KØBENHAVNS UNIVERSITET
INSTITUT FOR MATEMATISKE FAG

PhD thesis

Arithmetic and diophantine properties of elliptic curves with complex multiplication

Francesco Campagna

14 October 2021

Submission date	August 30, 2021
Defense date	October 14, 2021
Author	Francesco Campagna Institut for Matematiske Fag (IMF) - Københavns Universitet (KU) Universitetsparken 5, 2100 København Ø, DANMARK campagna@math.ku.dk
Advisor	Fabien Mehdi Pazuki Institut for Matematiske Fag (IMF) - Københavns Universitet (KU) Universitetsparken 5, 2100 København Ø, DANMARK fpazuki@math.ku.dk
Assessment committee	Jasmin Matz (Chair) Institut for Matematiske Fag (IMF) - Københavns Universitet (KU) Universitetsparken 5, 2100 København Ø, DANMARK matz@math.ku.dk
	Yuri Bilu Institut de Mathématiques de Bordeaux (IMB) - Université de Bordeaux Université de Bordeaux 351, cours de la Libération, Bordeaux (France) yuri@math.u-bordeaux.fr
	René Schoof Università di Roma “Tor Vergata” Dipartimento di Matematica Via della Ricerca Scientifica I-00133 Roma (Italy) schoof@mat.uniroma2.it
ISBN	978-87-7125-047-3

This thesis has been submitted to the PhD School of The Faculty of Science, University of Copenhagen

Abstract

In this thesis we consider elliptic curves with complex multiplication from three different angles: diophantine, algebraic and arithmetic statistical.

- **Diophantine point of view:** We study certain integrality properties of singular moduli *i.e.* of j-invariants of elliptic curves with complex multiplication. We prove various effective finiteness statements concerning differences of singular moduli that are S-units (Chapter 2).
- **Algebraic point of view:** For every CM elliptic curve E defined over a number field F, we analyze the Galois representation associated to the action of the absolute Galois group of F on the torsion points of E. This includes an investigation of the entanglement in the family of p^∞-division fields of E for p prime (Chapter 3 and Chapter 4).
- **Arithmetic statistical point of view:** Given an elliptic curve E over a number field F, we look at the density of the set of primes $\mathfrak{p} \subseteq F$ of good reduction for which the point group on the reduced elliptic curve $E \bmod \mathfrak{p}$ is cyclic. We detail both the CM and the non-CM case, outlining differences and similarities (Chapter 5).

Some of the material contained in the thesis has been used to write the following manuscripts: [Cam21b], [CS19], [CP21] and [Cam21a]. The article [CS19] has been written in collaboration with Peter Stevenhagen while the article [CP21] has been written in collaboration with Riccardo Pengo.

Resumé

I denne afhandling ser vi på elliptiske kurver med kompleks multiplikation fra tre forskellige vinkler: diophantin, algebraisk og aritmetisk-statistisk.

- **Diophantint synspunkt:** Vi studerer visse heltallighedsegenskaber af singulære moduli, dvs. af j-invarianter af elliptiske kurver med kompleks multiplikation. Vi beviser forskellige effektive endelighedssætninger omkring forskelle i singulære moduli, som er S-enheder (Chapter 2).
- **Algebraisk synspunkt:** For enhver KM elliptisk kurve E defineret over et tallegeme F, analyserer vi Galois repræsentationen associeret med virkningen af den absolutte Galois gruppe af F på torsionspunkterne på E. Dette inkluderer en undersøgelse af entaglement i p^∞-divisionslegemer associeret til E for primtal p (Chapter 3 og Chapter 4).
- **Aritmetisk-statistisk synspunkt:** Givet en elliptisk kurve E over et tallegeme F, ser vi på densiteten af sættet af primidealer $\mathfrak{p} \subseteq F$ af gode reduktioner, for hvilke punktgruppen på den reducerede elliptiske kurve E mod $\mathfrak{p}$ er cyklisk. Vi præsenterer i detaljer både KM og ikke-KM tilfældet og opridser forskellene og lighederne (Chapter 5).

Noget af materialet indeholdt i denne afhandling er brugt til at skrive følgende manuskripter: [Cam21b], [CS19], [CP21] og [Cam21a]. Artiklen [CS19] er skrevet i samarbejde med Peter Stevenhagen mens artiklen [CP21] er skrevet i samarbejde med Riccardo Pengo.

Acknowledgements

This thesis could have not existed if it weren't for the support of many people. I would like to thank all of them here.

First and foremost, I thank my advisor Fabien Pazuki for having always encouraged me during the whole PhD. His mentoring has gone way beyond a mere mathematical supervision between the narrow walls of the university, and Fabien has always had the maximum care in creating a stimulating research environment, whether it took the form of an informal home meeting or of an exotic *atelier de travail*. I am really grateful to him for having given me the opportunity of spending these three wonderful years in Copenhagen.

I heartily thank Peter Stevenhagen: since when I was a master student he has always guided and supported me, not only academically. Every time we discuss mathematics together, my passion for this subject lights up with renovated strength. Thanks to him, Leiden has become my second (mathematical) home.

There are countless reasons to thank Riccardo Pengo, but I will write here the most important: thanks Riccardo for being an invaluable friend on which I can always count. For all the long days and nights immersed in mathematical craziness. Together, we managed to swim across the Pacific!

I thank Yuri Bilu and Philipp Habegger for their hospitality during my stays at their institutions.

I thank all the members of my family because they always give me endless support, even from far away.

I thank all my present and past office mates Alex, Alexis, Clemens, David, Jeroen, Jingxuan, Kaif, Kevin, Mikala and my other fellow PhD students at the department for all the serious and funny moments spent together.

I thank all my friends around the world, without them I would have not been able to navigate in this sea of troubles. If I attempted to write all their names here I will certainly forget someone. I will not risk.

I finally thank Nanna Aamand for her help in writing the Danish version of the abstract (and for many other things!).

Table of contents

Prolegomena

Hic Rhodus, hic saltus

The first person to have intuited the phenomenon of complex multiplication seems to be, perhaps not surprisingly, Carl Friedrich Gauss. In the introduction to the celebrated *Sectio Septima* of his *Disquisitiones arithmeticae* (1801), the same section where he provides criteria for a regular polygon to be constructible with straightedge and compass, he enigmatically writes:

> *Ceterum principia theoriae, quam exponere aggredimur, multo latius patent, quam hic extendentur. Namque non solum ad functiones circulares, sed pari successu ad multas alias functiones transcendentes applicari possunt, e.g. ad eas quae ab integrali* $\int 1/\sqrt{1-x^4}$ *pendent...*

In brief, it seems to Gauss that his approach to the study of classical trigonometrical functions may be extended to investigate other kinds of transcendental functions such as the aforementioned $\mathrm{arcsl}(t) = \int_0^t 1/\sqrt{1-x^4}\,\mathrm{d}x$, nowadays known as the *lemniscate arcsine.* Here the mathematician is probably hinting to the fact that his theorem on the constructibility of n-th roots of unity using ruler and compass alone could be generalized to a theorem on the n-division points on the *Bernoulli lemniscate* (see Figure 0.1), whose arc length is precisely parametrized by $\mathrm{arcsl}(t)$. This clue did not go unnoticed, and thirty years later Abel [Abe28] managed to prove that the lemniscate could be divided into m equal parts using straightedge and compass if m is a power of 2 or if its odd prime factors p are of the form $p = 2^n + 1$. Using Abel's words: *"Ce thèorème est, comme on voit, précisément le même que celui de M. Gauss, relativement au cercle".*

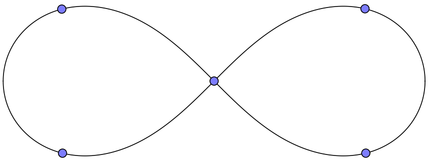

Figure 0.1: Bernoulli lemniscate $(x^2 + y^2)^2 = x^2 - y^2$ and the 6-division points on it. These divide the lemniscate into six arcs of equal length.

The heart of Abel's proof lies in the theory of complex multiplication for elliptic curves, even if the mathematician could not know it at the time. If we denote by $\varphi(z)$ the inverse function of $\operatorname{arcsl}(t)$, then φ extends to a doubly periodic meromorphic function on the complex plane. The association $z \mapsto (\varphi(z), \varphi'(z))$ gives a parametrization of the curve $C : y^2 = 1 - x^4$, whose Zariski closure in $\mathbb{P}^2_{\mathbb{C}}$ has a unique singular point at infinity. Its desingularization E turns out to be an elliptic curve with complex multiplication by $\mathbb{Z}[i]$, where multiplication by i is induced by the morphism $(x, y) \mapsto (ix, y)$ on C. Then proving Abel's theorem becomes essentially equivalent to studying the Galois groups $\operatorname{Gal}(K_m/\mathbb{Q}(i))$, where K_m are the fields obtained by adjoining to $\mathbb{Q}(i)$ the coordinates of the $(i+1)m$-torsion points of E for m odd. From the nice description of these Galois groups given by the inclusion $\operatorname{Gal}(K_m/\mathbb{Q}(i)) \subseteq (\mathbb{Z}[i]/m\mathbb{Z}[i])^\times$, one can easily deduce the desired result. A modern proof can be found in [Cox12, Chapter 15].

Abel's treatise *Recherches sur les fonctions elliptiques*, where the theorem on the lemniscate is contained, marks the beginning of the theory of complex multiplication (CM). Since then, several prominent mathematicians like Eisenstein, Kronecker, Weber, Deuring and many others have spent much effort in understanding, formalizing and systematizing this theory. Its consequences are so rich that CM elliptic curves even nowadays constitute an active area of research. This is why two hundred years after the publication of Abel's work you, reader, find in your hands yet another monograph on elliptic curves with complex multiplication (whose purposes are undoubtedly more modest than Abel's).

In this thesis we look at elliptic curves with complex multiplication from different perspectives. The first main characters to appear on the scene are j-invariants of CM elliptic curves over $\mathbb{C}$, classically known with the name of *singular moduli*. The word "modulus" comes from Latin and it means "unit of measurement". With time, in mathematics modulus became a synonym of "parameter" as for instance in the expression "moduli space", even if the original connotation is still used in some contexts (think to the modulus of a complex number). The term "singular" here has the signification of "unusual, unexpected". Hence singular moduli are literally unusual parameters of elliptic curves. What is so unusual about them? First of all, singular moduli are always algebraic integers. This is not a trivial statement, and is related with the fact that CM elliptic curves can be defined over number fields where they have everywhere good reduction. A second, even more surprising property of singular moduli is that they generate abelian extensions of imaginary quadratic fields. For instance, if an elliptic curve E has complex multiplication by the ring of integers of an imaginary quadratic field K, then the field obtained by adjoining the j-invariant of E to K is precisely the *Hilbert class field* of K.

Since singular moduli satisfy these strong number theoretical properties, they cannot possibly be random algebraic integers, and this is confirmed by their prime ideal factorization. For example, among the thirteen singular moduli belonging to $\mathbb{Q}$, eleven are cubes, and this is no coincidence. Also differences of singular moduli seem to show special patterns in their factorizations, as was already noticed by Berwick (see the beginning of Section 2.1). The question that we pose in Chapter 2 of this thesis concerns precisely prime factorizations of differences of singular moduli and can be formulated as follows: given a fixed singular modulus $j_0 \in \overline{\mathbb{Q}}$ and a fixed set S of rational primes, how many singular moduli j exist such that $j - j_0$ is an S-unit? Here, being an S-unit means that the primes appearing in the ideal factorization of $j - j_0$ lie all above primes belonging to S. We manage to give a complete answer to the above question for some singular moduli j_0 and some sets S that are infinite.

Theorem 0.0.1. *Let j_0 be a singular modulus of discriminant Δ and let $K := \mathbb{Q}(\sqrt{\Delta})$. Fix S to be the set of rational primes that are split in K. If $\{2, 3, 5, 7\} \not\subseteq S$, then for every singular modulus $j \in \overline{\mathbb{Q}}$ the difference $j - j_0$ is never an S-unit.*

See Theorem 2.2.1 for a proof of this result. In the statement, a singular modulus of discriminant Δ is simply the j-invariant of an elliptic curve with complex multiplication by an order of discriminant Δ, cfr. Chapter 1 for the terminology. Under certain assumptions, we can prove finiteness statements also in cases where, using the notation of the above theorem, the chosen set S contains primes that are non-split in K. As an example, we prove in Theorem 2.6.3 that if j is a singular modulus of discriminant Δ then $j + 3375$ can be a $\{13, 17\}$-unit only if $|\Delta| \leq 10^{84}$. Note that $j_0 = -3375$ is the j-invariant of any elliptic curve with CM by $\mathbb{Z}\left[\frac{1+\sqrt{-7}}{2}\right]$.

Starting from Chapter 3, the focus of the thesis shifts to Galois representations attached to CM elliptic curves. If F is a number field with algebraic closure $\overline{F}$ and $E_{/F}$ is an elliptic curve with complex multiplication by an imaginary quadratic order $\mathcal{O}$, then we can associate to E a continuous representation

$$\rho_E : G_F := \mathrm{Gal}(\overline{F}/F) \longrightarrow \mathrm{Aut}_{\mathbb{Z}}(E_{\mathrm{tors}})$$

using the natural action of G_F on the group $E_{\mathrm{tors}} = E(\overline{F})_{\mathrm{tors}}$ of torsion points on the elliptic curve E. Vaguely speaking, our goal in Chapters 3 and 4 is to understand as much as possible the image of ρ_E. The important point here is that we develop the theory for elliptic curves having complex multiplication by *general orders*, and not only by maximal ones.

The first thing to notice is that, contrarily to the non-CM case, $\rho_E(G_F)$ is not open in $\mathrm{Aut}_{\mathbb{Z}}(E_{\mathrm{tors}})$. Thus, if we want to recover an analogue of the celebrated Serre's Open Image Theorem in this setting, we need to define a smaller and, in some sense, canonical subgroup $\mathcal{G}(E/F) \subseteq \mathrm{Aut}_{\mathbb{Z}}(E_{\mathrm{tors}})$ in which the image of ρ_E is actually open. For example, if $\mathcal{O} \subseteq F$ we could take $\mathcal{G}(E/F) = \mathrm{Aut}_{\mathcal{O}}(E_{\mathrm{tors}})$, the group of automorphisms of E_{tors} as $\mathcal{O}$-module. Once this task is performed, we will try to understand how the Galois representation ρ_E is related to the Class Field Theory of the CM field of E. This will lead in Section 3.3 to the definition of *ray class fields for orders*, a generalization of the classical ray class fields where the moduli can be taken to be ideals (not necessarily invertible) of some order inside a fixed number field. The discussion in Chapter 3 culminates with the proof, in Theorem 3.5.2, of an explicit formula for the index $|\mathcal{G}(E/F) : \rho_E(G_F)|$ which generalizes upper bounds previously proved by Lombardo [Lom17, Theorem 6.6] and Bourdon and Clark [BC20, Corollary 1.5].

Theorem 0.0.2. *Let F be a number field and let $E_{/F}$ be an elliptic curve with complex multiplication by an order $\mathcal{O}$ in an imaginary quadratic field K. Then we have*

$$|\mathcal{G}(E/F) : \rho_E(G_F)| = [(FK) \cap K^{ab} \colon H_{\mathcal{O}}] \cdot \frac{\#\mathcal{O}^\times}{[F(E_{tors}) : (FK^{ab})]}$$

where $H_{\mathcal{O}}$ is the ring class field relative to $\mathcal{O}$ and K^{ab} is the maximal abelian extension of K.

After having obtained a fairly good understanding of the representation ρ_E, in Chapter 4 we turn to a more detailed study of its image $\rho_E(G_F)$. This is intimately related with the *entanglement problem* in the family of division fields of E, by which we mean the following. If for every prime $p \in \mathbb{N}$ we denote by $F(E[p^\infty])$ the field obtained by adjoining to F all the p-power torsion points of E, then classical Galois theory yields a natural map

$$\iota : \mathrm{Gal}(F(E_{\mathrm{tors}})/F) \hookrightarrow \prod_p \mathrm{Gal}(F(E[p^\infty])/F)$$

which is simply defined by restricting morphisms in $\mathrm{Gal}(F(E_{\mathrm{tors}})/F)$ to the various p^∞-division fields $F(E[p^\infty])$. When the map above is an isomorphism, we say that the p^∞-division fields of

E are *linearly disjoint* over F. Otherwise, we say that they are *entangled*, and the entanglement problem asks to precisely pin down the image of ι. We study this problem assuming that the CM order $\mathcal{O}$ is contained in the field of definition F (but this hypothesis is not too restrictive, see Theorem 5.6.2), in which case we obtain various explicit results. As an example, we state here the following theorem, which is proved in Corollary 4.4.7.

Theorem 0.0.3. *Let $\mathcal{O}$ be an order of discriminant $\Delta_{\mathcal{O}} < -3$ in an imaginary quadratic field $K \neq \mathbb{Q}(i)$. Denote by $H_{\mathcal{O}}$ the ring class field of $\mathcal{O}$ and fix $j \in H_{\mathcal{O}}$ to be the j-invariant of any elliptic curve with complex multiplication by $\mathcal{O}$. Then there exist infinitely many elliptic curves $E_{/H_{\mathcal{O}}}$ with $j(E) = j$ but non-isomorphic over $H_{\mathcal{O}}$, and such that*

- *$H_{\mathcal{O}}(E_{tors}) = K^{ab}$;*
- *The family $\{H_{\mathcal{O}}(E[p^\infty])\}_p$ is linearly disjoint over $H_{\mathcal{O}}$.*

Moreover, one can provide an explicit algorithm to determine a Weierstrass equation for these curves.

In Section 4.5 we also manage to classify all the possible entanglement scenarios that can occur in the family of p^∞-division fields of a CM elliptic curve over $\mathbb{Q}$ and base-changed over the corresponding CM field, provided that the CM order has discriminant $\Delta < -4$. See Theorem 4.5.2 for details.

Our entanglement investigations are not an end in themselves, but they can actually be applied to questions that at first sight seem of different nature. An example is provided by the cyclic reduction problem for elliptic curves, discussed in Chapter 5. Given an elliptic curve E defined over a number field F, the problem asks to determine, if it exists, the natural density $\delta(E)$ of the set of primes $\mathfrak{p}$ in F for which E has good reduction $\widetilde{E}$ and such that the point group of $\widetilde{E}$ over the residue field at $\mathfrak{p}$ is cyclic. It turns out that if the curve E has complex multiplication, this density exists, and it can be expressed as an infinite inclusion-exclusion sum involving the degrees of the squarefree division fields of E over F. This sum unfortunately converges rather slowly and it is not even clear when it vanishes. Obtaining a more enlightening expression for $\delta(E)$ from which, for instance, one could deduce vanishing criteria for the cyclic reduction density requires an understanding of the entanglement in the family of p-division fields of E for p-prime. This is almost the same topic we tackled in Chapter 4, and it may come as no surprise that our results therein allows us to obtain the desired expressions for $\delta(E)$. As a byproduct, we get the following result, which is a consequence of Theorem 5.6.3.

Theorem 0.0.4. *Let E be an elliptic curve with complex multiplication defined over $\mathbb{Q}(j(E))$. Then the cyclic reduction density $\delta(E)$ never vanishes.*

Using the work done in Section 4.5 we are also able to compute all the possible cyclic reduction densities for CM elliptic curves $E_{/\mathbb{Q}}$ with $j(E) \neq 0, 1728$. The results are summarized in Table 5.1.

Notation and conventions

From time to time, we may omit to recall in the text some standard notation or convention that we are tacitly adopting. This page collects the main potential sources of confusion.

Unless otherwise stated, we work inside a fixed algebraic closure $\overline{\mathbb{Q}}$ of the rational numbers. This enables us to take composita, intersections, etc. of number fields without particular worries. For a number field F we denote by $\mathcal{O}_F$ its ring of integers. The compositum of F with any other number field L is denoted by FL. When we say that an elliptic curve E defined over a number field F has good reduction modulo a certain prime $\mathfrak{p}$ of F we mean that E admits an integral model over $\mathcal{O}_F$ with good reduction at $\mathfrak{p}$.

Given a ring A, we denote by $A^\times$ its group of units. If G and H are two groups with $H \subseteq G$, we write $|G : H|$ for the index of H in G. For the cardinality of a set S we will not be strict, and we will use alternatively $\#S$ or $|S|$ according to graphical beauty.

We also adopt the usual Vinogradov notation: if $f, g : X \subseteq \mathbb{R} \to \mathbb{R}$ are two functions, we write $f = O(g)$ or $f \ll g$ to mean that there exists a constant $c \in \mathbb{R}_{>0}$ such that $|f(x)| \leq cg(x)$ for all $x \in X$.

The set $\mathbb{N}$ of natural numbers contains 0.

Preliminary definitions and results

1

To use a culinary metaphor, this chapter contains the ingredients to make a tasty pizza but it does not tell the secrets behind its preparation. In other words, the reader will find here the foundational definitions and results over which this entire thesis is built but they will not find a description of the more specific techniques used to attack the various problems treated. These techniques are instead described further in the text, when they will be more needed. For instance, in Section 1.2 of this chapter we discuss the definition and the main properties of quaternion algebras, but the theory of optimal embeddings will appear only in Section 2.4 where it will have an immediate application to the problem of singular S-units.

Having made this disclaimer, we now outline the content of this chapter. In Section 1.1 we discuss the theory of orders in number fields. After a completely general discussion on conductors and Picard groups, the focus will shift to the case of quadratic orders. In Section 1.2 we explain the needed concepts from the theory of quaternion algebras. In Section 1.3 we present some basic results on the theory of complex multiplication. These are complemented in Section 1.4 by some old and new theorems on the reduction theory of CM elliptic curves.

1.1 Orders in number fields

Definition 1.1.1. *Let F be a number field. An order in F is a subring $\mathcal{O} \subseteq F$ that is finitely generated as $\mathbb{Z}$-module and such that $\mathcal{O} \otimes_{\mathbb{Z}} \mathbb{Q} = F$.*

Example 1.1.2. The ring of integers $\mathcal{O}_F$ of a number field F is always an order. It is usually called the *maximal order* in F because any other order in F is contained in $\mathcal{O}_F$, as it is shown in Lemma 1.1.4.

Example 1.1.3. Let F be a number field and $\mathfrak{a} \subseteq \mathcal{O}_F$ a non-zero ideal. Then $\mathcal{O} = \mathbb{Z} + \mathfrak{a}$ is an order. In the special case when F is a quadratic field with ring of integers $\mathcal{O}_F = \mathbb{Z}[\omega]$ and $\mathfrak{a} = f\mathcal{O}_F$ with $f \in \mathbb{Z}_{>0}$, we obtain $\mathcal{O} = \mathbb{Z}[f\omega]$. One can prove that in the quadratic case all the orders have this form.

Lemma 1.1.4. *For every number field F and every order $\mathcal{O}$ we have $\mathcal{O} \subseteq \mathcal{O}_F$.*

Proof. This follows from the fact that $\mathcal{O}$ is finitely generated as $\mathbb{Z}$-module, see [AM69, Chapter 5, Proposition 5.1]. □

Definition 1.1.5. *Let $\mathcal{O}$ be an order in a number field F. The conductor of $\mathcal{O}$ is the set*

$$\mathfrak{f}_{\mathcal{O}} := \{x \in F : x\mathcal{O}_F \subseteq \mathcal{O}\}.$$

It is easy to see that the conductor $\mathfrak{f}_{\mathcal{O}}$ is an ideal of $\mathcal{O}$ which is trivial if and only if $\mathcal{O}$ is maximal. Moreover, $\mathfrak{f}_{\mathcal{O}}$ is also the largest ideal of $\mathcal{O}_F$ that is contained in $\mathcal{O}$.

Example 1.1.6. Let F be a number field and let $\mathcal{O} = \mathbb{Z} + \mathfrak{a}$, where $\mathfrak{a} \subseteq \mathcal{O}_F$ is a non-zero ideal. Then a computation shows that

$$\mathfrak{f}_{\mathcal{O}} = d\mathbb{Z} + \mathfrak{a}$$

where d is the exponent of $\mathcal{O}_F/\mathcal{O}$. In particular, if F is a quadratic field with ring of integers $\mathcal{O}_F = \mathbb{Z}[\omega]$, then for every $f \in \mathbb{Z}_{>0}$ the order $\mathcal{O} = \mathbb{Z}[f\omega]$ has conductor $f_{\mathcal{O}} = f\mathcal{O}_F$.

Non-maximal orders in number fields are not Dedekind domains since they are not integrally closed. In particular, unique factorization of ideals does not hold in general. However, unique factorization can be recovered by restricting to those ideals that are coprime with the conductor.

Theorem 1.1.7. *Let $\mathcal{O}$ be an order in a number field F and denote by $\mathfrak{f}_{\mathcal{O}}$ its conductor. Then every ideal $\mathfrak{a} \subseteq \mathcal{O}$ that is coprime to $\mathfrak{f}_{\mathcal{O}}$, i.e. such that $\mathfrak{a} + \mathfrak{f}_{\mathcal{O}} = \mathcal{O}$, can be written uniquely as a product of invertible prime ideals of $\mathcal{O}$. In particular, every ideal of $\mathcal{O}$ coprime with the conductor is invertible.*

Proof. See [Con, Theorem 3.6] and [Con, Corollary 3.11]. □

Remark 1.1.8. Note that being coprime with the conductor $\mathfrak{f}_{\mathcal{O}}$ of the order $\mathcal{O}$ is sufficient but not necessary to imply invertibility, since all principal ideals are invertible. However, for prime ideals this condition is indeed sufficient: a prime ideal $\mathfrak{p} \subseteq \mathcal{O}$ is invertible if and only if it is coprime with $\mathfrak{f}_{\mathcal{O}}$ [Con, Theorem 6.1].

For an order $\mathcal{O}$ and an ideal $\mathfrak{c} \subseteq \mathcal{O}$, we denote by $I_{\mathcal{O}}(\mathfrak{c})$ the group generated by the ideals of $\mathcal{O}$ that are coprime to $\mathfrak{c}$. Theorem 1.1.7 implies that $I_{\mathcal{O}}(\mathfrak{f}_{\mathcal{O}})$ is a subgroup of the group $I_{\mathcal{O}}$ of invertible fractional ideals of $\mathcal{O}$. Denote also by $P_{\mathcal{O}}$ the group of principal fractional ideals of $\mathcal{O}$ and by $P_{\mathcal{O}}(\mathfrak{c})$ the group generated by the principal ideals of $\mathcal{O}$ that are coprime to $\mathfrak{c}$.

Theorem 1.1.9. *Let $\mathcal{O}$ be an order in a number field F with conductor $\mathfrak{f}_{\mathcal{O}}$. Then for all ideals $\mathfrak{a} \subseteq \mathcal{O}$ and $\mathfrak{b} \subseteq \mathcal{O}_F$ coprime with $\mathfrak{f}_{\mathcal{O}}$ the associations*

$$\mathfrak{a} \mapsto \mathfrak{a}\mathcal{O}_F \qquad \text{and} \qquad \mathfrak{b} \mapsto \mathfrak{b} \cap \mathcal{O}$$

are each other inverses and induce a group isomorphism between $I_{\mathcal{O}}(\mathfrak{f}_{\mathcal{O}})$ and $I_{\mathcal{O}_F}(\mathfrak{f}_{\mathcal{O}})$. Moreover, the natural maps

$$\mathcal{O}/\mathfrak{a} \longrightarrow \mathcal{O}_F/\mathfrak{a}\mathcal{O}_F \qquad \text{and} \qquad \mathcal{O}/(\mathfrak{b} \cap \mathcal{O}) \longrightarrow \mathcal{O}_F/\mathfrak{b}$$

are isomorphisms for every pair of integral ideals $\mathfrak{a} \in I_{\mathcal{O}}(\mathfrak{f}_{\mathcal{O}})$ and $\mathfrak{b} \in I_{\mathcal{O}_F}(\mathfrak{f}_{\mathcal{O}})$.

Proof. See [Con, Theorem 3.8]. □

As in the case of Dedekind domains, one can also associate to every order $\mathcal{O}$ an ideal class group. In order to obtain a group, one has to disregard the non-invertible ideals of $\mathcal{O}$.

Definition 1.1.10. *Let $\mathcal{O}$ be an order in a number field F. The class group (or Picard group) of $\mathcal{O}$ is the quotient*

$$\operatorname{Pic}(\mathcal{O}) = I_{\mathcal{O}}/P_{\mathcal{O}}.$$

Theorem 1.1.11. *The natural map*

$$I_{\mathcal{O}}(\mathfrak{f}_{\mathcal{O}})/P_{\mathcal{O}}(\mathfrak{f}_{\mathcal{O}}) \longrightarrow \operatorname{Pic}(\mathcal{O})$$

is an isomorphism.

Proof. See [LD15, Theorem 3.11]. □

Theorem 1.1.11 allows to interpret $\operatorname{Pic}(\mathcal{O})$ as a generalized ideal class group modulo $\mathfrak{f}_{\mathcal{O}}$. Indeed, under the isomorphism $I_{\mathcal{O}}(\mathfrak{f}_{\mathcal{O}}) \cong I_{\mathcal{O}_F}(\mathfrak{f}_{\mathcal{O}})$ given by Theorem 1.1.9, the subgroup $P_{\mathcal{O}}(\mathfrak{f}_{\mathcal{O}})$ corresponds to the group $P(\mathcal{O}) \subseteq I_{\mathcal{O}_F}(\mathfrak{f}_{\mathcal{O}})$ generated by the principal ideals $\alpha\mathcal{O}_F$ such that $\alpha \in \mathcal{O}$ and $\alpha\mathcal{O} + \mathfrak{f}_{\mathcal{O}} = \mathcal{O}$. It is readily seen that $P(\mathcal{O})$ is a congruence subgroup modulo $\mathfrak{f}_{\mathcal{O}}$, since for every $\beta \in \mathcal{O}_F$ such that $\beta \equiv 1 \bmod \mathfrak{f}_{\mathcal{O}}$ we have $\beta \in 1 + \mathfrak{f}_{\mathcal{O}} \subseteq \mathcal{O}$. In particular, there exists an abelian extension $F \subseteq H_{\mathcal{O}}$ corresponding to $P(\mathcal{O})$ such that $\operatorname{Gal}(H_{\mathcal{O}}/F) \cong \operatorname{Pic}(\mathcal{O})$. We call $H_{\mathcal{O}}$ the *ring class field of F relative to the order $\mathcal{O}$*. Note that, since by definition $H_{\mathcal{O}}$ is contained in the ray class field modulo $\mathfrak{f}_{\mathcal{O}}$, in $F \subseteq H_{\mathcal{O}}$ the only possibly ramified primes are the ones dividing the conductor of $\mathcal{O}$. We will give an idelic characterization of $H_{\mathcal{O}}$ in Section 3.3. In the quadratic case, the congruence subgroup $P(\mathcal{O})$ admits an alternative description that will appear in Theorem 1.1.12.

We conclude our discussion on class groups by remarking that for every order $\mathcal{O}$ in a number field F, one always has an exact sequence

$$1 \longrightarrow \mathcal{O}^\times \longrightarrow \mathcal{O}_F^\times \longrightarrow (\mathcal{O}_F/\mathfrak{f}_{\mathcal{O}})^\times / (\mathcal{O}/\mathfrak{f}_{\mathcal{O}})^\times \longrightarrow \operatorname{Pic}(\mathcal{O}) \longrightarrow \operatorname{Pic}(\mathcal{O}_F) \longrightarrow 1$$

see [Neu99, Chapter I, Propositions 12.9 and 12.11]. In particular, the order of the Picard group of $\mathcal{O}$ can be related to the order of the class group of F by means of the formula

$$\#\operatorname{Pic}(\mathcal{O}) = \frac{\#\operatorname{Pic}(\mathcal{O}_F)}{|\mathcal{O}_F : \mathcal{O}|} \frac{\#\,(\mathcal{O}_F/\mathfrak{f}_{\mathcal{O}})^\times}{\#\,(\mathcal{O}/\mathfrak{f}_{\mathcal{O}})^\times}.$$

1.1.1 Orders in quadratic number fields

In this thesis, a major role is played by orders in imaginary quadratic number fields, since these occur as endomorphism rings of elliptic curves with complex multiplication. Hence, in this subsection we study the quadratic case in detail, collecting the relevant facts that will be used in the sequel. We fix a quadratic number field K of discriminant Δ_K and ring of integers $\mathcal{O}_K = \mathbb{Z}[\omega]$.

As explained in Example 1.1.3, the orders in K have all the form $\mathcal{O} = \mathbb{Z}[f\omega]$ for some $f \in \mathbb{Z}_{>0}$. Moreover, we saw in Example 1.1.6 that the conductor of the order $\mathbb{Z}[f\omega]$ is given by the ideal $\mathfrak{f}_{\mathcal{O}} = f\mathcal{O}_K$. For these reasons, in the quadratic case it is customary to call the integer f (rather than the ideal $f\mathcal{O}_K$) the conductor of $\mathcal{O}$. We will adopt this convention as well. Note also that $f = |\mathcal{O}_F : \mathcal{O}|$.

Fix then $f \in \mathbb{Z}_{>0}$ and let $\mathcal{O} \subseteq K$ be the order of conductor f. Its *discriminant* $\Delta_{\mathcal{O}}$ can be obtained by computing the discriminant of any $\mathbb{Z}$-basis of $\mathcal{O}$. If $f = 1$, *i.e.* if $\mathcal{O}$ is a maximal order, we call $\Delta_{\mathcal{O}} = \Delta_K$ a *fundamental discriminant*. In general, one always has $\Delta_{\mathcal{O}} = f^2\Delta_K$ and, in particular, it follows that $\Delta_{\mathcal{O}} \equiv 0, 1 \bmod 4$. Viceversa, for every integer $\Delta \equiv 0, 1 \bmod 4$ the order $\mathcal{O}_\Delta = \mathbb{Z}\left[\frac{\Delta+\sqrt{\Delta}}{2}\right]$ has discriminant Δ and it is contained in the field $\mathbb{Q}(\sqrt{\Delta})$. We obtain a one-to-one correspondence between integers $\Delta \equiv 0, 1 \bmod 4$ and quadratic orders $\mathcal{O}$. Clearly, if an order has negative discriminant then it is contained in an imaginary quadratic field and we call it an *imaginary quadratic order*. With the only exceptions of $\Delta_{\mathcal{O}} = -3, -4$, an imaginary quadratic order $\mathcal{O}$ always satisfies $\mathcal{O}^\times = \{\pm 1\}$. If $\Delta_{\mathcal{O}} = -3$ (resp. $\Delta_{\mathcal{O}} = -4$) the units in $\mathcal{O}$ are exactly the primitive 6-th (resp. 4-th) roots of unity in $\overline{\mathbb{Q}}$

In the quadratic case, more can be said also about the Picard group of an order. For instance, at the end of the previous section we have shown that $\operatorname{Pic}(\mathcal{O})$ can be seen as a generalized ideal class group modulo f, and we have also provided a corresponding congruence subgroup $P(\mathcal{O}) \subseteq I_{\mathcal{O}_K}(f)$. One can give an alternative description of $P(\mathcal{O})$, as in the following theorem.

Theorem 1.1.12. *Let $\mathcal{O}$ be an order of conductor f in a quadratic field K. Then there are natural isomorphisms*

$$\operatorname{Pic}(\mathcal{O}) \cong I_{\mathcal{O}}(f)/P_{\mathcal{O}}(f) \cong I_{\mathcal{O}_K}(f)/P_{\mathcal{O}_K,\mathbb{Z}}(f)$$

where $P_{\mathcal{O}_K,\mathbb{Z}}(f)$ is the subgroup of $I_{\mathcal{O}_K}(f)$ generated by the principal ideals $\alpha\mathcal{O}_K$ such that

$$\alpha \textit{ mod } f \in \operatorname{Im}\left((\mathbb{Z}/f\mathbb{Z})^\times \to (\mathcal{O}_K/f\mathcal{O}_K)^\times\right).$$

Proof. This is [Cox13, Theorem 7.22]. The proof therein is valid also in the real quadratic case. We again point out that the first isomorphism above is given by Theorem 1.1.11 while the second isomorphism is induced by the one in Theorem 1.1.9. □

We conclude this subsection by describing $\operatorname{Pic}(\mathcal{O})$ in the imaginary quadratic case. Assume that K is an imaginary quadratic field and $\mathcal{O} \subseteq K$ an imaginary quadratic order. Consider a non-zero fractional $\mathcal{O}$-ideal $\mathfrak{a} \subseteq K$. Since $\mathcal{O}$ is a quadratic order, the ideal $\mathfrak{a}$ is a free $\mathbb{Z}$-module of rank 2 and, in particular, can be written as $\mathfrak{a} = \mathbb{Z}a \oplus \mathbb{Z}b$ for some $a, b \in K$. After choosing an embedding $K \hookrightarrow \mathbb{C}$, we can then see $\mathfrak{a}$ as a lattice in the complex plane. If moreover $\mathfrak{a}$ is invertible, then its class $[\mathfrak{a}]$ in the class group $\operatorname{Pic}(\mathcal{O})$ corresponds to the homothety class of the lattice $\Lambda = \mathbb{Z}a + \mathbb{Z}b \subseteq \mathbb{C}$. In particular, there exists a unique lattice $\Lambda' = \mathbb{Z} + \mathbb{Z}\tau$ that is homothetic to Λ and such that $\tau \in \mathbb{C}$ belongs to the *fundamental domain*

$$\mathcal{F} := \left\{z \in \mathbb{C} : -\frac{1}{2} < \operatorname{Re}(z) \leq \frac{1}{2} \text{ and } |z| > 1\right\} \cup \left\{z \in \mathbb{H} : 0 \leq \operatorname{Re}(z) \leq \frac{1}{2} \text{ and } |z| = 1\right\} \tag{1.1}$$

where $\mathbb{H} = \{z \in \mathbb{C} : \operatorname{Im}(z) > 0\}$ denotes the Poincaré half plane. The following theorem, attributed to Gauss, provides a complete set of representatives of the ideal classes in $\operatorname{Pic}(\mathcal{O})$ containing only ideals of the form $\mathbb{Z} + \mathbb{Z}\tau$ with $\tau \in \mathcal{F}$.

Theorem 1.1.13. *Let $\mathcal{O}$ be an imaginary quadratic order of discriminant Δ. Define T_Δ as the set of triples of integers (a, b, c) such that*

$$\begin{aligned} &\gcd(a, b, c) = 1, \qquad \Delta = b^2 - 4ac, \\ &\textit{either} \quad -a < b \leq a < c \quad \textit{or} \quad 0 \leq b \leq a = c. \end{aligned}$$

and let

$$C = \left\{\frac{b + \sqrt{\Delta}}{2a} : (a, b, c) \in T_\Delta\right\} \subseteq \mathcal{F}.$$

Then the set of ideals $\{\mathbb{Z} + \mathbb{Z}\tau : \tau \in C\}$ is a complete set of representatives of the ideal classes in $\operatorname{Pic}(\mathcal{O})$.

Proof. See [Cox13, Theorems 2.8 and 7.7]. □

1.2 Rudiments on quaternion algebras

Let F be a field of characteristic $\operatorname{char}(F) \neq 2$ and fix an algebraic closure $\overline{F}$.

Definition 1.2.1. *An algebra $\mathbb{B}$ over F is a quaternion algebra if there exist $i, j \in \mathbb{B}$ such that $1, i, j, ij$ is an F-basis of $\mathbb{B}$ and*

$$i^2 = a, \; j^2 = b, \; ij = -ji \tag{1.2}$$

for some $a, b \in F^\times$.

It is clear that the relations (1.2) completely determine the multiplication on $\mathbb{B}$. For $a, b \in F^\times$ we then denote by $\left(\frac{a,b}{F}\right)$ the quaternion algebra with basis $\{1, i, j, ij\}$ satisfying (1.2).

Every quaternion algebra $\mathbb{B}$ (over F) comes equipped with a natural anti-commutative involution

$$\alpha = a + bi + cj + dij \mapsto \overline{\alpha} := a - bi - cj - dij, \qquad a, b, c, d \in F$$

called the *standard involution* on $\mathbb{B}$. It allows to define the two maps

$$\mathrm{trd}(\alpha) := \alpha + \overline{\alpha}, \qquad \mathrm{nrd}(\alpha) := \alpha\overline{\alpha}, \qquad \alpha \in \mathbb{B}$$

called, respectively, the *reduced trace* and the *reduced norm* on $\mathbb{B}$. It is easy to verify that $\mathrm{trd}(\alpha), \mathrm{nrd}(\alpha) \in F$ for all $\alpha \in \mathbb{B}$. We deduce that every element $\alpha \in \mathbb{B}$, being a root of the polynomial

$$f_\alpha(x) = x^2 - \mathrm{trd}(\alpha)x + \mathrm{nrd}(\alpha) \in F[x], \tag{1.3}$$

generates a field extension of F that is at most quadratic. The polynomial $f_\alpha(x)$ in (1.3) is called the *reduced characteristic polynomial* of α. The reduced trace also allows to define a bilinear pairing on $\mathbb{B}$ as follows:

$$\langle \alpha, \beta \rangle := \mathrm{trd}(\alpha\overline{\beta}) = \alpha\overline{\beta} + \beta\overline{\alpha} \tag{1.4}$$

for all $\alpha, \beta \in \mathbb{B}$. It is readily verified that the pairing in (1.4) is bilinear symmetric, hence the map

$$\alpha \mapsto \frac{1}{2}\langle \alpha, \alpha \rangle = \mathrm{nrd}(\alpha)$$

makes $\mathbb{B}$ into a 4-dimensional quadratic space.

Quaternion algebras are closely related to matrix algebras, as the following proposition explains.

Proposition 1.2.2. *Let $\mathbb{B}$ be a division algebra over F. The following are equivalent:*

1. *$\mathbb{B}$ is a quaternion algebra;*
2. *$\mathbb{B}$ is a central simple algebra;*
3. *$\mathbb{B} \otimes_F \overline{F}$ is isomorphic to the ring $M_2(\overline{F})$ of 2×2 matrices with coefficients in $\overline{F}$.*

Proof. See [Voi21, Proposition 7.6.1]. □

If a quaternion algebra $\mathbb{B}$ over F is isomorphic to $M_2(F)$ we say that $\mathbb{B}$ is *split*.

Example 1.2.3. By Proposition 1.2.2 every quaternion algebra defined over an algebraically closed field is split.

Example 1.2.4. The quaternion algebra $\left(\frac{a,b}{\mathbb{R}}\right)$ is split if and only if either $a > 0$ or $b > 0$, see [Voi21, Chapter 1, Exercise 4 (c)].

Clearly, being non-split is a necessary condition for a quaternion algebra to be a division ring. As a consequence of the Artin-Weddeburn Theorem, this condition turns out to be also sufficient (see [Voi21, Proposition 7.6.2]). We also point out that in a split quaternion algebra the reduced trace and norm correspond respectively to the matrix trace and determinant. This follows from the uniqueness of the standard involution [Voi21, Corollary 3.4.4].

Assume for the rest of this section that F is a number field and denote by $\mathcal{M}_F = \mathcal{M}_F^0 \cup \mathcal{M}_F^\infty$ the union of the sets of finite and infinite places of F respectively. For every $v \in \mathcal{M}_F$ denote by F_v the completion of F at v. In particular, $F_v = \mathbb{R}$ if v is real and $F_v = \mathbb{C}$ if v is complex.

Definition 1.2.5. *We say that a quaternion algebra $\mathbb{B}$ defined over F is ramified at the place $v \in \mathcal{M}_F$ if $\mathbb{B} \otimes_F F_v$ is a division algebra. Otherwise, we say that $\mathbb{B}$ is split at v. We also call $\mathbb{B}$ (totally) definite if $\mathbb{B}$ is ramified at all archimedean places of F.*

Example 1.2.6. By Example 1.2.3 quaternion algebras over F are split at all the infinite complex primes of F. In particular, if there exist a definite quaternion algebra over F then F must be totally real.

Not only the set $\mathrm{Ram}_F(\mathbb{B})$ of ramification places for a quaternion algebra $\mathbb{B}$ over F is finite, but it also determines $\mathbb{B}$ up to isomorphism, as explained in the following theorem.

Theorem 1.2.7. *Let F be a number field. The map $\mathbb{B} \mapsto Ram_F(\mathbb{B})$ is a bijection between the set of quaternion algebras over F up to isomorphism and the set of finite subset of non-complex places of F with even cardinality.*

Proof. See [Voi21, Main Theorem 14.6.1]. □

Example 1.2.8. By Theorem 1.2.7, for every prime $p \in \mathbb{N}$ there exist a unique (up to isomorphisms) definite quaternion algebra over $\mathbb{Q}$ with $\mathrm{disc}(\mathbb{B}) = p$. If $p \equiv 2 \bmod 3$ it can be verified (for instance using Hilbert symbols, see [Voi21, Section 12.4]) that a representative for this isomorphism class is given by $\mathbb{B} = \left(\frac{-3,-p}{\mathbb{Q}}\right)$.

Definition 1.2.9. *Let $\mathbb{B}$ be a quaternion algebra defined over a number field F. The discriminant of $\mathbb{B}$ is the ideal*

$$\mathrm{disc}(\mathbb{B}) = \prod_{\mathfrak{p} \in Ram_F(\mathbb{B}) \setminus \mathcal{M}_F^\infty} \mathfrak{p} \subseteq \mathcal{O}_F.$$

We conclude this section by recalling some useful facts on the integral theory of quaternion algebras. We continue to assume that F is a number field.

Definition 1.2.10. *Let $\mathbb{B}$ be a quaternion algebra over F. An order $\mathcal{O} \subseteq \mathbb{B}$ is a subring that is finitely generated as $\mathcal{O}_F$-module and such that $\mathcal{O} \otimes_{\mathcal{O}_F} F = \mathbb{B}$.*

Remark 1.2.11. Then reader has certainly noticed the similarity between Definition 1.1.1 and Definition 1.2.10. In fact, we can consider quaternion orders as the non-commutative analogue of the usual orders in number fields. As such, many classical constructions (such as Picard groups, zeta functions, etc.) can be performed also in the quaternionic setting, with some additional complication arising from the lack of commutativity.

Similarly to the number field case (cfr. Lemma 1.1.4), also quaternion orders satisfy the basic property that their elements are integral over the base field. More precisely, if $\mathcal{O} \subseteq \mathbb{B}$ is a quaternion order, then for every $\alpha \in \mathcal{O}$ we have $\mathrm{trd}(\alpha), \mathrm{nrd}(\alpha) \in \mathcal{O}_F$ (see [Voi21, Corollary 10.3.6]), and, in particular, the reduced characteristic polynomial $f_\alpha(x)$ in (1.3) has integral coefficients.

Given an order $\mathcal{O}$ in a quaternion algebra $\mathbb{B}$ over F, we can define in the standard way its discriminant ideal with respect to the bilinear form (1.4). More specifically, for every $\alpha_1, \dots, \alpha_4 \in \mathcal{O}$ we set

$$d(\alpha_1, \dots, \alpha_4) := \det(\mathrm{trd}(\alpha_i \overline{\alpha}_j))_{1 \leq i,j \leq 4}$$

and we define the *discriminant* of $\mathcal{O}$ as the $\mathcal{O}_F$-submodule $\operatorname{disc}(\mathcal{O}) \subseteq F$ generated by the set $\{d(\alpha_1, \dots, \alpha_4) : \alpha_1, \dots, \alpha_4 \in \mathcal{O}\}$. Since every element of an order is integral, we see that actually $\operatorname{disc}(\mathcal{O})$ is an ideal in $\mathcal{O}_F$. If in addition the ring of integers $\mathcal{O}_F$ is a principal ideal domain, then the order $\mathcal{O}$ is also free over $\mathcal{O}_F$ (being finitely generated by definition and clearly torsion-free) and one has

$$\operatorname{disc}(\mathcal{O}) = d(\alpha_1, \dots, \alpha_4)\mathcal{O}_F$$

for any $\mathcal{O}_F$-basis $\{\alpha_1, \dots, \alpha_4\} \subseteq \mathcal{O}$. We remark that when $F = \mathbb{Q}$, we will often confuse the discriminant of the order $\mathcal{O}$ with its positive generator.

The reader may at this point wonder what is the relation between the discriminant of a quaternion algebra $\mathbb{B}$ defined over a number field F as in Definition 1.2.9 and the discriminant of the various orders $\mathcal{O} \subseteq \mathbb{B}$. To answer this question, we need to introduce a couple of definitions.

Definition 1.2.12. *Let $\mathbb{B}$ be a quaternion algebra over F and let $\mathcal{O}_1, \mathcal{O}_2 \subseteq \mathbb{B}$ be two orders. The index module of $\mathcal{O}_2$ in $\mathcal{O}_1$ is the $\mathcal{O}_F$-module $|\mathcal{O}_1 : \mathcal{O}_2|$ generated by the set*

$$\{\det \phi : \phi \in \operatorname{End}_F(\mathbb{B}),\ \phi(\mathcal{O}_1) \subseteq \mathcal{O}_2\}$$

where $\operatorname{End}_F(\mathbb{B})$ is the set of endomorphisms of $\mathbb{B}$ as F-vector space.

We remark that if $F = \mathbb{Q}$ and $\mathcal{O}_2 \subseteq \mathcal{O}_1$ then the index module is principal, generated by $\#(\mathcal{O}_1/\mathcal{O}_2)$. In this case, for convenience we will identify $|\mathcal{O}_1 : \mathcal{O}_2|$ with its positive generator, recovering in this way the usual notion of index.

Definition 1.2.13. *An order $\mathcal{O} \subseteq \mathbb{B}$ is maximal if it is not properly contained in any other order.*

Theorem 1.2.14. *Let F be a number field and $\mathbb{B}$ a quaternion algebra over F.*

1. *If $\mathcal{O} \subseteq \mathbb{B}$ is a maximal order, then* $\operatorname{disc}(\mathcal{O}) = \operatorname{disc}_F(\mathbb{B})^2$.
2. *If $\mathcal{O}_2 \subseteq \mathcal{O}_1$ are two orders in $\mathbb{B}$ then* $\operatorname{disc}(\mathcal{O}_2) = |\mathcal{O}_1 : \mathcal{O}_2|^2 \cdot \operatorname{disc}(\mathcal{O}_2)$.

Proof. For the first part of the theorem see [Voi21, Theorem 15.5.5]. The second part is proved in [Voi21, Lemma 15.2.15]. □

1.3 Basic facts on elliptic curves with complex multiplication

Definition 1.3.1. *Let k be a field with fixed algebraic closure $\overline{k}$ and let $E_{/k}$ be an elliptic curve. We say that E has complex multiplication (or that E is a CM elliptic curve) if the geometric endomorphism ring $\operatorname{End}_{\overline{k}}(E)$ is isomorphic to an order $\mathcal{O}$ in an imaginary quadratic field. In this case, we also say that E has complex multiplication by $\mathcal{O}$.*

Remark 1.3.2. Note that in our definition an elliptic curve can have complex multiplication even if not all its geometric endomorphisms are defined over the base field.

If the reader seeks an explanation for the term *complex multiplication* in Definition 1.3.1, they have to turn to the analytic theory of elliptic curves over the complex numbers. By the uniformization theorem [Sil94, I, Corollary 4.3], every elliptic curve $E_{/\mathbb{C}}$ admits a complex parametrization

$$\xi : \mathbb{C}/\Lambda \to E(\mathbb{C})$$

where $\Lambda \subseteq \mathbb{C}$ is a lattice. This establishes a one-to-one correspondence between the set of lattices in $\mathbb{C}$ up to homothety and the set of complex elliptic curves up to isomorphism. This correspondence is functorial, in the sense that to every holomorphic homomorphism $\mathbb{C}/\Lambda_1 \to \mathbb{C}/\Lambda_2$ corresponds a unique isogeny $E_1 \to E_2$, where E_1, E_2 are elliptic curves corresponding to the lattices Λ_1, Λ_2 under the uniformization theorem. Now, by [Sil09, VI, Theorem 4.1] any holomorphic homomorphism $\mathbb{C}/\Lambda_1 \to \mathbb{C}/\Lambda_2$ has the form $z \mapsto \alpha z$ for some $\alpha \in \mathbb{C}$ such that $\alpha\Lambda_1 \subseteq \Lambda_2$. In particular, the endomorphisms of an elliptic curve E corresponding to a quotient $\mathbb{C}/\Lambda$ correspond to *multiplications* by complex numbers sending Λ to itself. Clearly, for every integer $n \in \mathbb{Z}$ we have $n\Lambda \subseteq \Lambda$, and this corresponds to the fact that on every abelian group one has a multiplication-by-n morphism. On the other hand, if there exists $\alpha \in \mathbb{C} \setminus \mathbb{Z}$ such that $\alpha\Lambda \subseteq \Lambda$ then it is not difficult to see that α must be an imaginary quadratic number. In particular, the elliptic curve E possesses a *complex multiplication*, whence the name.

This etymological digression triggers the following question: how do we find a lattice Λ for which $\mathcal{E} := \{\alpha \in \mathbb{C} : \alpha\Lambda \subseteq \Lambda\} \neq \mathbb{Z}$? There is an easy way: fix $\mathcal{O} \subseteq \mathbb{C}$ to be an imaginary quadratic order and let $\mathfrak{a} \subseteq \mathcal{O}$ be an invertible ideal. This assumption implies in particular that $\mathcal{O} = \{\alpha \in \mathbb{C} : \alpha\mathfrak{a} \subseteq \mathfrak{a}\}$, see [Cox13, proposition 7.4]. Since $\mathfrak{a}$ can be regarded as a complex lattice, we see that the quotient $\mathbb{C}/\mathfrak{a}$ corresponds to an elliptic curve with complex multiplication by $\mathcal{O}$. It may come as a surprise the fact that this construction gives all the complex elliptic curves with complex multiplication by $\mathcal{O}$.

Theorem 1.3.3. *Let $\mathcal{O} \subseteq \mathbb{C}$ be an order in an imaginary quadratic field K. Then the map $[\mathfrak{a}] \to \mathbb{C}/\mathfrak{a}$ gives a bijection between $\mathrm{Pic}(\mathcal{O})$ and the set of isomorphism classes of elliptic curves $E_{/\mathbb{C}}$ with complex multiplication by $\mathcal{O}$.*

Proof. See [Cox13, Corollary 10.20]. □

The $\mathbb{C}$-isomorphism class of a complex elliptic curve E is determined by the j-invariant $j(E)$. The j-invariant of a CM elliptic curve defined over $\mathbb{C}$ is called a *singular modulus*. For instance, $j_0 = 0$ is a singular modulus, since it is the j-invariant of the elliptic curve $E : y^2 = x^3 + 1$, which has complex multiplication by the maximal order in $\mathbb{Q}(\sqrt{-3})$. By Theorem 1.3.3, for every imaginary quadratic order $\mathcal{O}$ of discriminant $\Delta \in \mathbb{Z}_{<0}$ there are exactly C_Δ singular moduli, where $C_\Delta = \#\mathrm{Pic}(\mathcal{O})$ denotes the class number of the order $\mathcal{O}$. It turns out that these C_Δ singular moduli are actually all algebraic integers, and they form a full Galois orbit over $\mathbb{Q}$ (see [Cox13, Theorem 11.1] and [Cox13, Proposition 13.2]). We call them *singular moduli of discriminant* Δ or *singular moduli relative to the order* $\mathcal{O}$. Reversing subject and complements, we will sometimes also speak of discriminant, CM order, CM field, etc... associated to j. Moreover, when we talk about the class number of a singular modulus we are referring to the class number of the order relative to the singular modulus in question. Given a singular modulus of discriminant Δ, we call its minimal polynomial over $\mathbb{Q}$ the *Hilbert class polynomial* of discriminant Δ, and we denote it by $H_\Delta(x)$. By the above discussion, $H_\Delta(x)$ has integer coefficients, degree C_Δ and its roots in $\overline{\mathbb{Q}}$ are precisely all the singular moduli of discriminant Δ. Hilbert class polynomials play a fundamental role in the class field theory of imaginary quadratic fields because of the following result.

Theorem 1.3.4. *Let $\mathcal{O}$ be an order of discriminant Δ in an imaginary quadratic field K. Then $H_\Delta(x)$ is irreducible over K and $K[x]/(H_\Delta(x))$ is isomorphic to the ring class field $H_\mathcal{O}$ of K relative to the order $\mathcal{O}$. In particular, $H_\mathcal{O}$ is generated over K by any singular modulus of discriminant Δ.*

Proof. See [Cox13, Theorem 11.1]. □

Since singular moduli are algebraic numbers, every CM elliptic curve $E_{/\mathbb{C}}$ admits a model defined over some number field $F \subseteq \overline{\mathbb{Q}}$. We are then naturally led to consider the reduction theory of elliptic curves $E_{/\overline{\mathbb{Q}}}$ with complex multiplication. Historically, this theory has its roots in the works by Deuring and its essential points will be recalled in Section 1.4. Here we content ourselves to show the following consequence of the integrality properties of singular moduli.

Theorem 1.3.5. *Let F be a number field and $E_{/F}$ an elliptic curve with complex multiplication. Then E has potential good reduction at every prime of F.*

Proof. It follows from [Sil09, VII, Proposition 5.5] and the fact that singular moduli are algebraic integers. □

The minimal possible number field of definition for E is $F = \mathbb{Q}(j(E))$, and this is often called the *field of moduli* of E. However, in general the elliptic curve E will not have everywhere good reduction over its field of moduli.

We conclude this section by discussing the concept of *normalized isomorphisms* for CM elliptic curves. Given a number field F and an elliptic curve $E_{/F}$ with complex multiplication by an order $\mathcal{O}$ in an imaginary quadratic number field K, there exist exactly two isomorphisms $\mathcal{O} \longrightarrow \mathrm{End}_{\overline{F}}(E)$. One is obtained from the other by precomposing with the unique non-trivial ring automorphism of $\mathcal{O}$. However, one can make a canonical choice among these two isomorphisms: this is done by looking at the pullbacks of the invariant differentials on E via elements of $\mathrm{End}_{\overline{F}}(E)$, as the following proposition explains.

Proposition 1.3.6. *Let F be a number field, fix an algebraic closure $F \subseteq \overline{F}$ and let $E_{/F}$ be an elliptic curve with complex multiplication by an imaginary quadratic order $\mathcal{O} \subseteq \overline{F}$. Then there is a unique isomorphism $[\cdot]_E : \mathcal{O} \longrightarrow \mathrm{End}_{\overline{F}}(E)$ such that $[\alpha]_E^* \omega = \alpha\omega$ for all invariant differentials ω on E and all $\alpha \in \mathcal{O}$, where $[\alpha]_E^*\omega$ denotes the pull-back of ω via $[\alpha]_E$.*

Proof. Fix an embedding $\varphi : \overline{F} \hookrightarrow \mathbb{C}$. Then, for the base-change $E_{/\mathbb{C}}$ via φ, we can use [Sil94, II, Proposition 1.1] to see that there exists a unique isomorphism $[\cdot] : \varphi(\mathcal{O}) \longrightarrow \mathrm{End}_{\mathbb{C}}(E)$ such that for any invariant differential ω we have

$$[\varphi(\alpha)]^*\omega = \varphi(\alpha)\omega$$

for all $\alpha \in \mathcal{O}$. Since φ induces an isomorphism between $\mathrm{End}_{\overline{F}}(E)$ and $\mathrm{End}_{\mathbb{C}}(E)$, we can define $[\cdot]_E$ by means of the following diagram

$$\begin{tikzcd}
\varphi(\mathcal{O}) \arrow[r, "{[\cdot]}"] & \mathrm{End}_{\mathbb{C}}(E) \\
\mathcal{O} \arrow[u, "\varphi"] \arrow[r, dashed, "{[\cdot]_E}"'] & \mathrm{End}_{\overline{F}}(E) \arrow[u, "\wr"]
\end{tikzcd}$$

and the proposition follows. □

Definition 1.3.7. *Let E be an elliptic curve with complex multiplication by an order $\mathcal{O}$ and defined over a number field F. We call the unique isomorphism $[\cdot]_E : \mathcal{O} \longrightarrow \mathrm{End}_{\overline{F}}(E)$ appearing in Proposition 1.3.6 the normalized isomorphism associated to E. We also call the pair $(E, [\cdot]_E)$ normalized.*

With the above definition, we can now state the following useful theorem.

Theorem 1.3.8. *Let F be a number field and $E_{/F}$ an elliptic curve with complex multiplication by an order $\mathcal{O} \subseteq \overline{\mathbb{Q}}$. Then for every $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ and $\alpha \in \mathcal{O}$ we have*

$$\sigma([\alpha]_E) = [\sigma(\alpha)]_{E^\sigma}$$

where $[\cdot]_E$ and $[\cdot]_{E^\sigma}$ are respectively the normalized isomorphisms of E and of the conjugate elliptic curve E^σ.

Proof. See [Sil94, II, Theorem 2.2 (a)]. □

1.4 Deuring's reduction theory and beyond

Let k be a field of characteristic $\mathrm{char}(k) = p > 0$ with algebraic closure $\overline{k} \supseteq k$ and let $E_{/k}$ be an elliptic curve. We say that E is *supersingular* if the unique p-torsion point of E defined over $\overline{k}$ is the identity $O \in E(\overline{k})$. If this is the case, then the endomorphism ring $\mathrm{End}_{\overline{k}}(E)$ is isomorphic to a maximal order in the unique (up to isomorphism) quaternion algebra over $\mathbb{Q}$ ramified only at p and ∞ (see [Deu41] or [Voi21, Theorem 42.1.9] for a modern exposition). On the other hand, if E possesses a non-trivial p-torsion point then the endomorphism ring $\mathrm{End}_{\overline{k}}(E)$ is isomorphic to an order in an imaginary quadratic field. In this case, we say that E is *ordinary*.

Consider now an elliptic curve E defined over a number field F and given by a fixed model over $\mathcal{O}_F$. For how many primes of good reduction $\mathfrak{p} \subseteq \mathcal{O}_F$, the reduced elliptic curve $E \bmod \mathfrak{p}$ is ordinary? Supersingular? Do these set have a natural density? These apparently harmless questions turn out to be very hard if the elliptic curve E does not have complex multiplication. For instance, while it is relatively easy to see that there are infinitely many primes of ordinary reduction (see [Sil09, V, Exercise 5.11] for the case $F = \mathbb{Q}$) the existence of infinitely many primes of supersingular reduction is still unknown in general. Serre shows in [Ser89, IV–13, Exercise 1] that the natural density of the set of supersingular primes is 0 and, thanks to the relatively recent works of Elkies [Elk87], [Elk89], we now know that there are infinitely many primes of supersingular reduction for E if the field of definition F has odd degree over $\mathbb{Q}$ or if it has at least one real embedding. Even in these cases, the asymptotic behaviour of the supersingular primes counting function is still unknown at present.

On the other hand, if the elliptic curve E has complex multiplication, a complete characterization of ordinary and supersingular primes has been known since the first half of the twentieth century, thanks to the work of Deuring [Deu41]. It can be summarized in the following theorem.

Theorem 1.4.1. *Let E be an elliptic curve defined over a number field L and with complex multiplication by an order $\mathcal{O} = \mathbb{Z} + f\mathcal{O}_K$ of conductor f in an imaginary quadratic field K. Let $\mathfrak{p}$ be a prime of L lying over a rational prime p where E has good reduction $\widetilde{E}$. Then the reduction mod $\mathfrak{p}$ induces an injective homomorphism $\mathrm{End}_L(E) \hookrightarrow \mathrm{End}_{\overline{\mathbb{F}}_p}(\widetilde{E})$. Moreover:*

1. *if p is ramified or inert in $\mathbb{Q} \subseteq K$, then $\widetilde{E}$ is supersingular;*
2. *if p is split in $\mathbb{Q} \subseteq K$, then $\widetilde{E}$ is ordinary and $\mathrm{End}_{\overline{\mathbb{F}}_p}(\widetilde{E}) \cong \mathbb{Z} + f'\mathcal{O}_K$ where $f = f'p^n$ with $\gcd(f', p) = 1$;*

Proof. This is a combination of [Sil94, II, Proposition 4.4] and of [Lan87, Chapter 13, Theorem 12]. □

Fix now a rational prime $p \in \mathbb{N}$ and let $\mathcal{J}_p$ be the set of singular moduli relative to and order $\mathcal{O}$ such that p is split in $K = \mathrm{Frac}(\mathcal{O})$ and does not divide the conductor of $\mathcal{O}$. By Theorem

1.4.1, for every prime $\mathfrak{p} \subseteq \overline{\mathbb{Q}}$ lying above p (by which we mean a compatible system of primes lying above p), the reduction modulo $\mathfrak{p}$ gives a map from $\mathcal{J}_p$ to the set $\mathcal{J}_{\mathrm{ord}}(\overline{\mathbb{F}}_p)$ of ordinary j-invariants in $\overline{\mathbb{F}}_p$.

Theorem 1.4.2. *For every prime $\mathfrak{p} \subseteq \overline{\mathbb{Q}}$ lying above a rational $p \in \mathbb{N}$, the reduction modulo $\mathfrak{p}$ is a bijection between $\mathcal{J}_p$ and $\mathcal{J}_{ord}(\overline{\mathbb{F}}_p)$.*

Proof. See [Lan87, Chapter 13, Theorem 13]. □

Instead of investigating the various reduction types of elliptic curves defined over number fields, one can start with an elliptic curve $\widetilde{E}$ defined over a finite field of characteristic p and ask whether there exists an elliptic curve E defined over a number field F, and a prime $\mathfrak{p} \subseteq O_F$ lying above p, such that $E \bmod \mathfrak{p} \cong \widetilde{E}$ over $\overline{\mathbb{F}}_p$. Clearly, stated in this way the question has a trivial answer: it suffices to take any curve $E_{/\overline{\mathbb{Q}}}$ whose j-invariant is a lift in characteristic 0 of $j(\widetilde{E}) \in \overline{\mathbb{F}}_p$. However, the discussion at the beginning of this section tells us that every elliptic curve $\widetilde{E}_{/\overline{\mathbb{F}}_p}$ satisfies $\mathrm{End}_{\overline{\mathbb{F}}_p}(\widetilde{E}) \neq \mathbb{Z}$, while a random elliptic curve E obtained by lifting $j(\widetilde{E})$ will not have this property in general. We can then be more demanding and ask: can we lift $\widetilde{E}$ to an elliptic curve $E_{/\overline{\mathbb{Q}}}$ that has complex multiplication? Truth is, we can do even more. Not only we can lift $\widetilde{E}$ to an elliptic curve over $\overline{\mathbb{Q}}$, but also any fixed endomorphism $\alpha_0 \in \mathrm{End}_{\overline{\mathbb{F}}_p}(\widetilde{E})$. This is the content of the so-called *Deuring lifting theorem* which we now formally state.

Theorem 1.4.3. *Let $\widetilde{E}$ be an elliptic curve defined over a finite field of characteristic $p \in \mathbb{N}$ and let $\alpha_0 \in \mathrm{End}_{\overline{\mathbb{F}}_p}(\widetilde{E})$ be a non-trivial endomorphism. Then there exists an elliptic curve E defined over a number field F, an endomorphism $\alpha \in \mathrm{End}_F(E)$ and a prime $\mathfrak{p} \subseteq O_F$ of good reduction for E such that $E \bmod \mathfrak{p} \cong_{\overline{\mathbb{F}}_p} \widetilde{E}$ and the endomorphism α corresponds to α_0 under this isomorphism.*

Proof. See [Lan87, Chapter 13, Theorem 14]. □

Despite what may be suggested by the above discussion, there are still many unanswered questions revolving around the reduction theory of CM elliptic curves. For instance, let us formulate a problem that naturally arises form Deuring's theorems and that has been the object of recent works by Michel [Mic04] and Aka, Luethi, Michel, Wieser [Aka+20].

Let $p \in \mathbb{N}$ be a rational prime and fix a prime $\mathfrak{p} \subseteq \overline{\mathbb{Q}}$ lying above it. Let O be an order in an imaginary quadratic field K and assume that p is inert in K. We denote by $\mathrm{Ell}(O)$ the set of $\overline{\mathbb{Q}}$-isomorphism classes of elliptic curves with complex multiplication by O and by $\mathrm{Ell}_{\mathrm{ss}}(\overline{\mathbb{F}}_p)$ the set of isomorphism classes of supersingular elliptic curves over $\overline{\mathbb{F}}_p$. Both sets are finite: indeed, we have $\#\mathrm{Ell}(O) = \#\mathrm{Pic}(O)$ by Theorem 1.3.3 and subsequent discussion, while $\mathrm{Ell}_{\mathrm{ss}}(\overline{\mathbb{F}}_p)$ is finite by [Sil09, V, Theorem 4.1]. Moreover, by Theorem 1.3.5 every class in $\mathrm{Ell}(O)$ can be represented by an elliptic curve E that has good reduction at $\mathfrak{p}$. Using now Theorem 1.4.1, the reduction modulo $\mathfrak{p}$ induces a map

$$\Psi_{\mathfrak{p},O} : \mathrm{Ell}(O) \to \mathrm{Ell}_{\mathrm{ss}}(\overline{\mathbb{F}}_p), \qquad [E]_{\overline{\mathbb{Q}}} \mapsto [E \bmod \mathfrak{p}]_{\overline{\mathbb{F}}_p} \tag{1.5}$$

that is well-defined by [Sil94, II, Proposition 4.4]. The map $\Psi_{\mathfrak{p},O}$ is not injective in general, since the class number of imaginary quadratic orders tends to infinity as their discriminant grows in absolute value, while the cardinality of the set $\mathrm{Ell}_{\mathrm{ss}}(\overline{\mathbb{F}}_p)$ is fixed from the beginning. On the other hand, this same argument makes it reasonable to expect that the map $\Psi_{\mathfrak{p},O}$ becomes surjective when the discriminant of the order O is large enough. However, understanding the surjectivity of $\Psi_{\mathfrak{p},O}$ does not seem an easy task, and the only known results on the topic follow from deep equidistribution statements concerning Heegner points. We summarize these results in the statement of the following theorem.

Theorem 1.4.4. *Let $p, q_1, q_2 \in \mathbb{N}$ be distinct odd primes. Then there exists a constant $C = C(p, q_1, q_2) \geq 0$ such that the following holds: for every prime $\mathfrak{p} \subseteq \overline{\mathbb{Q}}$ lying above p and for every imaginary quadratic order O of discriminant Δ satisfying:*

1. *$|\Delta| \geq C$;*

2. *p is inert in $\mathbb{Q}(\sqrt{\Delta})$;*

3. *p does not divide Δ;*

4. *q_1 and q_2 are split in $\mathbb{Q}(\sqrt{\Delta})$;*

the supersingular reduction map $\Psi_{\mathfrak{p},O}$ in (1.5) is surjective. Moreover, for every prime $p \in \mathbb{N}$ there exists a constant $C' = C'(p) > 0$ such that for every for every prime $\mathfrak{p} \subseteq \overline{\mathbb{Q}}$ lying above p and for every imaginary quadratic field K of discriminant $|\Delta_K| \geq C'$, the map $\Psi_{\mathfrak{p},O_K}$ is surjective.

Proof. The first part of the theorem is a corollary of [Aka+20, Theorem 7.1]. The second part is a corollary of [Mic04, Theorem 3]. □

Remark 1.4.5. The constants appearing in the statement of Theorem 1.4.4 are not explicit.

Singular moduli and S-units 2

We have seen in Chapter 1 that the set of singular moduli, that is, the set of j-invariants of elliptic curves over $\overline{\mathbb{Q}}$ with complex multiplication, is contained in the ring of algebraic integers. A careful inspection reveals many regularities in their prime factorization, and since the beginning of the last century much effort has been made in order to formalize this regularity into precise formulas. In this chapter we look at integrality properties of singular moduli from a diophantine point of view and we ask the following questions: given a set S of rational primes and a fixed singular modulus $j_0 \in \overline{\mathbb{Q}}$, what can we say about the set of singular moduli $j \in \overline{\mathbb{Q}}$ such that $j - j_0$ is an S-unit? Is this set finite? If so, can we bound its cardinality?

In the first part of this chapter we frame the above problems both in a historical and in a mathematical context. In particular, we describe in Section 2.1 the progress that has been made towards their solution and we show how these results fit into a modular analogue of a conjecture by Su-ion Ih, originally formulated for abelian schemes. In the second part of this chapter, we prove some effective finiteness results concerning differences of singular moduli that are S-units for certain sets S of primes. In Section 2.2 we deal with some special infinite sets S for which one can provide complete answers to the above questions, see Theorem 2.2.1. This will naturally lead to the apparently unrelated problem, addressed in Section 2.3, of understanding when primes that are congruent to 1 modulo 3 can divide the norm of a singular modulus.

In order to deal with set of primes that are different from the ones considered above, we need to build some more machinery. For this reason, we discuss optimal embeddings in quaternion orders and their relation with the reduction theory of CM elliptic curves in Section 2.4, while in Section 2.5 we prove Theorem 2.5.1, which allows to bound the ℓ-adic absolute value of differences of singular moduli for certain primes ℓ. This will be used in Section 2.6 to provide other effective bounds on the number of S-differences $j - j_0$ with $j_0 \neq 0, 1728$, for some new sets S of cardinality at most 2. For instance, we will see in Theorem 2.6.3 that the discriminant Δ of any singular modulus j such that $j + 3375$ is an $\{13, 17\}$-unit satisfies $|\Delta| \leq 10^{84}$. Similar theorems also hold in the case $j_0 = 1728$ (Theorem 2.7.1) and $j_0 = 0$ (Theorem 2.7.2, under GRH), as we will see in Section 2.7. In Section 2.8 the optimality of the bounds found in Theorem 2.5.1 in the case $j_0 = 0$ is discussed. Finally in Section 2.9 we provide numerical evidence for some uniformity conjectures concerning differences of singular moduli that are S-units.

2.1 The problem of singular S-units

The fact that prime factorizations of singular moduli seem to follow certain patterns and are not completely random was noticed at the beginning of the 20th century by the British mathematician William Edward Hodgson Berwick. In 1928, Berwick published an article [Ber28] where he computed the factorization of all singular moduli of class number $h \leq 3$. His calculations organize and expand Weber's computations of CM j-invariants contained in the monumental work *Lehrbuch der Algebra* [Web28]. Given the fact that there are 146 singular moduli of class number smaller than 3, the computation must have certainly undergone to the same amount of tricks and numerical observations already used by Weber in his book. We have to keep in mind that computers were not available at the time, and the mathematician was only helped by the use of a Trinks-Brunsviga calculating machine, a precursor of the modern calculators appeared for the first time in the 1893 World's Fair in Chicago.

At the end of his paper (see [Ber28, §10]), Berwick formulates a series of conjectures relating the appearance of some rational primes dividing differences of singular moduli with certain congruence conditions satisfied by the corresponding discriminants. For instance, an inspection of his tables suggests him that for every singular modulus j of discriminant $\Delta \equiv 5 \bmod 8$ one has $j \equiv 0 \bmod 2^{15}$. As an illustration, Berwick computes

$$j_{-35} = -(2^5\sqrt{5}\varepsilon^4)^3 \qquad j_{-59} = -2^{15}\theta^{12}(\theta-1)^3(2\theta-1)^3$$

where j_Δ denotes a singular modulus of discriminant Δ (recall that singular moduli relative to the same discriminant are all Galois conjugate), $\varepsilon = \frac{1}{2}(1+\sqrt{5})$ is a fundamental unit in $\mathbb{Q}(\sqrt{5})$ and $\theta \in \overline{\mathbb{Q}}$ satisfies $\theta^3 - 2\theta^2 - 1 = 0$. These conjectures, nowadays known with the name of *Berwick congruences*, were proved only more than 50 years later by Gross and Zagier [GZ85]. Actually, their work does much more: it also provides explicit formulas for the prime factorization of the absolute norm $N(j_1 - j_2)$ where j_1, j_2 are singular moduli relative to coprime fundamental discriminants. These formulas have been recently generalized to arbitrary singular moduli by Lauter and Viray [LV15].

At this point, the reader may be tempted to think that, since we have explicit formulas, we then know everything about the factorization of singular moduli. However, they would be too quick in jumping to conclusions. For instance, suppose we ask the seemingly innocent question: is it possible for a singular modulus to have norm ±1? In other words, is it possible for a singular modulus to be an algebraic unit? In all probability the warned reader wouldn't inspect the formulas in [GZ85] and [LV15] with much enthusiasm, and we believe with good reason. Indeed, these formulas seem (at least in our opinion) too complicated to be used as a tool in the solution of this problem, since they require a very precise knowledge on the prime factorization of certain integers which, a priori, do not satisfy any nice arithmetical property. This makes Gross-Zagier and Lauter-Viray formulas easy to apply in order to compute specific examples but seemingly difficult to use in the proof of general statements.

If the curious reader is now wondering when and why someone became interested in singular moduli that are algebraic units, here is where our story begins.

2.1.1 The beginnings: a question and an answer

A theorem of André [And98, Théorème] asserts that, apart from some "obvious" exceptions, equations of the form $f(x, y) = 0$ for $f \in \mathbb{C}[x, y]$ have finitely many solutions (j_1, j_2) with j_1 and j_2 both singular moduli. More precisely, the theorem establishes the validity of André-Oort conjecture for $Y(1)^2_{\mathbb{C}} \cong \mathbb{A}^2_{\mathbb{C}}$, where $Y(1)_{\mathbb{C}}$ is the classical modular curve of level 1 and the isomorphism is given by applying the modular j-function on both components. Call a point of the form (j_1, j_2), with $j_1, j_2 \in \mathbb{C}$ singular moduli, a *special point*. Then Andrè-Oort conjecture in this context asserts that an irreducible algebraic curve $X \subseteq \mathbb{A}^2_{\mathbb{C}}$ contains infinitely many special points if and only if X is itself special, *i.e.* of the form $\mathbb{A}^1_{\mathbb{C}} \times \{x\}$, $\{x\} \times \mathbb{A}^1_{\mathbb{C}}$ with $x \in \mathbb{C}$ a singular modulus, or $\Phi_N(X, Y) = 0$, where Φ_N denotes the classical modular polynomial of level N.

The proof of André's result is not effective, meaning that, given a non-special curve $X \subseteq \mathbb{A}^2_{\mathbb{C}}$, it does not yield an explicit bound on the number of special points on X. In recent years, many efforts have been done in order to obtain effective results for special families of curves, see for instance [BMZ13], [Küh12] and [Küh13]. In particular, in [BMZ13] it is shown that the equation $xy = 1$ has no solution in singular moduli. Motivated by this result, Masser asked whether it is possible that a singular modulus can be a unit in the ring of algebraic integers. Such a singular modulus will be herein called a singular unit. A first, partial answer to this question has been given by Habegger in [Hab15], where it is proved the following theorem.

Theorem 2.1.1. *There exist at most finitely many singular units.*

Since it will be useful for the subsequent sections, in what follows we will try to give an overview of the proof of this result. The idea is, given a singular unit x of discriminant Δ, to provide an upper and a lower bound for its Weil height $h(x)$ which contradict each other when $|\Delta|$ is sufficently large. The (logarithmic) Weil height is defined, for every $x \in \overline{\mathbb{Q}}$, as

$$h(x) = \frac{1}{[K:\mathbb{Q}]} \sum_{v \in \mathcal{M}_K} [K_v : \mathbb{Q}_v] \log^+ |x|_v \tag{2.1}$$

where $K := \mathbb{Q}(x)$ is the field generated by x over the rationals, $\mathcal{M}_K$ is the set of all places of K, the integer $[K_v : \mathbb{Q}_v]$ is the local degree at the place v and $\log^+ |x|_v := \log \max\{1, |x|_v\}$. Here, for every non-archimedean place v corresponding to the prime ideal $\mathfrak{p}_v$ lying above the rational prime p_v, the absolute value $|\cdot|_v$ is normalized in such a way that

$$|x|_v = p_v^{-v_{\mathfrak{p}_v}(x)/e_v}$$

e_v being the ramification index of $\mathfrak{p}_v$ over p_v. From some results of Colmez [Col98] and Nakkajima-Taguchi [NT91] on the stable Faltings height of a CM elliptic curve one gets the lower bound

$$h(x) \geq c_1 \log |\Delta| - c_2 \tag{2.2}$$

for some constants $c_1, c_2 > 0$ (whose precise knowledge is not really needed for this proof). As far as the upper bound is concerned, the author proceeds as follows: since x^{-1} is also an algebraic integer, the finite places do not contribute to the computation of its Weil height. Hence we can write:

$$h(x) = h(x^{-1}) = \frac{1}{C_\Delta} \sum_{1 \leq k \leq C_\Delta} \log^+ |x_k^{-1}| \tag{2.3}$$

where C_Δ denotes the class number of the unique order of discriminant Δ and for every $k = 1, \ldots, C_\Delta$, the x_k are the Galois conjugates of the singular modulus x. We have then to control the conjugates that are small in absolute value. Fix $0 < \varepsilon < 1$ and let $\mathcal{F}$ be the usual fundamental domain for the action of $\mathrm{SL}_2(\mathbb{Z})$ on the Poincaré half plane defined in (1.1). Note that for every $k = 1, \ldots, C_\Delta$ there is a unique $\tau_k \in \mathcal{F}$ for which $x_k = j(\tau_k)$. Define the "cat's ears" as

$$U_\varepsilon := \{z \in \mathcal{F} : \min\{|z - \zeta_6|, |z - \zeta_3|\} < \varepsilon\}$$

where $\zeta_6 = e^{\frac{2\pi i}{6}}$ and $\zeta_3 = e^{\frac{2\pi i}{3}}$. Notice that the $\tau_k \in U_\varepsilon$ give rise to singular moduli x_k of small absolute value since ζ_6 and ζ_3 are zeros of the j-function. By splitting the sum in formula (2.3) as

$$h(x) = \frac{1}{C_\Delta} \sum_{\tau_k \in U_\varepsilon} \log^+ |x_k^{-1}| + \frac{1}{C_\Delta} \sum_{\tau_k \notin U_\varepsilon} \log^+ |x_k^{-1}|$$

and by estimating separately the two sums, the author gets

$$h(x) \leq \frac{C_{\Delta,\varepsilon}}{C_\Delta} c_3 \log |\Delta| + 3 \log \varepsilon^{-1} + c_4 \tag{2.4}$$

where $C_{\Delta,\varepsilon} = \#(\{\tau_1, \dots, \tau_k\} \cap U_\varepsilon)$ and c_3, c_4 are positive real constants. Hence, in order to conclude, one has to bound the quantity $\frac{C_{\Delta,\varepsilon}}{C_\Delta}$. Here Habegger uses Duke-Clozel-Ullmo equidistribution (see [CU04] and [Duk88]) to prove that, for $|\Delta|$ sufficiently large, one has

$$\frac{C_{\Delta,\varepsilon}}{C_\Delta} \ll \varepsilon^2.$$

With this estimate, for $|\Delta|$ sufficiently large, the height $h(x)$ can be bounded from below and from above by

$$c_1 \log|\Delta| - c_2 \leq h(x) \leq c\varepsilon^2 \log|\Delta| + 3\log\varepsilon^{-1} + c_4$$

and, by choosing ε properly, one gets a contradiction for $|\Delta|$ large enough. This implies that there are at most finitely many singular units.

2.1.2 No singular modulus is a unit

As we have just seen, the proof of the finiteness of singular units is not effective since it relies on an equidistribution result. However, in the subsequent paper [BHK20], Yu. Bilu, P. Habegger and L. Kühne managed to prove the following theorem.

Theorem 2.1.2. *Singular units do not exist.*

Roughly speaking, this result is achieved by carrying out an effective version of the proof contained in [Hab15] and by improving the obtained bounds in order to be able to use computer assisted techniques.

The first step is to explicitly describe those $\tau \in \mathcal{F}$ such that $j(\tau)$ is a singular modulus of fixed discriminant Δ. This can be achieved by means of Theorem 1.1.13 which in particular implies that, if we define T_Δ as the set of triples of integers (a, b, c) such that

$$\begin{aligned} &\gcd(a,b,c) = 1, \qquad\qquad \Delta = b^2 - 4ac \\ &\text{either} \quad -a < b \leq a < c \quad \text{or} \quad 0 \leq b \leq a = c. \end{aligned}$$

then the set

$$\{\tau_1, \dots, \tau_m\} = \left\{ \frac{b + \sqrt{\Delta}}{2a} : (a,b,c) \in T_\Delta \right\}$$

is precisely equal to the set of complex numbers τ in $\mathcal{F}$ such that $j(\tau)$ is a singular modulus of discriminant Δ. In this setting $m = C_\Delta$ and the number $C_{\Delta,\varepsilon}$ is precisely the number of triples $(a, b, c) \in T_\Delta$ such that $\tau = \tau(a, b, c)$ satisfies $\min\{|\tau - \zeta_6|, |\tau - \zeta_3|\} < \varepsilon\}$.

