Quadratic Points on Modular Curves

by

David Krumm

(Under the direction of Dino J. Lorenzini)

Abstract

The central focus of this thesis is a study of quadratic points on classical and dynamical modular curves. After establishing a set of core results and techniques, we give applications to the arithmetic theory of elliptic curves and to the study of preperiodic points in dynamics. In addition, we give a new algorithm – developed jointly with John Doyle – for listing elements of bounded height in number fields.

Index words: Tamagawa numbers, preperiodic points, bounded height, squarefree part, modular curves, uniform boundedness conjecture.

Quadratic Points on Modular Curves

by

David Krumm

B.S., University of Costa Rica, 2005

M.S., Georgia Institute of Technology, 2008

A Dissertation Submitted to the Graduate Faculty
of The University of Georgia in Partial Fulfillment
of the
Requirements for the Degree

Doctor of Philosophy

Athens, Georgia

2013

Quadratic Points on Modular Curves

by

David Krumm

Approved:

Professor:	Dino J. Lorenzini
Committee:	Robert Rumely Pete L. Clark Elham Izadi

Electronic Version Approved:

Maureen Grasso
Dean of the Graduate School
The University of Georgia
May 2013

Dedicado a mi abuelita, quien me enseñó a sumar.

Quadratic Points on Modular Curves

David Krumm

April 28, 2013

Acknowledgments

I would like to express my heartfelt appreciation to Dino Lorenzini for his expert guidance and encouragement during my years of study at the University of Georgia, and in particular during the preparation of this thesis. For a careful reading of this manuscript and for many insightful conversations I am especially grateful to Robert Rumely. I also thank Pete Clark and Robert Varley for their help in better understanding some of the theoretical background required to develop my ideas. Finally, I would like to give sincere thanks to my colleagues and friends in the mathematics department at the University of Georgia for creating an excellent working environment.

Contents

Chapter 1

Overview

The chapters of this thesis cover varied topics which at first sight may appear to be unrelated, though in fact there are several links between them; we give here a short description of the chapters and discuss their connections. For a more detailed summary of the contents of individual chapters we refer the reader to the introductory section of each chapter.

The material in this thesis was developed in response to various questions that arose from two entirely separate lines of inquiry which, surprisingly, in time became closely related.

On the one hand, we aimed to extend Lorenzini's work [40] on Tamagawa numbers of elliptic curves over $\mathbb{Q}$. It was noticed by Agashe that for optimal elliptic curves over $\mathbb{Q}$ with a rational point of order $N = 5$ or 7, the product of the Tamagawa numbers of the elliptic curve seemed to be always divisible by N. This phenomenon was later explained by Lorenzini, who also proved more general results concerning the interplay between torsion and Tamagawa numbers of elliptic curves over $\mathbb{Q}$. Similar patterns seem to hold for elliptic curves over number fields of higher degree. Explaining these patterns often requires understanding points of higher degree on the modular curves $X_1(N)$ from both a computational and theoretical perspective. In Chapter 2 we carry out a study of quadratic points on the modular curves $X_1(N)$ of genus 2, and in Chapter 5 we use these results along with other techniques to prove observed patterns in the Tamagawa numbers of elliptic curves over number fields of small degree. Our study of quadratic points on the modular curves of genus 2 also motivated a new question regarding congruences satisfied by the discriminants of the quadratic fields where a given hyperelliptic curve has points. An initial study of this question is contained in Chapter 3.

On the other hand, a separate project in arithmetic dynamics was developed in order to extend Poonen's analysis [58] of rational preperiodic points for quadratic polynomials over $\mathbb{Q}$ to the context of all quadratic fields. Gathering significant amounts of data on preperiodic points required an algorithm for computing elements of bounded height in number fields. A new algorithm for doing this is explained in Chapter 6, which is the basis for an article coauthored with John Doyle [15]. This algorithm opened up the possibility of computing the preperiodic points for any given quadratic polynomial over a number field. Large amounts of data over quadratic fields were gathered using this algorithm, and are summarized in Appendix A. The results of these computations will appear in a joint article with John Doyle and Xander Faber [13].

Having this data on preperiodic points for quadratic polynomials over quadratic fields, we observed several patterns and formulated questions about the possible preperiodic structures for such polynomials. It has been a surprising discovery that the modular curves $X_1(N)$ of genus 2, namely $X_1(13), X_1(16)$, and $X_1(18)$, arise naturally in the study of preperiodic points for quadratic polynomials, and that a good understanding of the quadratic points on these curves is essential to classifying the possible preperiodic structures for this family of polynomial maps. The material in Chapter 2 is therefore crucial in this context, and is applied very successfully in Chapter 4 to determine the full set of quadratic points on certain *dynamical modular curves.*

Chapter 2

Quadratic points on modular curves

2.1 Introduction

Following Mazur's theorem [43] on torsion subgroups of elliptic curves over the rational numbers, the possible torsion subgroups of elliptic curves over quadratic number fields were classified by Kamienny [31] and Kenku-Momose [35]:

Theorem 2.1.1. *Let K be a quadratic number field, and E/K an elliptic curve. Then the torsion subgroup of $E(K)$ is isomorphic to one of the following 26 groups:*

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

Kenku and Momose had conjectured this result, and proved it assuming that the order of a torsion point on an elliptic curve over a quadratic field can only be divisible by primes smaller than 17. Kamienny then proved the latter result.

In passing from the field $\mathbb{Q}$ to the context of all quadratic fields, new types of questions arise regarding the relations between a field K and the torsion structures that can occur over K:

1. Given a quadratic field K, which groups in the above list occur as torsion subgroups for elliptic curves over K?

2. Given a group G from the list, what can be said about the quadratic fields over which G occurs?

Question (1) was completely answered by Najman [52, 51] for the fields $\mathbb{Q}(\sqrt{-1})$ and $\mathbb{Q}(\sqrt{-3})$; in a subsequent paper, Kamienny and Najman [32] proposed some ideas for answering the question in general, and successfully applied their methods to several quadratic fields of small discriminant. Regarding question (2), we remark that for a given group G there may be properties that are common to all quadratic fields over which G occurs as a torsion subgroup. The only examples of this phenomenon we have found in the literature are due to Kenku-Momose [35] and Momose [46], who prove results about the splitting of rational primes in quadratic fields where the torsion groups $\mathbb{Z}/13$ and $\mathbb{Z}/18$ occur. For the group $\mathbb{Z}/16$, Momose makes a statement of similar type, but this turns out to be incorrect (see §2.6.3 below).

Our main goal in this chapter is to address question (2) when the group G is $\mathbb{Z}/13$, $\mathbb{Z}/16$, or $\mathbb{Z}/18$. We prove in §2.6 several results about the quadratic fields where these torsion subgroups occur, extending the results of Kenku and Momose. In addition, we discuss in §2.7 some improvements to the method proposed by Kamienny and Najman for answering question (1).

The natural way to address these questions is to study quadratic points on the modular curves $X_1(M, N)$. In this chapter we will restrict attention to the torsion structures that do not occur over $\mathbb{Q}$; moreover, question (2) is easily answered for the groups $G = \mathbb{Z}/4 \oplus \mathbb{Z}/4$

and $G = \mathbb{Z}/3 \oplus \mathbb{Z}/3n$: the properties of the Weil pairing [67, §3.8] imply that the group $\mathbb{Z}/4 \oplus \mathbb{Z}/4$ can only occur over the field $\mathbb{Q}(\sqrt{-1})$, and the groups $\mathbb{Z}/3 \oplus \mathbb{Z}/3n$ can only occur over $\mathbb{Q}(\sqrt{-3})$. Hence, we will not be concerned with these groups. The pairs (M, N) that are relevant to us are therefore $(1, N)$ for $N = 11, 13, 14, 15, 16, 18$; and $(2, 10), (2, 12)$. The genera of the corresponding modular curves are as follows: $X_1(N) := X_1(1, N)$ has genus 1 for $N \in \{11, 14, 15\}$ and genus 2 for $N \in \{13, 16, 18\}$; the curves $X_1(2, 10)$ and $X_1(2, 12)$ have genus 1. (Genus formulas for modular curves may be found in [27, Thm 1.1].)

Our initial motivation for studying quadratic points on modular curves was to add to the existing literature on torsion subgroups of elliptic curves over quadratic number fields. However, we have found surprising applications of the results of this chapter to the study of preperiodic points for quadratic polynomials — we refer the interested reader to the article [14].

2.2 The modular curves $X_1(N)$

We give here a brief sketch of the construction and modularity property of the curves $X_1(N)$. In addition, we discuss the question of finding explicit equations for these curves. For a detailed treatment of the subject see the books of Shimura [65], Katz-Mazur [33], Diamond-Shurman [12]; as well as Rohrlich's article [61].

2.2.1 Definition and properties

Let N be a positive integer. The *principal congruence subgroup of level* N is the group $\Gamma(N) \leq \mathrm{SL}_2(\mathbb{Z})$ consisting of matrices that are congruent to the identity matrix modulo N. A subgroup of $\mathrm{SL}_2(\mathbb{Z})$ is a *congruence subgroup* if it contains $\Gamma(N)$ for some N. Every congruence subgroup Γ acts by linear fractional transformations on the upper half plane $\mathcal{H} = \{z \in \mathbb{C} : \Im z > 0\}$. The quotient space $Y(\Gamma) = \Gamma\backslash\mathcal{H}$ carries a natural structure of

Riemann surface, and corresponds to the set of complex points on a smooth affine algebraic curve over $\mathbb{C}$. The Riemann surface $Y(\Gamma)$ is not compact, but can be compactified by adding a finite number of points, called *cusps*; the resulting compact Riemann surface is denoted by $X(\Gamma)$. Being a compact Riemann surface, $X(\Gamma)$ corresponds to the set of complex points on a smooth projective algebraic curve over $\mathbb{C}$ (see [21, App. B]).

The congruence subgroups that are most relevant here are the groups $\Gamma_1(N)$ defined by

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

We denote by $X_1(N)$ (resp. $Y_1(N)$) the smooth projective (resp. affine) curve corresponding to the Riemann surface $X(\Gamma_1(N))$ (resp. $Y(\Gamma_1(N))$). Though these curves are *a priori* defined over $\mathbb{C}$, it is known that they can in fact be defined over $\mathbb{Q}$. The main property of the modular curves $Y_1(N)$ we will need is given below.

Theorem 2.2.1. *For $N \geq 4$, the curve $Y_1(N)$ has the following property: for any field K of characteristic 0, the set $Y_1(N)(K)$ is in bijection with the set of isomorphism classes of pairs (E, P), where E/K is an elliptic curve and $P \in E(K)$ has order N.*

Pairs (E, P) and (E', P') as in the theorem are isomorphic if there is an isomorphism $E \longrightarrow E'$ taking P to P'.

2.2.2 Equations for modular curves

Given a positive integer N, one would like to write down an equation $f(x, y) = 0$ for a plane curve that is birational to $X_1(N)$. This problem has been studied by several authors, for various reasons. Lecacheux [39], Washington [75], and Darmon [10] computed equations for the curves $X_1(13), X_1(16)$, and $X_1(25)$, respectively, with the goal of constructing cyclic extensions of $\mathbb{Q}$. Their methods cannot be readily applied to all curves $X_1(N)$. General methods have been put forth by Ishida-Ishii [26], Yang [77], Baaziz [1], and Sutherland [72].

For our purposes, we need not only an equation for $X_1(N)$, but also an explicit method for constructing the pair (E, P) corresponding to a given point on an affine plane model. Using the interpretation of $X_1(N)$ as a moduli space for isomorphism classes of pairs (E, P), Reichert [60] computed equations for various curves $X_1(N)$ of small level and showed how to obtain the elliptic curves corresponding to a point on his affine models. Reichert's methods have since been extended and refined [1, 59, 72]. The starting point for the methods in these articles is the following result:

Lemma 2.2.2. *Let K be any field and E/K an elliptic curve. Suppose that $P \in E(K)$ is a torsion point of order $N \geq 4$. Then, after a change of variables, we can assume that $P = (0,0)$ and E is given by an equation of the form*

$$E(b,c) : y^2 + (1-c)xy - by = x^3 - bx^2$$

for some elements $b, c \in K$.

Proof. See [36, §V.5]. □

Setting the order of $P = (0,0)$ on the curve $E(b,c)$ to be N yields a relation between b and c which defines a plane curve birational to $X_1(N)$. As N grows, the resulting equation becomes increasingly complicated, so one must work with this equation in order to simplify it as much as possible; different ways of doing this are developed in the articles [1, 59, 72]. We remark that neither Reichert [60], Sutherland [72], nor Rabarison [59] seem to prove that their equations define plane curves birational to the curves $X_1(N)$ as we have defined them in §2.2.1. However, this is discussed by Baaziz — see [1, §3].

2.3 Preliminary results

For later reference we gather here a series of facts about integer polynomials. We encourage the reader to skip this section on a first reading and refer to it when necessary.

Notation 2.3.1. For of a nonzero rational number r we let $S(r)$ denote the squarefree part of r, i.e., the unique squarefree integer D such that r/D is a square in $\mathbb{Q}$.

Definition 2.3.2. Given a polynomial $f(x) \in \mathbb{Z}[x]$ we define $\Pi(f)$ to be the set of all prime numbers p such that $f(x)$ does not have a root modulo p.

Lemma 2.3.3. *Let $f(x) \in \mathbb{Z}[x]$ be an irreducible polynomial. Let $L/\mathbb{Q}$ be a splitting field of $f(x)$ and $G = \mathrm{Gal}(L/\mathbb{Q})$. Fix a root θ of $f(x)$ in L, and put $K = \mathbb{Q}(\theta)$, $H = \mathrm{Gal}(L/K) \leq G$. Then the density of the set of primes p for which $f(x)$ has a root modulo p is*

$$\frac{\left|\bigcup_{g\in G} g^{-1}Hg\right|}{|G|}.$$

Proof. This is a consequence of the Chebotarev density theorem. See [3, Thm. 2] for a proof of a more general result. □

Lemma 2.3.4. *Let $f(x) \in \mathbb{Z}[x]$ be a monic, irreducible polynomial of even degree, and let p be an odd prime. If $p \in \Pi(f)$, then p is unramified in every quadratic field of the form $\mathbb{Q}(\sqrt{f(r)})$ with $r \in \mathbb{Q}$.*

Proof. Given a prime $p \in \Pi(f)$ and a quadratic field K of the form $K = \mathbb{Q}(\sqrt{f(r)})$ we must show that p does not divide the discriminant of K. Let $D = S(f(r))$, so that $K = \mathbb{Q}(\sqrt{D})$. Since p is odd, it suffices to show that p does not divide D. Set

$$f(x) = x^{2k} + a_{2k-1}x^{2k-1} + \cdots + a_1x + a_0,$$

and let r be expressed in lowest terms as $r = n/d$. Note that $S(f(r)) = S(d^{2k}f(r)) = S(n^{2k} + a_{2k-1}n^{2k-1}d + \cdots + a_1nd^{2k-1} + a_0d^{2k})$, so that we have an equation

$$n^{2k} + a_{2k-1}n^{2k-1}d + \cdots + a_1nd^{2k-1} + a_0d^{2k} = Ds^2$$

for some integer s. Suppose that $d \equiv 0 \bmod p$. Then, reducing the above equation modulo p we obtain $n^{2k} \equiv Ds^2 \bmod p$. Since p cannot divide n (because n and d are coprime), we conclude that p does not divide D. Suppose now that $d \not\equiv 0 \bmod p$. We can then consider the equation $d^{2k}f(n/d) = Ds^2$ as taking place in the localization $\mathbb{Z}_{(p)}$, and reduce modulo p. Since $f(x)$ has no roots modulo p (by hypothesis), this equation implies that D is nonzero modulo p. □

Lemma 2.3.5. *Let $f(x) \in \mathbb{Z}[x]$ and let p be a prime. Suppose that $f(x)$ has a simple root modulo p. Then there is an integer n such that $\mathrm{ord}_p(f(n))$ is odd.*

Proof. Let r be an integer such that $f(r) \neq 0$ and p divides $f(r)$ but not $f'(r)$. If $\mathrm{ord}_p(f(r))$ is odd, then we can take $n = r$. Otherwise, let $\mathrm{ord}_p(f(r)) = 2s$ and set $n = r + p^{2s-1}$. By using a Taylor expansion we see that $f(n) = f(r) + f'(r)p^{2s-1} + m$, where m is divisible by p^{4s-2}. It follows that $\mathrm{ord}_p(f(n)) = 2s - 1$ is odd. □

Remark 2.3.6. The requirement in Lemma 2.3.5 that the root of $f(x)$ be simple is necessary. Consider, for example, $f(x) = x^d + p^2$, where $d > 2$. It is easy to see that for every integer r, $\mathrm{ord}_p(f(r))$ is either 0 or 2.

Lemma 2.3.7. *Let $f(x) \in \mathbb{Z}[x]$ be a polynomial with nonzero discriminant and degree at least 5. Suppose that $p_1, \ldots, p_t$ are distinct primes such that $f(x)$ has a simple root modulo p_i for all i. Then there exist infinitely many squarefree integers D such that D is divisible by $p_1 \cdots p_t$ and $D \in \{S(f(n)) : n \in \mathbb{Z} \text{ and } f(n) \neq 0\}$.*

Proof. By Lemma 2.3.5, there are integers n_i such that $\operatorname{ord}_{p_i}(f(n_i))$ is odd, say equal to $2s_i + 1$. Let

$$\mathcal{N} := \{n \in \mathbb{Z} : n \equiv n_i \bmod p_i^{2s_i+2} \text{ for all } i\}.$$

For every $n \in \mathcal{N}$ we have $f(n) \equiv f(n_i) \bmod p_i^{2s_i+2}$; in particular, $f(n) \neq 0$, and $\operatorname{ord}_{p_i}(f(n)) = 2s_i + 1$ is odd for all i, so that $p_1 \cdots p_t$ divides $S(f(n))$. Hence, every element of the set

$$\mathcal{D} = \{D \in \mathbb{Z} : D = S(f(n)) \text{ for some } n \in \mathcal{N}\}$$

is divisible by $p_1 \cdots p_t$. The lemma will be proved if we show that $\mathcal{D}$ is an infinite set.

Note that a squarefree integer D can only be equal to $S(f(n))$ for finitely many integers n. Indeed, if $D = S(f(n))$, then $f(n) = Ds^2$ for some integer s, so that (n, s) is a rational point on the hyperelliptic curve $Dy^2 = f(x)$. Since the degree of $f(x)$ is at least 5, this curve has genus greater than 1, so by Faltings' theorem the curve has only finitely many rational points. In particular, there are only finitely many options for n. This shows that the map $n \mapsto S(f(n))$ from $\mathcal{N}$ to $\mathcal{D}$ is finite-to-one. Since $\mathcal{N}$ is clearly an infinite set, this implies that $\mathcal{D}$ is also infinite. □

2.4 Non-obvious quadratic points on hyperelliptic curves

Let k be a number field, and fix an algebraic closure $\overline{k}$ of k. Let C be a smooth, projective, geometrically connected curve defined over k. We assume that C is hyperelliptic over k, so that there exists a morphism $\varphi : C \longrightarrow \mathbb{P}^1_k$ of degree 2. Let σ be the hyperelliptic involution on C, i.e., the unique involution such that $\varphi \circ \sigma = \varphi$. Corresponding to the map φ there is an affine model of C of the form $y^2 = f(x)$, where $f(x) \in k[x]$ has nonzero discriminant. With respect to this equation, σ is given by $(x, y) \mapsto (x, -y)$, and the quotient map $\varphi : C \longrightarrow C/\langle\sigma\rangle = \mathbb{P}^1_k$ is given by $(x, y) \mapsto x$.

Definition 2.4.1. A point $P \in C(\overline{k})$ is *quadratic over* k if $[k(P) : k] = 2$.

We wish to distinguish between two kinds of quadratic points on C. Given a model $y^2 = f(x)$ for C, there is an obvious way of producing quadratic points: choosing any element $x_0 \in k$ we obtain a point $(x_0, \sqrt{f(x_0)}) \in C(\overline{k})$ which will often be quadratic as we vary x_0. Indeed, Hilbert's irreducibility theorem [18, Chap. 12] implies that this will occur for infinitely many $x_0 \in k$. Points of this form will be called *obvious quadratic points* for the given model. Stated differently, these are the quadratic points $P \in C(\overline{k})$ such that $\varphi(P) \in \mathbb{P}^1(k)$, or equivalently $\sigma(P) = \overline{P}$, where $\overline{P}$ is the Galois conjugate of P. We are interested here in the problem of determining whether a given model for a hyperelliptic curve has finitely or infinitely many non-obvious quadratic points. The following result will provide an answer for curves of genus larger than 3.

Theorem 2.4.2 (Vojta [73], Cor. 0.3)**.** *Let C be a curve of genus g defined over a number field k, let v be a positive integer, and let $\varphi : C \longrightarrow \mathbb{P}^1$ be a dominant morphism. Assume that $g > 1 + (v-1) \cdot \deg \varphi$. Then the set $\{P \in C(\overline{k}) : [k(P) : k] \leq v \text{ and } k(\varphi(P)) = k(P)\}$ is finite.*

Corollary 2.4.3. *Let C/k be a hyperelliptic curve of genus $g \geq 4$, and fix a model $y^2 = f(x)$ for C. Then C has only finitely many non-obvious quadratic points for this model.*

Proof. Corresponding to the given model for C there is a morphism $\varphi : C \longrightarrow \mathbb{P}^1$ of degree 2. A non-obvious quadratic point P on C satisfies $[k(P) : k] = 2$ and $k(\varphi(P)) = k(P)$, since $k(\varphi(P)) \subseteq k(P)$ and $k(\varphi(P)) \neq k$. Applying Theorem 2.4.2 with $v = 2$ we conclude that the set of non-obvious quadratic points is finite. □

In contrast to the case of higher genera, we will see that set of non-obvious quadratic points on a curve of genus 2 can be empty, finite, or infinite.

2.5 Quadratic points on curves of genus 2

Let C/k be a curve of genus 2. Fix an affine model $y^2 = f(x)$ for C, where $f(x)$ has degree 5 or 6, and let σ be the hyperelliptic involution on C.

Lemma 2.5.1. *Suppose that C/k has genus 2 and $C(k) \neq \emptyset$. Let J be the Jacobian variety of C.*

1. *The set of non-obvious quadratic points for the model $y^2 = f(x)$ is finite if and only if $J(k)$ is finite.*

2. *Suppose that $J(k)$ is finite, and let q denote the number of non-obvious quadratic points for the given model. Then there is a relation*

$$q = 2j - 2 + w - c^2,$$

where $j = \#J(k)$, $c = \#C(k)$, and w is the number of points in $C(k)$ that are fixed by σ.

Proof. Fix a point $P_0 \in C(k)$ and let $\iota : C \hookrightarrow J$ be the embedding taking P_0 to 0. Let $\mathcal{S} = \mathrm{Sym}^2(C)$ denote the symmetric square of C. Points in $\mathcal{S}(\overline{k})$ correspond to unordered pairs $\{P, Q\}$, where $P, Q \in C(\overline{k})$. The embedding ι induces a morphism $f : \mathcal{S} \longrightarrow J$ taking $\{P, Q\}$ to $\iota(P) + \iota(Q)$. We will need a few facts concerning the fibers of this morphism; see the article of Milne [45] for the necessary background material. There is a copy of $\mathbb{P}^1_k$ inside $\mathcal{S}$ whose points correspond to pairs of the form $\{P, \sigma(P)\}$. The image of $\mathbb{P}^1$ under f is a single point $* \in J(k)$, and f restricts to an isomorphism $f : U = \mathcal{S} \backslash \mathbb{P}^1 \xrightarrow{\sim} J \backslash \{*\}$. In particular, there is a bijection

$$U(k) = \mathcal{S}(k) \backslash \mathbb{P}^1(k) \longleftrightarrow J(k) \backslash \{*\}. \tag{2.1}$$

Points in $\mathcal{S}(k)$ correspond to pairs of the form $\{P, Q\}$ where either P and Q are both in $C(k)$, or they are quadratic over k and $Q = \overline{P}$; in particular, points in $\mathbb{P}^1(k) \subset \mathcal{S}(k)$ correspond to pairs $\{P, \sigma(P)\}$ where either $P \in C(k)$ or P is an obvious quadratic point. Finally, the points of $U(k)$ are either pairs $\{P, \overline{P}\}$ with P a non-obvious quadratic point, or pairs $\{P, Q\}$ with $P, Q \in C(k)$ but $Q \neq \sigma(P)$.

Hence, there are three essentially distinct ways of producing points in $\mathcal{S}(k)$: first, we can take points P and Q in $C(k)$ and obtain a point $\{P, Q\} \in \mathcal{S}(k)$. Second, we can take an obvious quadratic point P and obtain $\{P, \sigma(P)\} \in \mathbb{P}^1(k) \subset \mathcal{S}(k)$. Finally, we can take a non-obvious quadratic point P and obtain $\{P, \overline{P}\} \in U(k) \subset \mathcal{S}(k)$.

Let Q^o and Q^n denote, respectively, the set of obvious and non-obvious quadratic points on C. We then have maps $\psi^o : Q^o \longrightarrow \mathbb{P}^1(k)$ and $\psi^n : Q^n \longrightarrow U(k)$, and a map $\varphi : C(k) \times C(k) \longrightarrow \mathcal{S}(k)$ defined as above. The proof of the lemma will be a careful analysis of the images of these three maps.

We have $\mathcal{S}(k) = \text{im}(\varphi) \sqcup \text{im}(\psi^o) \sqcup \text{im}(\psi^n)$. Removing the points of $\mathbb{P}^1(k)$ from both sides we obtain

$$U(k) = (\text{im}(\varphi) \backslash \mathbb{P}^1(k)) \sqcup \text{im}(\psi^n). \tag{2.2}$$

To prove part (1), suppose first that Q^n is finite. We know by Faltings' theorem that $C(k)$ is finite, so it follows from (2.2) that $U(k)$ is finite. By (2.1) we conclude that $J(k)$ is finite. Conversely, assume that $J(k)$ is finite. Then $U(k)$ is finite by (2.1), so $\text{im}(\psi^n)$ is finite by (2.2). But ψ^n is 2-to-1 onto its image, so we conclude that Q^n is finite. This completes the proof of part (1).

To prove part (2), suppose that $J(k)$ is finite and let $q = \#Q^n$, so that $\#\text{im}(\psi^n) = q/2$. By (2.1) and (2.2) we have

$$q/2 = \#U(k) - \#(\text{im}(\varphi) \backslash \mathbb{P}^1(k)) = j - 1 - \#(\text{im}(\varphi) \backslash \mathbb{P}^1(k)). \tag{2.3}$$

By simple combinatorial arguments we see that

$$\#\mathrm{im}(\varphi) = c + \frac{c(c-1)}{2} \quad \text{and} \quad \#(\mathbb{P}^1(k) \cap \mathrm{im}(\varphi)) = w + \frac{c-w}{2}.$$

Therefore,

$$\#(\mathrm{im}(\varphi) \backslash \mathbb{P}^1(k)) = c + \frac{c(c-1)}{2} - w - \frac{c-w}{2} = \frac{c^2-w}{2}.$$

By (2.3) we then have

$$j - 1 = \frac{q}{2} + \frac{c^2-w}{2},$$

and part (2) follows immediately. □

2.5.1 Methods of computation

We comment briefly on how the quantities appearing in Lemma 2.5.1 can be computed in the case where $k = \mathbb{Q}$. Modern computational methods provide a way of obtaining an upper bound for the rank of $J(\mathbb{Q})$. In particular, the Magma command `RankBound` implements Stoll's algorithm [69] of 2-descent. If $J(\mathbb{Q})$ has rank 0, this method will sometimes allow one to prove that the rank is 0. In this case, the function `Chabauty0` can be used to find all the rational points on C, thus determining the number c. The function `TorsionSubgroup` can compute the torsion subgroup of $J(\mathbb{Q})$; the algorithm used is due to Poonen [57]. Thus, assuming we know that $J(\mathbb{Q})$ has rank 0, the number j can be determined. Finally, the number w is closely related to the number r of roots of $f(x)$ in k: if $f(x)$ has even degree, then $w = r$ (since the two points at infinity are interchanged by σ); otherwise, $w = r + 1$ since the unique point at infinity is fixed by σ.

