use the result from [13, Section 4] about quadratic points on $X_0(65)$. The result states that all quadratic points on $X_0(65)$ are coming from $X_0(65)^+(\mathbb{Q})$ via a rational quotient map $\rho : X_0(65) \to X_0(65)^+$. Notice that $X_0(65)(\mathbb{Q})$ contains no non-cuspidal points by Theorem 1.1.19, so we can assume that E is represented by some quadratic, but not rational point Q on $X_0(65)$. If Q represents the pair (E,C), then $\rho(Q)$ is a rational point. That means that $\rho(Q) = \rho(Q)^\sigma = \rho(Q^\sigma)$. Hence, Q and Q^σ are paired up with w_{65} so $w_{65}(Q) = Q^\sigma$. Hence, $w_{65}(Q)$ represents a pair (E^σ, C'), where E and E^σ are 65-isogenous. Since E is defined over $\mathbb{Q}$, we have $E \cong E^\sigma$ and E is 65-isogenous to itself, hence it has CM, contradiction.

If $p = 3$, then we see from Subsection 4.1.7 that either E has a 3-isogeny defined over $\mathbb{Q}$ or $j(E) = h^3$. If E had a 3-isogeny defined over $\mathbb{Q}$, it would have a 39-isogeny over $\mathbb{Q}$, which is impossible. The remaining option is that $j(E) = h^3$ for some $h \in \mathbb{Q}$. We match that formula to the above formula for j-invariants allowing a rational 13-isogeny. We obtain a genus 2 curve with a Jacobian of rank 0. By using the built-in `Chabauty0()` function in `Magma` [12] which can provably compute rational points on a genus 2 rank 0 curve, we easily get that our curve has only one rational point at infinity which doesn't give us the desired elliptic curve. ■

If $p = 2$, then we see from Subsection 4.1.8 that either E has a 2-isogeny defined

over $\mathbb{Q}$ or $j(E) = h^2 + 1728$. If E had a 2-isogeny defined over $\mathbb{Q}$, it would have a 26-isogeny over $\mathbb{Q}$ by Lemma 2.2.10, which is impossible. The remaining option is that $j(E) = h^2 + 1728$ for some $h \in \mathbb{Q}$. We match that formula to the above formula for j-invariants allowing a rational 13-isogeny. This time we get a genus 1 curve which maps to the elliptic curve 52.a2 which has rank 0. By taking preimages of its rational points, we find that our curve has only one rational point at infinity which doesn't give us the desired elliptic curve.

Case $q = 11$: We know from Subsection 4.1.4 that the 11-isogeny is defined over $\mathbb{Q}$ and that $j(E) \in \{-11 \cdot 131^3, -11^2\}$. If $p = 7$, we see from Subsection 4.1.5 that $j(E) = \frac{(h^2+13h+49)(h^2+5h+1)^3}{h}$ for h in an (at most) quadratic extension of $\mathbb{Q}$. We again get a polynomial with no quadratic roots by matching that formula to the possible j-invariants allowing a rational 11-isogeny. Hence, this is impossible.

If $p = 5$, we see from Subsection 4.1.6 that $j(E) = \frac{(h^2+10h+5)^3}{h}$ for h in an (at most) quadratic extension of $\mathbb{Q}$. We again get a polynomial with no quadratic roots by matching that formula to the possible j-invariants allowing a rational 11-isogeny. Hence, this is impossible.

If $p = 3$, then we see from Subsection 4.1.7 that either E has a 3-isogeny defined over $\mathbb{Q}$ or $j(E) = h^3$ for $h \in \mathbb{Q}$. If E had a 3-isogeny defined over $\mathbb{Q}$, it would have a 33-isogeny over $\mathbb{Q}$ by Lemma 2.2.10, which is impossible. The remaining option is that $j(E) = h^3$ for some $h \in \mathbb{Q}$. We match that formula to the possible j-invariants allowing a rational 11-isogeny and we easily see that this case is impossible.

If $p = 2$, then we see from Subsection 4.1.8 that either E has a 2-isogeny defined over $\mathbb{Q}$ or $j(E) = h^2 + 1728$. If E had a 2-isogeny defined over $\mathbb{Q}$, it would have a 22-isogeny over $\mathbb{Q}$ by Lemma 2.2.10, which is impossible. The remaining option is that $j(E) = h^2 + 1728$ for some $h \in \mathbb{Q}$. We match that formula to the possible j-invariants allowing a rational 11-isogeny and we easily see that this case is impossible.

Case $q = 7$: The only situation we have to eliminate here is $p = 5$. If $p = 5$, we can use a similar argument as in the case $(p, q) = (5, 13)$. We use the result from [15, Table 9]: there is only one exceptional quadratic point on $X_0(35)$ and it corresponds to a CM curve. Therefore, all other quadratic points on $X_0(35)$ come from $X_0^+(35)(\mathbb{Q})$ (non-exceptional points). There are no non-cuspidal rational points on $X_0(35)$ by Theorem 1.1.19. By the

same argument as in the case $(p,q) = (5,13)$, any non-exceptional quadratic point P can be paired up with its Galois conjugate P^σ which is equal to $w_{35}(P)$. If P represented some E with a rational j-invariant, then $w_{35}(P)$ would represent E^σ which is 35-isogenous to E. Since $j(E) = j(E^\sigma)$, we have that E is 35-isogenous to itself, so it has CM, a contradiction. This completes the proof of Lemma 4.2.1.

4.3. NON-SQUAREFREE ISOGENY DEGREES

In this section we will consider a situation when $E/\mathbb{Q}$ without CM has an n-isogeny defined over a quadratic extension of $\mathbb{Q}$ and n is divisible by p^2 for some prime p. It is known that if we only consider the isogenies defined over $\mathbb{Q}$, then $p \in \{2,3,5\}$.

Proposition 4.3.1. Let $E/\mathbb{Q}$ be a non-CM elliptic curve with a cyclic n-isogeny defined over a quadratic number field K. Assume that $p^2 \mid n$ for some prime p. Then $p \in \{2,3,5\}$.

Proof. Clearly, E has a cyclic p^2-isogeny and a cyclic p-isogeny defined over K.

Assume $p > 7$. Then we know from Section 4.1 that our p-isogeny has to be defined over $\mathbb{Q}$. We can use [57, Theorem 3.9] to conclude that if E has a p-isogeny over $\mathbb{Q}$, then the image of ρ_{E,p^∞} contains a Sylow pro-p subgroup of $\mathrm{GL}_2(\mathbb{Z}_p)$.

Every Sylow pro-p subgroup of $\mathrm{GL}_2(\mathbb{Z}_p)$ is conjugate to this specific Sylow pro-p subgroup:

$$S = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(\mathbb{Z}_p) \mid a \equiv d \equiv 1 \pmod{p}, \quad c \equiv 0 \pmod{p} \right\}.$$

so we can choose compatible bases for all $E[p^k]$ such that the image of ρ_{E,p^∞} contains S. This means that p-adic representation ρ_{E,p^∞} is defined modulo p (see Definition 4.1.5). Now we can use Lemma 4.1.6 to conclude that for any cyclic subgroup C of $E(\overline{\mathbb{Q}})$ of order p^2, we have $[\mathbb{Q}(C) : \mathbb{Q}(pC)] = p$, so any p^2-isogeny has to be defined over a field of degree at least $p > 7$.

If $p = 7$ and E has a rational 7-isogeny, we can repeat the identical conclusions as above since the conditions of [57, Theorem 3.9] are again satisfied. Otherwise, we know from Subsection 4.1.5 that the image of $\rho_{E,7}$ is conjugate to a subgroup of $N_s(7)$. There are three such possible images, two of which only appear when $j(E) = 2268945/128$, according to [98, Theorem 1.5]. If we have $j(E) = 2268945/128$, we can use the classical modular polynomial $\Phi_N(X,Y)$. It is known from [47] that for a field F of characteristic not dividing N, a non-CM elliptic curve E/F has a cyclic N-isogeny if and only if $\Phi_N(X, j(E))$ has a zero in F. We can factor $\Phi_{49}(X, 2268945/128)$ into three irreducible factors of degrees 14, 14, 21 respectively. Therefore, a cyclic 49-isogeny is defined over a number field of degree (at least) 14.

The third and final possible image of $\rho_{E,7}$ is the whole $N_s(7)$. We use `Magma` [12] to check all subgroups of $\mathrm{GL}_2(\mathbb{Z}/49\mathbb{Z})$ and select only those which reduce modulo 7 to $N_s(7)$, all up to conjugation. There are 8 such subgroups of $\mathrm{GL}_2(\mathbb{Z}/49\mathbb{Z})$ up to conjugation. Call them H_i for $i \in \{1,2,\ldots,8\}$. By using [57, Theroem 3.16], we see that all H_i must contain all 7 scalars congruent to 1 modulo 7. This property is clearly not affected by conjugation. Here is some information about the subgroups H_i:

- The group H_1 is of order 72 and contains one scalar congruent to 1 modulo 7.
- The group H_2 is of order 504 and contains one scalar congruent to 1 modulo 7.
- The group H_3 is of order 504 and is conjugate to a subgroup of $N_s(49)$.
- The group H_4 is of order 3528 and contains one scalar congruent to 1 modulo 7.
- The group H_5 is of order 3528 and is conjugate to $N_s(49)$.
- The group H_6 is of order 24696 and contains one scalar congruent to 1 modulo 7.
- The group H_7 is of order 24696 and acts on the cyclic subgroups of $E[49]$ of order 49. The corresponding orbit lengths are 14 and 42, so a cyclic 49-isogeny is defined over the field of degree (at least) 14 by Lemma 2.2.14.
- The group H_8 is of order 172872 and acts on the cyclic subgroups of $E[49]$ of order 49. The corresponding orbit lengths are 14 and 42, so a cyclic 49-isogeny is defined over the field of degree (at least) 14 by Lemma 2.2.14.

The only subgroups we can't yet eliminate are those conjugate to some subgroup of $N_s(49)$ (H_3 and H_5). If there exists a non-CM elliptic curve over $\mathbb{Q}$ such that its mod 49 representation falls into that category, it will be represented by a point on $X_s(49)(\mathbb{Q})$ by Theorem 1.3.10. Recall that $X_s(n)$ is the modular curve associated to the normalizer of the split Cartan subgroup $N_s(n)$. We can, for example, use the comment from [75, p.3] which relies on [50] to recall that there is a $\mathbb{Q}$-isomorphism $X_s(N) \cong X_0(N^2)/w_{N^2} \equiv X_0^+(N^2)$, where w_{N^2} is the Atkin-Lehner involution. One can also look at [8, Section 2] for the modular interpretation of the aforementioned isomorphism to see that CM points and cusps on $X_s(p^r)$ correspond to CM points and cusps on $X_0^+(p^{2r})$ for a prime p. We

know from [66, Theorem 3.14] that $X_0^+(7^r)(\mathbb{Q})$ consists only of cusps and CM-points for $r \geq 3$. Since we were considering $X_s(7^2) \cong X_0(7^4)/w_{7^4} \equiv X_0^+(7^4)$, we are done. The cases $p \in \{2,3,5\}$ are already possible over $\mathbb{Q}$. Therefore, this completes the proof. ■

4.4. ISOGENIES OF PRIME POWER DEGREE

We will now consider cyclic isogenies of degree divisible by powers of primes 2, 3 and 5. They are the only primes that can occur more than once in the factorization of the degree of a cyclic isogeny over quadratic fields by Proposition 4.3.1.

4.4.1. Isogenies of degree 5^k

We will first consider isogenies of degree divisible by powers of 5. We will use the following theorem:

Theorem 4.4.1 ([40, Theorem 2])**.** Let $E/\mathbb{Q}$ be a non-CM elliptic curve with an isogeny of degree 5 defined over $\mathbb{Q}$. If no elliptic curve in the $\mathbb{Q}$-isogeny class of E has two independent isogenies of degree 5, then the image of $\rho_{E,5^\infty}$ contains a Sylow pro-5 subgroup of $\mathrm{GL}_2(\mathbb{Z}_5)$. Otherwise, the index $[\mathrm{GL}_2(\mathbb{Z}_5) : Im(\rho_{E,5^\infty})]$ is divisible by 5, but not by 25.

Here, the isogenies are considered *independent* if their kernels have trivial intersection. We first prove the following lemma which considers the situation when E has a rational 5-isogeny:

Lemma 4.4.2. Let $E/\mathbb{Q}$ be a non-CM elliptic curve with a cyclic n-isogeny defined over a number field K such that $5^k \mid n$ with $k \geq 2$. Assume E also has a 5-isogeny defined over $\mathbb{Q}$. Then $[K : \mathbb{Q}] \geq 5^{k-2}$.

Proof. Clearly, E has a cyclic 5^k-isogeny defined over K. If the $\mathbb{Q}$-isogeny class of E does not contain a curve with two independent 5-isogenies, we can use Theorem 4.4.1 to conclude that the image of $\rho_{E,5^\infty}$ contains a Sylow pro-5 subgroup of $\mathrm{GL}_2(\mathbb{Z}_5)$. We can conclude that $\rho_{E,5^\infty}$ is defined modulo 5 (similar as in Proposition 4.3.1), so we can use Lemma 4.1.6 to get that if C is a cyclic subgroup of $E(\overline{\mathbb{Q}})$ of order 5^k ($k \geq 2$), then $[\mathbb{Q}(C) : \mathbb{Q}(5C)] = 5$. Therefore, if the $\mathbb{Q}$-isogeny class of E does not contain a curve with two independent 5-isogenies, any cyclic 5^k-isogeny is defined over the number field of degree at least 5^{k-1} so $[K : \mathbb{Q}] \geq 5^{k-1}$.

Now assume that the $\mathbb{Q}$-isogeny class of E contains a curve E' with two independent 5-isogenies. Recall the fact that there is a cyclic isogeny $\phi : E \to E'$ of a unique degree d,

since they are non-CM curves (see [24, Lemma A.1.]). We consider two cases, depending on whether $5 \mid d$.

Case $5 \nmid d$: First we show that the images of $\rho_{E,5}$ and $\rho_{E',5}$ are the same, up to conjugation. Let $\{P,Q\}$ be a basis for $E[5]$. Then $\{\phi(P),\phi(Q)\}$ is a basis for $E'[5]$ since $5 \nmid d$ and ϕ is a homomorphism with no points of order 5 in its kernel. Notice that if $P^\sigma = aP + bQ$ for $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, then, since ϕ is defined over $\mathbb{Q}$, we have $\phi(P)^\sigma = \phi(P^\sigma) = a\phi(P) + b\phi(Q)$. We get the analogous result for Q so we get that $\rho_{E,5}(\sigma) = \rho_{E',5}(\sigma)$. Therefore, the images of $\rho_{E,5}$ and $\rho_{E',5}$ are the same, up to conjugation. By taking the generators of the kernels of two independent 5-isogenies as a basis for $E'[5]$, we get that $Im(\rho_{E',5})$, and hence $Im(\rho_{E,5})$, consists of diagonal matrices (up to conjugation). The subgroup of diagonal matrices in $\mathrm{GL}_2(\mathbb{Z}/5\mathbb{Z})$ has 16 elements, so $\#Im(\rho_{E,5}) \mid 16$. Let $\pi_5 : \mathrm{GL}_2(\mathbb{Z}_5) \to \mathrm{GL}_2(\mathbb{Z}/5\mathbb{Z})$ be the mod 5 reduction. We have from the first isomorphism theorem:

$$[Im(\rho_{E,5^\infty}) : Im(\rho_{E,5^\infty}) \cap ker(\pi_5)] = \#Im(\rho_{E,5}),$$
$$[\mathrm{GL}_2(\mathbb{Z}_5) : ker(\pi_5)] = \#\mathrm{GL}_2(\mathbb{Z}/5\mathbb{Z}) = 480.$$

We know that $Im(\rho_{E,5^\infty}) \cap ker(\pi_5)$ is of finite index in $Im(\rho_{E,5^\infty})$ and that $Im(\rho_{E,5^\infty})$ is of finite index in $\mathrm{GL}_2(\mathbb{Z}_5)$ due to Theorem 1.2.10 (Serre's open image theorem). Therefore, $Im(\rho_{E,5^\infty}) \cap ker(\pi_5)$ is of finite index in $\mathrm{GL}_2(\mathbb{Z}_5)$ and consequently in $ker(\pi_5)$ too. The group $ker(\pi_5)$ is a pro-5 group (see [10, p. 412]), so any of its subgroups of finite index has index which is a power of 5 (see [1, Theorem 1]). Now we have for some $m \geq 0$:

$$[\mathrm{GL}_2(\mathbb{Z}_5) : Im(\rho_{E,5^\infty}) \cap ker(\pi_5)] =$$
$$= [\mathrm{GL}_2(\mathbb{Z}_5) : ker(\pi_5)][ker(\pi_5) : Im(\rho_{E,5^\infty}) \cap ker(\pi_5)] = 480 \cdot 5^m.$$

We also have:

$$480 \cdot 5^m = [\mathrm{GL}_2(\mathbb{Z}_5) : Im(\rho_{E,5^\infty}) \cap ker(\pi_5)] =$$
$$= [\mathrm{GL}_2(\mathbb{Z}_5) : Im(\rho_{E,5^\infty})][Im(\rho_{E,5^\infty}) : Im(\rho_{E,5^\infty}) \cap ker(\pi_5)] =$$
$$= \#Im(\rho_{E,5}) \cdot [\mathrm{GL}_2(\mathbb{Z}_5) : Im(\rho_{E,5^\infty})].$$

We know that $\#Im(\rho_{E,5}) \mid 16$ and from Theorem 4.4.1 we know that $25 \nmid [\mathrm{GL}_2(\mathbb{Z}_5) : Im(\rho_{E,5^\infty})]$. Hence, $m = 0$, so $[ker(\pi_5) : Im(\rho_{E,5^\infty}) \cap ker(\pi_5)] = 5^m = 1$. Therefore,

$ker(\pi_5) \leq Im(\rho_{E,5^\infty})$. This means that $\rho_{E,5^\infty}$ is defined modulo 5. We can now use Lemma 4.1.6 like in the beginning of the proof and we get that cyclic 5^k-isogeny is defined over the number field of degree at least 5^{k-1} so $[K:\mathbb{Q}] \geq 5^{k-1}$.

Case $5 \mid d$**:** Our first step in this case is to compose ϕ with one of the two independent rational 5-isogenies on the curve E' such that the composition is still a cyclic isogeny. Assume $\{P,Q\}$ is a basis for $E[5]$ such that $\phi(P) = O_{E'}$. Then $\phi(Q) \neq O_{E'}$ since ϕ is cyclic. Also, $\phi(Q)$ is of order 5 since ϕ is a homomorphism. At least one of the two independent rational 5-isogenies of E' will not have $\phi(Q)$ in its kernel, call it α. Then the composition $\alpha \circ \phi$ will not have Q in its kernel. The kernel of $\alpha \circ \phi$ is of order $5d$ and since ϕ is cyclic, that kernel is isomorphic to either $\mathbb{Z}/5d\mathbb{Z}$ or $\mathbb{Z}/d\mathbb{Z} \oplus \mathbb{Z}/5\mathbb{Z}$. Since $5 \mid d$ and $Q \notin ker(\alpha \circ \phi)$, we have that $\alpha \circ \phi$ is cyclic of degree $5d$. Also notice that $\alpha \circ \phi$ is defined over $\mathbb{Q}$ and $25 \mid 5d$ so we must have $5d = 25$. This means that E has a cyclic 25-isogeny defined over $\mathbb{Q}$. Therefore, $Im(\rho_{E,25})$ consists of upper-triangular matrices (up to conjugation) by the discussion in Section 1.2. The subgroup of upper-triangluar matrices in $\mathrm{GL}_2(\mathbb{Z}/25\mathbb{Z})$ has 10000 elements, so $\#Im(\rho_{E,25}) \mid 2^4 \cdot 5^4$.