By using the explicit description above, the authors manage to prove that

$$C_{\Delta,\varepsilon} \leq |\Delta|^{\frac{1}{2}+o(1)} \cdot \varepsilon + |\Delta|^{o(1)}. \tag{2.5}$$

Combining this estimate with the inequality (2.4) and optimizing ε, they deduce that the height of a singular modulus x of discriminant Δ is effectively bounded by

$$h(x) \ll \frac{|\Delta|^{o(1)}}{C_\Delta} + \log\frac{|\Delta|^{\frac{1}{2}}}{C_\Delta} + o(\log|\Delta|) \tag{2.6}$$

all the implicit constants being explicitly computable. This removes the ineffectivity of the upper bound that was present in Habegger's proof.

As far as the lower bounds for $h(x)$ are concerned, the authors prove the following two inequalities:

(HL) $h(x) \geq \frac{3}{\sqrt{5}} \log|\Delta| - 9.79.$

(EL) $h(x) \geq \frac{\pi|\Delta|^{\frac{1}{2}} - 0.01}{C_\Delta}.$

The first estimate is an improvement of inequality (2.2), improvement needed due to numerical purposes. The second estimate follows essentially from the definition of Weil height and from the explicit description of singular moduli seen above.

By combining (2.6)+(HL) when C_Δ is big, while using (2.6)+(EL) when C_Δ is small, the authors conclude that, if a singular unit exists, its discriminant must be bounded by $|\Delta| < 10^{15}$. However, this bound is still too big to allow numerical computations and for this reason the rest of the proof is dedicated to its refinement. First, the range $10^{10} \leq |\Delta| < 10^{15}$ is ruled out by sharpening estimate (2.5) on $C_{\Delta,\varepsilon}$; the techniques used in this step are a combination of analytic number theory and numerical computations. The range $|\Delta| < 10^{10}$ is then studied by further computer-assisted arguments. The conclusion is that singular units do not exist.

2.1.3 Singular S-units and effectivity problems

Theorem 2.1.2 opened the way to a number of interesting questions. For instance one may ask, inspired by the work of Gross-Zagier [GZ85] and Lauter-Viray [LV15], whether there exist pairs $j_1, j_2 \in \overline{\mathbb{Q}}$ of singular moduli whose difference is a unit. After noticing that $j_1 - j_2 = \Phi_1(j_1, j_2)$, where $\Phi_N(X, Y) \in \mathbb{Z}[X, Y]$ denotes the classical modular polynomial of level $N \in \mathbb{N}_{>0}$, one may push this question a bit further.

Question 2.1.3. *Are there finitely many pairs of singular moduli (j_1, j_2) such that $\Phi_N(j_1, j_2)$ is a unit for some $N \in \mathbb{N}_{>0}$?*

We remark that Question 2.1.3 makes sense, since the classical modular polynomials always have integer coefficients, so that $\Phi_N(j_1, j_2)$ is an algebraic integer for every pair of singular moduli (j_1, j_2) and for every level $N \in \mathbb{N}_{>0}$. If we fix $j_2 = 0$ and $N = 1$, we recover the problem of singular units considered in the previous section. A complete answer to Question 2.1.3 has been very recently found by Li in [Li21], where he proves the following generalization of Theorem 2.1.2.

Theorem 2.1.4. *For every pair (j_1, j_2) of singular moduli and every $N \in \mathbb{N}_{>0}$, the algebraic integer $\Phi_N(j_1, j_2)$ is not a unit.*

The tools used by Li in the proof of Theorem 2.1.4 come into the frame of the so-called *Kudla program*, and are very different from the ones used by Bilu, Habegger and Kühne in [BHK20].

Question 2.1.3 could be reformulated by asking whether there exist only finitely many pairs of singular moduli (j_1, j_2) such that the norm of $\Phi_N(j_1, j_2)$ is not divisible by any rational prime. Being phrased in this way, one may also wonder what happens if we relax a bit our requirements by asking the norm of $\Phi_N(j_1, j_2)$ to be divisible only by a fixed set S of primes. This leads us to consider the problem of singular S-units.

Recall that if K is a number field and S is a set of rational primes, we say that an element $x \in K$ is an *S-unit* if, for every prime $p \notin S$ and for every prime $\mathfrak{p}$ of K lying over p, the element x is a unit in the ring of integers of $K_\mathfrak{p}$, where $K_\mathfrak{p}$ denotes the completion of K at the prime $\mathfrak{p}$. In other words x is an S-unit if and only if $x \neq 0$ and all the primes appearing in the prime ideal factorization of xO_K lie above primes in S. If x is an algebraic integer, this is equivalent to requiring that all the primes dividing its absolute norm over $\mathbb{Q}$ are in S. Hence, the last question above can be rephrased as follows:

Question 2.1.5. *Let S be a fixed set of rational primes (not necessarily finite). Are there finitely many pairs of singular moduli (j_1, j_2) such that $\Phi_N(j_1, j_2)$ is an S-unit for some $N \in \mathbb{N}_{>0}$?*

Clearly the answer to Question 2.1.5 depends on the chosen set S. If we take S to be the set of all rational primes, this answer is trivially no. Less trivially, Theorem 2.1.4 shows that for $S = \emptyset$ there are no such pairs at all. However, for different choices of the set S, it is not clear *a priori* what the answer to Question 2.1.5 should be. We will show in Proposition 2.2.10 that if S has a finite complement in the set of all rational primes, then there exist infinitely many pairs of singular moduli (j_1, j_2) such that $\Phi_N(j_1, j_2)$ is an S-unit for some $N \in \mathbb{N}_{>0}$. In all the remaining cases however, the problem is completely open.

To simplify a bit the setting, let us restrict to the case $N = 1$ and j_2 fixed. If for instance $j_2 = 0$, we are looking for the number of singular moduli that are S-units, or, in short, for the number of *singular S-units*. By Theorem 2.1.2, if $S = \emptyset$ there is no singular S-unit. However, if $S \neq \emptyset$ there can certainly exist singular moduli that are S-units. For instance, for $S = \{2, 3\}$, the integers $12^3, -32^3$ and -96^3 are three singular moduli that are $\{2, 3\}$-units (they are the j-invariants of elliptic curves having complex multiplication by $\mathbb{Z}[\sqrt{-1}], \mathbb{Z}[\frac{1+\sqrt{-11}}{2}]$ and $\mathbb{Z}[\frac{1+\sqrt{-19}}{2}]$ respectively). We are then looking for some finiteness statement that will in general depend on the choice of the set S. Very recently Herrero, Menares and Rivera-Letelier proved in [HMR21b] that for every fixed singular modulus $j_0 \in \overline{\mathbb{Q}}$ and for every finite set of primes S, the set of singular moduli j such that $j - j_0$ is an S-unit is finite. Their argument follows the lines of Habegger's proof outlined in Section 2.1.1, but they replace the use of Duke's equidistribution of Heegener points [Duk88] by the use of analogous equidistribution statements in the p-adic setting, proved by the authors themselves in [HMR20] and [HMR21a]. In particular, as in [Hab15], their argument is not effective. We have reached the fundamental question of this entire chapter: is it possible, for some non-empty sets of primes S and for some fixed singular moduli j_0, to give an explicit bound on the number of singular moduli j for which $j - j_0$ is an S-unit? In the second part of the chapter we are going to answer positively to this question for infinitely many choices of S and j_0.

2.1.4 A connection with abelian varieties

The problems described so far have interesting analogues in the world of abelian varieties. Or, we should rather say, the problem of singular differences that are S-units could be considered as the modular analogue of certain integrality questions previously asked in the context of abelian varieties and algebraic groups in general. An example is probably the best way to highlight this connection.

Assume that E is an elliptic curve defined over a number field K and given by an integral Weierstrass model

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

with $a_i \in O_K$. Fix a point $Q \in E(\overline{K})$ and a finite set S of non-archimedean primes of K containing the primes of bad reduction for E. Notice that for every prime $\mathfrak{p} \subseteq \overline{K}$ not lying above primes in S the reduction of Q modulo $\mathfrak{p}$ will be a torsion point on the reduced elliptic curve E mod $\mathfrak{p}$. We then ask the following question: how many torsion points $P \in E(\overline{K})_{\text{tors}}$ do not have the same reduction as Q modulo all the prime ideals $\mathfrak{p} \subseteq \overline{K}$, except possibly for primes above S? This question has a more captivating (and shorter) formulation as follows.

Question 2.1.6. *How many torsion points in $E(\overline{K})$ are S-integral with respect to Q?*

There is a very laconic answer to this question: it depends on Q.

- Suppose first that $Q = O \in E(\overline{K})_{\mathrm{tors}}$ is the zero element in E. By Cassels' generalization of Nagell-Lutz Theorem [Sil09, VII, Theorem 7.1] every torsion point whose order is not a prime power has coordinates that are algebraic integers. Hence for any set S of primes as above there are infinitely many $P \in E(\overline{K})_{\mathrm{tors}}$ that are S-integral with respect to O.

- Let now $Q \in E(\overline{K})_{\mathrm{tors}}$ with order $N \geq 2$ and let again S be any set of primes of K containing the places of bad reduction for E. Then, for every $P \in E(\overline{K})_{\mathrm{tors}}$ of order M coprime with N and every prime ideal $\mathfrak{p} \subseteq \overline{K}$ not lying above S, we have $P \equiv Q \bmod \mathfrak{p}$ if and only if $P \equiv Q \equiv O \bmod \mathfrak{p}$. However, since $\gcd(M, N) = 1$, by [Sil09, VII, Proposition 3.1 (b)] at most one among P and Q can reduce to O modulo $\mathfrak{p}$. This shows once again that there are infinitely many $P \in E(\overline{K})_{\mathrm{tors}}$ that are S-integral with respect to Q.

- If finally $Q \notin E(\overline{K})_{\mathrm{tors}}$ answering Question 2.1.6 requires much more work than the previous two cases: it is a theorem of Baker, Rumely and Ih [BIR08, Theorem 0.2] that, under this assumption, for every finite set S of non-archimedean primes of K containing the places of bad reduction for E there are finitely many torsion points that are S-integral with respect to Q.

Motivated by results of this nature, Ih proposed the following conjecture (see [BIR08, Conjecture 3.2]).

Conjecture 2.1.7. *Let $A_{/K}$ be an abelian variety, S a finite set of non-archimedean primes of K and let $\mathcal{A}_S \longrightarrow \operatorname{Spec}(\mathcal{O}_{K,S})$ be a model for A over the ring of S-integers of K. Fix D a non-zero effective divisor on A defined over $\overline{K}$, at least one of whose irreducible components is not the translate of an abelian subvariety by a torsion point, and let $Cl(D)$ be its Zariski closure in $\mathcal{A}_S$. Then the set of torsion points $P \in A(\overline{K})^{tors}$ whose closure in $\mathcal{A}_S$ is disjoint from $Cl(D)$ is not Zariski dense in A.*

In the theory of Unlikely Intersections, torsion points on abelian varieties are also called *special points*. This is because abelian varieties are special types of Shimura varieties, where a precise notion of special points can be defined. The latter specializes exactly to the notion of torsion points when our Shimura variety is also an abelian variety. One now notices that modular curves are also particular instances of Shimura varieties, and in this context special point is a synonym for CM point. If we try to rewrite our example above with the elliptic curve E replaced by the simplest modular curve $X(1)$, something familiar makes it appearance. Namely, if we consider as a model for $X(1)$ the projective line $\mathbb{P}^1_{\mathbb{Q}}$, so that special points correspond to j-invariants of CM elliptic curves over $\overline{\mathbb{Q}}$ (singular moduli!) then the analogue of Question 2.1.6 becomes the following: for a finite set S of rational primes and a given $x \in \mathbb{P}^1_{\mathbb{Q}}(\overline{\mathbb{Q}})$ are there finitely many singular moduli j such that $j - x$ is an S-unit? The "torsion counterexamples" given in the elliptic curve case would correspond to choosing x to be itself a singular modulus. And all the discussion developed in the previous sections shows that these choices are not sources of counterexamples anymore! In other words, it is true that the problem of singular differences that are S-units could be regarded as the modular analogue of the integrality problems addressed in [BIR08], but the solutions in these two cases do not need to be necessarily the same. It is nevertheless very likely that a modular analogue of Ih's conjecture could hold also in this case. In this direction, Schmid [Sch] proved that for every non-CM point $x \in \mathbb{P}^1_{\mathbb{Q}}(\overline{\mathbb{Q}})$, the set of singular moduli j for which $j - x$ is a unit is finite. A similar statement with $S \neq \emptyset$ does not seem to appear in the literature yet.

2.2 Finiteness statements for infinite S

In this section we begin our study of S-units of the form $j - j_0$ with $j, j_0 \in \overline{\mathbb{Q}}$ singular moduli. If $j_0 = 0$ is the unique singular modulus of discriminant $\Delta = -3$, we speak of *singular S-units*. For ease of notation, for every algebraic number $\alpha \in \overline{\mathbb{Q}}$ we will denote by $N(\alpha)$ the absolute norm $N_{\mathbb{Q}(\alpha)/\mathbb{Q}}(\alpha)$. The following theorem is the main result of this section.

Theorem 2.2.1. *Let j_0 be a singular modulus of discriminant Δ_0 and let $K := \mathbb{Q}(\sqrt{\Delta_0})$. Fix S_0 to be the set of rational primes that are split in K. If $\{2, 3, 5, 7\} \not\subseteq S_0$, then for every singular modulus $j \in \overline{\mathbb{Q}}$ the difference $j - j_0$ is never an S_0-unit.*

Note that the sets S_0 considered in the statement above are infinite, so that even an effective version of [HMR21b] would not be able to recover the result. To prove the theorem, we need the following auxiliary lemma.

Lemma 2.2.2. *Let $\mathcal{O}_1$ and $\mathcal{O}_2$ be orders in imaginary quadratic fields K_1 and K_2 of conductors f_1, f_2 respectively. For $i \in \{1, 2\}$ let j_i be a singular modulus relative to the order $\mathcal{O}_i$ and assume that $j_1 \neq j_2$. Suppose that L is a number field containing j_1 and j_2, and let $\mathfrak{p}$ be a prime of L lying over a rational prime p. For $i \in \{1, 2\}$ write $f_i = f_i' p^{n_i}$ with $p \nmid f_i'$. If $j_1 \equiv j_2 \bmod \mathfrak{p}$ then either $K_1 = K_2$ and p divides $f_1 f_2$ or p is non-split (inert/ramified) in K_1 and K_2. Moreover, in the first case we have $f_1' = f_2'$.*

Proof. For $i = 1, 2$ let E_i be an elliptic curve defined over L with complex multiplication by $\mathcal{O}_i$ and j-invariant j_i. After base-changing to a finite field extension, we can assume without loss of generality that the elliptic curves E_i have good reduction at $\mathfrak{p}$ and that all their endomorhisms are defined over the base field. The hypothesis $j_1 \equiv j_2 \bmod \mathfrak{p}$ then implies that the reduced elliptic curves $\widetilde{E}_1$ and $\widetilde{E}_2$ are isomorphic over $\overline{\mathbb{F}}_p$. In particular their endomorphism rings over $\overline{\mathbb{F}}_p$ must be isomorphic. By Theorem 1.4.1 these rings are either both isomorphic to an order in a quaternion algebra or to an order in an imaginary quadratic field. In the first case, p is non-split in K_1 and in K_2. In the second case, p splits in both K_1 and K_2, and we have

$$\operatorname{End}_{\overline{\mathbb{F}}_p}(\widetilde{E}_i) \cong \mathbb{Z} + f_i' \mathcal{O}_{K_i} \qquad \text{for } i = 1, 2$$

where $\mathcal{O}_{K_i}$ is the ring of integers of the field K_i. Since the two endomorphism rings must be isomorphic, we must have $K_1 = K_2$ and $f_1' = f_2'$. If p divides one among f_1 and f_2 we are done. Suppose on the contrary that $p \nmid f_1 f_2$; then, by the discussion above, we have $f_1 = f_2$. But then j_1 and j_2 cannot be congruent modulo $\mathfrak{p}$ by Theorem 1.4.2. This contradiction concludes the proof. □

Proof of Theorem 2.2.1. Let $j \in \overline{\mathbb{Q}}$ be a singular modulus such that $j - j_0$ is an S_0-unit. We are going to prove that this difference is in fact a unit. The result will then follow from a direct application of Theorem 2.1.4.

Assume then by contradiction that $p \in S_0$ divides the absolute norm $N(j - j_0)$. In particular, there exists a prime $\mathfrak{p} \subseteq \overline{\mathbb{Q}}$ lying above p such that $j \equiv j_0 \bmod \mathfrak{p}$. Since p is split in K, by Lemma 2.2.2 this implies that the order $\mathcal{O}_j$ relative to the singular modulus j is contained in K. Now, we know that at least one among $2, 3, 5, 7$ does not belong to S_0, say ℓ. Choose a number field L and two elliptic curves $E_{j/L}$ and $E_{0/L}$ with singular invariants j and j_0 respectively, such that there exists a prime $\mathfrak{l} \subseteq L$ above ℓ which is of good reduction for both the curves. Since ℓ is non-split in K, the reduced elliptic curves $E_j \bmod \mathfrak{l}$ and $E_0 \bmod \mathfrak{l}$ are both supersingular by Theorem 1.4.1.

But there exists only one isomorphism class $[E_\ell]_{\overline{\mathbb{F}}_\ell}$ of supersingular elliptic curves over $\overline{\mathbb{F}}_\ell$. More precisely, we can choose

$$E_2 : y^2 + y = x^3, \quad E_3 : y^2 = x^3 + x, \quad E_5 : y^2 = x^3 + 1, \quad E_7 : y^2 = x^3 + x.$$

as representatives for these classes for the different values of the prime ℓ. In particular, the two elliptic curves $E_j \bmod \mathfrak{l}$ and $E_0 \bmod \mathfrak{l}$ must be isomorphic over $\overline{\mathbb{F}}_\ell$, so that $j \equiv j_0 \bmod \mathfrak{l}$. We deduce that ℓ divides the norm of any difference $j - j_0$ for j singular modulus relative to an order in K. Hence, these differences cannot be S_0-units. This contradiction shows that $j - j_0$ is an algebraic unit, as we wanted to show. □

By specializing j_0 in Theorem 2.2.1, one can get several different results concerning singular differences that are S-units. For instance, for $j_0 = 0$ we obtain the following result.

Corollary 2.2.3. *Let S be the set of primes congruent to 1 modulo 3. Then no singular modulus is an S-unit.*

Proof. This is an immediate consequence of Theorem 2.2.1, where we take $j_0 = 0$. Notice that the set S consists precisely of the primes splitting in $K = \mathbb{Q}(\sqrt{-3})$ and does not contain any of the primes $2, 3, 5$. □

Remark 2.2.4. Primes congruent to 1 mod 3 do appear in the norm factorizations of singular moduli. More precisely, the techniques used in the proof of Theorem 2.2.1 yield the following statement: a prime $\ell \equiv 1 \bmod 3$ divides the norm of a singular modulus j if and only if j is a singular modulus relative to an order of discriminant $-3\ell^{2n}$ for some $n \in \mathbb{N}$. Moreover, in this case ℓ is the only prime 1 mod 3 that divides the norm of j. The exact power of ℓ that divides this norm will be studied in Section 2.3.

In the same way, taking $j_0 = 1728$ in Theorem 2.2.1, we have the following corollary.

Corollary 2.2.5. *Let S be the set of primes congruent to 1 modulo 4. Then for every singular modulus $j \in \overline{\mathbb{Q}}$ the difference $j - 1728$ is not an S-unit.*

Similar statements can be made for every singular difference $j - j_0$ with j_0 singular modulus of class number 1, since for these there is always at least one prime among $2, 3, 5, 7$ which is non-split in the corresponding imaginary quadratic field.

One may be tempted to think that Theorem 2.2.1 holds without any assumption on the set of split primes S_0. It is very difficult to test this numerically, since the first imaginary quadratic field where $2, 3, 5, 7$ are all split has discriminant $\Delta_K = -311$, with corresponding Hilbert class polynomial having degree 19 and huge coefficients. We have here managed to prove a weaker result, thus providing some evidence for the stronger claim. In order to state it, let us define for every pair of negative discriminants $\Delta_1, \Delta_2 \in \mathbb{Z}_{<0}$ the quantity

$$J(\Delta_1, \Delta_2) = \prod_{\operatorname{disc} j_i = \Delta_i} (j_1 - j_2).$$

Note that $J(\Delta_1, \Delta_2) \in \mathbb{Z}$ for every pair of discriminants Δ_1, Δ_2.

Theorem 2.2.6. *Let $\Delta_0 \in \mathbb{Z}_{<0}$ be the discriminant of an imaginary quadratic order and let $K := \mathbb{Q}(\sqrt{\Delta_0})$. Fix S_0 to be the set of rational primes that are split in K. Then there are only finitely many discriminants $\Delta \in \mathbb{Z}_{<0}$ such that $J(\Delta, \Delta_0)$ is an S_0-unit.*

Proof. Let $\Delta \in \mathbb{Z}_{<0}$ be a discriminant such that $J(\Delta, \Delta_0)$ is an S_0-unit. Let $\mathcal{O}_\Delta$ and $\mathcal{O}_{\Delta_0}$ be the orders of discriminant Δ and Δ_0 and denote by f_Δ and f_{Δ_0} the corresponding conductors.

First of all, note that $J(\Delta, \Delta_0)$ cannot be an algebraic unit. Indeed, for every pair j, j_0 of singular moduli of discriminants Δ, Δ_0 respectively, we have $N(j - j_0) \mid J(\Delta, \Delta_0)$ and $N(j - j_0) \neq \pm 1$ by Theorem 2.1.4. This argument also implies, using Lemma 2.2.2, that $\mathcal{O}_\Delta \subseteq K$ and that there exist $\ell \in S_0$ and $m, n, f \in \mathbb{N}$ with $\ell \nmid f$ such that $f_\Delta = \ell^m f$ and $f_{\Delta_0} = \ell^n f$. Therefore we see that the order $\mathcal{O}_\Delta$ belongs to the set $\mathcal{A}$ of orders in K whose conductors are of the form $c = q^k f$ for some $q \in S_0$ and $k \in \mathbb{N}$. Fix now $p \in \mathbb{N}$ to be an odd prime that is inert in K and does not divide f_{Δ_0}. We claim that for all but finitely many orders $\mathcal{O} \in \mathcal{A}$ of discriminant $\Delta(\mathcal{O})$ we have $p \mid J(\Delta(\mathcal{O}), \Delta_0)$. This claim clearly implies the theorem.

Choose a prime $\mathfrak{p} \subseteq \overline{\mathbb{Q}}$ lying above p. By Theorem 1.4.4, applied with the choice of any two odd primes $q_1, q_2 \in \mathbb{N}$ splitting in K, we see that the supersingular reduction map $\Psi_{\mathfrak{p},\mathcal{O}}$ in (1.5) is surjective for all orders $\mathcal{O} \subseteq K$ whose discriminant is large enough and coprime with p. In particular, $\Psi_{\mathfrak{p},\mathcal{O}}$ is surjective for all but finitely many orders $\mathcal{O} \in \mathcal{A}$. Since any elliptic curve $E_{0/\overline{\mathbb{Q}}}$ with complex multiplication by $\mathcal{O}_{\Delta_0}$ has supersingular reduction modulo $\mathfrak{p}$, we deduce that for all the orders $\mathcal{O} \in \mathcal{A}$ for which $\Psi_{\mathfrak{p},\mathcal{O}}$ is surjective, there exists at least one singular modulus j relative to $\mathcal{O}$ such that $\Psi_{\mathfrak{p},\mathcal{O}}(j) \in \mathrm{Im}(\Psi_{\mathfrak{p},\mathcal{O}_{\Delta_0}})$. Hence, there exists a singular modulus j_0 of discriminant Δ_0 such that $j \equiv j_0 \bmod \mathfrak{p}$. This in particular implies that p divides $N(j - j_0)$, which in turn is a divisor of $J(\Delta(\mathcal{O}), \Delta_0)$. The claim is thus proved. □

In the spirit of the arguments used in Theorems 2.2.1 and 2.2.6, we now give some remarks on singular S-units. As we mentioned in Section 2.1.3 Herrero, Menares and Rivera-Letelier recently proved [HMR21b] that, for every finite set of primes S, there are at most finitely many singular S-units. The proof of this result appears very deep, and relies on some p-adic equidistribution theorems proved in [HMR20] and [HMR21a]. We give here a much weaker statement than the one mentioned above, which however uses only elementary reduction theory for CM elliptic curves and was obtained before [HMR21b] was made publicly available. Proposition 2.2.7 can be considered as a weak converse to Theorem 2.1.2.

Proposition 2.2.7. *Let $S = \{p_1, ..., p_n\}$ be a finite set of rational primes. Then there exist infinitely many singular moduli of fundamental discriminant that are not S-units.*

Proof. We know by Theorem 2.1.2 that no singular modulus is a unit. In particular there is always a rational prime that divides the norm of any singular modulus. If j is a singular modulus of fundamental discriminant $-D < -3$ and p divides $N_{\mathbb{Q}(j)/\mathbb{Q}}(j)$, then by Lemma 2.2.2 the prime p cannot split in $\mathbb{Q}(\sqrt{-D})$. The idea for the proof of the proposition is then to find infinitely many fundamental discriminants $-D$ such that all the primes in S split in $\mathbb{Q}(\sqrt{-D})$. In this way the set of primes dividing the norm of any singular modulus of discriminant $-D$ (this set is nonempty by the above discussion) has trivial intersection with S.

Let q be a prime number such that

- $q \equiv -1 \bmod p_i$ for every $p_i \in S$.
- $q \equiv -1 \bmod 8$.

We know that there are infinitely many primes satisfying these conditions by Dirichlet's theorem on primes in arithmetic progression and the Chinese reminder theorem. We claim that in $\mathbb{Q}(\sqrt{-q})$ all the primes of S are split. First of all notice that $\mathrm{disc}\, \mathbb{Q}(\sqrt{-q}) = -q$ because clearly q is squarefree and $-q \equiv 1 \mod 4$ by assumption. To prove that every prime in S splits in this field we compute the Kronecker symbols $(-q/p_i)$. We have two cases:

- If $p_i = 2$ for some i then $\left(\frac{-q}{2}\right) = 1$ because $-q \equiv 1 \mod 8$.

- If $p_i > 2$ then
$$\left(\frac{-q}{p_i}\right) = \left(\frac{-1}{p_i}\right)\left(\frac{q}{p_i}\right) = (-1)^{\frac{p_i-1}{2}} \cdot \left(\frac{q}{p_i}\right) = (-1)^{\frac{p_i-1}{2}} \cdot \left(\frac{-1}{p_i}\right) = 1$$
because $(-1/p_i) = (-1)^{\frac{p_i-1}{2}}$ for every odd prime p_i.

Since the Kronecker symbols above are equal to 1, we deduce that all the primes in S are split in $\mathbb{Q}(\sqrt{-q})$. This proves the proposition. □

Remark 2.2.8. Using the same strategy, one can actually prove that for every finite set S of rational primes there exist a positive proportion of negative fundamental discriminants whose corresponding singular moduli are not S-units. Here is a sketch of the argument: as explained in the proof of Proposition 2.2.7, it suffices to consider the set of fundamental discriminants $-D$ for which every prime in S is split in $\mathbb{Q}(\sqrt{-D})$. The map $d \mapsto \mathbb{Q}(\sqrt{-d})$ gives a bijection between the set of squarefree positive integers and the set of imaginary quadratic fields. Under this bijection, the imaginary quadratic fields where every prime in S splits correspond to the squarefree integers d such that the equality of Kronecker symbols $(d/p) = (-1/p) = (-1)^{\frac{p-1}{2}}$ holds for all odd $p \in S$ and satisfying $d \equiv 7 \bmod 8$ if $2 \in S$. We are then reduced to find the proportion δ_S of all the positive squarefree numbers d satisfying these congruence conditions. By the Chinese Reminder Theorem, this is equivalent to studying the asymptotic distribution of squarefree numbers in the residue classes mod $N := 4 \cdot \prod_{p \in S} p$.

For $a, k \in \mathbb{N}$ we denote by $Q(x; a, k)$ the number of squarefree positive integers $d \leq x$ such that $d \equiv a \bmod k$. The study of the asymptotic behaviour of the function $Q(x; a, k)$ dates back to Landau [Lan53, pp. 633-636]. An equivalent formulation of his results is given in [Sch62, Lemma 8], which in particular yields
$$Q(x; a, k) \sim \frac{6}{\pi^2} x \cdot \delta(a, k) \qquad \text{as } x \longrightarrow \infty,$$
where
$$\delta(a,k) := \frac{1}{k} \prod_{p \mid k} \frac{1}{1-p^{-2}} \cdot \prod_{\substack{p \mid (a,k), \\ (p^2,k) \mid a}} \left(1 - \frac{(p^2,k)}{p^2}\right). \tag{2.7}$$

In the above formula p always denotes a prime number and for every pair of integers $u, v \in \mathbb{Z}$ we have set $(u, v) := \gcd(u, v)$. Since the natural density of the set of squarefree positive integers is $6/\pi^2$ (see [MV07, Theorem 2.2 pag. 36]) the number $\delta(a, k)$ in (2.7) represents the proportion of squarefree positive integers $d \equiv a \bmod k$. Notice that for every $a \in \mathbb{N}$ the arithmetic function $\delta(a, \cdot)$ is multiplicative. Moreover, one has
$$\begin{aligned} \delta(a,p) &= \frac{p}{p^2-1} \quad \text{for all } p \neq 2 \text{ and } p \nmid a, \\ \delta(a,8) &= \frac{1}{6} \quad \text{for all } a \not\equiv 0, 4 \bmod 8 \end{aligned}$$

and from this it is easy to deduce that $\delta_S = \prod_{p\in S} \delta_{S,p}$ with

$$\delta_{S,p} = \frac{p}{2p+2} \quad \text{if } p \neq 2, \qquad \delta_{S,2} = \frac{1}{6}.$$

In particular $\delta_S > 0$, as we wanted to show.

Remark 2.2.9. If S does not contain the primes $2, 3$ or 5, Proposition 2.2.7 could be proved by considering imaginary quadratic fields where these primes do not split. For instance, if $2 \notin S$ we may consider the fundamental discriminants $-D \equiv 0 \mod 4$: then 2 ramifies inside $\mathbb{Q}(\sqrt{-D})$ and by Theorem 1.4.1 it is a prime of supersingular reduction for any elliptic curve with complex multiplication by the ring of integers in $\mathbb{Q}(\sqrt{-D})$. Since 0 is the only supersingular j-invariant modulo 2, we deduce that singular moduli of discriminant D cannot be S-units.

We now prove a statement "dual" to Proposition 2.2.7, with which we also fulfill our promise of answering Question 2.1.5 in the case S has infinite complement in the set of all rational primes.

Proposition 2.2.10. *Let S be a set of rational primes that has finite complement in the set of all primes. Then there are infinitely many pairs (j_1, j_2) of singular moduli such that $\Phi_N(j_1, j_2)$ is an S-unit for some $N \in \mathbb{N}$.*

Proof. We will prove the stronger statement that there are infinitely many pairs (j_1, j_2) of singular moduli such that $\Phi_1(j_1, j_2) = j_1 - j_2$ is an S-unit. Let $\{p_1, ..., p_n\}$ be the complement of S in the set of all rational primes. An application of Dirichlet's theorem on primes in arithmetic progression similar to the one appearing in the proof of Proposition 2.2.7 shows that there exists an imaginary quadratic field K where $p_1, ..., p_n$ are all split. Let $j_1 \in \overline{\mathbb{Q}}$ be a singular modulus relative to the maximal order $\mathcal{O}_K$ in K. Then we claim that for every singular modulus j_2 relative to an order $\mathcal{O} \not\subseteq K$ the difference $j_1 - j_2$ is an S-unit. To see this, it suffices to show that no prime in the set $\{p_1, ..., p_n\}$ divides the norm $N(j_1 - j_2)$, and this in turn follows from the techniques that have been extensively used in this section. Let us be more precise: suppose by contradiction that $p = p_i$ divides $N(j_1 - j_2)$ for some $i = 1, ..., n$. By Theorem 1.3.5 there exists a number field F, a prime $\mathfrak{p} \subseteq F$ lying above p and two elliptic curves $(E_1)_{/F}$ and $(E_2)_{/F}$ such that the following holds: the elliptic curves E_1, E_2 have j-invariants j_1, j_2 respectively and have good, geometrically isomorphic reduction at $\mathfrak{p}$. Since p splits in K, the reduction $E_1 \bmod \mathfrak{p}$ is ordinary and its geometric endomorphism ring is isomorphic to $\mathcal{O}_K$ by Theorem 1.4.1. On the other hand, $E_1 \bmod \mathfrak{p}$ and $E_2 \bmod \mathfrak{p}$ are isomorphic over $\overline{\mathbb{F}}_p$, and we deduce that E_2 has ordinary reduction modulo $\mathfrak{p}$ with geometric endomorphism ring isomorphic to $\mathcal{O}_K$. However, since we are assuming that E_2 has complex multiplication by an order not contained in K, this contradicts Theorem 1.4.1 and we are done. □

2.3 Norms of singular moduli and primes 1 mod 3

We have seen in Remark 2.2.4 that a prime $p \equiv 1 \bmod 3$ divides the absolute norm of a singular modulus j if and only if j is relative to a CM order $\mathcal{O} \subseteq \mathbb{Q}(\sqrt{-3})$ with conductor a power of p. For instance, for $p \in \{7, 13, 19\}$ we have:

$$|N(j_{-3\cdot 7^2})| = 2^{30} \cdot 3^9 \cdot 5^6 \cdot 7 \cdot 17^3$$
$$|N(j_{-3\cdot 13^2})| = 2^{66} \cdot 3^{21} \cdot 5^{12} \cdot 11^6 \cdot 13 \cdot 23^3$$
$$|N(j_{-3\cdot 19^2})| = 2^{93} \cdot 3^{27} \cdot 5^{18} \cdot 11^6 \cdot 19 \cdot 29^6 \cdot 41^3 \cdot 53^3$$

where j_Δ is any singular modulus of discriminant Δ and, as in the previous section, $N(\cdot)$ denotes the absolute norm of an algebraic number. The attentive reader has certainly noticed that in the above factorizations the prime p always appears with exponent 1. This does not seem a coincidence, and, actually, it is not even a phenomenon involving only primes 1 mod 3. Indeed, by taking $p = 5$ we get the following norms:

$$\begin{aligned}
|N(j_{-3\cdot 5^2})| &= 2^{30} \cdot 3^6 \cdot 5 \cdot 11^3 \\
|N(j_{-3\cdot 5^4})| &= 2^{156} \cdot 3^{48} \cdot 5 \cdot 11^9 \cdot 17^6 \cdot 23^6 \cdot 47^6 \cdot 59^3 \cdot 71^3 \\
|N(j_{-3\cdot 5^6})| &= 2^{810} \cdot 3^{150} \cdot 5 \cdot 11^{54} \cdot 17^{48} \cdot 23^{24} \cdot 29^{30} \cdot 41^{18} \cdot 53^{12} \cdot 59^{12} \cdot 71^{18} \cdot 83^{12} \cdot 89^{12} \cdot 107^6 \cdot 113^6 \\
&\quad \cdot 131^6 \cdot 167^6 \cdot 179^9 \cdot 227^6 \cdot 251^6 \cdot 263^6 \cdot 311^3 \cdot 347^6 \cdot 359^3
\end{aligned}$$

and we see that 5 again appears with exponent 1 in these factorizations. Similar computations with orders of conductor $f = p^n$ for different odd primes $p \in \mathbb{N}$ show the same pattern. If $p = 2$ a different regularity can be observed:

$$\begin{aligned}
|N(j_{-3\cdot 2^2})| &= 2^4 \cdot 3^3 \cdot 5^3 \\
|N(j_{-3\cdot 2^4})| &= 2^4 \cdot 3^9 \cdot 5^6 \cdot 11^3 \\
|N(j_{-3\cdot 2^6})| &= 2^4 \cdot 3^{12} \cdot 5^{12} \cdot 11^6 \cdot 17^6 \cdot 23^3 \\
|N(j_{-3\cdot 2^8})| &= 2^4 \cdot 3^{42} \cdot 5^{24} \cdot 11^6 \cdot 17^6 \cdot 23^3 \cdot 29^6 \cdot 41^6 \cdot 47^3 \\
|N(j_{-3\cdot 2^{10}})| &= 2^4 \cdot 3^{48} \cdot 5^{48} \cdot 11^{24} \cdot 17^6 \cdot 23^{12} \cdot 29^{12} \cdot 47^9 \cdot 53^6 \cdot 59^6 \cdot 71^3 \cdot 83^6 \cdot 89^6.
\end{aligned}$$

Stimulated by these numerical figures, we decided to investigate further the norm factorizations of singular moduli relative to orders in $\mathbb{Q}(\sqrt{-3})$, even if this is only distantly related with the topic of singular S-units. Our main result confirms what the above computations only suggest.

Theorem 2.3.1. *Let j be a singular modulus of discriminant $\Delta = -3f^2$, i.e. a singular modulus relative to an order $\mathcal{O}_j \subseteq \mathbb{Q}(\sqrt{-3})$ of conductor f. Assume that $f = p^n$ is a perfect prime power with n a positive natural number.*

- *If $p \neq 3$ is odd then p divides exactly $N_{\mathbb{Q}(j)/\mathbb{Q}}(j)$.*
- *If $p = 2$ then 2^4 divides exactly $N_{\mathbb{Q}(j)/\mathbb{Q}}(j)$.*

Remark 2.3.2. We conjecture that if j is a singular modulus relative to an order $\mathcal{O}_j \subseteq \mathbb{Q}(\sqrt{-3})$ of conductor $f = 3^n$ with $n \in \mathbb{N}_{>0}$ then 3 divides exactly $N_{\mathbb{Q}(j)/\mathbb{Q}}(j)$. Our proof of Theorem 2.3.1 does not work in this case.

Proof. The proof of the theorem will rely on the formulas proved by Lauter and Viray in [LV15]. Following the same notation of their paper, set for n positive even

$$d_1 = -3,\ f_1 = 1,\ d_2 = -3p^{2n},\ f_2 = p^n$$

so that $j_2 = j$ is a singular modulus of discriminant d_2 and $j_1 = 0$ is the only singular modulus of discriminant d_1. Then

$$J(d_1, d_2) = \prod_{\operatorname{disc} j_i = d_i} (j_1 - j_2) = \pm N_{\mathbb{Q}(j)/\mathbb{Q}}(j)$$

since all the singular moduli of the same discriminant are conjugated. If now w_i denotes the number of units in the order $\mathcal{O}_{d_i}$ for $i = 1, 2$, then by our assumptions we have $w_1 = 6$ and $w_2 = 2$. By [LV15, Theorem 1.1] we get

$$|N_{\mathbb{Q}(j)/\mathbb{Q}}(j)|^{2/3} = \prod_{\substack{x^2 \leq 9p^{2n} \\ x^2 \equiv 9p^{2n} \bmod 4}} F\left(\frac{9p^{2n} - x^2}{4}\right) \tag{2.8}$$

where F is a function that takes non-negative integers of the form $\frac{9p^{2n}-x^2}{4}$ to possibly fractional prime powers. The precise definition of the function $F(\cdot)$ is somewhat involved and not needed for the proof of the theorem. For completeness of exposition, we decided however to incude it in the next paragraph. Our treatment follows closely the proof of [LV15, Theorem 1.1], where the function $F(\cdot)$ is defined.

Let $L/\mathbb{Q}$ be the minimal finite field extension containing $\mathbb{Q}(\sqrt{-3})$ with the property that, for every rational prime ℓ and every singular modulus j relative to the order $\mathcal{O}_j$, there exist elliptic curves E_0 and E_j defined over the ring of integers $\mathcal{O}_L$ such that $j(E_0) = 0$, $j(E_j) = j$ and which have good reduction at every prime $\mu \subseteq L$ above ℓ. Such an extension can always be found by [ST68, Sections 5 and 6]. For a fixed prime $\mu \subseteq L$ let L_μ^{unr} be the maximal unramified extension of the μ-completion of L and denote by $A \subseteq L_\mu^{\text{unr}}$ its ring of integers. Then for every $n \in \mathbb{N}$ and every isomorphism $f \in \operatorname{Iso}_{A/\mu^n}(E_0 \bmod \mu^n, E_j \bmod \mu^n)$ between the reduced elliptic curves mod μ^n, there is a canonical isomorphism of rings

$$\begin{aligned} i_f : \operatorname{End}_{A/\mu^n}(E_0 \bmod \mu^n) &\xrightarrow{\sim} \operatorname{End}_{A/\mu^n}(E_j \bmod \mu^n) \\ g &\mapsto f \circ g \circ f^{-1} \end{aligned}$$

which allows to write

$$\begin{tikzcd} \mathbb{Z}[\frac{1+\sqrt{-3}}{2}] \cong \operatorname{End}_A(E_0) \arrow[r, hook] & \operatorname{End}_{A/\mu^n}(E_0 \bmod \mu^n) \arrow[r, "i_f", "\sim"'] & \operatorname{End}_{A/\mu^n}(E_j \bmod \mu^n) \\ & & \mathcal{O}_j \cong \operatorname{End}_A(E_j) \arrow[u, hook] \end{tikzcd}$$

where the non-labelled inclusions are induced by the reductions mod μ^n. Let R_f be the order generated by the image of $\mathbb{Z}[\frac{1+\sqrt{-3}}{2}]$ and $\mathcal{O}_j$ in $\operatorname{End}_{A/\mu^n}(E_j \bmod \mu^n)$, and denote by D_f its discriminant. It is possible to prove that the discriminant D_f of the order R_f is of the form

$$D_f = \left(\frac{9p^{2n} - x^2}{4}\right)^2$$

for some $x \in \mathbb{Z}$ with $x^2 \leq 9p^{2n}$ and $x^2 \equiv 9p^{2n} \bmod 4$. Then for every prime ideal $\mu \subseteq L$ and every integer m of the form $\frac{9p^{2n}-x^2}{4}$ we define

$$N_{m,\mu} := \frac{1}{3C} \sum_j \sum_{n \geq 1} \#\{f \in \operatorname{Iso}_{A/\mu^n}(E_0 \bmod \mu^n, E_j \bmod \mu^n) : D_f = m^2\}$$

where the first sum is taken over all singular moduli j relative to the order $\mathcal{O}_j$ and $C \in \mathbb{Z}$ is such that $C = 1$ if $x = 0$ and $C = 2$ otherwise. We finally define

$$F(m) := \prod_{\mu \subseteq L} \mu^{N_{m,\mu}}$$

where the product is taken over all the prime ideals $\mu \subseteq L$. One can prove that, if $F(m)$ is non-trivial, there exists a unique rational prime ℓ such that $F(m)$ is supported only at prime ideals above ℓ. Since the conditions defining $F(m)$ are Galois invariant, one can consider $F(m)$ to be a fractional power of the prime ℓ.

Identity (2.8) shows that in order to understand the factorization of $N_{\mathbb{Q}(j)/\mathbb{Q}}(j)$ one should study the function $F\left(\frac{9p^{2n}-x^2}{4}\right)$ for different values of x. We begin by studying the case $x = \pm 3p^n$, *i.e.* the factorization of $F(0)$. We denote by $v_p(\cdot)$ the usual p-adic valuation. Then by the final part of [LV15, Theorem 1.5], since $f_1 = 1$ and $d_2 = d_1 p^{2n}$ we have

$$v_p(F(0)) = \frac{2}{6} \#\mathrm{Pic}(\mathcal{O}_{d_1}) = \frac{1}{3}$$

because $\mathbb{Z}[\frac{1+\sqrt{-3}}{2}]$ is a principal ideal domain. Combining this with (2.8) gives

$$|N_{\mathbb{Q}(j)/\mathbb{Q}}(j)|^{2/3} = p^{2/3} \cdot \prod_{\substack{x^2 < 9p^{2n} \\ x^2 \equiv 9p^{2n} \bmod 4}} F\left(\frac{9p^{2n} - x^2}{4}\right). \tag{2.9}$$

In what follows we will distinguish between the cases p odd and $p = 2$. In the first case we will have to prove that none of the factors appearing in the product on the right-hand side of (2.9) is a power of p. In the second case we shall prove that there are exactly two factors in the same product that are equal to 2.

Case 1: $p \neq 3$ odd. We are now supposing that $x \neq \pm 3p^n$, *i.e.* that $m = \frac{9p^{2n}-x^2}{4} > 0$. By the final part of [LV15, Theorem 1.1] we can have $v_p(F(m)) \neq 0$ only if p divides m. Hence we only have to study the values of $F(m)$ with $p \mid m$. By definition of m this implies that p divides x and we can then write $x = p^r k$, $0 < r \leq n$ (here we use the fact that p is odd), k coprime with p. Hence m can be factored as

$$m = \frac{9p^{2n} - k^2 p^{2r}}{4} = p^{2r} A, \qquad A = \frac{9p^{2(n-r)} - k^2}{4}.$$

Notice that p does not divide A.

By [LV15, Theorem 1.5] (which we can apply since $f_1 = 1$) we have that

$$v_p(F(m)) = \rho(m) \mathfrak{A}\left(\frac{m}{p^{1+n}}\right) \tag{2.10}$$

where $\rho(\cdot)$ and $\mathfrak{A}(\cdot)$ are two functions defined for every integer m, N as follows:

$$\rho(m) = \begin{cases} 0 & \text{if } (-3, -m)_3 = -1 \\ 1 & \text{if } 3 \nmid m \\ 2 & \text{otherwise} \end{cases}$$

$$\mathfrak{A}(N) = \#\left\{\mathfrak{A} \subseteq \mathbb{Z}\left[\frac{1+\sqrt{-3}}{2}\right] \text{ ideals} : N(\mathfrak{A}) = N\right\}.$$

where $(\cdot,\cdot)_3$ denotes the usual Hilbert symbol at 3. Notice that for a prime $\mathfrak{p} \subseteq \mathbb{Z}\left[\frac{1+\sqrt{-3}}{2}\right]$ we have

$$N_{\mathbb{Q}(\zeta_3)/\mathbb{Q}}(\mathfrak{p}) = \begin{cases} p & \text{if } \mathfrak{p} \text{ lies above a prime } p \equiv 1 \bmod 3 \text{ or } p = 3 \\ p^2 & \text{if } \mathfrak{p} \text{ lies above a prime } p \equiv 2 \bmod 3 \end{cases}$$

In particular, if N is a natural number in whose factorization appears a prime $p \equiv 2 \bmod 3$ raised to an odd power, there cannot be any ideal $\mathfrak{A}$ of $\mathbb{Q}(\zeta_3)$ of norm N, so $\mathfrak{A}(N) = 0$ in this case.

We now want to prove that $v_p(F(m)) = 0$ by showing that at least one among the two factors appearing in (2.10) is 0. We may assume that m/p^{1+n} is an integer, otherwise $\mathfrak{A}(m/p^{1+n}) = 0$. Write then $A = 3^\beta \tilde{A}$, with $3 \nmid \tilde{A}$ and $\beta \geq 0$. Then we have

$$(-3,-m)_3 = (-1)^\beta \left(\frac{-1}{3}\right)^\beta \left(\frac{-p^{2r}\tilde{A}}{3}\right) = \left(\frac{-p^{2r}\tilde{A}}{3}\right) = \left(\frac{-\tilde{A}}{3}\right).$$

Now, if $(-3,-m)_3 = -1$ we have $\rho(m) = 0$ and we are done. Otherwise, we have

$$\left(\frac{-\tilde{A}}{3}\right) = 1 \Rightarrow \tilde{A} \equiv 2 \bmod 3.$$

Hence $\tilde{A}$ has at least a prime factor congruent to 2 mod 3 appearing with odd exponent in its factorization. Since A is coprime with p, we have

$$\mathfrak{A}\left(\frac{m}{p^{1+n}}\right) = \mathfrak{A}(p^{2r-1-n}A) = 0$$

which is what we wanted to prove.

Case 2: $p = 2$**.** As in the previous case, we have that $v_2(F(m))$ can be nonzero only if 2 divides m, and this leads us to consider integers m of the form

$$m = \frac{2^{2n}9 - 2^{2r}k^2}{4} > 0 \tag{2.11}$$

where k is either 0 or coprime with 2. Again in this case we have

$$v_2(F(m)) = \rho(m)\mathfrak{A}\left(\frac{m}{2^{1+n}}\right). \tag{2.12}$$

First we study what happens for $k = 0$. In this case we have $m = 2^{2n-2}9$ and as above

$$v_2(F(m)) = \rho(m)\mathfrak{A}\left(\frac{m}{2^{1+n}}\right)$$

where the quantity on the right-hand side is again zero if either $\frac{m}{2^{1+n}}$ is not an integer or $v_2(\frac{m}{2^{1+n}}) \equiv 1 \mod 2$. But we see that $\frac{m}{2^{1+n}} = 2^{n-3}9$ and since n is even by assumption, we deduce that $v_2(F(m)) = 0$ in this case. Hence we may assume $k \neq 0$ and coprime with 2. Notice that (2.11) implies $r \leq n+1$. We consider two cases.

(i) Suppose that $r \leq n$. In this case we can write

$$m = \frac{2^{2r}(2^{2(n-r)}9 - k^2)}{4} = 2^{2r-2}(2^{2(n-r)}9 - k^2).$$

As in the previous case we have

$$v_2(F(m)) = \rho(m)\mathfrak{A}\left(\frac{m}{2^{1+n}}\right)$$

and we need to study

$$\frac{m}{2^{1+n}} = 2^{2r-n-3}(2^{2(n-r)}9 - k^2).$$

Notice now that, since k is coprime with 2, the quantity inside the parenthesis cannot be divided by 2 unless $n = r$ and $k \in \{\pm 1\}$. Suppose first that $n \neq r$: then

$$v_2\left(\frac{m}{2^{1+n}}\right) = 2r - n - 3 \equiv 1 \mod 2$$

since n is even by assumption. Using [LV15, Theorem 7.12] we deduce that $v_2(F(m)) = 0$ in this case.

Suppose now that $n = r$ and $k = \pm 1$: under these hypotheses we have $m = 2^{2n+1}$ and

$$v_2\left(\frac{m}{2^{1+n}}\right) = v_2(2^n) = n \equiv 0 \mod 2$$

by our assumptions on n. To compute the value of this valuation we have to use the full strength of [LV15, Theorem 7.12]: using the same notation of that theorem we have

$$v_2(F(m)) = \varepsilon_2(2^n)\prod_{\substack{q|2^n \\ q\neq 2}}(*)$$

where we see that the product on the right is empty, hence equal to 1, and by definition of $\varepsilon_2(\cdot)$ we have $\varepsilon_2(2^n) = 1$. Hence for $k = \pm 1$, we have $v_2(F(m)) = 1$.

(ii) Suppose now that $r = n + 1$ and $k = \pm 1$. In this case $m = 2^{2n-2}5$ and we see that $v_2\left(\frac{m}{2^{n+1}}\right) = v_2(2^{n-3}5) = n - 3$ is odd. As before we conclude that $v_2(F(m)) = 0$ in this case.

To sum up, if $p = 2$ the only integers m of the form $m = \frac{9p^{2n}-x^2}{4}$ for which $F(m)$ is a power of 2 are $m = 0$ ($x = \pm 2^n 3$) and $m = 2^{2n+1}$ ($x = \pm 2^{2n}$), in which cases we obtain

$$F(0) = 2^{1/3}, \qquad F(2^{2n+1}) = 2.$$

Combining these results with (2.8) we get

$$|N_{\mathbb{Q}(j)/\mathbb{Q}}(j)|^{2/3} = 2^{2/3} \cdot 2^2 \cdot B$$

where B is an integer coprime with 2. This concludes the proof. □

2.4 Supersingular elliptic curves and optimal embeddings

After the short interlude in the previous section, we now go back to the study of differences of singular moduli, or *singular differences*, that are S-units for some set $S \subseteq \mathbb{N}$ of primes. In Section 2.2 we fixed an appropriate singular modulus j_0 and a set S of primes splitting completely in the imaginary quadratic field K_{j_0} corresponding to j_0. We now want to analyze what happens if we choose S to contain some primes that are inert in K_{j_0}. Looking at Theorem 1.4.1, one can certainly imagine that this study is intimately related to the theory of supersingular elliptic curves and, in turn, of quaternion algebras. Hence, in this section we hone the theory explained in Section 1.4 by introducing the more sophisticated concept of *optimal embedding* in a quaternion algebra and by explaining how this relates to the deformation theory of CM elliptic curves defined over certain complete non-archimedean fields.

Let $\mathbb{B}$ be a quaternion algebra over $\mathbb{Q}$ and let $R \subseteq \mathbb{B}$ be an order. Let $\mathbb{Q} \subseteq K$ be a quadratic field extension and let $\mathcal{O} \subseteq K$ also be an order. Any ring homomorphism $\varphi : \mathcal{O} \to R$ can be naturally extended, after tensoring with $\mathbb{Q}$, to a ring homomorphism $K \to \mathbb{B}$ that we still denote by φ, with abuse of notation. We say that an injective ring homomorphism $\iota : \mathcal{O} \hookrightarrow R$ is an *optimal embedding* if

$$\iota(K) \cap R = \iota(\mathcal{O})$$

where the above intersection takes place in $\mathbb{B}$. There is a simple criterion which allows to determine whether a given imaginary quadratic order optimally embeds into a quaternionic order. In order to state it, let us denote by $\operatorname{trd}, \operatorname{nrd} : \mathbb{B} \to \mathbb{Q}$ respectively the reduced trace and the reduced norm in the quaternion algebra $\mathbb{B}$, see Section 1.2.

Lemma 2.4.1. *Let R be an order in a quaternion algebra $\mathbb{B}$ and $\mathcal{O}$ an order of discriminant Δ in an imaginary quadratic field K. Let $V \subseteq \mathbb{B}$ be the subspace of pure quaternions*

$$V := \{x \in \mathbb{B} : \operatorname{trd}(x) = 0\}.$$

Then $\mathcal{O}$ embeds (resp. optimally embeds) in R if and only if $|\Delta|$ is represented (resp. primitively represented) by the ternary quadratic lattice

$$R_0 := V \cap (\mathbb{Z} + 2R)$$

endowed with the natural scalar product induced by the reduced norm on $\mathbb{B}$.

Remark 2.4.2. This lemma has been proved for non-optimal embeddings and for maximal orders R in [Gro87, Proposition 12.9]. Probably for this reason, the lattice R_0 is sometimes called the *Gross lattice* associated to R. The argument in *loc. cit.* easily generalizes to our situation. We provide a full proof for completeness.

Proof. We first prove that $\mathcal{O}$ embeds in R if and only if it is represented by R_0, and we discuss conditions on the optimality of this embedding at a second stage.

Write $\mathcal{O} = \mathbb{Z}\left[\frac{\Delta+\sqrt{\Delta}}{2}\right]$ and suppose first that $f : \mathcal{O} \hookrightarrow R$ is an embedding. Let $b := f(\sqrt{\Delta})$ so that $\operatorname{trd}(b) = 0$ and $\operatorname{nrd}(b) = |\Delta|$. Since

$$f\left(\frac{\Delta + \sqrt{\Delta}}{2}\right) = \frac{\Delta + b}{2} \in R$$

we see that $b \in R_0$ so that $|\Delta|$ is represented by this lattice. Suppose conversely that there exists $b \in R_0$ such that $\mathrm{nrd}(b) = |\Delta|$. Since $\mathrm{trd}(b) = 0$, we see that $b^2 = \Delta$. By writing $b = a + 2r$ with $a \in \mathbb{Z}$ and $r \in R$, one has

$$b^2 = (a + 2r)^2 = a^2 + 4r^2 + 4ar = \Delta$$

and this immediately implies that $a \equiv \Delta \bmod 2$, so that $\Delta + b \in 2R$. Hence we have $(\Delta + b)/2 \in R$ and we obtain an embedding $f : \mathcal{O} \hookrightarrow R$ by setting

$$f\left(\frac{\Delta + \sqrt{\Delta}}{2}\right) = \frac{\Delta + b}{2}. \tag{2.13}$$

We now discuss optimality. Fix $\{\alpha_1, \alpha_2, \alpha_3\}$ to be a basis of R_0 as a $\mathbb{Z}$-module and let $Q(X, Y, Z)$ be the ternary quadratic form induced by the reduced norm with respect to this basis.

Assume that $f : \mathcal{O} \hookrightarrow R$ is an optimal embedding. By the proof above, we know that $b := f(\sqrt{\Delta}) \in R_0$ is such that $\mathrm{nrd}(b) = |\Delta|$. Suppose by contradiction that $b = a_1\alpha_1 + a_2\alpha_2 + a_3\alpha_3$ with $a_1, a_2, a_3 \in \mathbb{Z}$ not coprime, so that $c := \gcd(a_1, a_2, a_3) > 1$ (we adopt the convention that the greatest common divisor is always positive). Then $\widetilde{b} := b/c \in R_0$ satisfies

$$\widetilde{b}^2 = \frac{\Delta}{c^2} \in \mathbb{Z} \quad \text{and} \quad \frac{1}{2}\left(\frac{\Delta}{c^2} + \widetilde{b}\right) \in R.$$

in the same way as above. Thus $\frac{1}{2}\left(\frac{\sqrt{\Delta}}{c} + \frac{\Delta}{c^2}\right) \in K$ is an algebraic integer and the order $\widetilde{\mathcal{O}} := \mathbb{Z}\left[\frac{1}{2}\left(\frac{\sqrt{\Delta}}{c} + \frac{\Delta}{c^2}\right)\right]$, which strictly contains $\mathcal{O}$, also embeds in R through the extension $f : K \hookrightarrow \mathbb{B}$. This contradicts the optimality of $f : \mathcal{O} \hookrightarrow R$.

Suppose now that $|\Delta|$ is primitively represented by R_0 *i.e.* that there exist $a_1, a_2, a_3 \in \mathbb{Z}$ coprime such that $\mathrm{nrd}(a_1\alpha_1 + a_2\alpha_2 + a_3\alpha_3) = |\Delta|$. We want to show that, setting $b := a_1\alpha_1 + a_2\alpha_2 + a_3\alpha_3$, the embedding f defined by (2.13) is optimal. We will equivalentely prove that, if $c \in \mathbb{N}$ is such that $\widetilde{\mathcal{O}} := \mathbb{Z}\left[\frac{1}{2}\left(\frac{\sqrt{\Delta}}{c} + \frac{\Delta}{c^2}\right)\right]$ is an order, then

$$f(K) \cap R = f\left(\widetilde{\mathcal{O}}\right) \tag{2.14}$$

implies $\widetilde{\mathcal{O}} = \mathcal{O}$. Since $b = f(\sqrt{\Delta})$, equality (2.14) entails $\frac{1}{2}\left(\frac{b}{c} + \frac{\Delta}{c^2}\right) \in R$ so that $b/c \in R_0$. But now

$$b/c = \frac{a_1}{c}\alpha_1 + \frac{a_2}{c}\alpha_2 + \frac{a_3}{c}\alpha_3 \in R_0$$

and all the coefficients a_i/c must be integral since R_0 is a lattice. By assumption, the a_i's are coprime, so we must have $c = 1$. Hence $\widetilde{\mathcal{O}} = \mathcal{O}$ and this concludes the proof. □

Remark 2.4.3. The proof of Lemma 2.4.1 actually establishes a bijection between the set of embeddings $f : \mathcal{O} \hookrightarrow R$ and the set of elements $b \in R_0$ such that $\mathrm{nrd}(b) = |\Delta|$. Under this bijection, the embedding f corresponds to the element $f(\sqrt{\Delta}) \in R_0$.

In order to carry out our study of singular differences that are S-units, it is fundamental to understand what is the biggest exponent with which a prime ideal can appear in the factorization of such a difference. Roughly speaking, saying that a difference of singular moduli $j - j_0$ has a certain μ-adic valuation $n = v_\mu(j - j_0)$ for some prime ideal $\mu \subseteq \mathbb{Q}(j - j_0)$, is equivalent to saying that the CM elliptic curve E_j with $j(E_j) = j$ is isomorphic to the elliptic curve E_{j_0} with

$j(E_0) = j_0$ when reduced modulo μ^n. Therefore, in order to understand the exponents appearing in the prime ideal factorization of a singular modulus, it is crucial to determine when such isomorphisms can occur. With this goal in mind, we conclude this section by outlining some aspects of the deformation theory of CM elliptic curves defined over number fields. We refer the reader to [Con04], [Gro86], [GZ85] and [LV15] for further discussions on the topic.

Let $\mathcal{O}$ be an order of discriminant Δ in an imaginary quadratic field K and let $\ell \nmid \Delta$ be a prime inert in K. Consider an elliptic curve E with complex multiplication by the order $\mathcal{O}$ and defined over the ring class field $H_{\mathcal{O}} := K(j(E))$. After completing with respect to any prime above ℓ, we can consider $H_{\mathcal{O}}$ as a subfield of the maximal unramified extension $\mathbb{Q}_\ell^{\mathrm{unr}}$ of $\mathbb{Q}_\ell$. This is because the extension $\mathbb{Q} \subseteq H_{\mathcal{O}}$ is unramified at ℓ by the assumption $\ell \nmid \Delta$, see the end of Section 1.1. Let $L := \widehat{\mathbb{Q}_\ell^{\mathrm{unr}}}$ be the completion of $\mathbb{Q}_\ell^{\mathrm{unr}}$ with ring of integers W and uniformizer π. Then by [ST68, Theorems 8 and 9] and Theorem 1.4.1 there exists an elliptic scheme $\mathcal{E} \to \operatorname{Spec} W$ such that:

- the generic fiber $\mathcal{E} \times_W \operatorname{Spec} L$ is isomorphic over L to E. Since the CM order $\mathcal{O}$ is contained in W, all the endomorphisms of E are defined over L;
- the special fiber $E_0 := \mathcal{E} \times_W \operatorname{Spec} W/\pi$ is a supersingular elliptic curve since, by assumption, ℓ does not split in K. Note that $W/\pi \cong \overline{\mathbb{F}}_\ell$, the algebraic closure of the finite field with ℓ elements.

For all $n \in \mathbb{N}$, set $E_n := \mathcal{E} \times_W \operatorname{Spec} W/\pi^{n+1}$. We are interested in understanding the endomorphisms rings $A_{\ell,n} := \operatorname{End}_{W/\pi^{n+1}}(E_n)$. When $n = 0$, we have already seen that the ring $A_{\ell,0}$ is isomorphic to a maximal order in $\mathbb{B}_{\ell,\infty}$, the unique (up to isomorphism) definite quaternion algebra over the rationals which ramifies only at ℓ and ∞. All the other rings $A_{\ell,n}$ can be recovered from $A_{\ell,0}$, as explained in the following theorem.

Theorem 2.4.4. *Let $\mathcal{O}$ be an order of discriminant Δ in an imaginary quadratic field K and let $\ell \nmid \Delta$ be a prime inert in K. Set $L := \widehat{\mathbb{Q}_\ell^{unr}}$ to be the completion of the maximal unramified extension of $\mathbb{Q}_\ell$, with ring of integers W and uniformizer π. Let $\mathcal{E} \to \operatorname{Spec}(W)$ be an elliptic scheme whose generic fiber $E := \mathcal{E} \times_W \operatorname{Spec} L$ ha complex multiplication by $\mathcal{O}$. For every $n \in \mathbb{N}$, denote by*

$$E_n := \mathcal{E} \times_W \operatorname{Spec} W/\pi^{n+1} \qquad \text{and} \qquad A_{\ell,n} := \operatorname{End}_{W/\pi^{n+1}}(E_n)$$

respectively the reduction of $\mathcal{E}$ modulo π^{n+1} and its endomorphism ring. Then:

(a) for every $n \in \mathbb{N}_{\geq 1}$ the ring $\operatorname{End}_{W/\pi^n}(E_n)$ is isomorphic to a quaternion order in $\mathbb{B}_{\ell,\infty}$ and the natural reduction map

$$\mathcal{O} \cong \operatorname{End}_W(E) \longrightarrow \operatorname{End}_{W/\pi^{n+1}}(E_n)$$

induced by the reduction modulo π^{n+1} is an optimal embedding;

(b) for every $n \in \mathbb{N}$ we have

$$A_{\ell,n} \cong \mathcal{O} + \ell^n A_{\ell,0}$$

where the sum takes place in $A_{\ell,0}$.

The above theorem is a combination and a reformulation of various results already appearing in the literature. We give a brief overview of the proof and point out at the relevant references.

Proof of Theorem 2.4.4. We begin with the proof of (a). The first statement follows from the fact that ℓ is a prime of supersingular reduction for E_j and by Serre-Tate theory, see for instance [Con04, Theorem 3.3]. Reductions modulo π and π^n give the following diagram

$$\begin{tikzcd}
\mathcal{O} \arrow[r, hook, "\varphi_{n-1}"] \arrow[dr, hook, "\varphi_0"'] & \mathrm{End}_{W/\pi^n}(E_j) \arrow[d, hook] \\
 & \mathrm{End}_{W/\pi}(E_j)
\end{tikzcd}$$

which clearly commutes. Since ℓ does not divide the conductor of the order $\mathcal{O}$, the embedding φ_0 is optimal by [LV15, Proposition 2.2]. It follows from the commutativity of the diagram above that also the embedding φ_{n-1} is optimal, and the point (a) is proved. Part (b) of the proposition is a special case of [LV15, Formula 6.6]. □

2.5 The ℓ-adic valuation of differences of singular moduli

The goal of this section is to prove, under certain hypotheses, an upper bound for the exponents appearing in the prime factorization of a difference of singular moduli. Our bounds will be crucially used in the next section in order to provide new bounds on singular differences that are S-units. In what follows, we will always use $\mathbb{F}_\ell$ to denote the finite field with ℓ elements, where $\ell \in \mathbb{N}$ is a prime number, and $\overline{\mathbb{F}}_\ell$ to denote an algebraic closure of this field.

Theorem 2.5.1. *Let $j_0 \in \overline{\mathbb{Q}}$ be a singular modulus relative to an order $\mathcal{O}_{j_0}$ of discriminant Δ_0 and let $\ell \in \mathbb{Z}$ be a prime not dividing Δ_0. For any singular modulus $j \in \overline{\mathbb{Q}}$ relative to an order $\mathcal{O}_j$ of discriminant $\Delta \neq \Delta_0$, denote by H the compositum of the ring class fields relative to $\mathcal{O}_{j_0}$ and $\mathcal{O}_j$. Let $\mu \subseteq H$ be a prime ideal lying above ℓ and assume that:*

1. *the prime $\mu \cap \mathbb{Q}(j_0)$ has residue degree 1 over ℓ;*
2. *there exists an elliptic curve $(E_0)_{/\mathbb{Q}(j_0)}$ with $j(E_0) = j_0$ and having good reduction at μ.*

Then, if $v_\mu(\cdot)$ denotes the normalized valuation associated to μ, we have

$$v_\mu(j - j_0) \leq \begin{cases} \frac{d_0}{2}\left(\frac{\log(\Delta_0^2|\Delta|)}{2\log \ell} + \frac{1}{2}\right) & \text{if } \ell \nmid \Delta \text{ and } \mathcal{O}_{j_0} \not\subseteq \mathcal{O}_j, \\ \frac{d_0}{2} & \text{if } \ell \mid \Delta \end{cases} \tag{2.15}$$

where d_0 is the number of automorphisms of any elliptic curve $E_{/\overline{\mathbb{F}}_\ell}$ with $j(E) = j_0 \bmod \mu$.

Remark 2.5.2. Note that we have $d_0 = 2$ in all cases except if $j_0 \equiv 0$ or $j_0 \equiv 1728 \bmod \mu$. In these two cases, the value of d_0 also depends on ℓ, see [Sil09, III, Theorem 10.1].

The dichotomy in the conclusion of Theorem 2.5.1 is reflected by its proof, which we divide according to the conditions displayed in (2.15). In all cases, everything boils down to the study of optimal embeddings of the order $\mathcal{O}_j$ in a family of nested orders contained in the endomorphism ring of a certain supersingular elliptic curve defined over $\overline{\mathbb{F}}_\ell$. One of the main issues is that for a supersingular elliptic curve $E_{/\overline{\mathbb{F}}_\ell}$, explicitely computing its endomorphism ring is a difficult problem in general. An explicit parametrization of the endomorphism rings of supersingular elliptic curves over $\overline{\mathbb{F}}_\ell$ has been achieved by Lauter and Viray in [LV15, Section 6]. However, we found these parametrizations somehow difficult to use for explicit estimates. Therefore, in order to achieve our results, we adopted a different strategy. The idea is that, since we are only interested in providing estimates for the μ-adic valuation of singular differences and not in precisely determining their prime ideal factorization, we do not need the full knowledge of the supersingular endomorphism rings of the elliptic curves involved. We instead "approximate", when possible, the unknown quaternion orders with quaternion orders whose properties are less mysterious. The next proposition is the cornerstone of this strategy.

Proposition 2.5.3. *Let $j \in \overline{\mathbb{Q}}$ be a singular modulus of discriminant Δ and let $E_{/\mathbb{Q}(j)}$ be an elliptic curve with $j(E) = j$. Choose a degree 1 prime $\mathfrak{p} \subseteq \mathbb{Q}(j)$ lying above a rational prime $p \in \mathbb{Z}$ not dividing Δ and suppose that E has good supersingular reduction $\widetilde{E}$ modulo $\mathfrak{p}$. Denote by $\varphi \in \mathrm{End}_{\overline{\mathbb{F}}_p}(\widetilde{E})$ the Frobenius endomorphism $(x, y) \mapsto (x^p, y^p)$. Then there exists a morphism $\psi \in \mathrm{End}_{\overline{\mathbb{F}}_p}(\widetilde{E})$ such that*

$$\psi^2 + |\Delta|\psi + \frac{\Delta^2 + |\Delta|}{4} = 0 \qquad \textit{and} \qquad \psi \circ \varphi = \varphi \circ \overline{\psi}$$

where $\bar{\cdot} : \mathrm{End}_{\overline{\mathbb{F}}_p}(\widetilde{E}) \otimes_{\mathbb{Z}} \mathbb{Q} \longrightarrow \mathrm{End}_{\overline{\mathbb{F}}_p}(\widetilde{E}) \otimes_{\mathbb{Z}} \mathbb{Q}$ *denotes the standard involution.*

Remark 2.5.4. Recall that the standard involution on the quaternion algebra $\mathrm{End}_{\overline{\mathbb{F}}_p}(\widetilde{E}) \otimes_{\mathbb{Z}} \mathbb{Q}$ correspond to taking the dual isogeny when restricted to $\mathrm{End}_{\overline{\mathbb{F}}_p}(\widetilde{E})$. This essentially follows from the uniqueness of the standard involution on quaternion algebras, see [Voi21, Corollary 3.4.4].

Proof. Let $\mathcal{O}$ be the order of discriminant Δ and $K \subseteq \overline{\mathbb{Q}}$ be its field of fractions. For an element $\beta \in K$ we denote also by $\overline{\beta}$ its conjugate through the unique non-trivial automorphism of $K/\mathbb{Q}$ (this will not cause confusion with the standard involution on $\mathrm{End}_{\overline{\mathbb{F}}_p}(\widetilde{E}) \otimes_{\mathbb{Z}} \mathbb{Q}$, as we explain below). We also fix a normalized isomorphism

$$[\cdot]_E : \mathcal{O} \xrightarrow{\sim} \mathrm{End}_{\overline{\mathbb{Q}}}(E)$$

as in Definition 1.3.7. Let $\alpha := \frac{\Delta + \sqrt{\Delta}}{2} \in \mathcal{O}$. Since by [Shi98, Chapter II, Proposition 30], all the endomorphisms of E are defined over the compositum $H_{\mathcal{O}} := K(j)$, which is a degree 2 extension of $\mathbb{Q}(j)$, after fixing an affine Weierstrass model for E with coordinates X, Y, we can write

$$[\alpha]_E(X, Y) = \left(\frac{P(X, Y, \alpha)}{Q(X, Y, \alpha)}, \frac{R(X, Y, \alpha)}{S(X, Y, \alpha)} \right)$$

for some polynomials $P, Q, R, S \in \mathcal{O}_{\mathbb{Q}(j)}[X, Y, Z]$, where $\mathcal{O}_{\mathbb{Q}(j)}$ denotes the ring of integers of $\mathbb{Q}(j)$. Moreover, since $\alpha^2 + |\Delta|\alpha + \frac{\Delta^2 + |\Delta|}{4} = 0$, also $[\alpha]_E$ satisfies the same relation.

Let $\mathcal{P} \subseteq H_{\mathcal{O}}$ be a prime lying above $\mathfrak{p}$. Since E has supersingular reduction modulo $\mathfrak{p}$, the latter has degree 1 and p is unramified in K, by Theorem 1.4.1 we must have $f(\mathcal{P}/\mathfrak{p}) = 2$, where $f(\mathcal{P}/\mathfrak{p})$ denotes the inertia degree of $\mathcal{P}$ over $\mathfrak{p}$. In particular, we see that the decomposition group of $\mathcal{P}$ over $\mathfrak{p}$ is precisely $\mathrm{Gal}(H_{\mathcal{O}}/\mathbb{Q}(j))$. We fix $\sigma \in \mathrm{Gal}(H_{\mathcal{O}}/\mathbb{Q}(j))$ to be the unique non-trivial element. Then one has

$$\sigma([\alpha]_E) = [\sigma(\alpha)]_{E^\sigma} = [\overline{\alpha}]_E$$

where the first equality follows from Theorem 1.3.8 and in the second equality we are using the fact that E is defined over $\mathbb{Q}(j)$ and σ is non-trivial. Translating the above equality using coordinates, we get

$$[\overline{\alpha}]_E(X,Y) = \left(\frac{P(X,Y,\overline{\alpha})}{Q(X,Y,\overline{\alpha})}, \frac{R(X,Y,\overline{\alpha})}{S(X,Y,\overline{\alpha})}\right).$$

Let now $\psi := ([\alpha]_E \bmod \mathcal{P}) \in \mathrm{End}_{\overline{\mathbb{F}}_p}(\widetilde{E})$. For $\beta \in \mathcal{O}$ the association $[\beta]_E \mapsto [\overline{\beta}]_E$ defines a standard involution on on $\mathrm{End}_{\overline{\mathbb{Q}}}(E)$, in the sense of [Voi21, Definition 3.2.4]. Since reduction mod $\mathcal{P}$ defines an embedding of $\mathrm{End}_{\overline{\mathbb{Q}}}(E) \hookrightarrow \mathrm{End}_{\overline{\mathbb{F}}_p}(\widetilde{E})$, by the uniqueness of the standard involution on quadratic $\mathbb{Q}$-algebras (see [Voi21, Lemma 3.4.2]) we have $[\overline{\alpha}] \bmod \mathcal{P} = \overline{\psi}$, where now the conjugation above ψ denotes the usual standard involution on the quaternion algebra $\mathrm{End}_{\overline{\mathbb{F}}_p}(\widetilde{E}) \otimes_{\mathbb{Z}} \mathbb{Q}$. As σ is a generator of the decomposition group of $\mathcal{P}$ over $\mathfrak{p}$, it must act as the p-power Frobenius element over the residue field modulo $\mathcal{P}$. In particular we have

$$\overline{\psi}(X,Y) = \left(\frac{\widetilde{P}(X,Y,\widetilde{\alpha}^p)}{\widetilde{Q}(X,Y,\widetilde{\alpha}^p)}, \frac{\widetilde{R}(X,Y,\widetilde{\alpha}^p)}{\widetilde{S}(X,Y,\widetilde{\alpha}^p)}\right)$$

where $\widetilde{P}, \widetilde{Q}, \widetilde{R}, \widetilde{S} \in \mathbb{F}_p[X,Y,Z]$ are the reductions modulo $\mathcal{P}$ of the polynomials P,Q,R,S and $\widetilde{\alpha} = \alpha \bmod \mathcal{P}$. Now we see that

$$(\psi \circ \varphi)(X,Y) = \psi(X^p,Y^p) = \left(\frac{\widetilde{P}(X^p,Y^p,\widetilde{\alpha})}{\widetilde{Q}(X^p,Y^p,\widetilde{\alpha})}, \frac{\widetilde{R}(X^p,Y^p,\widetilde{\alpha})}{\widetilde{S}(X^p,Y^p,\widetilde{\alpha})}\right) = (\varphi \circ \overline{\psi})(X,Y).$$

Moreover, ψ is a root of the same minimal polynomial as α, since reduction modulo $\mathcal{P}$ is a ring homomorphism and this shows that ψ is the sought element. □

We are now ready to begin the proof of Theorem 2.5.1. Let us fix the notation that will be in force during the entire argument. Given the orders $\mathcal{O}_j = \mathbb{Z}\left[\frac{\Delta+\sqrt{\Delta}}{2}\right]$ and $\mathcal{O}_{j_0} = \mathbb{Z}\left[\frac{\Delta_0+\sqrt{\Delta_0}}{2}\right]$ as in the statement of Theorem 2.5.1, we denote by K_j and K_{j_0} the corresponding imaginary quadratic fields containing them. We then set H_j and H_{j_0} to be the ring class fields of K_j and K_{j_0} relative to the orders $\mathcal{O}_j$ and $\mathcal{O}_{j_0}$ respectively. Using this notation, the field H in the statement of Theorem 2.5.1 is the compositum in $\overline{\mathbb{Q}}$ of H_j and H_{j_0}.

2.5.1 First case of Theorem 2.5.1

Assume that E_0 in the statement of the theorem is given by an integral model over $\mathbb{Q}(j_0)$ with good reduction at μ. Let $(E_0)_{/H}$ be the base-change to H of the elliptic curve $(E_0)_{/\mathbb{Q}(j_0)}$, and let $(E_j)_{/H}$ be an elliptic curve with $j(E_j) = j$. We can always choose an integral model of E_j that has good reduction at all prime ideals above ℓ by [ST68, Theorems 8 and 9], which we can apply since $\ell \nmid \Delta$ by assumption. With this choice, E_j will have good reduction at the prime μ. We will always identify $\mathcal{O}_j$ and $\mathcal{O}_{j_0}$ with the endomorphism rings of E_j and E_{j_0} respectively.

Let H_μ be the completion of H at the prime μ. The extension $\mathbb{Q} \subseteq H$ is unramified at ℓ because $\ell \nmid \Delta\Delta_0$ (see Section 1.1), hence H_μ is contained in $\widehat{\mathbb{Q}_\ell^{\mathrm{unr}}}$, the completion of the maximal unramified extension of $\mathbb{Q}_\ell$. Denote by W the ring of integers in $\widehat{\mathbb{Q}_\ell^{\mathrm{unr}}}$ and let $\pi \in W$ be a uniformizer. The base-changed elliptic curves $(E_0)_{/W}$ and $(E_j)_{/W}$ have good reduction modulo π. Note also that, by our choices, E_0 mod π is defined over $\mathbb{F}_\ell$.

Lemma 2.5.5. *In the notation above, we have*

$$v_\mu(j - j_0) \leq \frac{d_0}{2} \cdot \max\{n \in \mathbb{N}_{\geq 1} : \mathrm{Iso}_{W/\pi^n}(E_j, E_0) \neq \emptyset\}$$

where, for every $n \in \mathbb{N}$, we denote by $\mathrm{Iso}_{W/\pi^n}(E_j, E_0)$ *the set of isomorphisms between E_j mod π^n and $E_0 \mod \pi^n$.*

Proof. Notice first of all that the normalized valuation on $\widehat{\mathbb{Q}_\ell^{\mathrm{unr}}}$, *i.e* the valuation v satisfying $v(\pi) = 1$, extends the μ-adic valuation v_μ on H because $v_\mu(\ell) = 1$. Since W is a complete discrete valuation ring whose quotient field has characteristic 0 and whose residue field $\overline{\mathbb{F}}_\ell$ is algebraically closed of characteristic $\ell > 0$, we can apply [GZ85, Proposition 2.3] which gives

$$v_\mu(j - j_0) = \frac{1}{2} \sum_{n=1}^{\infty} \# \mathrm{Iso}_{W/\pi^n}(E_j, E_0).$$

Now, certainly $\mathrm{Iso}_{W/\pi^{n+1}}(E_j, E_0) \neq \emptyset$ implies $\mathrm{Iso}_{W/\pi^n}(E_j, E_0) \neq \emptyset$ for every $n \in \mathbb{N}_{>0}$, since reduction of isomorphisms are isomorphisms. Moreover, whenever the set $\mathrm{Iso}_{W/\pi^n}(E_j, E_0)$ is non-empty, its cardinality equals the order of the automorphism group $\mathrm{Aut}_{W/\pi^n}(E_0)$ of E_0 mod π^n. By [Con04, Theorem 2.1 (2)], we always have the inclusions

$$\mathrm{End}_W(E_0) \hookrightarrow \mathrm{End}_{W/\pi^n}(E_0) \hookrightarrow \mathrm{End}_{W/\pi}(E_0)$$

induced respectively by the reduction modulo π^n and modulo π. This means that

$$\# \mathrm{Aut}_W(E_0) \leq \# \mathrm{Aut}_{W/\pi^n}(E_0) \leq \mathrm{Aut}_{W/\pi}(E_0) = d_0 \tag{2.16}$$

so, setting $M := \max\{n \in \mathbb{N}_{\geq 1} : \mathrm{Iso}_{W/\pi^n}(E_j, E_0) \neq \emptyset\}$, we obtain

$$v_\mu(j - j_0) = \frac{1}{2} \sum_{n=1}^{\infty} \# \mathrm{Iso}_{W/\pi^n}(E_j, E_0) = \frac{1}{2} \sum_{n=1}^{M} \# \mathrm{Aut}_{W/\pi^n}(E_0) \leq \frac{d_0}{2} \cdot M$$

which proves the lemma. □

By Lemma 2.5.5, in order to estimate the valuation at μ of the difference $j - j_0$, we need to bound the biggest index n such that the reduction modulo π^n of the elliptic curves E_j and E_0 are isomorphic. If this maximum is 0, then the two elliptic curves are not even isomorphic over $\overline{\mathbb{F}}_\ell \cong W/\pi$, so the prime μ cannot divide $j - j_0$ and there is nothing to prove. Hence, from now on we suppose that μ divides $j - j_0$ so that E_0 mod $\pi \cong E_j$ mod π over $\overline{\mathbb{F}}_\ell$. Since ℓ does not divide the conductor of the orders $\mathcal{O}_j$ and $\mathcal{O}_{j_0}$ by assumption, and the two orders are different, Theorem 1.4.1 ensures that ℓ is a prime of supersingular reduction for both E_j and E_0. In particular, the ring $R := \mathrm{End}_{W/\pi}(E_0)$ is isomorphic to a maximal order in $\mathbb{B}_{\ell,\infty} \cong R \otimes_{\mathbb{Z}} \mathbb{Q}$.

Suppose now that $\mathrm{Iso}_{W/\pi^{n+1}}(E_j, E_0)$ is non-empty. Our goal is to find a bound on the exponent $n + 1$. A choice of $f \in \mathrm{Iso}_{W/\pi^{n+1}}(E_j, E_0)$ induces an isomorphism

$$\widetilde{f} : \mathrm{End}_{W/\pi^{n+1}}(E_j) \longrightarrow \mathrm{End}_{W/\pi^{n+1}}(E_0), \qquad \alpha \longmapsto f \circ \alpha \circ f^{-1}$$

which, precomposed with the reduction map $\mathcal{O}_j \hookrightarrow \mathrm{End}_{W/\pi^{n+1}}(E_j)$, gives rise to an optimal embedding

$$\psi_{n+1} : \mathcal{O}_j \hookrightarrow \mathrm{End}_{W/\pi^{n+1}}(E_0) \tag{2.17}$$

by Theorem 2.4.4 (a). For growing n, Theorem 2.4.4 (b) shows that the endomorphism ring of E_0 mod π^{n+1} becomes more and more "ℓ-adically close" to the order $\mathcal{O}_{j_0}$. Intuitively, this must imply that having an embedding as in (2.17) should not be possible for n large enough, yielding the desired bound on $n+1$. This intuition is correct, as we show below. The main obstacle to make this idea precise is that, as we already said, it is not easy to explicitly compute the endomorphism rings $\mathrm{End}_{W/\pi^{n+1}}(E_0)$ for a generic elliptic curve $E_{0/W}$. To circumvent this problem, we "approximate" the rings $\mathrm{End}_{W/\pi^{n+1}}(E_0)$ with smaller orders where we are able to perform the relevant computations. The hypotheses on the prime μ and on the elliptic curve E_0 will make this strategy successful.

