Torsion of elliptic curves with rational j-invariant over number fields

Gužvić, Tomislav

Doctoral thesis / Disertacija

2021

Degree Grantor / Ustanova koja je dodijelila akademski / stručni stupanj: **University of Zagreb, Faculty of Science / Sveučilište u Zagrebu, Prirodoslovno-matematički fakultet**

Permanent link / Trajna poveznica: https://urn.nsk.hr/urn:nbn:hr:217:445466

Rights / Prava: In copyright / Zaštićeno autorskim pravom.

Download date / Datum preuzimanja: **2024-03-29**



Repository / Repozitorij:

Repository of the Faculty of Science - University of Zagreb







University of Zagreb

FACULTY OF SCIENCE

DEPARTMENT OF MATHEMATICS

Tomislav Gužvić

Torsion of elliptic curves with rational j-invariant over number fields

DOCTORAL DISSERTATION

Zagreb, 2021.



University of Zagreb

FACULTY OF SCIENCE

DEPARTMENT OF MATHEMATICS

Tomislav Gužvić

Torsion of elliptic curves with rational j-invariant over number fields

DOCTORAL DISSERTATION

Supervisor:

izv. prof. dr. sc. Filip Najman

Zagreb, 2021.



Sveučilište u Zagrebu

PRIRODOSLOVNO–MATEMATIČKI FAKULTET

MATEMATIČKI ODSJEK

Tomislav Gužvić

Torzija eliptičkih krivulja s racionalnom j-invarijantom nad poljima algebarskih brojeva

DOKTORSKI RAD

Mentor:

izv. prof. dr. sc. Filip Najman

Zagreb, 2021.

ACKNOWLEDGEMENTS

First and foremost, I have to thank my parents for their support throughout my life.

The author would like to thank his advisor, Filip Najman, for the multitude of helpful conversations, guidance and support during the last few years.

The author is immensely thankful to Harris Daniels for all the helpful discussions we had during the last year.

The author is thankful to David Zureick-Brown, Maarten Derickx, Jackson S. Morrow for their help and advice. I am thankful to Ivan Krijan for a fruitful collaboration and his help with technical aspect of this thesis.

Many thanks to Nikola Adžaga, Andrej Dujella and Matija Kazalicki for reading this thesis and for pointing out the mistakes in previous versions of this thesis.

The author acknowledges support 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

In this thesis we will classify the possible torsion structures of elliptic curves with rational j-invariant defined over number fields.

We start with elliptic curves defined over $\mathbb{Q}$. Let K be a sextic number field. We determine all the possibilities G for $E(K)_{tors}$ and we prove that for each such possible group G, with the exception of the group $C_3 \oplus C_{18}$, that there exist an elliptic curve $E/\mathbb{Q}$ and a sextic number field K such that $E(K)_{tors} \cong G$. Additionally, we provide a partial result regarding the group $C_3 \oplus C_{18}$.

For a positive integer d, define $\Phi(d)$ to be the set of possible isomorphism classes of groups $E(K)_{tors}$, where K runs through all number fields K of degree d and E runs through all elliptic curves over K.

For a positive integer d, define $\Phi_{\mathbb{Q}}(d)$ to be the set of possible isomorphism classes of groups $E(K)_{tors}$, where K runs through all number fields K of degree d and E runs through all elliptic curves over $\mathbb{Q}$.

Define $\Phi_{j\in\mathbb{Q}}(d)$ to be the set of possible isomorphism classes of groups $E(K)_{tors}$, where K runs through all number fields K of degree d and E runs through all elliptic curves over K with $j(E) \in \mathbb{Q}$.

With the help of the previously mentioned result, we are able to completely determine the sets $\Phi_{j\in\mathbb{Q}}(p)$, where p is a prime number. More precisely, our result is the following. Let K be a number field such that $[K : \mathbb{Q}] = p$ and E/K an elliptic curve with rational j-invariant. The following holds:

1. If $p \geq 7$, then $E(K)_{tors} \in \Phi(1)$.

2. If $p = 3$ or $p = 5$, then $E(K)_{tors} \in \Phi_{\mathbb{Q}}(p)$.

3. If $p = 2$, then $E(K)_{tors} \in \Phi_{\mathbb{Q}}(2)$ or $E(K)_{tors} \cong \mathbb{Z}/13\mathbb{Z}$.

In the sixth chapter, we are able to determine all the sets $\Phi_{\mathbb{Q}}(pq)$, where p and q are prime numbers. Most of these cases follow easily from previously known results and the results in the first two chapters of this thesis. In most cases we have $\Phi_{\mathbb{Q}}(pq) = \Phi_{\mathbb{Q}}(p) \cup \Phi_{\mathbb{Q}}(q)$. A detailed description of the sets $\Phi_{\mathbb{Q}}(pq)$ can be found in the fifth chapter of this thesis.

Some of the proofs in the thesis rely on extensive computations in Magma [3]. All of the programs and calculations used for the proofs can be found in the last chapter.

SAŽETAK

U ovoj disertaciji odredit ćemo moguće torzijske strukture eliptičkih krivulja s racionalnom j-invarijantom definiranih nad nekim poljem algebarskih brojeva .

Prvo ćemo promatrati eliptičke krivulje definirane nad $\mathbb{Q}$. Neka je K sekstično polje. Odredit ćemo sve mogućnosti G za $E(K)_{tors}$ i dokazati da za svaku moguću grupu G osim $C_3 \oplus C_{18}$ postoji eliptička krivulja $E/\mathbb{Q}$ i sekstično polje K takvo da je $E(K)_{tors} \cong G$. Nadalje, dokazat ćemo parcijalni rezultat za grupu $C_3 \oplus C_{18}$.

Za prirodan broj d definiramo $\Phi(d)$ kao skup mogućih klasa izomorfizama grupa $E(K)_{tors}$, gdje K varira po svim poljima algebarskih brojeva K stupnja d i E varira po svim eliptičkim krivuljama nad K.

Za prirodan broj d definiramo $\Phi_{\mathbb{Q}}(d)$ kao skup mogućih klasa izomorfizama grupa $E(K)_{tors}$, gdje K varira po svim poljima algebarskih brojeva K stupnja d i E varira po svim eliptičkim krivuljama nad $\mathbb{Q}$.

Za prirodan broj d definiramo $\Phi_{j\in\mathbb{Q}}(d)$ kao skup mogućih klasa izomorfizama grupa $E(K)_{tors}$, gdje K varira po svim poljima algebarskih brojeva K stupnja d i E varira po svim eliptičkim krivuljama nad K, te $j(E) \in \mathbb{Q}$.

Uz pomoć prethodnog rezultata u mogućnosti smo u potpunosti odrediti skupove $\Phi_{j\in\mathbb{Q}}(p)$, gdje je p prost broj. Preciznije, naši rezultati su sljedeći. Neka je K polje algebarskih brojeva takvo da je $[K:\mathbb{Q}] = p$ i E/K eliptička krivulja s racionalnom j-invarijantom. Tada

1. Ako je $p \geq 7$, tada $E(K)_{tors} \in \Phi(1)$.

2. Ako je $p = 3$ ili $p = 5$, tada $E(K)_{tors} \in \Phi_{\mathbb{Q}}(p)$.

3. Ako je $p = 2$, tada $E(K)_{tors} \in \Phi_{\mathbb{Q}}(2)$ ili $E(K)_{tors} \cong \mathbb{Z}/13\mathbb{Z}$.

U šestom poglavlju odredit ćemo sve skupove $\Phi_{\mathbb{Q}}(pq)$, gdje su p i q prosti brojevi. Mnoge takve skupove ćemo odrediti koristeći već poznate rezultate, te rezultate dokazane u drugom i trećem poglavlju. U većini slučajeva vrijedit će

$$\Phi_{\mathbb{Q}}(pq) = \Phi_{\mathbb{Q}}(p) \cup \Phi_{\mathbb{Q}}(q).$$

Detaljniji opis skupova $\Phi_{\mathbb{Q}}(pq)$ može se pronaći u petom poglavlju.

Dokazi nekih rezultata u ovoj disertaciji temelje se na računanju u Magmi [3]. Svi programi i izračuni korišteni u dokazima mogu se pronaći u posljednjem poglavlju.

CONTENTS

1 Introduction **1**

2 Known results **6**

2.1 Auxiliary results 7

3 Theoretical background **11**

3.1 The Weil pairing 11

3.2 Division polynomials 14

3.3 Galois representations 16

4 Torsion growth over sextic number fields **21**

4.1 Auxiliary results 21

4.2 Cyclic cases 24

4.3 Groups of the form $C_2 \oplus C_{2n}$ 26

4.4 Groups of the form $C_3 \oplus C_{3n}$ 27

4.5 Groups of the form $C_m \oplus C_{mn}$, $m \geq 4$ 28

4.6 Group $C_3 \oplus C_{18}$ 30

5 Torsion of elliptic curves with rational j-invariant **34**

5.1 Results 34

5.2 Classification of $\Phi_{j \in \mathbb{Q}}(p)$ 37

5.3 Proof of Theorem 5.1.2 (1) 43

5.4 Proof of Theorem 5.1.2 (2), case $p = 5$ 45

5.5 Proof of Theorem 5.1.2 (2), case $p = 3$ 48

5.6 Proof of Theorem 5.1.2 (3) 49

6 Torsion growth over number fields of degree pq **51**

6.1 Elliptic curves with CM 65

6.2 The set $\Phi_{\mathbb{Q}}(9)$ 68

6.2.1 Appendix: Images of Mod p Galois representations associated to elliptic curves over $\mathbb{Q}$ 74

7 Magma code used in the paper **76**

Conclusion **111**

Bibliography **112**

Curriculum Vitae **119**

1. INTRODUCTION

Definition 1.0.1. Let K be a number field and let $F \in K[x,y,z]$ be a homogenous polynomial. The set

$$C_F := \{P \in \mathbb{P}^2(K) : F(P) = 0\}$$

is the set of K-rational points on the curve C. The degree of a projective curve C is defined as the degree of the polynomial F.

A classical problem in number theory is to determine whether a certain curve C defined over a number field K has a K-rational point. Denote by $C(K)$ the set of K-rational points on C. If we know that a given curve C has a K-rational point, then it is natural to ask what is the cardinality of the set $C(K)$. If $card(C(K))$ is finite, can we determine $card(C(K))$? Can we find all the points on $C(K)$?

Let C be a smooth irreducible projective curve.

A celebrated theorem of Faltings gives an answer to some of the questions raised above.

Theorem 1.0.2. Let C be a smooth, irreducible, projective curve of genus at least 2 defined over number field K. Then the set $C(K)$ is finite.

It is natural to ask ourselves what happens if the curve C has genus equal to 1 or 0. In the second case, an elementary argument can be used to show that $C(K)$ is either empty or infinite. It remains to consider the case when C has genus 1.

In this thesis we will exclusively work with elliptic curves defined over number fields. We are interested in understanding the number theoretic properties of such curves. To begin with, we will list the basic definitions and results in the theory of elliptic curves.

Definition 1.0.3. Let K be a number field. An elliptic curve E defined over K is a smooth projective curve of genus 1 with a distinguished K-rational point O.

We note that although E is a projective curve, we will always use its affine model.

Lemma 1.0.4. Let K be a number field and E/K an elliptic curve. Then E has a model of the form

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

where $a_i \in K$, for all i. This model is called the long Weierstrass model of an elliptic curve E.

Since the characteristic of any number field is 0, we can actually obtain a simpler model for E,

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

where $a, b \in K$. This is called the short Weierstrass model.

Definition 1.0.5. Let K be a number field and E/K an elliptic curve. Assume that E is given in its short Weierstrass form. The discriminant $\Delta(E)$ of elliptic curve E is defined as

$$\Delta(E) := -16(4a^3 + 27b^2).$$

It is worth noting that the discriminant $\Delta(E)$ is equal (up to a constant 16) to the discriminant of the cubic polynomial $x^3 + ax + b$. It can be shown that E is smooth if and only if $\Delta(E) \neq 0$.

Obviously we can have different Weierstrass models for the same elliptic curve. In that case, we would like to have a way to see whether two Weierstrass models correspond to the same elliptic curve.

Definition 1.0.6. The j-invariant of an elliptic curve E/K is

$$j = j(E) = \frac{1728(-4a)^3}{\Delta(E)}.$$

We say that the elliptic curves

$$E : \ y^2 = x^3 + ax + b \text{ and } E' : \ y^2 = x^3 + a'x + b',$$

where $a, b, a', b' \in K$ are isomorphic (over a field L containing K) if there exists $u \in L \setminus \{0\}$ such that

$$a' = u^4 a,$$

$$b' = u^6 b.$$

If we are given two elliptic curves E and E', it is easier to see if they are isomorphic over $\overline{K}$ by using the j-invariant.

Proposition 1.0.7 ([50, Proposition 1.4])**.** Let E/K and E'/K be elliptic curves defined over a field K. Then

1. E and E' are isomorphic over $\bar{K}$ if and only if $j(E) = j(E')$.

2. For every $j \in K$, there exists an elliptic curve E_1/K such that $j = j(E_1)$.

We have seen that if elliptic curves E/K and E'/K have the same j-invariants, then they are isomorphic over $\bar{K}$. Actually, we can do much better then that. Most of the time these curves will be isomorphic over a quadratic extension L of K.

Proposition 1.0.8. Let E/K and E'/K be elliptic curves such that $j = j(E) = j(E')$. If $j \notin \{0, 1728\}$, then there exists a quadratic extension L of K such that E and E' are isomorphic over L.

We can define a group operation on the set $E(K)$. A famous theorem of Mordell and Weil tells us much more.

Theorem 1.0.9 (Mordell-Weil)**.** Let K be a number field and let E/K be an elliptic curve. Then the group $E(K)$ is a finitely generated abelian group.

An immediate consequence of this theorem and the classification theorem for finitely generated abelian groups is that

$$E(K) \cong E(K)_{tors} \oplus T^r,$$

where $r \geq 0$ is an integer, called the rank of E over K and $E(K)_{tors}$ denotes the torsion subgroup of $E(K)$.

We now state an important lemma and its corollary. Often when dealing with elliptic curve E/K with rational j-invariant that is not isomorphic to a base change of elliptic curve defined over $\mathbb{Q}$, we will make use of this result by taking a quadratic twist E' of E that is defined over $\mathbb{Q}$ and by studying its torsion growth. That way we can obtain some information about $E(K)_{tors}$.

Lemma 1.0.10 ([21, Theorem 3]). Let L/K be a quadratic extension of number fields and let $L = K(\sqrt{d})$. There exist homomorphisms

$$f : E(K) \oplus E^d(K) \to E(L),$$

$$g : E(L) \to E(K) \oplus E^d(K),$$

such that the kernels and cokernels of f and g are contained in the kernel of multiplication by 2.

Corollary 1.0.11. Let n be an odd integer. Using the same notation as in the previous Lemma, we have

$$E(K)[n] \oplus E^d(K)[n] \cong E(L)[n].$$

Let us now consider the simplest case, when $K = \mathbb{Q}$. It is natural to consider the following question. For an elliptic curve $E/\mathbb{Q}$, what are the possibilities for the rank r of E over $\mathbb{Q}$ and $E(\mathbb{Q})_{tors}$? The first part of the question is still unanswered. We know that there exists an elliptic curve $E/\mathbb{Q}$ with a rank of at least 28. This curve has been found by Noam Elkies and it is currently the elliptic curve with largest known rank. It is not known whether there exists an upper bound for r.

On the other hand, the second part of the question was completely answered by Mazur.

From now on we shall denote $\mathbb{Z}/n\mathbb{Z}$ by C_n.

Theorem 1.0.12 (Mazur, [35]). Let $E/\mathbb{Q}$ be an elliptic curve. Then

$$E(\mathbb{Q})_{tors} \cong \begin{cases} C_m, & m = 1, ..., 10, 12, \\ C_2 \oplus C_{2m}, & m = 1, ..., 4. \end{cases}$$

Following Mazur's theorem on torsion subgroups of elliptic curves over the rational numbers, the possible torsion subgroups of elliptic curves over quadratic number fields were classified by Kamienny and Kenku-Momose:

Theorem 1.0.13 (Kenku, Momose, [31], Kamienny [26]). Let E/F be an elliptic curve

over a quadratic number field F. Then

$$E(F)_{tors} \cong \begin{cases} C_m, & m = 1,...,16,18, \\ C_2 \oplus C_{2m}, & m = 1,...,6, \\ C_3 \oplus C_{3m}, & m = 1,2, \\ C_4 \oplus C_4. \end{cases}$$

One can ask a similar question.

Question. Let $E/\mathbb{Q}$ be an elliptic curve and d a positive integer. What are the possible torsion subgroup structures of $E(K)$, where K is a number field such that $[K:\mathbb{Q}] = d$?

This is a natural question to consider as, apart from being interesting in itself, it is often important to study how the torsion of elliptic curves defined over $\mathbb{Q}$ behaves after a base change to a number field.

Definition 1.0.14. Let E_1/K and E_2/K be elliptic curves defined over a number field K. An isogeny from E_1 to E_2 is a nonconstant morphism $\alpha : E_1 \to E_2$ that is given by rational functions and satisfying $\alpha(0) = 0$.

It can be shown that $\alpha(P+Q) = \alpha(P) + \alpha(Q)$ for all $P, Q \in E_1(\bar{K})$. If there exists an isogeny $\alpha : E_1 \to E_2$, then we say that elliptic curves E_1 and E_2 are isogenous.

An immediate example of an isogeny from one elliptic curve to itself is a multiplication by an integer n. More precisely, let E/K be an elliptic curve defined over a number field K and let n be an integer. Consider a function defined by

$$[n] : E \to E,\ [n](P) := \underbrace{P+P+\ldots+P}_{n\text{-times}}.$$

This is obviously an isogeny.

Definition 1.0.15. Let E/K be an elliptic curve defined over a number field K. We say that E has a complex multiplication (CM) if $\mathrm{End}(E) \supsetneq \mathbb{Z}$.

If $E/\mathbb{Q}$ is an elliptic curve with CM, then $j(E)$ is equal to one of the 13 possible values listed in [49, Appendix 3].

2. KNOWN RESULTS

Let K be a number field such that $[K:\mathbb{Q}] = d$ and let E/K be an elliptic curve. Theorem 1.0.9 shows that $E(K)$ is a finitely generated abelian group. Therefore this group can be decomposed as $E(K) = E(K)_{tors} \oplus \mathbb{Z}^r$, $r \geq 0$. It is known that $E(K)_{tors}$ is of the form $C_m \oplus C_n$ for two positive integers m,n such that m divides n, where C_m and C_n denote cyclic groups of order m and n, respectively.

One of the goals in the theory of elliptic curves is the classification of torsion groups of elliptic curves defined over various fields. We will now briefly describe results related to this thesis.

Let d be a positive integer. Define $\Phi(d)$ to be the set of possible isomorphism classes of groups $E(K)_{tors}$, where K runs through all number fields K of degree d and E runs through all elliptic curves over K. In [37], Merel proved that $\Phi(d)$ is finite for all positive integers d. The set $\Phi(1)$ can be seen in Theorem 1.0.12 and was determined by Mazur [35]. The set $\Phi(2)$ can be seen in Theorem 1.0.13 and was determined by Kenku, Momose and Kamienny [31], [26]. Derickx, Etropolski, Hoeij, Morrow and Zureick-Brown have determined $\Phi(3)$ in [13].

Define $\Phi^{\mathrm{CM}}(d)$ to be the set of possible isomorphism classes of groups $E(K)_{tors}$, where K runs through all number fields K of degree d and E runs through all elliptic curves with complex multiplication (CM). The set $\Phi^{\mathrm{CM}}(1)$ has been determined by Olson in [43] and $\Phi^{\mathrm{CM}}(d)$ for $d = 2,3$ by Zimmer and his collaborators in [15], [40] and [44]. The sets $\Phi^{\mathrm{CM}}(d)$, for $4 \leq d \leq 13$ have been determined by Clark, Corn, Rice and Stankiewicz in [9]. Bourdon and Pollack and Stankewicz have determined torsion groups of CM elliptic curves over odd degree number fields in [5].

Define $\Phi_{\mathbb{Q}}(d) \subseteq \Phi(d)$ to be the set of possible isomorphism classes of groups $E(K)_{tors}$, where K runs through all number fields K of degree d and E runs through all elliptic curves

defined over $\mathbb{Q}$. For $d = 2, 3$, the sets $\Phi_{\mathbb{Q}}(d)$ have been determined by Najman [42] while $\Phi_{\mathbb{Q}}(4)$ has been determined by Chou [7] and González-Jiménez and Najman [19]. The set $\Phi_{\mathbb{Q}}(5)$ has been determined by González-Jiménez in [16]. González-Jiménez and Najman have also proved that $\Phi_{\mathbb{Q}}(p) = \Phi(1)$ for primes $p \geq 7$ in [19]. For an odd prime ℓ and a positive integer d, Propp [45] has determined when there exists a degree d number field K and an elliptic curve E/K with $j(E) \in \mathbb{Q} \setminus \{0, 1728\}$ such that $E(K)_{tors}$ contains a point of order ℓ.

2.1. Auxiliary results

Let E/F be an elliptic curve defined over a number field F. There exists an F-rational cyclic isogeny $\phi : E \to E'$ of degree n if and only if $\langle P \rangle$, where $P \in E(\overline{F})$ is a point of order n, is a $\mathrm{Gal}(\overline{F}/F)$-invariant group; in this case we say that E has an F-rational n-isogeny. When $F = \mathbb{Q}$, the possible degrees of n-isogenies of elliptic curves over $\mathbb{Q}$ are known by the following theorem.

Theorem 2.1.1 (Mazur [36], Kenku [27], [29], [28], [30])**.** Let $E/\mathbb{Q}$ be an elliptic curve with a rational n-isogeny. Then

$$n \in \{1, ..., 19, 21, 25, 27, 37, 43, 67, 163\}.$$

There are infinitely many elliptic curves (up to $\bar{\mathbb{Q}}$-isomorphism) with a rational n-isogeny over $\mathbb{Q}$ for

$$n \in \{1, ..., 10, 12, 13, 16, 18, 25\}$$

and only finitely many for all the other n. If E does not have complex multiplication, then $n \leq 18$ or $n \in \{21, 25, 37\}$.

Now we mention a result which will be used frequently. If $E/\mathbb{Q}$ is an elliptic curve with independent rational m and n-isogenies, we can deduce the existence of a rational mn-isogeny on an isogenous curve $E'/\mathbb{Q}$.

Lemma 2.1.2 ([42, Lemma 7])**.** Let E/F be an elliptic curve with 2 independent F-rational isogenies (the intersection of their kernels is trivial) of degrees m and n. Then E is isogenous (over F) to an elliptic curve E'/F by an F-rational mn-isogeny.

We can ask ourselves what happens with the torsion subgroup of an elliptic curve $E/\mathbb{Q}$ over number fields. More precisely if $E/\mathbb{Q}$ is an elliptic curve and d is a positive integer, what are the possibilities for $E(F)_{tors}$, where F is a number field such that $[F:\mathbb{Q}]=d$? We now mention the results of this type that we will frequently use in this thesis.

Theorem 2.1.3 ([42, Theorem 2])**.** Let $E/\mathbb{Q}$ be an elliptic curve and F a quadratic field. Then

$$E(F)_{tors} \cong \begin{cases} C_m, & m=1,...,10,12,15,16, \\ C_2 \oplus C_{2m}, & m=1,...,6, \\ C_3 \oplus C_{3m}, & m=1,2, \\ C_4 \oplus C_4. \end{cases}$$

Theorem 2.1.4 ([42, Theorem 1])**.** Let $E/\mathbb{Q}$ be an elliptic curve and K a cubic field. Then

$$E(K)_{tors} \cong \begin{cases} C_m, & m=1,...,10,12,13,14,18,21, \\ C_2 \oplus C_{2m}, & m=1,...,4,7. \end{cases}$$

Chou [7] has first partially classified $\Phi_{\mathbb{Q}}(4)$ by considering only quartic Galois number fields. González-Jiménez and Najman [19] have completed the classification by considering the non-Galois number fields.

Theorem 2.1.5 ([7, 19])**.** Let $E/\mathbb{Q}$ be an elliptic curve and K a quartic field. Then

$$E(K)_{tors} \cong \begin{cases} C_m, & m=1,...,10,12,13,15,16,20,24, \\ C_2 \oplus C_{2m}, & m=1,...,6,8, \\ C_3 \oplus C_{3m}, & m=1,2, \\ C_4 \oplus C_{4m}, & m=1,2, \\ C_5 \oplus C_5, \\ C_6 \oplus C_6. \end{cases}$$

Theorem 2.1.6 ([16, Theorem 1])**.** Let $E/\mathbb{Q}$ be an elliptic curve and K a quintic field. Then

$$E(K)_{tors} \cong \begin{cases} C_m, & m=1,...,12,25, \\ C_2 \oplus C_{2m}, & m=1,...,4. \end{cases}$$

The next theorem is one of the most commonly used results in this thesis. When dealing with an elliptic curve $E/\mathbb{Q}$ and studying its torsion growth over number fields of fixed degree d, we always need to know the possibilities for $[\mathbb{Q}(P):\mathbb{Q}]$, where $P \in E(\overline{\mathbb{Q}})_{tors}$.

Theorem 2.1.7 ([19, Theorem 5.8.]). Let $E/\mathbb{Q}$ be an elliptic curve, p a prime and P a point of order p on E. Then all of the cases in the table below occur for $p \leq 13$ or $p = 37$, and they are the only ones possible. The possibilities listed in cases 3., 4. and 5. occur only for CM elliptic curves $E/\mathbb{Q}$.

p	$[\mathbb{Q}(P):\mathbb{Q}]$
2	$1,2,3$
3	$1,2,3,4,6,8$
5	$1,2,4,5,8,10,16,20,24$
7	$1,2,3,6,7,9,12,14,18,21,24,36,42,48$
11	$5,10,20,40,55,80,100,110,120$
13	$3,4,6,12,24,39,48,52,72,78,96,144,156,168$
37	$12,36,72,444,1296,1332,1368$

For all other p, for $[\mathbb{Q}(P):\mathbb{Q}]$ the following cases do occur:

1. p^2-1 for all p,
2. $8,\ 16,\ 32,\ 136,\ 256,\ 272,\ 288$ for $p = 17$,
3. $\frac{p-1}{2},\ p-1,\ \frac{p(p-1)}{2},\ p(p-1)$ if $p \in \{19,43,67,163\}$,
4. $2(p-1),\ (p-1)^2$ if $p \equiv 1 \pmod 3$ or $\frac{-D}{p} = 1$, for some $D \in \{1,2,7,11,19,43,67,163\}$,
5. $\frac{(p-1)^2}{3},\ \frac{2(p-1)^2}{3}$ if $p \equiv 4,7 \pmod 9$,
6. $\frac{p^2-1}{3},\ \frac{2(p^2-1)}{3}$ if $p \equiv 2,5 \pmod 9$,

Apart from the cases above that have been proven to appear, the only other options that might be possible are:

$$\frac{p^2-1}{3},\ \frac{2(p^2-1)}{3}, \quad \text{for } p \equiv 8 \pmod 9.$$

Proposition 2.1.8 ([19, Proposition 4.6.])**.** Let F be a number field and E/F be an elliptic curve. Let p be a prime number, $n \in \mathbb{N}$ and $P \in E(\overline{F})$ a point of order p^{n+1}. Then $[F(P) : F(pP)]$ divides p^2 or $(p-1)p$.

Assume that K is a number field such that $[K : \mathbb{Q}] = d$. Let $E/\mathbb{Q}$ be an elliptic curve and let $P_{p^2} \in E(K)$ be a point of order p^2. We want to determine $[\mathbb{Q}(P_{p^2}) : \mathbb{Q}]$. Obviously $[\mathbb{Q}(P_{p^2}) : \mathbb{Q}(pP_{p^2})]$ divides $[K : \mathbb{Q}] = d$. We also know by the previous proposition that $[\mathbb{Q}(P_{p^2}) : \mathbb{Q}(pP_{p^2})]$ divides $(p-1)p^2$, so it divides the $\gcd((p-1)p^2, d)$. Often we will have that d is either a prime or a product of two primes and p will be a relatively small prime number. That way we will be able to determine the possibilities for $[\mathbb{Q}(P_{p^2}) : \mathbb{Q}]$ without knowing what $G_E(p^2)$ actually is.

We now mention a result proved by Rouse, Sutherland and Zureick-Brown in [46].

Theorem 2.1.9. Let $E/\mathbb{Q}$ be an elliptic curve without CM and let G be the 3-adic representation of E. Let G_{3^k} be the group $G \pmod{3^k}$. Then the corresponding modular curve X_G has genus zero or G_{27} is contained in the normaliser of the non-split Cartan subgroup of level 27, which we will denote by 27Nn.

3. THEORETICAL BACKGROUND

The purpose of this chapter is to explain the basic notation and results which will be used in the thesis. The reader can find more information about the topics we will cover in [54], [50] and [49].

3.1. THE WEIL PAIRING

The Weil pairing on the torsion on an elliptic curve is a major tool in the study of elliptic curves. Let E be an elliptic curve over a number field K and let n be a positive integer. Denote by $E[n]$ the set of n-torsion points on E, i.e.

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

The group $E[n]$ is obviously a subgroup of $E(\overline{K})$. It can be shown that we have

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

Let

$$\mu_n = \{x \in \bar{K} : x^n = 1\}$$

be the group of nth roots of unity in K. This is a cyclic group. Any generator ζ of μ_n is called a primitive nth root of unity.

Theorem 3.1.1. Let E be an elliptic curve defined over a number field K and let n be a positive integer. Then there is a pairing

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

called the Weil pairing, that satisfies the following properties:

- e_n *is bilinear.* This means that for all $S, S_1, S_2, T, T_1, T_2 \in E[n]$ we have

$$e_n(S_1 + S_2, T) = e_n(S_1, T)e_n(S_2, T),$$
$$e_n(S, T_1 + T_2) = e_n(S, T_1)e_n(S, T_2).$$

- e_n *is alternating.* For every $T \in E[n]$ we have

$$e_n(T, T) = 1.$$

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

- e_n *is nondegenerate in each variable.* If $T \in E[n]$ is such that

$$e_n(S, T) = 1, \quad \text{for all } S \in E[n],$$

  then $T = 0$.

- e_n *is Galois invariant.* For each $S, T \in E[n]$ and for all $\sigma \in \mathrm{Gal}(K(E[n])/K)$ we have

$$(e_n(S, T))^\sigma = e_n(S^\sigma, T^\sigma).$$

- For every positive integer m and for all $S \in E[nm]$ and $T \in E[n]$ we have

$$e_{nm}(S, T) = e_n(mS, T).$$

We will derive some consequences of this theorem.

Corollary 3.1.2. Let $\{T_1, T_2\}$ be the basis for $E[n]$. Then $e_n(T_1, T_2)$ is a primitive nth root of unity.

Proof. Suppose that $e_n(T_1, T_2) = \zeta$, with $\zeta^d = 1$ for some positive integer d. Without the loss of generality, assume that d is the smallest positive integer with this property. Then $e_n(T_1, dT_2) = 1$. We also have $e_n(T_2, dT_2) = e_n(T_2, T_2)^d = 1$. Let $S \in E[n]$. Then $S = aT_1 + bT_2$, for some $a, b \in \mathbb{Z}$. Therefore

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

Since the equality holds for all $S \in E[n]$, we have that $dT_2 = 0$. This implies that n divides d. Therefore we conclude that $d = n$ and that $e_n(T_1, T_2) = \zeta$ is a primitive n-th root of unity. ■

We will now mention a fact which will be frequently used in this thesis. It allows us to immediately eliminate possibilities for full torsion over small number fields. We will often have plenty of information about the properties of the number field K so we will be able to deduce that it does not contain certain cyclotomic subfields.

Corollary 3.1.3. If $E[n] \subseteq E(K)$, then $\mu_n \subset K$.

Proof. Let $\sigma \in \mathrm{Gal}(\overline{K}/K)$. Let $\{T_1, T_2\}$ be a basis for $E[n]$. Since $E[n] \subseteq E(K)$, we have $T_1, T_2 \in E(K)$. It follows that $\sigma(T_1) = T_1$ and $\sigma(T_2) = T_2$. Finally we have

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

The fundamental theorem of Galois theory implies that if an element $x \in K$ is fixed by all such automorphisms σ, then $x \in K$. We conclude that $\zeta \in K$. Since ζ is a primitive nth root of unity by the previous corollary, it follows that $\mu_n \subset K$. ■

Corollary 3.1.4. Let E be an elliptic curve defined over $\mathbb{Q}$. Then $E[n] \not\subseteq E(\mathbb{Q})$, for $n \geq 3$.

Proof. By the previous corollary, we have $\mu_n \in \mathbb{Q}$. Therefore $\mathbb{Q}$ contains all primitive nth roots of unity. It is well known that the nth cyclotomic polynomial $\Phi_n(x) \in \mathbb{Z}[x]$ is irreducible and that the degree of $\Phi_n(x)$ is equal to $\phi(n)$, where ϕ denotes the Euler totient function. Let ζ be one root of $\Phi_n(x)$. On the one hand we have $[\mathbb{Q}(\zeta) : \mathbb{Q}] = \phi(n)$, but since $\zeta \in \mathbb{Q}$ by assumption, we need to have $\phi(n) = 1$. We conclude that $n \leq 2$. ■

3.2. DIVISION POLYNOMIALS

Let E be an elliptic curve defined over $\mathbb{Q}$. Assume that the model of E is given by the short Weierstrass form

$$E:\ y^2 = x^3 + Ax + B,$$

where $A, B \in \mathbb{Z}$.

We define division polynomials $\psi_m \in \mathbb{Z}[x,y]$ in the following manner:

$$\begin{aligned}
&\psi_0 = 0,\\
&\psi_1 = 1,\\
&\psi_2 = 2y,\\
&\psi_3 = 3x^4 + 6Ax^2 + 12Bx - A^2,\\
&\psi_4 = 4y(x^6 + 5Ax^4 + 20Bx^3 - 5A^2x^2 - 4ABx - 8B^2 - A^3),\\
&\psi_{2m+1} = \psi_{m+2}\psi_m^3 - \psi_{m-1}\psi_{m+1}^3,\ m \geq 2\\
&\psi_{2m} = (2y)^{-1} \cdot \psi_m \cdot (\psi_{m+2}\psi_{m-1}^2 - \psi_{m-2}\psi_{m+1}^2),\ m \geq 3
\end{aligned}$$

We now define the polynomials

$$\phi_m = x\psi_m^2 - \psi_{m+1}\psi_{m-1},$$

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

Now we state a Theorem which will be extremely useful to us.

