Number fields of small degree generated by points on some modular curves

Trbović, Antonela

University of Zagreb

FACULTY OF SCIENCE

DEPARTMENT OF MATHEMATICS

Antonela Trbović

Number fields of small degree generated by points on some modular curves

DOCTORAL DISSERTATION

Zagreb, 2021.

University of Zagreb

FACULTY OF SCIENCE

DEPARTMENT OF MATHEMATICS

Antonela Trbović

Number fields of small degree generated by points on some modular curves

DOCTORAL DISSERTATION

Supervisor:

prof. dr. sc. Filip Najman

Zagreb, 2021.

Sveučilište u Zagrebu

PRIRODOSLOVNO–MATEMATIČKI FAKULTET

MATEMATIČKI ODSJEK

Antonela Trbović

Polja algebarskih brojeva malog stupnja generirana točkama na nekim modularnim krivuljama

DOKTORSKI RAD

Mentor:

prof. dr. sc. Filip Najman

Zagreb, 2021.

SUMMARY

In 1978, Mazur proved his famous theorem on possible torsion subgroups of elliptic curves defined over the field of rational numbers [32]. In the 1990s, a similar result was proved by Kamienny, Kenku and Momose [20, 26], which says what are the possible torsion subgroups of all elliptic curves over all quadratic fields. However, that result tells us little about possible torsion subgroups if we fix a quadratic field.

In Chapter 6, which is based on the author's paper [47], we describe methods that we can use to determine all possible groups that can appear as torsion subgroups of elliptic curves if we fix a quadratic field. Furthermore, we give the classification of torsion subgroups of elliptic curves over quadratic fields $\mathbb{Q}(\sqrt{d})$, where $0 < d < 100$ is squarefree. Those results can be found in Table 6.1. We obtained a complete classification for 49 out of 60 such fields. Over the remaining 11 quadratic fields, we could not rule out the possibility of the group $\mathbb{Z}/16\mathbb{Z}$ appearing as the torsion group of an elliptic curve.

Except for the question about determining possible torsion subgroups of elliptic curves over number fields of certain degree, in this thesis we will also be interested in the inverse question, i.e. if we have a given group T and a positive integer d, what are we able to say about number fields of degree d over which an elliptic curve with torsion T appears? We can ask even more, what if instead of a group T we are given an $n-$isogeny?

The results of the author's paper in collaboration with Filip Najman [39] give some answers when the torsion $T \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/14\mathbb{Z}$ is given and $d = 3$, and when $d = 2$ with a given $n-$isogeny, for $n \in \{22, 23, 26, 28, 29, 30, 31, 33, 35, 39, 40, 41, 46, 47, 48, 50, 59, 71\}$, which correspond to the modular curves $X_0(n)$ that are hyperelliptic, except for $n = 37$. Those results are presented in Chapter 7. Specifically, in Theorems 7.1.1 and 7.1.10 some splitting behaviour of small primes in quadratic extensions over which $X_0(n)$ has a non-cuspidal point was presented. Moreover, we were able to prove some results about the

splitting of primes in cubic fields generated by points on $X_1(2,14)$. It turns out that 2 always splits in such fields, and rational primes $p \equiv \pm 1 \pmod 7$ of multiplicative reduction split as well (see Proposition 7.2.7). Bruin and Najman [5] proved that elliptic curves with torsion $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/14\mathbb{Z}$ over cubic fields are actually a base change of elliptic curves over $\mathbb{Q}$. It is also true that those curves defined over $\mathbb{Q}$ have multiplicative reduction of type I_{14k} at 2 (see Proposition 7.2.3) and in Chapter 8, Proposition 8.1.2, it was proved that the reduction is always split multiplicative.

In the final chapter, Chapter 8, which will follow the author's paper [46], we study the Tamagawa numbers of elliptic curves with torsion $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/14\mathbb{Z}$ and of elliptic curves with an $n-$isogeny, for

$$n \in \{6, 8, 10, 12, 14, 16, 17, 18, 19, 37, 43, 67, 163\}.$$

It makes sense to study how the value of the Tamagawa number c_E of elliptic curve E depends on $E(K)_{tors}$, since $c_E/\#E(K)_{tors}$ appears as a factor in the leading term of the $L-$function of E/K in the conjecture of Birch and Swinnerton-Dyer (see, for example, [16, Conj. F.4.1.6]). Some results on Tamagawa numbers of elliptic curves with a specific torsion subgroup and on the quotient $c_E/\#E(K)_{tors}$ are given by Lorenzini in [30, Chapter 2] for elliptic curves over the rationals and over quadratic extensions. Krumm [27, Chapter 5] proved some further results on Tamagawa numbers of elliptic curves with prescribed torsion over number fields of degree up to 5. He also conjectured that $ord_{13}(c_E)$ is even for all elliptic curves defined over quadratic fields with a point of order 13 and the same conjecture was later proved by Najman in [37]. We found in Proposition 8.1.4 that Tamagawa numbers of elliptic curves with torsion $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/14\mathbb{Z}$ are always divisible by 14^2, with factors 14 coming from rational primes with split multiplicative reduction of type I_{14k}, one of which is always $p = 2$ (see Proposition 8.1.2). The only exception is the curve 1922c1, with $c_E = c_2 = 14$.

The question which naturally arises next is how does the Tamagawa number of an elliptic curve depend on the isogenies of that elliptic curve. In Section 8.2 we give a series of propositions which give us first results about Tamagawa numbers of elliptic curves with prescribed isogeny. Tamagawa numbers of elliptic curves with an $18-$isogeny must be divisible by 4 (Proposition 8.2.2), while elliptic curves with an $n-$isogeny for the remaining n from the mentioned set must have Tamagawa numbers divisible by 2 (see

Propositions 8.2.3, 8.2.4, 8.2.5 and 8.2.6), except for finite sets of specified curves.

In Chapters 1-4 we give a short introduction to elliptic curves and we set the stage for studying all of the mentioned properties of curves and number fields. We include chapters about modular curves, elliptic and hyperelliptic curves, as well as a chapter on elliptic curves over local fields.

The computations in this thesis were executed in the computer algebra system Magma [2]. The code can be found at `https://web.math.pmf.unizg.hr/~atrbovi/cv.html` next to the corresponding paper, or in Appendices A, B and C.

SAŽETAK

Mazur je 1978. godine dokazao svoj poznati teorem o mogućim torzijskim podgrupama eliptičkih krivulja definiranih nad poljem racionalnih brojeva [32]. U 1990-ima, Kamienny, Kenku i Momose [20, 26] su dokazali sličan rezultat koji govori koje su moguće torzijske podgrupe svih eliptičkih krivulja nad svim kvadratnim poljima. No, taj rezultat nam ne govori puno o tome što se događa ako uzmemo neko fiksno kvadratno polje.

U Poglavlju 6, koje prati autoričin članak [47], opisujemo metode koje se mogu iskoristiti da bismo odredili sve moguće torzijske grupe eliptičkih krivulja nad nekim fiksnim kvadratnim poljem. Nadalje, dajemo klasifikaciju torzijskih podgrupa eliptičkih krivulja nad kvadratnim poljima $\mathbb{Q}(\sqrt{d})$, gdje je $0 < d < 100$ kvadratno slobodan. Ti rezultati se mogu naći u Tablici 6.1. Uspjeli smo dobiti potpunu klasifikaciju nad 49 od 60 takvih polja. Nad ostalim poljima nismo mogli zaključiti je li moguća pojava grupe $\mathbb{Z}/16\mathbb{Z}$ kao torzijske grupe neke eliptičke krivulje.

Osim problema o mogućim torzijskim podgrupama eliptičkih krivulja nad poljima algebarskih brojeva određenog stupnja, u ovoj disertaciji će nas zanimati i obratno pitanje, tj. ako imamo zadanu grupu T i prirodni broj d, što možemo reći o poljima algebarskih brojeva stupnja d nad kojima postoji neka eliptička krivulja s torzijom T? Možemo se pitati i više od toga, što ako umjesto grupe T imamo zadanu $n-$izogeniju?

Rezultati autoričinog članka u suradnji s Filipom Najmanom [39] daju neke odgovore na ta pitanja kad imamo zadanu torziju $T \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/14\mathbb{Z}$ i $d = 3$ te kada imamo $d = 2$ i zadanu $n-$izogeniju, za

$$n \in \{22, 23, 26, 28, 29, 30, 31, 33, 35, 39, 40, 41, 46, 47, 48, 50, 59, 71\},$$

a u skupu se nalaze svi n osim $n = 37$ takvi da je pripadna modularna krivulja $X_0(n)$ hipereliptička. Ti rezultati su predstavljeni u Poglavlju 7. U Teoremima 7.1.1 i 7.1.10 možemo naći neke rezultate o cijepanju malih prostih brojeva u kvadratnim proširenjima

nad kojima $X_0(n)$ ima točku koja nije kusp. Nadalje, bili smo u mogućnosti dokazati i neke rezultate o cijepanju prostih brojeva u kubičnim proširenjima koja su generirana točkama na $X_1(2,14)$. Može se dokazati da se u takvim poljima 2 uvijek cijepa te da se racionalni prosti brojevi $p \equiv \pm 1 \pmod 7$ multiplikativne redukcije također cijepaju (više u Propoziciji 7.2.7). Bruin i Najman [5] su dokazali da su eliptičke krivulje s torzijom $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/14\mathbb{Z}$ nad kubičnim poljima zapravo definirane nad $\mathbb{Q}$. Vrijedi i činjenica da te eliptičke krivulje definirane nad $\mathbb{Q}$ imaju multiplikativnu redukciju tipa I_{14k} u 2 (više u Propoziciji 7.2.3), a u Poglavlju 8, Propozicija 8.1.2, dokazali smo da je ta redukcija uvijek rascjepiva multiplikativna.

U zadnjem poglavlju, Poglavlju 8, koje prati autoričin članak [46], proučavamo Tamagawine brojeve eliptičkih krivulja s torzijom $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/14\mathbb{Z}$ i eliptičkih krivulja s $n-$izogenijom, za $n \in \{6,8,10,12,14,16,17,18,19,37,43,67,163\}$.

Ima smisla proučavati kako vrijednost Tamagawinog broja c_E eliptičke krivulje E ovisi o $E(K)_{tors}$, budući da se $c_E/\#E(K)_{tors}$ pojavljuje kao faktor u vodećem koeficijentu $L-$funkcije od E/K u slutnji od Bircha i Swinnerton-Dyera (vidjeti npr. [16, Conj. F.4.1.6]). Neke rezultate o Tamagawinim brojevima s određenom torzijskom podgrupom i o kvocijentu $c_E/\#E(K)_{tors}$ je dao Lorenzini u svom članku [30, Chapter 2], za eliptičke krivulje definirane nad poljem racionalnih brojeva i nad kvadratnim proširenjima. Krumm je u svojoj doktorskoj disertaciji [27, Chapter 5] dokazao još neke rezultate o Tamagawinim brojevima eliptičkih krivulja s određenom torzijom nad poljima algebarskih brojeva stupnja do 5. On je također naslutio da je $ord_{13}(c_E)$ paran za sve eliptičke krivulje definirane nad kvadratnim poljima s točkom reda 13, a tu slutnju je kasnije dokazao Najman u [37]. U Propoziciji 8.1.4 smo dokazali da Tamagawin broj eliptičkih krivulja s torzijom $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/14\mathbb{Z}$ mora uvijek biti djeljiv s 14^2, gdje svaki faktor 14 dolazi od racionalnog prostog broja s multiplikativnom redukcijom tipa I_{14k}, a jedan od tih prostih brojeva je uvijek $p = 2$ (vidjeti Propoziciju 8.1.2). Jedina iznimka je krivulja 1922c1, za koju je $c_E = c_2 = 14$.

Pitanje koje se sljedeće prirodno postavlja je kako Tamagawin broj eliptičke krivulje ovisi o izogenijama koje ima ta eliptička krivulja. U Poglavlju 8.2 dajemo niz propozicija koje nam daju prve rezultate o Tamagawinim brojevima eliptičkih krivulja s određenom izogenijom. Tamagawini brojevi eliptičkih krivulja s 18-izogenijom moraju biti djeljivi s

4 (Propozicija 8.2.2), dok eliptičke krivulje s $n-$izogenijom za preostale n iz spomenutog skupa imaju Tamagawine brojeve djeljive s 2, osim za konačno mnogo poznatih krivulja. Ti rezultati se nalaze u Propozicijama 8.2.3, 8.2.4, 8.2.5 i 8.2.6.

U poglavljima 1-4 dajemo kratak uvod u eliptičke krivulje i osnovne rezultate koje koristimo za proučavanje eliptičkih krivulja i polja algebarskih brojeva. Uključujemo poglavlja o modularnim krivuljama, eliptičkim i hipereliptičkim krivuljama i također o eliptičkim krivuljama nad lokalnim poljima.

Izračuni u ovoj disertaciji izvršeni su u računalnom sustavu Magma [2]. Svi kodovi se nalaze na `https://web.math.pmf.unizg.hr/~atrbovi/cv.html` kraj odgovarajućih članaka ili u Dodacima A, B i C.

CONTENTS

1. INTRODUCTION

The study of Diophantine equations, i.e. polynomial equations and their solutions over $\mathbb{Z}$ or $\mathbb{Q}$ exists since as early as ancient Greece. The most famous such problem is Fermat's last theorem, which says that the equation

$$a^n + b^n = c^n$$

has no solutions $(a,b,c) \in \mathbb{Z}^3$ such that $abc \neq 0$ and $n \geq 3$. The theorem was proved in 1994 by Andrew Wiles, for which he received the Abel prize in 2016.

For simple forms of Diophantine equations in two variables, which determine a curve of genus 0, the problem of finding solutions is solved. It can be shown that the set of solutions is either empty or infinite, in which case it is isomorphic to $\mathbb{P}^1(\mathbb{Q})$. On the other hand, if we study a more complicated case of cubic Diophantine equations in two variables, they determine a curve of genus 1, which is actually our motivation for the study of elliptic curves.

Definition 1.0.1. Let K be a number field. An elliptic curve E defined over K is a smooth projective curve of genus 1 with a distinguished K-rational point $\mathcal{O}$, which we call the point at infinity.

Furthermore, if we look at the curves of genus 2 and Diophantine equations associated to them, Faltings' theorem tells us about the number of solutions.

Theorem 1.0.2 (Faltings)**.** Let C be a smooth, irreducible, projective curve of genus $g \geq 2$ defined over a number field K. Then the set $C(K)$ of all $K-$rational points on C is finite.

In the case of curves C of genus 0, a simple argument can be used to show that $C(K)$ is either empty or infinite and that the curve C is isomorphic to $\mathbb{P}^1$. Furthermore, the

previous theorem states that if C has genus 2 or larger, then $C(K)$ is a finite set. As we can see, the curves of genus 1 are the most interesting ones, in terms of the number of solutions, and we will focus on those in this thesis. In the remainder of this chapter we will give some basic properties of such curves and set the field for studying the number of solutions and points on those curves.

Every elliptic curve defined over a field K has an equation of the form

$$Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3,$$

where $\mathscr{O} = [0,1,0]$ is the point at infinity and $a_1, a_2, a_3, a_4, a_6 \in K$. However, we will mostly be using the affine coordinates $x = X/Z, y = Y/Z$ and remembering we have one extra point at infinity. We now have the following equation for E

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

which we call the long Weierstrass model for E. If $char(K) \neq 2,3$ we can get the equation to be of the form

$$y^2 = x^3 + ax + b,$$

where $a, b \in K$, and this model is said to be the short Weierstrass model.

Even though we will mostly be encountering elliptic curves over fields of characteristic not equal to 2 or 3, in Chapter 8 those characteristics will be of great importance, so it is essential to include the following definition in full generality.

Definition 1.0.3. Let E be an elliptic curve defined over K, given in its long Weierstrass form $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$. We define

$$\begin{aligned} b_2 &= a_1^2 + 4a_2, \\ b_4 &= 2a_4 + a_1a_3, \\ b_6 &= a_3^2 + 4a_6, \\ b_8 &= a_1^2a_6 + 4a_2a_6 - a_1a_3a_4, + a_2a_3^2 - a_4^2. \end{aligned}$$

Now we can define the discriminant of E as

$$\Delta = -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6.$$

Furthermore, we have

$$c_4 = b_2^2 - 24b_4,$$
$$c_6 = -b_2^3 + 36b_2b_4 - 216b_6.$$

When the elliptic curve is given by the short Weierstrass equation $y^2 = x^3 + ax + b$, then

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

We also define the $j-$invariant of E as

$$j(E) = \frac{c_4^3}{\Delta}.$$

The quantities from the previous definition will be used extensively in Chapters 7 and 8, where we will be examining them in order to conclude something about the reduction type and Tamagawa numbers.

Theorem 1.0.4. ([43, Proposition III.1.4.(b)]). Let E and E' be elliptic curves defined over a field K. Then E and E' are isomorphic over $\overline{K}$ if and only if $j(E) = j(E')$.

The previous theorem confirms that the $j-$invariant just defined in Definition 1.0.3 really is an invariant. It is an invariant of the isomorphism class of the curve and it does not depend on the chosen Weierstrass equation.

It turns out that the Weierstrass equation for an elliptic curve is not unique. It can be shown that the only change of variables fixing the point at infinity and preserving the Weierstrass form is

$$x = u^2x' + r,$$
$$y = u^3y' + u^2sx' + t,$$

where $u, r, s, t \in \overline{K}$ and $u \neq 0$. It will be of importance to us to know the coefficients a_i' of the new Weierstrass equation that is obtained after the change of variables and how the already defined quantities change under that substitution. Those are given in Table 1.1 [43, Table 3.1]. We will be changing variables a lot in Chapter 8 to obtain a suitable model for which we can deduce some important properties of the curve.

Addition on points of $E(K)$ can be defined roughly in the following manner. If P and Q are points on E, let L be the line through P and Q (if $P = Q$, let L be the tangent line

ua_1'	$= a_1 + 2s$
u^2a_2'	$= a_2 - sa_1 + 3r - s^2$
u^3a_3'	$= a_3 + ra_1 + 2t$
u^4a_4'	$= a_4 - sa_3 + 2ra_2 - (t+rs)a_1 + 3r^2 - 2st$
u^6a_6'	$= a_6 + ra_4 + r^2a_2 + r^3 - ta_3 - t^2 - 2st$
u^2b_2'	$= b_2 + 12r$
u^4b_4'	$= b_4 + rb_2 + 6r^2$
u^6b_6'	$= b_6 + 2rb_4 + r^2b_2 + 4r^3$
u^8b_8'	$= b_8 + 3rb_6 + 3r^2b_4 + r^3b_2 + 3r^4$
u^4c_4'	$= c_4$
u^6c_6'	$= c_6$
$u^{12}\Delta'$	$= \Delta$
j'	$= j$

Table 1.1: Change-of-variable formulas for Weierstrass equations

to E at P), and let R be the third point of intersection of L with E. We know that the third point of intersection exists, according to Bézout's theorem [10, Theorem 10, p.10]. Let L' be the line through R and $\mathcal{O}$. Then L' intersects E at R, $\mathcal{O}$, and a third point. We denote that third point by $P+Q$. Explicit formulas for addition of points $P=(x_P,y_P)$ and $Q=(x_Q,y_Q)$ can be found in [43, Group Law Algorithm 2.3]. From those it can be easily seen that if P and Q are defined over a field K, then $P+Q$ is also defined over the same field K. This addition gives us an abelian group structure on $E(K)$.

Theorem 1.0.5 (Mordell-Weil)**.** Let K be a number field and let E be an elliptic curve defined over K. Then the group $E(K)$ is finitely generated abelian group.

As we can see, the theorem tell us that the group $E(K)$ is finitely generated, which together with the structure theorem for finitely generated abelian groups gives that

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

where $r \geq 0$ is an integer which we call the rank of E over K and $E(K)_{tors}$ is the torsion subgroup, the group of elements of finite order.

In Chapter 6 of this thesis we will focus on the torsion subgroup, specifically on the torsion subgroup of elliptic curves defined over a quadratic field K. We mention some famous results on torsion of elliptic curves.

Theorem 1.0.6 (Mazur [32])**.** Let E be an elliptic curve defined over $\mathbb{Q}$. Then $E(\mathbb{Q})$ is one of the following 15 groups

- $\mathbb{Z}/n\mathbb{Z},\ n = 1,...,10,12,$
- $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z},\ n = 1,2,3,4.$

Theorem 1.0.7 (Kamienny, Kenku, Momose [20,26])**.** Let E be an elliptic curve defined over a quadratic field K. Then $E(K)$ is one of the following 26 groups

- $\mathbb{Z}/n\mathbb{Z},\ n = 1,...,16,18,$
- $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z},\ n = 1,...,6,$
- $\mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3n\mathbb{Z},\ n = 1,2,$
- $\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}.$

The previous theorem tells us what are the possible torsion subgroups of all elliptic curves over all quadratic fields, but tells us little about what will happen if we fix a certain quadratic field. We will try to give an answer to that question in Chapter 6.

Now we introduce the definition of an isogeny of an elliptic curve, as this will be the center of our study in Chapter 7.

Definition 1.0.8. Let E_1 and E_2 be elliptic curves. An isogeny from E_1 to E_2 is a non-constant morphism $\phi : E_1 \to E_2$ satisfying $\phi(\mathcal{O}_{E_1}) = \mathcal{O}_{E_2}$. If there exists an isogeny $\phi : E_1 \to E_2$, then we say that elliptic curves E_1 and E_2 are isogenous.

Example 1.0.1. Let E be an elliptic curve defined over a number field K and let n be an integer. The morphism

$$[n] : E \to E$$

$$[n](P) = \begin{cases} \underbrace{P+P+\ldots+P}_{n\text{-times}}, \text{ if } n > 0 \\ [-n](-P), \text{ if } n < 0 \\ \mathcal{O}, \text{ if } n = 0 \end{cases}$$

is clearly an isogeny, as the addition formulas are given as $K-$rational functions.

It turns out that every isogeny is automatically a homomorphism, which is stated in the following theorem.

Theorem 1.0.9. ([43, Theorem III.4.8]). Let $\phi : E_1 \to E_2$ be an isogeny. Then

$$\phi(P+Q) = \phi(P) + \phi(Q),$$

for all $P, Q \in E_1$.

Corollary 1.0.10. ([43, Corollary III.4.9]). Let $\phi : E_1 \to E_2$ be an isogeny. Then

$$Ker\phi = \phi^{-1}(\mathscr{O})$$

is a finite group.

If we have an isogeny $\phi : E_1 \to E_2$ such that $Ker\phi = \phi^{-1}(\mathscr{O})$ is a cyclic group of order n, we say that ϕ is an $n-$isogeny. The following proposition introduces another kind of relationship between isogenies and finite subgroups of E.

Proposition 1.0.11. ([43, Proposition III.4.12]). Let E be an elliptic curve and let Φ be a finite subgroup of E. There are a unique elliptic curve E' and a separable isogeny $\phi : E \to E'$ satisfying $Ker\phi = \Phi$.

For the end of this chapter, we give the following theorem that tells us which are the possible values of n for elliptic curves defined over the field of rational numbers.

Theorem 1.0.12 (Kenku, Mazur [22–25, 33])**.** Let E be an elliptic curve defined over $\mathbb{Q}$ with a rational $n-$isogeny. Then

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

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

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

and only finitely many for other values of n.

2. QUADRATIC TWISTS OF ELLIPTIC CURVES

In this chapter we give the definition of a quadratic twist of an elliptic curve and we prove some important properties of twists that will be of importance to us in the subsequent chapters.

Definition 2.0.1. Let E be an elliptic curve defined over a number field K. A twist of E over K is a smooth curve that is isomorphic to E over $\overline{K}$.

Example 2.0.1. Let E be an elliptic curve given by a Weierstrass equation

$$E:\ y^2 = f(x)$$

and let $K(\sqrt{d})$ be a quadratic extension of K, where d is squarefree. The curve

$$E^d:\ dy^2 = f(x)$$

is a twist of E over K and the isomorphism $\phi : E^d \to E$ is given by $\phi(x,y) = (x, y\sqrt{d})$. We will refer to the twists described in this example as quadratic twists.

Proposition 2.0.2. ([43, Exercise 10.16]). Let K be an algebraic number field and $L = K(\sqrt{d})$ its quadratic extension. Let E be an elliptic curve defined over K. Then we have

$$r(E(L)) = r(E(K)) + r(E^d(K)).$$

Proof. Let E be an elliptic curve with its short Weierstrass equation

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

and let E^d be its quadratic twist given by

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

where $a, b \in K$. Let σ be the generator of $\mathrm{Gal}(L/K)$. Note that the points $(x,y) \in E^d(K)$ correspond to the points $(x, y\sqrt{d}) \in E(L)$, where $x, y \in K$. We will first prove the inequality

$$r(E(L)) \geq r(E(K)) + r(E^d(K)).$$

If $r(E(k)) = 0$ or $r(E^d(k)) = 0$, the claim trivially holds. If E and E^d have positive ranks, then we need to prove that any two points of infinite order coming from $E(K)$ and $E^d(K)$ are necessarily independent. Let $P_1 \in E(K)$ and $P_2 \in E^d(K)$ be two such points. If they were not independent, we would have $\alpha, \beta \in \mathbb{Z}$, $\alpha, \beta \neq 0$, such that

$$\alpha P_1 + \beta P_2 = \mathscr{O}.$$

Acting with σ to this equation we get

$$\alpha P_1 - \beta P_2 = \mathscr{O},$$

because $\sigma(P_2) = -P_2$. Now we easily get $\alpha = \beta = 0$, which is a contradiction.

Now we want to prove

$$r(E(L)) \leq r(E(K)) + r(E^d(K)).$$

Let us denote $r_1 = r(E(K))$, $r_2 = r(E^d(K))$, $r = r(E(L))$, which means that we can write

$$E(K)/E(K)_{tors} = \langle P_1, ..., P_{r_1} \rangle,$$

$$E^d(K)/E^d(K)_{tors} = \langle P_{r_1+1}, ..., P_{r_1+r_2} \rangle,$$

$$E(L)/E(L)_{tors} = \langle T_1, ..., T_r \rangle.$$

Suppose that $P = (x_1 + x_2\sqrt{d}, y_1 + y_2\sqrt{d}) \in E(L)$ is a point of infinite order. Direct calculation gives

$$P + \sigma(P) \in E(K), \ P - \sigma(P) \in E^d(K),$$

so we have

$$2P \in E(K) + E^d(K).$$

It follows that

$$2\langle T_1,...,T_r\rangle/E(L)_{tors}$$

is a subgroup of

$$\langle P_1,...,P_{r_1+r_2}\rangle/E(L)_{tors}.$$

Therefore, $\langle P_1,...,P_{r_1+r_2}\rangle$ has finite index in $E(L)/E(L)_{tors}$, and $r(E(L)) \leq r(E(K)) + r(E^d(K))$. ■

Proposition 2.0.3. Let E be an elliptic curve defined over K and let $L = K(\sqrt{d})$ be a quadratic extension of K. Then

$$E(L)_{(2')} = E(K)_{(2')} \oplus E^d(K)_{(2')},$$

where E^d is a quadratic twist of E over K and $E(K)_{(2')}$ is the subgroup of $E(K)$ of points of odd order.

The proof of this proposition is very similar to the proof of Proposition 2.0.2, if we exchange the points of infinite order with points of odd order.

Proposition 2.0.4. Let E be an elliptic curve defined over K and let $d \in K$ be squarefree. Then

$$E(K)[2] = E^d(K)[2].$$

Proof. Let

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

and

$$E^d:\ y^2 = x^3 + ad^2x + bd^3.$$

Recall that $P \in E(K)$ is a point of order 2 if and only if $y(P) = 0$, i.e. $P = (t,0)$, where $t \in K$ is a root of $x^3 + ax + b$. Furthermore, t is a root of $x^3 + ax + b$ if and only if td is a root of $x^3 + ad^2x + bd^3$. Hence, the number of roots of $x^3 + ax + b$ and $x^3 + ad^2x + bd^3$ is the same, so we have $E(K)[2] = E^d(K)[2]$. ■

In Chapter 6 we will use Propositions 2.0.2, 2.0.3 and 2.0.4 in order to obtain the rank and torsion of an elliptic curve over a quadratic field and the rank and torsion of the Jacobian variety of an elliptic curve, for which the claims are also true. The Jacobians will be defined later, in Section 5, Theorem 5.0.4.

3. MODULAR CURVES

The goal of this chapter is to define modular curves which will be moduli spaces of isomorphism classes of elliptic curves with a certain (torsion) structure. We will be using them throughout, as examining the points on those curves over an algebraic number field K can give us all elliptic curves over K with some specific property.

Definition 3.0.1. We define the modular group $SL_2(\mathbb{Z})$ as

$$SL_2(\mathbb{Z}) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} : a,b,c,d \in \mathbb{Z},\ ad-bc=1 \right\}.$$

We also define some subgroups of the just defined modular group.

Definition 3.0.2. Let $n \in \mathbb{N}$. The principal congruence subgroup of level n is

$$\Gamma(n) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in SL_2(\mathbb{Z}) : \begin{bmatrix} a & b \\ c & d \end{bmatrix} \equiv \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \pmod{n} \right\}.$$

A subgroup Γ of $SL_2(\mathbb{Z})$ is said to be a congruence subgroup if $\Gamma(n) \leq \Gamma$, for some $n \in \mathbb{N}$. If n is the smallest such number, we say that Γ is a congruence subgroup of level n.

We now give two very important definitions. The first one is of two congruence subgroups that we will use in the second definition, the definition of modular curves associated to those subgroups.

Definition 3.0.3.

$$\Gamma_0(n) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in SL_2(\mathbb{Z}) : \begin{bmatrix} a & b \\ c & d \end{bmatrix} \equiv \begin{bmatrix} * & * \\ 0 & * \end{bmatrix} \pmod{n} \right\},$$

$$\Gamma_1(n) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in SL_2(\mathbb{Z}) : \begin{bmatrix} a & b \\ c & d \end{bmatrix} \equiv \begin{bmatrix} 1 & * \\ 0 & 1 \end{bmatrix} \pmod{n} \right\}.$$

Note that we have

$$\Gamma(n) \leq \Gamma_1(n) \leq \Gamma_0(n) \leq SL_2(\mathbb{Z}).$$

Before proceeding with the definition of a modular curve, we have to define the action of the modular group $SL_2(\mathbb{Z})$ on the upper half plane $\mathscr{H}$. Let τ be an element of $\mathscr{H}$ and $\gamma = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ be an element of $SL_2(\mathbb{Z})$. We define the action as

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

The formula

$$\mathrm{Im}(\gamma(\tau)) = \frac{\mathrm{Im}(\tau)}{|c\tau + d|^2},$$

which can be found in [12, Exercise 1.1.2(a)], confirms that this truly is an action.

Definition 3.0.4. For a congruence subgroup $\Gamma \leq SL_2(\mathbb{Z})$ we define the modular curve $Y(\Gamma)$ as the quotient

$$Y(\Gamma) = \Gamma \backslash \mathscr{H} = \{\Gamma\tau : \tau \in \mathscr{H}\},$$

where $\mathscr{H} = \{\tau \in \mathbb{C} : Im(\tau) > 0\}$ is the upper half plane. Therefore, for the already mentioned congruence subgroups $\Gamma_0(n), \Gamma_1(n)$ and $\Gamma(n)$ we can define the following modular curves

$$Y_0(n) = \Gamma_0(n) \backslash \mathscr{H},$$

$$Y_1(n) = \Gamma_1(n) \backslash \mathscr{H},$$

$$Y(n) = \Gamma(n) \backslash \mathscr{H}.$$

Furthermore, we will define sets of isomorphism classes of elliptic curves with certain torsion structures and then see a relationship between those and modular curves defined in Definition 3.0.4.

Definition 3.0.5. Let $n \in \mathbb{N}$.

- Let (E, C) be an ordered pair, where E is a complex elliptic curve and C is a cyclic subgroup of E of order n. We say that two such pairs (E, C) and (E', C') are equivalent and we write $(E, C) \sim (E', C')$ if there exists an isomorphism from E to E' which maps C to C'. We denote by $S_0(n)$ the set of all equivalence classes with respect to $\sim$.

- Let (E,Q) be an ordered pair, where E is a complex elliptic curve and Q is a point on E of order n. We say that two such pairs (E,Q) and (E',Q') are equivalent and we write $(E,Q)\sim(E',Q')$ if there exists an isomorphism from E to E' which maps Q to Q'. We denote by $S_1(n)$ the set of all equivalence classes with respect to $\sim$.

- Let $(E,(P,Q))$ be an ordered pair, where E is a complex elliptic curve and (P,Q) is a pair of points on E which generate the $n-$torsion subgroup of E with Weil pairing $e_n(P,Q)=e^{\frac{2\pi i}{n}}$. We say that two such pairs $(E,(P,Q))$ and $(E',(P',Q'))$ are equivalent and we write $(E,(P,Q))\sim(E',(P',Q'))$ if there exists an isomorphism from E to E' which maps P to P' and Q to Q'. We denote by $S(n)$ the set of all equivalence classes with respect to $\sim$.

Theorem 3.0.6. There exist bijections

$$\phi_0 : S_0(n)\to Y_0(n),$$

$$\phi_1 : S_1(n)\to Y_1(n),$$

$$\phi : S(n)\to Y(n).$$

For in detail description of the bijections and the sketch of the proof one can look at [12, Theorem 1.5.1], but the detailed proof can be found in [45, Teorem 3.2.2]. We will not be including those here, since a lot of additional information, which is not the main focus in this thesis, would be necessary.

To compactify the modular curve $Y(\Gamma)=\Gamma\backslash\mathscr{H}$, we define $\mathscr{H}^*=\mathscr{H}\cup\mathbb{Q}\cup\{\infty\}$ and we take the quotient $X(\Gamma)=\Gamma\backslash\mathscr{H}^*=Y(\Gamma)\cup\Gamma\backslash(\mathbb{Q}\cup\{\infty\})$.

The compactified modular curves $X_0(n)=\Gamma_0(n)\backslash\mathscr{H}^*, X_1(n)=\Gamma_1(n)\backslash\mathscr{H}^*$ and $X(n)=\Gamma(n)\backslash\mathscr{H}^*$ turn out to be algebraic curves. Modular curves are in fact compact Riemann surfaces, so such polynomials with complex coefficients exist by a general theorem of Riemann surface theory, but $X_0(n)$ and $X_1(n)$ are in fact curves over the rational numbers, meaning the polynomials can be taken to have rational coefficients.

The points of the set $X(\Gamma)\backslash Y(\Gamma)$ are said to be cusps. It can be shown that the set of cusps is finite, and for the modular curves in this thesis, the exact elements of those sets are known.

Theorem 3.0.6 tells us that over the field K (which will in this thesis always be an algebraic number field), each point on $X_1(n)(K)$ is either a cusp or it parameterizes an elliptic curve with torsion $\mathbb{Z}/n\mathbb{Z}$ over K; and for the points on $X_0(n)(K)$, those are either cusps or they parameterize an elliptic curve over K with an $n-$isogeny. Now it is clear that studying elliptic curves with certain torsion subgroup or isogeny comes down to examining the points on modular curves $X_0(n)$ and $X_1(n)$.

In the subsequent chapters, these curves will be of great importance, since torsion subgroups and isogenies of elliptic curves will be the center of our study.

4. ELLIPTIC CURVES OVER LOCAL FIELDS

In this chapter we will describe some properties of rational points on elliptic curves defined over a field that is complete with respect to a descrete valuation. We will use the mentioned results throughout the thesis, as we will almost always, without explicitly mentioning it, be working with base changes to $\mathbb{Q}_p$ of elliptic curves defined over $\mathbb{Q}$. This chapter will mainly follow some sections of [43, Chapter VII], although the notation will mostly be different.

Let E be an elliptic curve over a number field K and denote by Σ the set of all finite primes of K. For each $p \in \Sigma$, K_p will denote the completion of K at p and $k_p = \mathcal{O}_{K_p}/(\pi)$ the residue field of p, where $\mathcal{O}_{K_p}$ is the ring of integers of K_p and π is a uniformizer of $\mathcal{O}_{K_p}$. The discrete valuation in respect to which K_p is complete, we will denote by v_p or just v if it is clear which p we are referring to. Let the equation for E over K be

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

With the substitution $x \mapsto u^{-2}x, y \mapsto u^{-3}y$, choosing the suitable value of u, we can make all the coefficients a_i to be elements of $\mathcal{O}_{K_p}$. Now for the discriminant Δ of E we have $v(\Delta) > 0$. The model for E with the minimal value of $v(\Delta)$ will be called the minimal model. In Chapter 8 we will often be searching for minimal models of elliptic curves for some primes p, since it will allow us to deduce some properties of reduction of E at p.

In essence, if $a_i \in \mathcal{O}_{K_p}$ and $v_p(\Delta) < 12$, for $p \neq 2, 3$, then the equation for E is minimal at p. For $char(k_p) = 2$ or 3 (and for arbitrary K), Tate's algorithm [44] can be used to

determine whether the equation is minimal.

4.1. Reduction modulo π

In this section we will be looking at the reduction modulo the uniformizer π. There is a natural reduction map

$$\mathcal{O}_{K_p} \to k_p = \mathcal{O}_{K_p}/(\pi)$$

$$t \mapsto \bar{t},$$

which we can apply to the coefficients of the minimal model of the equation for E. In other words, if we start with a minimal model

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

reducing its coefficients $a_i \in R$ modulo π, we obtain the equation

$$\overline{E}: \ y^2 + \overline{a_1}xy + \overline{a_3}y = x^3 + \overline{a_2}x^2 + \overline{a_4}x + \overline{a_6},$$

for the curve $\overline{E}$ defined over k_p that is possibly singular. This defines a reduction map

$$E(K_p) \to \overline{E}(k_p)$$

$$P \mapsto \overline{P}.$$

As mentioned, the curve $\overline{E}/k_p$ can be singular, but the set of all nonsingular points $\overline{E}_{ns}(k_p)$ forms a group [43, III.2.5.]. Now we can define the following subsets of $E(K)$.

Definition 4.1.1. Let E be an elliptic curve defined over K_p. We define the set of points of nonsingular reduction as

$$E_0(K_p) = \left\{P \in E(K_p) : \overline{P} \in \overline{E}_{ns}(k_p)\right\},$$

and the kernel of reduction as

$$E_1(K_p) = \left\{P \in E(K_p) : \overline{P} = \overline{\mathcal{O}}\right\}.$$

Note that the definition does not depend on the initial choice of a minimal Weierstrass equation [43, Proposition VII.1.3.b)].

4.1.1. Good and bad reduction

Definition 4.1.2. Let E be an elliptic curve defined over K_p and let $\overline{E}$ be the reduction modulo (π) of a minimal Weierstrass equation for E. We say that

(a) E has good reduction if $\overline{E}$ is nonsingular,

(b) E has multiplicative reduction if $\overline{E}$ has a node,

(c) E has additive reduction if $\overline{E}$ has a cusp.

In the last two cases we say that E has bad reduction. If E has multiplicative reduction, then the reduction is said to be split if the slopes of the tangent lines at the node are in k_p, and otherwise it is said to be nonsplit.

We will be needing a practical way to determine the reduction type, which is given with the following proposition.

Proposition 4.1.3. ([43, Proposition VII.5.1]). Let E be an elliptic curve defined over K_p with minimal Weierstrass equation

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

Let Δ be the discriminant and let c_4 be the usual expression involving $a_1, ..., a_6$ defined in Definition 1.0.3.

(a) E has good reduction if and only if $v(\Delta) = 0$.