Recall that $\mathcal{O}_{j_0} = \mathbb{Z}\left[\frac{\Delta_0+\sqrt{\Delta_0}}{2}\right]$ and let $\psi \in R$ be the image of $\frac{\Delta_0+\sqrt{\Delta_0}}{2}$ via the reduction map modulo π. Denote also by $\varphi \in \mathrm{End}_{W/\pi}(E_0)$ the Frobenius endomorphism $(x,y) \mapsto (x^\ell, y^\ell)$. By Proposition 2.5.3 and using the fact that E_0 mod π is a supersingular elliptic curve defined over $\mathbb{F}_\ell$, we have

$$\varphi^2 + \ell = 0, \qquad \psi^2 + |\Delta_0|\psi + \frac{\Delta_0^2 + |\Delta_0|}{4} = 0 \ \text{ and } \ \psi \circ \varphi = \varphi \circ \overline{\psi}. \tag{2.18}$$

Hence, the ring $\widetilde{R} := \mathbb{Z}[\psi, \varphi] \subseteq R$ is a rank-4 order inside $\mathbb{B}_{\ell,\infty}$ with basis $\mathcal{B} = \{1, \psi, \varphi, \psi\varphi\}$ satisfying the relations (2.18). Notice that the reduction map $\mathcal{O}_{j_0} \hookrightarrow R$ identifies $\mathcal{O}_{j_0}$ with the subring $\mathbb{Z}[\psi] \subseteq \mathbb{Z}[\psi, \varphi]$. The matrix of the bilinear pairing $\langle \alpha, \beta \rangle = \mathrm{trd}(\alpha\overline{\beta})$ computed on the basis $\mathcal{B}$ is given by

$$A = \begin{pmatrix} 2 & \Delta_0 & 0 & 0 \\ \Delta_0 & \frac{\Delta_0^2+|\Delta_0|}{2} & 0 & 0 \\ 0 & 0 & 2\ell & \Delta_0\ell \\ 0 & 0 & \Delta_0\ell & \frac{\Delta_0^2+|\Delta_0|}{2}\ell \end{pmatrix}$$

so the discriminant of the order $\widetilde{R}$ equals $\det A = \Delta_0^2\ell^2$. Hence, from Theorem 1.2.14 we see that $\widetilde{R}$ has index $|\Delta_0|$ inside any maximal order containing it, so in particular $|R : \widetilde{R}| = |\Delta_0|$. Now, since we are in the hypotheses of Theorem 2.4.4 (2), we have

$$\mathrm{End}_{W/\pi^{n+1}}(E_0) \cong \mathbb{Z}[\psi] + \ell^n R \supseteq \mathbb{Z}[\psi] + \ell^n \widetilde{R}$$

and we shall show that the index of the latter inclusion is also bounded by $|\Delta_0|$.

Lemma 2.5.6. *For all $n \in \mathbb{N}$ the index $\left|(\mathbb{Z}[\psi] + \ell^n R) : (\mathbb{Z}[\psi] + \ell^n \widetilde{R})\right|$ divides $|\Delta_0|$.*

Proof. Since $\widetilde{R} \subseteq R$, we have $\mathbb{Z}[\psi] + \ell^n R = \mathbb{Z}[\psi] + \ell^n R + \ell^n \widetilde{R}$. Hence

$$\frac{\mathbb{Z}[\psi] + \ell^n R}{\mathbb{Z}[\psi] + \ell^n \widetilde{R}} = \frac{\mathbb{Z}[\psi] + \ell^n R + \ell^n \widetilde{R}}{\mathbb{Z}[\psi] + \ell^n \widetilde{R}} \cong \frac{\ell^n R}{(\mathbb{Z}[\psi] + \ell^n \widetilde{R}) \cap \ell^n R}$$

as abelian groups. Now, the containment $\ell^n \widetilde{R} \subseteq (\mathbb{Z}[\psi] + \ell^n \widetilde{R}) \cap \ell^n R$ gives an epimorphism

$$\frac{\ell^n R}{\ell^n \widetilde{R}} \twoheadrightarrow \frac{\ell^n R}{(\mathbb{Z}[\psi] + \ell^n \widetilde{R}) \cap \ell^n R}.$$

and, since R is non-torsion, we have $\ell^n R / \ell^n \widetilde{R} \cong R/\widetilde{R}$. Since the latter has cardinality $|\Delta_0|$, the lemma is proved. □

Corollary 2.5.7. *The embedding* (2.17) *induces an injection*

$$\mathcal{O}_{j,|\Delta_0|} := \mathbb{Z}\left[\frac{\Delta_0^2\Delta + \sqrt{\Delta_0^2\Delta}}{2}\right] \hookrightarrow \mathbb{Z}[\psi] + \ell^n\widetilde{R}. \tag{2.19}$$

Proof. By Lemma 2.5.6, for every $x \in \mathbb{Z}[\psi] + \ell^n R$ we have $|\Delta_0|x \in \mathbb{Z}[\psi] + \ell^n\widetilde{R}$. Since the order $\mathcal{O}_{j,|\Delta_0|}$ has index $|\Delta_0|$ in $\mathcal{O}_j$, the corollary follows. □

Combining Corollary 2.5.7 with Lemma 2.4.1, we see that $|\operatorname{disc}(\mathcal{O}_{j,|\Delta_0|})| = \Delta_0^2|\Delta|$ must be represented by the Gross lattice $\Lambda_{\ell,n}$ of the order $\mathbb{Z}[\psi] + \ell^n\widetilde{R}$. Note that the this representation is not necessarily primitive, because the embedding (2.19) is not necessarily optimal. A computation shows that

$$\Lambda_{\ell,n} = \langle |\Delta_0| + 2\psi, 2\ell^n\varphi, 2\ell^n\psi\varphi\rangle_{\mathbb{Z}}$$

i.e. $\{|\Delta_0| + 2\psi, 2\ell^n\varphi, 2\ell^n\psi\varphi\}$ is a $\mathbb{Z}$-basis for the Gross lattice of $\mathbb{Z}[\psi] + \ell^n\widetilde{R}$. The reduced norm restricted to the lattice $\Lambda_{\ell,n}$ induces the ternary quadratic form

$$Q_{\ell,n}(X,Y,Z) = |\Delta_0|X^2 + 4\ell^{2n+1}Y^2 + \ell^{2n+1}(\Delta_0^2 + |\Delta_0|)Z^2 + 4\ell^{2n+1}\Delta_0 YZ. \tag{2.20}$$

After setting

$$\widetilde{X} = X, \qquad \widetilde{Y} = Y + \frac{1}{2}\Delta_0 Z, \qquad \widetilde{Z} = Z$$

we get the diagonal quadratic form

$$\widetilde{Q}_{\ell,n}(\widetilde{X},\widetilde{Y},\widetilde{Z}) = |\Delta_0|\widetilde{X}^2 + 4\ell^{2n+1}\widetilde{Y}^2 + \ell^{2n+1}|\Delta_0|\widetilde{Z}^2.$$

Suppose now that $Q_{\ell,n}(X,Y,Z) = \Delta_0^2|\Delta|$ has an integral solution $(x,y,z) \in \mathbb{Z}^3$ corresponding to the embedding (2.19). We first claim that at least one among y and z is non-zero. This follows from our assumptions on $\mathcal{O}_j$ and on the following proposition.

Proposition 2.5.8. *If* $y = z = 0$ *then* $\mathcal{O}_{j_0} \subseteq \mathcal{O}_j$.

Proof. Let $x \in \mathbb{Z}_{>0}$ be such that $Q_{\ell,n}(x,0,0) = \Delta_0^2|\Delta|$. By the proof of Lemma 2.4.1, this equality corresponds to the embedding

$$\mathbb{Z}\left[\frac{1}{2}\left(\Delta_0^2\Delta + \sqrt{\Delta_0^2\Delta}\right)\right] \hookrightarrow \mathbb{Z}[\psi] + \ell^n\widetilde{R}, \quad \frac{1}{2}\left(\Delta_0^2\Delta + \sqrt{\Delta_0^2\Delta}\right) \mapsto \frac{1}{2}\left(\Delta_0^2\Delta + x(|\Delta_0| + 2\psi)\right) \tag{2.21}$$

of the order $\mathcal{O}_{j,|\Delta_0|} \subseteq K := \mathbb{Q}(\sqrt{\Delta})$ into $\mathbb{Z}[\psi] + \ell^n\widetilde{R}$. The injection (2.21) is not optimal if $x \neq \pm 1$. Indeed, using again Lemma 2.4.1 we get the optimal embedding

$$\mathbb{Z}\left[\frac{1}{2}\left(\frac{\Delta_0^2}{x^2}\Delta + \sqrt{\frac{\Delta_0^2}{x^2}\Delta}\right)\right] \hookrightarrow \mathbb{Z}[\psi] + \ell^n\widetilde{R}, \quad \frac{1}{2}\left(\frac{\Delta_0^2}{x^2}\Delta + \sqrt{\frac{\Delta_0^2}{x^2}\Delta}\right) \mapsto \frac{1}{2}\left(\frac{\Delta_0^2}{x^2}\Delta + (|\Delta_0| + 2\psi)\right) \tag{2.22}$$

determined by the equality $Q_{\ell,n}(1,0,0) = (\Delta_0^2|\Delta|)/x^2$. Moreover, recall that we also have embedding (2.17), that can be rewritten as

$$\mathcal{O}_j = \mathbb{Z}\left[\frac{\Delta+\sqrt{\Delta}}{2}\right] \hookrightarrow \mathbb{Z}[\psi] + \ell^n R. \tag{2.23}$$

We remind the reader that the above injection (2.23) is again optimal, and that (2.21) is originally induced by (2.23). It is then clear that the injections (2.21), (2.22) and (2.23) are all compatible between each other, meaning that, after tensoring with $\mathbb{Q}$, one gets the same map $K \hookrightarrow \mathbb{B}_{\ell,\infty}$. Note also that the images of (2.21) and (2.22) are contained in $\mathrm{Frac}(\mathbb{Z}[\psi]) \cong \mathbb{Q}(\sqrt{\Delta_0})$. This implies that $K = \mathbb{Q}(\sqrt{\Delta}) = \mathbb{Q}(\sqrt{\Delta_0})$ so that the orders $\mathcal{O}_{j_0}$ and $\mathcal{O}_j$ are contained in the same imaginary quadratic field. For ease of notation, set

$$\mathcal{O} := \mathbb{Z}\left[\frac{1}{2}\left(\frac{\Delta_0^2}{x^2}\Delta + \sqrt{\frac{\Delta_0^2}{x^2}\Delta}\right)\right].$$

We first claim that x divides Δ_0. Suppose by contradiction that this is not the case, and write $x = d \cdot k$ with $d := \gcd(x, \Delta_0)$, so that $k \neq \pm 1$ and $\gcd(k, \Delta_0/d) = 1$. Since $(\Delta_0^2|\Delta|)/x^2$ must be an integer, we deduce that $k^2 \mid |\Delta|$. Write $\Delta = -f^2 D$ with $-D = \operatorname{disc} K \in \mathbb{Z}$ a fundamental discriminant and $f \in \mathbb{Z}_{>0}$. Then we are going to show that k^2 actually divides f^2.

For every odd prime $p \in \mathbb{N}$ with $p \mid k$, the fact that p^2 divides $-f^2 D$ and that p^2 cannot divide D since the latter is a fundamental discriminant, easily implies that $p^2 \mid f^2$. This shows that the odd part of k^2 divides f^2. On the other hand, suppose that $2 \mid k$. If D is odd there is nothing else to prove. If D is even instead, D is exactly divisible by either 4 or 8. Hence we can write the discriminant of the order $\mathcal{O}$ as

$$\operatorname{disc}(\mathcal{O}) = \frac{\Delta_0^2\Delta}{x^2} = -\left(\frac{\Delta_0}{d}\right)^2 \cdot \left(\frac{f}{k/2}\right)^2 \cdot \frac{D}{4} \in \mathbb{Z}$$

where all the factors of the product are integers by the above discussion. Since $\mathcal{O}$ is an order in K, its discriminant should be of the form $-D \cdot a^2$ for some $a \in \mathbb{N}$. Together with the fact that Δ_0/d is odd (because k is even) this implies that $(f/(k/2))^2$ is divisible by 4, which in turn means that $k^2 \mid f^2$, as wanted.

We are now ready to prove that $x \mid \Delta_0$. The map (2.22), composed with the natural inclusion $\mathbb{Z}[\psi] + \ell^n\widetilde{R} \subseteq \mathbb{Z}[\psi] + \ell^n R$, gives an embedding of the order $\mathcal{O}$ inside $\mathbb{Z}[\psi] + \ell^n R$. On the other hand, in the latter ring lies also the image of $\mathcal{O}_j$ through (2.23). This implies that $\mathbb{Z}[\psi] + \ell^n R$ must contain the image of the order in K whose conductor is the greatest common divisor of the two conductors $f_{\mathcal{O}}$ and f of the orders $\mathcal{O}$ and $\mathcal{O}_j$ respectively. Let $f' := \gcd(f_{\mathcal{O}}, f)$. The fact that $k \mid f$ gives

$$f_{\mathcal{O}} = \frac{|\Delta_0|}{d} \cdot \frac{f}{k}$$

and we deduce that $f' \neq f$, since otherwise we would have $f_{\mathcal{O}}/f \in \mathbb{N}$ and then $\gcd(k, \Delta_0/d) > 1$. Hence $\mathbb{Z}[\psi] + \ell^n R$ contains (the image of) an order of K whose conductor strictly divides the conductor of $\mathcal{O}_j$. However, this contradicts the optimality of the embedding (2.23) and proves that $x \mid |\Delta_0|$.

In order to conclude the proof of the proposition, write $x = |\Delta_0|/m$ for some integer m dividing Δ_0. Then equality $Q_{\ell,n}(x,0,0) = \Delta_0^2|\Delta|$ reads

$$|\Delta_0|x^2 = \Delta_0^2|\Delta|$$

which implies

$$|\Delta| = \frac{x^2}{|\Delta_0|} = \frac{|\Delta_0|}{m^2}.$$

Since $\mathcal{O}_{j_0}$ and $\mathcal{O}_j$ are contained in the same imaginary quadratic field, we deduce that $\mathcal{O}_{j_0} \subseteq \mathcal{O}_j$ and this concludes the proof. □

Since at least one among y and z is non-zero, we also have that at least one among $\widetilde{y} := y + (\Delta_0 z)/2$ and $\widetilde{z} = z$ is non-zero. Note that $\widetilde{y} \in \frac{1}{2}\mathbb{Z}$ and $\widetilde{z} \in \mathbb{Z}$. Then we have

$$\Delta_0^2|\Delta| = \widetilde{Q}_{\ell,n}(\widetilde{x},\widetilde{y},\widetilde{z}) = |\Delta_0|\widetilde{x}^2 + 4\ell^{2n+1}\widetilde{y}^2 + \ell^{2n+1}|\Delta_0|\widetilde{z}^2 \geq \max\{4\ell^{2n+1}\widetilde{y}^2, \ell^{2n+1}|\Delta_0|\widetilde{z}^2\} \geq \ell^{2n+1}$$

which implies

$$n + 1 \leq \frac{\log(\Delta_0^2|\Delta|)}{2\log \ell} + \frac{1}{2}. \tag{2.24}$$

Combining now (2.24) with Lemma 2.5.5 concludes the first case of the proof of Theorem 2.5.1.

2.5.2 Second case of Theorem 2.5.1

For this part of the proof, we are going to heavily rely on [LV15], of which we have kept the notation. We again assume that the elliptic curve E_0 is given by an integral model over $\mathbb{Q}(j_0)$ that has good reduction at μ.

Suppose initially that ℓ divides the conductor of the order $\mathcal{O}_j$. Let $H_j \subseteq F$ be the minimal extension of the ring class field H_j such that there exists an elliptic curve $E_{j/F}$ with $j(E_j) = j$ and having good reduction at all primes of F lying above ℓ. Fix such an elliptic curve E_j and base-change it to the compositum $L = F \cdot H_{j_0}$. Consider also a prime $\mu_L \subseteq L$ lying above $\mu \subseteq H$ and denote by A the ring of integers in the completion of the maximal unramified extension of L_{μ_L}, with maximal ideal $\mu_L A \subseteq A$. The elliptic curves E_j and E_0 have good reduction over A and, since A is a complete discrete valuation ring of characteristic 0 with algebraically closed residue field of characteristic $\ell > 0$, we can use the same proof of Lemma 2.5.5 to see that

$$v_\mu(j - j_0) \leq v_{\mu_L}(j - j_0) \leq \frac{d_0}{2} \cdot \max\{n \in \mathbb{N}_{\geq 1} : \mathrm{Iso}_{A/\mu_L^n A}(E_j, E_0) \neq \emptyset\}. \tag{2.25}$$

Since $\ell \nmid \Delta_0$, we can now apply [LV15, Proposition 4.1] with $E = E_0$, $\mathcal{O}_{d_1} = \mathcal{O}_{j_0}$ and $\mathcal{O}_{d_2} = \mathcal{O}_j$. This proposition, used together with the fact that ℓ divides the conductor of $\mathcal{O}_j$, implies that $\mathrm{Iso}_{A/\mu_L^n A}(E_j, E_0) = \emptyset$ if $n > 1$. Combined with (2.25), this gives

$$v_\mu(j - j_0) \leq \frac{d_0}{2}$$

as desired. This yields the theorem in the case that ℓ divides the conductor of $\mathcal{O}_j$.

Assume now that ℓ divides Δ but does not divide the conductor of the order $\mathcal{O}_j$. Then, if again E_j is an elliptic curve with $j(E_j) = j$, we can choose $F = H_j$ as a field where E_j has a model with good reduction at all primes dividing ℓ. This follows from [ST68, Theorem 9]. If we complete H at μ, and we take A to be the ring of integers in the completion of the maximal unramified extension of H_μ and W to be the ring of integers in the completion of the maximal unramified extension of $\mathbb{Q}_\ell$, then $\mathrm{Frac}(W) \subseteq \mathrm{Frac}(A)$ is a ramified degree 2 field extension because the ramification index $e(\mu/\ell) = 2$ by our assumptions. Again by [LV15, Proposition 4.1], since we are assuming that ℓ does not divide the conductor of $\mathcal{O}_j$, for every $n \in \mathbb{N}_{>0}$ we have

$$\#\,\mathrm{Iso}_{A/\mu^n}(E_0, E_j) \leq C \cdot \# S_n^{\mathrm{Lie}}(E_0/A) \tag{2.26}$$

where $C = C(j) \leq 6$ is a positive constant depending on j and $S_n^{\mathrm{Lie}}(E_0/A)$ is the set of all endomorphisms $\varphi \in \mathrm{End}_{A/\mu^n}(E_0)$ satisfying the following three conditions (cfr. [LV15, pag. 9218]):

1. $\varphi^2 - \Delta\varphi + \frac{1}{4}(\Delta^2 - \Delta) = 0$;

2. The inclusion $\mathbb{Z}[\varphi] \hookrightarrow \mathrm{End}_{A/\mu^n}(E_0)$ is optimal at all primes $p \neq \ell$, see [LV15, Definition 2.1];

3. As endomorphism of $\mathrm{Lie}(E_0 \bmod \mu^n)$ we have $\varphi \equiv \delta \bmod \mu^n$, where $\delta \in A$ is a fixed root of the polynomial $x^2 - \Delta x + \frac{1}{4}(\Delta^2 - \Delta)$.

The set $S_n^{\mathrm{Lie}}(E_0/A)$ can be partitioned as

$$S_n^{\mathrm{Lie}}(E_0/A) = \bigcup_{m \in \mathbb{N}} S_{n,m}^{\mathrm{Lie}}(E_0/A)$$

where $S_{n,m}^{\mathrm{Lie}}(E_0/A)$ consists of all the endomorphisms $\varphi \in S_n^{\mathrm{Lie}}(E_0/A)$ such that

$$\mathrm{disc}\left(\mathcal{O}_{j_0}[\varphi]\right) = m^2.$$

We first claim that, under our assumptions, the sets $S_{n,0}^{\mathrm{Lie}}(E_0/A)$ are empty for all $n \in \mathbb{N}_{>0}$. Indeed, let $\varphi \in S_{n,0}^{\mathrm{Lie}}(E_0/A)$ so that $\mathrm{disc}\left(\mathcal{O}_{j_0}[\varphi]\right) = 0$. Since a quaternion algebra does not contain suborders of rank 3, this in particular implies that $\mathcal{O}_{j_0}[\varphi]$ has rank 2 as $\mathbb{Z}$-module, so that $\mathbb{Z}[\varphi]$ is isomorphic to an order in K_{j_0}, not necessarily contained in $\mathcal{O}_{j_0}$. By the definition of $S_n^{\mathrm{Lie}}(E_0/A)$, the order $\mathbb{Z}[\varphi]$ has discriminant Δ, and we deduce that $\mathbb{Z}[\varphi] \cong \mathcal{O}_j \subseteq K_{j_0}$. However, by assumption ℓ divides Δ but does not divide the conductor of $\mathcal{O}_j$. Hence ℓ must divide the discriminant of K_{j_0} which in turn implies $\ell \mid \Delta_0$, contradicting our hypotheses. This proves the claim.

On the other hand, in the second paragraph of [LV15, pag. 9247] it is proved that, when ℓ divides Δ but does not divide the conductor of $\mathcal{O}_j$, and $\ell \nmid \Delta_0$, then for every $m > 0$ and $n > 1$, the set $S_{n,m}^{\mathrm{Lie}}(E/A)$ is empty. We deduce that $S_n^{\mathrm{Lie}}(E/A) = \emptyset$ for all $n > 1$, and combining this with inequality (2.26) we obtain $\mathrm{Iso}_{A/\mu^n}(E_0, E_j) = \emptyset$ for all $n > 1$. Finally, using [GZ85, Proposition 2.3] (or Lemma 2.5.5) we obtain

$$v_\mu(j - j_0) = \frac{1}{2}\#\,\mathrm{Iso}_{A/\mu}(E_0, E_j) \leq \frac{d_0}{2}$$

and this concludes the proof of Theorem 2.5.1.

2.6 Other effective bounds on differences of singular moduli that are S-units

It is finally time to provide, for a given singular modulus j_0 and for specific sets of primes S, new effective bounds on the cardinality of the set of singular moduli j such that $j - j_0$ is an S-unit. In order to better state our main results, we introduce the following definition.

Definition 2.6.1. *Let $j \in \overline{\mathbb{Q}}$ be a singular modulus of discriminant Δ and let $S \subseteq \mathbb{N}$ be a finite set of prime numbers. We call the pair (j, S) a nice Δ-pair if the following two conditions hold:*

1. *every prime $\ell \in S$ splits completely in $\mathbb{Q}(j)$;*

2. *we have $\ell \nmid N_{\mathbb{Q}(j)/\mathbb{Q}}(j)N_{\mathbb{Q}(j)/\mathbb{Q}}(j-1728)\Delta$ for all $\ell \in S$, where $N_{\mathbb{Q}(j)/\mathbb{Q}}(\cdot)$ denotes the norm map from $\mathbb{Q}(j)$ to $\mathbb{Q}$.*

The goal of this section is to prove the following theorem.

Theorem 2.6.2. *Let (j_0, S) be a nice Δ_0-pair with $\Delta_0 < -4$ and $\#S \leq 2$. Then there exists an effectively computable bound $B = B(j_0, S) \in \mathbb{R}_{\geq 0}$ such that the discriminant Δ of every singular modulus $j \in \overline{\mathbb{Q}}$ for which $j - j_0$ is an S-unit satisfies $|\Delta| \leq B$. Moreover, if the extension $\mathbb{Q} \subseteq \mathbb{Q}(j_0)$ is not Galois, then the discriminant Δ of any singular modulus j such that $j - j_0$ is an S-unit is of the form $\Delta = p^n\Delta_0$ for some prime $p \in S$.*

The reason why Theorem 2.6.2 only deals with sets S containing at most two primes will be apparent from its proof, which we now sketch. Our strategy follows the same idea used in [Hab15] and [BHK20]: given a singular modulus $j \in \overline{\mathbb{Q}}$ such that $j - j_0$ is an S-unit, we compute the (logarithmic) Weil height $h(j - j_0)$. As one can see from its definition (2.1), the logarithmic Weil height naturally decomposes into an "archimedean" and "non-archimedean" part. Since $j - j_0$ is an algebraic integer, the non-archimedean part of its Weil height vanishes. In order to exploit the fact that the above difference is an S-unit, we rather compute the height of $(j - j_0)^{-1}$. Using standard properties of the Weil height, we obtain

$$h(j - j_0) = h((j - j_0)^{-1}) = (\text{archimedean part}) + (\text{non-archimedean part})$$

with

$$(\text{non-archimedean part}) = \frac{\log \ell}{[\mathbb{Q}(j - j_0) : \mathbb{Q}]} \sum_{\mathfrak{p}} f_{\mathfrak{p}} \cdot v_{\mathfrak{p}}(j - j_0)$$

where the sum is taken over the prime ideals of $\mathbb{Q}(j - j_0)$ lying above the rational primes contained in S. Our goal is to effectively bound this height from above and from below in such a way that the two bounds contradict each other when the absolute value of the discriminant of the singular modulus j becomes large. This will give the desired effective bound.

An upper bound for the archimedean part has been already studied in [BHK20] and [Cai21]. In order to estimate from above the non-Archimedean part, we will use Theorem 2.5.1 proved in the previous section. Concerning the lower bound for the Weil height, we compare it to the stable Faltings height of the elliptic curve with complex multiplication having j as singular invariant. Using work of Colmez [Col98] and Nakkajima-Taguchi [NT91] it is possible to relate this Faltings height to the logarithmic derivative of the L-function corresponding to the CM field evaluated in 1. The known lower bounds on this logarithmic derivative become strong enough for our purposes only if we restrict to sets S containing no more than two primes.

Proof of Theorem 2.6.2. Let (j_0, S) be a nice Δ_0-pair with $\Delta_0 < -4$ and $\#S \leq 2$. We can assume without loss of generality that $\#S = 2$, since if S contains fewer than two elements the statement of the theorem becomes weaker. Hence we can write $S = \{\ell_1, \ell_2\}$ with $\ell_1, \ell_2 \in \mathbb{N}$ two distinct primes.

In order to prove Theorem 2.6.2, we follow the strategy used in [BHK20] to prove the emptiness of the set of singular units. Let j be a singular modulus of discriminant Δ such that $j - j_0$ is an S-unit, and let $h(\cdot)$ denote the logarithmic Weil height on algebraic numbers. By the usual properties of height functions [BG06, Lemma 1.5.18], we have

$$h(j - j_0) = h((j - j_0)^{-1}) = \frac{1}{[\mathbb{Q}(j - j_0) : \mathbb{Q}]} \sum_{v \in \mathcal{M}_{\mathbb{Q}(j-j_0)}} d_v \log^+ |(j - j_0)^{-1}|_v = A + N \tag{2.27}$$

where $d_v := [\mathbb{Q}_v(j - j_0) : \mathbb{Q}_v]$ is the local degree of the field $\mathbb{Q}(j - j_0)$ at the place v and

$$A := \frac{1}{[\mathbb{Q}(j - j_0) : \mathbb{Q}]} \sum_{v \in \mathcal{M}^{\infty}_{\mathbb{Q}(j-j_0)}} d_v \log^+ |(j - j_0)^{-1}|_v,$$
$$N := \frac{1}{[\mathbb{Q}(j - j_0) : \mathbb{Q}]} \sum_{v | \ell_1 \ell_2} d_v \log |(j - j_0)^{-1}|_v$$

are, respectively, the archimedean and non-archimedean components of the height. Notice that the expression for N follows from our assumption on j being an S-unit. We study these two components separately, starting with the archimedean one. From now on, we assume $|\Delta| > \max\{|\Delta_0|, 10^{15}\}$.

Denote by C_0 and C_Δ the class numbers of the orders associated to j_0 and to j respectively. Then by [Cai21, Corollary 4.2 (1)] we have

$$A \leq \frac{8F \log |\Delta| \cdot C_0}{[\mathbb{Q}(j - j_0) : \mathbb{Q}]} + \log \left(\frac{F \log |\Delta| \cdot C_0 \cdot |\Delta|^{1/2}}{[\mathbb{Q}(j - j_0) : \mathbb{Q}]} \right) + 4 \log |\Delta_0| + 0.33 \tag{2.28}$$

where $F := \max\{2^{\omega(a)} : a \leq |\Delta|^{1/2}\}$ and $\omega(n)$ denotes the number of prime divisors of an integer $n \in \mathbb{N}$. Using [FR18, Theorem 4.1] we have

$$[\mathbb{Q}(j - j_0) : \mathbb{Q}] = [\mathbb{Q}(j, j_0) : \mathbb{Q}] \geq [\mathbb{Q}(j) : \mathbb{Q}] = C_\Delta$$

which, combined with (2.28), gives

$$A \leq \frac{8F \log |\Delta| \cdot C_0}{C_\Delta} + \log \left(\frac{F \log |\Delta| \cdot C_0 \cdot |\Delta|^{1/2}}{C_\Delta} \right) + 4 \log |\Delta_0| + 0.33. \tag{2.29}$$

As far as the non-archimedean part is concerned, we have

$$\begin{aligned} N &= \frac{1}{[\mathbb{Q}(j - j_0) : \mathbb{Q}]} \sum_{v | \ell_1 \ell_2} d_v \log |(j - j_0)^{-1}|_v = \frac{1}{[\mathbb{Q}(j - j_0) : \mathbb{Q}]} \sum_{\mathfrak{p} | \ell_1 \ell_2} v_{\mathfrak{p}}(j - j_0) \log \ell_i^{f_{\mathfrak{p}}} \qquad (2.30) \\ &= \frac{\log \ell_1}{[\mathbb{Q}(j - j_0) : \mathbb{Q}]} \sum_{\mathfrak{p} | \ell_1} v_{\mathfrak{p}}(j - j_0) f_{\mathfrak{p}} + \frac{\log \ell_2}{[\mathbb{Q}(j - j_0) : \mathbb{Q}]} \sum_{\mathfrak{p} | \ell_2} v_{\mathfrak{p}}(j - j_0) f_{\mathfrak{p}} \end{aligned}$$

where $f_\mathfrak{p}$ denotes the residue degree of the prime $\mathfrak{p} \subseteq \mathbb{Q}(j-j_0)$ lying above ℓ. For every such $\mathfrak{p}$, we choose a prime ideal $\mu \subseteq H$ that divides $\mathfrak{p}$, where H denotes the compositum inside $\overline{\mathbb{Q}}$ of the ring class fields relative to j and j_0. Note that this makes sense, since we have $\mathbb{Q}(j-j_0) \subseteq \mathbb{Q}(j, j_0) \subseteq H$ (the first inclusion is actually an equality by [FR18, Theorem 4.1]). We wish now to use Theorem 2.5.1 to bound $v_\mu(j-j_0)$ for all these primes μ. Let's check that the hypotheses of the theorem are verified in our context:

- since we are assuming $|\Delta_0| < |\Delta|$, certainly we have $\Delta \neq \Delta_0$;
- since (j_0, S) is a nice Δ_0-pair, for $i \in \{1,2\}$ the prime ℓ_i splits completely in $\mathbb{Q}(j_0)$. In particular, $\mu \cap \mathbb{Q}(j_0)$ has residue degree 1, as required;
- since (j_0, S) is a nice Δ_0-pair, for $i \in \{1,2\}$ the prime ℓ_i does not divide both Δ_0 and $N_{\mathbb{Q}(j_0)/\mathbb{Q}}(j_0(j_0-1728))$. In particular, this last condition implies that $j_0 \neq 0, 1728$ and that the elliptic curve

$$E_{0/\mathbb{Q}(j_0)} : y^2 + xy = x^3 - \frac{36}{j_0 - 1728}x - \frac{1}{j_0 - 1728}$$

with $j(E_0) = j_0$, has good reduction at μ.

This discussion shows that we can apply Theorem 2.5.1 to bound $v_\mu(j-j_0)$. Notice that under our assumptions we have, in the notation of the theorem, that $d_0 = 2$ since $\ell_i \nmid N_{\mathbb{Q}(j_0)/\mathbb{Q}}(j_0(j_0-1728))$ for $i \in \{1,2\}$. Moreover, the imaginary quadratic order associated to j cannot contain the order associated to j_0 because $|\Delta| > |\Delta_0|$. Thus we obtain

$$v_\mathfrak{p}(j-j_0) \leq v_\mu(j-j_0) \leq \max\left\{\frac{\log(\Delta_0^2|\Delta|)}{2\log \ell_i} + \frac{1}{2}, 1\right\}$$

for all primes $\mathfrak{p} \mid \ell_i$. Combining this with (2.30) we obtain

$$\begin{aligned} N &\leq \max\left\{\frac{\log(\Delta_0^2|\Delta|)}{2\log(\min\{\ell_1,\ell_2\})} + \frac{1}{2}, 1\right\} \frac{\log(\max\{\ell_1,\ell_2\})}{[\mathbb{Q}(j-j_0):\mathbb{Q}]} \sum_{\mathfrak{p}|\ell_1\ell_2} f_\mathfrak{p} \\ &\leq 2\max\left\{\frac{\log(\Delta_0^2|\Delta|)}{2\log(\min\{\ell_1,\ell_2\})} + \frac{1}{2}, 1\right\} \cdot \log(\max\{\ell_1,\ell_2\}) \end{aligned} \tag{2.31}$$

where we have used the fact that, for every number field K and any prime $q \in \mathbb{N}$, we always have $\sum_{\mathfrak{q}|q} f_\mathfrak{q} \leq [K:\mathbb{Q}]$ (here the sum is taken over the prime ideals of K lying above q). For ease of notation, set $L := \max\{\ell_1,\ell_2\}$ and $\ell = \min\{\ell_1,\ell_2\}$. Using now together (2.29) and (2.31) we obtain the following upper bound

$$\begin{aligned} h(j-j_0) \leq \frac{8F\log|\Delta| \cdot C_0}{C_\Delta} &+ \log\left(\frac{F\log|\Delta| \cdot C_0 \cdot |\Delta|^{1/2}}{C_\Delta}\right) + 4\log|\Delta_0| + 0.33 \\ &+ \max\left\{\log(\Delta_0^2|\Delta|) \cdot \frac{\log L}{\log \ell} + \log L, 2\log L\right\} \end{aligned} \tag{2.32}$$

for the Weil height of $j - j_0$. We now look into lower bounds.

In order to find a lower bound for $h(j-j_0)$, we first reduce to the problem of finding a lower bound for $h(j)$ by means of the elementary inequality

$$h(j-j_0) \geq h(j) - h(j_0) - \log 2$$

see [BG06, Proposition 1.5.15]. As for bounding $h(j)$, we use the lower bound [BHK20, Proposition 4.3]

$$h(j) \geq \frac{3}{\sqrt{5}} \log|\Delta| - 9.79$$

together with [BHK20, Proposition 4.1]

$$h(j) \geq \frac{\pi|\Delta|^{1/2} - 0.01}{C_\Delta} \tag{2.33}$$

which generally holds for $|\Delta| \geq 16$. Combining (2.6) with (2.33), and adding 1 on both sides, we obtain

$$Y(\Delta) := \max\left\{\frac{3}{\sqrt{5}}\log|\Delta| - 9.78, \frac{\pi|\Delta|^{1/2}}{C_\Delta}\right\} \leq h(j-j_0) + h(j_0) + \log 2 + 1. \tag{2.34}$$

Concatenating now (2.34) with (2.32), and dividing both sides by $Y(\Delta)$, yields the inequality

$$1 \leq A(\Delta) + B(\Delta) + C_\Delta + D(\Delta) \tag{2.35}$$

where

$$\begin{aligned}
A(\Delta) &= \frac{8F\log|\Delta| \cdot C_0}{Y(\Delta)C_\Delta}, \\
B(\Delta) &= \frac{\log(F\log|\Delta|) + 4\log|\Delta_0| + h(j_0) + 1.33 + \log 2}{Y(\Delta)}, \\
C(\Delta) &= \frac{1}{Y(\Delta)}\log\left(\frac{|\Delta|^{1/2}}{C_\Delta}\right) \\
D(\Delta) &= \frac{1}{Y(\Delta)} \cdot \max\left\{\log(\Delta_0^2|\Delta|) \cdot \frac{\log L}{\log \ell} + \log L, 2\log L\right\}.
\end{aligned}$$

We want to show that (2.35) cannot hold if $|\Delta|$ is sufficiently large. As far as estimating the first three terms of (2.35) is concerned, we find ourselves in the same situation as Cai in [Cai21, Sections 6.1-6.4], and we can directly use the bounds therein obtained. More precisely from [Cai21, Section 6.2] we have, since $|\Delta| > 10^{15}$, that

$$A(\Delta) \leq \frac{8F\log|\Delta| \cdot C_0}{\pi|\Delta|^{1/2}} \leq \frac{8C_0}{\pi}|\Delta|^{-0.1908}$$

so for every $\varepsilon_A > 0$,

$$A(\Delta) \leq \frac{8C_0}{\pi}|\Delta|^{-0.1908} < \varepsilon_A \tag{2.36}$$

holds for $|\Delta|$ sufficiently large. Moreover, using

$$\log(F \log|\Delta|) \leq \frac{\log 2}{2} \cdot \frac{\log|\Delta|}{\log\log|\Delta| - c_1 - \log 2} + \log\log|\Delta|$$

which is [BHK20, Inequality (5.8)] (here $c_1 \in \mathbb{R}$ is an effectively computable absolute constant defined in [BHK20, Section 5.2]), we have that, for every $\varepsilon_B > 0$, the inequality

$$B(\Delta) \leq \frac{1}{(3/\sqrt{5})\log|\Delta| - 9.78}\left(\frac{\log 2}{2} \cdot \frac{\log|\Delta|}{\log\log|\Delta| - c_1 - \log 2} + \log\log|\Delta| + K\right) < \varepsilon_B \tag{2.37}$$

where $K := 4\log|\Delta_0| + h(j_0) + 1.33 + \log 2$, holds for $|\Delta|$ sufficiently large. Finally, using the fact that $x \mapsto \log(x)/x$ is a decreasing function when $x \geq 4$, for every $\varepsilon_C > 0$ one has

$$C_\Delta \leq \frac{1}{Y(\Delta)} \log\left(\pi^{-1} Y(\Delta)\right) \leq \frac{1}{(3/\sqrt{5})\log|\Delta| - 9.78} \log\left(\pi^{-1}\left(\frac{3}{\sqrt{5}}\log|\Delta| - 9.78\right)\right) < \varepsilon_C \tag{2.38}$$

for $|\Delta|$ sufficiently large. We are then left with bounding $D(\Delta)$ from above. For $|\Delta| \geq (\log \ell)/|\Delta_0|^2$ we have

$$\begin{aligned} D(\Delta) &= \frac{1}{Y(\Delta)} \cdot \log(\Delta_0^2|\Delta|) \cdot \frac{\log L}{\log \ell} + \log L \\ &\leq \frac{1}{\frac{3}{\sqrt{5}}\log|\Delta| - 9.78} \cdot \left(\log|\Delta| + \log L\left(\frac{\log \Delta_0^2}{\log \ell} + 1\right)\right) \\ &= \frac{\sqrt{5}}{3} + \frac{1}{\frac{3}{\sqrt{5}}\log|\Delta| - 9.78} \cdot \left(\frac{\sqrt{5}}{3} \cdot 9.78 + \log L\left(\frac{\log \Delta_0^2}{\log \ell} + 1\right)\right) \end{aligned}$$

so for every $\varepsilon_D > 0$ we obtain

$$D(\Delta) \leq \frac{\sqrt{5}}{3} + \varepsilon_D \leq 0.75 + \varepsilon_D \tag{2.39}$$

for $|\Delta|$ sufficiently large (depending on Δ_0 and ℓ_1, ℓ_2). We can now combine (2.36), (2.37), (2.38), (2.39) with (2.35) to obtain

$$1 \leq \varepsilon_A + \varepsilon_B + \varepsilon_C + \varepsilon_D + 0.75 \tag{2.40}$$

which holds for $|\Delta| \gg_{\ell_1,\ell_2,\Delta_0,\varepsilon_A,\varepsilon_B,\varepsilon_C,\varepsilon_D} 0$. Choosing $\varepsilon_A, \varepsilon_B, \varepsilon_C, \varepsilon_D$ small enough, the inequality cannot be verified for arbitrary large $|\Delta|$. This proves that there are finitely many singular moduli j such that $j - j_0$ is an S-unit, and concludes the proof of the first part of Theorem 2.6.2.

We now begin the proof of the second part of Theorem 2.6.2. Suppose $\mathbb{Q} \subseteq \mathbb{Q}(j_0)$ is not Galois. We first claim that every prime in S must be split in $\mathbb{Q}(\sqrt{\Delta_0})$. Indeed, assume by contradiction that a prime $\ell \in S$ is inert in $\mathbb{Q}(\sqrt{\Delta_0})$ (it cannot ramify by definition of nice Δ_0-pair). Let $H_O := \mathbb{Q}(j_0, \sqrt{\Delta_0})$ which is a semidihedral Galois extension of $\mathbb{Q}$, and let

$$H := \mathrm{Gal}(H_O/\mathbb{Q}(j_0)) \subseteq \mathrm{Gal}(H_O/\mathbb{Q}) =: G$$

with generator $\sigma \in H$. Consider the set $\mathcal{S}$ of left cosets of H in G. Since ℓ splits completely in $\mathbb{Q}(j_0)$ and is inert in $\mathbb{Q}(\sqrt{\Delta_0})$, there exists an element of G which does not restrict to the identity on $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{\Delta_0})$ and such that its left-multiplication action on $\mathcal{S}$ is trivial. The only possible automorphism which satisfies these two conditions is $\sigma \in H$. On the other hand, for every $\tau \in G$ with $\tau \notin H$, we must have $\sigma\tau H = \tau H$. This implies that either $\sigma\tau = \tau$ or $\sigma\tau = \tau\sigma$. Since $\sigma \neq 1$ by assumption, the first possibility cannot hold, and we deduce that σ commutes with every element of G. Hence G must be abelian, and we reach the desired contradiction.

Let now $j \in \overline{\mathbb{Q}}$ be a singular modulus of discriminant Δ such that $j - j_0$ is an S-unit. Since $j - j_0$ cannot be a unit by Theorem 2.1.4, there exists a prime $\ell \in S$ dividing the norm of $j - j_0$. This implies that there exists a number field K, a prime $\mu \subseteq K$ lying above ℓ and two elliptic curves E_0, E_j defined over K with good reduction at μ such that $j(E_j) = j$, $j(E_0) = j_0$ and $E_0 \bmod \mu \cong_{\overline{\mathbb{F}}_\ell} E_j \bmod \mu$. Moreover, since ℓ splits in $\mathbb{Q}(\sqrt{\Delta_0})$ by the discussion above, both E_0 and E_j have ordinary reduction modulo μ by Theorem 1.4.1. From the same theorem and the fact that $\ell \nmid \Delta_0$, we deduce that $\Delta = \ell^n \Delta_0$, as wanted. □

The bound $B(j_0, S)$ in the statement of Theorem 2.6.2 can be made explicit from its proof. To give an idea of what kind of bounds one can get, we take $j_0 = -3375$, the j-invariant of any elliptic curve with complex multiplication by $\mathbb{Z}[(1+\sqrt{-7})/2]$, and choose S to be any subset of at most two elements in $\{13, 17, 19\}$. We get the following result.

Theorem 2.6.3. *Let $j \in \overline{\mathbb{Q}}$ be a singular modulus of discriminant Δ, and let $S := \{13, 17\}$. If $j + 3375$ is an S-unit, then $|\Delta| \leq 10^{84}$. The same holds with $S' = \{13, 19\}$ and $S'' = \{17, 19\}$.*

Proof. Choose the nice (-7)-pair $(-3375, \{13, 17\})$ and $|\Delta| > 10^{84}$. A combination of the inequalities (2.36), (2.37), (2.38) and (2.39) gives

$$\varepsilon_A + \varepsilon_B + \varepsilon_C + \varepsilon_D < 0.2482$$

and this violates inequality (2.40). The same happens with the other choices of primes in the theorem. □

2.7 Round 2: more automorphisms enter the ring

In the statement of Theorem 2.6.2 we have excluded the discriminants $\Delta_0 \in \{-3, -4\}$, *i.e.* the singular moduli $j_0 \in \{0, 1728\}$. In these cases, the same techniques also lead to similar finiteness results, but one has to be more careful to the extra automorphisms possessed by the complex elliptic curves having j_0 as singular invariant. This is indeed a problem, and will force us to resort to the Generalized Riemann Hypothesis (GRH) in the case $j_0 = 0$. Here are the results that we obtain in these two cases.

Theorem 2.7.1. *Let S_0 be the set of rational primes congruent to 1 modulo 4, let $\ell \geq 5$ be an arbitrary prime and set $S_\ell := S_0 \cup \{\ell\}$. Then there exists an effectively computable bound $B = B(\ell) \in \mathbb{R}_{\geq 0}$ such that the discriminant Δ of every singular modulus $j \in \overline{\mathbb{Q}}$ for which $j - 1728$ is an S_ℓ-unit satisfies $|\Delta| \leq B$.*

Theorem 2.7.2. *Let S_0 be the set of rational primes congruent to 1 modulo 3, let $\ell \geq 5$ be an arbitrary prime and set $S_\ell := S_0 \cup \{\ell\}$. If the Generalized Riemann Hypothesis holds for the Dirichlet L-functions attached to imaginary quadratic number fields, then there exists an effectively computable bound $B = B(\ell) \in \mathbb{R}_{\geq 0}$ such that the discriminant Δ of every singular S_ℓ-unit $j \in \overline{\mathbb{Q}}$ satisfies $|\Delta| \leq B$.*

The proofs of Theorems 2.7.1 and 2.7.2, after a preliminary reduction step, become analogous to the proof of Theorem 2.6.2. We have chosen to only sketch the proofs of the two aforementioned theorems, outlining with all the details only the parts in which they differ from the proof of Theorem 2.6.2. We begin with Theorem 2.7.1.

Proof of Theorem 2.7.1. First of all, we show that it is sufficient to prove that, under the assumptions of the theorem, the set of singular moduli j such that $j - 1728$ is an $\{\ell\}$-unit is finite and its cardinality can be effectively bounded. Indeed, suppose that $j - 1728$ is a singular S_ℓ-unit and assume that $p \in S_0$ is a prime dividing its norm $N_{\mathbb{Q}(j)/\mathbb{Q}}(j - 1728)$. It has been proved in Theorem 2.2.1 that in this case, there are at least other 3 primes not congruent to 1 modulo 4 dividing this norm. In particular, $j - 1728$ cannot be a singular S_ℓ-unit.

Hence we are reduced to bound the number of singular moduli j such that $j - 1728$ is an $\{\ell\}$-unit for $\ell \geq 5$ a prime congruent to 3 modulo 4. Let then $j \in \overline{\mathbb{Q}}$ be a singular modulus such that $j - 1728$ is an $\{\ell\}$-unit. In the same way as in the previous section, we compute the Weil height

$$h(j-1728) = h((j-1728)^{-1}) = \frac{1}{[\mathbb{Q}(j):\mathbb{Q}]} \sum_{v \in M_{\mathbb{Q}(j)}} d_v \log^+ |(j-1728)^{-1}|_v = A + N \qquad (2.41)$$

where, again, $d_v := [\mathbb{Q}_v(j) : \mathbb{Q}_v]$ is the local degree at the place v and

$$A := \frac{1}{[\mathbb{Q}(j):\mathbb{Q}]} \sum_{v \in M_{\mathbb{Q}(j)}^\infty} d_v \log^+ |(j-1728)^{-1}|_v \quad \text{and} \quad N := \frac{1}{[\mathbb{Q}(j):\mathbb{Q}]} \sum_{v \mid \ell} d_v \log^+ |(j-1728)^{-1}|_v$$

are, respectively, the archimedean and non-archimedean components of the height. For $|\Delta|$ big enough, we can bound the archimedean component using again the work of Cai [Cai21]. More precisely, [Cai21, Corollary 4.2] gives for $|\Delta| \geq 10^{14}$

$$A \leq \frac{4F \log|\Delta|}{C_\Delta} + 2 \log \frac{F|\Delta|^{1/2} \log|\Delta|}{C_\Delta} - 2.68 \qquad (2.42)$$

where C_Δ is the class number of the order of discriminant Δ and $F = \max\{2^{\omega(a)} : a \leq |\Delta|^{1/2}\}$ as in the previous section. The non-archimedean component can be rewritten as

$$N = \frac{1}{[\mathbb{Q}(j):\mathbb{Q}]} \sum_{\mathfrak{p} \mid \ell} v_\mathfrak{p}(j-1728) \log \ell^{f_\mathfrak{p}} = \frac{\log \ell}{[\mathbb{Q}(j):\mathbb{Q}]} \sum_{\mathfrak{p} \mid \ell} v_\mathfrak{p}(j-1728) f_\mathfrak{p} \qquad (2.43)$$

where the sum runs over primes $\mathfrak{p}$ of $\mathbb{Q}(j)$ lying above ℓ, and $f_\mathfrak{p}$ denotes the residue degree of $\mathfrak{p}$ over ℓ. To estimate the valuation above, we can apply Theorem 2.5.1 since all the hypotheses are met also in this case: ℓ has certainly degree 1 in $\mathbb{Q}(1728) = \mathbb{Q}$ and is coprime with $-4 = \operatorname{disc} \mathbb{Q}(i)$. Moreover, the elliptic curve $E_{1728/\mathbb{Q}} : y^2 = x^3 + x$ has $j(E_{1728}) = 1728$ and good reduction at all primes $\ell \neq 2, 3$. We deduce that for all $\mathfrak{p} \mid \ell$ we have

$$v_\mathfrak{p}(j-1728) \leq \max\left\{\frac{\log(16|\Delta|)}{\log \ell} + 1, 2\right\}$$

where in the application of Theorem 2.5.1 one has $d_0 = 4$ since $\ell \geq 5$ (see [Sil09, III, Theorem 10.1]). Combining the above estimate with (2.43) we obtain

$$N \leq \max\{\log(16|\Delta|) + \log \ell, 2\log \ell\} \tag{2.44}$$

so putting together (2.42) and (2.44) we get

$$h(j - 1728) \leq \frac{4F \log|\Delta|}{h_\Delta} + 2\log \frac{F|\Delta|^{1/2} \log|\Delta|}{h_\Delta} - 2.68 + \max\{\log|\Delta| + \log \ell, 2\log \ell\} \tag{2.45}$$

for $|\Delta| \geq 10^{14}$. Now the lower bound (2.34) allows to conclude exactly in the same way as in the proof of Theorem 2.6.2. □

As the reader may have noticed, the intimate reason why the proofs of Theorems 2.6.2 and 2.7.1 work out, is that the lower bound (2.34) is sufficiently good to prevail on the estimates (2.31) and (2.44) for the non-archimedean parts of the relevant Weil heights. This will not be the case for $j_0 = 0$, since in this case one has to take $d_0 \geq 6$ in the inequalities of Theorem 2.5.1. This is the reason why the proof of Theorem 2.7.2 is conditional under GRH. However, Theorem 2.7.2 does not need the full strength of the Generalized Riemann Hypothesis to be proved, but only that a weaker condition on the Dirichlet L-functions associated to imaginary quadratic fields holds. The goal of the subsequent discussion is to introduce this condition, and to deduce from its assumption a lower bound for the Weil height of a singular modulus that is sharp enough to prove Theorem 2.7.2 with our methods.

Recall that non-principal real primitive Dirichlet characters are precisely the Kronecker symbols attached to quadratic field extensions of $\mathbb{Q}$. We say that such a Dirichlet character has discriminant $D \in \mathbb{Z}$ if it is the Kronecker symbol attached to a quadratic field of discriminant D.

Definition 2.7.3. *Let $k \in \mathbb{R}$ be a non-negative real number. A non-principal real primitive Dirichlet character χ of discriminant D is said to satisfy property $P(k)$ if*

$$\frac{L'(\chi, 1)}{L(\chi, 1)} \geq -0.2485 \log|D| - k$$

where the left-hand side of the inequality is the logarithmic derivative of the Dirichlet L-function $L(\chi, s)$ associated to χ.

Remark 2.7.4. The inequality appearing in Definition 2.7.3 may seem a bit arbitrary, and indeed it is. Actually for our purposes, we could take any inequality of the form

$$\frac{L'(\chi, 1)}{L(\chi, 1)} \geq -c \log|D| - k$$

with $c < 0.25$ as a definition for the property $P(k)$, and all the following proofs would work in the same way.

Remark 2.7.5. It is proved in [MK13] that the logarithmic derivative of Dirichlet L-functions attached to Kronecker symbols of imaginary quadratic fields is actually positive for infinitely many negative fundamental discriminants. In particular, property $P(0)$ holds for infinitely many real primitive Dirichlet characters of negative discriminant.

Let now $j \in \overline{\mathbb{Q}}$ be a singular modulus relative to an order in the imaginary quadratic field K. Under the assumption that the Legendre symbol associated to K satisfies property $P(k)$ for some non-negative $k \in \mathbb{R}$, we are able to provide a lower bound for the Weil height of j in terms of its discriminant Δ. In order to make this assertion precise, we introduce some notation. For an elliptic curve E defined over a number field L, denote by $h_F(E)$ its stable Faltings height [Fal83, pag. 354] with Deligne's normalization [Del85]. We continue writing $h : \overline{\mathbb{Q}} \longrightarrow \mathbb{R}$ for the logarithmic Weil height of an algebraic number.

Proposition 2.7.6. *Let j be a singular modulus of discriminant $\Delta = f^2\Delta_K$, where Δ_K is the discriminant of the imaginary quadratic field K relative to j. If for some $k \in \mathbb{R}_{\geq 0}$ property $P(k)$ holds for the non-principal real primitive Dirichlet character χ of discriminant Δ_K, then*

$$h(j) \geq 1.509 \log|\Delta| + C$$

for some absolute constant $C = C(k) \in \mathbb{R}$.

Proof. Let $E_{/\mathbb{Q}(j)}$ be an elliptic curve with $j(E) = j$. Using [GR14, Lemma 7.9], the logarithmic Weil height of j can be bounded from below by the stable Faltings height of E as follows:

$$h(j) \geq 12h_F(E) + 8.64. \tag{2.46}$$

The stable Faltings height of E can be explicitely computed using the well-known results of Colmez [Col98] and Nakkajima-Taguchi [NT91]. One has

$$h_F(E) = \frac{1}{4}\log(|\Delta|) + \frac{1}{2}\frac{L'(\chi,1)}{L(\chi,1)} - \frac{1}{2}\left(\sum_{p|f} e_f(p)\log p\right) - \frac{1}{2}(\gamma + \log(2\pi))$$

where χ is the Kronecker symbol relative to the CM field K, γ is the Euler-Mascheroni constant, f is the conductor of the CM order and for a prime p

$$e_f(p) := \frac{1-\chi(p)}{p-\chi(p)}\frac{1-p^{-v_p(f)}}{1-p^{-1}}.$$

Using property $P(k)$ we then get

$$\begin{aligned}
h_F(E) &> \frac{1}{4}\log(|\Delta|) + \frac{1}{2}\left(-0.2485\log|\Delta_K| - k\right) - \frac{1}{2}\left(\sum_{p|f} e_f(p)\log p\right) - \frac{1}{2}(\gamma + \log(2\pi)) \\
&= \frac{1}{4}\log(|\Delta|) + \frac{1}{2}(-0.2485\log|\Delta| - 0.2485\log f^{-2} - k) - \frac{1}{2}\left(\sum_{p|f} e_f(p)\log p\right) - \frac{1}{2}(\gamma + \log(2\pi)) \\
&= 0.12575\log|\Delta| + 0.2485\log f - \frac{1}{2}\left(\sum_{p|f} e_f(p)\log p\right) - \frac{1}{2}(\gamma + \log(2\pi) + k).
\end{aligned}$$

We want to bound from below the quantity

$$A(f) := 0.2485\log f - \frac{1}{2}\left(\sum_{p|f} e_f(p)\log p\right).$$

To do this, one can proceed exactly as in [BHK20, Section 4]. First, one notices that

$$e_f(p) \leq \frac{2}{p+1} \cdot \frac{1-p^{-v_p(f)}}{1-p^{-1}}$$

by considering all the possible values of the Dirichlet character $\chi(p)$. Setting now for all $n \in \mathbb{N}_{>0}$

$$\delta(n) := 0.2485 \log n - \left(\sum_{p \mid n} \frac{\log p}{p+1} \cdot \frac{1-p^{-v_p(n)}}{1-p^{-1}} \right),$$

one notices that $\delta(n)$ is an additive function and satisfies $\delta(p^{k+1}) \geq \delta(p^k)$ for all primes $p \in \mathbb{N}$ and integers $k > 0$. Since one has $\delta(2), \delta(3) < 0$ and $\delta(p) > 0$ for all primes $p \geq 5$, we deduce that $\delta(n) \geq \delta(2) + \delta(3)$ for all $n \in \mathbb{N}_{>0}$. We then have

$$A(f) \geq \delta(f) \geq \delta(2) + \delta(3) = 0.2485(\log 2 + \log 3) - \left(\frac{\log 2}{3} + \frac{\log 3}{4} \right) \geq -0.0605.$$

In conclusion, we obtain

$$h_F(E) > 0.12575 \log |\Delta| - C_0 \tag{2.47}$$

where we set

$$C_0 = \frac{1}{2}(\gamma + \log(2\pi) + k) + 0.0605.$$

Combining now (2.46) with (2.47) we obtain

$$h(j) > 1.509 \log |\Delta| - 12C_0 + 8.64$$

and this concludes the proof. □

We now state and prove a stronger version of Theorem 2.7.2, whose proof relies on the use of property $P(k)$ rather than on the use of GRH. We then show how Theorem 2.7.2 follows from this stronger statement.

Theorem 2.7.7. *Let S_0 be the set of rational primes congruent to 1 modulo 3, let $\ell \geq 5$ be an arbitrary prime and set $S_\ell := S_0 \cup \{\ell\}$. Assume that all the Kronecker symbols χ_D attached to an imaginary quadratic field of discriminant D satisfy property $P(k)$ for some fixed $k \in \mathbb{R}_{\geq 0}$. Then there exists an effectively computable bound $B = B(\ell, k) \in \mathbb{R}_{\geq 0}$ such that the discriminant Δ_j of every singular S_ℓ-unit $j \in \overline{\mathbb{Q}}$ satisfies $|\Delta_j| \leq B$. In particular, the set of singular moduli that are S_ℓ-units is finite and its cardinality can be effectively bounded.*

Proof. The proof is essentially identical to the proof of Theorem 2.7.1, and we only sketch the argument. First of all, it is again sufficient to prove that, under the assumptions of the theorem, the set of singular $\{\ell\}$-units is finite and its cardinality can be effectively bounded. This follows in the same way as done at the beginning of the proof of Theorem 2.7.1, again appealing to Theorem 2.2.1. Hence we are reduced to bound the number of singular $\{\ell\}$-units for $\ell \geq 5$ a prime congruent to 2 modulo 3. Let j be a singular $\{\ell\}$-unit relative to the order $\mathcal{O}$ of discriminant Δ. Again, one decomposes its logarithmic Weil $h(j)$ height into a sum $h(j) = A + N$ of an archimedean and a non-archimedean component.

The archimedean component A has been studied in [BHK20, Corollary 3.2]. Here it is proved that, for $|\Delta| \geq 10^{14}$, we have

$$A \leq \frac{12F\log|\Delta|}{C_\Delta} + 3\log\frac{F|\Delta|^{1/2}\log|\Delta|}{C_\Delta} - 3.77 \tag{2.48}$$

where C_Δ is the usual class number of the order of discriminant Δ and $F = \max\{2^{\omega(a)} : a \leq |\Delta|^{1/2}\}$. The non-archimedean part can be written as

$$N = \frac{\log\ell}{[\mathbb{Q}(j):\mathbb{Q}]}\sum_{\mathfrak{p}|\ell} v_{\mathfrak{p}}(j)f_{\mathfrak{p}} \tag{2.49}$$

where $f_{\mathfrak{p}}$ denotes the residue degree of the prime $\mathfrak{p} \subseteq \mathbb{Q}(j)$ lying above ℓ. Using Theorem 2.5.1 with the elliptic curve $E_{0/\mathbb{Q}} : y^2 = x^3 + 1$ with $j(E_0) = 0$ and noticing that $d_0 = 6$ because $\ell \geq 5$ we have

$$v_{\mathfrak{p}}(j) \leq \max\left\{3\left(\frac{\log 9|\Delta|}{2\log\ell} + \frac{1}{2}\right), 3\right\}$$

and, combining this estimate with equality (2.49), we get

$$N \leq \max\left\{\frac{3}{2}(\log 3|\Delta| + \log\ell), 3\log\ell\right\}. \tag{2.50}$$

A lower bound for the height $h(j)$ can be obtained by combining the conditional Proposition 2.7.6 with (2.33). The conclusion of the proof can be then carried out in the same way as the proof of Theorem 2.7.2. □

Proof of Theorem 2.7.2. The fact that the Dirichlet L-functions attached to imaginary quadratic fields satisfy GRH implies in particular that for every non-principal real primitive Dirichlet character χ of discriminant D we have

$$\frac{L'(\chi,1)}{L(\chi,1)} = O(\log\log|D|),$$

where the implied constant is absolute (see for instance [GS00, Section 3.1]). In particular, there exists $k \in \mathbb{R}_{\geq 0}$ such that property $P(k)$ holds for all Kronecker symbols attached to imaginary quadratic fields. Now one concludes by applying Theorem 2.7.7. □

2.8 An unsuccessful attempt at making Theorem 2.7.2 unconditional

The goal of this section is to show that the naive attempt at making Theorem 2.7.2 unconditional by improving the bounds obtained in Theorem 2.5.1 is fruitless. Namely, we will prove that the order of magnitude of the bounds appearing in Theorem 2.5.1 cannot be improved in general, at least in the case $j_0 = 0$. Under the condition that the considered prime ℓ divides the discriminant of the order $\mathcal{O}_j$ corresponding to the singular modulus j, it is easy to provide examples in which the second upper-bound of (2.15) is reached. For instance, each of the singular moduli j of discriminant $\Delta = -7 \cdot 5^2$ is divided by the unique prime $\mathfrak{p}_5 \subseteq \mathbb{Q}(j)$ above 5 and we have $v_{\mathfrak{p}_5}(j) = 3$ (note that $d_0 = 6$ in this case). On the other hand, if ℓ does not divide the discriminant of O_j the claimed optimality follows from the following theorem.

Theorem 2.8.1. *Let $\ell \geq 5$ be a prime with $\ell \equiv 2 \bmod 3$. There exists an infinite family of singular moduli j whose corresponding discriminant Δ_j is coprime with ℓ and which satisfy*

$$v_\mu(j) \geq 3\left(\frac{\log(|\Delta_j| - 3)}{2\log\ell} + \frac{1}{2} - \frac{\log 2}{\log\ell}\right)$$

for some prime ideal $\mu \subseteq H_O$ lying above ℓ.

To prove the theorem, we need two preliminary results.

Proposition 2.8.2. *Let $\ell \geq 5$ be a prime with $\ell \equiv 2 \bmod 3$. Then the elliptic curve $E_0 : y^2 = x^3 + 1$ over $\overline{\mathbb{F}}_\ell$ has complex multiplication by the order*

$$\mathbb{Z} + \mathbb{Z}\zeta_3 + \mathbb{Z}\frac{2 + \zeta_3 + 2\varphi + \zeta_3\varphi}{3} + \mathbb{Z}\frac{-1 + \zeta_3 - \varphi - 2\zeta_3\varphi}{3}$$

in the quaternion algebra $\mathbb{B}_{\ell,\infty}$. Here, if $\zeta \in \overline{\mathbb{F}}_\ell$ denotes a fixed 3-rd root of unity, the endomorphisms $\zeta_3, \varphi \in \mathrm{End}_{\overline{\mathbb{F}}_\ell}$ are such that $\zeta_3 : (x, y) \mapsto (\zeta x, y)$ and $\varphi : (x, y) \mapsto (x^\ell, y^\ell)$.

Proof. One could directly verify that the given order is a maximal order in $\mathbb{B}_{\ell,\infty}$ whose elements represent endomorphisms of the elliptic curve E_0. We outline a possible strategy leading to the computation of this endomorphism ring, kindly suggested to the author by John Voight.

Let $O_{E_0} := \mathrm{End}_{\overline{\mathbb{F}}_\ell}(E_0)$ and notice that O_{E_0} contains the order $O := \mathbb{Z}[\zeta_3, \varphi]$ having $\mathbb{Z}$-basis $\{1, \zeta_3, \varphi, \zeta_3\varphi\}$. Then $O_{E_0} \subseteq \mathbb{B}_{\ell,\infty}$ is a maximal order and $O \subseteq O_{E_0}$ with index 3. Hence, O_E contains an element of the form

$$\alpha = \frac{A + B\zeta_3 + C\varphi + D\zeta_3\varphi}{3}, \qquad A, B, C, D \in \mathbb{Z}$$

with $3 \nmid \gcd(A, B, C, D)$. Since α is an element of a quaternion order, it is in particular integral. This implies that its reduced trace and norm must both be integers. One has

$$\begin{aligned} \mathrm{trd}(\alpha) &= \frac{2A - B}{3} \\ \mathrm{nrd}(\alpha) &= \frac{-\ell CD - AB + A^2 + B^2 + \ell(C^2 + D^2)}{9}, \end{aligned}$$

where $\mathrm{trd}(\cdot)$ and $\mathrm{nrd}(\cdot)$ denote respectively the reduced trace and the reduced norm in the quaternion algebra $\mathbb{B}_{\ell,\infty}$. Note now that, since $O \subseteq O_{E_0}$, the integers A, B, C, D could be determined modulo 3. Hence there is just a finite number of possibilities to check. A computation shows that the possible options for the tuple (A, B, C, D) are the following four:

$$(1, 2, 1, 2) \qquad (1, 2, 2, 1) \qquad (2, 1, 1, 2) \qquad (2, 1, 2, 1).$$

By adding the corresponding α's to the order $\mathcal{O}$ we get the following possibilities:

$$\begin{aligned}
&(1,2,1,2), && \mathcal{O}_1 : \mathbb{Z} + \mathbb{Z}\zeta_3 + \mathbb{Z}\left(\frac{1}{3} - \frac{1}{3}\zeta_3 + \frac{1}{3}\varphi + \frac{2}{3}\zeta_3\varphi\right) + \mathbb{Z}\left(-\frac{2}{3} - \frac{1}{3}\zeta_3 - \frac{2}{3}\varphi - \frac{1}{3}\zeta_3\varphi\right)\\
&(1,2,2,1), && \mathcal{O}_2 : \mathbb{Z} + \mathbb{Z}\zeta_3 + \mathbb{Z}\left(\frac{1}{3} - \frac{1}{3}\zeta_3 + \frac{2}{3}\varphi + \frac{1}{3}\zeta_3\varphi\right) + \mathbb{Z}\left(-\frac{2}{3} - \frac{1}{3}\zeta_3 - \frac{1}{3}\varphi - \frac{2}{3}\zeta_3\varphi\right)\\
&(2,1,1,2), && \mathcal{O}_3 : \mathbb{Z} + \mathbb{Z}\zeta_3 + \mathbb{Z}\left(\frac{2}{3} + \frac{1}{3}\zeta_3 + \frac{1}{3}\varphi + \frac{2}{3}\zeta_3\varphi\right) + \mathbb{Z}\left(-\frac{1}{3} + \frac{1}{3}\zeta_3 - \frac{2}{3}\varphi - \frac{1}{3}\zeta_3\varphi\right)\\
&(2,1,2,1), && \mathcal{O}_4 : \mathbb{Z} + \mathbb{Z}\zeta_3 + \mathbb{Z}\left(\frac{2}{3} + \frac{1}{3}\zeta_3 + \frac{2}{3}\varphi + \frac{1}{3}\zeta_3\varphi\right) + \mathbb{Z}\left(-\frac{1}{3} + \frac{1}{3}\zeta_3 - \frac{1}{3}\varphi - \frac{2}{3}\zeta_3\varphi\right).
\end{aligned}$$

Looking at the generators of these orders, we see that $\mathcal{O}_1 = \mathcal{O}_4$ and $\mathcal{O}_2 = \mathcal{O}_3$, so we discard the first two and we only consider $\mathcal{O}_3$ and $\mathcal{O}_4$. We need to decide which of these two rings is the "correct one". Indeed, the desired order must be identified to the endomorphism ring of the elliptic curve E_0. An element of the form $\frac{1}{3}\beta$, with $\beta \in \mathrm{End}_{\overline{\mathbb{F}}_\ell}(E_0)$, is an endomorphism of E_0 if and only if the endomorphism β factors through the multiplication-by-3 morphism. This happens if and only if the 3-torsion points of E_0 are in the kernel of β. The idea is then to compute the generators of the group of 3-torsion points of E_0 and to test which order contains the "right" elements. The 3-division polynomial of E_0 is

$$\Phi_3(x) = 3x(x^3 + 4),$$

so we can choose as generators of the full 3-torsion subgroup $E_0[3](\overline{\mathbb{F}}_\ell)$ the points

$$P = (0,1), \qquad Q = (-\sqrt[3]{4}, \sqrt{-3})$$

for fixed choices of $\sqrt[3]{4}, \sqrt{-3} \in \overline{\mathbb{F}}_\ell$ as follows. Observe that for a prime $\ell \geq 5$ and $\ell \equiv 2 \bmod 3$, all elements in $\mathbb{F}_\ell$ are cubes and -3 is not a square modulo ℓ. In view of this remark, we choose Q in such a way that the first coordinate lies in $\mathbb{F}_\ell$. Instead the second coordinate of Q defines in any case a quadratic extension of $\mathbb{F}_\ell$, so that

$$(\sqrt{-3})^\ell = -\sqrt{-3}.$$

We are ready to verify that $\mathcal{O}_4$ is the correct order. Let

$$\begin{aligned}
\Phi &= 2 + \zeta_3 + 2\varphi + \zeta_3\varphi \in \mathcal{O}_E\\
\Psi &= -1 + \zeta_3 - \varphi - 2\zeta_3\varphi \in \mathcal{O}_E.
\end{aligned}$$

Then, using the fact that $2P = -P$ and $2Q = -Q$ we get that $\Phi = \Psi$ on the 3-tosion points, so

$$\begin{aligned}
\Phi(P) &= [2](0,1) + (0,1) + [2](0,1) + (0,1) = 0\\
\Phi(Q) &= (-\sqrt[3]{4}, -\sqrt{-3}) + (-\zeta\sqrt[3]{4}, \sqrt{-3}) + [2]((-\sqrt[3]{4})^p, (\sqrt{-3})^p) + (\zeta(-\sqrt[3]{4})^p, (\sqrt{-3})^p) = 0
\end{aligned}$$

which shows that $E[3] \subseteq \ker \Phi$ and $E[3] \subseteq \ker \Psi$. One can also verify that

$$(2 + \zeta_3 + \varphi + 2\zeta_3\varphi)(Q) \neq 0.$$

This proves the proposition. □

Proposition 2.8.3. *Let O be an order in an imaginary quadratic field K and $\ell \in \mathbb{N}$ be a prime inert in K that does not divide the conductor of O. Let W be the ring of integers in the completion $\widehat{\mathbb{Q}_\ell^{unr}}$ of the maximal unramified extension of $\mathbb{Q}_\ell$, with uniformizer $\pi \in W$. Fix $n \in \mathbb{N}$ and let $E_0 \longrightarrow \operatorname{Spec}(W/\pi^n)$ be an elliptic scheme such that the reduction modulo π is supersingular. If $f : O \hookrightarrow \operatorname{End}_{W/\pi^n}(E_0)$ is an optimal embedding, then there exists an elliptic curve $E_{/W}$ such that*

- *E mod $\pi^n \cong E_0$;*

- *$\operatorname{End}_W(E) \cong O$.*

Proof. This is an application Gross and Zagier's generalization [GZ85, Proposition 2.7] of Deuring's lifting Theorem (see Theorem 1.4.3). Note that the proof of Gross and Zagier's result in the supersingular case does not require, in their notation, the ring $\mathbb{Z}[\alpha_0]$ to be integrally closed but only ℓ not dividing its conductor.

Write $O = \mathbb{Z}[\tau]$ for some imaginary quadratic $\tau \in K$ and let $\alpha_0 := f(\tau)$. The endomorphism α_0 induces on the tangent space $\operatorname{Lie}(E_0)$ the multiplication by an element $w_0 \in W/\pi^n$ which is a root of the minimal polynomial $g(x) = x^2 + Ax + B \in \mathbb{Z}[x]$ of τ over $\mathbb{Q}$. In order to apply [GZ85, Proposition 2.7], we need to show that there exists $w \in W$ such that $w \mod \pi^n = w_0$. Let $\beta := w_0 \bmod \pi \in \overline{\mathbb{F}}_\ell$. Then β is a root of $g(x) \bmod \pi$ lying in $\overline{\mathbb{F}}_\ell$. If $g'(\beta) = 0$, then β would actually lie in $\mathbb{F}_\ell$. However, since ℓ is inert in O and does not divide its conductor, the polynomial $g(x)$ is irreducible over $\mathbb{F}_\ell$ by the Kummer-Dedekind Theorem [Neu99, Proposition 1.8.3], and this implies that the derivative of $g(x)$ does not vanish on β (the same argument holds for $\ell = 2$ by choosing appropriately τ in such a way that its trace is odd). Then by Hensel's lemma there exists a unique $w \in W$ lifting β. This w satisfies $w \bmod \pi^n = w_0$ by construction.

We now apply [GZ85, Proposition 2.7] to deduce that there exists an elliptic curve $E_{/W}$ and an endomorphism $\alpha \in \operatorname{End}_W(E)$ such that $E \bmod \pi^n \cong E_0$ and $\alpha \bmod \pi^n = \alpha_0$. In principle, the ring $\operatorname{End}_W(E)$ could strictly contain the order $\mathbb{Z}[\alpha]$. However, the reduction map identifies $\mathbb{Z}[\alpha]$ with O, and the latter optimally embeds in $\operatorname{End}_{W/\pi^n}(E_0)$. Since the reduction map also embeds $\operatorname{End}_W(E) \hookrightarrow \operatorname{End}_{W/\pi^n}(E_0)$, we deduce that $\operatorname{End}_W(E) = \mathbb{Z}[\alpha] \cong O$, as wanted. □

Proof of Theorem 2.8.1. Let W be the ring of integers in the completion $\widehat{\mathbb{Q}_\ell^{\mathrm{unr}}}$ of the maximal unramified extension of $\mathbb{Q}_\ell$, with uniformizer $\pi \in W$. For every $n \in \mathbb{N}$ let $R_n := \operatorname{End}_{W/\pi^{n+1}}(E_0)$ be the endomorphism ring of the reduction of $E_{0/W}$ modulo π^{n+1}. By Theorem 2.4.4 (b) we know that $R_n = \mathbb{Z}[\zeta_3] + \ell^n R_0$, where R_0 is the order appearing in the statement of Proposition 2.8.2. A computation similar to the one carried out during the proof of Theorem 2.5.1 shows that the ternary quadratic form induced by the reduced norm on the Gross lattice of R_n is given by

$$Q_{\ell,n}(X,Y,Z) = 3X^2 + \ell^{2n}\frac{4\ell+1}{3}Y^2 + 4\ell^{2n+1}Z^2 + 2\ell^n XY - 4\ell^{2n+1}YZ \in \mathbb{Z}[X,Y,Z] \qquad (2.51)$$

for all $n \in \mathbb{N}$. Proposition 2.8.3 combined with Lemma 2.4.1 implies in particular that, for any primitive triple of integers $(x,y,z) \in \mathbb{Z}^3$ such that $-D := Q_{\ell,n}(x,y,z)$ is not divisible by ℓ, there exists an elliptic curve $E'_{/W}$ with complex multiplication by the order of discriminant D and which is isomorphic to $E : y^2 = x^3 + 1$ modulo π^{n+1}. The primitive triple $(1, 0, 1)$ gives

$$Q_{\ell,n}(1, 0, 1) = 3 + 4\ell^{2n+1}$$

which is not divisible by ℓ. The j-invariant of the corresponding elliptic curve E with CM by the order of discriminant D will satisfy, by [GZ85, Proposition 2.3], the inequality

$$v_{\mu}(j) \geq 3(n+1) = 3\left(\frac{\log(|D|-3)}{2\log\ell} + \frac{1}{2} - \frac{\log 2}{\log\ell}\right)$$

for some prime $\mu \subseteq H_{\mathcal{O}}$ lying above ℓ. This concludes the proof of the theorem. □

2.9 A uniformity conjecture for singular moduli

In this final section we make some speculations, based on computer-assisted numerical calculations, concerning differences of singular moduli that are S-units. The starting point of our discussion is the following observation (compare also with [HMR21b, Question 1.2]): numerical computations seem to show that $j_{-11} = -2^{15}$, which is the unique singular modulus relative to the order of discriminant $\Delta = -11$, may also be the only singular modulus that is an $\{\ell\}$-unit for some prime ℓ. In other words, it seems that the set $\mathcal{J}_1$ of singular moduli that are S-units for some set of primes S of cardinality 1, contains only one element, namely j_{-11}. It appears then natural to ask what happens if we increase the cardinality of the set S. Motivated by this question, we have performed some computations, whose results are displayed in Table 2.1. Let us describe the notation and the content of this table.

If a singular modulus of discriminant Δ is an S-unit for some set S of rational primes, then actually all singular moduli of discriminant Δ are singular S-units since, as we discussed in Section 1.3, the set of singular moduli relative to the same discriminant form a full Galois orbit over $\mathbb{Q}$. For every $s, A \in \mathbb{N}$ denote then by $\mathcal{J}_s$ the set of Galois orbits of singular moduli that are S-units for some set S of rational primes satisfying $\#S = s$ and by $\mathcal{J}_s(A)$ the subset of $\mathcal{J}_s$ consisting of those orbits whose corresponding singular moduli have discriminant Δ satisfying $|\Delta| \leq A$. Similarly, denote by $\Delta_{\max,s}$ (resp. $\Delta_{\max,s}(A)$) the biggest (in absolute value) imaginary quadratic discriminant such that there exists a singular modulus of discriminant $\Delta_{\max,s}$ whose Galois orbit belongs to $\mathcal{J}_s$ (resp. to $\mathcal{J}_s(A)$). If $\mathcal{J}_s$ is an infinite set, we put $\Delta_{\max,s} = -\infty$. Clearly, for every pair of natural numbers $A_1 \leq A_2$ we have

$$|\Delta_{\max,s}(A_1)| \leq |\Delta_{\max,s}(A_2)| \leq |\Delta_{\max,s}|.$$

In Table 2.1 we have computed, with the help of SAGE [SAGE], the cardinality of $\mathcal{J}_s(50000)$ for $s \in \{1, \ldots, 7\}$, and the corresponding $\Delta_{\max,s}(50000)$. Moreover, in the last column we have collected all the primes appearing in the norm factorizations of $j \in \mathcal{J}_s(50000)$.

The results displayed in Table 2.1 show, for small values of $s \in \mathbb{N}$, that $\Delta_{\max,s}(50000)$ is much smaller compared to the bound $|\Delta| \leq 50000$ up to which we have performed our computations. For instance, we see that among all the Galois orbits of singular moduli with discriminant $|\Delta| \leq 50000$, only 9 orbits contain singular S-units for some set S with $\#S \leq 2$. Moreover, the biggest discriminant associated to a singular modulus belonging to one of these 9 orbits is $\Delta = -83$. All this seems to suggest that $\Delta_{\max,s}(A)$ will remain constant for all $A \geq 50000$ *i.e.* that $\Delta_{\max,s}(50000) = \Delta_{\max,s}$ for $s \in \{1, \ldots, 7\}$, which would mean that the number of primes dividing the norm of a singular modulus must increase as the absolute value of its discriminant gets

s	$\#\mathcal{J}_s(50000)$	$\Delta_{\max,s}(50000)$	primes appearing in the factorizations
1	1	-11	2
2	9	-83	2, 3, 5, 11
3	28	-227	2, 3, 5, 11, 17, 23, 29, 41
4	67	-523	2, 3, 5, 11, 17, 23, 29, 41, 47, 53, 59, 71, 83, 89
5	119	-987	2, 3, 5, 7, 11, 17, 23, 29, 41, 47, 53, 59, 71, 83, 89, 101, 107, 113, 131, 137, 149, 167, 173, 179, 281, 317
6	195	-2043	2, 3, 5, 7, 11, 13, 17, 23, 29, 41, 47, 53, 59, 71, 83, 89, 101, 107, 113, 131, 137, 149, 167, 173, 179, 191, 197, 227, 233, 239, 251, 257, 263, 269, 281, 293, 311, 317, 353, 383
7	291	-2587	2, 3, 5, 7, 11, 13, 17, 23, 29, 41, 47, 53, 59, 71, 83, 89, 101, 107, 113, 131, 137, 149, 167, 173, 179, 191, 197, 227, 233, 239, 251, 257, 263, 269, 281, 293, 311, 317, 347, 353, 359, 383, 389, 419, 431, 449, 467, 491, 509, 521, 557, 569, 617, 641, 653, 677

Table 2.1: The table displays for $s \in \{1, \dots, 7\}$ the number of imaginary quadratic discriminants up to $5 \cdot 10^4$ for which the corresponding singular moduli are S-units with $\#S = s$ (second column). The third column shows the biggest among the found discriminants and the fourth column shows all the primes appearing in the factorizations of the norms of the corresponding singular moduli.

bigger. If this were actually true, then the last column of Table 2.1 would show which primes a set S of cardinality s must contain in order for the set of singular S-units to be non-empty (but not all the possible s-tuples are possible). For example, it seems from these computations that the set of singular $\{17, 23\}$-units does not contain any singular modulus. All this discussion leads to the formulation of the following conjecture.

Conjecture 2.9.1 (Uniformity conjecture for singular S-units)**.** *For every $s \in \mathbb{N}$, the set $\mathcal{J}_s$ is finite.*

We could have equivalently formulated the above conjecture by saying that for every finite set S of rational primes, the set of singular S-units is finite and its cardinality can be bounded only in terms of the cardinality of S, regardless from the primes contained latter set. The fact that this statement is equivalent to Conjecture 2.9.1 can be seen as follows: suppose that for every $s \in \mathbb{N}$ there exists a constant $C(s) \geq 0$ such that the set of singular S-units has cardinality bounded by $C(s)$ whenever S is a set of rational primes satisfying $\#S = s$. Since being an S-unit is Galois invariant, this implies that $C(s)$ also bounds the size of the Galois orbit of any such singular S-unit, hence the class number of the corresponding imaginary quadratic order. By the Brauer-Siegel Theorem [Lan94, Chapter XIII, Theorem 4] this entails a bound on the discriminant of any singular S-unit with $\#S = s$. Hence any such singular modulus must lie in a finite set and Conjecture 2.9.1 follows.

Inspecting the computations displayed in Table 2.1, one could also try to be more precise on the cardinality of the sets $\mathcal{J}_s$. For instance, we may ask the following:

s	$\#\mathcal{J}_s(50000)$	$\Delta_{\max,s}(50000)$	primes appearing in the factorizations
1	0	/	/
2	3	-8	2, 3, 7
3	14	-52	2, 3, 7, 11, 19, 23, 31, 43
4	31	-139	2, 3, 7, 11, 19, 23, 31, 43, 47, 59, 67, 79, 83, 103, 127, 139
5	54	-259	2, 3, 7, 11, 19, 23, 31, 43, 47, 59, 67, 71, 79, 83, 103, 107, 127, 139, 151, 163, 211, 223
6	93	-571	2, 3, 5, 7, 11, 19, 23, 31, 43, 47, 59, 67, 71, 79, 83, 103, 107, 127, 131, 139, 151, 163, 167, 179, 191, 199, 211, 223, 271, 283, 307, 331, 571
7	145	-835	2, 3, 5, 7, 11, 19, 23, 31, 43, 47, 59, 67, 71, 79, 83, 103, 107, 127, 131, 139, 151, 163, 167, 179, 191, 199, 211, 223, 227, 239, 251, 271, 283, 307, 311, 331, 367, 379, 383, 439, 463, 487, 499, 523, 547, 571, 631, 691

Table 2.2: The table displays for $s \in \{1, \ldots, 7\}$ the number of imaginary quadratic discriminants up to $5 \cdot 10^4$ for which the corresponding singular moduli j are such that $j - 1728$ is an S-unit for some S with $\#S = s$ (second column). The third column shows the biggest among the found discriminants and the fourth column shows all the primes appearing in the factorizations of the corresponding norms of $j - 1728$.

Question 2.9.2. *Is it true that there exists only* 1 *singular modulus which is an S-unit for $\#S = 1$, and* 9 *Galois orbits of singular moduli that are S-units for $\#S = 2$?*

We find it more difficult to formulate precise conjectures on how the number of primes dividing the norm of a singular modulus increases with respect to its discriminant.

Of course, there is no reason to restrict our attention to singular S-units. One can make similar conjectures for differences of the form $j - j_0$ with j_0 a fixed singular modulus. For instance, Table 2.2 shows how the above considerations seem to hold true also for differences of the form $j - 1728$. The notation is the same used for Table 1, but with the necessary modifications: $\mathcal{J}_s$ is the set of Galois orbits of singular moduli j such that $j - 1728$ is an S-unit for some set S of rational primes satisfying $\#S = s$, etc. Further computations with other differences $j - j_0$ would probably shed more light on whether it is possible that for every $s \in \mathbb{N}$, there is only a finite number of singular differences $j_1 - j_2$ that is an S-unit for some set S of cardinality s. But we do not want to enter this territory here.