Theorem 3.2.1. Let $P = (x,y)$ be a point on the elliptic curve

$$E:\ y^2 = x^3 + Ax + B$$

and let n be a positive integer. Then

$$nP = \Big(\frac{\phi_n(x)}{\psi_n^2(x)}, \frac{\omega_n(x,y)}{\psi_n^3(x,y)}\Big).$$

Division polynomial method

Let $E/\mathbb{Q}$ be an elliptic curve and n a positive integer. We denote by $\psi_{E,n}$ the n-th division polynomial of E. If n is odd, then the roots of $\psi_{E,n}$ are precisely the x-coordinates of

the points $P \in E[n]$. Similarly, if n is even, then the roots of $\psi_{E,n}/\psi_{E,2}$ are precisely the x-coordinates of points $P \in E[n] \setminus E[2]$. Let $f_{E,n}$ denote the corresponding primitive n-division polynomial associated to E, i.e. its roots are the x-coordinates of points P on $E(\overline{\mathbb{Q}})$ of order n. We briefly describe the construction of $f_{E,n}$. If $n = p$ is prime, then $f_{E,p} = \psi_{E,p}$. For an arbitrary n, we have

$$f_{E,n} := \frac{\psi_{E,n}}{\prod_{d|n, d\neq n} f_{E,d}}.$$

Note that if $E^d/\mathbb{Q}$ is a quadratic twist of $E/\mathbb{Q}$, then $\psi_{E,n} = \alpha\psi_{E^d,n}$ and $f_{E,n} = \beta f_{E^d,n}$, for some rational constants α, β. Consider the following question:

Question. Given a rational number j and K a number field of degree d, does there exist an elliptic curve $E/\mathbb{Q}$ such that $j = j(E)$ and $E(K)$ contains a point P of order n?

Let $E_0/\mathbb{Q}$ be any elliptic curve with $j = j(E_0)$. In Magma [3], we compute the primitive division polynomial $f_{E_0,n}$. Since every elliptic curve $E/\mathbb{Q}$ with $j(E) = j$ is a quadratic twist of E_0, we have $f_{E_0,n} = \beta f_{E,n}$, for some rational number β. Next, we factor $f_{E_0,n}$ over $\mathbb{Q}[x]$. Let d' denote the degree of the smallest irreducible factor f of $f_{E_0,n}$ and let x_0 be a root of f. If $d' > d$, then $[\mathbb{Q}(P) : \mathbb{Q}] \geq [\mathbb{Q}(x_0) : \mathbb{Q}] = d' > d = [K : \mathbb{Q}]$ and so a point P of order n on $E(\overline{\mathbb{Q}})$ cannot be defined over K.

3.3. GALOIS REPRESENTATIONS

Let $E/\mathbb{Q}$ be an elliptic curve and let n a positive integer. The field $\mathbb{Q}(E[n])$ is the number field obtained by adjoining to $\mathbb{Q}$ all the x and y-coordinates of the points of $E[n]$. The absolute Galois group $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ acts on $E[n]$ by its action on the coordinates of the points, inducing a mod n Galois representation attached to E:

$$\rho_{E,n} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{Aut}(E[n]).$$

After we fix a basis for the n-torsion, we can identify $\mathrm{Aut}(E[n])$ with $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$. This means that we can consider $\rho_{E,n}(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}))$ as a subgroup of $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$, uniquely determined up to conjugacy. We shall denote $\rho_{E,n}(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}))$ by $G_E(n)$. Moreover, since $\mathbb{Q}(E[n])$ is a Galois extension of $\mathbb{Q}$ and $\ker\rho_{E,n} = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}(E[n]))$, by the first isomorphism theorem we have $G_E(n) \cong \mathrm{Gal}(\mathbb{Q}(E[n])/\mathbb{Q})$.

We would like to know what are the possibilities for $G_E(n)$ as a subgroup of $\mathrm{GL}(\mathbb{Z}/n\mathbb{Z})$. For some values of n, this can be seen in Tables 6.1 and 6.2. For most values of n we do not have a list of possibilities of $G_E(n)$, but we have a result that helps us see if for a given matrix subgroup M of $\mathrm{GL}(\mathbb{Z}/n\mathbb{Z})$ there exists an elliptic curve $E/\mathbb{Q}$ such that $\rho_{E,n}(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})) = M$ (up to conjugation).

Definition 3.3.1 ([55, Definition 2.1])**.** A subgroup G of $\mathrm{GL}(\mathbb{Z}/n\mathbb{Z})$ is called applicable if it satisfies the following conditions:

- $G \neq \mathrm{GL}(\mathbb{Z}/n\mathbb{Z})$
- $-I \in G$ and $\det(G) = (\mathbb{Z}/n\mathbb{Z})^\times$
- G contains an element with trace 0 and determinant -1 that fixes a point in $(\mathbb{Z}/n\mathbb{Z})^2$ of order n.

Proposition 3.3.2 ([55, Proposition 2.2])**.** Let E be an elliptic curve over $\mathbb{Q}$ for which $\rho_{E,n}$ is not surjective. Then $\pm\rho_{E,n}(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}))$ is an applicable subgroup of $\mathrm{GL}(\mathbb{Z}/n\mathbb{Z})$.

We will now briefly introduce the ℓ-adic Galois representation attached to elliptic curve.

Definition 3.3.3. Let E/K be an elliptic curve and let ℓ be a prime number. The Tate module of the elliptic curve E is the group

$$T_\ell(E) = \varprojlim_n E[\ell^n],$$

where the inverse limit is taken with respect to the maps

$$E[\ell^{n+1}] \xrightarrow{[\ell]} E[\ell^n].$$

Definition 3.3.4. Let E/K be an elliptic curve and let ℓ be a prime number. The ℓ-adic Galois representation of E is

$$\rho_\ell \colon \mathrm{Gal}(\overline{K}/K) \to \mathrm{Aut}(T_\ell(E))$$

induced by the action of $\mathrm{Gal}(\overline{K}/K)$ on the Tate module $T_\ell(E)$.

When E does not have CM, Rouse and Zureick-Brown [47] have classified all the possible 2-adic images of $\rho_{E,2^\infty} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{Z}_2)$, and have given explicitly all the 1208 possible images. When denoting certain subgroups of $\mathrm{GL}_2(\mathbb{Z}_2)$ we will use the same notation introduced by Rouse and Zureick-Brown in [47]. Those subgroups will be noted by H_s, where s is a string. The case for CM curves has been done by Lozano-Robledo in [33]. We will use the same notation as in [47] for the 2-adic image of a given elliptic curve $E/\mathbb{Q}$. In [17], González-Jiménez and Lozano-Robledo have determined for each possible image the degree of the field of definition of any 2-subgroup. From the results of [17] one can see if a given 2-subgroup is defined over a number field of given degree d.

Group labels

In this subsection we will define group labels used in this thesis. A more detailed description of these group labels can be found in [51, Page 35]. The explicit set of generators for each group mentioned in this thesis can be found in [51, Table 3].

Let p be an odd prime and $\phi = -1$ if $p \equiv 3 \pmod 4$ and otherwise let $\phi \geq 2$ be the smallest integer such that $(\frac{\phi}{p}) = -1$.

Define the following matrices in $\mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$, for some $a, b \in \mathbb{Z}/p\mathbb{Z}$:

$$D(a,b) = \begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix}, \quad M_\phi(a,b) = \begin{bmatrix} a & b\phi \\ b & a \end{bmatrix}, \quad T = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \quad \text{and} \quad J = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}.$$

We define the following subgroups of $\mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$:

$$\mathrm{pCs} = \{D(a,b) : a,b \in (\mathbb{Z}/p\mathbb{Z})^\times\},$$

$$\mathrm{pCn} = \{D(a,b), T \cdot D(a,b) : a,b \in (\mathbb{Z}/p\mathbb{Z})^\times\},$$

$$\mathrm{pNs} = \{M_\phi(a,b) : a,b \in (\mathbb{Z}/p\mathbb{Z})^2, (a,b) \neq (0,0)\},$$

$$\mathrm{pNn} = \{M_\phi(a,b), J \cdot M_\phi(a,b) : a,b \in (\mathbb{Z}/p\mathbb{Z})^2, (a,b) \neq (0,0)\}.$$

Let pB denote the subgroup of $\mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$ consisting of upper triangular matrices and let r be the smallest positive integer that generates $(\mathbb{Z}/p\mathbb{Z})^\times$.

1. The label pCs.a.b denotes the subgroup of pCs generated by

$$\begin{bmatrix} a & 0 \\ 0 & 1/a \end{bmatrix}, \begin{bmatrix} b & 0 \\ 0 & r/b \end{bmatrix},$$

   with $a,b > 0$ minimal.

2. For $p = 2$, the label 2Cn denotes the index 2 subgroup of $\mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z})$. For $p \geq 3$, the label pCn.a.b denotes the subgroup of pCn generated by

$$\begin{bmatrix} a & b\phi \\ b & a \end{bmatrix}$$

   with $a \geq 0$, $b > 0$ chosen to make (a,b) lexicographically minimal.

3. The label pNs.a.b denotes the subgroup of pNs generated by

$$\begin{bmatrix} a & 0 \\ 0 & 1/a \end{bmatrix}, \begin{bmatrix} 0 & b \\ -r/b & 0 \end{bmatrix},$$

   with $a,b > 0$ minimal.

4. The label pNn.a.b denotes the subgroup of pNn generated by

$$\begin{bmatrix} a & b\phi \\ b & a \end{bmatrix}, J,$$

   with (a,b) lexicographically minimal.

5. The label pB.a.b denotes the subgroup of pB generated by

$$\begin{bmatrix} a & 0 \\ 0 & 1/a \end{bmatrix}, \begin{bmatrix} b & 0 \\ 0 & r/b \end{bmatrix}, \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix},$$

   with $a, b > 0$ minimal.

We now mention a theorem proven by Dickson [14].

Theorem 3.3.5 (Dickson [14])**.** Let H be a subgroup of $\mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$ not containing $\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$. Then (up to conjugation)

1. Either $H \subseteq$ pB (Borel subgroup)
2. or $H \subseteq$ pNs (normalizer of split Cartan)
3. or $H \subseteq$ pNn (normalizer of non-split Cartan)
4. or the image of H in $\mathrm{PSL}_2(\mathbb{Z}/p\mathbb{Z})$ is isomorphic to A_4, S_4 or A_5 (these are called the exceptional subgroups of $\mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$).

A famous question of Serre is the following:

Question. Does there exist $C > 0$ such that for all primes $p > C$ and for all elliptic curves $E/\mathbb{Q}$ without CM, the mod p Galois representation $\rho_{E,p}$ is surjective?

The classification of maximal subgroups of $\mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$ by Dickson is extremely important in the general approach to this problem. The idea is to show the following: for p large enough, there are no elliptic curves without complex multiplication for which the image of $\rho_{E,p}$ is contained in any of these maximal subgroups. The exceptional cases were solved by Serre in [48]. In [36], Mazur solved the Borel case by finding all the possible prime degrees of rational isogenies of elliptic curves defined over $\mathbb{Q}$. Bilu, Parent and Rebolledo studied the case of the normaliser of a split Cartan. In [2], they proved that if $E/\mathbb{Q}$ is an elliptic curve without complex multiplication, and $p \geq 11$ is a prime different from 13, then the image of $\rho_{E,p}$ is not contained in the normaliser of a split Cartan subgroup of $\mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$. The case $p = 13$ has been covered in [1], by Balakrishnan, Dogra, Müller, Tuitman and Vonk. In order to give an answer to the question of Serre, it remains to show that the image of the mod p Galois representation of any elliptic curve defined

over $\mathbb{Q}$ without complex multiplication is not contained in the normaliser of the non-split Cartan subgroup of $\mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$. This is, as of writing this thesis, still an open problem, but some progress has has been made. In [32], Le Fourn and Lemos have shown that if $p > 1.4 \cdot 10^7$ and $E/\mathbb{Q}$ is an elliptic curve without CM, then the image of $\rho_{E,p}$ is equal to $\mathrm{GL}_2(\mathbb{F}_p)$ or to the normaliser of non-split Cartan subgroup of $\mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$.

4. TORSION GROWTH OVER SEXTIC NUMBER FIELDS

This chapter is based on the paper [22].

The main result of this chapter is the following theorem.

Theorem 4.0.1. Let $E/\mathbb{Q}$ be an elliptic curve and let K be a sextic number field. Then

$$E(K)_{tors} \cong \begin{cases} C_m, & m = 1,...,16,18,21,30, m \neq 11, \\ C_2 \oplus C_{2m}, & m = 1,...,7,9, \\ C_3 \oplus C_{3m}, & m = 1,...,4, \\ C_4 \oplus C_{4m}, & m = 1,3, \\ C_6 \oplus C_6, \\ C_3 \oplus C_{18}. \end{cases}$$

Additionally, if E does not have a $\mathbb{Q}$-rational point of order 2, then $E(K)_{tors}$ is not isomorphic to $C_3 \oplus C_{18}$.

We prove the theorem using a series of lemmas. At the end, we briefly discuss what problems occur when we consider the case $C_3 \oplus C_{18}$.

4.1. AUXILIARY RESULTS

From now on, let K denote a degree 6 extension of $\mathbb{Q}$. First we shall handle the CM case. This is done by the next two results.

Proposition 4.1.1 ([11, Proposition 7.]). Let $E/\mathbb{Q}$ be an elliptic curve with CM. Then $11, 13, 17$ and 19 do not divide the order of $E(K)_{tors}$.

Theorem 4.1.2. Let $E/\mathbb{Q}$ be an elliptic curve with CM. Then $E(K)_{tors}$ is one of the groups listed in Theorem 4.0.1.

Proof. By [9, Section 4], we see that the only groups contained in $\Phi^{\mathrm{CM}}(6)$ that do not appear in

$$\Phi_{\mathbb{Q}}(2) \cup \Phi_{\mathbb{Q}}(3) \cup \{C_{30}, C_2 \oplus C_{18}, C_3 \oplus C_9, C_3 \oplus C_{12}, C_4 \oplus C_{12}, C_6 \oplus C_6\}$$

are C_{19} and C_{26}. By Proposition 4.1.1, both of these groups cannot occur. ■

Lemma 4.1.3 ([18, Lemma 2.6, Lemma 2.8, Lemma 2.9]). Let $E/\mathbb{Q}$ be an elliptic curve without CM. Then the following claims hold:

- There are no points of order ℓ^2, where $\ell \geq 11$ on an elliptic curve $E/\mathbb{Q}$ over any number field of degree $d < 55$. If E has a rational ℓ-isogeny, then $[\mathbb{Q}(P_{\ell^2}) : \mathbb{Q}(\ell P_{\ell^2})]$ is divisible by ℓ^2.
- There are no points of order 49 on an elliptic curve $E/\mathbb{Q}$ over any number field of degree $d < 42$.
- There are no points of order 125 on an elliptic curve $E/\mathbb{Q}$ over any number field of degree $d < 50$.

Throughout this thesis, some elliptic curves will be denoted by their unique LMFDB [53] label. We note that LMFDB label of every elliptic curve is of the form a.bc, where a is the conductor of the elliptic curve, b is a string and c is an integer. More details can be found on LMFDB website lmfdb.org.

Lemma 4.1.4 ([11, Lemma 5]). Let $E/\mathbb{Q}$ be an elliptic curve without CM, $K/\mathbb{Q}$ a sextic field and $P_p \in E(K)_{tors}$ a point of odd prime order p. Then E has a rational p-isogeny, except if E has LMFDB label 2450.y1 or 2450.z1, and $p = 7$, where there are not rational 7-isogenies. Moreover, in those last cases, the unique sextic fields where the torsion grows are $K = \mathbb{Q}(E[2])$ and $K' = \mathbb{Q}(P_7)$ ($K'/\mathbb{Q}$ is non-Galois), where $E(K)_{tors} \cong C_2 \oplus C_2$ and $E(K)_{tors} \cong C_7$ respectively.

Lemma 4.1.5. Let K be a number field such that $[K:\mathbb{Q}] = 6$. If L and L' are cubic subextensions of K and if $L/\mathbb{Q}$ is Galois, then $L = L'$.

Proof. Assume that $L \neq L'$. Obviously $L \cap L' = \mathbb{Q}$ and $LL' = K$. By [10, Theorem 12.2.5] we have $\mathrm{Gal}(K/L') \cong \mathrm{Gal}(LL'/L') \cong \mathrm{Gal}(L/\mathbb{Q})$. Since $|\mathrm{Gal}(K/L')| = 2$ and $|\mathrm{Gal}(L/\mathbb{Q})| = 3$, we arrive at a contradiction. ■

Definition 4.1.6 ([12, Definition 3.1])**.** We say that a finite group G is of generalized S_3-type if it is isomorphic to a subgroup of the direct product $S_3 \times S_3 \times \ldots \times S_3$.

Theorem 4.1.7 ([12, Lemma 3.2, Corollary 3.4])**.** A finite group G is of generalized S_3-type if and only if

- G is supersolvable,
- Sylow subgroups of G are abelian, and
- Exponent of G divides 6.

Additionally, if G is of generalized S_3-type, then every subgroup and every quotient group of G is also of generalized S_3-type. If G_1 and G_2 are of generalized S_3-type, then so is $G_1 \times G_2$.

Theorem 4.1.8 ([12], Theorem 3.5, Theorem 3.6)**.** Let L be a number field such that $\mathrm{Gal}(\hat{L}/\mathbb{Q})$ is of generalized S_3-type, where $\hat{L}$ denotes the Galois closure of L over $\mathbb{Q}$. Then $L \subseteq \hat{L} \subseteq \mathbb{Q}(3^\infty)$. Let L be a number field in $\mathbb{Q}(3^\infty)$. Then $\hat{L} \subseteq \mathbb{Q}(3^\infty)$ and $\mathrm{Gal}(\hat{L}/\mathbb{Q})$ is of generalized S_3-type.

It is easy to see that the groups S_3, C_2 and C_3 are of generalized S_3-type and so are their direct products, $S_3 \times C_2$, $S_3 \times C_3$, $C_2 \times C_3 \cong C_6$.

4.2. CYCLIC CASES

Theorem 4.2.1. Let $E/\mathbb{Q}$ be an elliptic curve without CM. Then $E(K)_{tors}$ cannot contain $C_{20}, C_{24}, C_{25}, C_{26}, C_{27}, C_{28}, C_{32}, C_{35}, C_{36}, C_{39}, C_{42}, C_{45}, C_{49}, C_{63}, C_{65}, C_{91}, C_{169}$.

Proof. If E has LMFDB label 2450.y1 or 2450.z1, this holds by Lemma 4.1.4. Suppose this is not the case. By Lemma 4.1.3, $E(K)$ cannot contain C_{49} and C_{169}. By Lemma 4.1.4, if $E(K)$ contains points P_p, P_q of odd prime orders p and q, $p \neq q$, then $E(K)$ has rational p and q-isogenies, so it has a rational pq-isogeny. When $pq \in \{35, 39, 65, 91\}$, this cannot happen, because of Theorem 2.1.1 and so $E(K)$ cannot contain C_{35}, C_{39}, C_{65} or C_{91}. In [11, Proposition 6.], it has been proven that $E(K)$ cannot contain C_{20}, C_{26} or C_{28}.

$\boxed{C_{24}}$: By Lemma 4.1.4, $\rho_{E,3}$ is not surjective. Also $\rho_{E,8}$ cannot be surjective because a point P_8 of order 8 on $E(\overline{\mathbb{Q}})$ would satisfy $[\mathbb{Q}(P_8) : \mathbb{Q}] > 6$. By [39, Theorem A (3)], we have that $G_E(8) \subseteq H$, for $H \in \{H_{30}, H_{31}, H_{39}, H_{45}, H_{47}, H_{50}\}$. Each of these six groups has order equal to 128. This means that $[\mathbb{Q}(E[8]) : \mathbb{Q}]$ is a power of 2 that divides 128. Consequently, $[\mathbb{Q}(E[2]) : \mathbb{Q}]$ is a power of 2. Hence, each 2-torsion point on E is defined over an at most a quadratic extension of $\mathbb{Q}$. Since 2^k-torsion grows in extensions of degree $1, 2$ or 4 ([19, Proposition 4.8)]) and since $E(K) \supseteq C_8$, we need to have point of order 8 on E defined over at most a quadratic extension of $\mathbb{Q}$. Since E has a rational 3-isogeny, by Table 6.1 we see that E must have a point P_3 of order 3 such that $[\mathbb{Q}(P_3) : \mathbb{Q}] \in \{1, 2\}$. Therefore a point $P_8 + P_3$ of order 24 on E is defined over the field $F = \mathbb{Q}(P_3, P_8)$ for which $\mathrm{Gal}(F/\mathbb{Q}) \in \{C_1, C_2, C_2 \oplus C_2\}$. This is impossible because of Theorem 1.0.12, Theorem 2.1.3 and [7, Theorem 1.4.].

$\boxed{C_{25}}$: By Lemma 4.1.4, E has a rational 5-isogeny. By [19, Table 2], we see that $G_E(5) \in \{5\text{Cs}.1.1, 5\text{Cs}.1.3, 5\text{Cs}.4.1, 5\text{B}.1.1, 5\text{B}.1.4, 5\text{B}.4.1\}$. For each of these possibilities of $G_E(5)$, we find all subgroups G of $\mathrm{GL}_2(\mathbb{Z}/25\mathbb{Z})$ with surjective determinant that reduce to $G_E(5)$ modulo 5. Then for each vector $v \in (\mathbb{Z}/25\mathbb{Z})^2$ of order 25 we calculate the index of G_v in G, where G_v is stabiliser subgroup corresponding to vector v. By Theorem 1.0.12, Theorem 2.1.3 and Theorem 2.1.4 we have that $[\mathbb{Q}(P_{25}) : \mathbb{Q}] \notin \{1, 2, 3\}$, so we have $[\mathbb{Q}(P_{25}) : \mathbb{Q}] = 6$. This means that $[G : G_v] = 6$. Computation in Magma [3] (code 7.1) shows that this does not occur. Therefore, E cannot have a point P_{25} defined over K.

$\boxed{C_{27}}$: Let P_{27} be a point of order 27 in $E(K)$ and P_{81} be a point of order 81 in $E(\overline{\mathbb{Q}})$ such that $3P_{81} = P_{27}$. From [19, Proposition 4.6.], we have $[\mathbb{Q}(P_{81}) : \mathbb{Q}(P_{27})] \leq 9$. Since $[\mathbb{Q}(P_{27}) : \mathbb{Q}] \leq 6$, we have $[\mathbb{Q}(P_{81}) : \mathbb{Q}] = [\mathbb{Q}(P_{81}) : \mathbb{Q}(P_{27})] \cdot [\mathbb{Q}(P_{27}) : \mathbb{Q}] \leq 54$. From the results of [46] it follows that P_{81} is defined over a number field of degree at least 81, a contradiction.

$\boxed{C_{36}}$: Let P_9, P_4 be points of order 9 and 4, such that $[\mathbb{Q}(P_9 + P_4) : \mathbb{Q}] = 6$. If $[\mathbb{Q}(P_9) : \mathbb{Q}] \in \{1,2,3\}$, then we have $\mathbb{Q}(P_9) \subseteq \mathbb{Q}(3^\infty)$, since every quadratic and cubic extension is contained in $\mathbb{Q}(3^\infty)$. If $[\mathbb{Q}(P_9) : \mathbb{Q}] = 6$, we check using Magma [3] (code 7.2) that $\mathrm{Gal}(\widehat{\mathbb{Q}(P_9)}/\mathbb{Q})$ (where $\widehat{\mathbb{Q}(P_9)}$ denotes the Galois closure of $\mathbb{Q}(P_9)$ over $\mathbb{Q}$) is isomorphic to one of the following groups: $C_6, S_3, S_3 \times C_3, S_3 \times C_2$. All these groups are of generalized S_3-type, so it follows that $\mathbb{Q}(P_9) \subseteq \mathbb{Q}(3^\infty)$. Similarly, the point P_4 can be defined over extensions of degree $1,2,3$ or 6. If $[\mathbb{Q}(P_4) : \mathbb{Q}] \in \{1,2,3\}$, then we have $\mathbb{Q}(P_4) \subseteq \mathbb{Q}(3^\infty)$. If $[\mathbb{Q}(P_4) : \mathbb{Q}] = 6$, by a search through the data of [47] we see that we see that if $[\mathbb{Q}(P_4) : \mathbb{Q}] = 6$, then $\mathbb{Q}(P_4)$ is an S_3 extension of $\mathbb{Q}$, hence of generalized S_3-type. We conclude that in any case we have $\mathbb{Q}(P_4) \subseteq \mathbb{Q}(3^\infty)$. We can now conclude that $\mathbb{Q}(P_9 + P_4) = \mathbb{Q}(P_9, P_4) \subseteq \mathbb{Q}(3^\infty)$, which is impossible by [12, Theorem 1.8.].

$\boxed{C_{42},\ C_{63}}$: From Lemma 4.1.4 we conclude that E has rational 3 and 7-isogenies, so it has a rational 21-isogeny, so

$$j(E) \in \{-3^2 \cdot 5^6/2^3, 3^3 \cdot 5^3/2, 3^3 \cdot 5^3 \cdot 101^3/2^{21}, -3^3 \cdot 5^3 \cdot 383^3/2^7\}$$

by [34, Table 4]. For each of the possible j-invariants, using the division polynomial method in Magma [3] (code 7.3) we compute the primitive division polynomials $f_{E,63}$ and $f_{E,42}$. Neither of these polynomials has an irreducible factor of degree less then or equal to 6. Hence, a point P of order 63 (resp. 42) cannot be defined over K.

$\boxed{C_{45}}$: Since E has rational 3 and 5 isogenies by Lemma 4.1.4, E has a rational 15-isogeny, so $j(E) \in \{-5^2/2, -5^2 \cdot 241^3/2^3, -29^3 \cdot 5/2^5, 211^3 \cdot 5/2^{15}\}$ by [34, Table 4]. Using exactly the same method as in the C_{63} and C_{42} case (code 7.4), we find that a point of order 45 cannot be defined over K. ■

4.3. Groups of the form $C_2 \oplus C_{2n}$

Theorem 4.3.1. Let $E/\mathbb{Q}$ be an elliptic curve without CM. Then $E(K)_{tors}$ cannot contain $C_2 \oplus C_{16}$ or $C_2 \oplus C_{30}$.

Proof. $\boxed{C_2 \oplus C_{16}}$: By [17, Corollary 3.5], we get that if $T \cong C_2 \oplus C_{16}$, then $[\mathbb{Q}(T) : \mathbb{Q}]$ must be divisible by 4, which is impossible since $\mathbb{Q}(T) \subseteq K$.

$\boxed{C_2 \oplus C_{30}}$: By Lemma 4.1.4, E has rational 3 and 5-isogenies, so it has a rational 15-isogeny. If $E(\mathbb{Q})[2] \supseteq C_2$, then E has a rational 30-isogeny, which is impossible by Theorem 2.1.1. If $G_E(2) = 2\text{Cn}$, then $j(E) = y^2 + 1728$ for some $y \in \mathbb{Q}$ and since E has 15-isogeny, we have $j(E) \in \{-5^2/2, -5^2 \cdot 241^3/2^3, -29^3 \cdot 5/2^5, 211^3 \cdot 5/2^{15}\}$ by [34, Table 4]. Let a be one of those 4 values. We have that $a < 1728$, so $y^2 + 1728 = a$ does not have a solution in real numbers, so this case is impossible. Consider now the case when $G_E(2) = \text{GL}_2(\mathbb{F}_2)$. This means that E attains its full 2-torsion over a degree 6 extension of $\mathbb{Q}$. Since $E(K)[2] = C_2 \oplus C_2$, we have $K = \mathbb{Q}(E[2]) \subseteq \mathbb{Q}(3^\infty)$, because the Galois group of $\mathbb{Q}(E[2])$ is of generalized S_3-type. Therefore, $C_2 \oplus C_{30} \subseteq E(K) \subseteq E(3^\infty)$. By [12, Theorem 1.8., Table 1] we see that $j(E) \in \{-29^3 \cdot 5/2^5, 211^3 \cdot 5/2^{15}\}$. For each of these two possibilities, using the division polynomial method we calculate the primitive division polynomial $f_{E,30}$ whose roots are the x-coordinates of the points of order 30 on E. If $j(E) = -29^3 \cdot 5/2^5$, the smallest degree irreducible factors of f_{30} are polynomials f, g of degree 6. Since $C_{30} \subseteq E(K) = E(\mathbb{Q}(E[2]))$, one of those polynomials needs to have a root in K, but since K is Galois, it splits in K. But we check using Magma [3] (code 7.5) that the splitting fields of f and g are degree 12-extensions of $\mathbb{Q}$, which is a contradiction. If $j(E) = 211^3 \cdot 5/2^{15}$, we do the same as in the previous case. This time, the polynomial $f_{E,30}$ does not have irreducible factors of degree ≤ 6, so $C_{30} \not\subseteq E(K)$. ■

4.4. Groups of the form $C_3 \oplus C_{3n}$

Theorem 4.4.1. Let $E/\mathbb{Q}$ be an elliptic curve without CM. Then $E(K)_{tors}$ cannot contain $C_3 \oplus C_{15}$ or $C_3 \oplus C_{21}$.

Proof. $\boxed{C_3 \oplus C_{15}, C_3 \oplus C_{21}}$: Since $\mathbb{Q}(E[3]) \subseteq K$, we need to have $G_E(3) \in \{3\text{Cs}.1.1, 3\text{B}.1.1, 3\text{B}.1.2\}$. Assume that $G_E(3) = 3\text{Cs}.1.1$. From Lemma 4.1.4 it follows $p \in \{5,7\}$, then E has a rational p-isogeny. Let $P_p \in E(K)$ be a point of order p. Let $\{P_3, Q_3\}$ be a basis for $E[3]$ such that $G_E(3) = 3\text{Cs}.1.1$ with respect to this basis. This means that $\langle P_3 \rangle$ and $\langle Q_3 \rangle$ are kernels of two independent rational 3-isogenies. Now $\langle P_p + P_3 \rangle$ and $\langle Q_3 \rangle$ are kernels of independent rational $3p$ and 3 isogenies, respectively. We conclude that E is isogenous to $E'/\mathbb{Q}$ with a rational $9p$-isogeny, which is impossible by Theorem 2.1.1. Therefore it remains to consider the cases when $G_E(3) \in \{3\text{B}.1.1, 3\text{B}.1.2\}$.

Assume that $C_3 \oplus C_{15} \subseteq E(K)$. We have that $K = \mathbb{Q}(E[3])$ and $\text{Gal}(K/\mathbb{Q}) \cong S_3$. Let P_5 be a point of order 5 in $E(K)$. From Table 6.1 we see that $[\mathbb{Q}(P_5) : \mathbb{Q}] \in \{1,2\}$. Denote by F the unique quadratic subextension of K. By Table 6.1, we see that for both possibilities of $G_E(3)$ there exists a point P_3 of order 3 in $E(K)$ defined over F. Therefore we have $\mathbb{Q}(P_5), \mathbb{Q}(P_3) \subseteq F$. It follows that $C_{15} \subseteq E(F)$. By [42, Theorem 2.c)], the LMFDB label of E is 50.b3, 50.b4, 50.a2 or 450.g4. Using the algorithm from [18], we see that none of these four curves have $C_3 \oplus C_{15}$ torsion over sextic field.

Assume that $C_3 \oplus C_{21} \subseteq E(K)$. We have that $K = \mathbb{Q}(E[3])$ and $\text{Gal}(K/\mathbb{Q}) \cong S_3$. Let P_7 be a point of order 7 in $E(K)$. If $[\mathbb{Q}(P_7) : \mathbb{Q}] \in \{3,6\}$, then by Table 6.1 and [34, Theorem 9.3] it follows that $\mathbb{Q}(P_7)$ is cyclic over $\mathbb{Q}$. But K is not cyclic and it does not have any Galois cubic subextensions over $\mathbb{Q}$. We conclude that $[\mathbb{Q}(P_7) : \mathbb{Q}] \in \{1,2\}$. Let P_3 denote a point of order 3 in $E(K)$ defined over an at most a quadratic extension of $\mathbb{Q}$. Therefore, $\mathbb{Q}(P_7), \mathbb{Q}(P_3) \subseteq F$ so $E(F) \supseteq C_{21}$, but this is impossible, by Theorem 2.1.3. ∎

4.5. Groups of the form $C_m \oplus C_{mn}$, $m \geq 4$

Theorem 4.5.1. Let $E/\mathbb{Q}$ be an elliptic curve without CM. Then $E(K)_{tors}$ cannot contain $C_4 \oplus C_8$.

Proof. By [17, Corollary 3.5], we get that if T is one of these three groups, then $[\mathbb{Q}(T):\mathbb{Q}]$ must be divisible by 4, which is impossible since $\mathbb{Q}(T) \subseteq K$. ■

Theorem 4.5.2. Let $E/\mathbb{Q}$ be an elliptic curve without CM. Then $E(K)_{tors}$ cannot contain $C_6 \oplus C_{12}$.

Proof. If $G_E(3) \in \{3\text{B}.1.1, 3\text{B}.1.2\}$, we have $K = \mathbb{Q}(E[3])$, K is an S_3 extension of $\mathbb{Q}$ and $j(E) = \frac{27(y+1)(y+9)^3}{y^3}$, for some $y \in \mathbb{Q}^\times$.

If $G_E(2) = 2\text{Cn}$, then $\mathbb{Q}(E[2])$ is cubic Galois over $\mathbb{Q}$ contained in K, which is impossible since K is an S_3 extension of $\mathbb{Q}$ and hence cannot contain $\mathbb{Q}(E[2])$.

Assume that $G_E(2) = \mathrm{GL}_2(\mathbb{F}_2)$. By a search through the data of [47] we see that if E attains a point of order 4 over a sextic field and $G_E(2) = \mathrm{GL}_2(\mathbb{F}_2)$, then the image of 2-adic representation associated to E is contained in H_{20}, so $j(E) = \frac{(x^2-3)^3(-4x^2+32x+44)}{(x+1)^4}$. Taking the fiber product of $X_0(3)$ and X_{20} we get a singular genus 1 curve C whose normalization is the elliptic curve $E'/\mathbb{Q}$ with LMFDB label 48.a3 (code 7.6). Inspecting the rational points on C we get that there are 4 non-cuspidal points corresponding to the j-invariants $109503/64$ and $-35937/4$. Additionally, since $\mathbb{Q}(E[2]) \subseteq \mathbb{Q}(E[3])$, by [6, Remark 1.5], we have $j(E) = 2^{10}3^3y^3(1-4y^3)$. For $a \in \{109503/64, -35937/4\}$ we find that $2^{10}3^3y^3(1-4y^3) - a = 0$ has no rational solutions. Therefore, this case cannot occur.

Consider the case $G_E(2) \in \{2\text{B}, 2\text{Cs}\}$. There is a unique quadratic extension contained in $K = \mathbb{Q}(E[3])$, namely $\mathbb{Q}(\zeta_3)$ and we have $\mathbb{Q}(E[2]) \subseteq \mathbb{Q}(\zeta_3)$. Since every point P_2 of order 2 on E is defined over an at most a quadratic extension of $\mathbb{Q}$, by [19, Proposition 4.8] we have that a point P_4 of order 4 on $E(K)$ satisfies $[\mathbb{Q}(P_4):\mathbb{Q}] \in \{1,2\}$. It follows that $C_2 \oplus C_4 \subseteq E(\mathbb{Q}(E[2])) \subseteq E(\mathbb{Q}(\zeta_3))$. Since $G_E(3) \in \{3\text{B}.1.1, 3\text{B}.1.2\}$, by Table 6.1 we can see that there must exist a point P_3 of order 3 in $E(K)$ such that $[\mathbb{Q}(P_3):\mathbb{Q}] \in \{1,2\}$, so P_3 is defined over $\mathbb{Q}(E[2]) \subseteq \mathbb{Q}(\zeta_3)$. Finally, we have that $C_2 \oplus C_{12} \subseteq E(\mathbb{Q}(\zeta_3))$, but this is impossible by [41, Theorem 1, iii)].