We remark that the way in which elements of the Jacobian of a genus-2 curve are stored in Magma, namely the *Mumford representation*, makes it immediately clear what the non-obvious quadratic points on the curve are: a point in the Jacobian is represented by a pair of polynomials $(p(x), q(x))$, where $\deg(q(x)) < \deg(p(x) \leq 2$ and $p(x)$ divides $q(x)^2 - f(x)$. For those pairs where $p(x)$ is irreducible of degree 2 we obtain the non-obvious quadratic points $(\alpha, q(\alpha))$, where α is a root of $p(x)$. For more details on the Mumford representation, see Mumford's article [49, Chap. IIIa] and also [7, 19, 37].

2.6 Applications to the modular curves $X_1(N)$ of genus 2

In this section we apply Lemma 2.5.1 to the three modular curves $X_1(N)$ of genus 2, and use the result to obtain information about the quadratic fields where these curves have points. It is known that the Jacobians $J_1(N)$ for $N = 13, 16, 18$ have rank 0 over $\mathbb{Q}$ (see [44, §4] for the case of $J_1(13)$ and [34, Thm. 1] for $J_1(16)$). Hence, Lemma 2.5.1 implies that the curves $X_1(N)$ of genus 2 have only finitely many non-obvious quadratic points. We will fix models to be used throughout this chapter. The following equations are given in [59, pp. 32,38,39]:

$$\begin{aligned}
X_1(13) &: y^2 = f_{13}(x) := x^6 - 2x^5 + x^4 - 2x^3 + 6x^2 - 4x + 1;\\
X_1(16) &: y^2 = f_{16}(x) := x(x^2+1)(x^2+2x-1);\\
X_1(18) &: y^2 = f_{18}(x) := x^6 + 2x^5 + 5x^4 + 10x^3 + 10x^2 + 4x + 1.
\end{aligned}$$

The cusps on these curves satisfy, respectively,

$$\begin{aligned}
&x(x-1)(x^3 - 4x^2 + x + 1) = 0;\\
&x(x-1)(x+1)(x^2+1)(x^2-2x-1)(x^2+2x-1) = 0; \qquad (2.4)\\
&x(x+1)(x^2+x+1)(x^3-3x-1) = 0.
\end{aligned}$$

Of course, the rational points at infinity are also cusps.

With the notation introduced in (2.3.2), note that $\Pi(f_{16}) = \emptyset$ since $f_{16}(x)$ has an integer root. The first few elements of $\Pi(f_{13})$ and $\Pi(f_{18})$ are shown below.

$$\Pi(f_{13}) = \{2, 3, 5, 7, 11, 19, 23, 31, 43, 47, 53, 59, 67, 71, 73, 79, 83, 89, 97, \ldots\}$$

$$\Pi(f_{18}) = \{2, 5, 7, 13, 17, 19, 23, 29, 31, 37, 47, 53, 61, 71, 73, 79, 83, 101, \ldots\}$$

Proposition 2.6.1. *The sets $\Pi(f_{13})$ and $\Pi(f_{18})$ both have Dirichlet density $\frac{13}{18}$.*

Proof. We apply Lemma 2.3.3 to the polynomials $f_{13}(x)$ and $f_{18}(x)$, making use of the Galois theory functionality available in Magma. A splitting field L for $f_{13}(x)$ can be computed using the `SplittingField` function. The group $G = \mathrm{Gal}(L/\mathbb{Q})$ is computed with the `AutomorphismGroup` command. Choosing a root θ of $f_{13}(x)$ in L, we obtain the group $H = \mathrm{Gal}(L/\mathbb{Q}(\theta))$ by using the `FixedGroup` function. With this data computed it is then easy to construct the set $\cup_{g \in G} g^{-1}Hg$. We find that this set has order 5, and that G has order 18. Therefore, the set of primes p for which $f_{13}(x)$ has a root modulo p is 5/18. The complement of this set of primes, which is $\Pi(f_{13})$ by definition, has density $1 - \frac{5}{18} = \frac{13}{18}$. For the polynomial $f_{18}(x)$ we obtain the same numerical results: the order of the Galois group is 18, and the corresponding set $\cup_{g \in G} g^{-1}Hg$ has order 5. □

2.6.1 Quadratic Points on $X_1(18)$

We begin by recalling earlier results concerning the quadratic fields where $X_1(18)$ has points.

Theorem 2.6.2 (Kenku-Momose [35], Prop. 2.4). *Let K be a quadratic number field such that $Y_1(18)(K) \neq \emptyset$. Then 5 and 7 are unramified in K, and either 2 splits or 3 does not split in K. Moreover, 3 is not inert in K.*

The statement that either 2 splits or 3 does not split is strengthened below in part (2b) of Theorem 2.6.5; the fact that 3 is not inert in K is proved in a different way in part 2(c).

The fact that 5 and 7 are unramified in K is extended in part (2d): we have an infinite set of primes (of known density), containing 5 and 7, such that all primes in the set are unramified in K.

Theorem 2.6.3 (Najman)**.** *For the fields $K = \mathbb{Q}(\sqrt{-1})$ and $\mathbb{Q}(\sqrt{-3})$ we have $Y_1(18)(K) = \emptyset$.*

Proof. See [52, Lem. 4] and [51, §3]. □

One consequence of Theorem 2.6.5 is that $Y_1(18)(K) = \emptyset$ for *all* imaginary quadratic fields K, and that the only imaginary quadratic field where $X_1(18)$ has a quadratic point is $\mathbb{Q}(\sqrt{-3})$.

Theorem 2.6.4 (Kamienny-Najman [32], Thm. 8)**.** *Let $K = \mathbb{Q}(\sqrt{D})$, with D squarefree, be a quadratic field such that $Y_1(18)(K) \neq \emptyset$. Then $|D| \geq 33$.*

Theorem 2.6.5 implies that in fact $D \geq 33$ (without the absolute value), since 33 is the smallest squarefree integer that is greater than 1, congruent to 1 modulo 8, and not divisible by any prime in $\Pi(f_{18})$.

Theorem 2.6.5.

1. *The only non-obvious quadratic points for the model $y^2 = f_{18}(x)$ are the following four cusps:*

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

   where $\omega = \frac{-1+\sqrt{-3}}{2}$ is a primitive cube root of unity. In particular, every non-cuspidal quadratic point on $X_1(18)$ is obvious.

2. *If $X_1(18)$ has a quadratic point defined over the field $K = \mathbb{Q}(\sqrt{D})$ with $D \neq -3$ squarefree, then:*

(a) *$D > 0$. Hence, K is a real quadratic field.*

(b) *$D \equiv 1 \bmod 8$. Hence, the rational prime 2 splits in K.*

(c) *$D \not\equiv 2 \bmod 3$. Hence, the prime 3 is not inert in K.*

(d) *Every prime in the set $\Pi(f_{18})$ is unramified in K.*

Proof.

1. We apply Lemma 2.5.1 to the curve $C = X_1(18)$. Using Magma as explained in §2.5.1 we find that

$$j = 21,\ w = 0,\ c = 6,$$

and hence $q = 4$. Therefore, $X_1(18)$ has exactly four non-obvious quadratic points. Computing Mumford representations for the elements of $J_1(18)(\mathbb{Q})$ we obtain exactly two pairs $(p(x), q(x))$, namely $(x^2 + x + 1, x - 1)$ and $(x^2 + x + 1, -x + 1)$, for which $p(x)$ is irreducible of degree 2. These pairs clearly give rise to the four non-obvious quadratic points listed above. Note that these four points are cusps, by 2.4.

2. By part (1), every quadratic point defined over K is obvious for the model $y^2 = f_{18}(x)$, so there is an $x_0 \in \mathbb{Q}$ such that $K = \mathbb{Q}(\sqrt{f_{18}(x_0)})$.

   (a) The polynomial function $x \mapsto f_{18}(x)$ only takes positive values for $x \in \mathbb{R}$, so $f_{18}(x_0) > 0$.

   (b) Letting $x_0 = n/d$ with n and d coprime integers, we have that $K = \mathbb{Q}(\sqrt{g(n, d)})$, where

$$g(n, d) := d^6 f_{18}(n/d) = n^6 + 2n^5 d + 5n^4 d^2 + 10n^3 d^3 + 10n^2 d^4 + 4nd^5 + d^6.$$

We claim that $g(n,d)$ is congruent to 1 modulo 8. If n, d are both odd, then

$$g(n,d) \equiv 1 + 2nd + 5 + 10nd + 10 + 4nd + 1 = 17 + 16nd \equiv 1 \bmod 8.$$

If n is even and d is odd, then $g(n,d) \equiv d^6 \equiv 1 \bmod 8$. Finally, if n is odd and d is even, then $g(n,d) \equiv 1 + 2nd + 5nd^2 \bmod 8$. Writing $n = 2k+1$ for some integer k we see that $g(n,d) \equiv 5d^2 + 2d + 1 \equiv (d+1)^2 \equiv 1 \bmod 8$, proving the claim. Since D is the squarefree part of $g(n,d)$, this implies that $D \equiv 1 \bmod 8$.

(c) By a similar calculation as done in part (2b) we find that $g(n,d)$ is always congruent to 0 or 1 modulo 3. Considering all possible values of n and d modulo 9, we find that if $g(n,d)$ is divisible by 9, then n and d are both divisible by 3, which is a contradiction; hence $g(n,d)$ is not divisible by 9. Writing $g(n,d) = Ds^2$ for some integer s, this implies that s is not divisible by 3, and therefore $g(n,d) \equiv D \bmod 3$. Hence, D is congruent to 0 or 1 modulo 3.

(d) For the prime $p = 2$ this is a consequence of part (b). For odd primes p, the result follows from Lemma 2.3.4.

□

2.6.2 Quadratic Points on $X_1(13)$

We recall a few previously known results about the quadratic fields where $X_1(13)$ has points.

Theorem 2.6.6 (Momose). *Let K be a quadratic field such that $Y_1(13)(K) \neq \emptyset$. Then the rational prime 2 splits in K, and 3 is unramified in K.*

Proof. See Remark 3.3.3 in [46]. □

The fact that 2 splits is derived in a different way in part (2b) of Theorem 2.6.9, and the fact that 3 is unramified in K is extended in part (2c).

Theorem 2.6.7 (Najman)**.** *For the fields $K = \mathbb{Q}(\sqrt{-1})$ and $\mathbb{Q}(\sqrt{-3})$ we have $Y_1(13)(K) = \emptyset$.*

Proof. See [51, §2-3]. □

One consequence of Theorem 2.6.9 below is the stronger statement that $Y_1(13)(K) = \emptyset$ for *all* imaginary quadratic fields K.

Theorem 2.6.8 (Kamienny-Najman [32], Thm. 3)**.** *Let $K = \mathbb{Q}(\sqrt{D})$, with D squarefree, be a quadratic field such that $Y_1(13)(K) \neq \emptyset$. Then $|D| \geq 17$.*

The stronger result that $D \geq 17$ (without the absolute value) follows immediately from parts (2a) and (2b) of Theorem 2.6.9.

Theorem 2.6.9.

1. *All quadratic points on $X_1(13)$ are obvious for the model $y^2 = f_{13}(x)$.*

2. *If $X_1(13)$ has a quadratic point defined over the field $K = \mathbb{Q}(\sqrt{D})$ with D squarefree, then:*

   (a) $D > 0$. Hence, K is a real quadratic field.

   (b) $D \equiv 1 \bmod 8$. Hence, the rational prime 2 splits in K.

   (c) Every prime in the set $\Pi(f_{13})$ is unramified in K.

Proof.

1. We apply Lemma 2.5.1 to the curve $C = X_1(13)$. Using Magma we find that

$$j = 19,\ w = 0,\ c = 6,$$

and hence $q = 0$. Therefore, all quadratic points on $X_1(13)$ are obvious.

2. By part (1) we have $K = \mathbb{Q}(\sqrt{f_{13}(x_0)})$ for some rational number x_0.

   (a) The polynomial function $x \mapsto f_{13}(x)$ only takes positive values for $x \in \mathbb{R}$, so $f(x_0) > 0$.

   (b) Write $x_0 = n/d$ with n and d coprime integers. We have $K = \mathbb{Q}(\sqrt{g(n,d)})$, where

   $$g(n,d) = d^6 f_{13}(n/d) = n^6 - 2n^5 d + n^4 d^2 - 2n^3 d^3 + 6n^2 d^4 - 4nd^5 + d^6.$$

   Arguing in the same way as in the proof of part (2b) of Theorem 2.6.5 we conclude that $g(n,d)$ is congruent to 1 modulo 8. Since D is the squarefree part of $g(n,d)$, it follows that $D \equiv 1 \bmod 8$.

   (c) For the prime $p = 2$ this follows from part (b). For odd primes p, it is a consequence of Lemma 2.3.4.

□

2.6.3 Quadratic Points on $X_1(16)$

We have not found in the literature any results giving properties common to all quadratic fields where $X_1(16)$ has points. Momose [46, Remark 3.3.1] claims that if $Y_1(16)$ has a point over a quadratic field K, then the primes 3 and 5 are both unramified in K. However, we show below that this is false.

Proposition 2.6.10. *There are infinitely many quadratic number fields K such that $Y_1(16)(K) \neq \emptyset$ and both 3 and 5 ramify in K.*

Proof. The polynomial $f_{16}(x)$ has a simple root (namely $x = 0$) modulo 3 and 5. By Lemma 2.3.7, there are infinitely many squarefree integers D divisible by 15 such that D is of the form $D = S(f_{16}(n))$ for some integer n. Note that for every such integer D, the curve $X_1(16)$

has a quadratic point defined over the field $\mathbb{Q}(\sqrt{D})$. This construction gives infinitely many quadratic fields K such that 3 and 5 ramify in K, and $X_1(16)$ has a quadratic point over K. Since the cusps of $X_1(16)$ could only be defined over a finite number of these fields, the result follows. $\square$

By Proposition 2.6.10, there exist infinitely many quadratic fields $\mathbb{Q}(\sqrt{D})$ such that 15 divides D and there is an elliptic curve over K with a K-rational point of order 16. For concreteness, we give one explicit example of this phenomenon.

Example 2.6.11. Let $K = \mathbb{Q}(\sqrt{105})$ and let E/K be the elliptic curve defined by the Weierstrass equation

$$y^2 + (19\sqrt{105} + 343)xy + (727552\sqrt{105} + 8655360)y = x^3 + (1624\sqrt{105} + 19320)x^2.$$

One can verify that the point $(0,0) \in E(K)$ has order 16, and both 3 and 5 ramify in K.

From the factorization $f_{16}(x) = x(x^2+1)(x^2+2x-1)$ we see clearly that the chosen model for $X_1(16)$ has at least four non-obvious quadratic points, namely

$$(\sqrt{-1}, 0),\ (-\sqrt{-1}, 0),\ (-1+\sqrt{2}, 0),\ (-1-\sqrt{2}, 0).$$

By (2.4), these four points correspond to cusps on $X_1(16)$.

Theorem 2.6.12. *The only non-obvious quadratic points for the chosen model of $X_1(16)$ are the four cusps listed above.*

Proof. We apply Lemma 2.5.1 to the curve $C = X_1(16)$. Using Magma we find that

$$j = 20,\ w = 2,\ c = 6,$$

and hence $q = 4$. Therefore, $X_1(16)$ has exactly four non-obvious quadratic points. We have already listed four such points, so these must be all. □

It follows from Theorem 2.6.12 that all non-cuspidal quadratic points on $X_1(16)$ are obvious, so they occur over fields of the form $K = \mathbb{Q}(\sqrt{f_{16}(x_0)})$ with $x_0 \in \mathbb{Q}$. In contrast to the cases of $X_1(13)$ and $X_1(18)$, we cannot use this description to prove results about the splitting of rational primes in K. However, we have noticed the following property of the ideal class groups of such number fields K: when K is imaginary quadratic and $K \neq \mathbb{Q}(\sqrt{-15})$, its class number seems to be always divisible by 10. We have verified this for a total of 77,618 imaginary quadratic fields. More precisely, taking all rational numbers $x_0 \in \mathbb{Q}$ of height at most 10^3 we construct the corresponding number fields $K = \mathbb{Q}(\sqrt{f_{16}(x_0)})$ and keep only those fields whose discriminants are negative and do not exceed 10^{15} in absolute value. This amounts to a total of 77,618 distinct fields $\mathbb{Q}(\sqrt{D})$, where D is a squarefree integer ranging from -999970393954035 to -15. With the exception of $\mathbb{Q}(\sqrt{-15})$, which has class number 2, all of these fields have class number divisible by 10, ranging from 10 to 64445120. This leads us to ask:

Question 2.6.13. Let $K \neq \mathbb{Q}(\sqrt{-15})$ be an imaginary quadratic field where $Y_1(16)$ has a point. Is it necessarily the case that the class number of K is divisible by 10?

A partial result towards answering this question can be obtained using the fascinating work of Gillibert and Levin [20]. Computing the torsion subgroup of $J_1(16)(\mathbb{Q})$ we find that this group has a point of order 10. The techniques of [20] allow us to map this point to an ideal class in K which has order dividing 10. One must then ask whether this ideal class has order 10. At present, the best result we can prove is the following.

Theorem 2.6.14. *There are infinitely many imaginary quadratic fields K such that $X_1(16)$ has a quadratic point over K and the class number of K is divisible by 10.*

Proof. Note that $X_1(16)$ is a hyperelliptic curve with a rational Weierstrass point, and $J_1(16)$ has a rational point of order 10. The proofs of Corollaries 3.1 and 3.2 in [20] show how to construct an infinite set of imaginary quadratic fields K whose class numbers are divisible by 10. Moreover, these fields K are, by construction, the fields of definition of quadratic points on $X_1(16)$. □

2.7 Points over a given quadratic field

We address here the problem of determining whether the torsion structures $\mathbb{Z}/13, \mathbb{Z}/16$, and $\mathbb{Z}/18$ occur over a fixed quadratic field K. Before restricting to these groups, we briefly discuss the more general question:

Problem 2.7.1. Given a quadratic field K, determine which groups occur as torsion subgroups of elliptic curves E/K.

This is equivalent to deciding whether certain modular curves $X_1(M,N)$ have non-cuspidal points over K. We recall the approach to Problem 2.7.1 suggested in [32, p. 293]:

- If $X_1(M,N)$ is an elliptic curve: Try to compute its rank over K. If the rank is positive, then the curve $X_1(M,N)$ has infinitely many points over K, and therefore must have non-cuspidal points. If the rank is 0, then all the points of $X_1(M,N)$ over K can be determined, and one just has to check whether one of these points is not a cusp.

- If $X_1(M,N)$ has genus 2: The curve $X_1(M,N)$ has only a finite number of points over K, by Faltings' theorem, and one must try to find all of them. Let J be the Jacobian variety of $X_1(M,N)$. One has some hope of being able to determine all K-rational point on $X_1(M,N)$ if $J(K)$ is finite. Two ways are suggested for attempting to show that $J(K)$ has rank 0:

1. By performing a 2-descent one can obtain an upper bound for the rank. If this upper bound is 0, then $J(K)$ is certainly finite.
2. A criterion is given [32, Thm. 11] which provides sufficient conditions for $J(K)$ to be finite in the case of the curves $X_1(13)$ and $X_1(18)$.

Assuming success in proving that $J(K)$ is finite, one might then determine the K-rational points on $X_1(M,N)$ and see whether one of them is not a cusp. If the rank of $J(K)$ can be shown to be 1, then the method of Chabauty and Coleman might still be used to determine the K-rational points on $X_1(M,N)$.

There are a few drawbacks to the above strategy. For the curves of genus 2, even if $J(K)$ has rank 0, a 2-descent may be computationally expensive and moreover fail to prove that the rank is 0. Also, the criterion given to prove that $J_1(13)$ and $J_1(18)$ have finitely many points over K applies only to imaginary quadratic fields K, and in the case of $J_1(18)$ one must further assume that 2 does not split in K. However, by Theorems 2.6.5 and 2.6.9, for such fields K we already know that $Y_1(13)$ and $Y_1(18)$ have no points over K. Hence, for the purpose of computing the full set of K-rational points on these two curves, the criterion is irrelevant.

We propose here a different method, in which one only needs to determine whether a quadratic twist of $X_1(N)$ has a rational point.

Notation 2.7.2. Let C be a hyperelliptic curve given by a model $y^2 = f(x)$, and let d be a squarefree integer. We denote by C^d the quadratic twist of C by d, i.e., the hyperelliptic curve defined by $dy^2 = f(x)$.

Lemma 2.7.3. *Let $K = \mathbb{Q}(\sqrt{d})$ be a quadratic field, where d is a squarefree integer. For $N \in \{13, 18\}$ the following are equivalent:*

1. $Y_1(N)(K) \neq \emptyset$.

2. $X_1^d(N)(\mathbb{Q}) \neq \emptyset$.

Proof. (1) $\Longrightarrow$ (2): Note first that it follows from Theorems 2.6.5 and 2.6.9 that every non-cuspidal quadratic point on $X_1(N)$ is obvious for the model $y^2 = f_N(x)$. Suppose that $Y_1(N)$ has a point P defined over K. Since $Y_1(N)$ has no rational point, P is a non-cuspidal quadratic point on $X_1(N)$. Hence, P must be of the form $(x_0, \sqrt{f_N(x_0)})$ for some $x_0 \in \mathbb{Q}$. Then d must be the squarefree part of $f_N(x_0)$, so there is a rational s such that $ds^2 = f_N(x_0)$. This shows that $X_1^d(N)(\mathbb{Q}) \neq \emptyset$.

(2) $\Longrightarrow$ (1): Let $P \in X_1^d(N)(\mathbb{Q})$. Note that $X_1^d(N)$ has no rational point at infinity, since the leading coefficient of $d \cdot f_N(x)$ is d. Therefore, $P = (x_0, s)$ for some $x_0, s \in \mathbb{Q}$. We thus have $ds^2 = f_N(x_0)$ with $s \neq 0$, since $f_N(x)$ is irreducible. Hence, $Q := (x_0, s\sqrt{d}) \in X_1(N)(K)$ is an obvious quadratic point. By (2.4) we know that for $N = 13$, $X_1(N)$ has no quadratic cusp, and for $N = 18$ the only quadratic cusps are non-obvious. Therefore, Q must be a non-cuspidal quadratic point. This shows that $Y_1(N)(K) \neq \emptyset$. $\square$

In view of Lemma 2.7.3 we must discuss the following:

Problem 2.7.4. Given a curve $C/\mathbb{Q}$ of genus 2, decide whether $C(\mathbb{Q}) = \emptyset$.

There are several computational tools that can be used to attack this problem. First, a search for rational points on a given hyperelliptic curve can be carried out using Stoll's `ratpoints` program, which is available in Magma via the `Points` function. As explained in [71, §2.1], one can reasonably expect that if C has a rational point, it will be found by this method. If no rational point on C is found, we may attempt to show that $C(\mathbb{Q}) = \emptyset$. As a first test we determine whether C has points over all completions of $\mathbb{Q}$; this can be done using the Magma command `HasPointsEverywhereLocally`. If the result is negative, then we know that $C(\mathbb{Q}) = \emptyset$. If, however, C does have points over all completions, then we can compute the *fake 2-Selmer set* of C (see [6] for details); for this we use the Magma function `TwoCoverDescent`. If this set is empty, then we know with certainty that $C(\mathbb{Q}) = \emptyset$. For further techniques and more information on this problem we refer the reader to the articles [71, 5].

Example 2.7.5. Let $K = \mathbb{Q}(\sqrt{d})$, where $d = 1009$. We will determine whether the torsion structure $\mathbb{Z}/18$ occurs over K. A search for rational points on the twist $X_1^d(18)$ immediately yields the point $(\frac{5}{3}, \frac{11}{27})$. By Lemma 2.7.3 this implies that the group $\mathbb{Z}/18$ does occur as the torsion subgroup of an elliptic curve over K. Furthermore, since we have the point

$$\left(\frac{5}{3}, \frac{11\sqrt{d}}{27}\right) \in Y_1(18)(K),$$

we can use the change of variables in [59, p. 39] to find an elliptic curve over K with a point of order 18. We obtain the curve E/K with a-invariants $[a_1, a_2, a_3, a_4, a_6]$ as follows:

$$[1452\sqrt{1009}{+}49925, -42721140\sqrt{1009}{-}1355613420, -197585272500\sqrt{1009}{-}6269712067500, 0, 0].$$

One can verify that the point $(0, 0) \in E(K)$ has order 18, so that $E(K)_{\text{tors}} \cong \mathbb{Z}/18$.

Example 2.7.6. Let $K = \mathbb{Q}(\sqrt{d})$, where $d = 2657$. We will determine whether the torsion structure $\mathbb{Z}/13$ occurs over K. A 2-descent yields an upper bound of 2 for the rank of $J_1(13)(K)$. To see this we use the fact that, since $J_1(13)(\mathbb{Q})$ has rank 0, the rank of $J_1(13)(K)$ is equal to the rank of $\mathrm{Jac}(T)(\mathbb{Q})$, where $T := X_1^d(13)$ is the twist by d. The Magma code for this calculation is shown below.

```
> _<x> := PolynomialRing(Rationals());

> f13 := x^6 - 2*x^5 + x^4 - 2*x^3 + 6*x^2 - 4*x + 1;

> X13 := HyperellipticCurve(f13);

> T := QuadraticTwist(X13,2657);

> RankBound(Jacobian(T));

2
```

Note also that K is a real quadratic field where 2 splits. Hence, none of the ideas proposed in [32] apply in this context. By Lemma 2.7.3, the problem at hand is equivalent to deciding whether T has a rational point. To do this we will follow the steps suggested above. First, we carry out a search for rational points on T:

```
> Points(T : Bound := 10^5);
{@ @}
```

Since no points are found, we suspect that there are none. Next, we test whether T has points over all completions of $\mathbb{Q}$:

```
> g,h := HyperellipticPolynomials(T);
> HasPointsEverywhereLocally(g,2);
true
```

Hence, there is no local obstruction to T having a rational point. Finally, we compute the fake 2-Selmer set of T:

```
> IsEmpty(TwoCoverDescent(T));
true
```

Since the fake 2-Selmer set is empty, it follows that $T(\mathbb{Q}) = \emptyset$. We conclude that there does not exist an elliptic curve E over the field $K = \mathbb{Q}(\sqrt{2657})$ such that $E(K)_{\text{tors}} \cong \mathbb{Z}/13$.

To further illustrate the applicability of our method we will attempt to determine all fields $K = \mathbb{Q}(\sqrt{d})$ with $d < 1000$ where the curves $Y_1(N)$, $N \in \{13, 18\}$, have points.

Theorem 2.7.7. *The ordered set of squarefree integers d such that $Y_1(18)$ has a point over the field $K = \mathbb{Q}(\sqrt{d})$ begins with the values $d = 33, 337, 457$ and contains no other number smaller than 1000, except possibly $d = 681$.*

Proof. We make a list of all 607 squarefree integers d between 2 and 1000, and remove from the list all those values of d satisfying any of the following conditions:

1. $d \not\equiv 1 \bmod 8$ or $d \equiv 2 \bmod 3$.
2. d is divisible by some prime in $\Pi(f_{18})$.
3. The Jacobian of $X_1^d(18)$ has rank 0, and $X_1^d(18)(\mathbb{Q}) = \emptyset$.
4. $X_1^d(18)(\mathbb{Q}_p) = \emptyset$ for some prime p.
5. The fake 2-Selmer set of $X_1^d(18)$ is empty.