(b) E has multiplicative reduction if and only if $v(\Delta) > 0$ and $v(c_4) = 0$.

(c) E has additive reduction if and only if $v(\Delta) > 0$ and $v(c_4) > 0$.

4.2. TAMAGAWA NUMBERS

In this section we will focus on the quotient $E(K_p)/E_0(K_p)$, where $E_0(K_p)$ is the set of all points on $E(K_p)$ that do not reduce to a singular point in $\overline{E}(k_p)$. We already defined this set in Definition 4.1.1. The most important (and nontrivial) property of this quotiont is that it is finite. The proof of this fact can be found in [42, Chapter IV].

Theorem 4.2.1 (Kodaira, Néron)**.** Let E be an elliptic curve defined over K_p. If E has split multiplicative reduction over K_p, then $E(K_p)/E_0(K_p)$ is a cyclic group of order $v(\Delta) = -v(j)$. In all other cases the group $E(K_p)/E_0(K_p)$ is finite and has order at most 4.

Corollary 4.2.2. The subgroup $E_0(K_p)$ has finite index in $E(K_p)$.

Using the finiteness of the mentioned index, we can now define the Tamagawa number of elliptic curves (at a specified prime).

Definition 4.2.3. The Tamagawa number of E at a prime p is the index

$$c_p = [E(K_p) : E_0(K_p)].$$

We define the Tamagawa number of E over K to be the product

$$c_{E/K} = \prod_{p \in \Sigma} c_p.$$

Note that the Tamagawa number of an elliptic curve depends on the field over which it is defined. However, we will write c_E instead of $c_{E/K}$ wherever it does not cause confusion.

The entire Chapter 8 will be devoted to Tamagawa numbers of elliptic curves with some torsion subgroup or isogeny, so more interesting properties of Tamagawa numbers will be mentioned there.

5. HYPERELLIPTIC CURVES AND THEIR JACOBIANS

In this section we will define hyperelliptic curves and the Jacobian variety of a curve C defined over a perfect field K. We will mention the importance of Jacobians of hyperelliptic curves in general, as well as in Chapter 6 and give some well-known results that we will be using throughout. In the end, we will introduce Mumford representation of divisors on a curve, i.e. of points on the Jacobian. This is the representation in which Magma [2] stores and works with the points on the Jacobian, which will be of use to us in Chapter 6 when computing the Jacobians over $\mathbb{Q}$ of hyperelliptic modular curves $X_1(n)$, for $n = 13, 16, 18$.

Definition 5.0.1. A hyperelliptic curve over a field K such that $char(K) \neq 2$ is an algebraic curve given by the equation

$$y^2 = f(x),$$

where $f \in K[x]$ is a polynomial of degree $n > 4$ with n distinct roots.

Remark 5.0.2. A more general definition would be the one where we define a genus g hyperelliptic curve over K (of any characteristic) with the equation $y^2 + h(x)y = f(x)$, where $h, f \in K[x], deg(f) \leq 2g+2, deg(h) \leq g+1$. In the case of characteristic different from 2 we can always find a model of the form $y^2 = f(x)$ for the curve, so in this thesis we will always assume that $h = 0$.

The degree of the polynomial f determines the genus of the curve; polynomials of degree $2g+1$ and $2g+2$ give a curve of genus g. All curves of genus 2 are hyperelliptic.

Let K be a perfect field and C a curve defined over K. We define a group $Div(C)$ as the free Abelian group generated by points in $C(\overline{K})$, the set of points on the curve C defined

over the algebraic closure $\overline{K}$ of K. The elements of that group are called divisors. In other words, a divisor D is a $\mathbb{Z}-$linear combination of points on C, i.e.,

$$D = \sum_{P \in C} n_P P,$$

where $n_P \in \mathbb{Z}$ and $n_p = 0$ for all but finitely many P. The absolute Galois group $\mathrm{Gal}(\overline{K}/K)$ acts on the group $Div(C)$ in the usual manner,

$$D^\sigma = \sum_{P \in C} n_P P^\sigma,$$

for $\sigma \in \mathrm{Gal}(\overline{K}/K)$. The divisors that are invariant under the action of $\mathrm{Gal}(\overline{K}/K)$ are said to be $K-$rational divisors. The set of all $K-$rational divisors will be denoted by $Div_K(C)$.

Example 5.0.1. Let C be a hyperelliptic curve defined over K given by $y^2 = f(x)$. Fix $x_0 \in K$ and let y_0 be an element of $\overline{K}$ such that $y_0^2 = f(x_0)$. Then the divisor

$$D = (x_0, y_0) + (x_0, -y_0)$$

is a $K-$rational divisor on C, i.e. $D \in Div_K(C)$.

The degree of the divisor $D = \sum_{P \in C} n_P P$ is defined as the sum of its coefficients,

$$deg(D) = \sum_{P \in C} n_P \in \mathbb{Z}.$$

This gives us a homomorphism $deg : Div(C) \to \mathbb{Z}$. Its kernel, $Div^0(C)$, is the subgroup of divisors of $Div(C)$ of degree 0.

Now assume that the curve C is smooth and let f be a rational function in $\overline{K}(C)^*$. We can associate to it a divisor

$$div(f) = \sum_{P \in C} ord_P(f) P,$$

where $ord_P(f)$ is the order of f in the point P. This is distinct from zero only in the cases when P is a pole or a root of f. It is now clear that $deg(div(f)) = 0$ [43, Proposition II.3.1], since any function $f \in \overline{K}(C)^*$, for a smooth curve C, has the same number of poles and roots, counting multiplicities. This gives a homomorphism $div : \overline{K}(C)^* \to Div(C)$. We denote the image of this map by $Princ(C)$. We define the Picard group as the quotient $Pic(C) = Div(C)/Princ(C)$. We note that we can also write the mentioned homomorphism as $div : \overline{K}(C)^* \to Div^0(C)$ and we can define the quotient $Pic^0(C) = Div^0(C)/Princ(C)$.

Definition 5.0.3. We say that the divisors D and D' are linearly equivalent, and we write $D \sim D'$, if D and D' have the same image in the Picard group $Pic(C)$. We denote that image with $[D]$.

Theorem 5.0.4. Let C be a curve over K of genus g. Then there exists an abelian variety J over K of genus g such that there exists an isomorphism $Pic^0(C) \to J$.

The abelian variety from the theorem is called the Jacobian (variety) of the curve C. It is clear that we also have an isomorphism $Pic^0_K(C) \to J(K)$, from the $K-$rational divisors in the Picard group to the Jacobian of the curve C defined over K.

Proposition 5.0.5. Let C be a curve over K of genus $g \geq 1$ and with Jacobian J. Let $[D_0]$ be a class of $K-$rational divisor D_0 of degree 1. Then the map

$$i_{[D_0]} : C \to J,\ P \mapsto [P - D_0]$$

is injective.

The idea now is to get some information about $C(K)$ using the mentioned injection to $J(K)$ and some results about the group structure of $J(K)$. We know that J is an abelian variety, which means that $J(K)$ is an abelian group. The following result tells us more about the group structure.

Theorem 5.0.6 (Mordell-Weil)**.** Let J be the Jacobian of some curve C defined over K. The group $J(K)$ is finitely generated.

Using this theorem and the structure theorem for finitely generated abelian groups, we know that

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

If we specify the field K to be the field of rational numbers $\mathbb{Q}$, we can say even more about the torsion subgroup $J(\mathbb{Q})_{tors}$. Let p be a prime such that the curve E has good reduction in p so that we have the mapping

$$C(\mathbb{Q}) \to C(\mathbb{F}_p),\ P \mapsto \overline{P}.$$

Proposition 5.0.7. Let p be a prime of good reduction for C. Then J also has good reduction at p and the reduction map $J(\mathbb{Q}) \mapsto \overline{J}(\mathbb{F}_p)$ is a group homomorphism. If $p \geq$

3, then the restriction of the reduction map to $J(\mathbb{Q})_{tors}$ is injective. Furthermore, the following diagram commutes.

$$\begin{array}{ccc} C(\mathbb{Q}) & \xrightarrow{i_{[D_0]}} & J(\mathbb{Q}) \\ \downarrow & & \downarrow \\ \overline{C}(\mathbb{F}_p) & \xrightarrow{i_{[\overline{D_0}]}} & \overline{J}(\mathbb{F}_p) \end{array}$$

Proposition 5.0.7 is a very useful result since it gives an upper bound for $|J(\mathbb{Q})_{tors}|$ using the fact that $|J(\mathbb{Q})_{tors}|$ divides $|\overline{J}(\mathbb{F}_p)|$ for all p of good reduction.

5.1. MUMFORD REPRESENTATION

As mentioned, in this subsection we will explain the Mumford representation of the divisors on a curve, the representation in which the computer algebra system Magma stores them and works with them. We will be interested only in divisors of hyperelliptic curves in this thesis, hence we first have to learn how to differentiate between different kinds of hyperelliptic curves, since the way in which we obtain divisors on the curve from divisors in Mumford representation will be slightly different for each of the types.

If a hyperelliptic curve C has a unique point at infinity ∞, we say that C is an imaginary hyperelliptic curve. This happens when the defining polynomial f is of odd degree. If f has even degree, then C has two points at infinity, which we denote by ∞_- and ∞_+ and we say that C is a real hyperelliptic curve.

Definition 5.1.1. We say that a divisor D of C is reduced if it has the form

$$D = \sum_{i=1}^{k} P_i,$$

with $k \leq g$, where g is genus of C and $P_i \neq \overline{P_j}$, where $\overline{P} = \overline{(a,b)} = (a,-b)$. If C is an imaginary hyperelliptic curve, then we require $P_i \neq \infty$, and if C is a real hyperelliptic curve, then P_i can be one of the points at infinity.

If the curve C is a real hyperelliptic curve, it has 2 points at infinity, ∞_- and ∞_+. If the curve C has a $K-$rational point we can always move it to the line at infinity so that the

points at infinity of the curve are $K-$rational. Now we see that when we allowed some P_i in Definition 5.1.1 to be a point at infinity in the case of a real hyperelliptic curve, it will not affect the $K-$rationality of the divisor.

Definition 5.1.2. If C is an imaginary hyperelliptic curve, we define $D_\infty = g\infty$, where g is genus of C. If C is a real hyperelliptic curve, then $D_\infty = \frac{g}{2}(\infty_- + \infty_+)$.

Note that we will only be working with the case $g = 2$, as only the curves $X_0(n)$, for $n = 13, 16, 18$ will be of interest in this thesis.

For each divisor $D \in Div^0(C)$ it can be shown that it is equivalent, in the sense of Definition 5.0.3, to a unique divisor $D_0 - D_\infty$, where D_0 is reduced. Therefore, every class in the quotient group J is represented by exactly one such divisor, see [34, Theorem 47] for imaginary hyperelliptic curves or [14, Proposition 1] for real hyperelliptic curves.

There is a convenient representation of such divisors, which is called the Mumford representation. A divisor in Mumford representation is an ordered triple $(a(x), b(x), d)$ of polynomials $a, b \in K[x]$ such that:

- $a(x)$ is monic of degree at most g;
- $b(x)$ has degree at most $g+1$ and $a(x)$ divides $b(x)^2 - f(x)$, where $f(x)$ is the defining polynomial of C;
- d is a positive integer with $deg(a(x)) \leq d \leq g+1$, such that the degree of $b(x)^2 - f(x)$ is less than or equal to $2g+2-d+deg(a(x))$.

The conditions above ensure that we can get a unique divisor on J from a divisor in Mumford representation, see [7, Theorem 4.143 (iii)] for imaginary hyperelliptic curves or [14] for real hyperelliptic curves.

We will now describe a method, obtained from [2], on how to retrieve the point on the Jacobian from its Mumford representation.

For a triple $(a(x), b(x), d)$ in Mumford representation we define $A(x,z)$ as the homogenisation of the polynomial $a(x)$ of degree d and $B(x,z)$ as the homogenisation of the polynomial $b(x)$ of degree $g+1$, where g is a genus of C, in our case $g = 2$.

Now, by solving the equations

$$A(x,z) = 0,\ y = B(x,z),$$

we get the points $P_i = [x_i, y_i, 1]$, $i = 1, ..., d$, in projective coordinates. Note that the number of points is exactly d, as the polynomial $A(x,z)$ is of degree d (which will be even in our case).

The point on the Jacobian represented by $(a(x), b(x), d)$ is then the divisor class

$$[P_1 + ... + P_d - d\infty],$$

if there is a single point ∞ at infinity, or

$$\left[P_1 + ... + P_d - \frac{d}{2}(\infty_+ + \infty_-)\right],$$

if there are two points ∞_+ and ∞_- at infinity. We will use this method in Chapter 6, precisely, in Proposition 6.2.9 and Proposition 6.2.10.

6. TORSION GROUPS OF ELLIPTIC CURVES OVER QUADRATIC FIELDS $\mathbb{Q}(\sqrt{d}), 0 < d < 100$

The idea of this chapter is to examine the methods that can be used to determine all possible torsion subgroups over an arbitrary, but fixed, quadratic field. We will mostly follow the chapters in the author's paper [47]. In this chapter we will use the same notation as in previous chapters; for an elliptic curve E defined over a number field K, we will denote by $E(K)$ the set of all $K-$rational points on E, and by $E(K)_{tors}$ the torsion subgroup of E.

We already mentioned the famous result by Kamienny, Kenku and Momose [20, 26] concerning possible torsion subgroups of elliptic curves defined over any quadratic field, which are the following 26 groups:

$$\mathbb{Z}/n\mathbb{Z}, \ \ n = 1, ..., 16, 18,$$

$$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z}, \ \ n = 1, ..., 6,$$

$$\mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3n\mathbb{Z}, \ \ n = 1, 2,$$

$$\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}.$$

While this theorem settles the question on what are the possibilities for the torsion subgroup over all quadratic fields, we are interested in what happens when we fix a certain quadratic field. In order to see what happens over a fixed field, one would have to go through each of the 26 groups mentioned above and check whether that is a possible torsion subgroup or not.

First we are going to see why every group mentioned in Mazur's theorem has to appear as a possible torsion subgroup over all quadratic fields, and what happens with the groups

$\mathbb{Z}/3\mathbb{Z}\oplus\mathbb{Z}/3n\mathbb{Z}$, $n=1,2$, and $\mathbb{Z}/4\mathbb{Z}\oplus\mathbb{Z}/4\mathbb{Z}$. For the rest of the groups we will follow the methods described in [19].

From now on, let K be a fixed quadratic field. Let $Y_1(m,n)$ be the affine modular curve whose every $K-$rational point corresponds to an isomorphism class of an elliptic curve together with an $m-$torsion point $P_m \in E(K)$ and an $n-$torsion point $P_n \in E(K)$ such that P_m and P_n generate a subgroup isomorphic to $\mathbb{Z}/m\mathbb{Z}\oplus\mathbb{Z}/n\mathbb{Z}$. Let $X_1(m,n)$ be its compactification (the same curve with adjoined cusps). We denote $X_1(1,n)$ by $X_1(n)$. The mentioned modular curves were defined in Chapter 3.

More precisely, what we need to do in order to determine whether an elliptic curve with torsion $\mathbb{Z}/n\mathbb{Z}\oplus\mathbb{Z}/m\mathbb{Z}$ over K exists, for the remaining 26 groups, is to determine whether there are $K-$rational points on $X_1(m,n)$ that are not cusps. These modular curves are either elliptic or hyperelliptic.

If the modular curve $X_1(m,n)$ is elliptic, we compute its rank. If the rank is positive, there are infinitely many elliptic curves over K with the given torsion subgroup, as the number of cusps is finite. If the rank is 0, we have to compute the torsion subgroup and check whether any torsion point corresponds to a $K-$rational point on the modular curve that is not a cusp.

If the modular curve $X_1(m,n)$ is hyperelliptic, we compute the rank of the Jacobian of the curve. If the rank is 0, we also have to check whether any torsion point arises from a $K-$rational point on the modular curve that is not a cusp. If the rank is positive, the problem becomes more difficult. More about this can be found in [19].

One could also take a look at [18] for examples of quadratic fields where some of the groups, namely $\mathbb{Z}/2\mathbb{Z}\oplus\mathbb{Z}/10\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z}\oplus\mathbb{Z}/12\mathbb{Z}$, $\mathbb{Z}/15\mathbb{Z}$, $\mathbb{Z}/11\mathbb{Z}$ and $\mathbb{Z}/14\mathbb{Z}$, appear as torsion subgroups.

6.1. Groups from Mazur's theorem and $\mathbb{Z}/3\mathbb{Z}\oplus\mathbb{Z}/3n\mathbb{Z}$, $n=1,2$, $\mathbb{Z}/4\mathbb{Z}\oplus\mathbb{Z}/4\mathbb{Z}$

In this section, we are going to show that every group mentioned in Mazur's theorem has to appear as a possible torsion group over any quadratic field K and we are going to see

under which conditions the groups $\mathbb{Z}/3\mathbb{Z}\oplus\mathbb{Z}/3n\mathbb{Z}$, $n=1,2$, and $\mathbb{Z}/4\mathbb{Z}\oplus\mathbb{Z}/4\mathbb{Z}$ appear as a torsion of an elliptic curve over some quadratic field.

Let E be an elliptic curve and denote by $\rho_{E,n}:\mathrm{Gal}(K/\mathbb{Q})\to \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$ the *mod n* Galois representation attached to E.

If P,P' is a basis for $E[n]$, the subgroup of E of points of order n, and if P is a point of order n in $E(\mathbb{Q})$, then $\rho_{E,n}(\sigma)=\begin{bmatrix}1 & b\\ 0 & d\end{bmatrix}$, $b\in\mathbb{Z}/n\mathbb{Z}, d\in(\mathbb{Z}/n\mathbb{Z})^\times$ for every $\sigma\in\mathrm{Gal}(K/\mathbb{Q})$, with respect to the basis $\{P,P'\}$.

We define a subgroup of $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$,

$$\Gamma_1(n)=\left\{\begin{bmatrix}1 & b\\ 0 & d\end{bmatrix} : b\in\mathbb{Z}/n\mathbb{Z}, d\in(\mathbb{Z}/n\mathbb{Z})^\times\right\},$$

which corresponds to $X_1(n)$, i.e. the *mod n* representations of elliptic curves parameterized by the points on $X_1(n)$ are elements in $\Gamma_1(n)$, with an appropriate choice of basis. Similarly, we define a subgroup

$$\Gamma_1(2,2n)=\left\{\begin{bmatrix}1 & b\\ 0 & d\end{bmatrix} : b\in 2\mathbb{Z}/2n\mathbb{Z}, d\in(\mathbb{Z}/2n\mathbb{Z})^\times\right\},$$

which corresponds to $X_1(2,2n)$, in the sense described above.

For any of the groups $\mathbb{Z}/n\mathbb{Z}$ or $\mathbb{Z}/2\mathbb{Z}\oplus\mathbb{Z}/2n\mathbb{Z}$ appearing in Mazur's theorem, we have that the corresponding modular curve $X_1(n)$ or $X_1(2,2n)$, respectively, is of genus 0. Now, with $X_G=X_1(n)$ or $X_G=X_1(2,2n)$ in [48, Lemma 3.5], using the same arguments as in the proof of the lemma, but taking the base field to be a quadratic field K instead of $\mathbb{Q}$, we have that there are infinitely many elliptic curves E over K such that $\rho_{E,n}(\mathrm{Gal}(K/\mathbb{Q}))$ is conjugate (not just contained) in $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$ to $\Gamma_1(n)$ or $\Gamma_1(2,2n)$, respectively, proving our claim.

Now, we will focus on the groups

$$\mathbb{Z}/3\mathbb{Z}\oplus\mathbb{Z}/3n\mathbb{Z},\ n=1,2,$$

$$\mathbb{Z}/4\mathbb{Z}\oplus\mathbb{Z}/4\mathbb{Z}.$$

From the properties of the Weil pairing, we know that $\mathbb{Z}/n\mathbb{Z}\times\mathbb{Z}/n\mathbb{Z}\subset E(K)$ only if $\mathbb{Q}(\zeta_n)\subset K$.

Hence, $\mathbb{Z}/3\mathbb{Z}\times\mathbb{Z}/3n\mathbb{Z}\subset E(K)$, $n=1,2$, only when $K\supset\mathbb{Q}(\zeta_3)=\mathbb{Q}(\sqrt{-3})$ and $\mathbb{Z}/4\mathbb{Z}\times\mathbb{Z}/4\mathbb{Z}\subset E(K)$ only if $K\supset\mathbb{Q}(i)$. Moreover, the mentioned groups are the only groups, except the ones from Mazur's theorem, that appear over $\mathbb{Q}(\sqrt{-3})$ and $\mathbb{Q}(i)$, respectively [36, 38].

6.2. TORSION OVER $\mathbb{Q}(\sqrt{17})$

We will now demonstrate how to carry out the methods mentioned at the beginning of this chapter over the quadratic field $\mathbb{Q}(\sqrt{17})$. We chose $\mathbb{Q}(\sqrt{17})$ because $17 \equiv 1 \pmod 8$, and the significance of this relation will be clear later on.

As stated above, all groups from Mazur's theorem are possible torsion subgroups over $\mathbb{Q}(\sqrt{17})$, while the groups $\mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3n\mathbb{Z}$, $n = 1,2$, $\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$ are not.

For the rest of the groups we will follow the methods from [19] described above.

The equations for $X_1(m,n)$ can be found in [1,41].

All computations in the following propositions will be done in Magma [2]. Computations for this Chapter can be found at `http://web.math.pmf.unizg.hr/~atrbovi/magma.txt` or in Appendix A.

Proposition 6.2.1. There are infinitely many elliptic curves with torsion $\mathbb{Z}/11\mathbb{Z}$ over $\mathbb{Q}(\sqrt{17})$.

Proof. To show this, we have to prove that the modular curve $X_1(11)$ defined over $\mathbb{Q}(\sqrt{17})$ has infinitely many points. It will suffice to see that the rank is positive, since the number of cusps on $X_1(11)$ is finite. For the modular curve

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

we compute

$$rank(X_1(11)(\mathbb{Q}(\sqrt{17}))) = 1$$

in Magma. Now we can conclude that there are infinitely many elliptic curves with torsion $\mathbb{Z}/11\mathbb{Z}$ over $\mathbb{Q}(\sqrt{17})$.

We can also compute a generator of the group $X_1(11)(\mathbb{Q}(\sqrt{17}))$ (modulo the torsion subgroup), which is

$$\left(\frac{1}{8}(-\sqrt{17}+1), \frac{1}{16}(\sqrt{17}+7)\right).$$

■

Proposition 6.2.2. There are infinitely many elliptic curves with torsion $\mathbb{Z}/14\mathbb{Z}$ over $\mathbb{Q}(\sqrt{17})$.

Proof. For the modular curve

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

we compute

$$rank(X_1(14)(\mathbb{Q}(\sqrt{17})))=1.$$

Using similar reasoning to the one in Proposition 6.2.1 we conclude that there are infinitely many elliptic curves with torsion $\mathbb{Z}/14\mathbb{Z}$ over $\mathbb{Q}(\sqrt{17})$.

We can also compute a generator of the group $X_1(14)(\mathbb{Q}(\sqrt{17}))$ (modulo the torsion subgroup), which is

$$\left(\frac{1}{2}(\sqrt{17}+3),-\sqrt{17}-5\right).$$

■

Proposition 6.2.3. The group $\mathbb{Z}/15\mathbb{Z}$ cannot be a torsion group of an elliptic curve over $\mathbb{Q}(\sqrt{17})$.

Proof. For the modular curve

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

we compute

$$rank(X_1(15)(\mathbb{Q}(\sqrt{17})))=0.$$

Hence, we only have to show that

$$Y_1(15)(\mathbb{Q}(\sqrt{17}))=\emptyset,$$

i.e. that there are only cusps in $X_1(15)(\mathbb{Q}(\sqrt{17}))$.

The $x-$coordinates of the cusps on $X_1(15)$ satisfy the equation

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

So, the set of all $\mathbb{Q}(\sqrt{17})-$rational cusps is

$$X_1(15)(\mathbb{Q}(\sqrt{17}))\backslash Y_1(15)(\mathbb{Q}(\sqrt{17}))=\{O,(0,0),(0,-1),(-1,0)\}.$$

We compute

$$X_1(15)(\mathbb{Q}(\sqrt{17}))\cong\mathbb{Z}/4\mathbb{Z},$$

so now it is obvious that all points on the modular curve $X_1(15)$ defined over $\mathbb{Q}(\sqrt{17})$ are cusps. Therefore, $Y_1(15)(\mathbb{Q}(\sqrt{17})) = \emptyset$, so there are no elliptic curves with torsion $\mathbb{Z}/15\mathbb{Z}$ over $\mathbb{Q}(\sqrt{17})$. ■

Proposition 6.2.4. There are infinitely many elliptic curves with torsion $\mathbb{Z}/2\mathbb{Z}\oplus\mathbb{Z}/10\mathbb{Z}$ over $\mathbb{Q}(\sqrt{17})$.

Proof. For the modular curve

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

we compute

$$rank(X_1(2,10)(\mathbb{Q}(\sqrt{17}))) = 1.$$

We can also compute a generator of the group $X_1(2,10)(\mathbb{Q}(\sqrt{17}))$ (modulo the torsion subgroup), which is

$$\left(\sqrt{17}+4, 3\sqrt{17}+12\right).$$

■

Proposition 6.2.5. There are infinitely many elliptic curves with torsion $\mathbb{Z}/2\mathbb{Z}\oplus\mathbb{Z}/12\mathbb{Z}$ over $\mathbb{Q}(\sqrt{17})$.

Proof. For the modular curve

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

we compute

$$rank(X_1(2,12)(\mathbb{Q}(\sqrt{17}))) = 1.$$

We can also compute a generator of the group $X_1(2,12)(\mathbb{Q}(\sqrt{17}))$ (modulo the torsion subgroup), which is

$$\left(\frac{1}{2}(-\sqrt{17}+9), \frac{1}{2}(-3\sqrt{17}+19)\right).$$

■

Now we have determined whether $\mathbb{Z}/n\mathbb{Z}\oplus\mathbb{Z}/n\mathbb{Z}$ is a possible torsion of an elliptic curve over $\mathbb{Q}(\sqrt{17})$, for all modular curves $X_1(m,n)$ that are elliptic curves. To determine

if $\mathbb{Z}/n\mathbb{Z},\ n = 13, 16, 18$, are possible torsion groups is somewhat more difficult, since the corresponding modular curves are hyperelliptic curves.

The groups $\mathbb{Z}/n\mathbb{Z},\ n = 13, 18$, are generally easier to deal with over quadratic fields, since we have the two following results that can be found in [3, 27].

Theorem 6.2.6 (Bosman, Bruin, Dujella, Najman; Krumm)**.** If $X_1(13)$ has a point defined over $\mathbb{Q}(\sqrt{d})$, then:

1. $d > 0$,
2. $d \equiv 1 \pmod 8$.

Theorem 6.2.7 (Bosman, Bruin, Dujella, Najman; Krumm)**.** If $X_1(18)$ has a point defined over $\mathbb{Q}(\sqrt{d})$, $d \neq -3$, then:

1. $d > 0$,
2. $d \equiv 1 \pmod 8$,
3. $d \not\equiv 2 \pmod 3$.

Now it becomes clear why we chose the field $\mathbb{Q}(\sqrt{17})$, as we did not want to rule out the existence of the groups $\mathbb{Z}/n\mathbb{Z},\ n = 13, 18$, as possible torsion subgroups.

Proposition 6.2.8. The group $\mathbb{Z}/13\mathbb{Z}$ is a possible torsion over $\mathbb{Q}(\sqrt{17})$.

Proof. Let $J_1(13)$ be the Jacobian of the hyperelliptic curve

$$X_1(13):\ y^2 = x^6 - 2x^5 + x^4 - 2x^3 + 6x^2 - 4x + 1$$

and let $J_1^{17}(13)$ be its quadratic twist by 17, which becomes isomorphic to $J_1(13)$ over $\mathbb{Q}(\sqrt{17})$. We compute

$$rank(J_1(13)(\mathbb{Q})) = 0,$$

$$rank(J_1^{17}(13)(\mathbb{Q})) = 2.$$

Now, we have

$$rank(J_1(13)(\mathbb{Q}(\sqrt{17}))) = rank(J_1(13)(\mathbb{Q})) + rank(J_1^{17}(13)(\mathbb{Q})) = 2.$$

By searching for points on $X_1(13)(\mathbb{Q}(\sqrt{17}))$ in Magma, we find a point $\left(\frac{1}{2},\frac{1}{8}\sqrt{17}\right)$ on the curve.

Since the $x-$coordinates of the cusps on $X_1(13)$ are the solutions of the equation

$$x(x-1)(x^3-4x^2+x+1)=0,$$

the $\mathbb{Q}(\sqrt{17})-$rational cusps are

$$X_1(13)(\mathbb{Q}(\sqrt{17}))\backslash Y_1(13)(\mathbb{Q}(\sqrt{17}))=\{\infty_+,\infty_-,(0,\pm 1),(1,\pm 1)\}.$$

We conclude that the point $\left(\frac{1}{2},\frac{1}{8}\sqrt{17}\right)$ mentioned above is not a cusp and so the elliptic curve over $\mathbb{Q}(\sqrt{17})$ with a torsion subgroup $\mathbb{Z}/13\mathbb{Z}$ exists. ■

Unlike in the previous propositions, we do not have infinitely many elliptic curves with torsion $\mathbb{Z}/13\mathbb{Z}$, since by Falting's theorem (Theorem 1.0.2) the modular curve $X_1(13)$ can only have finitely many points over a number field.

Proposition 6.2.9. The group $\mathbb{Z}/16\mathbb{Z}$ cannot be a torsion group of an elliptic curve over $\mathbb{Q}(\sqrt{17})$.

Proof. Let $J_1(16)$ be the Jacobian of the hyperelliptic curve

$$X_1(16):\ y^2=x(x^2+1)(x^2+2x-1)$$

and let $J_1^{17}(16)$ be its quadratic twist.

We compute

$$rank(J_1(16)(\mathbb{Q}(\sqrt{17})))=rank(J_1(16)(\mathbb{Q}))+rank(J_1^{17}(16)(\mathbb{Q}))=0.$$

Since the rank is zero, we need to find the cusps in $X_1(16)(\mathbb{Q}(\sqrt{17}))$ and the torsion subgroup of $J_1(16)(\mathbb{Q}(\sqrt{17}))$ in order to determine if there exists a point on the Jacobian that arises from a point on the modular curve that is not a cusp.

As the $x-$coordinates of the cusps satisfy

$$x(x-1)(x+1)(x^2-2x-1)(x^2+2x-1)=0,$$

the cusps on $X_1(16)(\mathbb{Q}(\sqrt{17}))$ are

$$X_1(16)(\mathbb{Q}(\sqrt{17}))\backslash Y_1(16)(\mathbb{Q}(\sqrt{17}))=\{\infty,(0,0),(1,\pm 2),(-1,\pm 2)\}.$$

We also compute

$$J_1(16)(\mathbb{Q})_{tors} \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/10\mathbb{Z},$$

$$J_1^{17}(16)(\mathbb{Q})_{tors} \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}.$$

The set of points of odd order on the Jacobian $J_1(16)$ defined over $\mathbb{Q}(\sqrt{17})$ is

$$J_1(16)(\mathbb{Q}(\sqrt{17}))_{(2')} \cong J_1(16)(\mathbb{Q})_{(2')} \oplus J_1^{17}(16)(\mathbb{Q})_{(2')} \cong \mathbb{Z}/5\mathbb{Z},$$

and the $2-$torsion subgroup is

$$J_1(16)(\mathbb{Q}(\sqrt{17}))_{tors} \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}.$$

Thus, $J_1(16)(\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/10\mathbb{Z}$ and $J_1(16)(\mathbb{Q}) \cong J_1(16)(\mathbb{Q})_{tors}$.
In Magma, we find 20 divisor classes in Mumford representation [7],

$$(1,0,0),\ (x^2+2x+1,2x,2),\ (x^2+2x+1,-2x,2),\ (x^2-2x+1,4x-2,2),$$

$$(x^2-2x+1,-4x+2,2),\ (x+1,2,1),\ (x+1,-2,1),\ (x,0,1),$$

$$(x-1,2,1),\ (x-1,-2,1),\ (x^2+2x-1,0,2),\ (x^2+x,2x,2),\ (x^2+x,-2x,2),$$

$$(x^2-1,2x,2),\ (x^2-1,-2x,2),\ (x^2-1,2,2),\ (x^2-1,-2,2),$$

$$(x^2+1,0,2),\ (x^2-x,2x,2),\ (x^2-x,-2x,2).$$

The first divisor class represents the point at infinity, and for the rest of the divisor classes in Mumford representation, we follow the methods described in [2] in order to retrieve the point on the Jacobian from its Mumford representation. We presented the mentioned method in detail in Section 5.1.

For example, for the point $(x^2+2x+1,2x,2)$ on $J_1(16)(\mathbb{Q}(\sqrt{17}))$ in Mumford representation we have

$$A(x,z) = x^2+2xz+z^2,$$

$$B(x,z) = 2xz^2,$$

and $P_1 = P_2 = (-1:-2:1)$, so we conclude that the point $(x^2+2x+1,2x,2)$ represents the divisor class $[2(-1:-2:1)-2\infty]$ on the Jacobian $J_1(16)(\mathbb{Q}(\sqrt{17}))$.

By doing so for every divisor class in Mumford representation, one can check that all divisor points correspond to the cusps in $X_1(16)(\mathbb{Q}(\sqrt{17}))$, so we conclude that $\mathbb{Z}/16\mathbb{Z}$ cannot be a torsion group of an elliptic curve over $\mathbb{Q}(\sqrt{17})$. ■

Proposition 6.2.10. $\mathbb{Z}/18\mathbb{Z}$ cannot be a torsion group of an elliptic curve over $\mathbb{Q}(\sqrt{17})$.

Proof. Let $J_1(18)$ be the Jacobian of the hyperelliptic curve

$$X_1(18): \ y^2 = x^6 + 2x^5 + 5x^4 + 10x^3 + 10x^2 + 4x + 1$$

and let $J_1^{17}(18)$ be its quadratic twist. We compute

$$rank(J_1(18)(\mathbb{Q}(\sqrt{17}))) = rank(J_1(18)(\mathbb{Q})) + rank(J_1^{17}(18)(\mathbb{Q})) = 0.$$

The $x-$coordinates of the cusps in $X_1(18)$ satisfy the equation

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

so the cusps are

$$X_1(18)(\mathbb{Q}(\sqrt{17}))\backslash Y_1(18)(\mathbb{Q}(\sqrt{17})) = \{\infty_+, \infty_-, (0,\pm 1), (-1,\pm 1)\}.$$

On the other hand, we compute

$$J_1(18)(\mathbb{Q})_{tors} \cong \mathbb{Z}/21\mathbb{Z},$$

$$J_1^{17}(18)(\mathbb{Q})_{tors} \cong \{O\}.$$

The set of points of odd order is

$$J_1(18)(\mathbb{Q}(\sqrt{17}))_{(2')} \cong J_1(18)(\mathbb{Q})_{(2')} \oplus J_1^{17}(18)(\mathbb{Q})_{(2')} \cong \mathbb{Z}/21\mathbb{Z}.$$

As the polynomial

$$f(x) = x^6 + 2x^5 + 5x^4 + 10x^3 + 10x^2 + 4x + 1$$

has no zeros defined over $\mathbb{Q}(\sqrt{17})$, we conclude that $J_1(18)(\mathbb{Q}(\sqrt{17}))$ has no points of order 2, and

$$J_1(18)(\mathbb{Q}(\sqrt{17}))_{tors} \cong \mathbb{Z}/21\mathbb{Z}.$$

The elements of $J_1(18)(\mathbb{Q}(\sqrt{17}))_{tors}$ in Mumford representation are

$$(1,0,0),\ (1,x^3+x^2,2),\ (1,-x^3-x^2,2),\ (x^2+2x+1,x,2),\ (x^2+2x+1,-x,2),$$

$$(x^2,2x+1,2),\ (x^2,-2x-1,2),\ (x+1,x^3,2),\ (x+1,-x^3,2),$$

$$(x+1,x^3+2,2),\ (x+1,-x^3-2,2),\ (x,x^3-1,2),\ (x,-x^3+1,2),\ (x,x^3+1,2),$$

$$(x,-x^3-1,2),\ (x^2+x,2x+1,2),\ (x^2+x,-2x-1,2)),\ (x^2+x,1,2),$$

$$(x^2+x,-1,2),\ (x^2+x+1,x-1,2),\ (x^2+x+1,-x+1,2),$$

and one can easily conclude that all of the points correspond to the cusps, so we obtain our result. ■

We proved the following theorem:

Theorem 6.2.11. The possible torsion subgroups of elliptic curves defined over $\mathbb{Q}(\sqrt{17})$ are the following:

$$\mathbb{Z}/n\mathbb{Z},\ n=1,...,14,$$

$$\mathbb{Z}/2\mathbb{Z}\oplus\mathbb{Z}/2n\mathbb{Z},\ n=1,...,6.$$

Remark 6.2.1. In [27, Theorem 2.7.7, 2.7.8] Krumm found a list of possible quadratic fields $\mathbb{Q}(\sqrt{d})$ over which torsion subgroups $\mathbb{Z}/13\mathbb{Z}$ and $\mathbb{Z}/18\mathbb{Z}$ may appear, for $0<d<1000$.

In our case, for $0<d<100$, there are only two such fields, $\mathbb{Q}(\sqrt{17})$, over which $\mathbb{Z}/13\mathbb{Z}$ appears, and $\mathbb{Q}(\sqrt{33})$, over which $\mathbb{Z}/18\mathbb{Z}$ appears. We were able to eliminate the rest of the fields for $0<d<100$ using only conditions from Theorem 6.2.6 and Theorem 6.2.7 and methods described in Proposition 6.2.8 and Proposition 6.2.10.

6.3. TORSION OVER $\mathbb{Q}(\sqrt{d})$, $0 < d < 100$

For every quadratic field $\mathbb{Q}(\sqrt{d})$, where d is a non-negative squarefree integer $d \neq 1$, $0 < d < 100$, we found the torsion subgroups appearing over it by using methods similar to the ones described in Theorem 6.2.11, and those results are presented in Table 6.1. We have chosen to consider only real quadratic fields, because we expect the same problems to happen in the range $-100 < d < 0$, except with the groups $\mathbb{Z}/13\mathbb{Z}$ and $\mathbb{Z}/18\mathbb{Z}$, for which we already stated in Theorem 6.2.6 and Theorem 6.2.7 that they cannot appear as torsion subgroups over $\mathbb{Q}(\sqrt{d})$, for $d < 0$.

Since we know that the groups from Mazur's theorem appear as torsion subgroups, and the groups $\mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3n\mathbb{Z}$, $n = 1, 2$, $\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$ do not appear as torsion subgroups of elliptic curves over $\mathbb{Q}(\sqrt{d})$, for $0 < d < 100$, in Table 6.1 we give the list of possible torsion subgroups within the groups

$$\mathbb{Z}/n\mathbb{Z},\ n = 11, 13, 14, 15, 16, 18,$$

$$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z},\ n = 5, 6,$$

i.e. the rest of the possible 26 torsion subgroups over quadratic fields.

Note that the groups mentioned above appear as a torsion subgroup 37, 1, 38, 37, 6-17, 1, 35, 36 times, respectively, over all $\mathbb{Q}(\sqrt{d})$, where $0 < d < 100$.