Assume that $G_E(3) = 3\text{Cs}.1.1 \subseteq 3\text{Ns}$. It follows that $j(E) = y^3$ by [55, Theorem 1.1]. If $G_E(2) = \mathrm{GL}_2(\mathbb{F}_2)$, then again we get that the 2-adic representation associated to E is contained in H_{20}. We have that $y^3 = \frac{(x^2-3)^3(-4x^2+32x+44)}{(x+1)^4}$ induces a genus 2 hyperelliptic curve C. In Magma [3] (code 7.6), we compute its Jacobian $J(C)$ and see that it has rank 0 over $\mathbb{Q}$. Using the Chabauty method implemented in Magma [3] we conclude that it does not have an affine rational point. If $G_E(2) = 2\text{Cn}$ then $j(E) = x^2 + 1728$ and the corresponding fiber product $X_{2Cn} \times_{X_0(1)} X_{3Ns}$ is birational to $y^3 = x^2 + 1728$, which is an elliptic curve $E'/\mathbb{Q}$ with LMFDB label 36.a3. The rational point on E' corresponds to the j-invariant 1728, so E would have CM, which contradicts our assumption.

Consider the case $G_E(2) \in \{2\text{B}, 2\text{Cs}\}$. Using exactly the same reasoning as before, we conclude that $C_2 \oplus C_4 \subseteq E(\mathbb{Q}(E[2]))$ and $\mathbb{Q}(E[2])$ is an at most quadratic over $\mathbb{Q}$. On the other hand, since $G_E(3) = 3\text{Cs}.1.1$, $\mathbb{Q}(E[3])$ is quadratic over $\mathbb{Q}$. Therefore, the composite field $L := \mathbb{Q}(E[2])\mathbb{Q}(E[3])$ is either a $C_2 \oplus C_2$ or C_2 extension of $\mathbb{Q}$ and we have $C_6 \oplus C_{12} \subseteq E(L)$. But this is impossible by [7, Theorem 1.4.]. ■

Theorem 4.5.3. Let $E/\mathbb{Q}$ be an elliptic curve without CM. Then $E(K)_{tors}$ cannot contain $C_7 \oplus C_7$.

Proof. Since $\mathbb{Q}(E[7]) \subseteq K$ we have $|G_E(7)| \leq 6$, but looking at the possible mod 7 images in Table 6.1 we see that $|G_E(7)| \geq 18$, a contradiction. ■

Theorem 4.5.4. Let $E/\mathbb{Q}$ be an elliptic curve without CM. Then $E(K)_{tors}$ cannot contain $C_9 \oplus C_9$.

Proof. Since $\mathbb{Q}(E[9]) \subseteq K$ we have $|G_E(9)| = 6$, because otherwise we would have $C_9 \oplus C_9 \in \Phi_{\mathbb{Q}}(3)$ or $C_9 \oplus C_9 \in \Phi_{\mathbb{Q}}(2)$, which is not true by [42]. Using Magma [3] (code 7.2), we find all subgroups G of $\mathrm{GL}_2(\mathbb{Z}/9\mathbb{Z})$ of order 6 such that $\det(G) = (\mathbb{Z}/9\mathbb{Z})^\times$. All such groups G are (up to conjugacy) subgroups of the group of upper triangular matrices, so E has a rational 9-isogeny. Additionally, all such groups G reduce modulo 3 to 3Cs.1.1 (up to conjugacy), which implies that E has two independent rational 3-isogenies. Therefore E has independent rational 9 and 3-isogenies, so it is isogenous over $\mathbb{Q}$ to $E'/\mathbb{Q}$ with a rational 27-isogeny. It follows that E' has CM and so does E, which is a contradiction to our assumption. ■

4.6. GROUP $C_3 \oplus C_{18}$

Theorem 4.6.1. Let $E/\mathbb{Q}$ be an elliptic curve without CM. If E does not have a rational point of order 2, then $E(K)_{tors}$ cannot contain $C_3 \oplus C_{18}$.

Proof. We will split the proof into two main cases, depending on $G_E(3)$.

$\boxed{G_E(3) \in \{3\text{B}.1.1, 3\text{B}.1.2\}}$.

We have $K = \mathbb{Q}(E[3])$ and K is S_3 extension of $\mathbb{Q}$.

If $G_E(2) = 2\text{Cs}$, this is shown to be impossible by [11, Proposition 6.(m)].

If $G_E(2) = 2\text{Cn}$, then $\mathbb{Q}(E[2])$ is cubic Galois over $\mathbb{Q}$ contained in K, which is impossible since K is an S_3 extension of $\mathbb{Q}$.

Assume first that E has a rational 9-isogeny.

Assume that $G_E(2) = \mathrm{GL}_2(\mathbb{F}_2)$. Since K is Galois and E has a point of order 2 in K and the defining cubic polynomial $f(x)$ of E is irreducible and has a root in K, it splits in K. Therefore we have $K = \mathbb{Q}(E[2]) = \mathbb{Q}(E[3])$. Since E has a rational 9-isogeny, by [25, Appendix], we have that E is a twist of elliptic curve

$$E_t : y^2 = x^3 - 3t(t^3 - 24)x + 2(t^6 - 36t^3 + 216),$$

where $t \in \mathbb{Q} \setminus \{3\}$. We have $j(E_t) = \frac{t^3(t^3-24)^3}{t^3-27}$ and $\Delta(E_t) = 2^{12}3^6(t^3 - 27)$. Note that $j(E_0) = 0$ and $j(E_{-6}) = -2^{15} \cdot 3 \cdot 5^3$. It follows that for $t \in \{-6, 0\}$, E_t has CM by [49, Appendix 3]. Assume that $t \notin \{-6, 0, 3\}$. Since E is a twist of some E_t, we have $\Delta(E) = u^6\Delta(E_t)$, for some $u \in \mathbb{Q}$. The Corollary 3.1.3 implies that $\mathbb{Q}(\zeta_3) \subseteq K$ and since K is an S_3 extension of $\mathbb{Q}$, we conclude that $\mathrm{Gal}(K/\mathbb{Q}(\zeta_3)) \cong C_3$, which implies that the discriminant of E is a square in $\mathbb{Q}(\zeta_3)$, which is equivalent to

$$C : y^2 = t^3 - 27,\ t \in \mathbb{Q} \setminus \{-6, 0, 3\},\ y \in \mathbb{Q}(\zeta_3)$$

having a solution. Put $y := a + b\sqrt{-3}$, where $a, b \in \mathbb{Q}$. We get

$$a^2 + 2ab\sqrt{-3} - 3b^2 = t^3 - 27.$$

Since $a, b, t \in \mathbb{Q}$, we must have $2ab\sqrt{-3} \in \mathbb{Q}$. We conclude that $ab = 0$. If $b = 0$, then $y \in \mathbb{Q}$. The curve C has LMFDB label 36.a3 and it can be seen that $(0, 3)$ is the only

rational affine point on C, but this is impossible since $t \notin \{-6,0,3\}$. If $a = 0$, then we put $b := 3b_1$ and $t := -3t_1$. We get an elliptic curve

$$E' : \ b_1^2 = t_1^3 + 1.$$

The curve E' has LMFDB label 36.a4 and it can be seen that

$$E'(\mathbb{Q}) = \{O, (-1,0), (0,\pm 1), (2,\pm 3)\}.$$

It follows that $t_1 \in \{-1,0,2\}$, so $t \in \{3,0,-6\}$, but this contradicts our assumption. Therefore, in this case there does not exist an elliptic curve with $C_3 \oplus C_{18}$ torsion defined over $\mathbb{Q}$.

Assume now that E does not have a rational 9-isogeny.

Obviously, $E(\mathbb{Q}(3^\infty))$ contains a point of order 9, since $E(\mathbb{Q}(3^\infty)) \supseteq E(K)$. By [12, Lemma 6.13.], we get that $j(E) = \frac{(x+3)(x^2-3x+9)(x^3+3)^3}{x^3}$.

Assume that $G_E(2) = \mathrm{GL}_2(\mathbb{F}_2)$. Since $f(x)$ is irreducible and it has a root in K, it splits in K, since K is Galois. Therefore we have $\mathbb{Q}(E[2]) = \mathbb{Q}(E[3]) = K$. By [6, Remark 1.5], we have $j(E) = 2^{10}3^3y^3(1-4y^3)$, for some $y \in \mathbb{Q}$. As in the previous case, we must have

$$\frac{(x+3)(x^2-3x+9)(x^3+3)^3}{x^3} = 2^{10}3^3y^3(1-4y^3).$$

We obtain a curve C which is birational to the elliptic curve

$$E : \ y^2 + 52488y = x^3 - 918330048.$$

The elliptic curve E has C_3 torsion and rank 0 over $\mathbb{Q}$. None of the points on this curve correspond to elliptic curves with $C_3 \oplus C_{18}$ torsion over sextic field, which is checked using Magma [3] (code 7.8).

$\boxed{G_E(3) = \text{3Cs.1.1}}$ Since 3Cs.1.1 $\subseteq$ 3Ns, we have $j(E) = y^3$.

If $G_E(2) \in \{\text{2Cn}, \text{2Cs}\}$, this has already been shown to be impossible by Theorem 4.5.2, in $C_6 \oplus C_{12}$ case.

Assume that $G_E(2) = \mathrm{GL}_2(\mathbb{F}_2)$. We have $K = L\mathbb{Q}(\zeta_3)$, where L is degree 3 extension of $\mathbb{Q}$ contained in $\mathbb{Q}(E[2])$. Obviously, $E(L)[2] = C_2$.

Assume that $\mathbb{Q}(E[2])$ does not contain $\mathbb{Q}(\zeta_3)$. Then we have $\mathrm{Gal}(\hat{K}/\mathbb{Q}) \cong S_3 \times C_2$. In has been shown in the proof of [11, Proposition 8 (l)] that if P_9 is a point of order 9

defined over K and $G_E(3) = 3\text{Cs}.1.1$, then the Galois closure of $\mathbb{Q}(P_9)$ over $\mathbb{Q}$ is one of the following groups: C_6, S_3, $S_3 \times C_3$. It follows that we cannot have $[\mathbb{Q}(P_9) : \mathbb{Q}] = 6$ because $K = \mathbb{Q}(P_9)$ and $\text{Gal}(\hat{K}/\mathbb{Q}) \cong S_3 \times C_2$. Since K contains only two subfields, $\mathbb{Q}(\zeta_3)$ and L, we either have $\mathbb{Q}(P_9) \subseteq \mathbb{Q}(\zeta_3)$, in which case $E(\mathbb{Q}(\zeta_3)) \supseteq C_3 \times C_9$ (which is impossible by Theorem 2.1.3) or $\mathbb{Q}(P_9) = L$. Therefore we have $\mathbb{Q}(P_9) = L$. This means that $E(\mathbb{Q}) = C_3$ and $E(L) = C_{18}$, but this is impossible by [20, Theorem 2]. Therefore, we need to have $\mathbb{Q}(\zeta_3) \subseteq \mathbb{Q}(E[2])$. Since $\mathbb{Q}(\zeta_3) \subseteq \mathbb{Q}(E[2]) = K$, we need to have $\mathbb{Q}(\sqrt{\Delta}) = \mathbb{Q}(\zeta_3) = \mathbb{Q}(\sqrt{-3})$. From this equality it follows that $\sqrt{\Delta} = \alpha + \beta\sqrt{-3}$, for some rational α, β. It follows that $\Delta = \alpha^2 - 3\beta^2 + 2\alpha\beta\sqrt{-3}$. Since $\Delta - \alpha^2 - 3\beta^2 = 2\alpha\beta\sqrt{-3} \in \mathbb{Q}$, we must have $\alpha\beta = 0$. If $\beta = 0$, then Δ would be a square, a contradiction with the assumption that $G_E(2) = \text{GL}_2(\mathbb{F}_2)$. Therefore we have $\alpha = 0$ and $\Delta = -3\beta^2$. Since $G_E(3) = 3\text{Cs}.1.1$, by [55, Theorem 1.2.] we have that E is isomorphic to $y^2 = x^3 - 3(t+1)(t+3)(t^2+3)x - 2(t^2-3)(t^4+6t^3+18t^2+18t+9) = x^3 + ax + b$, for some $t \in \mathbb{Q}$ or a quadratic twist by -3 of such curve. Since twisting does not change 2-division field, we have that $\Delta = 4a^3 + 27b^2 = 4(-3(t+1)(t+3)(t^2+3))^3 + 27(2(t^2-3)(t^4+6t^3+18t^2+18t+9))^2 = (t(t^2+3t+3))^3 = -3\beta^2$. Plugging in $t = -3t_1$ and $\beta = \frac{\beta_1}{3^5}$ in $(t(t^2+3t+3))^3 = -3\beta^2$ we obtain $(t_1(t_1^2 - 9t_1 + 27))^3 = \beta_1^2$. Therefore, $t_1(t_1^2 - 9t_1 + 27)$ must be a square, so $t_1(t_1^2 - 9t_1 + 27) = \beta_2^2$, where $\beta_2^6 = \beta_1^2$. Finally, put $t_2 = t_1 - 3$ to obtain $t_2^3 + 27 = \beta_2^2$, which is an elliptic curve E' with LMFDB label 144.a4 and the only non trivial rational point on E' is $(-3, 0)$. We have that $\beta_2 = 0$ and so $\beta = 0$, but this is impossible, because $0 \neq \Delta = -3\beta^2$. ■

Remark 4.6.2. Let us address the issue that occurs in the case $G_E(2) = 2\text{B}$. Assume for example that $G_E(2) = 3\text{Cs}.1.1$. Using Magma [3], we search for possible mod 9 images of E such that E has a point of order 9 defined over a sextic number field. For each possibility for $G_E(9)$, we find that it is contained in one of the groups from [52, Table 1]. The modular curve induced by combining j-maps of one of these groups (also available in [52, Table 1]), along with j-map of elliptic curve E with $G_E(2) = 2\text{B}$, we get a few genus 3 and 4 curves that are not hyperelliptic and which do not have a nice quotient curve (code 7.9). At this time, we are unable to find all the rational points on such curves.

Proposition 4.6.3. Let $E/\mathbb{Q}$ be an elliptic curve without CM. If $G_E(2) = 2B$, $G_E(3) \in \{3\text{B}.1.1, 3\text{B}.1.2\}$ and E does not have a rational 9-isogeny, then $E(K)_{tors}$ cannot contain

$C_3 \oplus C_{18}$.

Proof. If $G_E(2) = 2\text{B}$, we have $j(E) = \frac{256(y+1)^3}{y}$. As in the previous theorem we see that $j(E) = \frac{(x+3)(x^2-3x+9)(x^3+3)^3}{x^3}$ because E does not have a rational 9-isogeny and $K \subset \mathbb{Q}(3^\infty)$. Therefore we must have

$$\frac{(x+3)(x^2-3x+9)(x^3+3)^3}{x^3} = \frac{256(y+1)^3}{y},$$

for some $x, y \in \mathbb{Q}^\times$. After clearing the denominators we obtain the curve C, which is birational to the curve $C_1 : \ y^2 + (x^3+1)y = -9x^3$. This a genus 2 hyperelliptic curve and its Jacobian has rank 0 over $\mathbb{Q}$. A computation in Magma [3] (code 7.8) shows that rational points on C do not correspond to elliptic curves with $C_3 \oplus C_{18}$ torsion over sextic fields. ■

5. TORSION OF ELLIPTIC CURVES WITH RATIONAL j-INVARIANT

This chapter is based on the paper [23].

5.1. RESULTS

Definition 5.1.1. For a positive integer d, let $\Phi_{j\in\mathbb{Q}}(d)$ be the set of possible isomorphism classes of groups $E(K)_{tors}$, where K runs through all number fields K of degree d and E runs through all elliptic curves over K with $j(E) \in \mathbb{Q}$.

We now state the main result of this chapter in which we classify the sets $\Phi_{j\in\mathbb{Q}}(p)$, where p is a prime number.

Theorem 5.1.2. Let K be a number field of prime degree p, and let E/K be an elliptic curve with $j(E) \in \mathbb{Q}$. Then:

1. If $p \geq 7$, then $E(K)_{tors} \in \Phi_{\mathbb{Q}}(p) = \Phi(1)$.

2. If $p = 3$ or $p = 5$, then $E(K)_{tors} \in \Phi_{\mathbb{Q}}(p)$.

3. If $p = 2$, then $E(K)_{tors} \in \Phi_{\mathbb{Q}}(2)$ or $E(K)_{tors} \cong \mathbb{Z}/13\mathbb{Z}$.

Obviously we have $\Phi_{\mathbb{Q}}(d) \subseteq \Phi_{j\in\mathbb{Q}}(d)$. If E/K is an elliptic curve such that $j(E) \in \mathbb{Q} \setminus \{0, 1728\}$, take $E'/\mathbb{Q}$ to be any elliptic curve such that $j(E') = j(E)$. Then E and E' are either isomorphic over K or over some quadratic extension L of K. Assume that $C_m \oplus C_n \subseteq E(K)$. This implies that $C_m \oplus C_n \subseteq E'(L)$, so $C_m \oplus C_n$ is a subgroup of one of the groups appearing in $\Phi_{\mathbb{Q}}(2d)$.

Let us consider the case when d is odd. Assume that $C_m \oplus C_n$, where m divides n is contained in $E(K)$. By Corollary 3.1.3 we have $\mathbb{Q}(\zeta_m) \subseteq K$. If $m \geq 3$, $[\mathbb{Q}(\zeta_m) : \mathbb{Q}]$ is even so $\mathbb{Q}(\zeta_m)$ cannot be a subfield of K. Therefore, when trying to classify $\Phi_{j\in\mathbb{Q}}(p)$ we shall consider only groups of the form C_n and $C_2 \oplus C_{2n}$.

We now describe the general strategy used to solve this problem. Let K be a number field of degree p and E/K be an elliptic curve with $j(E) \in \mathbb{Q} \setminus \{0, 1728\}$ and let $P_n \in E(K)$ be a point of order n. If E is a base change of an elliptic curve defined over $\mathbb{Q}$, we are done, because $E(K)_{tors} \in \Phi_{\mathbb{Q}}(p)$. Otherwise, we take any elliptic curve E' defined over $\mathbb{Q}$ such that $j(E') = j(E)$. With L we shall denote (unless otherwise stated) a quadratic extension of K such that E and E' are isomorphic over L, so they are quadratic twists of each other. We will often make use of Corollary 1.0.11 which says that if $n > 1$ is odd, then

$$E'(L)[n] \cong E'(K)[n] \oplus E(K)[n].$$

On the one hand, if $\{P_n, Q_n\}$ is a basis for $E[n]$, the image of $\rho_{E,n}$ is conjugate to a subgroup of B_0, where

$$B_0 := \left\{ \begin{bmatrix} 1 & * \\ 0 & * \end{bmatrix} \right\} \leq \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z}).$$

Since $\rho_{E,n} \sim \chi \cdot \rho_{E',n}$, where χ is a quadratic character, we can obtain some information about the mod n Galois representation of E'. On the other hand, since E and E' are isomorphic over L, there exists a point $P'_n \in E'(L)$ of order n. For each prime divisor q of n, let $P'_q \in E'(L)$ be a point of order q. Obviously $[\mathbb{Q}(P'_q) : \mathbb{Q}]$ is a divisor of $[L : \mathbb{Q}]$. Using the results of [19], we can check the possible values of $[\mathbb{Q}(P'_q) : \mathbb{Q}]$. Often it turns out that E' has a rational q-isogeny.

Note that Theorem 5.1.2 shows that if $p \geq 7$ is prime, then $\Phi_{j\in\mathbb{Q}}(p) \subseteq \Phi(1)$. The following result shows that we have an equality.

Proposition 5.1.3. Let p be a prime. We have $\Phi(1) \subseteq \Phi_{j\in\mathbb{Q}}(p)$.

Proof. For each group $G \in \Phi(1)$, we will show that there exists an elliptic curve $E/\mathbb{Q}$ and a number field K of degree p such that $E(K)_{tors} \cong G$.

Assume that $p \geq 11$ is prime. Let $G \in \Phi(1)$, $E/\mathbb{Q}$ be an elliptic curve with $E(\mathbb{Q})_{tors} \cong G$ and K a number field such that $[K : \mathbb{Q}] = p$. Then by [19, Theorem 7.2 (i)] we have

$E(K)_{tors} = E(\mathbb{Q})_{tors}$. Therefore we conclude that $G \in \Phi_{j\in\mathbb{Q}}(p)$.

Consider the case when $p = 7$. By [19, Proposition 7.1] we have $\Phi(1) = \Phi_{\mathbb{Q}}(p)$. Since $\Phi_{\mathbb{Q}}(p) \subseteq \Phi_{j\in\mathbb{Q}}(p)$, our claim follows. ■

5.2. Classification of $\Phi_{j\in\mathbb{Q}}(p)$

Let $R_{\mathbb{Q}}(d)$ be the set of all primes p such that there exists a number field K of degree d, an elliptic curve $E/\mathbb{Q}$ such that there exists a point of order p on $E(K)$. The set $R_{\mathbb{Q}}(d)$ has been partially determined by González-Jiménez and Najman in [19].

Throughout this chapter K will denote a number field of degree p and E/K an elliptic curve with $j(E) \in \mathbb{Q}$. With E' and L we will denote an elliptic curve defined over $\mathbb{Q}$ such that $j(E) = j(E')$ and quadratic extension of K over which E and E' are isomorphic, respectively.

Lemma 5.2.1. Let $p \geq 7$ be a prime number. Then $R_{\mathbb{Q}}(2p) = \{2,3,5,7\}$. Furthermore, we have $R_{\mathbb{Q}}(10) = \{2,3,5,7,11\}$ and $R_{\mathbb{Q}}(6) = \{2,3,5,7,13\}$.

Proof. The claim will follow easily by [19, Corollary 6.1.]. We briefly sketch the proof. Let $p \geq 7$ and $q \geq 23$, $q \neq 37,43,67,163$ be a prime numbers and assume that $q \in R_{\mathbb{Q}}(2p)$. We have that $2(q-1)|2p$ or $\frac{q^2-1}{3}|2p$. If $2(q-1)|2p$, we have $q \in \{2, p+1\}$, which is impossible. If $\frac{q^2-1}{3}|2p$, it follows that $(q-1)(q+1)|6p$. Since $q-1$ and $q+1$ are even, it follows that $4|6p$ so we must have $p = 2$, a contradiction. It remains to check that the claim holds for $q \in \{11,13,17,19,37,43,67,163\}$ which is easy to do. For $q \in \{19,43,67,163\}$ we have that $q \in R_{\mathbb{Q}}(2p)$ if and only if $\frac{q-1}{2} \mid 2p$. But for $q \in \{19,43,67,163\}$ we have $\frac{q-1}{2} \in \{9,21,33,81\}$ and none of these values can divide $2p$, because p is a prime number. If $q \in \{17,37\}$ we see that 4 must divide $2p$, a contradiction with out assumption that $p \geq 7$ is a prime number. Assume that $q = 11$ (resp. $q = 13$). By the same Corollary we have that $2p = 10$ (resp. $2p = 6$). The claims $R_{\mathbb{Q}}(10) = \{2,3,5,7,11\}$ and $R_{\mathbb{Q}}(6) = \{2,3,5,7,13\}$ follow from the previous discussion. ■

Theorem 5.2.2. Let K be a number field of prime degree p and let E/K be a CM elliptic curve. Then we have $E(K)_{tors} \in \Phi_{\mathbb{Q}}(p)$.

Proof. The claim follows easily by [4, Theorem 1.4]. ■

Therefore, from now on we shall assume that elliptic curves we are dealing with do not have CM.

Assume that $C_p \subseteq E(K)$. Since E and E' are isomorphic over L, it follows that $C_p \subseteq E'(L)$. Sometimes we will be able to conclude that the point P of order p on $E'(L)$ is defined over a proper subfield F of L. If $[F:\mathbb{Q}] = 2$, we can find $E''/\mathbb{Q}$ with $j(E) = j(E'')$ such that $C_p \subseteq E''(\mathbb{Q})$. Therefore we also have $C_p \subseteq E''(K)$ and we conclude that

$$C_p \oplus C_p \subseteq E(K)[p] \oplus E''(K)[p] \cong E''(L')[p], \tag{5.1}$$

where L' denotes the quadratic extension of K such that E'' and E are isomorphic over L'. By Corollary 3.1.3, we have $\mathbb{Q}(\zeta_p) \subseteq L'$. The field satisfying (5.1) will be denoted by L' throughout this chapter. We now formally state and prove the result mentioned in the previous discussion.

Lemma 5.2.3. Let $E/\mathbb{Q}$ be a non-CM elliptic curve and $p \geq 3$ a prime and $[F:\mathbb{Q}] = 2$. Assume that $E(F)[p] \supseteq C_p$, but $E(\mathbb{Q})[p] = O$. Then there there exists quadratic twist $E'/\mathbb{Q}$ of $E/\mathbb{Q}$ such that $E'(\mathbb{Q})[p] = C_p$.

Proof. Since $F = \mathbb{Q}(\sqrt{d})$, put $E' := E^d$, where E^d is the quadratic twist of E by d. The curves E' and E are isomorphic over F but not over $\mathbb{Q}$. Since $C_p \subseteq E(F)[p] \cong E(\mathbb{Q})[p] \oplus E'(\mathbb{Q})[p]$ and $E(\mathbb{Q})[p] = O$ it follows that $C_p \subseteq E'(\mathbb{Q})[p]$. Theorem 1.0.12 implies that we have an equality. ∎

Lemma 5.2.4. Let K be a number field, $m \geq 2$ an integer and E/K a non-CM elliptic curve with $j(E) \in \mathbb{Q}$ such that $C_m \subseteq E(K)$. If $E'/\mathbb{Q}$ is an elliptic such that $j(E) = j(E')$ and $\mathbb{Q}(E'[m]) \cap K = \mathbb{Q}$, then $G_{E'}(m)$ is conjugate to a subgroup of $B(m)$, where

$$B(m) := \left\{ \begin{bmatrix} \pm 1 & * \\ 0 & * \end{bmatrix} \right\} \subseteq \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z}).$$

Proof. By [51, Corollary 5.25.] we see that $\mathrm{Gal}(K\mathbb{Q}(E'[m])/K) \leq B(m)$ (up to conjugacy). Since $\mathbb{Q}(E'[m]) \cap K = \mathbb{Q}$ we have $\mathrm{Gal}(K\mathbb{Q}(E'[m])/K) \cong \mathrm{Gal}(\mathbb{Q}(E[m])/\mathbb{Q})$ by a basic Galois theory argument. Therefore, $G_{E'}(m)$ is conjugate to a subgroup of $B(m)$. ∎

Lemma 5.2.5. Let K be a number field such that $[K:\mathbb{Q}] \geq 5$ is prime and E/K be a non-CM elliptic curve with rational j-invariant and assume that $C_{2^k \cdot 3^l} \subseteq E(K)$. Then E' has a rational $2^k \cdot 3^l$-isogeny.

Proof. Assume that $(k,l) \neq (1,0)$. By [24, Corollary 2.8.] we have $|\mathrm{GL}_2(\mathbb{Z}/2^k\mathbb{Z})| = 2^{4k-3}\cdot 3$ and $|\mathrm{GL}_2(\mathbb{Z}/3^k\mathbb{Z})| = 3^{4k-3}\cdot 2^4$. Let $p \in \{2,3\}$ be a prime number. Since $G_{E'}(p^k) \leq \mathrm{GL}_2(\mathbb{Z}/p^k\mathbb{Z})$, we have that $[\mathbb{Q}(E'[p^k]):\mathbb{Q}] = |G_{E'}(p^k)|$ divides $|\mathrm{GL}_2(\mathbb{Z}/p^k\mathbb{Z})|$. But $|\mathrm{GL}_2(\mathbb{Z}/p^k\mathbb{Z})| \in \{2^{4k-3}\cdot 3, 3^{4k-3}\cdot 2^4\}$ so $\mathbb{Q}(E'[p^k])$ has a trivial intersection with K, i.e. $\mathbb{Q}(E'[p^k]) \cap K = \mathbb{Q}$. The claim now follows from Lemma 5.2.4.

Let us consider the case when $(k,l) = (1,0)$. Since having 2-torsion is twist invariant property, we have $C_2 \subseteq E'(K)[2] = E(K)[2]$. Since a point P_2 of order 2 on $E'(K)$ satisfies $[\mathbb{Q}(P_2):\mathbb{Q}] \leq 3$ and it is defined over K, we have $[\mathbb{Q}(P_2):\mathbb{Q}] = 1$. Therefore, E' has a rational point of order 2 and so it has a rational 2-isogeny. ■

Lemma 5.2.6. Let K be a number field such that $[K:\mathbb{Q}] \neq 5$ is an odd prime and let E/K be a non-CM elliptic curve with rational j-invariant such that $C_5 \subseteq E(K)_{tors}$. Then E is a base change of an elliptic curve defined over $\mathbb{Q}$. If $[K:\mathbb{Q}] = 5$ and $C_5 \subseteq E(K)_{tors}$, then E' has a rational 5-isogeny.

Proof. Assume that $[K:\mathbb{Q}] \neq 5$ is an odd prime and that E is not a base change of an elliptic curve defined over $\mathbb{Q}$. Since $C_5 \subseteq E(K)$, it follows that $C_5 \subseteq E'(L)$. Let P_5 be a point of order 5 on $E'(L)$. We have that $\mathbb{Q}(P_5) \subseteq L$ and so $[\mathbb{Q}(P_5):\mathbb{Q}]$ divides $[L:\mathbb{Q}] = 2p$, where $p = [K:\mathbb{Q}]$. By Table 6.1, we see that the only possibilities for $[\mathbb{Q}(P_5):\mathbb{Q}]$ are 1 and 2. Now we apply Lemma 5.2.3 to E' to obtain a quadratic twist $E''/\mathbb{Q}$ such that $C_5 \subseteq E''(\mathbb{Q})$. Since E and E'' are quadratic twists, they are isomorphic over some quadratic extension L' of K and we have $C_5 \oplus C_5 \subseteq E(K)[5] \oplus E''(K)[5] \cong E''(L')[5]$. Corollary 3.1.3 implies that $\mathbb{Q}(\zeta_5) \subseteq L'$ and so $[\mathbb{Q}(\zeta_5):\mathbb{Q}] = 4$ divides $[L':\mathbb{Q}] = 2p$, which is impossible.

If $[K:\mathbb{Q}] = 5$, by applying the same reasoning as in the previous paragraph it can be easily seen that E' must have a rational 5-isogeny. ■

Lemma 5.2.7. Let K be a number field such that $[K:\mathbb{Q}] \neq 3,7$ is prime and E/K be a non-CM elliptic curve with rational j-invariant such that $C_7 \subseteq E(K)_{tors}$. Then E is a base change of elliptic curve defined over $\mathbb{Q}$. If $[K:\mathbb{Q}] = 7$ and $C_7 \subseteq E(K)_{tors}$, then E' has a rational 7-isogeny. If $[K:\mathbb{Q}] = 3$ and $C_7 \subseteq E(K)_{tors}$, then E' has a rational 7-isogeny unless E' has LMFDB label 2450.y1 or 2450.z1 (or equivalently, if $G_{E'}(7)$ is conjugate to a group with label 7Ns.2.1.).

Proof. The proof is the same as the proof of Lemma 5.2.6. The last claim follows from [11, Lemma 5.]. ■

We will classify torsion growth of elliptic curves with LMFDB label 2450.y1 or 2450.z1 separately.

Lemma 5.2.8. Let $E'/\mathbb{Q}$ be a curve with LMFDB label 2450.y1 or 2450.z1 and let L be a number field such that $[L:\mathbb{Q}] = 2p$, where p is prime. Then

$$E'(L)_{tors} \in \{C_1, C_2, C_2 \oplus C_2, C_7\}.$$

Proof. Let $q \neq 7$ be a prime and let E' be either of these two curves. Then $G_{E'}(q) = \mathrm{GL}_2(\mathbb{Z}/q\mathbb{Z})$. By [34, Theorem 5.1.], a point P_q of order q on E' satisfies$[\mathbb{Q}(P_q):\mathbb{Q}] = q^2-1$. If $P_q \in E'(L)$, then $[\mathbb{Q}(P_q):\mathbb{Q}] = q^2-1$ would divide $[L:\mathbb{Q}] = 2p$. This implies that $q = 2$ and $p = 3$.

Consider the case $q = 7$. If $P_7 \in E'(L)$ is a point of order 7, by Table 6.1 we have $[\mathbb{Q}(P_7):\mathbb{Q}] \in \{6, 9, 18\}$. Since $[\mathbb{Q}(P_7):\mathbb{Q}]$ must also divide $[L:\mathbb{Q}] = 2p$, we conclude that $[\mathbb{Q}(P_7):\mathbb{Q}] = 6$. Using the algorithm from [18] we see that if $C_7 \subseteq E'(L)$, where $[L:\mathbb{Q}] = 6$, then $C_7 \cong E'(L)_{tors}$. ■

From now on, assume that E' is not one of these two curves. So if $C_7 \subseteq E(K)$, then E' will have a rational 7-isogeny by Lemma 5.2.7.

Lemma 5.2.9. Let K be a number field such that $[K:\mathbb{Q}] = p$ is an odd prime. Then there does not exist a non-CM elliptic curve E/K with rational j-invariant such that C_{16} or C_{27} is contained in $E(K)$. Additionally, if $[K:\mathbb{Q}] = p \geq 5$, then there does not exist a non-CM elliptic curve E/K with rational j-invariant such that C_{18} is contained in $E(K)$.

Proof. $\boxed{C_{16}}$: Assume the contrary, that $C_{16} \subseteq E(K)$. It follows that $C_{16} \subseteq E'(L)$ and let P_{16} be a point of order 16 in $E'(L)$. Since $[\mathbb{Q}(P_{16}):\mathbb{Q}]$ divides $[L:\mathbb{Q}]$ and 4 does not divide $[L:\mathbb{Q}]$, we have that $[\mathbb{Q}(P_{16}):\mathbb{Q}]$ is not divisible by 4. By the results of [39], we see that $G_{E'}(16) \in \{\mathrm{H}_{235\mathrm{l}}, \mathrm{H}_{235\mathrm{m}}\}$ and $[\mathbb{Q}(P_{16}):\mathbb{Q}] = 2$. In both cases we have $|G_{E'}(16)| = 256$. By Lemma 5.2.4, up to conjugacy we have $G_{E'}(16) \leq B(m)$, where $B(m)$ denotes the group in the same Lemma. Since $|B(m)| = 256$, the equality holds. But $-I \notin G_{E'}(16)$ and $-I \in B(m)$, a contradiction.