By Theorem 2.6.5 and Lemma 2.7.3, every $d < 1000$ such that $Y_1(18)$ has a point over $\mathbb{Q}(\sqrt{d})$ will belong to the resulting list. Initially, the list of numbers d contains 607 elements. After step (1), 58 remain; after step (2), 18 are left; after step (3) the following 6 numbers remain:

$$33, 201, 337, 417, 457, 681.$$

After step (4) we obtain the list

$$33, 337, 457, 681.$$

With step (5) we do not eliminate any numbers. For each of the remaining values of d we now search for rational points on the twist $X_1^d(18)$. For $d = 33, 337, 457$ we do find rational points, but not for $d = 681$. Our method has not succeeded in deciding whether the twist by 681 has a rational point. □

Theorem 2.7.8. *The ordered set of squarefree integers d such that $Y_1(13)$ has a point over the field $K = \mathbb{Q}(\sqrt{d})$ begins with the values $d = 17, 113, 193$. It contains the numbers $d = 313$ and 481, and no other number smaller than 1000, except possibly $d = 257, 353, 601, 673$.*

Proof. We make a list of all squarefree integers d between 2 and 1000, and remove from the list all those values of d satisfying any of the following conditions:

1. $d \not\equiv 1 \bmod 8$.

2. d is divisible by some prime in $\Pi(f_{13})$.

3. The Jacobian of $X_1^d(13)$ has rank 0, and $X_1^d(13)(\mathbb{Q}) = \emptyset$.

4. $X_1^d(13)(\mathbb{Q}_p) = \emptyset$ for some prime p.

5. The fake 2-Selmer set of $X_1^d(13)$ is empty.

By Theorem 2.6.9 and Lemma 2.7.3, every $d < 1000$ such that $Y_1(13)$ has a point over $\mathbb{Q}(\sqrt{d})$ will belong to the resulting list. Initially, the list of numbers d contains 607 elements. After step (1), 97 remain; after step (2), 26 are left; after step (3) the following 11 numbers remain:

$$17, 113, 193, 257, 313, 353, 377, 409, 481, 601, 673.$$

After step (4) the number 377 is removed and we obtain the list

$$17, 113, 193, 257, 313, 353, 409, 481, 601, 673.$$

With step (5) we eliminate the number 409 to obtain

$$17, 113, 193, 257, 313, 353, 481, 601, 673.$$

For each of these values of d we now search for rational points on the twist $X_1^d(13)$. For $d = 17, 113, 193, 313$, and 481 we do find rational points, but not for $d = 257, 353, 601, 673$. We suspect that the twists by the latter values of d have no rational point, but are unable to prove it. □

Chapter 3

Squarefree parts of polynomial values

3.1 Introduction

We studied in §2.6 three polynomials, namely $f_{13}(x), f_{16}(x), f_{18}(x)$, and showed that they have the following properties:

- If K is a quadratic field of the form $K = \mathbb{Q}(\sqrt{f_{13}(x_0)})$ with $x_0 \in \mathbb{Q}$, then its discriminant D satisfies $D \equiv 1 \bmod 8$.

- If K is a quadratic field of the form $K = \mathbb{Q}(\sqrt{f_{18}(x_0)})$ with $x_0 \in \mathbb{Q}$, then its discriminant D satisfies $D \equiv 1 \bmod 8$ and $D \equiv 0, 1 \bmod 3$.

- For $f_{16}(x)$ there appear to be no analogous congruences that are always satisfied.

What is different about $f_{16}(x)$ that we were not able to find such congruences? And for the polynomials $f_{13}(x)$ and $f_{18}(x)$, are there other congruences that we have not discovered? We mention the following facts which have been verified by explicit computation:

- Let $p < 10^5$ be a prime, $p \neq 2$. Then every nonzero congruence class modulo p is represented by the discriminant D of a quadratic field of the form $\mathbb{Q}(\sqrt{f_{13}(x_0)})$ with $x_0 \in \mathbb{Q}$.

- Let $p < 10^5$ be a prime, $p \neq 2, 3$. Then every nonzero congruence class modulo p is represented by the discriminant D of a quadratic field of the form $\mathbb{Q}(\sqrt{f_{18}(x_0)})$ with $x_0 \in \mathbb{Q}$.
- Let $p < 10^4$ be a prime. Then every nonzero congruence class modulo p is represented by the discriminant D of a quadratic field of the form $\mathbb{Q}(\sqrt{f_{16}(x_0)})$ with $x_0 \in \mathbb{Q}$.

Hence, the polynomials $f_{13}(x)$ and $f_{18}(x)$ exhibit special behavior at the primes $p = 2$ and $p = 2, 3$, respectively, and apparently at no other primes. In contrast, it seems that $f_{16}(x)$ does not exhibit similar behavior at any prime. In this chapter we explore phenomena of this type. Rather than restrict attention to the three polynomials above, we consider more generally an arbitrary polynomial $f(x) \in \mathbb{Z}[x]$ and ask whether there are any nontrivial congruences satisfied by the discriminants of quadratic fields $\mathbb{Q}(\sqrt{f(r)})$ for $r \in \mathbb{Q}$.

3.2 Statement of the problem

Recall that the *squarefree part* of a nonzero rational number r is the unique squarefree integer D such that r/D is a square in $\mathbb{Q}$. We will denote the squarefree part of r by $S(r)$. The number $S(r)$ can also be defined by the following formula:

$$S(r) = \operatorname{sign}(r) \cdot \prod_{\operatorname{ord}_p(r) \text{ odd}} p.$$

Let $f(x)$ be a polynomial with integer coefficients, and let p be a prime. In this chapter we consider the following question:

Does the set $\{S(f(r)) : r \in \mathbb{Q} \text{ and } f(r) \neq 0\}$ contain an element from every congruence class modulo p?

As will be seen below, there are pairs $(f(x), p)$ for which this property holds, and others for which it does not; our main goal is to understand precisely what makes the distinction. In studying the above question we will make two simplifying assumptions. First, we assume that $f(x)$ is squarefree. There is not much loss in this, because if $d(x)$ is the squarefree part of $f(x)$, then $S(f(r)) = S(d(r))$ for every rational number r which is not a root of $f(x)$. Second, in order to avoid certain degenerate behavior, a restriction will be made on the prime p:

Definition 3.2.1. We say that a prime p is *good* for a given polynomial $f(x) \in \mathbb{Z}[x]$ if the reduced polynomial $f(x) \bmod p \in \mathbb{F}_p[x]$ has the same degree as $f(x)$ and has nonzero discriminant.

Notation 3.2.2. For a polynomial $f(x) \in \mathbb{Z}[x]$ and a prime number p, we let $\Sigma(f, p)$ denote the image of the set $\{S(f(r)) : r \in \mathbb{Q} \text{ and } f(r) \neq 0\}$ under the reduction map $\mathbb{Z} \longrightarrow \mathbb{Z}/p$.

With this notation and terminology we can now rephrase our main question.

Let $f(x) \in \mathbb{Z}[x]$ have nonzero discriminant, and let p be a good prime for $f(x)$. Is

$$\Sigma(f, p) = \mathbb{F}_p?$$

We begin by giving necessary and sufficient conditions to have $0 \in \Sigma(f, p)$.

Proposition 3.2.3. *Let $f(x) \in \mathbb{Z}[x]$ have nonzero discriminant, and let p be a good prime for $f(x)$. If $f(x)$ has odd degree, then $0 \in \Sigma(f, p)$. If $f(x)$ has even degree, then $0 \in \Sigma(f, p)$ if and only if $f(x)$ has a root modulo p.*

Proof. Suppose that $f(x)$ has odd degree, and write $f(x) = a_{2k-1}x^{2k-1} + \cdots + a_1x + a_0$. Letting d be any integer such that $\operatorname{ord}_p(d)$ is odd and $f(1/d) \neq 0$, we claim that p divides $S(f(1/d))$. To see this, note first that $S(f(1/d)) = S(d^{2k}f(1/d)) = S(a_{2k-1}d + \cdots + a_0d^{2k})$, so it suffices to show that $\operatorname{ord}_p(a_{2k-1}d + \cdots + a_0d^{2k})$ is odd. But the latter is clearly equal to $\operatorname{ord}_p(d)$, which is odd by construction. This shows that $0 \in \Sigma(f, p)$.

Suppose now that $f(x)$ has even degree. Assuming that $f(x)$ has a root modulo p, we must show that $0 \in \Sigma(f,p)$. Since the root of $f(x)$ modulo p must be simple, there is an integer n such that $f(n) \neq 0$ and p divides $f(n)$ but not $f'(n)$. If $\mathrm{ord}_p(f(n))$ is odd, then we are done. Otherwise, let $\mathrm{ord}_p(f(n)) = 2s$, and $r = n + p^{2s-1}$. By doing a Taylor expansion we see that $f(r) = f(n) + f'(n)p^{2s-1} + A$, where A is divisible by p^{4s-2}. It follows that $\mathrm{ord}_p(f(r)) = 2s-1$ is odd, so p divides $S(f(r))$, and hence $0 \in \Sigma(f,p)$.

Finally, assuming that $f(x)$ does not have a root modulo p we must show that $0 \notin \Sigma(f,p)$. This will follow from the proof of Proposition 3.5.1 below, so we omit the proof here. □

In view of Proposition 3.2.3 we will henceforth be interested only in determining whether $\Sigma(f,p) \supseteq \mathbb{F}_p^*$.

3.3 Degrees 1 and 2

Proposition 3.3.1. *Suppose that $f(x) \in \mathbb{Z}[x]$ has degree 1, and let p be a good prime for $f(x)$. Then $\Sigma(f,p) = \mathbb{F}_p$.*

Proof. We know that $0 \in \Sigma(f,p)$ by Proposition 3.2.3. Given any integer $m \not\equiv 0 \bmod p$, we will show that there is an integer r such that $S(f(r)) \equiv m \bmod p$. We reduce easily to the case where $f(x) = d(ax+b)$ with $\gcd(a,b) = 1$ and d squarefree. Since p does not divide ad, there is an integer t such that $t \equiv b \bmod a$ and $dt \equiv m \bmod p$. The integer t is coprime to ap, so by Dirichlet's theorem on primes in arithmetic progressions, there are infinitely many prime numbers q such that $q \equiv t \bmod ap$. Choose such a prime q which does not divide d. By construction, there exists an integer n such that $q = an + b$. For this integer n we have $S(f(n)) = S(dq) = dq \equiv m \bmod p$. □

Next, we consider polynomials $f(x)$ of degree 2. We will need the following classical result due to Legendre. (See [25, §17.3] for a proof.)

Theorem 3.3.2 (Legendre)**.** *Let a, b, c be nonzero integers, squarefree, pairwise coprime, and not all positive nor all negative. Then the equation $ax^2 + by^2 + cz^2 = 0$ has a nontrivial integral solution if and only if the following conditions are satisfied:*

(i) $-bc$ is a square modulo a.

(ii) $-ac$ is a square modulo b.

(iii) $-ab$ is a square modulo c.

Proposition 3.3.3. *Suppose that $f(x) \in \mathbb{Z}[x]$ has degree 2 and nonzero discriminant. If p is a good prime for $f(x)$, then $\Sigma(f, p) \supseteq \mathbb{F}_p^*$.*

Proof. Let $f(x) = ax^2 + bx + c$ and $\Delta = b^2 - 4ac$. Let d be the squarefree part of a, and δ the squarefree part of Δ, so that we can write

$$a = ds^2 \ , \ \Delta = \delta t^2$$

for some integers s, t. Given any integer m coprime to p, we have to show that there is a rational number r such that $S(f(r)) \equiv m \bmod p$. We claim that there exists a prime number q such that

$$q \equiv 1 \bmod a\Delta \ , \ \ dq \equiv m \bmod p \ , \ \text{and } \delta \text{ is a square modulo } q.$$

Assuming this claim for the moment, it follows from Theorem 3.3.2 that there is a nontrivial integral solution to the equation $x^2 - qy^2 - \delta z^2 = 0$. The plane conic defined by this equation is then isomorphic to $\mathbb{P}^1$, and therefore has infinitely many rational points. In particular, there exists a rational solution to $x^2 - qy^2 = \delta$ with $y \neq 0$, and therefore a rational solution

(x, y) to the equation $x^2 - qy^2 = \Delta$, with $y \neq 0$. Letting

$$r = \frac{x-b}{2a}\ , \quad w = \frac{ys}{2a}$$

we obtain $dqw^2 = f(r)$ with $f(r) \neq 0$. Therefore, $dq = S(f(r))$ and, by construction, $dq \equiv m \bmod p$. This concludes the proof of the proposition.

Now for a proof of the claim. By the Chinese Remainder Theorem there exists an integer N such that $N \equiv 1 \bmod 8a\Delta$ and $dN \equiv m \bmod p$. (In the case $p = 2$ the numbers $8a\Delta$ and p are not coprime, but we can take $N = 1$ in this case.) Since N is coprime to $8ap\Delta$, by Dirichlet's theorem on primes in arithmetic progressions there exists a prime q such that $q \equiv N \bmod 8ap\Delta$. In particular,

$$q \equiv 1 \bmod a\Delta\ , \quad dq \equiv m \bmod p\ , \quad q \equiv 1 \bmod 8.$$

We will show that δ is a square modulo q. Write $\delta = (-1)^\eta 2^\varepsilon q_1 \cdots q_v$, where $\eta, \varepsilon \in \{0, 1\}$ and the q_i are distinct odd primes. Since $q \equiv 1 \bmod 8$ and $q \equiv 1 \bmod q_i$, then

$$\left(\frac{\delta}{q}\right) = \left(\frac{-1}{q}\right)^\eta \left(\frac{2}{q}\right)^\varepsilon \prod_{i=1}^{v} \left(\frac{q_i}{q}\right) = 1 \cdot 1 \cdot \prod_{i=1}^{v} \left(\frac{q}{q_i}\right) = \prod_{i=1}^{v} \left(\frac{1}{q_i}\right) = 1,$$

and this proves the claim. □

3.4 Degrees 3 and 4

Before considering polynomials of degrees 3 and 4 we recall the statement of the Parity Conjecture for elliptic curves over $\mathbb{Q}$. Let $E/\mathbb{Q}$ be an elliptic curve of conductor N_E. The L-function $L(E, s)$ admits an analytic continuation to the complex plane $\mathbb{C}$, and satisfies a functional equation

$$\Lambda(E, s) = w_E \Lambda(E, 2 - s)$$

where $w_E \in \{\pm 1\}$ is the *root number* of E and

$$\Lambda(E, s) = N_E^{s/2} (2\pi)^{-s} \Gamma(s) L(E, s).$$

Conjecture 3.4.1 (Parity Conjecture). *If E is an elliptic curve over $\mathbb{Q}$, then*

$$w_E = (-1)^{\operatorname{rank}(E(\mathbb{Q}))}.$$

The root number of E is related to the root number of a quadratic twist of E in the following way. For every quadratic number field K there is a *Dirichlet character*

$$\chi_K : (\mathbb{Z}/D\mathbb{Z})^\times \longrightarrow \{\pm 1\},$$

where D is the discriminant of K, satisfying the following properties:

- $\chi_K(-1) = \operatorname{sign}(D)$.
- If D is odd, then $\chi_K(2) = (-1)^{(D^2-1)/8}$.
- For an odd prime p not dividing D, $\chi_K(p) = \left(\frac{D}{p}\right)$.

Lemma 3.4.2. *Let E be an elliptic curve over $\mathbb{Q}$, D a squarefree integer, and E^D the quadratic twist of E by D. Let $K = \mathbb{Q}(\sqrt{D})$. If N_E is coprime to the discriminant of K, then*

$$w_{E^D} = w_E \cdot \chi_K(-N_E).$$

Proposition 3.4.3. *Assume the Parity Conjecture. Let $f(x) \in \mathbb{Z}[x]$ have degree 3 or 4, and nonzero discriminant. If p is a good prime for $f(x)$, then $\Sigma(f, p) \supseteq \mathbb{F}_p^*$.*

Proof. Given any integer m coprime to p, we have to show that there is a rational number r such that $S(f(r)) \equiv m \bmod p$. Let d be the squarefree part of the leading coefficient of $f(x)$, and let $g(x) = d \cdot f(x)$. The hyperelliptic curve E defined by the equation $y^2 = g(x)$ then has a rational point at infinity, so it is an elliptic curve over $\mathbb{Q}$. Let

$$N_E = 2^f \prod_{i=1}^{v} p_i^{f_i}$$

be the prime factorization of the conductor of E. Note that p is coprime to N_E, since p is good for $g(x)$. We will assume that $w_E = 1$; the other case is dealt with in a similar way. By Dirichlet's theorem on primes in arithmetic progressions, there are infinitely many prime numbers q such that

$$q \equiv -1 \bmod 8\ , \quad dq \equiv -m \bmod p\ , \text{ and } q \equiv -1 \bmod p_i \text{ for all } i.$$

Choose such a prime q not dividing d. Let $D = -q$, and let χ be the Dirichlet character associated to $\mathbb{Q}(\sqrt{D})$. By Lemma 3.4.2 we have

$$w_{E^D} = \chi(-N_E) = (-1) \cdot \chi(2)^f \prod_{i=1}^{v} \chi(p_i)^{f_i} = (-1) \cdot (-1)^{(D^2-1)/8} \prod_{i=1}^{v} \left(\frac{D}{p_i}\right)^{f_i} = -1.$$

By the Parity Conjecture, this implies that $\operatorname{rank}(E^D(\mathbb{Q}))$ is odd, hence positive, so there are infinitely many rational solutions to the equation $Dy^2 = g(x)$. In particular, there is a solution (r, s) with $g(r) \neq 0$. Note that $Dd(s/d)^2 = f(r)$ with Dd squarefree, so $Dd = S(f(r))$; and by construction, $Dd \equiv m \bmod p$. This completes the proof. □

3.5 Higher degrees

In view of the positive results in degrees 1-4 we naturally consider the following statement:

($\star$) *Let $f(x) \in \mathbb{Z}[x]$ have nonzero discriminant, and let p be a good prime for $f(x)$. Then $\Sigma(f,p) \supseteq \mathbb{F}_p^*$.*

We have shown that ($\star$) is true if $f(x)$ has degree 1 or 2, and — assuming the Parity Conjecture — that it also holds when $f(x)$ has degree 3 or 4. However, for polynomials of higher degree the statement may fail to hold; the following proposition gives a way of constructing examples where this occurs.

Proposition 3.5.1. *Let $f(x) \in \mathbb{Z}[x]$ have even degree $2k$, and let p be a good prime for $f(x)$ such that $f(x)$ has no roots modulo p. Let a_{2k} be the leading coefficient of $f(x)$, and suppose that $f(\mathbb{F}_p)$ is contained in the square class of a_{2k} modulo p. Then $\Sigma(f,p)$ is contained in the square class of a_{2k} modulo p.*

Proof. Set $f(x) = a_{2k}x^{2k} + \cdots + a_1x + a_0$. Let $r \in \mathbb{Q}$ be expressed as $r = n/d$ in lowest terms, and let $D = S(f(r))$. Note that $S(f(r)) = S(d^{2k}f(r)) = S(a_{2k}n^{2k} + \cdots + a_1nd^{2k-1} + a_0d^{2k})$, so that we have

$$a_{2k}n^{2k} + \cdots + a_1nd^{2k-1} + a_0d^{2k} = Ds^2$$

for some integer s.

Suppose first that $d \equiv 0 \bmod p$. Reducing the above equation modulo p we obtain $a_{2k}n^{2k} \equiv Ds^2 \bmod p$. Since p divides neither n nor a_{2k}, then D and s are coprime to p. Therefore, $D \equiv a_{2k}n^{2k}s^{-2} \bmod p$, so D is in the square class of a_{2k} modulo p.

Now suppose that $d \not\equiv 0 \bmod p$. We can then consider the equation $d^{2k}f(n/d) = Ds^2$ modulo p. Since f has no roots modulo p, this equation implies that D and s are coprime to p, so D and $f(n/d)$ are in the same square class modulo p. By hypothesis, $f(n/d)$ is in the square class of a_{2k}, so D is also in the square class of a_{2k} modulo p.

□

Corollary 3.5.2. *Let $f(x) \in \mathbb{Z}[x]$ have even degree, and let p be a good prime for $f(x)$. Suppose that the equation $y^2 = f(x)$ has no solutions modulo p, and that the leading coefficient* *of $f(x)$ is not a square modulo p. Then $\Sigma(f,p) \subseteq \mathbb{F}_p^* \backslash (\mathbb{F}_p^*)^2$.*

Proof. Let a be the leading coefficient of $f(x)$, which is not a square modulo p. The fact that there are no solutions to the equation $y^2 = f(x)$ modulo p implies that $f(x)$ has no roots modulo p, and that $f(\mathbb{F}_p)$ contains no squares. Hence $f(\mathbb{F}_p)$ is contained in the square class of a modulo p. It follows from Proposition 3.5.1 that $\Sigma(f,p)$ contains only nonsquares. □

We can use Corollary 3.5.2 to give examples where $(\star)$ fails to hold. To do this we need hyperelliptic curves having no rational points modulo p.

Definition 3.5.3. We say that a smooth projective curve C over $\mathbb{F}_p$ is *pointless* if $C(\mathbb{F}_p) = \emptyset$.

Theorem 3.5.4 (Hasse-Weil)**.** *Let C be a smooth projective curve of genus g over a finite field $\mathbb{F}_q$. Then*

$$|\#C(\mathbb{F}_q) - q - 1| \leq 2g\sqrt{q}.$$

We deduce from Theorem 3.5.4 that if C is a pointless curve over $\mathbb{F}_p$, then $p+1 \leq 2g\sqrt{p}$. This cannot occur if $g = 0$ or 1, but in genus 2 there are pointless curves. A complete list of such curves (up to isomorphism) is given in an article of Maisner and Nart [42]. For genera 3 and 4, pointless curves are studied in [22]. Using these results on pointless curves together with Corollary 3.5.2 we can produce infinitely many examples for which $(\star)$ does not hold.

Example 3.5.5.

1. Let $f(x) \in \mathbb{Z}[x]$ be any polynomial of degree 6 such that

$$f(x) \equiv (-x^2+2)(x^4-5x^3+x^2+x+4) \pmod{11}.$$

Then 11 is a good prime for $f(x)$, but by Corollary 3.5.2, $\Sigma(f, 11)$ does not contain any squares.

2. If $f(x) \in \mathbb{Z}[x]$ is any polynomial of degree 8 such that

$$f(x) \equiv 2x^8 - x^6 - 8x^4 - x^2 + 2 \pmod{19},$$

then $\Sigma(f, 19)$ does not contain any squares modulo 19.

Remark 3.5.6. When the degree of $f(x)$ is 4, we cannot use Corollary 3.5.2 to contradict Proposition 3.4.3 because the necessary hypotheses will never be satisfied: indeed, if $f(x)$ has degree 4 and p is a good prime for $f(x)$, then the equation $y^2 = f(x)$ defines a smooth projective curve C of genus 1 over $\mathbb{F}_p$, and such a curve will always have an $\mathbb{F}_p$-rational point, by the Hasse-Weil bounds. Since we are assuming that the leading coefficient of $f(x)$ is not a square in $\mathbb{F}_p$, the two points of C at infinity are not rational, and hence the equation $y^2 = f(x)$ must have a solution modulo p.

Just as we used pointless curves to give examples where $(\star)$ is false, we can also use curves having many rational points to give a different class of examples. The next result follows immediately from Proposition 3.5.1.

Corollary 3.5.7. *Let $f(x) \in \mathbb{Z}[x]$ have even degree, and let p be a good prime for $f(x)$. Suppose that the leading coefficient of $f(x)$ is a square modulo p, and that $f(\mathbb{F}_p) \subseteq (\mathbb{F}_p^*)^2$. Then $\Sigma(f, p) \subseteq (\mathbb{F}_p^*)^2$.*

Note that, with $f(x)$ as in the above corollary, the hyperelliptic curve defined by $y^2 = f(x)$ will have $2p + 2$ rational points.

Definition 3.5.8. We say that a hyperelliptic curve C over $\mathbb{F}_p$ is *pointful* if $\#C(\mathbb{F}_p) = 2p+2$, that is, if C has as many rational points as a hyperelliptic curve over $\mathbb{F}_p$ could possibly have.

Despite the opposite nature of pointless and pointful hyperelliptic curves, there is in fact a natural relation between the two: given a pointless curve we can construct from it a pointful one, and vice versa.

Lemma 3.5.9. *Let C be a hyperelliptic curve over $\mathbb{F}_p$ defined by an equation $y^2 = f(x)$, where $f(x)$ has even degree. Let $a \in \mathbb{F}_p^*$ be a non-square, and define $g(x) = a \cdot f(x)$. Let C' be the hyperelliptic curve defined by the equation $y^2 = g(x)$. Then C is pointless if and only if C' is pointful.*

Proof. Suppose that C is pointless. Since the leading coefficient of $f(x)$ is not a square, then the leading coefficient of $g(x)$ is a square; hence, the points of C' at infinity are rational. For any $\alpha \in \mathbb{F}_p$ we know that $f(\alpha)$ is not a square. It follows that $g(\alpha) = a \cdot f(\alpha)$ is a nonzero square, say $\beta^2 = g(\alpha)$. Thus, α gives rise to two rational points $(\alpha, \beta), (\alpha, -\beta)$. This shows that C' has $2p$ affine rational points, and we conclude that C' is pointful. The reverse direction of the lemma is entirely analogous to this one, so we omit the proof. □

Using Lemma 3.5.9 we can modify the polynomials from Example 3.5.5 to give infinitely many new examples where $(\star)$ fails.

Example 3.5.10.

1. Let $g(x) \in \mathbb{Z}[x]$ be any polynomial of degree 6 such that

$$g(x) \equiv -(-x^2 + 2)(x^4 - 5x^3 + x^2 + x + 4) \pmod{11}.$$

   Then 11 is a good prime for $g(x)$, but by Corollary 3.5.7, $\Sigma(g, 11)$ only contains squares.

2. If $g(x) \in \mathbb{Z}[x]$ is any polynomial of degree 8 such that $g(x) \equiv 2(2x^8 - x^6 - 8x^4 - x^2 + 2)$ (mod 19), then $\Sigma(g, 19)$ only contains squares.

We end by listing some questions for future work:

1. By the Hasse-Weil bounds, examples where $(\star)$ fails can only be constructed using Corollaries 3.5.2 and 3.5.7 if the prime p is small compared to the degree of $f(x)$. Does $(\star)$ hold for all large enough primes p?

2. Throughout this chapter we have evaluated $f(x)$ at rational numbers r. Would $(\star)$ hold if we restrict to integer values of r? The proof of Proposition 3.3.1 shows that this does hold when the degree of $f(x)$ is 1; however, it is not clear what will occur for larger degrees.

3. The same questions studied in this chapter could be asked for curves of the form $y^n = f(x)$ with $n > 2$, rather than just for $n = 2$. Do similar patterns hold for larger values of n?

4. All of the examples we have found where $(\star)$ fails to hold have $f(x)$ with even degree. Is $(\star)$ necessarily true for polynomials of odd degree?

Chapter 4

Preperiodic points for quadratic polynomials over number fields

4.1 Introduction

Let K be a field and let $\varphi : \mathbb{P}^n \longrightarrow \mathbb{P}^n$ be a morphism defined over K. For any point $P \in \mathbb{P}^n(K)$ we may consider the sequence of all iterates of P under φ:

$$P,\ \varphi(P),\ \varphi(\varphi(P)),\ \varphi(\varphi(\varphi(P))),\ \ldots.$$

We say that P is **preperiodic** for φ if this sequence contains only finitely many distinct elements; that is, if the set $\{\varphi^n(P) : n \geq 0\}$ is finite. Equivalently, P is preperiodic for φ if there are distinct positive integers m, n such that $\varphi^n(P) = \varphi^m(P)$. We say that P is **periodic** for φ if it satisfies the stronger condition that there exists a positive integer n for which $\varphi^n(P) = P$. The smallest integer n with this property is called the **period** of P.