We were unable to determine the exact number of times that the group $\mathbb{Z}/16\mathbb{Z}$ appears as a torsion subgroup because of the following problem: computing (in Magma) the rank of the Jacobian of the modular curve $X_1(16)$ defined over the problematic quadratic fields listed in the table did not give a result, only the lower and the upper bound that were not the same, and were always 0 and 2. That was a problem since it is important to know the mentioned rank in order to know which method to use for determining whether that is a possible torsion subgroup or not.

Also, searching for the points on the modular curve $X_1(16)$ over the same fields did not yield a result.

Fields	Possible torsion subgroups over a given field
$\mathbb{Q}(\sqrt{2})$	$\mathbb{Z}/n\mathbb{Z},\ n = 11$
$\mathbb{Q}(\sqrt{3})$	$\mathbb{Z}/n\mathbb{Z},\ n = 14, 15$ $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z},\ n = 6$
$\mathbb{Q}(\sqrt{5})$	$\mathbb{Z}/n\mathbb{Z},\ n = 15$
$\mathbb{Q}(\sqrt{6})$	$\mathbb{Z}/n\mathbb{Z},\ n = 11, 14$ $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z},\ n = 5, 6$
$\mathbb{Q}(\sqrt{7})$	$\mathbb{Z}/n\mathbb{Z},\ n = 11, 14, 15$ $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z},\ n = 6$
$\mathbb{Q}(\sqrt{10})$	$\mathbb{Z}/n\mathbb{Z},\ n = 11, 14, 15, 16$ $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z},\ n = 5, 6$
$\mathbb{Q}(\sqrt{11})$	$\mathbb{Z}/n\mathbb{Z},\ n = 11, 15$
$\mathbb{Q}(\sqrt{13})$	$\mathbb{Z}/n\mathbb{Z},\ n = 11, 15$ $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z},\ n = 5, 6$
$\mathbb{Q}(\sqrt{14})$	$\mathbb{Z}/n\mathbb{Z},\ n = 14, 15$ $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z},\ n = 5$
$\mathbb{Q}(\sqrt{15})$	$\mathbb{Z}/n\mathbb{Z},\ n = 15, 16$ $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z},\ n = 5$
$\mathbb{Q}(\sqrt{17})$	$\mathbb{Z}/n\mathbb{Z},\ n = 11, 13, 14$ $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z},\ n = 5, 6$
$\mathbb{Q}(\sqrt{19})$	$\mathbb{Z}/n\mathbb{Z},\ n = 11, 14$ $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z},\ n = 5$
$\mathbb{Q}(\sqrt{21})$	$\mathbb{Z}/n\mathbb{Z},\ n = 11$ $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z},\ n = 6$
$\mathbb{Q}(\sqrt{22})$	$\mathbb{Z}/n\mathbb{Z},\ n = 11, 14, 15$ $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z},\ n = 6$
$\mathbb{Q}(\sqrt{23})$	$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z},\ n = 6$
$\mathbb{Q}(\sqrt{26})$	$\mathbb{Z}/n\mathbb{Z},\ n = 14, 15,$ maybe $\mathbb{Z}/16\mathbb{Z}$ $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z},\ n = 5$
$\mathbb{Q}(\sqrt{29})$	$\mathbb{Z}/n\mathbb{Z},\ n = 11, 14, 15$ $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z},\ n = 5$

Fields	Possible torsion subgroups over a given field
$\mathbb{Q}(\sqrt{30})$	$\mathbb{Z}/n\mathbb{Z},\ n = 11, 15$
	$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z},\ n = 5, 6$
$\mathbb{Q}(\sqrt{31})$	$\mathbb{Z}/n\mathbb{Z},\ n = 14,$ maybe $\mathbb{Z}/16\mathbb{Z}$
	$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z},\ n = 5$
$\mathbb{Q}(\sqrt{33})$	$\mathbb{Z}/n\mathbb{Z},\ n = 11, 14, 15, 18$
	$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z},\ n = 5$
$\mathbb{Q}(\sqrt{34})$	$\mathbb{Z}/n\mathbb{Z},\ n = 14, 15$
	$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z},\ n = 5, 6$
$\mathbb{Q}(\sqrt{35})$	$\mathbb{Z}/n\mathbb{Z},\ n = 11, 14$
	$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z},\ n = 5, 6$
$\mathbb{Q}(\sqrt{37})$	$\mathbb{Z}/n\mathbb{Z},\ n = 14, 15$
	$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z},\ n = 5, 6$
$\mathbb{Q}(\sqrt{38})$	$\mathbb{Z}/n\mathbb{Z},\ n = 14, 15$
$\mathbb{Q}(\sqrt{39})$	$\mathbb{Z}/n\mathbb{Z},\ n = 11$
	$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z},\ n = 5, 6$
$\mathbb{Q}(\sqrt{41})$	$\mathbb{Z}/n\mathbb{Z},\ n = 11, 14, 15, 16$
	$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z},\ n = 6$
$\mathbb{Q}(\sqrt{42})$	$\mathbb{Z}/n\mathbb{Z},\ n = 14, 15$
	$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z},\ n = 6$
$\mathbb{Q}(\sqrt{43})$	$\mathbb{Z}/n\mathbb{Z},\ n = 11, 15$
$\mathbb{Q}(\sqrt{46})$	$\mathbb{Z}/n\mathbb{Z},\ n = 11$
	$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z},\ n = 5, 6$
$\mathbb{Q}(\sqrt{47})$	$\mathbb{Z}/n\mathbb{Z},\ n = 14,$ maybe $\mathbb{Z}/16\mathbb{Z}$
	$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z},\ n = 6$
$\mathbb{Q}(\sqrt{51})$	$\mathbb{Z}/n\mathbb{Z},\ n = 11, 14, 16$
	$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z},\ n = 5$
$\mathbb{Q}(\sqrt{53})$	$\mathbb{Z}/n\mathbb{Z},\ n = 14$
	$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z},\ n = 5$

Fields	Possible torsion subgroups over a given field
$\mathbb{Q}(\sqrt{55})$	$\mathbb{Z}/n\mathbb{Z},\ n = 11, 14, 15$
	$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z},\ n = 5, 6$
$\mathbb{Q}(\sqrt{57})$	$\mathbb{Z}/n\mathbb{Z},\ n = 11, 15$
	$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z},\ n = 5$
$\mathbb{Q}(\sqrt{58})$	$\mathbb{Z}/n\mathbb{Z},\ n = 11, 15,$ maybe $\mathbb{Z}/16\mathbb{Z}$
	$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z},\ n = 6$
$\mathbb{Q}(\sqrt{59})$	$\mathbb{Z}/n\mathbb{Z},\ n = 14, 15$
	$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z},\ n = 5, 6$
$\mathbb{Q}(\sqrt{61})$	$\mathbb{Z}/n\mathbb{Z},\ n = 11$
	$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z},\ n = 6$
$\mathbb{Q}(\sqrt{62})$	$\mathbb{Z}/n\mathbb{Z},\ n = 11, 14,$ maybe $\mathbb{Z}/16\mathbb{Z}$
$\mathbb{Q}(\sqrt{65})$	$\mathbb{Z}/n\mathbb{Z},\ n = 11$
	$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z},\ n = 6$
$\mathbb{Q}(\sqrt{66})$	$\mathbb{Z}/n\mathbb{Z},\ n = 11, 14$
	$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z},\ n = 5, 6$
$\mathbb{Q}(\sqrt{67})$	$\mathbb{Z}/n\mathbb{Z},\ n = 15$
$\mathbb{Q}(\sqrt{69})$	$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z},\ n = 6$
$\mathbb{Q}(\sqrt{70})$	$\mathbb{Z}/n\mathbb{Z},\ n = 14, 15, 16$
	$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z},\ n = 5, 6$
$\mathbb{Q}(\sqrt{71})$	$\mathbb{Z}/n\mathbb{Z},\ n = 14, 15$
	$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z},\ n = 5, 6$
$\mathbb{Q}(\sqrt{73})$	$\mathbb{Z}/n\mathbb{Z},\ n = 11, 14, 15$
	$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z},\ n = 5, 6$
$\mathbb{Q}(\sqrt{74})$	$\mathbb{Z}/n\mathbb{Z},\ n = 11, 15,$ maybe $\mathbb{Z}/16\mathbb{Z}$
	$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z},\ n = 5$
$\mathbb{Q}(\sqrt{77})$	$\mathbb{Z}/n\mathbb{Z},\ n = 11$
	$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z},\ n = 5$
$\mathbb{Q}(\sqrt{78})$	$\mathbb{Z}/n\mathbb{Z},\ n = 15,$ maybe $\mathbb{Z}/16\mathbb{Z}$
	$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z},\ n = 6$

Fields	Possible torsion subgroups over a given field
$\mathbb{Q}(\sqrt{79})$	$\mathbb{Z}/n\mathbb{Z},\ n = 11, 14,$ maybe $\mathbb{Z}/16\mathbb{Z}$
	$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z},\ n = 5$
$\mathbb{Q}(\sqrt{82})$	$\mathbb{Z}/n\mathbb{Z},\ n = 14, 15,$ maybe $\mathbb{Z}/16\mathbb{Z}$
	$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z},\ n = 6$
$\mathbb{Q}(\sqrt{83})$	$\mathbb{Z}/n\mathbb{Z},\ n = 11, 14$
	$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z},\ n = 6$
$\mathbb{Q}(\sqrt{85})$	$\mathbb{Z}/n\mathbb{Z},\ n = 11, 14, 15$
	$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z},\ n = 6$
$\mathbb{Q}(\sqrt{86})$	$\mathbb{Z}/n\mathbb{Z},\ n = 11, 15$
	$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z},\ n = 5$
$\mathbb{Q}(\sqrt{87})$	$\mathbb{Z}/n\mathbb{Z},\ n = 11, 14, 15,$ maybe $\mathbb{Z}/16\mathbb{Z}$
$\mathbb{Q}(\sqrt{89})$	$\mathbb{Z}/n\mathbb{Z},\ n = 14, 15$
	$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z},\ n = 5, 6$
$\mathbb{Q}(\sqrt{91})$	$\mathbb{Z}/n\mathbb{Z},\ n = 11, 14, 15$
	$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z},\ n = 5$
$\mathbb{Q}(\sqrt{93})$	$\mathbb{Z}/n\mathbb{Z},\ n = 14, 15, 16$
	$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z},\ n = 5, 6$
$\mathbb{Q}(\sqrt{94})$	$\mathbb{Z}/n\mathbb{Z},\ n = 11, 14,$ maybe $\mathbb{Z}/16\mathbb{Z}$
	$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z},\ n = 5, 6$
$\mathbb{Q}(\sqrt{95})$	$\mathbb{Z}/n\mathbb{Z},\ n = 11$
	$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z},\ n = 5, 6$
$\mathbb{Q}(\sqrt{97})$	$\mathbb{Z}/n\mathbb{Z},\ n = 14, 15$
	$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z},\ n = 5$

Table 6.1: The list of all possible torsion groups over quadratic fields $\mathbb{Q}(\sqrt{d})$, for $0 < d < 100$, with the exception of the groups from Mazur's theorem

7. SPLITTING OF PRIMES IN NUMBER FIELDS GENERATED BY POINTS ON SOME MODULAR CURVES

This chapter will mostly follow a paper by Filip Najman and the author [39]. We will focus here on finding some interesting properties of elliptic curves and number fields when elliptic curves have given torsion subgroup or isogeny and are defined over a number field of given degree.

A famous and much-studied problem in the theory of elliptic curves, going back to Mazur's torsion theorem [32], was to determine the possible torsion groups of elliptic curves over K, for a given number field K or over all number fields of degree d. We studied the special case of $d = 2$ of this question in Chapter 6. Here we are more interested in the inverse question:

Question 7.0.1. For a given torsion group T and a positive integer d, for which and what kind of number fields K of degree d do there exist elliptic curves E such that $E(K) \simeq T$?

To make Question 7.0.1 sensible, one should of course choose the group T in a such a way that the set of such fields should be non-empty and preferably infinite.

It has been noted already by Momose [35] in 1984 (see also [26]) that the existence of specific torsion groups T over a quadratic field K forces certain rational primes to split in a particular way in K. Krumm [27] in his PhD thesis obtained similar results about splitting of primes over quadratic fields K with $T \simeq \mathbb{Z}/13\mathbb{Z}$ or $\mathbb{Z}/18\mathbb{Z}$ and it was also proven by Bosman, Bruin, Dujella and Najman [3] and Krumm [27] independently that all such quadratic fields must be real. These results were already stated in Theorems 6.2.6

and 6.2.7.

The first such result over cubic fields was proven by Bruin and Najman [5], where it was shown for $T \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/14\mathbb{Z}$ that all such cubic fields K must be cyclic. In this chapter we explore this particular case further and prove in Section 7.2 that in such a field 2 always splits, giving the first description of a splitting behaviour forced by the existence of a torsion group of an elliptic curve over a cubic field. Furthermore, we show that all primes $q \equiv \pm 1 \pmod 7$ of multiplicative reduction for such curves split in K. The proof of these results turns out to be more intricate than in the quadratic case.

As Question 7.0.1 can equivalently be phrased as asking when the modular curve $X_1(M,N)$ parameterizing elliptic curves together with the generators of a torsion subgroup $T \cong \mathbb{Z}/M\mathbb{Z} \oplus \mathbb{Z}/N\mathbb{Z}$ has non-cuspidal points over K, one is naturally drawn to ask a more general question by replacing $X_1(M,N)$ by any modular curve X.

Question 7.0.2. For a given modular curve X and a positive integer d, for which and what kind of number fields K of degree d do there exist non-cuspidal points in $X(K)$?

The most natural modular curves to consider next are the classical modular curves $X_0(N)$ classifying elliptic curves with cyclic isogenies of degree N. For $N = 28$ and 40 Bruin and Najman [6] proved that quadratic fields K over which $X_0(N)$ have non-cuspidal points are always real. In this chapter we prove the first results about splitting of certain primes over quadratic fields where some modular curves $X_0(N)$ have non-cuspidal points. We consider all the N such that $X_0(N)$ is hyperelliptic except for $N = 37$, in particular

$$N \in \{22,23,26,28,29,30,31,33,35,39,40,41,46,47,48,50,59,71\}. \tag{7.0.1}$$

The reason we exclude $N = 37$ is that the quadratic points on $X_0(37)$ cannot all be described (with finitely many exceptions) as inverse images of $\mathbb{P}^1(\mathbb{Q})$ with respect to the degree 2 hyperelliptic map $X_0(37) \to \mathbb{P}^1$. For more details about quadratic points on $X_0(37)$, see [4]. In Section 7.1 we prove a series of results about the splitting behaviour of various primes in quadratic fields generated by quadratic points on $X_0(N)$.

A difficulty in proving these results that one immediately encounters is that the methods of [26] and [35] cannot be adapted to $X_0(N)$ as the existence of a torsion point of large order forces bad reduction on the elliptic curve (see for example [35, Lemma 1.9]), while the existence of an isogeny does not. Hence we approach the problem via explicit

equations and parameterizations of modular curves, more in the spirit of [3, 6, 27] instead of moduli-theoretic considerations as in [26, 35].

González [15] proved results about fields generated by j-invariants of $\mathbb{Q}$-curves. Since for the values N that we study almost all N-isogenies over quadratic fields come from $\mathbb{Q}$-curves, our results are reminiscent of his, but it turns out there is little overlap in the results that are proved. This is perhaps not very surprising as we do not use the fact that we are looking at $\mathbb{Q}$-curves at all.

The computations in this chapter were executed in the computer algebra system Magma [2]. The code used in this paper can be found at `https://web.math.pmf.unizg.hr/~atrbovi/magma/magma2.htm` or in Appendix B.

7.1. Splitting of primes in quadratic fields generated by points on $X_0(N)$

In this section we study the splitting behaviour of primes in quadratic fields over which the modular curves $X_0(N)$ have non-cuspidal points. Models for $X_0(N)$ have been obtained from the `SmallModularCurves` database in Magma and can be found in Table 7.1.

N	$f_N(x)$ from the equation $y^2 = f_N(x)$ for $X_0(N)$ and the factorization in $\mathbb{Q}[X]$
22	$x^6 - 4x^4 + 20x^3 - 40x^2 + 48x - 32$
	$= (x^3 - 2x^2 + 4x - 4)(x^3 + 2x^2 - 4x + 8)$
23	$x^6 - 8x^5 + 2x^4 + 2x^3 - 11x^2 + 10x - 7$
	$= (x^3 - 8x^2 + 3x - 7)(x^3 - x + 1)$
26	$x^6 - 8x^5 + 8x^4 - 18x^3 + 8x^2 - 8x + 1$
28	$4x^6 - 12x^5 + 25x^4 - 30x^3 + 25x^2 - 12x + 4$
	$= (2x^2 - 3x + 2)(x^2 - x + 2)(2x^2 - x + 1)$
29	$x^6 - 4x^5 - 12x^4 + 2x^3 + 8x^2 + 8x - 7$
30	$x^8 + 14x^7 + 79x^6 + 242x^5 + 441x^4 + 484x^3 + 316x^2 + 112x + 16$
	$= (x^2 + 3x + 1)(x^2 + 6x + 4)(x^4 + 5x^3 + 11x^2 + 10x + 4)$

31	$x^6-8x^5+6x^4+18x^3-11x^2-14x-3$
	$=(x^3-6x^2-5x-1)(x^3-2x^2-x+3)$
33	$x^8+10x^6-8x^5+47x^4-40x^3+82x^2-44x+33$
	$=(x^2-x+3)(x^6+x^5+8x^4-3x^3+20x^2-11x+11)$
35	$x^8-4x^7-6x^6-4x^5-9x^4+4x^3-6x^2+4x+1$
	$=(x^2+x-1)(x^6-5x^5-9x^3-5x-1)$
39	$x^8-6x^7+3x^6+12x^5-23x^4+12x^3+3x^2-6x+1$
	$=(x^4-7x^3+11x^2-7x+1)(x^4+x^3-x^2+x+1)$
40	$x^8+8x^6-2x^4+8x^2+1$
41	$x^8-4x^7-8x^6+10x^5+20x^4+8x^3-15x^2-20x-8$
46	$x^{12}-2x^{11}+5-x^{10}+6x^9-26x^8+84x^7-113x^6+134x^5-64x^4+26x^3+12x^2+8x-7$
	$=(x^3-2x^2+3x-1)(x^3+x^2-x+7)(x^6-x^5+4x^4-x^3+2x^2+2x+1)$
47	$x^{10}-6x^9+11x^8-24x^7+19x^6-16x^5-13x^4+30x^3-38x^2+28x-11$
	$=(x^5-5x^4+5x^3-15x^2+6x-11)(x^5-x^4+x^3+x^2-2x+1)$
48	x^8+14x^4+1
	$=(x^4-2x^3+2x^2+2x+1)(x^4+2x^3+2x^2-2x+1)$
50	$x^6-4x^5-10x^3-4x+1$
59	$x^{12}-8x^{11}+22x^{10}-28x^9+3x^8+40x^7-62x^6+40x^5-3x^4-24x^3+20x^2-4x-8$
	$=(x^3-x^2-x+2)(x^9-7x^8+16x^7-21x^6+12x^5-x^4-9x^3+6x^2-4x-4)$
71	$x^{14}+4x^{13}-2x^{12}-38x^{11}-77x^{10}-26x^9+111x^8+148x^7+$
	$+x^6-122x^5-70x^4+30x^3+40x^2+4x-11$
	$=(x^7-7x^5-11x^4+5x^3+18x^2+4x-11)(x^7+4x^6+5x^5+x^4-3x^3-2x^2+1)$

Table 7.1: Polynomials $f_N(x)$ in the equations $y^2=f_N(x)$ for $X_0(N)$.

Following [27], on a hyperelliptic curve X with a model $y^2=f(x)$, we say that the quadratic points on X of the form $(x_0,\sqrt{f(x_0)})$, where $x_0\in\mathbb{Q}$, are *obvious*. The quadratic points that are not obvious are called *non-obvious*. By the results of [6], all non-cuspidal quadratic points on $X_0(N)$ are obvious, with finitely many explicitly listed exceptions.

Theorem 7.1.1. Let $K=\mathbb{Q}(\sqrt{D})$, where D is squarefree, be a quadratic field over which $X_0(N)$ has an obvious non-cuspidal point.

(a) For each N, columns 2-5 in the table below show the splitting behaviour in K of some of the small primes, as well as some properties of D.

(b) For the pairs of N and a indicated in the table, if a prime p ramifies in K, then a is a square modulo p.

(c) For the pairs of N and b indicated in the table, if $p \neq 2$ is a prime such that b is a square modulo p, then there exist infinitely many quadratic fields generated by a point on $X_0(N)$ in which p ramifies.

N	not inert	unramified	splits	D	a	b
22	$\underline{2}^*$					
26	$\underline{13}$			odd	13	
28	$3,7$	3	3	>0	-7^{***}	-7
29	$\underline{29}$			odd	29	
30	$\underline{2},\underline{3},\underline{5}^{**}$	$\underline{2},\underline{3}$	$\underline{2},\underline{3}$	odd	5	5
33	$2,\underline{11}$	$\underline{2}$	2	>0 odd	-11	-11
35	$\underline{5}^{**},\underline{7}$	$\underline{2},\underline{7}$	$\underline{7}$	odd	5	5
39	$3,\underline{13}$	$\underline{2},\underline{13}$	$\underline{13}$	odd	13	
40	$2,3,5$	$2,3,5$	$2,3,5$	>0 odd	$-1,5$	
41	$\underline{41}$				41	
46	2	$\underline{2}$	2	odd		
48	2	$2,3,5$	$2,3,5$	>0 odd	$-1,3$	
50	5			odd	5	

* -even more is true, $D \equiv 1,2,6 \pmod 8$

** -even more is true, $D \equiv 0,1 \pmod 5$

*** -the statement of (b) is true with the exception of $p = 2$

_ -see Remark 7.1.9

Table 7.2: Splitting behaviour of small primes

Many proofs will be similar for different values of N and before proceeding to a case-by-case study, we mention some general results which will be useful.

We fix the following notation throughout this section. Let N be one of the integers from (7.0.1) and write

$$X_0(N) : y^2 = f_N(x) = \sum_{i=0}^{\deg f_N} a_{i,N} x^i,$$

with $a_{i,N} \in \mathbb{Z}$. Note that in all instances $\deg f_N$ is even. As already stated, all non-cuspidal quadratic points on $X_0(N)$ are obvious, with finitely many exceptions. Those exceptions can be found listed in [6, Tables 1-18]. Let $(x_0, \sqrt{f_N(x_0)})$, for some $x_0 \in \mathbb{Q}$, be an obvious point on $X_0(N)$ and write $x_0 = m/n$, with m and n coprime integers. Let $d := f_N(x_0)$, $s := n^{\deg f_N} d$, and let D be the square-free part of d, i.e. the unique square-free integer such that $n^{\deg f_N} d = Ds^2$, for some $s \in \mathbb{Q}$. Since $\deg f_N$ is even, it follows that $s \in \mathbb{Z}$. We get the equality

$$n^{\deg f_N} d = Ds^2 = \sum_{i=0}^{\deg f_N} a_{i,N} m^i n^{deg f_N - i}. \tag{7.1.1}$$

The point $(x_0, \sqrt{f_N(x_0)})$ will be defined over $K := \mathbb{Q}(\sqrt{D})$.

We will prove part (a) of the theorem for each N separately. This proof can unfortunately not be generalized for each column of Table 7.2 as it can be for parts (b) and (c) of the theorem. However, we do mention a number of lemmas that describe the splitting behaviour of primes in K, which we will be using throughout. They are well-known or obvious, so we omit the proofs.

Lemma 7.1.2. An odd prime p ramifies in K if and only if $p \mid D$, splits in K if and only if $\left(\frac{D}{p}\right) = 1$ and is inert in K if and only if $\left(\frac{D}{p}\right) = -1$.

Lemma 7.1.3. Let p be an odd prime and assume that we have $Ds^2 \equiv ap^t \pmod{p^\ell}$ with $p \nmid a$ and $\ell > t$.

a) If $t = 2k$ for some $k \in \mathbb{Z}_0^+$, then $v_p(s) = k$, $D \equiv a(p^k/s)^2 \pmod{p^{\ell-t}}$, and p splits in K if and only if a is a square modulo p.

b) If $t = 2k+1$ for some $k \in \mathbb{Z}_0^+$, then $p|D$ and p ramifies in K.

As previous lemmas stated results about splitting for odd primes, we include similar results for the prime $p = 2$.

Lemma 7.1.4. The prime 2 ramifies in K if and only if $D \not\equiv 1 \pmod 4$, splits in K if and only if $D \equiv 1 \pmod 8$ and is inert in K if and only if $D \equiv 5 \pmod 8$.

Lemma 7.1.5. Assume that we have $Ds^2 \equiv 2^t a \pmod{2^\ell}$, with $2 \nmid a$ and $\ell > t$.

(a) If $t = 2k$, for some $k \in \mathbb{Z}_0^+$, then $v_2(s) = k$ and $D \equiv a(2^k/s)^2 \pmod{2^{\ell-t}}$. If $a = 1$ and $\ell - t = 3$, then 2 splits in K.

(b) If $t = 2k+1$, for some $k \in \mathbb{Z}_0^+$, then $D \equiv 2a \pmod{2^{\ell-2k}}$.

All of the computations done in the following proofs are listed in the accompanying Magma code.

Proof of Theorem 7.1.1 (a).

$\boldsymbol{N = 22}$: In the manner already described above, in (7.1.1) we get

$$n^6 d = Ds^2 = m^6 - 4m^4n^2 + 20m^3n^3 - 40m^2n^4 + 48mn^5 - 32n^6.$$

Considering all of the possibilities of m and n modulo 512, we have that $Ds^2 \equiv 1 \pmod 8$, $Ds^2 \equiv 32 \pmod{64}$ or $Ds^2 \equiv 64 \pmod{512}$. Using Lemma 7.1.5 this becomes $D \equiv 1 \pmod 8$ or $D \equiv 2 \pmod 4$. In any case we have $D \equiv 1, 2, 6 \pmod 8$, so 2 is not inert, according to Lemma 7.1.4.

$\boldsymbol{N = 26}$: In (7.1.1) we get

$$n^6 d = Ds^2 = m^6 - 8m^5n + 8m^4n^2 - 18m^3n^3 + 8m^2n^4 - 8mn^5 + n^6.$$

Looking at all the possibilities of m and n modulo 13^2, we see that $Ds^2 \equiv 1, 3, 4, 9, 10, 12 \pmod{13}$ or $Ds^2 \equiv 4 \cdot 13, 9 \cdot 13 \pmod{13^2}$. It follows from Lemma 7.1.3 that $D \equiv 0, 1, 3, 4, 9, 10, 12 \pmod{13}$. Using Lemma 7.1.2 we immediately get that 13 is not inert.

Considering the possibilities of m and n modulo 128, we have that $Ds^2 \equiv 1 \pmod 2$, $Ds^2 \equiv 4 \pmod{16}$, $Ds^2 \equiv 16 \pmod{32}$ or $Ds^2 \equiv 64 \pmod{128}$. Using Lemma 7.1.5 this becomes $D \equiv 1 \pmod 2$ or $D \equiv 1 \pmod 4$, so D is always odd.

$N = 28$: In (7.1.1) we get

$$n^6 d = Ds^2 = 4m^6 - 12m^5 n + 25m^4 n^2 - 30m^3 n^3 + 25m^2 n^4 - 12mn^5 + 4n^6.$$

Considering the possibilities of m and n modulo 3, we get $Ds^2 \equiv 1 \pmod 3$, so from Lemma 7.1.3 we have $D \equiv 1 \pmod 3$, and the fact that 3 splits follows from Lemma 7.1.2.

Looking at all the possibilities of m and n modulo 7^2, we see that $Ds^2 \equiv 1,2,4 \pmod 7$ or $Ds^2 \equiv 14 \pmod{7^2}$. It follows from Lemma 7.1.3 that $D \equiv 0,1,2,4 \pmod 7$ and from Lemma 7.1.2 that 7 is not inert.

The proof of the fact that $D > 0$ can be found in [6, Theorem 4].

$N = 29$: In (7.1.1) we get

$$n^6 d = Ds^2 = m^6 - 4m^5 n - 12m^4 n^2 + 2m^3 n^3 + 8m^2 n^4 + 8mn^5 - 7n^6.$$

Considering the possibilities of m and n modulo 32, we have that $Ds^2 \equiv 1 \pmod 2$, $Ds^2 \equiv 12 \pmod{16}$ or $Ds^2 \equiv 16 \pmod{32}$. Using Lemma 7.1.5 this becomes $D \equiv 1 \pmod 2$ or $D \equiv 3 \pmod 4$, so D is always odd.

We write $D = 29^a \cdot p_1 \cdot \ldots \cdot p_k$, where $a \in \{0,1\}$ and $p_i \neq 2$, since D is odd. If $a = 1$, then $D \equiv 0 \pmod{29}$. If $a = 0$, then $\left(\frac{D}{29}\right) = \left(\frac{p_1}{29}\right) \cdot \ldots \cdot \left(\frac{p_k}{29}\right)$, which is equal to 1 after using the part (b) of this theorem for $N = 29$. In this case we have that $\left(\frac{D}{29}\right) = 1$, and Lemma 7.1.2 says that 29 is not inert.

$N = 30$: In (7.1.1) we get

$$\begin{aligned} n^8 d = Ds^2 =& m^8 + 14m^7 n + 79m^6 n^2 + 242m^5 n^3 + 441m^4 n^4 \\ &+ 484m^3 n^5 + 316m^2 n^6 + 112mn^7 + 16n^8. \end{aligned}$$

Considering the possibilities of m and n modulo 128, we have that $Ds^2 \equiv 16 \pmod{128}$ or $Ds^2 \equiv 1 \pmod 8$. Using Lemma 7.1.5 we get $D \equiv 1 \pmod 8$, and from Lemma 7.1.4 we conclude that 2 splits.

Considering the possibilities of m and n modulo 3, we have that $Ds^2 \equiv 1 \pmod 3$, and from Lemma 7.1.3 we conclude that $D \equiv 1 \pmod 3$. The fact that 3 splits follows from Lemma 7.1.2.

Looking at all the possibilities of m and n modulo 25, we see that $Ds^2 \equiv 1 \pmod 5$ or $Ds^2 \equiv 5 \pmod{25}$. Using Lemma 7.1.3 we get $D \equiv 0,1,4 \pmod 5$ and from Lemma 7.1.2 we see that 5 is not inert.

Furthermore, we want to eliminate the possibility $D \equiv 4 \pmod 5$. If it were true, then for s in $n^8 d = Ds^2$ it holds $s^2 \equiv 4 \pmod 5$, so s would be divisible by a prime p such that $p \equiv 2,3 \pmod 5$, i.e. $\left(\frac{5}{p}\right) = -1$.

The expression $n^8 d = Ds^2$ above factorizes as

$$n^8 d = Ds^2 = \left(m^2+6nm+4n^2\right)\left(m^2+3nm+n^2\right)\left(m^4+5m^3n+11m^2n^2+10mn^3+4n^4\right),$$

so p has to divide one of the 3 factors on the right.

- If p divides $m^2+6nm+4n^2 = (m+3n)^2-5n^2$, then $\left(\frac{5}{p}\right) = 1$, so $p \not\equiv 2,3 \pmod 5$.
- If p divides the second factor, it also divides $4(m^2+3nm+n^2) = (2m+3n)^2-5n^2$, then $\left(\frac{5}{p}\right) = 1$, so $p \not\equiv 2,3 \pmod 5$.
- If p divides $m^4+5m^3n+11m^2n^2+10mn^3+4n^4 = (2m^2+5mn+4n^2)^2+3m^2n^2$, then $\left(\frac{-3}{p}\right) = 1$. The third factor can also be written as $(2m^2+5mn+m^2)^2+15(n^2+mn)^2$, so we alse have $\left(\frac{-15}{p}\right) = 1$. Combining these two facts, we get $\left(\frac{5}{p}\right) = 1$, which is also a contradiction.

$\boldsymbol{N = 33}$: In (7.1.1) we get

$$n^8 d = Ds^2 = m^8+10m^6n^2-8m^5n^3+47m^4n^4-40m^3n^5+82m^2n^6-44mn^7+33n^8.$$

Considering the possibilities of m and n modulo 8, we have that $Ds^2 \equiv 1 \pmod 8$, so from Lemma 7.1.5 we conclude that $D \equiv 1 \pmod 8$ and from Lemma 7.1.4 that the prime 2 splits.

We write $D = 11^a \cdot p_1 \cdot \ldots \cdot p_k$, where $a \in \{0,1\}$ and $p_i \neq 2$, since $D \equiv 1 \pmod 8$. If $a = 1$, then $D \equiv 0 \pmod{11}$. If $a = 0$, then $\left(\frac{D}{11}\right) = \left(\frac{p_1}{11}\right) \cdot \ldots \cdot \left(\frac{p_k}{11}\right)$, which is equal to 1 after using the part (b) of this theorem for $N = 33$. In this case we have that $\left(\frac{D}{11}\right) = 1$, therefore 11 is not inert in K.

A point of the form $(x_0, \sqrt{f_{33}(x_0)})$ with $x_0 \in \mathbb{Q}$ is clearly defined over a real quadratic field, since $f_{33}(x_0) = x_0^8+10x_0^6-8x_0^5+47x_0^4-40x_0^3+82x_0^2-44x_0+33 > 0$, for every x_0.

Therefore, $D > 0$.

$\boldsymbol{N = 35}$: In (7.1.1) we get

$$n^8 d = Ds^2 = m^8 - 4m^7 n - 6m^6 n^2 - 4m^5 n^3 - 9m^4 n^4 + 4m^3 n^5 - 6m^2 n^6 + 4mn^7 + n^8.$$

Considering the possibilities of m and n modulo 4, we have that $Ds^2 \equiv 1 \pmod 4$ and from Lemma 7.1.5 we conclude $D \equiv 1 \pmod 4$. The fact that 2 is unramified now follows from Lemma 7.1.4.

Looking at all the possibilities of m and n modulo 25, we see that $Ds^2 \equiv 1 \pmod 5$ or $Ds^2 \equiv 5 \pmod{25}$. It follows from Lemma 7.1.3 that $D \equiv 0, 1, 4 \pmod 5$ and from Lemma 7.1.2 that 5 is not inert.

Now want to eliminate the possibility $D \equiv 4 \pmod 5$. If it were true, then for s in $n^8 d = Ds^2$ it holds $s^2 \equiv 4 \pmod 5$, so s would be divisible by a prime p such that $p \equiv 2, 3 \pmod 5$, i.e. $\left(\frac{5}{p}\right) = -1$.

The expression $n^8 d = Ds^2$ above factorizes as

$$n^8 d = Ds^2 = \left(-m^2 - mn + n^2\right)\left(-m^6 + 5m^5 n + 9m^3 n^3 + 5mn^5 + n^6\right),$$

so p has to divide one of the 2 factors on the right.

- If p divides the first factor, it also divides $4(-m^2 - nm + n^2) = (2m - n)^2 - 5m^2$, then $\left(\frac{5}{p}\right) = 1$, so $p \not\equiv 2, 3 \pmod 5$.
- If p divides the second factor, it also divides $4(-m^6 + 5m^5 n + 9m^3 n^3 + 5mn^5 + n^6) = (2n^3 + 5n^2 m + 5nm^2 + 4m^3)^2 - 5(3n^2 m + nm^2 + 2m^3)^2$, then $\left(\frac{5}{p}\right) = 1$, so $p \not\equiv 2, 3 \pmod 5$.

And in the end, considering the possibilities of m and n modulo 7, we have that $Ds^2 \equiv 1, 2, 4 \pmod 7$. It follows from Lemma 7.1.3 that $D \equiv 1, 2, 4 \pmod 7$ and from Lemma 7.1.2 that 7 splits.

$\boldsymbol{N = 39}$: In (7.1.1) we get

$$n^8 d = Ds^2 = m^8 - 6m^7 n + 3m^6 n^2 + 12m^5 n^3 - 23m^4 n^4 + 12m^3 n^5 + 3m^2 n^6 - 6mn^7 + n^8.$$

Considering the possibilities of m and n modulo 4, we have that $Ds^2 \equiv 1 \pmod 4$ and from Lemma 7.1.5 we conclude $D \equiv 1 \pmod 4$. The fact that 2 is unramified now follows from Lemma 7.1.4.

We have that the right side of $n^8 d = Ds^2$ above is congruent to $m^8 - 2m^4n^4 + n^8 = (m^4 - n^4)^2$ modulo 3.

Suppose first that $m \not\equiv n \pmod 3$. If $n \not\equiv 0 \pmod 3$ then D is a square modulo 3 and if $n \equiv 0 \pmod 3$ then it follows that $D \equiv 1 \pmod 3$ so D is again a square modulo 3. Suppose now that $m \equiv n \pmod 3$. Then we run through all the possibilities of m and n modulo 81 and note that either Ds^2 is divisible by an odd power of 3, so $D \equiv 0 \pmod 3$, or $Ds^2 \equiv 9k \pmod{81}$, where $k \not\equiv 0 \pmod{81}$ and k is a square modulo 9. Using Lemma 7.1.3 we get that $D \equiv k \pmod 9$, where k is a square modulo 9. Hence, in all cases we have $D \equiv 0, 1 \pmod 3$ and from Lemma 7.1.4 we immediately see that 3 is not inert.

Considering the possibilities of m and n modulo 13, we have that $Ds^2 \equiv 1, 3, 4, 9, 10, 12 \pmod{13}$, and from Lemma 7.1.3 we conclude $D \equiv 1, 3, 4, 9, 10, 12 \pmod{13}$. The fact that 13 splits now follows from Lemma 7.1.2.

$\boldsymbol{N = 40}$: In (7.1.1) we get

$$n^8 d = Ds^2 = m^8 + 8m^6n^2 - 2m^4n^4 + 8m^2n^6 + n^8.$$

We write $n^8 d = Ds^2$ as

$$n^8 d = Ds^2 = (m^4 - n^4)^2 + 8m^2n^2(m^4 + n^4).$$

The integer n has to be odd (otherwise m and n would both be even), and if m is even, then Ds^2 is an odd square modulo 8. It follows from Lemma 7.1.5 that $D \equiv 1 \pmod 8$ and from Lemma 7.1.4 that 2 splits.

If m and n are both odd, then $Ds^2 \equiv 16m^2n^2 \pmod{128}$. From Lemma 7.1.5 we get that D is an odd square modulo 8, i.e. $D \equiv 1 \pmod 8$. The fact that 2 splits now follows from Lemma 7.1.4.

Considering the possibilities of m and n modulo 3, we have that $Ds^2 \equiv 1 \pmod 3$. Using Lemma 7.1.3 we get $D \equiv 1 \pmod 3$, and from Lemma 7.1.2 we conclude that 3 splits.

Looking at all the possibilities of m and n modulo 5, we see that $Ds^2 \equiv 1,4 \pmod 5$. Using Lemma 7.1.3 we get $D \equiv 1,4 \pmod 5$, and from Lemma 7.1.2 we conclude that 5 splits.

The proof of the fact that $D > 0$ can be found in [6, Theorem 4].

$\boldsymbol{N = 41}$: In (7.1.1) we get

$$n^8 d = Ds^2 = m^8 - 4m^7 n - 8m^6 n^2 + 10m^5 n^3 + 20m^4 n^4 + 8m^3 n^5 - 15m^2 n^6 - 20mn^7 - 8n^8.$$

We write $D = 41^a \cdot p_1 \cdot \ldots \cdot p_k$, where $a \in \{0,1\}$. If $a = 0$, then $D \equiv 0 \pmod{41}$. If $a = 1$, then $\left(\frac{D}{41}\right) = \left(\frac{p_1}{41}\right) \cdot \ldots \cdot \left(\frac{p_k}{41}\right)$, which is equal to 1 after using the part (b) of this theorem, and the fact that $\left(\frac{2}{41}\right) = 1$, in case one of the p_i is 2. In this case we have that $\left(\frac{D}{41}\right) = 1$, and Lemma 7.1.2 says that 41 is not inert.