$\boxed{C_{18}}$: Assume that $C_{18} \subseteq E(K)$. Since having a 2-torsion is a twist invariant property, we have $C_2 \subseteq E'(K)$. Let P_2 be a point of order 2 in $E'(K)$. Since $[\mathbb{Q}(P_2):\mathbb{Q}] \in \{1,2,3\}$ and $[\mathbb{Q}(P_2):\mathbb{Q}]$ divides $[K:\mathbb{Q}] = p$, we have $[\mathbb{Q}(P_2):\mathbb{Q}] = 1$. Let $P_9 \in E'(L)$ be a point of order 9. We have that $[\mathbb{Q}(P_9):\mathbb{Q}]$ divides $[L:\mathbb{Q}] = 2p$. On the other hand, by Proposition 2.1.8 we have that $[\mathbb{Q}(P_9):\mathbb{Q}(3P_9)]$ divides 18. The point $3P_9 \in E'(L)$ is of order 3 and $[\mathbb{Q}(3P_9):\mathbb{Q}]$ divides $[L:\mathbb{Q}] = 2p$. By Table 6.1 we see that $[\mathbb{Q}(3P_9):\mathbb{Q}] \in \{1,2,3,6\}$. We conclude that $[\mathbb{Q}(P_9):\mathbb{Q}(3P_9)][\mathbb{Q}(3P_9):\mathbb{Q}]$ divides $18\cdot 6$, and since $\gcd(18\cdot 6, 2p) = 2$, we have $[\mathbb{Q}(P_9):\mathbb{Q}] \in \{1,2\}$. We conclude that P_9 is defined over an at most quadratic extension of $\mathbb{Q}$ and since $P_2 \in E'(\mathbb{Q})$, the point $P_2 + P_9$ of order 18 on E' is defined over a quadratic number field, which is impossible since $C_{18} \notin \Phi_{\mathbb{Q}}(2)$, by Theorem 2.1.3.

$\boxed{C_{27}}$: If $p \geq 5$, by Lemma 5.2.5, E' has a rational 27-isogeny, so it has CM by Theorem 2.1.1 and so E has CM as well, which contradicts our assumption that we are working with non-CM curves. On the other hand, if $p = 3$ then $E'(L)$ would contain C_{27}, so $C_{27} \in \Phi_{\mathbb{Q}}(6)$, which is not true by Theorem 4.0.1. ■

Lemma 5.2.10. Let K be a number field such that $[K:\mathbb{Q}]$ is an odd prime and let E/K be a non-CM elliptic curve with rational j-invariant. Then $E(K)$ cannot contain $C_2 \oplus C_{12}$ or $C_2 \oplus C_{10}$.

Proof. $\boxed{C_2 \oplus C_{12}}$: Assume that $C_2 \oplus C_{12} \subseteq E(K)$. This implies $C_2 \oplus C_{12} \subseteq E'(L)$. Since $[K:\mathbb{Q}]$ is odd we have that $[L:\mathbb{Q}]$ is not divisible by 4. By Table 6.1 we see that E' has a rational 3-isogeny and denote by $\langle P_3 \rangle$ the kernel of that isogeny. Obviously $G_{E'}(4)$ is not surjective, because otherwise a point P_4 of order 4 on E' would be defined over degree 12 extension of $\mathbb{Q}$, so 12 would divide $[L:\mathbb{Q}]$. By [39, Theorem A], we have that $G_{E'}(4) \subseteq H_i$, where $i \in \{9,10,11,12,13\}$. Since $|H_i| = 16$ for $i \in \{9,10,11,12,13\}$ it follows that $[\mathbb{Q}(E'[4]):\mathbb{Q}] = |G_{E'}(4)|$ is a power of 2. This implies that $\mathbb{Q}(E'[4]) \cap K = \mathbb{Q}$. Since having a 2-torsion is twist invariant property and $E(K)[2] = C_2 \oplus C_2$, we have $E'(K)[2] = C_2 \oplus C_2$. We now see that $\mathbb{Q}(E'[2]) \subseteq \mathbb{Q}(E'[4]) \cap K = \mathbb{Q}$, so $\mathbb{Q}(E[2]) = \mathbb{Q}$. Since $C_4 \subseteq E(K)$, by Lemma 5.2.4, E' has a rational 4-isogeny. Let $\langle P_4 \rangle$ be the kernel of that isogeny and Q_2 be such that $\{2P_4, Q_2\}$ is a basis for $E[2]$. The subgroups $\langle P_3 + P_4 \rangle$ and $\langle Q_2 \rangle$ are kernels of independent 12 and 2-isogenies, so E' is isogenous over $\mathbb{Q}$ to a curve $E''/\mathbb{Q}$ with a rational 24-isogeny by Lemma 2.1.2, which is impossible by Theorem 2.1.1.

$\boxed{C_2 \oplus C_{10}}$: Assume that $[K:\mathbb{Q}] = p \neq 5$ and that $C_2 \oplus C_{10} \subseteq E(K)$. By Lemma 5.2.6 we have that E is a base change of an elliptic curve defined over $\mathbb{Q}$. Therefore, $C_2 \oplus C_{10} = E(K)_{tors} \in \Phi_{\mathbb{Q}}(p)$. When $p \geq 7$, this is impossible by [19, Proposition 7.1, Corollary 7.3] and if $p = 3$ this is impossible by Theorem 2.1.4.

If $[K:\mathbb{Q}] = 5$, then Lemma 5.2.6 implies that E' has a rational 5-isogeny. Let $\langle P_5 \rangle$ be the kernel of that isogeny. Since having 2-torsion is twist invariant property, we have $E'(K)[2] = C_2 \oplus C_2$. Since $[K:\mathbb{Q}] = 5$ we conclude that $G_{E'}(2) = 2\text{Cs}$. Let $\{P_2, Q_2\}$ be a basis for $E'[2]$. The groups $\langle P_2 + P_5 \rangle$ and $\langle Q_2 \rangle$ are the kernels of rational 10 and 2-isogenies. Obviously those isogenies are independent. By Lemma 2.1.2, E' is isogenous to $E''/\mathbb{Q}$ with a rational 20-isogeny, which is impossible by Theorem 2.1.1. ■

5.3. Proof of Theorem 5.1.2 (1)

If $P_n \in E(K)$ is a point of order n, then $C_n \subseteq E'(L)$ (where E' denotes an elliptic curve defined over $\mathbb{Q}$ such that $j(E) = j(E')$ and L is the quadratic extension of K such that E and E' are isomorphic over L). By Lemma 5.2.1 we only need to consider those integers n whose prime factors are contained in $R_{\mathbb{Q}}(2p) = \{2,3,5,7\}$.

Theorem 5.3.1. Let K be a number field such that $[K:\mathbb{Q}] = p \geq 11$ is prime and let E/K be a non-CM elliptic curve with rational j-invariant. If $E(K)$ contains a point of order $n > 1$, then $C_n \in \Phi(1)$.

Proof. Assume that $E(K)$ contains a point P_n of order $n = 2^a 3^b 5^c 7^d$, where $a,b,c,d \geq 0$. If $(c,d) \neq (0,0)$, then by Lemma 5.2.6 and Lemma 5.2.7 we have that E is a base change of an elliptic curve defined over $\mathbb{Q}$, so the claim holds by [19, Corollary 7.3.]. Consider now the case when $c = d = 0$. By Lemma 5.2.5, E' has a rational $2^a 3^b$-isogeny. By Theorem 2.1.1 we have

$$n = 2^a 3^b \in \{1,2,3,4,6,8,9,12,16,18,27\}.$$

Among these values of n, we have $C_n \notin \Phi(1)$ only for $n \in \{16,18,27\}$. But each of these cases is impossible by Lemma 5.2.9. ■

Theorem 5.3.2. Let K be a number field such that $[K:\mathbb{Q}] = 7$ and let E/K be a non-CM elliptic curve with rational j-invariant. If $E(K)$ contains a point of order $n > 1$, then $C_n \in \Phi(1)$.

Proof. Assume that $E(K)$ contains a point P_n of order n. By Lemma 5.2.1, the prime factors of n can only be $2,3,5,7$. Therefore, write $n = 2^a 3^b 5^c 7^d$, where $a,b,c,d \geq 0$. If $c \neq 0$, then by Lemma 5.2.6 E is a base change of elliptic curve defined over $\mathbb{Q}$, so $C_n \in \Phi_{\mathbb{Q}}(7) = \Phi(1)$ by [19, Proposition 7.1.]. Assume that $c = 0$ and that $d \geq 1$. If $a \neq 0$, then $C_{14} \subseteq E(K)$. By Lemma 5.2.5 and Lemma 5.2.7 E' has a rational 2 and 7-isogenies, so it has a rational 14-isogeny. It follows that E' has CM by Theorem 2.1.1 which implies that E has CM as well, a contradiction. If $b \neq 0$, then we have $C_{21} \subseteq E(K)$. By Lemma 5.2.5 and Lemma 5.2.7, E' has a rational 3 and 7-isogenies, so it has a rational 21-isogeny.

By [34, Table 4], we have

$$j(E) \in \{-3^2 \cdot 5^6/2^3, 3^3 \cdot 5^3/2, 3^3 \cdot 5^3 \cdot 101^3/2^{21}, -3^3 \cdot 5^3 \cdot 383^3/2^7\}.$$

Using the division polynomial method in Magma [3] (code 7.3), we see that there does not exist an elliptic curve E' that obtains a point of order 21 over a degree 14 number field. Therefore, we cannot have $d \geq 1$ and $b \neq 0$. If $d \geq 2$, this is proven to be impossible in Lemma 4.1.3. It remains to consider the case $c = d = 0$. By Lemma 5.2.5, E' has a rational 2^a3^b-isogeny. By Theorem 2.1.1 we have

$$2^a3^b \in \{1,2,3,4,6,8,9,12,16,18,27\}.$$

Among these values of n, we have $C_n \notin \Phi(1)$ only for $n \in \{16,18,27\}$. But each of these cases is impossible by Lemma 5.2.9. ■

Proof of Theorem 5.1.2 (1). If E/K has CM, then the claim immediately follows from Theorem 5.2.2. Assume that E is non-CM. In order to complete the classification of $\Phi_{j\in\mathbb{Q}}(p)$, $p \geq 7$ we only need to consider groups G of the form $C_2 \oplus C_{2n}$. Assume that $C_2 \oplus C_{2n} \subseteq E(K)$ where $[K : \mathbb{Q}] = p$, E is non-CM and has a rational j-invariant. Then we obviously have $C_{2n} \subseteq E(K)$. By Theorem 5.3.2 and Theorem 5.3.1 we have $2n \in \{2,4,6,8,10,12\}$. If $2n \in \{10,12\}$, we know that this is impossible by Lemma 5.2.10. The remaining four cases are the groups contained in $\Phi(1)$. ■

5.4. Proof of Theorem 5.1.2 (2), case $p = 5$

We remind the reader that if E/K is an elliptic curve with rational j-invariant that is not isomorphic over K to a base change of elliptic curve defined over $\mathbb{Q}$, then $E'/\mathbb{Q}$ denotes an elliptic curve such that $j(E) = j(E')$ and L will denote the quadratic extension of K such that E and E' are isomorphic over L.

Lemma 5.4.1. Let K be a number field such that $[K : \mathbb{Q}] = 5$ and let E/K be a non-CM elliptic curve with rational j-invariant. Then $E(K)$ cannot contain C_{15}, C_{50}, C_{121} or C_{125}.

Proof. $\boxed{C_{15}}$: By Lemma 5.2.5 and Lemma 5.2.6, E' has a rational 15-isogeny. By [34, Table 4], we have $j(E') \in \{-5^2/2, -5^2 \cdot 241^3/2^3, -5 \cdot 29^3/2^5, 5 \cdot 211^3/2^{15}\}$. Let E_1, E_2, E_3, E_4 be the elliptic curves with LMFDB labels 50.a3, 450.g1, 50.a2, 450.g4, respectively. The j-invariants of these four curves are precisely the four possibilities for $j(E')$. We have $C_3 \subseteq E_i(\mathbb{Q})$, for $i \leq 4$. Since $j(E) = j(E_i)$, for some $i \leq 4$, they are isomorphic over quadratic extension L of K. Since $C_3 \oplus C_3 \cong E(K)[3] \oplus E_i(K)[3] \cong E_i(L)[3]$, Corollary 3.1.3 implies that $\mathbb{Q}(\zeta_3) \subseteq L$. Consider the primitive division polynomial $f_{E_i,15}$. Since $C_{15} \subseteq E_i(L)[15]$, $f_{E_i,15}$ has an irreducible factor f which has a root in L. A calculation in Magma [3] shows that every irreducible factor of $f_{E_i,15}$, $i \leq 4$ whose degree divides 10 has degree 2 or 10. Therefore $\deg(f) \in \{2, 10\}$. Depending on the degree of f, f either splits over $\mathbb{Q}(\zeta_3)$ (when $\deg(f) = 2$) or f splits into at least 2 irreducible factors over $\mathbb{Q}(\zeta_3)$ (when $\deg(f) = 10$). But a calculation in Magma [3] (code 7.10) shows that all irreducible factors of each polynomial $f_{E_i,15}$, $i \leq 4$ remain irreducible over $\mathbb{Q}(\zeta_3)$, a contradiction.

$\boxed{C_{50}}$: By Lemma 5.2.5 and Lemma 5.2.6 we have that E' has rational 2 and 5-isogenies. Suppose that $G_{E'}(5) \subseteq C_s(5)$. It follows that E' has two independent rational 5-isogenies and let $P_2 \in E'(\mathbb{Q})$ be a rational point of order 2. Denote by $\langle P \rangle$ and $\langle Q \rangle$ the kernels of these isogenies. We have that $\langle P_2 + P \rangle$ and $\langle Q \rangle$ are kernels of independent 10 and 5-isogenies, so E' is isogenous over $\mathbb{Q}$ to a curve $E''/\mathbb{Q}$ with a rational 50-isogeny by Lemma 2.1.2, which is impossible by Theorem 2.1.1. Therefore we conclude that $G_{E'}(5) \in \{5B.1.1, 5B.1.2, 5B.1.3, 5B.1.4, 5B.4.1, 5B.4.2, 5B\}$. Using Magma [3] (code 7.16) we first find all the possibilities for $G_{E'}(25)$ that are not con-

tained (up to conjugacy) in the Borel subgroup of $\mathrm{GL}_2(\mathbb{Z}/25\mathbb{Z})$. For each such possibility G of $G_{E'}(25)$, we check if G has a subgroup of index 5 or 10 that is a subgroup (up to conjugacy) of

$$B_0(25) := \left\{ \begin{bmatrix} 1 & * \\ 0 & * \end{bmatrix} \right\} \leq \mathrm{GL}_2(\mathbb{Z}/25\mathbb{Z}),$$

(or equivalently, if E' has a point of order 25 defined over a number field of degree 5 or 10). It turns out that there is no such groups G that satisfies these conditions. Therefore there does not exist an elliptic curve $E'/\mathbb{Q}$ with a rational 5-isogeny such that E' does not have a rational 25-isogeny and has a point of order 25 defined over a degree 5 or a degree 10 extension of $\mathbb{Q}$. This shows that if E' obtains a point P_{25} of order 25 over a degree 5 or 10 extension of $\mathbb{Q}$, then it must have a rational 25-isogeny. But since it has a rational 2-isogeny as well, it must have a rational 50-isogeny, which is impossible by Theorem 2.1.1.

$\boxed{C_{121},\, C_{125}}$: Since $C_{121} \subseteq E(K)$ (resp. $C_{125} \subseteq E(K)$) we have $C_{121} \subseteq E'(L)$ (resp. $C_{125} \subseteq E'(L)$). This is impossible by Lemma 4.1.3. ■

Theorem 5.4.2. Let K be a number field such that $[K : \mathbb{Q}] = 5$ and let E/K be a non-CM elliptic curve with rational j-invariant. If $E(K)$ contains a point of order $n > 1$, then $C_n \in \Phi_{\mathbb{Q}}(5)$.

Proof. Assume that $E(K)$ contains a point P_n of order n. By Lemma 5.2.1, the prime factors of n can only be $2,3,5,7,11$. Therefore, write $n = 2^a 3^b 5^c 7^d 11^e$, where $a,b,c,d,e \geq 0$. If $d \neq 0$, then by Lemma 5.2.7 E is a base change of an elliptic curve defined over $\mathbb{Q}$, so $C_n \in \Phi_{\mathbb{Q}}(5)$. Assume that $d = 0$. If $e \neq 0$, from [19, Table 2] we see that E' has a rational 11-isogeny. If one of a,b,c is not zero, E' would have a rational p-isogeny by Lemma 5.2.5 and Lemma 5.2.6, where $p \in \{2,3,5\}$ so it would have a rational $11p$-isogeny which is impossible by Theorem 2.1.1. Therefore we have $a = b = c = 0$. If $e \geq 2$, this is impossible by Lemma 5.4.1. We conclude that if $e \geq 1$, then $n = 11$. Consider now the case when $d = e = 0$. If $c \geq 1$, by Lemma 5.2.5 and Lemma 5.2.6 E' has a rational $2^a 3^b 5$-isogeny. By Theorem 2.1.1 we have $2^a 3^b 5 \in \{5,10,15\}$, so $(a,b) \in \{(0,0),(1,0),(0,1)\}$ and $n \in \{5^c, 2 \cdot 5^c, 3 \cdot 5^c\}$. We have that this is impossible by Lemma 5.4.1 unless $n \in \{5,10,25\}$, but for those values of n we have $C_n \in \Phi_{\mathbb{Q}}(5)$.

Finally let us consider the case when $n = 2^a 3^b$. By Theorem 2.1.1 and Lemma 5.2.5 we know that

$$n = 2^a 3^b \in \{1,2,3,4,6,8,9,12,16,18,27\}.$$

Removing the n for which $C_n \in \Phi_{\mathbb{Q}}(5)$ we only need to consider $n \in \{16,18,27\}$. These three cases have been proven to be impossible in Lemma 5.2.9. ■

Proof of Theorem 5.1.2 (2), case $p = 5$. If E/K has CM, then the claim immediately follows from Theorem 5.2.2. Assume that E is non-CM. In order to complete the classification of $\Phi_{j\in\mathbb{Q}}(5)$ we only need to consider groups G of the form $C_2 \oplus C_{2n}$. If $C_2 \oplus C_{2n} \subseteq E(K)$, then we obviously have $C_{2n} \subseteq E(K)$. By Theorem 5.4.2. we have $2n \in \{2,4,6,8,10,12\}$. If $2n \in \{10,12\}$, we know that this is impossible by Lemma 5.2.10. The remaining four cases are the groups already contained in $\Phi(1)$. ■

5.5. Proof of Theorem 5.1.2 (2), case $p = 3$

In this subsection, for an elliptic curve E/K with rational j-invariant that is not isomorphic over K to a base change of elliptic curve defined over $\mathbb{Q}$, let $E'/\mathbb{Q}$ be an elliptic curve such that $j(E) = j(E')$ and let L be a sextic number field over which E and E' are isomorphic.

Theorem 5.5.1. Let K be a number field such that $[K : \mathbb{Q}] = 3$ and let E/K be a non-CM elliptic curve with rational j-invariant. If $E(K)$ contains a point of order $n > 1$, then $C_n \in \Phi_{\mathbb{Q}}(3)$.

Proof. Let $C_n \subseteq E(K)$. We have that $C_n \subseteq E'(L)$ where $[L : \mathbb{Q}] = 6$. Therefore, by Theorem 4.0.1 we have that C_n is equal to the one of the following groups:

$$C_m : m = 1, \dots, 10, 12, 13, 14, 15, 16, 18, 21, 30.$$

If $C_n \in \Phi_{\mathbb{Q}}(3)$, we are done. Assume that this is not the case. Then $n \in \{15, 16, 30\}$. Obviously it is enough to show that $n = 15$ and $n = 16$ is impossible. If $n = 15$, by Lemma 5.2.6 we have that E is a base change of an elliptic curve defined over $\mathbb{Q}$. Since $C_{15} \notin \Phi_{\mathbb{Q}}(3)$, we are done. The case when $n = 16$ has been proven in Lemma 5.2.9. ■

Lemma 5.5.2. Let K be a number field such that $[K : \mathbb{Q}] = 3$ and let E/K be a non-CM elliptic curve with rational j-invariant. Then $E(K)$ cannot contain $C_2 \oplus C_{18}$.

Proof. Assume that $C_2 \oplus C_{18} \subseteq E(K)$. Since having a 2-torsion is a twist invariant property, we have $E'(K)[2] = C_2 \oplus C_2$. Since $[K : \mathbb{Q}] = 3$, we can conclude that $G_{E'}(2) \in \{2\text{Cs}, 2\text{Cn}\}$. A point P_3 of order 3 on E' is defined over an at most quadratic extension of $\mathbb{Q}$, by [18, Table 1]. Using Lemma 5.2.3 we can assume that $E'(\mathbb{Q})[3] = C_3$. Since $C_3 \oplus C_3 = E(K)[3] \oplus E'(K)[3] \cong E'(L)[3]$, $C_9 \subseteq E'(L)$ and $E'(L)[2] = C_2 \oplus C_2$, it follows that $C_6 \oplus C_{18} \subseteq E'(L)$, which is impossible by Theorem 4.0.1. ■

Proof of Theorem 5.1.2 (2), case $p = 3$. If E/K has CM, then the claim immediately follows from Theorem 5.2.2. Assume that E is non-CM. In order to complete the classification of $\Phi_{j \in \mathbb{Q}}(3)$ we only need to consider groups G of the form $C_2 \oplus C_{2n}$, where $n \geq 1$ is an integer and $G \in \Phi_{\mathbb{Q}}(6) \setminus \Phi_{\mathbb{Q}}(3)$. There are only three possibilites for G, namely $C_2 \oplus C_{10}$, $C_2 \oplus C_{12}$ and $C_2 \oplus C_{18}$. But all of these possibilites were already eliminated in Lemma 5.2.10 and Lemma 5.5.2. ■

5.6. Proof of Theorem 5.1.2 (3)

Theorem 5.6.1. Let K be a number field such that $[K:\mathbb{Q}]=2$ and let E/K be a non-CM elliptic curve with rational j-invariant. Then $E(K)_{tors} \in \Phi_{\mathbb{Q}}(2) \cup \{C_{13}\}$.

Proof. Obviously we have $\Phi_{\mathbb{Q}}(2) \subseteq \Phi_{j\in\mathbb{Q}}(2) \subseteq \Phi(2)$. By the classification of the set $\Phi(2)$ in [26], [31] and Theorem 2.1.3 we have $\Phi(2) \setminus \Phi_{\mathbb{Q}}(2) = \{C_{11}, C_{13}, C_{14}, C_{18}\}$. Let n be one of those values. Obviously E/K such that $E(K)$ contains a point P_n of order n cannot be a base change of an elliptic curve defined over $\mathbb{Q}$, by Theorem 2.1.3. Therefore, let $E'/\mathbb{Q}$ be an elliptic curve such that $j(E)=j(E')$ and let L be a quartic number field over which E and E' are isomorphic. This implies that $E'(L)$ contains a point of order $n \in \{11,14,18\}$, but this is impossible since $C_n \notin \Phi_{\mathbb{Q}}(4)$ by Theorem 2.1.5.

Let now $E''/\mathbb{Q}$ be an elliptic curve and L a quartic Galois extension of $\mathbb{Q}$ such that $P_{13} \in E''(L)$, where P_{13} is a point of order 13. Such an elliptic curve E'' and a field L exist by [7, Theorem 1.2]. Denote by K an intermediate field $\mathbb{Q} \subseteq K \subseteq L$. Since $L = K(\sqrt{d})$, consider a twist E^d/K of E''/K by d. We have

$$C_{13} \cong E''(L)[13] \cong E^d(K)[13] \oplus E''(K)[13].$$

We conclude that $C_{13} \subseteq E^d(K)[13]$ and so E^d/K is an elliptic curve with $j(E^d) \in \mathbb{Q}$ defined over a quadratic extension of $\mathbb{Q}$ with a point of order 13. ■

Proof of Theorem 5.1.2 (3). If E/K has CM, then the claim immediately follows from Theorem 5.2.2. If E is non-CM, then the claim follows directly from the previous theorem.

■

Remark 5.6.2. From [7, Proposition 5.3.] we see that there exists infinitely many elliptic curves $E/\mathbb{Q}$ such that there exists a cyclic quartic field K such that $C_{13} \subseteq E(K)$. Let E be one of those curves, K a number field such that $C_{13} \subseteq E(K)$ and F the unique quadratic subfield contained in K. Then we have $K = F(\sqrt{d})$, where d is square-free in F. We have

$$E^d(F)[13] \oplus E(F)[13] \cong E(K)[13].$$

Since $E(F)[13]$ cannot contain C_{13} because of Theorem 2.1.3, we have $C_{13} \subseteq E^d(F)[13]$. Therefore we obtain an elliptic curve E^d/F with rational j-invariant defined over quadratic

field F such that $C_{13} \subseteq E^d(F)$. Since there are infinitely many possibilities for E, it follows that there are infinitely many elliptic curves E' with rational j-invariant defined over some quadratic number field F such that $C_{13} \subseteq E'(F)$.

Remark 5.6.3. Consider the elliptic curve $E/\mathbb{Q}(\sqrt{17})$ defined by

$$E : y^2 + xy + y = x^3 - x^2 + (-131a - 205)x + 1758a + 2745,$$

where a is one of the roots of $x^2 - x - 4$. Short Weierstrass model of E is equal to

$$y^2 = x^3 + (-169776a - 265275)x + (80493264a + 125695638).$$

The j-invariant of this curve is equal to $\frac{-60698457}{40960}$. We have $E(\mathbb{Q}(\sqrt{17}))_{tors} \cong \mathbb{Z}/13\mathbb{Z}$. This curve has LMFDB label 100.1-e2.

Remark 5.6.4. For a positive integer d, define $\Phi^{\text{non}-\text{CM}}(d)$ to be the set of possible isomorphism classes of groups $E(K)_{tors}$, where K runs through all number fields K of degree d and E runs through all elliptic curves over K without CM. We expect that $\Phi_{j\in\mathbb{Q}}(d) \cap \Phi^{non-CM}(d)$ will often properly contain $\Phi_{\mathbb{Q}}(d) \cap \Phi^{non-CM}(d)$. To see that, assume that the Serre's uniformity conjecture holds (for example, see [19, Conjecture 3.3]) and take a prime $p \geq 37$. Assume that $E/\mathbb{Q}$ is an elliptic curve without complex multiplication. Then we have $G_E(p) = \mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$. By [19, Lemma 5.1.] we have that $[\mathbb{Q}(P) : \mathbb{Q}] = p^2 - 1$, where $P \in E(\overline{\mathbb{Q}})$ is a point of order p. The group $\mathrm{Gal}(\mathbb{Q}(E[p])/\mathbb{Q}(P))$ is an index 2 subgroup of

$$B(p) := \left\{ \begin{bmatrix} \pm 1 & * \\ 0 & * \end{bmatrix} \right\} \subseteq \mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z}).$$

Let L be the fixed field of B. By Galois theory, we have $[\mathbb{Q}(P) : L] = 2$. We conclude that $\mathbb{Q}(P) = L(\sqrt{d})$, for some square-free $d \in L$. Finally we have

$$E^d(L)[p] \oplus E(L)[p] \cong E(\mathbb{Q}(P))[p],$$

where E^d is a quadratic twist of E/L by d. Obviously $E(L)[p] = \{O\}$, so we must have $\mathbb{Z}/p\mathbb{Z} \subseteq E^d(L)[p]$. Therefore we have found an elliptic curve E^d/L with a rational j-invariant that has a point of order p defined over a field L of degree $\frac{p^2-1}{2}$. For this reason we expect that $\Phi_{j\in\mathbb{Q}}(\frac{p^2-1}{2}) \cap \Phi^{\text{non}-\text{CM}}(d)$ properly contains $\Phi_{\mathbb{Q}}(\frac{p^2-1}{2}) \cap \Phi^{\text{non}-\text{CM}}(d)$.

6. TORSION GROWTH OVER NUMBER FIELDS OF DEGREE pq

The main result of this chapter is the following theorem:

Theorem 6.0.1. Let $E/\mathbb{Q}$ be an elliptic curve and let K be a number field such that $[K:\mathbb{Q}] = pq$, where p,q are prime numbers such that $pq \neq 4,6$. Then we have

$$\Phi_{\mathbb{Q}}(pq) = \Phi_{\mathbb{Q}}(p) \cup \Phi_{\mathbb{Q}}(q),$$

for all primes p,q with the exception of the following:

$$\Phi_{\mathbb{Q}}(9) = \Phi_{\mathbb{Q}}(3) \cup \{C_{19}, C_{26}, C_{27}, C_{28}, C_{36}, C_{42}, C_2 \oplus C_{18}\},$$

$$\Phi_{\mathbb{Q}}(15) = \Phi_{\mathbb{Q}}(3) \cup \Phi_{\mathbb{Q}}(5) \cup \{C_{22}\} \cup \{C_{50}\},$$

$$\Phi_{\mathbb{Q}}(21) = \Phi_{\mathbb{Q}}(3) \cup \Phi_{\mathbb{Q}}(7) \cup \{C_{43}\},$$

$$\Phi_{\mathbb{Q}}(25) = \Phi_{\mathbb{Q}}(5) \cup \{C_{50}\},$$

$$\Phi_{\mathbb{Q}}(33) = \Phi_{\mathbb{Q}}(3) \cup \Phi_{\mathbb{Q}}(11) \cup \{C_{67}\},$$

$$\Phi_{\mathbb{Q}}(49) = \Phi_{\mathbb{Q}}(7) \cup \{C_{49}\}.$$

Let $E/\mathbb{Q}$ be an elliptic curve and let K be a number field such that $[K:\mathbb{Q}] = pq$, where p,q are prime numbers such that $pq \neq 4,6$. Assume that $r > 13$ is a prime number and that $P_r \in E(K)$ is a point of order r. We obviously must have that $[\mathbb{Q}(P_r):\mathbb{Q}]$ divides $[K:\mathbb{Q}] = pq$. Using Theorem 2.1.7, we look at the possible values of $[\mathbb{Q}(P_r):\mathbb{Q}]$. We can immediately see that $[\mathbb{Q}(P_r):\mathbb{Q}]$ is divisible by 4 except when $r \in \{19,43,67,163\}$. By the same theorem, we see that if $r \in \{19,163\}$ and $P_r \in E(K)$ is a point of order r, then $[\mathbb{Q}(P_r):\mathbb{Q}]$ divides a product of two prime numbers only if $r = 19$ and $[\mathbb{Q}(P_r):\mathbb{Q}] = 9$.

We also see that this happens only for CM elliptic curves. First we shall deal with elliptic curves without CM.

Let F_1 and F_2 be number fields. We say that these two fields are different if they are different as sets, i.e. if $F_1 \not\subseteq F_2$ or $F_2 \not\subseteq F_1$.

Lemma 6.0.2. Let K be a number field such that $[K:\mathbb{Q}] = pq$, where $p < q$ are prime numbers. Then there exists at most one subextension $\mathbb{Q} \subseteq F \subseteq K$ such that $[F:\mathbb{Q}] = p$.

Proof. Assume that there are two different fields F_1 and F_2 such that $[F_1:\mathbb{Q}] = [F_2:\mathbb{Q}] = p$. By the primitive element theorem, we can write $F_1 = \mathbb{Q}(\alpha_1)$ and $F_2 = \mathbb{Q}(\alpha_2)$ for some algebraic numbers α_1, α_2. We obviously have $1 < k = [F_1(\alpha_2) : F_1] \leq [\mathbb{Q}(\alpha_2) : \mathbb{Q}] = p$. Since the field $F_1F_2 = F_1(\alpha_2)$ is contained in K and has degree kp over $\mathbb{Q}$ it follows that $kp|pq$. We conclude that $k|q$. Since $k \leq p < q$, we have that $k = 1$. But this implies that $F_2 \subseteq F_1$, a contradiction. ■

From now on, when K is a number field such that $[K:\mathbb{Q}] = pq$ and $p < q$, by F we shall denote a unique subfield of K such that $[F:\mathbb{Q}] = p$ (if such field exists). Otherwise, we define F to be the field of rational numbers $\mathbb{Q}$.

Given an elliptic curve $E/\mathbb{Q}$ and a positive integer n, we denote by P_n a point of order n in $E(\overline{\mathbb{Q}})$.

Lemma 6.0.3. Let $E/\mathbb{Q}$ be an elliptic curve without complex multiplication and let K be a number field such that $[K:\mathbb{Q}] = pq$, where p, q are prime numbers such that $pq \notin \{4, 6\}$. Assume that $r \in \{2, 3, 5, 7, 11, 13\}$ is a prime number and that $P_r \in E(K)$, where P_r is a point of order r. Then E has a rational r-isogeny with the following two exceptions:

1. $3|pq$ and $r = 2$.
2. $p = q = 3$, $r = 7$ and E has LMFDB label 2450.y1 or 2450.z1 (or equivalently, if $G_E(7)$ is conjugate to a group with label 7Ns.2.1.).

Proof. The proof easily follows from the data available in Tables 6.1 and 6.2. ■

Lemma 6.0.4. Let K be a number field such that $[K:\mathbb{Q}] = pq$, where $p, q \geq 3$ are prime numbers and let E/K be an elliptic curve without CM. For a prime $r \in \{2, 3, 5, 7, 11, 13\}$

and a positive integer k, we have the following possibilities for $[\mathbb{Q}(P_{r^k}):\mathbb{Q}]$, where $P_{r^k} \in E(K)$ is a point of order r^k.

	$[\mathbb{Q}(P_{2^k}):\mathbb{Q}]$	$[\mathbb{Q}(P_{3^k}):\mathbb{Q}]$	$[\mathbb{Q}(P_{5^k}):\mathbb{Q}]$	$[\mathbb{Q}(P_{7^k}):\mathbb{Q}]$
$p,q \geq 11$	1	1	1	1
$p=7, q \geq 11$	1	1	1	1,7
$p=7, q=7$	1	1	1	1,7,49
$p=5, q \geq 11$	1	1	1,5	1
$p=5, q=7$	1	1	1,5	1,7
$p=5, q=5$	1	1	1,5,25	1
$p=3, q \geq 11$	1,3	1,3	1	1,3
$p=3, q=7$	1,3	1,3	1	1,3,7
$p=3, q=5$	1,3	1,3	1,5	1,3
$p=3, q=3$	1,3	1,3,9	1	1,3,9
$p=2, q \geq 11$	1,2	1,2	1,2	1,2
$p=2, q=7$	1,2	1,2	1,2	1,2,7,14
$p=2, q=5$	1,2	1,2	1,2,5,10	1,2

	$[\mathbb{Q}(P_{11^k}):\mathbb{Q}]$	$[\mathbb{Q}(P_{13^k}):\mathbb{Q}]$
$p,q \geq 7$	\	\
$p=5, q \geq 13$	\	\
$p=5, q=11$	$5, 55$	\
$p=5, q=7$	5	\
$p=5, q=5$	5	\
$p=3, q>13$	\	3
$p=3, q=13$	\	$3, 39$
$p=3, q=11$	\	3
$p=3, q=7$	\	3
$p=3, q=5$	5	\
$p=3, q=3$	\	3
$p=2, q \geq 11$	\	\
$p=2, q=7$	\	\
$p=2, q=5$	$5, 10$	\

The proof of this Lemma follows directly from the known results. We briefly describe the method of calculating the possibilities for $[\mathbb{Q}(P_{r^k}):\mathbb{Q}]$.