Galois representations attached to CM elliptic curves

3

In this chapter we study the theory of Galois representations associated to elliptic curves with complex multiplication, and its relations with the class field theory of imaginary quadratic fields. The purpose is double: first of all, we want to set the ground for the subsequent Chapter 4 and Chapter 5, where most of this material is heavily used. Secondly, we want to create a reference for a topic that does not seem to have a proper representation in the literature. The non-expert tends to treat and use the theory of CM Galois representations only in the case of complex multiplication by maximal orders, since the presence of non-integrally closed number rings brings several technical complications. It wouldn't be true to say that there are no general expositions for the general theory of complex multiplication: one can certainly consult, for instance, Lang [Lan87] and Shimura [Shi94; Shi98] to see that this is not the case. However, none of these references seems to give much space to the topic of Galois representations for elliptic curves with complex multiplication. Moreover, on the one hand Shimura's works treat generic CM abelian varieties and one has thus to dig in heavy notation in order to translate the needed results into the easier one-dimensional setting. On the other hand, Lang's book focuses only on elliptic curves, but using a somehow difficult exposition, which stands in the tradition of the classical works by Weber [Web28], Söhngen [Söh35], Deuring [Deu41], and many others. It seems that the lack of a modern account of the general theory of CM Galois representations has been recently noticed by some mathematicians. We mention here, by way of illustration, the two recent works of Bourdon and Clark [BC20] and Lozano-Robledo [Loz19]. The first one does not study Galois representations *per se*, but rather uses them as a tool to obtain results on torsion points and isogenies of CM elliptic curves. The second one investigates the possible ℓ-adic images of Galois representations attached to elliptic curves with complex multiplication defined over their field of moduli. The topic is here addressed in a matrix-based style and, in the parts focusing on Class Field Theory, by using a classical approach that can be traced back to Söhngen.

Differently from these two aforementioned works, this chapter is of foundational nature. It consists essentially of an exposition of old and new results on the theory of Galois representations attached to elliptic curves with complex multiplication by *general imaginary quadratic orders*. Of course, we have no pretence of completeness. We make use of the idelic language for class field theory, as in the case of Section 3.3, where we generalize and reformulate the theory of ray class field for orders first introduced by Söhngen in [Söh35] with a classical language. We also show how the classical main theorems of complex multiplication allow to understand the "size" of the image of a CM Galois representation in terms of the arithmetic properties satisfied by the division fields of the considered elliptic curve. As a byproduct, we improve in Corollary 3.5.4 the announced [Loz19, Theorem 1.3].

The outline of the chapter is the following: in Section 3.1 we recall the general theory of Galois representations attached to CM elliptic curves, with an eye towards the difference with the non-CM case. Section 3.2 is motivational, and treats the relation between Galois representations attached to elliptic curves with complex multiplication by maximal orders and the class field theory of the corresponding imaginary quadratic fields. In Section 3.3 we introduce the concept (for any number field) of ray class fields associated to orders that are not necessarily maximal and in Section 3.4 we study the relationship between this theory and the theory of CM elliptic curves. Finally, in Section 3.5 we study how big images of CM Galois representations can be with respect to certain precise subgroups of $\mathrm{GL}_2(\widehat{\mathbb{Z}})$.

3.1 General theory of CM Galois representations

Let E be an elliptic curve defined over a number field F, and let $\overline{F} \supseteq F$ be a fixed algebraic closure. The absolute Galois group $\mathrm{Gal}(\overline{F}/F)$ acts on the group $E_{\mathrm{tors}} := E(\overline{F})_{\mathrm{tors}}$ of all torsion points of E, giving rise to a Galois representation

$$\rho_E : \mathrm{Gal}(F(E_{\mathrm{tors}})/F) \hookrightarrow \mathrm{Aut}_{\mathbb{Z}}(E_{\mathrm{tors}}) \cong \mathrm{GL}_2(\widehat{\mathbb{Z}}) \tag{3.1}$$

where $F(E_{\mathrm{tors}})$ is the compositum of the family of fields $\{F(E[p^\infty])\}_p$ for $p \in \mathbb{N}$ prime. Each extension $F \subseteq F(E[p^\infty])$ is in turn defined as the compositum of the family $\{F(E[p^n])\}_{n\in\mathbb{N}}$, where, for every $N \in \mathbb{N}$, we denote by $F(E[N])$ the *division field* obtained by adjoining to F the coordinates of all the points belonging to the N-torsion subgroup $E[N] := E[N](\overline{F})$. Note that the last isomorphism appearing in (3.1) is non-canonical and depends on the choice of a $\widehat{\mathbb{Z}}$-basis of the Tate module $T_\infty(E) := \varprojlim_{N\in\mathbb{N}} E[N]$. Moreover, after restricting the automorphisms in the absolute Galois group of F to $F(E_{\mathrm{tors}})$ we get a Galois representation $\mathrm{Gal}(\overline{F}/F) \to \mathrm{Aut}_{\mathbb{Z}}(E_{\mathrm{tors}})$ that will be also called ρ_E with abuse of notation. For an elliptic curve E without complex multiplication, Serre's Open Image Theorem [Ser71, Théorème 3] asserts that the image of ρ_E is open, hence of finite index, in $\mathrm{GL}_2(\widehat{\mathbb{Z}})$. The situation is very different if E has complex multiplication, as we are going to explain.

Suppose that $E_{/F}$ is an elliptic curve with complex multiplication by an order $\mathcal{O}$ in an imaginary quadratic field K, and fix the normalized isomorphism $[\cdot]_E : \mathcal{O} \to \mathrm{End}_{\overline{F}}(E)$ described in Definition 1.3.7. The CM setting allows to consider not only N-torsion points for $N \in \mathbb{N}$ but also torsion points relative to an ideal $I \subseteq \mathcal{O}$. More precisely, for any field extension $F \subseteq L \subseteq \overline{F}$ and any ideal $I \subseteq \mathcal{O}$ we write

$$E(L)[I] := \{P \in E(L) : [\alpha]_E(P) = 0 \text{ for all } \alpha \in I\}$$

for the set of I-torsion points of E defined over L. The group $E(L)[I]$ is naturally a module over $\mathcal{O}/I$, using the action of complex multiplication. When $I = \alpha\mathcal{O}$ for some $\alpha \in \mathcal{O}$ we write $E(L)[\alpha] := E(L)[\alpha\mathcal{O}]$ and $E[\alpha] := E(\overline{F})[\alpha]$; more generally, we write $E[I] := E(\overline{F})[I]$. Note that by taking $I = N \cdot \mathcal{O}$ with $N \in \mathbb{N}$ the set $E[I]$ becomes the familiar set of N-torsion points defined over $\overline{F}$, so our notation is consistent. Moreover, all the definitions make sense also if the number field F is replaced by the field of complex numbers.

Lemma 3.1.1. *Let $E_{/\mathbb{C}}$ be an elliptic curve with complex multiplication by an order $\mathcal{O}$ in an imaginary quadratic field. If $I \subseteq \mathcal{O}$ is an invertible ideal then $E[I]$ is a free $\mathcal{O}/I$-module of rank* 1.

Proof. See [BC20, Lemma 2.4]. □

In order to study Galois representations, it is convenient to separate the discussion according to whether the field of definition F contains the endomorphism algebra of E or not. Suppose initially that $E_{/F}$ has complex multiplication by an order $\mathcal{O}$ in an imaginary quadratic field $K \subseteq F$. This assumption implies in particular that all the endomorphisms of E are already defined over F, as proved in [Shi98, Chapter II, Proposition 30]. For every invertible ideal $I \subseteq \mathcal{O}$ the Galois group $\operatorname{Gal}(\overline{F}/F)$ acts on $E[I]$ in similar way as above. However, in this case the action of the absolute Galois group of F is not only an action by $\mathbb{Z}$-automorphisms but also by $\mathcal{O}$-automorphisms. This follows from the fact that all the endomorphisms of E are already defined over F and thus the Galois action commutes with the CM action by Theorem 1.3.8. In particular, we obtain an injective Galois representation

$$\rho_{E,I} : \operatorname{Gal}(F(E[I])/F) \hookrightarrow \operatorname{Aut}_{\mathcal{O}}(E[I]) \cong (\mathcal{O}/I)^{\times} \tag{3.2}$$

where the last isomorphism follows from Lemma 3.1.1. It is worth noting that the isomorphism $\operatorname{Aut}_{\mathcal{O}}(E[I]) \cong (\mathcal{O}/I)^{\times}$ is *canonical*, that is, it does not depend on the specific basis of $\operatorname{Aut}_{\mathcal{O}}(E[I])$ used to describe it. For every pair of invertible ideals $J \subseteq I \subseteq \mathcal{O}$ we have a commutative diagram

$$\begin{tikzcd}
\operatorname{Gal}(F(E[J])/F) \arrow[r, "\rho_{E,J}"] \arrow[d] & (\mathcal{O}/J)^{\times} \arrow[d] \\
\operatorname{Gal}(F(E[I])/F) \arrow[r, "\rho_{E,I}"] & (\mathcal{O}/I)^{\times}
\end{tikzcd}$$

where the left vertical map is the canonical restriction map induced by the inclusion $E[I] \subseteq E[J]$ and the right vertical map is the canonical projection. By taking inverse limits in the above diagram, we obtain the adelic Galois representation

$$\rho_E : \operatorname{Gal}(F(E_{\text{tors}})/F) \hookrightarrow \operatorname{Aut}_{\mathcal{O}}(E_{\text{tors}}) \cong \widehat{\mathcal{O}}^{\times} \tag{3.3}$$

$\widehat{\mathcal{O}} = \varprojlim_{N \in \mathbb{N}} \mathcal{O}/N\mathcal{O}$ being the profinite completion of the order $\mathcal{O}$ (taking inverse limits on all the invertible ideals of $\mathcal{O}$ or over all the positive integers gives rise to isomorphic rings). Note that the map in (3.3) has the same name as the map in (3.1): this is because the two maps are really the same morphism and all we have done so far could be rephrased by saying that, in the case $E_{/F}$ is a CM elliptic curve whose field of definition F contains the corresponding CM order $\mathcal{O}$, the image of $\operatorname{Gal}(F(E_{\text{tors}})/F)$ under (3.1) is contained in the abelian subgroup $\operatorname{Aut}_{\mathcal{O}}(E_{\text{tors}})$ of $\operatorname{Aut}_{\mathbb{Z}}(E_{\text{tors}})$. Since $\operatorname{GL}_2(\widehat{\mathbb{Z}})$ does not contain abelian subgroups of finite index, we obtain as a corollary that the image under (3.1) of $\operatorname{Gal}(F(E_{\text{tors}})/F)$ is not open in $\operatorname{Aut}_{\mathbb{Z}}(E)$. Nevertheless, Serre's Open Image Theorem has a CM analogue.

Theorem 3.1.2. *Let E be an elliptic curve with complex multiplication by an order in an imaginary quadratic field K and defined over a number field $F \supseteq K$. Then the image of $\operatorname{Gal}(F(E_{tors})/F)$ under the Galois representation (3.3) is open in $\operatorname{Aut}_{\mathcal{O}}(E_{tors})$.*

Proof. See [Ser71, § 4.5]. □

We have seen that the isomorphism $\operatorname{Aut}_{\mathcal{O}}(E_{\text{tors}}) \cong \widehat{\mathcal{O}}^{\times}$ is canonical, in the sense that it does not depend on any choice of bases for torsion points. On the other hand, the choice of a $\widehat{\mathbb{Z}}$-basis for $T_{\infty}(E)$ gives an isomorphism $\operatorname{Aut}_{\mathbb{Z}}(E_{\text{tors}}) \cong \operatorname{GL}_2(\widehat{\mathbb{Z}})$ that, via

$$\widehat{\mathcal{O}}^{\times} \cong \operatorname{Aut}_{\mathcal{O}}(E_{\text{tors}}) \hookrightarrow \operatorname{Aut}_{\mathbb{Z}}(E_{\text{tors}}) \cong \operatorname{GL}_2(\widehat{\mathbb{Z}}),$$

identifies $\widehat{\mathcal{O}}^{\times}$ with a subgroup of $\operatorname{GL}_2(\widehat{\mathbb{Z}})$ in a *non-canonical* way. Explicitly describing the image of the morphism above may be difficult at first glance. However, after astutely choosing the basis for $T_{\infty}(E)$, one obtains an easy characterization of the image of $\widehat{\mathcal{O}}^{\times}$ inside $\operatorname{GL}_2(\widehat{\mathbb{Z}})$.

Lemma 3.1.3. *Let $E_{/\mathbb{C}}$ be an elliptic curve with complex multiplication by the imaginary quadratic order $\mathcal{O}$. There exists a sequence $\mathcal{P} = \{P_N\}_{N\in\mathbb{N}}$ of points on $E(\mathbb{C})$ such that:*

1. *The points P_N are a basis for $E[N]$ as free $\mathcal{O}/N\mathcal{O}$-module i.e. $\mathcal{O} \cdot P_N = E[N]$;*
2. *For all $M, N \in \mathbb{N}$ with $M \mid N$ we have $(N/M) \cdot P_N = P_M$.*

Proof. Choose an embedding $\mathcal{O} \hookrightarrow \mathbb{C}$ and let $E_{0/\mathbb{C}}$ be an elliptic curve for which there exists an analytic parametrization

$$\xi : \mathbb{C}/\mathcal{O} \to E_0(\mathbb{C}).$$

Then for E_0 the statement is easy, since the points $Q_N := \xi\left(\frac{1}{N} + \mathcal{O}\right) \in E_0(\mathbb{C})$ satisfy conditions (1) and (2) of the lemma. To pass from E_0 to E we remark first of all that, since singular moduli are all conjugated over $\overline{\mathbb{Q}}$, there exists $\sigma \in \operatorname{Aut}(\mathbb{C})$ such that $j(E_0^\sigma) = j(E)$, where σ acts on the coefficients of a fixed Weierstrass equation for E_0. Noticing that σ induces a ring automorphism on $\mathcal{O}$ and using Theorem 1.3.8 it is easy to deduce that the sequence $\{\sigma(Q_N)\}_{N\in\mathbb{N}}$ of points on $E_0^\sigma(\mathbb{C})$ still satisfies conditions (1) and (2) above. Finally, choosing an isomorphism $\phi : E_0^\sigma \to E$, an application of [Sil94, II, Corollary 1.1.1] shows that $\{P_N\}_{N\in\mathbb{N}} := \{\phi(\sigma(Q_N))\}_{N\in\mathbb{N}}$ gives the desired sequence of torsion points. □

Taking a sequence $\mathcal{P}$ as described in Lemma 3.1.3 corresponds to fixing a basis of $T_\infty(E)$ as a free $\widehat{\mathcal{O}}$-module of rank 1. In particular we have an isomorphism of $\widehat{\mathcal{O}}$-modules $T_\infty(E) \cong \widehat{\mathcal{O}}$, $\mathcal{P} \mapsto 1$. Writing $\mathcal{O} = \mathbb{Z}[\omega]$ with $\omega^2 = a\omega + b$ and $a, b \in \mathbb{Z}$ we have

$$\widehat{\mathcal{O}} = \mathcal{O} \otimes_{\mathbb{Z}} \widehat{\mathbb{Z}} = \widehat{\mathbb{Z}}[\omega]$$

and since $\widehat{\mathbb{Z}}[\omega] \cong \widehat{\mathbb{Z}}^2$ (as $\widehat{\mathbb{Z}}$-modules), we see that $\mathcal{B} := \{\mathcal{P}, \omega\mathcal{P}\}$ with $\omega\mathcal{P} = \{\omega \cdot P_N\}_{N\in\mathbb{N}}$ is a basis of $T_\infty(E)$ as a $\widehat{\mathbb{Z}}$-module. With respect to this basis, we obtain an embedding

$$\widehat{\mathcal{O}}^\times \hookrightarrow \mathrm{GL}_2(\widehat{\mathbb{Z}}), \qquad x + \omega y \mapsto \begin{pmatrix} x & yb \\ y & x + ya \end{pmatrix} \tag{3.4}$$

for all $x, y \in \widehat{\mathbb{Z}}$ such that $x^2 + axy - by^2 \in \widehat{\mathbb{Z}}^\times$. If $\Delta \in \mathbb{Z}$ is the discriminant of the order $\mathcal{O}$, then one can choose $\omega = \frac{\Delta+\sqrt{\Delta}}{2}$ as a generator for $\mathcal{O}$ over $\mathbb{Z}$ and with this choice, the map (3.4) reads

$$x + \omega y \mapsto \begin{pmatrix} x & y\frac{\Delta-\Delta^2}{4} \\ y & x + y\Delta \end{pmatrix}$$

for all $x, y \in \widehat{\mathbb{Z}}$ as above. We have proved the following theorem.

Theorem 3.1.4. *Let F be a number field and let $E_{/F}$ an elliptic curve with complex multiplication by an order of discriminant Δ in an imaginary quadratic field $K \subseteq F$. Then there exists a $\widehat{\mathbb{Z}}$-basis for the Tate module $T_\infty(E)$ such that the image of* $\operatorname{Gal}(F(E_{tors})/F)$ *under the Galois representation* (3.1) *corresponding to this basis is contained in*

$$\mathcal{C}_\infty(E) := \left\{ \begin{pmatrix} x & y\frac{\Delta-\Delta^2}{4} \\ y & x + y\Delta \end{pmatrix} : x, y \in \widehat{\mathbb{Z}},\ x^2 + \Delta xy + \frac{\Delta^2 - \Delta}{4} y^2 \in \widehat{\mathbb{Z}}^\times \right\}.$$

We now turn to the study of Galois representations attached to elliptic curves with complex multiplication whose field of definition *does not* contain the corresponding CM field. The crucial difference from the previous setting is that in this case, if $E_{/F}$ is an elliptic curve with CM by $\mathcal{O}$ and $\mathcal{O} \not\subseteq F$, then the absolute Galois group of F does not act by $\mathcal{O}$-automorphisms on E_{tors}, since the geometric endomorphisms of E are not defined over F (see again [Shi98, Chapter II, Proposition 30]). Let us be more precise.

If $[\cdot]_E : \mathcal{O} \to \operatorname{End}_{\overline{F}}(E)$ is the normalized isomorphism described in Definition 1.3.7 and $\alpha \in \mathcal{O}$, then an automorphism $\sigma \in \operatorname{Gal}(\overline{F}/F)$ acts on $[\alpha]_E(P)$ as

$$\sigma\left([\alpha]_E(P)\right) = [\sigma(\alpha)]_E(\sigma(P))$$

using Theorem 1.3.8. Hence, σ acts as $\mathcal{O}$-module automorphisms on E_{tors} if and only if σ restricts to the identity on the CM field K relative to E. We then see that for a fixed $\tau \in \operatorname{Gal}(\overline{F}/F)$ that restricts to the unique non-trivial element in $\operatorname{Gal}(FK/F)$ either σ or $\sigma\tau$ acts as $\mathcal{O}$-module automorphisms on E_{tors}. We deduce that

$$\rho_E\left(\operatorname{Gal}(\overline{F}/F)\right) \subseteq \langle \operatorname{Aut}_{\mathcal{O}}(E_{\text{tors}}), \rho_E(\tau)\rangle =: \mathcal{N}_\infty(E). \tag{3.5}$$

Note that our notation is validated by the fact that the definition of $\mathcal{N}_\infty(E)$ does not actually depend on the choice of τ: for any other $\tau' \in \operatorname{Gal}(\overline{F}/F)$ that restricts to the non-trivial element in $\operatorname{Gal}(FK/F)$, the same arguments displayed above imply that

$$\rho_E\left(\operatorname{Gal}(\overline{F}/F)\right) \subseteq \langle \operatorname{Aut}_{\mathcal{O}}(E_{\text{tors}}), \rho_E(\tau)\rangle \cap \langle \operatorname{Aut}_{\mathcal{O}}(E_{\text{tors}}), \rho_E(\tau')\rangle\,.$$

Since the image under ρ_E of absolute Galois group of F is not contained in $\operatorname{Aut}_{\mathcal{O}}(E_{\text{tors}})$ we must have

$$\langle \operatorname{Aut}_{\mathcal{O}}(E_{\text{tors}}), \rho_E(\tau)\rangle \cap \langle \operatorname{Aut}_{\mathcal{O}}(E_{\text{tors}}), \rho_E(\tau')\rangle = \langle \operatorname{Aut}_{\mathcal{O}}(E_{\text{tors}}), \rho_E(\tau)\rangle = \langle \operatorname{Aut}_{\mathcal{O}}(E_{\text{tors}}), \rho_E(\tau')\rangle$$

because $\rho_E(\tau)$ normalizes $\operatorname{Aut}_{\mathcal{O}}(E_{\text{tors}})$, and, since $\rho_E(\tau) \notin \operatorname{Aut}_{\mathcal{O}}(E_{\text{tors}})$ but $\rho_E(\tau)^2 \in \operatorname{Aut}_{\mathcal{O}}(E_{\text{tors}})$, the group $\operatorname{Aut}_{\mathcal{O}}(E_{\text{tors}})$ has index 2 inside $\mathcal{N}_\infty(E)$ (similarly with $\rho_E(\tau')$). However, we remark that $\mathcal{N}_\infty(E)$ has infinite index in the normalizer of $\operatorname{Aut}_{\mathcal{O}}(E_{\text{tors}})$ in $\operatorname{Aut}_{\mathbb{Z}}(E_{\text{tors}})$, and this can be seen for instance as follows: under the canonical isomorphisms

$$\operatorname{Aut}_{\mathcal{O}}(E_{\text{tors}}) \cong \widehat{\mathcal{O}}^\times \cong \prod_{\ell \text{ prime}} \mathcal{O}_\ell$$

the groups $\mathcal{O}_\ell := \mathcal{O} \otimes_{\mathbb{Z}} \mathbb{Z}_\ell$ are naturally identified with $\operatorname{Aut}_{\mathcal{O}}(E[\ell^\infty])$, where $E[\ell^\infty] = \varinjlim_{n\in\mathbb{N}} E[\ell^n]$ is the ℓ-primary component of E_{tors}. We then have the inclusions

$$\mathcal{O}_\ell \cong \operatorname{Aut}_{\mathcal{O}}(E[\ell^\infty]) \subseteq \operatorname{Aut}_{\mathbb{Z}}(E[\ell^\infty]) \cong \operatorname{GL}_2(\mathbb{Z}_\ell)$$

and, by choosing again an appropriate basis for the latter isomorphism above, it is proved in [Lom17, Lemma 6.8] that $\mathcal{O}_\ell$ has index 2 inside its normalizer in $\operatorname{GL}_2(\mathbb{Z}_\ell)$. By taking products, one deduces that $\operatorname{Aut}_{\mathcal{O}}(E_{\text{tors}})$ has infinite index inside its normalizer in $\operatorname{Aut}_{\mathbb{Z}}(E_{\text{tors}})$, as we wanted to show.

Similarly to what we did in Theorem 3.1.4, one can explicitly describe the group $\mathcal{N}_\infty(E)$ in terms of matrices. The idea is to find an element $c \in \mathcal{N}_\infty(E) \setminus \operatorname{Aut}_{\mathcal{O}}(E_{\text{tors}})$ which can be easily written down after choosing an appropriate $\widehat{\mathbb{Z}}$-basis of $T_\infty(E)$. Let $\mathcal{P} = \{P_N\}_{N\in\mathbb{N}}$ be a basis of $T_\infty(E)$ as $\widehat{\mathcal{O}}$-module, as constructed in Lemma 3.1.3. The unique non-trivial automorphism $\sigma \in \operatorname{Gal}(K/\mathbb{Q})$

of the CM field K induces an involution on $\mathcal{O}$ which in turn induces a compatible system of involutions $\mathcal{O}/N\mathcal{O} \to \mathcal{O}/N\mathcal{O}$. Every point $P_N \in \mathcal{P}$ determines an isomorphism $E[N] \cong \mathcal{O}/N\mathcal{O}$ for all $N \in \mathbb{N}$, thus we also obtain a compatible system of involutions $c_N : E[N] \to E[N]$ that gives rise to an element $c = c_{\mathcal{P}} \in \operatorname{Aut}_{\mathbb{Z}}(E_{\text{tors}})$. Explicitly, for every $N \in \mathbb{N}$ and every $Q \in E[N]$, writing $Q = [\alpha]_E(P_N)$ for some $\alpha \in \mathcal{O}$ we have

$$c(Q) = c([\alpha]_E(P_N)) = [\sigma(\alpha)]_E(P_N)$$

and in particular $c \notin \operatorname{Aut}_{\mathcal{O}}(E_{\text{tors}})$. As before, we deduce that

$$\rho_E\left(\operatorname{Gal}(\overline{F}/F)\right) \subseteq \langle \operatorname{Aut}_{\mathcal{O}}(E_{\text{tors}}), c\rangle$$

and the latter group contains $\operatorname{Aut}_{\mathcal{O}}(E_{\text{tors}})$ with index 2. Since we also have

$$\rho_E\left(\operatorname{Gal}(\overline{F}/F)\right) \subseteq \mathcal{N}_\infty(E), \qquad \rho_E\left(\operatorname{Gal}(\overline{F}/F)\right) \not\subseteq \operatorname{Aut}_{\mathcal{O}}(E_{\text{tors}})$$

we obtain that $\mathcal{N}_\infty(E) = \langle \operatorname{Aut}_{\mathcal{O}}(E_{\text{tors}}), c\rangle$. This allows also to conclude that, even if the very definition of c depends on the choice of $\mathcal{P}$, the subgroup generated by c and $\operatorname{Aut}_{\mathcal{O}}(E_{\text{tors}})$ inside $\operatorname{Aut}_{\mathbb{Z}}(E_{\text{tors}})$ does not. Let now $\Delta \in \mathbb{Z}$ be the discriminant of the order $\mathcal{O}$. If we take $\omega = \frac{\Delta+\sqrt{\Delta}}{2} \in \mathcal{O}$ and $\mathcal{B} = \{\mathcal{P}, \omega\mathcal{P}\}$ as a $\widehat{\mathbb{Z}}$-basis of $T_\infty(E)$ (this is the same basis that is considered in Theorem 3.1.4), then the image of c under the isomorphism $\operatorname{Aut}_{\mathbb{Z}}(E_{\text{tors}}) \cong \operatorname{GL}_2(\widehat{\mathbb{Z}})$ is given by the matrix

$$\begin{pmatrix} 1 & \Delta \\ 0 & -1 \end{pmatrix}.$$

We have proved the following theorem.

Theorem 3.1.5. *Let F be a number field and let $E_{/F}$ an elliptic curve with complex multiplication by an order of discriminant Δ in an imaginary quadratic field $K \not\subseteq F$. Then there exists a $\widehat{\mathbb{Z}}$-basis for the Tate module $T_\infty(E)$ such that the image of* $\operatorname{Gal}(F(E_{tors})/F)$ *under the Galois representation* (3.1) *corresponding to this basis is contained in*

$$N_\infty = \left\{ \begin{pmatrix} x & y\frac{\Delta-\Delta^2}{4} \\ y & x+y\Delta \end{pmatrix}, \begin{pmatrix} x & \Delta x + y\frac{\Delta^2-\Delta}{4} \\ y & -x \end{pmatrix} : x, y \in \widehat{\mathbb{Z}},\ x^2 + \Delta xy + \frac{\Delta^2-\Delta}{4}y^2 \in \widehat{\mathbb{Z}}^\times \right\}.$$

3.1.1 Who is scared of non-invertible ideals?

Several times in the previous section we have imposed the assumption of considering I-torsion points of a certain CM elliptic curve only for ideals I that were *invertible* in the corresponding endomorphism ring. The main problem that arises when considering I-torsion points for non-invertible ideals $I \subseteq \mathcal{O}$ is that the groups $E[I]$ are not free $\mathcal{O}/I$-modules of rank 1 in general (cfr. Lemma 3.1.1), so the map (3.2) does not necessarily exist. To give an example of what can happen in these cases, this section is dedicated to study in detail the structure of the I-torsion of certain CM elliptic curves $E_{/\mathbb{C}}$ for some specific non-invertible ideals $I \subseteq \operatorname{End}_{\mathbb{C}}(E)$.

Let $K \subseteq \mathbb{C}$ be an imaginary quadratic field, $p \in \mathbb{N}$ a prime number and $\mathcal{O} \subseteq K$ an order of conductor f divisible by p. Let $E_{/\mathbb{C}}$ be an elliptic curve for which there exists a complex uniformization

$$\xi : \mathbb{C}/\mathcal{O} \to E(\mathbb{C})$$

so that E has complex multiplication by $\mathcal{O}$, as explained at the beginning of Section 1.3. Since p divides the conductor of $\mathcal{O}$, there exists a unique maximal ideal $\mathfrak{p} \subseteq \mathcal{O}$ lying above p, containing the principal ideal $p\mathcal{O}$ with index p. If we write $\mathcal{O}_K = \mathbb{Z}[\omega_K]$ for some $\omega_K \in K$ then $\mathcal{O} = \mathbb{Z}[f\omega_K]$ and the ideal $\mathfrak{p}$ can be explicitly described as $\mathfrak{p} = (p, f\omega_K)$, see [Con, Theorem 3.15]. It is easy to prove that $\mathfrak{p}$ is not invertible in $\mathcal{O}$: for instance, one can verify that $(f/p)\omega_K \cdot \mathfrak{p} \subseteq \mathfrak{p}$ and then apply [Con, Corollary 4.4]. For every $n \in \mathbb{N}_{>0}$ we are interested in understanding the $\mathcal{O}$-module structure of the $\mathfrak{p}^n$-torsion subgroup of E. The analytic parametrization ξ induces an $\mathcal{O}$-module isomorphism

$$E[\mathfrak{p}^n] \cong (\mathcal{O} : \mathfrak{p}^n)/\mathcal{O}$$

where $(\mathcal{O} : \mathfrak{p}^n) := \{x \in K : x \cdot \mathfrak{p}^n \subseteq \mathcal{O}\}$, hence it suffices to study the right-hand side of this isomorphism. We begin with an easy lemma.

Lemma 3.1.6. *For every $n \in \mathbb{N}$ we have $\mathfrak{p}^n = (p^n, p^{n-1}f\omega_K)$.*

Proof. We have already seen the result for $n = 1$ and we can then proceed by induction on n. Suppose that $\mathfrak{p}^{n-1} = (p^{n-1}, p^{n-2}f\omega_K)$. Then we have

$$\mathfrak{p}^n = \mathfrak{p}^{n-1} \cdot \mathfrak{p} = (p^n, p^{n-1}f\omega_K, p^{n-2}f^2\omega_K^2).$$

Since $\omega_K \in \mathcal{O}_K$, there exist $a, b \in \mathbb{Z}$ such that $\omega_K^2 = a\omega_K + b$. Hence

$$p^{n-2}f^2\omega_K^2 = p^{n-2}f^2(a\omega_K + b) = \frac{af}{p} \cdot p^{n-1}f\omega_K + \left(\frac{f}{p}\right)^2 b \cdot p^n \in (p^n, p^{n-1}f\omega_K)$$

so the third generator can be obtained from the first two and we are done. □

We can now explicitly describe the group $(\mathcal{O} : \mathfrak{p}^n)$ for all $n \in \mathbb{N}_{>0}$.

Proposition 3.1.7. *Writing $\mathcal{O}_K = \mathbb{Z}[\omega_K]$ with $\omega_K \in K$, for all $n \in \mathbb{N}_{>0}$ we have*

$$(\mathcal{O} : \mathfrak{p}^n) = \frac{1}{p^{n-1}}\mathbb{Z} + \frac{1}{p^n}\mathbb{Z}f\omega_K$$

and, in particular, $(\mathcal{O} : \mathfrak{p})$ is the unique imaginary quadratic order containing $\mathcal{O}$ with index p.

Proof. Let $u + v\omega_K \in (\mathcal{O} : \mathfrak{p}^n)$ with $u, v \in \mathbb{Q}$ and write $\mathfrak{p}^n = (p^n, p^{n-1}f\omega_K)$ using Lemma 3.1.6. By definition we have that $p^n(u + v\omega_K) \in \mathcal{O}$ and $p^{n-1}f\omega_K(u + v\omega_K) \in \mathcal{O}$. The first containment readily implies that there exist $U, V \in \mathbb{Z}$ such that

$$u = \frac{U}{p^n} \quad \text{and} \quad v = \frac{f}{p^n}V.$$

Using these equalities and writing $\omega_K^2 = a\omega_K + b$ with $a, b \in \mathbb{Z}$ we obtain

$$p^{n-1}f\omega_K(u + v\omega_K) = \frac{U}{p}f\omega_K + \frac{f}{p}Va \cdot (f\omega_K) + \frac{f^2}{p}Vb \in \mathcal{O}.$$

Since f is divisible by p, we conclude that $p \mid U$. Hence $u = U'/p^{n-1}$ for some $U' \in \mathbb{Z}$ and we deduce that $(\mathcal{O} : \mathfrak{p}^n) \subseteq \frac{1}{p^{n-1}}\mathbb{Z} + \frac{1}{p^n}\mathbb{Z}f\omega_K$. The other inclusion is clear using once again Lemma 3.1.6. □

Using Proposition 3.1.7 we now have

$$E[\mathfrak{p}^n] \cong \tfrac{1}{p^{n-1}}\mathbb{Z} + \tfrac{1}{p^n}\mathbb{Z}f\omega_K \,/\, \mathcal{O} = \tfrac{1}{p^{n-1}}\mathbb{Z} + \tfrac{1}{p^n}\mathbb{Z}f\omega_K \Big/ \mathbb{Z} + \mathbb{Z}f\omega_K \tag{3.6}$$

for all $n \in \mathbb{N}_{>0}$, where again $\omega_K \in K$ is such that $\mathcal{O}_K = \mathbb{Z}[\omega_K]$ (notice, en passant, that $\# E[\mathfrak{p}^n] = p^{2n-1}$). We claim that $E[\mathfrak{p}^n]$ is a free $\mathcal{O}/\mathfrak{p}^n$-module of rank 1 if and only if $n = 1$.

First of all, if $n = 1$ it is clear from (3.6) that $E[\mathfrak{p}^n] = E[\mathfrak{p}]$ is a free $\mathcal{O}/\mathfrak{p}$-module of rank 1 generated by the preimage of $\frac{1}{p}f\omega_K + \mathcal{O}$ under the complex uniformization ξ (one could also notice that the quotient $\mathcal{O}/\mathfrak{p}$ is actually a field, hence the module must be certainly free). Suppose now that $n > 1$, and assume by contradiction that there exist $A, B \in \mathbb{Z}$ such that $\frac{A}{p^{n-1}} + \frac{B}{p^n}f\omega_K + \mathcal{O}$ is a generator of $E[\mathfrak{p}^n]$ as $\mathcal{O}/\mathfrak{p}^n$-module. For every $x, y \in \mathbb{Z}$ a direct computation shows that

$$(x + y \cdot f\omega_K)\left(\frac{A}{p^{n-1}} + \frac{B}{p^n}f\omega_K\right) = \frac{1}{p^{n-1}}\left(xA + \frac{yB}{p}f^2 b\right) + \frac{1}{p^n}(xB + yAp + yBfa) \cdot f\omega_K$$

where $a, b \in \mathbb{Z}$ are such that $\omega_K^2 = a\omega_K + b$. By definition of $\frac{A}{p^{n-1}} + \frac{B}{p^n}f\omega_K + \mathcal{O}$, there exist $x, y \in \mathbb{Z}$ such that

$$\begin{cases} xA + \frac{yB}{p}f^2 b \equiv 1 & \bmod p^{n-1} \\ xB + yAp + yBfa \equiv 0 & \bmod p^n \end{cases} \tag{3.7}$$

and similarly there exist $\tilde{x}, \tilde{y} \in \mathbb{Z}$ such that

$$\begin{cases} \tilde{x}A + \frac{\tilde{y}B}{p}f^2 b \equiv 0 & \bmod p^{n-1} \\ \tilde{x}B + \tilde{y}Ap + \tilde{y}Bfa \equiv 1 & \bmod p^n. \end{cases} \tag{3.8}$$

Reducing the first identity in (3.8) modulo p and using the fact that p divides the conductor f, we see that one among $\tilde{x}$ and A must be divisible by p. If $p \mid \tilde{x}$ then the second equation in (3.8) cannot have solutions, since again f is divisible by p. Similarly if $p \mid A$, the first equation in (3.7) cannot have solutions. This yields a contradiction, and we deduce that $E[\mathfrak{p}^n]$ cannot be free of rank 1 over $\mathcal{O}$, as claimed.

3.2 Galois representations and Class Field Theory

The theory of complex multiplication for elliptic curves is intimately related to the class field theory of imaginary quadratic fields. More precisely, elliptic curves with complex multiplication by maximal orders allow to give a complete answer to Hilbert's twelfth problem, *i.e.* the problem of explicitly describing generators for the ray class fields of a given number field, in the imaginary quadratic case. In this section we want to review this connection with Class Field Theory and what is the relationship with the theory of Galois representations studied in the previous section. Hence, we momentarily pause from treating complex multiplication for general orders, and we focus on elliptic curves whose endomorphism ring is isomorphic to the ring of integers of some imaginary quadratic field. This will serve as springboard towards the more general theory that will be introduced in the sequel of this chapter.

Let K be an imaginary quadratic field with ring of integers $\mathcal{O}_K$ and Hilbert class field H. We begin by reviewing the class field theoretical description of the Galois group $\mathrm{Gal}(K^{\mathrm{ab}}/H)$ of the maximal abelian extension $K \subseteq K^{\mathrm{ab}}$ over H. Let

$$\mathbb{A}_K^\times := \prod_{\mathfrak{p}}{}' K_{\mathfrak{p}}^\times = \left\{ (s_{\mathfrak{p}})_{\mathfrak{p}} \,:\, s_{\mathfrak{p}} \in \mathcal{O}_{K_{\mathfrak{p}}}^\times \text{ for almost all } \mathfrak{p} \right\}$$

be the *idèle group* of K. It consists of those elements in the cartesian product of the multiplicative groups $K_{\mathfrak{p}}^\times$ over all completions (including the infinite ones) $K_{\mathfrak{p}}$ of K whose $\mathfrak{p}$-components lie in the unit group $\mathcal{O}_{K_{\mathfrak{p}}}^\times$ for almost all $\mathfrak{p}$ (for the infinite component this unit group is simply $\mathbb{C}^\times$). The idèle group is a topological group with the restricted product topology, see [Neu99, pag. 361]. Class Field Theory asserts the existence of a continuous surjective homomorphism

$$[\cdot, K] : \mathbb{A}_K^\times \twoheadrightarrow \mathrm{Gal}(K^{\mathrm{ab}}/K)$$

sending a local uniformizer $\pi_{\mathfrak{p}} \in K_{\mathfrak{p}}$, for $\mathfrak{p} \subseteq K$ finite prime, to an element $\sigma \in \mathrm{Gal}(K^{\mathrm{ab}}/K)$ that restricts to the Frobenius element at $\mathfrak{p}$ in $\mathrm{Gal}(L/K)$ for every finite abelian extension $K \subseteq L$ unramified at $\mathfrak{p}$. By Artin reciprocity, this map factors through the *idèle class group* $\mathbb{A}_K^\times/K^\times$, giving rise to the *idelic Artin map* that we denote again by $[\cdot, K] : \mathbb{A}_K^\times/K^\times \to \mathrm{Gal}(K^{\mathrm{ab}}/K)$. For any modulus (ideal) $\mathfrak{m} \subseteq \mathcal{O}_K$, denote by $\mathrm{Cl}_{\mathfrak{m}}$ the ray class group modulo $\mathfrak{m}$ and by $H_{\mathfrak{m}}$ the ray class field modulo $\mathfrak{m}$. Then by [CS08, Lemma 3.4] there is a surjective homomorphism

$$\mathbb{A}_K^\times/K^\times \twoheadrightarrow \mathrm{Cl}_{\mathfrak{m}} \tag{3.9}$$

such that, if $\psi_{K,\mathfrak{m}} : \mathrm{Cl}_{\mathfrak{m}} \to \mathrm{Gal}(H_{\mathfrak{m}}/K)$ indicates the “classical” Artin isomorphism sending the class of a prime not dividing $\mathfrak{m}$ to its corresponding Frobenius element, the following diagram

$$\begin{tikzcd}
\mathbb{A}_K^\times/K^\times \arrow[r, "{[\cdot,K]}"] \arrow[dr] & \mathrm{Gal}(K^{\mathrm{ab}}/K) \arrow[r, two heads, "\mathrm{res}"] & \mathrm{Gal}(H_{\mathfrak{m}}/K) \\
& \mathrm{Cl}_{\mathfrak{m}} \arrow[ur, "\psi_{K,\mathfrak{m}}"'] &
\end{tikzcd} \tag{3.10}$$

commutes. Using the map (3.9) with $\mathfrak{m} = (1) = \mathcal{O}_K$ we obtain an exact sequence

$$1 \to \mathcal{O}_K^\times \to \widehat{\mathcal{O}}_K^\times \times \mathbb{C}^\times \to \mathbb{A}_K^\times/K^\times \to \mathrm{Cl}(K) \to 1 \tag{3.11}$$

where $\widehat{\mathcal{O}}_K^\times := \prod_{\mathfrak{p} \text{ finite}} \mathcal{O}_{K_{\mathfrak{p}}}^\times$ and $\mathbb{C}^\times$ can be viewed as subgroups of $\mathbb{A}_K^\times$. As a reference, one can look at [CS08, Equation (3-2)] with the caveat that, in their notation, one should replace the unit group $\mathbb{Z}_K^\times$ with its topological closure inside $\widehat{\mathbb{Z}}_K^\times \times \prod_{\mathfrak{p} \text{ real}} \langle -1 \rangle$. In our setting it is not necessary to take any topological closure since the unit group of an imaginary quadratic field is always finite.

Let $D \subseteq \mathbb{A}_K^\times/K^\times$ be the kernel of the Artin map, which is equal to the connected component of the identity in the idèle class group (see [AT09, Chapter IX]). In the imaginary quadratic case one has

$$D = K^\times \mathbb{C}^\times / K^\times$$

so that, using the commutativity of diagram (3.10) and the exact sequence (3.11) one obtains the isomorphism

$$\mathrm{Gal}(K^{\mathrm{ab}}/H) \cong (\widehat{\mathcal{O}}_K^\times \times \mathbb{C}^\times) K^\times / D \cong \widehat{\mathcal{O}}_K^\times / \mathcal{O}_K^\times. \tag{3.12}$$

Of course, since the kernel of the Artin map is equal to the image in the idèle class group of $(K \otimes_{\mathbb{Q}} \mathbb{R})^\times = \mathbb{C}^\times$, one could have more conveniently worked with the *finite idèles* $\mathbb{A}^\times_{K,\mathrm{fin}} := \prod'_{\mathfrak{p}\ \mathrm{finite}} K_{\mathfrak{p}}^\times$. Then the above discussion could be summarized by saying that the diagram

$$\begin{tikzcd}
\mathbb{A}^\times_{K,\mathrm{fin}} \arrow[r, two heads] & \mathbb{A}^\times_{K,\mathrm{fin}}/K^\times \arrow[r, two heads, "{[\cdot,K]}"] & \mathrm{Gal}(K^{\mathrm{ab}}/K) \\
\widehat{\mathcal{O}}_K^\times \arrow[r, two heads] \arrow[u, hook] & \widehat{\mathcal{O}}_K^\times/\mathcal{O}_K^\times \arrow[r, "\sim"] \arrow[u, hook] & \mathrm{Gal}(K^{\mathrm{ab}}/H) \arrow[u, hook]
\end{tikzcd}$$

commutes.

Fix now an elliptic curve $E_{/H}$ with complex multiplication by the ring of integers $\mathcal{O}_K$. We have already seen in Theorem 1.3.4 that H can be constructed by adjoining to K the singular modulus $j(E)$. Likewise, using the elliptic curve E one can explicitly construct for any modulus $\mathfrak{m} \subseteq \mathcal{O}_K$ the ray class field modulo $\mathfrak{m}$ of K. In order to do so, it suffices to fix a *Weber function* $\mathfrak{h}_E : E \longrightarrow E/\mathrm{Aut}(E)$ for E (see [Sil94, Page 134]) and to compute its values at the torsion points in $E[\mathfrak{m}]$. Then one always has $H_{\mathfrak{m}} = H(\mathfrak{h}_E(E[\mathfrak{m}]))$, as proved for instance in [Sil94, II, Theorem 5.6]. If the elliptic curve E is given by a short Weierstrass model $E : y^2 = x^3 + Ax + B$ with $A, B \in H$ and $j(E) \neq 0, 1728$ then we may take as Weber function $\mathfrak{h}_E$ simply the x-coordinate on E. In the two exceptional cases $j(E) = 0$ or $j(E) = 1728$ one has to “normalize" the x-coordinate to account for the extra automorphisms possessed by E, see [Sil94, II, Example 5.5.1]. Hence we find that for every ideal $\mathfrak{m} \subseteq \mathcal{O}_K$ there is always an inclusion $H_{\mathfrak{m}} \subseteq H(E[\mathfrak{m}])$ and, in particular, we have the containment $K^{\mathrm{ab}} \subseteq H(E_{\mathrm{tors}})$.

As we have studied in Section 3.1, the Galois representation (3.3) allows to identify the group $\mathrm{Gal}(H(E_{\mathrm{tors}})/H)$ with a subgroup of $\widehat{\mathcal{O}}_K^\times$. On the other hand, we have seen in (3.12) that the Artin map induces an isomorphism $\mathrm{Gal}(K^{\mathrm{ab}}/K) \cong \widehat{\mathcal{O}}_K/\mathcal{O}_K^\times$. Since we have both a restriction map $\mathrm{Gal}(H(E_{\mathrm{tors}})/H) \longrightarrow \mathrm{Gal}(K^{\mathrm{ab}}/K)$ and a projection map $\widehat{\mathcal{O}}_K^\times \twoheadrightarrow \widehat{\mathcal{O}}_K^\times/\mathcal{O}_K^\times$, it seems natural to ask if and how all these map are related between each other. The answer is given by the following theorem.

Theorem 3.2.1. *Let K be an imaginary quadratic field with ring of integers $\mathcal{O}_K \subseteq K$ and Hilbert class field H. Let $E_{/H}$ be an elliptic curve with complex multiplication by $\mathcal{O}_K$. Then the following diagram*

$$\begin{tikzcd}
\mathrm{Gal}(H(E_{tors})/H) \arrow[r, two heads] \arrow[d, hook, "\rho_E"'] & \mathrm{Gal}(K^{ab}/H) \\
\widehat{\mathcal{O}}_K^\times \arrow[r, two heads] & \widehat{\mathcal{O}}_K^\times/\mathcal{O}_K^\times \arrow[u, hook, "{1/[\cdot,K]}"']
\end{tikzcd}$$

commutes, where $1/[\cdot,K] : \widehat{\mathcal{O}}_K^\times/\mathcal{O}_K^\times \longrightarrow \mathrm{Gal}(K^{ab}/H)$ denotes the reciprocal of the Artin map (i.e. the Artin map followed by inversion).

We will prove a more general version of this result in Theorem 3.4.2. Here we content ourselves to give some comments on the statement. In particular, the reader may be a bit surprised by the appearance of the reciprocal of the Artin map in a place where it seems more natural to find the classical idelic Artin map. However, we want to show that such a phenomenon is not so shocking, since it already occurs when studying the class field theory of the rational numbers. Let us see how.

By the Kronecker-Weber Theorem, the maximal abelian extension $\mathbb{Q}^{\mathrm{ab}}$ of $\mathbb{Q}$ is obtained by adjoining to the field of rational numbers the group $\zeta_\infty \subseteq \overline{\mathbb{Q}}$ of all the roots of unity in the algebraic closure of $\mathbb{Q}$. In particular, we have a Galois representation

$$\rho : \mathrm{Gal}(\mathbb{Q}^{\mathrm{ab}}/\mathbb{Q}) \hookrightarrow \mathrm{Aut}_{\mathbb{Z}}(\zeta_\infty) \cong \mathrm{Aut}_{\mathbb{Z}}(\mathbb{Q}/\mathbb{Z}) = \mathrm{Aut}_{\mathbb{Z}}\left(\varinjlim_{N \in \mathbb{N}} \frac{1}{N}\mathbb{Z}/\mathbb{Z} \right) \cong \widehat{\mathbb{Z}}^\times$$

and it is easy to see that ρ is actually an isomorphism. The inverse ρ^{-1} sends an element $s = (s_N)_{N\in\mathbb{N}} \in \widehat{\mathbb{Z}}^\times$ to the field automorphism $\zeta_N \mapsto \zeta_N^{s_N}$ for every $N \in \mathbb{N}$, where ζ_N denotes any primitive N-root of unity. On the other hand, the idelic Artin map gives a surjection $\mathbb{A}_{\mathbb{Q}}^\times/\mathbb{Q}^\times \twoheadrightarrow \mathrm{Gal}(\mathbb{Q}^{\mathrm{ab}}/\mathbb{Q})$. Since every idèle $s = ((s_p)_p, s_\infty)$ can be uniquely written as a product of a rational number and a unit idèle $u_s \in \widehat{\mathbb{Z}}^\times \times \mathbb{R}_{>0}$, we have an isomorphism

$$\mathbb{A}_{\mathbb{Q}}^\times/\mathbb{Q}^\times \cong \widehat{\mathbb{Z}}^\times \times \mathbb{R}_{>0}$$

and we see in particular that the connected component of the identity element is given by $\{1\} \times \mathbb{R}_{>0}$. Hence, also the Artin map induces an isomorphism

$$[\cdot, \mathbb{Q}] : \widehat{\mathbb{Z}}^\times \cong \mathbb{A}_{\mathbb{Q}}^\times/(\mathbb{Q}^\times \cdot \mathbb{R}_{>0}) \longrightarrow \mathrm{Gal}(\mathbb{Q}^{\mathrm{ab}}/\mathbb{Q}).$$

However, this is *not* the same isomorphism induced by ρ^{-1}, *i.e.* the diagram

$$\begin{tikzcd}
\widehat{\mathbb{Z}}^\times \arrow[r, "\mathrm{id}"] \arrow[d, "\wr"'] & \widehat{\mathbb{Z}}^\times \arrow[d, "\rho^{-1}"] \\
\mathbb{A}_{\mathbb{Q}}^\times/(\mathbb{Q}^\times \cdot \mathbb{R}_{>0}) \arrow[r, "{[\cdot,\mathbb{Q}]}"'] & \mathrm{Gal}(\mathbb{Q}^{\mathrm{ab}}/\mathbb{Q})
\end{tikzcd}$$

does not commute. The right diagram to consider is rather

$$\begin{tikzcd}
\widehat{\mathbb{Z}}^\times \arrow[r, "-1"] \arrow[d, "\wr"'] & \widehat{\mathbb{Z}}^\times \arrow[d, "\rho^{-1}"] \\
\mathbb{A}_{\mathbb{Q}}^\times/(\mathbb{Q}^\times \cdot \mathbb{R}_{>0}) \arrow[r, "{[\cdot,\mathbb{Q}]}"'] & \mathrm{Gal}(\mathbb{Q}^{\mathrm{ab}}/\mathbb{Q})
\end{tikzcd} \tag{3.13}$$

where the map labelled with -1 denotes the inversion. This new diagram is instead commutative. To see it, notice that the prime $\ell \in \mathbb{Q}_\ell^\times \subseteq \mathbb{A}_{\mathbb{Q}}^\times$ is sent by the Artin map to the Frobenius at ℓ, which raises roots of unity of order coprime to ℓ to the ℓ-th power. On the other hand, a representative in $\widehat{\mathbb{Z}}^\times$ of the class of ℓ in $\mathbb{A}_{\mathbb{Q}}^\times/(\mathbb{Q}^\times \cdot \mathbb{R}_{>0})$ is given by $s = ((s_p)_p, s_\infty)$ with $s_p = \ell^{-1}$ if $p \neq \ell$ and $s_\ell = 1$. We then have that $[\ell, \mathbb{Q}] = \rho^{-1}(s^{-1})$, thus proving the commutativity of (3.13). The reciprocal of the Artin map in Theorem 3.2.1 arises in the same way as in (3.13). The proof of the more general Theorem 3.4.2 will make use of (one form of) the *Main Theorem of Complex Multiplication* which can be thought of as the imaginary quadratic version of the above discussion.

How does the exposition of this section change if we consider elliptic curves with complex multiplication by non-maximal orders? The first thing to understand is what kind of class fields one obtains after adjoining the values of Weber functions at torsion points of these elliptic curves to the corresponding ring class fields. It turns out that these extensions, that will be called ray class fields for orders, can be described idelically and one obtains a theory that is very similar to the theory of the usual ray class fields. This will allow to cast the situation considered in this section into a more general setting, and we will see that all the described results hold analogously in the world of non-maximal orders.

3.3 Ray class fields for orders

We have recalled in the previous section that, for an elliptic curve E with complex multiplication by the ring of integers $\mathcal{O}_K$ of an imaginary quadratic field K and defined over the Hilbert class field H of K, the division field $H(E[I])$ always contains the ray class field modulo I for every ideal $I \subseteq \mathcal{O}_K$. The situation is similar when E has complex multiplication by an order that is non-maximal. Also in this case the division fields associated to E contain some special abelian extensions of K, which are completely analogous to the ray class fields above. Since the construction of these fields can be performed in quite a general setting, in this chapter we will not restrict ourselves to the case of imaginary quadratic orders. Our goal is then to define, for every ideal I contained in a general order $\mathcal{O}$ of a number field F, an abelian extension $F \subseteq H_{I,\mathcal{O}}$ which we call the *ray class field modulo I for the order $\mathcal{O}$*. Our definition generalises the one given by Söhngen in [Söh35] and Stevenhagen in [Ste01, § 4], who restrict their attention to imaginary quadratic fields.

Let F be a number field. For a place $w \in M_F$ denote by F_w the completion of the number field F at w and by $\mathcal{O}_{F_w}$ its ring of integers. Let $\mathbb{A}_F$ be the *adèle ring* of F, defined by the restricted product

$$\mathbb{A}_F := \prod_{w \in M_F}{}' F_w = \left\{ s = (s_w)_{w \in M_F} \in \prod_{w \in M_F} F_w \,\middle|\, s_w \in \mathcal{O}_{F_w} \text{ for almost all } w \in M_F \right\}.$$

The discussion on [Neu99, Page 371] shows that $\mathbb{A}_F$ can be obtained from the rational adèle ring by extending scalars, *i.e.* there is a ring isomorphism $\mathbb{A}_F \cong \mathbb{A}_\mathbb{Q} \otimes_\mathbb{Q} F$. This enables us to talk, for a place $p \in M_\mathbb{Q}$, of the *p-component* $s_p \in F_p := \mathbb{Q}_p \otimes_\mathbb{Q} F$ of an adèle $s \in \mathbb{A}_F$; in particular if $p = \infty$ is the unique infinite place of $\mathbb{Q}$ we have the *infinity component* $s_\infty \in \mathbb{R} \otimes_\mathbb{Q} F$. Hence $s \in \mathbb{A}_F$ can be alternatively written as

$$s = (s_w)_{w \in M_F} \quad \text{or} \quad s = (s_p)_{p \in M_\mathbb{Q}} \tag{3.14}$$

and of course the same is true if s belongs to the *idèle group* $\mathbb{A}_F^\times$. In what follows, we will often confuse finite places $p \in M_\mathbb{Q}^0$ and rational primes $p \in \mathbb{N}$.

Using the language introduced above, we are now able to define the ray class fields $H_{I,\mathcal{O}}$.

Definition 3.3.1. *Let F be a number field, let $\mathcal{O} \subseteq \mathcal{O}_F$ be an order and let $I \subseteq \mathcal{O}$ be a non-zero ideal. Then we define the ray class field of F modulo I relative to the order $\mathcal{O}$ as*

$$H_{I,\mathcal{O}} := (F^{ab})^{[U_{I,\mathcal{O}},F]} \subseteq F^{ab} \tag{3.15}$$

where $[\cdot, F] \colon \mathbb{A}_F^\times \twoheadrightarrow \mathrm{Gal}(F^{ab}/F)$ is the idelic Artin map and $U_{I,\mathcal{O}} \subseteq \mathbb{A}_F^\times$ is the subgroup

$$U_{I,\mathcal{O}} := \left\{ s \in \mathbb{A}_F^\times \,\middle|\, s_p \in \left(\mathcal{O}_p^\times \cap (1 + I \cdot \mathcal{O}_p) \right) \textit{ for all rational primes } p \in \mathbb{N} \right\} \tag{3.16}$$

defined using the decomposition (3.14), *where*

$$\mathcal{O}_p := \varprojlim_{n\in\mathbb{N}} \frac{\mathcal{O}}{p^n\mathcal{O}} \cong \mathcal{O}\otimes_{\mathbb{Z}}\mathbb{Z}_p \tag{3.17}$$

denotes the completion of $\mathcal{O}$ *with respect to the ideal* $p\,\mathcal{O}$.

When $I = N\cdot\mathcal{O}$ for some $N\in\mathbb{Z}_{\geq 1}$ we denote $U_{I,\mathcal{O}}$ by $U_{N,\mathcal{O}}$, and we write $U_{\mathcal{O}} := U_{1,\mathcal{O}}$. Analogously, we will write $H_{N,\mathcal{O}}$ in place of $H_{N\cdot\mathcal{O},\mathcal{O}}$, and we will denote by $H_{\mathcal{O}} := H_{1,\mathcal{O}}$ the *ring class field* of $\mathcal{O}$.

Remark 3.3.2. When $\mathcal{O} = \mathcal{O}_F$ is the ring of integers, the ray class fields $H_{I,\mathcal{O}_F}$ coincide with the usual ray class fields of F modulo I (see [Neu99, Chapter VI, Definition 6.2]). Moreover, when $F = K$ is an imaginary quadratic field, the ray class fields $H_{I,\mathcal{O}}$ have been defined by Söhngen in [Söh35]. This work is exposed in great detail by Schertz in [Sch10, §3.3], and if $I = N\cdot\mathcal{O}$ for some $N\in\mathbb{N}$ the construction of $H_{I,\mathcal{O}} = H_{N,\mathcal{O}}$ has been reformulated using an adelic language by Stevenhagen in [Ste01, § 4]. Finally, the ring class fields $H_{\mathcal{O}}$ have been studied for general number fields F by Lv and Deng in [LD15] and by Yi and Lv in [YL18].

Remark 3.3.3. It is clear from the definition that for every pair of ideals $I\subseteq J\subseteq\mathcal{O}$ we have that $U_{I,\mathcal{O}}\subseteq U_{J,\mathcal{O}}$, which implies that $H_{I,\mathcal{O}}\supseteq H_{J,\mathcal{O}}$. In particular, $H_{\mathcal{O}}\subseteq H_{I,\mathcal{O}}$ for every ideal $I\subseteq\mathcal{O}$. Similarly, for every pair of orders $\mathcal{O}_1\subseteq\mathcal{O}_2\subseteq F$ and every ideal $I\subseteq\mathcal{O}_1$ we have that $U_{I,\mathcal{O}_1}\subseteq U_{I\cdot\mathcal{O}_2,\mathcal{O}_2}$ using the fact that $\mathbb{Z}_p$ is a flat $\mathbb{Z}$-module. This gives the containment $H_{I,\mathcal{O}_1}\supseteq H_{I\cdot\mathcal{O}_2,\mathcal{O}_2}$ and we recover the *Anordnungssatz* explained in [Ste01, Page 169]. Finally, for every ideal $I\subseteq\mathcal{O}$ we have $U_{I\cdot\mathfrak{f}_{\mathcal{O}}\cdot\mathcal{O}_F,\mathcal{O}_F}\subseteq U_{I,\mathcal{O}}$ where $\mathfrak{f}_{\mathcal{O}}\subseteq\mathcal{O}$ is the conductor of the order $\mathcal{O}$ (see Definition 1.1.5). The situation can be summarized by the following diagram

$$\begin{tikzcd}
 & H_{I\cdot\mathcal{O}_F,\mathcal{O}_F} \arrow[r, phantom, "\subseteq"] & H_{I,\mathcal{O}} \arrow[r, phantom, "\subseteq"] & H_{I\cdot\mathfrak{f}_{\mathcal{O}}\cdot\mathcal{O}_F,\mathcal{O}_F} \\
F \arrow[r, phantom, "\subseteq"] & H_{\mathcal{O}_F} \arrow[u, phantom, sloped, "\subseteq"] \arrow[r, phantom, "\subseteq"] & H_{\mathcal{O}} \arrow[u, phantom, sloped, "\subseteq"] \arrow[r, phantom, "\subseteq"] & H_{\mathfrak{f}_{\mathcal{O}},\mathcal{O}_F} \arrow[u, phantom, sloped, "\subseteq"]
\end{tikzcd}$$

which, among other things, shows that the extension $F\subseteq H_{I,\mathcal{O}}$ is unramified outside the set of primes dividing $I\cdot\mathfrak{f}_{\mathcal{O}}\cdot\mathcal{O}_F$.

We now describe the Galois groups of the abelian extensions $F\subseteq H_{I,\mathcal{O}}$.

Lemma 3.3.4. *Let* F *be a number field,* $\mathcal{O}\subseteq\mathcal{O}_F$ *be an order and* $I\subseteq\mathcal{O}$ *be a non-zero ideal. Then* $F^\times\cdot U_{I,\mathcal{O}}\subseteq\mathbb{A}_F^\times$ *is a closed subgroup of finite index and, after identifying the group*

$$F_\infty^\times := (F\otimes_{\mathbb{Q}}\mathbb{R})^\times \cong \prod_{v\in M_F^\infty} F_v^\times$$

with its image under the natural inclusion $F_\infty^\times \hookrightarrow \mathbb{A}_F^\times$, *one has*

$$F^\times\cdot F_\infty^\times \subseteq \ker([\cdot,F]) \subseteq F^\times\cdot U_{I,\mathcal{O}} = F^\times\cdot \mathrm{N}_{H_{I,\mathcal{O}}/F}(\mathbb{A}_{H_{I,\mathcal{O}}}^\times)$$

where $\mathrm{N}_{H_{I,\mathcal{O}}/F}\colon \mathbb{A}_{H_{I,\mathcal{O}}}^\times \to \mathbb{A}_F^\times$ *denotes the idelic norm map. Moreover, there is an isomorphism*

$$\mathrm{Gal}(H_{I,\mathcal{O}}/F) \cong \frac{\mathbb{A}_F^\times}{F^\times\cdot U_{I,\mathcal{O}}} \tag{3.18}$$

induced by the global Artin map.

Proof. The fact that $F^\times \cdot U_{I,\mathcal{O}}$ is closed of finite index follows from [Neu99, Chapter VI, Proposition 1.8], because $U_{I \cdot \mathfrak{f}_\mathcal{O} \cdot \mathcal{O}_F, \mathcal{O}_F} \subseteq U_{I,\mathcal{O}}$. Moreover, by definition $F_\infty^\times \subseteq U_{I,\mathcal{O}}$, so the inclusions $F^\times \cdot F_\infty^\times \subseteq \ker([\cdot, F]) \subseteq F^\times \cdot U_{I,\mathcal{O}}$ follow from the fact that $F^\times \cdot U_{I,\mathcal{O}}$ is closed in $\mathbb{A}_F^\times$ and $\ker([\cdot, F])$ is the closure of $F^\times \cdot F_\infty^\times$ inside $\mathbb{A}_F^\times$, as explained in [AT68, Chapter IX]. The global reciprocity law [Neu99, Chapter VI, Theorem 6.1] now gives (3.18) and shows that $F^\times \cdot \mathrm{N}_{H_{I,\mathcal{O}}/F}(\mathbb{A}_{H_{I,\mathcal{O}}}^\times) \subseteq \mathbb{A}_F^\times$ is also a closed subgroup of finite index containing the kernel of the Artin map and fixing precisely the field $H_{I,\mathcal{O}}$. Then by Galois theory we must have $F^\times \cdot U_{I,\mathcal{O}} = F^\times \cdot \mathrm{N}_{H_{I,\mathcal{O}}/F}(\mathbb{A}_{H_{I,\mathcal{O}}}^\times)$ and this concludes the proof. □

The previous description can be made more explicit by dividing the extension $F \subseteq H_{I,\mathcal{O}}$ in the two sub-extensions $F \subseteq H_\mathcal{O}$ and $H_\mathcal{O} \subseteq H_{I,\mathcal{O}}$.

Proposition 3.3.5. *Let $\mathcal{O}$ be an order inside a number field F. Then*

$$\mathrm{Gal}(H_\mathcal{O}/F) \cong \mathrm{Pic}(\mathcal{O})$$

where $\mathrm{Pic}(\mathcal{O})$ *denotes the class group of the order $\mathcal{O}$.*

Proof. Combine [YL18, Theorem and Definition 2.11] and [YL18, Theorem 4.2]. □

Theorem 3.3.6. *Let F be a number field, $\mathcal{O} \subseteq \mathcal{O}_F$ be an order and $I \subseteq \mathcal{O}$ be a non-zero ideal. Then the Artin map gives an isomorphism*

$$\mathrm{Gal}(H_{I,\mathcal{O}}/H_\mathcal{O}) \cong \frac{(\mathcal{O}/I)^\times}{\pi_I^\times(\mathcal{O}^\times)}$$

where $\pi_I^\times \colon \mathcal{O}^\times \longrightarrow (\mathcal{O}/I)^\times$ is the morphism induced by the projection $\pi_I \colon \mathcal{O} \twoheadrightarrow \mathcal{O}/I$. In particular, if F is totally complex, after taking inverse limits we obtain an isomorphism

$$\mathrm{Gal}(F^{ab}/H_\mathcal{O}) \cong \widehat{\mathcal{O}}^\times / \overline{\mathcal{O}^\times}$$

where $\overline{\mathcal{O}^\times}$ is the topological closure of $\mathcal{O}^\times$ in $\widehat{\mathcal{O}}^\times$.

Proof. First of all, we see that

$$\begin{aligned}
\mathrm{Gal}(H_{I,\mathcal{O}}/H_\mathcal{O}) = \ker\left(\mathrm{Gal}(H_{I,\mathcal{O}}/F) \twoheadrightarrow \mathrm{Gal}(H_\mathcal{O}/F)\right) &\overset{(a)}{\cong} \ker\left(\frac{\mathbb{A}_F^\times}{F^\times \cdot U_{I,\mathcal{O}}} \twoheadrightarrow \frac{\mathbb{A}_F^\times}{F^\times \cdot U_\mathcal{O}}\right) \cong \\
\cong \frac{F^\times \cdot U_\mathcal{O}}{F^\times \cdot U_{I,\mathcal{O}}} \cong \frac{F^\times \cdot U_\mathcal{O}/F^\times}{F^\times \cdot U_{I,\mathcal{O}}/F^\times} &\overset{(b)}{\cong} \frac{U_\mathcal{O}/(F^\times \cap U_\mathcal{O})}{(U_{I,\mathcal{O}} \cdot (F^\times \cap U_\mathcal{O}))/(F^\times \cap U_\mathcal{O})} \cong \\
\cong \frac{U_\mathcal{O}}{U_{I,\mathcal{O}} \cdot (F^\times \cap U_\mathcal{O})} &\overset{(c)}{=} \frac{U_\mathcal{O}}{U_{I,\mathcal{O}} \cdot \mathcal{O}^\times}
\end{aligned}$$

where (a) comes from Lemma 3.3.4, (b) holds because $U_{I,\mathcal{O}} \subseteq U_\mathcal{O}$ and (c) follows from the fact that $F^\times \cap U_\mathcal{O} = \mathcal{O}^\times$.

Now, observe that $F_\infty^\times \subseteq U_\mathcal{O}$, where $F_\infty := F \otimes_\mathbb{Q} \mathbb{R} \cong \prod_{w \mid \infty} F_w \hookrightarrow \mathbb{A}_F$. Moreover, we have

$$\frac{U_\mathcal{O}}{F_\infty^\times} \cong \prod_{p \in \mathbb{N}} \mathcal{O}_p^\times \cong \prod_{p \in \mathbb{N}} \varprojlim_{n \in \mathbb{N}} \left(\frac{\mathcal{O}}{p^n \mathcal{O}}\right)^\times \cong \varprojlim_{N \in \mathbb{Z}_{\geq 1}} \left(\frac{\mathcal{O}}{N\mathcal{O}}\right)^\times \cong \widehat{\mathcal{O}}^\times \tag{3.19}$$

where the products run over the rational primes $p \in \mathbb{N}$, and $\mathcal{O}_p$ is the ring defined in (3.17). In the chain of isomorphisms (3.19) the ring $\widehat{\mathcal{O}}$ is the profinite completion of $\mathcal{O}$, *i.e.*

$$\widehat{\mathcal{O}} := \varprojlim_{N \in \mathbb{Z}_{\geq 1}} \frac{\mathcal{O}}{N\mathcal{O}} \cong \prod_{p \in \mathbb{N}} \mathcal{O}_p \cong \prod_{\mathfrak{p} \subseteq \mathcal{O}} \mathcal{O}_{\mathfrak{p}} \tag{3.20}$$

where the second product runs over all the non-zero prime ideals $\mathfrak{p} \subseteq \mathcal{O}$ and $\mathcal{O}_{\mathfrak{p}} := \varprojlim_{n \in \mathbb{N}} \mathcal{O}/\mathfrak{p}^n$ is the completion of $\mathcal{O}$ at the prime $\mathfrak{p}$. The second isomorphism appearing in (3.20) can be obtained by applying [Eis95, Corollary 7.6] to $R = \mathbb{Z}_p$ and $A = \mathcal{O}_p$. This gives the decomposition

$$\mathcal{O}_p \cong \prod_{\mathfrak{p} \supseteq p} \mathcal{O}_{\mathfrak{p}}$$

where the product runs over all primes $\mathfrak{p} \subseteq \mathcal{O}$ lying above p.

Under the isomorphism (3.19) the subgroup $U_{I,\mathcal{O}}/F_\infty^\times \subseteq U_{\mathcal{O}}/F_\infty^\times \cong \widehat{\mathcal{O}}^\times$ is identified with the kernel of the map $\widehat{\pi}_I^\times : \widehat{\mathcal{O}}^\times \longrightarrow (\widehat{\mathcal{O}}/I\widehat{\mathcal{O}})^\times$ induced by the projection $\widehat{\pi}_I : \widehat{\mathcal{O}} \twoheadrightarrow \widehat{\mathcal{O}}/I\widehat{\mathcal{O}}$. Hence

$$\operatorname{Gal}(H_{I,\mathcal{O}}/H_{\mathcal{O}}) \cong \frac{U_{\mathcal{O}}}{U_{I,\mathcal{O}} \cdot \mathcal{O}^\times} \cong \frac{U_{\mathcal{O}}/F_\infty^\times}{(U_{I,\mathcal{O}} \cdot \mathcal{O}^\times)/F_\infty{}^\times} \cong \frac{\widehat{\mathcal{O}}^\times}{\ker(\widehat{\pi}_I{}^\times) \cdot \mathcal{O}^\times} \cong \frac{(\widehat{\mathcal{O}}/I\widehat{\mathcal{O}})^\times}{\widehat{\pi}_I{}^\times(\mathcal{O}^\times)}$$

because $\widehat{\pi}_I{}^\times$ is surjective. This surjectivity is shown by the factorisation

$$\begin{tikzcd}
\widehat{\mathcal{O}}^\times \arrow[rr, "\widehat{\pi}_I{}^\times"] \arrow[dr, two heads] & & \left(\widehat{\mathcal{O}}/I\widehat{\mathcal{O}}\right)^\times \\
& \prod_{\mathfrak{p} \supseteq I} \mathcal{O}_{\mathfrak{p}}^\times \arrow[ur, two heads] &
\end{tikzcd}$$

where the first map $\widehat{\mathcal{O}}^\times \twoheadrightarrow \prod_{\mathfrak{p} \supseteq I} \mathcal{O}_{\mathfrak{p}}^\times$ is surjective as follows from (3.20), and the second map

$$\prod_{\mathfrak{p} \supseteq I} \mathcal{O}_{\mathfrak{p}}^\times \twoheadrightarrow \prod_{\mathfrak{p} \supseteq I} \left(\frac{\mathcal{O}_{\mathfrak{p}}}{I\mathcal{O}_{\mathfrak{p}}}\right)^\times \cong \left(\frac{\widehat{\mathcal{O}}}{I\widehat{\mathcal{O}}}\right)^\times$$

is surjective by [Che, Corollary 2.3], which can be applied since the ring $\prod_{\mathfrak{p} \supseteq I} \mathcal{O}_{\mathfrak{p}}$ has finitely many maximal ideals.

To finish our proof we need to show that

$$\frac{(\widehat{\mathcal{O}}/I\widehat{\mathcal{O}})^\times}{\widehat{\pi}_I{}^\times(\mathcal{O}^\times)} \cong \frac{(\mathcal{O}/I)^\times}{\pi_I^\times(\mathcal{O}^\times)}.$$

To do this recall that π_I and $\widehat{\pi}_I$ are related by the commutative diagram

$$\begin{tikzcd}
\mathcal{O} \arrow[r, two heads, "\pi_I"] \arrow[d, hook] & \mathcal{O}/I \arrow[r, "\gamma"] \arrow[d] & \prod_{\mathfrak{p} \supseteq I} \frac{\mathcal{O}_{(\mathfrak{p})}}{I\mathcal{O}_{(\mathfrak{p})}} \arrow[d, "\beta"] \\
\widehat{\mathcal{O}} \arrow[r, two heads, "\widehat{\pi_I}"] & \widehat{\mathcal{O}}/I\widehat{\mathcal{O}} \arrow[r, "\alpha", "\sim"'] & \prod_{\mathfrak{p} \supseteq I} \frac{\mathcal{O}_{\mathfrak{p}}}{I\mathcal{O}_{\mathfrak{p}}}
\end{tikzcd}$$

where α is the isomorphism coming from the decomposition (3.20), and β and γ are the maps induced by the natural inclusions $\mathcal{O} \subseteq \mathcal{O}_{(\mathfrak{p})} \subseteq \mathcal{O}_{\mathfrak{p}}$. Moreover the products run over all the prime ideals $\mathfrak{p} \subseteq \mathcal{O}$ such that $\mathfrak{p} \supseteq I$, and $\mathcal{O}_{(\mathfrak{p})}$ denotes the localisation of $\mathcal{O}$ at the prime $\mathfrak{p}$.

Hence to conclude it is sufficient to observe that γ is an isomorphism by [Neu99, Chapter I, Proposition 12.3], and β is an isomorphism because $\mathcal{O}$ is a one-dimensional Noetherian domain (see [Neu99, Chapter I, Proposition 12.2]). More explicitly, for any prime $\mathfrak{p} \subseteq \mathcal{O}$ such that $\mathfrak{p} \supseteq I$ we have that $\mathfrak{p} \cdot \mathcal{O}_{(\mathfrak{p})} = \sqrt{I \cdot \mathcal{O}_{(\mathfrak{p})}}$ because $\mathcal{O}_{(\mathfrak{p})}$ is a one-dimensional local ring. Hence [Bou89, Chapter II, § 2.6, Proposition 15] shows that $\mathcal{O}_{(\mathfrak{p})}/I\mathcal{O}_{(\mathfrak{p})}$ is complete with respect to $\mathfrak{p}\mathcal{O}_{(\mathfrak{p})}$. Thus we can conclude that $\mathcal{O}_{(\mathfrak{p})}/I\mathcal{O}_{(\mathfrak{p})}$ is isomorphic to $\mathcal{O}_{\mathfrak{p}}/I\mathcal{O}_{\mathfrak{p}}$ using the exactness of completion, which holds because $\mathcal{O}_{(\mathfrak{p})}$ is Noetherian (see [Eis95, Lemma 7.15]). □

3.4 Ray class fields for orders and elliptic curves

Since the definition of the ray class fields $H_{I,\mathcal{O}}$ is somehow implicit, a natural question would be to provide an explicit set of generators for the extension $F \subseteq H_{I,\mathcal{O}}$. This can be done when $F = K$ is an imaginary quadratic field, and $I \subseteq \mathcal{O}$ is invertible, as we will see in Theorem 3.4.1. In order to show this, we now introduce some notation concerning lattices in number fields, following [Lan87, Chapter 8].

Let F be a number field. A *lattice* $\Lambda \subseteq F$ is an additive subgroup of F which is free of rank $[F : \mathbb{Q}]$ over $\mathbb{Z}$. Given a pair of lattices $\Lambda_1, \Lambda_2 \subseteq F$ we can form their sum $\Lambda_1 + \Lambda_2 \subseteq F$, their product $\Lambda_1 \cdot \Lambda_2 \subseteq F$ and their quotient $(\Lambda_1 \colon \Lambda_2) := \{x \in F \mid x \cdot \Lambda_2 \subseteq \Lambda_1\} \subseteq F$. Moreover, it is possible to define an action of the idèle group of F on the set $\{\Lambda \subseteq F : \Lambda \text{ lattice}\}$, as we are going to describe.

For a lattice $\Lambda \subseteq F$ and a prime $p \in \mathbb{N}$, denote by $\Lambda_p := \Lambda \otimes_{\mathbb{Z}} \mathbb{Z}_p$ the completion of the lattice Λ at p. Given an idèle $s = (s_p)_{p \in M_{\mathbb{Q}}} \in \mathbb{A}_F^\times$ there exists a unique lattice $s \cdot \Lambda \subseteq F$ with the property that $(s \cdot \Lambda)_p = s_p \cdot \Lambda_p$ for every prime $p \in \mathbb{N}$. This defines an action of the idèle group $\mathbb{A}_F^\times$ on the set of lattices in F, given by $(s, \Lambda) \mapsto s \cdot \Lambda$. We remark that the notation $s \cdot \Lambda$, although evocative of a multiplication between an idèle and a lattice, is purely formal and should not be confused with the notation $\Lambda_1 \cdot \Lambda_2$ for the usual product of lattices. Nevertheless, it is easy to see from the definitions that $(s \cdot \Lambda_1) \cdot \Lambda_2 = s \cdot (\Lambda_1 \cdot \Lambda_2)$ for every pair of lattices $\Lambda_1, \Lambda_2 \subseteq F$. Using the action just described, it is also possible to define a *multiplication by s* map $F/\Lambda \xrightarrow{s\cdot} F/(s \cdot \Lambda)$ by means of the following commutative diagram

$$\begin{tikzcd}
\frac{F}{\Lambda} \arrow[r, "s\cdot"] \arrow[d, "\wr"'] & \frac{F}{s \cdot \Lambda} \arrow[d, "\wr"'] \\
\bigoplus_{p \in M_{\mathbb{Q}}^0} \frac{F_p}{\Lambda_p} \arrow[r, "(s_p\cdot)_p"] & \bigoplus_{p \in M_{\mathbb{Q}}^0} \frac{F_p}{s_p\Lambda_p}
\end{tikzcd}$$

where the vertical maps are the obvious isomorphisms induced by the inclusions $F \hookrightarrow F_p$ and the bottom map is given by $(x_p)_p \mapsto (s_p\, x_p)_p$.

The case of lattices inside an imaginary quadratic field K is of particular interest for us. Indeed, if $\mathcal{O} \subseteq K$ is an order, any finitely generated $\mathcal{O}$-module $\Lambda \subseteq K$ is a lattice inside K. Moreover, if we fix an embedding $K \hookrightarrow \mathbb{C}$, the quotient $\mathbb{C}/\Lambda$ can be canonically identified with the complex points $E(\mathbb{C})$ of an elliptic curve $E_{/\mathbb{C}}$ having complex multiplication by $\mathcal{O}$. For any invertible ideal $I \subseteq \mathcal{O}$, the following Theorem 3.4.1 shows that the extension $H_{\mathcal{O}} \subseteq H_{I,\mathcal{O}}$ can be obtained by adjoining to the ring class field $H_{\mathcal{O}}$ the values of a Weber function $\mathfrak{h}_E \colon E \twoheadrightarrow E/\mathrm{Aut}(E) \cong \mathbb{P}^1$ at torsion points $z \in E[I] := E(\mathbb{C})[I]$.

Theorem 3.4.1. *Let $\mathcal{O}$ be an order inside an imaginary quadratic field $K \subseteq \mathbb{C}$, and let $I \subseteq \mathcal{O}$ be an invertible ideal. Then we have that*

$$H_{I,\mathcal{O}} = H_{\mathcal{O}}(\mathfrak{h}_E(E[I])) = K(j(E), \mathfrak{h}_E(E[I]))$$

for any elliptic curve $E_{/\mathbb{C}}$ such that $\mathrm{End}(E) \cong \mathcal{O}$. *In particular, if E is an elliptic curve defined over a number field F such that* $\mathrm{End}_F(E) \cong \mathcal{O}$ *then $H_{I,\mathcal{O}} \subseteq F(E[I])$.*

Proof. By the discussion in Section 3.2, we can assume that $j(E) \notin \{0, 1728\}$, because in this case $\mathcal{O} = \mathcal{O}_K$. Recall that, since $I \subseteq \mathcal{O}$ is an invertible ideal, $E[I]$ is a free $\mathcal{O}/I$-module of rank one (see Lemma 3.1.1). Fix a generator P of $E[I]$ as a module over $\mathcal{O}/I$. Then $H_{\mathcal{O}}(\mathfrak{h}_E(E[I])) = H_{\mathcal{O}}(\mathfrak{h}_E(P))$, as one can see by writing every endomorphism of E in the standard form described in [Was08, § 2.9] and applying [Lan87, Chapter I, Theorem 7].

Let now $\xi \colon \mathbb{C}/\mathfrak{a} \longrightarrow E(\mathbb{C})$ be a complex parametrisation, where $\mathfrak{a} \subseteq \mathcal{O}$ is an invertible ideal (see Theorem 1.3.3). Fix moreover $z \in (\mathfrak{a} \colon I) \subseteq K \subseteq \mathbb{C}$ such that $\xi(\overline{z}) = P$, where $\overline{z} := (z + \mathfrak{a})/\mathfrak{a}$ denotes the image of z in the quotient $K/\mathfrak{a} \subseteq \mathbb{C}/\mathfrak{a}$. Then [Shi94, Theorem 5.5] shows that

$$H_{\mathcal{O}}(\mathfrak{h}_E(P)) = (K^{\mathrm{ab}})^{[W_P, K]}$$

where $W_P \subseteq \mathbb{A}_K^\times$ is the subgroup defined by $W_P := \left\{ s \in \mathbb{A}_K^\times \;\middle|\; s \cdot \mathfrak{a} = \mathfrak{a},\; s \cdot \overline{z} = \overline{z} \right\}$. In particular, we recall that for any $s \in \mathbb{A}_K^\times$ such that $s \cdot \mathfrak{a} = \mathfrak{a}$ the notation $s \cdot \overline{z}$ stands for the image of $\overline{z} \in K/\mathfrak{a}$ under the multiplication-by-s map $K/\mathfrak{a} \longrightarrow K/\mathfrak{a}$. This map is defined by the commutative diagram

$$\begin{tikzcd}
\frac{K}{\mathfrak{a}} \arrow[r, "s\cdot"] \arrow[d, "\wr"'] & \frac{K}{s \cdot \mathfrak{a}} \arrow[r, phantom, "="] \arrow[d, "\wr"'] & \frac{K}{\mathfrak{a}} \arrow[d, "\wr"'] \\
\bigoplus\limits_{p \in M_{\mathbb{Q}}^0} \frac{K_p}{\mathfrak{a}_p} \arrow[r, "(s_p \cdot)_p"] & \bigoplus\limits_{p \in M_{\mathbb{Q}}^0} \frac{K_p}{s_p \mathfrak{a}_p} \arrow[r, phantom, "="] & \bigoplus\limits_{p \in M_{\mathbb{Q}}^0} \frac{K_p}{\mathfrak{a}_p}
\end{tikzcd}$$

where $\mathfrak{a}_p := \mathfrak{a} \otimes_{\mathbb{Z}} \mathbb{Z}_p = \mathfrak{a}\, \mathcal{O}_p$ for any rational prime $p \in \mathbb{N}$. Since $H_{\mathcal{O}} = K(j(E))$ the theorem will follow from the equality $W_P = U_{I,\mathcal{O}}$, where $U_{I,\mathcal{O}} \subseteq \mathbb{A}_K^\times$ is the subgroup defined in (3.16).