$\boldsymbol{N = 46}$: In (7.1.1) we get

$$\begin{aligned} n^{12} d = Ds^2 =& m^{12} - 2m^{11} n + 5m^{10} n^2 + 6m^9 n^3 - 26m^8 n^4 + 84m^7 n^5 \\ & - 113m^6 n^6 + 134m^5 n^7 - 64m^4 n^8 + 26m^3 n^9 + 12m^2 n^{10} + 8mn^{11} - 7n^{12}. \end{aligned}$$

Considering the possibilities of m and n modulo 512, we have that $Ds^2 \equiv 64 \pmod{512}$ or $Ds^2 \equiv 1 \pmod 8$. Using Lemma 7.1.5, in both cases we get $D \equiv 1 \pmod 8$, and from Lemma 7.1.4 we conclude that 2 splits.

$\boldsymbol{N = 48}$: In (7.1.1) we get

$$n^8 d = Ds^2 = m^8 + 14m^4 n^4 + n^8.$$

We write $n^8 d = Ds^2$ as

$$n^8 d = Ds^2 = (m^4 + n^4)^2 + 12m^4 n^4.$$

If either m or n is even (forcing the other to be odd), then Ds^2 is an odd square modulo 8. It follows from Lemma 7.1.5 that $D \equiv 1 \pmod 8$ and from Lemma 7.1.4 that 2 splits. If m and n are both odd, then $Ds^2 \equiv 16 \pmod{128}$. It follows from Lemma 7.1.5 that $D \equiv 1 \pmod 8$ and from Lemma 7.1.4 that 2 splits.

Considering the possibilities of m and n modulo 3, we have that $Ds^2 \equiv 1 \pmod 3$. Using Lemma 7.1.3, we get $D \equiv 1 \pmod 3$, and from Lemma 7.1.2 we conclude that 3 splits.

Looking at all the possibilities of m and n modulo 5, we see that $Ds^2 \equiv 1 \pmod 5$. Using Lemma 7.1.3, we get $D \equiv 1,4 \pmod 5$, and from Lemma 7.1.2 we conclude that 5 splits.

A point of the form $(x_0, \sqrt{f_{48}(x_0)})$ with $x_0 \in \mathbb{Q}$ is clearly defined over a real quadratic field, since $f_{48}(x_0) = x_0^8 + 14x_0^4 + 1 > 0$, for every x_0. Therefore, $D > 0$.

$\boldsymbol{N = 50}$: In (7.1.1) we get

$$n^6 d = Ds^2 = m^6 - 4m^5 n - 10m^3 n^3 - 4mn^5 + n^6.$$

Considering the possibilities of m and n modulo 5, we have that $Ds^2 \equiv 0,1,4 \pmod 5$. Using Lemma 7.1.3, we get $D \equiv 0,1,4 \pmod 5$, and from Lemma 7.1.2 we conclude that 5 is not inert.

We have

$$n^6 d = Ds^2 \equiv (m^3 - n^3)^2 \pmod 4.$$

If either m or n is even it follows that D is odd. If m and n are both odd, we have $Ds^2 \equiv 4 \pmod{16}$, $Ds^2 \equiv 16 \pmod{32}$ or $Ds^2 \equiv 64 \pmod{128}$. Using Lemma 7.1.5, in all cases we get that D is odd. ■

We now prove two lemmas that will be useful in the proof of part (b) of the theorem.

Lemma 7.1.6. Suppose f_N factorizes as $f_N = \prod_{i \in I} f_{N,i}$, where $f_{N,i} \in \mathbb{Z}[x]$ are irreducible factors of degree 2 or 3 and $p \nmid a_{0,N}$. If p ramifies in K, then there exists an $i \in I$ such that $\Delta(f_{N,i})$ is a square modulo p.

Proof. Assume that p ramifies in K; then by Lemma 7.1.2 it follows that $p|D$. If $p|n$, then it would follow that $p|m$, which is a contradiction, so we conclude that $p \nmid n$. Dividing out (7.1.1) by n, we see that m/n is a root of f_N modulo p and hence there exists an $i \in I$ such that m/n is a root of $f_{N,i}$ modulo p.

If $f_{N,i}$ is of degree 2 or 3, the formulas for the roots of quadratic and cubic polynomials imply that $\sqrt{\Delta(f_{N,i})}$ is defined over $\mathbb{F}_p$, which proves the statement. ■

Remark 7.1.7. Note that the statement of part (b) of the theorem can be proved with the previous lemma only for $(N,a) = (28,-7)$. We have $f_{28}(x) = (2x^2-3x+2)(x^2-x+2)(2x^2-x+1)$ and $\Delta(f_{28,i}) = -7$, for each i.

As mentioned in the remark, Lemma 7.1.6 is not enough to prove all of the statements in (b), so we provide a generalization.

Lemma 7.1.8. Let $f_N = \prod_{i\in I} f_{N,i}$ be the decomposition into irreducible factors, with $f_{N,i} \in \mathbb{Z}[x]$. Assume that there exists a quadratic field K_0 such that each $f_{N,i}$ becomes reducible in $K_0[x]$ and let p be an odd prime such that $(p,\Delta(f_{N,i})) = 1$ for all i. Then if p ramifies in K it follows that $\Delta(K_0)$ is a square modulo p, i.e. p is not inert in K_0.

Proof. Let σ be the generator of $\mathrm{Gal}(K_0/\mathbb{Q})$ and $f_{N,i,K_0} \in K_0[x]$ an irreducible factor of $f_{N,i}$. Then we obviously have

$$f_{N,i,K_0}(f_{N,i,K_0})^{\sigma} = f_{N,i}. \tag{7.1.2}$$

Assume that p ramifies in K. We will prove the lemma by contradiction, so we assume that p is inert in K_0. As in the proof of Lemma 7.1.6 we conclude that $f_{N,i}$ has a root a in $\mathbb{F}_p$ for some i. Hence a is a root of one of the factors on the left in (7.1.2). Assume without loss of generality that a is a root of $f_{N,i}$ in $\mathbb{F}_p$.

Let $\mathfrak{p}$ be the prime of K above p and denote by $\mathbb{F}_{\mathfrak{p}} := \mathcal{O}_{K_0}/\mathfrak{p}$ the residue field of $\mathfrak{p}$. Let $\tau = \mathrm{Gal}(\mathbb{F}_{\mathfrak{p}}/\mathbb{F}_p)$ and denote by $\overline{f}$ the reduction of a polynomial $f \in K_0[x]$ modulo $\mathfrak{p}$; then we have $\overline{f^{\sigma}} = \overline{f}^{\tau}$. Hence a^{τ} is a root of $\overline{f}^{\tau}_{N,i}$. But since $a \in \mathbb{F}_p$, it follows that $a = a^{\tau}$ and hence from (7.1.2) it follows that a is a double root of $f_{N,i}$ over $\mathbb{F}_p$ and hence $\Delta(f_{N,i})$ is divisible by p, which is in contradiction with the assumption $(p,\Delta(f_{N,i})) = 1$. ■

Proof of Theorem 7.1.1 (b). Let $f_N = \Pi_i f_{N,i}$ be the factorization of f_N in $\mathbb{Z}[X]$, as in Table 7.1. Table 7.3, which can be computed with the accompanying Magma code, contains for each N the number a such that every $f_{N,i}$ becomes reducible in $\mathbb{Q}(\sqrt{a})$, the factorization in $\mathbb{Q}(\sqrt{a})$ and discriminants of each $f_{N,i}$. Using the Lemma 7.1.8 we immediately get that if an odd prime p such that $(p,\Delta(f_{N,i})) = 1$ ramifies in K, then a is a square modulo p. For $p = 2$ and p that are not coprime to every $\Delta(f_{N,i})$ and can ramify (this can be checked in Theorem 7.1.10, which is proved independently) we can explicitly verify that $\left(\frac{a}{p}\right) \neq -1$. ■

Proof of Theorem 7.1.1 (c). For all pairs of N and b, in Table 7.3 we have the factorizations of f_N where some of the factors are linear over $\mathbb{Q}(\sqrt{b})$. Therefore, f_N has a root over each $\mathbb{F}_p$ such that $\sqrt{b}$ is defined modulo p, i.e. such that b is a square modulo p.

If $x_0 \in \mathbb{Z}$ is a root of f_N such that $f_N(x_0) \equiv 0 \pmod{p}$, then $f_N(x_0+kp) \equiv 0 \pmod{p}$, $k = 0, ..., p-1$. If $p > \deg f_N$, we have $f_N(x_0+kp) \not\equiv 0 \pmod{p^2}$ for at least one value of k. Now we know that for $p > \deg f_N$ there exists $a \in \mathbb{Z}$ be such that $f_N(a) \equiv 0 \pmod{p}$ and $f_N(a) \not\equiv 0 \pmod{p^2}$. For smaller values of p, with exception of $p = 2$, one can explicitly check that this claim remains true. Therefore, p ramifies in $\mathbb{Q}(\sqrt{f_N(a)})$.

It remains to show that there are infinitely many quadratic fields such that p ramifies. Let $S = \{u \in \mathbb{Z} : u \equiv a \pmod{p^2}\}$. Obviously $f_N(u) \equiv 0 \pmod{p}$ and $f_N(u) \not\equiv 0 \pmod{p^2}$ for all $u \in S$. Let d_u be the squarefree part of $f_N(u)$; the quadratic point $(u, \sqrt{f_N(u)})$ will be defined over $\mathbb{Q}(\sqrt{d_u})$. After writing $f_N(u) = d_u s_u^2$ for some $s_u \in \mathbb{Z}$, we observe that (u, s_u) is a rational point on the quadratic twists $C_N^{d_u}$ of $X_0(N)$,

$$C_N^{d_u} : d_u y^2 = f_N(x).$$

Since each $C_N^{d_u}$ is of genus ≥ 2, by Faltings' theorem it follows that $C_N^{d_u}(\mathbb{Q})$ is finite and hence $\{d_u : u \in S\}$ is infinite, proving the claim. ■

N	a	factorization of f_N in $\mathbb{Q}(\sqrt{a})$	$\Delta(f_{N,i})$
26	13	$\left((x^3+(-\sqrt{13}-4)x^2+\frac{1}{2}(\sqrt{13}+5)x+\frac{1}{2}(-3\sqrt{13}-11)\right)\times$ $\times\left(x^3+(\sqrt{13}-4)x^2+\frac{1}{2}(-\sqrt{13}+5)x+\frac{1}{2}(3\sqrt{13}-11)\right)$	$2^{20}\cdot 13^3$
28	-7	$\left(x+\frac{1}{2}(-\sqrt{-7}-1)\right)\left(x+\frac{1}{4}(-\sqrt{-7}-3\right)\times$ $\times\left(x+\frac{1}{4}(-\sqrt{-7}-1)\right)\left(x+\frac{1}{4}(\sqrt{-7}-3)\right)\times$ $\times\left(x+\frac{1}{4}(-\sqrt{-7}-1)\right)\left(x+\frac{1}{2}(\sqrt{-7}-1)\right)$	-7 -7 -7
29	29	$\left(x^3+(-\sqrt{29}-2)x^2+\frac{1}{2}(\sqrt{29}+13)x+\frac{1}{2}(-\sqrt{29}-1)\right)\times$ $\times\left(x^3+(\sqrt{29}-2)x^2+\frac{1}{2}(-\sqrt{29}+13)x+\frac{1}{2}(\sqrt{29}-1)\right)$	$2^{12}\cdot 29^5$
30	5	$\left(x-\sqrt{5}+3\right)\left(x+\frac{1}{2}(-\sqrt{5}+3)\right)\times$ $\times\left(x+\frac{1}{2}(\sqrt{5}+3)\right)\left(x+\sqrt{5}+3\right)\times$ $\times\left(x^2+\frac{1}{2}(-\sqrt{5}+5)x-\sqrt{5}+3\right)\left(x^2+\frac{1}{2}(\sqrt{5}+5)x+\sqrt{5}+3\right)$	5 $2^2\cdot 5$ $2^2\cdot 3^2\cdot 5^2$
33	-11	$\left(x+\frac{1}{2}(-\sqrt{-11}-1)\right)\left(x+\frac{1}{2}(\sqrt{-11}-1)\right)\times$ $\times\left(x^3+\frac{1}{2}(-\sqrt{-11}+1)x^2+\frac{1}{2}(\sqrt{-11}+5)x-\sqrt{-11}\right)\times$ $\times\left(x^3+\frac{1}{2}(\sqrt{-11}+1)x^2+\frac{1}{2}(-\sqrt{-11}+5)x+\sqrt{-11}\right)$	-11 $-2^8\cdot 3^6\cdot 11^5$

35	5	$\left(x+\frac{1}{2}(-\sqrt{5}+1)\right)\left(x+\frac{1}{2}(\sqrt{5}+1)\right)\times$ $\times\left(x^3+\frac{1}{2}(-3\sqrt{5}-5)x^2+\frac{1}{2}(\sqrt{5}+5)x-\sqrt{5}-2\right)\times$ $\times\left(x^3+\frac{1}{2}(3\sqrt{5}-5)x^2+\frac{1}{2}(-\sqrt{5}+5)x+\sqrt{5}-2\right)$	5 $2^8\cdot 5^7\cdot 7^2$
39	13	$\left(x^2+\frac{1}{2}(-\sqrt{13}-7)x+1\right)\left(x^2+\frac{1}{2}(-\sqrt{13}+1)x+1\right)\times$ $\times\left(x^2+\frac{1}{2}(\sqrt{13}-7)x+1\right)\left(x^2+\frac{1}{2}(\sqrt{13}+1)x+1\right)$	$-3^3\cdot 13^2$ $-3\cdot 13^2$
40	-1	$\left(x^4-2\sqrt{-1}x^3+2x^2+2\sqrt{-1}x+1\right)\times$ $\times\left(x^4+2\sqrt{-1}x^3+2x^2-2\sqrt{-1}x+1\right)$	$2^{40}\cdot 5^4$
	5	$\left(x^4+(-2\sqrt{5}+4)x^2+1\right)\left(x^4+(2\sqrt{5}+4)x^2+1\right)$	
41	41	$\left(x^4-2x^3+(-\sqrt{41}-6)x^2+(-\sqrt{41}-7)x+\frac{1}{2}(-\sqrt{41}-3)\right)\times$ $\times\left(x^4-2x^3+(\sqrt{41}-6)x^2+(\sqrt{41}-7)x+\frac{1}{2}(\sqrt{41}-3)\right)$	$-2^{16}\cdot 41^6$
48	-1	$\left(x^2+(-\sqrt{-1}-1)x-\sqrt{-1}\right)\left(x^2+(-\sqrt{-1}+1)x+\sqrt{-1}\right)\times$ $\times\left(x^2+(\sqrt{-1}-1)x+\sqrt{-1}\right)\left(x^2+(\sqrt{-1}+1)x-\sqrt{-1}\right)$	$2^8\cdot 3^2$
	3	$\left(x^2+(-\sqrt{3}-1)x+\sqrt{3}+2\right)\left(x^2+(-\sqrt{3}+1)x-\sqrt{3}+2\right)\times$ $\times\left(x^2+(+\sqrt{3}-1)x-\sqrt{3}+2\right)\left(x^2+(\sqrt{3}+1)x+\sqrt{3}+2\right)$	$2^8\cdot 3^2$
50	5	$\left(x^3+(-\sqrt{5}-2)x^2+\frac{1}{2}(-\sqrt{5}+1)x+\frac{1}{2}(-\sqrt{5}-3)\right)\times$ $\times\left(x^3+(\sqrt{5}-2)x^2+\frac{1}{2}(\sqrt{5}+1)x+\frac{1}{2}(\sqrt{5}-3)\right)$	$2^{16}\cdot 5^5$

Table 7.3: Factorizations of f_N in $\mathbb{Q}(\sqrt{\mathbf{a}})$, and the discriminants of $f_{N,i}$ defined in the statement of Lemma 7.1.8.

Remark 7.1.9. After we proved Theorem 7.1.1, we mention two papers [15, 40] that have some overlap with ours and show which of our results can be proved using their methods.

Obvious points on curves $X_0(N)$ are of the form $(x, y\sqrt{d})$, where $x, y \in \mathbb{Q}$. This gives us the point (x, y) on the quadratic twist $X_0^d(N)(\mathbb{Q})$ and hence $X_0^d(N)(\mathbb{Q}_p) \neq \emptyset$. Now the underlined entries in Table 7.2 can be alternatively proved using the results of Ozman [40, Theorem 1.1]. Note that the facts in Table 7.2 which have been marked by * or ** do not follow from [40, Theorem 1.1].

Recall that a $\mathbb{Q}$-curve is an elliptic curve that is isogenous to all its Galois conjugates. The *degree* of a $\mathbb{Q}$-curve over a quadratic field is the degree of a cyclic isogeny to its Galois conjugate. González proves the following statement [15, Proposition 1.1]:

Assume that there exists a quadratic $\mathbb{Q}$-curve of degree d defined over some quadratic field K. Then every divisor $N_1 \mid d$ such that

$$N_1 \equiv 1 \pmod 4 \quad \textit{or} \quad N_1 \textit{ is even and } d/N_1 \equiv 3 \pmod 4$$

is a norm of the field K.

For our values of N, all but finitely many known exceptions of elliptic curves with N-isogenies over quadratic fields are $\mathbb{Q}$-curves, as proved by Bruin and Najman [6]. Note that we do not use the fact that the curves we consider are $\mathbb{Q}$-curves in any essential way; we only use the fact that almost all the quadratic points on the modular curves $X_0(N) : y^2 = f_N(x)$ are of the form $(x_0, \sqrt{f_N(x_0)})$, for $x_0 \in \mathbb{Q}$ (and from this fact Bruin and Najman proved that the corresponding elliptic curves are $\mathbb{Q}$-curves).

After noting that an obvious quadratic point on $X_0(N)$ corresponds to a $\mathbb{Q}$-curve of degree d, where d can be obtained from the tables in [6], and applying González' proposition, we obtain that p is not inert in a quadratic field $K := \mathbb{Q}(\sqrt{D})$ generated by an obvious point on $X_0(N)$, for the following pairs (N, p):

$$(N,p) \in \{(26,13),(29,29),(30,5),(35,5),(41,41),(50,5)\}.$$

In all of the pairs above we have $d = N$, except for $N = 30$, where $d = 15$. ■

Theorem 7.1.10. In Table 7.4 below, we list the primes $p \leq 100$ which are unramified for all quadratic fields generated by quadratic points $X_0(N)$, for

$$N \in \{22,23,26,29,30,31,33,35,39,40,41,46,47,48,50,59,71\}.$$

Proof. The proofs of all the facts listed are easy and all basically the same; take some prime p in the table above. Using the notation as in (7.1.1), we run through all m and n in the appropriate equation modulo p and we get that $n^{2k}d \not\equiv 0 \pmod p$ for some positive integer k, which gives us that $D \not\equiv 0 \pmod p$ and hence p is unramified. ■

N	**unramified primes**
22	3,5,23,31,37,59,67,71,89,97
23	2,3,13,29,31,41,47,71,73
26	3,5,7,11,17,19,31,37,41,43,47,59,67,71,73,83,89,97
28	3,5,13,17,19,31,41,47,59,61,73,83,89,97
29	3,5,11,13,17,19,31,37,41,43,47,53,61,73,79,89,97
30	2,3,7,13,17,23,37,43,47,53,67,73,83,97
31	2,5,7,19,41,59,71,97
33	2,7,13,17,19,29,41,43,61,73,79,83
35	2,3,7,13,17,23,37,43,47,53,67,73,83,97
39	2,5,7,11,13,19,31,37,41,47,59,61,67,71,73,79,83,89,97
40	2,3,5,7,11,13,17,19,23,31,37,41,43,47,53,59,61,67,71,73,79,83,97
41	3,5,7,11,13,17,19,29,37,47,53,61,67,71,73,79,89,97
46	2,3,13,29,31,41,47,71,73
47	2,3,7,17,37,53,59,61,71,79,89,97
48	2,3,5,7,11,17,19,23,29,31,41,43,47,53,59,67,71,79,83,89
50	3,7,11,13,17,19,23,37,41,43,47,53,67,73,83,89,97
59	3,5,7,19,29,41,53,79
71	2,3,5,19,29,37,43,73,79,83,89

Table 7.4: Primes up to 100 that do not ramify in quadratic fields over which $X_0(N)$ has a point.

7.2. SPLITTING OF 2 IN CUBIC FIELDS GENERATED BY CUBIC POINTS OF $X_1(2,14)$

Let us fix the following notation for the remainder of this section. Denote $X := X_1(2,14)$ and $Y := Y_1(2,14)$. Let $\phi : X_1(2,14) \to X_1(14)$ be the forgetful map sending $(E,P,Q,R) \in X$ with P and Q of order 2 and R of order 7 to $(E,P,R) \in X_1(14)$. Let K be a cubic number field over which X has a non-cuspidal point $x = (E,P,Q,R)$ and let $\mathfrak{P}$ be a prime above p. By [5, Theorem 1.2], K is a cyclic cubic field. Denote by $\bar{x}$ the reduction of x mod $\mathfrak{P}$.

In this section we are going to prove that the prime 2 always splits in a cubic field over which X has a non-cuspidal point. Furthermore, we will show the same statement for all primes $p \equiv \pm 1 \pmod 7$ for which E has multiplicative reduction.

The curve X has the following model [5, Proposition 3.7] in $\mathbb{P}^1_{\mathbb{Q}} \times \mathbb{P}^1_{\mathbb{Q}}$:

$$X : f(u,v) = (u^3+u^2-2u-1)v(v+1) + (v^3+v^2-2v-1)u(u+1) = 0. \qquad (7.2.1)$$

The curve X has 18 cusps, 9 of which are defined over $\mathbb{Q}$ and 9 over $\mathbb{Q}(\zeta_7)^+$, forming 3 Galois orbits.

Let τ and ω be automorphisms of X, where the moduli interpretation of τ is that it acts as a permutation of order 3 on the points of order 2 of E and trivially on the point of order 7, and where the moduli interpretation of ω is that it acts trivially on the points of order 2 and as multiplication by 2 on the point of order 7. Let $\alpha := \omega\tau$ and $\beta := \omega\tau^2$.

From [5, Chapter 3] it follows that the only maps of degree 3 from X to $\mathbb{P}^1$ are quotienting out by subgroups generated by α and β (an automorphism of X interchanges these two maps) and that all non-cuspidal cubic points on X are inverse images of $\mathbb{P}^1(\mathbb{Q})$ with respect to these maps. Also, both α and β act without fixed points on the cusps.

As it has already been mentioned, the results of [5] tell us that elliptic curves with $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/14\mathbb{Z}$ torsion over a cubic field are parameterized by $\mathbb{P}^1(\mathbb{Q})$, so one can write every such curve as E_u for some $u \in \mathbb{Q}$. We do not display the model for E_u as it contains huge coefficients, but it can be found in the accompanying Magma code. In [5] it is proved that the curve $E := E_u$ is a base change of an elliptic curve defined over $\mathbb{Q}$.

We have

$$j(u) = \frac{(u^2+u+1)^3(u^6+u^5+2u^4+9u^3+12u^2+5u+1)f_{12}(u)^3}{u^{14}(u+1)^{14}(u^3+u^2-2u-1)^2},$$

where

$$f_{12}(u) = u^{12}+4u^{11}+3u^{10}-4u^9+6u^7-17u^6-30u^5+6u^4+34u^3+25u^2+8u+1,$$

and

$$\Delta(u) = \frac{u^{14}(u+1)^{14}(u^3+u^2-2u-1)^2}{h_{12}(u)^{12}},$$

$$c_4(u) = \frac{g_2(u)g_6(u)g_{12}(u)}{h_{12}(u)^4},$$

where g_i are polynomials in u of degree i, for $i = 2,6,12$, and h_{12} is of degree 12.

Let $\mathrm{res}(f,g)$ denote the resultant of the polynomials f and g. If $v_p(h_{12}(u)) > 0$, then E does not have multiplicative reduction at p, since

$$\mathrm{res}\,(h_{12}(u), g_\Delta(u)) = \mathrm{res}\,(h_{12}(u), g_{c_4}(u)) = 1,$$

where g_Δ is the numerator of $\Delta(u)$ and g_{c_4} is the numerator of $c_4(u)$, and therefore $v_p(j(u)) = 0$. Checking the factors of the discriminant, there are several possibilities for the elliptic curve E to have multiplicative reduction:

- If $v_p(u) =: k > 0$, then using the fact that

  $$\mathrm{res}\left(u, \frac{\Delta(u)}{u^{14}}\right) = \mathrm{res}\,(u, c_4(u)) = 1,$$

  we conclude that reduction mod p will be of type I_{14k}.

- If $v_p(u) =: -k < 0$, with the change of variables $v := \frac{1}{u}$ we get a similar situation as above, with

  $$\mathrm{res}\left(v, \frac{\Delta(v)}{v^{14}}\right) = \mathrm{res}\,(v, c_4(v)) = 1,$$

  so the reduction mod p will be of type I_{14k}.

- If $v_p(u) = 0$ and $v_p(u+1) := k > 0$, then using the fact that

  $$\mathrm{res}\left(u+1, \frac{\Delta(u)}{(u+1)^{14}}\right) = \mathrm{res}\,(u+1, c_4(u)) = 1,$$

  we conclude that the reduction mod p is of type I_{14k}.

- The only other possibility for multiplicative reduction is $v_p(u^3+u^2-2u-1) =: k > 0$. Note that a root α of $f(u) := u^3+u^2-2u-1$ generates the ring of integers $\mathbb{Z}[\alpha]$ of $\mathbb{Q}(\zeta_7)^+$. The fact that $p|f(u)$ implies that $f(u)$ has a root in $\mathbb{F}_p$ and hence p splits in $\mathbb{Q}(\zeta_7)^+$, implying $p \equiv \pm 1 \pmod 7$ or $p = 7$. Since

$$\operatorname{res}\left(u^3+u^2-2u-1, \frac{\Delta(u)}{(u^3+u^2-2u-1)^2}\right) = 7^{30}$$

and

$$\operatorname{res}\Big(u^3+u^2-2u-1, c_4(u)\Big) = 7^{12},$$

it follows that there can be cancellation with the numerator only in the case $p = 7$.

- Suppose $p = 7$, $v_7(u) = 0$ and $v_7(u^3+u^2-2u-1) = k > 0$. An easy computation shows that $u \equiv 2 \pmod 7$ and $k = 1$, and that the numerator of the $j-$invariant will be divisible by a higher power of 7 than u^3+u^2-2u-1, which show that the reduction will not be multiplicative.

In the discussion above we have proved the following two results:

Proposition 7.2.1. Suppose E has multiplicative reduction at a rational prime p. Then either the reduction is of type I_{14k} for some k, or $p \equiv \pm 1 \pmod 7$, in which case the reduction is I_{2k}.

Remark 7.2.2. As it has been mentioned, E is a base change of an elliptic curve over $\mathbb{Q}$, so in Proposition 7.2.1 and in the remainder of the section, when we consider the reduction of E (and also X and $X_1(14)$) modulo a rational prime, we will consider E to be defined over $\mathbb{Q}$ and when we consider it modulo a prime of K we consider its base change to K.

Proposition 7.2.3. The curve E has multiplicative reduction of type I_{14k} at 2.

Proof. This follows from the observation that $v_2(u) \neq 0$ or both $v_2(u) = 0$ and $v_2(u+1) > 0$, from which it follows, by what we have already proved, that in both cases the reduction type of E_u at 2 is I_{14k}. ■

We now prove 3 useful lemmas.

Lemma 7.2.4. Let $x \in Y(K)$ and let $\mathfrak{P}$ be a prime of K over 2. Then x modulo $\mathfrak{P}$ is defined over $\mathbb{F}_2$.

Proof. As mentioned above, the results of [5] imply that a non-cuspidal cubic point on $x \in X$ given by the equation $f(u,v) = 0$ in (7.2.1) satisfies either $u \in \mathbb{P}^1(\mathbb{Q})$ or $v \in \mathbb{P}^1(\mathbb{Q})$. Over $\mathbb{F}_2$, the polynomial f factors as

$$f(u,v) = (u+v)(uv+u+1)(uv+v+1),$$

which implies that if one of u or v is $\in \mathbb{P}^1(\mathbb{F}_2)$, then so is the other. This implies that the reduction of x modulo $\mathfrak{P}$ is defined over $\mathbb{F}_2$. ■

Lemma 7.2.5. Let $F = \mathbb{Q}(\zeta_7)^+$, let C be a cusp of X whose field of definition is F and let q be a rational prime. Then the field of definition of the reduction of C in $\overline{\mathbb{F}}_q$ is $\mathbb{F}_{q^3}$ if $q \not\equiv \pm 1 \pmod 7$ and $\mathbb{F}_q$ if $q \equiv \pm 1 \pmod 7$.

Proof. We have $[k(C) : \mathbb{F}_q] = [\mathbb{Q}_q(\zeta_7 + \zeta_7^{-1}) : \mathbb{Q}_q]$ from which the claim follows. ■

Lemma 7.2.6. Let $q \equiv \pm 1 \pmod 7$ be a rational prime such that E has multiplicative reduction over q and let $\mathfrak{P}$ be a prime of K over q. Then the reduction of $x \in X$ modulo $\mathfrak{P}$ corresponding to the curve E is $\mathbb{F}_q$.

Proof. Since x modulo $\mathfrak{P}$ is a cusp, the statement follows from Lemma 7.2.5. ■

Proposition 7.2.7. Let $q = 2$ or $q \equiv \pm 1 \pmod 7$ be a rational prime such that E has multiplicative reduction in q. Then q splits in K.

Proof. Let σ be a generator of $\mathrm{Gal}(K/\mathbb{Q})$ (recall that K is Galois over $\mathbb{Q}$) and suppose q is inert in K. As the degree 3 map $X \to \mathbb{P}^1$ is quotienting by α, it follows that

$$\left\{x, x^\sigma, x^{\sigma^2}\right\} = \left\{x, \alpha(x), \alpha^2(x)\right\},$$

so we can suppose without loss of generality that $x^\sigma = \alpha(x)$ and $x^{\sigma^2} = \alpha^2(x)$. Let $\bar{x} = \overline{C_0}$, for some cusp $C_0 \in X$. It follows that $\overline{\alpha(x)} = \overline{\alpha(C_0)}$ and $\overline{\alpha^2(x)} = \overline{\alpha^2(C_0)}$. Denote by $C_1 := \alpha(C_0)$ and by $C_2 := \alpha^2(C_0)$; all C_i are distinct as α acts without fixed points on the cusps. By Lemma 7.2.4 and Lemma 7.2.6, all $\overline{C}_i$ are defined over $\mathbb{F}_q$.

Denote by $K_i := \phi(C_i)$ and by $y = \phi(x) \in Y_1(14)$. Descending everything to $X_1(14)$, we have $\bar{y} = \overline{K_0}$, $\overline{y^\sigma} = \overline{K_1}$, $\overline{y^{\sigma^2}} = \overline{K_2}$. By Lemma 7.2.4 and Lemma 7.2.6, all $\overline{C_i}$ and hence all $\overline{K}_i$ are defined over $\mathbb{F}_q$.

Using the same arguments as in [37, Proposition 3.1] we get that $\overline{K_0} = \overline{K_1} = \overline{K_2}$. Reduction modulo q is injective on the torsion of $X_1(14)$ by [21, Appendix] for $q > 2$ and by explicitly checking injectivity for $q = 2$. Now from the fact that the rank of $X_1(14)(\mathbb{Q}(\zeta_7)^+)$ is 0, we conclude $K_0 = K_1 = K_2$. This is impossible since C_0, C_1, C_2 are distinct and ϕ is a degree 2 map. ■

8. TAMAGAWA NUMBERS OF ELLIPTIC CURVES WITH PRESCRIBED TORSION SUBGROUP OR ISOGENY

In this chapter, as the title suggests, we will be studying Tamagawa numbers (introduced in Section 4.2) of elliptic curves with a certain torsion subgroup or isogeny. We will mainly be following the author's paper [46]. Before proceeding, we will introduce the notation, which will not differ from the one in Chapter 4.

Let E be an elliptic curve over a number field K and denote by Σ the set of all finite primes of K. For each $v \in \Sigma$, K_v will denote the completion of K at v and $k_v = \mathcal{O}_{K_v}/(\pi)$ the residue field of v, where $\mathcal{O}_{K_v}$ is the ring of integers of K_v and π is a uniformizer of $\mathcal{O}_{K_v}$.

The subgroup $E_0(K_v)$ of $E(K_v)$ consists of all the points that reduce modulo π to a non-singular point of $E(k_v)$ (see Definition 4.1.1). It is known that this group has finite index in $E(K_v)$ so in Definition 4.2.3 we defined the Tamagawa number c_v of E at v to be that index, i.e.

$$c_v := [E(K_v) : E_0(K_v)].$$

Consequently, we defined the Tamagawa number of E over K to be the product $c_{E/K} := \prod_{v\in\Sigma} c_v$. We will write c_E instead of $c_{E/K}$ wherever it does not cause confusion.

It makes sense to study how the value c_E depends on $E(K)_{tors}$, since $c_E/\#E(K)_{tors}$ appears as a factor in the leading term of the $L-$function of E/K in the conjecture of Birch and Swinnerton-Dyer (see, for example, [16, Conj. F.4.1.6]).

Some results on Tamagawa numbers of elliptic curves with a specific torsion subgroup

and on the quotient $c_E/\#E(K)_{tors}$ are given by Lorenzini in [30, Chapter 2] for elliptic curves over the rationals and over quadratic extensions. Krumm [27, Chapter 5] proved some further results on Tamagawa numbers of elliptic curves with prescribed torsion over number fields of degree up to 5. He also conjectured that $ord_{13}(c_E)$ is even for all elliptic curves defined over quadratic fields with a point of order 13 and the same conjecture was later proved by Najman in [37].

In this chapter we explore this problem further and prove in Section 8.1 that the Tamagawa numbers of elliptic curves defined over cubic fields with torsion subgroup $\mathbb{Z}/2\mathbb{Z}\oplus\mathbb{Z}/14\mathbb{Z}$ are always divisible by 14^2, except in the case of the curve 1922c1 in [11], where $c_E = c_2 = 14$. For each such curve we prove that at $p = 2$ the reduction is split multiplicative, so $c_2 = 14k$. Bruin and Najman [5] proved that elliptic curves with torsion $\mathbb{Z}/2\mathbb{Z}\oplus\mathbb{Z}/14\mathbb{Z}$ over cubic fields are actually a base change of elliptic curves over $\mathbb{Q}$. It is also true that those curves defined over $\mathbb{Q}$ have multiplicative reduction of type I_{14t} at one more prime, distinct from 2, at which the reduction is also split multiplicative of type I_{14t}.

The question which naturally appears next is how does the Tamagawa number of an elliptic curve depend on the isogenies of that elliptic curve. In Section 8.2 we give a series of propositions which gives us the first results about Tamagawa numbers of elliptic curves with prescribed isogeny. For elliptic curves defined over $\mathbb{Q}$, we were able to prove that if an elliptic curve has an $18-$isogeny, then its Tamagawa number is always divisible by 4, and if it has an $n-$isogeny, for $n \in \{6,8,10,12,14,16,17,18,19,37,43,67,163\}$, then it has to be divisible by 2, with finitely many exceptions for some of these results, all of which we list and give their Tamagawa numbers.

Let E be an elliptic curve defined over K_v, given by a Weierstrass equation

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

with the discriminant Δ, invariants c_4 and c_6, and $j-$invariant $j_E = \frac{c_4^3}{\Delta}$, as defined in Definition 1.0.3. It will be important for us to distinguish between different types of reductions at finite primes, especially to know when the reduction is multiplicative. For that, we will often use the following well known result.

Proposition 8.0.1. ([43, Proposition VII.5.1.b]). With the above notation, the curve E in

its minimal model has multiplicative reduction at v of type I_k if and only if $k := ord_v(\Delta) > 0$ and $ord_v(c_4) = 0$.

As most Tamagawa numbers that we will consider in this paper are coming from primes of multiplicative reduction, it will be important to also distinguish between split and non-split multiplicative reductions and their Tamagawa numbers. One way to do that is by using the algorithm of Tate [44, Sections 7,8] which works in any characteristic of k_v. Going through the algorithm with a specific elliptic curve and a prime v, we get the reduction type at v, its Kodaira symbol and the Tamagawa number c_v. It turns out that in the case of split multiplicative reduction I_k we have $c_v = k$ and in the case of non-split multiplicative reduction I_k we have $c_v = 1$ or $c_v = 2$, depending on the parity of k, as indicated in Table 8.1, where we can find all the Tamagawa numbers associated to different reduction types. For distinguishing reduction types in $char(k_v) \neq 2,3$ one can also use the tables in [43, Table 15.1] or [44, Section 6].

reduction type at v	Kodaira symbol, $k \geq 1$	Tamagawa number at v
good	I_0	1
split multiplicative	I_k	k
non-split multiplicative	I_{2k}	2
non-split multiplicative	I_{2k-1}	1
additive	II, II^*	1
additive	III, III^*	2
additive	IV, IV^*	1,3
additive	I_0^*	$1,2,4$
potentially multiplicative	I_{2k}^*	$2,4$
potentially multiplicative	I_{2k-1}^*	$2,4$

Table 8.1: types of reduction and their Tamagawa numbers

The computations in this chapter were executed in the computer algebra system Magma [2]. The code can be found at https://web.math.pmf.unizg.hr/~atrbovi/magma/

magma3.htm or in Appendix C. Many of the proofs in this paper omit the information used in them, such as polynomials of very high degree or with large coefficients, but those can be computed with the given code. For the untrusting reader, we recommend that they go through the proofs and the code simultaneously.

All of the specific curves will be mentioned using their Cremona labels, with a clickable link to the corresponding webpage in [28].

8.1. Tamagawa numbers of elliptic curves with torsion subgroup $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/14\mathbb{Z}$

Filip Najman and the author have examined the reduction types of primes with multiplicative reduction of the elliptic curves with torsion $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/14\mathbb{Z}$ over a cubic field in Proposition 7.2.1. We will examine those primes further, as we want to be able to say more about their Tamagawa numbers. It was proved in Proposition 7.2.3 that the prime 2 always has multiplicative reduction of type I_{14k} in cubic extensions over which $X_1(2,14)$ has a non-cuspidal point. In this section we are going to prove that the mentioned multiplicative reduction always has to be split multiplicative, giving the Tamagawa number $c_2 = 14k$, as shown in Table 8.1. We are also going to prove that there always exists one more prime p, with the exception of the curve 1922c1, in which we have split multiplicative reduction of type I_{14t} and $c_p = 14t$, which means that the Tamagawa number of the elliptic curve contains the factor 14^2.