Proof. Using Theorem 2.1.7, we can see what the possible values of $[\mathbb{Q}(P_r):\mathbb{Q}]$ are. Since $[\mathbb{Q}(P_r):\mathbb{Q}]$ divides $[K:\mathbb{Q}]$, we can eliminate most of the possibilities for $[\mathbb{Q}(P_r):\mathbb{Q}]$. From Proposition 2.1.8 it follows that for $k \geq 2$ we have that $[\mathbb{Q}(P_{r^k}):\mathbb{Q}(P_{r^{k-1}})]$ divides $r^2(r-1)$. Since $r \in \{2,3,5,7,11,13\}$ we see that the prime factors of $[\mathbb{Q}(P_{r^k}):\mathbb{Q}(P_{r^{k-1}})$ are contained in the set $\{2,3,5,7,11,13\}$. Inductively, we see that the prime factors of $[\mathbb{Q}(P_{r^k}):\mathbb{Q}]$ are also contained in the set $\{2,3,5,7,11,13\}$. Assume that $P_{r^k} \in E(K)$. We have that $[\mathbb{Q}(P_{r^k}):\mathbb{Q}]$ divides $[K:\mathbb{Q}] = pq$. For example, if $p<q$ and $q>13$, then $[\mathbb{Q}(P_{r^k}):\mathbb{Q}]$ is relatively prime to q, so $[\mathbb{Q}(P_{r^k}):\mathbb{Q}]$ divides p. We conclude that $E(K)_{tors} = E(F)_{tors}$. Depending on the actual values of p and q, we can apply the reasoning analogous to this one. ■

We now state a useful fact we will use throughout this chapter.

Lemma 6.0.5. Let $E/\mathbb{Q}$ be an elliptic curve and $P_4 \in E(\overline{\mathbb{Q}})$ a point of order 4. Assume that $[\mathbb{Q}(P_4):\mathbb{Q}] = 3$. Then the 2-adic representation of E is has a label X_{20b}. Additionally, $G_E(2) = \mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z})$ and $\mathbb{Q}(E[2]) = \mathbb{Q}(E[4])$ is an S_3-extension of $\mathbb{Q}$.

Proof. This immediately follows by a search through the data of [47] (code 7.11). ■

Lemma 6.0.6. Let $E/\mathbb{Q}$ be an elliptic curve without CM and let K be a number field such that $[K:\mathbb{Q}] = pq$, where p and q are prime numbers and $pq \notin \{4,6,9\}$. Let $r \in \{11,13\}$ be a prime number. If $C_r \subseteq E(K)_{tors}$, then $E(K)_{tors} \cong C_r$ or $E(K)_{tors} \cong C_{2r}$. The latter case occurs only when $r = 11$ and $[K:\mathbb{Q}] = 15$,

Proof. Consider the case when $r = 11$. By Lemma 6.0.3 we see that E has a rational 11-isogeny. Additionally, if $P_{11} \in E(K)$, then $[\mathbb{Q}(P_{11}):\mathbb{Q}] \in \{5,10,55\}$. Assume that $E(K)$ contains a point P_ℓ of order ℓ, where $\ell \neq 2,11$ is a prime number. Then by the same lemma, E has a rational ℓ-isogeny, so it has a rational 11ℓ-isogeny, which contradicts Theorem 2.1.1. If $P_{121} \subseteq E(K)$, then by Lemma 6.0.4 we have that $[\mathbb{Q}(P_{121}):\mathbb{Q}] \leq 55$, which is impossible by Lemma 4.1.3. Finally, assume that $\ell = 2$ and $P_2 \in E(K)$. If E has a rational 2-isogeny, then it has a rational 22-isogeny, which contradicts Theorem 2.1.1. Assume that E does not have a rational 2-isogeny. It follows that $[\mathbb{Q}(P_2):\mathbb{Q}] = 3$. Since $\mathbb{Q} = \mathbb{Q}(P_2) \cap \mathbb{Q}(P_{11})$, it follows that the field compositum $\mathbb{Q}(P_2)\mathbb{Q}(P_{11})$ has degree divisible by 15, hence $[K:\mathbb{Q}] = 15$. It remains to show that if $[K:\mathbb{Q}] = 15$ and $C_{22} \subseteq E(K)_{tors}$, then $E(K)_{tors}$ cannot contain a point P_4 of order 4. Assume that this is the case. By Lemma 6.0.4, we have $[\mathbb{Q}(P_4):\mathbb{Q}] = 3$. By Lemma 6.0.5, the 2-adic Galois representation of E has a label X_{20b}. This implies that $j(E) = \frac{32t-4}{t^4}$, for some $t \in \mathbb{Q} \setminus \{0\}$. Since E has a rational 11-isogeny,

$$j(E) \in \{-11 \cdot 131^3, -2^{15}, -11^2\}$$

by [34, Table 4]. For $a \in \{-11 \cdot 131^3, -2^{15}, -11^2\}$ we see that the equation $a = \frac{32t-4}{t^4}$ has no solutions in the set of rational numbers except when $a = -2^{15}$, in which case we have $t = -\frac{1}{8}$. To see this, for every possibility of a we factor the polynomial $at^4 - 32t + 4$. If $a \neq -2^{15}$, this polynomial will be irreducible over $\mathbb{Q}$ so it has no rational solutions. If $a = -2^{15}$ we have

$$at^4 - 32t + 4 = -4(8t+1)(1024t^3 - 128t^2 + 16t - 1).$$

The polynomial $1024t^3 - 128t^2 + 16t - 1$ is irreducible over $\mathbb{Q}$, so it has no rational roots. Therefore the only rational solutions are $(a,t) = (-2^{15}, -\frac{1}{8})$. Using the division polynomial method we directly check that if $E/\mathbb{Q}$ is an elliptic curve with $j(E) = -2^{15}$, then E cannot contain a point of order 44 over a number field of degree 15.

Assume that $r = 13$. By Lemma 6.0.3 we see that E has a rational 13-isogeny. Additionally, if $P_{13} \in E(K)$, then $[\mathbb{Q}(P_{13}) : \mathbb{Q}] \in \{3, 39\}$ by Lemma 6.0.4. Assume that $E(K)$ contains a point P_ℓ of order ℓ, where $\ell \neq 2, 13$ is a prime number. Then by the same Lemma, E has a rational ℓ-isogeny, so it has a rational 13ℓ-isogeny, which contradicts Theorem 2.1.1. If $P_{169} \subseteq E(K)$, then by Lemma 6.0.4 we have that $[\mathbb{Q}(P_{169}) : \mathbb{Q}] \leq 39$, which is impossible by Lemma 4.1.3. It remains to consider the case when $\ell = 2$. Assume that $P_2 \in E(K)$. If E has a rational 2-isogeny, then it has a rational 26-isogeny, which contradicts Theorem 2.1.1. Assume that E does not have a rational 2-isogeny. It follows that $[\mathbb{Q}(P_2) : \mathbb{Q}] = 3$. We conclude that $\mathbb{Q}(P_2) = F$. If $[\mathbb{Q}(P_{13}) : \mathbb{Q}] = 3$, then $\mathbb{Q}(P_{13}) = F$, so we have $C_{26} \in \Phi_{\mathbb{Q}}(3)$, a contradiction by Theorem 2.1.4. Consider the case when $[\mathbb{Q}(P_{13}) : \mathbb{Q}] = 39$. From Table 6.2 we see that $G_E(13) = 13\text{B}.3.2$. A computation in Magma [3] (code 7.12) shows that $\mathrm{Gal}(\mathbb{Q}(E[13])/\mathbb{Q}(P_{13}))$ is contained in the group

$$H = \left\langle \begin{bmatrix} 3 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 2 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix} \right\rangle.$$

The group H is normal and of index 3 in $G_E(13)$. It follows that $\mathbb{Q}(P_{13})$ has a Galois cubic subfield and that subfield is equal to F. We conclude that $G_E(2) = 2\text{Cn}$, so $j(E) = t^2 + 1728$, for some $t \in \mathbb{Q}$. Since E has a rational 13-isogeny, we have

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

It remains to find rational numbers s,t with $s \neq 0$ satisfying

$$\frac{(s^2+5s+13)(s^4+7s^3+20s^2+19s+1)^3}{s} = t^2 + 1728.$$

This is equivalent to

$$\frac{(s^2+6s+13)}{s}(s^6+10s^5+46s^4+108s^3+122s^2+38s-1)^2 = t^2.$$

It follows that $\frac{(s^2+6s+13)}{s} = x^2$, for some $x \in \mathbb{Q}$. Putting $x := \frac{y}{s}$ we have $x^2 = \frac{y^2}{s^2} = \frac{(s^2+6s+13)}{s}$, so

$$y^2 = s^3 + 6s^2 + 13s.$$

A computation in Magma [3] (code 7.12) shows that the only rational solution to this equation is $(y,s)=(0,0)$, but this contradicts our assumption that $s\neq 0$. We conclude that our original equation does not have rational solutions, so there does not exist an elliptic curve $E/\mathbb{Q}$ with $G_E(2)=2\text{Cn}$ and a rational 13-isogeny. ■

Let r be a prime number and let $E/\mathbb{Q}$ be an elliptic curve. By $E(K)[p']$ we will denote the largest subgroup of $E(K)_{tors}$ that does not contain an element of order p.

Lemma 6.0.7. Let $E/\mathbb{Q}$ be an elliptic curve without CM and let K be a number field such that $[K:\mathbb{Q}]\in\{15,21,25,33,35,39,49,55,65,77,91\}$. If p is the smallest prime factor of $[K:\mathbb{Q}]$, then $\Phi_{\mathbb{Q}}([K:\mathbb{Q}])=\Phi_{\mathbb{Q}}(p)$.

Proof. We will split the proof in two parts. In the first part we will consider only cyclic groups, while in the second part we will consider the groups of the form $C_m\oplus C_{mn}$, where $m\geq 2$.

Cyclic cases

Assume that $P_n\in E(K)$ is a point of order n. In the previous lemma we have found all the possibilities for $E(K)_{tors}$ when $C_{11}\subseteq E(K)$ or $C_{13}\subseteq E(K)$. Therefore, we shall assume that this is not the case. It follows that the prime factors of n are contained in the set $\{2,3,5,7\}$ and we write $n=2^a3^b5^c7^d$.

$[K:\mathbb{Q}]=15$

By Lemma 6.0.4, we see that if $r\in\{2,3,7\}$, then $E(K)[r^\infty]=E(F)[r^\infty]$. Therefore if $c=0$, then $E(K)_{tors}\in\Phi_{\mathbb{Q}}(3)$. The case when $c\geq 3$ is impossible by Lemma 4.1.3. Assume that $c=2$. Then we have $[\mathbb{Q}(P_{25}):\mathbb{Q}]=5$ by Lemma 6.0.4 and E has a rational 25-isogeny by [16, Lemma 10 (3)]. If $E(K)$ contains a point of order $r\in\{3,7\}$, then by Lemma 6.0.3, E has a rational r-isogeny so it has a rational $25r$-isogeny. This contradicts Theorem 2.1.1. Assume that $a\geq 2$. We show that $E(K)$ cannot contain a point P_4 of order 4. By Lemma 6.0.4 we see that $[\mathbb{Q}(P_4):\mathbb{Q}]\in\{1,3\}$. If $[\mathbb{Q}(P_4):\mathbb{Q}]=1$, then E has a rational 4-isogeny, so it has a rational 100-isogeny, which contradicts Theorem 2.1.1. If $[\mathbb{Q}(P_4):\mathbb{Q}]=3$, Lemma 6.0.5 shows that the 2-adic image of E has a label X_{20b}. Since E has a rational 5-isogeny, it remains to show that there does not exist an elliptic curve $E/\mathbb{Q}$ with a rational 5-isogeny and a point P_4 of order 4 such that $[\mathbb{Q}(P_4):\mathbb{Q}]=3$. In order to do that, we consider the fiber product $X_{20}\times X_0(5)$. In [11, Proposition 6. (k)] it has

been proven that rational points on this curve are the 2 singular points $[0,-1,1],[0,1,0]$ and one cusp at infinity $[1,0,0]$, which do not correspond to elliptic curves. Therefore if $C_{25} \subseteq E(K)_{tors}$, then $E(K)_{tors} \cong C_{25}$ or $E(K)_{tors} \cong C_{50}$. Finally, assume that $c = 1$. If $d \neq 0$, then E has a rational 35-isogeny, a contradiction with Theorem 2.1.1. If $b \neq 0$, then E has a rational 15-isogeny, so

$$j(E) \in \{-5^2/2, -5^2 \cdot 241^3/2^3, -29^3 \cdot 5/2^5, 211^3 \cdot 5/2^{15}\}$$

by [34, Table 4]. Using the division polynomial method (code 7.4) we show that this is impossible.

$\boxed{[K:\mathbb{Q}] = 21}$

As in the previous case we conclude that if $r \in \{2,3,5\}$, then $E(K)[r^\infty] = E(F)[r^\infty]$. Assume that $d \neq 0$. If $c \neq 0$, then E has a rational 35-isogeny, which is impossible by Theorem 2.1.1. If $b \neq 0$, then E has a rational 21-isogeny. Using the division polynomial method (code 7.3) we show that if $C_{21} \subseteq E(K)$, then $E(K)_{tors} \cong C_{21}$. Finally, assume that $a \neq 0$. If E has a rational 2-isogeny, then E has a rational 14-isogeny so it has CM, a contradiction. It remains to consider the case when $G_E(2) = \mathrm{GL}_2(\mathbb{F}_2)$. If $a \geq 2$, then as before we conclude that the 2-adic image of E has label X_{20b}. There exists a morphism $X_{20b}(\mathbb{Q}) \to X_7(\mathbb{Q})$ and we can find all the points on $X_{20b}(\mathbb{Q})$ by finding all the points on $X_7(\mathbb{Q})$. We want to show that there does not exist an elliptic curve $E/\mathbb{Q}$ with a rational 7-isogeny and such that its 2-adic representation is contained in the group that is parameterized by $X_7(\mathbb{Q})$. For this purpose, we consider the fiber product $X_7 \times X_0(7)$ (code 7.14). It is birational to the hyperelliptic curve C of genus 2 and rank 1 over $\mathbb{Q}$ given by the equation

$$C:\ y^2 = x^6 + 2x^5 - 4x^4 + 4x^3 - 4x^2 + 2x + 1.$$

Using the Chabauty method in Magma [3] we see that $C(\mathbb{Q}) = \{(0,\pm 1)\}$. Pulling back these points to the corresponding points on $X_7 \times X_0(7)$ shows that the affine rational points on $X_7 \times X_0(7)$ are $(16/479, -49/4)$ and $(2/3,-4)$. These points correspond to elliptic curves with j-invariants $-38575685889/16384$ and $351/4$, respectively. Using the division polynomial method we check that if $j(E)$ is equal to one of these two values, then E does not have a point of order 28 defined over a number field of degree 21. Using the

division polynomial method we check that elliptic curve with j-invariant equal to one of these two values does not have a point of order 28 defined over a number field of degree 21.

$\boxed{[K:\mathbb{Q}]=25}$ By Lemma 6.0.4, we see that if $r\in\{2,3,7\}$, then $E(K)[r^\infty]=E(\mathbb{Q})[r^\infty]$. Lemma 4.1.3 shows that we cannot have $c\geq 3$. If $c=2$, then $P_{25}\in E(K)$. If $[\mathbb{Q}(P_{25}):\mathbb{Q}]=5$, then $E(K)_{tors}=E(\mathbb{Q}(P_{25}))_{tors}\in\Phi_{\mathbb{Q}}(5)$. It remains to consider the case when $[\mathbb{Q}(P_{25}):\mathbb{Q}]=25$. Since E has a rational 5-isogeny by Lemma 6.0.3, then as in the previous case we conclude that $d=0$. Additionally, if $b\neq 0$, we conclude that E has a rational 15-isogeny. Using the division polynomial method (code 7.4) we show that this is impossible. It remains to show that we cannot have $a\geq 2$. Assume that this is the case. It remains to check that it is not possible to have $C_{100}\subseteq E(K)_{tors}$. By Lemma 6.0.4 we see that if $P_4\in E(K)$ then $[\mathbb{Q}(P_4):\mathbb{Q}]=1$. We conclude that E has a rational 4-isogeny. Since E has a rational 5-isogeny, it has a rational 20-isogeny. This contradicts the Theorem 2.1.1.

An example of an elliptic curve $E/\mathbb{Q}$ such that E obtains a point of order 50 over a degree 25 number field is

$$E:\ y^2+xy=x^3-45x+81.$$

This can be checked using an algorithm from [18].

$\boxed{[K:\mathbb{Q}]\in\{33,39,55,65,77,91\}}$ By Lemma 6.0.4, we see that if $r\in\{2,3,5,7\}$, then $E(K)[r^\infty]=E(F)[r^\infty]$. Therefore we have $E(K)_{tors}\in\Phi_{\mathbb{Q}}(p)$.

$\boxed{[K:\mathbb{Q}]=35}$ If $cd\neq 0$, then by Lemma 6.0.3, E has rational 5 and 7-isogenies, so it has a rational 35-isogeny. This contradicts Theorem 2.1.1. If $d\neq 0$, we must therefore have $c=0$. By Lemma 6.0.4, we see that if $r\in\{2,3\}$, then $E(K)[r^\infty]=E(\mathbb{Q})[r^\infty]$. By the same Lemma we have $[\mathbb{Q}(P_7):\mathbb{Q}]\in\{1,7\}$. We conclude that $E(K)_{tors}=E(\mathbb{Q}(P_7))_{tors}\in\Phi_{\mathbb{Q}}(7)=\Phi(1)$. Assume that $d=0$. By the same argument we conclude that $E(K)_{tors}=E(F)_{tors}\in\Phi_{\mathbb{Q}}(5)$.

$\boxed{[K:\mathbb{Q}]=49}$ By Lemma 6.0.4, we see that if $r\in\{2,3,5\}$, then $E(K)[r^\infty]=E(\mathbb{Q})[r^\infty]$. Assume that $d=1$. Then $[\mathbb{Q}(P_7):\mathbb{Q}]\in\{1,7\}$ by the same Lemma. We conclude that $E(K)_{tors}=E(\mathbb{Q}(P_7))_{tors}\in\Phi_{\mathbb{Q}}(7)=\Phi(1)$. By Theorem 1.0.12 we have $E(K)_{tors}\cong C_7$. It remains to show that if $d\geq 2$ then $a=b=c=0$ and $d=2$. Assume that $d\geq 2$. Then

$P_{49} \in E(K)$, where P_{49} denotes a point of order 49. Obviously we cannot have $[\mathbb{Q}(P_{49}) : \mathbb{Q}] \in \{1,7\}$, since $C_{49} \notin \Phi_{\mathbb{Q}}(7) = \Phi(1)$ by Theorem 1.0.12. Therefore we have $[\mathbb{Q}(P_{49}) : \mathbb{Q}] = 49$. By Table 6.1 we see that $G_E(7) = 7\text{B}.1.3$ or $G_E(7) = 7\text{B}.1.1$. Assume that $G_E(7) = 7\text{B}.1.3$. Using Magma [3] (code 7.13), we search for all the possible subgroups G of $\mathrm{GL}_2(\mathbb{Z}/49\mathbb{Z})$ that reduce modulo 7 to a subgroup of $G_E(7)$. It turns out that all such groups are contained (up to conjugation) in Borel subgroup of $\mathrm{GL}_2(\mathbb{Z}/49\mathbb{Z})$. This means that E has a rational 49-isogeny, a contradiction by Theorem 2.1.1. Now we consider the remaining case when $G_E(7) = 7\text{B}.1.1$. It follows that $C_7 \subseteq E(\mathbb{Q})$. As we have previously noted, if $r \in \{2,3,5\}$ and $P_r \in E(K)$, then $P_r \in E(\mathbb{Q})$. Therefore we have $P_{7r} \in E(\mathbb{Q})$, a contradiction by Theorem 1.0.12. It remains to show that $d = 2$. It is enough to show that we cannot have $d = 3$. Assume that this is the case, so $E(K)$ contains a point P_{343} of order $7^3 = 343$. Since E has a rational 7-isogeny, by [18, Lema 2.7] we have that the 7-adic representation of E is as large as possible (meaning it is equal to the inverse image of the reduction mod 7) or $j_E \in \{-15^3, 255^3\}$. In the proof of the same Lemma it has been shown that in the latter case we have $[\mathbb{Q}(P_{49}) : \mathbb{Q}] \geq 147$. Therefore, the 7-adic representation of E is as large as possible. By the [18, Proposition 2.2] we see that if $P_{343} \in E(K)$ is a point of order 343, then $[\mathbb{Q}(P_{343}) : \mathbb{Q}(7P_{343})] = 49$. Therefore a point $7P_{343}$ of order 49 is defined over $\mathbb{Q}$, a contradiction with Theorem 1.0.12. Therefore we cannot have $d \geq 3$.

An example of an elliptic curve $E/\mathbb{Q}$ such that E attains a point of order 49 over a number field of degree 49 is

$$E : y^2 + xy + y = x^3 - x^2 - 3x + 3.$$

This can be seen by using an algorithm from [18].

Non-cyclic cases

It remains to consider the groups of the form $C_m \oplus C_{mn}$, $m \geq 2$. If $C_m \oplus C_{mn} \subseteq E(K)$, then by 3.1.3 we have $\mathbb{Q}(\zeta_m) \subseteq K$ and $\phi(m) = [\mathbb{Q}(\zeta_m) : \mathbb{Q}]$ is even for $m \geq 3$. Therefore we have $m = 2$.

Since $C_2 \oplus C_2 \subseteq E(K)$, we have $C_2 \oplus C_2 \in E(F)$, so $G_E(2)$ is the trivial group or $G_E(2) = 2\text{Cn}$. Note that in the latter case we have $F = \mathbb{Q}(E[2])$. First we consider the case when $G_E(2)$ is trivial. Then E has two independent rational 2-isogenies. Additionally, we

have $E(K)[2^\infty] = E(\mathbb{Q})[2^\infty]$ because of Proposition 2.1.8.

If $r \geq 5$ is a prime number and $P_r \in E(K)$, then by Lemma 6.0.3, E has a rational r-isogeny. By Lemma 2.1.2, E is isogenous over $\mathbb{Q}$ to an elliptic curve $E''/\mathbb{Q}$ that has a rational $4r$-isogeny, which is impossible by Theorem 2.1.1.

Assume that $r = 3$, $k \geq 1$ and that $P_{r^k} \in E(K)$. By Lemma 6.0.4 we see that $[\mathbb{Q}(P_{r^k}) : \mathbb{Q}] \in \{1,3\}$, so $C_{r^k} \in \Phi_{\mathbb{Q}}(3)$. Theorem 2.1.3 implies that $k \leq 2$. If $k = 2$, then we have $C_2 \oplus C_{18} \subseteq E(F)$, but this contradicts Theorem 2.1.4. Therefore $k = 1$ is the only possibility, but $C_2 \oplus C_6$ is already contained in $\Phi(1)$.

Assume now that $G_E(2) = 2\mathrm{Cn}$. It follows that K contains a cubic Galois subextension F and $j(E) = s^2 + 1728$, for some $s \in \mathbb{Q}$. If $P_5 \in E(K)$, then $j(E) = \frac{25(t^2+10t+5)^3}{t^5}$ for some $t \in \mathbb{Q} \setminus \{0\}$. It remains to find rational points s,t with $t \neq 0$ such that

$$\frac{25(t^2+10t+5)^3}{t^5} = s^2 + 1728.$$

This is equivalent to

$$(t^2-20t-25)^2\frac{(25t^2+22t+5)}{t^5} = s^2.$$

It follows that $\frac{(25t^2+22t+5)}{t^5}$ must be a square, i.e. $\frac{(25t^2+22t+5)}{t^5} = x^2$, for some $x \in \mathbb{Q}$. Putting $t := \frac{t_1}{25}$ and $x := \frac{25^2 y}{t_1^3}$ we obtain an elliptic curve

$$E' : \ y^2 = t_1^3 + 22t_1^2 + 125t_1.$$

A computation in Magma [3] (code 7.15) shows that $E'(\mathbb{Q}) = \{O, (0,0)\}$. It follows that $t_1 = 0$ and therefore $t = 0$, a contradiction. We conclude that there does not exist an elliptic curve $E/\mathbb{Q}$ with $G_E(2) = 2\mathrm{Cn}$ and a rational 5-isogeny.

Finally, assume that $P_7 \in E(K)$. By a search through the data of [47] we see that if $C_2 \oplus C_4 \subseteq E(F)$, then $C_2 \oplus C_4 \subseteq E(\mathbb{Q})$, so E has a rational 4-isogeny and therefore it has a rational 28-isogeny, a contradiction with Theorem 2.1.1. It has already been proven in this Lemma that if $C_{49} \in \Phi_{\mathbb{Q}}([K:\mathbb{Q}])$, then $[K:\mathbb{Q}] = 49$ which contradicts our assumption that K contains F. If $C_2 \oplus C_{42} \subseteq E(K)$, then E has a rational 21-isogeny, so

$$j(E) \in \{-3^2 \cdot 5^6/2^3, 3^3 \cdot 5^3/2, 3^3 \cdot 5^3 \cdot 101^3/2^{21}, -3^3 \cdot 5^3 \cdot 383^3/2^7\}$$

by [34, Table 4]. Additionally, since $G_E(2) = 2\mathrm{Cn}$, we have $j(E) = t^2 + 1728$, for some $t \in \mathbb{Q}$. It is easily seen that if a is one of the four values mentioned then the equation

$t^2+1728=a$ does not have rational solution t. Therefore if $C_2\oplus C_{14}\subseteq E(K)$, then $C_2\oplus C_{14}=E(K)_{tors}$. If $P_{3^k}\in E(K)$, then as in the previous case we conclude that $C_{3^k}\subseteq E(F)$, so $C_2\oplus C_{2\cdot 3^k}\subseteq E(F)_{tors}\in\Phi_{\mathbb{Q}}(3)$, which implies that $k=1$. It is impossible to have $C_2\oplus C_{12}\subseteq E(K)$ because (as we have previously noted) $C_2\oplus C_4\subseteq E(\mathbb{Q})$ and $P_3\in\Phi_{\mathbb{Q}}(3)$ which implies that $C_2\oplus C_{12}\in\Phi_{\mathbb{Q}}(3)$. This contradicts the Theorem 2.1.4. It remains to show that if $C_2\oplus C_{2^k}\in E(K)$, then $k\leq 3$. For this it is enough to show that it is impossible to have $k=4$. This has already been proven in Theorem 4.3.1. ■

Lemma 6.0.8. Let K be a number field such that $[K:\mathbb{Q}]=2p$, where $p\geq 5$ is prime and let $E/\mathbb{Q}$ be an elliptic curve without CM. Then $\Phi_{\mathbb{Q}}(2p)=\Phi_{\mathbb{Q}}(p)\cup\Phi_{\mathbb{Q}}(2)$.

Proof. Let us first consider the case when $p\geq 11$. Lemma 6.0.4 shows that if $r\in\{2,3,5,7\}$ then $E(K)[r^\infty]=E(F)[r^\infty]$. Therefore we conclude that $E(K)_{tors}=E(F)_{tors}$. This follows from the fact that $[\mathbb{Q}(P_{r^k}):\mathbb{Q}]\in\{1,2\}$ and that F is unique. It follows that $\Phi_{\mathbb{Q}}(2p)=\Phi_{\mathbb{Q}}(2)$. Note that by [19, Proposition 7.1.] we have $\Phi_{\mathbb{Q}}(p)=\Phi(1)$, so $\Phi_{\mathbb{Q}}(2p)=\Phi_{\mathbb{Q}}(p)\cup\Phi_{\mathbb{Q}}(2)$.

Assume that $p=7$. Lemma 4.1.3 shows that $E(K)$ cannot contain a point of order 49. By the analogous reasoning as in the previous case, Lemma 6.0.4 shows that if $r\in\{2,3,5\}$ then $E(K)[r^\infty]=E(F)[r^\infty]$. If $E(K)$ does not contain a point of order 7, then $E(K)_{tors}=E(F)_{tors}\in\Phi_{\mathbb{Q}}(2)$. If $E(K)$ contains a point of order 7, then E has a rational 7-isogeny, by Lemma 6.0.3. By the same lemma, if E contains a point of order $r\in\{2,3,5\}$, then E has a rational r-isogeny. For $r=2$, E would have a rational 14-isogeny so it has CM by Theorem 2.1.1. If $r=3$, then E has a rational 21-isogeny so

$$j(E)\in\{-3^2\cdot 5^6/2^3, 3^3\cdot 5^3/2, 3^3\cdot 5^3\cdot 101^3/2^{21}, -3^3\cdot 5^3\cdot 383^3/2^7\}$$

by [34, Table 4]. The division polynomial method shows that this case is impossible (code 7.17). If $r=5$, then E has a rational 35-isogeny, which is impossible by Theorem 2.1.1.

Finally, assume that $p=5$. Let $P_n\in E(K)$ be the point of order $n=2^a3^b5^c7^d11^e$. Assume that $e\geq 1$. We have that E has a rational 11-isogeny. If $r\in\{2,3,5,7\}$ and $E(K)$ contains a point of order r, then Lemma 6.0.3 implies that E has a rational r-isogeny. We conclude that E has a rational $11r$-isogeny, which is a contradiction by Theorem 2.1.1. Therefore if $C_{11}\subseteq E(K)_{tors}$, then $E(K)_{tors}\cong C_{11}$.

Assume that $e = 0$. If $c \geq 3$, then $E(K)$ contains a point of order 125, which is impossible by Lemma 4.1.3. Assume now that $c = 2$ and that $P_{25} \in E(K)$ is a point of order 25 such that $[\mathbb{Q}(P_{25}) : \mathbb{Q}] = 10$. Using Magma [3] (code 7.16) we find all the subgroups $G \leq \mathrm{GL}_2(\mathbb{Z}/25\mathbb{Z})$ with $G \equiv G_E(5) \pmod 5$, $\det(G) = (\mathbb{Z}/25\mathbb{Z})^\times$ and a subgroup of index 10 that fixes a non-zero vector of order 25. All such groups are contained (up to conjugation) in the Borel subgroup of $\mathrm{GL}_2(\mathbb{Z}/25\mathbb{Z})$. We conclude that E has a rational 25-isogeny. If $r \in \{2,3,7\}$ and $P_r \in E(K)$ is a point of order r, then by Lemma 6.0.3 E has a rational $25r$-isogeny, a contradiction by Theorem 2.1.1. Therefore if $P_{25} \in E(K)$, then $E(K)_{tors} \cong C_{25} \in \Phi_{\mathbb{Q}}(5)$. Assume that $c = 0$. By Lemma 6.0.4 we see that for $r \in \{2,3,7\}$ we have $E(K)[r^\infty] = E(F)[r^\infty]$, so we conclude that $E(K)[r^\infty] \in \Phi_{\mathbb{Q}}(2)$. Consider the remaining case, when $c = 1$. If $d \geq 1$, then by Lemma 6.0.3, E has a rational 7-isogeny so it has a rational 35-isogeny, a contradiction by Theorem 2.1.1. If $b \geq 1$, then by Lemma 6.0.3, E has a rational 3-isogeny so it has a rational 15-isogeny.

If we had $a \geq 1$, then E would have a rational point P_2 of order 2 (since E has a rational 2-isogeny). If $\langle P_{15} \rangle$ is the kernel of a rational 15-isogeny, where $P_{15} \in E(\overline{\mathbb{Q}})$ is a point of order 15, then $\langle P_2 + P_{15} \rangle$ is the kernel of rational 30-isogeny, a contradiction by Theorem 2.1.1.

Now we show that $E(K)$ cannot contain a point P_{45} of order 45. Assume the contrary, that $P_{45} \in E(K)$. If $P_9 \in E(K)$ is a point of order 9, then by Lemma 6.0.4 we have $[\mathbb{Q}(P_9) : \mathbb{Q}] \in \{1,2\}$. It follows that $C_9 \subseteq E(F)[9]$. By Theorem 2.1.3 we see that we have an equality. Since $F/\mathbb{Q}$ is Galois extension and $E(F)[9] \cong C_9$, E has a rational 9-isogeny. Since E has a rational 5-isogeny, it has a rational 45-isogeny, which contradicts the Theorem 2.1.1. We conclude that if $b \geq 1$, then $a = 0$ and $b = 1$.

It remains to consider the case when $a \geq 2$. Assume that E has full 2-torsion defined over $\mathbb{Q}$. Let $\{P_2, Q_2\}$ be a basis for $E[2]$ and $P_5 \in E(\overline{\mathbb{Q}})$ a point of order 5 such that the group $\langle P_5 \rangle$ is the kernel of a rational 5-isogeny. The groups $\langle P_2 + P_5 \rangle$ and $\langle Q_2 \rangle$ are kernels of two independent rational 10 and 2-isogenies. By using Lemma 2.1.2 we conclude that E is isogenous over $\mathbb{Q}$ to an elliptic curve $E''/\mathbb{Q}$ with a rational 20-isogeny, which contradicts Theorem 2.1.1. Therefore we conclude that E has only one rational point of order 2, since $G_E(2)$ must be equal to 2B. Assume that $P_4 \in E(K)$ is a point of order 4. The previous discussion shows that we have $P_4 \in E(F)$. By the results of [47] we see that

an elliptic curve with a point of order 4 defined over a quadratic extension of $\mathbb{Q}$ and with only one rational point of order 2 has a rational 4-isogeny. It follows that E has a rational 20-isogeny, a contradiction with the Theorem 2.1.1. We conclude that if $c = 1$ and $a \geq 1$, then we must have $a = 1$.

Now we will deal with the groups of the form $C_m \oplus C_{mn}$. Assume that $C_m \oplus C_{mn} \subseteq E(K)$. Then $E(K)$ contains a point P_m of order m. Previous discussion shows that $m = 2^a 3^b 5^c 7^d 11^e 13^f$. If $r \in \{5, 13\}$ is a prime divisor of m, then $C_r \oplus C_r \subseteq E(K)$. By Corollary 3.1.3 it follows that $\mathbb{Q}(\zeta_r) \subseteq K$. We also have that $\phi(r) = [\mathbb{Q}(\zeta_r) : \mathbb{Q}]$ is divisible by 4 and it divides $[K : \mathbb{Q}] = 2p$, a contradiction. By the analogous reasoning we see that if $r = 7$ then $[K : \mathbb{Q}] = 2p$ would have to be divisible by $\phi(7) = 6$, which is also impossible. Consider the case when $r = 11$. We have $\mathbb{Q}(\zeta_{11}) \subseteq K$. Therefore $[\mathbb{Q}(\zeta_{11}) : \mathbb{Q}] = \phi(11) = 10$ divides $2p = [K : \mathbb{Q}]$. It follows that $K = \mathbb{Q}(\zeta_{11})$ and $\mathbb{Q}(E[11]) \subseteq K$. By the main result of [38] we see that $\mathbb{Q}(E[11]) \supsetneq \mathbb{Q}(\zeta_{11})$, a contradiction. Finally, we look at the remaining case when $m = 2^a 3^b$. As before, we conclude that $\phi(m)$ divides $2p$. It follows that $m \in \{2, 3, 4, 6\}$.