Notation 4.1.1. The set of all points $P \in \mathbb{P}^n(K)$ that are preperiodic for φ is denoted by $\mathrm{PrePer}(\varphi, K)$.

In this chapter we carry out a study of preperiodic points in the case that K is a number field and $\varphi : \mathbb{P}^1 \longrightarrow \mathbb{P}^1$ is a quadratic polynomial map. In particular, we discuss in §4.3 an algorithm for computing the set $\mathrm{PrePer}(\varphi, K)$, and in §4.5 we specialize to the case where K is a quadratic number field. Known results in the case $K = \mathbb{Q}$ are summarized in §4.4.

4.2 Northcott's Theorem and Uniform Boundedness

We state here the Uniform Boundedness Conjecture, which was our main motivation for developing the material in this chapter.

Theorem 4.2.1 (Northcott [53])**.** *Let H be the absolute multiplicative height on $\mathbb{P}^n(\bar{\mathbb{Q}})$. For any constants B and D, the set*

$$\{P \in \mathbb{P}^n(\bar{\mathbb{Q}}) : H(P) \leq B \ \textit{ and } \ [\mathbb{Q}(P) : \mathbb{Q}] \leq D\}$$

is finite.

The following theorem is a fundamental finiteness result in arithmetic dynamics.

Theorem 4.2.2 (Northcott [53])**.** *Let K be a number field and let $\varphi : \mathbb{P}^n \longrightarrow \mathbb{P}^n$ be a morphism of degree $d \geq 2$ defined over K. Then the set $\mathrm{PrePer}(\varphi) \subset \mathbb{P}^n(\bar{K})$ is a set of bounded height. In particular, for every integer $D \geq 1$, the set*

$$\bigcup_{[L:K] \leq D} \mathrm{PrePer}(\varphi, L)$$

is finite.

Northcott's theorem implies that φ has only finitely many K-rational preperiodic points. One of the guiding questions in arithmetic dynamics is the following Uniform Boundedness

Conjecture, which predicts the existence of uniform bounds on the number of preperiodic points of a morphism.

Conjecture 4.2.3 (Morton, Silverman [48])**.** *Fix integers $n \geq 1, D \geq 1, d \geq 2$. There exists a constant $M(n, D, d)$ such that for every number field K of degree D, and every morphism $\varphi : \mathbb{P}^n \longrightarrow \mathbb{P}^n$ of degree d defined over K,*

$$\#\operatorname{PrePer}(\varphi, K) \leq M(n, D, d).$$

In the case where $\varphi : \mathbb{P}^1 \longrightarrow \mathbb{P}^1$ is a quadratic polynomial map, Conjecture 4.2.3 would imply that, for a fixed degree D, the number of preperiodic points of φ can be bounded in terms of D only. This special case of the conjecture has not been proved, although some progress has been made in the cases $D = 1$ and 2; a summary of earlier work as well as several new results are presented in §4.4 and §4.5.

4.3 Computation of preperiodic points

Given a number field K and a quadratic polynomial f with coefficients in K, we discuss here a method for computing the preperiodic points of f in K. A very different and more general method is given in a recent preprint of Hutz [23], although at present it has only been implemented in the case where $K = \mathbb{Q}$.

From a theoretical as well as computational perspective, it is useful to note that for the purpose of studying the dynamics of quadratic polynomials it is enough to consider only polynomials of the form $f_c(z) = z^2 + c$: for every quadratic polynomial $f(z) \in K[z]$ there is a unique linear polynomial $g(z) \in K[z]$ and a unique $c \in K$ such that $g \circ f \circ g^{-1} = f_c$. One sees easily that dynamical properties of f, such as the behavior of points under iteration by f, are reflected in the dynamical properties of f_c.

We can therefore restrict attention to the one-parameter family $\{f_c : c \in K\}$.

Notation 4.3.1. If K is a number field and $c \in K$, we let f_c denote the quadratic polynomial $f_c(z) = z^2 + c$.

The set $\mathrm{PrePer}(f_c, K)$ can be given in a natural way the structure of a directed graph by letting the vertices of the graph correspond to the elements $P \in \mathrm{PrePer}(f, K)$, and by drawing directed edges $P \longrightarrow f(P)$ for every such point P.

Notation 4.3.2. The directed graph corresponding to the set $\mathrm{PrePer}(f_c, K)$ will be denoted by $G(f_c, K)$.

We know by Northcott's theorem (4.2.2) that the set $\mathrm{PrePer}(f_c, K)$ is a set of bounded height. The following explicit height bound for the preperiodic points of f_c is proved in [13].

Lemma 4.3.3. *Let K be a number field, and $c \in K$. Then for all points $P \in \mathrm{PrePer}(f_c, K)$ we have*

$$H_K(P) \leq \left(\frac{1+\sqrt{5}}{2}\right)^{[K:\mathbb{Q}]} H_K(c)^{1/2}.$$

Our method for computing the set $\mathrm{PrePer}(f_c, K)$ is to first find all elements of K satisfying the height bound in Lemma 4.3.3, and then to determine which elements of this set of bounded height are preperiodic for f_c. A method for carrying out the first step is given in Chapter 6. For the second step, we need a way to quickly eliminate many elements from the set of elements of bounded height which are not preperiodic for f_c. We discuss here a series of local tests that can be used to do so. Full details and proofs appear in the article of Doyle, Faber, and Krumm [13].

Proposition 4.3.4. *Let K be a number field, and let $P, c \in K$.*

1. *If there exists a maximal ideal $\mathfrak{p}$ of $\mathcal{O}_K$ such that $\mathrm{ord}_{\mathfrak{p}}(P) < 0 \leq \mathrm{ord}_{\mathfrak{p}}(c)$, then P is not preperiodic for f_c.*

2. *If there exists a maximal ideal* $\mathfrak{p}$ *of* $\mathcal{O}_K$ *such that* $\operatorname{ord}_{\mathfrak{p}}(c) < 0$ *and* $\operatorname{ord}_{\mathfrak{p}}(P) \neq \frac{1}{2}\operatorname{ord}_{\mathfrak{p}}(c)$*, then* P *is not preperiodic for* f_c*. In particular, if* $\operatorname{ord}_{\mathfrak{p}}(c)$ *is negative and odd for some maximal ideal* $\mathfrak{p}$*, then* f_c *has no preperiodic point in* K*.*

3. *If there exists a maximal ideal* $\mathfrak{p}$ *of* $\mathcal{O}_K$*, lying above an odd rational prime, such that* $\operatorname{ord}_{\mathfrak{p}}(c) < 0$ *and* $-c$ *is not a square in the completion* $K_{\mathfrak{p}}$*, then* f_c *has no preperiodic point in* K*.*

Proof. See Lemma 4.1 in [13]. □

Proposition 4.3.4 provides a way of showing that a given element $P \in K$ is not preperiodic for f_c, by using the non-Archimedean places of K. Similar tests may be used at the Archimedean places, as shown below.

Proposition 4.3.5. *Let* K *be a number field, and let* $P, c \in K$*.*

1. *If* $|\sigma(P)| > \frac{1}{2} + \sqrt{\frac{1}{4} + |\sigma(c)|}$ *for some embedding* $\sigma : K \hookrightarrow \mathbb{C}$*, then* P *is not preperiodic for* f_c*.*

2. *If* $\sigma(c) > \frac{1}{4}$ *for some embedding* $\sigma : K \hookrightarrow \mathbb{R}$*, then* f_c *has no preperiodic point in* K*.*

3. *Suppose* σ *is a real embedding of* K *such that* $\sigma(c) \leq \frac{1}{4}$*, and set* $a = \frac{1}{2} + \sqrt{\frac{1}{4} - \sigma(c)}$*. If* $|\sigma(P)| > a$*, then* P *is not preperiodic for* f_c*.*

4. *Suppose* σ *is a real embedding of* K *such that* $\sigma(c) < -2$*, and set* $a = \frac{1}{2} + \sqrt{\frac{1}{4} - \sigma(c)}$*. If*
$$\sigma(P) \notin \left[-a, -\sqrt{-a - \sigma(c)}\right] \cup \left[\sqrt{-a - \sigma(c)}, a\right],$$
then P *is not preperiodic for* f_c*.*

Proof. See Lemma 4.2 in [13]. □

We now have in place all necessary tools for determining the set $\mathrm{PrePer}(f_c, K)$ for a given quadratic polynomial f_c over a number field K. First, we must find all elements of the set $\mathcal{B} = \{x \in K : H_K(x) \leq B\}$, where

$$B = \left(\frac{1+\sqrt{5}}{2}\right)^{[K:\mathbb{Q}]} H_K(c)^{1/2}.$$

By Lemma 4.3.3 we know that $\mathrm{PrePer}(f_c, K) \subseteq \mathcal{B}$. Next, every element of $\mathcal{B}$ must be tested using Propositions 4.3.4 and 4.3.5. Letting $\mathcal{C}$ be the set of elements of $\mathcal{B}$ which pass all the tests, we have $\mathrm{PrePer}(f_c, K) \subseteq \mathcal{C}$. Finally, for each element $P \in \mathcal{C}$ we can decide whether P is preperiodic for f_c or not by computing the first n iterates of P, where $n = 1 + \#\mathcal{C}$. To see this, note that if two of these iterates are equal, then P is preperiodic, by definition; and if all n iterates are distinct, then P cannot be preperiodic: if it was, then these n distinct iterates would also be preperiodic, and hence belong to $\mathcal{C}$; but the latter is a set with fewer than n elements.

4.4 Rational preperiodic points

The Uniform Boundedness Conjecture (4.2.3) predicts the existence of a constant M such that for every quadratic polynomial $f \in \mathbb{Q}[z]$ we have $\#\,\mathrm{PrePer}(f, \mathbb{Q}) \leq M$. Even this very special case of the conjecture has not been proved. Walde and Russo [74] carried out an initial study of periodic points for quadratic polynomials over $\mathbb{Q}$; in particular, they described quadratic polynomials with points of periods $1, 2$, and 3, and they asked the question of what the possible periods are for the rational periodic points of a quadratic polynomial over $\mathbb{Q}$. The following series of theorems gives a partial answer to this question.

Theorem 4.4.1 (Morton [47])**.** *There does not exist a quadratic polynomial over $\mathbb{Q}$ with a rational point of period 4.*

Theorem 4.4.2 (Flynn, Poonen, Schaefer [17]). *There does not exist a quadratic polynomial over $\mathbb{Q}$ with a rational point of period 5.*

Theorem 4.4.3 (Stoll [70]). *Assume the Birch and Swinnerton-Dyer Conjecture. Then there does not exist a quadratic polynomial over $\mathbb{Q}$ with a rational point of period 6.*

It is believed that a quadratic polynomial with rational coefficients cannot have rational periodic points of period greater than 3.

Conjecture 4.4.4 (Flynn, Poonen, Schaefer [17]). *If $n \geq 4$, then there does not exist a quadratic polyomial over $\mathbb{Q}$ with a rational periodic point of period n.*

In addition to the evidence provided by the above theorems, there is empirical evidence supporting this conjecture.

Proposition 4.4.5 (Hutz, Ingram [24]). *If c is a rational number with $H(c) \leq 10^8$, then the polynomial $f(z) = z^2 + c$ does not have a rational periodic point of period $n > 3$.*

Assuming Conjecture 4.4.4, Poonen obtained the following upper bound for the number of rational preperiodic points of a quadratic polynomial over $\mathbb{Q}$.

Theorem 4.4.6 (Poonen [58]). *Assume that there does not exist a quadratic polynomial over $\mathbb{Q}$ with a rational periodic point of period $n > 3$. Then for every quadratic polynomial $f(z) \in \mathbb{Q}[z]$,*

$$\#\operatorname{PrePer}(f, \mathbb{Q}) \leq 9.$$

In addition to an upper bound for the number of preperiodic points, Poonen determined that there are, up to isomorphism, only 12 possible graph structures $G(f_c, \mathbb{Q})$ for quadratic polynomials $f_c \in \mathbb{Q}[z]$.

4.5 Quadratic preperiodic points

As a next step to Poonen's results mentioned in the previous section, we consider quadratic polynomials defined over quadratic number fields and study their preperiodic points. In particular, we would like to know how many preperiodic points such a polynomial can have, and what the possible graph structures $G(f_c, K)$ are. A partial answer to these questions is provided by the following result, which was obtained using the computational methods discussed in §4.3.

Theorem 4.5.1 (Doyle, Faber, Krumm [13])**.** *Suppose that there exists a constant N such that $\#\,\mathrm{PrePer}(f, K) \leq N$ for every quadratic number field K and quadratic polynomial $f \in K[z]$. Then $N \geq 15$. Moreover, there are at least 46 directed graphs corresponding to sets $\mathrm{PrePer}(f, K)$ for such a K and f.*

We show in Appendices A.1 and A.2 the 46 graphs mentioned in the theorem, together with a representative example of a field and a polynomial giving rise to each particular structure. For every one of these graphs we may ask the following questions:

- Are there infinitely many quadratic polynomials whose set of preperiodic points has the given structure?
- If there are infinitely many, can they be described explicitly?
- If there are only finitely many, can they all be determined?

In what follows we give a series of four examples showing how the results of Chapter 2 can be used to address these questions. The general strategy is to associate to every graph an algebraic curve parametrizing quadratic polynomials whose preperiodic points have the given structure. In order to study the existence of particular graph structures over a quadratic field, we must then study the quadratic points on these curves.

The following terminology will be used throughout this section.

Definition 4.5.2. Let $f(z)$ be a quadratic polynomial over a field K. A *point of type* m_n for $f(z)$ is an element $x \in K$ that is preperiodic for $f(z)$ and enters an m-cycle after n iterations.

We will need in this section an explicit description of all quadratic points on an elliptic curve, which is provided by the following result.

Lemma 4.5.3. *Let k be a field, and let X/k be an affine curve defined by an equation of the form*

$$y^2 = ax^3 + bx^2 + cx + d,$$

where $a, b, c, d \in k$ and $a \neq 0$. Suppose that $(x, y) \in X(\overline{k})$ is a quadratic point with $x \notin k$. Then there is a point $(x_0, y_0) \in X(k)$ and an element $v \in k$ such that $y = y_0 + v(x - x_0)$ and

$$x^2 + \frac{ax_0 - v^2 + b}{a}x + \frac{ax_0^2 + v^2x_0 + bx_0 - 2y_0v + c}{a} = 0.$$

Proof. Since $y \in k(x)$, we can write $y = p(x)$ for some polynomial $p(t) \in k[t]$ of degree at most 1. Note that x is a root of the polynomial

$$F(t) := at^3 + bt^2 + ct + d - p(t)^2,$$

so $F(t)$ must factor as $F(t) = a(t - x_0)m(t)$, where $m(t)$ is the minimal polynomial of x, and $x_0 \in k$. Since $F(x_0) = 0$, then $(x_0, p(x_0)) \in X(k)$. Letting $y_0 = p(x_0)$ we can write $p(t) = y_0 + v(t - x_0)$ for some $v \in k$; in particular, $y = p(x) = y_0 + v(x - x_0)$. Carrying out the division

$$\frac{F(t)}{a(t - x_0)} = \frac{at^3 + bt^2 + ct + d - (y_0 + v(t - x_0))^2}{a(t - x_0)}$$

we obtain

$$m(t) = t^2 + \frac{ax_0 - v^2 + b}{a}t + \frac{ax_0^2 + v^2x_0 + bx_0 - 2y_0v + c}{a}.$$

□

4.5.1 Graph 10(1,1)a

The search carried out in [13] found the pair

$$(K, c) = \left(\mathbb{Q}(\sqrt{-7}), \frac{3}{16}\right)$$

for which the graph $G(f_c, K)$ is of type 10(1,1)a. We now show that this is the only such pair (K, c) with K a quadratic number field and $c \in K$.

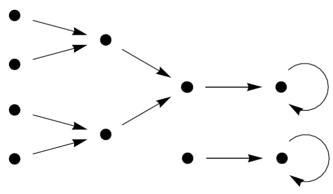


Figure 4.1: Graph type 10(1,1)a

Lemma 4.5.4. *Let $C/\mathbb{Q}$ be the curve of genus 4 defined by the equations*

$$\begin{cases} y^2 = 2(x^3 + x^2 - x + 1) \\ z^2 = -2(x^3 - x^2 - x - 1). \end{cases} \tag{4.1}$$

Consider the rational map $\varphi : C \dashrightarrow \mathbb{A}^3 = \operatorname{Spec} \mathbb{Q}[a, b, c]$ given by

$$a = \frac{y}{x^2 - 1} \quad , \quad b = \frac{z}{x^2 - 1} \quad , \quad c = \frac{-2(x^2 + 1)}{(x^2 - 1)^2}.$$

For every number field K, the map φ induces a surjection from the set

$$\{(x, y, z) \in C(K) : x(x^2 - 1) \neq 0\}$$

to the set of all triples $(a, b, c) \in K^3$ such that a and b are points of type 1_3 for the map f_c satisfying $f_c(a) = -f_c(b)$ and $a \neq \pm b$.

Proof. Fix a number field K and let $(x, y, z) \in C(K)$ satisfy $x(x^2 - 1) \neq 0$. Defining a, b, c as in the lemma, it is a routine calculation to verify that a and b are points of type 1_3 for the map f_c satisfying $f_c(a) = -f_c(b)$. Moreover, $a^2 - b^2 = 4x/(x^2 - 1) \neq 0$, so $a \neq \pm b$. Hence, φ gives a well-defined map.

To see surjectivity, suppose that $a, b, c \in K$ are such that a and b are points of type 1_3 for the map f_c satisfying $f_c(a) = -f_c(b)$ and $a \neq \pm b$. The argument given in [58, p. 22] shows that there is an element $x \in K \setminus \{\pm 1\}$ such that

$$c = \frac{-2(x^2 + 1)}{(x^2 - 1)^2} \quad \text{and} \quad a^2 = \frac{2(x^3 + x^2 - x + 1)}{(x^2 - 1)^2}. \tag{4.2}$$

Since $a^2 + c = f_c(a) = -f_c(b) = -b^2 - c$, then using (4.2) we obtain

$$b^2 = \frac{-2(x^3 - x^2 - x - 1)}{(x^2 - 1)^2}.$$

By assumption we have $a^2 \neq b^2$, and this implies $x \neq 0$. Letting $y = a(x^2 - 1)$, $z = b(x^2 - 1)$ we then have $(x, y, z) \in C(K)$ with $x(x^2 - 1) \neq 0$ and $\varphi(x, y, z) = (a, b, c)$. □

Theorem 4.5.5. *With C as in Lemma 4.5.4 we have the following:*

1. *$C(\mathbb{Q}) = \{(\pm 1, \pm 2, \pm 2)\}$.*

2. *If K is a quadratic field different from $\mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}(\sqrt{-7})$, then $C(K) = C(\mathbb{Q})$.*

3. *For $K = \mathbb{Q}(\sqrt{2})$, $C(K) \setminus C(\mathbb{Q}) = \{(0, \pm\sqrt{2}, \pm\sqrt{2})\}$.*

4. *For $K = \mathbb{Q}(\sqrt{-7})$, $C(K) \setminus C(\mathbb{Q})$ consists of the points $(x, \pm(2x - 4), \pm(2x + 4))$ with $x^2 + 7 = 0$.*

Proof. The equation $y^2 = 2(x^3 + x^2 - x + 1)$ defines the elliptic curve with Cremona label 11a3. This curve has rank 0 and torsion order 5; the affine rational points are $(\pm 1, \pm 2)$. The equation $z^2 = -2(x^3 - x^2 - x - 1)$ defines the same elliptic curve, and the rational points are again $(\pm 1, \pm 2)$. Therefore, $C(\mathbb{Q}) = \{(\pm 1, \pm 2, \pm 2)\}$.

Suppose now that $(x, y, z) \in C(\overline{\mathbb{Q}})$ is a point with $[\mathbb{Q}(x, y, z) : \mathbb{Q}] = 2$, and let $K = \mathbb{Q}(x, y, z)$.

Case 1: $x \in \mathbb{Q}$. We cannot have $x = \pm 1$, since this would imply that $y = \pm 2$ and $z = \pm 2$, contradicting the assumption that (x, y, z) is a quadratic point on C. Hence, $x \neq \pm 1$. It follows that $y \notin \mathbb{Q}$, since having $x, y \in \mathbb{Q}$ would imply that $x = \pm 1$. Similarly, $z \notin \mathbb{Q}$. Therefore, $K = \mathbb{Q}(y) = \mathbb{Q}(z)$, so there is a rational number q such that

$$x^3 + x^2 - x + 1 = -q^2(x^3 - x^2 - x - 1).$$

Letting $w = q(x^3 - x^2 - x - 1)$ we have

$$w^2 = -x^6 + 3x^4 + x^2 + 1 \tag{4.3}$$

Let X be the hyperelliptic curve of genus 2 defined by (4.3). We claim that the following is a complete list of rational points on X:

$$X(\mathbb{Q}) = \{(\pm 1, \pm 2), (0, \pm 1)\}.$$

To see this, note that X has an involution $(x, w) \mapsto (-x, -w)$. The quotient of X by this involution is the elliptic curve 44a1 defined by the equation $v^2 = u^3 + u^2 + 3u - 1$. The quotient map $X \longrightarrow 44a1$ of degree 2 is given by $(x, w) \mapsto (1/x^2, w/x^3)$. The curve 44a1 has exactly 3 rational points, so it follows that X can have at most 6 rational points. Since we have already displayed 6 rational points on X, these must be all such points. Now, we have

$(x, w) \in X(\mathbb{Q})$ with $x \neq \pm 1$, so $x = 0$. By (4.1) we then have $y^2 = z^2 = 2$, so we obtain the quadratic point $(x, y, z) = (0, \pm\sqrt{2}, \pm\sqrt{2})$.

Case 2: x is quadratic. By Lemma 4.5.3 applied to the equation $y^2 = 2(x^3 + x^2 - x + 1)$, there exist a rational number v and a point $(x_0, y_0) \in \{(\pm 1, \pm 2)\}$ such that

$$x^2 + \frac{2x_0 - v^2 + 2}{2} x + \frac{2x_0^2 + v^2 x_0 + 2x_0 - 2y_0 v - 2}{2} = 0. \tag{4.4}$$

Similarly, applying Lemma 4.5.3 to the equation $z^2 = -2(x^3 - x^2 - x - 1)$ we see that there exist a rational number w and a point $(x_1, z_1) \in \{(\pm 1, \pm 2)\}$ such that

$$x^2 + \frac{2x_1 + w^2 - 2}{2} x + \frac{2x_1^2 - w^2 x_1 - 2x_1 + 2z_1 w - 2}{2} = 0. \tag{4.5}$$

Comparing (4.4) and (4.5) we obtain the system

$$\begin{cases} 2x_0 - v^2 + 4 = 2x_1 + w^2 \\ 2x_0^2 + v^2 x_0 + 2x_0 - 2y_0 v = 2x_1^2 - w^2 x_1 - 2x_1 + 2z_1 w. \end{cases}$$

For each choice of points $(x_0, y_0), (x_1, z_1)$ the above system defines a zero-dimensional scheme S in the (v, w) plane over $\mathbb{Q}$, so all its rational points may be determined. There are a total of 16 choices of pairs $(x_0, y_0), (x_1, z_1)$, leading to 16 schemes S. Using the Magma function `RationalPoints` we find all the rational points (v, w) on these schemes, and in every case check whether the polynomial (4.4) is irreducible. This occurs for four of these schemes, and for all of these (4.4) becomes $x^2 + 7 = 0$. The equations (4.1) now imply that $y^2 = (2x - 4)^2$ and $z^2 = (2x + 4)^2$. Therefore, $(x, y, z) \in \{(x, \pm(2x - 4), \pm(2x + 4))\}$. □

Corollary 4.5.6. *Let K be a quadratic field and let $c \in K$. Suppose that $G(f_c, K)$ contains a graph of type* 10(1,1)a. Then $c = 3/16$ and $K = \mathbb{Q}(\sqrt{-7})$.

Proof. By Lemma 4.5.4 there is a point $(x, y, z) \in C(K)$ with $x(x^2 - 1) \neq 0$ such that

$$c = \frac{-2(x^2+1)}{(x^2-1)^2}.$$

It follows from Theorem 4.5.5 that $K = \mathbb{Q}(\sqrt{-7})$ and $x^2 + 7 = 0$. We then obtain $c = \frac{3}{16}$. □

4.5.2 Graph 10(3,2)

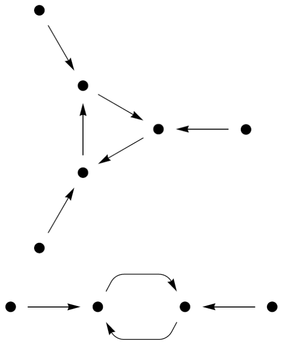


Figure 4.2: Graph type 10(3,2)

Lemma 4.5.7. *Let $C/\mathbb{Q}$ be the affine curve of genus 2 defined by the equation*

$$y^2 = F_{13}(x) := x^6 + 2x^5 + x^4 + 2x^3 + 6x^2 + 4x + 1. \tag{4.6}$$

Consider the rational map $\varphi : C \dashrightarrow \mathbb{A}^3 = \operatorname{Spec} \mathbb{Q}[a, b, c]$ given by

$$a = \frac{x^3 + 2x^2 + x + 1}{2x(x+1)} \quad , \quad b = -\frac{1}{2} + \frac{y}{2x(x+1)} \quad , \quad c = -\frac{x^6 + 2x^5 + 4x^4 + 8x^3 + 9x^2 + 4x + 1}{4x^2(x+1)^2}.$$

For every number field K, the map φ induces a surjection from the set

$$\{(x, y) \in C(K) : x(x+1)(x^2 + x + 1)F_{13}(x) \neq 0\}$$

to the set of all triples $(a, b, c) \in K^3$ *such that* a *and* b *are points of periods* 3 *and* 2*, respectively, for the map* f_c*.*

Proof. Fix a number field K and let $(x, y) \in C(K)$ with $x(x+1)(x^2+x+1)F_{13}(x) \neq 0$. Defining a, b, c as in the lemma, is it easy to check that a is a point of period 3 for f_c and b is a point of period 2. Hence, φ gives a well-defined map.

To see surjectivity, suppose that $a, b, c \in K$ are such that a and b are points of periods 3 and 2, respectively, for f_c. Since b has period 2, then by [58, Thm. 1] there is an element $\sigma \in K$ such that

$$c = -3/4 - \sigma^2 \text{ and } b = -1/2 + \sigma.$$

Moreover, since a is a point of period 3 for f_c, then by [58, Thm. 1] there is an element $\tau \in K \setminus \{0, -1\}$ such that

$$c = -\frac{\tau^6 + 2\tau^5 + 4\tau^4 + 8\tau^3 + 9\tau^2 + 4\tau + 1}{4\tau^2(\tau+1)^2}$$

and a belongs to the set $S = \{\frac{\tau^3+2\tau^2+\tau+1}{2\tau(\tau+1)}, \frac{\tau^3-\tau-1}{2\tau(\tau+1)}, -\frac{\tau^3+2\tau^2+3\tau+1}{2\tau(\tau+1)}\}$. We define an element $x \in K$ as follows: if a is the first element of S, then we set $x = \tau$; if a is the second element of S, then $x = -(\tau+1)/\tau$; if a is the third element of S, then $x = -1/(\tau+1)$. One can verify that in all three cases, $x \neq 0, -1$ and

$$a = \frac{x^3 + 2x^2 + x + 1}{2x(x+1)} \quad , \quad c = -\frac{x^6 + 2x^5 + 4x^4 + 8x^3 + 9x^2 + 4x + 1}{4x^2(x+1)^2}.$$

Furthermore, we must have $x^2 + x + 1 \neq 0$, since otherwise a would be fixed by f_c; similarly, $F_{13}(x) \neq 0$ since otherwise b would be fixed. Equating the above expression for c with the expression $c = -3/4 - \sigma^2$ and letting $y = 2x(x+1)\sigma$ we obtain

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

Thus, we have a point $(x, y) \in C(K)$ with $x(x+1)(x^2+x+1)F_{13}(x) \neq 0$ and $\varphi(x, y) = (a, b, c)$. □

Theorem 4.5.8. *There are infinitely many quadratic fields K containing an element c for which $G(f_c, K)$ admits a subgraph of type* 10(3,2). *Moreover, every such field K is a real quadratic field.*

Proof. As noted in §2.6, the curve $y^2 = F_{13}(-x)$ is an affine model for the modular curve $X_1(13)$. This curve has exactly 6 rational points:

$$X_1(13)(\mathbb{Q}) = \{\infty^+, \infty^-, (0, \pm 1), (-1, \pm 1)\}.$$

Hence, if $x \in \mathbb{Q} \setminus \{0, -1\}$, then $F_{13}(x)$ is not a square. For any such rational number x we let $y = \sqrt{F_{13}(x)}$ and $K = \mathbb{Q}(y)$, thus obtaining a quadratic field K and a point $(x, y) \in C(K)$ with $x(x+1)(x^2+x+1)F_{13}(x) \neq 0$. By Lemma 4.5.7 this implies that there is an element $c \in K$ for which $G(f_c, K)$ admits a subgraph of type 10(3,2). Clearly, as we vary $x \in \mathbb{Q}$ we obtain infinitely many quadratic fields K in this form. This proves the first part of the theorem.