Bruin and Najman [5] showed that every elliptic curve with torsion $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/14\mathbb{Z}$ over a cubic field is a base change of an elliptic curve defined over $\mathbb{Q}$. Those elliptic curves are also parameterized with $\mathbb{P}^1(\mathbb{Q})$, so we can write each such curve as E_u, for some $u \in \mathbb{Q}$. They also provided a model, which was used for obtaining the results of Chapter 7.2. We used a different model here, specifically, the one given by Jeon and Schweizer in [17, §2.4], since the one in [39] was dependant on 2 parameters. It did not impose a problem there, since we did not have the need to work with the coefficients of

the curve. Even though Jeon and Schweizer do not state that their family consists of all elliptic curves over cubic fields with torsion $\mathbb{Z}/2\mathbb{Z}\oplus\mathbb{Z}/14\mathbb{Z}$, it turns out that it is the case and the reasoning behind it can be found in the accompanying Magma code. Briefly, we compute the isomorphism between different fields of definition of elliptic curves with torsion $\mathbb{Z}/2\mathbb{Z}\oplus\mathbb{Z}/14\mathbb{Z}$, those are F and L given in [5] and [17, §2.4], respectively. With that isomorphism we map every curve from the family in [5] and we see that it is isomorphic to one of the curves from the family in [17, §2.4]. Since [5] gives us all of the elliptic curves with needed properties, we see that it suffices to only look at the family from [17, §2.4].

Jeon and Schweizer provided two models for E_u, one of which is

$$y^2+xy=x^3+A_2(u)x^2+A_4(u)x+A_6(u),$$

and its short Weierstrass model

$$y^2=x^3+A(u)x+B(u),$$

where we omit $A_2(u),A_4(u),A_6(u),A(u),B(u)$, since they are very large, but they can be found in the accompanying Magma code or in [17, §2.4]. We will be working with the long Weierstrass model when considering the reduction at the prime 2, but generally we will be using the short Weierstrass model, since it is easier to work with.

In Proposition 8.0.1 we mentioned a way of confirming whether the curve has multiplicative reduction at a finite prime. As already stated, it will be very important to distinguish between split and non-split multiplicative reduction, since the associated Tamagawa numbers are different (see Table 8.1). The following lemma will be useful in differentiating between those, and it is taken directly from a step in Tate's algorithm.

Lemma 8.1.1. ([44, §7. Case 2)]). Let E be an elliptic curve and let p be a prime of multiplicative reduction of type I_t for E. Let $ord_p(a_i)>0$, for $i=3,4,6$, and $ord_p(b_2)=0$. If $T^2+a_1T-a_2$ splits over k_p, then E has split multiplicative reduction at p and $c_p=t$.

As a part of the proof of the following proposition we will show that the reduction at the prime 2 is multiplicative of type I_{14k}, which is already proved in Proposition 7.2.3. We had to include it here again and could not continue from there because of the already mentioned differences in the models we used.

Proposition 8.1.2. Let E be an elliptic curve defined over a cubic field with torsion subgroup $\mathbb{Z}/2\mathbb{Z}\oplus\mathbb{Z}/14\mathbb{Z}$. Then the reduction at 2 is split multiplicative of type I_{14k} and $c_2 = 14k$.

Proof. From the long Weierstrass model of E_u from [17, §2.4] we get the associated discriminant and the c_4-invariant:

$$\Delta(u) = \frac{2^{14}(u-1)^{14}(u+1)^{14}f_3(u)^2}{f_2(u)^{12}f_6(u)^4}, \quad c_4(u) = \frac{f_{12}(u)}{f_2(u)^3 f_6(u)},$$

where $f_i(u)$ are monic polynomials of degree i, which can be computed with the accompanying Magma code. We will go through all of the possibilities of the prime 2 dividing u and see that the reduction at 2 in all of those cases is split multiplicative and $14 \mid c_2$.

- If $ord_2(u) > 0$, then it is obvious from the polynomials above that $ord_2\left(\frac{\Delta(u)}{2^{14}}\right) = ord_2(c_4(u)) = 0$ and from Proposition 8.0.1 we conclude that the reduction at 2 is multiplicative of type I_{14}. We compute $a_1 = 1$ and $ord_2(a_2) > 0$ and since our model satisfies the conditions of Lemma 8.1.1, we get that $c_2 = 14$.

- If $ord_2(u) < 0$, then we make the substitution $u \mapsto \frac{1}{m}$ so $ord_2(m) > 0$, and in the new model we get

  $$\Delta(m) = \frac{2^{14}(m-1)^{14}m^{14}(m+1)^{14}g_3(m)^2}{3^{12}31^4 g_2(m)^{12}g_6(m)^4}, \quad c_4(m) = \frac{37g_{12}(m)}{3^3 31 g_2(m)^3 g_6(m)},$$

  where $g_i(m)$ are monic polynomials of degree i, which can be computed with the accompanying Magma code. Since $ord_2(m) > 0$, it is obvious from the polynomials that $ord_2\left(\frac{\Delta(m)}{2^{14}m^{14}}\right) = ord_2(c_4(m)) = 0$ and as in the previous case, using Proposition 8.0.1 and Lemma 8.1.1 we get that the reduction at 2 is split multiplicative of type $I_{14(k+1)}$ and $c_2 = 14(k+1)$.

- If $ord_2(u) = 0$, then $ord_2(u-1) > 0$. After the substitution $u - 1 \mapsto m$ we have $k := ord_2(m) > 0$ and

  $$\Delta(m) = \frac{2^{14}m^{14}(m+2)^{14}h_3(m)^8}{h_2(m)^{12}h_6(m)^4}, \quad c_4(m) = \frac{h_{12}(m)}{h_2(m)^3 h_6(m)},$$

  where $h_i(u)$ are monic polynomials of degree i, which can be computed with the accompanying Magma code.

We can divide both numerator and the denominator of $\Delta(m)$ with 2^{48} and we get $ord_2(\Delta(m)) = 14(k-1)$ and if we divide the numerator and the denominator of $c_4(m)$ with 2^{24} and we get $ord_2(c_4(m)) = 0$. So if $k > 1$, by Proposition 8.0.1 we have that the reduction at 2 is multiplicative of type $I_{14(k-1)}$. We compute $a_1 = 1$ and $ord_2(a_2) > 0$ (after dividing both numerator and the denominator with 2^{12}) and since our model satisfies the conditions of Lemma 8.1.1, we get that $c_2 = 14(k-1)$.

Obviously we have to look at the case $k = 1$ separately. This means that $u = 2n+1$, where $ord_2(n) = 0$. After the substitution $u \mapsto 2n+1$ we have

$$\Delta(n) = \frac{n^{14}(n+1)^{14}p_3(n)^2}{p_2(n)^{12}p_6(n)^4}, \quad c_4(n) = \frac{p_{12}(n)}{p_2(n)^3 p_6(n)},$$

where $p_i(n)$ are monic polynomials of degree i, which can be computed with the accompanying Magma code. Since $ord_2(n) = 0$, we have $t := ord_2(n+1) > 0$ and $ord_2(p_i(n)) = 0$, for each i, so $ord_2(\Delta(n)) = 14t$ and $ord_2(c_4(n)) = 0$. By Proposition 8.0.1 we see that the reduction at 2 is multiplicative of type I_{14t} and similarly as in previous cases, Lemma 8.1.1 gives that the reduction is split multiplicative with $c_2 = 14t$.

■

In the following proposition we will deal with primes distinct from 2, for which we have a simpler way of determining split multiplicative reduction than going through Tate's algorithm as we did in the previous proposition.

Lemma 8.1.3. ([9, Lemma 2.2]). Let $p \neq 2$ and let E be an elliptic curve defined over $\mathbb{Q}_p$ with multiplicative reduction at p. The reduction is split multiplicative if and only if $-c_6$ is a square in $\mathbb{F}_p^\times$.

Proposition 8.1.4. Let E be an elliptic curve defined over a cubic field with torsion subgroup $\mathbb{Z}/2\mathbb{Z}\oplus\mathbb{Z}/14\mathbb{Z}$. Then there exist at least 2 rational primes with split multiplicative reduction of type I_{14k}, one of which is always the prime 2, so $14^2 \mid c_E$, except for the curve 1922*c*1, where $c_E = c_2 = 14$.

Proof. In Proposition 8.1.2 we have already seen that the reduction at 2 is split multiplicative of type I_{14k} and therefore $c_2 = 14k$. It remains to prove that there exists one more prime with the same property for each of those curves.

From the short Weierstrass model of E_u from [17, §2.4] we get the associated discriminant and the c_4-invariant:

$$\Delta(u) = 2^{14}(u-1)^{14}(u+1)^{14}f_3(u)^2f_6(u)^8,$$
$$c_4(u) = f_2(u)f_6(u)^3f_{12}(u),$$

where $f_i(u)$ are polynomials of degree i, which can be computed with the accompanying Magma code.

- Assume that there exists a prime p such that $k := ord_p(u-1) > 0$. Let $res(f,g)$ denote the resultant of the polynomials f and g. We compute

$$res\left(u-1, \frac{\Delta(u)}{(u-1)^{14}}\right) = 2^{82},$$
$$res\,(u-1, c_4(u)) = 2^{32}.$$

  For $p \neq 2$ this means that $p^{14k} \mid \Delta(u)$ and $p \nmid c_4(u)$ and from Proposition 8.0.1 we find that the reduction of E at p is multiplicative of type I_{14k}. We want to see that $c_p = 14k$, i.e. that the reduction at p is split multiplicative. According to Proposition 8.1.3, it will suffice to check the value of $-c_6$ modulo p. Having in mind that $u \equiv 1 \pmod{p}$, we get that $-c_6 \equiv 2^{48} \pmod{p}$, which is a square mod p.

- Assume now that there exists a prime p such that $k := ord_p(u-1) < 0$. We put $m := \frac{1}{u-1}$ so $ord_p(m) = k > 0$ and we get an elliptic curve with

$$\Delta(m) = \frac{1}{2^{14}}m^{14}(m+1/2)^{14}g_3(m)^2g_6(m)^8,$$
$$c_4(m) = g_2(m)g_6(m)^3g_{12}(m),$$

  where $g_i(m)$ are polynomials of degree i, which can be computed with the accompanying Magma code.

$$res\left(m, \frac{\Delta(m)}{m^{14}}\right) = 2^{-82},$$
$$res\,(m, c_4(m)) = 2^{-32}.$$

  For $p \neq 2$ this means that $p^{14k} \mid \Delta(m)$ and $p \nmid c_4(m)$ and from Proposition 8.0.1 we find that the reduction of E at p is multiplicative of type I_{14k}. Having in mind that

$m \equiv 0 \pmod{p}$, we get that $-c_6 \equiv 2^{-48} \pmod{p}$, which is a square mod p, so by Lemma 8.1.3 we have $c_p = 14k$.

So far we have proved that if we have a prime $p \neq 2$ and $k := ord_p(u-1) \neq 0$, then we have split multiplicative reduction at p with $c_p = 14|k|$. We have several possibilities when $ord_p(u-1) = 0$ and those are $u-1 = 0$ or $u-1 = \pm 2^k$, $k \in \mathbb{Z}$.
When $u-1 = \pm 2^k$, $k \neq 0,1$, then $ord_p(u+1) > 0$, for some prime $p \neq 2$. In the cases $u-1 = \pm 2^k$, $k = 0,1$, or $u-1 = 0$ we get that $u \in \{0, \pm 1, 3\}$. For $u = \pm 1$ we get a singular curve and for $u \in \{0,3\}$ we get the same curve, 1922c1, with $c_E = c_2 = 14$.
Therefore, if we have a curve distinct from 1922c1, it certainly has a prime p such that $ord_p(u-1) \neq 0$ or $ord_p(u+1) > 0$. It remains to see what happens in the case $ord_p(u+1) > 0$.

- Assume that there exists a prime p such that $k := ord_p(u+1) > 0$. We compute

$$res\left(u+1, \frac{\Delta(u)}{(u+1)^{14}}\right) = 2^{82},$$

$$res\,(u+1, c_4(u)) = 2^{32}.$$

For $p \neq 2$ this means that $p^{14k} \mid \Delta(u)$ and $p \nmid c_4(u)$ and from Proposition 8.0.1 we find that the reduction of E at p is multiplicative of type I_{14k}. Having in mind that $u \equiv -1 \pmod{p}$, we get that $-c_6 \equiv 2^{48} \pmod{p}$, which is a square mod p, so by Lemma 8.1.3 we have $c_p = 14k$.

■

8.2. TAMAGAWA NUMBERS OF ELLIPTIC CURVES WITH PRESCRIBED ISOGENY

In [31, Table 3] we can find the $j-$invariants of elliptic curves parameterized by points on modular curves $X_0(n)$ defined over $\mathbb{Q}$, for $X_0(n)$ of genus 0, and in [31, Table 4] there are $j-$invariants of elliptic curves parameterized by points on modular curves $X_0(n)$ defined over $\mathbb{Q}$, with genus of $X_0(n)$ larger than 0. In this section we will examine the properties of Tamagawa numbers of elliptic curves defined over $\mathbb{Q}$ with an $n-$isogeny, i.e. the properties of Tamagawa numbers of elliptic curves obtained from the mentioned $j-$invariants.

In Section 8.1 we worked with a specific model for the curve $X_1(2,14)$. However, the points on $X_0(n)$ give us $j-$invariants of curves with an $n-$isogeny, which give us elliptic curves up to a twist, so now, as opposed to the situation in Section 8.1, we also have to take into consideration the twists of the curves we get from those $j-$invariants. Therefore, we will be interested in how the reduction types at primes $p \in \mathbb{Q}$ change under the twisting of the curve.

Let E be an elliptic curve, which will always be defined over $\mathbb{Q}$ in this section. Denote by E^d its quadratic twist by d, where d is a squarefree integer. When $p \neq 2$, the reduction type change is quite straightforward, and is presented in Table 8.2. In essence, if $p \nmid d$, the reduction type does not change, and when $p \mid d$, reduction types change as indicated in the third column.

reduction type of E at p	reduction type of E^d at $p \nmid d$	reduction type of E^d at $p \mid d$
I_0	I_0	I_0^*
I_m	I_m	I_m^*
II	II	IV^*
III	III	III^*
IV	IV	II^*
I_0^*	I_0^*	I_0
I_m^*	I_m^*	I_m
IV^*	IV^*	II
III^*	III^*	III
II^*	II^*	IV

Table 8.2: change of reduction types at $p \neq 2$ under twisting [8, Prop.1]

When $p = 2$, the situation gets more complicated. As most of the relevant Tamagawa numbers we will have in the following proofs come from primes of multiplicative reduction, we give a lemma that will be especially useful for dealing with quadratic twists of a large family of elliptic curves with multiplicative reduction at $p = 2$.

Lemma 8.2.1. ([13, Thm.A.5], [29, Thm.2.8]). Let E be an elliptic curve with multiplicative reduction of type I_n at $p = 2$. Denote by E^d the twist of E by d, where d is a squarefree integer.

(a) If $d \equiv 2,3 \pmod 4$, then the reduction of E^d at p is of type I_n^*.

(b) If $d \equiv 1 \pmod 4$, then the reduction of E^d at p is of type I_n.

For other types of reduction, some results can also be found in [8, Section 2]. Since we will deal here with only finitely many explicitly known elliptic curves with non-multiplicative reduction at $p = 2$, for those curves we can simply check all of the possibilities for reduction type at $p = 2$ of quadratic twists, since $\mathbb{Q}_2^\times / \left(\mathbb{Q}_2^\times\right)^2 = \langle -1, 2, 5 \rangle$.

Proposition 8.2.2. Let E be an elliptic curve over $\mathbb{Q}$ with an $18-$isogeny. Then $4|c_E$, except for the curves $14a3, 14a4, 14a5, 14a6$, where $c_E = 2$.

Proof. From [31, Table 3] we take the parameterization of the $j-$invariants of the curves that are non-cuspidal points on $X_0(18)$,

$$j(h) = \frac{(h^3-2)^3(h^9-6h^6-12h^3-8)^3}{h^9(h^3-8)(h^3+1)^2},\ h \in \mathbb{Q}.$$

From it we can acquire the discriminant and the c_4-invariant of the minimal model up to a twist,

$$\Delta(h) = (h-2)h^9(h+1)^2(h^2-h+1)^2(h^2+2h+4)f_3(h)^6f_6(h)^6f_9(h)^6f_{12}(h)^6,$$

$$c_4(h) = f_3(h)^3f_6(h)^2f_9(h)^3f_{12}(h)^2,$$

where $f_i(h)$ are polynomials of degree i, which can be computed with the accompanying Magma code.

Assume that there exists a prime p such that $k := ord_p(h+1) > 0$. We compute

$$res\left(h+1, \frac{\Delta(h)}{(h+1)^2}\right) = 3^{34},$$

$$res\,(h+1, c_4(h)) = 3^{12}.$$

If $p \neq 3$, this means that $p^{2k} \mid \Delta(h)$ and $p \nmid c_4(h)$, so from Proposition 8.0.1 we find that the reduction of E at p is multiplicative of type I_{2k}, and therefore c_p is even (see Table 8.1). If there exists a second prime p' distinct from p and 3 with $k' := ord_{p'}(h+1) > 0$, then we have another prime with multiplicative reduction of type $I_{2k'}$ and therefore with even $c_{p'}$.

Assume now that there exists a prime p such that $k := ord_p(h+1) < 0$. We put $m := \frac{1}{h+1}$ and after the substitution $x \mapsto x \cdot 3^{-6}, y \mapsto y \cdot 3^{-9}$ we get an elliptic curve with

$$\Delta(m) = (m-1)^9(3m-1)m^{18}(3m^2-3m+1)^2(3m^2+1)g_3(h)^6g_6(h)^6g_9(h)^6g_{12}(h)^6,$$

up to a twist, and

$$c_4(m) = g_3(h)^3g_6(h)^2g_9(h)^3g_{12}(h)^2,$$

up to a twist, where $g_i(h)$ are polynomials of degree i, which can be computed with the accompanying Magma code. We compute

$$res\left(m, \frac{\Delta(m)}{m^{18}}\right) = 1,$$

$$res(m, c_4(m)) = 1.$$

We see from Proposition 8.0.1 that the reduction at p is multiplicative of type I_{18k}, with even c_p (see Table 8.1). If we have another prime $p' \neq p$ with $k' := ord_{p'}(h+1) < 0$, then the reduction at p' is also multiplicative of type $I_{18k'}$ with even $c_{p'}$.

Assume now that there exists only one prime p such that $k := ord_p(h+1) \neq 0$. That means that either $h+1 \in \mathbb{Z}$ or $m = \frac{1}{h+1} \in \mathbb{Z}$. We consider the following cases:

(1) If $h+1 \in \mathbb{Z}$ and $h+1 = \pm p^k, p \neq 3$, we have $ord_p(h^2-h+1) = 0$, since $res(h+1, h^2-h+1) = 3$, where h^2-h+1 is one of the factors in the discriminant. Then there exists $p' \neq p, 3$ such that $ord_{p'}(h^2-h+1) > 0$. Otherwise, we have $h^2-h+1 \in \{\pm 1, \pm 3\}$, i.e. $h \in \{0, \pm 1, 2\}$. For $h = 1$ we get a twist of the curve 14a4 which has $c_E = 2$, while for $h = 0, -1, 2$ we do not get an elliptic curve (look at the $j-$invariant).

(2) If $h+1 \in \mathbb{Z}$ and $h+1 = \pm 3^k$, for $k = 0$ we have $h+1 = \pm 1$, i.e. $h \in \{0, -2\}$. We already know that h cannot be 0, but for $h = -2$ we get a twist of the curve 14a6, for which we have $c_E = 2$. When $k = 1$ we have $h+1 = \pm 3$, i.e. $h \in \{-4, 2\}$. For $h = -4$ we get a twist of 14a5, with $c_E = 2$, and $h = 2$ cannot happen. Assume now that $h+1 = \pm 3^k, k > 1$. Counting the multiplicities of 3 in $\Delta(h)$ and $c_4(h)$ we get that the factor 3^{2-2k} appears in the $j-$invariant. Furthermore, if we write $\pm 3^k - 1$ instead of h in the equation for E and make the substitution $x \mapsto x \cdot 3^6, y \mapsto y \cdot 3^9$, we get a model where $ord_3(c_4) = 0$, and it follows from Proposition 8.0.1 that for $k > 1$ we have multiplicative reduction I_{2k-2} in 3, with c_3 being even (see Table 8.1). Note that in any case we also have a prime $p \neq 3$ dividing h^2-h+1 in $\Delta(h)$ with multiplicative reduction I_{2n}, which makes c_E divisible by 4.

(3) If $m \in \mathbb{Z}$, then $m = \pm p^k$, for some prime p, and clearly $ord_p(3m^2-3m+1) = 0$, since $res(m, 3m^2-3m+1) = 1$. Then there exists $p' \neq p$ such that $ord_{p'}(3m^2-3m+1) > 0$. Otherwise, we have $3m^2-3m+1 \in \{\pm 1\}$, i.e. $m \in \{0, 1\}$ which only makes sense for $h = 0$ but, as we noted earlier, h cannot be 0.

The only thing left to consider is when we have only 2 primes with $ord_p(h+1) \neq 0$, one of which is 3 and divides the numerator; in other words the cases $h+1 = \pm 3^k p^l$

and $h+1=\pm\frac{3^k}{p^l}, p\neq 3, k,l>0$. From the reasoning in (2) above, it is clear that if $k>1$, we have multiplicative reduction in 3 and from the part of the proof where we had $ord_p(h+1)<0$ we see that the reduction is multiplicative in p as well, which gives us c_E that is divisible by 4. For $k=1$, we have $h+1=\pm 3p^l$ or $h+1=\pm\frac{3}{p^l}$.

- If $h+1=\pm 3p^l$, we have another prime $p'\neq p,3$ dividing h^2-h+1 in the discriminant (similarly as in (1)) with multiplicative reduction.
- If $h+1=\frac{1}{m}=\pm\frac{3}{p^l}$, we also have another prime $p'\neq p$ dividing the numerator of $3m^2-3m+1$ in the discriminant (as in (3)) with multiplicative reduction, except possibly when $3m^2-3m+1=\frac{1}{a^n}, a\in\mathbb{Z}, n>0$ (this situation couldn't have happened in (3), because we had $m\in\mathbb{Z}$). By putting $\pm\frac{p^l}{3}$ instead of m, we get

$$\pm\frac{p^{2l}}{3}\mp p^l+1=\frac{1}{a^n},$$

which only has solutions for $a=3, n=1, p=2, l=1$, i.e. if $h\in\left\{-\frac{5}{2},\frac{1}{2}\right\}$. For $h=\frac{1}{2}$ we get a twist of the elliptic curve 14a3, with $c_E=2$, and for $h=-\frac{5}{2}$ we get a curve that already has 2 primes of reduction type I_{2k}, namely 2 and 13.

To conclude the proof of this proposition, it remains to see how these reduction types and Tamagawa numbers would change under twisting of the curves. All even Tamagawa numbers mentioned in the proof above come from multiplicative reductions I_{2n} at primes p, so by using Table 8.1, Table 2 and Lemma 8.2.1, we conclude that all reduction types of twists at p are either I_{2n} or I^*_{2n}, so the Tamagawa numbers stay even.

As for the curves 14a3, 14a4, 14a5 and 14a6, they have $c_E=c_2=2$. By using the fact that $\mathbb{Q}_p^\times/\left(\mathbb{Q}_p^\times\right)^2=\langle -1,2,5\rangle$, we explicitly compute all possible reduction types of quadratic twists at $p=2$ and conclude that for every twist of those curves $4\mid c_E$.

■

Proposition 8.2.3. Let E be an elliptic curve over $\mathbb{Q}$ with a $10-$isogeny. Then $2|c_E$.

Proof. From [31, Table 3] we take the parameterization of the $j-$invariants of the curves that are non-cuspidal points on $X_0(10)$,

$$j(h)=\frac{(h^6-4h^5+16h+16)^3}{(h+1)^2(h-4)h^5}, h\in\mathbb{Q}.$$

From it we can acquire the discriminant and the c_4-invariant up to a twist,

$$\Delta(h) = (h-4)h^5(h+1)^2(h^2-2h-4)^6(h^2-2h+2)^6 f_2(h)^9 f_4(h)^6 f_6(h)^6,$$

$$c_4(h) = (h^2-2h-4)^2(h^2-2h+2)^2 f_2(h)^3 f_4(h)^2 f_6(h)^3,$$

where $f_i(h)$ are polynomials of degree i, which can be computed with the accompanying Magma code.

Assume that there exists a prime p such that $k := ord_p(h+1) > 0$. We compute

$$res\left(h+1, \frac{\Delta(h)}{(h+1)^2}\right) = 5^{22},$$

$$res\,(h+1, c_4(h)) = 5^8.$$

If $p \neq 5$, this means that $p^{2k} \mid \Delta(h)$ and $p \nmid c_4(h)$, and we find from Proposition 8.0.1 that the reduction of E at p is multiplicative of type I_{2k}, and therefore c_p is even (see Table 8.1).

For the case $h+1 = \pm 5^k$, after the change of variables $x \mapsto x \cdot 5^4, y \mapsto y \cdot 5^6$, counting the multiplicities of 5 in $\Delta(h)$ and $c_4(h)$ we get that the factor 5^{2-2k} appears in the $j-$invariant, with $5 \nmid c_4(h)$. Therefore, when $k > 1$, by Proposition 8.0.1 we have multiplicative reduction at 5 of type I_{2k-2} with even c_p (see Table 8.1). For $k \in \{0,1\}$ we have $h \in \{-6,-2,0,4\}$. For the values $h \in \{0,4\}$ we do not have an elliptic curve, and for the values $h \in \{-6,-2\}$ we get twists of curves 768d3 and 768d1, which have $c_E = 2$, both with bad prime 2 with reduction type III, so $c_2 = 2$.

Assume now that there exists a prime p such that $k := ord_p(h+1) < 0$. We put $m := \frac{1}{h+1}$ and after the substitution $x \mapsto x \cdot 5^{-4}, y \mapsto y \cdot 5^{-6}$ we get an elliptic curve with

$$\Delta(m) = (m-1)^5(5m-1)m^{10}(5m^2-4m+1)^6(5m^2-2m+1)^9 g_2(h)^6 g_4(h)^6 g_6(h)^6$$

up to a twist, and

$$c_4(m) = (5m^2-4m+1)^2(5m^2-2m+1)^3 g_2(h)^2 g_4(h)^2 g_6(h)^3$$

up to a twist, where $g_i(h)$ are polynomials of degree i, which can be computed with the accompanying Magma code. We compute

$$res\left(m, \frac{\Delta(m)}{m^{10}}\right) = 1,$$

$$res\,(m, c_4(m)) = 1.$$

We see by Proposition 8.0.1 that the reduction at p is multiplicative of type I_{10k}, with even c_p (see Table 8.1).

To conclude the proof of this proposition, it remains to see how these reduction types and Tamagawa numbers would change under the twisting of the curves. All even Tamagawa numbers mentioned in the proof above come from multiplicative reductions I_{2n} at primes p, so by using Table 8.1, Table 2 and Lemma 8.2.1, we conclude that all reduction types of twists at p are either I_{2n} or I_{2n}^*, so the Tamagawa numbers stay even.

As for the curves 768d3 and 768d1, they have $c_E = c_2 = 2$. By using the fact that $\mathbb{Q}_p^\times / \left(\mathbb{Q}_p^\times\right)^2 = \langle -1, 2, 5\rangle$, we explicitly compute all possible reduction types of quadratic twists at $p = 2$ and conclude that for every twist of those curves $2 \mid c_E$.

■

Proposition 8.2.4. Let E be an elliptic curve over $\mathbb{Q}$ with an $8-$isogeny. Then $2|c_E$, except for the curves $15a7$, $15a8$, $48a4$, where $c_E = 1$.

Proof. From [31, Table 3] we take the parameterization of the $j-$invariants of the curves that are non-cuspidal points on $X_0(8)$,

$$j(h) = \frac{(h^4 - 16h^2 + 16)^3}{(h^2 - 16)h^2}, h \in \mathbb{Q}.$$

From it we can acquire the discriminant and the c_4-invariant up to a twist,

$$\Delta(h) = (h-4)h^2(h+4)f_2(h)^6 f_4(h)^6 f_6(h)^6,$$

$$c_4(h) = f_2(h)^2 f_4(h)^2 f_6(h)^3,$$

where $f_i(h)$ are polynomials of degree i, which can be computed with the accompanying Magma code.

Assume that there exists a prime p such that $k := ord_p(h) > 0$. We compute

$$res\left(h, \frac{\Delta(h)}{h^2}\right) = 2^{64},$$

$$res\,(h, c_4(h)) = 2^{24}.$$

If $p \neq 2$, then this means that $p^{2k} \mid \Delta(h)$ and $p \nmid c_4(h)$, and from Proposition 8.0.1 we find that the reduction of E at p is multiplicative of type I_{2k}, and therefore c_p is even (see Table 8.1).

For the case $h = \pm 2^k$, after the change of variables $x \mapsto x \cdot 2^{12}, y \mapsto y \cdot 2^{18}$, counting the multiplicities of 2 in $\Delta(h)$ and $c_4(h)$ we get that the factor 2^{8-2k} appears in the $j-$invariant, with $2 \nmid c_4(h)$. Therefore, when $k > 4$, we have multiplicative reduction at 2 of type I_{2k-8} with even c_p, by Proposition 8.0.1 and Table 8.1. For $k = 0$ we have $h = \pm 1$ and for the both values we get a twist of the curve 15a8 with $c_E = 1$. For $k = 1$ we have $h = \pm 2$, i.e. a curve 48a4 up to a twist, with $c_E = 1$. When $k = 2$ we do not get a curve and, for $k = 3$ and $h = \pm 8$ we have a twist of 24a3, where $c_E = 2$, and finally for $k = 4$ and $h = \pm 16$ we have a twist of 15a7, where $c_E = 1$.

Assume now that there exists a prime p such that $k := ord_p(h) < 0$. We put $m := \frac{1}{h}$ and after the substitution $x \mapsto x \cdot 2^{-12}, y \mapsto y \cdot 2^{-18}$ we get an elliptic curve with

$$\Delta(m) = -(4m-1)m^8(4m+1)g_2(h)^6 g_4(h)^6 g_6(h)^6$$

up to a twist, and

$$c_4(m) = g_2(h)^2 g_4(h)^3 g_6(h)^2$$

up to a twist, where $g_i(h)$ are polynomials of degree i, which can be computed with the accompanying Magma code. We compute

$$res\left(m, \frac{\Delta(m)}{m^8}\right) = 1,$$

$$res\,(m, c_4(m)) = 1.$$

We see from Proposition 8.0.1 and Table 8.1 that the reduction at p is multiplicative of type I_{8k}, with even c_p.

To conclude the proof of this proposition, it remains to see how these reduction types and Tamagawa numbers would change under the twisting of the curves. All even Tamagawa numbers mentioned in the proof above come from multiplicative reductions I_{2n} at primes p, so by using Table 8.1, Table 2 and Lemma 8.2.1, we conclude that all reduction types of twists at p are either I_{2n} or I^*_{2n}, so the Tamagawa numbers stay even.

As for the curves 15a7, 15a8 and 48a4, they have $c_E = 1$. By using the fact that $\mathbb{Q}_p^\times / \left(\mathbb{Q}_p^\times\right)^2 = \langle -1, 2, 5 \rangle$, we explicitly compute all possible reduction types of quadratic twists at $p = 2$ and conclude that for every twist of those curves $2 \mid c_E$. Lastly, for every twist of the curve 24a3 we have $2 \mid c_E$.

■

Proposition 8.2.5. Let E be an elliptic curve over $\mathbb{Q}$ with a 6−isogeny. Then $2|c_E$, except for the curves 20*a*2, 80*b*2, where $c_E = 1$, and also the curves 27*a*3, 80*b*4 and possibly their twists.

Proof. From [31, Table 3] we take the parameterization of the j−invariants of the curves that are non-cuspidal points on $X_0(6)$,

$$j(h) = \frac{(h+6)^3(h^3+18h^2+84h+24)^3}{h(h+8)^3(h+9)^2}, h \in \mathbb{Q}.$$

From it we can acquire the discriminant and the c_4−invariant up to a twist,

$$\Delta(h) = h(h+6)^6(h+8)^3(h+9)^2 f_2(h)^6 f_3(h)^6 f_4(h)^6,$$

$$c_4(h) = (h+6)^3 f_2(h)^2 f_3(h)^3 f_4(h)^2,$$

where $f_i(h)$ are polynomials of degree i, which can be computed with the accompanying Magma code.

Assume that there exists a prime p such that $k := ord_p(h+9) > 0$. We compute

$$res\left(h+9, \frac{\Delta(h)}{(h+9)^2}\right) = 3^{32},$$

$$res\,(h+9, c_4(h)) = 3^{12}.$$

If $p \neq 3$, this means that $p^{2k} \mid \Delta(h)$ and $p \nmid c_4(h)$, and from Proposition 8.0.1 we find that the reduction of E at p is multiplicative of type I_{2k}, and therefore c_p is even (see Table 8.1).

For the case $h+9 = \pm 3^k$, after the change of variables $x \mapsto x \cdot 3^6, y \mapsto y \cdot 3^9$, counting the multiplicities of 3 in $\Delta(h)$ and $c_4(h)$ we get that the factor 3^{4-2k} appears in the j−invariant, with $3 \nmid c_4(h)$. Therefore, when $k > 2$, we have multiplicative reduction at 3 of type I_{2k-4} with even c_p, by Proposition 8.0.1 and Table 8.1. For $k = 0$ we have $h \in \{-10, -8\}$. With $h = -10$ we have a twist of the elliptic curve 20a2 which has $c_E = 3$, coming from the reduction at 2 of type *IV*, and $h = -8$ does not give us an elliptic curve. For $k = 1$ we have $h \in \{-12, -6\}$. For $h = -12$ we get the curve 36a2 with $c_E = 6$ and for $h = -6$ we have 27a3, where $c_E = 1$. Lastly, if $k = 2$, then $h \in \{-18, 0\}$. For $h = 0$ we do not get an elliptic curve, but for $h = -18$ we get a twist of the curve 80b4, with $c_E = 1$.

Assume now that there exists a prime p such that $k := ord_p(h+9) < 0$. We put $m := \frac{1}{h+9}$ and after the substitution $x \mapsto x \cdot 3^{-6}, y \mapsto y \cdot 3^{-9}$ we get an elliptic curve with

$$\Delta(m) = (m-1)^3(3m-1)^6(9m-1)m^6 g_2(h)^6 g_3(h)^6 g_4(h)^6$$

up to a twist, and

$$c_4(m) = (3m-1)^3 g_2(h)^2 g_3(h)^3 g_4(h)^2,$$

up to a twist, where $g_i(h)$ are polynomials of degree i, which can be computed with the accompanying Magma code. We compute

$$res\left(m, \frac{\Delta(m)}{m^6}\right) = 1,$$

$$res\,(m, c_4(m)) = 1.$$

We see that the reduction at p is multiplicative of type I_{6k}, with even c_p, by Proposition 8.0.1 and Table 8.1.

To conclude the proof of this proposition, it remains to see how these reduction types and Tamagawa numbers would change under the twisting of the curves. All even Tamagawa numbers mentioned in the proof above come from multiplicative reductions I_{2n} at primes p, so by using Table 8.1, Table 2 and Lemma 8.2.1, we conclude that all reduction types of twists at p are either I_{2n} or I^*_{2n}, so the Tamagawa numbers stay even.

As for the curve 20a2, using the fact that $\mathbb{Q}_p^\times / \left(\mathbb{Q}_p^\times\right)^2 = \langle -1, 2, 5 \rangle$, we explicitly compute all possible reduction types of quadratic twists at $p = 2$ and conclude that for every twist of that curve $2 \mid c_E$. The curve 36a2 already has $c_3 = 2$, which will stay the same under every twist. For curves 27a3 and 80b4 we were unable to conclude what will happen with all of the twists, since some of the twists have $c_E = 1$.

■

Proposition 8.2.6. Let E be an elliptic curve over $\mathbb{Q}$ with an $n-$isogeny, $n \in \{14, 17, 19, 37, 43, 67, 163\}$. Then $2 | c_E$.

Proof. For each value of n, from [31, Table 4] we took all the possible $j-$invariants. They can be found in Table 8.3 in the second column. In the third column we have the Cremona label of one of the curves in the class of twists represented by each $j-$invariant. For each of those curves in the fourth column we have a prime of bad reduction of type *III*. That

reduction can only change to III^*, and vice versa, after twisting, as we see in Table 8.2. Table 8.1 tells us that the Tamagawa number at primes of reduction type III and III^* is always 2, so the claim follows.

■

n	$j-$invariant	Cremona label	bad prime with reduction type III
14	$-3^3 \cdot 5^3$	49a1	7
	$3^3 \cdot 5^3 \cdot 17^3$	49a2	7
17	$-\frac{17^2 \cdot 101^3}{2}$	14450p1	5
	$-\frac{17 \cdot 373^3}{2^{17}}$	14450p2	5
19	$-2^{15} \cdot 3^3$	361a1	19
37	$-7 \cdot 11^3$	1225h1	5
	$-7 \cdot 137^3 \cdot 2083^3$	1225h2	5
43	$-2^{18} \cdot 3^3 \cdot 5^3$	1849a1	43
67	$-2^{15} \cdot 3^3 \cdot 5^3 \cdot 11^3$	4489a1	67
163	$-2^{18} \cdot 3^3 \cdot 5^3 \cdot 23^3 \cdot 29^3$	26569a1	163

Table 8.3: $j-$invariants of the curves $X_0(n)$; their Cremona labels are representatives in the class of twists of least conductor with reduction type III at some prime

APPENDIX A

This chapter contains the Magma code used in Chapter 6 for Theorem 6.2.11 (for each group separately) and Table 6.1.