Assume that $C_2 \oplus C_{2n} \subseteq E(K)$. Then we obviously have $C_{2n} \subseteq E(K)$. By what we have just proven, we have $C_{2n} \in \Phi_{\mathbb{Q}}(2) \cup \Phi_{\mathbb{Q}}(p)$. It follows that $2n \in \{2, 4, 6, 8, 10, 12, 16\}$. We need to show that it is not possible to have $n = 8$, since all the other possibilities already occur in $\Phi_{\mathbb{Q}}(2)$. By [17, Corollary 3.5], we get that if $T \cong C_2 \oplus C_{16}$ then $[\mathbb{Q}(T) : \mathbb{Q}]$ must be divisible by 4, which is impossible since $\mathbb{Q}(T) \subseteq K$.

Assume that $C_3 \oplus C_{3n} \subseteq E(K)$. As in the previous paragraph, we conclude that $C_{3n} \in \Phi_{\mathbb{Q}}(2) \cup \Phi_{\mathbb{Q}}(p)$ and that $3n \in \{3, 6, 9, 12, 15\}$. We need to eliminate the cases when $n \in \{3, 4, 5\}$. By Corollary 3.1.3 we see that $\mathbb{Q}(\zeta_3) \subseteq K$. Obviously $|G_E(3)| = [\mathbb{Q}(E[3]) : \mathbb{Q}]$ has to divide $[K : \mathbb{Q}] = 2p$. By Lemma 6.0.3 we have that $G_E(3) \subseteq 3\text{B}$. From Table 6.1 we see that $|G_E(3)| \in \{2, 4, 6, 12\}$. The only possibility is $|G_E(3)| = 2$, so we have $G_E(3) = 3\text{Cs}.1.1$, which means that $C_3 \oplus C_3 \cong E(\mathbb{Q}(\zeta_3))[3]$. If $n = 3$, then by Proposition 2.1.8 we see that $E(\mathbb{Q}(\zeta_3))[9] \cong C_3 \oplus C_9$, which is impossible by Theorem 2.1.3. If $n = 4$, then by Lemma 6.0.4 we see that $C_4 \subseteq E(\mathbb{Q}(\zeta_3))[4]$ and we conclude that $C_3 \oplus C_{12} \subseteq E(\mathbb{Q}(\zeta_3))$, which contradicts Theorem 2.1.3. Finally, assume that $n = 5$. By Lemma 6.0.3, E has a rational 5-isogeny. Since E has two independent rational 3-isogenies, by using Lemma 2.1.2 we conclude that E is isogenous over $\mathbb{Q}$ to an elliptic curve $E''/\mathbb{Q}$ with a rational

45-isogeny, which contradicts Theorem 2.1.1.

Assume that $C_4 \oplus C_{4n}$. By Corollary 3.1.3. we see that $\mathbb{Q}(i) \subseteq K$. As before, we conclude that $4n \in \{4,8,12,16\}$. We need to show that we must have $n = 1$. If $n = 4$, this is already shown to be impossible because $E(K)$ cannot contain a subgroup isomorphic to $C_2 \oplus C_{16}$. If $n = 3$, then by Lemma 6.0.4 we have $C_4 \oplus C_4 \subseteq E(\mathbb{Q}(i))[4]$ and $C_3 \subseteq E(\mathbb{Q}(i))[3]$. We conclude that $C_4 \oplus C_{12} \subseteq E(\mathbb{Q}(i))$, which is impossible by Theorem 2.1.3. Finally, assume that $n = 2$. By [17, Corollary 3.5], we get that if $T \cong C_4 \oplus C_8$ then $[\mathbb{Q}(T) : \mathbb{Q}]$ must be divisible by 4, which is impossible since $\mathbb{Q}(T) \subseteq K$.

If $C_6 \oplus C_6 \subseteq E(K)$, then by Corollary 3.1.3 we have $\mathbb{Q}(\zeta_3) \subseteq K$ and $G_E(3) = 3\text{Cs}.1.1$. By Lemma 6.0.3 we see that E has a rational 2-isogeny. Therefore $G_E(2) \subseteq 2\text{B}$. Since $|2\text{B}| = 2$, we have $|G_E(2)| = [\mathbb{Q}(E[2]) : \mathbb{Q}] \leq 2$. Since $\mathbb{Q}(\zeta_3)$ is a unique quadratic extension contained in K it follows that $E(K)[2] = E(\mathbb{Q}(\zeta_3))[2]$. We conclude that $C_6 \oplus C_6 \subseteq E(\mathbb{Q}(\zeta_3))$, which is impossible by Theorem 2.1.3. ■

6.1. Elliptic curves with CM

In this section we will consider elliptic curves with CM. The theory of Galois representations of CM elliptic curves is well understood, so the results we list here follow easily from the previously known results.

Lemma 6.1.1. Let K be a number field such that $[K : \mathbb{Q}] = pq$, where p and q are prime numbers such that $pq \notin \{4,6\}$ and let E/K be an elliptic curve with CM. If $r \in \{5,13,163\}$, then $E(K)$ cannot contain a point of order r.
For a prime $r \in \{2,3,7,11,19,43,67\}$ and a positive integer k, we have the following possibilities for $[\mathbb{Q}(P_{r^k}) : \mathbb{Q}]$, where $P_{r^k} \in E(K)$ is a point of order r^k.

- $[\mathbb{Q}(P_{2^k}) : \mathbb{Q}] \in \{1,2,3\}$, $[\mathbb{Q}(P_{3^k}) : \mathbb{Q}] \in \{1,2,3\}$, $[\mathbb{Q}(P_{7^k}) : \mathbb{Q}] \in \{3,21\}$,
- $[\mathbb{Q}(P_{11^k}) : \mathbb{Q}] \in \{5,10\}$, $[\mathbb{Q}(P_{19^k}) : \mathbb{Q}] \in \{9\}$, $[\mathbb{Q}(P_{43^k}) : \mathbb{Q}] \in \{21\}$,
- $[\mathbb{Q}(P_{67^k}) : \mathbb{Q}] \in \{33\}$.

Additionally, we have the following:

- If $P_7 \in E(K)$ and $[K:\mathbb{Q}] = 21$, then $E(K)_{tors} \cong C_{14}$,
- If $P_{11} \in E(K)$ and $[K:\mathbb{Q}] = 10$, then $E(K)_{tors} \in \{C_{11}, C_{22}, C_2 \oplus C_{22}\}$,
- If $P_{19} \in E(K)$, then $[K:\mathbb{Q}] = 9$ and $E(K)_{tors} \cong C_{19}$,
- If $P_{43} \in E(K)$, then $[K:\mathbb{Q}] = 21$ and $E(K)_{tors} \cong C_{43}$,
- If $P_{67} \in E(K)$, then $[K:\mathbb{Q}] = 33$ and $E(K)_{tors} \cong C_{67}$.

Proof. The first statements follow from [19, Theorem 3.6., Theorem 5.6.] and Proposition 2.1.8. The approach is the same as the proof of Lemma 6.0.4. Since we know the possible values for $[\mathbb{Q}(P_r):\mathbb{Q}]$, applying Proposition 2.1.8 and keeping in mind that $[\mathbb{Q}(P_{r^k}):\mathbb{Q}]$ divides $pq = [K:\mathbb{Q}]$, the proof of our claims follows by an easy calculation. The last statements follow directly from [5, Chapter 7] and [9, Chapter 4.]. Authors of the first cited paper have classified possible values of $\Phi_{CM}(d)$, for $d \leq 99$ and d odd. The set $\Phi_{CM}(10)$ was determined in the second cited paper. ■

In the previous lemma we have shown what the torsion group of $E(K)$ looks like if there exists a prime $r \geq 13$ that divides $|E(K)_{tors}|$. Therefore it remains to consider the case when the prime divisors of $|E(K)_{tors}|$ are contained in $\{2,3,7,11\}$.

Lemma 6.1.2. Let K be a number field such that $[K:\mathbb{Q}] = pq$, where p and q are prime numbers such that $pq \notin \{4,6,9\}$ and let E/K be an elliptic curve with CM. Then $E(K)_{tors} \in \Phi_{\mathbb{Q}}(p) \cup \Phi_{\mathbb{Q}}(q)$ unless $pq \in \{15,21,33\}$. If $pq = 15$, then $E(K)_{tors} \in \Phi_{\mathbb{Q}}(3) \cup \Phi_{\mathbb{Q}}(5) \cup \{C_{22}\}$. If $pq = 21$, then $E(K)_{tors} \in \Phi_{\mathbb{Q}}(3) \cup \Phi_{\mathbb{Q}}(7) \cup \{C_{43}\}$. If $pq = 33$, then $E(K)_{tors} \in \Phi_{\mathbb{Q}}(3) \cup \Phi_{\mathbb{Q}}(11) \cup \{C_{67}\}$.

Proof. Assume that $E(K)$ contains a point P_r of order $r \in \{2,3,7,11\}$. By [19, Theorem 3.6] and [19, Theorem 5.6] we see that if $r \in \{3,7,11\}$, then $[\mathbb{Q}(P_r):\mathbb{Q}]$ is divisible by 4 or E has a rational r-isogeny. Since $[K:\mathbb{Q}]$ is not divisible by 4, we conclude that E has a rational r-isogeny. When $r = 2$ we have that E has a rational 2-isogeny or $G_E(2) = \mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z})$.

Assume that $P_{11} \in E(K)$ is a point of order 11. It follows that E has a rational 11-isogeny and by [34, Table 4] we have $j(E) = -2^{15}$. If $r \in \{2,3,7\}$ and $P_r \in E(K)$ is a point of order r, then E has a rational r-isogeny so it has a rational $11r$-isogeny (which is

impossible by Theorem 2.1.1) or $r = 2$ and $G_E(2) = \mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z})$ in which case we have $[\mathbb{Q}(P_2) : \mathbb{Q}] = 3$. Therefore $3 \mid [K : \mathbb{Q}]$. By the previous lemma we know that $5 \mid [\mathbb{Q}(P_{11}) : \mathbb{Q}]$. We conclude that $15 \mid [K : \mathbb{Q}]$ and so $[K : \mathbb{Q}] = 15$. By [18, Table 1] we already know that $C_{22} \in \Phi_{\mathbb{Q}}(15)$ and by [5, Chapter 7] we can see that if $[K : \mathbb{Q}] = 15$ and E/K is an elliptic curve with CM such that $C_{11} \subseteq E(K)$, then $E(K)_{tors} \cong C_{11}, C_{22}$. It remains to show that $E(K)$ cannot contain a point of order 121. Assume that $P_{121} \in E(K)$ is a point of order 121. By the previous lemma, we have $[\mathbb{Q}(P_{121}) : \mathbb{Q}] \leq 10$, but this is impossible by Lemma 4.1.3.

By the previous lemma we see that if $P_{49} \in E(K)$, then $[\mathbb{Q}(P_{49}) : \mathbb{Q}] \leq 21$ and this is impossible by Lemma 4.1.3. Again by the previous lemma we see that if $P_7 \in E(K)$ is a point of order 7 and $[\mathbb{Q}(P_7) : \mathbb{Q}] = 21$, then $E(K)_{tors} \cong C_{14}$. The group C_{14} is contained in $\Phi_{\mathbb{Q}}(3) \subseteq \Phi_{\mathbb{Q}}(21)$ by Theorem 2.1.4. From now on, if $P_7 \in E(K)$ is a point of order 7, then assume that $[\mathbb{Q}(P_7) : \mathbb{Q}] = 3$ (by the previous lemma, this is the only possibility for $[\mathbb{Q}(P_7) : \mathbb{Q}]$ except $[\mathbb{Q}(P_7) : \mathbb{Q}] = 21$). Assume that $n = 2^a 3^b 7^c$ and $P_n \in E(K)$ is a point of order n. By the previous lemma, we see that we have $[\mathbb{Q}(P_n) : \mathbb{Q}] = 2^k 3^l$, for some nonnegative integers k, l. Since $[\mathbb{Q}(P_n) : \mathbb{Q}]$ divides $[K : \mathbb{Q}] = pq$ and $pq \notin \{4, 6, 9\}$ we get $[\mathbb{Q}(P_n) : \mathbb{Q}] \in \{2, 3\}$. By the results of [9], Theorem 2.1.3 and Theorem 2.1.4 we see that $\Phi_{CM}(d) \subseteq \Phi_{\mathbb{Q}}(d)$ for $d = 2, 3$.

It remains to show that for $r \in \{43, 67\}$ there exists an elliptic curve $E/\mathbb{Q}$ with CM and a number field K of degree $\frac{r-1}{2}$ such that $E(K)_{tors} \cong C_r$. This is a direct consequence of [4, Theorem 5.6.] ■

This concludes the proof of the Theorem 6.0.1 when $pq \neq 9$. The case $pq = 9$ will be sorted out in the next section.

6.2. THE SET $\Phi_{\mathbb{Q}}(9)$

Throughout this section K will denote a number field such that $[K:\mathbb{Q}]=9$. We remind the reader that the set S of prime factors dividing $E(K)_{tors}$ satisfies $S \subseteq \{2,3,5,7,11,13,19\}$.

The main result we prove in this section is the following theorem.

Theorem 6.2.1. Let $E/\mathbb{Q}$ be an elliptic curve. Then

$$E(K)_{tors} \cong \begin{cases} C_m, & m = 1,...,10,12,13,14,18,19,21,26,27,28,36,42 \\ C_2 \oplus C_{2m}, & m = 1,...,4,7,9. \end{cases}$$

We note that the above theorem is equivalent to the following

$$\Phi_{\mathbb{Q}}(9) = \Phi_{\mathbb{Q}}(3) \cup \{C_{19}, C_{26}, C_{27}, C_{28}, C_{36}, C_{42}, C_2 \oplus C_{18}\}.$$

We shall first address the CM case. This has been proven by Clark, Corn, Rice and Stankewicz in [9].

Theorem 6.2.2 ([9, Chapter 4])**.** Let E/K be an elliptic curve with CM. Then

$$E(K)_{tors} \cong \begin{cases} C_m, & m = 1,2,3,4,6,9,14,18,19,27 \\ C_2 \oplus C_2. \end{cases}$$

Lemma 6.2.3. Let $E/\mathbb{Q}$ be an elliptic curve such that $C_{19} \subseteq E(K)_{tors}$. Then E has CM and $E(K)_{tors} \cong C_{19}$.

Proof. Since $C_{19} \subseteq E(K)_{tors}$, by Theorem 2.1.7 we have that E has CM. The second claim follows from the previous theorem. ∎

Since $\Phi_{CM}(9) \cap \Phi_{\mathbb{Q}}(9)$ is contained in the set

$$\Phi_{\mathbb{Q}}(3) \cup \{C_{19}, C_{26}, C_{27}, C_{28}, C_{36}, C_{42}, C_2 \oplus C_{18}\},$$

we only need to consider elliptic curves without CM.

Lemma 6.2.4. Let $E/\mathbb{Q}$ be an elliptic curve without CM such that $C_{13n} \subseteq E(K)$. Then $n \in \{1,2\}$.

Proof. By Lemma 4.1.3, we have that $E(K)$ cannot contain a point of order 169.

Assume that $P_r \in E(K)$, where $r \in \{3,5,7\}$. Then E has a rational r-isogeny by Lemma 6.0.3, so it has a rational $13r$-isogeny , which is impossible by Theorem 2.1.1.

Assume that $P_4 \in E(K)$. From Lemma 6.0.4 we see that we must have $[\mathbb{Q}(P_{13}) : \mathbb{Q}] = 3$ and $[\mathbb{Q}(P_4) : \mathbb{Q}] \in \{1,3\}$. If $[\mathbb{Q}(P_4) : \mathbb{Q}] = 1$, then E attains a point of order 52 over a cubic field which contradicts Theorem 2.1.4. Therefore we have $[\mathbb{Q}(P_4) : \mathbb{Q}] = 3$. By Lemma 6.0.5 we have $G_E(4) = X_{20b}$ and $\mathbb{Q}(E[4])$ is a S_3-extension of $\mathbb{Q}$. From Table 6.1 we see that $G_E(13) = 13\text{B}.3.1$. We have that $\mathbb{Q}(P_{13})$ is a cubic Galois extension of $\mathbb{Q}$ by [34, Theorem 9.3]. The intersection $\mathbb{Q}(E[4]) \cap \mathbb{Q}(P_{13})$ is trivial because otherwise we would have $\mathbb{Q}(P_{13}) \subset \mathbb{Q}(E[4])$, but $\mathbb{Q}(E[4])$ does not contain a Galois cubic subextension. Therefore we have $\text{Gal}(\mathbb{Q}(E[4])\mathbb{Q}(P_{13})/\mathbb{Q}) \cong S_3 \times C_3$, making it of generalized S_3-type. We have $C_4 \oplus C_{52} \subseteq E(\mathbb{Q}(E[4])\mathbb{Q}(P_{13}))_{tors}$, but this is impossible by [12, Theorem 1.8].

■

Lemma 6.2.5. Let $E/\mathbb{Q}$ be an elliptic curve without CM such that $C_{7n} \subseteq E(K)$. Then $n \in \{1,2,3,4,6\}$.

Proof. By Lemma 4.1.3, we have that $E(K)$ cannot contain a point of order 49. Additionally, by Lemma 6.0.3 we see that E has a rational 7-isogeny or the LMFDB label of E is 2450.y1 or 2450.z1. If E has a label 2450.y1 or 2450.z1 and $C_7 \subseteq E(K)$, then $E(K)_{tors} \cong C_7$. This can be seen on the LMFDB pages of these curves.

Assume that $r \in \{3,5\}$ and $P_r \in E(K)$. Then E has a rational r-isogeny by Lemma 6.0.3. If $r = 5$, then E would have a rational 35-isogeny, which is impossible by Theorem 2.1.1. If $r = 3$, then E has a rational 21-isogeny so

$$j(E) \in \{-3^2 \cdot 5^6/2^3, 3^3 \cdot 5^3/2, 3^3 \cdot 5^3 \cdot 101^3/2^{21}, -3^3 \cdot 5^3 \cdot 383^3/2^7\}$$

by [34, Table 4]. We need to check that a point of order $7 \cdot 3^2$ or $7 \cdot 4 \cdot 3$ cannot occur. This is done by the division polynomial method (code 7.17). It remains to eliminate a possibility for a point of order 56. By the results of [47] (code 7.11), we see that if $P_{2^k} \in E(K)$ is a point of order 2^k and $k \geq 3$ then $[\mathbb{Q}(P_{2^k}) : \mathbb{Q}] = 1$ so E has a rational 56-isogeny, which is impossible by Theorem 2.1.1.

■

Lemma 6.2.6. Let $E/\mathbb{Q}$ be an elliptic curve without CM such that $C_{5n} \subseteq E(K)$. Then $n \in \{1,2\}$.

Proof. By Lemma 6.0.4 we have $P_5 \in E(\mathbb{Q})$. If $5|n$, then $C_{25} \subseteq E(K)$. Using Lemma 6.0.4 we get that $P_{25} \in E(\mathbb{Q})$ which is impossible since $C_{25} \notin \Phi(1)$.

If $P_3 \in E(K)$, then by Lemma 6.0.4 we have $[\mathbb{Q}(P_3) : \mathbb{Q}] \in \{1,3\}$. Therefore, E attains a point of order 15 over a subfield F of K such that $[F : \mathbb{Q}] \in \{1,3\}$, which is a contradiction with Theorem 2.1.4.

If $P_4 \in E(K)$, then $[\mathbb{Q}(P_4) : \mathbb{Q}] \leq 3$ by Lemma 6.0.4, so $[\mathbb{Q}(P_4 + P_5) : \mathbb{Q}] \leq 3$, which contradicts Theorem 2.1.4. ■

Lemma 6.2.7. Let $E/\mathbb{Q}$ be an elliptic curve without CM. Then $E(K)$ cannot contain C_{16}, C_{24}, C_{54} or C_{81}.

Proof. $\boxed{C_{16}}$: By Lemma 6.2.5 we see that if $P_{16} \in E(K)$, then $[\mathbb{Q}(P_{16}) : \mathbb{Q}] = 1$, but this is impossible by Theorem 1.0.12.

$\boxed{C_{24}}$: It was demonstrated in the proof of Lemma 6.2.5 that if $P_8 \in E(K)$ is a point of order 8 then $[\mathbb{Q}(P_8) : \mathbb{Q}] = 1$, so E has a rational 8-isogeny. By Lemma 6.0.3 we see that E has a rational 3-isogeny. We conclude that E has a rational 24-isogeny, which is impossible by Theorem 2.1.1.

$\boxed{C_{54}}$: Let G be the 3-adic Galois representation of E. By Theorem 2.1.9, the modular curve X_G is of genus zero or G_{27} is contained in the 27Nn.

Assume that G_{27} is contained in 27Nn. Using Magma [3] (code 7.18), we first find all the possibilities for $G_E(54)$ by searching for admissible subgroups H of $\mathrm{GL}_2(\mathbb{Z}/54\mathbb{Z})$ such that H has a subgroup K of index 9 that fixes a non-zero vector of order 54 and such that the group $G_E(27) \equiv G_E(54) \pmod{27}$ is a conjugate subgroup of 27Nn. There are only four such groups H_1, H_2, H_3, H_4. For $i \in \{1,2,3\}$ we have that H_i is cyclic of order 18. The group H_4 is isomorphic to $C_2 \oplus C_{18}$. Since K is contained in $\mathbb{Q}(E[54])$ and $\mathbb{Q}(E[54])$ is abelian over $\mathbb{Q}$, it follows that K is abelian over $\mathbb{Q}$. It follows that $K \subset \mathbb{Q}^{ab}$, where $\mathbb{Q}^{ab}$ denotes the maximal abelian extension of $\mathbb{Q}$. We conclude that if $C_{54} \subseteq E(K)_{tors}$, then $C_{54} \subseteq E(\mathbb{Q}^{ab})_{tors}$, but this is impossible by [8, Theorem 1.2].

Now we deal with the case when X_G is of genus 0. The list of all possibilities for G such that $-I \in G$ can be found in [52, Table 1]. For each such group G, every subgroup

of index 2 that does not contain $-I$ is also of genus 0. Therefore we from now on we consider all the groups listed in [52, Table 1] along with their index 2 subgroups that do not contain $-I$. Denote by S the set of all such groups of genus 0. For each group T in S, we first lift T to a subgroup of $\mathrm{GL}_2(\mathbb{Z}/27\mathbb{Z})$ and compute the stabiliser subgroups of index 9 that fix a non-zero vector of order 27. It turns out that such a subgroup exists only when T is an index 2 subgroup of the group with label $9I^0-9c$ (label is taken from [52]). Furthermore we check that a curve with $G_E(27)\cong T$ must have a rational point of order 9 (Magma [3] code 7.19).

Assume that $C_2\subseteq E(K)_{tors}$. We want to prove that this leads to a contradiction. We split the proof in three cases.

If $G_E(2)\subseteq$ 2B, then $C_2\oplus C_{18}\subseteq E(\mathbb{Q}(E[2]))$, which contradicts the Theorem 2.1.3. If $G_E(2)\subseteq$ 2Cn, then $C_2\oplus C_{18}\subseteq E(\mathbb{Q}(E[2]))$, which contradicts the Theorem 2.1.4.

Finally, consider the case when $G_E(2)=\mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z})$. A Magma [3] search shows that there is only 1 possible subgroup H_1 of $\mathrm{GL}_2(\mathbb{Z}/54\mathbb{Z})$ such that $H_1\cong T \pmod 9$, $H_1\cong G_E(2) \pmod 2$, H_1 has a stabiliser subgroup of index 9 that fixes a non-zero vector of order 54, has surjective determinant and contains complex conjugation. Reducing H_1 modulo 6 we obtain the group $G_E(6)$. The field $\mathbb{Q}(E[6])$ contains quadratic extensions $\mathbb{Q}(\Delta)$ and $\mathbb{Q}(\zeta_3)$. A computation in Magma [3] shows that the group $G_E(6)$ has a unique subgroup of index 2. By the Galois theory, it follows that there is a unique quadratic field contained in $\mathbb{Q}(E[6])$. We conclude that $\mathbb{Q}(\Delta)=\mathbb{Q}(\zeta_3)$. Assume that the affine model of E is given by the equation

$$E:\ y^2=x^3+Ax+B,$$

where $A,B\in\mathbb{Q}$. Since $\mathbb{Q}(\Delta)=\mathbb{Q}(\sqrt{-3})$, we have that $\sqrt{4A^3+27B^2}=\alpha+\beta\sqrt{-3}$. As in the proof of Theorem 4.6.1, we conclude that $\alpha=0$. It follows that $4A^3+27B^2=-3\beta^2$. Since

$$j(E)=1728\frac{4A^3}{4A^3+27B^2}=1728\frac{-3\beta^2-27B^2}{-3\beta^2}=1728(1+9(B/\beta)^2).$$

If we put $u=B/\beta$ and $t=3u$, we get $j(E)=1728(t^2+1)$. On the other hand, since $G_E(9)$ is contained in the group with label $9I^0-9c$, by [52, Table 1] we have that $j(E)=\frac{s^3-6s^2+3s+1}{s^2-s}$, for some $s\in\mathbb{Q}\setminus\{0,1\}$. The equation

$$1728(t^2+1)=\frac{s^3-6s^2+3s+1}{s^2-s}$$

induces a genus 2 hyperelliptic curve C. In Magma [3], we compute its Jacobian $J(C)$ and see that it has rank 0 over $\mathbb{Q}$. Using the Chabauty method implemented in Magma [3] we conclude that it does not have an affine rational point (code 7.20). Therefore there does not exist an elliptic curve $E/\mathbb{Q}$ with a point of order 54 over K.

$\boxed{C_{81}}$: By Theorem 2.1.9 it follows that there are only finitely many possibilities for $G_E(81)$. For each such possibility H, one can calculate if H contains a stabiliser subgroup H_v such that $[H : H_v] = 9$, where $v \in (\mathbb{Z}/81\mathbb{Z})^2$ is of order 81. An existence of such a subgroup H_v would imply that E obtains a point P_{81} of order 81 over some number field of degree 9 over $\mathbb{Q}$. It turns out that this does not occur for any possible H. Therefore, $E(K)$ cannot contain a point of order 81. ■

Before considering the case of $C_2 \oplus C_{2n}$ torsion, let us briefly address an important fact. Assume that $C_2 \oplus C_{2n} \subseteq E(K)$. Since $C_2 \oplus C_2 \subseteq E(K)$, we have that $|G_E(2)|$ divides $[K : \mathbb{Q}] = 9$. Therefore we conclude that $G_E(2) \in \{2\text{Cs}, 2\text{Cn}\}$. We also note that by the results of [47] we see that if $C_2 \oplus C_4 \in E(K)$, then $C_2 \oplus C_4 \in E(\mathbb{Q})$ and E has two independent rational 2 and rational 4-isogenies.

Lemma 6.2.8. Let $E/\mathbb{Q}$ be an elliptic curve without CM. Then $E(K)$ cannot contain $C_2 \oplus C_{10}$, $C_2 \oplus C_{12}$, $C_2 \oplus C_{26}$, $C_2 \oplus C_{28}$ or $C_2 \oplus C_{42}$.

Proof. Assume that $C_2 \oplus C_2 \subseteq E(K)$. We split the proof in two cases depending on what $G_E(2)$ is.

Assume that $G_E(2)$ is trivial and $r \geq 3$ is a prime number such that $P_r \in E(K)$. Then E has a rational r-isogeny by Lemma 6.0.3. Applying Lemma 2.1.2, we obtain the elliptic curve $E''/\mathbb{Q}$ with a rational $4r$-isogeny, which is impossible by Theorem 2.1.1 unless $r = 3$. By Lemma 2.1.8 we have that if $P_4 \in E(K)$, then $P_4 \in E(\mathbb{Q})$. If this is the case, then E has a rational 4-isogeny. Assume that $C_2 \oplus C_{12} \in E(K)$. It follows that $C_2 \oplus C_4 \in E(\mathbb{Q})$ and E has a rational 3-isogeny. Applying Lemma 2.1.2, we obtain the elliptic curve $E''/\mathbb{Q}$ with a rational 24-isogeny, which is impossible by Theorem 2.1.1.

Let us now consider the case when $G_E(2) = 2Cn$. By Lemma 6.0.5 and Lemma 6.0.4 it follows that a point of order 4 on $E(\overline{\mathbb{Q}})$ cannot be defined over the cubic field $\mathbb{Q}(E[2])$ or over K. Therefore $E(K)[2^\infty] \cong C_2 \oplus C_2$. This eliminates the possibilities $C_2 \oplus C_{28}$ or $C_2 \oplus C_{12}$. By [55, Theorem 1.1] we have $j(E) = t^2 + 1728$, for some $t \in \mathbb{Q}$. For

$r \in \{5,13\}$, it has already been demonstrated in the proofs of Lemma 6.0.7 and Lemma 6.0.6 that there does not exist an elliptic curve $E/\mathbb{Q}$ with $G_E(2) = 2\text{Cn}$ and rational r-isogeny. Finally, consider the case when $C_2 \oplus C_{42} \in E(K)$. We know that E has a rational 3 and a rational 7-isogeny by Lemma 6.0.3, so E has a rational 21-isogeny and

$$j(E) \in \{-3^2 \cdot 5^6/2^3, 3^3 \cdot 5^3/2, 3^3 \cdot 5^3 \cdot 101^3/2^{21}, -3^3 \cdot 5^3 \cdot 383^3/2^7\}$$

by [34, Table 4]. It is easy to check that for each of the four possible values of $j(E)$, the equation $j(E) = t^2 + 1728$ does not have rational solutions. Therefore, this case is also impossible. ■

All the groups appearing in Theorem 6.2.1 have been proven to occur for some number field K of degree 9 and some elliptic curve $E/\mathbb{Q}$. This has been proven in [18] and can be seen from the Table 1 of the same paper. This concludes the proof of Theorem 6.2.1 and consequently the proof of Theorem 6.0.1.

6.2.1. Appendix: Images of Mod p Galois representations associated to elliptic curves over $\mathbb{Q}$

For each possible known subgroup $G_E(p) \subsetneq \mathrm{GL}_2(\mathbb{F}_p)$ where $E/\mathbb{Q}$ is a non-CM elliptic curve and p is a prime, Tables 6.1 and 6.2 list in the first and second column the corresponding labels in Sutherland and Zywina notations, and the following data:

- $d_v = [G_E(p) : G_E(p)_v] = |G_E(p).v|$ for $v \in \mathbb{F}_p^2$, $v \neq (0,0)$; equivalently, the degrees of the extensions $\mathbb{Q}(P)$ over $\mathbb{Q}$ for points $P \in E(\overline{\mathbb{Q}})$ of order p.
- $d = |G_E(p)|$; equivalently, the degree $\mathbb{Q}(E[p])$ over $\mathbb{Q}$.

Note that Tables 6.1 and 6.2 are partially extracted from Table 3 of [51]. The difference is that [51, Table 3] only lists the minimum of d_v, which is denoted by d_1 therein.

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

Table 6.1: 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 6.2: Known images $G_E(p) \neq \mathrm{GL}_2(\mathbb{F}_p)$, for $p = 13, 17$ or 37, for non-CM elliptic curves $E/\mathbb{Q}$.

7. MAGMA CODE USED IN THE PAPER

Some Magma [3] codes were taken from E. González-Jiménez's website.