To prove the inclusion $U_{I,\mathcal{O}} \subseteq W_P$ take any $s \in U_{I,\mathcal{O}}$. Then $s \cdot \mathfrak{a} = \mathfrak{a}$ because $s_p \mathfrak{a}_p = \mathfrak{a}_p$ for every rational prime $p \in \mathbb{N}$, since by definition $s_p \in \mathcal{O}_p^\times$. Moreover, $s \cdot \overline{z} = \overline{z}$ because $z \in (\mathfrak{a} \colon I)$ and $s_p \in 1 + I\mathcal{O}_p$ for every rational prime $p \in \mathbb{N}$, which implies that $(s_p - 1)z \in \mathfrak{a}_p$. This shows that $U_{I,\mathcal{O}} \subseteq W_z$

To prove the opposite inclusion $W_P \subseteq U_{I,\mathcal{O}}$ fix any rational prime $p \in \mathbb{N}$ and take $s \in W_P$, so that $s \cdot \mathfrak{a} = \mathfrak{a}$ and $s \cdot \overline{z} = \overline{z}$. Since $\mathfrak{a} \subseteq \mathcal{O}$ is invertible we have that $\mathfrak{a} \cdot (\mathcal{O} \colon \mathfrak{a}) = \mathcal{O}$ and

$$s \cdot \mathcal{O} = s \cdot (\mathfrak{a} \cdot (\mathcal{O} \colon \mathfrak{a})) = (s \cdot \mathfrak{a}) \cdot (\mathcal{O} \colon \mathfrak{a}) = \mathfrak{a} \cdot (\mathcal{O} \colon \mathfrak{a}) = \mathcal{O}$$

which shows that $s_p \in \mathcal{O}_p^\times$. Let us now prove that $s_p \in 1 + I \cdot \mathcal{O}_p$. Since $I \subseteq \mathcal{O}$ and $\mathfrak{a} \subseteq \mathcal{O}$ are both invertible we have that $I \cdot (\mathcal{O} \colon \mathfrak{a}) \cdot (\mathfrak{a} \colon I) = \mathcal{O}$, so that we can write $1 = \sum_{j=1}^{J} \alpha_j \beta_j \tau_j$ with $\alpha_j \in I$, $\beta_j \in (\mathcal{O} \colon \mathfrak{a})$ and $\tau_j \in (\mathfrak{a} \colon I)$. Notice that $s \cdot \overline{\tau_j} = \overline{\tau_j}$ for every $j \in \{1, \dots, J\}$ because $s \cdot \overline{z} = \overline{z}$ and $P = \xi(\overline{z})$ generates $E[I]$ as a module over $\mathcal{O}/I$. Hence $s_p - 1 \in I \cdot \mathcal{O}_p$ because we can write

$$s_p - 1 = \sum_{j=1}^{J} \alpha_j \, \beta_j \, (s_p \, \tau_j - \tau_j)$$

where $s_p \, \tau_j - \tau_j \in \mathfrak{a}_p = \mathfrak{a} \, \mathcal{O}_p$ and $\beta_j (s_p \, \tau_j - \tau_j) \in \mathcal{O}_p$ since $\beta_j \in (\mathcal{O} \colon \mathfrak{a})$ for every $j \in \{1, \dots, J\}$. Thus we have shown that $s_p \in \mathcal{O}_p^\times$ and $s_p \in 1 + I \cdot \mathcal{O}_p$ for every prime $p \in \mathbb{N}$, which gives $W_P \subseteq U_{I,\mathcal{O}}$ as we wanted to prove. □

In particular, Theorem 3.4.1 shows that for every invertible ideal $I \subseteq \mathcal{O}$ one has the containment $H_{I,\mathcal{O}} \subseteq H_{\mathcal{O}}(E[I])$. Using the Anordnungsatz, this yields the containment $K^{\mathrm{ab}} \subseteq H_{\mathcal{O}}(E_{\mathrm{tors}})$. We then find ourselves in the analogous situation described in Section 3.2 for classical ray class fields: we have both a Galois representation $\mathrm{Gal}(H_{\mathcal{O}}(E_{\mathrm{tors}})/H_{\mathcal{O}})) \hookrightarrow \widehat{\mathcal{O}}^\times$ and the Artin isomorphism $\mathrm{Gal}(K^{\mathrm{ab}}/H_{\mathcal{O}}) \cong \widehat{\mathcal{O}}^\times/\mathcal{O}^\times$ appearing in Theorem 3.3.6. The relation between these two maps is given by the following theorem, which generalizes Theorem 3.2.1.

Theorem 3.4.2. *Let $\mathcal{O}$ be an order in the imaginary quadratic field K, with corresponding ring class field $H_{\mathcal{O}}$, and let $E_{/H_{\mathcal{O}}}$ be an elliptic curve with complex multiplication by $\mathcal{O}$. Denote by $1/[\cdot, K]$ the reciprocal of the Artin map $[\cdot, K] : \mathbb{A}_K^\times/K^\times \to \mathrm{Gal}(K^{ab}/K)$. Then the following diagram*

$$\begin{tikzcd}
\mathrm{Gal}(H_{\mathcal{O}}(E_{tors})/H_{\mathcal{O}}) \arrow[r, two heads] \arrow[d, hook, "\rho_E"'] & \mathrm{Gal}(K^{ab}/H_{\mathcal{O}}) \\
\widehat{\mathcal{O}}^\times \arrow[r, two heads] & \widehat{\mathcal{O}}^\times/\mathcal{O}^\times \arrow[u, "1/[\cdot,K]"']
\end{tikzcd}$$

commutes.

The proof of Theorem 3.4.2 relies on the so-called *Main Theorem of Complex Multiplication*, which we recall here for the reader's convenience.

Theorem 3.4.3. *Let $F \subseteq \mathbb{C}$ be a number field, $E_{/F}$ be an elliptic curve such that $\mathrm{End}_F(E) \cong \mathcal{O}$ for some order $\mathcal{O}$ inside an imaginary quadratic field $K \subseteq F$. Then there exists a unique group homomorphism $\alpha = \alpha_{E/F} : \mathbb{A}_F^\times \to K^\times \subseteq \mathbb{C}^\times$ such that for every lattice $\Lambda \subseteq K \subseteq \mathbb{C}$, for every analytic isomorphism $\xi : \mathbb{C}/\Lambda \to E(\mathbb{C})$ and for every $s \in \mathbb{A}_F^\times$ we have $(\alpha(s) \cdot \mathrm{N}_{F/K}(s)^{-1})\Lambda = \Lambda$ and the following diagram*

$$\begin{tikzcd}
K/\Lambda \arrow[r, "\alpha(s) \cdot \mathrm{N}_{F/K}(s)^{-1} \cdot"] \arrow[d, "\xi"'] & K/\Lambda \arrow[d, "\xi"] \\
E(F^{ab}) \arrow[r, "{[s,F]}"'] & E(F^{ab})
\end{tikzcd}$$

commutes.

Proof. See [Lan87, Chapter 10, Theorem 8]. □

Proof of Theorem 3.4.2. Consider the diagram

$$\begin{tikzcd}
\mathbb{A}^\times_{H_\mathcal{O}} \arrow[r, two heads, "{[\cdot,H_\mathcal{O}]}"] \arrow[dr, "(\alpha(\cdot)N_{H_\mathcal{O}/K}(\cdot)^{-1})_{\mathrm{fin}}"'] & \mathrm{Gal}(H_\mathcal{O}(E_{\mathrm{tors}})/H_\mathcal{O}) \arrow[d, hook, "\rho_E"] \\
 & \widehat{\mathcal{O}}^\times
\end{tikzcd} \tag{3.21}$$

where $\alpha : \mathbb{A}^\times_{H_\mathcal{O}} \to K^\times$ is the homomorphism appearing in Theorem 3.4.3, the horizontal map is, with a slight abuse of notation, the composition of the Artin map with the natural restriction $\mathrm{Gal}(H^{\mathrm{ab}}_\mathcal{O}/H_\mathcal{O}) \to \mathrm{Gal}(H_\mathcal{O}(E_{\mathrm{tors}})/H_\mathcal{O})$, and the subscript $(\cdot)_{\mathrm{fin}}$ appearing in front of an idéle denotes its finite part. We claim the following two facts concerning diagram (3.21):

- The diagonal arrow is well defined *i.e.* for every $s \in \mathbb{A}^\times_{H_\mathcal{O}}$ we have $(\alpha(s)N_{H_\mathcal{O}/K}(s)^{-1})_{\mathrm{fin}} \in \widehat{\mathcal{O}}^\times$. To see this, suppose we have an embedding $H_\mathcal{O} \subseteq \mathbb{C}$ and choose an invertible ideal $\mathfrak{a} \subseteq \mathcal{O}$ for which there exists a complex analytic isomorphism $\xi : \mathbb{C}/\mathfrak{a} \to E(\mathbb{C})$. Then Theorem 3.4.3 ensures that $(\alpha(s)N_{H_\mathcal{O}/K}(s)^{-1}) \cdot \mathfrak{a} = \mathfrak{a}$ for every $s \in \mathbb{A}^\times_{H_\mathcal{O}}$. Since $\mathfrak{a}$ is invertible, this easily implies (as we have already seen in the proof of Theorem 3.4.1) that $(\alpha(s)N_{H_\mathcal{O}/K}(s)^{-1}) \cdot \mathcal{O} = \mathcal{O}$ so that $(\alpha(s)N_{H_\mathcal{O}/K}(s)^{-1})_p \in \mathcal{O}_p^\times$ for all p primes. This proves the first claim;

- Diagram (3.21) commutes. This immediately follows from Theorem 3.4.3, which says that the $\mathcal{O}$-module automorphism induced by $[s, H_\mathcal{O}]$ on torsion points of E corresponds to multiplication by $\alpha(s)N_{H_\mathcal{O}/K}(s)^{-1}$ on $K/\mathfrak{a}$.

The proof can now be concluded essentially by looking at the diagram

$$\begin{tikzcd}
\mathbb{A}^\times_{H_\mathcal{O}} \arrow[r, two heads, "{[\cdot,H_\mathcal{O}]}"] \arrow[dr, "(\alpha(\cdot)N_{H_\mathcal{O}/K}(\cdot)^{-1})_{\mathrm{fin}}"'] & \mathrm{Gal}(H_\mathcal{O}(E_{\mathrm{tors}})/H_\mathcal{O}) \arrow[r] \arrow[d, hook, "\rho_E"'] & \mathrm{Gal}(K^{\mathrm{ab}}/H_\mathcal{O}) \\
 & \widehat{\mathcal{O}}^\times \arrow[r, two heads] & \widehat{\mathcal{O}}^\times/\mathcal{O}^\times \arrow[u, "{1/[\cdot,K]}"']
\end{tikzcd}$$

which can easily be shown to commute (the left triangular part already does by the above discussion). Indeed, let $\sigma \in \mathrm{Gal}(H_\mathcal{O}(E_{\mathrm{tors}})/H_\mathcal{O})$ and let $s \in \mathbb{A}^\times_{H_\mathcal{O}}$ be such that $[s, H_\mathcal{O}] = \sigma$. Then by Class Field Theory we have $\sigma\big|_{K^{\mathrm{ab}}} = [N_{H_\mathcal{O}/K}(s), K]$. On the other hand, the commutativity of (3.21) shows that $\rho_E(\sigma) = (\alpha(s)N_{H_\mathcal{O}/K}(s)^{-1})_{\mathrm{fin}}$ and by the properties of the Artin map we have

$$[(\alpha(s)N_{H_\mathcal{O}/K}(s)^{-1})_{\mathrm{fin}} \bmod \mathcal{O}^\times, K] = [\alpha(s)N_{H_\mathcal{O}/K}(s)^{-1}, K] = [N_{H_\mathcal{O}/K}(s)^{-1}, K]$$

where the last equality follows from the fact that $\alpha(s) \in K^\times$. Since the Artin map is a group homomorphism, this concludes the proof. □

3.5 A formula for the index of a CM Galois representation

Let F be a number field with absolute Galois group $G_F := \mathrm{Gal}(\overline{F}/F)$ and let $E_{/F}$ be an elliptic curve with complex multiplication by an order $\mathcal{O}$ in an imaginary quadratic field K. Set

$$\mathcal{G}(E/F) := \begin{cases} \mathrm{Aut}_{\mathcal{O}}(E_{\mathrm{tors}}) & \text{if } K \subseteq F, \\ \mathcal{N}_\infty(E) & \text{if } K \nsubseteq F \end{cases}$$

where $\mathcal{N}_\infty(E)$ is defined as in (3.5). We have seen in Section 3.1 that the image of the Galois representation $\rho_E : G_F \longrightarrow \mathrm{Aut}_{\mathbb{Z}}(E_{\mathrm{tors}})$ described in (3.1) is not open in $\mathrm{Aut}_{\mathbb{Z}}(E_{\mathrm{tors}})$, as we always have the containment $\rho_E(G_F) \subseteq \mathcal{G}(E/F)$. On the other hand, Theorem 3.1.2 asserts that if $K \subseteq F$ then $\rho_E(G_F)$ is open in $\mathcal{G}(E/F)$. Since $\mathrm{Aut}_{\mathcal{O}}(E_{\mathrm{tors}}) \cong \widehat{\mathcal{O}}^\times$ is profinite, we deduce that the index $|\mathcal{G}(E/F) : \rho_E(G_F)|$ is finite in this case. A similar result holds in the case F does not contain the CM field.

Proposition 3.5.1. *Let $E_{/F}$ be an elliptic curve with complex multiplication by an order $\mathcal{O}$ in an imaginary quadratic field K, and assume that F is a number field not containing K. Then the following holds:*

1. *The group $\mathcal{N}_\infty(E)$ is profinite and $\rho_E(G_F)$ is open (in particular of finite index) in it;*
2. *If $E' := E_{FK}$ denotes the base-change of E to the compositum FK, then*

$$|\mathcal{N}_\infty(E) : \rho_E(G_F)| = \left|\mathrm{Aut}_{\mathcal{O}}(E'_{tors}) : \rho_{E'}(G_{FK})\right|.$$

Proof. To prove that $\mathcal{N}_\infty(E)$ is a profinite group, note first of all that $\mathrm{Aut}_{\mathcal{O}}(E_{\mathrm{tors}})$ is closed inside $\mathrm{Aut}_{\mathbb{Z}}(E_{\mathrm{tors}})$ because

$$\mathrm{Aut}_{\mathcal{O}}(E_{\mathrm{tors}}) = \bigcap_{n \in \mathbb{N}} \mathrm{res}_n^{-1}(\mathrm{Aut}_{\mathcal{O}}(E[n]))$$

where $\mathrm{res}_n : \mathrm{Aut}_{\mathbb{Z}}(E_{\mathrm{tors}}) \longrightarrow \mathrm{Aut}_{\mathbb{Z}}(E[n])$ denotes the natural restriction map. Since we have $|\mathcal{N}_\infty(E) : \mathrm{Aut}_{\mathcal{O}}(E_{\mathrm{tors}})| = 2$, the group $\mathcal{N}_\infty(E)$ is the union of two closed subsets, hence it is itself closed. As $\mathrm{Aut}_{\mathbb{Z}}(E_{\mathrm{tors}})$ is a profinite group, this proves that also $\mathcal{N}_\infty(E)$ is profinite.

Now, $\mathrm{Aut}_{\mathcal{O}}(E_{\mathrm{tors}})$ is closed and of finite index in $\mathcal{N}_\infty(E)$, so it is also open in the same group. Moreover by Theorem 3.1.2 the inclusion $\rho_{E'}(G_{FK}) \subseteq \mathrm{Aut}_{\mathcal{O}}(E'_{\mathrm{tors}})$ is open and clearly $\rho_{E'}(G_{FK}) = \rho_E(G_{FK})$ and $\mathrm{Aut}_{\mathcal{O}}(E'_{\mathrm{tors}}) = \mathrm{Aut}_{\mathcal{O}}(E_{\mathrm{tors}})$. Thus we see that $\rho_E(G_{FK})$ is an open subgroup of $\rho_E(G_F)$ and we conclude that the latter is open in $\mathcal{N}_\infty(E)$.

We finally turn to the proof of (2). By [BCS17, Lemma 3.15] (that will be reproved in Theorem 5.6.2 of this thesis) we know that $FK \subseteq F(E_{\mathrm{tors}})$. Since ρ_E induces an injective Galois representation $\mathrm{Gal}(F(E_{\mathrm{tors}})/F) \hookrightarrow \mathcal{N}_\infty(E)$, we have $|\rho_E(G_F) : \rho_E(G_{FK})| = 2$. Now the index computation

$$|\mathcal{N}_\infty(E) : \rho_E(G_F)| = \frac{1}{2}\,|\mathcal{N}_\infty(E) : \rho_E(G_{FK})| = |\mathrm{Aut}_{\mathcal{O}}(E_{\mathrm{tors}}) : \rho_E(G_{FK})|$$

allows to conclude. □

For a generic non-CM elliptic curve E defined over a number field F, computing the index $|\mathrm{Aut}_{\mathbb{Z}}(E_{\mathrm{tors}}) : \rho_E(G_F)|$ is a difficult problem that nowadays constitutes an active area of research.

On the other hand, the corresponding problem for CM elliptic curves is much easier, and one can even obtain a closed formula for the index $|\mathcal{G}(E/F) : \rho_E(G_F)|$.

Theorem 3.5.2. *Let F be a number field and let $E_{/F}$ be an elliptic curve with complex multiplication by an order $\mathcal{O}$ in an imaginary quadratic field K. Then we have*

$$|\mathcal{G}(E/F) : \rho_E(G_F)| = [(FK) \cap K^{ab} \colon H_{\mathcal{O}}] \cdot \frac{|\mathcal{O}^\times|}{[F(E_{tors}) : (FK^{ab})]} \tag{3.22}$$

where K^{ab} denotes the maximal abelian extension of K and $H_{\mathcal{O}} \subseteq K^{ab}$ is the ring class field of K relative to the order $\mathcal{O}$.

Remark 3.5.3. We remark that formula (3.22) makes sense: the first factor appearing on the right hand side is well defined because $H_{\mathcal{O}}$ is always contained in FK by Theorem 1.3.4, and we will show in the course of the proof that the second factor is actually an integer.

Proof. By Proposition 3.5.1 we can assume without loss of generality that $K \subseteq F$. The exact same proof of Theorem 3.4.2 shows that the diagram

$$\begin{tikzcd}
\mathrm{Gal}(F(E_{\mathrm{tors}})/F) \arrow[r, two heads] \arrow[d, hook, "\rho_E"'] & \mathrm{Gal}(FK^{\mathrm{ab}}/F) \arrow[r, two heads] & \mathrm{Gal}(K^{\mathrm{ab}}/F \cap K^{\mathrm{ab}}) \arrow[d, hook] \\
\mathrm{Aut}_{\mathcal{O}}(E_{\mathrm{tors}}) \cong \widehat{\mathcal{O}}^\times \arrow[r, two heads] & \widehat{\mathcal{O}}^\times/\mathcal{O}^\times \arrow[r, "1/{[\cdot,K]}"] & \mathrm{Gal}(K^{\mathrm{ab}}/H_{\mathcal{O}})
\end{tikzcd} \tag{3.23}$$

commutes, where $1/[\cdot, K]$ denotes again the isomorphism given by the reciprocal of the Artin map and the upper horizontal morphisms are the natural restrictions. Let $\psi_E : \mathrm{Aut}_{\mathcal{O}}(E_{\mathrm{tors}}) \to \mathrm{Gal}(K^{\mathrm{ab}}/H_{\mathcal{O}})$ be the surjection obtained by composing the maps appearing in the lower horizontal line of diagram (3.23). Then we obtain an induced commutative diagram

$$\begin{tikzcd}
1 \arrow[r] & \mathrm{Gal}(F(E_{\mathrm{tors}})/F \cdot K^{\mathrm{ab}}) \arrow[r] \arrow[d, hook, dashed, "\iota'"] & \mathrm{Gal}(F(E_{\mathrm{tors}})/F) \arrow[r] \arrow[d, hook, "\rho_E"] \arrow[dr, phantom, "(3.23)"] & \mathrm{Gal}(K^{\mathrm{ab}}/F \cap K^{\mathrm{ab}}) \arrow[r] \arrow[d, hook, "\iota"] & 1 \\
1 \arrow[r] & \mathrm{Aut}_F(E) \arrow[r] & \mathrm{Aut}_{\mathcal{O}}(E_{\mathrm{tors}}) \arrow[r, "\psi_E"'] & \mathrm{Gal}(K^{\mathrm{ab}}/H_{\mathcal{O}}) \arrow[r] & 1
\end{tikzcd}$$

whose rows are exact. This shows in particular that the degree of the extension $F \cdot K^{\mathrm{ab}} \subseteq F(E_{\mathrm{tors}})$ is finite and divides $|\mathrm{Aut}_F(E)| = |\mathcal{O}^\times|$. Moreover, the snake lemma gives:

$$|\mathcal{G}(E/F) : \rho_E(G_F)| = |\mathrm{coker}(\rho_E)| = |\mathrm{coker}(\iota)| \cdot |\mathrm{coker}(\iota')| = [F \cap K^{\mathrm{ab}} \colon H_{\mathcal{O}}] \cdot \frac{|\mathcal{O}^\times|}{[F(E_{\mathrm{tors}}) : F \cdot K^{\mathrm{ab}}]}$$

which allows us to conclude. □

Corollary 3.5.4. *Let $\mathcal{O}$ be an order in an imaginary quadratic field K with corresponding ring class field $H_{\mathcal{O}}$. Then for an elliptic curve $E_{/H_{\mathcal{O}}}$ with complex multiplication by $\mathcal{O}$ we have:*

$$\left|\mathrm{Aut}_{\mathcal{O}}(E_{tors}) : \rho_E(G_{H_{\mathcal{O}}})\right| = \begin{cases} 1 & \text{if } H_{\mathcal{O}}(E_{tors}) \neq K^{ab} \\ |\mathcal{O}^\times| & \text{otherwise.} \end{cases}$$

Proof. If $j(E) \neq 0, 1728$ then $\mathcal{O}^\times = \{\pm 1\}$ and we conclude using Theorem 3.5.2. If instead $j(E) = 0$ or $j(E) = 1728$ then $H_\mathcal{O} = K$. In particular, we always have $H_\mathcal{O}(E_{\text{tors}}) = K^{\text{ab}}$ and using again Theorem 3.5.2 the result follows. □

Hence, for all CM elliptic curves $E_{/\mathbb{Q}}$ the above corollary and Proposition 3.5.1 imply that we always have $\left|\mathcal{G}(E/\mathbb{Q}) : \rho_E(G_\mathbb{Q})\right| = |\mathcal{O}^\times|$. This improves [Loz19, Theorem 1.3], whose proof is bounded to appear in a follow-up paper. We will see in Theorem 4.4.6 that there exists an infinite family of imaginary quadratic orders $\mathcal{O}$ for which every elliptic curve $E_{/H_\mathcal{O}}$ with complex multiplication by $\mathcal{O}$ satisfies $\left|\mathcal{G}(E/H_\mathcal{O}) : \rho_E(G_{H_\mathcal{O}})\right| = 1$.

4 Entanglement problems for division fields of CM elliptic curves

This chapter constitutes a natural continuation of the previous Chapter 3. The starting point of the whole discussion is the Galois representation (3.1)

$$\rho_E : \mathrm{Gal}(F(E_{\mathrm{tors}})/F) \hookrightarrow \mathrm{Aut}_{\mathbb{Z}}(E_{\mathrm{tors}}) \cong \mathrm{GL}_2(\widehat{\mathbb{Z}})$$

associated to an elliptic curve E defined over a number field F. As we have already explained in Section 3.1, if E does not have complex multiplication then Serre's Open Image Theorem [Ser71, Théorème 3] implies that the image of ρ_E has finite index in $\mathrm{GL}_2(\widehat{\mathbb{Z}})$. However, explicitly describing this image is a non-trivial problem in general which is connected to the celebrated Uniformity Conjecture [Ser71, § 4.3]. A first step in this direction is to study the *entanglement* in the family $\{F(E[p^\infty])\}_p$ for p prime, *i.e.* to describe the image of the natural inclusion

$$\mathrm{Gal}(F(E_{\mathrm{tors}})/F) \hookrightarrow \prod_p \mathrm{Gal}(F(E[p^\infty])/F) \tag{4.1}$$

where the product runs over all primes $p \in \mathbb{N}$. This problem can be very difficult in general, and in recent years much effort has been done to understand the possible entanglement situations that can occur for elliptic curves defined over $\mathbb{Q}$. In this chapter we study the map (4.1) in the case E has complex multiplication and F contains the corresponding CM field. If $j(E) \notin \{0, 1728\}$ and $F = H_{\mathcal{O}}$ is the ring class field relative to the CM order $\mathcal{O}$, the results in Chapter 3 imply that the entanglement in the family of p^∞-division fields of E can be at most *quadratic*, meaning that the image of (4.1) has index at most 2 in its codomain. When and for what reasons is this index exactly equal to 2? Do CM elliptic curves with entangled division fields satisfy special properties? These are just some of the questions over which we want to shed some light. Having to deal with quadratic entanglement makes the study easier than the general case, but this does not prevent to come across some surprises. For instance, we will see in Theorem 4.4.6 that if an elliptic curve E has complex multiplication by an order $\mathcal{O} \subseteq \mathbb{Q}(i)$ of conductor divisible only by primes $p \equiv 1 \bmod 4$ and is defined over the corresponding ring class field $H_{\mathcal{O}}$ then the family of p^∞-division fields $\{H_{\mathcal{O}}(E[p^\infty])\}_p$ is always linearly disjoint over $H_{\mathcal{O}}$ (see Definition 4.1.1).

We begin by shortly contextualizing the entanglement problem in Section 4.1, where we provide some recent references on the topic. In Section 4.2 we introduce the concept of *formal group law* attached to an elliptic curve. The properties of the formal group laws attached to elliptic curves with complex multiplication play a crucial role in Section 4.3, where we study the first ramification and entanglement properties of the family of p^∞-division fields of a CM elliptic curve. In Section 4.4 we restrict our attention to elliptic curves with complex multiplication defined over the ring class field relative to their endomorphism order and we investigate when division fields are *minimal* *i.e.* when they are equal to the corresponding x-coordinate field.

This investigation has many important consequences for the entanglement problem. Finally, in Section 4.5 we classify all the possible entanglement scenarios that can occur for elliptic curves $E_{/\mathbb{Q}}$ that have complex multiplication by orders of discriminant $\Delta < -4$ and that are base-changed to their CM field.

4.1 Entanglement problems for division fields of elliptic curves

Definition 4.1.1. *Let F be a field and let $\mathcal{F} = \{F_n\}_{n \in X}$ a family of Galois extensions of F inside an algebraic closure of F. We call $\mathcal{F}$ linearly disjoint over F if for the compositum L of the fields F_n, the natural inclusion map*

$$\mathrm{Gal}(L/F) \hookrightarrow \prod_{n \in X} \mathrm{Gal}(F_n/F) \tag{4.2}$$

is an isomorphism. If this is not the case, we call the family $\mathcal{F}$ entangled over K.

A family as in Definition 4.1.1 is linearly disjoint over F if and only if for every individual field $F_n \in \mathcal{F}$, the field F_n and the compositum of the fields F_m with $m \neq n$ are linearly disjoint over F. Note that the fields $F_n \in \mathcal{F}$ are not required to be finite extensions of F.

Example 4.1.2. For $\ell \in \mathbb{N}$ prime denote by

$$\mathbb{Q}(\zeta_{\ell^\infty}) = \bigcup_{k \in \mathbb{N}} \mathbb{Q}(\zeta_{\ell^k}) \subseteq \overline{\mathbb{Q}}$$

the field obtained by adjoining to $\mathbb{Q}$ all the ℓ-power roots of unity, and consider the family $\mathcal{F} = \{\mathbb{Q}(\zeta_{p^\infty})\}_p$ for p prime. Then the family $\mathcal{F}$ is linearly disjoint over $\mathbb{Q}$ since each field $\mathbb{Q}(\zeta_{p^\infty})$ is totally ramified at p and unramified at all primes $\ell \neq p$. Note, however, that the linear disjointness of the family $\mathcal{F}$ is not preserved if we "base-change" it to a number field $F \neq \mathbb{Q}$. For instance, let $L = \mathbb{Q}(\sqrt{-15})$ and consider the family $\mathcal{F}_L = \{L(\zeta_{p^\infty})\}_p$. Since $L(\zeta_3) \subseteq L(\zeta_5)$, we see that the family $\mathcal{F}_L$ is entangled over L.

Let now E be an elliptic curve defined over a number field F, and consider the adelic Galois representation

$$\rho_E : \mathrm{Gal}(F(E_{\mathrm{tors}})/F) \hookrightarrow \mathrm{GL}_2(\widehat{\mathbb{Z}})$$

associated to a fixed basis of the Tate module $T_\infty(E)$, as described in (3.1). A crucial problem, that has been concisely called "Program B" by Mazur [Maz77, pag. 109], consists in classifying the possible images of the morphism ρ_E. Ideally, this program should be realized in two steps: first of all one has to determine, for every prime $p \in \mathbb{N}$, the possible images of the p-adic Galois representation

$$\rho_{E,p} : \mathrm{Gal}(F(E_{\mathrm{tors}})/F) \longrightarrow \mathrm{GL}_2(\mathbb{Z}_p)$$

associated to the Galois action on the group $E[p^\infty]$ of p-power torsion points of E; this is the same map that one would obtain by composing ρ_E with the natural projection $\mathrm{GL}_2(\widehat{\mathbb{Z}}) \twoheadrightarrow \mathrm{GL}_2(\mathbb{Z}_p)$. Secondly, one has to work out all the possible ways in which the various maps $\rho_{E,p}$ can "glue together" to give a single adelic representation ρ_E. Concretely, this means understanding the entanglement in the family of division fields $\mathcal{F}_E = \{F(E[p^\infty])\}_p$ for $p \in \mathbb{N}$ prime, and this can be thought of as a generalization of Example 4.1.2, where the multiplicative group $\mathbb{G}_{m,F}$ is replaced by the elliptic curve $E_{/F}$. However, already for $F = \mathbb{Q}$, the situation is far more complicated than its cyclotomic analogue.

Suppose that $E_{/\mathbb{Q}}$ is an elliptic curve given by a short Weierstrass model

$$E : y^2 = x^3 + Ax + B, \qquad A, B \in \mathbb{Q}$$

with discriminant $\Delta_E \in \mathbb{Q}^\times$. Then the 2-division field $\mathbb{Q}(E[2])$ is the splitting field of the Weierstrass polynomial $f(x) = x^3 + Ax + B$ and thus it contains $\mathbb{Q}(\sqrt{\Delta_E})$ as a subfield. If the discriminant $\Delta := \operatorname{disc} \mathbb{Q}(\sqrt{\Delta_E})$ is odd, the inclusions $\mathbb{Q}(\sqrt{\Delta_E}) \subseteq \mathbb{Q}(\zeta_{|\Delta|}) \subseteq \mathbb{Q}(E[\Delta])$ show that the family $\mathcal{F}_E$ is entangled over $\mathbb{Q}$. It can be proved [Jon10] that for almost all (in a sense which can be made precise) elliptic curves over the rationals, the image of the map (4.1) has index at most 2 in the codomain. In other words, for almost all elliptic curves $E_{/\mathbb{Q}}$ either the family $\mathcal{F}_E$ is linearly disjoint over $\mathbb{Q}$ or the quadratic intersection between two different division fields is the only source of entanglement. However, this does not apply to *all* elliptic curves over $\mathbb{Q}$. For example, Jones and Brau describe in [BJ16] an infinite family of elliptic curves $E_{/\mathbb{Q}}$ for which $[\mathbb{Q}(E[2]) : \mathbb{Q}] = 6$ and $\mathbb{Q}(E[2]) \subseteq \mathbb{Q}(E[3])$, while more recently Jones and McMurdy [JM20, Theorem 5.7] found an infinite family of elliptic curves $E_{/\mathbb{Q}}$ for which $[\mathbb{Q}(E[2]) : \mathbb{Q}] = 6$ and $\mathbb{Q}(E[2]) \subseteq \mathbb{Q}(E[5])$.

Despite the potentially rich zoological diversity of the various entanglement scenarios suggested by the above discussion, one can try to put some order in the chaos. For instance, for every number field F and for every elliptic curve $E_{/F}$ *without complex multiplication*, Serre's Open Image Theorem implies that the entanglement in the family $\mathcal{F}_E$ is *finite*. This means that there exists a finite set of primes $S_E \subseteq \mathbb{N}$ such that, if $F(E[S_E^\infty])$ denotes the compositum of all the fields $F(E[p^\infty])$ for $p \in S_E$, the family $\{F(E[S_E^\infty])\} \cup \{F(E[p^\infty]\}_{p \notin S_E}$ is linearly disjoint over F. We will make the set S_E explicit in Theorem 5.4.3. On the other hand, if an elliptic curve $E_{/F}$ has complex multiplication, the analogue of this result is false in general (cfr. Theorem 5.6.2). However, the presence of extra endomorphisms in $\operatorname{End}_{\overline{F}}(E)$ makes the entanglement problem easier than the non-CM case, to the point that, at least over $\mathbb{Q}$, one can reach almost complete classification of the possible entanglement scenarios, see Theorem 4.5.2. However, in this chapter we focus primarily on the entanglement problem for CM elliptic curves defined over *general number fields*, and this classification theorem will come only as a byproduct of our investigations.

4.2 Formal groups and elliptic curves

Our declared goal is to study the entanglement in the family of p^∞-division fields of an elliptic curve with complex multiplication. As Example 4.1.2 suggests, the knowledge of the ramification properties of these fields may help to understand also their behaviour in terms of entanglement. Ramification in division fields of elliptic curves turns out to be strictly related to the theory of formal groups. For this reason we dedicate this section to recall some of the main points from that theory (mainly following [Sil09, Chapter IV]) and to deduce some easy but useful results.

4.2.1 Formal groups

Roughly speaking, a formal group is a power series $\mathcal{F} \in R[\![z_1, z_2]\!]$ for which the association $x +_{\mathcal{F}} y := \mathcal{F}(x, y)$ behaves like an abelian group law. Here is the rigorous definition.

Definition 4.2.1. *Let R be a ring. A (one-parameter commutative) formal group $\mathcal{F}$ over R is a power series $F(z_1, z_2) \in R[\![z_1, z_2]\!]$ satisfying the following properties:*

- *$F(z_1, 0) = z_1$ and $F(0, z_2) = z_2$;*
- *$F(F(z_1, z_2), z_3) = F(z_1, F(z_2, z_3))$ (associativity);*

- *$F(z_1, z_2) = F(z_2, z_1)$ (commutativity).*

Given a formal group $\mathcal{F} \in R[\![z_1, z_2]\!]$ we denote the set of endomorphisms of $\mathcal{F}$ by

$$\operatorname{End}_R(\mathcal{F}) := \{f \in tR[\![t]\!] \mid f(x +_{\mathcal{F}} y) = f(x) +_{\mathcal{F}} f(y)\}$$

which is a ring under the operations $(f +_{\mathcal{F}} g)(t) := \mathcal{F}(f(t), g(t))$ and $(g \circ f)(t) := g(f(t))$. We write $\operatorname{Aut}_R(\mathcal{F})$ for the unit group $\operatorname{End}_R(\mathcal{F})^\times$ and we denote by $[\cdot]_{\mathcal{F}}$ the unique ring homomorphism $\mathbb{Z} \to \operatorname{End}_R(\mathcal{F})$. For every $\phi \in \operatorname{End}_R(\mathcal{F})$ one has that $\phi \in \operatorname{Aut}_R(\mathcal{F})$ if and only if $\phi'(0) \in R^\times$ where $\phi'(t) \in R[\![t]\!]$ denotes the formal derivative (see [Sil09, IV, Lemma 2.4]). Moreover, every $\phi \in \operatorname{End}_R(\mathcal{F})$ is uniquely determined by $\phi'(0)$ whenever R is torsion-free as an abelian group. More precisely, there exist two power series $\exp_{\mathcal{F}}, \log_{\mathcal{F}} \in (R \otimes_{\mathbb{Z}} \mathbb{Q})[\![t]\!]$ such that

$$\phi(t) = \exp_{\mathcal{F}}(\phi'(0) \cdot \log_{\mathcal{F}}(t)) \tag{4.3}$$

as explained in [Sil09, IV, § 5].

Let us now recall that if $(R, \mathfrak{m})$ is a complete local ring there is a well defined map

$$\begin{aligned} \mathfrak{m} \times \mathfrak{m} &\xrightarrow{+_{\mathcal{F}}} \mathfrak{m} \\ (x, y) &\mapsto \mathcal{F}(x, y) \end{aligned}$$

endowing the set $\mathfrak{m}$ with the structure of an abelian group, which will be denoted by $\mathcal{F}(\mathfrak{m})$. We will sometimes refer to $\mathcal{F}(\mathfrak{m})$ as the *group of $\mathfrak{m}$-points of $\mathcal{F}$*. Every $\phi \in \operatorname{End}_R(\mathcal{F})$ induces an endomorphism $\phi_{\mathfrak{m}} \colon \mathcal{F}(\mathfrak{m}) \to \mathcal{F}(\mathfrak{m})$, and for every subset $\Phi \subseteq \operatorname{End}_R(\mathcal{F})$ we define the Φ-torsion subgroup $\mathcal{F}(\mathfrak{m})[\Phi] \subseteq \mathcal{F}(\mathfrak{m})$ as

$$\mathcal{F}(\mathfrak{m})[\Phi] := \bigcap_{\phi \in \Phi} \ker(\phi_{\mathfrak{m}}).$$

These Φ-torsion subgroups generalise the usual N-torsion subgroups $\mathcal{F}(\mathfrak{m})[N] \subseteq \mathcal{F}(\mathfrak{m})$ defined for every $N \in \mathbb{Z}$. The following lemma provides some information about the behaviour of $\mathcal{F}(\mathfrak{m})[p^n]$ under finite extensions of local rings with residue characteristic p.

Lemma 4.2.2 (see [Sil09, IV, Exercise 4.6] and [Sil15, Page 15])**.** *Let $R \subseteq S$ be a finite extension of complete discrete valuation rings of characteristic zero with maximal ideals $\mathfrak{m}_R \subseteq \mathfrak{m}_S$ and residue fields $k_R \subseteq k_S$. Let $p := \operatorname{char}(k_R) > 0$ be the residue characteristic of R and S, and suppose that $\mathfrak{m}_R = pR$. Then for every formal group $\mathcal{F} \in R[\![z_1, z_2]\!]$ and every $x \in \mathcal{F}(\mathfrak{m}_S)[p^n] \setminus \mathcal{F}(\mathfrak{m}_S)[p^{n-1}]$ with $n \in \mathbb{Z}_{\geq 1}$ we have that*

$$v_S(x) \leq \frac{v_S(p)}{p^{h(n-1)} \cdot (p^h - 1)}$$

where v_S denotes the normalised valuation on S, and

$$h = \operatorname{ht}(\overline{\mathcal{F}}) := \max\left\{ n \in \mathbb{N} \;\middle|\; [p]_{\overline{\mathcal{F}}} \in k_R[\![t^{p^n}]\!] \right\}$$

is the height of the reduced formal group $\overline{\mathcal{F}} \in k_R[\![z_1, z_2]\!]$.

Proof. Using that $h = \operatorname{ht}(\overline{\mathcal{F}})$ and that $\mathfrak{m}_R = p \cdot R$ we see that there exist $f, g \in R[\![t]\!]$ such that $[p]_{\mathcal{F}} = f(t^{p^h}) + p\,g(t)$. We can assume that $f, g \in t\,R[\![t]\!]$ and $g'(0) = 1$ because $[p]_{\mathcal{F}} \in t\,R[\![t]\!]$ and $[p]'_{\mathcal{F}}(0) = p$. Now fix $x \in \mathcal{F}(\mathfrak{m}_S)[p^n] \setminus \mathcal{F}(\mathfrak{m}_S)[p^{n-1}]$ and proceed by induction on $n \in \mathbb{Z}_{\geq 1}$.

If $n = 1$ then $f(x^{p^h}) + p\,g(x) = [p]_{\mathcal{F}}(x) = 0$, hence $v_S(p) + v_S(g(x)) = v_S(f(x^{p^h}))$. Now $v_S(g(x)) = v_S(x)$ because $g(0) = 0$ and $g'(0) = 1$, and $v_S(f(x^{p^h})) \geq v_S(x^{p^h}) = p^h\, v_S(x)$ because $f(0) = 0$. Hence $v_S(p) \geq (p^h - 1) \cdot v_S(x)$, which is what we wanted to prove.

If $n \geq 2$ we know by induction that

$$\frac{v_S(p)}{p^{h(n-2)} \cdot (p^h - 1)} \geq v_S([p]_{\mathcal{F}}(x)) = v_S(f(x^{p^h}) + p\,g(x)) \geq \min(v_S(x^{p^h}), v_S(px))$$

because $[p]_{\mathcal{F}}(x) \in \mathcal{F}(\mathfrak{m}_S)[p^{n-1}] \setminus \mathcal{F}(\mathfrak{m}_S)[p^{n-2}]$. This implies that $\min(v_S(x^{p^h}), v_S(px)) = v_S(x^{p^h})$. Otherwise we would get the contradiction $v_S(p) \geq p^{h(n-2)} \cdot (p^h - 1) \cdot v_S(px) > v_S(p)$ because $n \geq 2$, $v_S(x) > 0$ and $h \geq 1$. Hence we have that

$$v_S(x) = \frac{v_S(x^{p^h})}{p^h} \leq \frac{v_S(p)}{p^h \cdot (p^{h(n-2)} \cdot (p^h - 1))} = \frac{v_S(p)}{p^{h(n-1)} \cdot (p^h - 1)}$$

which is what we wanted to prove. □

4.2.2 Formal groups and elliptic curves

Given an elliptic curve E defined over a number field F by an integral Weierstrass equation one can construct, following for example [Sil09, Chapter IV], a formal group $\widehat{E} \in \mathcal{O}_F[\![z_1, z_2]\!]$ which can be thought of as the formal counterpart of the addition law on E. The association $E \mapsto \widehat{E}$ is functorial and in particular induces a map

$$\begin{aligned} \mathrm{End}_F(E) &\longrightarrow \mathrm{End}_F(\widehat{E}) \\ \phi &\mapsto \widehat{\phi} \end{aligned} \tag{4.4}$$

between the endomorphism rings of E and $\widehat{E}$. The power series lying in the image of (4.4) have integral coefficients, as proved in the following theorem, due to Streng.

Theorem 4.2.3. *Let E be an elliptic curve defined over a number field F and let $\widehat{E} \in \mathcal{O}_F[\![z_1, z_2]\!]$ be the formal group law associated to a Weierstrass model of E with coefficients $a_1, \ldots, a_6 \in \mathcal{O}_F$. Then for every $\phi \in \mathrm{End}_F(E)$ we have that $\widehat{\phi} \in \mathcal{O}_F[\![t]\!]$.*

Proof. This is [Str08, Theorem 2.9]. □

Example 4.2.4. Let E be the elliptic curve given by the Weierstrass equation $y^2 = x^3 + x$. Then E has complex multiplication by $\mathcal{O} = \mathbb{Z}[i]$, and we take $F = \mathbb{Q}(i)$ as field of definition for the curve. If $[\cdot]_E \colon \mathcal{O} \longrightarrow \mathrm{End}_F(E)$ denotes the normalized isomorphism described in Definition 1.3.7, then we have $[i]_E(x, y) = (-x, iy)$ for all $(x, y) \in E(\overline{F})$. In order to compute the formal group associated to E we operate the change of variables $z = -x/y$ and $w = -1/y$, bringing the point at infinity on E to the origin of the affine plane $\mathbb{A}^2 = \mathbb{A}^2(z, w)$. In these new coordinates we have $E : w = z^3 + zw^2$ and the morphism $[i]_E$ is now given by $(z, w) \mapsto (iz, -iw)$. One can then compute the first few terms of the formal formal group associated to E:

$$\widehat{E}(z_1, z_2) = z_1 + z_2 - 2z_1^4 z_2 - 4z_1^3 z_2^2 - 4z_1^2 z_2^3 - 2z_1 z_2^4 + \ldots$$

To obtain the power series $\widehat{[i]}_E(t) \in \mathrm{End}_F(\widehat{E})$ it suffices to compute the formal expansion of the pull-back $[i]_E^*(z) := z \circ [i]_E$. In this case we simply get $\widehat{[i]}_E(t) = it$, and this explains why every monomial appearing in the power series $\widehat{E}(z_1, z_2)$ has degree congruent to 1 modulo 4. One can perform similar calculations for every $\alpha \in \mathrm{End}_F(E)$. For instance, we have

$$\widehat{[1+i]}_E = \widehat{E}(t, it) = (1+i)t + 2(1+i)t^5 + 6(1+i)t^9 + O(t^{10}).$$

Let now $\mathfrak{P} \subseteq \mathcal{O}_F$ be a prime of F with residue field $k_{\mathfrak{P}}$ and corresponding maximal ideal $\mathfrak{m}_{\mathfrak{P}} \subseteq \mathcal{O}_{F_{\mathfrak{P}}}$, where $F_{\mathfrak{P}}$ denotes the completion of F at $\mathfrak{P}$. Then [Str08, § 2] shows that there is a unique injective group homomorphism $\iota_{\mathfrak{P}} \colon \widehat{E}(\mathfrak{m}_{\mathfrak{P}}) \to E(F_{\mathfrak{P}})$ making the following diagram

$$\begin{tikzcd}
\widehat{E}(\mathfrak{m}_{\mathfrak{P}}) \arrow[r, "\iota_{\mathfrak{P}}"] \arrow[d, "\widehat{\phi}_{\mathfrak{P}}"'] & E(F_{\mathfrak{P}}) \arrow[d, "\phi"] \\
\widehat{E}(\mathfrak{m}_{\mathfrak{P}}) \arrow[r, "\iota_{\mathfrak{P}}"] & E(F_{\mathfrak{P}})
\end{tikzcd} \tag{4.5}$$

commute for every $\phi \in \mathrm{End}_{F_{\mathfrak{P}}}(E)$, where $\widehat{\phi}_{\mathfrak{P}} := (\widehat{\phi})_{\mathfrak{m}_{\mathfrak{P}}}$ (see Section 4.2.1).

Suppose now that E has good reduction at $\mathfrak{P}$. Then [Sil09, VII, Proposition 2.1 and Proposition 2.2] imply that $\iota_{\mathfrak{P}}$ fits in the following exact sequence

$$0 \longrightarrow \widehat{E}(\mathfrak{m}_{\mathfrak{P}}) \xrightarrow{\iota_{\mathfrak{P}}} E(F_{\mathfrak{P}}) \xrightarrow{\pi_{\mathfrak{P}}} \widetilde{E}(k_{\mathfrak{P}}) \longrightarrow 0$$

in which $\widetilde{E}$ denotes the reduction of E modulo $\mathfrak{P}$ and $\pi_{\mathfrak{P}} \colon E(F_{\mathfrak{P}}) \twoheadrightarrow \widetilde{E}(k_{\mathfrak{P}})$ is the canonical projection. Taking torsion and using (4.5) we get a left-exact sequence

$$0 \longrightarrow \widehat{E}(\mathfrak{m}_{\mathfrak{P}})[\widehat{\Phi}] \xrightarrow{\iota_{\mathfrak{P}}} E(F_{\mathfrak{P}})[\Phi] \xrightarrow{\pi_{\mathfrak{P}}} \widetilde{E}(k_{\mathfrak{P}})[\Phi] \tag{4.6}$$

for every ideal $\Phi \subseteq \mathrm{End}_{F_{\mathfrak{P}}}(E)$. Here $E(F_{\mathfrak{P}})[\Phi] \subseteq E(F_{\mathfrak{P}})$ is the Φ-torsion subgroup

$$E(F_{\mathfrak{P}})[\Phi] := \bigcap_{\phi \in \Phi} \ker(\phi)$$

and $\widetilde{E}(k_{\mathfrak{P}})[\Phi]$ is defined analogously, noting that the map $\mathrm{End}_{F_{\mathfrak{P}}}(E) \to \mathrm{End}_{k_{\mathfrak{P}}}(\widetilde{E})$ is injective (see [Sil94, II, Proposition 4.4]). We remark that $\widehat{E}(\mathfrak{m}_{\mathfrak{P}})[\widehat{\Phi}]$ is well defined since $\widehat{\Phi} \subseteq \mathcal{O}_F[\![t]\!]$ by Theorem 4.2.3. Sequence (4.6) will be extensively used in the next section.

4.3 Division fields of CM elliptic curves: ramification and entanglement

In this section we are initially concerned with ramification properties of division fields of CM elliptic curves. This investigation, besides being of independent interest, will also naturally lead to Theorem 4.3.4, a first general result on the entanglement properties of division fields of elliptic curves with complex multiplication which will find its non-CM analogue in Theorem 5.4.3. As a major tool, we will heavily use the theory of formal groups outlined in Section 4.2.

Let $F \subseteq \overline{\mathbb{Q}}$ be a number field and let $E_{/F}$ be an elliptic curve with complex multiplication by an order $\mathcal{O}$ in an imaginary quadratic field K. For our purposes, it is not very restrictive to assume (as we will do in the rest of this chapter) that there is an inclusion $K \subseteq F$. Indeed, if $K \not\subseteq F$, one can prove (see Theorem 5.6.2) that $K \subseteq F(E[N])$ for every $N > 2$. In particular, in this case the

study of the entanglement in the family of p^∞-division fields of $E_{/F}$ is essentially equivalent to the same study for the base-changed elliptic curve E_{KF} (we may possibly miss what happens for the 2-division field, but this situation will be studied in Chapter 5). Note also that, as we already recalled in Section 3.1, the hypothesis $K \subseteq F$ implies that all the geometric endomorphisms of E are actually defined over F.
We will also always fix the normalized isomorphism $[\cdot]_E \colon \mathcal{O} \to \mathrm{End}_{\overline{\mathbb{Q}}}(E)$ appearing in Definition 1.3.7. With this choice, it follows from [Sil09, IV, Corollary 4.3] that $\widehat{[\alpha]}_E'(0) = \alpha$ for every $\alpha \in \mathcal{O}$, where $\widehat{[\alpha]}_E \in \mathrm{End}_{\overline{\mathbb{Q}}}(\widehat{E})$ denotes the endomorphism of the formal group $\widehat{E}$ associated to $[\alpha]_E$ by (4.4).

Our first result consists in finding an explicit finite set of prime ideals outside which the extensions $F \subseteq F(E[I])$, for invertible ideals $I \subseteq \mathcal{O}$, are unramified.

Proposition 4.3.1. *Let F be a number field and $E_{/F}$ an elliptic curve with complex multiplication by an order $\mathcal{O}$ in an imaginary quadratic field $K \subseteq F$. Denote by $\mathfrak{f}_{\mathcal{O}} := |\mathcal{O}_K \colon \mathcal{O}|$ the conductor of the order $\mathcal{O}$ and by $\mathfrak{f}_E \subseteq \mathcal{O}_F$ the conductor ideal of the elliptic curve E. Then for every ideal $I \subseteq \mathcal{O}$ coprime with $\mathfrak{f}_{\mathcal{O}}$ the extension $F \subseteq F(E[I])$ is unramified at all primes not dividing $(I \cdot \mathcal{O}_F) \cdot \mathfrak{f}_E$.*

Proof. Since I is coprime with the conductor of the order $\mathcal{O}$, it can be uniquely factored into a product of invertible prime ideals of $\mathcal{O}$ (see [Cox13, Proposition 7.20]). The field $F(E[I])$ is then the compositum of all the division fields $F(E[\mathfrak{p}^n])$ with $\mathfrak{p}^n$ the prime power factors of I in $\mathcal{O}$. Hence it suffices to prove that for every invertible prime ideal $\mathfrak{p} \subseteq \mathcal{O}$ and $n \in \mathbb{N}$, the field extension $F \subseteq F(E[\mathfrak{p}^n])$ is unramified at every prime of F not dividing $(\mathfrak{p}\,\mathcal{O}_F) \cdot \mathfrak{f}_E$.

Fix an invertible prime $\mathfrak{p} \subseteq \mathcal{O}$ and write $L := F(E[\mathfrak{p}^n])$. Let $\mathfrak{q} \nmid (\mathfrak{p}\,\mathcal{O}_F) \cdot \mathfrak{f}_E$ be a prime of F and fix a prime $\mathfrak{Q} \subseteq \mathcal{O}_L$ lying above $\mathfrak{q}$, with residue field k. Since $\mathfrak{q}$ does not divide the conductor $\mathfrak{f}_E$ of the elliptic curve, E has good reduction $\widetilde{E}$ modulo $\mathfrak{q}$ and we then denote by $\pi \colon E(L) \to \widetilde{E}(k)$ the reduction modulo $\mathfrak{Q}$. Take $\sigma \in I(\mathfrak{Q}/\mathfrak{q})$, where $I(\mathfrak{Q}/\mathfrak{q}) \subseteq \mathrm{Gal}(L/F)$ denotes the inertia subgroup of $\mathfrak{q} \subseteq \mathfrak{Q}$, and fix a torsion point $Q \in E[\mathfrak{p}^n] = E(L)[\mathfrak{p}^n]$. By definition of inertia σ acts trivially on the residue field k, hence

$$\pi(Q^\sigma - Q) = \pi(Q^\sigma) - \pi(Q) = \pi(Q) - \pi(Q) = 0 \tag{4.7}$$

i.e. the point $Q^\sigma - Q$ is in the kernel of the reduction map π. We are going to use the exact sequence (4.6) to show that the only $\mathfrak{p}^n$-torsion point contained in this kernel is 0. To this aim, we embed L in its $\mathfrak{Q}$-adic completion $L_{\mathfrak{Q}}$ with ring of integers $\mathcal{O}_{L_{\mathfrak{Q}}}$ and maximal ideal $\mathfrak{m}_{\mathfrak{Q}}$. Notice that the set $(\mathfrak{p}^n \cap \mathcal{O}) \setminus (\mathfrak{Q} \cap \mathcal{O})$ is non-empty because $\mathfrak{p} \nmid \mathfrak{f}_{\mathcal{O}}$ and $\mathfrak{q} \nmid (\mathfrak{p}\,\mathcal{O}_F)$. Consider then the formal group $\widehat{E} \in \mathcal{O}_F[\![z_1, z_2]\!]$ associated to an integral Weierstrass model of E, and let $\alpha \in (\mathfrak{p}^n \cap \mathcal{O}) \setminus (\mathfrak{Q} \cap \mathcal{O})$. The endomorphism $\widehat{[\alpha]}_E \in \mathrm{End}_F(\widehat{E})$ corresponding to $[\alpha]_E \in \mathrm{End}_F(E)$ via (4.4) becomes an automorphism over $L_{\mathfrak{Q}}$, because $\widehat{[\alpha]}_E'(0) = \alpha \in \mathcal{O}_{L_{\mathfrak{Q}}}^\times$. Hence taking $\Phi = [\mathfrak{p}^n]_E$ in (4.6) shows that $E[\mathfrak{p}^n] \cap \ker(\pi) \subseteq E[\alpha] \cap \ker(\pi) = \{0\}$, where the last equality holds because $\widehat{E}(\mathfrak{m}_{\mathfrak{Q}})\widehat{[\alpha]}_E = 0$. Combining this with (4.7) we see that $Q^\sigma = Q$ for every $Q \in E[\mathfrak{p}^n]$ and $\sigma \in I(\mathfrak{Q}/\mathfrak{q})$. Since L is generated over F by the elements of $E[\mathfrak{p}^n]$, we deduce that the inertia group $I(\mathfrak{Q}/\mathfrak{q})$ is trivial. In particular, $F \subseteq L$ is unramified at every prime not dividing $(\mathfrak{p} \cdot \mathcal{O}_F)\,\mathfrak{f}_E$, as wanted. □

We now turn to the study of the primes which ramify in $F \subseteq F(E[I])$. To do this it suffices to restrict our attention to the case $I = \mathfrak{p}^n$ for some prime $\mathfrak{p} \subseteq \mathcal{O}$ and some $n \in \mathbb{N}$, as we do in the following proposition.

Proposition 4.3.2. *Let F be a number field and $E_{/F}$ an elliptic curve with complex multiplication by an order $\mathcal{O}$ in an imaginary quadratic field $K \subseteq F$. Denote by $B_E := \mathfrak{f}_{\mathcal{O}}\, \Delta_F\, N_{F/\mathbb{Q}}(\mathfrak{f}_E)$ the product of the conductor $\mathfrak{f}_{\mathcal{O}} := |\mathcal{O}_K \colon \mathcal{O}|$ of the order $\mathcal{O}$, the absolute discriminant $\Delta_F \in \mathbb{Z}$ of the number field F and the norm $N_{F/\mathbb{Q}}(\mathfrak{f}_E) := |\mathcal{O}_F/\mathfrak{f}_E|$ of the conductor ideal $\mathfrak{f}_E \subseteq \mathcal{O}_F$. Then for any $n \in \mathbb{N}$ and any prime ideal $\mathfrak{p} \subseteq \mathcal{O}$ coprime with $B_E\,\mathcal{O}$ the extension $F \subseteq F(E[\mathfrak{p}^n])$ is totally ramified at each prime dividing $\mathfrak{p}\,\mathcal{O}_F$. Moreover, the Galois representation*

$$\rho_{E,\mathfrak{p}^n} \colon \operatorname{Gal}(F(E[\mathfrak{p}^n])/F) \hookrightarrow (\mathcal{O}/\mathfrak{p}^n)^\times$$

defined in (3.2) is an isomorphism.

Proof. The statement is trivially true if $n = 0$, hence we assume that $n \geq 1$. Fix $\widehat{E} \in \mathcal{O}_F[\![z_1, z_2]\!]$ to be the formal group associated to an integral Weierstrass model of E, and let $\mathfrak{p} \subseteq \mathcal{O}$ be as in the statement. The hypothesis of coprimality with $B_E\,\mathcal{O}$ implies that $\mathfrak{p}$ is invertible in $\mathcal{O}$ and that it lies above a rational prime $p \in \mathbb{N}$ that is unramified in K. We divide the proof according to the splitting behaviour of p in $\mathcal{O}$, which is the same as the splitting behaviour in K, since $p \nmid \mathfrak{f}_{\mathcal{O}}$.

First, assume that p is inert in K, so that $\mathfrak{p} = p\mathcal{O}$. In this case, $L := F(E[\mathfrak{p}^n])$ coincides with the p^n-division field $F(E[p^n])$. The injectivity of the Galois representation

$$\rho_{E,p^n} \colon \operatorname{Gal}(L/F) \hookrightarrow (\mathcal{O}/p^n\mathcal{O})^\times \cong (\mathcal{O}_K/p^n\mathcal{O}_K)^\times$$

shows that the degree of the extension $F \subseteq L$ is bounded as

$$[L : F] \leq |(\mathcal{O}_K/p^n\mathcal{O}_K)^\times| = p^{2(n-1)}(p^2 - 1).$$

Let $\mathfrak{p} \subseteq \mathcal{O}_L$ be a prime of L lying above p and denote by $L_{\mathfrak{p}}$ the $\mathfrak{p}$-adic completion of L with ring of integers $\mathcal{O}_{L_{\mathfrak{p}}}$, maximal ideal $\mathfrak{m}_{\mathfrak{p}}$ and residue field $k_{\mathfrak{p}}$. We want to determine the ramification index $e(\mathfrak{p}/(\mathfrak{p} \cap \mathcal{O}_F))$.

Since p is inert in K, the reduced elliptic curve $\widetilde{E}$ is supersingular by Theorem 1.4.1, hence $\widetilde{E}(k_{\mathfrak{p}})[p^n] = 0$. Taking $\Phi = [p^n]_E$ in (4.6), we see that the group $\widehat{E}(\mathfrak{m}_{\mathfrak{p}})$ contains a non-zero point of exact order p^n. We can now use Lemma 4.2.2 and the hypothesis $p \nmid \Delta_F$ to get

$$p^{h(n-1)}(p^h - 1) \leq v_{L_{\mathfrak{p}}}(p) = e(\mathfrak{p}/p) = e(\mathfrak{p}/(\mathfrak{p} \cap \mathcal{O}_F)) \leq [L \colon F] \leq p^{2(n-1)}(p^2 - 1). \tag{4.8}$$

where $h \in \mathbb{N}$ denotes the height of the reduction modulo $\mathfrak{P}$ of the formal group $\widehat{E}$. Since the latter is precisely the formal group associated to $\widetilde{E}$, we have that $h = 2$ by [Sil09, V, Theorem 3.1]. Thus all the inequalities appearing in (4.8) are actually equalities, and we see at once that $e(\mathfrak{p}/(\mathfrak{p} \cap \mathcal{O}_F)) = [L \colon F] = p^{2(n-1)}(p^2 - 1)$, which implies that ρ_{E,p^n} is an isomorphism and that $\mathfrak{p} \cap \mathcal{O}_F$ is totally ramified in L. This concludes the proof of the inert case.

Suppose now that p splits in K, so that $p\mathcal{O} = \mathfrak{p}\overline{\mathfrak{p}}$, where $\overline{\mathfrak{p}}$ is the image of $\mathfrak{p}$ under the unique non-trivial automorphism of K. If we put again $L := F(E[\mathfrak{p}^n])$, the injectivity of $\rho_{E,\mathfrak{p}^n}$ gives

$$[L : F] \leq |(\mathcal{O}_K/p^n\mathcal{O}_K)^\times| = p^{n-1}(p - 1).$$

It is convenient in this case to work inside the bigger division field $M := F(E[p^n])$, which contains both L and $L' := F(E[\,\overline{\mathfrak{p}}^n\,])$. We then fix $\mathfrak{p}, \overline{\mathfrak{p}} \subseteq \mathcal{O}_M$ two primes of M lying respectively above $\mathfrak{p}\mathcal{O}_K$ and $\overline{\mathfrak{p}}\mathcal{O}_K$, and we denote by $\mathcal{P} := \mathfrak{p} \cap \mathcal{O}_L$ and $\overline{\mathcal{P}} := \overline{\mathfrak{p}} \cap \mathcal{O}_L$ the corresponding primes in L. For every prime ideal $\mathfrak{q} \in \{\mathfrak{p}, \overline{\mathfrak{p}}\}$ we denote by $M_{\mathfrak{q}}$ the $\mathfrak{q}$-adic completion of M with ring of integers $\mathcal{O}_{M_{\mathfrak{q}}}$ and residue field $k_{\mathfrak{q}}$, and by $\widetilde{E}_{\mathfrak{q}}$ the reduction of $E_{/M}$ modulo $\mathfrak{q}$. We use analogous notation for $\mathcal{P}$ and $\overline{\mathcal{P}}$. The goal is to compute the ramification index $e(\mathcal{P}/\mathcal{P} \cap \mathcal{O}_F)$, and we divide our argument in three steps.

$\boxed{\textbf{Step 1}}$ First of all, we prove that $E(M)[\mathfrak{p}^n] \cap \ker(\pi_{\overline{\mathfrak{P}}}) = 0$, where $\pi_{\overline{\mathfrak{P}}} \colon E(M) \to \widetilde{E}_{\overline{\mathfrak{P}}}(k_{\overline{\mathfrak{P}}})$ denotes the reduction modulo $\overline{\mathfrak{P}}$. Since $E(M)[\mathfrak{p}^n] \subseteq E(L) \subseteq E(L_{\overline{\mathcal{P}}})$, this is equivalent to say that $E(L_{\overline{\mathcal{P}}})[\mathfrak{p}^n] \cap \ker(\pi_{\overline{\mathcal{P}}}) = 0$, where

$$\pi_{\overline{\mathcal{P}}} \colon E(L_{\overline{\mathcal{P}}}) \twoheadrightarrow \widetilde{E}_{\overline{\mathcal{P}}}(k_{\overline{\mathcal{P}}}) \subseteq \widetilde{E}_{\overline{\mathfrak{P}}}(k_{\overline{\mathfrak{p}}})$$

denotes the reduction modulo $\overline{\mathcal{P}}$. Since p is coprime with the conductor of the order $\mathcal{O}$ by assumption, it is possible to find $\alpha \in \mathfrak{p}^n$ such that $\alpha \notin \overline{\mathfrak{p}}$. The endomorphism $\widehat{[\alpha]}_E \in \mathrm{End}_F(\widehat{E})$ corresponding to $[\alpha]_E \in \mathrm{End}_F(E)$ via (4.4) becomes an automorphism over $L_{\overline{\mathcal{P}}}$, because $\widehat{[\alpha]}_E'(0) = \alpha \in \mathcal{O}_{L_{\overline{\mathcal{P}}}}^\times$. Hence taking $\Phi = [\mathfrak{p}^n]_E$ in (4.6) shows that

$$\ker(\pi_{\overline{\mathcal{P}}}) \cap E(L_{\overline{\mathcal{P}}})[\mathfrak{p}^n] \subseteq \ker(\pi_{\overline{\mathcal{P}}}) \cap E(L_{\overline{\mathcal{P}}})[\alpha] = 0$$

where the last equality holds because $\widehat{E}(\mathfrak{m}_{\overline{\mathcal{P}}})\widehat{[\alpha]}_E = 0$. In exactly the same way, using L' in place of L, one shows that $E(M)[\overline{\mathfrak{p}}^n] \cap \ker(\pi_{\mathfrak{P}}) = 0$.

$\boxed{\textbf{Step 2}}$ We now claim that $E(M)[p^n] \cap \ker(\pi_{\mathfrak{p}}) = E(M)[\mathfrak{p}^n]$ where $\pi_{\mathfrak{p}} : E(M) \to \widetilde{E}_{\mathfrak{p}}(k_{\mathfrak{p}})$ denotes the reduction modulo $\mathfrak{p}$. Since $p^n\mathcal{O} = \mathfrak{p}^n\overline{\mathfrak{p}}^n$ with $\mathfrak{p}^n + \overline{\mathfrak{p}}^n = \mathcal{O}$, there is a decomposition of the group $E(M)[p^n]$ into the direct sum of $E(M)[\,\mathfrak{p}^n\,]$ and $E(M)[\,\overline{\mathfrak{p}}^n\,]$, which are cyclic groups of order p^n by Lemma 3.1.1. In particular, there exists $A \in E(M)[\mathfrak{p}^n]$ and $B \in E(M)[\overline{\mathfrak{p}}^n]$ such that every p^n-torsion point $Q \in E(M)[p^n]$ can be written as

$$Q = [a](A) + [b](B)$$

for unique $a, b \in \{0, \dots, p^n - 1\}$. If $\pi_{\mathfrak{p}}(Q) = 0$ then

$$\pi_{\mathfrak{p}}([b](B)) = \pi_{\mathfrak{p}}([-a](A)) \in \widetilde{E}_{\mathfrak{P}}(k_{\mathfrak{p}})[\,\mathfrak{p}^n\,] \cap \widetilde{E}_{\mathfrak{P}}(k_{\mathfrak{p}})[\,\overline{\mathfrak{p}}^n\,] = \{0\}$$

where the last equality follows from the fact that $\mathfrak{p}^n$ and $\overline{\mathfrak{p}}^n$ are coprime in $\mathcal{O}$. In particular, $[b](B) \in \ker(\pi_{\mathfrak{P}}) \cap E(M)[\overline{\mathfrak{p}}^n]$, and the latter is trivial by **Step 1**. Hence we have $Q = [a](A) \in E(M)[\mathfrak{p}^n]$, and this shows the inclusion $\ker(\pi_{\mathfrak{p}}) \cap E(M)[p^n] \subseteq E(M)[\mathfrak{p}^n]$. To prove the other inclusion first notice that the restriction of $\pi_{\mathfrak{p}}$ to $E(M)[p^n]$ gives rise to a surjection

$$E(M)[p^n] \twoheadrightarrow \widetilde{E}_{\mathfrak{P}}(k_{\mathfrak{p}})[p^n]$$

because $E(M)[\overline{\mathfrak{p}}^n] \to \widetilde{E}_{\mathfrak{P}}(k_{\mathfrak{p}})[p^n]$ is injective and the elliptic curve $\widetilde{E}_{\mathfrak{p}}$ is ordinary by Theorem 1.4.1. This gives

$$\frac{E(M)[p^n]}{\ker(\pi_{\mathfrak{p}}) \cap E(M)[p^n]} \cong \widetilde{E}_{\mathfrak{P}}(k_{\mathfrak{p}})[p^n]$$

which in turn shows that

$$|\ker(\pi_{\mathfrak{p}}) \cap E(M)[p^n]| = \frac{|E(M)[p^n]|}{|\widetilde{E}_{\mathfrak{P}}(k_{\mathfrak{p}})[p^n]|} = \frac{p^{2n}}{p^n} = p^n = |E(M)[\mathfrak{p}^n]|.$$

We conclude that $\ker(\pi_{\mathfrak{p}}) \cap E(M)[p^n] = E(M)[\mathfrak{p}^n]$.

$\boxed{\textbf{Step 3}}$ Using (4.6) with $\Phi = [p^n]_E$ and **Step 2**, after recalling that $\mathfrak{p}$ lies over $\mathcal{P}$, one can see that the group $\widehat{E}(\mathfrak{m}_{\mathcal{P}})$ contains a point of exact order p^n. We now apply Lemma 4.2.2 and the hypothesis $p \nmid \Delta_F$ to get

$$p^{h(n-1)}(p^h - 1) \leq v_{L_{\mathcal{P}}}(p) = e(\mathcal{P}/p) = e(\mathcal{P}/(\mathcal{P} \cap \mathcal{O}_F)) \leq [L\colon F] \leq p^{n-1}(p-1). \tag{4.9}$$

where $h \in \mathbb{N}$ denotes the height of the reduction modulo $\mathcal{P}$ of the formal group $\widehat{E}$. Since the latter is precisely the formal group associated to the ordinary elliptic curve $\widetilde{E}_{\mathcal{P}}$, we have that $h = 1$ by [Sil09, V, Theorem 3.1]. Thus all the inequalities appearing in (4.9) are actually equalities, and we see at once that $e(\mathcal{P}/(\mathcal{P} \cap \mathcal{O}_F)) = [L\colon F] = p^{n-1}(p-1)$, which implies that $\rho_{E,\mathfrak{p}^n}$ is an isomorphism and that $\mathcal{P} \cap \mathcal{O}_F$ is totally ramified in L. This concludes the proof. □

Remark 4.3.3. Let $E_{/F}$ be any elliptic curve (not necessarily with complex multiplication) which has good supersingular reduction at a prime $\mathfrak{p} \subseteq \mathcal{O}_F$ lying above a prime $p \in \mathbb{N}$ which does not ramify in $\mathbb{Q} \subseteq F$. Then one can use the same argument provided in the first part of the proof of Proposition 4.3.2 to show that the ramification index $e(\mathfrak{P}/\mathfrak{p})$ is bounded from below by $p^{2(n-1)}(p^2-1)$, where $\mathfrak{P} \subseteq F(E[p^n])$ is any prime lying above $\mathfrak{p}$. This result has already been proved by Lozano-Robledo in [Loz16, Proposition 5.6] and by Smith in [Smi18, Theorem 2.1].

With the above ramification results at our disposal, we can now prove our first main theorem concerning entanglement in division fields of CM elliptic curves.

Theorem 4.3.4. *Let F be a number field and $E_{/F}$ an elliptic curve with complex multiplication by an order $\mathcal{O}$ in an imaginary quadratic field $K \subseteq F$. Denote by $B_E := \mathfrak{f}_{\mathcal{O}}\, \Delta_F\, N_{F/\mathbb{Q}}(\mathfrak{f}_E) \in \mathbb{Z}$ the product of the conductor $\mathfrak{f}_{\mathcal{O}} := |\mathcal{O}_K \colon \mathcal{O}| \in \mathbb{N}$ of the order $\mathcal{O}$, the absolute discriminant $\Delta_F \in \mathbb{Z}$ of the number field F and the absolute norm $N_{F/\mathbb{Q}}(\mathfrak{f}_E) := |\mathcal{O}_F/\mathfrak{f}_E| \in \mathbb{N}$ of the conductor ideal $\mathfrak{f}_E \subseteq \mathcal{O}_F$ of E. Then the map* (4.1) *induces an isomorphism*

$$\mathrm{Gal}(F(E_{tors})/F) \xrightarrow{\sim} \mathrm{Gal}(F(E[S^\infty])/F) \times \prod_{p \notin S} \mathrm{Gal}(F(E[p^\infty])/F) \tag{4.10}$$

for any finite set of primes $S \subseteq \mathbb{N}$ containing the primes dividing B_E.

Proof. The family $\{F(E[p^\infty])\}_{q \notin S} \cup \{F(E[S^\infty])\}$ appearing in the statement of Theorem 4.3.4 is linearly disjoint over F if and only if $F(E[p^n]) \cap F(E[m]) = F$ for every prime $p \notin S$, every $n \in \mathbb{N}$ and every $m \in \mathbb{Z}$ coprime with p. To prove this latter statement, we first show that every non-trivial subextension of $M := F(E[p^n])$ is ramified at some prime dividing p.

When p is inert in K, this follows immediately from Proposition 4.3.2. Suppose then that p is split in K, with $p\mathcal{O}_K = \mathfrak{p}\overline{\mathfrak{p}}$. The division field M is the compositum over F of the extensions $L := F(E[\mathfrak{p}^n])$ and $L' := F(E[\overline{\mathfrak{p}}^n])$. By Proposition 4.3.2 the extension $F \subseteq L$ (respectively $F \subseteq L'$) is totally ramified at every prime of F lying over $\mathfrak{p}$ (resp. $\overline{\mathfrak{p}}$). Let $\mathfrak{p}$ be a prime of F lying above $\mathfrak{p}$, and denote by $I(\mathfrak{p}) \subseteq \mathrm{Gal}(M/F)$ its inertia group and by $e(\mathfrak{p})$ its ramification index in the extension $F \subseteq M$. If $F \subsetneq \widetilde{F}$ is a subextension of $F \subseteq M$ in which $\mathfrak{p}$ does not ramify, then $\widetilde{F}$ must be contained in the inertia field $T = (M)^{I(\mathfrak{p})}$ relative to $\mathfrak{p}$. Notice that the latter also contains L', since by Proposition 4.3.1 the extension $F \subseteq L'$ is unramified at $\mathfrak{p}$. On the other hand, the fact that $F \subseteq L$ is totally ramified at $\mathfrak{p}$ gives the chain of inequalities

$$[L'\colon F] \leq [T\colon F] = \frac{[M\colon F]}{|I(\mathfrak{p})|} = \frac{[M\colon F]}{e(\mathfrak{p})} \leq \frac{[L\colon F] \cdot [L'\colon F]}{e(\mathfrak{p})} \leq [L'\colon F]$$

which shows that $T = L'$. Hence Proposition 4.3.2 implies that any extension $F \subsetneq \widetilde{F}$ which is unramified at every prime above $\mathfrak{p}$ is totally ramified at every prime above $\overline{\mathfrak{p}}$.

Now it is easy to conclude that $M \cap F(E[m]) = F$, since otherwise $F \subsetneq F(E[m])$ would ramify at some prime of F dividing p, contradicting Proposition 4.3.1. □

The description of the set of primes S in Theorem 4.3.4 is actually redundant, since all the primes p dividing the conductor $\mathfrak{f}_{\mathcal{O}}$, with the possible exception of $p = 2$, also divide the absolute discriminant Δ_F of the field of definition of E. This can be seen as follows: since $K \subseteq F$, the field F always contains the field $K(j(E))$, obtained by adjoining to K the j-invariant $j(E)$ of the elliptic curve E. By Theorem 1.3.4 this is precisely the ring class field $H_{\mathcal{O}}$ relative to the CM order $\mathcal{O}$. The initial assertion now follows from the following proposition, which is a weaker form of [Cox13, Exercise 9.20].

Proposition 4.3.5. *Let $\mathcal{O}$ be an order of conductor $\mathfrak{f}_{\mathcal{O}} := |\mathcal{O}_K : \mathcal{O}|$ in an imaginary quadratic field K. Then the extension $\mathbb{Q} \subseteq H_{\mathcal{O}}$ is ramified at all the odd primes dividing $\mathfrak{f}_{\mathcal{O}}$. Moreover if $4 \mid \mathfrak{f}_{\mathcal{O}}$ the same extension is also ramified at 2.*

Proof. If $\mathfrak{f}_{\mathcal{O}} = 1$ there is nothing to prove. Otherwise let $\mathfrak{f}_{\mathcal{O}} = p_1^{a_1} \cdots p_n^{a_n}$ be the prime factorisation of $\mathfrak{f}_{\mathcal{O}}$, and observe that, for every $i \in \{1, \dots, n\}$, one has the chain of inclusions

$$K \subseteq H_{\mathcal{O}_K} \subseteq H_{\mathcal{O}_i} \subseteq H_{\mathcal{O}}$$

given by the *Anordnungsatz* for ring class fields (see Remark 3.3.3), where $\mathcal{O}_i$ denotes the order of conductor $p_i^{a_i}$. Now, the class number formula [Cox13, Theorem 7.24] yields

$$[H_{\mathcal{O}_i} : H_{\mathcal{O}_K}] = \frac{[H_{\mathcal{O}_i} : K]}{[H_{\mathcal{O}_K} : K]} = \frac{h_{\mathcal{O}_i}}{h_K} = \frac{p_i^{a_i}}{|\mathcal{O}_K^\times : \mathcal{O}_i^\times|} \left(1 - \left(\frac{\Delta_K}{p_i}\right) \frac{1}{p_i}\right). \tag{4.11}$$

where $h_{\mathcal{O}_i} := [H_{\mathcal{O}_i} : K] = |\mathrm{Pic}(\mathcal{O}_i)|$ and analogously $h_K := [H_{\mathcal{O}_K} : K] = |\mathrm{Pic}(\mathcal{O}_K)|$. If $p_i \geq 3$ or $p_i = 2$ and $a_i \geq 2$, we see from (4.11) that $H_{\mathcal{O}_i} \neq H_{\mathcal{O}_K}$ except when $p_i = 3$, $a_i = 1$ and $K = \mathbb{Q}(\sqrt{-3})$. In this last case the extension $\mathbb{Q} \subseteq K$ is ramified at $p_i = 3$. Otherwise the extension $H_{\mathcal{O}_K} \subsetneq H_{\mathcal{O}_i}$ is ramified at some prime dividing p_i. Indeed, $H_{\mathcal{O}_K} \subsetneq H_{\mathcal{O}_i}$ is ramified at some prime because $K \subseteq H_{\mathcal{O}_i}$ is abelian and $H_{\mathcal{O}_K}$ is the Hilbert class field of K, and this suffices to conclude because $K \subseteq H_{\mathcal{O}_i}$ can ramify only at primes lying above p_i. □

Remark 4.3.6. If $2 \mid \mathfrak{f}_{\mathcal{O}}$ but $4 \nmid \mathfrak{f}_{\mathcal{O}}$ the extension $\mathbb{Q} \subseteq H_{\mathcal{O}}$ could still be unramified at 2. This happens, for instance, if $\mathfrak{f}_{\mathcal{O}} = 2$ and 2 splits in K, because in this case the ring class field $H_{\mathcal{O}}$ is equal to the Hilbert class field $H_{\mathcal{O}_K}$.

Proposition 4.3.5 shows that the set S in Theorem 4.3.4 could be replaced by the set S' of primes dividing $2 \cdot \Delta_F \cdot \mathrm{N}_{F/\mathbb{Q}}(\mathfrak{f}_E)$, even if this results in a slightly weaker statement. However, choosing the set S' instead of the set S allows to draw a comparison with a result of Lombardo on the image of p-adic Galois representations attached to CM elliptic curves, which is shown in [Lom17, Theorem 6.6]. In this paper Lombardo proves the isomorphism

$$\mathrm{Gal}(F(E[p^\infty])/F) \cong (\mathcal{O} \otimes_{\mathbb{Z}} \mathbb{Z}_p)^\times = \mathcal{O}_p^\times$$

for every prime $p \nmid \Delta_F \cdot \mathrm{N}_{F/\mathbb{Q}}(\mathfrak{f}_E)$. If moreover $p \geq 3$, *i.e.* $p \notin S'$, this isomorphism follows also from Proposition 4.3.2 by taking inverse limits. The methods used in [Lom17] are different from ours and generalise also to higher dimensional abelian varieties.

4.4 Minimality of division fields

We have seen in Proposition 4.3.2 and Theorem 4.3.4 that for every CM elliptic curve E defined over a number field F with $\operatorname{End}_F(E) \cong \mathcal{O}$ for some order $\mathcal{O}$ in an imaginary quadratic field $K \subseteq F$, the division fields $F(E[N])$ are *maximal* for all integers N coprime with a fixed integer $B_E \in \mathbb{Z}$. This is to say that the associated Galois representation $\rho_{E,N}$ given by (3.2) is surjective. When E is defined over the ring class field $H_{\mathcal{O}}$ of K relative to $\mathcal{O}$, the division fields $H_{\mathcal{O}}(E[N])$ always contain the ray class field $H_{N,\mathcal{O}} \subseteq K^{\text{ab}}$, as we have shown in Theorem 3.4.1. If the division field $H_{\mathcal{O}}(E[N])$ is maximal and $N > 2$ then the containment $H_{N,\mathcal{O}} \subsetneq H_{\mathcal{O}}(E[N])$ is strict. In this section we want to study for which integers N the division fields are *minimal*, in the sense that $H_{\mathcal{O}}(E[N]) = H_{N,\mathcal{O}}$. At first glance this investigation may appear completely unrelated to the entanglement problems studied in this chapter. Its importance is nonetheless readily explained: suppose that the family of division fields $\{H_{\mathcal{O}}(E[p^\infty])\}_p$ is entangled over the ring class field. This in particular implies, using Theorem 4.3.4, that there exists a finite set of primes $p_i \in \mathbb{N}$ and a finite set of integers $n_i \in \mathbb{N}$ for $i \in \{1, \dots, k\}$ such that the family $\{H_{\mathcal{O}}(E[p_i^{n_i}])\}_i$ is entangled over $H_{\mathcal{O}}$. Hence the compositum of the fields $H_{\mathcal{O}}(E[p_i^{n_i}])$, *i.e.* the division field $H_{\mathcal{O}}(E[N])$ with $N := \prod_{i=1}^k p_i^{n_i}$, does not have the maximal possible degree over $H_{\mathcal{O}}$. However, if $j(E) \notin \{0, 1728\}$, every division field must contain the corresponding ray class field with index at most 2. Therefore we see that, under the above conditions on $j(E)$, the entanglement in the family $\{H_{\mathcal{O}}(E[p_i^{n_i}])\}_i$ entails the equality $H_{\mathcal{O}}(E[N]) = H_{N,\mathcal{O}}$.

Prompted by this discussion, we begin the section by studying how the maximality of division fields changes upon twisting. Given an elliptic curve E defined over a number field F and an element $\alpha \in F^\times$, we denote by $E^{(\alpha)}$ the *quadratic twist* of E by α, as described in [Sil09, X, § 5]. We recall that two twists $E^{(\alpha)}$ and $E^{(\alpha')}$ are isomorphic over F if and only if α and α' represent the same class in $F^\times/(F^\times)^2$, *i.e.* if and only if $F(\sqrt{\alpha}) = F(\sqrt{\alpha'})$.

Proposition 4.4.1. *Let $\mathcal{O}$ be an order of discriminant $\Delta_{\mathcal{O}} < -4$ in an imaginary quadratic field K, and let $H_{\mathcal{O}}$ be the ring class field of K relative to the order $\mathcal{O}$. Consider an elliptic curve $E_{/H_{\mathcal{O}}}$ with complex multiplication by $\mathcal{O}$ and fix $\alpha \in H_{\mathcal{O}}^\times$. Then for every invertible ideal $I \subseteq \mathcal{O}$ such that $I \cap \mathbb{Z} = N\mathbb{Z}$ with $N > 2$, the surjectivity of the Galois representation $\rho_{E,I}$ defined in* (3.2) *determines the surjectivity of $\rho_{E^{(\alpha)},I}$ as follows:*

$\boxed{1}$ *if $\rho_{E,I}$ is surjective, then $\rho_{E^{(\alpha)},I}$ is surjective if and only if*

$$H_{\mathcal{O}}(E[I]) \neq H_{I,\mathcal{O}}(\sqrt{\alpha})$$

where $H_{I,\mathcal{O}}$ is the ray class field of K modulo I relative to $\mathcal{O}$;

$\boxed{2}$ *if $\rho_{E,I}$ is not surjective, then $\rho_{E^{(\alpha)},I}$ is surjective if and only if $H_{\mathcal{O}}(\sqrt{\alpha}) \neq H_{\mathcal{O}}$ and*

$$H_{\mathcal{O}}(E[I]) \cap H_{\mathcal{O}}(\sqrt{\alpha}) = H_{\mathcal{O}}.$$

Proof. First of all, we claim that $\rho_{E,I}$ (respectively $\rho_{E^{(\alpha)},I}$) has maximal image if and only if there exists $\sigma \in \operatorname{Gal}(\overline{\mathbb{Q}}/H_{\mathcal{O}})$ such that $\rho_{E,I}(\sigma) = -1 \in (\mathcal{O}/I)^\times$ (respectively $\rho_{E^{(\alpha)},I}(\sigma) = -1$). Indeed, $H_{\mathcal{O}}(E[I])$ contains the ray class field $H_{I,\mathcal{O}}$, which is generated over $H_{\mathcal{O}}$ by the values of the Weber function $\mathfrak{h}_E \colon E \twoheadrightarrow E/\operatorname{Aut}(E) \cong \mathbb{P}^1$ at I-torsion points (see Theorem 3.4.1). Since

$\mathfrak{h}_E([\varepsilon](P)) = \mathfrak{h}_E(P)$ for every $P \in E[I]$ and $\varepsilon \in \{\pm 1\} = \mathcal{O}^\times \cong \mathrm{Aut}(E)$, we see that $\rho_{E,I}$ induces the identification

$$\mathrm{Gal}(H_{\mathcal{O}}(E[I])/H_{I,\mathcal{O}}) \cong \mathrm{Im}(\pi_I^\times) \cap \mathrm{Im}(\rho_{E,I}) = \{\pm 1\} \cap \mathrm{Im}(\rho_{E,I}) \subseteq (\mathcal{O}/I)^\times \tag{4.12}$$

where $\pi_I^\times \colon \mathcal{O}^\times \longrightarrow (\mathcal{O}/I)^\times$ denotes the map induced by the quotient $\pi_I \colon \mathcal{O} \twoheadrightarrow \mathcal{O}/I$. Hence $\rho_{E,I}$ is surjective if and only if $-1 \in \mathrm{Im}(\rho_{E,I})$, and the same holds for $\rho_{E^{(\alpha)},I}$. Moreover $\rho_{E^{(\alpha)},I}$ is linked to $\rho_{E,I}$, after choosing compatible generators of $E[I]$ and $E^{(\alpha)}[I]$ as $\mathcal{O}/I$-modules, by the formula

$$\rho_{E^{(\alpha)},I} = \rho_{E,I} \cdot \chi_\alpha \tag{4.13}$$

where $\chi_\alpha \colon \mathrm{Gal}(\overline{\mathbb{Q}}/H_{\mathcal{O}}) \longrightarrow \{\pm 1\} \subseteq (\mathcal{O}/I)^\times$ is the quadratic character associated to $H_{\mathcal{O}}(\sqrt{\alpha})$.