Now we proceed very similar to the case $5 \nmid d$. We set $\pi_{25} : \mathrm{GL}_2(\mathbb{Z}_5) \to \mathrm{GL}_2(\mathbb{Z}/25\mathbb{Z})$ to be the mod 25 reduction map. We have from the first isomorphism theorem:

$$[Im(\rho_{E,5^\infty}) : Im(\rho_{E,5^\infty}) \cap ker(\pi_{25})] = \#Im(\rho_{E,25}),$$
$$[\mathrm{GL}_2(\mathbb{Z}_5) : ker(\pi_{25})] = \#\mathrm{GL}_2(\mathbb{Z}/25\mathbb{Z}) = 5^4 \cdot 480.$$

We know that $Im(\rho_{E,5^\infty}) \cap ker(\pi_{25})$ is of finite index in $Im(\rho_{E,5^\infty})$ and that $Im(\rho_{E,5^\infty})$ is of finite index in $\mathrm{GL}_2(\mathbb{Z}_5)$ due to Theorem 1.2.10 (Serre's open image theorem). Therefore, $Im(\rho_{E,5^\infty}) \cap ker(\pi_{25})$ is of finite index in $\mathrm{GL}_2(\mathbb{Z}_5)$ and consequently in $ker(\pi_{25})$ too. The group $ker(\pi_{25})$ is a subgroup of $ker(\pi_5)$ of finite index equal to 5^4. That can be easily obtained by applying the first isomorphism theorem on the homomorphism $\pi_{25} : ker(\pi_5) \to \mathrm{GL}_2(\mathbb{Z}/25\mathbb{Z})$. Therefore, $Im(\rho_{E,5^\infty}) \cap ker(\pi_{25})$ is a subgroup of $ker(\pi_5)$ of finite index. Like before, $ker(\pi_5)$ is a pro-5 group and any its subgroup of finite index has index which is a power of 5 (see [1, Theorem 1]). Hence the index $[ker(\pi_{25}) : Im(\rho_{E,5^\infty}) \cap ker(\pi_{25})]$ is also a power of 5. Now we have for some $m \geq 0$:

$$[\mathrm{GL}_2(\mathbb{Z}_5) : Im(\rho_{E,5^\infty}) \cap ker(\pi_{25})] =$$
$$= [\mathrm{GL}_2(\mathbb{Z}_5) : ker(\pi_{25})][ker(\pi_{25}) : Im(\rho_{E,5^\infty}) \cap ker(\pi_{25})] = 5^4 \cdot 480 \cdot 5^m$$

We also have:

$$\begin{aligned}5^4 \cdot 480 \cdot 5^m &= [\mathrm{GL}_2(\mathbb{Z}_5) : Im(\rho_{E,5^\infty}) \cap ker(\pi_{25})] = \\ &= [\mathrm{GL}_2(\mathbb{Z}_5) : Im(\rho_{E,5^\infty})][Im(\rho_{E,5^\infty}) : Im(\rho_{E,5^\infty}) \cap ker(\pi_{25})] = \\ &= \#Im(\rho_{E,25}) \cdot [\mathrm{GL}_2(\mathbb{Z}_5) : Im(\rho_{E,5^\infty})].\end{aligned}$$

We know that $\#Im(\rho_{E,25}) \mid 2^4 \cdot 5^4$ and from Theorem 4.4.1 we know that $25 \nmid [\mathrm{GL}_2(\mathbb{Z}_5) : Im(\rho_{E,5^\infty})]$. Since $5^5 \mid 5^4 \cdot 480 \cdot 5^m$, we can conclude that $m = 0$, so we have $ker(\pi_{25}) \leq Im(\rho_{E,5^\infty})$ similar as before. This means that $\rho_{E,5^\infty}$ is defined modulo 25. We can now use Lemma 4.1.6 like before and we get that any cyclic 5^k-isogeny is defined over the number field of degree at least 5^{k-2} so $[K : \mathbb{Q}] \geq 5^{k-2}$. This completes the proof. ■

Next we consider the situation when E doesn't have a rational 5-isogeny.

Lemma 4.4.3. Let $E/\mathbb{Q}$ be a non-CM elliptic curve which doesn't have a 5-isogeny defined over $\mathbb{Q}$. Then any cyclic 25-isogeny of E is defined over a number field of degree at least 6.

Proof. We know from Subsection 4.1.6 that if the image of $\rho_{E,5}$ is surjective, conjugate to $N_{ns}(5)$ or to G_9 from [98, Theorem 1.4], then any 5-isogeny (and hence any cyclic 25-isogeny) is defined over a number field of degree at least 6. The only remaining possible images of $\rho_{E,5}$ such that E doesn't have a 5-isogeny defined over $\mathbb{Q}$ are $N_s(5)$ and one of its subgroups (G_3 from [98, Theorem 1.4]). We eliminate these using `Magma` [12] the same way we did in Proposition 4.3.1: we check all subgroups of $\mathrm{GL}_2(\mathbb{Z}/25\mathbb{Z})$ and select only those which reduce modulo 5 to $N_s(5)$ or G_3, all up to conjugation. Those are the possible images of $\rho_{E,25}$. Similarly to the proof of Proposition 4.3.1, for each possible subgroup $H \leq \mathrm{GL}_2(\mathbb{Z}/25\mathbb{Z})$, one of the following happens:

- The group H does not contain all scalars congruent to 1 modulo 5, a contradiction with [57, Theroem 3.16].
- The orbit lengths of cyclic subgroups of $E[25]$ of order 25 under the action of H are 10 and 20, so a cyclic 25-isogeny is defined over the number field of degree at least 10 by Lemma 2.2.14.

- The group H is conjugate to a subgroup of $N_s(25)$.

We can conclude that the last case is impossible by again using $X_s(5^2) \cong X_0^+(5^4)$ (via a $\mathbb{Q}$-isomorphism) and [66, Theroem 3.14] like in the end of the proof of Proposition 4.3.1. This tells us that all rational points on $X_0^+(5^4)$, and hence also on $X_s(5^2)$, are cusps or CM points. This completes the proof. ■

Clearly, these results are useful even if we consider not only quadratic fields, but also of number fields larger degree. Adapting them to our case of quadratic fields, we get the following proposition:

Proposition 4.4.4. Let $E/\mathbb{Q}$ be a non-CM elliptic curve with a cyclic n-isogeny defined over a quadratic number field K. Assume that $5^k \mid n$. Then $k \leq 2$.

Proof. This follows directly from Lemmas 4.4.2 and 4.4.3. ■

4.4.2. Isogenies of degree 3^k

We will now consider isogenies divisible by powers of 3. To begin, we will prove a simple group-theoretic Lemma to make later proofs easier:

Lemma 4.4.5. Let G be a group and H, L its subgroups such that $[G : L] \leq 2$. Then $[H : H \cap L] \leq 2$.

Proof. If $[G : L] = 1$ then $G = L$ and $[H : H \cap L] = [H : H] = 1$. The same holds if $H \leq L$. Now assume $[G : L] = 2$ and $H \nsubseteq L$. Then $L \trianglelefteq G$. We can use the second isomorphism theorem saying that $(HL)/L \cong H/(H \cap L)$. Since $H \nsubseteq L$ and there are only two L-cosets in G, we know that $HL = G$. Hence $H/(H \cap L) \cong G/L$, so $[H : H \cap L] \leq 2$. ■

First we consider the situation when E has a rational 3-isogeny.

Lemma 4.4.6. Let $E/\mathbb{Q}$ be a non-CM elliptic curve with a cyclic n-isogeny defined over a number field K such that $3^k \mid n$ with $k \geq 2$. Assume E also has a 3-isogeny defined over $\mathbb{Q}$. Then $[K : \mathbb{Q}] \geq 3^{k-2}$.

Proof. Clearly, E has a cyclic 3^k-isogeny defined over K. If E has a 3-isogeny defined over $\mathbb{Q}$, we can use the [78, Corollary 1.3.1.]. Notice that it tells us that $\langle Im(\rho_{E,3^\infty}), -I \rangle$

is of level at most 9, except for one case which we will solve later. For now assume $\langle Im(\rho_{E,3^\infty}), -I\rangle$ is of level at most 9. Let $\pi_9 : \mathrm{GL}_2(\mathbb{Z}_3) \to \mathrm{GL}_2(\mathbb{Z}/9\mathbb{Z})$ and $\pi_3 : \mathrm{GL}_2(\mathbb{Z}_3) \to \mathrm{GL}_2(\mathbb{Z}/3\mathbb{Z})$ be the mod 9 and mod 3 reductions. We have that $ker(\pi_9) \leq \langle Im(\rho_{E,3^\infty}), -I\rangle$. We can use Lemma 4.4.5 with $G := \langle Im(\rho_{E,3^\infty}), -I\rangle$, $H := ker(\pi_9)$, $L := Im(\rho_{E,3^\infty})$ to get that $[ker(\pi_9) : ker(\pi_9) \cap Im(\rho_{E,3^\infty})] \leq 2$. The group $ker(\pi_9)$ is a subgroup of $ker(\pi_3)$ of finite index equal to 3^4. That can be easily obtained by applying the first isomorphism theorem on the homomorphism $\pi_9 : ker(\pi_3) \to \mathrm{GL}_2(\mathbb{Z}/9\mathbb{Z})$. Hence $ker(\pi_9) \cap Im(\rho_{E,3^\infty})$ is a subgroup of $ker(\pi_3)$ of finite index. Since $ker(\pi_3)$ is a pro-3 group, any subgroup of finite index has index which is a power of 3 (see [1, Theorem 1]). Hence, $[ker(\pi_9) : ker(\pi_9) \cap Im(\rho_{E,3^\infty})] = 1$. Therefore, $ker(\pi_9) \leq Im(\rho_{E,3^\infty})$, so $\rho_{E,3^\infty}$ is defined modulo 9. Now we can use Lemma 4.1.6 to see that if E has a cyclic 3^k-isogeny defined over K for $k \geq 2$, then $[K : \mathbb{Q}] \geq 3^{k-2}$.

Recall that there is still one group of level 27 that $\langle Im(\rho_{E,3^\infty}), -I\rangle$ can be conjugate to. We can find its generators in [92, Table 1]. Either $Im(\rho_{E,3^\infty})$ contains $-I$ and is therefore equal to the mentioned group, or it is a subgroup of index 2 which doesn't contain $-I$. Using `Magma` [12], we see that orbit lengths of cyclic subgroups of $E[27]$ of order 27 are $3, 6, 27$ in all cases, so cyclic 27-isogeny is defined over the field of degree at least 3 by Lemma 2.2.14. Since $\rho_{E,3^\infty}$ is defined modulo 27 in this case, we can again use Lemma 4.1.6 and conclude that if K is the field of definition of some cyclic 3^k-isogeny with $k \geq 2$, we have $[K : \mathbb{Q}] \geq 3^{k-2}$. This completes the proof. ■

Now we consider the situation when E doesn't have a rational 3-isogeny.

Lemma 4.4.7. Let $E/\mathbb{Q}$ be a non-CM elliptic curve which doesn't have a 3-isogeny defined over $\mathbb{Q}$. Then a cyclic 9-isogeny of E is defined over a number field of degree at least 4.

Proof. We know from Subsection 4.1.7 that if $\rho_{E,3}$ is surjective or if its image is conjugate to $N_{ns}(3)$, then any 3-isogeny is defined over a number field of degree 4. Hence, any cyclic 9-isogeny is defined over a number field of degree at least 4 in those cases. The remaining option is that the image of $\rho_{E,3}$ is conjugate to $N_s(3)$ by [98, Theorem 1.2.]. In that case, 3-isogeny is defined over a number field of degree 2. We analyze this the same way we did for the similar situation with 5-isogeny and 7-isogeny. We consider all possible images

of $\rho_{E,9}$. Those are the subgroups of $\mathrm{GL}_2(\mathbb{Z}/9\mathbb{Z})$ that reduce to $N_s(3)$ modulo 3, up to conjugation. Using `Magma` [12], we see that there are 12 such subgroups: 8 of them have orbit lengths of cyclic subgroups of $E[9]$ of order 9 all equal to 6, so any cyclic 9-isogeny is defined over the number field of degree 6 in those cases by Lemma 2.2.14. The other 4 are conjugate to a subgroup of $N_s(9)$. We can conclude that these 4 subgroups can't appear by using [66, Theorem 3.14] like in the end of the proof of Proposition 4.3.1 and Lemma 4.4.3. ■

Combining these lemmas, we arrive at our desired result:

Proposition 4.4.8. Let $E/\mathbb{Q}$ be a non-CM elliptic curve with a cyclic n-isogeny defined over a quadratic number field K. Assume that $3^k \mid n$. Then $k \leq 2$.

Proof. This follows directly from Lemmas 4.4.6 and 4.4.7. ■

4.4.3. Isogenies of degree 2^k

We will now consider isogenies divisible by powers of 2. This part will be very easy since 2-adic representations are well understood.

Lemma 4.4.9. Let $E/\mathbb{Q}$ be a non-CM elliptic curve with a cyclic n-isogeny defined over a number field K such that $2^k \mid n$ with $k \geq 4$. Then $[K:\mathbb{Q}] \geq 2^{k-4}$. If K is quadratic, then $k \leq 5$.

Proof. Clearly E has a cyclic 2^k-isogeny defined over K. We know from [79, Corollary 1.3] that $\rho_{E,2^\infty}$ is defined modulo 32. We also know that a cyclic 32-isogeny can't be defined over $\mathbb{Q}$, so it is defined over at least a quadratic extension of $\mathbb{Q}$. We can now use Lemma 4.1.6 to conclude that $[K:\mathbb{Q}] \geq 2^{k-4}$. It is now easy to see that if K is a quadratic number field, then $k \leq 5$. ■

4.5. Isogenies of remaining composite degrees

Now we will eliminate the remaining cases, with the exception of a cyclic 91-isogeny which we handle in the last chapter.

4.5.1. Isogenies of degree $2^a \cdot 3^b$

We will now consider isogenies whose degree is of the form $2^a \cdot 3^b$. Clearly, we need to only consider $a, b \geq 1$ since the other cases are considered in the previous sections.

Lemma 4.5.1. Let $E/\mathbb{Q}$ be a non-CM elliptic curve with a cyclic n-isogeny defined over a quadratic number field K, where $n = 2^a 3^b$. Then $n \in \{2,4,6,8,9,12,16,18,24,32,36\}$.

Proof. We can use Proposition 4.4.8 to conclude that $b \leq 2$.

Case $b = 2$: Clearly, it is enough to show that $n = 72$ is impossible. This follows directly from [74, Table 8.13.].

Case $b = 1$: Clearly, it is enough to show that $n = 48$ is impossible. One can use [15, Table 15.] to see that the only exceptional quadratic points on $X_0(48)$ are CM points. All non-exceptional quadratic points are paired up via hyperelliptic involution induced by $\beta_{48} = \begin{pmatrix} -6 & 1 \\ -48 & 6 \end{pmatrix}$, see [15, Subsection 3.4]. We can also refer to [15, Subsection 3.4] to conclude that curves linked with this hyperelliptic involution are 12-isogenous. Therefore, if there was an elliptic curve defined over $\mathbb{Q}$ among the non-exceptional points, it would be 12-isogenous to its Galois conjugate (itself) since hyperelliptic involution and Galois conjugation act identically on the non-exceptional points. Therefore, it would have CM, which is a contradiction. The proof is now complete. ■

4.5.2. Isogenies of degree $2^a \cdot 5^b$

We will now consider isogenies whose degree is of the form $2^a \cdot 5^b$. Clearly, we need to only consider $a, b \geq 1$ since other cases are considered in the previous sections.

Lemma 4.5.2. Let $E/\mathbb{Q}$ be a non-CM elliptic curve with a cyclic n-isogeny defined over a quadratic number field K, where $n = 2^a5^b$. Then $n \in \{2,4,5,8,10,16,20,25,32\}$.

Proof. We can use Proposition 4.4.4 to conclude that $b \leq 2$.

Case $b = 2$: Clearly, it is enough to show that $n = 50$ is impossible. We will use [15, Table 16.]. We see from there that the only exceptional quadratic points on $X_0(50)$ are two CM points and four non-CM points which don't correspond to a rational j-invariant. Non-exceptional points come in pairs via hyperelliptic involution which is also the Atkin-Lehner involution w_{50}. Therefore, if there was an elliptic curve defined over $\mathbb{Q}$ among the non-exceptional points, it would be 50-isogenous to its Galois conjugate (itself) since hyperelliptic involution and Galois conjugation act identically on the non-exceptional points. Therefore, it would have CM, which is a contradiction. The proof is now complete.

Case $b = 1$: Clearly, it is enough to show that $n = 40$ is impossible. We can use [15, Table 11]. It tells us that all exceptional quadratic points on $X_0(40)$ correspond to CM-curves. The remaining quadratic points are non-exceptional points, so the hyperelliptic involution acts the same way on them as Galois conjugation. The hyperelliptic involution ι is induced by $\beta_{40} = \begin{pmatrix} -10 & 1 \\ -120 & 10 \end{pmatrix}$, see [15, Subsection 3.4]. We can refer to [15, Subsection 3.4] to conclude that curves linked with this hyperelliptic involution are 20-isogenous. Therefore, if there was an elliptic curve defined over $\mathbb{Q}$ among the non-exceptional points, it would be 20-isogenous to itself. Therefore, it would have CM, which is a contradiction.

■

4.5.3. Isogenies of degree $3^a \cdot 5^b$

We will now consider isogenies whose degree is of the form $3^a \cdot 5^b$. Clearly, we need to only consider $a, b \geq 1$ since other cases are considered in the above sections.

Lemma 4.5.3. Let $E/\mathbb{Q}$ be a non-CM elliptic curve with a cyclic n-isogeny defined over a quadratic number field K, where $n = 3^a5^b$. Then $n \in \{3,5,9,15,25\}$.

Proof. Clearly, it is enough to show that $n = 45$ and $n = 75$ are both impossible. This follows from [74, Tables 8.5., 8.14.]. The curve $X_0(45)$ has two quadratic CM points

and four quadratic non-CM points which don't give us a rational j-invariant. The curve $X_0(75)$ has no non-cuspidal, non-CM quadratic points. ■

4.5.4. Isogenies of degree $14, 30, 63$

Only a few more cases remain. We will now eliminate isogeny degrees 14, 30 and 63.

Lemma 4.5.4. Let $E/\mathbb{Q}$ be a non-CM elliptic curve with a cyclic n-isogeny defined over a quadratic number field K. Then $n \notin \{30, 63\}$.

Proof. To eliminate the option $n = 30$, we can use [15, Table 6.] to see that $X_0(30)$ has six exceptional quadratic points. Two of them are CM points and four are non-CM points which don't correspond to a rational j-invariant. The remaining quadratic points are non-exceptional points which come in pairs via hyperelliptic involution w_{15} and we can use the same argument as before to show that they can't correspond to a rational non-CM j-invariant.

To eliminate the option $n = 63$, we can use [74, Table 8.11.] to see that $X_0(63)$ has no non-CM non-cuspidal quadratic points.

■

Lemma 4.5.5. Let $E/\mathbb{Q}$ be a non-CM elliptic curve with a cyclic n-isogeny defined over a quadratic number field K. Then $n \neq 14$.

Proof. Notice that E can have a rational 14-isogeny, but then E has to be CM. If E didn't have a rational 2-isogeny, then any 2-isogeny would be defined over a number field of degree 3 (see Subsection 4.1.8), making it impossible for E to have a 14-isogeny defined over a quadratic number field. Hence, E has a rational 2-isogeny. This means that E must have a 7-isogeny defined over a quadratic number field, but not over $\mathbb{Q}$. By recalling Subsection 4.1.5, we see that the image of $\rho_{E,7}$ has to be a subgroup of $N_s(7)$. We can get the form for j-invariant of such curves from [98, Theorem 1.5.]. We match that form with the form of the j-invariants allowing a rational 2-isogeny from [58, Table 3]:

$$\frac{t(t+1)^3(t^2-5t+1)^3(t^2-5t+8)^3(t^4-5t^3+8t^2-7t+7)^3}{(t^3-4t^2+3t+1)^7} = \frac{(s+16)^3}{s}.$$

We get a genus 3 projective curve on which we want to find all the rational points. We map it to a curve which has a degree 2 quotient that is the elliptic curve 14.a5 with only

6 rational points. By taking the preimages, we find all the rational points on the starting curve, none of which give us a desired non-CM curve E. Those points are: $(2:-256:1), (-1:-16:1), (0:-16:1), (0:1:0), (1:0:0)$. The last two are cusps and other give us j-invariants 0 or 54000. That completes the proof. ■

4.6. ISOGENIES OF DEGREE 91

The advantage of the approach we took for 14-isogenies is the fact that we had to look for rational points on a curve of genus 3 instead of quadratic points on the curve $X_0(14)$ which has genus 1. The disadvantage is the fact that very often we will get a curve of much higher genus and looking for quadratic points on a curve of lower genus might be easier. This happens with 91-isogenies.

Method description

Our goal is to show that there are no elliptic curves $E/\mathbb{Q}$ with a cyclic 91-isogeny defined over a quadratic extension of $\mathbb{Q}$. We will determine all quadratic points on $X_0(91)$ up to those points that appear as pullbacks of rational points on $X_0^+(91)$ (non-exceptional points). We will see that all the exceptional points are either cusps or CM points. On the other hand, we can use the identical modular interpretation argument as several times before to show that if a non-exceptional point on $X_0(91)$ represents an E with a rational j-invariant, then E is 91-isogenous to itself so it has CM.