$\mathbb{Z}/11\mathbb{Z}$:

```
S:=[n : n in [2..100] | SquareFree(n) eq n];
// set of all non-negative squarefree integers <100
_<x>:=PolynomialRing(Rationals());
E:=EllipticCurve([0,-1,-1,0,0]);
RankBounds(E);

for d in S do
   printf "d=%o\n", d;
   E1:=QuadraticTwist(E,d);
   r1,r2:=RankBounds(E1);
   r1; r2;
   if r2 eq 0 then
      E2:=BaseChange(E,QuadraticField(d));
      TorsionSubgroup(E2);
   end if;
end for;
```

$\mathbb{Z}/14\mathbb{Z}$:

```
S:=[n : n in [2..100] | SquareFree(n) eq n];
_<x>:=PolynomialRing(Rationals());
E:=EllipticCurve([1,0,1,-1,0]);
RankBounds(E);

```

```
for d in S do
   printf "d=%o\n", d;
   E1:=QuadraticTwist(E,d);
   r1,r2:=RankBounds(E1);
   r1; r2;
   if r2 eq 0 then
      E2:=BaseChange(E,QuadraticField(d));
      TorsionSubgroup(E2);
   end if;
end for;
```

$\mathbb{Z}/15\mathbb{Z}$:

```
S:=[n : n in [2..100] | SquareFree(n) eq n];
_<x>:=PolynomialRing(Rationals());
E:=EllipticCurve([1,1,1,0,0]);
RankBounds(E);

for d in S do
   printf "d=%o\n", d;
   E1:=QuadraticTwist(E,d);
   r1,r2:=RankBounds(E1);
   r1; r2;
   if r2 eq 0 then
      E2:=BaseChange(E,QuadraticField(d));
      TorsionSubgroup(E2);
   end if;
end for;
```

$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/10\mathbb{Z}$:

```
S:=[n : n in [2..100] | SquareFree(n) eq n];
_<x>:=PolynomialRing(Rationals());
E:=EllipticCurve([0,1,0,-1,0]);
RankBounds(E);

for d in S do
```

```
   printf "d=%o\n", d;
   E1:=QuadraticTwist(E,d);
   r1,r2:=RankBounds(E1);
   r1; r2;
   if r2 eq 0 then
      E2:=BaseChange(E,QuadraticField(d));
      TorsionSubgroup(E2);
   end if;
end for;
```

$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/12\mathbb{Z}$:

```
S:=[n : n in [2..100] | SquareFree(n) eq n];
_<x>:=PolynomialRing(Rationals());
E:=EllipticCurve([0,-1,0,1,0]);
RankBounds(E);

for d in S do
   printf "d=%o\n", d;
   E1:=QuadraticTwist(E,d);
   r1,r2:=RankBounds(E1);
   r1; r2;
   if r2 eq 0 then
      E2:=BaseChange(E,QuadraticField(d));
      TorsionSubgroup(E2);
   end if;
end for;
```

$\mathbb{Z}/13\mathbb{Z}$:

```
// In the set S we put only d such that d=1(mod 8) (see Theorem 6.2.6)
S:=[17,33,41,57,65,73,89,97];
_<x>:=PolynomialRing(Rationals());
C:=HyperellipticCurve(x^6-2*x^5+x^4-2*x^3+6*x^2-4*x+1);
J:=Jacobian(C);
RankBounds(J);
TorsionSubgroup(J);
```

```
Points(J:Bound:=100);

for d in S do
   printf "d=%o\n", d;
   C1:=QuadraticTwist(C,d);
   J1:=Jacobian(C1);
   r1,r2:=RankBounds(J1);
   r1; r2;
   TorsionSubgroup(J1);
   if r2 ne 0 then
      C2:=ChangeRing(C,QuadraticField(d));
      Points(C2:Bound:=200);
   end if;
end for;
```

$\mathbb{Z}/16\mathbb{Z}$:

```
S:=[n : n in [2..100] | SquareFree(n) eq n];
_<x>:=PolynomialRing(Rationals());
J:=JOne(16);
L:=LSeries(J);
IsZeroAt(L,1);
// this is false iff rank(J_1(16)(Q))=0
tr, p:=NewModularHyperellipticCurve(ModularSymbols(J));
C1:=HyperellipticCurve(p);

C:=HyperellipticCurve(x*(x^2+1)*(x^2+2*x-1));
J1:=Jacobian(C);
TorsionSubgroup(J1);
Points(J1:Bound:=100);

for d in S do
   printf "d=%o\n", d;
   C2:=QuadraticTwist(C1,d);
   J2:=Jacobian(C2);
   r1, r2:=RankBounds(J2);
   r1; r2;
```

```
   if r2 eq 0 then
   // if the rank of the Jacobian is 0, then we compute
   // the torsion subgroup (as in Proposition 6.2.9)
      C2:=QuadraticTwist(C,d);
      J2:=Jacobian(C2);
      TorsionSubgroup(J2);
      Points(J2:Bound:=100);
      J3:=BaseChange(J1,QuadraticField(d));
      TwoTorsionSubgroup(J3);
   else
   // if the rank of the Jacobian is not 0, then we cannot
   // use the methods described in Proposition 6.2.9,
   // so we are searching for the points on the curve
      C3:=ChangeRing(C,QuadraticField(d));
      Points(C3:Bound:=1000);
      // we can put whichever bound we want
   end if;
end for;
```

$\mathbb{Z}/18\mathbb{Z}$:

```
// In the set S we put only d such that d=1(mod 8) and d!=2(mod 3) (see Theorem 6.2.7)
S:=[33,57,73,97];
_<x>:=PolynomialRing(Rationals());
C:=HyperellipticCurve(x^6+2*x^5+5*x^4+10*x^3+10*x^2+4*x+1);
J:=Jacobian(C);
RankBounds(J);
TorsionSubgroup(J);
Points(J:Bound:=100);

for d in S do
   printf "d=%o\n", d;
   C1:=QuadraticTwist(C,d);
   J1:=Jacobian(C1);
   r1,r2:=RankBounds(J1);
   r1; r2;
   TorsionSubgroup(J1);
```

```
17      if r2 ne 0 then
18         C2:=ChangeRing(C,QuadraticField(d));
19         Points(C2:Bound:=200);
20      end if;
21   end for;
```

APPENDIX B

This chapter contains the Magma code used in Chapter 7.

B.1. Code for Table 7.1

Code for finding the model $y^2 = f_{22}(x)$ for $X_0(22)$ and the factorization of f_{22} in $\mathbb{Q}[X]$:

```
1 _<x>:=PolynomialRing(Rationals());
2 C:=SimplifiedModel(SmallModularCurve(22));
3 C;
4 f:=x^6-4*x^4+20*x^3-40*x^2+48*x-32;
5 Factorization(f);
```

Code for finding the model $y^2 = f_{23}(x)$ for $X_0(23)$ and the factorization of f_{23} in $\mathbb{Q}[X]$:

```
1 _<x>:=PolynomialRing(Rationals());
2 C:=SimplifiedModel(SmallModularCurve(23));
3 C;
4 f:=x^6-8*x^5+2*x^4+2*x^3-11*x^2+10*x-7;
5 Factorization(f);
```

Code for finding the model $y^2 = f_{26}(x)$ for $X_0(26)$ and the factorization of f_{26} in $\mathbb{Q}[X]$:

```
1 _<x>:=PolynomialRing(Rationals());
2 C:=SimplifiedModel(SmallModularCurve(26));
3 C;
4 f:=x^6-8*x^5+8*x^4-18*x^3+8*x^2-8*x+1;
5 Factorization(f);
```

Appendix B

Code for finding the model $y^2 = f_{28}(x)$ for $X_0(28)$ and the factorization of f_{28} in $\mathbb{Q}[X]$:

```
_<x>:=PolynomialRing(Rationals());
C:=SimplifiedModel(SmallModularCurve(28));
C;
f:=4*x^6-12*x^5+25*x^4-30*x^3+25*x^2-12*x+4;
Factorization(f);
// this is the factorization of the normalized model,
// so we have to multiply it by 4, which is the leading coefficient of f
```

Code for finding the model $y^2 = f_{29}(x)$ for $X_0(29)$ and the factorization of f_{29} in $\mathbb{Q}[X]$:

```
_<x>:=PolynomialRing(Rationals());
C:=SimplifiedModel(SmallModularCurve(29));
C;
f:=x^6-4*x^5-12*x^4+2*x^3+8*x^2+8*x-7;
Factorization(f);
```

Code for finding the model $y^2 = f_{30}(x)$ for $X_0(30)$ and the factorization of f_{30} in $\mathbb{Q}[X]$:

```
_<x>:=PolynomialRing(Rationals());
C:=SimplifiedModel(SmallModularCurve(30));
C;
f:=x^8+14*x^7+79*x^6+242*x^5+441*x^4+484*x^3+316*x^2+112*x+16;
Factorization(f);
```

Code for finding the model $y^2 = f_{31}(x)$ for $X_0(31)$ and the factorization of f_{31} in $\mathbb{Q}[X]$:

```
_<x>:=PolynomialRing(Rationals());
C:=SimplifiedModel(SmallModularCurve(31));
C;
f:=x^6-8*x^5+6*x^4+18*x^3-11*x^2-14*x-3;
Factorization(f);
```

Code for finding the model $y^2 = f_{33}(x)$ for $X_0(33)$ and the factorization of f_{33} in $\mathbb{Q}[X]$:

```
_<x>:=PolynomialRing(Rationals());
```

```
C:=SimplifiedModel(SmallModularCurve(33));
C;
f:=x^8+10*x^6-8*x^5+47*x^4-40*x^3+82*x^2-44*x+33;
Factorization(f);
```

Code for finding the model $y^2 = f_{35}(x)$ for $X_0(35)$ and the factorization of f_{35} in $\mathbb{Q}[X]$:

```
_<x>:=PolynomialRing(Rationals());
C:=SimplifiedModel(SmallModularCurve(35));
C;
f:=x^8-4*x^7-6*x^6-4*x^5-9*x^4+4*x^3-6*x^2+4*x+1;
Factorization(f);
```

Code for finding the model $y^2 = f_{39}(x)$ for $X_0(39)$ and the factorization of f_{39} in $\mathbb{Q}[X]$:

```
_<x>:=PolynomialRing(Rationals());
C:=SimplifiedModel(SmallModularCurve(39));
C;
f:=x^8-6*x^7+3*x^6+12*x^5-23*x^4+12*x^3+3*x^2-6*x+1;
Factorization(f);
```

Code for finding the model $y^2 = f_{40}(x)$ for $X_0(40)$ and the factorization of f_{40} in $\mathbb{Q}[X]$:

```
_<x>:=PolynomialRing(Rationals());
C:=SimplifiedModel(SmallModularCurve(40));
C;
f:=x^8+8*x^6-2*x^4+8*x^2+1;
Factorization(f);
```

Code for finding the model $y^2 = f_{41}(x)$ for $X_0(41)$ and the factorization of f_{41} in $\mathbb{Q}[X]$:

```
_<x>:=PolynomialRing(Rationals());
C:=SimplifiedModel(SmallModularCurve(41));
C;
f:=x^8-4*x^7-8*x^6+10*x^5+20*x^4+8*x^3-15*x^2-20*x-8;
Factorization(f);
```

Appendix B

Code for finding the model $y^2 = f_{46}(x)$ for $X_0(46)$ and the factorization of f_{46} in $\mathbb{Q}[X]$:

```
_<x>:=PolynomialRing(Rationals());
C:=SimplifiedModel(SmallModularCurve(46));
C;
f:=x^12-2*x^11+5*x^10+6*x^9-26*x^8+84*x^7-113*x^6+134*x^5-64*x^4+26*x^3+12*x^2+8*x-7;
Factorization(f);
```

Code for finding the model $y^2 = f_{47}(x)$ for $X_0(47)$ and the factorization of f_{47} in $\mathbb{Q}[X]$:

```
_<x>:=PolynomialRing(Rationals());
C:=SimplifiedModel(SmallModularCurve(47));
C;
f:=x^10-6*x^9+11*x^8-24*x^7+19*x^6-16*x^5-13*x^4+30*x^3-38*x^2+28*x-11;
Factorization(f);
```

Code for finding the model $y^2 = f_{48}(x)$ for $X_0(48)$ and the factorization of f_{48} in $\mathbb{Q}[X]$:

```
_<x>:=PolynomialRing(Rationals());
C:=SimplifiedModel(SmallModularCurve(48));
C;
f:=x^8+14*x^4+1;
Factorization(f);
```

Code for finding the model $y^2 = f_{50}(x)$ for $X_0(50)$ and the factorization of f_{50} in $\mathbb{Q}[X]$:

```
_<x>:=PolynomialRing(Rationals());
C:=SimplifiedModel(SmallModularCurve(50));
C;
f:=x^6-4*x^5-10*x^3-4*x+1;
Factorization(f);
```

Code for finding the model $y^2 = f_{59}(x)$ for $X_0(59)$ and the factorization of f_{59} in $\mathbb{Q}[X]$:

```
_<x>:=PolynomialRing(Rationals());
C:=SimplifiedModel(SmallModularCurve(59));
C;
```

```
f:=x^12-8*x^11+22*x^10-28*x^9+3*x^8+40*x^7-62*x^6+40*x^5-3*x^4-24*x^3+20*x^2-4*x-8;
Factorization(f);
```

Code for finding the model $y^2 = f_{71}(x)$ for $X_0(71)$ and the factorization of f_{71} in $\mathbb{Q}[X]$:

```
_<x>:=PolynomialRing(Rationals());
C:=SimplifiedModel(SmallModularCurve(71));
C;
f:=x^14+4*x^13-2*x^12-38*x^11-77*x^10-26*x^9+111*x^8+148*x^7
+x^6-122*x^5-70*x^4+30*x^3+40*x^2+4*x-11;
Factorization(f);
```

B.2. Code for Theorem 7.1.1 a)

$N = 22$:

```
C:=SmallModularCurve(22);
//gives a modular curve X_0(22)
SimplifiedModel(C);
//gives C=X_0(22) in the form y^2=f_22(x)

A:={};
S:=[0..512];
for m in S do
   for n in S do
      if ((m mod 2) ne 0) or ((n mod 2) ne 0) then
      //because (m,n)=1
         f:=m^6-4*m^4*n^2+20*m^3*n^3-40*m^2*n^4+48*m*n^5-32*n^6;
         //this is n^6d=Ds^2 in (7.1.1), obtained by putting x=m/n in
         //SimplifiedModel(C) from above and multiplying with the denominator n^6
         A:=A join {f mod 512};
         //we put the residues modulo 512 in the set A
      end if;
   end for;
end for;
A;
//in the end the set A will contain all possible values
```

```
22  //of Ds^2 modulo 512, for Ds^2 from (7.1.1)
```

$N = 26$:

```
1   C:=SmallModularCurve(26);
2   //gives a modular curve X_0(26)
3   SimplifiedModel(C);
4   //gives C=X_0(26) in the form y^2=f_26(x)
5
6   A:={};
7   S:=[0..169];
8   for m in S do
9      for n in S do
10        if ((m mod 13) ne 0) or ((n mod 13) ne 0) then
11        //because (m,n)=1
12           f:=m^6-8*m^5*n+8*m^4*n^2-18*m^3*n^3+8*m^2*n^4-8*m*n^5+n^6;
13           //this is n^6d=Ds^2 from (7.1.1), obtained by putting x=m/n in
14           //SimplifiedModel(C) from above and multiplying with the denominator n^6
15           A:=A join {f mod 169};
16           //we put the residues modulo 169 in the set A
17        end if;
18     end for;
19  end for;
20  A;
21  //in the end the set A will contain all possible values
22  //of Ds^2 modulo 169=13^2, for Ds^2 from (7.1.1)
23
24  A:={};
25  S:=[0..128];
26  for m in S do
27     for n in S do
28        if ((m mod 2) ne 0) or ((n mod 2) ne 0) then
29        //because (m,n)=1
30           f:=m^6-8*m^5*n+8*m^4*n^2-18*m^3*n^3+8*m^2*n^4-8*m*n^5+n^6;
31           //this is n^6d=Ds^2 from (7.1.1), obtained by putting x=m/n in
32           //SimplifiedModel(C) from above and multiplying with the denominator n^6
33           A:=A join {f mod 128};
```

```
        //we put the residues modulo 128 in the set A
     end if;
   end for;
end for;
A;
//in the end the set A will contain all possible values
//of Ds^2 modulo 128, for Ds^2 from (7.1.1)
```

$N = 28$:

```
C:=SmallModularCurve(28);
//gives a modular curve X_0(28)
SimplifiedModel(C);
//gives C=X_0(28) in the form y^2=f_28(x)

A:={};
S:=[0..3];
for m in S do
   for n in S do
      if ((m mod 3) ne 0) or ((n mod 3) ne 0) then
      //because (m,n)=1
         f:=4*m^6-12*m^5*n+25*m^4*n^2-30*m^3*n^3+25*m^2*n^4-12*m*n^5+4*n^6;
         //this is n^6d=Ds^2 from (7.1.1), obtained by putting x=m/n in
         //SimplifiedModel(C) from above and multiplying with the denominator n^6
         A:=A join {f mod 3};
         //we put the residues modulo 128 in the set A
      end if;
   end for;
end for;
A;
//in the end the set A will contain all possible values
//of Ds^2 modulo 128, for Ds^2 from (7.1.1)

A:={};
S:=[0..49];
for m in S do
   for n in S do
```

```
28      if ((m mod 7) ne 0) or ((n mod 7) ne 0) then       //because (m,n)=1
29         f:=4*m^6-12*m^5*n+25*m^4*n^2-30*m^3*n^3+25*m^2*n^4-12*m*n^5+4*n^6;
30         //this is n^6d=Ds^2 from (7.1.1), obtained by putting x=m/n in
31         //SimplifiedModel(C) from above and multiplying with the denominator n^6
32         A:=A join {f mod 49};
33         //we put the residues modulo 49 in the set A
34      end if;
35   end for;
36end for;
37A;
38//in the end the set A will contain all possible values
39//of Ds^2 modulo 49, for Ds^2 from (7.1.1)
```

$N = 29$:

```
1 C:=SmallModularCurve(29);
2 //gives a modular curve X_0(29)
3 SimplifiedModel(C);
4 //gives C=X_0(29) in the form y^2=f_29(x)
5
6 A:={};
7 S:=[0..32];
8 for m in S do
9    for n in S do
10      if ((m mod 2) ne 0) or ((n mod 2) ne 0) then
11      //because (m,n)=1
12         f:=m^6-4*m^5*n-12*m^4*n^2+2*m^3*n^3+8*m^2*n^4+8*m*n^5-7*n^6;
13         //this is n^6d=Ds^2 from (7.1.1), obtained by putting x=m/n in
14         //SimplifiedModel(C) from above and multiplying with the denominator n^6
15         A:=A join {f mod 32};
16         //we put the residues modulo 32 in the set A
17      end if;
18   end for;
19end for;
20A;
21//in the end the set A will contain all possible values
22//of Ds^2 modulo 32, for Ds^2 from (7.1.1)
```

$N = 30$:

```
C:=SmallModularCurve(30);
//gives a modular curve X_0(30)
SimplifiedModel(C);
//gives C=X_0(30) in the form y^2=f_30(x)

A:={};
S:=[0..128];
for m in S do
   for n in S do
      if ((m mod 2) ne 0) or ((n mod 2) ne 0) then
      //because (m,n)=1
         f:=m^8+14*m^7*n+79*m^6*n^2+242*m^5*n^3+441*m^4*n^4
         +484*m^3*n^5+316*m^2*n^6+112*m*n^7+16*n^8;
         //this is n^8d=Ds^2 from (7.1.1), obtained by putting x=m/n in
         //SimplifiedModel(C) from above and multiplying with the denominator n^8
         A:=A join {f mod 128};
         //we put the residues modulo 128 in the set A
      end if;
   end for;
end for;
A;
//in the end the set A will contain all possible values
//of Ds^2 modulo 128, for Ds^2 from (7.1.1)

A:={};
S:=[0..3];
for m in S do
   for n in S do
      if ((m mod 3) ne 0) or ((n mod 3) ne 0) then
      //because (m,n)=1
         f:=m^8+14*m^7*n+79*m^6*n^2+242*m^5*n^3+441*m^4*n^4
         +484*m^3*n^5+316*m^2*n^6+112*m*n^7+16*n^8;
         //this is n^8d=Ds^2 from (7.1.1), obtained by putting x=m/n in
         //SimplifiedModel(C) from above and multiplying with the denominator n^8
         A:=A join {f mod 3};
         //we put the residues modulo 3 in the set A
```

```
37      end if;
38    end for;
39  end for;
40  A;
41  //in the end the set A will contain all possible values
42  //of Ds^2 modulo 3, for Ds^2 from (7.1.1)
43
44  A:={};
45  S:=[0..25];
46  for m in S do
47    for n in S do
48      if ((m mod 5) ne 0) or ((n mod 5) ne 0) then
49      //because (m,n)=1
50        f:=m^8+14*m^7*n+79*m^6*n^2+242*m^5*n^3+441*m^4*n^4
51        +484*m^3*n^5+316*m^2*n^6+112*m*n^7+16*n^8;
52        //this is n^8d=Ds^2 from (7.1.1), obtained by putting x=m/n in
53        //SimplifiedModel(C) from above and multiplying with the denominator n^8
54        A:=A join {f mod 25};
55        //we put the residues modulo 25 in the set A
56      end if;
57    end for;
58  end for;
59  A;
60  //in the end the set A will contain all possible values
61  //of Ds^2 modulo 25, for Ds^2 from (7.1.1)
```

$N = 33$:

```
1   C:=SmallModularCurve(33);
2   //gives a modular curve X_0(33)
3   SimplifiedModel(C);
4   //gives C=X_0(33) in the form y^2=f_33(x)
5
6   A:={};
7   S:=[0..8];
8   for m in S do
9     for n in S do
```

```
10      if ((m mod 2) ne 0) or ((n mod 2) ne 0) then
11         //because (m,n)=1
12         f:=m^8+10*m^6*n^2-8*m^5*n^3+47*m^4*n^4-40*m^3*n^5+82*m^2*n^6-44*m*n^7+33*n^8;
13         //this is n^8d=Ds^2 from (7.1.1), obtained by putting x=m/n in
14         //SimplifiedModel(C) from above and multiplying with the denominator n^8
15         A:=A join {f mod 8};
16         //we put the residues modulo 8 in the set A
17      end if;
18   end for;
19 end for;
20 A;
21 //in the end the set A will contain all possible values
22 //of Ds^2 modulo 8, for Ds^2 from (7.1.1)
```

$N = 35$:

```
1  C:=SmallModularCurve(35);
2  //gives a modular curve X_0(35)
3  SimplifiedModel(C);
4  //gives C=X_0(35) in the form y^2=f_35(x)
5
6  A:={};
7  S:=[0..4];
8  for m in S do
9     for n in S do
10       if ((m mod 2) ne 0) or ((n mod 2) ne 0) then
11       //because (m,n)=1
12          f:=m^8-4*m^7*n-6*m^6*n^2-4*m^5*n^3-9*m^4*n^4 + 4*m^3*n^5-6*m^2*n^6+4*m*n^7+n^8;
13          //this is n^8d=Ds^2 from (7.1.1), obtained by putting x=m/n in
14          //SimplifiedModel(C) from above and multiplying with the denominator n^8
15          A:=A join {f mod 4};
16          //we put the residues modulo 4 in the set A
17       end if;
18    end for;
19 end for;
20 A;
21 //in the end the set A will contain all possible values
```

```
//of Ds^2 modulo 4, for Ds^2 from (7.1.1)

A:={};
S:=[0..25];
for m in S do
   for n in S do
      if ((m mod 5) ne 0) or ((n mod 5) ne 0) then
      //because (m,n)=1
         f:=m^8-4*m^7*n-6*m^6*n^2-4*m^5*n^3-9*m^4*n^4 + 4*m^3*n^5-6*m^2*n^6+4*m*n^7+n^8;
         //this is n^8d=Ds^2 from (7.1.1), obtained by putting x=m/n in
         //SimplifiedModel(C) from above and multiplying with the denominator n^8
         A:=A join {f mod 25};
         //we put the residues modulo 25 in the set A
      end if;
   end for;
end for;
A;
//in the end the set A will contain all possible values
//of Ds^2 modulo 25, for Ds^2 from (7.1.1)

A:={};
S:=[0..7];
for m in S do
   for n in S do
      if ((m mod 7) ne 0) or ((n mod 7) ne 0) then
      //because (m,n)=1
         f:=m^8-4*m^7*n-6*m^6*n^2-4*m^5*n^3-9*m^4*n^4 + 4*m^3*n^5-6*m^2*n^6+4*m*n^7+n^8;
         //this is n^8d=Ds^2 from (7.1.1), obtained by putting x=m/n in
         //SimplifiedModel(C) from above and multiplying with the denominator n^8
         A:=A join {f mod 7};
         //we put the residues modulo 7 in the set A
      end if;
   end for;
end for;
A;
//in the end the set A will contain all possible values
//of Ds^2 modulo 7, for Ds^2 from (7.1.1)
```

$N = 39$:

```
C:=SmallModularCurve(39);
//gives a modular curve X_0(39)
SimplifiedModel(C);
//gives C=X_0(39) in the form y^2=f_39(x)

A:={};
S:=[0..4];
for m in S do
   for n in S do
      if ((m mod 2) ne 0) or ((n mod 2) ne 0) then
      //because (m,n)=1
         f:=m^8-6*m^7*n+3*m^6*n^2+12*m^5*n^3-23*m^4*n^4+12*m^3*n^5+3*m^2*n^6-6*m*n^7+n^8;
         //this is n^8d=Ds^2 from (7.1.1), obtained by putting x=m/n in
         //SimplifiedModel(C) from above and multiplying with the denominator n^8
         A:=A join {f mod 4};
         //we put the residues modulo 4 in the set A
      end if;
   end for;
end for;
A;
//in the end the set A will contain all possible values
//of Ds^2 modulo 4, for Ds^2 from (7.1.1)

A:={};
S:=[0..13];
for m in S do
   for n in S do
      if ((m mod 13) ne 0) or ((n mod 13) ne 0) then
      //because (m,n)=1
         f:=m^8-6*m^7*n+3*m^6*n^2+12*m^5*n^3-23*m^4*n^4+12*m^3*n^5+3*m^2*n^6-6*m*n^7+n^8;
         //this is n^8d=Ds^2 from (7.1.1), obtained by putting x=m/n in
         //SimplifiedModel(C) from above and multiplying with the denominator n^8
         A:=A join {f mod 13};
         //we put the residues modulo 13 in the set A
      end if;
   end for;
```

```
end for;
A;
//in the end the set A will contain all possible values
//of Ds^2 modulo 13, for Ds^2 from (7.1.1)
```

$N = 40$:

```
C:=SmallModularCurve(40);
//gives a modular curve X_0(40)
SimplifiedModel(C);
//gives C=X_0(40) in the form y^2=f_40(x)

A:={};
S:=[0..3];
for m in S do
   for n in S do
      if ((m mod 3) ne 0) or ((n mod 3) ne 0) then
      //because (m,n)=1
         f:=m^8+8*m^6*n^2-2*m^4*n^4+8*m^2*n^6+n^8;
         //this is n^8d=Ds^2 from (7.1.1), obtained by putting x=m/n in
         //SimplifiedModel(C) from above and multiplying with the denominator n^8
         A:=A join {f mod 3};
         //we put the residues modulo 3 in the set A
      end if;
   end for;
end for;
A;
//in the end the set A will contain all possible values
//of Ds^2 modulo 3, for Ds^2 from (7.1.1)

A:={};
S:=[0..5];
for m in S do
   for n in S do
      if ((m mod 5) ne 0) or ((n mod 5) ne 0) then
      //because (m,n)=1
         f:=m^8+8*m^6*n^2-2*m^4*n^4+8*m^2*n^6+n^8;
```

```
        //this is n^8d=Ds^2 from (7.1.1), obtained by putting x=m/n in
        //SimplifiedModel(C) from above and multiplying with the denominator n^8
        A:=A join {f mod 5};
        //we put the residues modulo 5 in the set A
     end if;
   end for;
end for;
A;
//in the end the set A will contain all possible values
//of Ds^2 modulo 5, for Ds^2 from (7.1.1)
```

$N = 46$:

```
C:=SmallModularCurve(46);
//gives a modular curve X_0(46)
SimplifiedModel(C);
//gives C=X_0(46) in the form y^2=f_46(x)

A:={};
S:=[0..512];
for m in S do
   for n in S do
      if ((m mod 2) ne 0) or ((n mod 2) ne 0) then
      //because (m,n)=1
         f:=m^12-2*m^11*n+5*m^10*n^2+6*m^9*n^3-26*m^8*n^4+84*m^7*n^5-
         113*m^6*n^6+134*m^5*n^7-64*m^4*n^8+26*m^3*n^9+12*m^2*n^10+8*m*n^11-7*n^12;
         //this is n^12d=Ds^2 from (7.1.1), obtained by putting x=m/n in
         //SimplifiedModel(C) from above and multiplying with the denominator n^12
         A:=A join {f mod 512};
         //we put the residues modulo 512 in the set A
      end if;
   end for;
end for;
A;
//in the end the set A will contain all possible values
//of Ds^2 modulo 512, for Ds^2 from (7.1.1)
```

$N = 48$:

```
C:=SmallModularCurve(48);
//gives a modular curve X_0(48)
SimplifiedModel(C);
//gives C=X_0(48) in the form y^2=f_48(x)

A:={};
S:=[0..128];
for m in S do
   for n in S do
      if ((m mod 2) ne 0) and ((n mod 2) ne 0) then
      //because (m,n)=1
         f:=m^8 + 14*m^4*n^4 + n^8;
         //this is n^8d=Ds^2 from (7.1.1), obtained by putting x=m/n in
         //SimplifiedModel(C) from above and multiplying with the denominator n^8
         A:=A join {f mod 128};
         //we put the residues modulo 128 in the set A
      end if;
   end for;
end for;
A;
//in the end the set A will contain all possible values
//of Ds^2 modulo 128, for Ds^2 from (7.1.1)

A:={};
S:=[0..3];
for m in S do
   for n in S do
      if ((m mod 3) ne 0) or ((n mod 3) ne 0) then
      //because (m,n)=1
         f:=m^8 + 14*m^4*n^4 + n^8;
         //this is n^8d=Ds^2 from (7.1.1), obtained by putting x=m/n in
         //SimplifiedModel(C) from above and multiplying with the denominator n^8
         A:=A join {f mod 3};
         //we put the residues modulo 3 in the set A
      end if;
   end for;
```

```
end for;
A;
//in the end the set A will contain all possible values
//of Ds^2 modulo 3, for Ds^2 from (7.1.1)

A:={};
S:=[0..5];
for m in S do
   for n in S do
      if ((m mod 5) ne 0) or ((n mod 5) ne 0) then
      //because (m,n)=1
         f:=m^8 + 14*m^4*n^4 + n^8;
         //this is n^8d=Ds^2 from (7.1.1), obtained by putting x=m/n in
         //SimplifiedModel(C) from above and multiplying with the denominator n^8
         A:=A join {f mod 5};
         //we put the residues modulo 5 in the set A
      end if;
   end for;
end for;
A;
//in the end the set A will contain all possible values
//of Ds^2 modulo 5, for Ds^2 from (7.1.1)
```

$N = 50$:

```
C:=SmallModularCurve(50);
//gives a modular curve X_0(50)
SimplifiedModel(C);
//gives C=X_0(50) in the form y^2=f_50(x)

A:={};
S:=[0..128];
for m in S do
   for n in S do
      if ((m mod 2) ne 0) and ((n mod 2) ne 0) then
      //because (m,n)=1
         f:=m^6-4*m^5*n-10*m^3*n^3-4*m*n^5+n^6;
```

```
13          //this is n^6d=Ds^2 from (7.1.1), obtained by putting x=m/n in
14          //SimplifiedModel(C) from above and multiplying with the denominator n^6
15          A:=A join {f mod 128};
16          //we put the residues modulo 128 in the set A
17        end if;
18      end for;
19  end for;
20  A;
21  //in the end the set A will contain all possible values
22  //of Ds^2 modulo 128, for Ds^2 from (7.1.1)
```

B.3. Code for Table 7.3

Code for finding the model $y^2 = f_{26}(x)$ for $X_0(26)$ and the factorization of f_{26} in $\mathbb{Q}(\sqrt{13})[X]$:

```
1   _<x>:=PolynomialRing(Rationals());
2   C:=SimplifiedModel(SmallModularCurve(26));
3   C;
4   f:=x^6-8*x^5+8*x^4-18*x^3+8*x^2-8*x+1;
5   Factorization(f);
6   Discriminant(f);
7   Factorization(Integers()!Discriminant(f));
8
9   K<x>:=PolynomialRing(QuadraticField(13));
10  Factorization(f, K);
```

Code for finding the model $y^2 = f_{28}(x)$ for $X_0(28)$ and the factorization of f_{28} in $\mathbb{Q}(\sqrt{7})[X]$:

```
1   _<x>:=PolynomialRing(Rationals());
2   C:=SimplifiedModel(SmallModularCurve(28));
3   C;
4   f:=4*x^6-12*x^5+25*x^4-30*x^3+25*x^2-12*x+4;
5   Factorization(f);
6   // this is the factorization of the normalized model, so we have
7   //to multiply it by 4, which is the leading coefficient of f
8   Discriminant(2*Factorization(f)[1][1]);
```

```
Factorization(Integers()!Discriminant(2*Factorization(f)[1][1]));
Discriminant(Factorization(f)[2][1]);
Factorization(Integers()!Discriminant(Factorization(f)[2][1]));
Discriminant(2*Factorization(f)[3][1]);
Factorization(Integers()!Discriminant(2*Factorization(f)[3][1]));

K<x>:=PolynomialRing(QuadraticField(-7));
Factorization(f, K);
```

Code for finding the model $y^2 = f_{29}(x)$ for $X_0(29)$ and the factorization of f_{29} in $\mathbb{Q}(\sqrt{9})[X]$:

```
_<x>:=PolynomialRing(Rationals());
C:=SimplifiedModel(SmallModularCurve(29));
C;
f:=x^6-4*x^5-12*x^4+2*x^3+8*x^2+8*x-7;
Factorization(f);
Discriminant(f);
Factorization(Integers()!Discriminant(f));

K<x>:=PolynomialRing(QuadraticField(29));
Factorization(f, K);
```

Code for finding the model $y^2 = f_{30}(x)$ for $X_0(30)$ and the factorization of f_{30} in $\mathbb{Q}(\sqrt{5})[X]$:

```
_<x>:=PolynomialRing(Rationals());
C:=SimplifiedModel(SmallModularCurve(30));
C;
f:=x^8+14*x^7+79*x^6+242*x^5+441*x^4+484*x^3+316*x^2+112*x+16;
Factorization(f);
Discriminant(Factorization(f)[1][1]);
Factorization(Integers()!Discriminant(Factorization(f)[1][1]));
Discriminant(Factorization(f)[2][1]);
Factorization(Integers()!Discriminant(Factorization(f)[2][1]));
Discriminant(Factorization(f)[3][1]);
Factorization(Integers()!Discriminant(Factorization(f)[3][1]));

K<x>:=PolynomialRing(QuadraticField(5));
```

```
14 Factorization(f, K);
```

Code for finding the model $y^2 = f_{33}(x)$ for $X_0(33)$ and the factorization of f_{33} in $\mathbb{Q}(\sqrt{-11})[X]$:

```
1  _<x>:=PolynomialRing(Rationals());
2  C:=SimplifiedModel(SmallModularCurve(33));
3  C;
4  f:=x^8+10*x^6-8*x^5+47*x^4-40*x^3+82*x^2-44*x+33;
5  Factorization(f);
6  Discriminant(Factorization(f)[1][1]);
7  Factorization(Integers()!Discriminant(Factorization(f)[1][1]));
8  Discriminant(Factorization(f)[2][1]);
9  Factorization(Integers()!Discriminant(Factorization(f)[2][1]));
10
11 K<x>:=PolynomialRing(QuadraticField(-11));
12 Factorization(f, K);
```

Code for finding the model $y^2 = f_{35}(x)$ for $X_0(35)$ and the factorization of f_{35} in $\mathbb{Q}(\sqrt{5})[X]$:

```
1  _<x>:=PolynomialRing(Rationals());
2  C:=SimplifiedModel(SmallModularCurve(35));
3  C;
4  f:=x^8-4*x^7-6*x^6-4*x^5-9*x^4+4*x^3-6*x^2+4*x+1;
5  Factorization(f);
6  Discriminant(Factorization(f)[1][1]);
7  Factorization(Integers()!Discriminant(Factorization(f)[1][1]));
8  Discriminant(Factorization(f)[2][1]);
9  Factorization(Integers()!Discriminant(Factorization(f)[2][1]));
10
11 K<x>:=PolynomialRing(QuadraticField(5));
12 Factorization(f, K);
```

Code for finding the model $y^2 = f_{39}(x)$ for $X_0(39)$ and the factorization of f_{39} in $\mathbb{Q}(\sqrt{13})[X]$:

```
1  _<x>:=PolynomialRing(Rationals());
2  C:=SimplifiedModel(SmallModularCurve(39));
```

```
C;
f:=x^8-6*x^7+3*x^6+12*x^5-23*x^4+12*x^3+3*x^2-6*x+1;
Factorization(f);
Discriminant(Factorization(f)[1][1]);
Factorization(Integers()!Discriminant(Factorization(f)[1][1]));
Discriminant(Factorization(f)[2][1]);
Factorization(Integers()!Discriminant(Factorization(f)[2][1]));

K<x>:=PolynomialRing(QuadraticField(13));
Factorization(f, K);
```

Code for finding the model $y^2 = f_{40}(x)$ for $X_0(40)$ and the factorization of f_{40} in $\mathbb{Q}(\sqrt{-1})[X]$ and $\mathbb{Q}(\sqrt{5})[X]$:

```
_<x>:=PolynomialRing(Rationals());
C:=SimplifiedModel(SmallModularCurve(40));
C;
f:=x^8+8*x^6-2*x^4+8*x^2+1;
Factorization(f);
Discriminant(f);
Factorization(Integers()!Discriminant(f));

K<x>:=PolynomialRing(QuadraticField(-1));
Factorization(f, K);

K<x>:=PolynomialRing(QuadraticField(5));
Factorization(f, K);
```

Code for finding the model $y^2 = f_{41}(x)$ for $X_0(41)$ and the factorization of f_{41} in $\mathbb{Q}(\sqrt{41})[X]$:

```
_<x>:=PolynomialRing(Rationals());
C:=SimplifiedModel(SmallModularCurve(41));
C;
f:=x^8-4*x^7-8*x^6+10*x^5+20*x^4+8*x^3-15*x^2-20*x-8;
Factorization(f);
Discriminant(f);
Factorization(Integers()!Discriminant(f));
```

```
8
9  K<x>:=PolynomialRing(QuadraticField(41));
10 Factorization(f, K);
```

Code for finding the model $y^2 = f_{48}(x)$ for $X_0(48)$ and the factorization of f_{48} in $\mathbb{Q}(\sqrt{-1})[X]$ and $\mathbb{Q}(\sqrt{3})[X]$:

```
1  _<x>:=PolynomialRing(Rationals());
2  C:=SimplifiedModel(SmallModularCurve(48));
3  C;
4  f:=x^8+14*x^4+1;
5  Factorization(f);
6  Discriminant(Factorization(f)[1][1]);
7  Factorization(Integers()!Discriminant(Factorization(f)[1][1]));
8  Discriminant(Factorization(f)[2][1]);
9  Factorization(Integers()!Discriminant(Factorization(f)[2][1]));
10
11 K<x>:=PolynomialRing(QuadraticField(-1));
12 Factorization(f, K);
13
14 K<x>:=PolynomialRing(QuadraticField(3));
15 Factorization(f, K);
```

Code for finding the model $y^2 = f_{50}(x)$ for $X_0(50)$ and the factorization of f_{50} in $\mathbb{Q}(\sqrt{5})[X]$:

```
1  _<x>:=PolynomialRing(Rationals());
2  C:=SimplifiedModel(SmallModularCurve(50));
3  C;
4  f:=x^6-4*x^5-10*x^3-4*x+1;
5  Factorization(f);
6  Discriminant(f);
7  Factorization(Integers()!Discriminant(f));
8
9  K<x>:=PolynomialRing(QuadraticField(5));
10 Factorization(f, K);
```

B.4. Code for Table 7.4

```
function check(p,f);
// this function returns the set of all possible residues
// of f mod p if p is not 2, and mod 4 if p is 2
A:={};
S:=[0..p];
for m in S do
   for n in S do
      if ((m mod p) ne 0) or ((n mod p) ne 0) then
      // because (m,n)=1
         g:=Integers()!Evaluate(f, [m, 0, n]);
         if p eq 2 then
            A:=A join {-g mod 4};
            // we put the residues modulo 4 in the set A
         else
            A:=A join {-g mod p};
            // we put the residues modulo p in the set A
         end if;
      end if;
   end for;
end for;
return A;
end function;

function Unramified(N);
// this function returns the set of primes between 1 and 100
// that are unramified in all quadratic fields generated by points on X0(22)
f:=DefiningPolynomial(SimplifiedModel(SmallModularCurve(N)));
A:={i:i in PrimesUpTo(100)};
for p in PrimesUpTo(100) do
B:=check(p,f);
if p eq 2 then
   for k in B do
      if B ne {1} then
         A:=A diff {2};
```

```
35          // if (k mod 4) is not 1, then 2 may ramify
36        end if;
37     end for;
38  else
39     if 0 in B then
40        A:=A diff {p};
41        // if 0 is in B, then p may ramify
42        end if;
43     end if;
44  end for;
45  return A;
46  end function;
47
48  Table4:=[*[*22, {3, 5, 23, 31, 37, 59, 67, 71, 89, 97}*],
49  // [*N, {primes that are unramified in all quadratic fields generated by points on X0(N)}*],
50  // according to Theorem 7.1.10
51  [*23, {2, 3, 13, 29, 31, 41, 47, 71, 73}*],
52  [*26, {3, 5, 7, 11, 17, 19, 31, 37, 41, 43, 47, 59, 67, 71, 73, 83, 89, 97}*],
53  [*28, {3, 5, 13, 17, 19, 31, 41, 47, 59, 61, 73, 83, 89, 97}*],
54  [*29, {3, 5, 11, 13, 17, 19, 31, 37, 41, 43, 47, 53, 61, 73, 79, 89, 97}*],
55  // we exclude p=2 here, it was proved in Theorem 2.1.a)
56  [*30, {3, 7, 13, 17, 23, 37, 43, 47, 53, 67, 73, 83, 97}*],
57  [*31, {2, 5, 7, 19, 41, 59, 71, 97}*],
58  [*33, {2, 7, 13, 17, 19, 29, 41, 43, 61, 73, 79, 83}*],
59  [*35, {2, 3, 7, 13, 17, 23, 37, 43, 47, 53, 67, 73, 83, 97}*],
60  [*39, {2, 5, 7, 11, 13, 19, 31, 37, 41, 47, 59, 61, 67, 71, 73, 79, 83, 89, 97}*],
61  [*40, {3, 5, 7, 11, 13, 17, 19, 23, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 97}*],
62  // we exclude p=2 here, it was proved in Theorem 2.1.a)
63  [*41, {3, 5, 7, 11, 13, 17, 19, 29, 37, 47, 53, 61, 67, 71, 73, 79, 89, 97}*],
64  [*46, {3, 13, 29, 31, 41, 47, 71, 73}*],
65  // we exclude p=2 here, because it was proved in Theorem 2.1.a)
66  [*47, {2, 3, 7, 17, 37, 53, 59, 61, 71, 79, 89, 97}*],
67  [*48, {3, 5, 7, 11, 17, 19, 23, 29, 31, 41, 43, 47, 53, 59, 67, 71, 79, 83, 89}*],
68  // we exclude p=2 here, because it was proved in Theorem 2.1.a)
69  [*50, {3, 7, 11, 13, 17, 19, 23, 37, 41, 43, 47, 53, 67, 73, 83, 89, 97}*],
70  [*59, {3, 5, 7, 19, 29, 41, 53, 79}*],
71  [*71, {2, 3, 5, 19, 29, 37, 43, 73, 79, 83, 89}*]*];
```

```
72
73 A:={}; B:={};
74 for i in [1..#Table4] do
75 N:=Table4[i][1];
76 B:=Table4[i][2];
77 // the set of primes that are unramified in all quadratic fields
78 // generated by points on X0(N), according to Theorem 7.1.10
79 A:=Unramified(N);
80 // the set of primes that are unramified in all quadratic fields generated by
81 // points on X0(N), according to the function Unramified()
82 assert A eq B;
83 end for;
```

B.5. A model for E_u

Model for E_u with torsion $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/14\mathbb{Z}$, mentioned at the beginning of Section 7.2, along with factorizations of the $j-$invariant, c_4-invariant and discriminant of E_u and factorization of f in $\mathbb{F}_2$ used in Lemma 7.2.4.

```
1  K<u>:=FunctionField(Rationals());
2  _<x>:=PolynomialRing(K);
3  F<v>:=ext<K|((u^3+u^2-2*u-1)*x*(x+1) +(x^3+x^2-2*x-1)*u*(u+1))>;
4
5  // this part is taken from https://math.mit.edu/~drew/X1/X1_2_14.txt
6  q := (u+v)/(v-u);
7  t := (u-v)*(u+v)*(u+v+2)/(u^3+u^2*v+2*u^2+u*v^2+2*u*v+v^3+2*v^2);
8  E := EllipticCurve([0,t^2-2*q*t-2,0,-(t^2-1)*(q*t+1)^2,0]);
9  E;
10 // this is the elliptic curve E=E_u mentioned in Section 7.2
11
12 // factorization of the j-invariant of the elliptic curve E from above
13 den_j:=Denominator(jInvariant(E));
14 num_j:=Denominator(1/jInvariant(E));
15 Factorization(den_j);
16 Factorization(num_j);
17
```

```
// factorization of the c_4-invariant of the elliptic curve E from above
den_c4:=Denominator(cInvariants(E)[1]);
num_c4:=Denominator(1/cInvariants(E)[1]);
Factorization(den_c4);
Factorization(num_c4);

// factorization of the discriminant of the elliptic curve E from above
den_D:=Denominator(Discriminant(E));
num_D:=Denominator(1/Discriminant(E));
Factorization(den_D);
Factorization(num_D);

// factorization of f in F_2 used in Lemma 7.2.4
K<u,v>:=PolynomialRing(FiniteField(2),2);
f:=(u^3 + u^2 - 2*u - 1)*v*(v + 1)+(v^3 + v^2 - 2*v - 1)*u*(u + 1);
Factorization(f);
```

APPENDIX C

This chapter contains the Magma code used in Chapter 8.