Listing 7.1: Code used in Theorem 4.2.1

```
Z25:=Integers(25);
Z5:=Integers(5);
Sub25:=[H`subgroup: H in Subgroups(GL(2,Z25))];

// Let G be a subgroup of GL(2,Z/nZ) acts on the left: M*v (M in G)
// then we need to transpose to work in Magma
// (since Magma the subgroups of GL(2,Z/nZ) acts on the right: v*M (M in G)

G5B11:=sub<GL(2,Z5) | {[1,0,0,2],[1,0,1,1]}>; // Transpose the generators on Sutherland
G5Cs11:=sub<GL(2,Z5) | {[1,0,0,2]}>;
G5Cs13:=sub<GL(2,Z5)|{[3,0,0,4]}>;
G5Cs41:=sub<GL(2,Z5)|{[4,0,0,4],[1,0,0,2]}>;
G5B14:=sub<GL(2,Z5)|[[4,0,0,3],[1,0,1,1]]>;
G5B41:=sub<GL(2,Z5)|[[4,0,0,4],[1,0,1,1],[1,0,0,2]]>;

// Imm5B11 is the set of subgroups GG of GL(2,Z/25Z) (up to
// conjugacy) such that GG = G (mod 5), where G=5B.1.1
Im_rho:=G5B11;
Imm5B11:=[H : H in Sub25 | IsConjugate(GL(2,Z5),sub<GL(2,Z5) |
{GL(2,Z5)!m : m in Generators(H)}>,Im_rho)];

// Imm5Cs11 is the set of subgroups GG of GL(2,Z/25Z) (up to
//conjugacy) such that GG = G (mod 5), where G=5Cs.1.1
Im_rho:=G5Cs11;
Imm5Cs11:=[H : H in Sub25 | IsConjugate(GL(2,Z5),sub<GL(2,Z5) |
{GL(2,Z5)!m : m in Generators(H)}>,Im_rho)];
```

```
27
28  // Imm5Cs13 is the set of subgroups GG of GL(2,Z/25Z) (up to
29  //conjugacy) such that GG = G (mod 5), where G=5Cs.1.3
30  Im_rho:=G5Cs13;
31  Imm5Cs13:=[H : H in Sub25 | IsConjugate(GL(2,Z5),sub<GL(2,Z5) |
32  {GL(2,Z5)!m : m in Generators(H)}>,Im_rho)];
33
34  // Imm5Cs41 is the set of subgroups GG of GL(2,Z/25Z) (up to
35  //conjugacy) such that GG = G (mod 5), where G=5Cs.4.1
36  Im_rho:=G5Cs41;
37  Imm5Cs41:=[H : H in Sub25 | IsConjugate(GL(2,Z5),sub<GL(2,Z5) |
38  {GL(2,Z5)!m : m in Generators(H)}>,Im_rho)];
39
40  // Imm5B14 is the set of subgroups GG of GL(2,Z/25Z) (up to
41  //conjugacy) such that GG = G (mod 5), where G=5B.1.4
42  Im_rho:=G5B14;
43  Imm5B14:=[H : H in Sub25 | IsConjugate(GL(2,Z5),sub<GL(2,Z5) |
44  {GL(2,Z5)!m : m in Generators(H)}>,Im_rho)];
45
46  // Imm5B41 is the set of subgroups GG of GL(2,Z/25Z) (up to
47  //conjugacy) such that GG = G (mod 5), where G=5B.4.1
48  Im_rho:=G5B41;
49  Imm5B41:=[H : H in Sub25 | IsConjugate(GL(2,Z5),sub<GL(2,Z5) |
50  {GL(2,Z5)!m : m in Generators(H)}>,Im_rho)];
51
52  Imm:=Imm5B11;
53
54  G_25:={};
55  for GG in Imm do
56      V25:={ v : v in RSpace(GG) | not IsZero(v) and not
57      &and[IsDivisibleBy(Eltseq(v)[1],5),IsDivisibleBy(Eltseq(v)[2],5)] };
58      names:={GroupName(quo<GG | Core(GG,Stabiliser(GG,v))>) : v in
59      V25 | Integers()!(Order(GG)/Order(Stabiliser(GG,v))) eq 6};
60      G_25:=G_25 join names;
61  end for;
62  G_25;
63
```

```
Imm:=Imm5Cs11;

G_25:={};
for GG in Imm do
    V25:={ v : v in RSpace(GG) | not IsZero(v) and not
    &and[IsDivisibleBy(Eltseq(v)[1],5),IsDivisibleBy(Eltseq(v)[2],5)] };
    names:={GroupName(quo<GG | Core(GG,Stabiliser(GG,v))>) : v in
    V25 | Integers()!(Order(GG)/Order(Stabiliser(GG,v))) eq 6};
    G_25:=G_25 join names;
end for;
G_25;

Imm:=Imm5B41;

G_25:={};
for GG in Imm do
    V25:={ v : v in RSpace(GG) | not IsZero(v) and not
    &and[IsDivisibleBy(Eltseq(v)[1],5),IsDivisibleBy(Eltseq(v)[2],5)] };
    names:={GroupName(quo<GG | Core(GG,Stabiliser(GG,v))>) : v in
    V25 | Integers()!(Order(GG)/Order(Stabiliser(GG,v))) eq 6};
    G_25:=G_25 join names;
end for;
G_25;

Imm:=Imm5B14;

G_25:={};
for GG in Imm do
    V25:={ v : v in RSpace(GG) | not IsZero(v) and not
    &and[IsDivisibleBy(Eltseq(v)[1],5),IsDivisibleBy(Eltseq(v)[2],5)] };
    names:={GroupName(quo<GG | Core(GG,Stabiliser(GG,v))>) : v in
    V25 | Integers()!(Order(GG)/Order(Stabiliser(GG,v))) eq 6};
    G_25:=G_25 join names;
end for;
G_25;

Imm:=Imm5Cs41;
```

```
101
102 G_25:={};
103 for GG in Imm do
104     V25:={ v : v in RSpace(GG) | not IsZero(v) and not
105     &and[IsDivisibleBy(Eltseq(v)[1],5),IsDivisibleBy(Eltseq(v)[2],5)] };
106     names:={GroupName(quo<GG | Core(GG,Stabiliser(GG,v))>) : v in
107     V25 | Integers()!(Order(GG)/Order(Stabiliser(GG,v))) eq 6};
108     G_25:=G_25 join names;
109 end for;
110 G_25;
111
112 Imm:=Imm5Cs13;
113
114 G_25:={};
115 for GG in Imm do
116     V25:={ v : v in RSpace(GG) | not IsZero(v) and not
117     &and[IsDivisibleBy(Eltseq(v)[1],5),IsDivisibleBy(Eltseq(v)[2],5)] };
118     names:={GroupName(quo<GG | Core(GG,Stabiliser(GG,v))>) : v in
119     V25 | Integers()!(Order(GG)/Order(Stabiliser(GG,v))) eq 6};
120     G_25:=G_25 join names;
121 end for;
122 G_25;
```

Listing 7.2: Code used in Theorem 4.2.1

```
1  Z9:=Integers(9);
2  Z3:=Integers(3);
3  Sub9:=[H`subgroup: H in Subgroups(GL(2,Z9))];
4
5  B311:=sub<GL(2,Z3)|[1,0,0,2],[1,0,1,1]>;
6  B312:=sub<GL(2,Z3)|[2,0,0,1],[1,0,1,1]>;
7  Cs311:=sub<GL(2,Z3)|[1,0,0,2]>;
8  Cs3:=sub<GL(2,Z3)|[1,0,0,2],[2,0,0,2]>;
9  B3:=sub<GL(2,Z3)|[1,0,0,2],[2,0,0,2],[1,0,1,1]>;
10
11 ImmB311:=[H: H in Sub9 | IsConjugate(GL(2,Z3),sub<GL(2,Z3) |
12 {GL(2,Z3)!m : m in Generators(H)}>,B311)];
13 ImmB311:=[H: H in ImmB311 | #{Determinant(g): g in
```

```
sub<GL(2,Z9)|H,[8,0,0,8]>} eq 6];
#ImmB311; //No group is of order 6

ImmB312:=[H: H in Sub9 | IsConjugate(GL(2,Z3),sub<GL(2,Z3) |
{GL(2,Z3)!m : m in Generators(H)}>,B312)];
ImmB312:=[H: H in ImmB312 | #{Determinant(g): g in
sub<GL(2,Z9)|H,[8,0,0,8]>} eq 6];
#ImmB312; //No group is of order 6

ImmCs311:=[H: H in Sub9 | IsConjugate(GL(2,Z3),sub<GL(2,Z3) |
{GL(2,Z3)!m : m in Generators(H)}>,Cs311)];
ImmCs311:=[H: H in ImmCs311 | #{Determinant(g): g in
sub<GL(2,Z9)|H,[8,0,0,8]>} eq 6];
#ImmCs311; //No group is of order 6

ImmCs3:=[H: H in Sub9 | IsConjugate(GL(2,Z3),sub<GL(2,Z3) |
{GL(2,Z3)!m : m in Generators(H)}>,Cs3)];
ImmCs3:=[H: H in ImmCs3 | #{Determinant(g): g in
sub<GL(2,Z9)|H,[8,0,0,8]>} eq 6];
#ImmCs3;

ImmB3:=[H: H in Sub9 | IsConjugate(GL(2,Z3),sub<GL(2,Z3) |
{GL(2,Z3)!m : m in Generators(H)}>,B3)];
ImmB3:=[H: H in ImmB3 | #{Determinant(g): g in
sub<GL(2,Z9)|H,[8,0,0,8]>} eq 6];
#ImmB3;

G_9:={};
for GG in ImmB311 do
    V25:={ v : v in RSpace(GG) | not IsZero(v) and not
    &and[IsDivisibleBy(Eltseq(v)[1],3),IsDivisibleBy(Eltseq(v)[2],3)] };
    names:={GroupName(quo<GG | Core(GG,Stabiliser(GG,v))>) : v in
    V25 | Integers()!(Order(GG)/Order(Stabiliser(GG,v))) eq 6};
    G_9:=G_9 join names;
end for;
G_9;

```

```
G_9:={};
for GG in ImmB312 do
    V9:={ v : v in RSpace(GG) | not IsZero(v) and not
    &and[IsDivisibleBy(Eltseq(v)[1],3),IsDivisibleBy(Eltseq(v)[2],3)] };
    names:={GroupName(quo<GG | Core(GG,Stabiliser(GG,v))>) : v in
    V25 | Integers()!(Order(GG)/Order(Stabiliser(GG,v))) eq 6};
    G_9:=G_9 join names;
end for;
G_9;


G_9:={};
for GG in ImmCs311 do
    V9:={ v : v in RSpace(GG) | not IsZero(v) and not
    &and[IsDivisibleBy(Eltseq(v)[1],3),IsDivisibleBy(Eltseq(v)[2],3)] };
    names:={GroupName(quo<GG | Core(GG,Stabiliser(GG,v))>) : v in
    V9 | Integers()!(Order(GG)/Order(Stabiliser(GG,v))) eq 6};
    G_9:=G_9 join names;
end for;
G_9;


G_9:={};
for GG in ImmCs3 do
    V9:={ v : v in RSpace(GG) | not IsZero(v) and not
    &and[IsDivisibleBy(Eltseq(v)[1],3),IsDivisibleBy(Eltseq(v)[2],3)] };
    names:={GroupName(quo<GG | Core(GG,Stabiliser(GG,v))>) : v in
    V9 | Integers()!(Order(GG)/Order(Stabiliser(GG,v))) eq 6};
    G_9:=G_9 join names;
end for;
G_9;


G_9:={};
for GG in ImmB3 do
    V9:={ v : v in RSpace(GG) | not IsZero(v) and not
    &and[IsDivisibleBy(Eltseq(v)[1],3),IsDivisibleBy(Eltseq(v)[2],3)] };
```

```
    names:={GroupName(quo<GG | Core(GG,Stabiliser(GG,v))>) : v in
    V9 | Integers()!(Order(GG)/Order(Stabiliser(GG,v))) eq 6};
    G_9:=G_9 join names;
end for;
G_9;

//All the groups are of generalized S3-type. It follows that Q(P_9)<=Q(3^inf).


for rzb in RZB do
   T:=rzb[3];
   if T[1][2] eq 6 then
   rzb[1];
   end if;
end for;

//Output: X20,X20a. Hence, Q(P_4) is S3 extension of Q, so Q(P_4)<=Q(3^inf).
```

Listing 7.3: Code used in Lemma 4.2.1 and Theorem 5.3.2

```
//C63
//If E/Q has a rational 21-isogeny, then j(E)=a_i, for i<=4.
a1:=-3^2*5^6/2^3;
a2:=3^3*5^3/2^1;
a3:=3^3*5^3*101^3/2^(21);
a4:=-3^3*5^3*383^3/2^7;

list:=<a1,a2,a3,a4>;

//take a random elliptic curve with j(E)=a
for a in list do
E:=EllipticCurveWithjInvariant(a);

//computing primitive division polynomial g63.
g3:=DivisionPolynomial(E,3);
g7:=DivisionPolynomial(E,7);
f9:=DivisionPolynomial(E,9);
f21:=DivisionPolynomial(E,21);
```

```
19
20  Factorisation(f21: DegreeLimit:=14);
21  //This is needed for Theorem 5.3.2
22  //Irreducible factors that appear are of degrees 3, 6 or 9. Let n be any of these
23  //3 values. This means that there exista point P=(x,y) on E' of order 21 such
24  // that [Q(P):Q] is either n or 2n.
25  //But we also need to have that P is defined over L, a degree 14 number field.
26  //This implies that [Q(P):Q]<=2, which is impossible
27
28  g9:=f9 div g3; //this is the 9th primitive division polynomial
29
30  g21:=f21 div g7;
31  g21:=g21 div g3; //this is the 21st primitive division polynomial
32
33  f63:=DivisionPolynomial(E,63);
34
35  g63:=f63 div g21;
36  g63:=g63 div g9;
37  g63:=g63 div g7;
38  g63:=g63 div g3; //this is the 63rd primitive division polynomial
39
40  //g63 is a polynomial whose roots are x-coordinates of point of exact order 63 on E.
41  Factorisation(g63: DegreeLimit:=21);
42  end for;
43
44  //C42
45  //We do exactly the same as in the C63 case.
46
47  a1:=-3^2*5^6/2^3;
48  a2:=3^3*5^3/2^1;
49  a3:=3^3*5^3*101^3/2^(21);
50  a4:=-3^3*5^3*383^3/2^7;
51
52  list:=<a1,a2,a3,a4>;
53
54  for a in list do
55  E:=EllipticCurveWithjInvariant(a);
```

```
56
57 g2:=DivisionPolynomial(E,2);
58 g3:=DivisionPolynomial(E,3);
59 g7:=DivisionPolynomial(E,7);
60 f6:=DivisionPolynomial(E,6);
61 f21:=DivisionPolynomial(E,21);
62
63 g6:=f6 div g2;
64 g6:=g6 div g3;
65
66 g14:=f14 div g2;
67 g14:=g14 div g7;
68
69 g21:=f21 div g7;
70 g21:=g21 div g3;
71
72 f42:=DivisionPolynomial(E,42);
73
74 g42:=f42 div g21;
75 g42:=g42 div g14;
76 g42:=g42 div g7;
77 g42:=g42 div g6;
78 g42:=g42 div g3;
79 g42:=g42 div g2;
80
81 //Now g42 is a polynomial whose roots are x-coordinates of point of exact order 42 on E.
82 Factorisation(g42: DegreeLimit:=6);
83 end for;
```

Listing 7.4: Code used in Lemma 4.2.1 and Lemma 6.0.7

```
1 // If E/Q has a rational 15-isogeny, then j(E)=a_i, for i<=4.
2
3 a1:=-5^2/2;
4 a2:=-5^2*241^3/2^3;
5 a3:=-29^3*5/2^(5);
6 a4:=211^3*5/2^(15);
7
```

```
list:=<a1,a2,a3,a4>;

for a in list do
E:=EllipticCurveWithjInvariant(a);

g2:=DivisionPolynomial(E,2);
g3:=DivisionPolynomial(E,3);
g5:=DivisionPolynomial(E,5);

g6:=DivisionPolynomial(E,6);
g6:=g6 div g2;
g6:=g6 div g3;

g10:=DivisionPolynomial(E,10);
g10:=g10 div g2;
g10:=g10 div g5;

f9:=DivisionPolynomial(E,9);
f15:=DivisionPolynomial(E,15);

g9:=f9 div g3;

g15:=f15 div g5;
g15:=g15 div g3;

f45:=DivisionPolynomial(E,45);

g45:=f45 div g15;
g45:=f45 div g9;
g45:=f45 div g5;
g45:=f45 div g3;

//Now g45 is a polynomial whose roots are x-coordinates of point of exact order 45 on E.

Factorisation(g45: DegreeLimit:=6);

//The following line of code is used in Lemma 6.0.7., case [K:Q]=15.
```

```
45
46  Factorisation(g15: DegreeLimit:=15);
47
48  //Output shows that all irreducible factors of g15 of degree less then $15$ have
49  //even degrees. Hence E cannot have a point P_15 of order 15 defined over a number
50  //field of degree 15.
51
52  //The following line of code is used in Lemma 6.0.7., case [K:Q]=25.
53
54  Factorisation(g15: DegreeLimit:=25);
55
56  //Output shows that all irreducible factors of g15 of degree less then $25$ have
57  //even degrees. Hence E cannot have a point P_15 of order 15 defined over a number
58  //field of degree 25.
59  end for;
```

Listing 7.5: Code used in Theorem 4.3.1

```
1   P< x >:=PolynomialAlgebra(Rationals());
2
3   E:=EllipticCurve([1,1,1,-3,1]); //j-Invariant equals -121945/32
4
5   f2:=DivisionPolynomial(E,2);
6   f3:=DivisionPolynomial(E,3);
7   f5:=DivisionPolynomial(E,5);
8   f6:=DivisionPolynomial(E,6);
9   f10:=DivisionPolynomial(E,10);
10  f15:=DivisionPolynomial(E,15);
11  f30:=DivisionPolynomial(E,30);
12
13  g6:=f6 div f2;
14  g6:=g6 div f3;
15
16  g10:=f10 div f2;
17  g10:=g10 div f5;
18
19  g15:=f15 div f3;
20  g15:=g15 div f5;
```

```
21
22  g30:=f30 div f2;
23  g30:=g30 div f3;
24  g30:=g30 div f5;
25  g30:=g30 div g6;
26  g30:=g30 div g10;
27  g30:=g30 div g15; //g30 is now a primitive 30th division polynomial attached to E.
28
29  Factorisation(g30: DegreeLimit:=6);
30
31  //This outputs polynomials f and g defined below.
32
33  f:=x^6-40*x^5+45*x^4-120*x^3+75*x^2-25;
34  g:=x^6+10*x^5+25*x^4-20*x^3-25*x^2+50*x-25;
35
36  Order(GaloisGroup(f));
37  Order(GaloisGroup(g));
38  //Splitting fields of f and g are fields K1,K2 such that [K_1:Q]=[K_2:Q]=12.
39
40  E:=EllipticCurve([1,1,1,549,-2202]);
41  f2:=DivisionPolynomial(E,2);
42  f3:=DivisionPolynomial(E,3);
43  f5:=DivisionPolynomial(E,5);
44  f6:=DivisionPolynomial(E,6);
45  f10:=DivisionPolynomial(E,10);
46  f15:=DivisionPolynomial(E,15);
47  f30:=DivisionPolynomial(E,30);
48
49  g6:=f6 div f2;
50  g6:=g6 div f3;
51  g10:=f10 div f2;
52  g10:=g10 div f5;
53
54  g15:=f15 div f3;
55  g15:=g15 div f5;
56
57  g30:=f30 div f2;
```

```
g30:=g30 div f3;
g30:=g30 div f5;
g30:=g30 div g6;
g30:=g30 div g10;
g30:=g30 div g15;

Factorisation(g30: DegreeLimit:=6);
//Output: []
//In this case g_30 does not have any irreducible factors of degree less then or equal to 6.
```

Listing 7.6: Code used in Theorem 4.5.2

```
//X_(3B)xX_20
_<t>:=RationalFunctionField(Rationals());
f1:=27*(t+1)*(t+9)^3/t^3; //3B.1.1 or 3B.1.2
f2:=(t^2-3)^3*(-4*t^2+32*t+44)/(t+1)^4; //X_20
R<x,y>:=PolynomialRing(Rationals(),2);
C:=ProjectiveClosure(Curve(AffineSpace(R),Numerator(Evaluate(f1,x)-Evaluate(f2,y))));

bound:=10^3;
Pts := PointSearch(C,bound);
Pts:=[p : p in Pts | Multiplicity(p) eq 1];
assert #Pts ne 0;
Pt:=Pts[1];
E,mp1 := EllipticCurve(C,Pt);
CremonaReference(E);
EE,mm := MinimalModel(E);
mm:=mm^-1;
MW:=AbelianInvariants(MordellWeilGroup(EE));
//printf "Abelian Invariants of MW %o\n", MW;
DescentInformation(E);


T,mp2 := TorsionSubgroup(EE);
PtsC := { };
for p in T do
   PtsC := PtsC join RationalPoints(mm(mp2(p)) @@ mp1);
end for;
```

```
PtsC;
j:=f1;
{Evaluate(j,P[1]/P[3]) : P in PtsC | Evaluate(Denominator(j),P[1]) ne 0 and P[3] ne 0};

//Output: {-35937/4, 109503/64}


//But Q(E[2]) is contained in Q(E[3])), so j(E)=2^10*3^3*t^3*(1-4*t^3) for
// some rational number t and
// none of the two invariants listed above is of that form, which we now check.

P<t>:=PolynomialRing(Rationals());
f:=2^10*3^3*t^3*(1-4*t^3)-35937/4;
g:=2^10*3^3*t^3*(1-4*t^3)-109503/64;
Roots(f), Roots(g);
//Output gives us that no rational roots of these equation exist.


/////// X_(3Ns) x X_(20)
A<x,t>:=AffineSpace(Rationals(),2);
C:=Curve(A,x^3*(t+1)^4-(-4*t^2+32*t+44)*(t^2-3)^3);
D:=ProjectiveClosure(C);
R<x,y>:=PolynomialRing(Rationals(),2);
tr,x:=IsHyperelliptic(D);
x1,f:=SimplifiedModel(x);
f2:=Inverse(f);
x1;
J:=Jacobian(x1);
RankBound(J);

tr,g:=IsIsomorphic(D, x);
tr,g2:=IsInvertible(g);
g2:=Inverse(g);

pts:=Chabauty0(J);
for i:=1 to #pts do
g2(f2(pts[i]));
```

```
end for;
//////


//3Cs1.1 i 2Cn
_<t>:=RationalFunctionField(Rationals());
f1:=t^3; //3Cs.1.1
f2:=t^2+1728; //2Cn
R<x,y>:=PolynomialRing(Rationals(),2);
C:=ProjectiveClosure(Curve(AffineSpace(R),Numerator(Evaluate(f1,x)-Evaluate(f2,y))));

bound:=10^3;
Pts := PointSearch(C,bound);
Pts;
Pts:=[p : p in Pts | Multiplicity(p) eq 1];
assert #Pts ne 0;
Pt:=Pts[1];
E,mp1 := EllipticCurve(C,Pt);
CremonaReference(E);
EE,mm := MinimalModel(E);
mm:=mm^-1;
MW:=AbelianInvariants(MordellWeilGroup(EE));
//printf "Abelian Invariants of MW %o\n", MW;
DescentInformation(E);


T,mp2 := TorsionSubgroup(EE);
PtsC := { };
for p in T do
   PtsC := PtsC join RationalPoints(mm(mp2(p)) @@ mp1);
end for;
j:=f1;
{Evaluate(j,P[1]/P[3]) : P in PtsC | Evaluate(Denominator(j),P[1]) ne 0 and P[3] ne 0};
//Output: {1728}
```

Listing 7.7: Code used in Theorem 4.5.4

```
Z9:=Integers(9);
```

```
Z3:=Integers(3);
Sub9:=[H`subgroup: H in Subgroups(GL(2,Z9))];
Borel9:=sub<GL(2,Z9)|[1,1,0,1],[1,0,0,2],[8,0,0,8],[2,0,0,1]>;


B311:=sub<GL(2,Z3)|[1,0,0,2],[1,0,1,1]>;
B312:=sub<GL(2,Z3)|[2,0,0,1],[1,0,1,1]>;
Cs311:=sub<GL(2,Z3)|[1,0,0,2]>;

ImmB311:=[H: H in Sub9 | IsConjugate(GL(2,Z3),sub<GL(2,Z3) |
{GL(2,Z3)!m : m in Generators(H)}>,B311)];
ImmB311:=[H: H in ImmB311 | #{Determinant(g): g in sub<GL(2,Z9)|H,[8,0,0,8]>} eq 6];
ImmB311:=[H: H in ImmB311 | Order(H) le 6];
ImmB311;
//Output: []

ImmB312:=[H: H in Sub9 | IsConjugate(GL(2,Z3),sub<GL(2,Z3) |
{GL(2,Z3)!m : m in Generators(H)}>,B312)];
ImmB312:=[H: H in ImmB312 | #{Determinant(g): g in sub<GL(2,Z9)|H,[8,0,0,8]>} eq 6];
ImmB312:=[H: H in ImmB312 | Order(H) le 6];
ImmB312;
//Output: []

ImmCs311:=[H: H in Sub9 | IsConjugate(GL(2,Z3),sub<GL(2,Z3) |
{GL(2,Z3)!m : m in Generators(H)}>,Cs311)];
ImmCs311:=[H: H in ImmCs311 | #{Determinant(g): g in sub<GL(2,Z9)|H,[8,0,0,8]>} eq 6];
ImmCs311:=[H: H in ImmCs311| Order(H) le 6];
ImmCs311;
//Output: Three groups are given in the output,
//but they're all conjugate subgroups of Borel subgroup of
//GL(2,9). We check this.

for h in ImmCs311 do
   if IsConjugateSubgroup(GL(2,Z9),Borel9,h) eq false then
      h;
   end if;
end for;
```

```
39
40  //Previous loop outputs nothing, as expected.
```

Listing 7.8: Code used in Theorem 4.6.1 and Proposition 4.6.3

```
1   //E has a rational 9 isogeny and mod 2 Galois representation is surjective
2
3   E:=EllipticCurve([0,-27]);
4   E;
5   Q<x>:=PolynomialRing(Rationals());
6   K<w>:=NumberField(x^2+3);
7   E0:=BaseChange(E,K);
8   DescentInformation(E0);
9   //Torsion subgroup of E0 contains 12 points.
10  Points(E0:Bound:=30);
11  //This outputs 12 points on E0, so we've found them all.
12
13  //For each point (x,y) on E(K<w>), we have that if x is rational, then x is one
14  // of the values 0,3 or -6, which is impossible.
15
16
17  //E does not have a rational 9-isogeny and
18  //has a rational 3-isogeny and G_E(2)=2B
19
20  A<x,y>:=AffineSpace(Rationals(),2);
21  C:=Curve(A,(x+3)*(x^2-3*x+9)*(x^3+3)^3*y-256*(y+1)^3*x^3);
22  D:=ProjectiveClosure(C);
23  R<x,y>:=PolynomialRing(Rationals(),2);
24  tr,x:=IsHyperelliptic(D);
25  x1,f:=SimplifiedModel(x);
26  f2:=Inverse(f);
27  x1;
28  J:=Jacobian(x1);
29  RankBound(J);
30
31  tr,g:=IsIsomorphic(D, x);
32  tr,g2:=IsInvertible(g);
33  g2:=Inverse(g);
```

```
34
35  pts:=Chabauty0(J);
36  for i:=1 to #pts do
37  g2(f2(pts[i]));
38  end for;
39
40  //The only points on D for which xy=/=0 are (3,-16,1) and (-3,-1,1).
41  //Plugging in y=-16 and y=-1 in j(E)=256(y+1)^3/y we get that
42  // j(E)=54000 or j(E)=0. In both of these cases, E has CM.
43
44
45  _<t>:=RationalFunctionField(Rationals());
46  f1:=2^(10)*3^(3)*t^3*(1-4*t^3); //Q(E[2])<=Q(E[3])
47  f2:=(t+3)*(t^2-3*t+9)*(t^3+3)^3/t^3;
48  //E does not have a rational 9-isogeny, has a rational 3-isogeny
49  R<x,y>:=PolynomialRing(Rationals(),2);
50  C:=ProjectiveClosure(Curve(AffineSpace(R),Numerator(Evaluate(f1,x)-Evaluate(f2,y))));
51  Genus(C);
52  bound:=10^3;
53  Pts := PointSearch(C,bound);
54  Pts:=[p : p in Pts | Multiplicity(p) eq 1];
55  assert #Pts ne 0;
56  Pt:=Pts[1];
57  E,mp1 := EllipticCurve(C,Pt);
58  CremonaReference(E);
59  EE,mm := MinimalModel(E);
60  mm:=mm^-1;
61  MW:=AbelianInvariants(MordellWeilGroup(EE));
62  //printf "Abelian Invariants of MW %o\n", MW;
63  DescentInformation(E);
64
65
66  T,mp2 := TorsionSubgroup(EE);
67  PtsC := { };
68  for p in T do
69     PtsC := PtsC join RationalPoints(mm(mp2(p)) @@ mp1);
70  end for;
```

```
PtsC;
j:=f1;
{Evaluate(j,P[1]/P[3]) : P in PtsC | Evaluate(Denominator(j),P[1]) ne 0 and P[3] ne 0};

//Output: {0}. But since j(E)=0 implies that E has CM, we are done.
```

Listing 7.9: Code used in Remark 4.6.2

```
//A standard computation analogous to the one used in Lemma 6.2.7 (case C_54) shows
//that the following five j-maps correspond to elliptic curves E that
//obtain a point of order 9 over a sextic number field.

F<t> := FunctionField(Rationals());

//Level 9 maps
ja1 := 3*(t^3+9)/t^3;
ja2 := 3*t/(2*t^2-3*t+6);
jb1 := 3*(t^3+9*t^2-9*t-9)/(t^3-9*t^2-9*t+9);
jc1 := -6*(t^3-9*t)/(t^3+9*t^2-9*t-9);
jc2 := -(t^2+3)/(t^2+8*t+3);

J1 := [ja1,ja2,jb1,jc1,jc2];

//Level 2 map
j2 := t^3/(t+16);

A<x,y> := AffineSpace(Rationals(),2);
Curves := [ ProjectiveClosure( Curve(A, Numerator( Evaluate(js,x) - Evaluate(j2,y)
))) : js in J1 ];
```

Listing 7.10: Code used in Lemma 5.4.1

```
Q<x>:=PolynomialRing(Rationals());
K:=CyclotomicField(3);

E1:=EllipticCurve("50a1"); // j(E1)=-25/2
E2:=EllipticCurve("450b2"); // j(E2)=-5^2*241^3/2^3
E3:=EllipticCurve("50a3"); // j(E3)=-29^3*5/2^(5)
E4:=EllipticCurve("450b4"); // j(E4)=211^3*5/2^(15)
```

```
8
9  list:=<E1,E2,E3,E4>;
10
11 for E in list do
12 f3:=DivisionPolynomial(E,3);
13 f5:=DivisionPolynomial(E,5);
14 f15:=DivisionPolynomial(E,15);
15
16 f15:=f15 div f3;
17 f15:=f15 div f5; //f15 is primitive 15th division polynomial associated to E.
18
19 Factorization(f15: DegreeLimit:=10);
20 Factorization(f15,K);
21 end for;
22
23 //All irreducible factors of f15 remain irreducible over cyclotomic field K.
```

Listing 7.11: Code used in Lemma 6.0.5 and Lemma 6.2.5

```
1  load "2primary_Ss.txt";
2  //This is the 2adic data available at
3  //https://verso.mat.uam.es/~enrique.gonzalez.jimenez/research/tables/tors6/2primary_Ss.txt
4
5  for rzb in RZB do
6     T:=rzb[3];
7     if T[1][2] eq 3 then
8        rzb[1];
9     end if;
10 end for;
11
12 //The following code is used in Lemma 6.2.5. and shows that if a point of order 2^k defined
13 //over K must be defined over Q.
14
15 for rzb in RZB do
16    T:=rzb[3];
17    if T[1][3] eq 3 or T[1][3] eq 9 then
18       rzb[1];
19    end if;
```

```
end for;
```

Listing 7.12: Code used in Lemma 6.0.6

```
//Magma code used in Lemma 6.0.6.
//This magma code shows that the field Q(P_13) of degree 39 over Q
//contains a Galois subextension that is of degree 3 over Q.

G:=sub<GL(2,13)|[1,1,0,1],[3,0,0,9],[2,0,0,1]>; //G_{E}(13)=13B.3.2.
Borel1:=sub<GL(2,13)|[1,1,0,1],[1,0,0,2],[1,0,0,3],[1,0,0,5]>;
M:=[K`subgroup: K in Subgroups(G: IndexEqual:=39)];

N:=[H`subgroup: H in Subgroups(G: IndexEqual:=3)];
N:=[H: H in N | IsConjugateSubgroup(GL(2,13),H,M[2]) eq true];
#N;
//The output shows that there exists such a subfield.
//M[2] is the only group in M that fixes a non-zero vector of order 13.
//Therefore, M[2] is the group Gal(Q(E[13])/Q(P_13)), where
//P_13 is a point of order 13 on E defined over a number field of degree 39.


//Using division polynomial method, we take a random elliptic curve with
//j-invariant equal to -2^{15} and we compute its 44th primitive division polynomial
//f44. It does not have a factor of degree <= 15.

E:=EllipticCurveWithjInvariant(-2^15);

f11:=DivisionPolynomial(E,11);

f2:=DivisionPolynomial(E,2);
f4:=DivisionPolynomial(E,4) div f2; //Primitive 4th division polynomial of E

f22:=DivisionPolynomial(E,22) div f11;
f22:= f22 div f2; //Primitive 22nd division polynomial of E

f44:=DivisionPolynomial(E,44) div f22;
f44:=f44 div f11;
f44:= f44 div f4;
```

```
f44:= f44 div f2; //Primitive 44th division polynomial of E

Factorisation(f44: DegreeLimit:=15);

//Output: []

//We check what the rational points on the elliptic curve y^2=s^3+6s^2+13s are.

E:=EllipticCurve([0,6,0,13,0]);
DescentInformation(E);
```

Listing 7.13: Code used in Lemma 6.0.7

```
//We search for subgroups of GL(2,Z49) that reduce mod 7 to 7B.1.3 and
//are not subgroups (up to conjugation) of Borel subgroup of GL(2,Z49), have
//surjective determinant and a stabiliser subgroup of index 49.

Z49:=Integers(49);
Z7:=Integers(7);

Borel49:=sub<GL(2,Z49)|[1,1,0,1],[1,0,0,2],[1,0,0,3],[5,0,0,1]>;
Borel1:=sub<GL(2,Z49)|[1,1,0,1],[1,0,0,2],[1,0,0,3],[1,0,0,5]>;
G7B13:=sub<GL(2,Z7)|[3,0,0,1],[1,1,0,1]>;

Sub49:=[H`subgroup: H in Subgroups(GL(2,Z49)) | IsConjugate(GL(2,Z7), G7B13,
sub<GL(2,Z7)|{GL(2,Z7)!m: m in Generators(H`subgroup)}>) eq true and
IsConjugateSubgroup(GL(2,Z49),Borel49,H`subgroup) eq false and #{Determinant(h): h
in H`subgroup} eq 42];

//#Sub49 is equal to 1.

Subs:=[H`subgroup: H in Subgroups(Sub49[1]: IndexEqual:=49)];
for H in Subs do
    if IsConjugateSubgroup(GL(2,Z49),Borel1,H) eq true then
    H;
    end if;
end for;

```

```
//This shows that Sub49[1] does not have a stabiliser subgroup of index 49.
//Therefore the group Sub49[1] cannot correspond to an elliptic curve E/Q with
//a point of order 49 defined over a number field of degree 49.
```

Listing 7.14: Code used in Lemma 6.0.7

```
//We find all the rational points genus 2 curve with rank 1 over Q using Chabauty method
//implemented in Magma
//j-invariant of elliptic curve E/Q with 2-adic representation contained in the group
//parameterised by X_7 is of the form (32t-4)/t^4, for some non-zero rational number t.

A<x,y>:=AffineSpace(Rationals(),2);
C:=Curve(A,(32*x-4)*(y)-x^4*(y^2+13*y+49)*(y^2+5*y+1)^3);

tr,x, map:=IsHyperelliptic(ProjectiveClosure(C));
J:=Jacobian(x);
pts:=Points(J: Bound:=100);
gen:=pts[2];
pts:=Chabauty(gen);

for p in pts do
RationalPoints(p @@ map);
end for;

//We plug in the values t_1=16/479 and t_2=2/3 in (32t-4)/t^4 to obtain the following
//two values a1,a2.

a1:=-38575685889/16384;
a2:=351/4;

list:=<a1,a2>;

//take a random elliptic curve with j(E)=a
for a in list do
E:=EllipticCurveWithjInvariant(a);

g2:=DivisionPolynomial(E,2);
g4:=DivisionPolynomial(E,4) div g2;
```

```
33
34 g7:=DivisionPolynomial(E,7);
35 g14:=DivisionPolynomial(E,14) div g7;
36 g14:=g14 div g2;
37
38 g28:=DivisionPolynomial(E,28) div g14;
39 g28:=g28 div g7;
40 g28:=g28 div g4;
41 g28:=g28 div g2;
42
43 Factorisation(g28: DegreeLimit:=21);
44 end for;
45
46 //Output: All irreducible factors of g28 of degree less then or equal to 21 have degree
47 //divisible by 9. Therefore, elliptic curve E/Q with j(E)=a1 or j(E)=a2
48 // does not have a point of order 28 defined over a number field of degree 21.
```

Listing 7.15: Code used in Lemma 6.0.7

```
1 E:=EllipticCurve([0,22,0,125,0]);
2 DescentInformation(E);
```