We will use the relative symmetric Chabauty developed by Siksek in [82] and used by Box in [13]. We will follow the approach and the implementation of Box and easily adapt it to $X_0(91)$. Notice that our problem for $X_0(91)$ is the same problem Box tackled. The Chabauty method and computations will be identical to Box's work and we will make some changes to the algorithm for getting the model of $X_0(91)$.

For some smooth, projective, non-hyperelliptic curve $X/\mathbb{Q}$, the method provides an easily computable criterion [13, Theorem 2.1.] for a point on $X^{(2)}(\mathbb{Q})$ to be the only point in its residue class modulo prime $p > 2$. Also, the method provides another easily computable criterion [13, Theorem 2.4.] for a point on $X^{(2)}(\mathbb{Q})$ to be the only point in its residue class modulo prime $p > 2$, up to points appearing as pullbacks of points on $C(\mathbb{Q})$, where C is a degree 2 quotient of X.

In our case, we have $X = X_0(91)$ and $C = X_0^+(91)$. We also need $\mathrm{rk}(J(X)) = \mathrm{rk}(J(C))$ for the method to work, which is true in our case as both ranks are 2. With this, we can easily find a subgroup $G \leq J_0(91)(\mathbb{Q})$ such that $2 \cdot J_0(91)(\mathbb{Q}) \leq G$, see [13, Proprosition 3.1.]. Also, the equality of ranks gives us an easy way of finding annihilating differentials,

see [13, Lemma 3.4.]. For a more detailed description of this method, see [73, Section 6] or Chapter 5 of this thesis. For the full description, see [13] or [14].

Computing the model, rank and torsion

To get the model of $X_0(91)$, we use the approach of Özman and Siksek [74, Section 3], but we use a different basis for the space $S_2(91)$ of weight 2 cuspforms of level 91. We choose a basis for $S_2(91)$ such that the matrix of w_{91} is diagonal with all the diagonal elements equal to 1 or -1 in that basis. This reduces the time needed to obtain the model and the resulting model has smaller coefficients. We remove the part in the Özman-Siksek code which computes a Gröbner basis since it is only used to potentially simplify the equations and didn't seem to give us noticeable gains. With these minor adjustments, we were able to obtain the model for $X_0(91)$ and the quotient $X_0^+(91)$ relatively quickly. To get the rank of $J_0(91)(\mathbb{Q})$, we can use the modular symbols package in `Magma` [12] developed by W. Stein in [86, 87] and also the Kolyvagin-Logachev theorem [53] identically as in [73, Proposition 5.1.] to get that $\mathrm{rk}(J_0(91)) = 2$.

Take an odd prime p of good reduction for $X_0(91)$. By Theorem 2.2.8, $J_0(91)(\mathbb{Q})_{tors}$ injects into $J_0(91)(\mathbb{F}_p)$. By doing this for primes 3, 5 and 19, we get that $\#J_0(91)(\mathbb{Q})_{tors} \leq 336$. By taking the differences of cusps of $X_0(91)$, we are able to generate a torsion subgroup isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/168\mathbb{Z}$. Hence, $J_0(91)(\mathbb{Q})_{tors} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/168\mathbb{Z}$.

Computations on quotient

We can easily compute the degree 2 quotient $X_0^+(91)$ in `Magma` [12] which is a genus 2 hyperelliptic curve. We can use Stoll's algorithm [88] to determine the generators of the free part of $J_0^+(91)(\mathbb{Q})$ which also has rank 2. By taking their pullbacks, we are able to generate a subgroup $G \leq J_0(91)(\mathbb{Q})$ such that $2 \cdot J_0(91)(\mathbb{Q}) \leq G$ (see [13, Proposition 3.1.]).

Finding some quadratic points

The curve $X_0(91)$ has 4 cusps which are defined over $\mathbb{Q}$. We can get 8 more Galois-conjugate pairs of quadratic points on $X_0(91)$ by taking pullbacks of the 10 known rational points on $X_0^+(91)$. We can get one more pair of Galois-conjugate quadratic points by

examining the fixed points of w_{91}. Notice that those points are CM points as they represent elliptic curves 91-isogenous to themselves.

Chabauty computations and finishing

With all that information, we are able to replicate the same method used by Box in [13] and to show that there are no other quadratic points on $X_0(91)$ apart from the known ones and the pullbacks of rational points on $X_0^+(91)$. All the exceptional (non-pullback) quadratic points on $X_0(91)$ are the four cusps and a pair of conjugate CM points. The remaining, non-exceptional quadratic points, are pullbacks of rational points on $X_0^+(91)$. Hence, w_{91} acts the same way on them as Galois conjugation. If some non-exceptional point represents an E with a rational j-invariant, we see that it is 91-isogenous to itself by a similar argument already used several times before (see, for example, Lemma 4.2.1, case $(p,q) = (5,13)$). Therefore, a non-CM $E/\mathbb{Q}$ can't have a cyclic 91-isogeny defined over a quadratic field. Also notice that all the rational points on $X_0^+(91)$ have been determined in [3, Example 7.1.], so we are also able to get all the quadratic points on $X_0(91)$.

Model and data for $X_0(91)$

Model for $X_0(91)$:

$$
\begin{aligned}
&x_0^2 - 12x_1x_2 + 4x_1x_4 - 14x_2^2 + 12x_2x_3 + 24x_2x_4 - 14x_3^2 + 16x_3x_4 - 23x_4^2 - x_5^2 - 4x_6^2 = 0,\\
&x_0x_1 - 6x_1x_2 + 6x_1x_4 - 3x_2^2 + 2x_2x_3 + 7x_2x_4 - 5x_3^2 + 8x_3x_4 - 7x_4^2 - x_5x_6 - x_6^2 = 0,\\
&x_0x_2 - 2x_1x_2 + x_1x_4 - 3x_2^2 + 6x_2x_3 + 4x_2x_4 - 5x_3^2 + 4x_3x_4 - 3x_4^2 - x_6^2 = 0,\\
&x_0x_3 - x_1x_2 + x_1x_4 + 2x_2x_3 - x_2x_4 - x_3^2 + x_3x_4 + x_4^2 = 0,\\
&x_0x_4 - x_2^2 + 2x_2x_3 - x_3^2 + 2x_4^2 = 0,\\
&x_0x_6 - x_1x_5 + x_2x_5 + x_4x_6 = 0,\\
&x_1^2 - 2x_1x_2 - 3x_2^2 + 4x_2x_3 + 4x_2x_4 - 4x_3^2 + 4x_3x_4 - 4x_4^2 - x_6^2 = 0,\\
&x_1x_3 - x_1x_4 - x_2^2 + x_2x_3 + x_2x_4 - x_3x_4 = 0,\\
&x_1x_6 - x_2x_5 + x_3x_5 = 0,\\
&x_2x_6 - x_3x_5 + x_4x_5 - x_4x_6 = 0.
\end{aligned}
$$

Genus of $X_0(91)$: 7.

Atkin-Lehner: $w_{91}(X_0 : X_1 : X_2 : X_3 : X_4 : X_5 : X_6) = (X_0 : X_1 : X_2 : X_3 : X_4 : -X_5 : -X_6)$.

Cusps: $(1:0:0:0:0:1:0), (-1:0:0:0:0:1:0), (2:0:-1:-1:-1:1:1), (-2:0:1:1:1:1:1)$.

$C = X_0^+(91)$: hyperelliptic curve $y^2 = x^6 + 2x^5 - x^4 - 8x^3 - x^2 + 2x + 1$.

Group structure of $J_0(91)(\mathbb{Q})$: $J_0(91)(\mathbb{Q}) \simeq \mathbb{Z} \oplus \mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/168\mathbb{Z}$.

The only quadratic points on $X_0(91)$ are cusps (which are all defined over $\mathbb{Q}$), pull-backs of rational points on $X_0^+(91)$ and a pair of CM points P, P^σ fixed by w_{91}, where:

$$P = \Big(\frac{-8\alpha+7}{5} : \frac{3\alpha-7}{5} : \frac{-\alpha+9}{5} : \alpha : 1 : 0 : 0\Big), \quad \alpha = \frac{17+5\sqrt{13}}{18}.$$

For the record, these are the non-cuspidal quadratic points on $X_0(91)$ which arise as pull-backs of rational points on $X_0^+(91)$ (up to Galois conjugation):

$$\begin{aligned}
P_1 &= \Big(\frac{-\sqrt{-3}}{3} : 0 : \frac{\sqrt{-3}}{3} : \frac{\sqrt{-3}}{3} : 0 : 1 : 1\Big),\\
P_2 &= \Big(\frac{-\sqrt{-3}}{3} : 0 : \frac{\sqrt{-3}}{3} : 0 : \frac{\sqrt{-3}}{3} : 0 : 1\Big),\\
P_3 &= \Big(\frac{-\sqrt{-3}}{3} : 0 : \frac{\sqrt{-3}}{3} : \frac{2\sqrt{-3}}{3} : \frac{\sqrt{-3}}{3} : 0 : 1\Big),\\
P_4 &= \Big(\frac{-2\sqrt{-3}}{3} : \frac{\sqrt{-3}}{3} : \frac{\sqrt{-3}}{3} : \frac{\sqrt{-3}}{3} : \frac{\sqrt{-3}}{3} : 1 : 0\Big),\\
P_5 &= \Big(\frac{-\sqrt{-3}}{9} : \frac{\sqrt{-3}}{6} : \frac{5\sqrt{-3}}{18} : \frac{\sqrt{-3}}{6} : \frac{-\sqrt{-3}}{18} : \frac{3}{2} : 1\Big),\\
P_6 &= \Big(\frac{-7\sqrt{-3}}{9} : \frac{2\sqrt{-3}}{3} : \frac{7\sqrt{-3}}{9} : \frac{5\sqrt{-3}}{9} : \frac{4\sqrt{-3}}{9} : 3 : 1\Big),\\
P_7 &= \Big(\frac{-31\sqrt{-87}}{174} : \frac{-3\sqrt{-87}}{87} : \frac{2\sqrt{-87}}{87} : \frac{4\sqrt{-87}}{87} : \frac{8\sqrt{-87}}{87} : \frac{3}{2} : 1\Big),\\
P_8 &= \Big(\frac{-14\sqrt{-87}}{87} : \frac{-12\sqrt{-87}}{87} : \frac{-7\sqrt{-87}}{87} : \frac{-3\sqrt{-87}}{87} : \frac{-\sqrt{-87}}{87} : 3 : 1\Big).
\end{aligned}$$

With that, we have achieved our goal and have proved Theorem 4.0.1.

5. QUADRATIC POINTS ON BIELLIPTIC CURVES

Definition 5.0.1. Let K be a number field and X/K a smooth projective curve. We say that X is bielliptic if it admits a map $b : X \to C$, where C is a curve of genus 1. We say that the map b is a bielliptic map.

As mentioned in Section 2.1, there has been some progress in our understanding of quadratic points on modular curves $X_0(n)$. Box [13] has described all the quadratic points on all $X_0(n)$ of genus $2 \leq g \leq 5$ with $\mathrm{rk}(J_0(n)(\mathbb{Q})) > 0$. Three of those curves are bielliptic, when $n \in \{43, 53, 61\}$. In those cases, the corresponding degree 2 quotients $X_0^+(n)$ are elliptic curves of positive rank. Let $b : X_0(n) \to X_0^+(n)$ be a bielliptic map. It turns out that all but finitely many quadratic points are in $b^{-1}(X_0^+(n)(\mathbb{Q}))$ and correspond to $\mathbb{Q}$-curves of degree n. These points are called *non-exceptional*, while the (finitely many) remaining points are called *exceptional*. One of the main tools Box uses, and one we will make abundant use of, is the relative symmetric Chabauty method.

Recall (or see [46]) that a curve $X/\mathbb{Q}$ and having a $\mathbb{Q}$-rational point can have infinitely many quadratic points if and only if it is of gonality at most 2 or if it is bielliptic with a bielliptic map $b_X : X \to E$ such that the elliptic curve E has positive rank over $\mathbb{Q}$. Since the quadratic points on all hyperelliptic curves $X_0(n)$ have already been described, the next logical step towards the problem of determining all the quadratic points on all $X_0(n)$ is to study the bielliptic curves $X_0(n)$. Exactly this has been posed as a Question by Mazur [59, Question 1 (iv)] at the workshop *Rational Points and Galois Representations* held in May 2021.

Bars [7] determined all the bielliptic modular curves $X_0(n)$ (there are 41 of them) and

those among them with infinitely many quadratic points (28 out of the 41 satisfy this). Since many of the bielliptic curves have genus $g \leq 5$, the quadratic points on all but 12 have already been described in the aforementioned papers [13, 16, 74]. In the table below we list the remaining values of n, their genus $g(X_0(n))$, and the rank $\mathrm{rk}(J_0(n)(\mathbb{Q}))$ of their Jacobian over $\mathbb{Q}$.

n	$g(X_0(n))$	$\mathrm{rk}(J_0(n)(\mathbb{Q}))$	n	$g(X_0(n))$	$\mathrm{rk}(J_0(n)(\mathbb{Q}))$
60	7	0	62	7	0
69	7	0	79	6	1
83	7	1	89	7	1
92	10	1	94	11	0
95	9	0	101	8	1
119	11	0	131	11	1

Table 5.1: The remaining curves

In this chapter we describe the quadratic points on all these modular curves, answering Mazur's question completely. Furthermore, as mentioned above, this also completes the description of quadratic points on all $X_0(n)$ with infinitely many quadratic points. We explicitly find all the exceptional points and show that they correspond to CM elliptic curves and show that the non-exceptional points correspond to $\mathbb{Q}$-curves of degree d_n for some $d_n \mid n$.

Although the approach for each of the modular curves is at least a bit different than for the others, our proofs can roughly be grouped into two main methods. The first method, described in Section 5.1, which allows us to solve the cases $n \in \{62, 69, 92, 94\}$, is to exploit the fact that for some of the n there is a divisor d of n such that $X_0(d)$ is hyperelliptic and hence any putative elliptic curve E with a cyclic n-isogeny (and hence a cyclic d-isogeny) over a quadratic field K, by the results of [16], has to either correspond to one of the explicitly known exceptional quadratic points on $X_0(d)$ (and we directly check whether they have a cyclic n-isogeny over the quadratic field they are defined over) or be a $\mathbb{Q}$-curve of degree d' for some divisor d' of d for which $w_{d'}$ is the hyperelliptic involution; in all our cases we have $\gcd(d', (n/d')) = 1$. In the latter case E has to be a $\mathbb{Q}$-curve which in addition has a cyclic (n/d')-isogeny defined over K. This leads to the question: is there

a modular curve whose points parametrize such elliptic curves? We give an answer to this question and show that such an elliptic curve either corresponds or is isogenous over K to an elliptic curve which corresponds to a $\mathbb{Q}$-rational point on one of 2 or 3 modular curves. The advantage of this method is that it requires very little explicit computation, as it is usually not too challenging to find all the rational points on the necessary modular curves.

The second method, used to deal with $n \in \{60, 79, 83, 89, 95, 101, 119, 131\}$ is, following Siksek [82] and Box [13], the relative symmetric Chabauty method. In principle what we do in these cases is very similar to [13], but there are a number of tweaks and minor improvements that we do to make the necessary computations, which have previously been done on curves of genus only up to 5, work on our curves, which are of genus $6 \leq g \leq 11$. Most notably, for $n = 131$ we modify the method so that it doesn't require a finite index subgroup of $X_0(131)$, which is a considerable improvement. We explain these cases in detail in the later sections.

The techniques used in the second method are applicable for general curves, not just modular curves. However, the information we have about cusps and automorphisms of modular curves does make some parts of the algorithms easier.

The work in this chapter is also documented in the paper by Najman and the author of this thesis [73]. The code that verifies all our computations, along with the outputs containing time and memory consumption in their last line, can be found on:

`https://github.com/brutalni-vux/QuadPtsBielliptic`.

All of our computations were performed on an Intel Xeon W-2133 CPU running at 3.60GHz and with 64 Gb of RAM.

5.1. $\mathbb{Q}$-CURVES

Recall that we have already defined the $\mathbb{Q}$-curves in Definition 1.1.22. Here, we will focus on $\mathbb{Q}$-curves over quadratic fields. Throughout this chapter, when saying that curves are isogenous, without mentioning over which field, we will always mean over $\overline{\mathbb{Q}}$. Let K be a quadratic field and σ the generator of $\mathrm{Gal}(K/\mathbb{Q})$. By factorising isogenies, we may assume our given isogeny $E \to E^\sigma$ is cyclic [24, Lemma A.1], and if this cyclic isogeny

$E \to E^\sigma$ is of degree d, we say that E is a $\mathbb{Q}$-*curve of degree* d. Throughout this section, for a positive integer m, by C_m we will denote a cyclic group of order m. Note that we allow $\mathbb{Q}$-curves to have complex multiplication.

Let n be a positive integer and factor $n = dm$ with $\gcd(d,m) = 1$. Notice that the non-cuspidal points on $X_0(n)$ represent triples (E, C_d, C_m) (see Theorem 1.3.7). Let L be a number field and let w_d be the Atkin-Lehner involution sending a non-cuspidal point $x \in X_0(n)(L)$, where x corresponds to (E, C_d, C_m), to the point $w_d(x)$, corresponding to $(E/C_d, E[d]/C_d, (C_m + C_d)/C_d)$. Here, quotienting out by C_d means mapping by the cyclic d-isogeny μ such that $\ker \mu = C_d$, i.e. $w_d(x) = (\mu(E), \mu(E[d]), \mu(C_m))$ (see Definition 1.3.15 and the discussion after it). Thus, non-cuspidal $\mathbb{Q}$-rational points on $X_0(n)/w_d$ correspond to unordered pairs

$$\{(E, C_d, C_m), (E/C_d, E[d]/C_d, (C_m + C_d)/C_d)\}$$

which are $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-invariant, meaning that either the point (E, C_d, C_m) is defined over $\mathbb{Q}$ or there exists a quadratic extension $K/\mathbb{Q}$ with σ generating $\mathrm{Gal}(K/\mathbb{Q})$ such that

$$(E, C_d, C_m)^\sigma = (E/C_d, E[d]/C_d, (C_m + C_d)/C_d), \tag{5.1}$$

implying that E is a $\mathbb{Q}$-curve of degree d with the additional property that $\mu(C_m) = C_m^\sigma$. We will say that an elliptic curve F *corresponds* to a point on $X_0(n)/w_d$ if there exists an E as above such that $j(F) = j(E)$ or $j(F) = j(\mu(E))$. In the case of $d = n$, the curve $X_0(n)/w_n$ is denoted by $X_0^+(n)$, as mentioned in Definition 1.3.15, and it parametrizes pairs consisting of a $\mathbb{Q}$-curve of degree n together with its Galois conjugate (without any further conditions). All the fixed points of w_d correspond to CM elliptic curves since they represent elliptic curves isogenous to themselves.

We emphasize that the equality in (5.1) is an equality of points on the modular curve $X_0(n)$, which is equivalent to the existence of an isomorphism $\phi : E^\sigma \to E/C_d$, defined over $\overline{\mathbb{Q}}$, sending C_d^σ to $E[d]/C_d$ and C_m^σ to $(C_m + C_d)/C_d$.

Let S_1 be a subgroup of E_1 and S_2 a subgroup of E_2, both cyclic of order n. We will say that these two subgroups are equal and write $S_1 = S_2$ if (E_1, S_1) and (E_2, S_2) correspond to the same point on $X_0(n)$, or equivalently, there exists an isomorphism $\phi : E_1 \to E_2$, defined over $\overline{\mathbb{Q}}$, such that $\phi(S_1) = S_2$. Similarly, throughout the section, we will write $E_1 = E_2$

if these two elliptic curves are isomorphic over $\overline{\mathbb{Q}}$, or equivalently, their j-invariants are equal.

We now consider the following problem: for any such m and d, describe a finite collection of modular curves Γ such that any $\mathbb{Q}$-curve of degree d over a quadratic field with an additional cyclic m-isogeny satisfying $(m,d)=1$ gives rise to a rational point on some member of Γ. Note that a somewhat similar problem is considered in [33, Proposition 2.2.]. The following propositions answer this question for m prime and $m=4$, which will be sufficient for our purposes.

Proposition 5.1.1. Let E be a non-CM $\mathbb{Q}$-curve of degree d defined over a quadratic field K having in addition a cyclic m-isogeny defined over K with $(m,d)=1$ and m prime. Then either E corresponds to a rational point on $X_0(dm)/w_d$ or is isogenous over K to an elliptic curve which corresponds to a rational point on $X_0^+(dm^2)$.