C.1. Families in the beginning of Section 8.1 are isomorphic

In this portion of the code we check if the family of elliptic curves given in D. Jeon, A. Schweizer "*Torsion of rational elliptic curves over different types of cubic fields*" contains all elliptic curves with torsion $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/14\mathbb{Z}$.

```
K<u>:=FunctionField(Rationals());
_<x>:=PolynomialRing(K);
F<v>:=ext<K|((u^3+u^2-2*u-1)*x*(x+1) +(x^3+x^2-2*x-1)*u*(u+1))>;
// the field over which curve E_u is defined, given by P. Bruin
// and F. Najman in "Fields of definition of elliptic curves with prescribed torsion"
L<w>:=ext<K|((u^2-1)*x^3+(u^3+2*u^2-9*u-2)*x^2-9*(u^2-1)*x-u^3-2*u^2+9*u+2)>;
// the field over which curve E_u is defined, given by D. Jeon and A. Schweizer
// in "Torsion of rational elliptic curves over different types of cubic fields"

tr,f:=IsIsomorphic(F,L);
// here we check whether the fields are isomorphic; tr=true
// and f is an isomorphism between F and L

// here is the model E_u presented in the paper of D. Jeon
// and A. Schweizer defined over the field L
A:=-(u^12+4*u^11-10*u^10-68*u^9+3*u^8+552*u^7+4*u^6-2568*u^5
+2103*u^4+1684*u^3+1958*u^2+396*u+37)
/(48*(u^2+3)^3*(u^6+4*u^5+13*u^4-40*u^3+19*u^2+36*u+31));
B:=(u^24+8*u^23+12*u^22-120*u^21-518*u^20+504*u^19+5068*u^18+568*u^17
-24009*u^16-15024*u^15+62936*u^14+183120*u^13-550452*u^12-851984*u^11+4384056*u^10
```

```
-3808912*u^9+1467519*u^8-4083672*u^7+3590300*u^6+5512360*u^5+6945498*u^4
+2943128*u^3+893052*u^2+120024*u+3753)
/(864*(u^2+3)^6*(u^6+4*u^5+13*u^4-40*u^3+19*u^2+36*u+31)^2);
E1:=EllipticCurve([A, B]);
E1:=BaseChange(E1, L);

// this part is from https://math.mit.edu/~drew/X1/X1_2_14.txt
q := (u+v)/(v-u);
t := (u-v)*(u+v)*(u+v+2)/(u^3+u^2*v+2*u^2+u*v^2+2*u*v+v^3+2*v^2);
E2 := EllipticCurve([f(0),f(t^2-2*q*t-2),f(0),f(-(t^2-1)*(q*t+1)^2),f(0)]);
// we create an elliptic curve with coefficients
// after they are mapped by the isomorphism f

IsIsomorphic(E1,E2);
// we check whether the curves are isomorphic, this returns "true"
```

C.2. Code for Proposition 8.1.2

```
K<u>:=PolynomialRing(Rationals());

A2:=(-4*(u^6+2*u^5+15*u^4-20*u^3+15*u^2+18*u+33)*(u-1)^2*(u+1)^2)/
((u^2+3)^3*(u^6+4*u^5+13*u^4-40*u^3+19*u^2+36*u+31));
A4:=(64*(u^6+2*u^5+3*u^4-20*u^3+39*u^2+18*u+21)*(u-1)^6*(u+1)^6)/
((u^2+3)^6*(u^6+4*u^5+13*u^4-40*u^3+19*u^2+36*u+31)^2);
A6:=(4096*(u-1)^12*(u+1)^12)/((u^6+4*u^5+13*u^4-40*u^3+19*u^2+36*u+31)^3*(u^2+3)^9);
E:=EllipticCurve([1,A2,0,A4,A6]);
// we create an elliptic curve given by the long Weierstrass model in
// section 2.4 of the paper D. Jeon, A. Schweizer
// "Torsion of rational elliptic curves over different types of cubic fields"

Factorization(Numerator(Discriminant(E)));
// gives the normalized factorization of the numerator of the discriminant
Factorization(Denominator(Discriminant(E)));
// gives the normalized factorization of the denominator of the discriminant
Numerator(Discriminant(E));
```

```
// we have to check those because the factorization is normalized and we
// want to see whether there are any leading coefficients
Denominator(Discriminant(E));

Factorization(Numerator(cInvariants(E)[1]));
// gives the normalized factorization of the numerator of the c_4-invariant
Factorization(Denominator(cInvariants(E)[1]));
// gives the normalized factorization of the denominator of the c_4-invariant
Numerator(cInvariants(E)[1]);
// we have to check those because the factorization is normalized and we
//want to see whether there are any leading coefficients
Denominator(cInvariants(E)[1]);
```

$ord_2(u) > 0$:

```
K<u>:=PolynomialRing(Rationals());

A2:=(-4*(u^6+2*u^5+15*u^4-20*u^3+15*u^2+18*u+33)*(u-1)^2*(u+1)^2)/
((u^2+3)^3*(u^6+4*u^5+13*u^4-40*u^3+19*u^2+36*u+31));
A4:=(64*(u^6+2*u^5+3*u^4-20*u^3+39*u^2+18*u+21)*(u-1)^6*(u+1)^6)/
((u^2+3)^6*(u^6+4*u^5+13*u^4-40*u^3+19*u^2+36*u+31)^2);
A6:=(4096*(u-1)^12*(u+1)^12)/((u^6+4*u^5+13*u^4-40*u^3+19*u^2+36*u+31)^3*(u^2+3)^9);
E:=EllipticCurve([1,A2,0,A4,A6]);

aInvariants(E)[3];
// gives a_3, and we see that ord_2(a_3)>0
aInvariants(E)[4];
// gives a_4, and we see that ord_2(a_4)>0 (we have to look at the numerator)
aInvariants(E)[5];
// gives a_6, and we see that ord_2(a_6)>0 (we have to look at the numerator)
bInvariants(E)[1];
// gives b_2, and ord_2(b_2)=0, so the conditions of Lemma 8.1.1 are satisfied

aInvariants(E)[1];
// gives a_1=1
aInvariants(E)[2];
// gives a_2, and ord_2(a_2)>0 so we get the equation T^2+T=0 over F_2 in Lemma 8.1.1
```

$ord_2(u) < 0$:

```
K<m>:=PolynomialRing(Rationals());
u:=1/m;
// the substitution u-->1/m

A2:=(-4*(u^6+2*u^5+15*u^4-20*u^3+15*u^2+18*u+33)*(u-1)^2*(u+1)^2)/
((u^2+3)^3*(u^6+4*u^5+13*u^4-40*u^3+19*u^2+36*u+31));
A4:=(64*(u^6+2*u^5+3*u^4-20*u^3+39*u^2+18*u+21)*(u-1)^6*(u+1)^6)/
((u^2+3)^6*(u^6+4*u^5+13*u^4-40*u^3+19*u^2+36*u+31)^2);
A6:=(4096*(u-1)^12*(u+1)^12)/((u^6+4*u^5+13*u^4-40*u^3+19*u^2+36*u+31)^3*(u^2+3)^9);
E:=EllipticCurve([1,A2,0,A4,A6]);
// we create an elliptic curve given by the long Weierstrass model in
// section 2.4 of the paper D. Jeon, A. Schweizer
// "Torsion of rational elliptic curves over different types of cubic fields"

Factorization(Numerator(Discriminant(E)));
// gives the normalized factorization of the numerator of the discriminant
Factorization(Denominator(Discriminant(E)));
// gives the normalized factorization of the denominator of the discriminant
Numerator(Discriminant(E));
// we have to check those because the factorization is normalized and we
// want to see whether there are any leading coefficients
Denominator(Discriminant(E));

Factorization(Numerator(cInvariants(E)[1]));
// gives the normalized factorization of the numerator of the c_4-invariant
Factorization(Denominator(cInvariants(E)[1]));
// gives the normalized factorization of the denominator of the c_4-invariant
Numerator(cInvariants(E)[1]);
// we have to check those because the factorization is normalized and we
// want to see whether there are any leading coefficients
Denominator(cInvariants(E)[1]);

aInvariants(E)[3];
// gives a_3, and we see that ord_2(a_3)>0
aInvariants(E)[4];
// gives a_4, and we see that ord_2(a_4)>0 (we have to look at the numerator)
```

```
aInvariants(E)[5];
// gives a_6, and we see that ord_2(a_6)>0 (we have to look at the numerator)
bInvariants(E)[1];
// gives b_2, and ord_2(b_2)=0, so the conditions of Lemma 2.1 are satisfied

aInvariants(E)[1];
// gives a_1=1
aInvariants(E)[2];
// gives a_2, and ord_2(a_2)>0 so we get the equation T^2+T=0 over F_2 in Lemma 8.1.1
```

$ord_2(u) = 0$:

```
K<m>:=PolynomialRing(Rationals());
u:=m+1;
// the substitution u-1-->m

A2:=(-4*(u^6+2*u^5+15*u^4-20*u^3+15*u^2+18*u+33)*(u-1)^2*(u+1)^2)/
((u^2+3)^3*(u^6+4*u^5+13*u^4-40*u^3+19*u^2+36*u+31));
A4:=(64*(u^6+2*u^5+3*u^4-20*u^3+39*u^2+18*u+21)*(u-1)^6*(u+1)^6)/
((u^2+3)^6*(u^6+4*u^5+13*u^4-40*u^3+19*u^2+36*u+31)^2);
A6:=(4096*(u-1)^12*(u+1)^12)/((u^6+4*u^5+13*u^4-40*u^3+19*u^2+36*u+31)^3*(u^2+3)^9);
E:=EllipticCurve([1,A2,0,A4,A6]);
// we create an elliptic curve given by the long Weierstrass model in
// section 2.4 of the paper D. Jeon, A. Schweizer
// "Torsion of rational elliptic curves over different types of cubic fields"



aInvariants(E)[3];
// gives a_3, and we see that ord_2(a_3)>0
aInvariants(E)[4];
// gives a_4, and we see that for k>1 we have ord_2(a_4)>0
aInvariants(E)[5];
// gives a_6, and we see that for k>1 we have ord_2(a_6)>0
bInvariants(E)[1];
// gives b_2, and ord_2(b_2)=0 (when we divide both numerator and the denominator with 2^12),
// so the conditions of Lemma 8.1.1 are satisfied
```

```
26
27 aInvariants(E)[1];
28 // gives a_1=1
29 aInvariants(E)[2];
30 // gives a_2, and for k>1 we have ord_2(a_2)>0
31 // so we get the equation T^2+T=0 over F_2 in Lemma 8.1.1
```

$k = 1$:

```
1  K<n>:=PolynomialRing(Rationals());
2  u:=2*n+1;
3  // the substitution u-->2n+1
4
5  A2:=(-4*(u^6+2*u^5+15*u^4-20*u^3+15*u^2+18*u+33)*(u-1)^2*(u+1)^2)/
6  ((u^2+3)^3*(u^6+4*u^5+13*u^4-40*u^3+19*u^2+36*u+31));
7  A4:=(64*(u^6+2*u^5+3*u^4-20*u^3+39*u^2+18*u+21)*(u-1)^6*(u+1)^6)/
8  ((u^2+3)^6*(u^6+4*u^5+13*u^4-40*u^3+19*u^2+36*u+31)^2);
9  A6:=(4096*(u-1)^12*(u+1)^12)/((u^6+4*u^5+13*u^4-40*u^3+19*u^2+36*u+31)^3*(u^2+3)^9);
10 E:=EllipticCurve([1,A2,0,A4,A6]);
11 // we create an elliptic curve given by the long Weierstrass model in
12 // section 2.4 of the paper D. Jeon, A. Schweizer
13 // "Torsion of rational elliptic curves over different types of cubic fields"
14
15 Factorization(Numerator(Discriminant(E)));
16 // gives the normalized factorization of the numerator of the discriminant
17 Factorization(Denominator(Discriminant(E)));
18 // gives the normalized factorization of the denominator of the discriminant
19 Numerator(Discriminant(E));
20 // we have to check those because the factorization is normalized and we
21 // want to see whether there are any leading coefficients
22 Denominator(Discriminant(E));
23
24 Factorization(Numerator(cInvariants(E)[1]));
25 // gives the normalized factorization of the numerator of the c_4-invariant
26 Factorization(Denominator(cInvariants(E)[1]));
27 // gives the normalized factorization of the denominator of the c_4-invariant
28 Numerator(cInvariants(E)[1]);
```

```
// we have to check those because the factorization is normalized and we
// want to see whether there are any leading coefficients
Denominator(cInvariants(E)[1]);

aInvariants(E)[3];
// gives a_3, and we see that ord_2(a_3)>0
aInvariants(E)[4];
// gives a_4, and we see that ord_2(a_4)>0 (taking into consideration that ord_2(n)=0)
aInvariants(E)[5];
// gives a_6, and we see that ord_2(a_6)>0 (taking into consideration that ord_2(n)=0)
bInvariants(E)[1];
// gives b_2, and ord_2(b_2)=0 (taking into consideration that ord_2(n)=0),
// so the conditions of Lemma 8.1.1 are satisfied

aInvariants(E)[1];
// gives a_1=1
aInvariants(E)[2];
// gives a_2, and taking into consideration that ord_2(n)=0 we
// have ord_2(a_2)>0 so we get the equation T^2+T=0 over F_2 in Lemma 8.1.1
```

C.3. Code for Proposition 8.1.4

```
K<u>:=PolynomialRing(Rationals());

A:=-(u^12+4*u^11-10*u^10-68*u^9+3*u^8+552*u^7+4*u^6-2568*u^5+2103*u^4
+1684*u^3+1958*u^2+396*u+37)/(48*(u^2+3)^3
*(u^6+4*u^5+13*u^4-40*u^3+19*u^2+36*u+31));
B:=(u^24+8*u^23+12*u^22-120*u^21-518*u^20+504*u^19
+5068*u^18+568*u^17-24009*u^16-15024*u^15+62936*u^14+183120*u^13-550452*u^12-851984*u^11
+4384056*u^10-3808912*u^9+1467519*u^8-4083672*u^7+3590300*u^6+5512360*u^5
+6945498*u^4+2943128*u^3+893052*u^2+120024*u+3753)/(864*(u^2+3)^6*(u^6
+4*u^5+13*u^4-40*u^3+19*u^2+36*u+31)^2);
E:=MinimalModel(EllipticCurve([A,B]));
// we create an elliptic curve given by the short Weierstrass model in
// section 2.4 of the paper D. Jeon, A. Schweizer
```

```
// "Torsion of rational elliptic curves over different types of cubic fields"

Factorization(K!Discriminant(E));
// gives the normalized factorization of the discriminant
Discriminant(E);
// we have to check this because the factorization is normalized and we
//want to see whether there are any leading coefficients

Factorization(K!cInvariants(E)[1]);
// gives the normalized factorization of the c_4-invariant
cInvariants(E)[1];
// we have to check this because the factorization is normalized and we
// want to see whether there are any leading coefficients
```

$ord_p(u-1) > 0$:

```
K<u>:=PolynomialRing(Rationals());

A:=-(u^12+4*u^11-10*u^10-68*u^9+3*u^8+552*u^7+4*u^6-2568*u^5+2103*u^4
+1684*u^3+1958*u^2+396*u+37)/(48*(u^2+3)^3
*(u^6+4*u^5+13*u^4-40*u^3+19*u^2+36*u+31));
B:=(u^24+8*u^23+12*u^22-120*u^21-518*u^20+504*u^19
+5068*u^18+568*u^17-24009*u^16-15024*u^15+62936*u^14+183120*u^13-550452*u^12-851984*u^11
+4384056*u^10-3808912*u^9+1467519*u^8-4083672*u^7+3590300*u^6+5512360*u^5
+6945498*u^4+2943128*u^3+893052*u^2+120024*u+3753)/(864*(u^2+3)^6*(u^6
+4*u^5+13*u^4-40*u^3+19*u^2+36*u+31)^2);
E:=MinimalModel(EllipticCurve([A,B]));

Factorization(Integers()!Resultant(K!(u-1), K!(Discriminant(E)/(u-1)^14)));
// res(u-1, Delta(u)/(u-1)^14)=2^82
Factorization(Integers()!Resultant(K!(u-1), K!cInvariants(E)[1]));
// res(u-1, c_4(u))=2^32

Evaluate(-cInvariants(E)[2],1);
// we evaluate -c_6 in u=1 because u=1(mod p)
Factorization(Integers()!Evaluate(-cInvariants(E)[2],1));
// -c_6=2^48
```

$ord_p(u-1) < 0$:

```
K<m>:=PolynomialRing(Rationals());
u:=(1+m)/m;

A:=-(u^12+4*u^11-10*u^10-68*u^9+3*u^8+552*u^7+4*u^6-2568*u^5+2103*u^4
+1684*u^3+1958*u^2+396*u+37)/(48*(u^2+3)^3
*(u^6+4*u^5+13*u^4-40*u^3+19*u^2+36*u+31));
B:=(u^24+8*u^23+12*u^22-120*u^21-518*u^20+504*u^19
+5068*u^18+568*u^17-24009*u^16-15024*u^15+62936*u^14+183120*u^13-550452*u^12-851984*u^11
+4384056*u^10-3808912*u^9+1467519*u^8-4083672*u^7+3590300*u^6+5512360*u^5
+6945498*u^4+2943128*u^3+893052*u^2+120024*u+3753)/(864*(u^2+3)^6*(u^6
+4*u^5+13*u^4-40*u^3+19*u^2+36*u+31)^2);
E:=MinimalModel(EllipticCurve([A,B]));

Factorization(K!Discriminant(E));
// gives the normalized factorization of the discriminant
Discriminant(E);
// we have to check this because the factorization is normalized and we
// want to see whether there are any leading coefficients

Factorization(K!cInvariants(E)[1]);
// gives the normalized factorization of the c_4-invariant
cInvariants(E)[1];
// we have to check this because the factorization is normalized and we
// want to see whether there are any leading coefficients

Resultant(K!m, K!(Discriminant(E)/m^14));
Factorization(Integers()!Denominator(Resultant(K!m, K!(Discriminant(E)/m^14))));
// res(m, Delta(m)/m^14)=2^-82

Resultant(K!m, K!cInvariants(E)[1]);
Factorization(Integers()!Denominator(Resultant(K!m, K!cInvariants(E)[1])));
// res(m, c_4(m))=2^-32

Evaluate(-cInvariants(E)[2],0);
// we evaluate -c_6 in m=0 because m=0(mod p)
Factorization(Integers()!Denominator(Evaluate(-cInvariants(E)[2],1)));
```

```
// -c_6=2^-48
```

Special cases $u = -1, 0, 1, 3$:

```
u:=0;
A:=-(u^12+4*u^11-10*u^10-68*u^9+3*u^8+552*u^7+4*u^6-2568*u^5+2103*u^4
+1684*u^3+1958*u^2+396*u+37)/(48*(u^2+3)^3
*(u^6+4*u^5+13*u^4-40*u^3+19*u^2+36*u+31));
B:=(u^24+8*u^23+12*u^22-120*u^21-518*u^20+504*u^19
+5068*u^18+568*u^17-24009*u^16-15024*u^15+62936*u^14+183120*u^13-550452*u^12-851984*u^11
+4384056*u^10-3808912*u^9+1467519*u^8-4083672*u^7+3590300*u^6+5512360*u^5
+6945498*u^4+2943128*u^3+893052*u^2+120024*u+3753)/(864*(u^2+3)^6*(u^6
+4*u^5+13*u^4-40*u^3+19*u^2+36*u+31)^2);
E:=MinimalModel(EllipticCurve([A,B]));
CremonaReference(E);
LocalInformation(E);

u:=3;
A:=-(u^12+4*u^11-10*u^10-68*u^9+3*u^8+552*u^7+4*u^6-2568*u^5+2103*u^4
+1684*u^3+1958*u^2+396*u+37)/(48*(u^2+3)^3
*(u^6+4*u^5+13*u^4-40*u^3+19*u^2+36*u+31));
B:=(u^24+8*u^23+12*u^22-120*u^21-518*u^20+504*u^19
+5068*u^18+568*u^17-24009*u^16-15024*u^15+62936*u^14+183120*u^13-550452*u^12-851984*u^11
+4384056*u^10-3808912*u^9+1467519*u^8-4083672*u^7+3590300*u^6+5512360*u^5
+6945498*u^4+2943128*u^3+893052*u^2+120024*u+3753)/(864*(u^2+3)^6*(u^6
+4*u^5+13*u^4-40*u^3+19*u^2+36*u+31)^2);
E:=MinimalModel(EllipticCurve([A,B]));
CremonaReference(E);
LocalInformation(E);

u:=1;
A:=-(u^12+4*u^11-10*u^10-68*u^9+3*u^8+552*u^7+4*u^6-2568*u^5+2103*u^4
+1684*u^3+1958*u^2+396*u+37)/(48*(u^2+3)^3
*(u^6+4*u^5+13*u^4-40*u^3+19*u^2+36*u+31));
B:=(u^24+8*u^23+12*u^22-120*u^21-518*u^20+504*u^19
+5068*u^18+568*u^17-24009*u^16-15024*u^15+62936*u^14+183120*u^13-550452*u^12-851984*u^11
+4384056*u^10-3808912*u^9+1467519*u^8-4083672*u^7+3590300*u^6+5512360*u^5
```

```
+6945498*u^4+2943128*u^3+893052*u^2+120024*u+3753)/(864*(u^2+3)^6*(u^6
+4*u^5+13*u^4-40*u^3+19*u^2+36*u+31)^2);
E:=MinimalModel(EllipticCurve([A,B]));
// the curve is singular

u:=-1;
A:=-(u^12+4*u^11-10*u^10-68*u^9+3*u^8+552*u^7+4*u^6-2568*u^5+2103*u^4
+1684*u^3+1958*u^2+396*u+37)/(48*(u^2+3)^3
*(u^6+4*u^5+13*u^4-40*u^3+19*u^2+36*u+31));
B:=(u^24+8*u^23+12*u^22-120*u^21-518*u^20+504*u^19
+5068*u^18+568*u^17-24009*u^16-15024*u^15+62936*u^14+183120*u^13-550452*u^12-851984*u^11
+4384056*u^10-3808912*u^9+1467519*u^8-4083672*u^7+3590300*u^6+5512360*u^5
+6945498*u^4+2943128*u^3+893052*u^2+120024*u+3753)/(864*(u^2+3)^6*(u^6
+4*u^5+13*u^4-40*u^3+19*u^2+36*u+31)^2);
E:=MinimalModel(EllipticCurve([A,B]));
// the curve is singular
```

$ord_p(u-1) > 0$:

```
K<u>:=PolynomialRing(Rationals());

A:=-(u^12+4*u^11-10*u^10-68*u^9+3*u^8+552*u^7+4*u^6-2568*u^5+2103*u^4
+1684*u^3+1958*u^2+396*u+37)/(48*(u^2+3)^3
*(u^6+4*u^5+13*u^4-40*u^3+19*u^2+36*u+31));
B:=(u^24+8*u^23+12*u^22-120*u^21-518*u^20+504*u^19
+5068*u^18+568*u^17-24009*u^16-15024*u^15+62936*u^14+183120*u^13-550452*u^12-851984*u^11
+4384056*u^10-3808912*u^9+1467519*u^8-4083672*u^7+3590300*u^6+5512360*u^5
+6945498*u^4+2943128*u^3+893052*u^2+120024*u+3753)/(864*(u^2+3)^6*(u^6
+4*u^5+13*u^4-40*u^3+19*u^2+36*u+31)^2);
E:=MinimalModel(EllipticCurve([A,B]));

Factorization(K!Discriminant(E));
// gives the normalized factorization of the discriminant
Discriminant(E);
// we have to check this because the factorization is normalized and we
// want to see whether there are any leading coefficients

```

```
Factorization(K!cInvariants(E)[1]);
// gives the normalized factorization of the c_4-invariant
cInvariants(E)[1];
// we have to check this because the factorization is normalized and we
// want to see whether there are any leading coefficients

Factorization(Integers()!Resultant(K!(u+1), K!(Discriminant(E)/(u+1)^14)));
// res(u+1, Delta(u)/(u+1)^14)=2^82
Factorization(Integers()!Resultant(K!(u+1), K!cInvariants(E)[1]));
// res(u+1, c_4(u))=2^32

Evaluate(-cInvariants(E)[2],-1);
// we evaluate -c_6 in u=-1 because u=-1(mod p)
Factorization(Integers()!Evaluate(-cInvariants(E)[2],-1));
// -c_6=2^48
```

C.4. Code for Proposition 8.2.2

```
K<h>:=PolynomialRing(Rationals());
j:=(((h^3-2)^3)*((h^9-6*h^6-12*h^3-8)^3))/((h^9)*(h^3-8)*((h^3+1)^2));
// this is the parameterization of the j-invariants of
// curves that are non-cuspidal points on X0(18)

E:=MinimalModel(EllipticCurveFromjInvariant(j));
// we get an elliptic curve from j (up to a twist)
D:=Discriminant(E);
// this gives the discriminant of E
c4:=cInvariants(E)[1];
// this gives the c4-invariant of E

Factorization(K!D);
Factorization(K!c4);

Factorization(Integers()!Resultant(h+1, K!(D/(h+1)^2)));
// =3^34, the factorization of the resultant of the factor h+1 from
```

```
// the discriminant with the remaining factors
Factorization(Integers()!Resultant(h+1, K!c4));
// =3^12, the factorization of the resultant of the factor h+1 from
// the discriminant with c4-invariant




K<m>:=PolynomialRing(Rationals());
h:=(1-m)/m;
// this is the substitution m:=1/(h+1)
j:=(((h^3-2)^3)*((h^9-6*h^6-12*h^3-8)^3))/((h^9)*(h^3-8)*((h^3+1)^2));
// this is the parameterization of the j-invariants of curves
// that are non-cuspidal points on X0(18)

E:=MinimalModel(EllipticCurveFromjInvariant(j));
// we get an elliptic curve from j (up to a twist)
D:=Discriminant(E);
// this gives the discriminant of E
c4:=cInvariants(E)[1];
// this gives the c4-invariant of E

Factorization(K!D);
// we have to have in mind that this function gives the factorization
// where each irreducible factor is normalized, so to get the
//complete factorization we have to multiply what we get with 1/9 (in this case)
Factorization(K!c4);
// this was already normalized

// The factorizations of delta(m) and c_4(m) that we have in the proposition are
// after the change
 of variables x->x*3^(-6), y->y*3^(-9).
// We got the factorizations as delta(m)=3^36*D, c_4(m)=3^12*c4
// (see Table 3.1 in J. Silverman: The arithmetic of elliptic curves).

Resultant(m, K!(3^36*(D/m^18)));
// =1, the resultant of the factor m from the discriminant with the remaining factors
Resultant(m, K!(3^12*c4));
```

```
55 // =1, the resultant of the factor m from the discriminant with the c4-invariant
56
57
58
59 K<t>:=PolynomialRing(Rationals());
60 h:=t-1;
61 // here we put +/-3^k-1 instead of h, with t being t=+/-3^k
62 j:=(((h^3-2)^3)*((h^9-6*h^6-12*h^3-8)^3))/((h^9)*(h^3-8)*((h^3+1)^2));
63 // this is the parameterization of the j-invariants of
64 // curves that are non-cuspidal points on X0(18)
65
66 E:=MinimalModel(EllipticCurveFromjInvariant(j));
67 // we get an elliptic curve from j (up to a twist)
68 D:=Discriminant(E);
69 // this gives the discriminant of E
70 c4:=cInvariants(E)[1];
71 // this gives the c4-invariant of E
72
73 Factorization(K!D);
74 // we get the factorization with a variable t, but t represents t=+/-3^k so
75 // now we can count multiplicities of 3 in the discriminant,
76 // we do the same thing for the c4-invariant
77 Factorization(K!c4);
78
79 // We can count the multiplicities of 3 in delta(t) and c_4(t) that we
80 // have in the proposition after the change of variables x->x*3^6, y->y*3^9 having
81 // in mind that delta(t)=3^(-36)*D, c_4(t)=3^(-12)*c4
82 // (see Table 3.1 in J. Silverman: The arithmetic of elliptic curves).
83
84
85
86 // below is the code used for specific h in the proof
87
88
89 h:=1;
90 j:=(((h^3-2)^3)*((h^9-6*h^6-12*h^3-8)^3))/((h^9)*(h^3-8)*((h^3+1)^2));
91 // this is the parameterization of the j-invariants of curves
```

```
92  // that are non-cuspidal points on X0(18)
93  E:=MinimalModel(EllipticCurveFromjInvariant(j));
94  IsQuadraticTwist(E, EllipticCurve("14A4"));
95  // here we see that E is really a twist of 14a4 and we get d such
96  // that E^d is the curve 14a4 (this we use in the next row)
97  LocalInformation(QuadraticTwist(E, 253));
98  // this function gives us primes of bad reduction and their
99  // reduction types and Tamagawa numbers
100
101 LocalInformation(QuadraticTwist(EllipticCurve("14A4"), -1));
102 // the next 7 lines are examining the properties of Tamagawa
103 // numbers at p=2 of the curve 14a4 under twisting
104 LocalInformation(QuadraticTwist(EllipticCurve("14A4"), 2));
105 LocalInformation(QuadraticTwist(EllipticCurve("14A4"), 5));
106 LocalInformation(QuadraticTwist(EllipticCurve("14A4"), -2));
107 LocalInformation(QuadraticTwist(EllipticCurve("14A4"), -5));
108 LocalInformation(QuadraticTwist(EllipticCurve("14A4"), 10));
109 LocalInformation(QuadraticTwist(EllipticCurve("14A4"), -10));
110
111
112 h:=-2;
113 j:=(((h^3-2)^3)*((h^9-6*h^6-12*h^3-8)^3))/((h^9)*(h^3-8)*((h^3+1)^2));
114 // this is the parameterization of the j-invariants of curves
115 // that are non-cuspidal points on X0(18)
116 E:=MinimalModel(EllipticCurveFromjInvariant(j));
117 IsQuadraticTwist(E, EllipticCurve("14A6"));
118 // here we see that E is really a twist of 14a6 and we get d such
119 // that E^d is the curve 14a6 (this we use in the next row)
120 LocalInformation(QuadraticTwist(E, 5727205));
121 // this function gives us primes of bad reduction and their
122 // reduction types and Tamagawa numbers
123
124 LocalInformation(QuadraticTwist(EllipticCurve("14A6"), -1));
125 // the next 7 lines are examining the properties of Tamagawa
126 // numbers at p=2 of the curve 14a6 under twisting
127 LocalInformation(QuadraticTwist(EllipticCurve("14A6"), 2));
128 LocalInformation(QuadraticTwist(EllipticCurve("14A6"), 5));
```

```
129 LocalInformation(QuadraticTwist(EllipticCurve("14A6"), -2));
130 LocalInformation(QuadraticTwist(EllipticCurve("14A6"), -5));
131 LocalInformation(QuadraticTwist(EllipticCurve("14A6"), 10));
132 LocalInformation(QuadraticTwist(EllipticCurve("14A6"), -10));
133
134
135 h:=-4;
136 j:=(((h^3-2)^3)*((h^9-6*h^6-12*h^3-8)^3))/((h^9)*(h^3-8)*((h^3+1)^2));
137 // this is the parameterization of the j-invariants of curves
138 // that are non-cuspidal points on X0(18)
139 E:=MinimalModel(EllipticCurveFromjInvariant(j));
140 IsQuadraticTwist(E, EllipticCurve("14A5"));
141 // here we see that E is really a twist of 14a5 and we get d
142 // such that E^d is the curve 14a5 (this we use in the next row)
143 LocalInformation(QuadraticTwist(E, -6218946567515));
144 // this function gives us primes of bad reduction and their
145 // reduction types and Tamagawa numbers
146
147 LocalInformation(QuadraticTwist(EllipticCurve("14A5"), -1));
148 // the next 7 lines are examining the properties of Tamagawa
149 // numbers at p=2 of the curve 14a5 under twisting
150 LocalInformation(QuadraticTwist(EllipticCurve("14A5"), 2));
151 LocalInformation(QuadraticTwist(EllipticCurve("14A5"), 5));
152 LocalInformation(QuadraticTwist(EllipticCurve("14A5"), -2));
153 LocalInformation(QuadraticTwist(EllipticCurve("14A5"), -5));
154 LocalInformation(QuadraticTwist(EllipticCurve("14A5"), 10));
155 LocalInformation(QuadraticTwist(EllipticCurve("14A5"), -10));
156
157
158 h:=1/2;
159 j:=(((h^3-2)^3)*((h^9-6*h^6-12*h^3-8)^3))/((h^9)*(h^3-8)*((h^3+1)^2));
160 // this is the parameterization of the j-invariants of
161 // curves that are non-cuspidal points on X0(18)
162 E:=MinimalModel(EllipticCurveFromjInvariant(j));
163 IsQuadraticTwist(E, EllipticCurve("14A3"));
164 // here we see that E is really a twist of 14a3 and we get d such
165 // that E^d is the curve 14a3 (this we use in the next row)
```

```
166
167 LocalInformation(QuadraticTwist(E, -6078532955));
168 // this function gives us primes of bad reduction and their
169 // reduction types and Tamagawa numbers
170 LocalInformation(QuadraticTwist(EllipticCurve("14A3"), -1));
171 // the next 7 lines are examining the properties of Tamagawa
172 // numbers at p=2 of the curve 14a3 under twisting
173 LocalInformation(QuadraticTwist(EllipticCurve("14A3"), 2));
174 LocalInformation(QuadraticTwist(EllipticCurve("14A3"), 5));
175 LocalInformation(QuadraticTwist(EllipticCurve("14A3"), -2));
176 LocalInformation(QuadraticTwist(EllipticCurve("14A3"), -5));
177 LocalInformation(QuadraticTwist(EllipticCurve("14A3"), 10));
178 LocalInformation(QuadraticTwist(EllipticCurve("14A3"), -10));
179
180
181 h:=-5/2;
182 j:=(((h^3-2)^3)*((h^9-6*h^6-12*h^3-8)^3))/((h^9)*(h^3-8)*((h^3+1)^2));
183 // this is the parameterization of the j-invariants of curves
184 // that are non-cuspidal points on X0(18)
185 E:=MinimalModel(EllipticCurveFromjInvariant(j));
186 LocalInformation(E);
187 // this function gives us primes of bad reduction and their
188 // reduction types and Tamagawa numbers, where we see that we already
189 // have 2 primes (2 and 13) of multiplicative reduction with reduction type I_2k
```