Suppose now that K is a quadratic field such that there is some $c \in K$ for which $G(f_c, K)$ admits a subgraph of type 10(3,2). By Lemma 4.5.7 there is a point $(x, y) \in C(K)$ with $x(x+1) \neq 0$. We cannot have both $x, y \in \mathbb{Q}$ since this would imply that $x \in \{0, -1\}$, which we are assuming is not the case. Therefore, (x, y) is a quadratic point on $X_1(13)$, so it follows from Theorem 2.6.9 that $x \in \mathbb{Q}$. Since $K = \mathbb{Q}(x, y) = \mathbb{Q}(y) = \mathbb{Q}(\sqrt{F_{13}(x)})$, to show that K is a real quadratic field it suffices to note that $F_{13}(x)$ only takes positive values for $x \in \mathbb{Q}$. □

We end our discussion of the graph type 10(3,2) by stating explicitly how to obtain all pairs (K, c) consisting of a quadratic field K and an element $c \in K$ for which $G(f_c, K)$ is of this type.

Theorem 4.5.9. *Let K be a quadratic field. Suppose that there exists an element $c \in K$ such that $G(f_c, K)$ is of type* 10(3,2)*. Then there is a rational number $x \notin \{0, -1\}$ such that*

$$c = -\frac{x^6 + 2x^5 + 4x^4 + 8x^3 + 9x^2 + 4x + 1}{4x^2(x+1)^2}. \tag{4.7}$$

Moreover, the graph $G(f_c, \mathbb{Q})$ is of type 6(3) *and $K = \mathbb{Q}(\sqrt{-3-4c})$.*

Proof. By Lemma 4.5.7 there is a point $(x, y) \in C(K)$ with $x(x+1) \neq 0$ such that c is given by (4.7). As seen in the proof of Theorem 4.5.8, we must have $x \in \mathbb{Q}$. Moreover, x cannot equal 1, since this would lead to $c = -29/16$; however, the map f_c would then have a point of type 3_2 (see [58, Thm. 3]). Letting $\sigma = y/2x(x+1)$ we have $c = -3/4 - \sigma^2$. Clearly then, $K = \mathbb{Q}(y) = \mathbb{Q}(\sigma) = \mathbb{Q}(\sqrt{-3-4c})$. To see that $G(f_c, \mathbb{Q})$ is of type 6(3), note that since $x \in \mathbb{Q}$, the three points of period 3 for f_c are also rational. Hence, we have $c \in \mathbb{Q} \setminus \{-29/16\}$ such that f_c has a rational point of period 3. It follows from Poonen's classification [58] that $G(f_c, \mathbb{Q})$ is of type 6(3). □

4.5.3 Graph 12(2,1,1)a

The search carried out in [13] produced the pair

$$(K, c) = \left(\mathbb{Q}(\sqrt{17}), -\frac{13}{16}\right)$$

for which the graph $G(f_c, K)$ is of type 12(2,1,1)a. We show here that this is the only such pair (K, c) with K a quadratic number field and $c \in K$.

Lemma 4.5.10. *Let $C/\mathbb{Q}$ be the affine curve of genus 5 defined by the equations*

$$\begin{cases} y^2 = 2(x^4 + 2x^3 - 2x + 1) \\ z^2 = 5x^4 + 8x^3 + 6x^2 - 8x + 5. \end{cases} \tag{4.8}$$

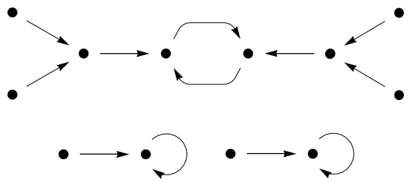


Figure 4.3: Graph type 12(2,1,1)a

Consider the rational map $\varphi : C \dashrightarrow \mathbb{A}^4 = \operatorname{Spec} \mathbb{Q}[r, s, p, c]$ given by

$$r = -\frac{x^2+1}{x^2-1} \ , \ s = \frac{y}{x^2-1} \ , \ p = \frac{1}{2} + \frac{z}{2(x^2-1)} \ , \ c = -\frac{x^4+2x^3+2x^2-2x+1}{(x^2-1)^2} \ .$$

For every number field K, the map φ induces a surjection from the set

$$\{(x, y, z) \in C(K) : x(x^2-1)(x^2+4x-1) \neq 0\}$$

to the set of all tuples $(r, s, p, c) \in K^4$ such that p is a fixed point of the map f_c and r, s are points of type 2_2 for f_c satisfying $f_c(s) = -f_c^2(r)$ and $r \neq \pm s$.

Proof. Fix a number field K and let $(x, y, z) \in C(K)$ be a point with $x(x^2-1)(x^2+4x-1) \neq 0$. Defining $r, s, p, c \in K$ as in the lemma, it is a simple calculation to verify that p is a fixed point of the map f_c and that r, s are of type 2_2 for f_c satisfying $f_c(s) = -f_c^2(r)$. Moreover, we have $s^2 - r^2 = (x^2+4x-1)/(x^2-1) \neq 0$, so $r \neq \pm s$. Hence, φ gives a well-defined map.

To see surjectivity, suppose that $r, s, p, c \in K$ are such that p is a fixed point of the map f_c and r, s are points of type 2_2 for f_c satisfying $f_c(s) = -f_c^2(r)$ and $r \neq \pm s$. The argument given in [58, p. 20] shows that there is an element $x \in K \setminus \{0, \pm 1\}$ such that

$$c = -\frac{x^4+2x^3+2x^2-2x+1}{(x^2-1)^2} \ , \ r = -\frac{x^2+1}{x^2-1} \ , \ s^2 = \frac{2(x^4+2x^3-2x+1)}{(x^2-1)^2} \ .$$

The condition $r \neq \pm s$ implies that $x^2+4x-1 \neq 0$. By [58, Thm. 1] there is an element $\rho \in K$ such that $c = \frac{1}{4} - \rho^2$ and $p = 1/2 + \rho$. Letting $y = s(x^2-1)$ and $z = 2\rho(x^2-1)$ we obtain a point $(x, y, z) \in C(K)$ with $x(x^2-1)(x^2+4x-1) \neq 0$ and $\varphi(x, y, z) = (r, s, p, c)$. □

Theorem 4.5.11. *With C as in Lemma 4.5.10 we have the following:*

1. $C(\mathbb{Q}) = \{(\pm 1, \pm 2, \pm 4)\}$.
2. *If K is a quadratic field different from $\mathbb{Q}(\sqrt{5})$ and $\mathbb{Q}(\sqrt{17})$, then $C(K) = C(\mathbb{Q})$.*
3. *For $K = \mathbb{Q}(\sqrt{5})$, $C(K) \setminus C(\mathbb{Q}) = \{(x, \pm(4x-2), \pm 8x) : x^2+4x-1 = 0\}$.*
4. *For $K = \mathbb{Q}(\sqrt{17})$, $C(K) \setminus C(\mathbb{Q})$ consists of the points $(-3, \pm 2\sqrt{17}, \pm 4\sqrt{17})$, $(1/3, \pm 2\sqrt{17}/9, \pm 4\sqrt{17}/9)$, and the points $(x, \pm 10x, \pm(16x-4))$ with $x^2+8x-1 = 0$.*

Proof. The curve $y^2 = 2(x^4+2x^3-2x+1)$ is birational to the elliptic curve with Cremona label 40a3, which has rank 0 and torsion order 4. The rational points on this curve are $(\pm 1, \pm 2)$. The curve $z^2 = 5x^4+8x^3+6x^2-8x+5$ is birational to the elliptic curve 17a4, which has rank 0 and torsion order 4; the rational points are $(\pm 1, \pm 4)$. Hence, $C(\mathbb{Q}) = \{(\pm 1, \pm 2, \pm 4)\}$.

Suppose now that $(x, y, z) \in C(\bar{\mathbb{Q}})$ satisfies $[\mathbb{Q}(x, y, z) : \mathbb{Q}] = 2$, and let $K = \mathbb{Q}(x, y, z)$.

Case 1: $x \in \mathbb{Q}$. We cannot have $x = \pm 1$, since this would imply that $y = \pm 2$ and $z = \pm 4$, contradicting the assumption that (x, y, z) is a quadratic point on C. Hence, $x \neq \pm 1$. It follows that $y \notin \mathbb{Q}$, since having $x, y \in \mathbb{Q}$ would imply that $x = \pm 1$. Similarly, $z \notin \mathbb{Q}$. Therefore, $K = \mathbb{Q}(y) = \mathbb{Q}(z)$, so there is a rational number q such that

$$2(x^4+2x^3-2x+1) = q^2(5x^4+8x^3+6x^2-8x+5).$$

Letting $w = q(5x^4+8x^3+6x^2-8x+5)$ we obtain

$$w^2 = 10x^8+36x^7+44x^6-12x^5-44x^4+12x^3+44x^2-36x+10 \tag{4.9}$$

with $x, w \in \mathbb{Q}$ and $x \neq \pm 1$. Let X be the hyperelliptic curve of genus 3 defined by (4.9). We claim that the following is a complete list of rational points on X:

$$X(\mathbb{Q}) = \{(\pm 1, \pm 8), (-3, \pm 136), (1/3, \pm 136/81)\}.$$

Assuming this for the moment, we must then have $x = -3$ or $x = 1/3$. Taking $x = -3$ we obtain by (4.8) that $y^2 = 68$ and $z^2 = 272$. If $x = 1/3$, then $y^2 = 68/81$ and $z^2 = 272/81$. Thus, we obtain the quadratic points $(-3, \pm 2\sqrt{17}, \pm 4\sqrt{17})$ and $(1/3, \pm 2\sqrt{17}/9, \pm 4\sqrt{17}/9)$.

In order to determine all rational points on X we note that X has an involution $(x, w) \mapsto (-1/x, w/x^4)$. The quotient of X by this involution is the elliptic curve

$$17a2: \; v^2 + uv + v = u^3 - u^2 - 6u - 4.$$

The quotient map $X \longrightarrow 17a2$ of degree 2 is given by

$$\begin{aligned} u &= \frac{2x^6 + 6x^5 + 2x^4 - 12x^3 - x^2w - 2x^2 + 6x + w - 2}{x^6 - 3x^4 + 3x^2 - 1}, \\ v &= \frac{-6x^6 - 24x^5 - 22x^4 + 16x^3 + 2x^2w + 22x^2 + 4xw - 24x - 2w + 6}{x^6 - 3x^4 + 3x^2 - 1}. \end{aligned}$$

Since 17a2 has only 4 rational points, it follows that X has at most 8 rational points. We have already found 8 points in $X(\mathbb{Q})$, so these must be all of them.

Case 2: x is quadratic. We make the change of variables

$$X = \frac{2x^2 + y}{(x-1)^2}, \; Y = \frac{3x^3 + 3x^2 + 2xy - 3x + 1}{(x-1)^3} \tag{4.10}$$

$$S = \frac{5x^2 + 2x + 2z + 1}{(x-1)^2}, \; T = \frac{2(7x^3 + 9x^2 + 3xz - 3x + z + 3)}{(x-1)^3} \tag{4.11}$$

satisfying

$$\frac{X^2+2Y}{X^2-4X+2} = x = \frac{S^2+2S+4T+1}{S^2-10S+5} \tag{4.12}$$

to obtain the equations

$$\begin{cases} Y^2 = X^3 - 2X + 1 \\ T^2 = S^3 - 11S + 6. \end{cases}$$

The idea of the proof is to use these two equations together with Lemma 4.5.3 to find the minimal polynomials of X and S, and then using (4.12) to find the minimal polynomial of x. It may occur that X or S is rational rather than quadratic, so we must consider this possibility. If $X \in \mathbb{Q}$, then substituting $y = X(x-1)^2 - 2x^2$ into the equation $y^2 = 2(x^4 + 2x^3 - 2x + 1)$ we obtain the following expression for the minimal polynomial of x:

$$x^2 - \frac{2X^2}{X^2-4X+2}x + \frac{X^2-2}{X^2-4X+2} = 0. \tag{4.13}$$

Similarly, if $S \in \mathbb{Q}$, then substituting $z = \frac{1}{2}[S(x-1)^2 - 5x^2 - 2x - 1]$ into the equation $z^2 = 5x^4 + 8x^3 + 6x^2 - 8x + 5$ we find that

$$x^2 - \frac{2S^2+4S+2}{S^2-10S+5}x + \frac{S^2-2S-19}{S^2-10S+5} = 0. \tag{4.14}$$

Now, if X is quadratic, then by Lemma 4.5.3 applied to the equation $Y^2 = X^3 - 2X + 1$, there is a rational number v and a point $(X_0, Y_0) \in \{(0, \pm 1), (1, 0)\}$ such that

$$X^2 + (X_0 - v^2)X + X_0^2 + v^2 X_0 - 2Y_0 v - 2 = 0\ ,\ Y = Y_0 + v(X - X_0). \tag{4.15}$$

The point $(0, -1)$ is excluded in this case because (4.12) would imply that $x = \frac{v}{v-2} \in \mathbb{Q}$.

If $(X_0, Y_0) = (0, 1)$, then (4.12) and (4.15) imply that

$$x^2 - \frac{4(v+1)}{v^2-2}x - 1 = 0. \tag{4.16}$$

If instead $(X_0, Y_0) = (1, 0)$, then

$$x^2 - \frac{4x}{v^2-2v-1} - \frac{v^2+2v-1}{v^2-2v-1} = 0. \tag{4.17}$$

Similarly, if $S \notin \mathbb{Q}$, then by Lemma 4.5.3 applied to the equation $T^2 = S^3 - 11S + 6$, there is a rational number w and a point $(S_0, T_0) \in \{(-1, \pm 4), (3, 0)\}$ such that

$$S^2 + (S_0 - w^2)S + S_0^2 + w^2 S_0 - 2T_0 w - 11 = 0\ ,\ T = T_0 + w(S - S_0). \tag{4.18}$$

The point $(-1, -4)$ is excluded because it would lead to $x = \frac{w+1}{w-3} \in \mathbb{Q}$. If $(S_0, T_0) = (3, 0)$, then (4.12) and (4.18) imply that

$$x^2 - \frac{8x}{w^2-4w-1} - \frac{w^2+4w-1}{w^2-4w-1} = 0, \tag{4.19}$$

and if $(S_0, T_0) = (-1, 4)$, then

$$x^2 - \frac{8w+8}{w^2-5}x - 1 = 0. \tag{4.20}$$

We now split the proof into four cases, according to whether X and S are rational or quadratic.

Case 2a: $X, S \in \mathbb{Q}$. We simultaneously have relations (4.13) and (4.14). Comparing these equations we obtain the system

$$\begin{cases} X^2(S^2 - 10S + 5) = (X^2 - 4X + 2)(S^2 + 2S + 1) \\ (X^2 - 2)(S^2 - 10S + 5) = (X^2 - 4X + 2)(S^2 - 2S - 19), \end{cases}$$

whose rational solutions are $(X, S) = (0, -1)$ and $(X, S) = (1, 3)$. However, both solutions lead to $x = \pm 1$ by applying (4.13) and (4.14). We conclude that X and S cannot both be rational.

Case 2b: $X \in \mathbb{Q}, S \notin \mathbb{Q}$. We have (4.13) and (4.18). If $(S_0, T_0) = (3, 0)$, then we compare (4.13) and (4.19) to arrive at the system

$$\begin{cases} X^2(w^2 - 4w - 1) = 4(X^2 - 4X + 2) \\ (X^2 - 2)(w^2 - 4w - 1) = -(X^2 - 4X + 2)(w^2 + 4w - 1), \end{cases}$$

whose only rational solution is $(X, w) = (1, 1)$. However, when $w = 1$, (4.19) becomes $(x + 1)^2 = 0$, a contradiction.

If $(S_0, T_0) = (-1, 4)$, then we compare (4.13) and (4.20) to conclude that $X = 0$ or 2. Then (4.13) becomes $x^2 - 1 = 0$ (a contradiction) or $x^2 + 4x - 1 = 0$.

Case 2c: $X \notin \mathbb{Q}, S \in \mathbb{Q}$. In this case we have (4.14) and (4.15). If $(X_0, Y_0) = (0, 1)$, then we compare (4.14) and (4.16) to conclude that $S = 7$ and $x^2 + 8x - 1 = 0$.

If $(X_0, Y_0) = (1, 0)$, then we compare (4.14) and (4.17) to arrive at the system

$$\begin{cases} 2(S^2 - 10S + 5) = (v^2 - 2v - 1)(S + 1)^2 \\ -(v^2 + 2v - 1)(S^2 - 10S + 5) = (v^2 - 2v - 1)(S^2 - 2S - 19), \end{cases}$$

whose only rational solution is $(S, v) = (3, 1)$. However, if $v = 1$, then (4.17) becomes $(x + 1)^2 = 0$, a contradiction.

Case 2d: $X, S \notin \mathbb{Q}$. We have (4.15) and (4.18).

- If $(X_0, Y_0) = (1, 0)$ and $(S_0, T_0) = (3, 0)$, then comparing (4.17) and (4.19) we find that $v = w = \pm 1$. But then (4.17) implies that $x = \pm 1$, a contradiction.

- If $(X_0, Y_0) = (1, 0)$ and $(S_0, T_0) = (-1, 4)$, then we compare (4.17) and (4.20) to see that $v = 0$ and $x^2 + 4x - 1 = 0$.

- If $(X_0, Y_0) = (0, 1)$ and $(S_0, T_0) = (3, 0)$, then we compare (4.16) and (4.19) to conclude that $w = 0$, and therefore $x^2 + 8x - 1 = 0$.

- If $(X_0, Y_0) = (0, 1)$ and $(S_0, T_0) = (-1, 4)$, then comparing (4.16) and (4.20) we obtain

  $$(v + 1)(w^2 - 5) = 2(w + 1)(v^2 - 2).$$

  Let $E \subset \mathbb{P}^2$ be the projective closure of the curve defined by this equation. Then E is a nonsingular plane cubic with at least four rational points, namely the affine point $(-1, -1)$ and three points at infinity. Using Magma we find that E is the elliptic curve 17a4, which has exactly 4 rational points. It follows that $(v, w) = (-1, -1)$ is the only affine point on E. But then (4.16) becomes $x^2 - 1 = 0$, which is a contradiction.

In all cases that have not led to a contradiction we have concluded that either $x^2+4x-1 = 0$ or $x^2 + 8x - 1 = 0$. If $x^2 + 4x - 1 = 0$, then (4.8) implies that $y = \pm(4x - 2)$ and $z = \pm 8x$. If $x^2 + 8x - 1 = 0$, then $y = \pm 10x$ and $z = \pm(16x - 4)$. □

Corollary 4.5.12. *Let K be a quadratic field, and let $c \in K$. Suppose that $G(f_c, K)$ contains a graph of type* 12(2,1,1)a. *Then $c = -13/16$ and $K = \mathbb{Q}(\sqrt{17})$.*

Proof. By Lemma 4.5.10 there is a point $(x, y, z) \in C(K)$ with $x(x^2 - 1)(x^2 + 4x - 1) \neq 0$ such that

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

It follows from Theorem 4.5.11 that $K = \mathbb{Q}(\sqrt{17})$ and that x is either $-3, 1/3$, or a quadratic number satisfying $x^2 + 8x - 1 = 0$. In all three cases we obtain $c = -\frac{13}{16}$. □

4.5.4 Graph 12(4)

The search carried out in [13] produced a unique pair

$$(K, c) = \left(\mathbb{Q}(\sqrt{105}), -95/48\right)$$

consisting of a quadratic field K and an element $c \in K$ for which the graph $G(f_c, K)$ is of type 12(4). We show here that in addition to this known example there are at most five other pairs (K, c) with this property.

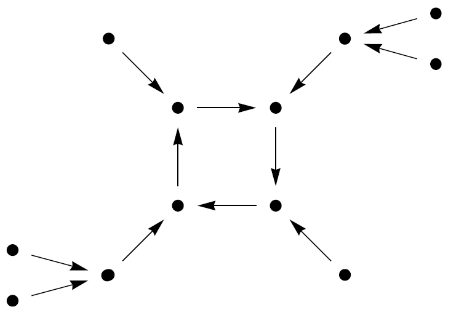


Figure 4.4: Graph type 12(4)

Lemma 4.5.13. *Let $C/\mathbb{Q}$ be the affine curve of genus 9 defined by the equations*

$$\begin{cases} y^2 = -x(x^2+1)(x^2-2x-1) \\ z^2 = x(-x^6+x^5+7x^4+10x^3-7x^2+5x+1) - 2x(x-1)(x+1)^2y. \end{cases} \tag{4.21}$$

Consider the rational map $\varphi : C \dashrightarrow \mathbb{A}^2 = \operatorname{Spec}\mathbb{Q}[p, c]$ given by

$$p = \frac{z}{2x(x^2-1)} \quad , \quad c = \frac{(x^2-4x-1)(x^4+x^3+2x^2-x+1)}{4x(x^2-1)^2}.$$

For every number field K, the map φ induces a surjection from the set

$$\{(x,y,z) \in C(K) : x(x^4-1)(x^2-2x-1) \neq 0\}$$

to the set of all pairs $(p,c) \in K^2$ such that p is a point of type 4_2 for the map f_c.

Proof. Fix a number field K. Suppose $(x,y,z) \in C(K)$ is a point with $x(x^4-1)(x^2-2x-1) \neq 0$, and define $p, c \in K$ as in the lemma. It is then a simple calculation to verify that p is a point of type 4_2 for f_c. Hence, φ gives a well-defined map.

To prove surjectivity, suppose that $p, c \in K$ are such that p is a point of type 4_2 for the map f_c. Then $q := p^2 + c$ is a point of type 4_1, so $-q$ is a point of period 4. By [47, pp. 92–93] there are elements $x, y \in K$ satisfying $y^2 = -x(x^2+1)(x^2-2x-1)$ such that

$$c = \frac{(x^2-4x-1)(x^4+x^3+2x^2-x+1)}{4x(x-1)^2(x+1)^2}\ , \quad -q = \frac{x-1}{2(x+1)} + \frac{y}{2x(x-1)},$$

and $x(x^4-1)(x^2-2x-1) \neq 0$. Clearing denominators in the equation

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

and letting $z = 2x(x^2-1)p$ we obtain

$$z^2 = x(-x^6+x^5+7x^4+10x^3-7x^2+5x+1) - 2x(x-1)(x+1)^2y.$$

Thus, we have a point $(x,y,z) \in C(K)$ with $x(x^4-1)(x^2-2x-1) \neq 0$ and $\varphi(x,y,z) = (p,c)$. □

Lemma 4.5.14. *Let $X/\mathbb{Q}$ be the hyperelliptic curve of genus 5 defined by the equation*

$$w^2 = x^{12} + 2x^{11} - 13x^{10} - 26x^9 + 67x^8 + 124x^7 + 26x^6 - 44x^5 + 179x^4 - 62x^3 - 5x^2 + 6x + 1.$$

Then $X(\mathbb{Q})$ contains the points $\infty^+, \infty^-, (\pm 1, \pm 16), (0, \pm 1), (-3, \pm 368)$ and at most 10 other points.

Proof. Using the Magma function `Points` we search for rational points on X of height at most 10^5 and obtain the points listed above. Using the `RankBound` function we obtain an upper bound of 4 for the rank of $\mathrm{Jac}(X)(\mathbb{Q})$; we are thus in a position to bound the number of rational points on X using the method of Chabauty. The primes $3, 5, 7, 11$, and 13 are of good reduction for X, and Magma's `Points` function yields

$$\#X(\mathbb{F}_3) = 8,\ \#X(\mathbb{F}_5) = 12,\ \#X(\mathbb{F}_7) = 12,\ \#X(\mathbb{F}_{11}) = 20,\ \#X(\mathbb{F}_{13}) = 19.$$

Applying the Coleman bound [9] at the prime $p = 13$ we deduce that $\#X(\mathbb{Q}) \leq 27$. The Lorenzini-Tucker bounds [41, Thm 1.1] give a smaller bound using $p = 7, d = 2$:

$$\#X(\mathbb{Q}) \leq \#X(\mathbb{F}_7) + \frac{6}{5}(8) = 12 + \frac{6}{5}(8) < 22,$$

so $\#X(\mathbb{Q}) \leq 21$. However, since X has no rational point with $w = 0$, the number of rational points must be even, and therefore $\#X(\mathbb{Q}) \leq 20$. Since we have already found 10 rational points, we conclude that there are at most 10 additional rational points on X. □

Theorem 4.5.15. *With C as in Lemma 4.5.13 we have the following:*

1. $C(\mathbb{Q}) = \{(0, 0, 0), (\pm 1, \pm 2, \pm 4)\}$.

2. *If (x, y, z) is a quadratic point on C, then $x \in \mathbb{Q} \setminus \{0, \pm 1\}$. Moreover, there exists $w \in \mathbb{Q}$ such that $(x, w) \in X(\mathbb{Q})$, where X is the curve defined in Lemma 4.5.14.*

Proof. As noted in §2.6, the curve $y^2 = -x(x^2 + 1)(x^2 - 2x - 1)$ is an affine model for the modular curve $X_1(16)$. This curve has exactly six rational points:

$$X_1(16)(\mathbb{Q}) = \{\infty, (0, 0), (\pm 1, \pm 2)\}.$$

The affine rational points on $X_1(16)$ give rise to the listed rational points on C.