Proof. Suppose E/K is a $\mathbb{Q}$-curve of degree d, $C_d=\ker\mu$ where $\mu: E\to E^\sigma$ is a cyclic d-isogeny and C_m is a cyclic subgroup of order m of E defined over K. By [24, Lemma A.4], we may assume μ is defined over K and so (E,C_d,C_m) defines a non-cuspidal point on $X_0(dm)(K)$. Since E is a $\mathbb{Q}$-curve of degree d, we have $E^\sigma=E/C_d$ and $C_d^\sigma=E[d]/C_d$. Now there are two possibilities: either $\mu(C_m)=C_m^\sigma$ or $\mu(C_m)\neq C_m^\sigma$.

- Assume that $\mu(C_m)=C_m^\sigma$. In this case, by the discussion before the proposition, we see that E corresponds to a rational point on $X_0(dm)/w_d$.
- Assume that $\mu(C_m)\neq C_m^\sigma$. Denote by $E_1:=E/C_m$, by $E_2:=E^\sigma/(C_m)^\sigma$ and by $E_3:=E/(C_m+C_d)=E^\sigma/(\mu(C_m))$. As $\mu(C_m)\neq C_m^\sigma$, it follows that E_2 and E_3 are m^2-isogenous. Since E_1 and E_3 are d-isogenous, and by construction we have $E_1=E_2^\sigma$, it follows that E_1 is a $\mathbb{Q}$-curve of degree dm^2.

■

Proposition 5.1.2. Let E be a non-CM $\mathbb{Q}$-curve of odd degree d defined over a quadratic field K having in addition a cyclic 4-isogeny defined over K. Then either E or a curve isogenous over K to E corresponds to a rational point on $X_0^+(2d)$, $X_0^+(16d)$ or $X_0(4d)/w_d$.

Proof. Suppose E/K is a $\mathbb{Q}$-curve of degree d, $C_d=\ker\mu$ where $\mu: E\to E^\sigma$ is a d-isogeny and C_4 is a cyclic subgroup of order 4 of E defined over K. By [24, Lemma A.4],

we may assume μ is defined over K and so (E, C_d, C_4) defines a non-cuspidal point on $X_0(4d)(K)$.

- Assume that $\mu(C_4) = C_4^\sigma$. In this case, by the discussion before Proposition 5.1.1, we see that E corresponds to a rational point on $X_0(4d)/w_d$.

- Assume that $\mu(C_4) \cap C_4^\sigma = \{O\}$. Using the same arguments as in the $\mu(C_m) \neq C_m^\sigma$ case in Proposition 5.1.1, one proves that E is isogenous to an elliptic curve corresponding to a point on $X_0^+(16d)$.

- Assume that $\mu(C_4) \cap C_4^\sigma = 2(C_4)^\sigma = 2\mu(C_4)$. Let $E_1 = E/(2C_4)$; it is d-isogenous to E_1^σ and has all 3 of its subgroups of order 2 defined over K. Indeed, as μ is defined over K and of degree coprime to two, the subgroup of E^σ generated by $\mu(C_4)$ and C_4^σ is defined over K and isomorphic to $C_2 \times C_4$. The quotient of this latter group by the subgroup $\mu(C_4) \cap C_4^\sigma$ is isomorphic to $C_2 \times C_2$ and thus the 2-torsion of E_1^σ is defined over K. Finally, using again that μ is defined over K and has degree coprime to two, we find the same is true for E_1. One of the subgroups of $E_1[2]$ of order 2 is $E[2]/(2C_4)$. Call the other two S_1 and S_2. Since $\mu(C_4) \neq C_4^\sigma$, it follows that $S_1^\sigma = \mu(S_2)$ and $S_2^\sigma = \mu(S_1)$. It follows E_1/S_1 is $4d$-isogenous to $(E_1)^\sigma/(S_1)^\sigma = (E_1)^\sigma/\mu(S_2)$, and hence corresponds to a rational point on $X_0^+(4d)$.

■

5.2. RESULTS FOR $n \in \{62,69,92,94\}$.

We will use the following result of Momose, which we state in a weaker form, but is sufficient for our purposes.

Theorem 5.2.1 ([64, Theorem 0.1])**.** Let N be a composite number. If N has a prime divisor p such that $X_0(p)$ is of positive genus and such that $J_0(p)(\mathbb{Q})$ is finite, then $X_0^+(N)$ has no non-cuspidal non-CM $\mathbb{Q}$-rational points.

Our main result of this section is:

Theorem 5.2.2.

- If (E,C) is a non-cuspidal point on $X_0(62)(K)$, where K is a quadratic field, then $K = \mathbb{Q}(\sqrt{-3})$, and either $j(E) = 54000$ or $j(E) = 0$ and E has a point of order 2 over K.
- If (E,C) is a non-cuspidal point on $X_0(69)(K)$, where K is a quadratic field, then $j(E) = -2^{15}$ and $K = \mathbb{Q}(\sqrt{-11})$.
- If (E,C) is a non-cuspidal point on $X_0(92)(K)$, where K is a quadratic field, then $K = \mathbb{Q}(\sqrt{-7})$ and $j(E) = -3375$ or $j(E) = 16581375$.
- There are no non-cuspidal quadratic points on $X_0(94)$.

Proof. All the values n for which we consider the modular curves $X_0(n)$ are of the form $n = mp$, where $m = 2,3$ or 4 and $p = 23,31$ or 47. Let K be a quadratic field, (E,C) a K-rational non-cuspidal point on $X_0(n)$, where E/K is an elliptic curve and C is a $\mathrm{Gal}(\overline{K}/K)$-invariant cyclic subgroup of E of order n. It follows that $y = (E,mC)$ is a K-rational non-cuspidal point on $X_0(p)$. By the results of [16], we know that E is either a $\mathbb{Q}$-curve of degree p or y is one of the *exceptional* points listed in the appropriate table in [16].

For each of the exceptional points y listed in the appropriate table in [16] we construct an elliptic curve with j-invariant $j(y)$ and determine whether it admits an m-isogeny. For $m = 2$ this is done by checking whether the curve has a 2-torsion point and for $m = 3$ it is done by checking whether the division polynomial $\psi_{E,3}$ has a linear factor; this is a necessary and sufficient condition for the existence of a 3-isogeny. We obtain that for $n =$

69 this occurs if and only if $K = \mathbb{Q}(\sqrt{-11})$ and $j(y) = -2^{15}$, i.e. when the elliptic curve has complex multiplication by $\mathbb{Z}[\frac{1+\sqrt{-11}}{2}]$, and it does not occur for the exceptional points in the cases $n = 62$ and 94. In the remaining case $n = 92$ with $m = 4$, all computation can be avoided by noting that $(E, 2C)$ defines a non-cuspidal point on $X_0(46)(K)$, and hence E is necessarily a $\mathbb{Q}$-curve of degree 23 by [16, Table 13].

It remains to consider the non-exceptional points, which are $\mathbb{Q}$-curves of degree p. Suppose first that E does not have CM. Let first $n = 62, 69$ or 94. By Proposition 5.1.1, either E corresponds to a rational point on $X_0(n)/w_p$ or is isogenous to a non-CM elliptic curve corresponding to a rational point on $X_0^+(pm^2)$. The latter is impossible by Theorem 5.2.1. For $n = 92$, by Proposition 5.1.2 we obtain that an elliptic curve isogenous to E corresponds to a rational point on $X_0(92)/w_{23}$, $X_0^+(92)$ or $X_0^+(368)$, the last two again being impossible by Theorem 5.2.1. By [35], $X_0(69)/w_{23}$ is the elliptic curve 69.a2, $X_0(94)/w_{47}$ is the elliptic curve 94.a2 and $X_0(92)/w_{23}$ is the elliptic curve 92.b2. In the first two cases the elliptic curve has 2 rational points and in the final case it has 3 rational points, which is in all cases the same as the number of rational cusps. On the other hand, the curve $X := X_0(62)/w_{31}$ is, by [35], the elliptic curve 62.a4. It has 4 rational points, 2 of which are cusps, while the remaining two correspond to elliptic curves defined with j-invariant 54000 and 0, which give one point each. The pullbacks of both of these two non-cuspdial rational points on X, with respect to the quotient map $X_0(62) \to X$, are defined over $\mathbb{Q}(\sqrt{-3})$. Note that for elliptic curves with $j(E) = 0$ only those with a $\mathbb{Q}(\sqrt{-3})$-rational 2-torsion point correspond to a quadratic point on $X_0(62)$, i.e. the elliptic curves $y^2 = x^3 + d$ for which d is a cube in $\mathbb{Q}(\sqrt{-3})$.

It remains to check the existence of quadratic CM points on all the $X_0(n)$. From [20, Corollary 8.9.c)] we conclude that $X_0(n)$ has no CM points for $n = 94$. Using data provided by the authors of [20], which can be obtained using [20, Theorem 3.7], we find that the only quadratic CM points for the values n that we haven't already found are the ones with $j(E) = -3375$ or $j(E) = 16581375$ over $K = \mathbb{Q}(\sqrt{-7})$ for $n = 92$. ■

5.3. Obtaining models for $X_0(n)$ and their quotients

For the remaining values of n, it will be necessary to obtain models for $X_0(n)$ and their quotients by Atkin-Lehner involutions. We use the approach of Özman and Siksek [74, Section 3], but we use a different basis for the space $S_2(n)$ of weight 2, level n cuspforms.

We select an Atkin-Lehner operator w_d, with $d \mid n$ and $d > 1$, which we will be using to get the quotient $X_0(n)/w_d$. Then we choose a basis for $S_2(n)$ such that the matrix of w_d is diagonal with all the diagonal elements equal to 1 or -1 in that basis. This reduces the time needed to obtain a model for $X_0(n)$ and especially reduces the time needed to compute $C = X_0(n)/w_d$. A method to compute a model for C that will often work in our setting, i.e. when C is an elliptic curve, is to take the variables of $X_0(n)$ on which w_d acts non-trivially and compute relations between them. If we succeed in obtaining a model for C in this way, then the map $X_0(n) \to C$ is just the projection map.

We obtain the quotient map using this approach only for $n = 101$ as the default `Magma` function was fast enough for all other n, except for $n = 131$, where we use a different approach which avoids computing the quotient completely. In addition, the models we got using our basis had shorter equations and generally smaller coefficients.

We remove the part in the Özman-Siksek code which computes a Gröbner basis since it is only used to potentially simplify the equations and didn't seem to give us noticeable gains, while it made the computations considerably slower.

With these adjustments, we were able to obtain models for $X_0(n)$ and the quotients $X_0(n)/w_d$ quickly. For example, the computation of the model of $X_0(131)$ along with the quotient using the diagonal basis took 3.560 seconds. On the other hand, when using the basis of $S_2(n)$ that `Magma` returns by default, the computation of the model for $X_0(131)$ took 489.579 seconds and it was not possible to compute the quotient map in reasonable time. The files comparing those computations can be found in our code repository.

5.4. Determining the Mordell-Weil groups of $J_0(n)(\mathbb{Q})$

5.4.1. Determining the ranks

Here we will prove that the ranks of $J_0(n)(\mathbb{Q})$ for our values of n are as listed in Table 5.1. Some of that data is already known: all the Jacobians of $X_0(n)$ of rank 0 over $\mathbb{Q}$ are determined in [25, Theorem 3.1].

Proposition 5.4.1. The values of $\mathrm{rk}(J_0(n)(\mathbb{Q}))$ are as listed in Table 5.1.

Proof. We can use the modular symbols package in `Magma` developed by W. Stein in [86, 87]. See [83, Chapter 6] for more details and worked examples of this method for computing the ranks of modular Jacobians. If $L(\mathcal{A}_f,1)\neq 0$ for some representative f of some Galois orbit of Hecke eigenforms, the Kolyvagin-Logachev theorem [53] tells us that $\mathrm{rk}(\mathcal{A}_f(\mathbb{Q}))=0$. Furthermore, if $L(\mathcal{A}_f,1)=0$ for some representative f of some Galois orbit of Hecke eigenforms and the order of vanishing of $L(f,1)$ is 1, the Kolyvagin-Logachev theorem tells us that $\mathrm{rk}(\mathcal{A}_f)=[K_f:\mathbb{Q}]$, where K_f is the Hecke eigenvalue field of f, which is directly computed.

All our calculations fall into one of the two aforementioned categories and by summing all $\mathrm{rk}(\mathcal{A}_f)$ we get $\mathrm{rk}(J_0(n)(\mathbb{Q}))$ and check that the values in the Table 5.1 are correct. ■

5.4.2. Determining the torsion

Here we will describe the methods we used in our attempt to determine $J_0(n)(\mathbb{Q})_{tors}$ for the values of n from Table 5.1. For the prime values of n we will use the following result of Mazur:

Theorem 5.4.2 ([60, Theorem (1)])**.** For a prime number p, the number of elements in $J_0(p)(\mathbb{Q})_{tors}$ is equal to the numerator of $(p-1)/12$ in minimal form and $J_0(p)(\mathbb{Q})_{tors}$ is generated by the difference of two cusps.

Proposition 5.4.1 and Theorem 5.4.2 now determine the Mordell-Weil group of all $J_0(p)(\mathbb{Q})$ for prime $p \in \{79, 83, 89, 101, 131\}$.

Denote by $\mathcal{C}_n$ the subgroup of $J_0(n)$ generated by linear equivalence classes of differences of cusps. This subgroup is called the *cuspidal subgroup* of $J_0(n)$. The *rational cuspidal subgroup* is defined to be $\mathcal{C}_n(\mathbb{Q}) := \mathcal{C}_n \cap J_0(n)(\mathbb{Q})$. The Manin-Drinfeld theorem states that $\mathcal{C}_n(\mathbb{Q}) \subseteq J_0(n)(\mathbb{Q})_{tors}$. Ogg conjectured and Mazur proved (see Theorem 5.4.2) that $\mathcal{C}_n(\mathbb{Q}) = J_0(n)(\mathbb{Q})_{tors}$ for prime n. The *Generalized Ogg Conjecture*, which is still open, says that $\mathcal{C}_n(\mathbb{Q}) = J_0(n)(\mathbb{Q})_{tors}$ for all positive integers n. For a nice overview of the current status of the proven cases of the Generalized Ogg Conjecture, see [97].

For composite $n \in \{60, 95, 119\}$, we will use the fact that $J_0(n)(\mathbb{Q})_{tors}$ injects into $J_0(n)(\mathbb{F}_p)$ for an odd prime p of good reduction by Theorem 2.2.8.

Proposition 5.4.3. The following holds:

a) $J_0(60)(\mathbb{Q})_{tors} \cong \mathbb{Z}/4\mathbb{Z} \oplus (\mathbb{Z}/24\mathbb{Z})^3$,

b) $\mathbb{Z}/6\mathbb{Z} \oplus \mathbb{Z}/180\mathbb{Z} \leq J_0(95)(\mathbb{Q})_{tors} \leq (\mathbb{Z}/2\mathbb{Z})^2 \oplus \mathbb{Z}/6\mathbb{Z} \oplus \mathbb{Z}/180\mathbb{Z}$,

c) $J_0(119)(\mathbb{Q})_{tors} \cong \mathbb{Z}/8\mathbb{Z} \oplus \mathbb{Z}/288\mathbb{Z}$.

Remark 5.4.4. In b), by the Generalized Ogg Conjecture, we expect $J_0(95)(\mathbb{Q})_{tors}$ to be equal to the lower bound, but what we prove will already be good enough for our purposes.

Proof of Proposition 5.4.3. For $n = 60$ we use the code of Özman and Siksek from [74, Section 5] to get that rational cuspidal subgroup of $J_0(60)(\mathbb{Q})$ is isomorphic to $\mathbb{Z}/4\mathbb{Z} \oplus (\mathbb{Z}/24\mathbb{Z})^3$. We also get that $J_0(60)(\mathbb{Q})_{tors}$ is isomorphic either to $\mathbb{Z}/4\mathbb{Z} \oplus (\mathbb{Z}/24\mathbb{Z})^3$ or to $\mathbb{Z}/4\mathbb{Z} \oplus (\mathbb{Z}/24\mathbb{Z})^2 \oplus \mathbb{Z}/48\mathbb{Z}$. We then compute that $J_0(60)(\mathbb{F}_{23})$ doesn't have an element of order 48, so we must have $J_0(60)(\mathbb{Q})_{tors} \cong \mathbb{Z}/4\mathbb{Z} \oplus (\mathbb{Z}/24\mathbb{Z})^3$.

For n squarefree, every cusp of $X_0(n)$ is defined over $\mathbb{Q}$ by Theorem 1.3.9 (more generally the field of definition of the cusps can be determined using [56, Section 2] for any modular curve), in particular the rational cuspidal subgroup coincides with the full cuspidal subgroup.

For $n = 95$, we compute that the cuspidal group is isomorphic to $\mathbb{Z}/6\mathbb{Z} \oplus \mathbb{Z}/180\mathbb{Z}$, so clearly $\mathbb{Z}/6\mathbb{Z} \oplus \mathbb{Z}/180\mathbb{Z} \leq J_0(95)(\mathbb{Q})_{tors}$. We also get the following local information:

- $J_0(95)(\mathbb{F}_3) \cong (\mathbb{Z}/2\mathbb{Z})^2 \oplus \mathbb{Z}/60\mathbb{Z} \oplus \mathbb{Z}/180\mathbb{Z}$,
- $J_0(95)(\mathbb{F}_7) \cong (\mathbb{Z}/2\mathbb{Z})^5 \oplus \mathbb{Z}/18\mathbb{Z} \oplus \mathbb{Z}/90\mathbb{Z} \oplus \mathbb{Z}/900\mathbb{Z}$,
- $J_0(95)(\mathbb{F}_{11}) \cong \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/12\mathbb{Z} \oplus \mathbb{Z}/36\mathbb{Z} \oplus \mathbb{Z}/1658340\mathbb{Z}$.

Reduction modulo 7 tells us that $J_0(95)(\mathbb{Q})_{tors}$ can't have $(\mathbb{Z}/4\mathbb{Z})^2$ as a subgroup. Reduction modulo 11 tells us that $J_0(95)(\mathbb{Q})_{tors}$ can't have $(\mathbb{Z}/5\mathbb{Z})^2$ as a subgroup. Since we already know that $\mathbb{Z}/6\mathbb{Z} \oplus \mathbb{Z}/180\mathbb{Z} \leq J_0(95)(\mathbb{Q})_{tors}$, we can conclude that $J_0(95)(\mathbb{Q})_{tors} \leq (\mathbb{Z}/2\mathbb{Z})^2 \oplus \mathbb{Z}/6\mathbb{Z} \oplus \mathbb{Z}/180\mathbb{Z}$.

For $n = 119$, we compute $J_0(119)(\mathbb{F}_3)$ and $J_0(119)(\mathbb{F}_5)$ and we get that $J_0(119)(\mathbb{Q})_{tors}$ has at most $gcd(\#J_0(119)(\mathbb{F}_3), \#J_0(119)(\mathbb{F}_5)) = 2304$ elements. We can directly compute that differences of cusps generate a group isomorphic to $\mathbb{Z}/8\mathbb{Z} \oplus \mathbb{Z}/288\mathbb{Z}$, so we can conclude $J_0(119)(\mathbb{Q})_{tors} \cong \mathbb{Z}/8\mathbb{Z} \oplus \mathbb{Z}/288\mathbb{Z}$. ■

5.5. The Relative symmetric Chabauty method

Our main tools for determining quadratic points on $X_0(n)$ for $n \in \{60, 79, 83, 89, 95, 101, 119, 131\}$ are symmetric Chabauty and relative symmetric Chabauty combined with the Mordell-Weil sieve. We first define the annihilating differentials:

Definition 5.5.1. Let $X/\mathbb{Q}$ be a curve and $\Omega_{X/\mathbb{Q}_p}$ the space of differentials of X when X is considered over $\mathbb{Q}_p$. Coleman integration [22, 23] defines a bilinear pairing:

$$\Omega_{X/\mathbb{Q}_p} \times J(X)(\mathbb{Q}_p) \to \mathbb{Q}_p, \quad (\omega, \sum_i (P_i - Q_i)) \mapsto \sum_i \int_{P_i}^{Q_i} \omega.$$

The annihilator of $J(X)(\mathbb{Q})$ is called the space of annihilating differentials.

The survey article of McCallum and Poonen [62] is also a great source of information about Coleman integration and annihilating differentials.

We will be building upon the work of Box in [13], which in turns builds on the work of Siksek [82]. In [13, Theorem 2.1.] Box uses a directly computable criterion of Siksek for a known point of $X^{(2)}(\mathbb{Q})$ to be the only point in its residue class modulo a prime p of good reduction. However, there might be infinitely many quadratic points on X. This will indeed happen when we have a degree 2 map $X \to C$ and C has infinitely many rational points.