To prove 1 suppose that $\rho_{E,I}$ has maximal image. First, assume that $H_{\mathcal{O}}(E[I]) \neq H_{I,\mathcal{O}}(\sqrt{\alpha})$. Then, either $H_{\mathcal{O}}(\sqrt{\alpha}) \cap H_{\mathcal{O}}(E[I]) = H_{\mathcal{O}}$ or we have $H_{\mathcal{O}}(\sqrt{\alpha}) \subseteq H_{I,\mathcal{O}}$. In the first case, we can certainly find $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/H_{\mathcal{O}})$ acting trivially on $H_{\mathcal{O}}(\sqrt{\alpha})$ and such that $\rho_{E,I}(\sigma) = -1$. Hence we can use (4.13) to see that $\rho_{E^{(\alpha)},I}(\sigma) = \rho_{E,I}(\sigma) \cdot \chi_\alpha(\sigma) = -1$. This implies, by the initial discussion, that $\rho_{E^{(\alpha)},I}$ has maximal image. In the second case, any $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/H_{\mathcal{O}})$ with $\rho_{E,I}(\sigma) = -1$ will act trivially on $H_{I,\mathcal{O}} \supseteq H_{\mathcal{O}}(\sqrt{\alpha})$ by (4.12). As before, we can use (4.13) to conclude that $\rho_{E^{(\alpha)},I}$ has maximal image.

Assume now that $H_{\mathcal{O}}(E[I]) = H_{I,\mathcal{O}}(\sqrt{\alpha})$. This implies that the extensions $H_{\mathcal{O}} \subseteq H_{\mathcal{O}}(\sqrt{\alpha})$ and $H_{\mathcal{O}} \subseteq H_{I,\mathcal{O}}$ are linearly disjoint over $H_{\mathcal{O}}$, because $\rho_{E,I}$ has maximal image. In particular

$$\mathrm{Gal}(H_{\mathcal{O}}(E[I])/H_{\mathcal{O}}) \cong \mathrm{Gal}(H_{I,\mathcal{O}}/H_{\mathcal{O}}) \times \mathrm{Gal}(H_{\mathcal{O}}(\sqrt{\alpha})/H_{\mathcal{O}}).$$

We deduce that any $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/H_{\mathcal{O}})$ with $\rho_{E,I}(\sigma) = -1$, being the identity on $H_{I,\mathcal{O}}$ by (4.12), must act non-trivially on $H_{\mathcal{O}}(\sqrt{\alpha})$. Then (4.13) gives

$$\rho_{E^{(\alpha)},I}(\sigma) = \rho_{E,I}(\sigma) \cdot \chi_\alpha(\sigma) = 1$$

and this suffices to see that $\rho_{E^{(\alpha)},I}$ is non-maximal. This concludes the proof of 1.

The proof of 2 can be carried out in a similar fashion. First of all, notice that the non-maximality of $\rho_{E,I}$ and (4.12) imply that $H_{I,\mathcal{O}} = H_{\mathcal{O}}(E[I])$. Now, by (4.13) the only possibility for $\rho_{E^{(\alpha)},I}$ to be surjective in this case is to find an automorphism $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/H_{\mathcal{O}})$ with $\rho_{E,I}(\sigma) = 1$ and $\chi_\alpha(\sigma) = -1$, which is clearly impossible if $H_{\mathcal{O}}(\sqrt{\alpha}) \subseteq H_{\mathcal{O}}(E[I]) = H_{I,\mathcal{O}}$. On the other hand, if $H_{\mathcal{O}}(E[I]) \cap H_{\mathcal{O}}(\sqrt{\alpha}) = H_{\mathcal{O}}$ one can certainly find $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/H_{\mathcal{O}})$ such that $\chi_\alpha(\sigma) = -1$ and $\rho_{E,I}(\sigma) = 1$, which shows by (4.13) that $\rho_{E^{(\alpha)},I}$ has maximal image. □

In order to apply Proposition 4.4.1 to entanglement questions, it is essential to identify elliptic curves having an infinite family of minimal division fields. A first step in this direction is given by Theorem 4.4.4, which provides a sufficient condition on an elliptic curve E, ensuring the existence of an explicit set of invertible ideals $I \subseteq \mathcal{O}$ for which the corresponding division fields $H_{\mathcal{O}}(E[I])$ are minimal. The proof of this result crucially relies on the subsequent Theorem 4.4.2, which describes the action of complex automorphisms on torsion points of a CM elliptic curve in terms of its analytic parametrisation. The statement of the result involves the global Artin map $[\cdot, F] \colon \mathbb{A}_F^\times \twoheadrightarrow \mathrm{Gal}(F^{\mathrm{ab}}/F)$ and the notion of *Hecke character*. We recall that an Hecke character on a number field F is a continuous group homomorphism

$$\psi \colon \mathbb{A}_F^\times \to \mathbb{C}^\times$$

such that $\psi(F^\times) = 1$. Given a Hecke character ψ we denote by $\mathfrak{f}_\psi \subseteq \mathcal{O}_F$ its conductor, as defined in [Hus04, Chapter 16, Definition 5.7]. For every place $w \in M_F$ we denote by $\psi_w \colon F_w^\times \to \mathbb{C}^\times$ the group homomorphism $\psi_w := \psi \circ \iota_w$, where $\iota_w \colon F_w^\times \hookrightarrow \mathbb{A}_F^\times$ is the natural inclusion. Similarly, for every rational prime $p \in \mathbb{N}$ we denote by $\psi_p \colon F_p^\times \to \mathbb{C}^\times$ the group homomorphism $\psi_p := \psi \circ \iota_p$ where $\iota_p \colon F_p^\times \hookrightarrow \mathbb{A}_F^\times$ is the analogous inclusion induced by the decomposition (3.14).

Theorem 4.4.2. *Let $F \subseteq \mathbb{C}$ be a number field, $E_{/F}$ be an elliptic curve such that $\mathrm{End}_F(E) \cong \mathcal{O}$ for some order $\mathcal{O}$ inside an imaginary quadratic field $K \subseteq F$. Let $K \subseteq M \subseteq F$ be a subfield such that $F(E_{tors}) \subseteq M^{ab} \cdot F$. Then there exist $[M^{ab} \cap F \colon M]$ group homomorphisms $\alpha \colon \mathbb{A}_M^\times \to K^\times \subseteq \mathbb{C}^\times$ such that:*

1. *the map $\varphi \colon \mathbb{A}_M^\times \to \mathbb{C}^\times$ defined as $\varphi(s) := \alpha(s) \cdot \mathrm{N}_{M/K}(s)_\infty^{-1}$ is a Hecke character, where $\mathrm{N}_{M/K} \colon \mathbb{A}_M^\times \to \mathbb{A}_K^\times$ is the idelic norm map;*
2. *for every lattice $\Lambda \subseteq K \subseteq \mathbb{C}$, every analytic isomorphism $\xi \colon \mathbb{C}/\Lambda \to E(\mathbb{C})$ and every $s \in M^\times \cdot \mathrm{N}_{F/M}(\mathbb{A}_F^\times) \subseteq \mathbb{A}_M^\times$ we have that $(\alpha(s) \cdot \mathrm{N}_{M/K}(s)^{-1}) \cdot \Lambda = \Lambda$ and the following diagram*

$$\begin{tikzcd}
K/\Lambda \arrow[r, "(\alpha(s) \cdot \mathrm{N}_{M/K}(s)^{-1}) \cdot"] \arrow[d, "\xi"'] & K/\Lambda \arrow[d, "\xi"] \\
E(M^{ab} \cdot F) \arrow[r, "\tau"'] & E(M^{ab} \cdot F)
\end{tikzcd}$$

commutes, where $\tau \in \mathrm{Gal}(M^{ab} \cdot F/F)$ is the unique automorphism such that $\tau\big|_{M^{ab}} = [s, M]$.

Proof. Combine [Shi94, Proposition 7.40] and [Shi94, Proposition 7.41] when $M = F$ and use [Shi94, Theorem 7.44] for the general case. Notice that, by class field theory, for every $s \in M^\times \cdot \mathrm{N}_{F/M}(\mathbb{A}_F^\times)$ the restriction $[s, M]\big|_{M^{\mathrm{ab}} \cap F}$ is trivial. This gives a unique $\tau \in \mathrm{Gal}(M^{\mathrm{ab}} \cdot F/F)$ such that $\tau\big|_{M^{\mathrm{ab}}} = [s, M]$. Moreover, fixing an embedding $F \subseteq \mathbb{C}$ automatically fixes an embedding $M^{\mathrm{ab}} \cdot F \subseteq \mathbb{C}$, hence $E(M^{\mathrm{ab}} \cdot F) \subseteq E(\mathbb{C})$, which gives a meaning to the vertical arrows in the diagram. □

Remark 4.4.3. If $K \subseteq M \subseteq M' \subseteq F$ and $F(E_{\mathrm{tors}}) \subseteq M^{\mathrm{ab}}$ then $M \subseteq F$ is abelian and Theorem 4.4.2 gives us $[M^{\mathrm{ab}} \cap F \colon M] = [F \colon M]$ Hecke characters $\varphi \colon \mathbb{A}_M^\times \to \mathbb{C}^\times$ and $[(M')^{\mathrm{ab}} \cap F \colon M'] = [F \colon M']$ Hecke characters $\widetilde{\varphi} \colon \mathbb{A}_{M'}^\times \to \mathbb{C}^\times$. We can observe that

$$\frac{[M^{\mathrm{ab}} \cap F \colon M]}{[(M')^{\mathrm{ab}} \cap F \colon M']} = \frac{[F \colon M]}{[F \colon M']} = [M' \colon M] \in \mathbb{N}$$

and that for every Hecke character $\widetilde{\varphi} \colon \mathbb{A}_{M'}^\times \to \mathbb{C}^\times$ given by Theorem 4.4.2 there are exactly $[M' \colon M]$ Hecke characters $\varphi \colon \mathbb{A}_M^\times \to \mathbb{C}^\times$ such that $\widetilde{\varphi} = \varphi \circ \mathrm{N}_{M'/M}$. If $K = M$ and $F = M'$ then we have a unique Hecke character $\widetilde{\varphi} \colon \mathbb{A}_F^\times \to \mathbb{C}^\times$ which coincides with the usual Hecke character associated to elliptic curves with complex multiplication, defined for example in [Sil94, II, § 9] and [Lan87, Chapter 10, Theorem 9].

We can now state Theorem 4.4.4, recalling that for every order $\mathcal{O}$ contained in an imaginary quadratic field K and every ideal $I \subseteq \mathcal{O}$ we denote by $H_{I,\mathcal{O}}$ the ray class field of K modulo I relative to the order $\mathcal{O}$ (see Section 3.3).

Theorem 4.4.4. *Let $F \subseteq \mathbb{C}$ be a number field and let $E_{/F}$ be an elliptic curve such that $\mathrm{End}_F(E) \cong \mathcal{O}$ for some order $\mathcal{O}$ inside an imaginary quadratic field $K \subseteq F$. Suppose that $F(E_{tors}) \subseteq K^{ab}$. Let*

$H := H_{\mathcal{O}}$ the ring class field of $\mathcal{O}$, and fix $\alpha\colon \mathbb{A}_K^\times \to \mathbb{C}^\times$ as in Theorem 4.4.2, with $M = K$. Then we have that $F(E[I]) = F \cdot H_{I,\mathcal{O}}$ for every invertible ideal $I \subseteq \mathcal{O}$ such that $I \subseteq \mathfrak{f}_\varphi \cap \mathcal{O}$, where $\mathfrak{f}_\varphi \subseteq \mathcal{O}_K$ is the conductor of the Hecke character $\varphi\colon \mathbb{A}_K^\times \to \mathbb{C}^\times$ defined by $\varphi(s) := \alpha(s) \cdot s_\infty^{-1}$.

We remark that Theorem 4.4.4 has been proved by Coates and Wiles (see [CW77, Lemma 3]) if $\mathcal{O} = \mathcal{O}_K$ is a maximal order of class number one. Their result has been generalised in the PhD thesis of Kuhman (see [Kuh78, Chapter II, Lemma 3]) to maximal orders $\mathcal{O} = \mathcal{O}_K$, under the hypothesis that $F \subseteq H_{I,\mathcal{O}_K}$.

Proof of Theorem 4.4.4. The containment $H_{I,\mathcal{O}} \subseteq F(E[I])$ is given by Theorem 3.4.1. Observe moreover that $K \subseteq F$ is an abelian extension, since $F \subseteq F(E_{\mathrm{tors}}) \subseteq K^{\mathrm{ab}}$ by assumption. Hence to prove that $F(E[I]) \subseteq F \cdot H_{I,\mathcal{O}}$ it is sufficient to show that every I-torsion point of E is fixed by $[s,K]$, for any $s \in \mathbb{A}_K^\times$ such that $[s,K]|_{H_{I,\mathcal{O}}} = \mathrm{Id}$. Moreover, it suffices to consider only those $s \in \mathbb{A}_K^\times$ such that $s_\infty = 1$ and $s \in U_{I,\mathcal{O}}$, where $U_{I,\mathcal{O}} \leq \mathbb{A}_K^\times$ is the subgroup defined in (3.16). This follows from the fact that $[U_{I,\mathcal{O}}, K] = \mathrm{Gal}(K^{\mathrm{ab}}/H_{I,\mathcal{O}})$ and $K_\infty^\times \subseteq \ker([\cdot,K]) \cap U_{I,\mathcal{O}}$ by Definition 3.3.1 and Lemma 3.3.4.

Fix then $s \in U_{I,\mathcal{O}}$ with $s_\infty = 1$. To study the action of $[s,K]$ on $E[I]$, we fix an invertible ideal $\mathfrak{a} \subseteq \mathcal{O} \subseteq \mathbb{C}$ and a complex uniformisation $\xi\colon \mathbb{C}/\mathfrak{a} \to E(\mathbb{C})$, which exists by [Shi94, Proposition 4.8]. Take a torsion point $P \in E[I]$, and let $z \in (\mathfrak{a} : I)$ be any element such that $\xi(\overline{z}) = P$, where $\overline{z} \in (\mathfrak{a} : I)/\mathfrak{a}$ denotes the image of z in the quotient. Since $s \in K^\times \cdot \mathrm{N}_{H/K}(\mathbb{A}_H^\times)$, we have that

$$P^{[s,K]} = \xi(\overline{z})^{[s,K]} = \xi\left((\alpha(s)\, s^{-1}) \cdot \overline{z}\right)$$

which follows from applying Theorem 4.4.2 with $M = K$. This can be applied because

$$s \in U_{I,\mathcal{O}} \subseteq U_{\mathcal{O}} \subseteq K^\times \cdot U_{\mathcal{O}} = K^\times \cdot \mathrm{N}_{H/K}(\mathbb{A}_H^\times)$$

where the last equality is given by Lemma 3.3.4.

To conclude, it suffices to show that $s^{-1} \cdot \overline{z} = \overline{z}$ and $\alpha(s) = 1$. Notice that $s^{-1} \cdot \mathfrak{a} = \mathfrak{a}$ because $\mathfrak{a} \subseteq \mathcal{O}$ is invertible and $s_p \in \mathcal{O}_p^\times$ for every rational prime $p \in \mathbb{N}$. The equality $s^{-1} \cdot \overline{z} = \overline{z}$ then follows from the fact that, for every prime $p \in \mathbb{N}$, we have $s_p^{-1} z - z \in \mathfrak{a}_p$ because $z \in (\mathfrak{a} : I)$ and $s_p^{-1} \in 1 + I\,\mathcal{O}_p$. To prove the equality $\alpha(s) = 1$, notice that for every prime $p \in \mathbb{N}$ we have

$$1 + I\,\mathcal{O}_p \subseteq \prod_{\substack{w \mid p \\ w \in M_K^0}} (1 + \mathfrak{f}_\varphi\, \mathcal{O}_{K_w})$$

since $I \subseteq \mathfrak{f}_\varphi \cap \mathcal{O}$ by assumption. This implies that $\varphi_p(s_p) = 1$ for every prime $p \in \mathbb{N}$. Indeed $s_p \in 1 + I\,\mathcal{O}_p$ by the definition of $U_{I,\mathcal{O}}$ and for every $w \in M_K^0$ we have that $\varphi_w(1 + \mathfrak{f}_\varphi\, \mathcal{O}_{K_w}) = 1$ because $\mathfrak{f}_\varphi$ is the conductor of φ. Since $s_\infty = 1$ we get that $\alpha(s) = \varphi(s) = 1$, as was to be shown. □

Theorem 4.4.4 has a partial converse, as we show in the following proposition.

Proposition 4.4.5. *Let $\mathcal{O}$ be an order in an imaginary quadratic field K and $F \supseteq K$ be an abelian extension. Let $E_{/F}$ be an elliptic curve with complex multiplication by the order $\mathcal{O}$. Suppose that there exists an invertible ideal $I \subseteq \mathcal{O}$ such that $F(E[I]) \subseteq K^{ab}$ and $I \cap \mathbb{Z} = N\mathbb{Z}$ with $N > 2$ if $j(E) \neq 0$ or $N > 3$ if $j(E) = 0$. Then $F(E_{tors}) = K^{ab}$.*

Proof. It is sufficient to prove that $F(E_{\mathrm{tors}}) \subseteq K^{\mathrm{ab}}$, since the other inclusion follows from the class field theory of imaginary quadratic fields and the fact that $K \subseteq F$ is abelian.

Fix an embedding $K \hookrightarrow \mathbb{C}$ and let $\xi : \mathbb{C}/\Lambda \longrightarrow E(\mathbb{C})$ be a complex parametrization for E, where $\Lambda \subseteq K$ is a lattice. Take $\sigma \in \mathrm{Aut}(\mathbb{C}/K^{\mathrm{ab}})$. By [Shi94, Theorem 5.4] with $s = 1$, there exists a complex parametrization $\xi' : \mathbb{C}/\Lambda \longrightarrow E(\mathbb{C})$ such that the following diagram

$$\begin{tikzcd}
E(\mathbb{C}) \arrow[rr, "\sigma"] & & E(\mathbb{C}) \\
& K/\Lambda \arrow[ul, "\xi"] \arrow[ur, "\xi'"'] &
\end{tikzcd}$$

commutes. This means that σ acts on E_{tors} as an automorphism $\gamma = \xi' \circ \xi^{-1} \in \mathrm{Aut}(E) \cong \mathcal{O}^\times$. In particular, for any point $P \in E[I]$ we have

$$\gamma(P) = \sigma(P) = P \tag{4.14}$$

since by assumption $F(E[I]) \subseteq K^{\mathrm{ab}}$. Notice now that if $j(E) \neq 0, 1728$ we have $\mathrm{Aut}(E) = \{\pm 1\}$ and equality (4.14) can occur for $\gamma = -1$ only when $I \cap \mathbb{Z} = 2\mathbb{Z}$. Similarly, if $j(E) = 1728$ or $j(E) = 0$ one sees that a non-trivial element of $\mathrm{Aut}(E)$ can possibly fix only points of $E[2]$ or points of $E[2] \cup E[3]$, respectively. Our assumptions on I allow then to conclude that γ must be the identity on E.

We have shown that every complex automorphism which fixes the maximal abelian extension of K fixes also the torsion points of E. We conclude that $F(E_{\mathrm{tors}}) \subseteq K^{\mathrm{ab}}$ and this finishes the proof. □

We now want to connect the above discussion to the entanglement problems we are interested in this chapter. More specifically, our goal in the final part of this section is to try to give an answer to the following three questions:

Q1. Let $\mathcal{O}$ be an order in an imaginary quadratic field K with corresponding ring class field $H_\mathcal{O}$ and let j be a singular modulus relative to the order $\mathcal{O}$. Is it true that there are infinitely many elliptic curves $E_{/H_\mathcal{O}}$ with $j(E) = j$ (but non $H_\mathcal{O}$-isomorphic) for which the family $\{H_\mathcal{O}(E[p^\infty])\}_p$ is linearly disjoint over $H_\mathcal{O}$?

Q2. Does the answer to **Q1** change if we further impose the condition that the elliptic curves E must satisfy $H_\mathcal{O}(E_{\mathrm{tors}}) = K^{\mathrm{ab}}$?

Q3. In case of affirmative answer to **Q1** or **Q2**, can the construction of the relevant elliptic curves be made explicit?

As a starting point, it seems natural to ask whether, for a fixed order $\mathcal{O}$ in an imaginary quadratic field K, there exists any elliptic curve E with complex multiplication by $\mathcal{O}$ and defined over the ring class field $H_\mathcal{O}$ with the property that $H_\mathcal{O}(E_{\mathrm{tors}}) = K^{\mathrm{ab}}$. To the best our knowledge, this question was first discussed by Shimura in [Shi94, Page 217] and subsequently studied by various authors, including Shimura himself [Shi71, § 5], Robert [Rob83] and more recently Gurney [Gur, § 4]. One of the main outcomes of these investigations is the following: for every order $\mathcal{O}$ in an imaginary quadratic field $K \neq \mathbb{Q}(i)$, there exists an elliptic curve $E_{/H_\mathcal{O}}$ satisfying $H_\mathcal{O}(E_{\mathrm{tors}}) = K^{\mathrm{ab}}$. Moreover, the same is true for orders $\mathcal{O} \subseteq \mathbb{Q}(i)$ if and only if either $\mathcal{O} = \mathbb{Z}[i]$ or the conductor $\mathfrak{f}_\mathcal{O} := |\mathbb{Z}[i] : \mathcal{O}|$ is divisible by at least one prime $p \not\equiv 1 \bmod 4$. However, none of the available arguments seems to provide a way of finding, when possible, an explicit elliptic curve $E_{/H_\mathcal{O}}$ satisfying the property $H_\mathcal{O}(E_{\mathrm{tors}}) = K^{\mathrm{ab}}$. We therefore decided to give a different proof of the above result, which yields an explicit construction of infinitely many such elliptic curves. As a bonus, in many cases the family of p^∞-division fields associated to these elliptic curves will be linearly disjoint over the ring class field.

Theorem 4.4.6. *Let $\mathcal{O}$ be an order of discriminant $\Delta_\mathcal{O} \in \mathbb{Z}$ inside an imaginary quadratic field K, and let $j \in H_\mathcal{O}$ be the j-invariant of any elliptic curve with complex multiplication by $\mathcal{O}$. Then:*

(a) if $\Delta_\mathcal{O} \neq -4f^2$ for every $f \in \mathbb{Z}_{\geq 2}$ which is only divisible by primes $p \equiv 1 \bmod 4$, there exist infinitely many elliptic curves $E_{/H_\mathcal{O}}$, pairwise non-isomorphic over $H_\mathcal{O}$, with $j(E) = j$ and such that $H_\mathcal{O}(E_{tors}) = K^{ab}$;

(b) if $\Delta_\mathcal{O} = -4f^2$ for some $f \in \mathbb{Z}_{\geq 2}$ which is a product of primes $p \equiv 1 \bmod 4$, then $H_\mathcal{O}(E_{tors}) \neq K^{ab}$ for every elliptic curve $E_{/H_\mathcal{O}}$ with $j(E) = j$.

Proof. We begin by proving (a). When $\mathcal{O}$ has class number 1 the statement is trivially true. We may then assume that $\mathrm{Pic}(\mathcal{O}) \neq \{1\}$, and in particular that $\Delta_\mathcal{O} < -4$. We fix moreover $E_{0/H_\mathcal{O}}$ to be any elliptic curve with $j(E_0) = j$.

Suppose first of all that $K \neq \mathbb{Q}(i)$, where $i^2 = -1$. Let $p \in \mathbb{N}$ be a prime satisfying

$\boxed{1}$ $p \equiv 3 \bmod 4$, *i.e.* p is inert in $\mathbb{Q}(i)$;

$\boxed{2}$ p does not divide $\mathfrak{f}_\mathcal{O} \cdot N_{H_\mathcal{O}/\mathbb{Q}}(\mathfrak{f}_{E_0})$, where $\mathfrak{f}_\mathcal{O} := |\mathcal{O}_K : \mathcal{O}|$ denotes the conductor of the order $\mathcal{O}$ and $\mathfrak{f}_{E_0} \subseteq \mathcal{O}_{H_\mathcal{O}}$ is the conductor ideal of the elliptic curve E_0;

$\boxed{3}$ p splits completely in K.

Since we are assuming that $K \neq \mathbb{Q}(i)$, there are infinitely many such primes by Dirichlet's theorem on primes in arithmetic progression.

Let $\mathfrak{p} \subseteq \mathcal{O}$ be a prime ideal lying over p and note that $\mathfrak{p}$ is invertible by condition $\boxed{2}$. We define a new elliptic curve $E_\mathfrak{p}$ over $H_\mathcal{O}$, as follows. By Proposition 4.3.2 there is an isomorphism

$$\mathrm{Gal}(H_\mathcal{O}(E_0[\mathfrak{p}])/H_\mathcal{O}) \cong (\mathcal{O}/\mathfrak{p}\mathcal{O})^\times \cong \mathbb{F}_p^\times$$

where the last isomorphism follows from the fact that p splits in K. In particular, the group $\mathrm{Gal}(H_\mathcal{O}(E_0[\mathfrak{p}])/H_\mathcal{O})$ is cyclic of order $p-1$, so $H_\mathcal{O} \subseteq H_\mathcal{O}(E_0[\mathfrak{p}])$ contains unique sub-extensions of degree $(p-1)/2$ and of degree 2 over $H_\mathcal{O}$. The first one is necessarily the ray class field $H_{\mathfrak{p},\mathcal{O}}$ (see Theorem 3.4.1), the second one is of the form $H_\mathcal{O}(\sqrt{\alpha})$ for some element $\alpha = \alpha_\mathfrak{p} \in H_\mathcal{O}^\times$. By condition $\boxed{1}$, the integer $p - 1$ is not divisible by 4, hence these two extensions must be linearly disjoint over $H_\mathcal{O}$. We deduce that $H_\mathcal{O}(E_0[\mathfrak{p}]) = H_{\mathfrak{p},\mathcal{O}}(\sqrt{\alpha})$. We set $E_\mathfrak{p} := E_0^{(\alpha)}$, where $E_0^{(\alpha)}$ denotes the twist of E_0 by $\alpha \in H_\mathcal{O}^\times$.

By Proposition 4.4.1, the Galois representation

$$\rho_{E_\mathfrak{p},\mathfrak{p}} : \mathrm{Gal}(H_\mathcal{O}(E_\mathfrak{p}[\mathfrak{p}])/H_\mathcal{O}) \hookrightarrow (\mathcal{O}/\mathfrak{p}\mathcal{O})^\times$$

is not surjective. This in particular implies that $H_\mathcal{O}(E_\mathfrak{p}[\mathfrak{p}]) = H_{\mathfrak{p},\mathcal{O}}$. It follows then from Proposition 4.4.5 that $H_\mathcal{O}((E_\mathfrak{p})_{\text{tors}}) = K^{\text{ab}}$.

We claim that the infinitely many elliptic curves $E_\mathfrak{p}$ with $\mathfrak{p} \subseteq \mathcal{O}$ chosen as above, are pairwise non-isomorphic over $H_\mathcal{O}$. To show this, it suffices to prove that the fields $H_\mathcal{O}(\sqrt{\alpha_\mathfrak{p}})$ associated to the quadratic twists are pairwise distinct. But this follows from Proposition 4.3.1 and Proposition 4.3.2, which show that the extension $H_\mathcal{O} \subseteq H_\mathcal{O}(\sqrt{\alpha_\mathfrak{p}})$ is ramified at all primes of $H_\mathcal{O}$ lying above $\mathfrak{p}$ and unramified at all primes of $H_\mathcal{O}$ which do not divide $\mathfrak{p} \cdot \mathfrak{f}_{E_\mathfrak{p}} \cdot \mathcal{O}_{H_\mathcal{O}}$, because $H_\mathcal{O}(\sqrt{\alpha_\mathfrak{p}}) \subseteq H_\mathcal{O}(E_0[\mathfrak{p}])$.

Suppose now that $K = \mathbb{Q}(i)$. We show first of all how to obtain from E_0 an elliptic curve $E_{1/H_{\mathcal{O}}}$ such that $H_{\mathcal{O}}((E_1)_{\text{tors}}) = \mathbb{Q}(i)^{\text{ab}}$. If there exists an integer $N \in \mathbb{N}$ such that $N > 2$ and $H_{\mathcal{O}}(E_0[N]) = H_{N,\mathcal{O}}$, then Proposition 4.4.5 shows that we can take $E_1 = E_0$. Suppose on the contrary that $H_{\mathcal{O}}(E_0[N]) \neq H_{N,\mathcal{O}}$ for every $N \in \mathbb{Z}_{\geq 3}$, which implies by Lemma 3.1.1 and Theorem 3.4.1 that

$$G_N := \mathrm{Gal}(H_{\mathcal{O}}(E_0[N])/H_{\mathcal{O}}) \cong (\mathcal{O}/N\mathcal{O})^\times$$

for every $N \in \mathbb{Z}_{\geq 3}$. Then we distinguish two cases:

- if the conductor $\mathfrak{f}_{\mathcal{O}} := |\mathbb{Z}[i] \colon \mathcal{O}|$ is even, the isomorphism

  $$\frac{\mathcal{O}}{4\mathcal{O}} \cong \frac{\mathbb{Z}[x]}{(x^2 + \mathfrak{f}_{\mathcal{O}}^2, 4)} \cong \frac{(\mathbb{Z}/4\mathbb{Z})[x]}{(x^2)}$$

  holds. Hence the group G_4 contains a subgroup $Q \subseteq G_4$ of index two, corresponding via the following isomorphism

  $$G_4 \cong \left(\frac{\mathcal{O}}{4\mathcal{O}}\right)^\times \cong \left(\frac{(\mathbb{Z}/4\mathbb{Z})[x]}{(x^2)}\right)^\times \cong \left\{ \begin{pmatrix} a & b \\ 0 & a \end{pmatrix} \middle| \begin{array}{l} a \in (\mathbb{Z}/4\mathbb{Z})^\times \\ b \in \mathbb{Z}/4\mathbb{Z} \end{array} \right\} \subseteq \mathrm{GL}_2(\mathbb{Z}/4\mathbb{Z})$$

  to the group of matrices of the form $\left(\begin{smallmatrix} 1 & b \\ 0 & 1 \end{smallmatrix}\right)$ with $b \in \mathbb{Z}/4\mathbb{Z}$. Therefore the sub-extension of $H_{\mathcal{O}} \subseteq H_{\mathcal{O}}(E_0[4])$ fixed by Q is given by $H_{\mathcal{O}}(\sqrt{\alpha})$ for some $\alpha \in H_{\mathcal{O}}$. Moreover $H_{\mathcal{O}}(\sqrt{\alpha}) \cap H_{4,\mathcal{O}} = H_{\mathcal{O}}$, because Q does not contain the subgroup $\mathrm{Gal}(H_{\mathcal{O}}(E_0[4])/H_{4,\mathcal{O}})$, since the latter corresponds via the previous isomorphism to the group of matrices $\left\{\pm\left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)\right\}$. Hence $H_{\mathcal{O}}(E_0[4]) = H_{4,\mathcal{O}}(\sqrt{\alpha})$, and Proposition 4.4.1 shows that the twisted elliptic curve $E_1 := E_0^{(\alpha)}$ has the property that $H_{\mathcal{O}}(E_1[4]) = H_{4,\mathcal{O}}$. Therefore, Proposition 4.4.5 shows that $H_{\mathcal{O}}((E_1)_{\text{tors}}) = \mathbb{Q}(i)^{\text{ab}}$;

- if $\mathfrak{f}_{\mathcal{O}}$ is odd, our assumptions on $\mathcal{O}$ imply that there exists a prime $p \mid \mathfrak{f}_{\mathcal{O}}$ such that $p \equiv 3 \bmod 4$. Then the group

  $$G_p \cong \left(\frac{\mathcal{O}}{p\mathcal{O}}\right)^\times \cong \left(\frac{\mathbb{F}_p[x]}{(x^2)}\right)^\times \cong \left\{ \begin{pmatrix} a & b \\ 0 & a \end{pmatrix} \middle| \begin{array}{l} a \in \mathbb{F}_p^\times \\ b \in \mathbb{F}_p \end{array} \right\} \subseteq \mathrm{GL}_2(\mathbb{F}_p)$$

  contains a subgroup of index two, corresponding to the group of matrices of the form $\left(\begin{smallmatrix} a^2 & b \\ 0 & a^2 \end{smallmatrix}\right)$ with $a \in \mathbb{F}_p^\times$ and $b \in \mathbb{F}_p$. The sub-extension of $H_{\mathcal{O}} \subseteq H_{\mathcal{O}}(E_0[p])$ fixed by this subgroup is given by $H_{\mathcal{O}}(\sqrt{\alpha})$ for some $\alpha \in H_{\mathcal{O}}$. Moreover $H_{\mathcal{O}}(\sqrt{\alpha}) \cap H_{p,\mathcal{O}} = H_{\mathcal{O}}$, since the degree $[H_{p,\mathcal{O}} \colon H_{\mathcal{O}}] = p(p-1)/2$ is odd. Hence $H_{\mathcal{O}}(E_0[p]) = H_{p,\mathcal{O}}(\sqrt{\alpha})$, and again Proposition 4.4.1 shows that the twisted elliptic curve $E_1 := E_0^{(\alpha)}$ has the property that $H_{\mathcal{O}}(E_1[p]) = H_{p,\mathcal{O}}$. Therefore, Proposition 4.4.5 shows that $H_{\mathcal{O}}((E_1)_{\text{tors}}) = \mathbb{Q}(i)^{\text{ab}}$.

Finally, we construct, by suitably twisting E_1, infinitely many elliptic curves $E_{/H_{\mathcal{O}}}$ which are pairwise non-isomorphic over $H_{\mathcal{O}}$ and share the property that $H_{\mathcal{O}}(E_{\text{tors}}) = \mathbb{Q}(i)^{\text{ab}}$. To do this, fix an integer $m \in \mathbb{Z}_{\geq 3}$ such that $m \mid \Delta_{\mathcal{O}}$ and $H_{\mathcal{O}}(E_1[m]) = H_{m,\mathcal{O}}$, which exists by the previous discussion. Now, observe that for every prime ideal $\mathfrak{p} \subseteq \mathcal{O}$ which is coprime with $\mathrm{N}_{H_{\mathcal{O}}/\mathbb{Q}}(\mathfrak{f}_{E_1}) \cdot \Delta_{\mathcal{O}}$, the Galois group

$$\mathrm{Gal}(H_{\mathfrak{p},\mathcal{O}}/H_{\mathcal{O}}) \cong \frac{(\mathcal{O}/\mathfrak{p})^\times}{\mathcal{O}^\times} \cong \frac{(\mathbb{Z}[i]/\mathfrak{p}\mathbb{Z}[i])^\times}{\{\pm 1\}}$$

is cyclic, and its order is even. Thus the extension $H_{\mathcal{O}} \subseteq H_{\mathfrak{p},\mathcal{O}}$ contains a unique quadratic sub-extension, of the form $H_{\mathcal{O}}(\sqrt{\alpha_{\mathfrak{p}}})$ for some $\alpha_{\mathfrak{p}} \in H_{\mathcal{O}}$. Since $\mathfrak{p}$ is invertible in $\mathcal{O}$, Theorem 3.4.1 shows that $H_{\mathfrak{p},\mathcal{O}} \subseteq H_{\mathcal{O}}(E[\mathfrak{p}])$, and Proposition 4.4.1 shows that the twisted elliptic curve $E_{\mathfrak{p}} := E_1^{(\alpha_{\mathfrak{p}})}$ has the property that $H_{\mathcal{O}}(E_{\mathfrak{p}}[m]) \cap H_{\mathcal{O}}(E_{\mathfrak{p}}[\mathfrak{p}]) = H_{\mathcal{O}}(\sqrt{\alpha_{\mathfrak{p}}})$. Thus $H_{\mathcal{O}}(E_{\mathfrak{p}}[m\mathfrak{p}]) = H_{m\mathfrak{p},\mathcal{O}}$, and Proposition 4.4.5 shows that $H_{\mathcal{O}}((E_{\mathfrak{p}})_{\text{tors}}) = \mathbb{Q}(i)^{\text{ab}}$. To conclude our proof of (a), we observe that the elliptic curves $E_{\mathfrak{p}}$ are pairwise non-isomorphic over $H_{\mathcal{O}}$, by the same argument used in the case $K \neq \mathbb{Q}(i)$.

We now prove (b). Fix a non-maximal order $\mathcal{O} \subseteq \mathbb{Z}[i]$ whose conductor $\mathfrak{f}_{\mathcal{O}} \in \mathbb{Z}_{\geq 2}$ is divided only by primes $p \equiv 1 \bmod 4$. Then $\widehat{\mathcal{O}} = \prod_p (\mathcal{O} \otimes_{\mathbb{Z}} \mathbb{Z}_p) \cong \widehat{\mathbb{Z}}[i]$, because for each prime $p \nmid \mathfrak{f}_{\mathcal{O}}$ one evidently has that $\mathcal{O} \otimes_{\mathbb{Z}} \mathbb{Z}_p \cong \mathbb{Z}_p[i]$, and for each prime $p \mid \mathfrak{f}_{\mathcal{O}}$, since $p \equiv 1 \bmod 4$ by our assumptions, one has that $\mathbb{Z}[i] \subseteq \mathbb{Z}_p$, which shows that $\mathcal{O} \otimes_{\mathbb{Z}} \mathbb{Z}_p \cong \mathbb{Z}_p[i]$ also in this case. In particular, for every $N \in \mathbb{N}$ we have that $-1 \in (\mathcal{O}/N\mathcal{O})^\times$ is a square.

Suppose now by contradiction that there exists an elliptic curve $E_{/H_{\mathcal{O}}}$ such that $H_{\mathcal{O}}(E_{\text{tors}}) = \mathbb{Q}(i)^{\text{ab}}$. Then Theorem 4.4.4 shows that $H_{\mathcal{O}}(E[N]) = H_{N,\mathcal{O}}$ for some integer $N \in \mathbb{Z}_{\geq 3}$. Using the Galois representation $\rho_{E,N}$ defined in (3.2), one gets an embedding

$$\iota \colon \frac{(\mathcal{O}/N\mathcal{O})^\times}{\mathcal{O}^\times} \overset{(\dagger)}{\cong} \operatorname{Gal}(H_{N,\mathcal{O}}/H_{\mathcal{O}}) = \operatorname{Gal}(H_{\mathcal{O}}(E[N])/H_{\mathcal{O}}) \hookrightarrow (\mathcal{O}/N\mathcal{O})^\times$$

where $(\dagger)$ is the reciprocal of the isomorphism given by Theorem 3.3.6. Hence $\iota \colon (\mathcal{O}/N\mathcal{O})^\times/\mathcal{O}^\times \hookrightarrow (\mathcal{O}/N\mathcal{O})^\times$ is a section of the quotient map $(\mathcal{O}/N\mathcal{O})^\times \twoheadrightarrow (\mathcal{O}/N\mathcal{O})^\times/\mathcal{O}^\times$, and the short exact sequence

$$1 \to \mathcal{O}^\times \to (\mathcal{O}/N\mathcal{O})^\times \to (\mathcal{O}/N\mathcal{O})^\times/\mathcal{O}^\times \to 1$$

splits. Thus there exists a map $h \colon (\mathcal{O}/N\mathcal{O})^\times \twoheadrightarrow \mathcal{O}^\times$ which is a retraction of the inclusion $\mathcal{O}^\times \hookrightarrow (\mathcal{O}/N\mathcal{O})^\times$. In particular, one has that $h(-1) = -1$, which yields a contradiction because $-1 \in \mathcal{O}^\times = \{\pm 1\}$ is not a square. This concludes the proof of (b). □

We can now give a partial answer to Question **Q2**.

Corollary 4.4.7. *Let $\mathcal{O}$ be an order of discriminant $\Delta_{\mathcal{O}} < -3$ in an imaginary quadratic field $K \neq \mathbb{Q}(i)$ and fix $j \in H_{\mathcal{O}}$ to be the j-invariant of any elliptic curve with complex multiplication by $\mathcal{O}$. Then there exist infinitely many elliptic curves $E_{/H_{\mathcal{O}}}$ with $j(E) = j$ but non-isomorphic over $H_{\mathcal{O}}$, and such that*

- *$H_{\mathcal{O}}(E_{tors}) = K^{ab}$;*
- *The family $\{H_{\mathcal{O}}(E[p^\infty])\}_p$ is linearly disjoint over $H_{\mathcal{O}}$.*

Proof. The infinitely many elliptic curves $E_{\mathfrak{p}/H_{\mathcal{O}}}$ with $j(E_{\mathfrak{p}}) = j$ obtained in the first part of the proof of Theorem 4.4.6 are such that the corresponding $\mathfrak{p}$-division field is minimal. Since $\mathfrak{p} \subseteq \mathcal{O}$ is a prime ideal and $j(E_{\mathfrak{p}}) \neq 0, 1728$, this means that the family $\{H_{\mathcal{O}}(E_{\mathfrak{p}}[p^\infty])\}_p$ for p prime cannot be entangled over $H_{\mathcal{O}}$, since otherwise there would exist a division field $H_{\mathcal{O}}(E_{\mathfrak{p}}[N])$ such that $[H_{\mathcal{O}}(E_{\mathfrak{p}}[N]) : H_{\mathcal{O}}] < \#(\mathcal{O}/N\mathcal{O})^\times/2$, contradicting Theorem 3.4.1 (one could have equivalently argued by applying Corollary 3.5.4). □

For any order $\mathcal{O} \subseteq \mathbb{Q}(i)$ whose conductor is divided only by primes $p \equiv 1 \bmod 4$ the statement of Corollary 4.4.7 cannot hold true for any singular modulus relative to $\mathcal{O}$, as it follows from Theorem 4.4.6 (b). On the other hand, if $\mathcal{O} \subseteq \mathbb{Q}(i)$ but its conductor is divisible by at least one prime not splitting in $\mathbb{Q}(i)$, it is unclear to us whether the statement of the corollary remains valid in this case. Certainly the proof of Theorem 4.4.6 explicitly constructs infinitely many elliptic curves $E_{/H_{\mathcal{O}}}$ satisfying $H_{\mathcal{O}}(E_{\text{tors}}) = K^{\text{ab}}$. However, the construction shows that for almost all these elliptic curves the family $\{H_{\mathcal{O}}(E[p^\infty])\}_p$ is entangled over $H_{\mathcal{O}}$. Finally, we remark that the proof of Theorem 4.4.6 gives an explicit way of finding the elliptic curves in the statement of Corollary 4.4.7, thus answering affirmatively to Question **Q3** in this case.

If we now try to not impose anymore the assumption that torsion points should generate abelian extensions of the CM field, we reach the following result.

Theorem 4.4.8. *Let $\mathcal{O}$ be an order in an imaginary quadratic field K with $\operatorname{Pic}(\mathcal{O}) \neq \{1\}$ and fix $j \in H_{\mathcal{O}}$ to be the j-invariant of any elliptic curve with complex multiplication by $\mathcal{O}$. Then there exist infinitely many elliptic curves $E_{/H_{\mathcal{O}}}$ with $j(E) = j$ but non-isomorphic over $H_{\mathcal{O}}$, for which the family $\{H_{\mathcal{O}}(E[p^\infty])\}_p$ is linearly disjoint over $H_{\mathcal{O}}$.*

Proof. As we have already noticed at the beginning of the section, if an elliptic curve $E_{/H_{\mathcal{O}}}$ has p^∞-division fields that are entangled over the ring class field, then by Proposition 4.4.5 the curve E must satisfy $H_{\mathcal{O}}(E_{\text{tors}}) = K^{\text{ab}}$. Thus it is sufficient to show that, under the assumption $\operatorname{Pic}(\mathcal{O}) \neq \{1\}$, there are infinitely many elliptic curves $E_{/H_{\mathcal{O}}}$ as in the statement of the theorem with $H_{\mathcal{O}}(E_{\text{tors}}) \neq K^{\text{ab}}$.

If $\mathcal{O}$ is an order of discriminant $\Delta_{\mathcal{O}} = -4f_{\mathcal{O}}^2$ whose conductor $f_{\mathcal{O}} \in \mathbb{Z}_{\geq 2}$ is only divisible by primes $p \equiv 1 \bmod 4$, then by Theorem 4.4.6(b) all elliptic curves $E_{/H_{\mathcal{O}}}$ with complex multiplication by $\mathcal{O}$ satisfy $H_{\mathcal{O}}(E_{\text{tors}}) \neq K^{\text{ab}}$. Hence the statement is trivially true in this case.

Suppose now that $\mathcal{O}$ is not as above. Fix an elliptic curve E_0 defined over $H_{\mathcal{O}}$ such that $j(E_0) = j$ and $H_{\mathcal{O}}((E_0)_{\text{tors}}) = K^{\text{ab}}$. We know that infinitely many such elliptic curves E_0 exist by Theorem 4.4.6. We observe now that for every $\alpha \in H_{\mathcal{O}}^\times$ such that the extension $K \subseteq H_{\mathcal{O}}(\sqrt{\alpha})$ is not abelian, we have that

$$H_{\mathcal{O}}((E_0^{(\alpha)})_{\text{tors}}) \neq K^{\text{ab}}$$

where $E_0^{(\alpha)}$ denotes the quadratic twist of E_0 by $\alpha \in H_{\mathcal{O}}^\times$. Indeed, Theorem 4.4.4 shows that $H_{\mathcal{O}}(E_0[N]) = H_{N,\mathcal{O}}$ for some $N \in \mathbb{N}$, and this combined with Proposition 4.4.1, implies that $H_{\mathcal{O}}(E_0^{(\alpha)}[N]) = H_{N,\mathcal{O}}(\sqrt{\alpha}) \nsubseteq K^{\text{ab}}$.

In order to conclude the proof it is thus sufficient to show that there exist infinitely many $\alpha \in H_{\mathcal{O}}^\times$ such that $\sqrt{\alpha} \notin K^{\text{ab}}$ and the elliptic curves $E_0^{(\alpha)}$ are pairwise not isomorphic over $H_{\mathcal{O}}$. This is equivalent to say that there exist infinitely many distinct quadratic extensions of $H_{\mathcal{O}}$ which are not abelian over K. This can be shown, for instance, as follows.

Since $\operatorname{Pic}(\mathcal{O}) \neq \{1\}$ we have that $K \neq H_{\mathcal{O}}$. Hence the Chebotarëv density theorem shows that there exists $r \in \mathbb{Z}_{\geq 2}$ and an infinite set of prime ideals $\Lambda_0 = \{\mathfrak{p}_j \subseteq \mathcal{O}_K\}_{j \in \mathbb{N}}$ such that for every index $j \in \mathbb{N}$ we have that $2 \notin \mathfrak{p}_j$ and $\mathfrak{p}_j \cdot \mathcal{O}_{H_{\mathcal{O}}} = \mathfrak{P}_{1,j} \cdots \mathfrak{P}_{r,j}$ where $\mathfrak{P}_{1,j}, \dots, \mathfrak{P}_{r,j} \subseteq \mathcal{O}_{H_{\mathcal{O}}}$ are distinct prime ideals. Fix now an index $j_0 \in \mathbb{N}$ (*e.g.* $j_0 = 0$), and take any element $\alpha_0 \in \mathfrak{P}_{1,j_0} \setminus (\mathfrak{P}_{1,j_0}^2 \cup \mathfrak{P}_{2,j_0})$. Now, elementary ramification theory of quadratic extensions (see for instance [Gra03, Chapter I, Theorem 6.3]) shows that the extension $H_{\mathcal{O}} \subseteq H_{\mathcal{O}}(\sqrt{\alpha_0})$ ramifies at $\mathfrak{P}_{1,j_0}$ but not at $\mathfrak{P}_{2,j_0}$. This implies that the extension $K \subseteq H_{\mathcal{O}}(\sqrt{\alpha_0})$ is not Galois, hence in particular not abelian. Now, let Γ_0 be the finite set of prime ideals of $\mathcal{O}_K$ dividing $\mathrm{N}_{H_{\mathcal{O}}/K}(\alpha_0)$ and put $\Lambda_1 := \Lambda_0 \setminus \Gamma_0$, which is still an infinite set. Fix an index $j_1 \in \mathbb{N}$ such that $\mathfrak{p}_{j_1} \in \Lambda_1$ and take any element $\alpha_1 \in \mathfrak{P}_{1,j_1} \setminus (\mathfrak{P}_{1,j_1}^2 \cup \mathfrak{P}_{2,j_1})$. Again $K \subseteq H_{\mathcal{O}}(\sqrt{\alpha_1})$ is a non-abelian extension. Moreover we have that $H_{\mathcal{O}}(\sqrt{\alpha_0}) \neq H_{\mathcal{O}}(\sqrt{\alpha_1})$ since the prime $\mathfrak{P}_{1,j_1}$ ramifies in the extension $H_{\mathcal{O}} \subseteq H_{\mathcal{O}}(\sqrt{\alpha_1})$, but the same prime does not ramify in $H_{\mathcal{O}} \subseteq H_{\mathcal{O}}(\sqrt{\alpha_0})$. Repeating this process, we construct an infinite set of pairwise distinct quadratic extensions $\{H_{\mathcal{O}} \subseteq H_{\mathcal{O}}(\sqrt{\alpha_j}) : j \in \mathbb{N}\}$ that are non-abelian over K. This concludes the proof. □

Here is a summary of the entanglement investigations carried out in this section. Let $\mathcal{O}$ be an order of discriminant $\Delta_{\mathcal{O}} \notin \{-3,-4,-16\}$ in an imaginary quadratic field K and fix $j \in \overline{\mathbb{Q}}$ to be a singular modulus relative to $\mathcal{O}$. Then there exist infinitely many elliptic curves $E_{/H_{\mathcal{O}}}$ with $j(E) = j$ but non-isomorphic over $H_{\mathcal{O}}$, for which the family $\{H_{\mathcal{O}}(E[p^\infty])\}_p$ is linearly disjoint over $H_{\mathcal{O}}$. This gives a partial answer to Question **Q1**. Moreover, if $\mathcal{O} \nsubseteq \mathbb{Q}(i)$, there are infinitely many such elliptic curves satisfying the additional condition $H_{\mathcal{O}}(E_{\text{tors}}) = K^{\text{ab}}$. This gives a partial answer to Question **Q2**. Finally, the construction of the aforementioned elliptic curves is explicit, thus giving an answer to question **Q3**.

4.5 Entanglement in the family of division fields of CM elliptic curves over $\mathbb{Q}$

Let $E_{/\mathbb{Q}}$ be an elliptic curve with complex multiplication by an order in an imaginary quadratic field K. The aim of this section is to explicitly determine the image of the natural map

$$\operatorname{Gal}(K(E_{\text{tors}})/K) \hookrightarrow \prod_q \operatorname{Gal}(K(E[q^\infty])/K) \tag{4.15}$$

where the product runs over all rational primes $q \in \mathbb{N}$ and $K(E[q^\infty])$ denotes the compositum of the q-power division fields of $E_{/K}$. In other words, we want to analyse the entanglement in the family of Galois extensions $\{K(E[q^\infty])\}_q$ over K. The conclusion of this study will be Theorem 4.5.2, which provides a complete description of the image of (4.15) for all CM elliptic curves $E_{/\mathbb{Q}}$ such that $j(E) \notin \{0, 1728\}$. Observe that there is essentially no difference in considering the division fields of the elliptic curve $E_{/\mathbb{Q}}$ and of its base change $E_{/K}$, because $\mathbb{Q}(E[n]) = K(E[n])$ for every $n > 2$ as we will prove in Theorem 5.6.2. In particular, the family of division fields $\{\mathbb{Q}(E[q^\infty])\}_q$ is always entangled over $\mathbb{Q}$, but there are elliptic curves for which it is linearly disjoint over K, as we will see in Theorem 4.5.2.

We briefly outline the strategy of our proof: since E is defined over $\mathbb{Q}$ we have that $|\operatorname{Pic}(\mathcal{O})| = [\mathbb{Q}(j(E))\colon \mathbb{Q}] = 1$ (see [Cox13, Proposition 13.2]) which implies that the elliptic curve E has complex multiplication by one of the thirteen imaginary quadratic orders $\mathcal{O}$ of class number 1, listed in [Cox13, Theorem 7.30]. For each of these orders $\mathcal{O}$, we first find an elliptic curve $E_{0/\mathbb{Q}}$ with complex multiplication by $\mathcal{O}$ such that $|\mathfrak{f}_{E_0}| \in \mathbb{N}$ is minimal among all the conductors[1] of elliptic curves defined over $\mathbb{Q}$ which have complex multiplication by $\mathcal{O}$. We then proceed to compute the full entanglement in the family of division fields of $E_{0/K}$, using Theorem 4.3.4, Theorem 4.4.4, and Proposition 4.5.1. Since $\mathcal{O}$ is an order of class number 1 and $j(E) \notin \{0, 1728\}$, we have that E is a quadratic twist of E_0. We then use Proposition 4.4.1, which describes how Galois representations attached to CM elliptic curves behave under quadratic twisting, to determine the complete entanglement in the family of division fields of $E_{/K}$.

We begin by deriving some consequences of Proposition 4.4.1 when $\operatorname{Pic}(\mathcal{O}) = 1$ and the elliptic curve $E_{/K}$ is the base change to the imaginary quadratic field $K = H_{\mathcal{O}}$ of an elliptic curve defined over $\mathbb{Q}$. To do this, we need a formula originally due to Deuring that relates the conductor of a CM elliptic curve defined over $\mathbb{Q}$ to the conductor of the unique Hecke character $\varphi\colon \mathbb{A}_K^\times \to \mathbb{C}^\times$ associated to its base change over K by Theorem 4.4.2.

Proposition 4.5.1 (Deuring). *Let $\mathcal{O} \subseteq K$ be an order inside an imaginary quadratic field K. Let E be an elliptic curve defined over $\mathbb{Q}(j(E))$ with complex multiplication by $\mathcal{O}$. Denote by*

[1] The symbol $|\mathfrak{f}_A| \in \mathbb{N}$ denotes the positive generator of the conductor ideal $\mathfrak{f}_A \subseteq \mathbb{Z}$ of an elliptic curve $A_{/\mathbb{Q}}$

$\varphi\colon \mathbb{A}_{H_{\mathcal{O}}}^{\times} \to \mathbb{C}^{\times}$ the unique Hecke character associated by Theorem 4.4.2 to the base change of E over $K(j(E)) = H_{\mathcal{O}}$. Then, letting $j = j(E)$, one can write the conductor $\mathfrak{f}_E \subseteq \mathcal{O}_{\mathbb{Q}(j)}$ of E as

$$\mathfrak{f}_E = \mathrm{N}_{K(j)/\mathbb{Q}(j)}(\mathfrak{f}_{\varphi}) \cdot \delta_{K(j)/\mathbb{Q}(j)}$$

where $\mathrm{N}_{K(j)/\mathbb{Q}(j)}(\mathfrak{f}_{\varphi}) \subseteq \mathcal{O}_{\mathbb{Q}(j)}$ denotes the relative norm of the conductor $\mathfrak{f}_{\varphi} \subseteq \mathcal{O}_{K(j)}$ of the Hecke character φ and $\delta_{K(j)/\mathbb{Q}(j)} \subseteq \mathcal{O}_{\mathbb{Q}(j)}$ denotes the relative discriminant ideal associated to the quadratic extension $\mathbb{Q}(j) \subseteq K(j)$.

Proof. A modern proof of this formula can be obtained using [Mil72, Theorem 3] and [ST68, Theorem 12]. This is detailed in [Pen20, Appendix A]. □

We go back to study the consequences of Proposition 4.4.1. Let $E_{/K}$ be the base change to an imaginary quadratic field $K = H_{\mathcal{O}}$ of an elliptic curve $E_{/\mathbb{Q}}$ of conductor $\mathfrak{f}_E \subseteq \mathbb{Z}$ and with complex multiplication by an order $\mathcal{O}$ of class number one and discriminant $\Delta_{\mathcal{O}} < -4$. Fix also $\alpha \in \mathbb{Q}^{\times}$. Under these assumptions we may assume that $\alpha = \Delta$ where $\Delta = \Delta_F \in \mathbb{Z}$ is the fundamental discriminant associated to some quadratic extension $\mathbb{Q} \subseteq F$. Since $E^{(\alpha\beta)} = (E^{(\alpha)})^{(\beta)}$ for any $\alpha, \beta \in \mathbb{Q}^{\times}$, we reduce the study of the Galois representation $\rho_{E^{(\Delta)},p^n}$ for any prime $p \in \mathbb{Z}_{\geq 1}$ and any $n \in \mathbb{N}$ to the following cases:

T.1 $\Delta = (-1)^{(q-1)/2}\, q$ for some prime $q \in \mathbb{Z}_{\geq 3}$ with $q \nmid p\,\mathfrak{f}_E$. In this case $K(\sqrt{\Delta}) \cap K(E[p^n]) = K$. Indeed any prime $\mathfrak{q} \subseteq \mathcal{O}_K$ such that $\mathfrak{q} \mid q\mathcal{O}_K$ does not ramify in $K \subseteq K(E[p^n])$, as follows from Proposition 4.3.1 because $q \nmid p\,\mathfrak{f}_E$. On the other hand, any prime $\mathfrak{q} \mid q\mathcal{O}_K$ ramifies in $K \subseteq K(\sqrt{\Delta})$ since Proposition 4.5.1 shows that $q \nmid \Delta_K$, where $\Delta_K \in \mathbb{Z}_{<0}$ denotes the absolute discriminant of the imaginary quadratic field K. Thus Proposition 4.4.1 implies that $\rho_{E^{(\Delta)},p^n}$ will have maximal image independently from the behaviour of ρ_{E,p^n};

T.2 $p \geq 3$ and $\Delta = (-1)^{(p-1)/2}\, p$. In this case class field theory shows that

$$\mathbb{Q}(\sqrt{\Delta}) \subseteq \mathbb{Q}(\mu_p) \subseteq H_{p^n,\mathcal{O}}$$

where for every $m \in \mathbb{N}$ we let $\mu_m \subseteq \overline{\mathbb{Q}}$ denote the group of m-th roots of unity. Hence Proposition 4.4.1 implies that $\rho_{E^{(\Delta)},p^n}$ has maximal image if and only if ρ_{E,p^n} does;

T.3 $\Delta \in \{-4, -8, 8\}$ and $2 \nmid p\,\mathfrak{f}_E$. In this case $K(\sqrt{\Delta}) \cap K(E[p^n]) = K$, as in T.1, hence Proposition 4.4.1 shows that $\rho_{E^{(\Delta)},p^n}$ will have maximal image independently from the behaviour of ρ_{E,p^n};

T.4 $\Delta \in \{-4, -8, 8\}$ and $p = 2$. In this case $\mathbb{Q}(\sqrt{\Delta}) \subseteq \mathbb{Q}(\mu_{|\Delta|}) \subseteq H_{|\Delta|,\mathcal{O}}$ by class field theory. Hence Proposition 4.4.1 implies that for every $n \in \mathbb{N}$ such that $2^n \geq |\Delta|$ the representation $\rho_{E^{(\Delta)},2^n}$ has maximal image if and only if $\rho_{E,2^n}$ does, similarly to what we proved in T.2.

We are now ready to study the entanglement of division fields of CM elliptic curves E defined over $\mathbb{Q}$ such that $j(E) \notin \{0, 1728\}$.

First of all, assume that E has complex multiplication by an order $\mathcal{O}$ with $\gcd(\Delta_{\mathcal{O}}, 6) = 1$. Here $\Delta_{\mathcal{O}} := \mathfrak{f}_{\mathcal{O}}^2\, \Delta_K$ denotes the discriminant of $\mathcal{O}$, where $\Delta_K \in \mathbb{Z}$ denotes the absolute discriminant of K and $\mathfrak{f}_{\mathcal{O}} := [\mathcal{O}_K \colon \mathcal{O}]$ denotes the conductor of $\mathcal{O}$. Since $\mathrm{Pic}(\mathcal{O}) = \{1\}$ we have that $\mathcal{O} = \mathcal{O}_K$ and $\Delta_{\mathcal{O}} = \Delta_K = -p$ where $p \in \mathbb{N}$ is a prime number such that $p \geq 7$ and $p \equiv 3 \bmod 4$ (see [Cox13, Theorem 7.30]). Moreover $E = E_0^{(\Delta)}$ for some fundamental discriminant $\Delta \in \mathbb{Z}$, where E_0 is one of the two elliptic curves with $j(E_0) = j(E)$ appearing in Table 4.1, which lists the CM elliptic curves defined over $\mathbb{Q}$ whose conductor $|\mathfrak{f}_E| \in \mathbb{N}$ is minimal among their twists.

Let us study the division fields of E_0, as a first step towards the analysis of the division fields of E. Theorem 4.3.4 provides a decomposition

$$\operatorname{Gal}(K((E_0)_{\text{tors}})/K) \cong \prod_q \operatorname{Gal}(K(E_0[q^\infty])/K) \tag{4.16}$$

where the product runs over all the rational primes $q \in \mathbb{N}$. Indeed in this case the set S_{E_0} appearing in Theorem 4.3.4 consists of the single prime p because $|\mathfrak{f}_{E_0}| = p^2$ as follows from an inspection of Table 4.1. The isomorphism (4.16) shows that the family of division fields $\{K(E_0[q^\infty])\}_q$ is linearly disjoint over K, where $q \in \mathbb{N}$ runs over all the rational primes. Proposition 4.3.2 implies also that $\operatorname{Gal}(K(E_0[q^m])/K) \cong (\mathcal{O}/q^m\mathcal{O})^\times$ for every prime $q \neq p$ and every $m \in \mathbb{N}$. On the other hand we have that $\operatorname{Gal}(K(E_0[p^m])/K) \cong (\mathcal{O}/p^m\mathcal{O})^\times/\{\pm 1\}$ for every $m \in \mathbb{N}$. Indeed, it follows from Proposition 4.5.1 that $\mathfrak{f}_{\varphi_0} = \mathfrak{p}$, where $\mathfrak{p} \subseteq \mathcal{O}$ is the unique prime lying above p and $\varphi_0 \colon \mathbb{A}_K^\times \to \mathbb{C}^\times$ is the unique Hecke character associated to E_0 by Theorem 4.4.2. Hence Theorem 4.4.4 shows that $K(E_0[p^m]) = H_{p^m,\mathcal{O}}$ for every $m \in \mathbb{N}$, where $H_{p^m,\mathcal{O}}$ is the ray class field of K modulo p^m because $\mathcal{O} = \mathcal{O}_K$. Hence we can conclude that $\operatorname{Gal}(K(E_0[p^m])/K) \cong (\mathcal{O}/p^m\mathcal{O})^\times/\{\pm 1\}$ using Theorem 3.3.6.

Let us now go back to the division fields of $E = E_0^{(\Delta)}$. We can assume that $p \nmid \Delta$ because otherwise $\Delta = -p\,\Delta'$ for some fundamental discriminant $\Delta' \in \mathbb{Z}$, hence $E \cong_K E_0^{(\Delta')}$ since $\sqrt{-p} \in K$. Here the symbol $\cong_K$ means that the two elliptic curves E and $E_0^{(\Delta')}$, which are defined over $\mathbb{Q}$, become isomorphic when base-changed to K. Observe that $|\mathfrak{f}_E| = (p\,\Delta)^2$, which follows from (4.13) and [Ulm16, § 10, Proposition 1] because $|\mathfrak{f}_{E_0}|$ is coprime with Δ. Now, Theorem 4.3.4 gives

$$\operatorname{Gal}(K(E_{\text{tors}})/K) \cong \left(\prod_{q \notin S} \operatorname{Gal}(K(E[q^\infty])/K) \right) \times \operatorname{Gal}(K(E[S^\infty])/K)$$

with the product running over the rational primes $q \in \mathbb{N}$ such that $q \notin S$, where in this case the finite set $S = S_E \subseteq \mathbb{N}$ appearing in Theorem 4.3.4 consists uniquely of the primes dividing $|\mathfrak{f}_E| = (p\,\Delta)^2$. Moreover, $\operatorname{Gal}(K(E[\ell^m])/K) \cong (\mathcal{O}/\ell^m\mathcal{O})^\times$ for every prime $\ell \in \mathbb{N}$ and every $m \in \mathbb{N}$, since $\boxed{\text{T.1}}$ and $\boxed{\text{T.3}}$ show that for every $m \in \mathbb{N}$ the Galois representation ρ_{E,ℓ^m} has maximal image. On the other hand, Proposition 4.4.1 shows that $K(E[p^m]) = H_{p^m,\mathcal{O}}(\sqrt{\Delta})$ and

$$K(E[p^m]) \cap K(E[\Delta]) = K(\sqrt{\Delta})$$

for every $m \in \mathbb{Z}_{\geq 1}$. Hence the family of division fields $\{K(E[q^\infty])\}_{q \in S}$ is entangled over K, and for every collection of integers $\{a_q\}_{q \in S} \subseteq \mathbb{Z}_{\geq 1}$ such that $a_2 \geq 3$ we get

$$\operatorname{Gal}(L/K) \cong \frac{\prod_{q \in S} (\mathcal{O}/q^{a_q}\mathcal{O})^\times}{\{\pm 1\}}$$

where L is the compositum of all the division fields $K(E[q^{a_q}])$ for $q \in S$.

Let us now consider orders $\mathcal{O}$ such that $\gcd(\Delta_{\mathcal{O}}, 6) \neq 1$. The analysis of the division fields of an elliptic curve $E_{/\mathbb{Q}}$ having complex multiplication by $\mathcal{O}$ proceeds similarly to what happened before, with the only exception of the order $\mathcal{O} = \mathbb{Z}[\sqrt{-3}]$. Indeed if

$$\mathcal{O} \in \{\mathbb{Z}[3\zeta_3], \mathbb{Z}[2i], \mathbb{Z}[\sqrt{-2}], \mathbb{Z}[\sqrt{-7}]\}$$

where $\zeta_3 := (-1 + \sqrt{-3})/2$ and $i := \sqrt{-1}$, then all the elliptic curves E_0 appearing in Table 4.1 with complex multiplication by $\mathcal{O}$ share the property that $|\mathfrak{f}_{E_0}|$ is a power of the unique rational prime $p \in \mathbb{N}$ which ramifies in the quadratic extension $\mathbb{Q} \subseteq K$. Hence Theorem 4.3.4 provides a decomposition

$$\operatorname{Gal}(K((E_0)_{\text{tors}})/K) \cong \prod_q \operatorname{Gal}(K(E_0[q^\infty])/K)$$

where the product runs over all rational primes $q \in \mathbb{N}$, because in this case the finite set $S_{E_0} \subseteq \mathbb{N}$ appearing in Theorem 4.3.4 consists of the single prime p. This shows that the division fields of E_0 are linearly disjoint over K. Moreover, Proposition 4.3.2 implies that $\operatorname{Gal}(K(E_0[q^m])/K) \cong (\mathcal{O}/q^m\mathcal{O})^\times$ for every rational prime $q \neq p$ and every $m \in \mathbb{N}$. On the other hand, Proposition 4.5.1 shows that $\mathfrak{f}_{\varphi_0} = \mathfrak{p}^k$ is a power of the unique prime ideal $\mathfrak{p} \subseteq \mathcal{O}_K$ lying over p, with $k \leq 2$ if $\mathcal{O} \notin \{\mathbb{Z}[2i], \mathbb{Z}[\sqrt{-2}]\}$ and $k \leq 6$ otherwise. Hence Theorem 4.4.4 and Theorem 3.3.6 give $\operatorname{Gal}(K(E_0[p^m])/K) \cong (\mathcal{O}/p^m)^\times/\{\pm 1\}$ for every $m \in \mathbb{N}$ such that $m \geq 1$ if $\mathcal{O} \notin \{\mathbb{Z}[2i], \mathbb{Z}[\sqrt{-2}]\}$ and $m \geq 3$ otherwise.

Let now $E_{/\mathbb{Q}}$ be any elliptic curve with complex multiplication by $\mathcal{O}$. Since $j(E) = j(E_0) \notin \{0, 1728\}$ we know that $E = E_0^{(\Delta)}$ for some fundamental discriminant $\Delta \in \mathbb{Z}$. If $\mathcal{O} = \mathbb{Z}[3\zeta_3]$ or $\mathcal{O} = \mathbb{Z}[\sqrt{-7}]$ we can assume that $p \nmid \Delta$ because $\sqrt{-p} \in K$. Hence Theorem 4.3.4 shows that

$$\operatorname{Gal}(K(E_{\text{tors}})/K) \cong \left(\prod_{q \notin S} \operatorname{Gal}(K(E[q^\infty])/K) \right) \times \operatorname{Gal}(K(E[S^\infty])/K)$$

with the product running over the rational primes $q \in \mathbb{N}$ such that $q \notin S$, where in this case the finite set $S = S_E \subseteq \mathbb{N}$ appearing in Theorem 4.3.4 consists uniquely of the primes dividing $|\mathfrak{f}_E| = (p\,\Delta)^2$. Exactly as before T.1 and T.3 show that $\operatorname{Gal}(K(E[\ell^m])/K) \cong (\mathcal{O}/\ell^m\mathcal{O})^\times$ for every prime $\ell \in \mathbb{N}$ and every $m \in \mathbb{N}$. Moreover, Proposition 4.4.1 shows that $K(E[p^m]) = H_{p^m,\mathcal{O}}(\sqrt{\Delta})$ and $K(E[p^m]) \cap K(E[\Delta]) = K(\sqrt{\Delta})$ for every $m \in \mathbb{Z}_{\geq 1}$. Hence the family of division fields $\{K(E[q^\infty])\}_{q \in S}$ is entangled over K, and for every collection of integers $\{a_q\}_{q \in S} \subseteq \mathbb{Z}_{\geq 1}$ with $a_2 \geq 3$ we get

$$\operatorname{Gal}(L/K) \cong \frac{\prod_{q \in S} (\mathcal{O}/q^{a_q}\mathcal{O})^\times}{\{\pm 1\}}$$

where L is the compositum of all the division fields $K(E[q^{a_q}])$ for $q \in S$.

Studying the entanglement in the family of division fields of E becomes slightly more complicated if $\mathcal{O} \in \{\mathbb{Z}[2i], \mathbb{Z}[\sqrt{-2}]\}$. First of all, note that there exists a unique $\Delta_2 \in \{1, -4, -8, 8\}$ such that $\Delta = \Delta_2\,\Delta'$ where $\Delta' \in \mathbb{Z}$ is an odd fundamental discriminant. We can now write $E = E_1^{(\Delta')}$ where $E_1 := E_0^{(\Delta_2)}$. One can check that if $\mathcal{O} = \mathbb{Z}[\sqrt{-2}]$ then E_1 is isomorphic to one of the four elliptic curves with complex multiplication by $\mathbb{Z}[\sqrt{-2}]$ appearing in Table 4.1. On the other hand, if $\mathcal{O} = \mathbb{Z}[2i]$ then E_1 can be either one of the two elliptic curves

$$\begin{aligned} y^2 &= x^3 - 44x - 112 \\ y^2 &= x^3 - 44x + 112 \end{aligned} \tag{4.17}$$

or one of the two elliptic curves with complex multiplication by $\mathbb{Z}[2i]$ appearing in Table 4.1. In each case it is not difficult to see that $|\mathfrak{f}_{E_1}| \in \mathbb{N}$ is a power of 2, which shows that the division fields of E_1 behave similarly to the division fields of E_0. More precisely, Theorem 4.3.4 gives

$$\mathrm{Gal}(K((E_1)_{\mathrm{tors}})/K) \cong \prod_q \mathrm{Gal}(K(E_1[q^\infty])/K)$$

where the product runs over all the rational primes $q \in \mathbb{N}$. This shows that the division fields of E_1 are linearly disjoint over K. Moreover, Proposition 4.3.2 shows that $\mathrm{Gal}(K(E_1[q^m])/K) \cong (\mathcal{O}/q^m\mathcal{O})^\times$ for every rational prime $q \geq 3$ and every $m \in \mathbb{N}$, and a combination of Proposition 4.5.1 and Theorem 4.4.4 gives $\mathrm{Gal}(K(E_1[2^m])/K) \cong (\mathcal{O}/2^m\mathcal{O})^\times/\{\pm 1\}$ for every $m \in \mathbb{N}$ such that $m \geq 3$. This concludes the analysis of the division fields of $E = E_1$ if $\Delta' = 1$. On the other hand, if $\Delta' \neq 1$ then $|\mathfrak{f}_E| = |\mathfrak{f}_{E_1}|\,(\Delta')^2$ where $|\mathfrak{f}_{E_1}|$ is a power of 2. Hence Theorem 4.3.4 shows that

$$\mathrm{Gal}(K(E_{\mathrm{tors}})/K) \cong \left(\prod_{q \notin S} \mathrm{Gal}(K(E[q^\infty])/K) \right) \times \mathrm{Gal}(K(E[S^\infty])/K)$$

with the product running over the rational primes $q \in \mathbb{N}$ such that $q \notin S$ where $S = S_E$ denotes the finite set appearing in Theorem 4.3.4, which in this case consists of the primes dividing $2 \cdot \Delta'$. Similarly to what happened before, T.1 and T.4 show that $\mathrm{Gal}(K(E[\ell^m])/K) \cong (\mathcal{O}/\ell^m\mathcal{O})^\times$ for every prime $\ell \in \mathbb{N}$ and every $m \in \mathbb{N}$. Moreover, Proposition 4.4.1 gives $K(E[2^m]) = H_{2^m,\mathcal{O}}(\sqrt{\Delta'})$ and $K(E[2^m]) \cap K(E[\Delta']) = K(\sqrt{\Delta'})$ for every $m \geq 3$. Hence the family of division fields $\{K(E[q^\infty])\}_{q \in S}$ is entangled over K, and for all $\{a_q\}_{q \in S} \subseteq \mathbb{Z}_{\geq 1}$ with $a_2 \geq 3$ we get

$$\mathrm{Gal}(L/K) \cong \frac{\prod_{q \in S} (\mathcal{O}/q^{a_q}\mathcal{O})^\times}{\{\pm 1\}}$$

where L is the compositum of all the division fields $K(E[q^{a_q}])$ for $q \in S$.

We are left with the analysis of the entanglement between the division fields of an elliptic curve E defined over $\mathbb{Q}$ which has complex multiplication by $\mathcal{O} = \mathbb{Z}[\sqrt{-3}]$. As usual $E = E_0^{(\Delta)}$ for some fundamental discriminant $\Delta \in \mathbb{Z}$, where E_0 is one of the two elliptic curves with complex multiplication by $\mathbb{Z}[\sqrt{-3}]$ appearing in Table 4.1. In contrast to what we have seen before, here $|\mathfrak{f}_{E_0}| = 2^2\,3^2$ is not a prime power. This forces us to study separately the division fields $K(E_0[2^\infty])$ and $K(E_0[3^\infty])$. First of all, one can compute that for any of the two possibilities for E_0, given by the Weierstrass equations $y^2 = x^3 - 15x + 22$ and $y^2 = x^3 - 135x - 594$, the representation $\rho_{E_0,3}$ is not surjective, *i.e.* $K(E_0[3]) = H_{3,\mathcal{O}} = K(\sqrt[3]{2})$. This clearly shows that $\rho_{E_0,3^n}$ is not surjective for every $n \in \mathbb{Z}_{\geq 1}$. Moreover, $\rho_{E_0,2^n}$ is surjective for every $n \in \mathbb{Z}_{\geq 1}$. Indeed, Theorem 3.3.6 and Theorem 3.4.1 imply that

$$\left| \left(\frac{\mathcal{O}}{2^n\mathcal{O}} \right)^\times \right| = \frac{[H_{2^n 3,\mathcal{O}} \colon K]}{[H_{3,\mathcal{O}} \colon K]} = \frac{[H_{2^n 3,\mathcal{O}} \colon K]}{[K(E_0[3]) \colon K]} \leq \frac{[K(E_0[2^n 3]) \colon K]}{[K(E_0[3]) \colon K]} \leq [K(E_0[2^n]) \colon K]$$

hence Lemma 3.1.1 shows that every inequality is actually an equality, and $\rho_{E_0,2^n}$ is surjective. This gives that $K(E_0[2^n]) \cap K(E_0[3^m]) = K$ for every $n, m \in \mathbb{Z}_{\geq 1}$. These considerations together with Theorem 4.3.4 and Proposition 4.3.2 give a decomposition

$$\operatorname{Gal}(K((E_0)_{\text{tors}})/K) \cong \prod_q \operatorname{Gal}(K(E_0[q^\infty])/K)$$

where the product runs over all rational primes $q \in \mathbb{N}$. Moreover, for every $m \in \mathbb{N}$ we get

$$\operatorname{Gal}(K(E_0[q^m])/K) \cong \begin{cases} (\mathcal{O}/q^m\mathcal{O})^\times, & \text{if } q \neq 3 \\ (\mathcal{O}/3^m\mathcal{O})^\times/\{\pm 1\}, & \text{if } q = 3 \end{cases}$$

and the family of division fields $\{K(E[q^\infty])\}_q$ is linearly disjoint over K.

Let us go back to the division fields of $E = E_0^{(\Delta)}$, where we can assume that $3 \nmid \Delta$ because $\sqrt{-3} \in K$. Write now $\Delta = \Delta_2 \Delta'$ as above, where $\Delta_2 \in \{1, -4, -8, 8\}$ and $\Delta' \in \mathbb{Z}$ an odd fundamental discriminant, and let $E_1 := E_0^{(\Delta_2)}$. Then T.4 implies that $\rho_{E_1,2^n}$ is surjective for every $n \geq 3$. Moreover, $\rho_{E_1,3^n}$ is surjective for every $n \geq 1$, which follows from Proposition 4.4.1 after observing that $K(E_0[3]) \cap K(\sqrt{\Delta_2}) = K$ because $[K(E_0[3]) \colon K] = 3$. These considerations, together with Theorem 4.3.4, show that

$$\operatorname{Gal}(K((E_1)_{\text{tors}})/K) \cong \left(\prod_{q \notin S} \operatorname{Gal}(K(E_1[q^\infty])/K)\right) \times \operatorname{Gal}(K(E_1[S^\infty])/K)$$

with the product running over the rational primes $q \in \mathbb{N}$ such that $q \notin S$ where $S = \{2, 3\}$ and $K(E_1[S^\infty])$ denotes the compositum of the division fields $K(E_1[2^\infty])$ and $K(E_1[3^\infty])$. Moreover, T.1, T.2 and the previous considerations show that $\operatorname{Gal}(K(E_1[\ell^m])/K) \cong (\mathcal{O}/\ell^m\mathcal{O})^\times$ for every prime $\ell \in \mathbb{N}$ and every $m \in \mathbb{N}$. Now, Proposition 4.4.1 shows that $K(E_1[3^m]) = H_{3^m,\mathcal{O}}(\sqrt{\Delta_2})$ and $K(E_1[3^m]) \cap K(E_1[\Delta_2]) = K(\sqrt{\Delta_2})$ for every $m \in \mathbb{Z}_{\geq 1}$. Hence $K(E_1[2^\infty])$ and $K(E_1[3^\infty])$ are entangled over K, and for every pair of integers $a, b \in \mathbb{Z}_{\geq 1}$ with $a \geq 3$ we have that

$$\operatorname{Gal}(L/K) \cong \frac{(\mathcal{O}/2^a\mathcal{O})^\times \times (\mathcal{O}/3^b\mathcal{O})^\times}{\{\pm 1\}}$$

where L denotes the compositum of $K(E_1[2^a])$ and $K(E_1[3^b])$.

To conclude our analysis of the division fields of $E = E_0^{(\Delta)}$ we can observe that $E = E_1^{(\Delta')}$ and that $\gcd(\Delta', \mathfrak{f}_{E_1}) = \gcd(\Delta', 6) = 1$. Hence Theorem 4.3.4 gives the decomposition

$$\operatorname{Gal}(K(E_{\text{tors}})/K) \cong \left(\prod_{q \notin S} \operatorname{Gal}(K(E[q^\infty])/K)\right) \times \operatorname{Gal}(K(E[S^\infty])/K)$$

with the product running over the rational primes $q \in \mathbb{N}$ such that $q \notin S$ where $S \subseteq \mathbb{N}$ denotes the finite set of primes dividing $6\Delta'$. Now, T.1 and T.2 show that $\operatorname{Gal}(K(E[\ell^m])/K) \cong (\mathcal{O}/\ell^m)^\times$ for all rational primes $\ell \in \mathbb{Z}$ and all $m \in \mathbb{N}$. Moreover, Proposition 4.4.1 shows that $K(E[3^m]) \cap K(E[\Delta]) = K(\sqrt{\Delta})$ and $K(E[3^m]) = H_{3^m,\mathcal{O}}(\sqrt{\Delta})$ for every $m \in \mathbb{Z}_{\geq 1}$. Hence the family $\{K(E[q^\infty])\}_{q\in S}$ is entangled over K, and for every collection of integers $\{a_q\}_{q\in S} \subseteq \mathbb{Z}_{\geq 1}$ such that $a_2 \geq 3$ we get

$$\operatorname{Gal}(L/K) \cong \frac{\prod_{q\in S} (\mathcal{O}/q^{a_q}\mathcal{O})^\times}{\{\pm 1\}}$$

where L is the compositum of all the division fields $K(E[q^{a_q}])$ for $q \in S$.

The following theorem summarises the previous discussion. Recall that, for every rational prime $q \in \mathbb{N}$, we denote by $K(E[q^\infty])$ the compositum of all the division fields $\{K(E[q^n])\}_{n\in\mathbb{N}}$ associated to an elliptic curve E, and for every finite set of primes $S \subseteq \mathbb{N}$ we denote by $K(E[S^\infty])$ the compositum of all the fields $\{K(E[q^\infty])\}_{q\in S}$.