Suppose now that $(x, y, z) \in C(\overline{\mathbb{Q}})$ is a point with $[\mathbb{Q}(x, y, z) : \mathbb{Q}] = 2$, and let $K = \mathbb{Q}(x, y, z)$. We cannot have $x \in \{0, \pm 1\}$ since this would imply that $(x, y, z) \in C(\mathbb{Q})$. It follows that (x, y) cannot be a rational point on $X_1(16)$ and must therefore be quadratic. If $x \notin \mathbb{Q}$, then by Theorem 2.6.12 either $x^2 = -1$ and $y = 0$, or $x^2 - 2x - 1 = 0$ and $y = 0$. In both cases we find that the second equation in (4.21) has no solution in K. We conclude that x must be a rational number different from $0, \pm 1$. Since $y^2 \in \mathbb{Q}$, the Galois conjugate of y is $-y$. Hence, taking norms on both sides of the second equation in (4.21) we obtain

$$w^2 = x^{12} + 2x^{11} - 13x^{10} - 26x^9 + 67x^8 + 124x^7 + 26x^6 - 44x^5 + 179x^4 - 62x^3 - 5x^2 + 6x + 1,$$

where $w = N_{K/\mathbb{Q}}(z)/x$. □

Corollary 4.5.16. *In addition to the known pair* $(\mathbb{Q}(\sqrt{105}), -95/48)$ *there are at most five pairs* (K, c)*, with* K *a quadratic number field and* $c \in K$*, for which* $G(f_c, K)$ *contains a graph of type* 12(4)*. Moreover, for every such pair we must have* $c \in \mathbb{Q}$*.*

Proof. Suppose that (K, c) is such a pair. Since f_c has a point of type 4_2 in K, then by Lemma 4.5.13 there is a point $(x, y, z) \in C(K)$ with $x(x^2 - 1) \neq 0$ such that

$$c = \frac{(x^2 - 4x - 1)(x^4 + x^3 + 2x^2 - x + 1)}{4x(x^2 - 1)^2}. \tag{4.22}$$

We cannot have $(x, y, z) \in C(\mathbb{Q})$ since this would imply that $x \in \{0, \pm 1\}$. Hence, (x, y, z) is a quadratic point on C. By Theorem 4.5.15, $x \in \mathbb{Q}$, and thus $c \in \mathbb{Q}$. Moreover, there is a rational number w such that $(x, w) \in X(\mathbb{Q})$. It follows from Lemma 4.5.14 that either $x = -3$ or x belongs to a list of at most 5 other rational numbers. Setting $x = -3$ yields

$c = -95/48$, and the system (4.21) becomes

$$\begin{cases} y^2 = 420 \\ z^2 = 2256 - 96y. \end{cases}$$

Hence, $y = \pm 2\sqrt{105}$ and $z = \pm(2y - 24)$. In particular, $K = \mathbb{Q}(\sqrt{105})$, so we have recovered the known pair $(\mathbb{Q}(\sqrt{105}), -95/48)$. If $x \neq -3$, then there are at most five options for x; each value of x determines the number c by (4.22) and the field K by (4.21). This gives at most five options for the pair (K, c). □

Remark 4.5.17. The map $z^2 - 95/48$ has no preperiodic point in $\mathbb{Q}$. This follows, for instance, from part (2) of Proposition 4.3.4, since $\operatorname{ord}_3(-95/48) = -1$. Hence, the twelve preperiodic points that this map has over the field $\mathbb{Q}(\sqrt{105})$ are all quadratic over $\mathbb{Q}$.

Note that the proof of Corollary 4.5.16 only used the existence of one pair of points of type 4_2 for f_c, rather than the two pairs of such points which occur in a graph of type 12(4). However, there is no loss in doing this since, for quadratic fields K, the existence of one pair of points of type 4_2 implies the existence of a second pair, as shown below.

Corollary 4.5.18. *Let K be a quadratic field and let $c \in K$. Suppose that the map f_c has a point $p \in K$ of type 4_2. Then $\sigma(p)$ is another point of type 4_2 for f_c (different from $\pm p$), where σ is the nontrivial element of* $\operatorname{Gal}(K/\mathbb{Q})$.

Proof. By Lemma 4.5.13 there is a point $(x, y, z) \in C(K)$ such that $\varphi(x, y, z) = (p, c)$. Moreover, as seen in the proof of Corollary 4.5.16, we must have $x \in \mathbb{Q} \setminus \{0, \pm 1\}$. Applying σ to the system (4.21) we obtain the point $(x, -y, \sigma(z)) \in C(K)$. Applying the map φ we obtain $\varphi(x, -y, \sigma(z)) = (\sigma(p), c)$. Hence, Lemma 4.5.13 shows that $\sigma(p)$ is a point of type 4_2 for f_c. Using the defining equations of C we see that neither y nor z^2 are rational; it follows that $\sigma(z) \notin \{\pm z\}$, and therefore $\sigma(p) \notin \{\pm p\}$. □

From this result we immediately deduce the following:

Corollary 4.5.19. *There does not exist a pair (K, c) consisting of a quadratic number field K and an element $c \in K$ for which the graph $G(f_c, K)$ has a unique pair of points of type 4_2. In other words, the following graph structure 10(4) cannot occur over a quadratic field:*

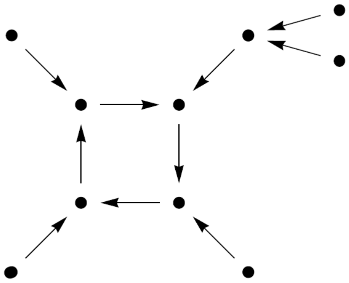


Figure 4.5: Graph type 10(4)

Chapter 5

Tamagawa numbers and torsion of elliptic curves

5.1 Introduction

Let K be a number field and E an elliptic curve defined over K. The L-series of E/K is an analytic function $L(E,s)$ on the half-plane $\mathrm{Re}(s) > 3/2$, and it is conjectured that this function admits an analytic continuation to the complex plane $\mathbb{C}$. Our goal in this chapter is to study several questions regarding the quotient

$$\left(\prod_v c_v\right) /|E(K)_{\mathrm{tors}}|$$

appearing in the leading term of the L-function of E in the conjecture of Birch and Swinnerton-Dyer.

For every finite place v of K we let K_v denote the completion of K at v, and k_v the residue field. After a base change, we may consider E as an elliptic curve over K_v. The subgroup $E_0(K_v)$ of $E(K_v)$ consisting of points of nonsingular reduction has finite index, and we define the *Tamagawa number* of E at v to be this index:

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

If $\mathfrak{p}$ is the maximal ideal of the ring of integers $\mathcal{O}_K$ corresponding to a place v, we will also denote c_v by $c_{\mathfrak{p}}$.

In order to state the questions addressed in this chapter we introduce the following notation and terminology.

- If E is an elliptic curve over K, define

  $$c_{E/K} := \prod_v c_v \; .$$

  If the field K is clear from context, we will write c_E instead of $c_{E/K}$.

- We will say that a pair (N, d) of positive integers is *admissible* if there exists some number field K of degree d, and some elliptic curve over K with a K-rational point of order N. Equivalently, the pair (N, d) is admissible if the modular curve $Y_1(N)$ has a point over some number field of degree d.

- For integers N and c with $c \neq 0$, let $\operatorname{ord}_N(c)$ denote the largest integer m such that N^m divides c.

We can now define our main object of study.

Definition 5.1.1. If (N, d) is an admissible pair, we let $V(N, d)$ denote the ordered set of all numbers $\operatorname{ord}_N(c_{E/K})$, where K ranges over all number fields of degree $\leq d$ and E ranges over all elliptic curves defined over K having a K-rational point of order N.

We would like to understand the set $V(N, d)$ as well as possible. Since $V(N, d) \subseteq \mathbb{N}$, a natural first question is to determine its least element.

Question 5.1.2. What is the smallest element of the set $V(N, d)$?

If we know that a particular integer n belongs to $V(N, d)$, then we can consider the elliptic curves E and the number fields K such that $n = \mathrm{ord}_N(c_{E/K})$. All the evidence available at present suggests that the first few elements of $V(N, d)$ arise from only finitely many elliptic curves, while the remaining values can be obtained from infinitely many curves.

Question 5.1.3. Which elements of $V(N, d)$, if any, occur as $\mathrm{ord}_N(c_E)$ for only finitely many elliptic curves E?

This chapter is organized as follows: in sections 5.2-5.6 we consider the above questions for number fields of degrees $d \leq 5$. A large amount of computations have been done in preparing this chapter; our methods are explained in §5.7. Sections 5.8 and 5.9 contain background material which we use throughout the chapter.

5.2 Elliptic curves over $\mathbb{Q}$

The admissible pairs $(N, 1)$ have $N = 1, \ldots, 10$ or 12, as follows from Mazur's theorem [43]. Our main questions introduced above were treated in detail by Lorenzini [40] for elliptic curves over $\mathbb{Q}$. We include in this section a few refinements of his results.

Theorem 5.2.1 (Lorenzini)**.**

1. *Let $E/\mathbb{Q}$ be an elliptic curve with a $\mathbb{Q}$-rational point of order 5. Then $5|c_E$ unless $E = X_1(11)$, in which case $c_E = 1$. In particular, $\min V(5, 1) = 0$.*

2. *If $E/\mathbb{Q}$ is an elliptic curve with a $\mathbb{Q}$-rational point of order 7, then $7|c_E$. The elliptic curve E = 26b1 has $\mathrm{ord}_7(c_E) = 1$, so that $\min V(7, 1) = 1$. Moreover, the value $1 \in V(7, 1)$ is taken only by 26b1.*

3. *If $E/\mathbb{Q}$ is an elliptic curve with a $\mathbb{Q}$-rational point of order 9, then $27|c_E$. The elliptic*

curve $E = 54b3$ has a rational point of order 9 and $c_E = 27$. However, every other elliptic curve E over $\mathbb{Q}$ with a rational point of order 9 has $9^2 | c_E$.

Proof. See (2.7), (2.10), and (2.17) in [40]. □

Our results below make the divisibility statements of Theorem 5.2.1 more precise.

Proposition 5.2.2. *Let $E/\mathbb{Q}$ be an elliptic curve with a $\mathbb{Q}$-rational point of order 7. Then the Tamagawa number of E at 2 is divisible by 7.*

Proof. Let $P \in E(\mathbb{Q})$ have order 7. We claim that $P \notin E_0(\mathbb{Q}_2)$, which will imply the result because the image of P in the group $E(\mathbb{Q}_2)/E_0(\mathbb{Q}_2)$ will then have order 7. Suppose that $P \in E_0(\mathbb{Q}_2)$. By Theorem 5.9.4 we have $P \notin E_1(\mathbb{Q}_2)$, so $\tilde{P} \in \tilde{E}_{\text{ns}}(\mathbb{F}_2)$ has order 7. However, it follows from Theorems 5.8.1 and 5.9.1 that, regardless of the reduction type of E at 2, the order of the group $\tilde{E}_{\text{ns}}(\mathbb{F}_2)$ is at most 5. This is a contradiction, so we conclude that $P \notin E_0(\mathbb{Q}_2)$, as claimed. □

Proposition 5.2.3. *Let $E/\mathbb{Q}$ be an elliptic curve with a $\mathbb{Q}$-rational point of order 9. Then the Tamagawa number of E at 2 is divisible by 9, and the Tamagawa number of E at 3 is divisible by 3.*

Proof. Let $P \in E(\mathbb{Q})$ have order 9. We claim that $P \notin E_0(\mathbb{Q}_2)$. Suppose that $P \in E_0(\mathbb{Q}_2)$. By Theorem 5.9.4 we see that $\tilde{P} \in \tilde{E}_{\text{ns}}(\mathbb{F}_2)$ has order 9. However, it follows from Theorems 5.8.1 and 5.9.1 that, regardless of the reduction type of E at 2, the order of the group $\tilde{E}_{\text{ns}}(\mathbb{F}_2)$ is at most 5. This is a contradiction, so $P \notin E_0(\mathbb{Q}_2)$, as claimed. Note that in particular this implies that E cannot have good reduction at 2.

We now show that $[3]P \notin E_0(\mathbb{Q}_2)$, which will imply that 9 divides c_2. Suppose that $R = [3]P \in E_0(\mathbb{Q}_2)$. Since R has order 3 we have $R \notin E_1(\mathbb{Q}_2)$, so $\tilde{R} \in \tilde{E}_{\text{ns}}(\mathbb{F}_2)$ has order 3. Hence, the group $\tilde{E}_{\text{ns}}(\mathbb{F}_2)$ has order divisible by 3. Since E does not have good reduction at 2, this implies by Theorem 5.9.1 that E has non-split multiplicative reduction at 2. But then by Theorem 5.9.3 we have $c_2 = 1$ or 2. This implies that $[2]P \in E_0(\mathbb{Q}_2)$, but we have already shown that $E_0(\mathbb{Q}_2)$ cannot contain elements of order 9. This contradiction proves that $[3]P \notin E_0(\mathbb{Q}_2)$, and hence that $9|c_2$.

To show that c_3 is divisible by 3 it suffices to show that $P \notin E_0(\mathbb{Q}_3)$. Suppose that $P \in E_0(\mathbb{Q}_3)$. Using Theorem 5.9.4 we see that $\tilde{P} \in \tilde{E}_{\mathrm{ns}}(\mathbb{F}_3)$ has order 9. However, it follows from Theorems 5.8.1 and 5.9.1 that, regardless of the reduction type of E at 3, the order of the group $\tilde{E}_{\mathrm{ns}}(\mathbb{F}_3)$ is at most 7. This is a contradiction, so we conclude that $P \notin E_0(\mathbb{Q}_3)$. □

5.3 Elliptic curves over quadratic fields

We recall the list of possible torsion subgroups of elliptic curves over quadratic fields:

Theorem 5.3.1 (Kamienny [31], Kenku-Momose [35]). *Let K be a quadratic number field, and E/K an elliptic curve. Then $E(K)_{\mathrm{tors}}$ is isomorphic to one of the following 26 groups:*

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

It follows from Theorem 5.3.1 that the admissible pairs $(N, 2)$ have $N = 1, \ldots, 16$ or 18. Lorenzini considered the values $N = 11$ and 13; we will improve slightly on his results here, and also consider the case $N = 15$.

Theorem 5.3.2 (Lorenzini). *Let K be a quadratic number field, and E/K an elliptic curve with a K-rational point of order $N = 11$ or 13. Then $N|c_{\mathfrak{p}}$ for every prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$ lying over 2. In particular,* $\min V(11, 2) \geq 1$ *and* $\min V(13, 2) \geq 1$.

Proof. See [40, Cor. 3.4]. □

We have found exactly two non-isomorphic examples of an elliptic curve E over a quadratic field K such that E has a K-rational point of order 11 and $\mathrm{ord}_{11}(c_E) = 1$. These examples are the two Galois conjugates of the following curve:

Example 5.3.3. Let $K = \mathbb{Q}(\sqrt{2})$ and let E be the following elliptic curve over K:

$$E: \ y^2 + (\sqrt{2}+3)xy + 4\sqrt{2}y = x^3 + \sqrt{2}x^2.$$

Then $E(K)_{\mathrm{tors}} \cong \mathbb{Z}/11$. We have $c_{\mathfrak{p}_2} = 11$ for the unique prime $\mathfrak{p}_2$ of K lying over 2, and for all other primes $\mathfrak{p}$, $c_{\mathfrak{p}} = 1$. We remark that K is second smallest quadratic field (in terms of absolute discriminant) where $Y_1(11)$ has points; this follows from [32, Thm. 2]. From this example we conclude that $\min V(11, 2) = 1$. However, we do not know whether the two Galois conjugates of E are the only curves achieving the minimal value $\mathrm{ord}_{11}(c_E) = 1$.

Proposition 5.3.4. *Let K be a quadratic number field, and E/K an elliptic curve with a K-rational point of order 13. Then* $13^2 | c_E$.

Proof. By Theorem 2.6.9, if the modular curve $X_1(13)$ has a quadratic point over a quadratic number field K, then the rational prime 2 must split in K. The result then follows from Theorem 5.3.2. □

We have found exactly one example of an elliptic curve E over a quadratic field K such that E has a K-rational point of order 13 and $\mathrm{ord}_{13}(c_E) = 2$. This curve is isomorphic to its Galois conjugate over K.

Example 5.3.5. Let $K = \mathbb{Q}(\sqrt{17})$ and let E be the following elliptic curve:

$$E: \ y^2 + (2\sqrt{17}-9)xy + (18\sqrt{17}-74)y = x^3 + (18\sqrt{17}-74)x^2.$$

Then $E(K)_{\text{tors}} \cong \mathbb{Z}/13$. We find that $c_{\mathfrak{p}} = 13$ for each of the two primes $\mathfrak{p}$ of K lying over 2, and $c_{\mathfrak{p}} = 1$ for all other primes $\mathfrak{p}$. We remark that K is smallest quadratic field (in terms of absolute discriminant) where $Y_1(13)$ has points [32, Thm. 3]. From this example we conclude that $\min V(13,2) = 2$. However, we do not know whether this is the unique curve achieving the minimal value $\operatorname{ord}_{13}(c_E) = 2$.

Based on extensive computations we make the conjecture that all elements of $V(13,2)$ are even. We have verified, for a total of 48,925 elliptic curves E over quadratic fields having a point of order 13, that the power of 13 dividing c_E is even.

Conjecture 5.3.6. *Every element of the set $V(13,2)$ is even.*

Proposition 5.3.7. *Let K be a quadratic number field, and E/K an elliptic curve with a K-rational point of order 15. Then $5|c_{\mathfrak{p}}$ for every prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$ lying over 2.*

Proof. Let $\mathfrak{p}$ be a prime lying over 2, and let v be the place of K corresponding to $\mathfrak{p}$. We will show that $5|c_v$.

Let $P \in E(K)$ have order 15. We claim that $P \notin E_0(K_v)$. Suppose that $P \in E_0(K_v)$. By Theorem 5.9.4 we see that $\tilde{P} \in \tilde{E}_{\text{ns}}(k_v)$ has order 15. However, it follows from Theorems 5.8.1 and 5.9.1 that, regardless of the reduction type of E at v, the order of the group $\tilde{E}_{\text{ns}}(k_v)$ is at most 9. This is a contradiction, so $P \notin E_0(K_v)$, as claimed. Note that in particular this implies that E cannot have good reduction at v.

We now show that $[3]P \notin E_0(K_v)$, which will imply that 5 divides c_v. Suppose that $R = [3]P \in E_0(K_v)$. Since R has order 5 we have $R \notin E_1(K_v)$, so $\tilde{R} \in \tilde{E}_{\text{ns}}(k_v)$ has order 5. Hence, the group $\tilde{E}_{\text{ns}}(k_v)$ has order divisible by 5. By Theorem 5.9.1 this can only happen if either E has good reduction at v, which we have already ruled out, or if $k_v = \mathbb{F}_4$ and E has non-split multiplicative reduction at v. In the latter case, $c_v = 1$ or 2 by Theorem 5.9.3. But then $[2]P \in E_0(K_v)$, and we have already shown that $E_0(K_v)$ cannot contain elements of order 15. This contradiction proves that $[3]P \notin E_0(K_v)$, and hence that $5|c_v$. □

Remark 5.3.8. Our computations suggest that, in the context of the above proposition, $3|c_E$. However, there does not appear to be any particular rational prime p such that $c_{\mathfrak{p}}$ is always divisible by 3 for some prime $\mathfrak{p}$ of $\mathcal{O}_K$ lying over p.

We have found exactly one example of an elliptic curve E over a quadratic field K such that E has a K-rational point of order 15 and $\operatorname{ord}_{15}(c_E) = 1$. This curve is isomorphic to its Galois conjugate over K.

Example 5.3.9. Let $K = \mathbb{Q}(\sqrt{5})$ and let E be the following elliptic curve over K:

$$E:\ y^2 + \sqrt{5}xy + (50 - 22\sqrt{5})y = x^3 + (25 - 11\sqrt{5})x^2.$$

Then $E(K)_{\text{tors}} \cong \mathbb{Z}/15$. The prime 2 is inert in K, and $c_{(2)} = 5$. There is a unique prime $\mathfrak{p}$ lying over 5, and $c_{\mathfrak{p}} = 3$; for all other primes $\mathfrak{p}$, $c_{\mathfrak{p}} = 1$. In view of this example we expect that $\min V(15, 2) = 1$. We remark that K is smallest quadratic field (in terms of absolute discriminant) where $Y_1(15)$ has points [32, Thm. 5].

5.4 Elliptic curves over cubic fields

In contrast to the cases of $\mathbb{Q}$ and quadratic number fields, a complete list of possible torsion subgroups of elliptic curves over cubic fields is not known. However, there is the following partial result:

Theorem 5.4.1 (Jeon, Kim, Schweizer)**.** *As K varies over all cubic fields and E varies over all elliptic curves over K, the groups which appear infinitely often as $E(K)_{\text{tors}}$ are exactly the following:*

- $\mathbb{Z}/n$ *for* $n = 1, \ldots, 16$ *and* $18, 20$.
- $\mathbb{Z}/2 \oplus \mathbb{Z}/2n$ *for* $n = 1, \ldots, 7$.

Proof. See [29, Thm. 3.4]. □

Hence, we have admissible pairs $(N, 3)$ for $N = 1, \dots, 16, 18, 20$. It is also known by work of Parent [55, Thm. 5.1] that the only prime values of N for which $(N, 3)$ is admissible are $N = 2, 3, 5, 7, 11, 13$.

Proposition 5.4.2. *Let K be a cubic number field, and E/K an elliptic curve with a K-rational point of order 11. Then $11|c_{\mathfrak{p}}$ for every prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$ lying over 2.*

Proof. Let $P \in E(K)$ have order 11, and let $\mathfrak{p}$ be a prime ideal of $\mathcal{O}_K$ lying over 2. Let v be the place of K corresponding to $\mathfrak{p}$. We claim that $P \notin E_0(K_v)$, which will imply that $11|c_v$. Suppose that $P \in E_0(K_v)$. By Theorem 5.9.4 we have $P \notin E_1(K_v)$, so $\tilde{P} \in \tilde{E}_{\mathrm{ns}}(k_v)$ has order 11. Since k_v is either $\mathbb{F}_2, \mathbb{F}_4$ or $\mathbb{F}_8$, it follows from Theorems 5.8.1 and 5.9.1 that $k_v = \mathbb{F}_8$ and E has good reduction at v. But then $\tilde{E}$ is an elliptic curve over $\mathbb{F}_8$ with a point of order 11, and such a curve does not exist, by Theorem 5.8.2. □

Up to Galois conjugates, we have found exactly one example of an elliptic curve E over a cubic field K such that E has a K-rational point of order 11 and $\mathrm{ord}_{11}(c_E) = 1$.

Example 5.4.3. Let K be the cubic field generated by a root g of the polynomial $t^3 - t^2 + t + 1$, and let E/K be the elliptic curve with a-invariants $[a_1, a_2, a_3, a_4, a_6]$ as follows:

$$[-g, g^2 - 3g - 2, g^2 - 3g - 2, 0, 0].$$

Then $E(K)_{\mathrm{tors}} \cong \mathbb{Z}/11$ and $c_E = 11$. More precisely, the ideal (2) factors as $\mathfrak{p}_2^3$ and $c_{\mathfrak{p}_2} = 11$; for all other prime ideals $\mathfrak{p}$, $c_{\mathfrak{p}} = 1$. From this example we conclude that $\min V(11, 3) = 1$. However, we do not know whether this is the unique example achieving the minimal value $\mathrm{ord}_{11}(c_E) = 1$. We remark that the field K has very small discriminant, namely -44, and is only the third field in Jones's database [30] of cubic fields ordered by discriminant.

Considering now $N = 13$, we can show that $\min V(13, 3) = 0$. Up to Galois conjugates, we have found exactly one example of an elliptic curve E over a cubic field K such that E has a K-rational point of order 13 and $\operatorname{ord}_{13}(c_E) = 0$.

Example 5.4.4. Let $K = \mathbb{Q}(g)$, where g is a root of the polynomial $t^3 + 2t^2 - t - 1$, and let E/K be the elliptic curve with a-invariants $[a_1, a_2, a_3, a_4, a_6]$ as follows:

$$[-2g^2 + 2, -9g^2 + 2g + 4, -9g^2 + 2g + 4, 0, 0].$$

Then $E(K)_{\text{tors}} \cong \mathbb{Z}/13$ and $c_E = 1$. Note that K has very small discriminant, namely 49, and is only the fourth field in Jones's list of cubic fields ordered by discriminant.

Proposition 5.4.5. *Let K be a cubic number field, and E/K an elliptic curve with a K-rational point of order 15. Then $15|c_{\mathfrak{p}}$ for some prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$ lying over 2.*

Proof. There is some prime ideal $\mathfrak{p}$ lying over 2 such that the norm of $\mathfrak{p}$ is not 4. We will show that $15|c_{\mathfrak{p}}$. Let v be the place of K corresponding to $\mathfrak{p}$. Note that $k_v = \mathbb{F}_2$ of $\mathbb{F}_8$. The group $E(K)$ has a point P_3 of order 3 and a point P_5 of order 5. We will show that neither point can belong to $E_0(K_v)$, and this will imply that $15|c_v$.

First of all, we cannot have both $P_3 \in E_0(K_v)$ and $P_5 \in E_0(K_v)$: if this were the case, then by Theorem 5.9.4 the group $\tilde{E}_{\text{ns}}(k_v)$ would have order divisible by 15. However, it follows from Theorems 5.8.1 and 5.9.1 that, regardless of the reduction type of E at v, the order of the group $\tilde{E}_{\text{ns}}(k_v)$ is at most 14. Thus, either P_3 or P_5 does not belong to $E_0(K_v)$. We show now that in fact neither point belongs to $E_0(K_v)$.

Suppose that $P_3 \in E_0(K_v)$. Then $P_5 \notin E_0(K_v)$, so $5|c_v$. By Theorem 5.9.3 this implies that E has split multiplicative reduction at v, so $\tilde{E}_{\text{ns}}(k_v) \cong \mathbb{G}_m(k_v)$ by Theorem 5.9.1. But by Theorem 5.9.4 we have that $\tilde{P}_3 \in \tilde{E}_{\text{ns}}(k_v)$ has order 3, so 3 divides the order of k_v^*, which is either 1 or 7. This is a contradiction, so we conclude that $P_3 \notin E_0(K_v)$.

Finally, suppose that $P_5 \in E_0(K_v)$. Since $P_3 \notin E_0(K_v)$, E cannot have good reduction at v. Since $k_v = \mathbb{F}_2$ or $\mathbb{F}_8$, by Theorem 5.9.1 the order of the group $\tilde{E}_{\mathrm{ns}}(k_v)$ is either $1, 2, 3, 7, 8$ or 9. But the image of P_5 in this group has order 5 by Theorem 5.9.4, so we have a contradiction. Therefore, $P_5 \notin E_0(K_v)$, and we are done. □

Up to Galois conjugates, we have found exactly two examples of an elliptic curve E over a cubic field K such that E has a K-rational point of order 15 and $\mathrm{ord}_{15}(c_E) = 1$.

Example 5.4.6.

- Let K be the cubic field generated by a root α of the polynomial $t^3 + 2t - 1$, and let E/K be the elliptic curve with a-invariants $[a_1, a_2, a_3, a_4, a_6]$ as follows:

  $$[-2\alpha^2 - 2\alpha - 3, 22\alpha^2 + 10\alpha + 48, 22\alpha^2 + 10\alpha + 48, 0, 0].$$

  Then $E(K)_{\mathrm{tors}} \cong \mathbb{Z}/15$ and $c_E = 3 \cdot 5^2$. More precisely: the ideal (2) factors as $\mathfrak{p}_{2,1} \cdot \mathfrak{p}_{2,2}$ with $c_{\mathfrak{p}_{2,1}} = 15$ and $c_{\mathfrak{p}_{2,2}} = 5$; for every other prime ideal $\mathfrak{p}$, $c_{\mathfrak{p}} = 1$. The field K has discriminant -59, making it the fifth field in Jones's list of cubic fields.

- Let K be the cubic field generated by a root α of the polynomial $t^3 - t^2 + t + 1$, and let E/K be the elliptic curve with a-invariants $[a_1, a_2, a_3, a_4, a_6]$ as follows:

  $$[-2\alpha^2 + 12\alpha + 15, 70\alpha^2 - 126\alpha - 84, 490\alpha^2 - 882\alpha - 588, 0, 0].$$

  Then $E(K)_{\mathrm{tors}} \cong \mathbb{Z}/15$ and $c_E = 3 \cdot 5^2$. More precisely: the ideal (2) factors as $\mathfrak{p}_2^3$ with $c_{\mathfrak{p}_2} = 15$. The ideal (7) factors as $\mathfrak{p}_{7,1} \cdot \mathfrak{p}_{7,2}$ with $c_{\mathfrak{p}_{7,1}} = 5$; for every other prime ideal $\mathfrak{p}$, $c_{\mathfrak{p}} = 1$. The field K has discriminant -44, making it the third field in Jones's list of cubic fields.

From these examples we conclude that $\min V(15,3) = 1$. However, we do not know whether these are the only examples achieving the minimal value $\mathrm{ord}_{15}(c_E) = 1$.