To circumvent this problem, Box [13, Theorem 2.4.], again building on work of Siksek [82], gives a directly computable criterion for a known point of $X^{(2)}(\mathbb{Q})$ to be the only point in its residue class modulo prime p of good reduction, *up to pullbacks* from $C(\mathbb{Q})$. One can then, if needed, combine the information acquired from the aforementioned two theorems for different values of p by using the Mordell-Weil sieve as described in [13, Section 2.5].

The input for Box's method is:

(a) a model for a non-hyperelliptic projective curve $X(\mathbb{Q})$,

(b) a set of known rational effective degree 2 divisors on X;

(c) a set Γ of matrices defining Atkin-Lehner operators on X such that $C = X/\Gamma$; in all our cases Γ will have only one element (not counting the identity),

(d) a set of degree 0 divisors that generate a subgroup G of $J(X)(\mathbb{Q})$ of finite index;

(e) an integer I such that $I \cdot J(X)(\mathbb{Q}) \subseteq G$;

(f) a degree 2 effective divisor D_{pull} on X that is a pullback of a rational point on C, used to embed $X^{(2)}$ into $J(X)$.

For Box's method to work, the following conditions need to be satisfied:

1. $\mathrm{rk}(J(X)(\mathbb{Q})) < g(X) - 1$,
2. $\mathrm{rk}(J(X)(\mathbb{Q})) = \mathrm{rk}(J(C)(\mathbb{Q}))$.

The first condition ensures that we can find at least two linearly independent annihilating differentials, see [13, Section 2.2.1]. The second condition ensures that we can find a suitable I in (e), see [13, Proposition 3.1.]. It also helps us in finding annihilating differentials, see [13, Lemma 3.4.]. Also notice that Box proved his results [13, Lemma 3.4. and Proposition 3.5.] for the values of n he considered, but it is clear that analogous proofs also work for all $n \in \{60, 79, 83, 89, 95, 101, 119, 131\}$ and for the Atkin-Lehner operators we will be using. Hence we can use the same method as Box for determining annihilating differentials.

For $Q \in X^{(2)}(\mathbb{Q})$, let ϕ be the map sending Q to $\phi(Q) = I \cdot [Q - D_{pull}] \in G$. For a $B \leq G$, $w \in G$, we call the set $w + B$ a B-coset represented by w. Suppose now that $Q \in X^{(2)}(\mathbb{Q})$ is some unknown point. We start with $B_0 \leq G$ and $W_0 \subseteq G$ which satisfy $\bigcup_{w \in W_0}(w + B_0) = G$, (e.g. in some instances we choose $B_0 := G, W_0 := \{0\}$), from which it follows that $\phi(Q) \in \bigcup_{w \in W_0}(w + B_0) = G$. In the i-th step, for $i \geq 1$, after applying Chabauty and the Mordell-Weil sieve using some prime p_i, we create a new subgroup $B_i \leq G$ and a set W_i of B_i-coset representatives, which satisfy $\phi(Q) \in \bigcup_{w \in W_i}(w + B_i)$. Using the information we obtained using Chabauty and the Mordell-Weil sieve, in each step we aim to shrink the set W_i, in the aim of getting $W_i = \emptyset$, which would prove that there are no unknown points and hence our known points are equal to $X^{(2)}(\mathbb{Q})$. For more details on how Chabauty and the Mordell-Weil sieve are applied see [13, Section 2] or the next section.

We apply and, when needed, modify Box's method to describe all quadratic points on $X_0(n)$ for $n \in \{60, 79, 83, 89, 95, 101, 119, 131\}$. For composite values of n, we use Box's method with only a small change in how the models of $X_0(n)$ are obtained, which made some of the computations considerably faster.

For prime values of $n < 131$, we will make some adjustments, described in the next section, that were already partially made in [14, Sections 3 and 4]. For $n = 131$, we will make one substantial adjustment, which we describe in Subsection 5.6.5.

5.6. METHODS AND COMPUTATIONS FOR $n \in \{60,79,83,89,95,101,119,131\}$

Here we describe the methods and computations for $n \in \{60,79,83,89,95,101,119,131\}$ which help us describe all quadratic points on those $X_0(n)$. For $n \in \{60,95,119\}$ we use Box's method as described in Section 5.5 and the computations successfully determine the quadratic points on those $X_0(n)$. Therefore, in the rest of this section we will be describing the methods used for $n \in \{79,83,89,101,131\}$. The changes that we make to the method from Section 5.5 will be based on Box's unpublished work on $X_0(79)$ and [14]. For prime values of n, using the same approach as in Section 5.5 does not give us the desired results because we never seem to be able to get $W_i = \emptyset$.

We improve on [13] and Box's unpublished work by using the improved algorithms to obtain "diagonal" (with respect to the action of w_d) models of $X_0(n)$, which makes our computations feasible, as explained in Section 5.3. Let $w_n' : J_0(n) \to J_0(n)$ be the map induced by w_n. For $n = 131$, we use a different operator $1 - w_n'$ for I, which seems to be a novel idea (I has usually been chosen to be multiplication by an integer).

Notice that for all these values of n we have $\mathrm{rk}(J_0(n)(\mathbb{Q})) = 1$ and we have a degree 2 quotient map $X_0(n) \to X_0^+(n)$, where $X_0^+(n)$ is an elliptic curve of rank 1. Since Box's unpublished `Magma` file for $X_0(79)$ and the methods of [14] work a bit differently than the method described in [13], we will first describe that method, which we will call here the "updated method" and then build upon it for larger values of n.

5.6.1. Description of the updated method

The notation and input are the same as in Section 5.5. Furthermore, for any object (point, divisor or divisor class) M we denote by $\widetilde{M}$ the reduction of that object modulo p; it will always be clear from the context which prime this is. Let X be a non-hyperelliptic curve of genus $g \geq 3$. For a prime $p > 2$ of good reduction for X, define the following mappings:

- $\iota : X^{(2)}(\mathbb{Q}) \to J(X)(\mathbb{Q})$, $\iota(P) = [P - D_{pull}]$;
- $\phi : X^{(2)}(\mathbb{Q}) \to G$, $\phi(P) = I \cdot [P - D_{pull}]$;

- $m : J(X)(\mathbb{Q}) \to G$, $m(A) = I \cdot A$;
- $red_p : J(X)(\mathbb{Q}) \to J(X)(\mathbb{F}_p)$, $red_p(A) = \widetilde{A}$;
- $h_p : G \to J(X)(\mathbb{F}_p)$, $h_p(A) = red_p(A) = \widetilde{A}$;
- $m_p : J(X)(\mathbb{F}_p) \to J(X)(\mathbb{F}_p)$, $m_p(\widetilde{A}) = I \cdot \widetilde{A}$;

Notice that the images of m and ϕ really are in G by (e). Also, ι is injective since X is not hyperelliptic by Proposition 1.3.31. These maps fit into a commutative diagram:

$$\begin{array}{ccc} X^{(2)}(\mathbb{Q}) & & \\ \downarrow{\scriptstyle \iota} & \searrow^{\phi} & \\ J(X)(\mathbb{Q}) & \xrightarrow{m} & G \\ \downarrow{\scriptstyle red_p} & & \downarrow{\scriptstyle h_p} \\ J(X)(\mathbb{F}_p) & \xrightarrow{m_p} & J(X)(\mathbb{F}_p). \end{array}$$

Assume there is some unknown point $Q \in X^{(2)}(\mathbb{Q})$. As mentioned before, in Box's original method, described in Section 5.5, the goal was to get that $\phi(Q) \in \emptyset$, a contradiction. Here we aim to either get the same result, or, if that is not possible, obtain some information about what Q has to look like (e.g. to get that Q is a pullback of a rational point on $X_0^+(n)$ in our case of $X := X_0(n)$). This additional information will allow us to solve the problem.

As in Section 5.5, in the i-th step we want to determine $B_i \leq G$ and $W_i \subseteq G$ such that $\phi(Q)$ is a member of some B_i-coset represented by some $w \in W_i$. We start with $i = 0$, $B_0 = G_{free}$ and $W_0 = G_{tors}$, where G_{free} is the free part of G and G_{tors} is the torsion subgroup of G. Clearly, $\phi(Q)$ is a member of some B_0-coset represented by some $w \in W_0$, since $G = \bigcup_{w \in W_0}(w + B_0)$.

Now take some prime $p := p_{i+1} > 2$ of good reduction for X. Assume we have determined B_i and W_i and now want to construct B_{i+1} and W_{i+1}. We set $B_{i+1} = B_i \cap \ker(h_p)$ and split each of the B_i-cosets represented by elements of W_i into B_{i+1}-cosets. We then create the set W_{i+1} of representatives of B_{i+1}-cosets we just produced. It follows that h_p is constant on each of the B_{i+1}-cosets represented by some $w \in W_{i+1}$ (in particular this was the goal of choosing this B_{i+1}). Clearly, $\phi(Q)$ will be in some B_{i+1}-coset represented by some element of W_{i+1} since $\bigcup_{w \in W_i}(w + B_i) = \bigcup_{w \in W_{i+1}}(w + B_{i+1})$.

This splitting is useful because

$$h_p\left(\bigcup_{w\in W_{i+1}}(w+B_{i+1})\right)=h_p(W_{i+1}).$$

We now apply the Mordell-Weil sieve and the Chabauty method to eliminate some elements from W_{i+1}. Notice that $h_p(\phi(Q))\in Im(m_p)$, so we need to only consider those $w\in W_{i+1}$ such that $h_p(w)\in Im(m_p)$. Let $H_{i+1}=h_p(W_{i+1})\cap Im(m_p)$. Since we know that $h_p(\phi(Q))\in H_{i+1}$, it follows that $red_p(\iota(Q))\in m_p^{-1}(H_{i+1})$.

We now give a criterion based on [13, Theorem 2.1.] which, if satisfied, will allow us to remove more elements from W_{i+1}. Take some $A_p\in m_p^{-1}(H_{i+1})$ and assume $red_p(\iota(Q))=A_p$. Denote by $l(D)$ the dimension of the Riemann-Roch space of the divisor D. If we have $l(A_p+[\widetilde{D_{pull}}])=0$, then we get a contradiction immediately since we must have $l(A_p+[\widetilde{D_{pull}}])=l([\widetilde{Q}])>0$ since $\widetilde{Q}$ is an effective degree 2 divisor. If one of our known points $Q_{known}\in X^{(2)}(\mathbb{Q})$ satisfies $red_p(\iota(Q_{known}))=A_p$ and fulfills the criterion given by [13, Theorem 2.1.] then $(red_p\circ\iota)^{-1}(A_p)=\{Q_{known}\}$. Notice that $Q\neq Q_{known}$ because Q is an unknown point. If the criterion succeeds, that means that Q_{known} is the only point in its residue disc modulo p. If we had $[\widetilde{Q_{known}}-\widetilde{D_{pull}}]=[\widetilde{Q}-\widetilde{D_{pull}}]$, that would imply $\widetilde{Q}=\widetilde{Q_{known}}$ by Proposition 1.3.31, since X is non-hyperelliptic, which is a contradiction. Hence, if the criterion succeeds, we cannot have $red_p(\iota(Q))=A_p$ for an unknown Q.

Clearly, if $w_h\in H_{i+1}$ and if $red_p(\iota(Q))$ can't equal any of the elements of $m_p^{-1}(w_h)$, then $h_p(\phi(Q))\neq w_h$, hence $\phi(Q)\notin h_p^{-1}(w_h)$. That means we can remove the elements of $h_p^{-1}(w_h)$ from W_{i+1} while still having $\phi(Q)\in\bigcup_{w\in W_{i+1}}(w+B_{i+1})$ satisfied.

To recapitulate, we have obtained $B_{i+1}\leq G$ and a set W_{i+1} of B_{i+1}-coset representatives such that $\phi(Q)\in\bigcup_{w\in W_{i+1}}(w+B_{i+1})$ and

$$\bigcup_{w\in W_{i+1}}(w+B_{i+1})\subseteq\bigcup_{w\in W_i}(w+B_i).$$

By repeating this for various primes p, it would be ideal to get $W_s=\emptyset$ for some s, which would imply that there are no unknown points in $X^{(2)}(\mathbb{Q})$.

Unfortunately, we are unable to get $W_s=\emptyset$ when $X=X_0(n)$ and $n\in\{79,83,89,101,131\}$. This is not surprising as $X^{(2)}(\mathbb{Q})$ is infinite in these cases. However, we get that for some s both B_s and W_s contain only elements of the form aD_n, where D_n is a pullback

of a generator of $J_0^+(n)(\mathbb{Q})$ that generates the free part of G. That means that for any $Q \in X^{(2)}(\mathbb{Q})$ we have $\phi(Q) = I \cdot [Q - D_{pull}] = aD_n$, which will be very useful to us, as will be explained in more detail in the next subsections. Note that in the method described in this subsection we use only [13, Theorem 2.1.] and do not use [13, Theorem 2.4.].

5.6.2. Selecting G and I

We now describe how to select an appropriate G and I (see also [13, Section 3.3.]). Let $\rho_n : X_0(n) \to X_0^+(n)$ be the degree 2 quotient map we get from w_n and $(\rho_n)_* : J_0(n) \to J_0^+(n)$ the induced (pushforward) map on $J_0(n)$. We have the following commutative diagram:

$$\begin{array}{ccc} X_0(n) & \xrightarrow{\iota_1} & J_0(n) \\ \downarrow{\scriptstyle \rho_n} & & \downarrow{\scriptstyle (\rho_n)_*} \\ X_0^+(n) & \xrightarrow{\iota_2} & J_0^+(n). \end{array}$$

For all $n \in \{79,83,89,101,131\}$ we have that $J_0^+(n)(\mathbb{Q})$ is an elliptic curve with Mordell-Weil group isomorphic to $\mathbb{Z}$. Let P_n be a generator of $J_0^+(n)(\mathbb{Q})$ and set $D_n = ((\rho_n)_*)^*(P_n)$. Let $T_n \in J_0(n)(\mathbb{Q})$ be the divisor class of the difference of the two cusps, which is a generator of $J_0(n)(\mathbb{Q})_{tors}$ (see Theorem 5.4.2).

Suppose now $n \neq 131$, as for $n = 131$ we will select different G and I, see Subsection 5.6.5. Set $G = \langle D_n, T_n \rangle$. Now we can use [13, Proposition 3.1.] to conclude that $2 \cdot J_0(n)(\mathbb{Q}) \subseteq G$ so we can use $I = 2$. Notice that $w_n'(D_n) = D_n$ since D_n is a pullback and that $w_n'(T_n) = -T_n$ since w_n swaps the cusps.

Lemma 5.6.1. Let $n \in \{79,83,89,101,131\}$. Then for every $D \in J_0(n)(\mathbb{Q})$ we have $(1 - w_n')(D) \in J_0(n)(\mathbb{Q})_{tors}$.

Proof. By the information above, we know that $2D \in \langle D_n, T_n \rangle$, so $2D = aD_n + bT_n$. Hence $(1 - w_n')(2D) = (1 - w_n')(aD_n + bT_n) = 2bT_n$, which is of finite order. ■

5.6.3. Quadratic points on $X_0(n)$ for $n \in \{79,83,101\}$

Before proceeding any further, we mention again that $n = 79$ was solved completely by Box in an unpublished `Magma` file. By performing the computations described in Subsection 5.6.1, we get that if there is an unknown $Q \in X_0(n)^{(2)}(\mathbb{Q})$, then $\phi(Q) =$

$2 \cdot [Q - D_{pull}] = kD_n$ for some integer k. Hence $w_n'(2 \cdot [Q - D_{pull}]) = 2 \cdot [Q - D_{pull}]$ which means that $w_n'([Q - D_{pull}]) - [Q - D_{pull}]$ is of order at most 2. Since $J_0(n)(\mathbb{Q})$ doesn't have an element of order 2 for $n \in \{79,83,101\}$, we have $w_n'([Q - D_{pull}]) = [Q - D_{pull}]$. Since D_{pull} is a pullback and $X_0(n)$ is not hyperelliptic, we get $w_n(Q) = Q$. Since $Q = \{Q_1, Q_2\}$ (as a 2-set), where $Q_i \in X_0(n)(\overline{\mathbb{Q}})$, we conclude that either w_n swaps Q_1 and Q_2 or it fixes them both. In the first case, Q is a pullback of a rational point on $X_0^+(n)$. To deal with the second case, we compute the fixed points of w_n, which all correspond to CM curves (note that the fixed points could also have been determined using the methods of [20]).

5.6.4. Quadratic points on $X_0(89)$

Notice that $J_0(89)(\mathbb{Q}) \cong \mathbb{Z} \times \mathbb{Z}/22\mathbb{Z}$ has an element of order 2, so the approach from Subsection 5.6.3 won't work without modification. We need more information and we get it by inspecting the possibilities for $\phi(Q)$ a bit more closely. By performing the computations from Subsection 5.6.1, we get that if there is an unknown $Q \in X_0(89)^{(2)}(\mathbb{Q})$, then $\phi(Q) = 2 \cdot [Q - D_{pull}] = 2kD_{89}$ for some integer k. Hence $[Q - D_{pull}] - kD_{89}$ is of order at most 2. If we have $[Q - D_{pull}] = kD_{89}$, then $w_n'([Q - D_{pull}]) = [Q - D_{pull}]$ and we continue as in Subsection 5.6.3. The other possibility is that $[Q - D_{pull}] = kD_{89} + 11T_{89}$, but since $w_n'(T_{89}) = -T_{89}$ and $11T_{89} = -11T_{89}$, we would have $w_n'([Q - D_{pull}]) = [Q - D_{pull}]$ and again we can continue as in Subsection 5.6.3.

5.6.5. Quadratic points on $X_0(131)$

In this case we use a different approach. We will take I to be the operator $1 - w_{131}'$. The reason for doing this is that we had originally been unable to compute the quotient curve and hence could not proceed as in the other cases. Although we now know how to compute the quotient map, we have left this case as it was. This is because it is possible that the strategy of applying the operator $I = 1 - w_{131}'$ might be useful in future applications. An additional benefit of using this operator I is that we do not need to choose a finite index subgroup for G. We set $G = \langle T_{131} \rangle = J_0(131)(\mathbb{Q})_{tors}$, where T_{131} is the divisor class of the difference of the two cusps of $X_0(131)$ as before, and $I = 1 - w_{131}'$. By Lemma 5.6.1, we know that $I \cdot J_0(131)(\mathbb{Q}) \subseteq G$. Since the action of w_{131}' commutes with the reduction

modulo a prime p of good reduction, we now proceed as in Subsection 5.6.1.

After doing the computations described in Subsection 5.6.1, we get that if there is an unknown $Q \in X_0(131)^{(2)}(\mathbb{Q})$, then $\phi(Q) = (1 - w'_{131}) \cdot [Q - D_{pull}] = 0$, so $w'_{131}([Q - D_{pull}]) = [Q - D_{pull}]$. Now we can again continue as in Subsection 5.6.3.

5.7. EXAMPLE OF THE SIEVING PROCESS FOR $N = 89$

Here we describe the whole process for determining the quadratic points on $X_0(89)$ in more detail. As mentioned before, we know that $J_0(89)(\mathbb{Q}) \cong \mathbb{Z} \times \mathbb{Z}/22\mathbb{Z}$. Following the notation and method from Subsection 5.6.2, we are able to find a finite index subgroup $G \leq J_0(89)(\mathbb{Q})$, where $G = \langle D_{89}, T_{89} \rangle$. The group is of index at most 2, so we use $I = 2$. We will use the primes 3, 5 and 7 for the sieving method described in Subsection 5.6.1. We have $B_0 = \langle D_{89} \rangle$ and $W_0 = \{k \cdot T_{89} : 0 \leq k \leq 21\}$. After performing the sieve with $p = 3$, we get $B_1 = \langle 5D_{89} \rangle$ and $W_1 = \{0, D_{89}, 2D_{89}, -D_{89}, -2D_{89}, 2T_{89}, 20T_{89}\}$. After performing the sieve with $p = 5$, we get $B_2 = \langle 35D_{89} \rangle$ and $W_2 = \{0, k \cdot D_{89} : 0 \leq k \leq 34\}$. After performing the sieve with $p = 7$, we get $B_3 = \langle 210D_{89} \rangle$ and $W_3 = \{0, 2k \cdot D_{89} : 0 \leq k \leq 104\}$. That means that $\phi(Q) = 2 \cdot [Q - D_{pull}] = 2kD_{89}$ for an unknown $Q \in X_0(89)^{(2)}(\mathbb{Q})$ and we can continue as described in Subsection 5.6.4.

This example is instructive because it shows that even if we sometimes don't reach an empty set with the sieve, we might be able to reach a set with a property which enables us to proceed.