Theorem 4.5.2. *Let $\mathcal{O}$ be an order inside an imaginary quadratic field K such that $\operatorname{Pic}(\mathcal{O}) = 1$ and $\Delta_{\mathcal{O}} < -4$. We introduce the following notation:*

$$n = n(\mathcal{O}) := \begin{cases} 4, & \textit{if } \mathcal{O} \in \{\mathbb{Z}[2i], \mathbb{Z}[\sqrt{-2}]\} \\ 2, & \textit{otherwise} \end{cases} \qquad \textit{and} \qquad \begin{array}{l} p \in \mathbb{N} \textit{ the unique prime ramifying in } \mathbb{Q} \subseteq K, \\ \mathfrak{p} \subseteq \mathcal{O}_K \textit{ the unique prime lying above } p. \end{array}$$

Label all the elliptic curves defined over $\mathbb{Q}$ which have complex multiplication by $\mathcal{O}$ as $\{A_r\}_{r\in\mathbb{Z}_{\geq 1}}$ in such a way that $|\mathfrak{f}_{A_r}| \leq |\mathfrak{f}_{A_{r+1}}|$ for every $r \in \mathbb{Z}_{\geq 1}$. Then $|\mathfrak{f}_{A_n}| < |\mathfrak{f}_{A_{n+1}}|$ and the properties of the division fields associated to the elliptic curve A_r depend on r as follows:

$\boxed{r \leq n}$ ***Disjointness*** *the family $\{K(A_r[q^\infty])\}_q$, where $q \in \mathbb{N}$ runs over all the rational primes, is linearly disjoint over K;*

Maximality $\operatorname{Gal}(K(A_r[q^m])/K) \cong (\mathcal{O}/q^m\mathcal{O})^\times$ *for every prime $q \neq p$ and every $m \in \mathbb{N}$;*

Minimality $\operatorname{Gal}(K(A_r[p^m])/K) \cong (\mathcal{O}/p^m\mathcal{O})^\times/\{\pm 1\}$ *for every $m \geq n-1$;*

$\boxed{r > n}$ **Twist** *there exists a unique $r_0 \leq n$ and a unique fundamental discriminant $\Delta_r \in \mathbb{Z}$ coprime with p such that $A_r = A_{r_0}^{(\Delta_r)}$;*

Disjointess *there is a decomposition*

$$\mathrm{Gal}(K((A_r)_{tors})/K) \cong \left(\prod_{q \notin S_r} \mathrm{Gal}(K(A_r[q^\infty])/K) \right) \times \mathrm{Gal}(K(A_r[S^\infty])/K)$$

where $S_r \subseteq \mathbb{N}$ denotes the finite set of primes dividing $p \cdot \Delta_r$ and the product runs over the rational primes $q \in \mathbb{N}$ such that $q \notin S_r$. This shows that the family

$$\{ K(A_r[S_r^\infty]) \} \cup \{ K(A_r[q^\infty]) \}_{q \notin S_r}$$

is linearly disjoint over K;

Entanglement *for every $m \in \mathbb{N}$ such that $m \geq n-1$ we have that*

$$K(A_r[p^m]) = H_{p^m,\mathcal{O}}(\sqrt{\Delta_r}) \qquad \text{and} \qquad K(A_r[p^m]) \cap K(A_r[\Delta_r]) = K(\sqrt{\Delta_r})$$

which shows that the family $\{K(A_r[q^\infty])\}_{q \in S_r}$ is entangled over K;

Maximality $\mathrm{Gal}(K(A_r[q^m])/K) \cong (\mathcal{O}/q^m\mathcal{O})^\times$ *for every prime $q \in \mathbb{N}$ and every $m \in \mathbb{N}$;*

Minimality *for every collection of integers $\{a_q\}_{q \in S_r} \subseteq \mathbb{Z}_{\geq 1}$ with $a_2 \geq 3$ we get*

$$\mathrm{Gal}(L/K) \cong \frac{\prod_{q \in S_r} (\mathcal{O}/q^{a_q}\mathcal{O})^\times}{\{\pm 1\}}$$

where L is the compositum of all the division fields $K(A_r[q^{a_q}])$ for $q \in S_r$.

Notice that Theorem 4.5.2 implies that the isomorphism (4.10) appearing in Theorem 4.3.4 does not hold in general if the set S does not contain all the primes dividing the integer $B_E := \mathfrak{f}_{\mathcal{O}}\, \Delta_F\, N_{F/\mathbb{Q}}(\mathfrak{f}_E) \in \mathbb{Z}$. To see this, fix an imaginary quadratic order $\mathcal{O}$ having trivial class group $\mathrm{Pic}(\mathcal{O}) = \{1\}$, conductor $\mathfrak{f}_{\mathcal{O}} \neq 2$ and discriminant $\Delta_{\mathcal{O}} < -4$. Let $n = n(\mathcal{O}) \in \{2, 4\}$ be as in Theorem 4.5.2. Then, if we take $E = A_r$ for any $r > n$, Theorem 4.5.2 shows that (4.10) does not hold for any set S which does not contain the set S_r appearing in Theorem 4.5.2. Since this set S_r coincides with the set of primes dividing the integer $B_E = B_{A_r}$, this proves our claim.

We conclude with the following immediate consequence of Theorem 4.5.2.

Corollary 4.5.3. *Let $\mathcal{O}$ be an order of discriminant $\Delta_{\mathcal{O}} < -4$ inside an imaginary quadratic field K, and suppose that $\mathrm{Pic}(\mathcal{O}) = \{1\}$. Let $E_{/\mathbb{Q}}$ be an elliptic curve with complex multiplication by $\mathcal{O}$. Then the family of division fields $\{K(E[p^\infty])\}_p$, where p runs over the rational primes $p \in \mathbb{N}$, is linearly disjoint over K if and only if E is isomorphic over K to one of the thirty elliptic curves appearing either in Table 4.1 or in (4.17).*

Δ_K	$\mathfrak{f}_\mathcal{O}$	$j(E)$	$\lvert\mathfrak{f}_E\rvert$	Equations
-3	1	0	3^3	$y^2 + y = x^3 - 7$ $y^2 + y = x^3$
	2	$2^4\,3^3\,5^3$	$2^2 3^2$	$y^2 = x^3 - 15x + 22$ $y^2 = x^3 - 135x - 594$
	3	$-2^{15}\,3\,5^3$	3^3	$y^2 + y = x^3 - 30x + 63$ $y^2 + y = x^3 - 270x - 1708$
-4	1	$2^6\,3^3$	2^5	$y^2 = x^3 - x$ $y^2 = x^3 + 4x$
	2	$2^3\,3^3\,11^3$	2^5	$y^2 = x^3 - 11x - 14$ $y^2 = x^3 - 11x + 14$
-7	1	$-3^3\,5^3$	7^2	$y^2 + xy = x^3 - x^2 - 2x - 1$ $y^2 + xy = x^3 - x^2 - 107x + 552$
	2	$3^3\,5^3\,17^3$	7^2	$y^2 + xy = x^3 - x^2 - 37x - 78$ $y^2 + xy = x^3 - x^2 - 1822x + 30393$
-8	1	$2^6\,5^3$	2^8	$y^2 = x^3 - x^2 - 3x - 1$ $y^2 = x^3 + x^2 - 3x + 1$ $y^2 = x^3 - x^2 - 13x + 21$ $y^2 = x^3 + x^2 - 13x - 21$
-11	1	-2^{15}	11^2	$y^2 + y = x^3 - x^2 - 7x + 10$ $y^2 + y = x^3 - x^2 - 887x - 10143$
-19	1	$-2^{15}\,3^3$	19^2	$y^2 + y = x^3 - 38x + 90$ $y^2 + y = x^3 - 13718x - 619025$
-43	1	$-2^{18}\,3^3\,5^3$	43^2	$y^2 + y = x^3 - 860x + 9707$ $y^2 + y = x^3 - 1590140x - 771794326$
-67	1	$-2^{15}\,3^3\,5^3\,11^3$	67^2	$y^2 + y = x^3 - 7370x + 243528$ $y^2 + y = x^3 - 33083930x - 73244287055$
-163	1	$-2^{18}\,3^3\,5^3\,23^3\,29^3$	163^2	$y^2 + y = x^3 - 2174420x + 1234136692$ $y^2 + y = x^3 - 57772164980x - 5344733777551611$

Table 4.1: Minimal Weierstrass equations of CM elliptic curves defined over $\mathbb{Q}$ having the smallest conductor $\lvert\mathfrak{f}\rvert$ amongst all their twists, where $\lvert\mathfrak{f}_E\rvert \in \mathbb{N}$ denotes the unique positive generator of the conductor ideal $\mathfrak{f}_E \subseteq \mathbb{Z}$.

5 Cyclic reduction of elliptic curves

Let E be an elliptic curve defined over a number field F, and $\mathfrak{p}$ a prime of F for which E has good reduction. Then the point group $E_{\mathfrak{p}}(k_{\mathfrak{p}})$ of the reduced curve over the residue class field $k_{\mathfrak{p}}$ is a finite abelian group on at most two generators [Sil09, III, Corollary 6.4]. If one generator suffices, we call $\mathfrak{p}$ a prime *of cyclic reduction* of E. The question considered in this chapter is whether the set $S_{E/F}$ of primes of cyclic reduction of E is infinite and, if so, whether it has a (natural) density inside the set of all primes of F. Serre [Ser78] observed in 1977 that this problem is very similar to *Artin's primitive root problem*, which asks for the density of the set of primes $p \in \mathbb{N}$ for which a fixed element $a \in \mathbb{Q}^{\times}$ is a primitive root modulo p. In this situation, these primes are (up to finitely many primes of "bad reduction" for a) the primes p that do not split completely in any of the fields $F_\ell := \mathbb{Q}(\zeta_\ell, \sqrt[\ell]{a}) = \mathrm{Split}_{\mathbb{Q}}(X^\ell - a)$ for $\ell \in \mathbb{Z}$ prime. We review in more details this problem and its conjectural solution given by Artin in Section 5.1. From a correspondence between Artin and the Lehmer's family [ALL] we learn that in the very first formulation of his heuristics, Artin overlooked an important point: for some values of $a \in \mathbb{Q}^{\times}$, the family $\{F_\ell\}_\ell$ can be entangled over $\mathbb{Q}$ and this means that the splitting conditions at the various fields F_ℓ may not be independent. In order to find the exact heuristic, one has to multiply Artin's "naive density" by a rational correction factor depending on a. This situation is not an hapax legomenon but occurs in many similar density questions, including the cyclic reduction problem considered in this chapter. A general conceptual way of dealing with correction factors to primitive-root densities has been found in [LSM14] and goes under the name of *character-sum method*. We review a special case of this method in Section 5.2. Having prepared the ground, in Section 5.3 we finally begin to discuss the cyclic reduction problem after which this chapter is named. We prove that, under the assumption of the Generalized Riemann Hypothesis, the density of the set $S_{E/F}$ exists, and it can be written as an inclusion-exclusion sum involving the degrees of the N-division fields of E. However, this way of expressing the density is in many ways unsatisfactory as, for instance, it does not even allow to tell when this density vanishes. We then seek for alternative expressions and, to this aim, it is convenient to divide the discussion according to whether the elliptic curve E has complex multiplication or not. The non-CM case is studied in Section 5.4 and is accompanied by several numerical illustrations. If E does not have complex multiplication, the density of the set $S_{E/F}$ can be expressed as a corrected naive density in a way that is reminiscent of Artin's primitive root conjecture. We begin the investigation of the CM case in Section 5.5, where we show that the density of $S_{E/F}$ exists *unconditionally*. Unlike the non-CM case however, the inclusion-exclusion sum representing this density cannot be expressed as a corrected infinite product in general. We detail upon this in Section 5.6 where it is proved, among other things, that the density of $S_{E/F}$ never vanishes if $F = \mathbb{Q}(j(E))$ is the field of moduli of E. Finally, in Section 5.7 we reap the fruits of the work done in Chapter 4 and we compute the cyclic reduction densities of all the CM elliptic curves defined over $\mathbb{Q}$ with $j(E) \neq 0, 1728$.

5.1 Artin's primitive root conjecture

As a motivation, we begin the chapter by describing Artin's primitive root problem and the heuristic argument that led to Artin's primitive root conjecture. For an account of the rich and interesting story that brought to the formulation of the present form of the conjecture the reader can consult [Ste03, Section 2].

Given a prime number $p \in \mathbb{N}$, we say that a rational number $a \in \mathbb{Q}$ is a *primitive root* modulo p if p does not divide neither the numerator nor the denominator of a and $\langle a \bmod \ell \rangle = \mathbb{F}_\ell^\times$. For instance, 2 is a primitive root modulo 5 but not modulo 7, and for every prime number p one can decide in a finite amount of steps whether 2 is a primitive root modulo p or not. After seeking for a certain number of primes for which 2 is a primitive root, one is certainly led to the following natural, but highly non-trivial, question: is it true that 2 is a primitive root modulo infinitely many primes? Since 2 does not have any particular role as an integer, we can replace it by any $a \in \mathbb{Q}$. Then the *primitive root problem* for a asks whether there exist infinitely many primes $p \in \mathbb{N}$ such that a is a primitive root modulo p. Of course, if $a = \pm 1$ or a is a square then a can be a primitive root only modulo $p = 2$. With the exception of these trivial cases, it is not known at present an unconditional answer to the primitive root problem for any other $a \in \mathbb{Q}$.

In 1927 Artin [Art65, pp. viii-ix] formulated some heuristics suggesting that the set of primes p for which a given rational number a is a primitive root modulo p has a natural density, and he even proposed an explicit conjectural density for this set. His argument goes as follows: fix $a \in \mathbb{Q} \setminus \{0, \pm 1\}$ and let p be a prime non dividing neither the numerator nor the denominator of a. The number a being a primitive root modulo p means by definition that $I_p := |\mathbb{F}_p^\times : \langle a \bmod p \rangle| = 1$. On the other hand, a prime ℓ divides the index I_p if and only if a belongs to the group of ℓ-th powers in $\mathbb{F}_p^\times$, in which case there are exactly ℓ elements whose ℓ-th power is equal to a. In other words, ℓ divides I_p if and only if the polynomial $X^\ell - a \in \mathbb{F}_p[X]$ has all its roots in $\mathbb{F}_p$. It follows that a is a primitive root modulo p if and only if p does not split completely in any extension $\mathbb{Q} \subseteq F_\ell := \mathrm{Split}_{\mathbb{Q}}(X^\ell - a) = \mathbb{Q}(\zeta_\ell, \sqrt[\ell]{a})$ for every prime $\ell < p$. Therefore, we want to understand whether the set S_a of primes p that do not split completely in any of the extensions $\mathbb{Q} \subseteq F_\ell$ has a density $\delta(S_a)$. If one looks at a fixed prime $\ell \in \mathbb{N}$, then by the Chebotarëv's density theorem the density of the set of primes that do not split completely in $\mathbb{Q} \subseteq F_\ell$ equals

$$\delta_\ell = 1 - \frac{1}{[F_\ell : \mathbb{Q}]}$$

and, assuming that the splitting conditions at the various primes ℓ are *independent*, it seems reasonable to expect the heuristic density

$$\delta(S_a) = \prod_\ell \delta_\ell = \prod_\ell \left(1 - \frac{1}{[F_\ell : \mathbb{Q}]}\right). \tag{5.1}$$

Note that, with only finitely many exceptions, we have $[F_\ell : \mathbb{Q}] = \ell(\ell - 1)$, so the expected density (5.1) is a rational multiple of the *universal Artin constant*

$$A_\infty = \prod_\ell \left(1 - \frac{1}{\ell(\ell - 1)}\right) \approx 0.3739558. \tag{5.2}$$

We need however to be careful with the above reasoning, since the assumption on the independence of the splitting conditions in $\mathbb{Q} \subseteq F_\ell$ is not always satisfied. This is better explained with an example (due to Artin himself).

Suppose $a = 5$. Then the field $F_2 = \mathbb{Q}(\sqrt{5})$ is contained in the cyclotomic field $\mathbb{Q}(\zeta_5)$, and so we have the inclusion $F_2 \subseteq F_5$. This means that in the moment we impose the condition of not splitting completely in F_2, we automatically impose the condition of not splitting completely in F_5. In order to take this containment into account, we need to scale the density in (5.1) by a factor $c_5 = 20/19$. This adjustment is numerically very visible, as Artin himself noticed ("So I was careless, but the machine caught up with me").

The moral of this example is that in expression (5.1) we have to introduce a correction factor which takes into account the entanglement in the family $\mathcal{F} = \{F_\ell\}_\ell$. One can prove that the family $\mathcal{F}$ is entangled over $\mathbb{Q}$ if and only if the discriminant $\Delta = \Delta(F_2/\mathbb{Q})$ is odd, in which case the only source of entanglement is given by the inclusion $F_2 \subseteq F_{|\Delta|}$. We will see in Section 5.2 that this yields the corrected heuristic density

$$\delta(S_a) = C_a \cdot \prod_\ell \left(1 - \frac{1}{[F_\ell : \mathbb{Q}]}\right) \quad \text{where} \quad C_a = \begin{cases} 1 + \prod_{\ell \mid 2\Delta} \frac{-1}{[F_\ell : \mathbb{Q}] - 1} & \text{if } \Delta \equiv 1 \bmod 4, \\ 1 & \text{if } \Delta \equiv 0 \bmod 4. \end{cases} \tag{5.3}$$

Hooley [Hoo67] proved in 1967 that, under the assumption of the Generalized Riemann Hypothesis for the Dedekind zeta function of the fields F_p, the primitive root density $\delta(S_a)$ exists and we have

$$\delta(S_a) = \sum_{n=1}^{\infty} \frac{\mu(n)}{[F_n : \mathbb{Q}]} \tag{5.4}$$

where $\mu(\cdot)$ denotes the Möbius function. It is not difficult to see (cfr. Theorem 5.4.4) that this sum is equal to the product appearing in (5.3).

There are many variants of the primitive root problem. We mention some of them here:

- **Primes in arithmetic progression with prescribed primitive root:** for a given $a \in \mathbb{Q}$ the problem asks for the density of the set of primes p lying in a given arithmetic progression such that a is a primitive root modulo p;

- **Near-primitive roots:** given a natural number $t \in \mathbb{N}$ and $a \in \mathbb{Q}$ the problem asks for the density of the set of primes p such that a mod p generates a subgroup of index exactly t in $\mathbb{F}_p^\times$ (in this sense a is a *near-primitive root*);

- **Higher rank Artin densities:** given a finite set $\{a_1, \dots, a_n\} \subseteq \mathbb{Q}$ the problem asks for the density of the set of primes p such that a_1 mod $p, \dots, a_n$ mod p generate the group $\mathbb{F}_p^\times$;

- Arbitrary combinations of the above problems, also formulated over more general number fields.

In all these cases, an heuristic argument à la Artin can be applied and the resulting conjectural densities has a shape very similar to (5.3), in the sense that they can be written as a product of a "naive density" δ_{naive} and a rational correction factor C. The character-sum method, described in a special case in the following section, allows to compute the constant C in a fairly mechanical way (see [LSM14]).

Also the cyclic reduction problem for elliptic curves involves the study of the splitting behaviour of prime ideals of a number field F in a family of Galois extensions $F \subseteq F_\ell$ for ℓ prime. However, the heuristic density has a very different shape according to whether the considered elliptic curve has complex multiplication or not. In the first case, a factorization as in (5.3) for the density may not exist, as we will show in Section 5.5.

5.2 Frobenius densities and the character-sum formula

Very often, when dealing with Artin-like problems, one is given a family $\mathcal{F} = \{F_\ell\}_\ell$ of finite Galois extensions of a fixed number field F indexed by prime numbers $\ell \in \mathbb{N}$ and, for each such prime ℓ, a non-empty subset $S_\ell \subseteq A_\ell := \operatorname{Gal}(F_\ell/F)$ which is stable under conjugation. The problem is then to determine, if it exists, the natural density of the set $\mathcal{P}$ of primes $\mathfrak{p} \subseteq F$ such that $\operatorname{Frob}_{F_\ell}(\mathfrak{p}) \subseteq S_\ell$ for all primes ℓ for which the Frobenius class $\operatorname{Frob}_{F_\ell}(\mathfrak{p}) \subseteq A_\ell$ is well-defined (*i.e.* for all primes ℓ for which the prime $\mathfrak{p}$ does not ramify in F_ℓ). Heuristically, one can proceed as follows: for a fixed $n \in \mathbb{N}$, let F_n be the compositum of all the fields F_ℓ for $\ell \mid n$. Then $G_n := \operatorname{Gal}(F_n/F)$ is naturally identified as a subgroup of the product $\prod_{\ell \mid n} A_\ell$ and by the Chebotarëv's density theorem the natural density of the set of primes $\mathfrak{p} \subseteq F$ such that $\operatorname{Frob}_{F_\ell}(\mathfrak{p}) \subseteq S_\ell$ for all $\ell \mid n$ (we can disregard the finitely many primes ramifying in F_n) is given by

$$\delta_n(\mathcal{P}) = \frac{\#(S_n \cap G_n)}{\# G_n}$$

where $S_n := \prod_{\ell \mid n} S_\ell$. By taking the limit as n goes to infinity by divisibility one obtains the heuristic density

$$\delta(\mathcal{P}) = \frac{\mu(S \cap G)}{\mu(G)} \tag{5.5}$$

where $G := \operatorname{Gal}(F_\infty/F)$ is the Galois group of the compositum F_∞ of the family $\{F_\ell\}_\ell$ and μ is the normalized Haar measure on $A = \prod_\ell A_\ell$, obtained as the product measure of the various normalized counting measures on the A_ℓ's. Making this heuristic precise is usually very hard, and even for the classical primitive root problem this is known only under the assumption of GRH.

Example 5.2.1. For every prime $\ell \in \mathbb{N}$ consider the Kummer extension $\mathbb{Q} \subseteq F_\ell := \mathbb{Q}(\zeta_\ell, \sqrt[\ell]{2})$ where $\zeta_\ell \in \overline{\mathbb{Q}}$ denotes a primitive ℓ-root of unity, and let $S_\ell := A_\ell \setminus \{1\}$. Then the family $\{F_\ell\}_\ell$ is linearly disjoint over $\mathbb{Q}$, hence $G = \operatorname{Gal}(F_\infty/F) = \prod_\ell A_\ell = A$ and the heuristic density (5.5) becomes

$$\delta(\mathcal{P}) = \frac{\mu(S)}{\mu(A)} = \prod_\ell \frac{\# S_\ell}{\# A_\ell} = \prod_\ell \left(1 - \frac{1}{[F_\ell : \mathbb{Q}]}\right).$$

The fact that we find back the heuristic Artin's primitive root density should not be of any surprise since for a prime $p \in \mathbb{Z}$ that is unramified in F_ℓ imposing the condition $\operatorname{Frob}_{F_\ell}(p) \in S_\ell$ is equivalent to requiring that p does not split completely in F_ℓ.

The previous example should not deceive the reader. In general, the family $\{F_\ell\}_\ell$ does not have any reason to be linearly disjoint over the base field F and this means that the computation of the heuristic density $\delta(\mathcal{P})$ may be very involved a priori. However, besides the case of linear disjointness, there is another situation where $\delta(\mathcal{P})$ can be easily determined. It is when the entanglement in $\mathcal{F}$ is finite quadratic, *i.e.* when there exists $m \in \mathbb{N}$ such that the family $\{F_m\} \cup \{F_\ell\}_{\ell \nmid m}$ is linearly disjoint over F and the inclusion $G_m \subseteq \prod_{\ell \mid m} A_\ell$ is of index 2. In order to explain how to compute $\delta(\mathcal{P})$ in this case, let us place in a slightly more general setting, whose notation has been chosen to be evocative of the context described so far.

For every $i \in \mathbb{N}$, let A_i be a profinite group and $A := \prod_{i \in \mathbb{N}} A_i$. Each A_i is a compact topological group and thus comes naturally endowed with a Haar measure μ_i, which we normalize in such a way that $\mu_i(A_i) = 1$. With this choice, the product measure $\mu = \prod_{i \in \mathbb{N}} \mu_i$ is also a normalized Haar measure on A. For each $i \in \mathbb{N}$ choose a μ_i-measurable subset $S_i \subseteq A_i$. Fix $\chi = \prod_{i\in\mathbb{N}} \chi_i : A \to \{\pm 1\}$ to be a non-trivial quadratic character obtained from a family of continuous quadratic characters $\chi_i : A_i \to \{\pm 1\}$ that are trivial for almost all $i \in \mathbb{N}$. If we let $G := \ker \chi$, then the integer

$$\delta_\chi(S) = \frac{\mu(G \cap S)}{\mu(G)}. \tag{5.6}$$

represents the proportion of elements of G that are contained in S.

Theorem 5.2.2. *If $\mu_i(S_i) > 0$ for all $i \in \mathbb{N}$ then*

$$\delta_\chi(S) = \left(1 + \prod_{i\in\mathbb{N}} \delta_i\right) \frac{\mu(S)}{\mu(A)}$$

where

$$\delta_i = \begin{cases} 1 & \text{if } A_i \subseteq G \\ -\frac{1}{\mu_i(S_i)} \int_{A_i \setminus S_i} \chi_i \, d\mu_i & \text{otherwise.} \end{cases} \tag{5.7}$$

Proof. We can assume that $\mu(S) = \prod_{i\in\mathbb{N}} \mu_i(S_i)$ is non-zero, since the theorem trivially holds otherwise. Let $\mathbb{1}_G : A \to \mathbb{R}$ be the indicator function of the group G. We have $\mathbb{1}_G = \frac{1+\chi}{2}$ because G equals the kernel of χ. Hence we can write

$$\delta_\chi(S) = \frac{1}{\mu(G)} \int_S \mathbb{1}_G \, d\mu = \frac{1}{\mu(G)} \int_S \frac{1+\chi}{2} \, d\mu = \frac{1}{2\mu(G)} \int_S (1+\chi) \, d\mu.$$

Since χ is non-trivial and the total space has measure $\mu(A) = \prod_{i\in\mathbb{N}} \mu_i(A_i) = 1$, we have $\mu(G) = 1/2$ and so

$$\delta_\chi(S) = \int_S (1+\chi) \, d\mu = \mu(S) + \int_S \chi \, d\mu = \mu(S) \left(1 + \frac{1}{\mu(S)} \int_S \chi \, d\mu\right) = \frac{\mu(S)}{\mu(A)} \left(1 + \frac{1}{\mu(S)} \int_S \chi \, d\mu\right).$$

In order to conclude, we need to study the integral appearing in the final equality. By Tonelli's theorem [Rud87, Theorem 8.8 (b), (c)], which we can apply because the characters χ_i are trivial for almost all $i \in \mathbb{N}$ and the total space has bounded measure, we have

$$\int_S \chi \, d\mu = \prod_{i\in\mathbb{N}} \int_{S_i} \chi_i \, d\mu \quad \text{hence} \quad \frac{1}{\mu(S)} \int_S \chi \, d\mu = \prod_{i\in\mathbb{N}} \frac{1}{\mu_i(S_i)} \int_{S_i} \chi_i \, d\mu_i$$

by the definition of product measure. We define $\delta_i = \frac{1}{\mu_i(S_i)} \int_{S_i} \chi_i \, d\mu_i$ and we claim that this is the same quantity appearing in the statement of the theorem. To see this, it suffices to write

$$\frac{1}{\mu_i(S_i)} \int_{S_i} \chi_i \, d\mu_i = \frac{1}{\mu_i(S_i)} \left(\int_{A_i} \chi_i \, d\mu_i - \int_{A_i \setminus S_i} \chi_i \, d\mu_i \right)$$

and apply the orthogonality relations

$$\int_{A_i} \chi_i \, d\mu_i = \begin{cases} \mu_i(A_i) = 1 & \text{if } \chi_i \text{ is trivial on } A_i, \\ 0 & \text{otherwise} \end{cases}$$

as in [Bum13, Theorem 2.5]. Since χ_i is trivial on A_i if and only if $A_i \subseteq G$, this concludes the proof. □

We now go back to our initial number field setting and notation, but we further assume that the entanglement in the family $\mathcal{F} = \{F_\ell\}_\ell$ is finite quadratic. In this case, we see that $G = \mathrm{Gal}(F_\infty/F)$ is obtained as the kernel of a non-trivial quadratic character $\chi = \prod_{i \in \mathbb{N}} \chi_\ell : A \longrightarrow \{\pm 1\}$ which is the product of a family of continuous quadratic characters $\chi_\ell : A_\ell \longrightarrow \{\pm 1\}$ that are trivial for almost all primes $\ell \in \mathbb{N}$. Noticing now that $\delta(\mathcal{P})$ as in (5.5) is equal to $\delta_\chi(S)$ as defined in (5.6), we can apply Theorem 5.2.2 and obtain

$$\delta(\mathcal{P}) = \left(1 + \prod_\ell \delta_\ell\right) \cdot \frac{\mu(S)}{\mu(A)} = C_{\mathcal{F}} \cdot \delta_{\text{naive}} \tag{5.8}$$

where δ_ℓ is defined in (5.7). We call $\delta_{\text{naive}} = \frac{\mu(S)}{\mu(A)} = \prod_\ell \frac{\#S_\ell}{\#A_\ell}$ the *naive density* of $\mathcal{P}$ because it is the density one would obtain if the family $\mathcal{F}$ were linearly disjoint over F. The rational number $C_{\mathcal{F}}$ is the *correction factor* to the naive density, and takes into account the quadratic entanglement in $\mathcal{F}$. We note that an expression of the form (correction factor)×(naive density) is always valid as long as the entanglement in $\mathcal{F}$ is finite. However, computing the correction factor may be more involved in the case the entanglement in the family $\mathcal{F}$ is not quadratic anymore.

If for every prime $\ell \in \mathbb{N}$ the set $N_\ell := A_\ell \setminus S_\ell$ is a *subgroup* of A_ℓ, then one has

$$\delta_\ell = \begin{cases} 1 & \text{if } A_\ell \subseteq G \\ 0 & \text{if } N_\ell \not\subseteq G \\ -\frac{\#N_\ell}{\#S_\ell} & \text{if } A_\ell \not\subseteq G \text{ and } N_\ell \subseteq G \end{cases}$$

as follows immediately from Theorem 5.2.2 and from the usual orthogonality relations for characters. In the special case where we take $S_\ell = A_\ell \setminus \{1\}$ for all primes $\ell \in \mathbb{N}$ equality (5.8) reads

$$\delta(\mathcal{P}) = \left(1 + \prod_\ell \frac{-1}{[F_\ell : F] - 1}\right) \prod_\ell \left(1 - \frac{1}{[F_\ell : F]}\right). \tag{5.9}$$

We call (5.9) the *character-sum formula* for the density $\delta(\mathcal{P})$.

5.3 Cyclic reduction of elliptic curves

Let E be an elliptic curve defined by an integral Weierstrass equation $y^2 = x^3 + Ax + B$ with coefficients A, B in the ring of integers $\mathcal{O}_F$ of a number field F. To E we associate its discriminant

$$\Delta_E = -16(4A^3 + 27B^2) \in \mathcal{O}_F \setminus \{0\}. \tag{5.10}$$

The primes $\mathfrak{p}$ of F coprime to Δ_E are the primes *of good reduction* of E. For such $\mathfrak{p}$, reduction modulo $\mathfrak{p}$ yields an elliptic curve $E_\mathfrak{p}$ over the residue class field $k_\mathfrak{p}$. Note that with this model of E, primes $\mathfrak{p}$ of F over 2 are never primes of good reduction.

We begin by formally stating the criterion for a prime $\mathfrak{p}$ of good reduction of (the given model of) E to be a *prime of cyclic reduction* of E, i.e., a prime for which the finite group $E_\mathfrak{p}(k_\mathfrak{p})$ is cyclic.

Lemma 5.3.1. *For a prime $\mathfrak{p}$ of good reduction of E, the following are equivalent:*

1. *$\mathfrak{p}$ is a prime of cyclic reduction of E;*

2. *for no prime number ℓ coprime to $\mathfrak{p}$, the prime $\mathfrak{p}$ splits completely in $F \subset F_\ell$, with $F_\ell := F(E[\ell])$ the ℓ-division field of E.*

Proof. Let $\mathfrak{p}$ be a prime of good reduction for E. Then $E_\mathfrak{p}(k_\mathfrak{p})$ is a cyclic group if and only if for no prime ℓ, its ℓ-torsion subgroup $E_\mathfrak{p}[\ell](k_\mathfrak{p})$ has order ℓ^2. For $\ell = \mathrm{char}(k_\mathfrak{p})$, it is a generality on elliptic curves in positive characteristic that the group $E_\mathfrak{p}[\ell](k_\mathfrak{p})$ is cyclic, so we further assume $\ell \neq \mathrm{char}(k_\mathfrak{p})$. Then $\mathfrak{p}$ is unramified in the Galois extension $F \subset F_\ell$ as it is a prime of good reduction of E coprime to ℓ.

The group $E[\ell](F_\ell)$ has order ℓ^2 by definition of F_ℓ, and at every prime $\mathfrak{q}|\mathfrak{p}$ of F_ℓ, the natural reduction map $E[\ell](F_\ell) \longrightarrow E_\mathfrak{q}(k_\mathfrak{q})$ is injective as $\mathfrak{q} \nmid \ell\Delta_E$ is a prime of good reduction of E in F_ℓ. Thus $E_\mathfrak{q}[\ell](k_\mathfrak{q})$ has order ℓ^2. Now $k_\mathfrak{q}$ is generated over $k_\mathfrak{p}$ by the coordinates of the points in $E_\mathfrak{q}[\ell](k_\mathfrak{q})$, as $F \subset F_\ell$ is generated by the coordinates of the ℓ-torsion points of E. It follows that the natural inclusion $k_\mathfrak{p} \subset k_\mathfrak{q}$ is an equality for all $\mathfrak{q}|\mathfrak{p}$ in F_ℓ, i.e., $\mathfrak{p}$ splits completely in $F \subset F_\ell$, if and only each of the natural inclusions $E_\mathfrak{p}[\ell](k_\mathfrak{p}) \subset E_\mathfrak{q}[\ell](k_\mathfrak{q})$ is an equality. As $E_\mathfrak{q}[\ell](k_\mathfrak{q})$ has order ℓ^2, this proves the lemma. □

If $\mathfrak{p}$ is a prime of good reduction of E of characteristic p coprime to the discriminant Δ_F of F, then $\mathfrak{p}$ can not split completely in the division field F_p, as it is totally ramified in the subextension $F \subset F(\zeta_p)$ of degree $p - 1 > 1$ of F_p that is generated by a primitive p-th root of unity ζ_p. This shows that, for primes $\mathfrak{p}$ coprime to both Δ_E and Δ_F, being in the set $S_{E/F}$ of primes of cyclic reduction of E is tantamount to *not* splitting completely in any division field extension $F \subset F_\ell$ at a rational prime ℓ.

Corollary 5.3.2. *For a prime $\mathfrak{p} \nmid \Delta_E\Delta_F$, we have $\mathfrak{p} \in S_{E/F}$ if and only if $\mathfrak{p}$ does not split completely in any of the division fields F_ℓ, with $\ell \in \mathbb{Z}$ prime.*

The proof of Lemma 5.3.1 shows that if a prime $\mathfrak{p} \nmid \Delta_E\Delta_F$ splits completely in $F \subset F_\ell$, then $E_\mathfrak{p}(k_\mathfrak{p})$ has complete ℓ-torsion, so we have $\ell \leq \sqrt{N_{F/\mathbb{Q}}(\mathfrak{p})} + 1$ by the Hasse-Weil bound. For a squarefree integer m and a prime $\mathfrak{p} \nmid \Delta_E\Delta_F$, we similarly obtain

$$\mathfrak{p} \nmid \Delta_E\Delta_F \text{ splits completely in } F_m = F(E[m]) \Longrightarrow m \leq \sqrt{N_{F/\mathbb{Q}}(\mathfrak{p})} + 1. \tag{5.11}$$

Using the characterization of the primes of cyclic reduction given by Corollary 5.3.2, we want to show that under GRH the set $S_{E/F}$ has a natural density $\delta_{E/F}$ that, at least typographically, is identical to Artin's primitive root density appearing in (5.4).

Theorem 5.3.3. *Let E be an elliptic curve defined over a number field F. Under GRH, the set $S_{E/F}$ of primes of F of cyclic reduction has the density $\delta_{E/F}$ defined by*

$$\delta_{E/F} = \sum_{m=1}^{\infty} \frac{\mu(m)}{[F_m : F]}. \tag{5.12}$$

Remark 5.3.4. For $F = \mathbb{Q}$, Serre showed that, under GRH, the set $S_{E/\mathbb{Q}}$ does have density $\delta_{E/\mathbb{Q}}$ as in (5.12). His proof, which is along Hooley's lines, was published in 1983 by Murty [Mur83].

In order to count the cardinality $\#S_{E/F}(x)$ of primes $\mathfrak{p}$ in the set $S_{E/F}$ of good reduction of norm $N_{F/\mathbb{Q}}(\mathfrak{p}) \leq x \in \mathbb{R}_{>0}$, we introduce the counting function

$$\pi_F(x, F_m) = \#\{\mathfrak{p} \nmid \Delta_E\Delta_F : \ N_{F/\mathbb{Q}}(\mathfrak{p}) \leq x \text{ and } \mathfrak{p} \text{ splits completely in } F \subseteq F_m\}.$$

The function $\pi_F(x, F)$ counts primes $\mathfrak{p} \nmid \Delta_F$ of good reduction of E of norm at most x, and, disregarding the primes $\mathfrak{p}|\Delta_F$ in $S_{E/F}$, Corollary 5.3.2 and inclusion-exclusion yield

$$\#S_{E/F}(x) = \sum_{m=1}^{\infty} \mu(m)\pi_F(x, F_m). \tag{5.13}$$

Note that by (5.11), the function $\pi_F(x, F_m)$ vanishes for $m > \sqrt{x} + 1$, so the infinite sum of integers in (5.13) is actually finite, and therefore convergent.

In order to obtain the desired asymptotic relation $\#S_{E/F}(x) \sim \delta_{E/F} \cdot x/\log x$ claimed in Theorem 5.3.3, we want to use the asymptotic relations $\pi_F(x, F_m) \sim \frac{1}{[F_m:F]} \cdot x/\log x$. Dividing both sides in (5.13) by $x/\log x$, proving the theorem comes down to interchanging the infinite sum and the limit $x \longrightarrow \infty$ in the right hand side of (5.13). This requires GRH to bound the error terms in these asymptotic relations, and a variant of Hooley's argument in [Hoo67]. Murty [Mur83, Theorem 1] has shown that in this setting, one can prove under GRH that the inclusion-exclusion density is correct if $[F_m : F]$ grows sufficiently rapidly with m (as it does in our case) and *two* conditions are satisfied. The first condition is that the root discriminant of the division fields F_m does not grow too rapidly with m, as follows.

Proposition 5.3.5. *For $m \in \mathbb{Z}_{>0}$ tending to infinity, we have*

$$\frac{1}{[F_m : F]} \log|\Delta_{F_m}| = \mathrm{O}(\log m)$$

Note that the quantity in the Proposition is $[F : \mathbb{Q}]$ times the logarithm of the ordinary root discriminant $|\Delta_{F_m}|^{1/[F_m:\mathbb{Q}]}$.

The second condition is that 'not too many' primes $\mathfrak{p}$ of F split in the division fields F_ℓ for 'large' primes ℓ, in the following sense.

Proposition 5.3.6. *The number of primes $\mathfrak{p}$ of F of norm $N_{F/\mathbb{Q}}(\mathfrak{p}) \leq x$ that split completely in $F \subset F_\ell$ for some prime $\ell > \frac{x^{1/2}}{\log^2 x}$ is $\mathrm{o}(\frac{x}{\log x})$ for $x \longrightarrow \infty$.*

Proof of Proposition 5.3.5. Bounding absolute root discriminants already dates back to Hensel [Ser79, pag.58]. For the relative extension $F \subset F_m$ we can use the version found in [MM97, pag. 44]. It states that for a finite Galois extension of number fields $F \subset L$ with relative discriminant $\Delta_{L/F}$ of norm $D(L/F) = N_{F/\mathbb{Q}}(\Delta_{L/F}) \in \mathbb{Z}_{>0}$, we have

$$\log D(L/F) \leq ([L : \mathbb{Q}] - [F : \mathbb{Q}]) \sum_{p|D(L/F)} \log p + [L : \mathbb{Q}] \log([L : F]). \tag{5.14}$$

As the absolute discriminant of L equals $|\Delta_L| = D(L/F)|\Delta_F|^{[L:F]}$, the identity

$$\log D(L/F) = \log|\Delta_L| - [L : F] \log|\Delta_F|$$

can be combined with the inequality (5.14) in the case $L = F_m$ to obtain, after division by $n(m) = [F_m : F]$, the estimate

$$\begin{aligned}\frac{1}{n(m)}\log|\Delta_{F_m}| - \log|\Delta_F| &\leq \frac{[F_m:\mathbb{Q}]-[F:\mathbb{Q}]}{n(m)}\sum_{p|D(F_m/F)}\log p + \frac{[F_m:\mathbb{Q}]}{n(m)}\log n(m)\\ &\leq [F:\mathbb{Q}]\cdot\big(\sum_{p|D(F_m/F)}\log p + \log n(m)\big).\end{aligned}$$

The primes $p|D(F_m/F)$ either divide m, or they lie under one of the finitely many primes of bad reduction of E, so we have $\sum_{p|D(F_m/F)}\log p \leq C_E + \log m$ for some constant C_E depending only on E. We obtain

$$\frac{1}{n(m)}\log|\Delta_{F_m}| \leq [F:\mathbb{Q}]\cdot\big(\log|\Delta_F| + C_E + \log m + \log n(m)\big).$$

As we have $n(m) = \mathrm{O}(m^4)$, this yields the desired asymptotic relation. □

Proof of Proposition 5.3.6. When showing that the cardinality of the set of primes $\mathfrak{p}$ of F of norm $N_{F/\mathbb{Q}}(\mathfrak{p}) \leq x$ that split completely in $F \subset F_\ell$ for some prime $\ell > \frac{x^{1/2}}{\log^2 x}$ is asymptotically $\mathrm{o}(\frac{x}{\log x})$, we may disregard primes $\mathfrak{p}|\Delta_F\Delta_E$, as they are finite in number, and primes $\mathfrak{p}$ that are not of degree 1, as there are no more than $\mathrm{o}(\sqrt{x})$ of them.

Suppose now that $\mathfrak{p} \nmid \Delta_F\Delta_E$ is of prime norm $N_{F/\mathbb{Q}}(\mathfrak{p}) = p \leq x$, and that $\mathfrak{p}$ splits completely in an ℓ-division field F_ℓ with $\ell > 2$. By (5.11), this implies $\ell \leq \sqrt{x}+1$. As $\mathfrak{p} \nmid \Delta_F$ necessarily splits completely in the subextension $F \subset F(\zeta_\ell)$, we have $\mathfrak{p} \nmid \ell$, and $\mathfrak{p}$ lies over a rational prime $p \equiv 1 \bmod \ell$. Any such p gives rise to at most $[F:\mathbb{Q}]$ primes $\mathfrak{p}$ in F of norm p. Thus, the number $B(x)$ of such $\mathfrak{p}$ can be bounded by

$$B(x) \leq [F:\mathbb{Q}]\cdot \sum_{\frac{x^{1/2}}{\log^2 x}<\ell<x^{1/2}+1} \pi(x,1,\ell), \tag{5.15}$$

with $\pi(x,1,\ell)$ denoting the number of primes $p \leq x$ satisfying $p \equiv 1 \bmod \ell$. By the Brun-Titchmarsh theorem, we have

$$\pi(x,1,\ell) \leq \frac{2x}{\varphi(\ell)\log(\frac{x}{\ell})} \ll \frac{x}{\ell\log(\frac{x}{\ell})},$$

so we obtain

$$B(x) \ll \sum_{\frac{x^{1/2}}{\log^2 x}<\ell<x^{1/2}+1}\frac{x}{\ell\log(\frac{x}{\ell})} \ll \frac{x}{\log(x)}\cdot\sum_{\frac{x^{1/2}}{\log^2 x}<\ell<x^{1/2}+1}\frac{1}{\ell}.$$

It now suffices to show that

$$\sum_{\frac{x^{1/2}}{\log^2 x}<\ell<x^{1/2}}\frac{1}{\ell}$$

tends to zero for $x \longrightarrow \infty$. This follows from the well-known estimate [Apo76, Theorem 4.12]

$$\sum_{\ell\leq X,\ \ell\text{ prime}}\frac{1}{\ell} = \log\log X + C + \mathrm{O}\left(\frac{1}{\log X}\right) \tag{5.16}$$

with C some absolute positive constant. Applying (5.16) for $X = x^{1/2}$ and $X = \frac{x^{1/2}}{\log^2 x}$ and subtracting, we do obtain a quantity tending to zero for $x \to \infty$:

$$\begin{aligned} \sum_{\frac{x^{1/2}}{\log^2 x} < \ell < x^{1/2}} \frac{1}{l} &= \log\log x^{1/2} - \log\log\left(\frac{x^{1/2}}{\log^2 x}\right) + \mathrm{O}\left(\frac{1}{\log x^{1/2}}\right) \\ &= \log\left(\frac{\frac{1}{2}\log x}{\frac{1}{2}\log x - 2\log\log x}\right) + \mathrm{O}\left(\frac{1}{\log x}\right). \end{aligned}$$ □

Proof of Theorem 5.3.3. By [Mur83, Theorem 1], this follows from Propositions 5.3.5 and 5.3.6. □

The number $\delta_{E/F}$ in (5.12) is defined by a series that converges rather slowly, and it is unclear when it vanishes. We thus seek for a representation as an infinite product in the spirit of (5.3). This will not always be possible, as we will show in the subsequent sections, and the existence of a product representation for $\delta_{E/F}$ crucially depends on whether the elliptic curve E has complex multiplication or not. We will discuss the two cases separately.

5.4 Non-CM cyclic reduction densities

The first goal of this section is to show that the cyclic reduction density $\delta_{E/F}$ associated to a non-CM elliptic curve E defined over a number field F can be expressed as a product of a naive density $A_{E/F}$ and an entanglement correction factor $\alpha_{E/F}$. This result, which is analogous to the factorization (5.3) in Artin's primitive root conjecture, follows from a study of the entanglement in the family $\{F_\ell\}_\ell$ of ℓ-division fields of E for $\ell \in \mathbb{N}$ prime. We keep the notation as in the previous section.

Theorem 5.4.1. *Let F be a number field, $E_{/F}$ an elliptic curve without complex multiplication, and $N = N(E, F) \in \mathbb{Z}_{>0}$ be the product of all prime numbers ℓ satisfying one of*

1. *$\ell \mid 2 \cdot 3 \cdot 5 \cdot \Delta_F$;*
2. *ℓ lies below a prime of bad reduction of E;*
3. *the Galois group $\mathrm{Gal}(F_\ell/F)$ is not isomorphic to $\mathrm{GL}_2(\mathbb{F}_\ell)$.*

Then for any $N' \in \mathbb{N}$ which is divisible by N, the family consisting of $F_{N'}$ and $\{F_\ell\}_{\ell \nmid N'}$ is linearly disjoint over F.

The proof of Theorem 5.4.1 relies on a group theoretical result on the Jordan-Hölder factors that can occur in subgroups of $H \subset \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$.

Lemma 5.4.2. *Let $N \in \mathbb{Z}_{>0}$ be an integer and $H \subset \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ a subgroup. Suppose S is a non-abelian simple group that occurs in H. Then S is isomorphic to either A_5 or $\mathrm{PSL}_2(\mathbb{F}_\ell)$, with ℓ a prime dividing N.*

Proof. We may assume $H \subset \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z}) = \prod_{\ell \mid N} \mathrm{SL}_2(\mathbb{Z}/\ell\mathbb{Z})$ as we only care about non-abelian simple Jordan-Hölder factors. In addition, we may assume that N is squarefree, i.e., equal to its own radical $N_0 = \mathrm{rad}(N)$; indeed, the natural map $r : \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z}) \to \mathrm{SL}_2(\mathbb{Z}/N_0\mathbb{Z})$ has a solvable kernel that is a product of ℓ-groups, and the groups H and $H/(H \cap \ker r) \subset \mathrm{SL}_2(\mathbb{Z}/N_0\mathbb{Z})$ have the same non-abelian simple Jordan-Hölder factors. Thus, every non-abelian simple group that occurs in H occurs in a subgroup of some $\mathrm{SL}_2(\mathbb{Z}/\ell\mathbb{Z})$, so we can reduce to the case that $N = \ell$ is prime. In this case the statement is a classical result that can be found in [Ser89, p. IV-23]. □

Proof of Theorem 5.4.1. It suffices to show that for a number N' divisible by $N(E,F)$ and $\ell \nmid N'$ a prime number, we have $F_{N'} \cap F_\ell = F$. Take such N' and ℓ. Then $\ell \nmid N'$ is unramified in the tower $\mathbb{Q} \subset F \subset F_{N'}$ by (2), and since $F \subset F(\zeta_\ell)$ is totally ramified over ℓ of degree $\ell - 1 > 1$ by (1), the fields $F_{N'}$ and $F(\zeta_\ell)$ are F-linearly disjoint. It now suffices to prove that the normal extensions $F(\zeta_\ell) \subset F_\ell$ and $F(\zeta_\ell) \subset F_{N'}(\zeta_\ell)$ are linearly disjoint.

We have $\mathrm{Gal}(F_\ell/F(\zeta_\ell)) \cong \mathrm{SL}_2(\mathbb{F}_\ell)$ by (3), and for $\ell \geq 5$ this group has a unique non-trivial normal subgroup $\{\pm\mathrm{id}_\ell\}$ with simple quotient $\mathrm{PSL}_2(\mathbb{F}_\ell)$. If $F_\ell \cap F_{N'}(\zeta_\ell)$ is not equal to $F(\zeta_\ell)$, we find that the non-abelian simple group $\mathrm{PSL}_2(\mathbb{F}_\ell)$, which is not A_5 as we assume $\ell \neq 5$ by (1), is a Jordan-Hölder factor of $\mathrm{Gal}(F_{N'}(\zeta_\ell)/F(\zeta_\ell)) \cong \mathrm{Gal}(F_{N'}/F)$. As we can view $\mathrm{Gal}(F_{N'}/F)$ as a subgroup of $\mathrm{GL}_2(\mathbb{Z}/N'\mathbb{Z})$, this contradicts Lemma 5.4.2, since we have $\ell \nmid N'$. □

For the purposes of this chapter, we only need to apply Theorem 5.4.1 for squarefree values of N. We can however strengthen its conclusion a bit and reformulate it in the following way, as a non-CM analogue of Theorem 4.3.4.

Theorem 5.4.3. *Let F be a number field, $E_{/F}$ an elliptic curve without CM, and S the set of prime numbers ℓ satisfying one of*

1. *$\ell \mid 2 \cdot 3 \cdot 5 \cdot \Delta_F$;*
2. *ℓ lies below a prime of bad reduction of E;*
3. *the Galois group $\mathrm{Gal}(F_\ell/F)$ is not isomorphic to $\mathrm{GL}_2(\mathbb{F}_\ell)$.*

Write F_{ℓ^∞} for the compositum of all ℓ-power division fields of E over F, and F_S for the compositum of the fields F_{ℓ^∞} with $\ell \in S$. Then the family consisting of F_S and $\{F_{\ell^\infty}\}_{\ell \notin S}$ is linearly disjoint over F.

Proof. It suffices to show that for N an integer divisible by all primes in S and $\ell \nmid N$ prime, we have $F_N \cap F_{\ell^n} = F$ for every $n \in \mathbb{Z}_{>0}$. For $n = 1$, this is Theorem 5.4.1.

As $F \subset F_N$ is unramified over $\ell \nmid N$ by condition (2), the intersection is F-linearly disjoint from $F(\zeta_{\ell^n})$ by the condition $\ell \nmid \Delta_F$ in (1), and it is F-linearly disjoint from F_ℓ by Theorem 5.4.1. It therefore corresponds to a subgroup of $\mathrm{Gal}(F_{\ell^n}/F) \subset \mathrm{GL}_2(\mathbb{Z}/\ell^n\mathbb{Z})$ that maps surjectively to $\mathrm{Gal}(F_\ell/F) = \mathrm{GL}_2(\mathbb{F}_\ell)$ by (3) and has surjective image $(\mathbb{Z}/\ell^n\mathbb{Z})^*$ under the determinant map. By a result of Serre [Ser89, p. IV-23, Lemma 3], valid for $\ell \geq 5$, such a group is the full group $\mathrm{GL}_2(\mathbb{Z}/\ell^n\mathbb{Z})$, proving $F_N \cap F_{\ell^n} = F$. □

We are now ready to prove the factorization theorem for non-CM cyclic reduction densities.

Theorem 5.4.4. *Let $E_{/F}$ be an elliptic curve without CM. If $N = N(E,F) \in \mathbb{Z}_{>0}$ is the integer appearing in Theorem 5.4.1, then $\delta_{E/F}$ can be factored as*

$$\delta_{E/F} = \alpha_{E/F} \cdot A_{E/F} \tag{5.17}$$

where

$$\alpha_{E/F} = \left(\sum_{m|N} \frac{\mu(m)}{[F_m : F]} \right) \quad \text{and} \quad A_{E/F} = \prod_{\ell \nmid N,\ \ell \text{ prime}} \left(1 - \frac{1}{[F_\ell : F]} \right).$$

Remark 5.4.5. In the spirit of Section 5.2 we call $A_{E/F}$ the *naive density* associated to E and $\alpha_{E/F}$ the *entanglement correction factor.*

Proof. First of all, notice that $\delta_{E/F}$ is the limit of the finite sums

$$\delta_{E/F}(n) = \sum_{m|n} \frac{\mu(m)}{[F_m : F]} \tag{5.18}$$

for n tending to infinity under the partial ordering of divisibility. Under this ordering, we have

$$m|n \Longrightarrow \delta_{E/F}(m) \geq \delta_{E/F}(n) \geq 0, \tag{5.19}$$

so the limit exists and is non-negative. We now simply note that the quantity $\delta_{E/F}(n)$ in (5.18) is the inclusion-exclusion fraction of elements in the Galois group $\mathrm{Gal}(F_n/F)$ that have non-trivial restriction on every subfield F_ℓ with $\ell|N$. Thus, if n_1 and n_2 are coprime numbers for which the division fields F_{n_1} and F_{n_2} are F-linearly disjoint, we have an equality $\delta_{E/F}(n_1n_2) = \delta_{E/F}(n_1)\delta_{E/F}(n_2)$. If N' is any squarefree multiple of the number $N = N(E,F)$ in Theorem 5.4.1, this yields

$$\delta_{N'}(E) = \delta_N(E) \cdot \prod_{\ell|N'/N,\ \ell \text{ prime}} \left(1 - \frac{1}{[F_\ell : F]}\right).$$

Taking the limit $N' \to \infty$ with respect to the divisibility ordering yields Theorem 5.4.4. □

As almost all division fields F_ℓ for E without CM have maximal degree $(\ell^2-1)(\ell^2-\ell)$, it follows from Theorem 5.4.4 that, just as for $\delta(S_a)$ in (5.2), the number $\delta_{E/F}$ can be written as a product

$$\delta_{E/F} = c_{E/F} \cdot A_\infty \tag{5.20}$$

of a rational number $c_{E/F} \in \mathbb{Q}_{\geq 0}$ and a universal non-CM elliptic Artin constant

$$A_\infty = \prod_{\ell \text{ prime}} \left(1 - \frac{1}{(\ell^2-1)(\ell^2-\ell)}\right) \approx 0.8137519. \tag{5.21}$$

We have $c_{E/F} = 1$ when the division fields F_ℓ for ℓ prime all assume the maximal degree *and* they form a linearly disjoint family over F. The first condition is often not satisfied, and for this reason Theorem 5.4.4 gives a more satisfactory decomposition than (5.20).

From the factorization (5.17), it is clear that there are two possible causes for the vanishing of $\delta_{E/F}$. If the naive density $A_{E/F}$ vanishes, at least one ℓ-division field F_ℓ is equal to F. For such ℓ, the full ℓ-torsion of E is defined over F, and therefore over almost all residue class fields $k_\mathfrak{p}$, making $S_{E/F}$ finite. We call this the *trivial vanishing* of the density. Note that $F = F_\ell$ can only occur for primes $\ell|2\Delta_F$.

The more subtle cause of vanishing of $\delta_{E/F}$ that we refer to as *non-trivial vanishing* occurs when we have

$$\delta_{E/F} = 0 \quad \text{and} \quad A_{E/F} > 0, \tag{5.22}$$

i.e., when the naive density $A_{E/F}$ is positive but the entanglement correction factor $\alpha_{E/F}$ vanishes. In this case all F_ℓ are different from F, but the non-splitting conditions in the various F_ℓ cannot be satisfied simultaneously. Murty proved [GM90, Theorem 1] that non-trivial vanishing does not happen for $F = \mathbb{Q}$: we have $\delta_{E/\mathbb{Q}} = 0$ if and only if E has full 2-torsion over $\mathbb{Q}$. Over a general number field F, non-trivial vanishing of $\delta_{E/F}$ is a rare occurrence, but we can make it happen by base changing elliptic curves E defined over a small field such as $\mathbb{Q}$ to a well-chosen number field.

The underlying idea is the following: one starts with a non-CM elliptic curve $E_{/F}$ and considers it over an extension $F \subset F'$ for which the ℓ-division fields F'_ℓ of E over F' for primes ℓ_1, ℓ_2, and ℓ_3 are different *quadratic* extensions of F', but with compositum $F'_{\ell_1\ell_2\ell_3}$ a multi-quadratic extension of F' of degree 4, and not 8. In this case, no prime of F' can be inert in all three subextensions F'_ℓ, and almost all reduced curves at primes of F' will have complete ℓ-torsion for at least one value $\ell \in \{\ell_1, \ell_2, \ell_3\}$, implying that $S_{E/F'}$ is finite. The construction has many degrees of freedom, leading to infinitely many different curves and number fields for which non-trivial vanishing as in (5.22) occurs.

Theorem 5.4.6. *Let E be an elliptic curve without CM defined over a number field F, with naive density $A_{E/F} > 0$. Then for any finite normal extension $F \subset L$, there exists a linearly disjoint normal extension $F \subset F'$ for which $\delta_{E/F'}$ vanishes non-trivially.*

Proof. Let $N = N(E, F)$ be as in Theorem 5.4.1. Then the N-division field F_N and the ℓ-division fields F_ℓ at $\ell \nmid N$ of E form a linearly disjoint family over F. Now let $F \subset L$ be a finite normal extension, and replace F_N by the compositum LF_N. Then the family may no longer be F-linearly disjoint, but it becomes F-linearly disjoint again after leaving out finitely many well-chosen F_ℓ from the family. This is because any finite extension of F contained in the compositum of some F-linearly disjoint family of division fields F_ℓ is contained in the compositum of *finitely many* F_ℓ, and these are the ones that we leave out.

Now pick *any* set $\{\ell_1, \ell_2, \ell_3\}$ of primes that have not been left out. Then the $\ell_1\ell_2\ell_3$-division field $F_{\ell_1\ell_2\ell_3}$ of E is Galois over F with group

$$G = \mathrm{GL}_2(\mathbb{Z}/\ell_1\ell_2\ell_3\mathbb{Z}) = \prod_{i=1}^{3} \mathrm{GL}_2(\mathbb{F}_{\ell_i}).$$

Every $\mathrm{GL}_2(\mathbb{F}_{\ell_i})$ contains a normal subgroup $\langle -1 \rangle$ generated by $-\mathrm{id}_{\ell_i} \in \mathrm{GL}_2(\mathbb{F}_{\ell_i})$, so the center of G contains an elementary abelian 2-group $H' = \prod_{i=1}^{3} \langle -1 \rangle \subset G$ of order 8. We let $H \subset H'$ be the 'norm-1-subgroup' of order 4 consisting of elements $(e_i)_{i=1}^3 \in H$ with $e_1e_2e_3 = 1$. Then H is normal in G, and we take for F' the invariant field $F' = F_{\ell_1\ell_2\ell_3}^H$.

We now view E as an elliptic curve over the finite normal extension F' of F, and note that the division field $F'_{\ell_1\ell_2\ell_3} = F_{\ell_1\ell_2\ell_3}$ is by construction Galois over F' with group isomorphic to the Klein four-group H. As every non-trivial element of H is the identity on exactly one of the division fields F'_{ℓ_i}, the three intermediate quadratic extensions of $F' \subset F'_{\ell_1\ell_2\ell_3}$ are the division fields F'_{ℓ_i}, and no prime of F' will be inert in all three of them. This implies that we have $\delta_{E/F'} = 0$.

As the naive density $A_{E/F'}$ differs from $A_{E/F} > 0$ only in the three factors corresponding to the primes ℓ_i, with the degree $[F_{\ell_i} : F] = \#\,\mathrm{GL}_2(\mathbb{F}_{\ell_i})$ being replaced by $[F'_{\ell_i} : F'] = 2$, we still have $A_{E/F'} > 0$, so the vanishing of $\delta_{E/F'}$ is non-trivial. □

Remark 5.4.7. Our proof of Theorem 5.4.6 only uses the fact that $-\mathrm{id}_{\ell_i}$ is contained in $\mathrm{Gal}(F_{\ell_i}/F) \subset \mathrm{GL}_2(\mathbb{F}_{\ell_i})$, and that the Klein four-group H in the proof is contained in $G = \mathrm{Gal}(F_{\ell_1\ell_2\ell_3}/F) \subset \prod_{i=1}^3 \mathrm{GL}_2(\mathbb{F}_{\ell_i})$. This observation is useful when constructing an explicit example of an elliptic curve E over a "small" normal number field F' for which $\delta_{E/F'}$ vanishes non-trivially. If one does not insist on F' being normal over $F = \mathbb{Q}$, one can use any element of order 2 in $\mathrm{Gal}(F_{\ell_i}/F) \subset \mathrm{GL}_2(\mathbb{F}_{\ell_i})$ instead of $-\mathrm{id}_{\ell_i}$, and use small primes ℓ_i for which F_{ℓ_i} is of small degree.

Example 5.4.8. The elliptic curve E defined over $F = \mathbb{Q}$ by the minimal Weierstrass equation

$$y^2 + xy + y = x^3 - 76x + 298$$

has discriminant $\Delta_E = -2^5 \cdot 5^8$ and, according to [LMFDB], its mod ℓ Galois representations are maximal at $\ell \neq 3, 5$. The division field F_3 is non-abelian of degree 6, smaller than the generic degree $48 = \#\,\mathrm{GL}_2(\mathbb{Q}_3)$, and at $\ell = 5$ it is Galois with group $A_{20} = C_5 \rtimes \mathrm{Aut}(C_5)$, the affine group over $\mathbb{Q}_5$ of order 20, much smaller than the generic group $\mathrm{GL}_2(\mathbb{Q}_5)$ of order 480. As the division fields F_2 and F_3 are non-abelian of degree 6 with different quadratic subfields $\mathbb{Q}(\sqrt{\Delta_E}) = \mathbb{Q}(\sqrt{-2})$ and $\mathbb{Q}(\zeta_3)$, they are linearly disjoint over $F = \mathbb{Q}$. As F_6 and F_5 are solvable extensions of $\mathbb{Q}$ with maximal abelian subfields $\mathbb{Q}(\sqrt{-2}, \zeta_3)$ and $\mathbb{Q}(\zeta_5)$ that are linearly disjoint over $\mathbb{Q}$, the division fields F_2, F_3 and F_5 are $\mathbb{Q}$ linearly disjoint of even degree, so $\mathrm{Gal}(F_{30}/\mathbb{Q}) \cong S_3 \times S_3 \times A_{20}$ does contain an elementary abelian 2-subgroup H' of order 8 as in the proof of Theorem 5.4.6. We can therefore find a non-normal field F' of degree $[F' : \mathbb{Q}] = 6 \cdot 6 \cdot 20/4 = 180$ inside F_{30} for which $\delta_{E/F'}$ vanishes non-trivially.

We do not know whether there exist examples of non-trivial vanishing over number fields of degree less than 180. We also do not know if there are non-CM examples that do not arise by base change, i.e., an example in which $\delta_{E/F}$ vanishes non-trivially for $F = \mathbb{Q}(j(E))$ and E without complex multiplication. On the other hand, if E has complex multiplication and is defined over $\mathbb{Q}(j(E))$, we will see in Section 5.6 that $\delta_{E/F}$ never vanishes trivially.

5.4.1 Some numerical examples

In order to compute $\delta_{E/F} = \alpha_{E/F} \cdot A_{E/F}$ for a non-CM elliptic curve $E_{/F}$ as in (5.17), one starts by finding $[F_\ell : F]$ at all primes ℓ where F_ℓ has non-maximal degree. This easily can be done for small examples using [LMFDB], which provides a list of non-maximal degrees $[F_\ell : F]$. This enables us to find the naive density $A_{E/F}$ as a rational multiple of the universal constant A_∞ from (5.21). Typically, $A_{E/F}$ has a value close to $\delta_{E/F}$, and its approximate correctness can be confirmed by a computer count of the fraction of primes of cyclic reduction among primes of norm below some modest bound. Finding the exact entanglement correction factor $\alpha_{E/F}$ can be more complicated. It typically involves group theory and ramification arguments. This section provides some easy examples.

We treat the five non-CM elliptic curves $E_{/\mathbb{Q}}$ listed in the table below. There are 78,498 rational primes below 10^6, and the table lists the number of them that give rise to cyclic reduction, and the fraction $d(E)$ this represents. The computations have been performed using [SAGE].

E	$p < 10^6$ of cyclic reduction	$d(E)$
$y^2 = x^3 - 3x + 1$	51,105	0.6510
$y^2 = x^3 + 2x + 3$	38,383	0.4889
$y^2 = x^3 - 12096x - 544752$	32,652	0.4159
$y^2 = x^3 + x + 3$	63,910	0.8141
$y^2 = x^3 - 13392x - 1080432$	48,026	0.6118

Example 5.4.9. For the elliptic curve $E_{/\mathbb{Q}}$ with LMFDB label 1296.e1 defined by

$$E : y^2 = x^3 - 3x + 1$$

we have $\Delta_E = 2^4 \cdot 3^4$, and F_2, the splitting field of the polynomial $x^3 - 3x + 1$ of discriminant 3^4, is the real subfield of $\mathbb{Q}(\zeta_9)$, which is cubic, and not of maximal degree 6. All other division fields F_ℓ have maximal degree, so the naive density equals

$$A_{E/\mathbb{Q}} = \prod_{\ell \text{ prime}} \left(1 - \frac{1}{[F_\ell : \mathbb{Q}]}\right) = \frac{2}{3} \cdot \frac{6}{5} \cdot A_\infty \approx 0.6510015.$$

The cyclic cubic field F_2 is not a subfield of F_3 as $\mathrm{Gal}(F_3/\mathbb{Q}) \cong \mathrm{GL}_2(\mathbb{F}_3)$ has no quotient of order 3, so F_6 is a linearly disjoint compositum of F_2 and F_3. We have $F_6 \cap F_5 = F$ as the intersection is solvable over F, but does not contain $\sqrt{5} \notin F_6$. As we can take $N(E, \mathbb{Q}) = 2 \cdot 3 \cdot 5$ in Theorem 5.4.1, we find that the family of ℓ-division fields F_ℓ is $\mathbb{Q}$-linearly disjoint. In this case there is no entanglement correction, and $\delta_{E/\mathbb{Q}}$ is equal to the naive density $A_{E/\mathbb{Q}}$. The numerical agreement is excellent.

Example 5.4.10. The elliptic curve $E_{/\mathbb{Q}}$ with LMFDB label 880.e2 defined by

$$E : y^2 = x^3 + 2x + 3 = (x + 1)(x^2 - x + 3)$$

of discriminant $\Delta_E = -2^4 \cdot 5^2 \cdot 11$ has a unique rational torsion point of order 2, and $F_2 = \mathbb{Q}(\sqrt{-11})$. For $\ell > 2$, the degree of F_ℓ is maximal, so the naive density equals

$$A_{E/\mathbb{Q}} = \frac{1}{2} \cdot \frac{6}{5} \cdot A_\infty \approx 0.48825114.$$

We can take $N(E, \mathbb{Q}) = 2 \cdot 3 \cdot 5 \cdot 11$ in Theorem 5.4.1. As F_2 is not the unique quadratic subfield $\mathbb{Q}(\zeta_3)$ of F_3, the extension F_6 is a linearly disjoint compositum of F_2 and F_3. Again, F_6 is solvable and does not contain $\sqrt{5}$, so it is linearly disjoint from F_5.

We now know that the family of division fields $\{F_\ell\}_{\ell \neq 11}$ is linearly disjoint over $\mathbb{Q}$. As F_{11} contains the quadratic field $F_2 = \mathbb{Q}(\sqrt{-11}) \subset \mathbb{Q}(\zeta_{11})$, any rational prime that does not split completely in F_2 *automatically* does not split completely in F_{11}, making the non-splitting condition in F_{11} for primes of cyclic reduction superfluous. Thus, the entanglement correction in this case amounts to leaving out the factor $1 - 1/[F_{11} : \mathbb{Q}] = \frac{13199}{13200}$ from the naive density. The resulting value $\delta_{E/\mathbb{Q}} = \frac{13200}{13199} A_{E/\mathbb{Q}} \approx 0.4882881$ is so close to the naive density that the correction is not easily detected numerically. Our value of $d(E)$ obtained by checking less than 80,000 primes is less than .15% away from either of these values: a good match.

Example 5.4.11. The elliptic curve $E_{/\mathbb{Q}}$ with LMFDB label 19.a2 defined by

$$E : y^2 = x^3 - 12096x - 544752$$

of discriminant $\Delta_E = -2^{12} \cdot 3^{12} \cdot 19^3$ has division fields F_ℓ of maximal degree at all primes $\ell \neq 3$, and a minimal 3-division field $F_3 = \mathbb{Q}(\zeta_3)$. This makes the naive density equal to

$$A_{E/\mathbb{Q}} = \frac{48}{47} \cdot \frac{1}{2} A_\infty \approx 0.4155329.$$

We can take $N(E, \mathbb{Q}) = 2 \cdot 3 \cdot 5 \cdot 19$ in this case. The quadratic subfield $\mathbb{Q}(\sqrt{-19})$ of F_2 is different from $F_3 = \mathbb{Q}(\zeta_3)$, and again F_2, F_3 and F_5 are linearly disjoint as we have $\sqrt{5} \notin F_6$. This time $\{F_\ell\}_{\ell \neq 19}$ a linearly disjoint family over $\mathbb{Q}$, and F_2 has a non-trivial intersection $F_2 \cap F_{19} = \mathbb{Q}(\sqrt{-19})$, but *not* an inclusion $F_2 \subset F_{19}$.

This is a very common form of entanglement over $F = \mathbb{Q}$: if the quadratic subfield $\mathbb{Q}(\sqrt{\Delta_E})$ of F_2 has *odd* discriminant D, it is a subfield of the cyclotomic field $\mathbb{Q}(\zeta_{|D|})$, and therefore of the compositum $F_{|D|}$ of the division fields F_ℓ with $\ell|D$. If this quadratic intersection between F_2 and $F_{|D|}$ is the *only* entanglement between the fields F_ℓ, then $G = \mathrm{Gal}(F_{2|D|}/\mathbb{Q}) \subset G' = \prod_{\ell|2D} \mathrm{Gal}(F_\ell/\mathbb{Q})$ is a subgroup of index 2 arising as the kernel of a quadratic character on G'. In this case we can apply the character-sum formula (5.9), which gives an entanglement correction

$$\alpha_{E/\mathbb{Q}} = 1 + \prod_{\ell|2D,\ \ell \text{ prime}} \frac{-1}{[F_\ell : \mathbb{Q}] - 1}. \tag{5.23}$$

For $D = -19$ we obtain $\alpha_{E/\mathbb{Q}} = \frac{615596}{615595}$ and $\delta_{E/\mathbb{Q}} = 0.4155335$, a figure which is not noticeably different from the naive density from a numerical point of view.

Example 5.4.12. Let E be the elliptic curve with LMFDB label 1976.a1 defined by

$$E : y^2 = x^3 + x + 3$$

with discriminant $\Delta_E = -2^4 \cdot 13 \cdot 19$. In this case the mod ℓ Galois representation associated to E has maximal image $\mathrm{GL}_2(\mathbb{F}_\ell)$ for all primes ℓ, so the naive density is equal to A_∞. We can take $N(E, \mathbb{Q}) = 2 \cdot 3 \cdot 5 \cdot 13 \cdot 19$ in Theorem 5.4.1. One can check that the only entanglement here comes from the quadratic subfield $\mathbb{Q}(\sqrt{-13 \cdot 19})$ of discriminant $-13 \cdot 19 = -247$ of F_2, which is contained in the compositum of F_{13} and F_{19}. The entanglement correction factor given by the character sum formula (5.9) is

$$\alpha_{E/\mathbb{Q}} = 1 + \prod_{\ell|2\cdot 13\cdot 19} \frac{-1}{[F_\ell : \mathbb{Q}] - 1} \approx 0.999999999938,$$

making $\delta_{E/F}$ numerically indistinguishable from A_∞.

Example 5.4.13. The final elliptic curve in our table, which has LMFDB label 11.a2 and is defined by

$$y^2 = x^3 - 13392x - 1080432,$$

has discriminant $\Delta_E = -2^{12} \cdot 3^{12} \cdot 11^5$ and is special for having minimal 5-division field $F_5 = \mathbb{Q}(\zeta_5)$ of degree 4. At primes $\ell \neq 5$ the degree of F_ℓ is maximal, so the naive density equals

$$A_{E/\mathbb{Q}} = \frac{3}{4} \cdot \frac{480}{479} \cdot A_\infty \approx 0.6115881,$$

very close to the fraction $d(E)$ we computed. We take $N(E, \mathbb{Q}) = 2 \cdot 3 \cdot 5 \cdot 11$ and check easily that the only entanglement comes from the non-trivial intersection $F_2 \cap F_{11} = \mathbb{Q}(\sqrt{-11})$. As in the previous example, the entanglement correction factor

$$\alpha_{E/\mathbb{Q}} = 1 + \prod_{\ell|2\cdot 11} \frac{-1}{[F_\ell : \mathbb{Q}] - 1} = 1 + \frac{1}{5 \cdot 13199}$$

yields $\delta_{E/\mathbb{Q}} = 0.6115973$, and is too small to be observed numerically.

5.5 An unconditional result in the complex multiplication setting

In this section we turn to the case where the considered elliptic curves $E_{/F}$ in the cyclic reduction problem have complex multiplication. In this case it possible to prove *unconditionally* that $S_{E/F}$ has density $\delta_{E/F}$ using explicit versions of the Chebotarëv density theorem. For $F = \mathbb{Q}$, this has been written down in [Coj03], and the proof given there extends without essential changes to arbitrary number fields F. For completeness, we give some details here, neglecting the parts where the arguments are equal to the ones presented in [Coj03].

Theorem 5.5.1. *Let F be a number field and $E_{/F}$ an elliptic curve with complex multiplication. Then the density $\delta_{E/F}$ of the set of primes of cyclic reduction for E always exists and equals*

$$\delta_{E/F} = \sum_{m=1}^{\infty} \frac{\mu(m)}{[F_m : F]}. \tag{5.24}$$

The proof relies on the following effective version of the Chebotarëv's density theorem.

Proposition 5.5.2. *Let L/K be a Galois extension of number fields and set Δ_L to be the absolute discriminant of $L/\mathbb{Q}$ and $n_L := [L : \mathbb{Q}]$. Then there exists an absolute constant $C > 0$ such that for every $x \in \mathbb{R}$ satisfying*

$$\sqrt{\frac{\log x}{n_L}} \geq C \cdot \max\{\log|\Delta_L|, |\Delta_L|^{\frac{1}{n_L}}\}$$

we have

$$\pi(x, L) = \frac{\mathrm{li}(x)}{[L : K]} + O\left(x \exp\left(-\frac{1}{99} \cdot \sqrt{\frac{\log x}{n_L}}\right)\right)$$

where $\pi(x, L)$ is the number of prime ideals $\mathfrak{p} \subseteq K$ such that $N_{K/\mathbb{Q}}(\mathfrak{p}) \leq x$ and $\mathfrak{p}$ splits completely in L. The constant implied in the symbol O is absolute.

Proof. The statement of this result for $K = \mathbb{Q}$ is already contained in [Ram84, Lemma 2]. To prove the more general version of the proposition, we use [Win13, Théorème 1.1] which gives

$$\left|\pi(x, L) - \frac{1}{[L : K]}\,\mathrm{li}(x)\right| \leq \frac{1}{[L : K]}\,\mathrm{li}(x^{\beta}) + C_0 x \exp\left(-\frac{1}{99}\sqrt{\frac{\log x}{n_L}}\right) \tag{5.25}$$

where the inequality holds for every $x \geq \exp(8n_L \log(150867|\Delta_L|^{44/5})^2)$ and C_0 is an explicit absolute constant. Moreover by [Sta74, pag. 148], there exists an effectively computable absolute constant C such that

$$\beta < 1 - \frac{1}{C|\Delta_L|^{1/n_L}}. \tag{5.26}$$

Notice first of all that we can substitute the condition $x \geq \exp(8n_L \log(150867|\Delta_L|^{44/5})^2)$ with the weaker condition

$$\sqrt{\frac{\log x}{n_L}} \geq 60 \log|\Delta_L| \tag{5.27}$$

and that, under this condition on x, we can write (5.25) as

$$\pi(x,L) = \frac{1}{[L:K]}\,\mathrm{li}(x) + O\left(\frac{\mathrm{li}(x^\beta)}{[L:K]}\right) + O\left(x\exp\left(-\frac{1}{99}\sqrt{\frac{\log x}{n_L}}\right)\right). \tag{5.28}$$

Now (5.26) gives

$$\begin{aligned}\frac{\mathrm{li}(x^\beta)}{[L:K]} \le \mathrm{li}(x^\beta) \le x^\beta = \exp(\beta\log x) &\le \exp\left(\left(1-\frac{1}{C|\Delta_L|^{1/n_L}}\right)\log x\right)\\ &= x\exp\left(-\frac{\log x}{C|\Delta_L|^{1/n_L}}\right)\end{aligned}$$

and one has

$$-\frac{\log x}{C|\Delta_L|^{1/n_L}} \le -\frac{1}{99}\sqrt{\frac{\log x}{n_L}} \iff \sqrt{\frac{\log x}{n_L}} \ge \frac{C}{99n_L}|\Delta_L|^{1/n_L}.$$

Hence for

$$\sqrt{\frac{\log x}{n_L}} \ge \max\{60\log|\Delta_L|, \frac{C}{99}|\Delta_L|^{1/n_L}\}$$

we have

$$\frac{\mathrm{li}(x^\beta)}{[L:K]} = O\left(x\exp\left(-\frac{1}{99}\sqrt{\frac{\log x}{n_L}}\right)\right)$$

and the proposition follows. □

Remark 5.5.3. In the following, if we want to emphasize the base field we will also write $\pi(x, L/K)$ in place of $\pi(x,L)$.

Proof of Theorem 5.5.1. Let S be the set of primes of F that do not split completely in any F_ℓ and let

$$g(x,F) := \#\{\mathfrak{p}\subseteq F : N_{F/\mathbb{Q}}(\mathfrak{p}) \le x, \deg(\mathfrak{p}) = 1, \mathfrak{p}\nmid \Delta_E\cdot\Delta_F \text{ and } \mathfrak{p}\in S\}.$$

We have to prove that

$$\lim_{x\to\infty}\frac{g(x,L)}{x/\log x}$$

exists, since then this limit is also equal to $\delta_{E/F}$ by Corollary 5.3.2 and by the fact that the density of any set of primes $\mathcal{A}$ of F is equal to density of the set of primes of degree 1 contained in $\mathcal{A}$. Notice also that, by ignoring finitely many primes and by the implication (5.11), we can substitute the function $g(x,F)$ in the limit above with the function

$$f(x,F) := \#\{\mathfrak{p}\subseteq F : N_{F/\mathbb{Q}}(\mathfrak{p}) \le x, \deg(\mathfrak{p}) = 1, \mathfrak{p}\in S(\sqrt{x}+1)\}$$

where, for every $a\in\mathbb{R}$, we set $S(a)$ to be the set of primes of F that do not split completely in any F_ℓ with $\ell\le a$.

Let now $0 \leq y \leq \sqrt{x}+1$ to be fixed later, and set

$$\begin{aligned} N(x,y) &:= \#\{\mathfrak{p} \subseteq F : N_{F/\mathbb{Q}}(\mathfrak{p}) \leq x, \deg(\mathfrak{p}) = 1, \mathfrak{p} \in S(y)\} \\ M(x,y,\sqrt{x}+1) &:= \#\{\mathfrak{p} \subseteq F : N_{F/\mathbb{Q}}(\mathfrak{p}) \leq x, \deg(\mathfrak{p}) = 1,\ \mathfrak{p} \text{ splits completely in } F_\ell \\ &\qquad\qquad \text{for some prime } y < \ell \leq \sqrt{x}+1\}. \end{aligned}$$

Since $N(x,y) - M(x,y,\sqrt{x}+1) \leq f(x,F) \leq N(x,y)$ we can write

$$f(x,F) = N(x,y) + O\left(M(x,y,\sqrt{x}+1)\right)$$

and bound the two terms appearing in the above equality separately. We start by bounding $N(x,y)$. We have

$$N(x,y) = \sum \mu(k)\pi(x, F_k/F)$$

where the sum is taken over all integers $k \leq \sqrt{x}+1$ (squarefree) whose prime factors are all $\leq y$. To bound the terms $\pi(x,F_k/F)$ appearing in the sum, we would like to use the effective version of the Chebotarëv density theorem given by Proposition 5.5.2. In order to apply the proposition, we need to verify the following two hypotheses:

(a) $n_{F_k}(\log|\Delta_{F_k}|)^2 \ll \log x$;

(b) $n_{F_k}|\Delta_{F_k}|^{2/n_{F_k}} \ll \log x$,

where $n_{F_k} = [F_k : \mathbb{Q}]$ and the implied constants must be absolute. In this process, we will also need to choose the parameter y in a clever way.

Using the proof of Proposition 5.3.5 one has

$$\frac{1}{[F_k:F]}\log|\Delta_{F_k}| - \log|\Delta_F| \leq [F:\mathbb{Q}]\left(\sum_{p \mid N_{F/\mathbb{Q}}(\Delta_{F_k/F})} \log p + \log[F_k:F]\right)$$

and dividing both sides of the inequality above by $[F:\mathbb{Q}]$ we get

$$\begin{aligned} \frac{1}{n_{F_k}}\log|\Delta_{F_k}| - \frac{1}{[F:\mathbb{Q}]}\log|\Delta_F| \leq \sum_{p \mid N_{F/\mathbb{Q}}(\Delta_{F_k/F})} \log p + \log[F_k:F] &\leq \sum_{p \mid k\cdot N_E} \log p + \log[F_k:F] \\ &\leq \log(k\cdot N_E) + \log[F_k:F] \\ &= \log(k\cdot N_E\cdot[F_k:F]) \end{aligned}$$

where N_E denotes the norm of the conductor of the elliptic curve E. Using the fact that $[F_k : F] \ll k^2$ we finally obtain

$$\frac{1}{n_{F_k}}\log|\Delta_{F_k}| \ll \log(k^3 N_E) \tag{5.29}$$

and from this inequality it is easy to deduce that

$$n_{F_k}(\log|\Delta_{F_k}|)^2 \ll k^6(\log(k^3N_E))^2 \quad \text{and} \quad n_{F_k}|\Delta_{F_k}|^{2/n_{F_k}} \ll k^8N_E^2$$

so that in particular

$$\max\{n_{F_k}(\log|\Delta_{F_k}|)^2, n_{F_k}|\Delta_{F_k}|^{2/n_{F_k}}\} \ll k^8N_E^2.$$

Since now k is the squarefree product of primes $\leq y$ we have $k \leq e^{2y}$, so by choosing

$$y = \frac{1}{16}(\log\log x - 2\log N_E) \tag{5.30}$$

we get

$$k^8 N_E^2 \leq e^{16y} N_E^2 = e^{\log\log x - 2\log N_E} N_E^2 = \log x.$$

Hence the choice of y as in (5.30) allows us to apply Proposition 5.5.2 and obtain

$$N(x,y) = \sum \mu(k)\pi(x, F_k/F) = \left(\sum \frac{\mu(k)}{[F_k : F]}\right)\mathrm{li}(x) + O\left(\sum \mu(k) x \exp\left(-\frac{1}{99}\sqrt{\frac{\log x}{n_{F_k}}}\right)\right)$$

and using the same estimate of [Coj03] (compare the expression above with [Coj03, Formula (7)]) we obtain

$$N(x,y) = \sum \mu(k)\pi(x, F_k/F) = \left(\sum \frac{\mu(k)}{[F_k : F]}\right)\mathrm{li}(x) + O\left(\frac{x}{N_E^{1/4}(\log x)^B}\right) \tag{5.31}$$

for any positive constant B.

We now proceed to bound $M(x, y, \sqrt{x}+1)$. We split this quantity in two terms

$$M(x, y, \sqrt{x}+1) = M_{\mathrm{o}}(x, y, \sqrt{x}+1) + M_{\mathrm{ss}}(x, y, \sqrt{x}+1) \tag{5.32}$$

where

- $M_{\mathrm{o}}(x, y, \sqrt{x}+1)$ is the cardinality of the set of degree 1 primes $\mathfrak{p} \subseteq F$ which split completely in some F_ℓ for $y < \ell \leq \sqrt{x}+1$ and which are primes of good ordinary reduction for the elliptic curve E;
- $M_{\mathrm{ss}}(x, y, \sqrt{x}+1)$ is the cardinality of the set of degree 1 primes $\mathfrak{p} \subseteq F$ which split completely in some F_ℓ for some $y < \ell \leq \sqrt{x}+1$ and which are primes of good supersingular reduction for the elliptic curve E.