5.5 Elliptic curves over quartic fields

As in the case of cubic fields, a complete list of possible torsion subgroups of elliptic curves over quartic fields is not known. However, Jeon, Kim, and Park [28, Thm. 3.6] showed that there are exactly 38 groups occurring infinitely often as $E(K)_{\mathrm{tors}}$ over quartic number fields K. Kamienny, Stein, and Stoll have announced a proof that the only admissible pairs $(N, 4)$ with N prime have $N = 2, 3, 5, 7, 11, 13, 17$. We will consider here only $N = 17$, which does not occur over fields of degree smaller than 4.

Proposition 5.5.1. *Let K be a quartic number field, and E/K an elliptic curve with a K-rational point of order 17. If 2 is not inert in K, then $17 | c_{\mathfrak{p}}$ for every prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$ lying over 2.*

Proof. Let $P \in E(K)$ have order 17, and let $\mathfrak{p}$ be a prime ideal of $\mathcal{O}_K$ lying over 2. Let v be the place of K corresponding to $\mathfrak{p}$. We claim that $P \notin E_0(K_v)$, which will imply that $17 | c_v$. Suppose that $P \in E_0(K_v)$. By Theorem 5.9.4 we have $P \notin E_1(K_v)$, so $\tilde{P} \in \tilde{E}_{\mathrm{ns}}(k_v)$ has order 17. Since 2 is not inert in K, the residue field k_v is either $\mathbb{F}_2, \mathbb{F}_4$ or $\mathbb{F}_8$. It follows from Theorems 5.8.1 and 5.9.1 that, regardless of the reduction type of E at v, the order of the group $\tilde{E}_{\mathrm{ns}}(k_v)$ is at most 14. This is a contradiction, so $P \notin E_0(K_v)$, as claimed. □

The following example was found using the main algorithm in the paper [15]; see Example 5.7.6 below for more details. Up to Galois conjugates, we have found exactly one example of an elliptic curve E over a quartic field K such that E has a K-rational point of order 17 and $\mathrm{ord}_{17}(c_E) = 0$.

Example 5.5.2. Let K be the quartic field generated by a root g of the polynomial $t^4 - t^3 - 3t^2 + t + 1$, and let E/K be the elliptic curve with a-invariants $[a_1, a_2, a_3, a_4, a_6]$ as follows:

$$[-6g^3 - 7g^2 + 4g + 4, -155g^3 - 170g^2 + 109g + 74, -155g^3 - 170g^2 + 109g + 74, 0, 0].$$

Then $E(K)_{\mathrm{tors}} \cong \mathbb{Z}/17$ and $c_E = 1$. In view of this example we conclude that $\min V(17, 4) = 0$. We remark that K has very small discriminant for a quartic field, namely 725, making it the 37th quartic field in Jones's list of fields ordered by discriminant.

5.6 Elliptic curves over quintic fields

We are not aware of any published work giving a conjecturally complete list of torsion subgroups of elliptic curves over quintic number fields. However, Derickx, Kamienny, Stein, and Stoll have claimed a proof that the only admissible pairs $(N, 5)$ with N prime have $N = 2, 3, 5, 7, 11, 13, 17, 19$. We will consider here only $N = 19$, which does not occur over fields of degree smaller than 5.

Proposition 5.6.1. *Let K be a quintic number field, and E/K an elliptic curve with a K-rational point of order* 19*. If 2 is not inert in K, then* $19|c_{\mathfrak{p}}$ *for every prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$ lying over 2.*

Proof. Let $P \in E(K)$ have order 19, and let $\mathfrak{p}$ be a prime ideal of $\mathcal{O}_K$ lying over 2. Let v be the place of K corresponding to $\mathfrak{p}$. We claim that $P \notin E_0(K_v)$, which will imply that $19|c_v$. Suppose that $P \in E_0(K_v)$. By Theorem 5.9.4 we have $P \notin E_1(K_v)$, so $\tilde{P} \in \tilde{E}_{\mathrm{ns}}(k_v)$ has order 19. Since 2 is not inert in K, the residue field k_v is either $\mathbb{F}_2, \mathbb{F}_4, \mathbb{F}_8$ or $\mathbb{F}_{16}$. It follows from Theorems 5.8.1 and 5.9.1 that the only way that the order of the group $\tilde{E}_{\mathrm{ns}}(k_v)$ can be divisible by 19 is if $k_v = \mathbb{F}_{16}$ and E has good reduction at v. But in this case $\tilde{E}$ is an elliptic curve over $\mathbb{F}_{16}$ with a point of order 19, and such a curve does not exist, by Theorem 5.8.2.

This is a contradiction, so $P \notin E_0(K_v)$, as claimed. □

The following example was found using the same method as Example 5.5.2 above. Up to Galois conjugates, we have found exactly one example of an elliptic curve E over a quintic field K such that E has a K-rational point of order 19 and $\mathrm{ord}_{19}(c_E) = 0$.

Example 5.6.2. Let K be the quintic field generated by a root g of the polynomial $t^5 - t^3 - 2t^2 + 1$, and let E/K be the elliptic curve with a-invariants $[a_1, a_2, a_3, a_4, a_6]$ as follows:

$$[-5g^4+4g^3+2g^2+8g-6, -37g^4+29g^3+15g^2+62g-49, -37g^4+29g^3+15g^2+62g-49, 0, 0].$$

Then $E(K)_{\mathrm{tors}} \cong \mathbb{Z}/19$ and $c_E = 1$. From this example we conclude that $\min V(19, 5) = 0$. We remark that K has very small discriminant for a quintic field, namely -4511, making it the 22nd quintic field in Jones's list of fields ordered by discriminant.

5.7 Computational methods

In order to study the main questions of this article by means of gathering computational evidence, one needs an efficient way of producing elliptic curves E over number fields K of various degrees, such that E has a K-rational torsion point of given order N. One way of doing this is to produce points of a given degree on the modular curve $X_1(N)$. We have discussed in §2.2.2 how to obtain equations for $X_1(N)$. Once such an equation is known, one would like a method of finding points of a given degree d which satisfy this equation. Moreover, it would be desirable that *all* points of degree d will be found by this method. We will show in §5.7.1 that this can be done in degrees 2 and 3 when $X_1(N)$ is an elliptic curve (which occurs when $N = 11, 14, 15$). When $X_1(N)$ has genus 2 (i.e. for $N = 13, 16, 18$), the quadratic points are described in Chapter 2. For curves of larger genera we take a different approach based on the algorithm [15] for listing elements of bounded height in number fields.

5.7.1 Quadratic and cubic points on elliptic curves

Let k be a field and let E be an elliptic curve over k defined by a Weierstrass equation $y^2 = x^3 + Ax + B$. We give here a way of describing all points in $E(\overline{k})$ that have degree 2 or 3 over k.

Proposition 5.7.1. *Suppose that $(\alpha, \beta) \in E(\overline{k})$ has degree 2 over k. Then one of the following occurs:*

1. *$\alpha \in k$ and the minimal polynomial of β is $t^2 - (\alpha^3 + A\alpha + B)$.*
2. *There is a point $(x_0, y_0) \in E(k)$ and an element $v \in k$ such that $\beta = y_0 + v(\alpha - x_0)$ and the minimal polynomial of α is $t^2 + (x_0 - v^2)t + x_0^2 + v^2x_0 + A - 2vy_0$.*

Conversely,

(i) Let $\alpha \in k$ be such that the polynomial $t^2 - (\alpha^3 + A\alpha + B)$ is irreducible, and let β be a root of this polynomial. Then $(\alpha, \beta) \in E(\overline{k})$ and has degree 2.

(ii) Let $(x_0, y_0) \in E(k)$ and $v \in k$ be such that the polynomial

$$t^2 + (x_0 - v^2)t + x_0^2 + v^2x_0 + A - 2vy_0$$

is irreducible. Let α be a root of this polynomial and let $\beta = y_0 + v(\alpha - x_0)$. Then $(\alpha, \beta) \in E(\overline{k})$ and has degree 2 over k.

Proof. Clearly $[k(\alpha) : k] = 1$ or 2, and likewise for $k(\beta)$. Suppose first that $\alpha \in k$. We cannot have $\beta \in k$, for then $k(\alpha, \beta) = k$. Therefore, $[k(\beta) : k] = 2$. Since β is a root of the polynomial $t^2 - (\alpha^3 + A\alpha + B) \in k[t]$, this must be its minimal polynomial. Thus we are led to case (1). Now suppose that $[k(\alpha) : k] = 2$. Since $\beta \in k(\alpha)$, we can write $\beta = p(\alpha)$ for some $p(t) \in k[t]$ of degree at most 1. Since α is a root of the polynomial $F(t) = t^3 + At + B - p(t)^2$, which has degree 3, $F(t)$ must factor as $F(t) = (t - x_0)m(t)$, where $m(t)$ is the minimal polynomial of α and $x_0 \in k$. Since $F(x_0) = 0$, then $(x_0, p(x_0)) \in E(k)$. Letting $y_0 = p(x_0)$ we can write $p(t) = y_0 + v(t - x_0)$ for some $v \in k$. Carrying out the division $F(t)/(t - x_0)$ we obtain $m(t)$ as in case (2) of the proposition.

We now prove the converse. The proof of (i) is trivial, so we omit it. With notation as in (ii) we have the identity

$$t^3+At+B-(y_0+v(t-x_0))^2 = (t-x_0)\left(t^2 + (x_0 - v^2)t + x_0^2 + v^2x_0 + A - 2vy_0\right)+x_0^3+Ax_0+B-y_0^2.$$

Evaluating at α we obtain $\alpha^3 + A\alpha + B - \beta^2 = 0$, so $(\alpha, \beta) \in E(\overline{k})$. It is clear that (α, β) has degree 2. □

Remark 5.7.2. The description of quadratic points on E given in the above proposition has the following geometric interpretation: suppose $P = (\alpha, \beta) \in E(\overline{k})$ is quadratic over k, let $K = k(\alpha, \beta)$ be the field of definition of P, and let σ be the nontrivial element of $\mathrm{Gal}(K/k)$. We can then consider the point $Q = P + P^\sigma \in E(k)$, where $P^\sigma = (\sigma(\alpha), \sigma(\beta))$ denotes the Galois conjugate point of P. If Q is the point at infinity on E, then the line through P and P^σ is vertical, so that $\alpha = \sigma(\alpha)$ and hence $\alpha \in k$; this gives rise to the points of type 1 in Proposition 5.7.1. If Q is not the point at infinity, then it is an affine point in $E(k)$, say $Q = (x_0, -y_0)$ for some elements $x_0, y_0 \in k$. The points P, P^σ, and (x_0, y_0) are collinear, and the line containing them has slope in k, say equal to $v \in k$; we then have $\beta = y_0 + v(\alpha - x_0)$. This gives rise to points of type 2 in Proposition 5.7.1.

Proposition 5.7.3. *Suppose that $(\alpha, \beta) \in E(\overline{k})$ has degree 3 over k. Then one of the following occurs:*

1. *$\beta \in k$ and the minimal polynomial of α is $t^3 + At + B - \beta^2$.*

2. *There is a polynomial $p(t) \in k[t]$ of degree 1 such that $\beta = p(\alpha)$ and the minimal*

polynomial of α is $t^3 + At + B - p(t)^2$.

3. *There is a point $(x_0, y_0) \in E(k)$ and elements $u, v \in k$ with $v \neq 0$ such that*

$$\beta = y_0 + u(\alpha - x_0) + v(\alpha - x_0)^2$$

and the minimal polynomial of α is given by $t^3 + c_2t^2 + c_1t + c_0$, where

$$c_2 = \frac{-3x_0v^2 + 2uv - 1}{v^2}, \qquad c_1 = \frac{3v^2x_0^2 - 4uvx_0 - x_0 + u^2 + 2vy_0}{v^2},$$

$$c_0 = \frac{-x_0^3v^2 - x_0^2 + 2x_0^2uv - x_0u^2 - 2x_0vy_0 + 2uy_0 - A}{v^2}.$$

Conversely,

(i) *Let $\beta \in k$ be such that the polynomial $t^3 + At + B - \beta^2$ is irreducible, and let α be a root of this polynomial. Then $(\alpha, \beta) \in E(\overline{k})$ and has degree 3 over k.*

(ii) *Let $p(t) \in k[t]$ be such that $\deg(p) = 1$ and the polynomial $m(t) = t^3 + At + B - p(t)^2$ is irreducible. Let α be a root of $m(t)$ and $\beta = p(\alpha)$. Then $(\alpha, \beta) \in E(\overline{k})$ and has degree 3 over k.*

(iii) *Let $(x_0, y_0) \in E(k)$ and $u, v \in k$ be such that the polynomial $m(t) = t^3 + c_2t^2 + c_1t + c_0$ (with c_i as above) is irreducible. Let α be a root of $m(t)$ and let*

$$\beta = y_0 + u(\alpha - x_0) + v(\alpha - x_0)^2.$$

Then $(\alpha, \beta) \in E(\overline{k})$ and has degree 3 over k.

Proof. We cannot have $\alpha \in k$, for then $\beta^2 \in k$, which implies that either $\beta \in k$ (in which case $[k(\alpha, \beta) : k] = 1$), or $[k(\beta) : k] = 2$, which is impossible since $[k(\alpha, \beta) : k] = 3$ is not divisible by 2. Therefore, we must have $[k(\alpha) : k] = 3$. Since $\beta \in k(\alpha)$, we can write $\beta = p(\alpha)$ for some polynomial $p(t) \in k[t]$ of degree at most 2. If $\deg(p) = 0$, so that $\beta \in k$, then α is a root of the polynomial $t^3 + At + B - \beta^2$, which has degree 3. It follows that this is the minimal polynomial of α, and we are lead to case (1). If $\deg(p) = 1$ then α is a root of the polynomial $t^3 + At + B - p(t)^2$, which has degree 3 and must therefore be the minimal polynomial of α. This leads us to case (2). Finally, suppose that $\deg(p) = 2$. Let $F(t) = p(t)^2 - (t^3 + At + B)$ and let $m(t)$ be the minimal polynomial of α. Since $F(\alpha) = 0$, then $m(t)$ divides $F(t)$, so we can write $F(t) = v^2(t - x_0)m(t)$, where v is the leading coefficient of $p(t)$ and $x_0 \in k$. Letting $y_0 = p(x_0)$ we have that $(x_0, y_0) \in E(k)$, and writing $p(t) = y_0 + u(t - x_0) + v(t - x_0)^2$ we compute $F(t)/[v^2(t - x_0)]$ and obtain $m(t)$ as in case (3).

We now prove the converse. In all cases it suffices to show that $(\alpha, \beta) \in E(\overline{k})$, for it is clear that this point has degree 3. The proofs of (i) and (ii) are trivial, so we omit them. With notation as in (iii), let $p(t) = y_0 + u(t - x_0) + v(t - x_0)^2$. We have the identity

$$p(t)^2 - (t^3 + At + B) = v^2(t - x_0)m(t) - (x_0^3 + Ax_0 + B - y_0^2);$$

evaluating at α we obtain $\beta^2 - (\alpha^3 + A\alpha + B) = 0$. □

5.7.2 Sample computations

We give here full details of three computations in order to illustrate the methods by which all the examples in previous sections were found.

Example 5.7.4. A search for $\min V(13, 2)$. We use the following equation for $X_1(13)$ given in [59]:

$$y^2 = f_{13}(x) := x^6 - 2x^5 + x^4 - 2x^3 + 6x^2 - 4x + 1.$$

By Theorem 2.6.9, all quadratic points on $X_1(13)$ are the form $(t, \sqrt{f_{13}(t)})$ for some $t \in \mathbb{Q}$.

For every rational number t such that $f_{13}(t)$ is not a square, the change of variables in [59, p. 32] allows us to construct an elliptic curve E over the quadratic field $K = \mathbb{Q}(\sqrt{f_{13}(t)})$ such that $(0,0) \in E(K)$ is a point of order 13. We can then compute the Tamagawa numbers of E using the Magma function `LocalInformation`, and thus determine the value of $\operatorname{ord}_{13}(c_E)$. We have carried out this procedure for all rational numbers t of height at most 100, keeping all those values of t which yield an elliptic curve with $\operatorname{ord}_{13}(c_E) \leq 2$. The result is that the values $t = -1, 1/2$, and 2 yield elliptic curves over $\mathbb{Q}(\sqrt{17})$ with $\operatorname{ord}_{13}(c_E) = 2$. The three curves obtained in this way are isomorphic to Galois conjugates of the curve given in Example 5.3.5.

Example 5.7.5. A search for $\min V(15,3)$. We use the following equation for $X_1(15)$ given in [59]:

$$X_1(15) : y^2 = x^3 - 27x + 8694.$$

The change of variables

$$s = \frac{y}{216} - \frac{x}{72} - \frac{7}{24}\,, \; t = \frac{x}{36} - \frac{5}{12} \tag{5.1}$$

gives the alternate equation

$$s^2 + st + s = t^3 + t^2.$$

Using Proposition 5.7.3 we will make an exhaustive search for cubic points on $X_1(15)$ within some range, and then compute the product of the Tamagawa numbers of the elliptic curves corresponding to these points. Proposition 5.7.3 divides cubic points into three classes, which we will refer to as Types 1, 2, and 3.

Type 1: We consider all rational numbers r such that the polynomial $f(x) := x^3 - 27x + 8694 - r^2$ is irreducible. We then let K be the cubic field defined by $f(x)$, and g a root of $f(x)$ in K, so that the relation $r^2 = g^3 - 27g + 8694$ is satisfied.

Type 2: We consider all rational numbers c_1, c_0 such that the polynomial

$$f(x) := x^3 - 27x + 8694 - (c_1x + c_0)^2$$

is irreducible. We then let K be the cubic field defined by $f(x)$, and g a root of $f(x)$ in K. We set $r = c_1g + c_0$ so that the relation $r^2 = g^3 - 27g + 8694$ is satisfied.

Type 3: For every point $(x_0, y_0) \in X_1(15)(\mathbb{Q})\backslash\{\infty\} = \{(15, \pm 108), (-21, 0)\}$ we consider all the rational numbers u, v such that, defining c_2, c_1 and c_0 as in Proposition 5.7.3, the polynomial $f(x) := x^3 + c_2x^2 + c_1x + c_0$ is irreducible. We then let K be the cubic field defined by $f(x)$, and g a root of $f(x)$ in K. We set $r = y_0 + u(g - x_0) + v(g - x_0)^2$ so that the relation $r^2 = g^3 - 27g + 8694$ is satisfied.

Once a cubic point (g, r) on $X_1(15)$ has been found as explained above, we make the change of variables (5.1) to obtain a cubic point (s, t) satisfying the equation $s^2 + st + s = t^3 + t^2$. We can then use the change of variables in [59, p. 36] to construct an elliptic curve E/K with a K-rational point of order 15.

We have carried out the above procedure for all rational numbers within certain height bounds: for points of Type 1 we considered all $r \in \mathbb{Q}$ with height at most 40; for points of Type 2 we considered all $c_1, c_0 \in \mathbb{Q}$ of height at most 20; and for points of Type 3 we considered all $u, v \in \mathbb{Q}$ of height at most 10. In every case we record the data giving rise to elliptic curves E with $\mathrm{ord}_{15}(c_E) \leq 1$. The result is that points of Types 1 and 2 yield no curves with this property, while points of Type 3 yield four examples which in the end are found to be only two distinct examples:

- Taking $(x_0, y_0) = (15, 108)$ and $u = 9, v = 1/3$ we obtain the cubic field K_1 with defining polynomial $x^3 + 297x + 3834$, and an elliptic curve E_1/K_1 with $\mathrm{ord}_{15}(c_{E_1}) = 1$. The field K_1 can also be defined by the simpler polynomial $x^3 + 2x - 1$; making the corresponding change of variables to the equation for E_1 we obtain the first curve given in Example 5.4.6.

- Taking $(x_0, y_0) = (15, 108)$ and $u = -9, v = -1/6$ we obtain the cubic field K_2 with defining polynomial $x^3 + 27x^2 - 1485x - 80487$, and an elliptic curve E_2/K_2 with $\mathrm{ord}_{15}(c_{E_2}) = 1$. The field K_2 can also be defined by the simpler polynomial $x^3 - x^2 + x + 1$; making the corresponding change of variables to the equation for E_2 we obtain the second curve given in Example 5.4.6.

- With $(x_0, y_0) = (-21, 0)$ and $u = -3, v = -1/6$ we are led to the same cubic field and elliptic curve as in the first example.

- With $(x_0, y_0) = (15, -108)$ and $u = 3, v = -1/6$ we are led to the same cubic field and elliptic curve as in the first example.

Example 5.7.6. A search for $\min V(17, 4)$. We need a method for producing an exhaustive list of quartic points on $X_1(17)$ within some range. Since $X_1(17)$ has genus 5, we cannot apply the methods above to give a simple description of all quartic points on it. We will therefore take a different approach.

We propose the following as a method of search for points on any affine plane curve over $\mathbb{Q}$.

Algorithm 5.7.7. Let $C/\mathbb{Q}$ be an affine plane curve defined by an equation $f(x, y) = 0$, and let K be a number field. In order to search for points in $C(K)$:

1. Choose a height bound B and make a list L of all elements of K of height at most B.

2. For each $x_0 \in L$, determine whether the polynomial $f(x_0, y)$ has a root in K; if so, we have found a point on C defined over K.

3. Similarly, for each $y_0 \in L$, determine whether the polynomial $f(x, y_0)$ has a root in K.

An equation $f(x,y)=0$ for $X_1(17)$ may be found in [72, p. 1144]. From Jones's database [30] we obtain the first 100 quartic fields. For each quartic field K, we use the algorithm [15] to make a list L of all elements of K of height at most 50. Next, we apply Algorithm 5.7.7 to search for points that $X_1(17)$ has over these quartic fields. For each point (x_0, y_0), we use the change of variables in [72, p. 1145] together with [72, Prop. 1] to construct an elliptic curve over K having a K-rational point of order 17. We record the fields K and elliptic curves E/K for which $\operatorname{ord}_{17}(c_E) \leq 1$. The result of this computation is that only one field K yields such examples, and in every case the elliptic curve E is isomorphic to a Galois conjugate of the one given in Example 5.5.2.

Remark 5.7.8. To the best of our knowledge, there are no currently implemented methods for searching for points on curves defined over general number fields, except in special families such as elliptic and hyperelliptic curves. Hence, the approach taken above using the algorithm [15] may at the moment be the only way to carry out an exhaustive search for quartic points on $X_1(17)$.

5.8 Elliptic curves over finite fields

We recall in this section a few results concerning the group of rational points on an elliptic curve over a finite field. See [67, §V.1] for more information.

Theorem 5.8.1 (Hasse)**.** *Let E be an elliptic curve over the finite field $\mathbb{F}_q$. Then*

$$|\#E(\mathbb{F}_q) - (q+1)| \leq 2\sqrt{q}.$$

Thus, the order of the group $E(\mathbb{F}_q)$ is an integer in the interval $[q+1-2\sqrt{q}, q+1+2\sqrt{q}]$. Conversely, we can ask which integers in this interval occur as the order of the group of rational points on some elliptic curve over $\mathbb{F}_q$. The answer is provided by the following result.

Theorem 5.8.2 (Waterhouse [76])**.** *Let $q = p^n$ be a power of a prime. The possible orders $\#E(\mathbb{F}_q)$, where E is an elliptic curve over $\mathbb{F}_q$, are the numbers of the form $h = q + 1 - a$ where a is an integer with $|a| \leq 2\sqrt{q}$ satisfying any one of the following:*

(a) p does not divide a.

(b) n is even and $a = \pm 2\sqrt{q}$.

(c) n is even, $p \not\equiv 1 \bmod 3$, and $a = \pm\sqrt{q}$.

(d) n is odd, $p = 2$ or 3, and $a = \pm p^{(n+1)/2}$.

(e1) n is odd and $a = 0$.

(e2) n is even, $p \not\equiv 1 \bmod 4$, and $a = 0$.

In particular, note that if q is prime, then all integers in the interval given by Hasse's theorem occur as the order of $E(\mathbb{F}_q)$ for some elliptic curve E.

Theorem 5.8.2 can be made more precise: it is known exactly which groups can occur as the group of rational points on an elliptic curve over a given finite field $\mathbb{F}_q$.

Theorem 5.8.3 (Rück [62])**.** *Let $h = \prod_\ell \ell^{h_\ell}$ be a possible order $\#E(\mathbb{F}_q)$, as described in Theorem 5.8.2. Then all possible groups $E(\mathbb{F}_q)$ with $\#E(\mathbb{F}_q) = h$ are the following:*

$$\mathbb{Z}/p^{h_p} \times \prod_{\ell \neq p} \left(\mathbb{Z}/\ell^{a_\ell} \times \mathbb{Z}/\ell^{h_\ell - a_\ell}\right)$$

with:

- *In case (b) of Theorem 5.8.2, each a_ℓ is equal to $h_\ell/2$.*
- *In all other cases, a_ℓ is any integer satisfying $0 \leq a_\ell \leq \min\{\operatorname{ord}_\ell(q-1), \lfloor h_\ell/2 \rfloor\}$.*

5.9 Reduction of elliptic curves

We recall here some facts about reductions of elliptic curves defined over local fields. A standard reference for this material is [67, Chap. VII].

Let (K, v) be a complete, discretely valued field with residue field k. We assume that v has value group $\mathbb{Z}$. If E/K is an elliptic curve, the *reduction* of E is a curve $\tilde{E}/k$ with at most one singularity. If it has no singularities, then it is an elliptic curve; in this case we say that E has *good reduction*. If there is a singularity, then it can either be a node, in which case we say that E has *multiplicative reduction*; or it can be a cusp, in which case we say that E has *additive reduction*. In the case of multiplicative reduction, we say the reduction type is *split* if the slopes of the tangent lines of $\tilde{E}$ at the singularity are in k, and the reduction is *non-split* otherwise. Regardless of reduction type, the set $\tilde{E}_{\mathrm{ns}}(k)$ of non-singular k-rational points on $\tilde{E}$ has a natural group structure.

Theorem 5.9.1 ([67], Exercise 3.5)**.** *Let K and E be as above.*

1. *If E has additive reduction, then $\tilde{E}_{\mathrm{ns}}(k)$ is isomorphic to $\mathbb{G}_a(k)$, the additive group of k.*

2. *If E has split multiplicative reduction, then $\tilde{E}_{\mathrm{ns}}(k)$ is isomorphic to $\mathbb{G}_m(k)$, the multiplicative group of k.*

3. *If E has non-split multiplicative reduction, then $\tilde{E}_{\mathrm{ns}}(k) \cong \{x \in \ell^* : N_{\ell/k}(x) = 1\}$ for some quadratic extension ℓ/k. In particular, if k is a finite field, then $|\tilde{E}_{\mathrm{ns}}(k)| = |k|+1$.*

There is a reduction map

$$E(K) \longrightarrow \tilde{E}(k)\ , \quad P \longmapsto \tilde{P}$$

giving rise to two subgroups of $E(K)$:

$$E_0(K) = \{P \in E(K) : \tilde{P} \text{ is nonsingular}\}, \quad E_1(K) = \{P \in E_0(K) : \tilde{P} = 0\}.$$

Note that if E has good reduction, then $E_0(K) = E(K)$.

Proposition 5.9.2. *The reduction map $E_0(K) \longrightarrow \tilde{E}_{\mathrm{ns}}(k)$ is a group homomorphism with kernel $E_1(K)$, and there is an exact sequence of abelian groups*

$$0 \longrightarrow E_1(K) \longrightarrow E_0(K) \longrightarrow \tilde{E}_{\mathrm{ns}}(k) \longrightarrow 0.$$

This fact allows us to study the group $E(K)$ indirectly by studying the groups appearing in the above sequence, as well as the group $E(K)/E_0(K)$. The next two results give structural information about these groups.