5.8. FINAL RESULTS AND TABLES

Here we describe the results that we get for $n \in \{60, 79, 83, 89, 95, 101, 119, 131\}$. Recall that the results for $n \in \{62, 69, 92, 94\}$ can be found in Section 5.2. We describe all quadratic points on those $X_0(n)$. By C we always denote the quotient of $X_0(n)$ by an Atkin–Lehner involution which we used while doing the appropriate computations described in Section 5.6. As usual, for elliptic curves O always denotes the point at infinity. The column denoted by CM lists the discriminant of the order by which the elliptic curve has complex multiplication if it does, and NO if it does not have CM.

For $n \in \{62, 69, 92, 94\}$ we did not need to do almost any computations and did not even need to compute a model for $X_0(n)$. Hence we do not display any information for these values of n.

We list for each n the elliptic curve C which we use in our computations, where $b : X_0(n) \to C$ is of degree 2. We call the quadratic points on $X_0(n)$ which no not lie in $b^{-1}(C(\mathbb{Q}))$ *exceptional*. Note that since a bielliptic curve might have multiple maps of degree 2 to elliptic curves, whether a point is exceptional depends on the choice of C (or equivalently b). The points we list are exceptional with respect to our choice of C.

5.8.1. $X_0(60)$

Model for $X_0(60)$:

$$
\begin{aligned}
&x_0^2+2x_1^2-x_2^2+6x_3^2-6x_3x_5+x_4^2+4x_5^2-x_6^2=0,\\
&x_0x_2-x_1^2+x_3^2+x_3x_5=0,\\
&x_0x_3-x_1x_2=0,\\
&x_0x_4-x_2^2-x_3^2-x_3x_5+x_5^2=0,\\
&x_0x_5-x_2x_3-x_3x_4=0,\\
&x_1x_3-x_2^2-x_3x_5=0,\\
&x_1x_4-x_2x_3-x_3x_4=0,\\
&x_1x_5-x_3^2-x_3x_5=0,\\
&x_2x_4-x_3^2-x_3x_5+x_5^2=0,\\
&x_2x_5-x_3x_4=0.
\end{aligned}
$$

Genus of $X_0(60)$: 7.

Cusps: $(0:0:0:0:-1:0:1),(0:0:0:0:1:0:1),(0:0:-1/4:-1/4:1/4:1/4:1),(0:0:-1/4:1/4:1/4:-1/4:1),(0:0:1/4:-1/4:-1/4:1/4:1),(0:0:1/4:1/4:-1/4:-1/4:1),(-1:0:0:0:0:0:1),(-1/2:-1/2:-1/4:-1/4:-1/4:-1/4:1),(-1/2:1/2:-1/4:1/4:-1/4:1/4:1),(1/2:-1/2:1/4:-1/4:1/4:-1/4:1),(1/2:1/2:1/4:1/4:1/4:1/4:1),(1:0:0:0:0:0:1)$.

$C = X_0(60)/w_{15}$: elliptic curve $y^2 = x^3+x^2-x$.

Group structure of $J(C)(\mathbb{Q})$: $J(C)(\mathbb{Q}) \simeq \mathbb{Z}/6\mathbb{Z}\cdot[Q_C - O]$, where $Q_C := (1,-1)$.

Group structure of $G \subseteq J_0(60)(\mathbb{Q})$: $G \simeq \mathbb{Z}/4\mathbb{Z}\cdot D_1 \oplus \mathbb{Z}/24\mathbb{Z}\cdot D_2 \oplus \mathbb{Z}/24\mathbb{Z}\cdot D_3 \oplus \mathbb{Z}/24\mathbb{Z}\cdot D_4$, where $D_1,\ldots,D_4$ are generated by differences of cusps.

There are **no** quadratic points on $X_0(60)$ apart from cusps which are all defined over $\mathbb{Q}$.

Primes used in sieve: 13.

5.8.2. $X_0(79)$

Model for $X_0(79)$:

$$x_0^2 - 2x_0x_1 - x_1^2 - 3x_2^2 - 2x_2x_3 + 4x_2x_4 + 3x_3^2 + 2x_3x_4 - 11x_4^2 - x_5^2 = 0,$$
$$x_0x_2 - x_1^2 + 3x_2x_3 - x_2x_4 - 2x_3^2 - x_3x_4 + 4x_4^2 = 0,$$
$$x_0x_3 - x_1x_2 + 2x_2x_3 - x_3^2 + x_4^2 = 0,$$
$$x_0x_4 - x_2^2 + 2x_2x_3 + x_2x_4 - x_3^2 - x_3x_4 + 2x_4^2 = 0,$$
$$x_1x_3 - x_2^2 + 2x_2x_4 - x_4^2 = 0,$$
$$x_1x_4 - x_2x_3 + x_2x_4 + x_3^2 - 2x_4^2 = 0.$$

Genus of $X_0(79)$: 6.

Cusps: $(1:0:0:0:0:1), (-1:0:0:0:0:1)$.

$C = X_0^+(79)$: elliptic curve $y^2 + xy + y = x^3 + x^2 - 2x$.

Group structure of $J(C)(\mathbb{Q})$: $J(C)(\mathbb{Q}) \simeq \mathbb{Z} \cdot [Q_C - O]$, where $Q_C := (0,0)$.

Group structure of $G \subseteq J_0(79)(\mathbb{Q})$: $G \simeq \mathbb{Z} \cdot D_{79} \oplus \mathbb{Z}/13\mathbb{Z} \cdot T_{79}$, where D_{79}, T_{79} are as in Subsection 5.6.2.

There are **no** exceptional non-cuspidal quadratic points on $X_0(79)$.

Primes used in sieve: 3, 5.

5.8.3. $X_0(83)$

Model for $X_0(83)$:

$$x_0^2 - 2x_0x_1 - x_1^2 - x_2^2 + 2x_2x_3 - x_3^2 - 4x_3x_4 + 2x_3x_5 - 10x_4^2 + 24x_4x_5 - 31x_5^2 - x_6^2 = 0,$$
$$x_0x_2 - x_1^2 + 2x_2x_3 - 2x_3^2 + 6x_3x_4 - 6x_3x_5 - 3x_4^2 + 6x_4x_5 = 0,$$
$$x_0x_3 - x_1x_2 + 2x_2x_3 - 2x_3^2 + 5x_3x_4 - 2x_3x_5 - 4x_4^2 + 8x_4x_5 - 6x_5^2 = 0,$$
$$x_0x_4 - x_2^2 + x_2x_3 + x_3x_4 - 3x_3x_5 + 4x_4^2 - 6x_4x_5 + 9x_5^2 = 0,$$
$$x_0x_5 - x_3^2 + 2x_3x_4 - x_4^2 + 2x_4x_5 = 0,$$
$$x_1x_3 - x_2^2 + 2x_3^2 - 4x_3x_4 - x_3x_5 + 7x_4^2 - 14x_4x_5 + 15x_5^2 = 0,$$
$$x_1x_4 - x_2x_3 + x_3^2 - 2x_3x_4 + 2x_3x_5 + 3x_4^2 - 8x_4x_5 + 6x_5^2 = 0,$$
$$x_1x_5 - x_3x_4 + x_3x_5 + x_4^2 - 2x_4x_5 = 0,$$
$$x_2x_4 - x_3^2 + x_3x_4 + x_3x_5 - 3x_4^2 + 5x_4x_5 - 6x_5^2 = 0,$$
$$x_2x_5 - x_4^2 + 2x_4x_5 - 3x_5^2 = 0.$$

Genus of $X_0(83)$: 7.

Cusps: $(1:0:0:0:0:0:1), (-1:0:0:0:0:0:1)$.

$C = X_0^+(83)$: elliptic curve $y^2 + xy + y = x^3 + x^2 + x$.

Group structure of $J(C)(\mathbb{Q})$: $J(C)(\mathbb{Q}) \simeq \mathbb{Z} \cdot [Q_C - O]$, where $Q_C := (0,0)$.

Group structure of $G \subseteq J_0(83)(\mathbb{Q})$: $G \simeq \mathbb{Z} \cdot D_{83} \oplus \mathbb{Z}/41\mathbb{Z} \cdot T_{83}$, where D_{83}, T_{83} are as in Subsection 5.6.2.

There are **no** exceptional non-cuspidal quadratic points on $X_0(83)$.

Primes used in sieve: 3, 5.

5.8.4. $X_0(89)$

Model for $X_0(89)$:

$$x_0^2 - 2x_0x_1 - x_1^2 + x_2^2 + 6x_2x_3 - 21x_3^2 + 12x_3x_4 + 36x_3x_5 - 13x_4^2 - 6x_4x_5 - 21x_5^2 - x_6^2 = 0,$$
$$x_0x_2 - x_1^2 + 3x_3^2 - 8x_3x_5 + x_4^2 + x_4x_5 + 5x_5^2 = 0,$$
$$x_0x_3 - x_1x_2 + 3x_3^2 - 6x_3x_5 + 2x_4x_5 + 3x_5^2 = 0,$$
$$x_0x_4 - x_2^2 + 2x_3^2 + 2x_3x_4 - 7x_3x_5 + 2x_4^2 - 2x_4x_5 + 5x_5^2 = 0,$$
$$x_0x_5 - x_2x_3 + x_3^2 + 2x_3x_4 - 3x_3x_5 - x_4x_5 + 3x_5^2 = 0,$$
$$x_1x_3 - x_2^2 + 3x_3x_4 - 4x_3x_5 + x_4^2 - 4x_4x_5 + 4x_5^2 = 0,$$
$$x_1x_4 - x_2x_3 + 2x_3x_4 - x_3x_5 - 2x_4x_5 + x_5^2 = 0,$$
$$x_1x_5 - x_3^2 + x_3x_4 + 2x_3x_5 - 2x_4x_5 - x_5^2 = 0,$$
$$x_2x_4 - x_3^2 + 3x_3x_5 - x_4^2 - x_4x_5 - x_5^2 = 0,$$
$$x_2x_5 - x_3x_4 + x_3x_5 + x_4x_5 - 2x_5^2 = 0.$$

Genus of $X_0(89)$: 7.

Cusps: $(1:0:0:0:0:0:1), (-1:0:0:0:0:0:1)$.

$C = X_0^+(89)$: elliptic curve $y^2 - 19xy - y = x^3 - 89x^2 - 10x$.

Group structure of $J(C)(\mathbb{Q})$: $J(C)(\mathbb{Q}) \simeq \mathbb{Z} \cdot [Q_C - O]$, where $Q_C := (0,0)$.

Group structure of $G \subseteq J_0(89)(\mathbb{Q})$: $G \simeq \mathbb{Z} \cdot D_{89} \oplus \mathbb{Z}/22\mathbb{Z} \cdot T_{89}$, where D_{89}, T_{89} are as in Subsection 5.6.2.

There are **no** exceptional non-cuspidal quadratic points on $X_0(89)$.

Primes used in sieve: 3, 5, 7.

5.8.5. $X_0(95)$

Model for $X_0(95)$:

$$x_0^2+4x_2x_3+4x_2x_5-3x_3^2+2x_3x_4+4x_3x_5+19x_4^2-32x_4x_5+10x_5^2-x_6^2+2x_7x_8+4x_8^2=0,$$
$$x_0x_1+2x_1x_5+3x_2x_3-3x_2x_5-5x_3^2-2x_3x_4+6x_3x_5+14x_4^2-26x_4x_5+13x_5^2-x_6x_7+x_8^2=0,$$
$$x_0x_2-2x_2x_5-2x_3^2-x_3x_4+x_3x_5-2x_4^2+x_4x_5+x_5^2-x_7^2=0,$$
$$x_0x_3-2x_2x_3+3x_3^2-2x_3x_5-9x_4^2+16x_4x_5-7x_5^2-x_7x_8-x_8^2=0,$$
$$x_0x_4-2x_2x_3+x_3^2+2x_3x_4-2x_3x_5-6x_4^2+10x_4x_5-4x_5^2-x_8^2=0,$$
$$x_0x_5-x_2x_3-x_2x_5-x_3^2+x_3x_4+x_3x_5-x_4^2-x_4x_5+2x_5^2=0,$$
$$x_0x_7-x_1x_6+x_4x_6+2x_4x_7-x_4x_8-x_5x_6+x_5x_8=0,$$
$$x_0x_8-x_2x_6+x_3x_6-x_4x_7+3x_4x_8+x_5x_6+x_5x_7-x_5x_8=0,$$
$$x_1^2-4x_4^2+8x_4x_5-4x_5^2-x_7^2=0,$$
$$x_1x_2-2x_1x_5-2x_2x_3+2x_2x_5+4x_3^2-2x_3x_4-2x_3x_5-8x_4^2+18x_4x_5-10x_5^2-x_7x_8-x_8^2=0,$$
$$x_1x_3-x_1x_5-2x_2x_3+2x_2x_5+2x_3^2+2x_3x_4-2x_3x_5-8x_4^2+14x_4x_5-8x_5^2-x_8^2=0,$$
$$x_1x_4-x_1x_5-x_2x_3+x_2x_5+x_3^2-2x_4^2+4x_4x_5-3x_5^2=0,$$
$$x_1x_7-x_2x_6-x_4x_7+2x_5x_6+x_5x_7=0,$$
$$x_1x_8-x_3x_6+x_4x_6-x_4x_8+x_5x_8=0,$$
$$x_2^2-2x_2x_3-2x_2x_5+x_3^2+4x_3x_4-2x_3x_5-8x_4^2+12x_4x_5-3x_5^2-x_8^2=0,$$
$$x_2x_4-x_2x_5-x_3^2+x_3x_4+x_3x_5-3x_4x_5+2x_5^2=0,$$
$$x_2x_7-x_3x_6-x_4x_7+x_5x_6-x_5x_7=0,$$
$$x_2x_8-x_4x_6-x_4x_8+x_5x_6-x_5x_8=0,$$
$$x_3x_7-x_4x_6-x_4x_7-x_4x_8+x_5x_6+x_5x_8=0,$$
$$x_3x_8-x_4x_7+x_5x_7-x_5x_8=0,$$
$$x_6x_8-x_7^2+x_7x_8+x_8^2=0.$$

Genus of $X_0(95)$: 9.

Cusps: $(-1:0:0:0:0:0:1:0:0),(1:0:0:0:0:0:1:0:0),(-3/5:0:-2/5:-1/5:-1/5:-1/5:1:0:0),(3/5:0:2/5:1/5:1/5:1/5:1:0:0)$.

$C=X_0(95)/w_{19}$: hyperelliptic curve $y^2=x^8-2x^7-7x^6+16x^5-2x^4-2x^3-4x^2+5$.

Group structure of $J(C)(\mathbb{Q})$: $J(C)(\mathbb{Q})\simeq\mathbb{Z}/2\mathbb{Z}\cdot[P+P^\sigma-2\infty_+]\oplus\mathbb{Z}/10\mathbb{Z}\cdot[\infty_--\infty_+]$, where

$$P:=\Big(\frac{1}{2}(-\sqrt{5}+3):\frac{1}{2}(5\sqrt{5}-7):1\Big)\in C(\mathbb{Q}(\sqrt{5})).$$

Group structure of $G \subseteq J_0(95)(\mathbb{Q})$: $G \simeq \mathbb{Z}/6\mathbb{Z} \cdot D_1 \oplus \mathbb{Z}/180\mathbb{Z} \cdot D_2$, where D_1, D_2 are generated by differences of cusps.

Below is the table of **all** quadratic points on $X_0(95)$ (up to Galois conjugacy) apart from cusps, which are all defined over $\mathbb{Q}$.

Name	θ^2	Coordinates	j-invariant	CM
P_1	-19	$(\frac{1}{14}(-\theta-17):\frac{1}{7}(\theta-11):\frac{1}{7}(\theta+3):\frac{1}{7}(\theta-4):\frac{1}{14}(\theta+3):1:0:0:0)$	-884736	-19

Primes used in sieve: 11, 13.

5.8.6. $X_0(101)$

Model for $X_0(101)$:

$$x_0^2-4x_1^2-4x_1x_2+2x_2^2+8x_2x_3+4x_3^2-20x_3x_4-41x_4^2+112x_4x_5+18x_4x_6-22x_5^2-204x_5x_6+170x_6^2-x_7^2=0,$$
$$x_0x_2-x_1^2+8x_3x_4-8x_4^2-15x_4x_5+21x_4x_6+32x_5^2-61x_5x_6+31x_6^2=0,$$
$$x_0x_3-x_1x_2+8x_3x_4-10x_4^2-5x_4x_5+17x_4x_6+22x_5^2-54x_5x_6+30x_6^2=0,$$
$$x_0x_4-x_2^2+6x_3x_4-x_4^2-20x_4x_5+15x_4x_6+25x_5^2-30x_5x_6+9x_6^2=0,$$
$$x_0x_5-x_2x_3+4x_3x_4-x_4^2-10x_4x_5+6x_4x_6+12x_5^2-8x_5x_6=0,$$
$$x_0x_6-x_3^2+2x_3x_4-x_4x_5-x_4x_6-2x_5^2+10x_5x_6-5x_6^2=0,$$
$$x_1x_3-x_2^2+8x_4^2-18x_4x_5-2x_4x_6+5x_5^2+26x_5x_6-23x_6^2=0,$$
$$x_1x_4-x_2x_3+6x_4^2-9x_4x_5-6x_4x_6-4x_5^2+33x_5x_6-24x_6^2=0,$$
$$x_1x_5-x_3^2+4x_4^2-x_4x_5-8x_4x_6-10x_5^2+32x_5x_6-20x_6^2=0,$$
$$x_1x_6-x_3x_4+2x_4^2-3x_4x_6-4x_5^2+12x_5x_6-8x_6^2=0,$$
$$x_2x_4-x_3^2+6x_4x_5-7x_4x_6-10x_5^2+18x_5x_6-8x_6^2=0,$$
$$x_2x_5-x_3x_4+4x_4x_5-2x_4x_6-5x_5^2+3x_5x_6=0,$$
$$x_2x_6-x_4^2+2x_4x_5-5x_5x_6+3x_6^2=0,$$
$$x_3x_5-x_4^2+2x_4x_6+2x_5^2-9x_5x_6+6x_6^2=0,$$
$$x_3x_6-x_4x_5+2x_5^2-4x_5x_6+2x_6^2=0.$$

Genus of $X_0(101)$: 8.

Cusps: $(1:0:0:0:0:0:0:1),(-1:0:0:0:0:0:0:1)$.

$C=X_0^+(101)$: elliptic curve $y^2+y=x^3+x^2-x-1$.

Group structure of $J(C)(\mathbb{Q})$: $J(C)(\mathbb{Q})\simeq\mathbb{Z}\cdot[Q_C-O]$, where $Q_C:=(-1,0)$.

Group structure of $G\subseteq J_0(101)(\mathbb{Q})$: $G\simeq\mathbb{Z}\cdot D_{101}\oplus\mathbb{Z}/25\mathbb{Z}\cdot T_{101}$, where D_{101}, T_{101} are as in Subsection 5.6.2.

There are **no** exceptional non-cuspidal quadratic points on $X_0(101)$.

Primes used in sieve: 3, 5.