In what follows, for a given prime $\mathfrak{p} \subseteq F$ we denote by $\widetilde{E}$ the reduction of E modulo $\mathfrak{p}$ and by $a_{\mathfrak{p}}$ the trace of the Frobenius endomorphism $\pi_{\mathfrak{p}}$ of $\widetilde{E}$. We estimate the two terms in (5.32) separately. We begin with $M_{\mathrm{o}}(x, y, \sqrt{x}+1)$, which we brutally estimate by

$$M_{\mathrm{o}}(x, y, \sqrt{x}+1) \leq \sum_{y<\ell\leq\sqrt{x}+1} \pi_{\mathrm{o}}(x, F_\ell/F)$$

where in the sum above ℓ denotes a prime number and $\pi_{\mathrm{o}}(x, F_\ell/F)$ counts the degree 1 primes $\mathfrak{p} \subseteq F$ which split completely in $F \subseteq F_\ell$ and which are of good ordinary reduction for E. Notice that for every such prime, the reduced elliptic curve $\widetilde{E}$ is ordinary and defined over $\mathbb{F}_p$, with $p = N_{F/\mathbb{Q}}(\mathfrak{p})$. Moreover, we always have an embedding

$$K = \mathrm{End}_{\overline{F}}(E) \otimes_{\mathbb{Z}} \mathbb{Q} \hookrightarrow \mathrm{End}_{\overline{\mathbb{F}}_p}(\widetilde{E}) \otimes_{\mathbb{Z}} \mathbb{Q}$$

where K is the CM-field of $E_{/F}$. Since $\widetilde{E}$ is ordinary, we have $\mathrm{End}_{\overline{\mathbb{F}}_p}(\widetilde{E}) \otimes_{\mathbb{Z}} \mathbb{Q} = \mathbb{Q}(\pi_{\mathfrak{p}})$, and this yields $K = \mathbb{Q}(\pi_{\mathfrak{p}})$. Now, $\mathfrak{p}$ splits completely in F_ℓ, which means that the group of points

$\widetilde{E}(\mathbb{F}_p)$ contains the full ℓ-torsion of the elliptic curve $\widetilde{E}$, and this in particular implies that $\ker[\ell] \subseteq \ker(\pi_{\mathfrak{p}} - 1)$. By the factorization theorem for isogenies, we have

$$\frac{\pi_{\mathfrak{p}} - 1}{\ell} \in \operatorname{End}_{\overline{\mathbb{F}}_p}(\widetilde{E}) \subseteq \mathcal{O}_K.$$

Suppose for a moment that the absolute discriminant Δ_K of K satisfies $\Delta_K \equiv 2, 3 \bmod 4$ so that $\mathcal{O}_K = \mathbb{Z}[\sqrt{\Delta_K}]$. Then

$$\frac{\pi_{\mathfrak{p}} - 1}{\ell} \in \mathcal{O}_K \iff N_{K/\mathbb{Q}}(\pi_{\mathfrak{p}}) = (a\ell + 1)^2 + |\Delta_K| b^2 \ell^2$$

for some $a, b \in \mathbb{Z}$. Since $\mathfrak{p}$ has degree 1, one has $N_{K/\mathbb{Q}}(\pi_{\mathfrak{p}}) = N_{F/\mathbb{Q}}(\mathfrak{p}) = p$ and we get

$$\begin{aligned}\pi_o(x, F_\ell/F) &\leq \#\{\mathfrak{p} \subseteq F : N_{F/\mathbb{Q}}(\mathfrak{p}) \leq x, \deg \mathfrak{p} = 1, \frac{\pi_{\mathfrak{p}} - 1}{\ell} \in \mathcal{O}_K\} \\ &\leq [F : \mathbb{Q}] \cdot \#\{p \leq x \text{ prime} : p = (a\ell + 1)^2 + |\Delta_K| b^2 \ell^2 \text{ for some } a, b \in \mathbb{Z}\}.\end{aligned}$$

Now $[F : \mathbb{Q}]$ is fixed, so one can apply exactly the same arguments contained in [Coj03, pag. 2659] to obtain

$$M_o(x, y, \sqrt{x} + 1) = O\left(\frac{x \log\log x}{\log x \cdot (\log\log x - 2 \log N_E) \cdot (\log\log(\log x / N_E^2))}\right). \tag{5.33}$$

The same conclusion is reached if $\Delta_K \equiv 1 \bmod 4$.

We now estimate $M_{\mathrm{ss}}(x, y, \sqrt{x} + 1)$. A prime $\mathfrak{p}$ counted by this function is a prime of degree 1 and of supersingular reduction for E which splits completely in some F_ℓ for $y < \ell \leq \sqrt{x} + 1$ prime. In particular, the reduced elliptic curve $\widetilde{E}$ is defined over $\mathbb{F}_p$ with $p := N_{F/\mathbb{Q}}(\mathfrak{p})$, and it is supersingular. The fact that $\mathfrak{p}$ splits completely in F_ℓ implies on the one hand that $\ell^2 \mid \#\widetilde{E}(\mathbb{F}_p) = p + 1$ (since $\widetilde{E}$ is supersingular) and on the other hand that $\mathbb{F}_p^\times$ contains a primitive ℓ-th root of unity, which in particular means that $\ell \mid p - 1$. We deduce that $\ell = 2$. Since $y > 2$ by (5.30), we conclude that

$$M_{\mathrm{ss}}(x, y, \sqrt{x} + 1) = 0. \tag{5.34}$$

Now the proof of the theorem can be concluded by putting together the estimates (5.31), (5.33) and (5.34), as done by Cojocaru in [Coj03, pag. 2660]. □

5.6 CM cyclic reduction densities

We now want to investigate whether the cyclic reduction density $\delta_{E/F}$ associated to an elliptic curve $E_{/F}$ with complex multiplication can be factored as a product of a naive density $A_{E/F}$ and an entanglement correction factor $\alpha_{E/F}$, in a similar fashion to (5.4.4).

If F contains the CM-field K, the situation is structurally reminiscent of the non-CM-case, but, as we explained in Proposition 4.3.2, this time the ℓ-division fields have Galois group $\operatorname{Gal}(F_\ell/F) \cong (\mathcal{O}/\ell\mathcal{O})^\times$ for almost all primes ℓ, instead of the group $\operatorname{GL}_2(\mathbb{F}_\ell)$ that we had before. Again, the fields F_ℓ form a linearly disjoint family over F for ℓ ranging over the prime numbers outside the finite set $T_{E/F}$ of critical prime numbers described in Theorem 4.3.4 (in the statement of the theorem, these are the primes dividing the integer B_E). To ease notation, we define

$$A_{\mathcal{O},\ell} = 1 - \frac{1}{\#(\mathcal{O}/\ell\mathcal{O})^\times} = \begin{cases} 1-(\ell-1)^{-2} & \text{if } \left(\frac{D}{\ell}\right) = 1 \\ 1-(\ell^2-1)^{-1} & \text{if } \left(\frac{D}{\ell}\right) = -1 \\ 1-(\ell^2-\ell)^{-1} & \text{if } \left(\frac{D}{\ell}\right) = 0 \end{cases} \tag{5.35}$$

and call $A_{\mathcal{O}} = \prod_{\ell \text{ prime}} A_{\mathcal{O},\ell}$ the *Artin constant* of the order $\mathcal{O}$. We then have the following result, completely analogous to Theorem 5.4.4, with the only difference that we now know that the density of the set of primes of cyclic reduction for E is equal to $\delta_{E/F}$ by Theorem 5.5.1.

Theorem 5.6.1. *Let $E_{/F}$ be a CM-elliptic curve with CM-order $\mathcal{O} \subset F$. Then the set of primes of cyclic reduction of E has density*

$$\delta_{E/F} = \left(\sum_{m \mid T_{E/F}} \frac{\mu(m)}{[F_m : F]} \right) \cdot \prod_{\ell \notin T_{E/F}} A_{\mathcal{O},\ell}. \tag{5.36}$$

In particular, we have $\delta_{E/F} = c_{E/F} \cdot A_{\mathcal{O}}$ for some $c_{E/F} \in \mathbb{Q}_{\geq 0}$.

Proof. By Theorem 4.3.4 the family of division fields $\{F_{T_{E/F}}\} \cup \{F_\ell\}_{\ell \nmid T_{E/F}}$ is linearly disjoint over F. Hence the same proof of Theorem 5.4.4 carries over to this case and allows to write

$$\delta_{E/F} = \sum_{m \mid T_{E/F}} \frac{\mu(m)}{[F_m : F]} \cdot \prod_{\ell \notin T_{E/F}} \left(1 - \frac{1}{[F_\ell : F]} \right).$$

On the other hand, Proposition 4.3.2 implies that for $\ell \nmid T_{E/F}$ we have an isomorphism $\mathrm{Gal}(F_\ell/F) \cong (\mathcal{O}/\ell\mathcal{O})^\times$ and this suffices to conclude. □

When the field of definition F of the elliptic curve E does not contain the CM field, the situation is somehow different since, in this case, it is not true anymore that the family of division fields $\{F_\ell\}_\ell$ for ℓ prime becomes linearly disjoint after removing a finite set of fields.

Theorem 5.6.2. *Let $E_{/F}$ be an elliptic curve with complex multiplication by an order in an imaginary quadratic field K. Then F_ℓ contains K for all primes $\ell \geq 3$.*

Proof. If F already contains K there is nothing to prove, so we assume $F \not\supseteq K$. In this case the compositum FK is a quadratic extension of F, so if there exists a prime ℓ such that F_ℓ does not contain FK, then the two fields are linearly disjoint over F. By the Chebotarëv Density Theorem, there is a degree 1 prime ideal $\mathfrak{p} \subseteq F$ coprime with ℓ that is inert in FK and splits completely in F_ℓ. If we denote by $p \in \mathbb{N}$ the rational prime lying below $\mathfrak{p}$, the first condition implies, by Theorem 1.4.1, that the reduced curve $\widetilde{E} := E \bmod \mathfrak{p}$ is a supersingular elliptic curve defined over $\mathbb{F}_p$. In particular, $\#\widetilde{E}(\mathbb{F}_p) = p + 1$. On the other hand, the fact that $\mathfrak{p}$ splits completely in F_ℓ implies that $\widetilde{E}(\mathbb{F}_p)$ contains the full ℓ-torsion of $\widetilde{E}(\overline{\mathbb{F}}_p)$, so that $\ell \mid p + 1$. Since $F(\zeta_\ell) \subseteq F_\ell$, we also have that $\ell \mid p - 1$. We conclude that $\ell = 2$, and the theorem follows. □

Theorem 5.6.2 shows that the entanglement in the family of division fields $\{F_\ell\}_\ell$ is not finite anymore if the base-field F does not contain the CM field K. However, we can always recover the more familiar quadratic entanglement setting after base-changing E to the compositum FK. This allows us to prove the following analogue of Theorem 5.6.1.

Theorem 5.6.3. *Let E be an elliptic curve with complex multiplication by an order $\mathcal{O}$ of discriminant $\Delta_{\mathcal{O}} < -4$ in an imaginary quadratic field K and defined over $F \not\supseteq K$. Write $H_{2,\mathcal{O}}$ for the ray class field modulo 2 relative to the order $\mathcal{O}$. Then there exists a non-negative rational number $c_{E/F} \in \mathbb{Q}_{\geq 0}$ such that:*

1. *If $\Delta_{\mathcal{O}} \equiv 0 \bmod 4$ then either F is linearly disjoint from $H_{2,\mathcal{O}}$ over $\mathbb{Q}(j(E))$ and*
$$\delta_{E/F} = \frac{1}{4} + \frac{c_{E/F}}{2} \cdot A_{\mathcal{O}}$$
or $F \cap H_{2,\mathcal{O}} \supsetneq \mathbb{Q}(j(E))$ and we have
$$\delta_{E/F} = \begin{cases} 0 & \text{if } F = F_2 \\ \frac{1}{2} & \text{otherwise} \end{cases}$$

2. *If $\Delta_{\mathcal{O}} \equiv 5 \bmod 8$ then*
$$\delta_{E/F} = \frac{1}{2} + \frac{c_{E/F}}{2} \cdot A_{\mathcal{O}}.$$

3. *If $\Delta_{\mathcal{O}} \equiv 1 \bmod 8$ then $\delta_{E/F} = 1/2$.*

Proof. Let S be the set of primes of F that do not split completely in any division field F_ℓ with ℓ prime. By Corollary 5.3.2 and Theorem 5.5.1, the natural density $\delta(S)$ of the set S equals $\delta_{E/F}$. In order to compute the former density, we need to understand the behaviour of the field F_2 since by Theorem 5.6.2 all the other division fields contain the compositum FK.

Let $L := \mathbb{Q}(j(E))$ and let E'/L be any elliptic curve with $j(E') = j(E)$. Following the notation adopted in this chapter, we denote by $L_2 := L(E'[2](\overline{\mathbb{Q}}))$. Then we have the following diagram of fields:

$$\begin{tikzcd}
 & H_{2,\mathcal{O}} \arrow[ld, no head] \arrow[rd, no head] & & \\
L_2 \arrow[rd, no head] & & H_{\mathcal{O}} \arrow[ld, no head, "2"'] \arrow[rd, no head] & \\
 & L \arrow[rd, no head] & & F \arrow[ld, no head, "2"] \\
 & & \mathbb{Q} &
\end{tikzcd}$$

where $H_{2,\mathcal{O}}$ is the the compositum of the ring class field $H_{\mathcal{O}}$ with the 2-division field L_2, since $j(E) \neq 0, 1728$ by hypothesis. The extension $L \subseteq H_{2,\mathcal{O}}$ is Galois and one has

$$\mathrm{Gal}(H_{2,\mathcal{O}}/H_{\mathcal{O}}) \cong (\mathcal{O}/2\mathcal{O})^{\times}, \qquad \mathrm{Gal}(H_{2,\mathcal{O}}/L) \cong \mathrm{Gal}(H_{2,\mathcal{O}}/H_{\mathcal{O}}) \rtimes \langle \sigma \rangle$$

where the first isomorphism is given by the Artin map and σ is the unique non-trivial element of $\mathrm{Gal}(H_{\mathcal{O}}/L)$ whose action on $\mathrm{Gal}(H_{2,\mathcal{O}}/H_{\mathcal{O}})$ is induced by the natural Galois action on $\mathcal{O}$. We notice now that $F \supseteq L$ since $j(E) \in F$, and that $L_2F = F_2$ since E is a twist of the base-change of E' to F and the 2-division field is generated by the values of a Weber function for E (resp. E') at

2-torsion points. Moreover $F \cap H_{\mathcal{O}} = L$ because by assumption F does not contain the CM field K. Hence $[F \cdot H_{\mathcal{O}} : F] = 2$ and we write $S = S_1 \sqcup S_2$ where

$$S_1 := \{\mathfrak{p} \in S : \mathfrak{p} \text{ does not split in } F \cdot H_{\mathcal{O}}\},$$
$$S_2 := \{\mathfrak{p} \in S : \mathfrak{p} \text{ splits in } F \cdot H_{\mathcal{O}}\},$$

so that $\delta(S) = \delta(S_1) + \delta(S_2)$. We now divide the proof according to the different cases appearing in the statement of the theorem.

Case 1: Assume that $\Delta_{\mathcal{O}} \equiv 0 \bmod 4$. Under this assumption, either 2 ramifies in K or 2 divides the conductor of $\mathcal{O}$ or both. Suppose first that 2 is coprime with the conductor of $\mathcal{O}$. Then we have

$$\mathrm{Gal}(H_{2,\mathcal{O}}/H_{\mathcal{O}}) = (\mathcal{O}/2\mathcal{O})^\times \cong (\mathcal{O}_K/2\mathcal{O}_K)^\times \cong \left(\mathbb{F}_2[x]/(x^2)\right)^\times \cong C_2$$

where C_N denotes the cyclic group of order N. On the other hand, if 2 divides the conductor of $\mathcal{O}$ there exists a unique prime ideal $\mathfrak{p}_{2,\mathcal{O}} \subseteq \mathcal{O}$ lying over 2 for which the inclusions $2\mathcal{O} \subsetneq \mathfrak{p}_{2,\mathcal{O}} \subsetneq \mathcal{O}$ have at each step index 2. Again one has

$$(\mathcal{O}/2\mathcal{O})^\times \cong \left(\mathbb{F}_2[x]/(x^2)\right)^\times \cong C_2$$

showing that in any case $[H_{2,\mathcal{O}} : H_{\mathcal{O}}] = 2$. This implies that $L \subseteq H_{2,\mathcal{O}}$ is a Klein extension obtained as compositum of the two disjoint quadratic extensions $L \subseteq L_2$ and $L \subseteq H_{\mathcal{O}}$.

Suppose now that $F \cap H_{2,\mathcal{O}} = \mathbb{Q}(j(E))$. Then we also have that F_2 and $F \cdot H_{\mathcal{O}}$ are two quadratic linearly disjoint extensions of F. Since $F \cdot H_{\mathcal{O}}$ is contained in all the ℓ-division fields with $\ell \geq 3$, the set S_1 is equal to the set of primes of F that do not split neither in F_2 nor in $F \cdot H_{\mathcal{O}}$. Since these two fields are linearly disjoint over F, we have

$$\delta(S_1) = \left(1 - \frac{1}{[F_2 : F]}\right)\left(1 - \frac{1}{[F \cdot H_{\mathcal{O}} : F]}\right) = \frac{1}{4}.$$

On the other hand, if a prime $\mathfrak{p} \subseteq F$ splits in $F \cdot H_{\mathcal{O}}$, then $\mathfrak{p}$ does not split in F_2 if and only if all the primes of $F \cdot H_{\mathcal{O}}$ lying above $\mathfrak{p}$ do not split in $F \cdot H_{2,\mathcal{O}}$. So we have

$$\delta(S_2) = \frac{1}{2} \cdot \delta(\widetilde{S})$$

where $\widetilde{S}$ is the set of primes of $F \cdot H_{\mathcal{O}}$ that do not split completely in any $(F \cdot H_{\mathcal{O}})(E[\ell])$ for ℓ prime. But this is equal to the density $\delta_{E/F \cdot H_{\mathcal{O}}}$ of the set of primes of cyclic reduction of the base-change $E_{/F \cdot H_{\mathcal{O}}}$. Theorem 5.6.1 then gives

$$\delta(S_2) = \frac{1}{2} \cdot \delta_{E/F \cdot H_{\mathcal{O}}} = \frac{1}{2} \cdot c_{E/F} \cdot A_{\mathcal{O}}$$

with $c_{E/F}$ the entanglement correction factor to the Artin constant $A_{\mathcal{O}}$.

Suppose now that $F \cap H_{2,\mathcal{O}} \supsetneq \mathbb{Q}(j(E))$. Since $F \not\supset H_{\mathcal{O}}$, the intersection $F \cap H_{2,\mathcal{O}}$ is either equal to L_2 or is a quadratic extension of L that is distinct from both L_2 and $H_{\mathcal{O}}$. In the first case, we have $F = F_2$ and $\delta_{E/F} = 0$. In the second case, $F_2 = F \cdot L_2 = F \cdot H_{2,\mathcal{O}} = F \cdot H_{\mathcal{O}}$, so by Theorem 5.6.2 the set S consists precisely of the primes of F that do not split completely in $F \cdot H_{\mathcal{O}}$. Hence we have $\delta_{E/F} = \frac{1}{2}$ and this concludes the study of Case 1.

Case 2: Suppose now that $\Delta_{\mathcal{O}} \equiv 5 \bmod 8$. Under this assumption, the prime 2 is inert in $\mathcal{O}$ and we then have

$$(\mathcal{O}/2\mathcal{O})^\times \cong (\mathcal{O}_K/2\mathcal{O}_K)^\times \cong \mathbb{F}_4^\times \cong C_3$$

from which we get

$$\mathrm{Gal}(H_{2,\mathcal{O}}/L) \cong \mathrm{Gal}(H_{2,\mathcal{O}}/H_{\mathcal{O}}) \rtimes \mathrm{Gal}(H_{\mathcal{O}}/L) \cong C_3 \rtimes C_2 \cong S_3$$

where S_3 denotes the symmetric group with 6 elements. This implies that the degree $[L_2 : L]$ can be either 3 or 6. However, the first possibility is cannot hold, since otherwise the fields L_2 and $H_{\mathcal{O}}$ would be linearly disjoint over L and $\mathrm{Gal}(H_{2,\mathcal{O}}/L)$ would then be abelian. We deduce that $L_2 = H_{2,\mathcal{O}} \supseteq H_{\mathcal{O}}$. After composing with F, we obtain the analogous inclusion $F_2 \supseteq F \cdot H_{\mathcal{O}}$. Hence by Theorem 5.6.2 all the ℓ-division fields of $E_{/F}$ contain $F \cdot H_{\mathcal{O}}$. After using Theorem 5.6.1 we obtain

$$\delta(S_1) = \frac{1}{2}, \qquad \delta(S_2) = \frac{1}{2} \cdot \delta_{E/F \cdot H_{\mathcal{O}}} = \frac{1}{2} \cdot c_{E/F} \cdot A_{\mathcal{O}}$$

with $c_{E/F}$ the entanglement correction factor to the Artin constant $A_{\mathcal{O}}$ for the division fields of $E_{/F \cdot H_{\mathcal{O}}}$. This concludes the study of this case.

Case 3: We finally suppose that $\Delta_{\mathcal{O}} \equiv 1 \bmod 8$. Under this assumption, the prime 2 splits in $\mathcal{O}$ and we have

$$\mathcal{O}/2\mathcal{O} \cong \mathcal{O}_K/2\mathcal{O}_K \cong \mathbb{F}_2 \times \mathbb{F}_2.$$

The group of units of this ring is trivial and we deduce that $H_{2,\mathcal{O}} = H_{\mathcal{O}}$. In particular, we have the inclusions $L \subseteq L_2 \subseteq H_{\mathcal{O}}$ with $[H_{\mathcal{O}} : L] = 2$, so either $L_2 = L$ or $L_2 = H_{\mathcal{O}}$. We claim that the first possibility cannot hold.

To see this, choose an embedding $H_{\mathcal{O}} \hookrightarrow \mathbb{C}$ under which $j(E)$ corresponds to $j(\mathcal{O})$, the modular j-function computed on the image of $\mathcal{O}$ through the embedding itself. This can be done, since all the j-invariants of elliptic curves with complex multiplication by the same order form a full Galois orbit over $\mathbb{Q}$. Since $j(\mathcal{O}) \in \mathbb{R}$, as can be verified by acting with complex conjugation $\sigma \in \mathrm{Aut}(\mathbb{C})$, we see that the image of L under the above embedding is contained in $\mathbb{R}$. Hence, if we show that σ acts non-trivially on $L_2 \subseteq \mathbb{C}$ the claim follows. Over $\mathbb{C}$, the curve E' is isomorphic to an elliptic curve of the form $E'' : y^2 = 4x^3 + g_2 x + g_3$ where $g_2 = g_2(\mathcal{O})$ and $g_3 = g_3(\mathcal{O})$ are the usual normalized Eiseinstein series computed on the lattice $\mathcal{O}$. We have a complex analytic isomorphism

$$\mathbb{C}/\mathcal{O} \to E''(\mathbb{C}), \qquad z \mapsto (\wp(z;\mathcal{O}), \wp'(z;\mathcal{O}))$$

where $\wp(z;\mathcal{O})$ denotes the Weierstrass $\wp$-function relative to the lattice $\mathcal{O}$. Then L_2 is obtained by adjoining to L the values of the Weber functions

$$\mathfrak{h}_E^1(z) = \frac{g_2(\mathcal{O}) g_3(\mathcal{O})}{\Delta(\mathcal{O})} \wp(z;\mathcal{O})$$

at torsion points $\frac{1}{2}\mathcal{O}/\mathcal{O}$, where $\Delta(\cdot)$ is the modular discriminant. Since complex conjugation stabilizes $\mathcal{O}$, we see that for every $z \in \mathbb{C}$ one has $\sigma(\mathfrak{h}_E^1(z)) = \mathfrak{h}_E^1(\sigma(z))$, and $\mathfrak{h}_E^1(\sigma(z)) = \mathfrak{h}_E^1(z)$ if and only if $\sigma(z) = \pm z$ in $\mathbb{C}/\mathcal{O}$. For a 2-torsion point $z \in \frac{1}{2}\mathcal{O}/\mathcal{O}$ this happens if and only if $\Delta_{\mathcal{O}}$ is even, which is not the case under our hypotheses. This proves the claim.

To conclude the study of this case, observe that $F_2 = F \cdot L_2 = F \cdot H_{\mathcal{O}}$, so that, by Theorem 5.6.2, the density $\delta(S)$ is precisely equal to the density of the set of primes of F that do not split completely in the quadratic extension $F \subseteq F \cdot H_{\mathcal{O}}$. We conclude that $\delta(S) = \frac{1}{2}$ and the proof of the theorem is complete. □

For elliptic curves with complex multiplication by orders $\mathcal{O}$ of discriminant $\Delta_{\mathcal{O}} \in \{-3, -4\}$ one can argue similarly to the proof of Theorem 5.6.3 . One obtains the following results.

Theorem 5.6.4. *Let F be a number field such that $\mathbb{Q}(i) \nsubseteq F$, let $a \in F^\times$ and consider the elliptic curve $E : y^2 = x^3 - ax$ with complex multiplication by $\mathcal{O} = \mathbb{Z}[i]$.*

1. *If $a \in (F^\times)^2$ then $\delta_{E/F} = 0$;*
2. *If $-a \in (F^\times)^2$ then $\delta_{E/F} = \frac{1}{2}$;*
3. *If $\pm a \notin (F^\times)^2$ then*
$$\delta_{E/F} = \frac{1}{4} + \frac{C_{E,F}}{2} \cdot A_{\mathcal{O}}.$$

Theorem 5.6.5. *Let F be a number field such that $\mathbb{Q}(\zeta_3) \nsubseteq F$, let $a \in F^\times$ and consider the elliptic curve $E : y^2 = x^3 - a$ with complex multiplication by $\mathcal{O} = \mathbb{Z}[\zeta_3]$.*

1. *If $a \in (F^\times)^3$ then $\delta_{E/F} = \frac{1}{2}$;*
2. *If $a \notin (F^\times)^3$ then*
$$\delta_{E/F} = \frac{1}{2} + \frac{C_{E,F}}{2} \cdot A_{\mathcal{O}}.$$

In particular, the results proved in this section show that for a CM elliptic curve E defined over a field F not containing the CM field the cyclic reduction density $\delta_{E/F}$ never vanishes trivially, in the sense of Section 5.4.

5.7 Cyclic reduction densities for CM elliptic curves defined over $\mathbb{Q}$

In this final section we put together the results in Chapter 4 with the results in Section 5.6. The outcome is a computation, for every elliptic curve E defined over the rationals and with complex multiplication by an order $\mathcal{O}$ of discriminant $\Delta_{\mathcal{O}} < -4$, of the exact cyclic reduction density $\delta_{E/\mathbb{Q}}$. We achieve this by means of a two-step strategy.

As a first step, we determine the density $\delta_{E/K}$ for the base-change of E to the CM field K. By Theorem 5.6.1, this amounts to study the entanglement in the family of division fields $\mathcal{F} = \{K_\ell\}_\ell$ for ℓ prime. Since the entanglement in this family is at most quadratic as we know from Chapter 4, one can make use of the character-sum formula (5.9) to determine the exact correction factor to the naive density over K. Notice, however, that in order to avoid trivial terms in the character-sum formula it is necessary to precisely pin down the minimal squarefree integer $S \in \mathbb{N}$ for which the family $\{K_S, F_\ell\}_{\ell \nmid S}$ is linearly disjoint over K. In Theorem 4.5.2 we have studied the entanglement in the family $\mathcal{F}' = \{K(E[\ell^\infty])\}_\ell$ for ℓ prime. More precisely, we have classified all the possible images of the natural map

$$\operatorname{Gal}(K(E_{\text{tors}})/K) \hookrightarrow \prod_{\ell \text{ prime}} \operatorname{Gal}(K(E[\ell^\infty])/K)$$

for any given elliptic curve $E_{/\mathbb{Q}}$ with CM by an order of discriminant $\Delta_{\mathcal{O}} < -4$. This unfortunately is not enough for our purposes. Indeed, as we will see, it is possible that the family $\mathcal{F}'$ is entangled over K while the family $\mathcal{F}$ is linearly disjoint over the same field. This situation will be studied in detail. Once the density $\delta_{E/K}$ has been explicitly computed, the second step is to determine the density $\delta_{E/\mathbb{Q}}$ for the initial elliptic curve $E_{/\mathbb{Q}}$. This density can be obtained from a direct application of Theorem 5.6.3, which allows to descend over $\mathbb{Q}$ by looking at the congruence class of the discriminant of the CM order modulo 8.

A similar discussion could in principle be carried out also for elliptic curves with CM by the two orders of discriminant $\Delta_{\mathcal{O}} \in \{-3, -4\}$. However, for such an elliptic curve E the entanglement in the family $\mathcal{F}$ can be respectively sextic and quartic, thus leading to considerably more complicated general formulas for the density $\delta_{E/\mathbb{Q}}$. Rather than writing out all the details of a possible comprehensive computation in these cases, we have decided to focus on specific examples, which are in many ways more illuminating and give the flavour of what can happen in these particular situations.

Before stating our results, we recall some facts, proved in Section 4.5, concerning CM elliptic curves defined over the rationals. A CM elliptic curve E defined over $\mathbb{Q}$ can have complex multiplication only by an imaginary quadratic order $\mathcal{O}$ of class number 1, whose discriminant $\Delta_{\mathcal{O}}$ then belongs to the list

$$\Delta_{\mathcal{O}} \in \{-3, -4, -7, -8, -11, -12, -16, -19, -27, -28, -43, -67, -163\}.$$

For every such order $\mathcal{O}$ in an imaginary quadratic field K, there exist at most 4 non-isomorphic elliptic curves defined over $\mathbb{Q}$ with CM by $\mathcal{O}$ and whose conductor is minimal (in absolute value) among all their twists, see Table 4.1. From now on we consider only elliptic curves with complex multiplication by orders $\mathcal{O}$ of discriminant $\Delta_{\mathcal{O}} < -4$. By Theorem 4.5.2, for every such elliptic curve $E_{/\mathbb{Q}}$, there exist a unique elliptic curve $(E_0)_{/\mathbb{Q}}$ with CM by $\mathcal{O}$ and minimal conductor (if $\mathcal{O} = \mathbb{Z}[2i]$ minimal means divisible by the smallest amount of primes), and there exists a unique fundamental discriminant $\Delta \in \mathbb{Z}$ coprime with the absolute discriminant Δ_K of the CM field K such that E is the quadratic twist of E_0 by the quadratic field $\mathbb{Q}(\sqrt{\Delta})$. We denote this quadratic twist by $E_0^{(\Delta)}$ and we call the unique pair (E_0, Δ) as above the *twist type* of E, the integer Δ being the *twisting discriminant*. Note that if the twist type of the elliptic curve E has twisting discriminant $\Delta = 1$, then E is $\mathbb{Q}$-isomorphic to one of the elliptic curves with minimal conductor appearing in Table 4.1.

Before being completely ready to dive into our study of cyclic reduction densities, we need to prove a technical class-field theoretical result that will be repeatedly used in our analysis.

Proposition 5.7.1. *Let $\mathcal{O}$ be an order of discriminant $\Delta_{\mathcal{O}} < -4$ inside an imaginary quadratic field K. For every odd integer $M \in \mathbb{N}$ we have*

$$H_{2M,\mathcal{O}} = H_{2,\mathcal{O}} \cdot H_{M,\mathcal{O}}$$

where, for every $N \in \mathbb{N}$, we denote by $H_{N,\mathcal{O}}$ the ray class field modulo N of F relative to $\mathcal{O}$.

Proof. For $M = 1$ the result is trivially true, so we assume $M > 1$. Class Field Theory always implies the inclusion $H_{2,\mathcal{O}} \cdot H_{M,\mathcal{O}} \subseteq H_{2M,\mathcal{O}}$, but a priori this may not be an equality. The functoriality of the Artin isomorphism $\mathrm{Gal}(K^{\mathrm{ab}}/H_{\mathcal{O}}) \cong \widehat{\mathcal{O}}^{\times}/\mathrm{Im}(\mathcal{O}^{\times}) = \widehat{\mathcal{O}}^{\times}/\{\pm 1\}$ (see Theorem 3.3.6) gives, for every odd integer $M \in \mathbb{N}_{>1}$, the commutative diagram

$$\begin{tikzcd}
\mathrm{Gal}(H_{2M,\mathcal{O}}/H_{\mathcal{O}}) \arrow[r] \arrow[d, "\cong"] & \mathrm{Gal}(H_{2,\mathcal{O}}/H_{\mathcal{O}}) \times \mathrm{Gal}(H_{M,\mathcal{O}}/H_{\mathcal{O}}) \arrow[d, "\cong"] \\
(\mathcal{O}/2M\mathcal{O})^{\times}/\{\pm 1\} \arrow[r] & (\mathcal{O}/2\mathcal{O})^{\times} \times (\mathcal{O}/M\mathcal{O})^{\times}/\{\pm 1\}
\end{tikzcd}$$

where the upper horizontal map is the restriction of field automorphisms, the lower horizontal map is given by the pair of natural projections on the two factors and the vertical isomorphisms are induced by the Artin map. The proposition now follows after noticing the the lower horizontal map is precisely the isomorphism given by the Chinese Reminder Theorem. □

We now have all the tools to carry out the said explicit densities computations. While performing this study, one soon notices that some of the elliptic curves share a similar behaviour in terms of cyclic reduction densities. We formulate and divide our statements accordingly. In all the displayed numerical computations we have used SAGE [SAGE] and the results obtained in this section are summarized in Table 5.1.

Theorem 5.7.2. *Let $E_{/\mathbb{Q}}$ be an elliptic curve with complex multiplication by an order $\mathcal{O}$ of discriminant $\Delta_{\mathcal{O}} \in \{-11, -19, -27, -43, -67, -163\}$ and denote by (E_0, Δ) the twist type of E. Let $A_{\mathcal{O}}$ be the Artin constant relative to the order $\mathcal{O}$ and let $p = -\Delta_K$ be the unique prime dividing the discriminant of the CM field K.*

- *If $\Delta \equiv 1 \bmod 4$ then*

$$\delta_{E/\mathbb{Q}} = \frac{1}{2} + \frac{1}{2}\left(1 + \prod_{\ell \mid p\Delta} \frac{-1}{\#(\mathcal{O}/\ell\mathcal{O})^\times - 1}\right) A_{\mathcal{O}}$$

- *If $\Delta \equiv 0 \bmod 4$ then*

$$\delta_{E/\mathbb{Q}} = \frac{1}{2} + \frac{1}{2} A_{\mathcal{O}}.$$

Proof. Assume first of all that $\Delta = 1$, so that the elliptic curve E has minimal conductor among all its twists. Let $E_{/K}$ be the base-change of E to the CM field K. Then by Theorem 4.5.2, the family $\mathcal{F}'$ of ℓ^∞-division fields of $E_{/K}$ is linearly disjoint over K, and the field K_p is equal to the ray class field $H_{p,\mathcal{O}}$. In particular,

$$[K_p : K] = [H_{p,\mathcal{O}} : K] = \frac{1}{2} \cdot \#\,(\mathcal{O}/p\mathcal{O})^\times = \frac{1}{2} \cdot p(p-1)$$

which implies that we have to correct the naive cyclic reduction density $A_{\mathcal{O}}$ over K taking into account the minimality of the p-division field. This yields

$$\delta_{E/K} = \left(1 - \frac{2}{p(p-1)}\right)\left(1 - \frac{1}{p(p-1)}\right)^{-1} \cdot A_{\mathcal{O}} = \left(1 - \frac{1}{p(p-1)-1}\right) A_{\mathcal{O}}.$$

Since now $\Delta_{\mathcal{O}} \equiv 5 \bmod 8$, Theorem 5.6.3 gives

$$\delta_{E/\mathbb{Q}} = \frac{1}{2} + \frac{1}{2}\left(1 - \frac{1}{p(p-1)-1}\right) A_{\mathcal{O}}$$

concluding the proof in this case.

Suppose now that $\Delta \neq 1$ and $\Delta \equiv 1 \bmod 4$, so that $\Delta = \pm p_1 \cdot \ldots \cdot p_n$ with $p_i \in \mathbb{N}$ odd primes. By Theorem 4.5.2 the entanglement in the family $\mathcal{F}'$ is given by the intersection $K_{|\Delta|} \cap K_p = K(\sqrt{\Delta})$, and in particular the family $\mathcal{F}_{\Delta,p} = \{K_{p_1}, \ldots, K_{p_n}, K_p\}$ is entangled over K. We want to show that $\mathcal{F}_{\Delta,p}$ is the smallest possible entangled subfamily of $\mathcal{F}$, *i.e.* that for every $S \subsetneq \{p, p_1, \ldots, p_n\}$ the family $\{K_\ell\}_{\ell \in S}$ is linearly disjoint over K. Since the family $\{K_{p_1}, \ldots, K_{p_n}\}$ is linearly disjoint over K (because the entanglement in the family of ℓ-division fields of E is at most quadratic), it suffices to prove that $K_N \cap K_p = K$ for every integer $N = \prod_{\ell \in S} \ell$ with $S \subsetneq \{p_1, \dots, p_n\}$. Fixed such an integer $N = p_{j_1} \cdot \dots \cdot p_{j_r}$, we show that $K(\sqrt{\Delta})$ is not contained in the division field K_N.

Let $H_{N,\mathcal{O}} \subseteq K_N$ be the ray class field of K modulo N relative to the order $\mathcal{O}$. The extension $K \subseteq H_{N,\mathcal{O}}$ can be ramified only at primes dividing pN. On the other hand, the extension $K \subseteq K(\sqrt{\Delta})$ is certainly ramified at some prime $\mathfrak{p} \subseteq K$ not dividing pN since, by definition of twist type, Δ is coprime with p and, by assumption, there is at least one prime that divides Δ but that does not divide N. Hence $K(\sqrt{\Delta}) \cap H_{N,\mathcal{O}} = K$.

Let us now consider the intersection $H_{N,\mathcal{O}}(\sqrt{\Delta}) \cap K_N$. Since $[K_N : H_{N,\mathcal{O}}] \leq 2$, if this intersection is not equal to $H_{N,\mathcal{O}}$, we must have $K_N = H_N(\sqrt{\Delta})$. Suppose by contradiction that this is the case. Then the mod N Galois representation for $E_{/K}$ has maximal image. On the other hand, also the mod N Galois representation of E_0 has maximal image, as follows from Theorem 4.5.2 and from the fact that N is coprime with p. However, since $E_0 = E^{(\Delta)}$, this contradicts Proposition 4.4.1 [1]. We deduce that $H_{N,\mathcal{O}}(\sqrt{\Delta}) \cap K_N = H_{N,\mathcal{O}}$, so that

$$K(\sqrt{\Delta}) \cap K_N = K(\sqrt{\Delta}) \cap H_{N,\mathcal{O}}(\sqrt{\Delta}) \cap K_N = K(\sqrt{\Delta}) \cap H_{N,\mathcal{O}} = K$$

which proves the minimality of the family $\mathcal{F}_{\Delta,p}$.

We can now use the character sum formula (5.9) to deduce that

$$\delta_{E/K} = \left(1 + \prod_{\ell \mid p\Delta} \frac{-1}{\#(\mathcal{O}/\ell\mathcal{O})^\times - 1}\right) A_{\mathcal{O}}$$

and use Theorem 5.6.3 to get the wanted statement over $\mathbb{Q}$.

Suppose finally that $\Delta \equiv 0 \bmod 4$, so that we can write $\Delta = \pm 2^a \cdot p_1 \cdot \dots \cdot p_n$ with $a \in \{2, 3\}$. Again by Theorem 4.5.2 we know that $K_p \cap K_{|\Delta|} = K(\sqrt{\Delta})$, and that this is the only entanglement in the family $\mathcal{F}'$. Nevertheless, we are going to prove that the family $\{K_2, K_{p_1}, \dots, K_{p_n}, K_p\}$ is linearly disjoint over K. To this aim, it is again sufficient to prove that, if $N := 2 \cdot p_1 \cdot \dots \cdot p_n \in \mathbb{N}$, then $K(\sqrt{\Delta}) \cap K_N = K$.

Certainly the fields $K(\sqrt{\Delta})$ and $H_{N/2,\mathcal{O}}$ are linearly disjoint over K since by assumption every prime above 2 ramifies in $K \subseteq K(\sqrt{\Delta})$ but cannot ramify in $K \subseteq H_{N/2,\mathcal{O}}$. Furthermore, we have $H_{N/2,\mathcal{O}}(\sqrt{\Delta}) \cap H_{N,\mathcal{O}} = H_{N/2,\mathcal{O}}$ since, by Proposition 5.7.1, we have

$$[H_{N,\mathcal{O}} : H_{N/2,\mathcal{O}}] = [H_{2,\mathcal{O}} : K] = \#(\mathcal{O}/2\mathcal{O})^\times = 3$$

where the last equality follows from the fact that $\Delta_{\mathcal{O}} \equiv 5 \bmod 8$. Finally, again by Proposition 4.4.1 [1] applied as in the previous case, one also has $H_{N,\mathcal{O}}(\sqrt{\Delta}) \cap K_N = H_{N,\mathcal{O}}$. All this implies that $K(\sqrt{\Delta}) \cap K_N = K$, thus proving that the family $\{K_2, K_{p_1}, \dots, K_{p_n}, K_p\}$ is linearly disjoint over K. This means that $\delta_{E/K}$ is equal to the naive density $A_{\mathcal{O}}$ in this case. By applying Theorem 5.6.3, we obtain

$$\delta_{E/\mathbb{Q}} = \frac{1}{2} + \frac{1}{2} A_{\mathcal{O}}$$

and the proof is concluded. □

Example 5.7.3. Let E_0 be the elliptic curve with LMFDB label 27.*a*2, defined by the Weierstrass equation

$$E_0 : y^2 + y = x^3 - 30x + 63.$$

Then E_0 has complex multiplication by the order $\mathcal{O} = \mathbb{Z}[3\zeta_3]$ and it has minimal conductor among all its twists, hence its twist type is $(E_0, 1)$. According to Theorem 5.7.2, the expected cyclic reduction density is

$$\delta_{\text{exp}} = \frac{1}{2} + \frac{2}{5}A_{\mathcal{O}} \approx 0.7004$$

and a numerical computation of the fraction of primes up to 10^6 that are of cyclic reduction for E_0 gives

$$\delta_{\text{num}} \approx 0.7012$$

an excellent numerical agreement. Consider now the elliptic curve E defined by the Weierstrass equation

$$E : y^2 = x^3 - 480x - 4048$$

with LMFDB label 432.e2 and twist type $(E_0, -4)$. Then according to Theorem 5.7.2, the expected cyclic reduction density is

$$\delta_{\text{exp}} = \frac{1}{2} + \frac{1}{2}A_{\mathcal{O}} \approx 0.7505$$

and a numerical computation as above gives

$$\delta_{\text{num}} \approx 0.7518$$

again a good agreement.

The proof of the subsequent results is very similar to the one just presented for Theorem 5.7.2, so we decided to sketch only the parts where the arguments differ from the ones above.

Theorem 5.7.4. *Let $E_{/\mathbb{Q}}$ be an elliptic curve with complex multiplication by the order $\mathcal{O} \subseteq K$ of discriminant $\Delta_{\mathcal{O}} \in \{-12, -28\}$ and denote by (E_0, Δ) the twist type of E. Let $A_{\mathcal{O}}$ be the Artin constant relative to the order $\mathcal{O}$ and let $p = -\Delta_K$ be the unique prime dividing the discriminant of the CM field K.*

- *If $\Delta \equiv 1 \bmod 4$ or $\Delta \equiv 4 \bmod 8$ then*

$$\delta_{E/\mathbb{Q}} = \frac{1}{4} + \frac{1}{2}\left(1 + \prod_{\ell \mid p\Delta} \frac{-1}{(\mathcal{O}/\ell\mathcal{O})^\times - 1}\right)A_{\mathcal{O}}$$

- *If $\Delta \equiv 0 \bmod 8$ then*

$$\delta_{E/\mathbb{Q}} = \frac{1}{4} + \frac{1}{2}A_{\mathcal{O}}.$$

Proof. First of all we consider the case $\Delta_{\mathcal{O}} = -28$. If $\Delta \equiv 1 \bmod 4$ then the proof works out, mutatis mutandis, in the same way as the proof of the analogous case in Theorem 5.7.2. Suppose then that $\Delta \equiv 0 \bmod 4$, so that we can write $\Delta = \pm 2^a p_1 \cdot \ldots \cdot p_n$ with $p_i \in \mathbb{N}$ odd primes and $a \in \{2, 3\}$. In this case Theorem 4.5.2 implies that $K_p \cap K_{|\Delta|} = K(\sqrt{\Delta})$, and this intersection explains all the entanglement in the family $\mathcal{F}'$.

If $\Delta \equiv 4 \bmod 8$ then, using the fact that $H_{2,\mathcal{O}} = K(i)$, one sees that $K(\sqrt{\Delta}) \subseteq K_N$, where $N = \prod_{\ell \mid \Delta} \ell$ is the radical of Δ. Moreover, with the same strategy used in the proof of Theorem

5.7.2, it is possible to show that $\{K_2, K_{p_1}, \ldots, K_{p_n}, K_7\}$ is the minimal family of ℓ-division fields which is entangled over K. This gives the density

$$\delta_{E/K} = \left(1 + \prod_{\ell \mid 7\Delta} \frac{-1}{(\mathcal{O}/\ell\mathcal{O})^\times - 1}\right) A_\mathcal{O}$$

and the desired density over $\mathbb{Q}$ can be obtained using Theorem 5.6.3.

On the other hand, if $\Delta \equiv 0 \bmod 8$, one can prove by means of Proposition 5.7.1 that the family $\{K_2, K_{p_1}, \ldots, K_{p_n}, K_7\}$ is linearly disjoint over K. The proof is similar to the proof of the analogous statement in Theorem 5.7.2, and we omit it.

In the case $\Delta_\mathcal{O} = -12$ one can mimic the same arguments, after noticing that the 3-division field of the elliptic curve E_0 is equal to $H_{3,\mathcal{O}} = K(\sqrt[3]{2}) = \mathbb{Q}(\zeta_3, \sqrt[3]{2})$ while $H_{2,\mathcal{O}} = K(i) = \mathbb{Q}(\zeta_3, i)$. □

Example 5.7.5. Let E_0 be the elliptic curve with LMFDB label 36.*a*2, defined by the Weierstrass equation

$$E_0 : y^2 = x^3 - 15x + 22.$$

The curve E_0 has complex multiplication by the order $\mathcal{O} = \mathbb{Z}[\sqrt{3}]$ and it has minimal conductor among all its twists, so that its twist type is $(E_0, 1)$. According to Theorem 5.7.4, the expected cyclic reduction density is

$$\delta_{\text{exp}} = \frac{1}{4} + \frac{2}{5} A_\mathcal{O} \approx 0.4003$$

while a numerical computation of the fraction of primes up to 10^6 of cyclic reduction for E_0 gives

$$\delta_{\text{num}} = 0.4006$$

an excellent agreement. Consider now the elliptic curve E defined by the Weierstrass equation

$$E : y^2 = x^3 - 60x + 176$$

with LMFDB label 576.*e*2 and twist type $(E_0, 8)$. Then according to Theorem 5.7.4, the expected cyclic reduction density is

$$\delta_{\text{exp}} = \frac{1}{4} + \frac{1}{2} A_\mathcal{O} \approx 0.4379$$

and a numerical computation as above gives

$$\delta_{\text{num}} \approx 0.4377$$

again a good agreement.

Theorem 5.7.6. *Let $E_{/\mathbb{Q}}$ be an elliptic curve with complex multiplication by the order $\mathcal{O}$ of discriminant $\Delta_\mathcal{O} = -7$. Then $\delta_{E/\mathbb{Q}} = \frac{1}{2}$.*

Proof. This is an immediate application of Theorem 5.6.3. □

Theorem 5.7.7. *Let $E_{/\mathbb{Q}}$ be an elliptic curve with complex multiplication by an order $\mathcal{O} \subsetneq K$ of discriminant $\Delta_\mathcal{O} \in \{-8, -16\}$. Let $A_\mathcal{O}$ be the Artin constant relative to the order $\mathcal{O}$. Then*

$$\delta_{E/\mathbb{Q}} = \frac{1}{4} + \frac{1}{2} A_\mathcal{O} \approx \begin{cases} 0.4201 & \text{if } \Delta_\mathcal{O} = -8 \\ 0.4443 & \text{if } \Delta_\mathcal{O} = -16 \end{cases}$$

and in particular the density does not depend on the twist type of E.

Proof. Let (E_0, Δ) be the twist type of E. If $\Delta = 1$ then by Theorem 4.5.2 the family $\mathcal{F}$ is linearly disjoint over K. On the other hand, if $\Delta \neq 1$ we have again by Theorem 4.5.2 that $K_8 \cap K_{|\Delta|} = K(\sqrt{\Delta})$ and this is the only cause of entanglement in the family $\mathcal{F}'$. We claim that the family $\mathcal{F}$ is linearly disjoint over K. This amounts to show that $K_2 \cap K_{|\Delta|} = K$.

Since in the hypotheses of the theorem we have $[K_2 : K] = 2$, if the previous intersection were non-trivial we would obtain $K_2 = K(\sqrt{\Delta})$. However $K_2 = H_{2,\mathcal{O}}$ is the ray class field modulo 2 for K, which can only ramify at primes above 2. Since by definition of twist type Δ must be odd, this is a contradiction and we obtain $K_2 \cap K_{|\Delta|} = F$, as we wanted to show. Therefore, over K we always have $\delta_{E/K} = A_{\mathcal{O}}$, and we obtain the corresponding density over $\mathbb{Q}$ using Theorem 5.6.3. □

Example 5.7.8. Let E_0, E_1, E_2 be the three elliptic curves with complex multiplication by $\mathbb{Z}[\sqrt{-2}]$ given by

$E_0 : y^2 = x^3 - x^2 - 3x - 1,$	LMFDB label: $256.d2$,	twist type: $(E_0, 1)$
$E_1 : y^2 = x^3 - 30x + 56,$	LMFDB label: $2304.h2$,	twist type: $(E_0, -3)$
$E_2 : y^2 = x^3 + x^2 - 83x - 287,$	LMFDB label: $6400.a2$,	twist type: $(E_0, 5)$.

Then a numerical computation shows that, for the three elliptic curves, the fraction of primes up to 10^6 of cyclic reduction is respectively

$$\delta_{E_0,\mathrm{num}} \approx 0.4197, \qquad \delta_{E_1,\mathrm{num}} \approx 0.4196, \qquad \delta_{E_2,\mathrm{num}} \approx 0.4199$$

in accordance with Theorem 5.7.7.

We conclude this section by discussing what happens for elliptic curves $E/\mathbb{Q}$ with complex multiplication by an order $\mathcal{O}$ of discriminant $\Delta_{\mathcal{O}} \in \{-3, -4\}$ *i.e.* with $\mathcal{O} = \mathbb{Z}[\zeta_3]$ or $\mathcal{O} = \mathbb{Z}[i]$ respectively. Such an elliptic curve admits a Weierstrass model over the rationals of the form

$$\begin{aligned} E : y^2 &= x^3 + d, && \text{if } \Delta_{\mathcal{O}} = -3, \\ E : y^2 &= x^3 + dx, && \text{if } \Delta_{\mathcal{O}} = -4, \end{aligned}$$

with $d \in \mathbb{Z}$ a non-zero integer. Studying the cyclic reduction density of these elliptic curves is more involved, and ultimately the main reason is to be found in the fact that the unit group $\mathcal{O}^\times$ has order $n > 2$. This implies, on the one hand, that the entanglement in the family $\mathcal{F}$ may be not quadratic anymore, and, on the other hand, that there are more possibilities for twisting the elliptic curve E, in principle all leading to different expressions for the seeked densities. Another important difference with the cases $\Delta_{\mathcal{O}} < -4$ is that for such an elliptic curve E the 2-division field does not need to be equal to the ray class field modulo 2 for the order $\mathcal{O}$, and thus it is not invariant under twisting. However, since the 2-division field can be easily read from the given model of E, this is more a bothering complication than a substantial problem.

For all these reasons, we decided not to provide general formulas for the density $\delta_{E/\mathbb{Q}}$ in these cases, but rather to give explicit examples which are significant of the possible situations that can arise.

Example 5.7.9. In this example we consider some elliptic curves defined over $\mathbb{Q}$ with complex multiplication by $\mathcal{O} = \mathbb{Z}[i] \subseteq \mathbb{Q}(i) =: K$. For simplicity, we denote by H_N the ray class field modulo N of K and by conductor of an elliptic curve defined over $\mathbb{Q}$ we always mean the positive generator of its conductor ideal.

As a first example, we study the cyclic reduction density of the elliptic curve

$$E_{-2}/\mathbb{Q}: \; y^2 = x^3 - 2x$$

with conductor $\mathfrak{f}_{E_{-2}} = 2^8$. Its 2-division field $\mathbb{Q}(\sqrt{2})$ is linearly disjoint from the CM field K, so that $[K_2 : K] = 2 = \#(\mathcal{O}/2\mathcal{O})^\times$. By Theorem 5.6.2, all the other division fields over $\mathbb{Q}$ contain K, so for our purposes we can reduce to study the family of division fields K_N, with N squarefree, associated to the base-change $E_{/K}$. By Theorem 4.3.4 this family is linearly disjoint over K and by Proposition 4.3.2 all the division fields K_N with squarefree $N > 3$ have maximal degree $[K_N : K] = \#(\mathcal{O}/N\mathcal{O})^\times$. Using Theorem 5.6.4 we obtain

$$\delta_{E_{-2}/\mathbb{Q}} = \frac{1}{4} + \frac{1}{2} A_{\mathcal{O}} \approx 0.4443$$

and a numerical computation provides an approximate density of 0.4445.

We now twist the elliptic curve E_{-2} by $\mathbb{Q}(\sqrt[4]{3})$. A representative for the $\mathbb{Q}$-isomorphism class of this twist is given by

$$E_{-6}/\mathbb{Q} : y^2 = x^3 - 6x$$

with conductor $\mathfrak{f}_{E_{-6}} = 2^8 3^2$. Again the 2-division field $\mathbb{Q}(\sqrt{6})$ is quadratic over the rationals and we can reduce to study the division fields of $E_{/K}$. By Theorem 4.3.4 the family $\{K_6, K_\ell\}_{\ell > 3 \text{ prime}}$ is linearly disjoint over K. On the other hand, the extension $K \subseteq F_3$ is cyclic and can contain at most one quadratic subextension. By the properties of the Weil pairing [Sil09, III, Corollary 8.1.1], this extension is given by $K(\zeta_3) = K(\sqrt{-3})$ and we deduce that $K_2 \cap K_3 = K$, so that already the family $\{K_\ell\}_{\ell \text{ prime}}$ is linearly disjoint over K. We remark that it is not true that the family $\{K_{\ell^\infty}\}_{\ell \text{ prime}}$ is linearly disjoint over K: one can see that $K_8 \cap K_3 = K(\sqrt[4]{3})$. As in the first case, the expected cyclic reduction density in this case is

$$\delta_{E_{-6}/\mathbb{Q}} = \frac{1}{4} + \frac{1}{2} A_{\mathcal{O}} \approx 0.4443$$

which agrees with the numerical datum 0.4447.

The elliptic curve

$$E_{-1}/\mathbb{Q} : y^2 = x^3 - x$$

has $\delta_{E_{-1}/\mathbb{Q}} = 0$ since its 2-torsion is all defined over the rationals. We consider its twist by $\mathbb{Q}(\sqrt[4]{3})$ given by the model

$$E_{-3}/\mathbb{Q} : y^2 = x^3 - 3x$$

of conductor $\mathfrak{f}_{E_{-3}} = 2^6 3^2$. Also in this case the 2-division field $\mathbb{Q}(\sqrt{3})$ is quadratic over the rationals and we can reduce to study the division fields of $E_{/K}$. By Theorem 4.3.4 the family $\{K_6, K_\ell\}_{\ell > 3 \text{ prime}}$ is linearly disjoint over K. On the other hand, we see that the field $K_2 = K(\sqrt{3})$ is equal to the ray class field $H_3 = K(\zeta_3)$, and the latter is contained in K_3. We conclude that $K_2 \cap K_3 = K_2 = K(\sqrt{3})$. Using the character-sum formula (5.9), we deduce that the expected density in this case is given by

$$\delta_{E_{-3}/\mathbb{Q}} = \frac{1}{4} + \frac{4}{7} A_{\mathcal{O}} \approx 0.4721$$

while a numerical computation gives an approximate density of 0.4724. An excellent agreement.

$\Delta_{\mathcal{O}}$	Approximate $A_{\mathcal{O}}$	Twisting discriminant Δ	$\delta_{E/\mathbb{Q}}$
-7	0	any Δ	$\frac{1}{2}$
-8	0.3403	any Δ	$\frac{1}{4}+\frac{1}{2}A_{\mathcal{O}}$
-11	0.4445	$\Delta \equiv 1 \bmod 4$	$\frac{1}{2}+\frac{1}{2}\left(1+\prod_{\ell \mid 11\Delta}\frac{-1}{\#(\mathcal{O}/\ell\mathcal{O})^{\times}-1}\right)A_{\mathcal{O}}$
		$\Delta \equiv 0 \bmod 4$	$\frac{1}{2}+\frac{1}{2}A_{\mathcal{O}}$
-12	0.3758	$\Delta \equiv 1 \bmod 4$	$\frac{1}{4}+\frac{1}{2}\left(1+\prod_{\ell \mid 3\Delta}\frac{-1}{(\mathcal{O}/\ell\mathcal{O})^{\times}-1}\right)A_{\mathcal{O}}$
		$\Delta \equiv 4 \bmod 8$	$\frac{1}{4}+\frac{1}{2}\left(1+\prod_{\ell \mid 3\Delta}\frac{-1}{(\mathcal{O}/\ell\mathcal{O})^{\times}-1}\right)A_{\mathcal{O}}$
		$\Delta \equiv 0 \bmod 8$	$\frac{1}{4}+\frac{1}{2}A_{\mathcal{O}}$
-16	0.3887	any Δ	$\frac{1}{4}+\frac{1}{2}A_{\mathcal{O}}$
-19	0.5142	$\Delta \equiv 1 \bmod 4$	$\frac{1}{2}+\frac{1}{2}\left(1+\prod_{\ell \mid 19\Delta}\frac{-1}{\#(\mathcal{O}/\ell\mathcal{O})^{\times}-1}\right)A_{\mathcal{O}}$
		$\Delta \equiv 0 \bmod 4$	$\frac{1}{2}+\frac{1}{2}A_{\mathcal{O}}$
-27	0.5011	$\Delta \equiv 1 \bmod 4$	$\frac{1}{2}+\frac{1}{2}\left(1+\prod_{\ell \mid 3\Delta}\frac{-1}{\#(\mathcal{O}/\ell\mathcal{O})^{\times}-1}\right)A_{\mathcal{O}}$
		$\Delta \equiv 0 \bmod 4$	$\frac{1}{2}+\frac{1}{2}A_{\mathcal{O}}$
-28	0.3960	$\Delta \equiv 1 \bmod 4$	$\frac{1}{4}+\frac{1}{2}\left(1+\prod_{\ell \mid 7\Delta}\frac{-1}{(\mathcal{O}/\ell\mathcal{O})^{\times}-1}\right)A_{\mathcal{O}}$
		$\Delta \equiv 4 \bmod 8$	$\frac{1}{4}+\frac{1}{2}\left(1+\prod_{\ell \mid 7\Delta}\frac{-1}{(\mathcal{O}/\ell\mathcal{O})^{\times}-1}\right)A_{\mathcal{O}}$
		$\Delta \equiv 0 \bmod 8$	$\frac{1}{4}+\frac{1}{2}A_{\mathcal{O}}$
-43	0.5288	$\Delta \equiv 1 \bmod 4$	$\frac{1}{2}+\frac{1}{2}\left(1+\prod_{\ell \mid 43\Delta}\frac{-1}{\#(\mathcal{O}/\ell\mathcal{O})^{\times}-1}\right)A_{\mathcal{O}}$
		$\Delta \equiv 0 \bmod 4$	$\frac{1}{2}+\frac{1}{2}A_{\mathcal{O}}$
-67	0.5301	$\Delta \equiv 1 \bmod 4$	$\frac{1}{2}+\frac{1}{2}\left(1+\prod_{\ell \mid 67\Delta}\frac{-1}{\#(\mathcal{O}/\ell\mathcal{O})^{\times}-1}\right)A_{\mathcal{O}}$
		$\Delta \equiv 0 \bmod 4$	$\frac{1}{2}+\frac{1}{2}A_{\mathcal{O}}$
-163	0.5306	$\Delta \equiv 1 \bmod 4$	$\frac{1}{2}+\frac{1}{2}\left(1+\prod_{\ell \mid 163\Delta}\frac{-1}{\#(\mathcal{O}/\ell\mathcal{O})^{\times}-1}\right)A_{\mathcal{O}}$
		$\Delta \equiv 0 \bmod 4$	$\frac{1}{2}+\frac{1}{2}A_{\mathcal{O}}$

Table 5.1: Cyclic reduction densities for elliptic curves over $\mathbb{Q}$ with CM by an order of discriminant < -4.

Bibliography

[Abe28] N. H. Abel. *Recherches sur les fonctions elliptiques. (Suite du mémoire Nr. 12. tom. II. cah. 2 de ce journal).* In: *J. Reine Angew. Math.* 3 (1828), pp. 160–190 (cit. on p. ix).

[Aka+20] M. Aka, M. Luethi, P. Michel, and A. Wieser. *Simultaneous supersingular reductions of CM elliptic curves*. arXiv:2005.01537. 2020 (cit. on pp. 11, 12).

[And98] Y. André. *Finitude des couples d'invariants modulaires singuliers sur une courbe algébrique plane non modulaire*. In: *J. Reine Angew. Math.* 505 (1998), pp. 203–208 (cit. on p. 14).

[Apo76] T. M. Apostol. *Introduction to analytic number theory*. Undergraduate Texts in Mathematics. Springer-Verlag, New York-Heidelberg, 1976, pp. xii+338 (cit. on p. 119).

[AT68] E. Artin and J. Tate. *Class field theory*. W. A. Benjamin, Inc., New York-Amsterdam, 1968 (cit. on p. 72).

[Art65] E. Artin. *The collected papers of Emil Artin*. Edited by Serge Lang and John T. Tate. Addison–Wesley Publishing Co., Inc., Reading, Mass.-London, 1965, xvi+560 pp. (2 plates) (cit. on p. 112).

[ALL] E. Artin, D. H. Lehmer, and E. Lehmer. *Correspondence 1957-1958*. In: Archives of D. H. Lehmer, Bancroft Library, Berkley (cit. on p. 111).

[AT09] E. Artin and J. Tate. *Class field theory*. Reprinted with corrections from the 1967 original. AMS Chelsea Publishing, Providence, RI, 2009, pp. viii+194 (cit. on p. 67).

[AM69] M. F. Atiyah and I. G. Macdonald. *Introduction to commutative algebra*. Addison-Wesley Publishing Co., Reading, Mass.-London-Don Mills, Ont., 1969, pp. ix+128 (cit. on p. 1).

[BIR08] M. Baker, S.-i. Ih, and R. Rumely. *A finiteness property of torsion points*. In: *Algebra Number Theory* 2.2 (2008), pp. 217–248 (cit. on p. 19).

[Ber28] W. E. H. Berwick. *Modular Invariants Expressible in Terms of Quadratic and Cubic Irrationalities*. In: *Proc. London Math. Soc. (2)* 28.1 (1928), pp. 53–69 (cit. on pp. 13, 14).

[BHK20] Y. Bilu, P. Habegger, and L. Kühne. *No Singular Modulus Is a Unit*. In: *Int. Math. Res. Not. IMRN* 24 (2020), pp. 10005–10041 (cit. on pp. 16, 17, 42, 43, 45, 46, 51, 52).

[BMZ13] Y. Bilu, D. Masser, and U. Zannier. *An effective "theorem of André" for CM-points on a plane curve*. In: *Math. Proc. Cambridge Philos. Soc.* 154.1 (2013), pp. 145–152 (cit. on p. 14).

[BG06] E. Bombieri and W. Gubler. *Heights in Diophantine geometry*. Vol. 4. New Mathematical Monographs. Cambridge University Press, Cambridge, 2006, pp. xvi+652 (cit. on pp. 43, 45).

[Bou89] N. Bourbaki. *Commutative algebra. Chapters 1–7*. Springer-Verlag, Berlin, 1989 (cit. on p. 74).

[BCS17] A. Bourdon, P. Clark, and J. Stankewicz. *Torsion points on CM elliptic curves over real number fields*. In: *Transactions of the American Mathematical Society* 369.12 (2017), pp. 8457–8496 (cit. on p. 78).

[BC20] A. Bourdon and P. L. Clark. *Torsion points and Galois representations on CM elliptic curves*. In: *Pacific Journal of Mathematics* 305.1 (2020), pp. 43–88 (cit. on pp. xi, 59, 60).

[BJ16] J. Brau and N. Jones. *Elliptic curves with 2-torsion contained in the 3-torsion field*. In: *Proc. Amer. Math. Soc.* 144.3 (2016), pp. 925–936 (cit. on p. 83).

[Bum13] D. Bump. *Lie groups*. Second edition. Vol. 225. Graduate Texts in Mathematics. Springer, New York, 2013, pp. xiv+551 (cit. on p. 116).

[Cai21] Y. Cai. *Bounding the difference of two singular moduli*. In: *Moscow Journal of Combinatorics and Number Theory* 10.2 (2021), pp. 95–110 (cit. on pp. 42, 43, 45, 48).

[Cam21a] F. Campagna. *Effective bounds on differences of singular moduli that are S-units*. arXiv:2102.06396. 2021 (cit. on pp. i, iii).

[Cam21b] F. Campagna. *On singular moduli that are S-units*. In: *Manuscripta Math.* 166.1-2 (2021), pp. 73–90 (cit. on pp. i, iii).

[CP21] F. Campagna and R. Pengo. *Entanglement in the family of division fields of elliptic curves with complex multiplication*. In: *Pacific journal of mathematics* (to appear). 2021 (cit. on pp. i, iii).

[CS19] F. Campagna and P. Stevenhagen. *Cyclic reduction of Elliptic Curves*. arXiv:2001.00028. 2019 (cit. on pp. i, iii).

[Che] J. Chen. *Surjections of unit groups and semi-inverses*. In: *Journal of Commutative Algebra* (to appear) (cit. on p. 73).

[CU04] L. Clozel and E. Ullmo. *Équidistribution des points de Hecke*. In: *Contributions to automorphic forms, geometry, and number theory*. Johns Hopkins Univ. Press, Baltimore, MD, 2004, pp. 193–254 (cit. on p. 16).

[CW77] J. Coates and A. Wiles. *On the conjecture of Birch and Swinnerton-Dyer*. In: *Inventiones mathematicæ* 39.3 (1977), pp. 223–251 (cit. on p. 95).

[CS08] H. Cohen and P. Stevenhagen. *Computational class field theory*. In: *Algorithmic number theory: lattices, number fields, curves and cryptography*. Vol. 44. Math. Sci. Res. Inst. Publ. Cambridge Univ. Press, Cambridge, 2008, pp. 497–534 (cit. on p. 67).

[Coj03] A. C. Cojocaru. *Cyclicity of CM elliptic curves modulo p*. In: *Trans. Amer. Math. Soc.* 355.7 (2003), pp. 2651–2662 (cit. on pp. 127, 130, 131).

[Col98] P. Colmez. *Sur la hauteur de Faltings des variétés abéliennes à multiplication complexe*. In: *Compositio Math.* 111.3 (1998), pp. 359–368 (cit. on pp. 15, 42, 50).

[Con04] B. Conrad. *Gross-Zagier revisited*. In: *Heegner points and Rankin L-series*. Vol. 49. Math. Sci. Res. Inst. Publ. With an appendix by W. R. Mann. Cambridge Univ. Press, Cambridge, 2004, pp. 67–163 (cit. on pp. 32, 36).

[Con] K. Conrad. *The conductor ideal*. Available at: https://kconrad.math.uconn.edu/blurbs/ (cit. on pp. 2, 65).

[Cox12] D. A. Cox. *Galois theory*. Second. Pure and Applied Mathematics (Hoboken). John Wiley & Sons, Inc., Hoboken, NJ, 2012, pp. xxviii+570 (cit. on p. x).

[Cox13] D. A. Cox. *Primes of the form $x^2 + ny^2$*. Second. Pure and Applied Mathematics (Hoboken). Fermat, class field theory, and complex multiplication. John Wiley & Sons, Inc., Hoboken, NJ, 2013, pp. xviii+356 (cit. on pp. 4, 8, 87, 91, 101, 102).

[Del85] P. Deligne. *Preuve des conjectures de Tate et de Shafarevitch (d'après G. Faltings)*. In: 121-122. Seminar Bourbaki, Vol. 1983/84. 1985, pp. 25–41 (cit. on p. 50).

[Deu41] M. Deuring. *Die typen der multiplikatorenringe elliptischer funktionenkörper*. In: *Abhandlungen aus dem mathematischen Seminar der Universität Hamburg*. Vol. 14. 1. Springer. 1941, pp. 197–272 (cit. on pp. 10, 59).

[Duk88] W. Duke. *Hyperbolic distribution problems and half-integral weight Maass forms*. In: *Invent. Math.* 92.1 (1988), pp. 73–90 (cit. on pp. 16, 18).

[Eis95] D. Eisenbud. *Commutative algebra*. Vol. 150. Graduate Texts in Mathematics. Springer-Verlag, New York, 1995 (cit. on pp. 73, 74).

[Elk87] N. D. Elkies. *The existence of infinitely many supersingular primes for every elliptic curve over $\mathbb{Q}$*. In: *Invent. Math.* 89.3 (1987), pp. 561–567 (cit. on p. 10).

[Elk89] N. D. Elkies. *Supersingular primes for elliptic curves over real number fields*. In: *Compositio Math.* 72.2 (1989), pp. 165–172 (cit. on p. 10).

[Fal83] G. Faltings. *Endlichkeitssätze für abelsche Varietäten über Zahlkörpern*. In: *Invent. Math.* 73.3 (1983), pp. 349–366 (cit. on p. 50).

[FR18] B. Faye and A. Riffaut. *Fields generated by sums and products of singular moduli*. In: *J. Number Theory* 192 (2018), pp. 37–46 (cit. on pp. 43, 44).

[GR14] É. Gaudron and G. Rémond. *Théorème des périodes et degrés minimaux d'isogénies*. In: *Comment. Math. Helv.* 89.2 (2014), pp. 343–403 (cit. on p. 50).

[GS00] A. Granville and H. M. Stark. *abc implies no "Siegel zeros" for L-functions of characters with negative discriminant*. In: *Invent. Math.* 139.3 (2000), pp. 509–523 (cit. on p. 52).

[Gra03] G. Gras. *Class field theory*. Springer Monographs in Mathematics. Springer-Verlag, Berlin, 2003 (cit. on p. 100).

[Gro86] B. H. Gross. *On canonical and quasicanonical liftings*. In: *Invent. Math.* 84.2 (1986), pp. 321–326 (cit. on p. 32).

[Gro87] B. H. Gross. *Heights and the special values of L-series*. In: *Number theory (Montreal, Que., 1985)*. Vol. 7. CMS Conf. Proc. Amer. Math. Soc., Providence, RI, 1987, pp. 115–187 (cit. on p. 30).

[GZ85] B. H. Gross and D. B. Zagier. *On singular moduli*. In: *J. Reine Angew. Math.* 355 (1985), pp. 191–220 (cit. on pp. 14, 17, 32, 36, 41, 55, 56).

[GM90] R. Gupta and M. R. Murty. *Cyclicity and generation of points mod p on elliptic curves*. In: *Invent. Math.* 101.1 (1990), pp. 225–235 (cit. on p. 122).

[Gur] L. Gurney. *Frobenius lifts and elliptic curves with complex multiplication*. In: *Algebra & Number Theory (to appear)* (cit. on p. 96).

[Hab15] P. Habegger. *Singular moduli that are algebraic units*. In: *Algebra Number Theory* 9.7 (2015), pp. 1515–1524 (cit. on pp. 15, 16, 18, 42).

[HMR20] S. Herrero, R. Menares, and J. Rivera-Letelier. *p-adic distribution of CM points and Hecke orbits I: Convergence towards the Gauss point*. In: *Algebra Number Theory* 14.5 (2020), pp. 1239–1290 (cit. on pp. 18, 22).

[HMR21a] S. Herrero, R. Menares, and J. Rivera-Letelier. *p-Adic distribution of CM points and Hecke orbits. II: Linnik equidistribution on the supersingular locus*. arXiv:2102.04865. 2021 (cit. on pp. 18, 22).

[HMR21b] S. Herrero, R. Menares, and J. Rivera-Letelier. *There are at most finitely many singular moduli that are S-units*. arXiv:2102.05041. 2021 (cit. on pp. 18, 20, 22, 56).

[Hoo67] C. Hooley. *On Artin's conjecture*. In: *J. Reine Angew. Math.* 225 (1967), pp. 209–220 (cit. on pp. 113, 118).

[Hus04] D. Husemöller. *Elliptic curves*. Second edition. Vol. 111. Graduate Texts in Mathematics. Springer-Verlag, New York, 2004 (cit. on p. 94).

[Jon10] N. Jones. *Almost all elliptic curves are Serre curves*. In: *Trans. Amer. Math. Soc.* 362.3 (2010), pp. 1547–1570 (cit. on p. 83).

[JM20] N. Jones and K. McMurdy. *Elliptic curves with non-abelian entanglements*. arXiv: 2008.09087. 2020 (cit. on p. 83).

[Kuh78] N. C. Kuhman. *On the Conjecture of Birch and Swinnerton-Dyer for Elliptic Curves with Complex Multiplication.* PhD thesis. Stanford University, 1978 (cit. on p. 95).

[Küh12] L. Kühne. *An effective result of André-Oort type*. In: *Ann. of Math. (2)* 176.1 (2012), pp. 651–671 (cit. on p. 14).

[Küh13] L. Kühne. *An effective result of André-Oort type II*. In: *Acta Arith.* 161.1 (2013), pp. 1–19 (cit. on p. 14).

[Lan53] E. Landau. *Handbuch der Lehre von der Verteilung der Primzahlen. 2 Bände*. 2d ed, With an appendix by Paul T. Bateman. Chelsea Publishing Co., New York, 1953, xviii+pp. 1–564, ix+pp. 565–1001 (cit. on p. 23).

[Lan87] S. Lang. *Elliptic functions. Second edition.* Vol. 112. Springer, New York, NY, 1987 (cit. on pp. 10, 11, 59, 74, 75, 77, 94).

[Lan94] S. Lang. *Algebraic number theory*. Second. Vol. 110. Graduate Texts in Mathematics. Springer-Verlag, New York, 1994, pp. xiv+357 (cit. on p. 57).

[LV15] K. Lauter and B. Viray. *On singular moduli for arbitrary discriminants*. In: *Int. Math. Res. Not. IMRN* 19 (2015), pp. 9206–9250 (cit. on pp. 14, 17, 25–27, 29, 32, 33, 40, 41).

[LSM14] H. W. Lenstra Jr., P. Stevenhagen, and P. Moree. *Character sums for primitive root densities*. In: *Math. Proc. Cambridge Philos. Soc.* 157.3 (2014), pp. 489–511 (cit. on pp. 111, 113).

[Li21] Y. Li. *Singular units and isogenies between CM elliptic curves*. In: *Compos. Math.* 157.5 (2021), pp. 1022–1035 (cit. on p. 17).

[Lom17] D. Lombardo. *Galois representations attached to abelian varieties of CM type*. In: *Bulletin de la Société Mathématique de France* 145.3 (2017), pp. 469–501 (cit. on pp. xi, 63, 91).

[Loz16] Á. Lozano-Robledo. *Ramification in the division fields of elliptic curves with potential supersingular reduction*. In: *Research in Number Theory* 2.1 (2016), p. 8 (cit. on p. 90).

[Loz19] Á. Lozano-Robledo. *Galois representations attached to elliptic curves with complex multiplication*. arXiv:1809.02584. 2019 (cit. on pp. 59, 80).

[LD15] C. Lv and Y. Deng. *On orders in number fields: Picard groups, ring class fields and applications*. In: *Science China Mathematics* 58.8 (2015), pp. 1627–1638 (cit. on pp. 2, 71).

[Maz77] B. Mazur. *Rational points on modular curves*. In: *Modular functions of one variable, V (Proc. Second Internat. Conf., Univ. Bonn, Bonn, 1976)*. 1977, 107–148. Lecture Notes in Math., Vol. 601 (cit. on p. 82).

[Mic04] P. Michel. *The subconvexity problem for Rankin-Selberg L-functions and equidistribution of Heegner points*. In: *Ann. of Math. (2)* 160.1 (2004), pp. 185–236 (cit. on pp. 11, 12).

[Mil72] J. S. Milne. *On the arithmetic of abelian varieties*. In: *Inventiones mathematicae* 17.3 (1972), pp. 177–190 (cit. on p. 102).

[MV07] H. L. Montgomery and R. C. Vaughan. *Multiplicative number theory. I. Classical theory*. Vol. 97. Cambridge Studies in Advanced Mathematics. Cambridge University Press, Cambridge, 2007, pp. xviii+552 (cit. on p. 23).

[MK13] M. Mourtada and V. Kumar Murty. *Omega theorems for $\frac{L'}{L}(1,\chi_D)$*. In: *Int. J. Number Theory* 9.3 (2013), pp. 561–581 (cit. on p. 49).

[Mur83] M. R. Murty. *On Artin's conjecture*. In: *Journal of Number Theory* 16.2 (1983), pp. 147–168 (cit. on pp. 117, 118, 120).

[MM97] M. R. Murty and V. K. Murty. *Non-vanishing of L-functions and applications*. Modern Birkhäuser Classics. Birkhäuser/Springer Basel AG, Basel, 1997, pp. xii+196 (cit. on p. 118).

[NT91] Y. Nakkajima and Y. Taguchi. *A generalization of the Chowla-Selberg formula*. In: *J. Reine Angew. Math.* 419 (1991), pp. 119–124 (cit. on pp. 15, 42, 50).

[Neu99] J. Neukirch. *Algebraic Number Theory*. Vol. 322. Grundlehren der mathematischen Wissenschaften. Springer Berlin Heidelberg, 1999 (cit. on pp. 3, 55, 67, 70–72, 74).

[Pen20] R. Pengo. *Mahler's measure and elliptic curves with potential complex multiplication*. arXiv:2005.04159. 2020 (cit. on p. 102).

[Ram84] M. Ram Murty. *An analogue of Artin's conjecture for abelian extensions*. In: *J. Number Theory* 18.3 (1984), pp. 241–248 (cit. on p. 127).

[Rob83] G. Robert. *Sur le corps de définition de certaines courbes elliptiques à multiplications complexes*. In: *Séminaire de Théorie des Nombres de Bordeaux* (1983), pp. 1–18 (cit. on p. 96).

[Rud87] W. Rudin. *Real and complex analysis*. Third edition. McGraw-Hill Book Co., New York, 1987, pp. xiv+416 (cit. on p. 115).

[SAGE] The Sage Developers. *SageMath, the Sage Mathematics Software System (Version 9.0)*. 2020 (cit. on pp. 56, 124, 138).

[Sch10] R. Schertz. *Complex multiplication*. Vol. 15. New Mathematical Monographs. Cambridge University Press, Cambridge, 2010, pp. xiv+361 (cit. on p. 71).

[Sch] S. Schmid. *Integrality properties in the moduli space of elliptic curves: CM case*. In: *International Journal of Number Theory* (to appear) (cit. on p. 19).

[Sch62] W. Schwarz. *Über die Summe $\sum_{n\leq x}\varphi(f(n))$ und verwandte Probleme*. In: *Monatsh. Math.* 66 (1962), pp. 43–54 (cit. on p. 23).

[Ser71] J.-P. Serre. *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques*. In: *Inventiones mathematicæ* 15.4 (1971), pp. 259–331 (cit. on pp. 60, 61, 81).

[Ser79] J.-P. Serre. *Local fields*. Vol. 67. Graduate Texts in Mathematics. Translated from the French by Marvin Jay Greenberg. Springer-Verlag, New York-Berlin, 1979, pp. viii+241 (cit. on p. 118).

[Ser89] J.-P. Serre. *Abelian l-adic representations and elliptic curves*. Second. Advanced Book Classics. With the collaboration of Willem Kuyk and John Labute. Addison-Wesley Publishing Company, Advanced Book Program, Redwood City, CA, 1989, pp. xxiv+184 (cit. on pp. 10, 120, 121).

[ST68] J.-P. Serre and J. Tate. *Good reduction of abelian varieties*. In: *Ann. of Math. (2)* 88 (1968), pp. 492–517 (cit. on pp. 26, 32, 35, 40, 102).

[Ser78] J. Serre. *Résumé des cours de l'année scolaire 1977-1978*. In: *Ann. Coll. France* (1978), pp. 67–70 (cit. on p. 111).

[Shi71] G. Shimura. *On the Zeta-Function of an Abelian Variety with Complex Multiplication*. In: *Annals of Mathematics* 94.3 (1971), pp. 504–533 (cit. on p. 96).

[Shi94] G. Shimura. *Introduction to the arithmetic theory of automorphic functions*. Vol. 11. Publications of the Mathematical Society of Japan. Princeton University Press, Princeton, NJ, 1994 (cit. on pp. 59, 75, 94–96).

[Shi98] G. Shimura. *Abelian varieties with complex multiplication and modular functions*. Vol. 46. Princeton Mathematical Series. Princeton University Press, Princeton, NJ, 1998, pp. xvi+218 (cit. on pp. 34, 59, 61, 63).

[Sil94] J. H. Silverman. *Advanced topics in the arithmetic of elliptic curves*. Vol. 151. Graduate Texts in Mathematics. Springer-Verlag, New York, 1994, pp. xiv+525 (cit. on pp. 7, 9–11, 62, 68, 86, 94).

[Sil09] J. H. Silverman. *The arithmetic of elliptic curves*. Second. Vol. 106. Graduate Texts in Mathematics. Springer, Dordrecht, 2009, pp. xx+513 (cit. on pp. 8–11, 19, 33, 49, 83–88, 90, 92, 111, 143).

[Sil15] J. H. Silverman. *Errata and Corrections to The Arithmetic of Elliptic Curves, 2nd Edition*. 2015 (cit. on p. 84).

[Smi18] H. Smith. *Ramification in the Division Fields of Elliptic Curves and an Application to Sporadic Points on Modular Curves*. arXiv:1810.04809. 2018 (cit. on p. 90).

[Söh35] H. Söhngen. *Zur komplexen Multiplikation*. In: *Mathematische Annalen* 111.1 (1935), pp. 302–328 (cit. on pp. 59, 70, 71).

[Sta74] H. M. Stark. *Some effective cases of the Brauer-Siegel theorem*. In: *Invent. Math.* 23 (1974), pp. 135–152 (cit. on p. 127).

[Ste01] P. Stevenhagen. *Hilbert's 12th Problem, Complex Multiplication and Shimura Reciprocity*. In: *Class Field Theory – Its Centenary and Prospect*. Mathematical Society of Japan, 2001, pp. 161–176 (cit. on pp. 70, 71).

[Ste03] P. Stevenhagen. *The correction factor in Artin's primitive root conjecture*. In: vol. 15. 1. Les XXIIèmes Journées Arithmetiques (Lille, 2001). 2003, pp. 383–391 (cit. on p. 112).

[Str08] M. Streng. *Divisibility sequences for elliptic curves with complex multiplication.* In: *Algebra & Number Theory* 2.2 (2008), pp. 183–208 (cit. on pp. 85, 86).

[LMFDB] The LMFDB Collaboration. *The L-functions and Modular Forms Database* (cit. on p. 124).

[Ulm16] D. Ulmer. *Conductors of ℓ-adic representations*. In: *Proceedings of the American Mathematical Society* 144.6 (2016), pp. 2291–2299 (cit. on p. 103).

[Voi21] J. Voight. *Quaternion algebras*. First. Vol. 288. Graduate Texts in Mathematics. Springer International Publishing, 2021, pp. XXIII, 885 (cit. on pp. 5–7, 10, 34, 35).

[Was08] L. C. Washington. *Elliptic curves*. Second edition. Discrete Mathematics and its Applications (Boca Raton). Chapman & Hall/CRC, Boca Raton, FL, 2008 (cit. on p. 75).

[Web28] H. Weber. *Lehrbuch der algebra*. Vol. 3. Chelsea reprint, 1928 (cit. on pp. 13, 59).

[Win13] B. Winckler. *Théorème de Chebotarev effectif*. arXiv:1311.5715. 2013 (cit. on p. 127).

[YL18] H. Yi and C. Lv. *On Ring Class Fields of Number Rings*. arXiv:1810.04810. 2018 (cit. on pp. 71, 72).