Listing 7.16: Code used in Lemma 6.0.8

```
1 //We will show that E' has a rational 25-isogeny.
2
3 Z25:=Integers(25);
4 Z5:=Integers(5);
5 Sub25:=[H`subgroup: H in Subgroups(GL(2,Z25))];
6
7 Borel25:=sub<GL(2,Z25)|[1,1,0,1],[1,0,0,2],[24,0,0,24],[1,0,0,3],[7,0,0,1],[19,0,0,1]>;
8 //group of upper triang.matrices.
9 B0:=sub<GL(2,Z25)|[1,1,0,1],[1,0,0,2],[1,0,0,3]>;
10 //Subgroup of Borel25 such that each matrix in B0 has first column vector equal to [1,0]^T.
11
12 G5B11:=sub<GL(2,Z5) | {[1,0,0,2],[1,1,0,1]}>;
13 G5B12:=sub<GL(2,Z5) | {[2,0,0,1],[1,1,0,1]}>;
14 G5B14:=sub<GL(2,Z5) | {[4,0,0,3],[1,1,0,1]}>;
15 G5B13:=sub<GL(2,Z5) | {[3,0,0,4],[1,1,0,1]}>;
```

```
G5B41:=sub<GL(2,Z5) | {[4,0,0,4],[1,1,0,1],[1,0,0,2]}>;
G5B42:=sub<GL(2,Z5) | {[4,0,0,4],[2,0,0,1],[1,1,0,1]}>;
G5B:=sub<GL(2,Z5) | {[2,0,0,3],[1,0,0,2],[1,1,0,1]}>;

//We first find all possibilities for G_E(25) such that E does not have a rational
//25-isogeny. Equivalently, G_E(25)
//is not conjugate subgroup to Borel25, a group of upper triangular matrices in GL(2,Z25).

// Imm5B11 is the set of subgroups GG of GL(2,Z/25Z)
//(up to conjugacy) such that GG = G (mod 5), where G=5B.1.1
Im_rho:=G5B11;
Imm5B11:=[H : H in Sub25 | IsConjugate(GL(2,Z5),sub<GL(2,Z5) |
{GL(2,Z5)!m : m in Generators(H)}>,Im_rho)];
Imm5B11:=[H : H in Imm5B11 | IsConjugateSubgroup(GL(2,Z25),Borel25,H) eq false];

// Imm5B12 is the set of subgroups GG of GL(2,Z/25Z) (up to
//conjugacy) such that GG = G (mod 5), where G=5B.1.2
Im_rho:=G5B12;
Imm5B12:=[H : H in Sub25 | IsConjugate(GL(2,Z5),sub<GL(2,Z5) |
{GL(2,Z5)!m : m in Generators(H)}>,Im_rho)];
Imm5B12:=[H : H in Imm5B12 | IsConjugateSubgroup(GL(2,Z25),Borel25,H) eq false];


// Imm5B14 is the set of subgroups GG of GL(2,Z/25Z) (up to
//conjugacy) such that GG = G (mod 5), where G=5B.1.4
Im_rho:=G5B14;
Imm5B14:=[H : H in Sub25 | IsConjugate(GL(2,Z5),sub<GL(2,Z5) |
{GL(2,Z5)!m : m in Generators(H)}>,Im_rho)];
Imm5B14:=[H : H in Imm5B14 | IsConjugateSubgroup(GL(2,Z25),Borel25,H) eq false];

// Imm5B13 is the set of subgroups GG of GL(2,Z/25Z) (up to
//conjugacy) such that GG = G (mod 5), where G=5B.1.3
Im_rho:=G5B13;
Imm5B13:=[H : H in Sub25 | IsConjugate(GL(2,Z5),sub<GL(2,Z5) |
{GL(2,Z5)!m : m in Generators(H)}>,Im_rho)];
Imm5B13:=[H : H in Imm5B13 | IsConjugateSubgroup(GL(2,Z25),Borel25,H) eq false];

```

```
53
54  // Imm5B41 is the set of subgroups GG of GL(2,Z/25Z) (up to
55  //conjugacy) such that GG = G (mod 5), where G=5B.4.1
56  Im_rho:=G5B41;
57  Imm5B41:=[H : H in Sub25 | IsConjugate(GL(2,Z5),sub<GL(2,Z5) |
58  {GL(2,Z5)!m : m in Generators(H)}>,Im_rho)];
59  Imm5B41:=[H : H in Imm5B41 | IsConjugateSubgroup(GL(2,Z25),Borel25,H) eq false];
60
61  // Imm5B42 is the set of subgroups GG of GL(2,Z/25Z) (up to
62  //conjugacy) such that GG = G (mod 5), where G=5B.4.2
63  Im_rho:=G5B42;
64  Imm5B42:=[H : H in Sub25 | IsConjugate(GL(2,Z5),sub<GL(2,Z5) |
65  {GL(2,Z5)!m : m in Generators(H)}>,Im_rho)];
66  Imm5B42:=[H : H in Imm5B42 | IsConjugateSubgroup(GL(2,Z25),Borel25,H) eq false];
67
68  // Imm5B is the set of subgroups GG of GL(2,Z/25Z) (up to
69  //conjugacy) such that GG = G (mod 5), where G=5B
70  Im_rho:=G5B;
71  Imm5B:=[H : H in Sub25 | IsConjugate(GL(2,Z5),sub<GL(2,Z5) |
72  {GL(2,Z5)!m : m in Generators(H)}>,Im_rho)];
73  Imm5B:=[H : H in Imm5B | IsConjugateSubgroup(GL(2,Z25),Borel25,H) eq false];
74
75
76  list:=<Imm5B11, Imm5B12, Imm5B14, Imm5B13, Imm5B41, Imm5B42, Imm5B>;
77
78  //for each possibility G of G_E'(25), we check if G has a
79  //subgroup of index 10 that is conjugate
80  //subgroup of B0. Equivalently, if E' has a point of order 25
81  //defined over degree 10 extension of Q.
82
83
84  for GG in list do
85     for G in GG do
86        M:=[s`subgroup: s in Subgroups(G: IndexEqual:=10)];
87        for m in M do
88           if IsConjugateSubgroup(GL(2,Z25),B0,m) eq true then
89              m;
```

```
        end if;
      end for;
   end for;
end for;

//The code outputs nothing, which means that there does not exist an elliptic curve E'/Q
//with a rational 5-isogeny such that
//E' does not have a rational 25-isogeny and a point of order 25 defined over
//a degree 10 extension of Q.
```

Listing 7.17: Code used in Lemma 6.0.8 and Lemma 6.2.5

```
// If E/Q has a rational 21-isogeny, then j(E)=a_i, for i<=4.
a1:=-3^2*5^6/2^3;
a2:=3^3*5^3/2^1;
a3:=3^3*5^3*101^3/2^(21);
a4:=-3^3*5^3*383^3/2^7;

list:=<a1,a2,a3,a4>;

//take a random elliptic curve with j(E)=a
for a in list do
E:=EllipticCurveWithjInvariant(a);

g2:=DivisionPolynomial(E,2);

g3:=DivisionPolynomial(E,3);

f4:=DivisionPolynomial(E,4);
g4:=f4 div g2; //4th primitive division polynomial

g6:=DivisionPolynomial(E,6) div g3;
g6:=g6 div g2; //6th primitive division polynomial

g7:=DivisionPolynomial(E,7);

f9:=DivisionPolynomial(E,9);
g9:=f9 div g3; //this is the 9th primitive division polynomial
```

```
27
28  f12:=DivisionPolynomial(E,12);
29  g12:=f12 div g6;
30  g12:=g12 div g4;
31  g12:=g12 div g3;
32  g12:=g12 div g2; //12th primitive division polynomial
33
34  f13:=DivisionPolynomial(E,13);
35
36  g14:=DivisionPolynomial(E,14) div g7;
37  g14:=g14 div g2; //14th primitive division polynomial
38
39  f21:=DivisionPolynomial(E,21);
40  g21:=f21 div g7;
41  g21:=g21 div g3; //21st primitive division polynomial
42
43  g28:=DivisionPolynomial(E,28);
44  g28:=g28 div g2;
45  g28:=g28 div g4;
46  g28:=g28 div g7;
47  g28:=g28 div g14; //28th primitive division polynomial
48
49  g42:=DivisionPolynomial(E,42);
50  g42:=g42 div g2;
51  g42:=g42 div g3;
52  g42:=g42 div g6;
53  g42:=g42 div g7;
54  g42:=g42 div g14;
55  g42:=g42 div g21; //42nd primitive division polynomial
56
57
58  f63:=DivisionPolynomial(E,63);
59  g63:=f63 div g21;
60  g63:=g63 div g9;
61  g63:=g63 div g7;
62  g63:=g63 div g3; //63rd primitive division polynomial
63
```

```
f84:=DivisionPolynomial(E,84);
g84:=f84 div g2;
g84:=g84 div g4;
g84:=g84 div g3;
g84:=g84 div g6;
g84:=g84 div g7;
g84:=g84 div g12;
g84:=g84 div g14;
g84:=g84 div g21;
g84:=g84 div g28;
g84:=g84 div g42; //84th primitive division polynomial

Factorisation(g21: DegreeLimit:=14);
Factorisation(g63: DegreeLimit:=9);
Factorisation(g84: DegreeLimit:=9);

end for;

//Output: The only irreducible factors of g21 of degree less then or equal to 14 have
//degree divisible by 3. Therefore such a curve E cannot have a point of order 21
//defined over a number field of degree 14.
//g63 and g84 do not have irreducible factors of degree less then or equal to 9.
```

Listing 7.18: Code used in Lemma 6.2.7

```
//We show that if G_{E}(27) is contained (up to conjugation) in 27Nn then G_{E}(27)
//has order 18 or 36 and is abelian.

load "gl2data3.txt";

Nn27 := newsublist[60][3];

function FixModule(H)
   V := Eigenspace(Identity(H),1);
   for h in Generators(H) do V:= V meet Eigenspace(Transpose(h),1); end for;
   // take transpose to work with right eigenspaces
   return ModuleInvariants(V);
end function;
```

```

function FullDeterminantMap(H)
    M,pi:=MultiplicativeGroup(BaseRing(H));
    return sub<M|[Inverse(pi)(Determinant(h)):h in Generators(H)]> eq M;
end function;

function ContainsComplexConjugation(H)
    return #[h:h in H|Determinant(h) eq -1 and Trace(h) eq 0 and
    ModuleContains(FixModule(sub<H|h>),[#BaseRing(H)])] gt 0;
end function;

Subgroups54:= [g`subgroup : g in Subgroups(GL(2,Integers(54))) |
ContainsComplexConjugation(g`subgroup) and FullDeterminantMap(g`subgroup) and
IsConjugateSubgroup(GL(2,Integers(27)),Nn27,sub<GL(2,Integers(27))|{GL(2,Integers(27))!m: m
in Generators(g`subgroup)}>) eq true];


for G in Subgroups54 do
   GT:=sub<GL(2,Integers(54))|{Transpose(m): m in Generators(G)}>;
   V54:={ v : v in RSpace(GT) | not IsZero(v) and not
   &and[IsDivisibleBy(Eltseq(v)[1],3),IsDivisibleBy(Eltseq(v)[2],3)] and not
   &and[IsDivisibleBy(Eltseq(v)[1],2),IsDivisibleBy(Eltseq(v)[2],2)]};

        names:={Integers()!(Order(GT)/Order(Stabiliser(GT,v))) : v in V54 |
        Integers()!(Order(GT)/Order(Stabiliser(GT,v))) eq 9 };
      if #names ne 0 then
      IsAbelian(G);
   end if;
end for;

//This shows that all possible groups G_{E}(54) are abelian.
```

Listing 7.19: Code used in Lemma 6.2.7

```
//This code is used when we consider X_G of genus 0.
GL54 := GL(2,Integers(54));
GL27 := GL(2,Integers(27));
GL9 := GL(2,Integers(9));
```

```
GL2 := GL(2,Integers(2));

//Compute the invariant factors of a finite Z/nZ-module of rank at most 2
function ModuleInvariants(V)
    if Dimension(V) eq 0 then return []; end if;
    if Dimension(V) eq 1 then return [#V]; end if;
    assert Dimension(V) le 2;
    r1:=#sub<V|V.1>; r2:=#sub<V|V.2>;
    return [GCD(r1,r2),LCM(r1,r2)];
end function;

//Given a subgroup of GL(2,Z/nZ), computes the invariants of the sub-module of Z/nZ x Z/nZ
//fixed by G (returns a list [], [a], or [a,b] with a|b|n)
function FixModule(H)
   V := Eigenspace(Identity(H),1);
   for h in Generators(H) do V:= V meet Eigenspace(Transpose(h),1); end for;
   return ModuleInvariants(V);
end function;

//Returns if the Z/nZ-module A contains a submodule isomorphic to B

function ModuleContains(A,B)
    i:=#A-#B;
    if i lt 0 then return false; end if;
    for j in [1..#B] do if not IsDivisibleBy(A[i+j],B[j]) then return false; end if; end for;
    return true;
end function;

//Returns true of a matrix group over a ring R contains elements of every possible
//determinant
function FullDeterminantMap(H)
    M,pi:=MultiplicativeGroup(BaseRing(H));
    return sub<M|[Inverse(pi)(Determinant(h)):h in Generators(H)]> eq M;
end function;

//Returns true if a give subgroup of GL(2,Z/nZ) contains an element corresponding to
//complex conjugation
```

```
function ContainsComplexConjugation(H)
    return #[h:h in H|Determinant(h) eq -1 and Trace(h) eq 0 and
    ModuleContains(FixModule(sub<H|h>),[#BaseRing(H)])] gt 0;
end function;

function ChangeLevel(G,n)
    I := BaseRing(G);
    if #I ge n then
    H := ChangeRing(G,Integers(n));
    end if;
    if not #I ge n then
    GL2n := GL(2,Integers(n));
    _,pi  := ChangeRing(GL(2,Integers(n)),I);
    H := sub<GL2n | Inverse(pi)(G),Kernel(pi) >;
    end if;
    return H;
end function;

//We transpose each group of genus 0 in order to find the Stabilisers

A3:=sub<GL(2,Integers(3))|[0,2,1,0],[1,1,1,2],[1,0,0,2]>;
B3:=sub<GL(2,Integers(3))|[0,2,1,1],[1,0,2,2]>;
C3:=sub<GL(2,Integers(3))|[0,2,1,0],[1,0,0,2]>;
D3:=sub<GL(2,Integers(3))|[2,0,0,2],[1,0,0,2]>;


A9:=sub<GL(2,Integers(9))|[0,4,2,0], [1,4,1,5],[1,0,0,2]>;
B9:=sub<GL(2,Integers(9))|[1,0,1,1],[2,0,0,5],[1,0,0,2]>;
C9:=sub<GL(2,Integers(9))|[2,0,0,5],[4,3,2,4],[1,0,0,2]>;
D9:=sub<GL(2,Integers(9))|[2,0,0,5],[1,3,3,1],[0,4,2,0],[1,0,0,2]>;

E9:=sub<GL(2,Integers(9))|[1,0,3,1],[2,1,1,1],[4,0,2,5]>;
F9:=sub<GL(2,Integers(9))|[0,4,2,1],[4,5,3,4],[4,0,5,5]>;
G9:=sub<GL(2,Integers(9))|[0,2,4,3],[5,1,1,4],[5,0,3,4]>;
H9:=sub<GL(2,Integers(9))|[1,0,3,1],[5,3,0,2],[1,2,0,2]>;

H9b:=sub<GL(2,Integers(9))|[1,0,3,1],[5,3,0,2],[2,0,1,1]>;
```

```
79  H9c:=sub<GL(2,Integers(9))|[1,0,3,1],[5,3,0,2],[4,0,2,5]>;
80
81  I9:=sub<GL(2,Integers(9))|[2,0,1,5],[1,3,2,2]>;
82  I9b:=sub<GL(2,Integers(9))|[2,0,1,5],[4,3,0,5]>;
83  I9c:=sub<GL(2,Integers(9))|[2,0,2,5],[2,3,2,1]>;
84
85  J9:=sub<GL(2,Integers(9))|[1,0,3,1],[2,3,2,8],[1,0,2,2]>;
86  J9b:=sub<GL(2,Integers(9))|[1,0,3,1],[2,3,2,8],[2,0,1,1]>;
87  J9c:=sub<GL(2,Integers(9))|[1,0,3,1],[5,3,2,5],[4,0,0,5]>;
88
89  A27:=sub<GL(2,Integers(27))|[1,0,1,1],[2,9,1,5],[1,3,2,2]>;
90
91  list:=<A3,B3,C3,D3,A9,B9,C9,D9,E9,F9,G9,H9,H9b,H9c,I9,I9b,I9c,J9,J9b,J9c,A27>;
92
93  //adding the index 2 subgroups of in the list
94  for H in list do
95     Indeks2 := [g`subgroup : g in Subgroups(H: IndexEqual:=2)];
96     for K in Indeks2 do
97        Append(~list,K);
98     end for;
99  end for;
100 liftlista:=<>;
101
102 //lifting each group in list to a subgroup of GL(2,Integers(27))
103 for i in [1..#list] do
104    Append(~liftlista,ChangeLevel(list[i],27));
105 end for;
106
107
108 JedinaGrupa:=<>;
109
110 //Checking which groups have a point of order 27 defined over a number field of degree 9
111 for i in [1..#liftlista] do
112    V27:={ v : v in RSpace(liftlista[i]) | not IsZero(v) and not
113    &and[IsDivisibleBy(Eltseq(v)[1],3),IsDivisibleBy(Eltseq(v)[2],3)] };
114         names:={Integers()!(Order(liftlista[i])/Order(Stabiliser(liftlista[i],v))) : v in V27
115         | Integers()!(Order(liftlista[i])/Order(Stabiliser(liftlista[i],v))) eq 9 };
```

```
     if #names ne 0 then
     Append(~JedinaGrupa,sub<GL9|{GL9!m: m in Generators(liftlista[i])}>);
   end if;
end for;


//Function that determines if an elliptic curve E/Q with G_{E}(54)=GG has a point of order 54
//defined over degree 9 number field
function ImaTockuReda54(GG)
    t:=0;
    V54:={ v : v in RSpace(GG) | not IsZero(v) and not
    &and[IsDivisibleBy(Eltseq(v)[1],3),IsDivisibleBy(Eltseq(v)[2],3)] and not
     &and[IsDivisibleBy(Eltseq(v)[1],2),IsDivisibleBy(Eltseq(v)[2],2)] };

    names:={Stabiliser(GG,v) : v in V54 | Integers()!(Order(GG)/Order(Stabiliser(GG,v))) eq 9
    };
    if #names ne 0 then
      t:=1;
    end if;
   return t;
end function;

//Searching through all possible subgroups of GL(2,Integers(54)) and finding the groups
//satisfying various conditions
AdmisIms := [g`subgroup : g in Subgroups(GL54) | ContainsComplexConjugation(g`subgroup) and
FullDeterminantMap(g`subgroup) and Order(sub<GL2|{GL2!m: m in Generators(g`subgroup)}>) eq 6
and IsConjugate(GL9,sub<GL9|{GL9!m: m in Generators(g`subgroup)}>,sub<GL9|{GL9!m: m in
Generators(JedinaGrupa[1])}>) eq true and ImaTockuReda54(g`subgroup) eq 1 and
IsConjugate(GL27,sub<GL27|{GL27!m: m in Generators(g`subgroup)}>,sub<GL27|{GL27!m: m in
Generators(JedinaGrupa[1])}>) eq true];

//This shows that G_{E}(6) is of order 18 and has a unique subgroup of index 2.
for G in AdmisIms do
   Order(sub<GL(2,Integers(6))|{GL(2,Integers(6))!m: m in Generators(G)}>);
   Subgroups(sub<GL(2,Integers(6))|{GL(2,Integers(6))!m: m in Generators(G)}>: IndexEqual:=2);
end for;
```

Listing 7.20: Code used in Lemma 6.2.7

```
//We classify all the rational points on the corresponding genus
//2 curve

A<x,y>:=AffineSpace(Rationals(),2);
C:=Curve(A,(y^2-y)*1728*(x^2+1)-(y^3-6*y^2+3*y+1));
tr,x, map:=IsHyperelliptic(ProjectiveClosure(C));
x1,f:=SimplifiedModel(x);
f2:=Inverse(f);
J:=Jacobian(x1);
RankBound(J);
pts:=Chabauty0(J);
for i:=1 to #pts do RationalPoints(pts[i] @@ map); end for;
```

CONCLUSION

In this paper we gave a complete classification of the set $\Phi_{j\in\mathbb{Q}}(p)$, where p is a prime number. More precisely, let K be a number field of prime degree p, and let E/K be an elliptic curve with $j(E) \in \mathbb{Q}$. Then:

1. If $p \geq 7$, then $E(K)_{tors} \in \Phi(1)$.

2. If $p = 3$ or $p = 5$, then $E(K)_{tors} \in \Phi_{\mathbb{Q}}(p)$.

3. If $p = 2$, then $E(K)_{tors} \in \Phi_{\mathbb{Q}}(2)$ or $E(K)_{tors} \cong \mathbb{Z}/13\mathbb{Z}$.

Let p and q be prime numbers. We succeeded in giving a complete classification of the sets $\Phi_{\mathbb{Q}}(pq)$, except in the case when $pq = 6$. The author was unable to eliminate the group $C_3 \oplus C_{18}$ from the set $\Phi_{\mathbb{Q}}(6)$, but has given a partial result for that case.
If K is a sextic number field and E/K is an elliptic curve, then $E(K)_{tors}$ is one of the following groups:

1. C_m, $m = 1, ..., 16, 18, 21, 30$, $m \neq 11$

2. $C_2 \oplus C_{2m}$, $m = 1, ..., 7, 9$

3. $C_3 \oplus C_{3m}$, $m = 1, ..., 4$

4. $C_4 \oplus C_{4m}$, $m = 1, 3$

5. $C_6 \oplus C_6$

6. $C_3 \oplus C_{18}$

Additionally, if $G_E(2) \neq 2B$, then $E(K)_{tors}$ is not isomorphic to $C_3 \oplus C_{18}$.

BIBLIOGRAPHY

[1] Balakrishnan, J. S., Dogra, N., Müller, J. S., Tuitman, J., and Vonk, J.: *Explicit Chabauty—Kim for the split Cartan modular curve of level* 13. Annals of Mathematics, 189:885–944, 2019. https://doi.org/10.4007/annals.2019.189.3.6. ↑ 19.

[2] Bilu, Y., Parent, P., and Rebolledo, M.: *Rational points on* $X_0^+(p^r)$. Ann. Inst. Fourier (Grenoble), 63:957–984, 2013. https://doi.org/10.5802/aif.2781. ↑ 19.

[3] Bosma, W., Cannon, J., and Playoust, C.: *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). ↑ iii, v, 15, 24, 25, 26, 29, 31, 32, 33, 44, 45, 56, 57, 58, 60, 61, 63, 70, 71, 72, 76.

[4] Bourdon, A., Clark, P. L., and Stankewicz, J.: *Torsion points on* CM *elliptic curves over real number fields*. Trans. Amer. Math. Soc., 12:8457–8496, 2017. https://doi.org/10.1090/tran/6905. ↑ 37, 67.

[5] Bourdon, A. and Pollack, P.: *Torsion subgroups of* CM *elliptic curves over odd degree number fields*. Int. Math. Res. Not. IMRN, 16:4923–4961, 2017. https://doi.org/10.1093/imrn/rnw163. ↑ 6, 66, 67.

[6] Brau, J. and Jones, N.: *Elliptic curves with 2-torsion contained in the 3-torsion field*. Proc. Amer. Math. Soc., 144:925–936, 2016. https://doi.org/10.1090/proc/12786. ↑ 28, 31.

[7] 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. ↑ 7, 8, 24, 29, 49.

[8] 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. ↑ 70.

[9] Clark, P. L., Corn, P., Rice, A., and Stankiewicz, J.: *Computation on elliptic curves with complex multiplication*. LMS J. Comput. Math., 17:509–539, 2014. https://doi.org/10.1112/S1461157014000072. ↑ 6, 22, 66, 67, 68.

[10] Cox, D. A.: *Galois Theory*. Pure and Applied Mathematics: A Wiley Series of Texts, Monographs and Tracts. John Wiley & Sons, Inc., 2nd edition, 2012. https://doi.org/10.1002/9781118218457.scard. ↑ 23.

[11] Daniels, H. B. and González-Jiménez, E.: *On the torsion of rational elliptic curves over sextic fields*. Mathematics of Computation, 89:411–439, 2020. https://doi.org/10.1090/mcom/3440. ↑ 22, 24, 30, 31, 40, 57.

[12] Daniels, H. B., Lozano-Robledo, Á., Najman, F., and Sutherland, A. V.: *Torsion points on rational elliptic curves over the compositum of all cubic fields*. Math. Comp., 87:425–458, 2018. https://doi.org/10.1090/mcom/3213. ↑ 23, 25, 26, 31, 69.

[13] Derickx, M., Etropolski, A., Hoeij, M. V., Morrow, J. S., and Zureick-Brown, D.: *Sporadic cubic torsion*. https://arxiv.org/abs/2007.13929, Submitted. ↑ 6.

[14] Dickson, L. E.: *Linear groups: With an exposition of the Galois field theory*. Leipzig: B. G. Teubner., 1901. ↑ 19.

[15] Fung, G., Ströher, H., Williams, H., and Zimmer, H.: *Torsion groups of elliptic curves with integral j-invariant over pure cubic fields*. J. Number Theory, 36:12–45, 1990. https://doi.org/10.1016/0022-314X(90)90003-A. ↑ 6.

[16] González-Jiménez, E.: *Complete classification of the torsion structures of rational elliptic curves over quintic number fields*. J. Algebra, 478:484–505, 2017. https://doi.org/10.1016/j.jalgebra.2017.01.012. ↑ 7, 8, 57.

[17] González-Jiménez, E. and Lozano-Robledo, Á.: *On the minimal degree of definition of p-primary torsion subgroups of elliptic curves*. Math. Res. Lett., 24:1067–1096, 2017. https://dx.doi.org/10.4310/MRL.2017.v24.n4.a7. ↑ 17, 26, 28, 64, 65.

[18] González-Jiménez, E. and Najman, F.: *An algorithm for determining torsion growth of elliptic curves*. https://doi.org/10.1080/10586458.2020.1771638, Exp. Math. to appear. ↑ 22, 27, 40, 48, 59, 60, 67, 73.

[19] González-Jiménez, E. and Najman, F.: *Growth of torsion groups of elliptic curves upon base change*. Math. Comp., 89:1457–1485, 2020. https://doi.org/10.1090/mcom/3478. ↑ 7, 8, 9, 10, 24, 25, 28, 35, 36, 37, 42, 43, 46, 50, 62, 66.

[20] González-Jiménez, E., Najman, F., and Tornero, J. M.: *Torsion of rational elliptic curves over cubic fields*. Mountain J. Math., 46:1899–1917, 2016. https://doi.org/10.1216/RMJ-2016-46-6-1899. ↑ 32.

[21] González-Jiménez, E. and Tornero, J. M.: *Torsion of rational elliptic curves over quadratic fields*. Revista de la Real Academia de Ciencias Exactas, Físicas y Naturales. Serie A. Matemáticas., 108:923–934, 2014. https://doi.org/10.1007/s13398-013-0152-4. ↑ 4.

[22] 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. ↑ 21.

[23] Gužvić, T.: *Torsion of elliptic curves with rational j-invariant defined over number fields of prime degree*. https://arxiv.org/abs/1912.04037, Submitted, 2021. ↑ 34.

[24] Han, J.: *The general linear group over a ring*. Bull. Korean Math. Soc., 43:619–626, 2006. https://doi.org/10.4134/BKMS.2006.43.3.619. ↑ 39.

[25] Ingram, P.: *Diophantine analysis and torsion points on elliptic curves*. Proc. London Math. Soc., 94:473–486, 2007. https://doi.org/10.1112/plms/pdl008. ↑ 30.

[26] Kamienny, S.: *Torsion points on elliptic curves and q-coefficients of modular forms*. Invent. Math., 109:221–229, 1992. https://doi.org/10.1007/BF01232025. ↑ 4, 6, 49.

[27] Kenku, M. A.: *The modular curve $X_0(39)$ and rational isogeny*. Math. Proc. Cambridge Philos. Soc., 85:21–23, 1979. https://doi.org/10.1017/S0305004100055444. ↑ 7.

[28] Kenku, M. A.: *The modular curve $X_0(169)$ and rational isogeny*. J. London Math. Soc., s2-22:239–244, 1980. https://doi.org/10.1112/jlms/s2-22.2.239, Corrigendum: https://doi.org/10.1112/jlms/s2-23.3.428-s. ↑ 7.

[29] Kenku, M. A.: *The modular curves $X_0(65)$ and $X_0(91)$ and rational isogeny*. Math. Proc. Cambridge Philos. Soc., 87:15–20, 1980. https://doi.org/10.1017/S0305004100056462. ↑ 7.

[30] Kenku, M. A.: *The modular curve $X_0(125)$, $X_1(25)$ and $X_1(49)$*. J. London Math. Soc., s2-23:415–427, 1981. https://doi.org/10.1112/jlms/s2-23.3.415. ↑ 7.

[31] Kenku, M. A. and Momose, F.: *Torsion points on elliptic curves defined over quadratic fields*. Nagoya Math. J., 109:125–149, 1988. https://doi.org/10.1017/S0027763000002816. ↑ 4, 6, 49.

[32] Le Fourn, S. and Lemos, P.: *Residual Galois representations of elliptic curves with image contained in the normaliser of a non-split Cartan*. arXiv:2002.02714. ↑ 20.

[33] Lozano-Robledo, Á: *Galois representations attached to elliptic curves with complex multiplication*. arXiv:1809.02584. ↑ 17.

[34] Lozano-Robledo, Á: *On the field of definition of p-torsion points on elliptic curves over the rationals*. Math. Ann., 357:279–305, 2013. https://doi.org/10.1007/s00208-013-0906-5. ↑ 25, 26, 27, 40, 44, 45, 55, 58, 61, 62, 66, 69, 73.

[35] Mazur, B.: *Modular curves and the Eisenstein ideal*. Inst. Hautes Etudes Sci. Publ. Math., 47:33–186, 1978. https://doi.org/10.1007/BF02684339. ↑ 4, 6.

[36] Mazur, B.: *Rational isogenies of prime degree*. Invent. Math., 44:129–162, 1978. https://doi.org/10.1007/BF01390348. ↑ 7, 19.

[37] Merel, L.: *Bornes pour la torsion des courbes elliptiques sur les corps de nombres*. Invent. Math., 124:437–449, 1996. https://doi.org/10.1007/s002220050059. ↑ 6.

[38] Merel, L. and Stein, W. A.: *The field generated by the points of small prime order on an elliptic curve*. International Mathematics Research Notices, 2001:1075–1082, 2001. https://doi.org/10.1155/S1073792801000514. ↑ 64.

[39] Morrow, J. S.: *Composite images of Galois for elliptic curves over $\mathbb{Q}$ and entanglement fields*. Math. Comp., 88:2389–2421, 2019. https://doi.org/10.1090/mcom/3426. ↑ 24, 40, 41.

[40] Müller, H., Ströher, H., and Zimmer, H.: *Torsion groups of elliptic curves with integral j-invariant over quadratic fields*. J. Reine Angew. Math., 397:100–161, 1989. https://doi.org/10.1515/crll.1989.397.100. ↑ 6.

[41] Najman, F.: *Complete classification of torsion of elliptic curves over quadratic cyclotomic fields*. J. Number Theory, 130:1964–1968, 2010. https://doi.org/10.1016/j.jnt.2009.12.008. ↑ 28.

[42] 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. ↑ 7, 8, 27, 29.

[43] Olson, L. D.: *Points of finite order on elliptic curves with complex multiplication*. Manuscripta Math., 14:195–205, 1974. https://doi.org/10.1007/BF01171442. ↑ 6.

[44] Pethő, A., Weis, T., and Zimmer, H.: *Torsion groups of elliptic curves with integral j-invariant over general cubic number fields*. Internat. J. Algebra Comput., 7:353–413, 1997. https://doi.org/10.1142/S0218196797000174. ↑ 6.

[45] Propp, O.: *Cartan images and ℓ-torsion points of elliptic curves with rational j-invariant*. Res. Number Theory, 4, 2018. https://doi.org/10.1007/s40993-018-0097-y. ↑ 7.

[46] Rouse, J., Sutherland, A. V., and Zureick-Brown, D.: *ℓ-adic images of Galois for elliptic curves over $\mathbb{Q}$*. preprint. ↑ 10, 25.

[47] Rouse, J. and Zureick-Brown, D.: *Elliptic curves over $\mathbb{Q}$ and 2-adic images of Galois*. Res. Number Theory, 1(12), 2015. https://doi.org/10.1007/s40993-015-0013-7. ↑ 17, 25, 28, 55, 61, 63, 69, 72.

[48] Serre, J. P.: *Quelques applications du théoremé du densité de Chebotarev*. Inst. Hautes Etudes Sci. Publ.Math., (54):323–401, 1981. http://www.numdam.org/item/PMIHES_1981__54__123_0/. ↑ 19.

[49] Silverman, J. H.: *Advanced Topics in the Arithmetic of Elliptic Curves*, volume 151 of *Graduate Texts in Mathematics*. Springer-Verlag New York, 1st edition, 1994. https://doi.org/10.1007/978-1-4612-0851-8. ↑ 5, 11, 30.

[50] Silverman, J. H.: *The Arithmetic of Elliptic Curves*, volume 106 of *Graduate Texts in Mathematics*. Springer-Verlag New York, 2nd edition, 2009. https://doi.org/10.1007/978-0-387-09494-6. ↑ 3, 11.

[51] Sutherland, A. V.: *Computing images of Galois representations attached to elliptic curves*. Forum Math. Sigma, 4:41–79, 2016. https://doi.org/10.1017/fms.2015.33. ↑ 17, 38, 74.

[52] Sutherland, A. V. and Zywina, D.: *Modular curves of prime-power level with infinitely many rational points*. Algebra Number Theory, 11:199–1299, 2017. https://doi.org/10.2140/ant.2017.11.1199. ↑ 32, 70, 71.

[53] The LMFDB Collaboration: *The L-functions and modular forms database*, 2019. http://www.lmfdb.org, [Online; accessed 30 October 2019]. ↑ 22.

[54] Washington, L.: *Elliptic Curves. Number Theory and Cryptography*. Discrete Mathematics and its Applications. Chapman and Hall/CRC, 2nd edition, 2003. ↑ 11.

[55] Zywina, D.: *On the possible images of the mod ℓ representations associated to elliptic curves over $\mathbb{Q}$*. https://arxiv.org/pdf/1508.07660.pdf, Submitted. ↑ 16, 29, 32, 72.

CURRICULUM VITAE

Tomislav Gužvić was born on 15.09.1991 in Pula. In 2011 he started his studies at the University of Zagreb, where he studied at the Mathematics Department of the Faculty of Science. He graduated summa cum laude with the thesis ”Galois representations of elliptic curves” (”Galoisove reprezentacije eliptičkih krivulja”) (2016), under the supervision of Filip Najman. After graduation, he started working as an assistant at the Mathematics Department of Faculty of Science of University of Zagreb where he enrolled in the PhD program.