5.8.7. $X_0(119)$

Model for $X_0(119)$:

$$x_0^2+8x_1x_6-8x_3x_4+24x_3x_6+17x_4^2-24x_4x_5-4x_4x_6+5x_5^2+38x_5x_6-39x_6^2-x_7^2+2x_9^2+2x_9x_{10}+6x_{10}^2=0,$$

$$x_0x_1+4x_1x_6-x_3x_4+2x_3x_6+3x_4x_5-4x_5^2+2x_5x_6-4x_6^2-x_7x_8+x_9x_{10}+x_{10}^2=0,$$

$$x_0x_2-2x_1x_6+4x_2x_6+2x_3x_4-6x_3x_6-4x_4^2+4x_4x_5+2x_4x_6+3x_5^2-14x_5x_6+7x_6^2-x_8^2=0,$$

$$x_0x_3-3x_1x_6+x_3x_4-x_3x_6-3x_4^2+3x_4x_5-4x_5^2+2x_5x_6-4x_6^2-x_8x_9-x_9x_{10}=0,$$

$$x_0x_4-2x_1x_6+3x_3x_4-8x_3x_6-4x_4^2+5x_4x_5+2x_4x_6+x_5^2-12x_5x_6+13x_6^2-x_9^2-2x_{10}^2=0,$$

$$x_0x_5-x_1x_6-x_3x_6+x_4x_5-3x_4x_6-x_5^2+4x_5x_6+x_6^2-x_9x_{10}=0,$$

$$x_0x_6-x_1x_6+x_3x_4-3x_3x_6-2x_4^2+3x_4x_5-6x_5x_6+8x_6^2-x_{10}^2=0,$$

$$x_0x_8-x_1x_7+x_5x_7+2x_5x_8-x_6x_7+2x_6x_8=0,$$

$$x_0x_9-x_2x_7+x_4x_7+x_5x_8+4x_5x_9-x_5x_{10}-x_6x_8+x_6x_{10}=0,$$

$$x_0x_{10}-x_3x_7+x_5x_7-2x_5x_8+x_5x_9+4x_5x_{10}+2x_6x_7+2x_6x_8-x_6x_9=0,$$

$$x_1^2+4x_5^2-8x_5x_6+4x_6^2-x_8^2=0,$$

$$x_1x_2-2x_1x_6-x_4^2+x_4x_5+3x_4x_6-3x_5^2+4x_5x_6-5x_6^2-x_8x_9-x_9x_{10}=0,$$

$$x_1x_3-3x_1x_6+3x_3x_4-6x_3x_6-3x_4^2+2x_4x_5+x_4x_6+3x_5^2-10x_5x_6+13x_6^2-x_9^2-2x_{10}^2=0,$$

$$x_1x_4-2x_1x_6+x_4^2-x_4x_5-3x_4x_6-x_5^2+4x_5x_6+x_6^2-x_9x_{10}=0,$$

$$x_1x_5-x_1x_6+x_3x_4-2x_3x_6-x_4^2+2x_4x_5-x_4x_6+x_5^2-6x_5x_6+7x_6^2-x_{10}^2=0,$$

$$x_1x_8-x_2x_7-x_5x_8+2x_6x_7+x_6x_8=0,$$

$$x_1x_9-x_3x_7+x_5x_7-2x_5x_8+2x_5x_{10}+2x_6x_7+2x_6x_8-2x_6x_{10}=0,$$

$$x_1x_{10}-x_4x_7-x_5x_8-2x_5x_9+2x_6x_7+x_6x_8+2x_6x_9=0,$$

$$x_2^2-4x_2x_6+x_4^2-2x_4x_5-2x_4x_6+2x_5^2+6x_6^2-x_9^2-2x_{10}^2=0,$$

$$x_2x_3-3x_2x_6-2x_3x_4+2x_3x_6+3x_4^2-2x_4x_5-4x_4x_6-3x_5^2+10x_5x_6-x_6^2-x_9x_{10}=0,$$

$$x_2x_4-2x_2x_6+x_4x_5-3x_4x_6+x_5^2-4x_5x_6+7x_6^2-x_{10}^2=0,$$

$$x_2x_5-x_2x_6-x_3x_4+2x_3x_6+x_4^2-x_4x_5-x_5^2+2x_5x_6-3x_6^2=0,$$

$$x_2x_8-x_3x_7-3x_5x_8+3x_6x_7+x_6x_8=0,$$

$$x_2x_9-x_4x_7-x_5x_8-2x_5x_9+x_5x_{10}+2x_6x_7+x_6x_8-x_6x_{10}=0,$$

$$x_2x_{10}-x_5x_7-x_5x_8-x_5x_9-2x_5x_{10}+x_6x_7+x_6x_8+x_6x_9=0,$$

$$x_3^2-6x_3x_6-2x_4^2+6x_4x_5+2x_4x_6-3x_5^2-6x_5x_6+10x_6^2-x_{10}^2=0,$$

$$x_3x_5-x_3x_6-x_4^2+x_4x_5+3x_4x_6-2x_5^2-x_5x_6-x_6^2=0,$$

$$x_3x_8-x_4x_7-2x_5x_8+2x_6x_7-x_6x_8=0,$$

$$x_3x_9-x_5x_7-x_5x_8-x_5x_9+x_5x_{10}+x_6x_7+x_6x_8-2x_6x_9-x_6x_{10}=0,$$

$$x_3x_{10}-x_5x_8-x_5x_9-x_5x_{10}+x_6x_8+x_6x_9-2x_6x_{10}=0,$$

$$x_4x_8-x_5x_7-x_5x_8+x_6x_7-x_6x_8=0,$$

$$x_4x_9-x_5x_8-x_5x_9+x_5x_{10}+x_6x_8-x_6x_9-x_6x_{10}=0,$$

$$x_4x_{10}-x_5x_9-x_5x_{10}+x_6x_9-x_6x_{10}=0,$$

$$x_7x_9-x_8^2+x_9^2+x_{10}^2=0,$$

$$x_7x_{10}-x_8x_9=0,$$

$$x_8x_{10}-x_9^2-x_{10}^2=0.$$

Genus of $X_0(119)$: 11.

Cusps: $(-1:0:0:0:0:0:0:1:0:0:0:0), (1:0:0:0:0:0:0:0:1:0:0:0:0), (-3/7:0:-2/7:-3/7:-2/7:-1/7:-1/7:1:0:0:0), (3/7:0:2/7:3/7:2/7:1/7:1/7:1:0:0:0)$.

$C = X_0(119)/w_{17}$: hyperelliptic curve $y^2 = x^{10} + 2x^8 - 11x^6 + 14x^5 - 40x^4 + 42x^3 - 48x^2 + 28x - 7$.

Group structure of $J(C)(\mathbb{Q})$: $J(C)(\mathbb{Q}) \simeq \mathbb{Z}/9\mathbb{Z} \cdot [\infty_+ - \infty_-]$.

Group structure of $G \subseteq J_0(119)(\mathbb{Q})$: $G \simeq \mathbb{Z}/8\mathbb{Z} \cdot D_1 \oplus \mathbb{Z}/288\mathbb{Z} \cdot D_2$, where D_1, D_2 are generated by differences of cusps.

Below is the table of **all** quadratic points on $X_0(119)$ (up to Galois conjugacy) apart from cusps which are all defined over $\mathbb{Q}$.

Name	θ^2	Coordinates	j-invariant	CM
P_1	-19	$(\frac{1}{7}(-2\theta+1):0:\frac{1}{7}(\theta-4):\frac{1}{14}(3\theta-19):\frac{1}{7}(\theta+3):\frac{1}{14}(\theta-11):\frac{1}{14}(\theta+3):-2:2:-1:1)$	-884736	-19
P_2	-19	$(\frac{1}{7}(-2\theta+1):0:\frac{1}{7}(\theta-4):\frac{1}{14}(3\theta-19):\frac{1}{7}(\theta+3):\frac{1}{14}(\theta-11):\frac{1}{14}(\theta+3):2:-2:1:-1)$	-884736	-19

Primes used in sieve: 5.

5.8.8. $X_0(131)$

Model for $X_0(131)$:

$$x_0^2-2x_1^2-4x_1x_2-3x_2^2+4x_2x_3+6x_3^2+8x_3x_4+2x_4^2-48x_4x_5-44x_5^2+38x_5x_6+337x_6^2-244x_6x_7-1368x_7^2+$$
$$3738x_7x_8-4056x_7x_9-4088x_8^2+6808x_8x_9-2706x_9^2-x_{10}^2=0,$$
$$x_0x_2-x_1^2+12x_4x_5-2x_5^2-36x_5x_6-3x_6^2+119x_6x_7-108x_7^2+38x_7x_8-12x_7x_9+22x_8^2-8x_8x_9+98x_9^2=0,$$
$$x_0x_3-x_1x_2+14x_4x_5-12x_5^2-14x_5x_6-15x_6^2+113x_6x_7-106x_7^2+31x_7x_8-20x_7x_9+32x_8^2-3x_8x_9+86x_9^2=0,$$
$$x_0x_4-x_2^2+12x_4x_5-35x_5x_6+x_6^2+92x_6x_7-71x_7^2+4x_7x_8+21x_7x_9+42x_8^2-54x_8x_9+93x_9^2=0,$$
$$x_0x_5-x_2x_3+9x_4x_5-22x_5x_6-12x_6^2+87x_6x_7-43x_7^2-59x_7x_8+84x_7x_9+109x_8^2-162x_8x_9+128x_9^2=0,$$
$$x_0x_6-x_3^2+6x_4x_5-5x_5x_6-27x_6^2+48x_6x_7+67x_7^2-255x_7x_8+280x_7x_9+297x_8^2-480x_8x_9+214x_9^2=0,$$
$$x_0x_7-x_3x_4+4x_4x_5-4x_5x_6-12x_6^2+21x_6x_7+35x_7^2-116x_7x_8+128x_7x_9+134x_8^2-218x_8x_9+94x_9^2=0,$$
$$x_0x_8-x_4^2+2x_4x_5-x_5x_6+x_6^2-8x_6x_7+18x_7^2-25x_7x_8+29x_7x_9+29x_8^2-45x_8x_9+11x_9^2=0,$$
$$x_0x_9-x_5^2+2x_5x_6+x_6^2-2x_6x_7-7x_7^2+20x_7x_8-16x_7x_9-20x_8^2+37x_8x_9-10x_9^2=0,$$
$$x_1x_3-x_2^2+14x_5^2-24x_5x_6-12x_6^2+21x_6x_7+98x_7^2-261x_7x_8+298x_7x_9+281x_8^2-492x_8x_9+202x_9^2=0,$$
$$x_1x_4-x_2x_3+12x_5^2-14x_5x_6-23x_6^2+15x_6x_7+131x_7^2-334x_7x_8+370x_7x_9+357x_8^2-613x_8x_9+240x_9^2=0,$$
$$x_1x_5-x_3^2+9x_5^2-36x_6^2+182x_7^2-436x_7x_8+468x_7x_9+460x_8^2-777x_8x_9+287x_9^2=0,$$
$$x_1x_6-x_3x_4+6x_5^2-17x_6^2-13x_6x_7+113x_7^2-244x_7x_8+261x_7x_9+249x_8^2-428x_8x_9+148x_9^2=0,$$
$$x_1x_7-x_4^2+4x_5^2-4x_6^2-24x_6x_7+71x_7^2-122x_7x_8+129x_7x_9+115x_8^2-205x_8x_9+59x_9^2=0,$$
$$x_1x_8-x_4x_5+2x_5^2-x_6^2-8x_6x_7+22x_7^2-36x_7x_8+39x_7x_9+33x_8^2-62x_8x_9+17x_9^2=0,$$
$$x_1x_9-x_5x_6+2x_6^2+x_6x_7-8x_7^2+18x_7x_8-19x_7x_9-19x_8^2+31x_8x_9-12x_9^2=0,$$
$$x_2x_4-x_3^2+12x_5x_6-28x_6^2+x_6x_7+99x_7^2-246x_7x_8+258x_7x_9+264x_8^2-434x_8x_9+160x_9^2=0,$$
$$x_2x_5-x_3x_4+9x_5x_6-12x_6^2-22x_6x_7+77x_7^2-146x_7x_8+149x_7x_9+144x_8^2-243x_8x_9+72x_9^2=0,$$
$$x_2x_6-x_4^2+6x_5x_6-29x_6x_7+37x_7^2-34x_7x_8+30x_7x_9+21x_8^2-42x_8x_9-7x_9^2=0,$$
$$x_2x_7-x_4x_5+4x_5x_6-13x_6x_7+12x_7^2-9x_7x_8+6x_7x_9+3x_8^2-7x_8x_9-7x_9^2=0,$$
$$x_2x_8-x_5^2+2x_5x_6-x_6x_7-5x_7^2+12x_7x_8-16x_7x_9-16x_8^2+26x_8x_9-11x_9^2=0,$$
$$x_2x_9-x_6^2+2x_6x_7+x_7^2-6x_7x_8+4x_7x_9+7x_8^2-12x_8x_9+4x_9^2=0,$$
$$x_3x_5-x_4^2+9x_6^2-24x_6x_7+6x_7^2+34x_7x_8-39x_7x_9-50x_8^2+74x_8x_9-45x_9^2=0,$$
$$x_3x_6-x_4x_5+6x_6^2-9x_6x_7-17x_7^2+59x_7x_8-64x_7x_9-67x_8^2+109x_8x_9-47x_9^2=0,$$
$$x_3x_7-x_5^2+4x_6^2-22x_7^2+48x_7x_8-52x_7x_9-51x_8^2+86x_8x_9-31x_9^2=0,$$
$$x_3x_8-x_5x_6+2x_6^2-7x_7^2+16x_7x_8-19x_7x_9-21x_8^2+32x_8x_9-12x_9^2=0,$$
$$x_3x_9-x_6x_7+2x_7^2-3x_7x_8-x_7x_9+2x_8^2-4x_8x_9-2x_9^2=0,$$
$$x_4x_6-x_5^2+6x_6x_7-18x_7^2+31x_7x_8-33x_7x_9-29x_8^2+52x_8x_9-15x_9^2=0,$$
$$x_4x_7-x_5x_6+4x_6x_7-6x_7^2+3x_7x_8-2x_7x_9-x_8^2+2x_8x_9+4x_9^2=0,$$
$$x_4x_8-x_6^2+2x_6x_7-5x_7x_8+4x_7x_9+3x_8^2-7x_8x_9+4x_9^2=0,$$
$$x_4x_9-x_7^2+2x_7x_8-6x_7x_9-3x_8^2+5x_8x_9-5x_9^2=0,$$
$$x_5x_7-x_6^2+4x_7^2-12x_7x_8+14x_7x_9+13x_8^2-23x_8x_9+10x_9^2=0,$$
$$x_5x_8-x_6x_7+2x_7^2-4x_7x_8+2x_7x_9+x_8^2-3x_8x_9=0,$$
$$x_5x_9-x_7x_8-3x_7x_9+x_8x_9-3x_9^2=0,$$
$$x_6x_8-x_7^2+2x_7x_8-3x_7x_9-4x_8^2+5x_8x_9-2x_9^2=0,$$
$$x_6x_9-2x_7x_9-x_8^2+x_8x_9-2x_9^2=0.$$

Genus of $X_0(131)$: 11.

Cusps: $(1:0:0:0:0:0:0:0:0:0:1), (-1:0:0:0:0:0:0:0:0:0:1)$.

$C = X_0^+(131)$: elliptic curve $y^2 + y = x^3 - x^2 + x$

Group structure of $J(C)(\mathbb{Q})$: $J(C)(\mathbb{Q}) \simeq \mathbb{Z} \cdot [Q_C - O]$, where $Q_C := (0,0)$.

Group structure of $G \subseteq J_0(131)(\mathbb{Q})$: $G \simeq \mathbb{Z}/65\mathbb{Z} \cdot T_{131}$, where T_{131} is as in Subsection 5.6.2.

There are **no** exceptional non-cuspidal quadratic points on $X_0(131)$.

Primes used in sieve: 3, 5.

CONCLUSION

In this thesis, we gave a complete classification of $E(\mathbb{Q}(\mu_{p^\infty}))_{tors}$, where $E/\mathbb{Q}$ is an elliptic curve and $p \leq 11$ a prime number. We have shown that, given an elliptic curve $E/\mathbb{Q}$, the group $E(\mathbb{Q}(\mu_{p^\infty}))_{tors}$ is either one of the groups from Mazur's theorem or one of the following groups:

- For $p = 2$: $\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$ or $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/10\mathbb{Z}$.
- For $p = 3$: $\mathbb{Z}/21\mathbb{Z}$, $\mathbb{Z}/27\mathbb{Z}$, $\mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}$, $\mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}$ or $\mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/9\mathbb{Z}$.
- For $p = 5$: $\mathbb{Z}/15\mathbb{Z}$, $\mathbb{Z}/16\mathbb{Z}$ or $\mathbb{Z}/5\mathbb{Z} \oplus \mathbb{Z}/5\mathbb{Z}$.
- For $p = 7$: $\mathbb{Z}/13\mathbb{Z}$, $\mathbb{Z}/14\mathbb{Z}$, $\mathbb{Z}/18\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/14\mathbb{Z}$ or $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/18\mathbb{Z}$.
- For $p = 11$: $\mathbb{Z}/11\mathbb{Z}$, $\mathbb{Z}/25\mathbb{Z}$ or $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/10\mathbb{Z}$.

We also gave a complete classification of the possible cyclic isogeny degrees of non-CM elliptic curves over quadratic fields with a rational j-invariant. We proved that, given a non-CM elliptic curve E/K where K is some quadratic field, the possible cyclic isogeny degrees of E are those from the Mazur's theorem on isogenies plus the elements of the set $\{20, 24, 32, 36\}$. We also determined all the quadratic points on $X_0(91)$ in the process.

Lastly, we described all the quadratic points on all bielliptic curves $X_0(n)$ for the values of n for which this has not been done before. This includes $n \in \{60, 62, 69, 79, 83, 89, 92, 94, 95, 101, 119, 131\}$.

BIBLIOGRAPHY

[1] Anderson, M.: *Subgroups of finite index in profinite groups*. Pacific J. Math., 62(1):19–28, 1976, ISSN 0030-8730. http://projecteuclid.org/euclid.pjm/1102867855. ↑ 64, 65, 68.

[2] B. S. Banwait, F. Najman, O. Padurariu: *Cyclic isogenies of elliptic curves over a fixed quadratic field*. https://arxiv.org/abs/2206.08891. ↑ 23.

[3] Balakrishnan, J., A. Besser, F. Bianchi, and J. S. Müller: *Explicit quadratic Chabauty over number fields*. Israel J. Math., 243(1):185–232, 2021, ISSN 0021-2172. https://doi.org/10.1007/s11856-021-2158-5. ↑ 76.

[4] Balakrishnan, J., N. Dogra, J.S. Müller, J. Tuitman, and J. Vonk: *Explicit Chabauty-Kim for the split Cartan modular curve of level 13*. Ann. of Math. (2), 189(3):885–944, 2019, ISSN 0003-486X. https://doi.org/10.4007/annals.2019.189.3.6. ↑ 10, 52.

[5] Balakrishnan, J., N. Dogra, J. S. Müller, J. Tuitman, and J. Vonk: *Quadratic Chabauty for modular curves: Algorithms and examples*. https://arxiv.org/pdf/2101.01862.pdf. ↑ 10, 52.

[6] Banwait, B. S.: *Explicit Isogenies of Prime Degree Over Quadratic Fields*. International Mathematics Research Notices, 2022, ISSN 1073-7928. https://doi.org/10.1093/imrn/rnac134. ↑ 22, 23.

[7] Bars, Francesc: *Bielliptic modular curves*. J. Number Theory, 76(1):154–165, 1999, ISSN 0022-314X. https://doi.org/10.1006/jnth.1998.2343. ↑ 78.

[8] Bilu, Y., P. Parent, and M. Rebolledo: *Rational points on $X_0^+(p^r)$*. Ann. Inst. Fourier (Grenoble), 63(3):957–984, 2013, ISSN 0373-0956. https://doi.org/10.5802/aif.2781. ↑ 61.

[9] Birch, B. J. and W. Kuyk (editors): *Modular functions of one variable IV*, volume 476. Springer Berlin, Heidelberg, 1975. ↑ 47.

[10] Borovik, A. V., R. M. Bryant, B. Hartley, and G. M. Seitz (editors): *Finite and Locally Finite Groups*, volume 471. Springer Dordrecht, 1995. ↑ 64.

[11] Bosma, W., J. Cannon, C. Fieker, and A. Steel (editors): *Handbook of Magma functions*. 2013. https://www.math.uzh.ch/sepp/magma-2.19.8-cr/Handbook.pdf. ↑ 19.

[12] Bosma, W., J. Cannon, and C. Playoust: *The Magma Algebra System I: The User Language*. J. Symbolic Comput., 24(3-4):235–265, 1997, ISSN 0747-7171. http://dx.doi.org/10.1006/jsco.1996.0125, Computational algebra and number theory (London, 1993). ↑ ii, v, 19, 42, 46, 47, 57, 61, 66, 68, 69, 75.

[13] Box, J.: *Quadratic points on modular curves with infinite Mordell-Weil group*. Math. Comp., 90(327):321–343, 2021, ISSN 0025-5718. ↑ ii, iv, 23, 57, 74, 75, 76, 78, 79, 80, 90, 91, 93, 95, 96.

[14] Box, J., S. Gajović, and P. Goodman: *Cubic and quartic points on modular curves using generalised symmetric Chabauty*. International Mathematics Research Notices, February 2022, ISSN 1073-7928. https://doi.org/10.1093/imrn/rnab358, rnab358. ↑ 23, 75, 92, 93.

[15] Bruin, P. and F. Najman: *Hyperelliptic modular curves $X_0(n)$ and isogenies of elliptic curves over quadratic fields*. LMS J. Comput. Math., 18(1):578–602, 2015. https://doi.org/10.1112/S1461157015000157. ↑ 23, 58, 70, 71, 72.

[16] Bruin, P. and F. Najman: *A criterion to rule out torsion groups for elliptic curves over number fields*. Res. Number Theory, 2(3), 2016. https://doi.org/10.1007/s40993-015-0031-5. ↑ 21, 38, 45, 79, 84, 85.

[17] Chou, M.: *Torsion of rational elliptic curves over quartic Galois number fields*. J. Number Theory, 160:603–628, 2016. https://doi.org/10.1016/j.jnt.2015.09.013. ↑ 24.

[18] Chou, M.: *Torsion of rational elliptic curves over the maximal abelian extension of* $\mathbb{Q}$. Pacific J. Math., 302(2):481–509, 2019. https://doi.org/10.2140/pjm.2019.302.481. ↑ 21, 22, 25, 31, 35, 36.