C.5. Code for Proposition 8.2.3

```
1 K<h>:=PolynomialRing(Rationals());
2 j:=((h^6-4*h^5+16*h+16)^3)/(((h+1)^2)*(h-4)*(h^5));
3 // this is the parameterization of the j-invariants of
4 // curves that are non-cuspidal points on X0(10)
5
6 E:=MinimalModel(EllipticCurveFromjInvariant(j));
7 // we get an elliptic curve from j (up to a twist)
8 D:=Discriminant(E);
```

```
// this gives the discriminant of E
c4:=cInvariants(E)[1];
// this gives the c4-invariant of E

Factorization(K!D);
Factorization(K!c4);

Factorization(Integers()!Resultant(h+1, K!(D/(h+1)^2)));
// =5^22, the factorization of the resultant of the factor
// h+1 from the discriminant with the remaining factors
Factorization(Integers()!Resultant(h+1, K!c4));
// =5^8, the factorization of the resultant of the factor
// h+1 from the discriminant with c4-invariant




K<t>:=PolynomialRing(Rationals());
h:=t-1;
// here we put +/-5^k-1 instead of h, with t being t=+/-5^k
j:=((h^6-4*h^5+16*h+16)^3)/(((h+1)^2)*(h-4)*(h^5));
// this is the parameterization of the j-invariants of
// curves that are non-cuspidal points on X0(10)

E:=MinimalModel(EllipticCurveFromjInvariant(j));
// we get an elliptic curve from j (up to a twist)
D:=Discriminant(E);
// this gives the discriminant of E
c4:=cInvariants(E)[1];
// this gives the c4-invariant of E

Factorization(K!D);
// we get the factorization with a variable t, but t represents
// t=+/-5^k so now we can count multiplicities of 5
// in the discriminant, we do the same thing for the c4-invariant
Factorization(K!c4);

// We can count the multiplicities of 5 in delta(t) and c_4(t)
```

```
// that we have after the change of variables x->x*5^4, y->y*5^6
// having in mind that delta(t)=5^(-24)*D, c_4(t)=5^(-8)*c4
// (see Table 3.1 in J. Silverman: The arithmetic of elliptic curves).



// below is the code used for specific h in the proof


h:=-6;
j:=((h^6-4*h^5+16*h+16)^3)/(((h+1)^2)*(h-4)*(h^5));
// this is the parameterization of the j-invariants of
// curves that are non-cuspidal points on X0(10)
E:=MinimalModel(EllipticCurveFromjInvariant(j));
IsQuadraticTwist(E, EllipticCurve("768D3"));
// here we see that E is really a twist of 768d3 and we get d
// such that E^d is the curve 768d3 (this we use in the next row)
LocalInformation(QuadraticTwist(E, -41549090));
// this function gives us primes of bad reduction and
// their reduction types and Tamagawa numbers

LocalInformation(QuadraticTwist(EllipticCurve("768D3"), -1));
// the next 7 lines are examining the properties of Tamagawa
// numbers at p=2 of the curve 768d3 under twisting
LocalInformation(QuadraticTwist(EllipticCurve("768D3"), 2));
LocalInformation(QuadraticTwist(EllipticCurve("768D3"), 5));
LocalInformation(QuadraticTwist(EllipticCurve("768D3"), -2));
LocalInformation(QuadraticTwist(EllipticCurve("768D3"), -5));
LocalInformation(QuadraticTwist(EllipticCurve("768D3"), 10));
LocalInformation(QuadraticTwist(EllipticCurve("768D3"), -10));


h:=-2;
j:=((h^6-4*h^5+16*h+16)^3)/(((h+1)^2)*(h-4)*(h^5));
// this is the parameterization of the j-invariants of
// curves that are non-cuspidal points on X0(10)
E:=MinimalModel(EllipticCurveFromjInvariant(j));
```

```
IsQuadraticTwist(E, EllipticCurve("768D1"));
// here we see that E is really a twist of 768d1 and we get d
// such that E^d is the curve 768d1 (this we use in the next row)
LocalInformation(QuadraticTwist(E, 22));
// this function gives us primes of bad reduction and their
// reduction types and Tamagawa numbers

LocalInformation(QuadraticTwist(EllipticCurve("768D1"), -1));
// the next 7 lines are examining the properties of Tamagawa
// numbers at p=2 of the curve 768d1 under twisting
LocalInformation(QuadraticTwist(EllipticCurve("768D1"), 2));
LocalInformation(QuadraticTwist(EllipticCurve("768D1"), 5));
LocalInformation(QuadraticTwist(EllipticCurve("768D1"), -2));
LocalInformation(QuadraticTwist(EllipticCurve("768D1"), -5));
LocalInformation(QuadraticTwist(EllipticCurve("768D1"), 10));
LocalInformation(QuadraticTwist(EllipticCurve("768D1"), -10));



K<m>:=PolynomialRing(Rationals());
h:=(1-m)/m;
// this is the substitution m:=1/(h+1)
j:=((h^6-4*h^5+16*h+16)^3)/(((h+1)^2)*(h-4)*(h^5));
// this is the parameterization of the j-invariants of
// curves that are non-cuspidal points on X0(10)

E:=MinimalModel(EllipticCurveFromjInvariant(j));
// we get an elliptic curve from j (up to a twist)
D:=Discriminant(E);
// this gives the discriminant of E
c4:=cInvariants(E)[1];
// this gives the c4-invariant of E

Factorization(K!D);
// we have to have in mind that this function gives the
// factorization where each irreducible factor is normalized, so
// to get the complete factorization we have to multiply
```

```
120 //what we get with 1/25 (in this case)
121 Factorization(K!c4);
122 // this was already normalized
123
124 // The factorizations of delta(m) and c_4(m) that we have
125 // after the change of variables x->x*5^(-4), y->y*5^(-6).
126 // We got the factorizations as delta(m)=5^24*D, c_4(m)=5^8*c4
127 // (see Table 3.1 in J. Silverman: The arithmetic of elliptic curves).
128
129 Resultant(m, K!(5^24*(D/m^10)));
130 // =1, the resultant of the factor m from the discriminant with the remaining factors
131 Resultant(m, K!(5^8*c4));
132 // =1, the resultant of the factor m from the discriminant with the c4-invariant
```

C.6. Code for Proposition 8.2.4

```
1  K<h>:=PolynomialRing(Rationals());
2  j:=((h^4-16*h^2+16)^3)/((h^2-16)*h^2);
3  // this is the parameterization of the j-invariants of
4  // curves that are non-cuspidal points on X0(8)
5
6  E:=MinimalModel(EllipticCurveFromjInvariant(j));
7  // we get an elliptic curve from j (up to a twist)
8  D:=Discriminant(E)
9  // this gives the discriminant of E
10 c4:=cInvariants(E)[1];
11 // this gives the c4-invariant of E
12
13 Factorization(K!D);
14 Factorization(K!c4);
15
16 Factorization(Integers()!Resultant(h, K!(D/(h^2))));
17 // =2^64, the factorization of the resultant of the factor
18 // h from the discriminant with the remaining factors
19 Factorization(Integers()!Resultant(h, K!c4));
```

```
// =2^24, the factorization of the resultant of the factor
// h from the discriminant with c4-invariant




K<h>:=PolynomialRing(Rationals());
// here we are thinking of h as +/-2^k
j:=((h^4-16*h^2+16)^3)/((h^2-16)*h^2);
// this is the parameterization of the j-invariants of
// curves that are non-cuspidal points on X0(8)

E:=MinimalModel(EllipticCurveFromjInvariant(j));
// we get an elliptic curve from j (up to a twist)
D:=Discriminant(E);
// this gives the discriminant of E
c4:=cInvariants(E)[1];
// this gives the c4-invariant of E

Factorization(K!D);
// we get the factorization with a variable h, but h represents
// h=+/-2^k so now we can count multiplicities of 2 in
//the discriminant, we do the same thing for the c4-invariant
Factorization(K!c4);

// We can count the multiplicities of 2 in delta(t) and c_4(t) that we
// have in the proposition after the change of variables x->x*2^12, y->y*2^18
// having in mind that delta(t)=2^(-72)*D, c_4(t)=2^(-24)*c4
// (see Table 3.1 in J. Silverman: The arithmetic of elliptic curves).




// below is the code used for specific h in the proof


h:=-1;
// it is clear from the j-invariant that we
// will get the same curve for h=1 and h=-1
```

```
57 j:=((h^4-16*h^2+16)^3)/((h^2-16)*h^2);
58 // this is the parameterization of the j-invariants of
59 // curves that are non-cuspidal points on X0(8)
60 E:=MinimalModel(EllipticCurveFromjInvariant(j));
61 IsQuadraticTwist(E, EllipticCurve("15A8"));
62 // here we see that E is really a twist of 15a8 and we get d
63 // such that E^d is the curve 15a8 (this we use in the next row)
64 LocalInformation(QuadraticTwist(E, 161));
65 // this function gives us primes of bad reduction
66 // and their reduction types and Tamagawa numbers
67
68 LocalInformation(QuadraticTwist(EllipticCurve("15A8"), -1));
69 // the next 7 lines are examining the properties of Tamagawa
70 // numbers at p=2 of the curve 15a8 under twisting
71 LocalInformation(QuadraticTwist(EllipticCurve("15A8"), 2));
72 LocalInformation(QuadraticTwist(EllipticCurve("15A8"), 5));
73 LocalInformation(QuadraticTwist(EllipticCurve("15A8"), -2));
74 LocalInformation(QuadraticTwist(EllipticCurve("15A8"), -5));
75 LocalInformation(QuadraticTwist(EllipticCurve("15A8"), 10));
76 LocalInformation(QuadraticTwist(EllipticCurve("15A8"), -10));
77
78
79 h:=-2;
80 // it is clear from the j-invariant that we
81 // will get the same curve for h=2 and h=-2
82 j:=((h^4-16*h^2+16)^3)/((h^2-16)*h^2);
83 // this is the parameterization of the j-invariants of
84 // curves that are non-cuspidal points on X0(8)
85 E:=MinimalModel(EllipticCurveFromjInvariant(j));
86 IsQuadraticTwist(E, EllipticCurve("48A4"));
87 // here we see that E is really a twist of 48a4 and we get d
88 // such that E^d is the curve 48a4 (this we use in the next row)
89 LocalInformation(QuadraticTwist(E, 7));
90 // this function gives us primes of bad reduction
91 // and their reduction types and Tamagawa numbers
92
93 LocalInformation(QuadraticTwist(EllipticCurve("48A4"), -1));
```

```
94  // the next 7 lines are examining the properties of Tamagawa
95  // numbers at p=2 of the curve 48a4 under twisting
96  LocalInformation(QuadraticTwist(EllipticCurve("48A4"), 2));
97  LocalInformation(QuadraticTwist(EllipticCurve("48A4"), 5));
98  LocalInformation(QuadraticTwist(EllipticCurve("48A4"), -2));
99  LocalInformation(QuadraticTwist(EllipticCurve("48A4"), -5));
100 LocalInformation(QuadraticTwist(EllipticCurve("48A4"), 10));
101 LocalInformation(QuadraticTwist(EllipticCurve("48A4"), -10));
102
103
104 h:=-8;
105 // it is clear from the j-invariant that we
106 // will get the same curve for h=8 and h=-8
107 j:=((h^4-16*h^2+16)^3)/((h^2-16)*h^2);
108 // this is the parameterization of the j-invariants of
109 // curves that are non-cuspidal points on X0(8)
110 E:=MinimalModel(EllipticCurveFromjInvariant(j));
111 IsQuadraticTwist(E, EllipticCurve("24A3"));
112 // here we see that E is really a twist of 24a3 and we get d
113 // such that E^d is the curve 24a3 (this we use in the next row)
114 LocalInformation(QuadraticTwist(E, 517433));
115 // this function gives us primes of bad reduction and
116 // their reduction types and Tamagawa numbers
117
118 LocalInformation(QuadraticTwist(EllipticCurve("24A3"), -1));
119 // the next 7 lines are examining the properties of Tamagawa
120 // numbers at p=2 of the curve 24a3 under twisting
121 LocalInformation(QuadraticTwist(EllipticCurve("24A3"), 2));
122 LocalInformation(QuadraticTwist(EllipticCurve("24A3"), 5));
123 LocalInformation(QuadraticTwist(EllipticCurve("24A3"), -2));
124 LocalInformation(QuadraticTwist(EllipticCurve("24A3"), -5));
125 LocalInformation(QuadraticTwist(EllipticCurve("24A3"), 10));
126 LocalInformation(QuadraticTwist(EllipticCurve("24A3"), -10));
127
128
129 h:=-16;
130 // it is clear from the j-invariant that we
```

```
131 // will get the same curve for h=16 and h=-16
132 j:=((h^4-16*h^2+16)^3)/((h^2-16)*h^2);
133 // this is the parameterization of the j-invariants of
134 // curves that are non-cuspidal points on X0(8)
135 E:=MinimalModel(EllipticCurveFromjInvariant(j));
136 IsQuadraticTwist(E, EllipticCurve("15A7"));
137 // here we see that E is really a twist of 15a7 and we get d
138 // such that E^d is the curve 15a7 (this we use in the next row)
139 LocalInformation(QuadraticTwist(E, 914346209));
140 // this function gives us primes of bad reduction and their
141 // reduction types and Tamagawa numbers
142
143 LocalInformation(QuadraticTwist(EllipticCurve("15A7"), -1));
144 // the next 7 lines are examining the properties of Tamagawa
145 // numbers at p=2 of the curve 15a7 under twisting
146 LocalInformation(QuadraticTwist(EllipticCurve("15A7"), 2));
147 LocalInformation(QuadraticTwist(EllipticCurve("15A7"), 5));
148 LocalInformation(QuadraticTwist(EllipticCurve("15A7"), -2));
149 LocalInformation(QuadraticTwist(EllipticCurve("15A7"), -5));
150 LocalInformation(QuadraticTwist(EllipticCurve("15A7"), 10));
151 LocalInformation(QuadraticTwist(EllipticCurve("15A7"), -10));
152
153
154
155 K<m>:=PolynomialRing(Rationals());
156 h:=1/m;
157 // this is the substitution m:=1/h
158 j:=((h^4-16*h^2+16)^3)/((h^2-16)*h^2);
159 // this is the parameterization of the j-invariants of
160 // curves that are non-cuspidal points on X0(8)
161
162 E:=MinimalModel(EllipticCurveFromjInvariant(j));
163 // we get an elliptic curve from j (up to a twist)
164 D:=Discriminant(E);
165 // this gives the discriminant of E
166 c4:=cInvariants(E)[1];
167 // this gives the c4-invariant of E
```

```
168
169 Factorization(K!D);
170 // we have to have in mind that this function gives the
171 // factorization where each irreducible factor is normalized,
172 // so to get the complete factorization we have to multiply
173 // what we get with -1/256 (in this case)
174 Factorization(K!c4);
175 // this was already normalized
176
177 // The factorizations of delta(m) and c_4(m) that we have
178 // in the proposition are after the change of variables x->x*2^(-12), y->y*2^(-18).
179 // We got the factorizations as delta(m)=2^72*D, c_4(m)=2^24*c4
180 // (see Table 3.1 in J. Silverman: The arithmetic of elliptic curves).
181
182 Resultant(m, K!(2^72*(D/m^8)));
183 // =1, the resultant of the factor m from the
184 // discriminant with the remaining factors
185 Resultant(m, K!(2^24*c4));
186 // =1, the resultant of the factor m from the
187 // discriminant with the c4-invariant
```

C.7. Code for Proposition 8.2.5

```
1  K<h>:=PolynomialRing(Rationals());
2  j:=(((h+6)^3)*((h^3+18*h^2+84*h+24)^3))/(h*((h+8)^3)*((h+9)^2));
3  // this is the parameterization of the j-invariants of
4  // curves that are non-cuspidal points on X0(6)
5
6  E:=MinimalModel(EllipticCurveFromjInvariant(j));
7  // we get an elliptic curve from j (up to a twist)
8  D:=Discriminant(E);
9  // this gives the discriminant of E
10 c4:=cInvariants(E)[1];
11 // this gives the c4-invariant of E
12
```

```
Factorization(K!D);
Factorization(K!c4);

Factorization(Integers()!Resultant(h+9, K!(D/(h+9)^2)));
// =3^32, the factorization of the resultant of the factor
// h+9 from the discriminant with the remaining factors
Factorization(Integers()!Resultant(h+9, K!c4));
// =3^12, the factorization of the resultant of the factor
// h+9 from the discriminant with c4-invariant




K<t>:=PolynomialRing(Rationals());
h:=t-9;
// here we put +/-3^k-9 instead of h, with t being t=+/-3^k
j:=(((h+6)^3)*((h^3+18*h^2+84*h+24)^3))/(h*((h+8)^3)*((h+9)^2));
// this is the parameterization of the j-invariants of
// curves that are non-cuspidal points on X0(6)

E:=MinimalModel(EllipticCurveFromjInvariant(j));
// we get an elliptic curve from j (up to a twist)
D:=Discriminant(E);
// this gives the discriminant of E
c4:=cInvariants(E)[1];
// this gives the c4-invariant of E

Factorization(K!D);
// we get the factorization with a variable h, but h represents
// h=+/-3^k so now we can count multiplicities of 3 in the
// discriminant, we do the same thing for the c4-invariant
Factorization(K!c4);

// We can count the multiplicities of 3 in delta(t) and c_4(t) that we have
// in the proposition after the change of variables x->x*3^6,
// y->y*3^9 having in mind that delta(t)=3^(-36)*D, c_4(t)=3^(-12)*c4
// (see Table 3.1 in J. Silverman: The arithmetic of elliptic curves).

```

```
50
51
52  // below is the code used for specific h in the proof
53
54
55  h:=-10;
56  j:=(((h+6)^3)*((h^3+18*h^2+84*h+24)^3))/(h*((h+8)^3)*((h+9)^2));
57  // this is the parameterization of the j-invariants of
58  // curves that are non-cuspidal points on X0(6)
59  E:=MinimalModel(EllipticCurveFromjInvariant(j));
60  IsQuadraticTwist(E, EllipticCurve("20A2"));
61  // here we see that E is really a twist of 20a2 and we get d
62  // such that E^d is the curve 20a2 (this we use in the next row)
63  LocalInformation(QuadraticTwist(E, 22));
64  // this function gives us primes of bad reduction and
65  // their reduction types and Tamagawa numbers
66
67  LocalInformation(QuadraticTwist(EllipticCurve("20A2"), -1));
68  // the next 7 lines are examining the properties of Tamagawa
69  // numbers at p=2 of the curve 20a2 under twisting
70  CremonaReference(QuadraticTwist(EllipticCurve("20A2"), -1));
71  // in the line above we got that c_E=1, so we want to see which curve is that
72  LocalInformation(QuadraticTwist(EllipticCurve("20A2"), 2));
73  LocalInformation(QuadraticTwist(EllipticCurve("20A2"), 5));
74  LocalInformation(QuadraticTwist(EllipticCurve("20A2"), -2));
75  LocalInformation(QuadraticTwist(EllipticCurve("20A2"), -5));
76  LocalInformation(QuadraticTwist(EllipticCurve("20A2"), 10));
77  LocalInformation(QuadraticTwist(EllipticCurve("20A2"), -10));
78
79
80  h:=-12;
81  j:=(((h+6)^3)*((h^3+18*h^2+84*h+24)^3))/(h*((h+8)^3)*((h+9)^2));
82  // this is the parameterization of the j-invariants of
83  // curves that are non-cuspidal points on X0(6)
84  E:=MinimalModel(EllipticCurveFromjInvariant(j));
85  IsQuadraticTwist(E, EllipticCurve("36A2"));
86  // here we see that E is really a twist of 36a2 and we get d
```

```
87  // such that E^d is the curve 36a2 (this we use in the next row)
88  LocalInformation(QuadraticTwist(E, 165));
89  // this function gives us primes of bad reduction and
90  // their reduction types and Tamagawa numbers
91
92
93  h:=-6;
94  j:=(((h+6)^3)*((h^3+18*h^2+84*h+24)^3))/(h*((h+8)^3)*((h+9)^2));
95  // this is the parameterization of the j-invariants of
96  // curves that are non-cuspidal points on X0(6)
97  E:=MinimalModel(EllipticCurveFromjInvariant(j));
98  IsQuadraticTwist(E, EllipticCurve("27A3"));
99  // here we see that E is really the curve 27a3
100 LocalInformation(E);
101 // this function gives us primes of bad reduction and
102 // their reduction types and Tamagawa numbers
103
104
105 h:=-18;
106 j:=(((h+6)^3)*((h^3+18*h^2+84*h+24)^3))/(h*((h+8)^3)*((h+9)^2));
107 // this is the parameterization of the j-invariants of
108 // curves that are non-cuspidal points on X0(6)
109 E:=MinimalModel(EllipticCurveFromjInvariant(j));
110 IsQuadraticTwist(E, EllipticCurve("80B4"));
111 // here we see that E is really a twist of 80b4 and we get d
112 // such that E^d is the curve 80b4 (this we use in the next row)
113 LocalInformation(QuadraticTwist(E, 171182));
114 // this function gives us primes of bad reduction and
115 // their reduction types and Tamagawa numbers
116
117
118
119 K<m>:=PolynomialRing(Rationals());
120 h:=(1-9*m)/m;
121 // this is the substitution m:=1/(h+9)
122 j:=(((h+6)^3)*((h^3+18*h^2+84*h+24)^3))/(h*((h+8)^3)*((h+9)^2));
123 // this is the parameterization of the j-invariants of
```

```
124 // curves that are non-cuspidal points on X0(6)
125
126 E:=MinimalModel(EllipticCurveFromjInvariant(j));
127 // we get an elliptic curve from j (up to a twist)
128 D:=Discriminant(E);
129 // this gives the discriminant of E
130 c4:=cInvariants(E)[1];
131 // this gives the c4-invariant of E
132
133 Factorization(K!D);
134 // we have to have in mind that this function gives the factorization
135 // where each irreducible factor is normalized, so to get the complete
136 // factorization we have to multiply what we get with 1/81 (in this case)
137 Factorization(K!c4);
138 // this was already normalized
139
140 // The factorizations of delta(m) and c_4(m) that we have in
141 // the proposition are after the change of variables x->x*3^(-6), y->y*3^(-9).
142 // We got the factorizations as delta(m)=3^36*D, c_4(m)=3^12*c4
143 // (see Table 3.1 in J. Silverman: The arithmetic of elliptic curves).
144
145 Resultant(m, K!(3^36*(D/m^6)));
146 // =1, the resultant of the factor m from the discriminant with the remaining factors
147 Resultant(m, K!(3^12*c4));
148 // =1, the resultant of the factor m from the discriminant with the c4-invariant
```

C.8. Code for Proposition 8.2.6

$N = 14$:

```
1 j:=-3^3*5^3;
2 E:=EllipticCurveFromjInvariant(j);
3 E:=QuadraticTwist(E,-5*7);
4 // we are twisting by -5*7 to get a curve with the least conductor
5 CremonaReference(E);
6 // we get the curve 49a1
7 LocalInformation(E);
8 // we have reduction type III at p=7
```

```
9
10 j:=3^3*5^3*17^3;
11 E:=EllipticCurveFromjInvariant(j);
12 E:=QuadraticTwist(E,-3*5*7*17*19);
13 // we are twisting by -3*5*7*17*19 to get a curve with the least conductor
14 CremonaReference(E);
15 // we get the curve 49a2
16 LocalInformation(E);
17 // we have reduction type III at p=7
```

$N = 17$:

```
1  j:=-(17^2*101^3)/2;
2  E:=EllipticCurveFromjInvariant(j);
3  E:=QuadraticTwist(E,5*101*7717);
4  // we are twisting by 5*101*7717 to get a curve with the least conductor
5  CremonaReference(E);
6  // we get the curve 14450p1
7  LocalInformation(E);
8  // we have reduction type III at p=5
9
10 j:=-(17*373^3)/2^17;
11 E:=EllipticCurveFromjInvariant(j);
12 E:=QuadraticTwist(E,-5*17*373*14891);
13 // we are twisting by -5*17*373*14891 to get a curve with the least conductor
14 CremonaReference(E);
15 // we get the curve 14450p2
16 LocalInformation(E);
17 // we have reduction type III at p=5
```

$N = 19$:

```
1 j:=-2^15*3^3;
2 E:=EllipticCurveFromjInvariant(j);
3 E:=QuadraticTwist(E,19);
4 // we are twisting by 19 to get a curve with the least conductor
5 CremonaReference(E);
```

```
// we get the curve 361a1
LocalInformation(E);
// we have reduction type III at p=19
```

$N = 37$:

```
j:=-7*11^3;
E:=EllipticCurveFromjInvariant(j);
E:=QuadraticTwist(E,5*11*47);
// we are twisting by 5*11*47 to get a curve with the least conductor
CremonaReference(E);
// we get the curve 1225h1
LocalInformation(E);
// we have reduction type III at p=5

j:=-7*137^3*2083^3;
E:=EllipticCurveFromjInvariant(j);
E:=QuadraticTwist(E,-5*11*137*1433*2083*11443);
// we are twisting by -5*11*137*1433*2083*11443 to get a curve with the least conductor
CremonaReference(E);
// we get the curve 1225h2
LocalInformation(E);
// we have reduction type III at p=5
```

$N = 43$:

```
j:=-2^18*3^3*5^3;
E:=EllipticCurveFromjInvariant(j);
E:=QuadraticTwist(E,-2*3*5*7*43);
// we are twisting by -2*3*5*7*43 to get a curve with the least conductor
CremonaReference(E);
// we get the curve 1849a1
LocalInformation(E);
// we have reduction type III at p=43
```

$N = 67$:

```
1 j:=-2^15*3^3*5^3*11^3;
2 E:=EllipticCurveFromjInvariant(j);
3 E:=QuadraticTwist(E,5*7*11*31*67);
4 // we are twisting by 5*7*11*31*67 to get a curve with the least conductor
5 CremonaReference(E);
6 // we get the curve 4489a1
7 LocalInformation(E);
8 // we have reduction type III at p=67
```

$N = 163$:

```
1 j:=-2^18*3^3*5^3*23^3*29^3;
2 E:=EllipticCurveFromjInvariant(j);
3 E:=QuadraticTwist(E,2*5*7*11*19*23*29*127*163);
4 // we are twisting by 2*5*7*11*19*23*29*127*163 to get a curve with the least conductor
5 CremonaReference(E);
6 // we get the curve 26569a1
7 LocalInformation(E);
8 // we have reduction type III at p=163
```

CONCLUSION

In this thesis we have three main chapters, one about torsion subgroups of elliptic curves over quadratic fields, the second about splitting of primes in number fields generated by points on some modular curves, and the third about Tamagawa numbers of elliptic curves with prescribed torsion subgroup or isogeny. Those are Chapters 6, 7 and 8, respectively. In this conclusion we will give an overview of the original results obtained in papers [39, 46, 47] that the mentioned chapters were based upon.

In Chapter 6 we gave the classification of torsion subgroups of elliptic curves over quadratic fields $\mathbb{Q}(\sqrt{d})$, where $0 < d < 100$ is squarefree. The result is given in Table 6.1. We obtained a complete classification for 49 out of 60 such fields. Over the remaining 11 quadratic fields, we could not rule out the possibility of the group $\mathbb{Z}/16\mathbb{Z}$ appearing as the torsion group of an elliptic curve, since we were unable to compute the rank of $X_1(16)$ over the corresponding quadratic field. We presented the methods that we used in detail in the proof of Theorem 6.2.11.

In Chapter 7 we studied the splitting of primes in number fields generated by points on some modular curves. We proved results about the splitting behaviour of primes in quadratic fields generated by points on modular curves $X_0(n)$ which are hyperelliptic (except for $n = 37$) and those results are listed in Theorems 7.1.1 and 7.1.10. We were also able to prove some results about the splitting of primes in cubic fields generated by points on $X_1(2,14)$. It turns out that 2 always splits in such fields, and rational primes $p \equiv \pm 1 \pmod 7$ of multiplicative reduction also split (see Proposition 7.2.7). There was also a mention, in Proposition 7.2.3, of the fact that elliptic curves over cubic fields with torsion $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/14\mathbb{Z}$ have multiplicative reduction of type I_{14k} at prime 2. That result was expanded upon in the subsequent chapter, in Proposition 8.1.2, which says that the reduction at 2 is split multiplicative.

In Chapter 8 we studied the Tamagawa numbers of elliptic curves with torsion $\mathbb{Z}/2\mathbb{Z}\oplus\mathbb{Z}/14\mathbb{Z}$ and of elliptic curves with an $n-$isogeny, for

$$n \in \{6,8,10,12,14,16,17,18,19,37,43,67,163\}.$$

We found in Proposition 8.1.4 that Tamagawa numbers of elliptic curves with torsion $\mathbb{Z}/2\mathbb{Z}\oplus\mathbb{Z}/14\mathbb{Z}$ are always divisible by 14^2, with factors 14 coming from rational primes with split multiplicative reduction of type I_{14k}, one of which is always $p=2$ (see Proposition 8.1.2). The only exception is the curve 1922c1, with $c_E = c_2 = 14$. As for $n-$isogenies, Tamagawa numbers of elliptic curves with an $18-$isogeny must be divisible by 4 (Proposition 8.2.2), while elliptic curves with an $n-$isogeny for the remaining n from the mentioned set must have Tamagawa numbers divisible by 2 (see Propositions 8.2.3, 8.2.4, 8.2.5 and 8.2.6), except for finite sets of specified curves.

BIBLIOGRAPHY

[1] H. Baaziz, *Equations for the modular curve $X_1(N)$ and models of elliptic curves with torsion points*, Math. Comp. **79** (2010), 2371–2386. ↑ 28.

[2] W. Bosma, J. Cannon and C. Playoust: *The Magma Algebra System I: The User Language*, J. Symb. Comp. **24** (1997), 235–265. ↑ iii, vi, 18, 22, 28, 33, 43, 66.

[3] J. G. Bosman, P. J. Bruin, A. Dujella and F. Najman, *Ranks of elliptic curves with prescribed torsion over number fields*, Int. Math. Res. Notices **14** (2014), 2885–2923. ↑ 31, 41, 43.

[4] J. Box, *Quadratic points on modular curves with infinite Mordell–Weil group*, Math. Comp. **90** (2021), 321–343. ↑ 42.

[5] P. Bruin and F. Najman, *Fields of definition of elliptic curves with prescribed torsion*, Acta Arith. **181** (2017), 85–96. ↑ ii, v, 42, 59, 62, 65, 67, 68.

[6] P. Bruin and F. Najman, *Hyperelliptic modular curves $X_0(n)$ and isogenies of elliptic curves over quadratic fields*, LMS J. Comput. Math. **18** (2015), 578–602. ↑ 42, 43, 44, 46, 48, 52, 57.

[7] H. Cohen and G. Frey, Handbook of Elliptic and Hyperelliptic Curve Cryptography, Chapman & Hall/CRC, Boca Raton, FL, 2006. ↑ 22, 33.

[8] S. Comalada, *Twists and reduction of an elliptic curve*, J. Number Theory **49** (1994), 45–62. ↑ 74.

[9] B. Conrad, C. Conrad and H. Helfgott, *Root numbers and ranks in positive characteristic*, Adv. Math. **198** (2005), 684–731. ↑ 70.

[10] J. L. Coolidge, A treatise on algebraic plane curves, Dover Publications, New York, 1959. ↑ 4.

[11] J. E. Cremona, Algorithms for modular elliptic curves, second ed., Cambridge University Press, Cambridge, 1997. ↑ 65.

[12] F. Diamond and J. Shurman, A First Course in Modular Forms, Springer, New York, 2005. ↑ 11, 12.

[13] T. Dokchitser and V. Dokchitser, *Local invariants of isogenous elliptic curves*, Trans. Amer. Math. Soc. **367** (2015), 4339–4358. ↑ 74.

[14] S. D. Galbraith, M. Harrison and D. J. Mireles Morales, *Efficient Hyperelliptic Arithmetic Using Balanced Representation for Divisors*, in: Algorithmic number theory, Lecture Notes in Comput. Sci. 5011, Springer, Berlin, 2008, 342–356. ↑ 22.

[15] J. González, *On the j-invariants of the quadratic $\mathbb{Q}$-curves*, J. Lond. Math. Soc. **63** (2001), 52–68. ↑ 43, 56.

[16] M. Hindry and J.H. Silverman, Diophantine geometry, Springer-Verlag, New York, 2000. ↑ ii, v, 64.

[17] D. Jeon and A. Schweizer, *Torsion of rational elliptic curves over different types of cubic fields*, Int. J. Number Theory, **16** (2020), 1307–1323. ↑ 67, 68, 69, 71.

[18] M. Jukić Bokun, *Elliptic curves over quadratic fields with fixed torsion subgroup and positive rank*, Glas. Mat. Ser. III **47** (2012), 277–284. ↑ 25.

[19] S. Kamienny and F. Najman, *Torsion groups of elliptic curves over quadratic fields*, Acta. Arith. **152** (2012), 291–305. ↑ 25, 28.

[20] S. Kamienny, *Torsion points on elliptic curves and q-coefficients of modular forms*, Invent. Math. **109** (1992), 221–229. ↑ i, iv, 5, 24.

[21] N. M. Katz, *Galois properties of torsion points on abelian varieties*, Invent. Math. **62** (1981), 481–502. ↑ 63.

[22] M. A. Kenku, *The modular curve $X_0(39)$ and rational isogeny*, Math. Proc. Cambridge Philos. Soc. **85** (1979), 21–23. ↑ 6.

[23] M. A. Kenku, *The modular curves $X_0(65)$ and $X_0(91)$ and rational isogeny*, Math. Proc. Cambridge Philos. Soc. **87** (1980), 15–20. ↑ 6.

[24] M. A. Kenku, *The modular curve $X_0(169)$ and rational isogeny*, J. London Math. Soc. **22** (1980), 239–244. ↑ 6.

[25] M. A. Kenku, *The modular curves $X_0(125), X_1(25)$ and $X_1(49)$*, J. London Math. Soc. **23** (1981), 415–427 ↑ 6.

[26] M. A. Kenku and F. Momose, *Torsion points on elliptic curves defined over quadratic fields*, Nagoya Math. J. **109** (1988), 125–149. ↑ i, iv, 5, 24, 41, 42, 43.

[27] D. Krumm, Quadratic Points on Modular Curves, Doctoral thesis, Athens, Georgia, 2013. ↑ ii, v, 31, 35, 41, 43, 44, 65.

[28] The LMFDB Collaboration, *The L-functions and Modular Forms Database*, `http://www.lmfdb.org`, 2021, [Online; accessed 21. April 2021]. ↑ 67.

[29] D. Lorenzini, *Models of Curves and Wild Ramification*, Pure Appl. Math. Q. **6** (2010), 41–82. ↑ 74.

[30] D. Lorenzini, *Torsion and Tamagawa numbers*, Ann. Inst. Fourier (Grenoble) **61** (2011), 1995–2037. ↑ ii, v, 65.

[31] Á. Lozano-Robledo, *On the field of definition of p-torsion points on elliptic curves over the rationals*, Math. Ann. **357** (2013), 279–305. ↑ 73, 75, 77, 79, 81, 82.

[32] B. Mazur, *Modular curves and the Eisenstein ideal*, Inst. Hautes Études Sci. Publ. Math. **47** (1978), 33–186. ↑ i, iv, 5, 41.

[33] B. Mazur, *Rational isogenies of prime degree*, Invent. Math. **44** (1978), 129–162. ↑ 6.

[34] A. J. Menezes, Y.Wu, and R. J. Zuccherato, An elementary introduction to hyperelliptic curves, appendix in Algebraic Aspects of Cryptography by Neal Koblitz, Springer, Berlin, 1998, 155–178. ↑ 22.

[35] F. Momose, *p-torsion points on elliptic curves defined over quadratic fields,* Nagoya Math. J. **96** (1984), 139–165. ↑ 41, 42, 43.

[36] F. Najman, *Complete classification of torsion of elliptic curves over quadratic cyclotomic fields*, J. Number Theory **130** (2010), 1964–1968. ↑ 27.

[37] F. Najman, *Tamagawa numbers of elliptic curves with C_{13} torsion over quadratic fields,* Proc. Amer. Math. Soc. **145** (2017), 3747–3753. ↑ ii, v, 63, 65.

[38] F. Najman, *Torsion of elliptic curves over quadratic cyclotomic fields*, Math. J. Okayama Univ. **53** (2011), 75–82. ↑ 27.

[39] F. Najman and A. Trbović, *Splitting of primes in number fields generated by points on some modular curves*, preprint, available at https://arxiv.org/abs/2009.02485 ↑ i, iv, 41, 67, 149.

[40] E. Ozman, *Points on quadratic twists of $X_0(N)$,* Acta Arith. **152** (2012), 323–348. ↑ 56.

[41] F. P. Rabarison, *Structure de torsion des courbes elliptiques sur les corps quadratiques*, Acta Arith. **144** (2010), 17–52. ↑ 28.

[42] J. H. Silverman, Advanced topics in the arithmetic of elliptic curves, Springer, New York, 1994. ↑ 17.

[43] J. H. Silverman, The arithmetic of elliptic curves, Second Edition, Springer, Dordrecht, 2009. ↑ 3, 4, 6, 7, 14, 15, 16, 19, 65, 66.

[44] J. Tate, *Algorithm for determining the type of the singular fiber in an elliptic pencil*, in: Modular functions of one variable, IV (Proc. Internat. Summer School, Univ. Antwerp, Antwerp, 1972), Springer, Berlin, 1975, 33–52. ↑ 14, 66, 68.

[45] A. Trbović, Modularne krivulje, diplomski rad, 2017. ↑ 12.

[46] A. Trbović, *Tamagawa numbers of elliptic curves with prescribed torsion subgroup or isogeny*, preprint, available at https://arxiv.org/abs/2102.04834 ↑ ii, v, 64, 149.

[47] A. Trbović, *Torsion groups of elliptic curves over quadratic fields* $\mathbb{Q}(\sqrt{d})$, $0 < d < 100$, Acta Arith. **192** (2020), 141–153. ↑ i, iv, 24, 149.

[48] D. J. Zywina, *On the possible images of the mod l representations associated to elliptic curves over* $\mathbb{Q}$, preprint, available at https://arxiv.org/abs/1508.07660 ↑ 26.

CURRICULUM VITAE

Antonela Trbović was born on October 20th 1993 in Rijeka. She attended elementary school and gymnasium in Rijeka and started her studies at the University of Zagreb, Faculty of Science, Department of Mathematics in 2012. In 2015 she finished the Undergraduate University Programme and in 2017 she finished the Graduate University Programme of Theoretical Mathematics and was awarded the title summa cum laude. Her Master's thesis was entitled *Modular curves* and was written under the supervision of prof.dr.sc. Filip Najman.

In the year 2016 she was awarded the Rector's award of the University of Zagreb for the work entitled *Torsion subgroups of elliptic curves over quadratic fields* and in the years 2015 and 2017 she got the award for best students of final year of undergraduate/graduate programmes.

In 2017 she started a doctoral programme in mathematics and is working as a research assistant at University of Zagreb. She participates in the work of the Seminar for Number Theory and Algebra. She has participated in several international conferences and schools, and written a number of papers, some of which published and some of which submitted.

The author was supported by the QuantiXLie Centre of Excellence, a project co-financed by the Croatian Government and European Union through the European Regional Development Fund - the Competitiveness and Cohesion Operational Programme (Grant KK.01.1.1.01.0004) and by the Croatian Science Foundation under the project no. IP-2018-01-1313.