[19] Chou, M., H. B. Daniels, I. Krijan, and F. Najman: *Torsion groups of elliptic curves over the* $\mathbb{Z}_p$*-extensions of* $\mathbb{Q}$. New York J. Math., 27:99–123, 2021. ↑ 22, 31.

[20] Clark, P. L., T. Genao, P. Pollack, and F. Saia: *The least degree of a CM point on a modular curve*. J. London. Math. Soc., 105(2):825–883, 2022. ↑ 85, 97.

[21] Cohen, H., G. Frey, R. Avanzi, C. Doche, T. Lange, K. Nguyen, and F. Vercauteren (editors): *Handbook of elliptic and hyperelliptic curve cryptography*. Discrete Mathematics and its Applications (Boca Raton). Chapman & Hall/CRC, Boca Raton, FL, 2006, ISBN 978-1-58488-518-4; 1-58488-518-1. ↑ 19.

[22] Coleman, R. F.: *Effective Chabauty*. Duke Math. J., 52(3):765–770, 1985, ISSN 0012-7094. https://doi.org/10.1215/S0012-7094-85-05240-8. ↑ 90.

[23] Coleman, R. F.: *Torsion points on curves and p-adic abelian integrals*. Ann. of Math. (2), 121(1):111–168, 1985, ISSN 0003-486X. https://doi.org/10.2307/1971194. ↑ 90.

[24] Cremona, J. and F. Najman: $\mathbb{Q}$*-curves over odd degree number fields*. Res. Number Theory, 7(4):Paper No. 62, 30, 2021, ISSN 2522-0160. https://doi.org/10.1007/s40993-021-00270-0. ↑ 7, 51, 64, 80, 82.

[25] Derickx, M., A. Etropolski, M. van Hoeij, J. S. Morrow, and D. Zureick-Brown: *Sporadic cubic torsion*. Algebra Number Theory, 15(7):1837–1864, 2021, ISSN 1937-0652. ↑ 21, 87.

[26] Derickx, M., S. Kamienny, W. Stein, and M. Stoll: *Torsion points on elliptic curves over number fields of small degree*. https://arxiv.org/abs/1707.00364, Algebra Number Theory, to appear. ↑ 21.

[27] Derickx, M. and A. V. Sutherland: *Optimized equations for $X_1(m,mn)$*. 2017. https://math.mit.edu/~drew/X1mn.html. ↑ 14.

[28] Derickx, M. and A. V. Sutherland: *Torsion subgroups of elliptic curves over quintic and sextic number fields*. Proc. Amer. Math. Soc., 145(10):4233–4245, 2017, ISSN 0002-9939. https://doi.org/10.1090/proc/13605. ↑ 13.

[29] Diamond, F. and J. Shurman: *A First Course in Modular Forms*, volume 228 of *Graduate Texts in Mathematics*. Springer New York, NY, first edition, 2005, ISBN 978-0-387-23229-4. ↑ 14.

[30] Dickson, L. E.: *Linear groups: With an exposition of the Galois field theory*. Leipzig: B. G. Teubner., 1901. ↑ 10.

[31] Elkies, N. D.: *On elliptic K-curves*. In *Modular curves and Abelian varieties. Based on lectures of the conference, Bellaterra, Barcelona, July 15–18, 2002*, pages 81–91. Basel: Birkhäuser, 2004, ISBN 3-7643-6586-2. ↑ 7, 22.

[32] Elkies, N. D.: *$\mathbb{Z}^{28}$ in $E(\mathbb{Q})$ etc.* https://web.math.pmf.unizg.hr/~duje/tors/rk28.html, 2006. ↑ 3.

[33] Ellenberg, J. S.: *Galois representations attached to $\mathbb{Q}$-curves and the generalized fermat equation $A^4 + B^2 = C^p$*. Am. J. Math., 126(4):763–787, 2004, ISSN 0002-9327. ↑ 82.

[34] Galbraith, S. D.: *Equations for Modular Curves*. 1996. https://www.math.auckland.ac.nz/~sgal018/thesis.pdf, DPhil Thesis, University of Oxford. ↑ 15, 16.

[35] González, Josep: *Equations of bielliptic modular curves*. JP J. Algebra Number Theory Appl., 27(1):45–60, 2012, ISSN 0972-5555. ↑ 85.

[36] González-Jiménez, E. and F. Najman: *Growth of torsion groups of elliptic curves upon base change*. Math. Comp., 89(323):1457–1485, 2020, ISSN 0025-5718. https://doi.org/10.1090/mcom/3478. ↑ 21, 22, 24, 29, 36, 37, 42, 47.

[37] González-Jiménez, E. and J. M. Tornero: *Torsion of rational elliptic curves over quadratic fields II*. Rev. R. Acad. Cienc. Exactas Fís. Nat. Ser. A Mat. RACSAM, 110(1):121–143, 2016, ISSN 1578-7303. https://doi.org/10.1007/s13398-015-0223-9. ↑ 34.

[38] González-Jiménez, Enrique: *Complete classification of the torsion structures of rational elliptic curves over quintic number fields*. J. Algebra, 478:484–505, 2017, ISSN 0021-8693. https://doi.org/10.1016/j.jalgebra.2017.01.012. ↑ 21.

[39] González-Jiménez, Enrique and Álvaro Lozano-Robledo: *Elliptic curves with abelian division fields*. Math. Z., 283(3-4):835–859, 2016, ISSN 0025-5874. https://doi.org/10.1007/s00209-016-1623-z. ↑ 44.

[40] Greenberg, R.: *The image of Galois representations attached to elliptic curves with an isogeny*. Amer. J. Math., 134(5):1167–1196, 2012, ISSN 0002-9327. https://doi.org/10.1353/ajm.2012.0040. ↑ 63.

[41] Gužvić, T. and I. Krijan: *Torsion groups of elliptic curves over some infinite abelian extensions of* $\mathbb{Q}$. https://arxiv.org/abs/2003.08308, Submitted. ↑ ii, iv, 31, 33.

[42] Gužvić, T. and B. Vukorepa: *Torsion groups of elliptic curves over* $\mathbb{Q}(\mu_{p^\infty})$. https://arxiv.org/abs/2206.15208. ↑ 31.

[43] Gužvić, Tomislav: *Torsion of elliptic curves with rational j-invariant defined over number fields of prime degree*. Proc. Amer. Math. Soc., 149(8):3261–3275, 2021, ISSN 0002-9939. https://doi.org/10.1090/proc/15500. ↑ 21.

[44] Gužvić, T.: *Torsion growth of rational elliptic curves in sextic number fields*. Journal of Number Theory, 220:330–345, 2021. https://doi.org/10.1016/j.jnt.2020.09.010. ↑ 22, 47.

[45] Gužvić, T.: *Torsion of elliptic curves with rational j-invariant over number fields*. https://web.math.pmf.unizg.hr/~tguzvic/PHD.pdf, PhD thesis, 2021. ↑ 43, 48.

[46] Harris, J. and J. H. Silverman: *Bielliptic curves and symmetric products*. Proc. Am. Math. Soc., 112(2):347–356, 1991, ISSN 0002-9939. ↑ 78.

[47] Igusa, J. I.: *Kroneckerian model of fields of elliptic modular functions*. Amer. J. Math., 81:561–577, 1959, ISSN 0002-9327. https://doi.org/10.2307/2372914. ↑ 60.

[48] Kamienny, S.: *Torsion points on elliptic curves and q-coefficients of modular forms*. Invent. Math., 109(2):221–229, 1992, ISSN 0020-9910. http://dx.doi.org/10.1007/BF01232025. ↑ 4, 21.

[49] Katz, N. M.: *Galois properties of torsion points on abelian varieties*. Invent. Math., 62(3):481–502, 1981, ISSN 0020-9910. https://doi.org/10.1007/BF01394256. ↑ 26.

[50] Katz, N. M. and B. Mazur: *Arithmetic moduli of elliptic curves*, volume 108 of *Annals of Mathematics Studies*. Princeton University Press, Princeton, NJ, 1985, ISBN 0-691-08349-5; 0-691-08352-5. https://doi.org/10.1515/9781400881710. ↑ 61.

[51] Kenku, M. A.: *On the modular curves $X_0(125)$, $X_1(25)$ and $X_1(49)$*. J. Lond. Math. Soc., II. Ser., 23:415–427, 1981, ISSN 0024-6107. ↑ 6, 22.

[52] Kenku, M. A. and F. Momose: *Torsion points on elliptic curves defined over quadratic fields*. Nagoya Math. J., 109:125–149, 1988, ISSN 0027-7630. http://projecteuclid.org/euclid.nmj/1118780896. ↑ 4, 21.

[53] Kolyvagin, V. A. and D. Yu. Logachëv: *Finiteness of the Shafarevich-Tate group and the group of rational points for some modular abelian varieties*. Algebra i Analiz, 1(5):171–196, 1989, ISSN 0234-0852. ↑ 75, 87.

[54] Krijan, I.: *Torsion groups of elliptic curves over infinite abelian extensions of $\mathbb{Q}$*. https://web.math.pmf.unizg.hr/~ikrijan/pdfs/disertacija.pdf, Phd thesis, 2020. ↑ 43.

[55] Laska, M. and M. Lorenz: *Rational points on elliptic curves over $\mathbb{Q}$ in elementary abelian 2-extensions of $\mathbb{Q}$*. J. Reine Angew. Math., 355:163–172, 1985, ISSN 0075-4102. https://doi.org/10.1515/crll.1985.355.163. ↑ 34.

[56] Le Fourn, S. and P. Lemos: *Residual Galois representations of elliptic curves with image contained in the normaliser of a nonsplit Cartan*. Algebra Number Theory, 15(3):747–771, 2021, ISSN 1937-0652. ↑ 22, 88.

[57] Lombardo, D. and S. Tronto: *Some uniform bounds for elliptic curves over $\mathbb{Q}$*. 2021. https://arxiv.org/pdf/2106.09950.pdf. ↑ 60, 61, 66.

[58] Lozano-Robledo, Á.: *On the field of definition of p-torsion points on elliptic curves over the rationals*. Math. Ann., 357(1):279–305, 2013, ISSN 0025-5831. https://doi.org/10.1007/s00208-013-0906-5. ↑ 42, 53, 54, 56, 72.

[59] Mazur, B.: *A question about quadratic points on $X_0(N)$*. available at https://people.math.harvard.edu/~mazur/papers/2021.07.20.Scorecard.pdf. ↑ 78.

[60] Mazur, B.: *Modular curves and the Eisenstein ideal*. Inst. Hautes Études Sci. Publ. Math., (47):33–186 (1978), 1977, ISSN 0073-8301. http://www.numdam.org/item?id=PMIHES_1977__47__33_0. ↑ 6, 22, 87.

[61] Mazur, B.: *Rational isogenies of prime degree (with an appendix by D. Goldfeld)*. Invent. Math., 44(2):129–162, 1978, ISSN 0020-9910. http://dx.doi.org/10.1007/BF01390348. ↑ 3, 21.

[62] McCallum, W. and B. Poonen: *The method of Chabauty and Coleman*. In *Explicit methods in number theory*, volume 36 of *Panor. Synthèses*, pages 99–117. Soc. Math. France, Paris, 2012. ↑ 90.

[63] Merel, L.: *Bornes pour la torsion des courbes elliptiques sur les corps de nombres*. Invent. Math., 124(1-3):437–449, 1996, ISSN 0020-9910. http://dx.doi.org/10.1007/s002220050059. ↑ 21.

[64] Momose, F.: *Rational points on the modular curves $(X_0^+(N))$*. J. Math. Soc. Japan, 39:269–286, 1987, ISSN 0025-5645. ↑ 84.

[65] Momose, F.: *Isogenies of prime degree over number fields*. Compos. Math., 97(3):329–348, 1995, ISSN 0010-437X. http://www.numdam.org/item?id=CM_1995__97_3_329_0. ↑ 22.

[66] Momose, F. and M. Shimura: *Lifting of supersingular points on $X_0(p^r)$ and lower bound of ramification index*. Nagoya Math. J., 165:159–178, 2002, ISSN 0027-7630. https://doi.org/10.1017/S0027763000008199. ↑ 62, 67, 69.

[67] Mordell, L. J.: *On the rational solutions of the indeterminate equations of the third and fourth degrees*. Proc. Cambridge Phil. Soc., 22:179–192, 1922. ↑ 3.

[68] Najman, F.: *Complete classification of torsion of elliptic curves over quadratic cyclotomic fields*. J. Number Theory, 130(9):1964–1968, 2010, ISSN 0022-314X. ↑ 21.

[69] Najman, F.: *Torsion of elliptic curves over cyclotomic quadratic fields*. Math. J. Okayama Univ., 53:75–82, 2011. https://web.math.pmf.unizg.hr/~fnajman/tors_kon.pdf. ↑ 38, 42, 43, 44.

[70] Najman, F.: *Exceptional elliptic curves over quartic fields*. Int. J. Number Theory, 8(5):1231–1246, 2012, ISSN 1793-0421. https://doi.org/10.1142/S1793042112500716. ↑ 38.

[71] Najman, F.: *Torsion of rational elliptic curves over cubic fields and sporadic points on $X_1(n)$*. Math. Res. Lett., 23(1):245–272, 2016. https://dx.doi.org/10.4310/MRL.2016.v23.n1.a12. ↑ 21, 24.

[72] Najman, F.: *Isogenies of non-CM elliptic curves with rational j-invariants over number fields*. Math. Proc. Cambridge Philos. Soc., 164(1):179–184, 2018, ISSN 0305-0041. https://doi.org/10.1017/S0305004117000160. ↑ 22, 26, 49, 51.

[73] Najman, F. and B. Vukorepa: *Quadratic points on bielliptic modular curves*. https://arxiv.org/pdf/2112.03226v1.pdf. ↑ 75, 80.

[74] Ozman, E. and S. Siksek: *Quadratic points on modular curves*. Math. Comp., 88(319):2461–2484, 2019, ISSN 0025-5718. https://doi.org/10.1090/mcom/3407. ↑ 14, 23, 70, 71, 72, 75, 79, 86, 88.

[75] Parent, P.: *Towards the triviality of $X_0^+(p^r)(\mathbb{Q})$ for $r > 1$*. Compos. Math., 141(3):561–572, 2005, ISSN 0010-437X. https://doi.org/10.1112/S0010437X04001022. ↑ 61.

[76] Poonen, B. and E. F. Schaefer: *Explicit descent for Jacobians of cyclic covers of the projective line*. J. Reine Angew. Math., 488:141–188, 1997, ISSN 0075-4102. ↑ 18.

[77] Rabarison, F. Patrick: *Structure de torsion des courbes elliptiques sur les corps quadratiques*. Acta Arith., 144(1):17–52, 2010, ISSN 0065-1036. https://doi.org/10.4064/aa144-1-3. ↑ 14, 38, 39.

[78] Rouse, J., A. Sutherland, and D. Zureick-Brown: *l-adic images of Galois for elliptic curves over $\mathbb{Q}$*. https://arxiv.org/abs/2106.11141. ↑ 11, 67.

[79] Rouse, J. and D. Zureick-Brown: *Elliptic curves over $\mathbb{Q}$ and 2-adic images of Galois*. Res. Number Theory, 1:Paper No. 12, 34, 2015, ISSN 2522-0160. https://doi.org/10.1007/s40993-015-0013-7. ↑ 11, 69.

[80] Serre, J. P.: *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques*. Invent. Math.., 15(4):259–331, 1972. ↑ 10, 11.

[81] Serre, J. P.: *Quelques applications du théorème de densité de Chebotarev*. Inst. Hautes Études Sci. Publ. Math., (54):323–401, 1981, ISSN 0073-8301. http://archive.numdam.org/article/PMIHES_1981__54__123_0.pdf. ↑ 10.

[82] Siksek, S.: *Chabauty for symmetric powers of curves*. Algebra Number Theory, 3(2):209–236, 2009, ISSN 1937-0652. https://doi.org/10.2140/ant.2009.3.209. ↑ ii, iv, 74, 80, 90.

[83] Siksek, S.: *Explicit Arithmetic of Modular Curves*. https://homepages.warwick.ac.uk/staff/S.Siksek/teaching/modcurves/lecturenotes.pdf, 2019. ↑ 7, 13, 14, 15, 17, 18, 25, 26, 43, 44, 87.

[84] Silverman, J. H.: *The Arithmetic of Elliptic Curves*, volume 106 of *Graduate Texts in Mathematics*. Springer, Dordrecht, second edition, 2009, ISBN 978-0-387-09493-9. http://dx.doi.org/10.1007/978-0-387-09494-6. ↑ 1, 2, 3, 5, 6, 8, 25.

[85] Silverman, J. H. and J. T. Tate: *Rational Points on Elliptic Curves*, volume 106 of *Undergraduate Texts in Mathematics*. Springer Cham, second edition, 2015, ISBN 978-3-319-18587-3. ↑ 8, 9.

[86] Stein, W.: *Explicit approaches to modular abelian varieties*. ProQuest LLC, Ann Arbor, MI, 2000, ISBN 978-0599-86094-0. http://gateway.proquest.com/openurl?url_ver=Z39.88-2004&rft_val_fmt=info:ofi/fmt:kev:mtx:dissertation&res_dat=xri:pqdiss&rft_dat=xri:pqdiss:9979818, Thesis (Ph.D.)–University of California, Berkeley. ↑ 75, 87.

[87] Stein, W.: *Modular forms, a computational approach*, volume 79 of *Graduate Studies in Mathematics*. American Mathematical Society, Providence, RI, 2007, ISBN 978-0-8218-3960-7; 0-8218-3960-8. https://doi.org/10.1090/gsm/079, With an appendix by Paul E. Gunnells. ↑ 75, 87.

[88] Stoll, M.: *On the height constant for curves of genus two. II*. Acta Arith., 104(2):165–182, 2002, ISSN 0065-1036. https://doi.org/10.4064/aa104-2-6. ↑ 75.

[89] Sutherland, A. V.: *Constructing elliptic curves over finite fields with prescribed torsion*. Math. Comp., 81(278):1131–1147, 2012, ISSN 0025-5718. https://doi.org/10.1090/S0025-5718-2011-02538-X. ↑ 14.

[90] Sutherland, A. V.: *Computing images of Galois representations attached to elliptic curves*. Forum Math. Sigma, 4:Paper No. e4, 79, 2016. https://doi.org/10.1017/fms.2015.33. ↑ 10, 29.

[91] Sutherland, A. V. and M. van Hoeij: *Optimized equations for $X_1(N)$*. 2014. https://math.mit.edu/~drew/X1_optcurves.html. ↑ 14.

[92] Sutherland, A. V. and D. Zywina: *Modular curves of prime-power level with infinitely many rational points*. Algebra Number Theory, 11(5):1199–1229, 2017, ISSN 1937-0652. https://doi.org/10.2140/ant.2017.11.1199. ↑ 68.

[93] Trbović, A.: *Torsion groups of elliptic curves over quadratic fields* $\mathbb{Q}(\sqrt{d})$, $0 < d < 100$. Acta Arith., 192:141–153, 2020. https://arxiv.org/abs/1806.05993. ↑ 19, 21.

[94] Vukorepa, B.: *Isogenies over quadratic fields of elliptic curves with rational j-invariant*. https://arxiv.org/abs/2203.10672. ↑ 49.

[95] Washington, C. L.: *Elliptic curves. Number theory and cryptography*. Boca Raton, FL: Chapman and Hall/CRC, 2nd ed. edition, 2008, ISBN 978-1-4200-7146-7. ↑ 4, 5.

[96] Weil, A.: *L'arithmétique sur les courbes algébriques*. Acta Math., 52.1:281–315, 1929. ↑ 3.

[97] Yoo, H.: *The rational torsion of* $J_0(n)$. preprint, available at https://arxiv.org/abs/2106.01020. ↑ 88.

[98] Zywina, D.: *On the possible images of the mod l representations associated to elliptic curves over* $\mathbb{Q}$. 2015. https://arxiv.org/pdf/1508.07660.pdf. ↑ 10, 52, 53, 54, 60, 66, 68, 72.

CURRICULUM VITAE

Borna Vukorepa was born on the 16th of October 1994 in Zagreb. He studied mathematics at the Department of Mathematics of the Faculty of Science, University of Zagreb from 2013. He graduated with the thesis ”Torsion subgroups of elliptic curves” (”Torzijske podgrupe eliptičkih krivulja”) in 2018 under the supervision of Filip Najman. In 2018, he started working as a research assistant at the Department of Mathematics of the Faculty of Science, University of Zagreb where he enrolled in the PhD program. He participated in numerous mathematical competitions, the highlight being the International Mathematical Olympiad in 2013 where he won gold medal.