Theorem 5.9.3. *The group $E(K)/E_0(K)$ is finite and*

1. *cyclic if E has split multiplicative reduction.*
2. *of order 1 or 2 if E has non-split multiplicative reduction.*
3. *of order at most 4 if E has additive reduction.*

Theorem 5.9.4. *Let $p = \mathrm{char}(k)$.*

1. *If $E_1(K)$ contains an element of finite order m, then m is a power of p.*
2. *If $E_1(K)$ has a point of order p^n, then $p^{n-1}(p-1) \leq v(p)$.*

Proof. Let $\mathcal{M}$ be the valuation ideal of K, and let $\hat{E}$ be the formal group of E. Then $E_1(K) \cong \hat{E}(\mathcal{M})$, so the theorem follows from general facts about formal groups (see [67, Chap. IV]). □

Chapter 6

Computing algebraic numbers of bounded height

6.1 Introduction

All the material in this chapter is joint work with John Doyle. Let K be a number field with ring of integers $\mathcal{O}_K$, and let H_K be the relative height function on K. For any bound B it is known that the set of all $x \in K$ with $H_K(x) \leq B$ is finite [66, §3.1]. Moreover, there is an asymptotic formula for the number of such elements, due to Schanuel [64]:

$$\#\{x \in K : H_K(x) \leq B\} \sim C_K B^2,$$

where C_K is an explicit constant which depends only on K. However, there does not appear to be in the literature an algorithm that would allow fast computation of all these elements. In [56] Pethő and Schmitt require such an algorithm to be able to compute the Mordell-Weil groups of certain elliptic curves over real quadratic fields. They obtain an algorithm by showing that if $\omega_1, \ldots, \omega_n$ is an LLL-reduced integral basis of K, then every element $x \in K$

with $H_K(x) \leq B$ can be written as

$$x = \frac{a_1\omega_1 + \cdots + a_n\omega_n}{c},$$

where $a_1, \ldots, a_n, c$ are integers within certain explicit bounds depending only on B and K. The set of all such numbers x is finite, so one would only need to search through this set and discard elements whose height is greater than B. Unfortunately, in practice this method is slow because the search space is very large. We describe in this paper an algorithm which is faster, assuming class group representatives for $\mathcal{O}_K$ and a basis for the unit group of $\mathcal{O}_K$ can be computed efficiently. Sample computations showing the improvement in performance may be seen in §6.6.

Our motivation for designing a fast algorithm that can handle relatively large bounds B comes from arithmetic dynamics. In [58] Poonen provides a conjecturally complete list of rational preperiodic graph structures for quadratic polynomial maps defined over $\mathbb{Q}$. It is then natural to ask what preperiodic graph structures can occur for such maps over other number fields. In order to gather data about these graphs one needs to be able to compute all the preperiodic points of a given quadratic polynomial. It is possible to give an explicit upper bound for the height of any preperiodic point of a given map, so a first step towards computing preperiodic points is computing all points of bounded height. Further details on this question, together with the generated data, will be presented in a subsequent paper [13].

6.2 Background and notation

Let K be a number field; let $\sigma_1, \ldots, \sigma_{r_1}$ be the real embeddings of K, and $\tau_1, \overline{\tau}_1, \ldots, \tau_{r_2}, \overline{\tau}_{r_2}$ the complex embeddings. Corresponding to each of these embeddings there is an archimedean absolute value on K extending the usual absolute value on $\mathbb{Q}$. For an embedding σ, the corresponding absolute value $| \, |_\sigma$ is given by $|x|_\sigma = |\sigma(x)|_{\mathbb{C}}$, where $| \cdot |_{\mathbb{C}}$ is the usual complex absolute value. Note that $| \, |_{\bar{\tau}_i} = | \, |_{\tau_i}$ for every i. We will denote by M_K^∞ the set of absolute values corresponding to $\sigma_1, \dots, \sigma_{r_1}, \tau_1, \dots, \tau_{r_2}$.

For every maximal ideal $\mathfrak{p}$ of the ring of integers $\mathcal{O}_K$ there is a discrete valuation $v_{\mathfrak{p}}$ on K with the property that for every $a \in K^*$, $v_{\mathfrak{p}}(a)$ is the power of $\mathfrak{p}$ dividing the principal ideal (a). If $\mathfrak{p}$ lies over the prime p of $\mathbb{Z}$, there is an absolute value $| \, |_{\mathfrak{p}}$ on K extending the p-adic absolute value on $\mathbb{Q}$. Let $e(\mathfrak{p})$ and $f(\mathfrak{p})$ denote the ramification index and residual degree of $\mathfrak{p}$, respectively. This absolute value is then given by $|x|_{\mathfrak{p}} = (N\mathfrak{p})^{-v_{\mathfrak{p}}(x)/(e(\mathfrak{p})f(\mathfrak{p}))}$. We denote by M_K^0 the set of all absolute values $| \, |_{\mathfrak{p}}$, and we let $M_K = M_K^\infty \cup M_K^0$.

For an absolute value $v \in M_K$, let K_v be the completion of K with respect to v, and let $\mathbb{Q}_v$ be the completion of $\mathbb{Q}$ with respect to the restriction of v to $\mathbb{Q}$. Note that $\mathbb{Q}_v = \mathbb{R}$ if $v \in M_K^\infty$, and $\mathbb{Q}_v = \mathbb{Q}_p$ if $v \in M_K^0$ corresponds to a maximal ideal $\mathfrak{p}$ lying over p. The *local degree* of K at v is given by $n_v = [K_v : \mathbb{Q}_v]$. If v corresponds to a real embedding of K, then $K_v = \mathbb{Q}_v = \mathbb{R}$, so $n_v = 1$. If v corresponds to a complex embedding of K, then $K_v = \mathbb{C}$ and $\mathbb{Q}_v = \mathbb{R}$, so $n_v = 2$. Finally, if v corresponds to a maximal ideal $\mathfrak{p}$, then $n_v = e(\mathfrak{p})f(\mathfrak{p})$.

The *relative height* function $H_K : K \longrightarrow \mathbb{R}_{\geq 1}$ is defined by

$$H_K(\gamma) = \prod_{v \in M_K} \max\{|\gamma|_v^{n_v}, 1\}$$

and has the following properties:

- For any $\alpha, \beta \in K$ with $\beta \neq 0$, $H_K(\alpha/\beta) = \prod_{v \in M_K} \max\{|\alpha|_v^{n_v}, |\beta|_v^{n_v}\}$.

- For any $\alpha, \beta \in K$, $H_K(\alpha\beta) \leq H_K(\alpha)H_K(\beta)$.

- For any $\alpha, \beta \in \mathcal{O}_K$ with $\beta \neq 0$, $H_K(\alpha/\beta) = N(\alpha, \beta)^{-1} \prod_{v \in M_K^\infty} \max\{|\alpha|_v^{n_v}, |\beta|_v^{n_v}\}$. Here $N(\alpha, \beta)$ denotes the norm of the ideal generated by α and β.

- For any $\gamma \in K^*$, $H_K(\gamma) = H_K(1/\gamma)$.

- For any $\gamma \in K$ and any root of unity $\zeta \in K$, $H_K(\zeta\gamma) = H_K(\gamma)$.

It will sometimes be convenient to use the logarithmic height function $h_K = \log \circ H_K$.

The following notation will be used throughout: $\mathcal{O}_K^\times$ is the unit group of $\mathcal{O}_K$, μ_K is the group of roots of unity in K, $r = r_1 + r_2 - 1$ is the rank of $\mathcal{O}_K^\times$, and h is the class number of K. For an ideal I of $\mathcal{O}_K$ we let $N(I)$ denote the norm of the ideal.

Define a logarithmic map $\Lambda : K^* \longrightarrow \mathbb{R}^{r+1}$ by

$$\Lambda(x) = (\log |x|_v^{n_v})_{v \in M_K^\infty} = \left(\log |x|_{\sigma_1}, \ldots, \log |x|_{\sigma_{r_1}}, \log |x|_{\tau_1}^2, \ldots, \log |x|_{\tau_{r_2}}^2\right).$$

Note that Λ is a group homomorphism. By a classical result of Kronecker, the kernel of Λ is μ_K. Letting $\pi : \mathbb{R}^{r+1} \longrightarrow \mathbb{R}^r$ be the projection map that deletes the last coordinate, we set $\Lambda' = \pi \circ \Lambda$.

Recall [38, Chap. 5] that there is a system $\boldsymbol{\varepsilon} = \{\varepsilon_1, \ldots, \varepsilon_r\} \subset \mathcal{O}_K^\times$ of *fundamental units* such that every unit $u \in \mathcal{O}_K^\times$ can be written uniquely as $u = \zeta\varepsilon_1^{n_1} \cdots \varepsilon_r^{n_r}$ for some integers $n_1, \ldots, n_r$ and some $\zeta \in \mu_K$. We denote by $S(\boldsymbol{\varepsilon})$ the $r \times r$ matrix with column vectors $\Lambda'(\varepsilon_i)$.

6.3 The method

Let K be a number field with relative height function $H_K : K \longrightarrow \mathbb{R}_{\geq 1}$. Given a bound $B \geq 1$, we want to list the elements $\gamma \in K$ satisfying $H_K(\gamma) \leq B$. Our method for finding all such numbers is based on the observation that this problem can be reduced to the question of finding all units of bounded height. In essence, the idea is to generalize the following statement that holds over $\mathbb{Q}$: if $x \in \mathbb{Q}^*$ and $H_\mathbb{Q}(x) \leq B$, then x can be written as $x = \pm a/b$ where a and b are integers such that $(a, b) = 1$ and $|a|, |b| \leq B$. For a general number field K, the analogous statement we make is that given $x \in K^*$ with $H_K(x) \leq B$, it is possible to write x in the form $x = u \cdot a/b$, where $u \in \mathcal{O}_K^\times$ is a unit whose height is explicitly bounded;

a and b are elements of $\mathcal{O}_K$ such that $(a, b) = \mathfrak{a}$, where $\mathfrak{a}$ is one ideal from a predetermined list of ideal class representatives for $\mathcal{O}_K$; and $|N_{K/\mathbb{Q}}(a)|, |N_{K/\mathbb{Q}}(b)| \leq B \cdot N(\mathfrak{a})$.

6.3.1 The main algorithm

Theorem 6.3.1 below provides the theoretical basis for our algorithm. In order to describe all elements of bounded height in K we fix integral ideals $\mathfrak{a}_1, \ldots, \mathfrak{a}_h$ forming a complete set of ideal class representatives for $\mathcal{O}_K$. Suppose we are given a bound $B \geq 1$. For each ideal $\mathfrak{a}_\ell$, let $g_{\ell,1}, \ldots, g_{\ell,s_\ell}$ be generators for all the nonzero principal ideals contained in $\mathfrak{a}_\ell$ whose norms are at most $B \cdot N(\mathfrak{a}_\ell)$. We define a *B-packet* to be a tuple of the form

$$P = (\ell, (i, j), (n_1, \ldots, n_r))$$

satisfying the following conditions:

- $1 \leq \ell \leq h$;
- $1 \leq i < j \leq s_\ell$;
- $(g_{\ell,i}, g_{\ell,j}) = \mathfrak{a}_\ell$; and
- $H_K(\varepsilon_1^{n_1} \cdots \varepsilon_r^{n_r}) \leq B \cdot H_K(g_{\ell,i}/g_{\ell,j})$.

To a packet P we associate the number

$$c(P) = \varepsilon_1^{n_1} \cdots \varepsilon_r^{n_r} \cdot \frac{g_{\ell,i}}{g_{\ell,j}} \in K^* \backslash \mathcal{O}_K^\times$$

and the set

$$F(P) = \{\zeta \cdot c(P) : \zeta \in \mu_K\} \cup \{\zeta / c(P) : \zeta \in \mu_K\}.$$

Note that the union defining $F(P)$ is disjoint, and that $F(P)$ does not contain units. Moreover, all the elements of $F(P)$ have the same height. If $r = 0$, then a packet is a tuple of the form $(\ell, (i, j))$ satisfying only the first three defining conditions above, and in this case $c(P) = g_{\ell,i}/g_{\ell,j}$.

With the notation and terminology introduced above we can now describe all elements of K whose height is at most B.

Theorem 6.3.1. *Suppose that $\gamma \in K^*$ satisfies $H_K(\gamma) \leq B$. Then either $\gamma \in \mathcal{O}_K^\times$ or γ belongs to the disjoint union*

$$\bigcup_{B\text{-packets } P} F(P).$$

Proof. Assuming that $\gamma \notin \mathcal{O}_K^\times$ we must show that there is a packet P such that $\gamma \in F(P)$. We can write the fractional ideal generated by γ as $(\gamma) = IJ^{-1}$, where I and J are coprime integral ideals. Since I and J are in the same ideal class, there is some ideal $\mathfrak{a}_\ell$ (namely the one representing the inverse class of I and J) such that $\mathfrak{a}_\ell I$ and $\mathfrak{a}_\ell J$ are principal; say $(\alpha) = \mathfrak{a}_\ell I, (\beta) = \mathfrak{a}_\ell J$. Note that $(\alpha, \beta) = \mathfrak{a}_\ell$ because I and J are coprime. Since $(\gamma) = (\alpha)(\beta)^{-1}$ we may assume, after scaling α by a unit, that $\gamma = \alpha/\beta$. From the bound $H_K(\gamma) \leq B$ it follows that

$$\prod_{v \in M_K^\infty} \max\{|\alpha|_v^{n_v}, |\beta|_v^{n_v}\} \leq B \cdot N(\mathfrak{a}_\ell).$$

In particular,

$$|N_{K/\mathbb{Q}}(\alpha)| = \prod_{v \in M_K^\infty} |\alpha|_v^{n_v} \leq B \cdot N(\mathfrak{a}_\ell) \quad \text{and} \quad |N_{K/\mathbb{Q}}(\beta)| = \prod_{v \in M_K^\infty} |\beta|_v^{n_v} \leq B \cdot N(\mathfrak{a}_\ell).$$

Since $N(\alpha), N(\beta) \leq B \cdot N(\mathfrak{a}_\ell)$, there must be some indices $a, b \leq s_\ell$ such that $(\alpha) = (g_{\ell,a})$ and $(\beta) = (g_{\ell,b})$. Hence, we have $\alpha = g_{\ell,a}u_a$ and $\beta = g_{\ell,b}u_b$ for some units u_a, u_b. Letting $t = u_a/u_b$ we have $\gamma = tg_{\ell,a}/g_{\ell,b}$, and since $H_K(\gamma) \leq B$, then

$$H_K(t) = H_K(\gamma g_{\ell,b}/g_{\ell,a}) \leq H_K(\gamma)H_K(g_{\ell,b}/g_{\ell,a}) \leq B \cdot H_K(g_{\ell,b}/g_{\ell,a}).$$

Write $t = \zeta\varepsilon_1^{m_1} \cdots \varepsilon_r^{m_r}$ for some integers $m_1, \ldots, m_r$ and some $\zeta \in \mu_K$. We define indices i, j and an integer tuple $(n_1, \ldots, n_r)$ as follows: if $a < b$, we let $i = a, j = b, (n_1, \ldots, n_r) = (m_1, \ldots, m_r)$; and if $a > b$, we let $i = b, j = a, (n_1, \ldots, n_r) = (-m_1, \ldots, -m_r)$. (The case $a = b$ cannot occur since γ is not a unit.) Note that in either case we have $i < j$ and $(g_{\ell,i}, g_{\ell,j}) = (\alpha, \beta) = \mathfrak{a}_\ell$. Letting $u = \varepsilon_1^{n_1} \cdots \varepsilon_r^{n_r}$ we have $H_K(u) = H_K(t)$, so $H_K(u) \leq B \cdot H_K(g_{\ell,i}/g_{\ell,j})$. This proves that $P := (\ell, (i,j), (n_1, \ldots, n_r))$ is a B-packet. Finally, if we set $c = ug_{\ell,i}/g_{\ell,j}$, then $\zeta c = \gamma$ if $a < b$; and $\zeta/c = \gamma$ if $a > b$. Therefore, $\gamma \in F(P)$.

We show now that the union in the statement of the theorem is disjoint. Suppose that

$$P = (\ell, (i,j), (n_1, \ldots, n_r)) \text{ and } P' = (\ell', (i',j'), (n'_1, \ldots, n'_r))$$

are packets such that $F(P) \cap F(P') \neq \emptyset$. We aim to show that $P = P'$. Let $u = \varepsilon_1^{n_1} \cdots \varepsilon_r^{n_r}$, and similarly define u'. From the assumption that $F(P)$ and $F(P')$ have a common element it follows that either

$$c(P) \cdot c(P') \in \mu_K \text{ or } c(P)/c(P') \in \mu_K.$$

We consider the latter case first. There are ideals $\mathfrak{b}_{\ell,i}, \mathfrak{b}_{\ell,j}, \mathfrak{b}_{\ell',i'}, \mathfrak{b}_{\ell',j'}$ such that

$$(g_{\ell,i}) = \mathfrak{a}_\ell \mathfrak{b}_{\ell,i} \text{ ; } (g_{\ell,j}) = \mathfrak{a}_\ell \mathfrak{b}_{\ell,j} \text{ ; } (g_{\ell',i'}) = \mathfrak{a}_{\ell'} \mathfrak{b}_{\ell',i'} \text{ ; } (g_{\ell',j'}) = \mathfrak{a}_{\ell'} \mathfrak{b}_{\ell',j'} \text{ .} \tag{6.1}$$

Note that $\mathfrak{b}_{\ell,i}$ and $\mathfrak{b}_{\ell,j}$ are coprime because $(g_{\ell,i}, g_{\ell,j}) = \mathfrak{a}_\ell$; similarly, $\mathfrak{b}_{\ell',i'}$ and $\mathfrak{b}_{\ell',j'}$ are coprime. Now, since $c(P)/c(P') \in \mu_K$, there is an equality of ideals $(g_{\ell,i})(g_{\ell',j'}) = (g_{\ell,j})(g_{\ell',i'})$. Therefore, $\mathfrak{b}_{\ell,i}\mathfrak{b}_{\ell',j'} = \mathfrak{b}_{\ell,j}\mathfrak{b}_{\ell',i'}$ and by coprimality we conclude that

$$\mathfrak{b}_{\ell,i} = \mathfrak{b}_{\ell',i'} \text{ and } \mathfrak{b}_{\ell,j} = \mathfrak{b}_{\ell',j'}. \tag{6.2}$$

Considering ideal classes, by (6.1) and (6.2) we obtain

$$[\mathfrak{a}_\ell]^{-1} = [\mathfrak{b}_{\ell,i}] = [\mathfrak{b}_{\ell',i'}] = [\mathfrak{a}_{\ell'}]^{-1},$$

so $\ell = \ell'$. Thus, again using (6.1) and (6.2),

$$(g_{\ell,i}) = \mathfrak{a}_\ell \mathfrak{b}_{\ell,i} = \mathfrak{a}_{\ell'} \mathfrak{b}_{\ell',i'} = (g_{\ell',i'}) = (g_{\ell,i'}),$$

and hence $i = i'$. Similarly, $j = j'$. It follows that $u/u' = c(P)/c(P') \in \mu_K$, so $(n_1, \ldots, n_r) = (n'_1, \ldots, n'_r)$, and therefore $P = P'$.

The case where $c(P) \cdot c(P') \in \mu_K$ is dealt with similarly, and leads to the conclusion that $(i, j) = (j', i')$. But this is a contradiction, since $i < j$ and $i' < j'$; therefore, this case cannot occur. □

Remark 6.3.2. In the case where $r = 0$, Theorem 6.3.1 and its proof still hold if we omit mention of the fundamental units. See §6.4.4 for a refinement of the theorem in this case.

From Theorem 6.3.1 we deduce the following algorithm.

Algorithm 6.3.3 (Algebraic numbers of bounded height)**.**
Input: A number field K and a bound $B \geq 1$.
Output: A list of all elements $x \in K$ satisfying $H_K(x) \leq B$.

1. Create a list L containing only the element 0.

2. Determine a complete set $\mathfrak{a}_1, \ldots, \mathfrak{a}_h$ of ideal class representatives for $\mathcal{O}_K$.

3. Compute fundamental units $\varepsilon_1, \ldots, \varepsilon_r$.

4. Include in L all units $u \in \mathcal{O}_K^\times$ with $H_K(u) \leq B$.

5. For each ideal $\mathfrak{a}_\ell$:

(a) Find generators $g_{\ell,1}, \dots, g_{\ell,s_\ell}$ for all the nonzero principal ideals contained in $\mathfrak{a}_\ell$ whose norms are at most $B \cdot N(\mathfrak{a}_\ell)$.

(b) For each pair of indices i, j such that $1 \le i < j \le s_\ell$ and $(g_{\ell,i}, g_{\ell,j}) = \mathfrak{a}_\ell$:

i. Find all units u of the form $u = \varepsilon_1^{n_1} \cdots \varepsilon_r^{n_r}$ such that $H_K(u) \le B \cdot H_K(g_{\ell,i}/g_{\ell,j})$.

ii. For all such units u, let $c = u \cdot g_{\ell,i}/g_{\ell,j}$. If $H_K(c) \le B$, then append to L all elements of the form $\zeta \cdot c$ and ζ/c with $\zeta \in \mu_K$.

6. Return the list L.

Note that, by Theorem 6.3.1, the list L will not contain duplicate elements. There are known methods [8, §6.5] for carrying out steps 2 and 3 of Algorithm 6.3.3. An efficient method for step 5a can be found in the article of Fincke and Pohst [16]. It remains to explain how a set of units of bounded height can be computed.

6.3.2 Units of bounded height

For a given bound $D \ge 1$ we wish to determine all units $u \in \mathcal{O}_K^\times$ such that $H_K(u) \le D$. Our method for doing this makes use of the following classical result.

Theorem 6.3.4 (Dirichlet)**.** *The map $\Lambda' : \mathcal{O}_K^\times \longrightarrow \mathbb{R}^r$ is a group homomorphism with kernel μ_K, and $\Lambda'(\mathcal{O}_K^\times)$ is a lattice of full rank in $\mathbb{R}^r$ spanned by the vectors $\Lambda'(\varepsilon_1), \dots, \Lambda'(\varepsilon_r)$.*

Let $S = S(\boldsymbol{\varepsilon})$ be the $r \times r$ matrix with column vectors $\Lambda'(\varepsilon_i)$, and let $T = S^{-1}$ be the linear automorphism of $\mathbb{R}^r$ taking the basis $\Lambda'(\varepsilon_1), \dots, \Lambda'(\varepsilon_r)$ to the standard basis for $\mathbb{R}^r$.

Proposition 6.3.5. *Suppose $u \in \mathcal{O}_K^\times$ satisfies $H_K(u) \le D$. Then there exist an integer point $(n_1, \dots, n_r)$ in the polytope $T([-\log D, \log D]^r)$ and a root of unity $\zeta \in \mu_K$ such that $u = \zeta \varepsilon_1^{n_1} \cdots \varepsilon_r^{n_r}$.*

Proof. The bound $H_K(u) \leq D$ implies that $|u|_v^{n_v} \leq D$ for all $v \in M_K^\infty$. Since $H_K(1/u) = H_K(u)$ we also have $1/|u|_v^{n_v} \leq D$. Therefore,

$$-\log D \leq \log |u|_v^{n_v} \leq \log D \quad \text{for all } v \in M_K^\infty,$$

so $\Lambda'(u) \in [-\log D, \log D]^r$. We can write $u = \zeta \varepsilon_1^{n_1} \cdots \varepsilon_r^{n_r}$ for some $\zeta \in \mu_K$ and some integers n_i. Then $(n_1, \ldots, n_r) = T(\Lambda'(u)) \in T([-\log D, \log D]^r)$. □

The proposition leads to the following algorithm.

Algorithm 6.3.6 (Units of bounded height)**.**

Input: A number field K and a bound $D \geq 1$.

Output: A list of all units $u \in \mathcal{O}_K^\times$ satisfying $H_K(u) \leq D$.

```
1. If $r = 0$, return $\mu_K$. Otherwise:
2. Create an empty list $U$.
3. Compute fundamental units $\varepsilon_1, \ldots, \varepsilon_r$.
4. Find all integer points $Q$ in the polytope $T([-\log D, \log D]^r)$.
5. For all such points $Q = (n_1, \ldots, n_r)$ :
    (a) Let $u = \varepsilon_1^{n_1} \cdots \varepsilon_r^{n_r}$.
    (b) If $H_K(u) \leq D$, then include $u\zeta$ in $U$ for all $\zeta \in \mu_K$.
6. Return the list $U$.
```

Step 4 of Algorithm 6.3.6 can be done using known methods for finding integer points in polytopes; see, for instance, the articles [2, 11].

Remark 6.3.7. With more work it is possible to replace the box $[-\log D, \log D]^r$ in step 4 of Algorithm 6.3.6 with a substantially smaller set, namely the polytope $\mathcal{P}(D)$ in $\mathbb{R}^r$ cut out by the inequalities

$$-\log D \leq \sum_{i \in I} x_i \leq \log D,$$

where I runs through all nonempty subsets of $\{1, \dots, r\}$. This polytope is contained in the box $[-\log D, \log D]^r$, and one can show that its volume is smaller than that of the box by a factor of at least $(\lfloor r/2 \rfloor !)^2$. In addition to providing a smaller search space, using $\mathcal{P}(D)$ eliminates the need to check the heights of the units obtained. This is due to the fact that for units u, $H_K(u) \leq D$ if and only if $\Lambda'(u) \in \mathcal{P}(D)$. We omit the proofs of these statements since we will not use the polytope $\mathcal{P}(D)$ here — the box $[-\log D, \log D]^r$ works well in practice and will suffice for the theoretical analysis of the main algorithm.

For later reference we record the following facts concerning units of bounded height.

Lemma 6.3.8. *If the unit $u = \zeta \varepsilon_1^{n_1} \cdots \varepsilon_r^{n_r}$ satisfies $H_K(u) \leq D$, then*

$$\max_{1 \leq i \leq r} |n_i| \leq M := \lceil \|T\| \cdot \sqrt{r} \cdot \log D \rceil,$$

where $\|T\|$ denotes the operator norm of T.

Proof. By Proposition 6.3.5, the point $(n_1, \dots, n_r)$ belongs to $T([-\log D, \log D]^r)$. Every vector in this polytope has Euclidean norm at most M, so the polytope is contained in $[-M, M]^r$. Hence, $(n_1, \dots, n_r) \in [-M, M]^r$. □

Corollary 6.3.9. *Fix $\lambda > 0$. There is a constant $q = q(\lambda, K, \boldsymbol{\varepsilon})$ such that for every bound $D \geq 1 + \lambda$, the number of units $u \in \mathcal{O}_K^\times$ satisfying $H_K(u) \leq D$ is at most $q \cdot (\log D)^r$.*

Proof. Suppose $u = \zeta \varepsilon_1^{n_1} \cdots \varepsilon_r^{n_r}$ is a unit with $H_K(u) \leq D$. By Lemma 6.3.8, $(n_1, \dots, n_r) \in [-M, M]^r$. This gives at most $(2M + 1)^r$ options for the tuple $(n_1, \dots, n_r)$, and hence at most $(\#\mu_K) \cdot (2M+1)^r$ options for u. Therefore,

$$\frac{\#\{u \in \mathcal{O}_K^\times : H_K(u) \leq D\}}{(\log D)^r} \leq (\#\mu_K) \left(\frac{3}{\log(1+\lambda)} + 2\sqrt{r} \cdot \|T\| \right)^r ,$$

and the result follows. □

While Algorithms 6.3.3 and 6.3.6 form a theoretically accurate description of our method, for purposes of computing they are not optimal. We discuss now a few changes to the method which will make it more efficient.

6.3.3 Computational improvements to the method

We aim in this section to modify Algorithms 6.3.3 and 6.3.6 with the following goals in mind: to avoid computing any given piece of data more than once; to minimize the cost of height computations; and to avoid, as much as possible, doing arithmetic with fundamental units. The latter is desirable because fundamental units in a number field can be very large, so that arithmetic operations with them might be costly.

Regarding the expense of height computations, we begin by noting that the height of an element of K can be computed by using the logarithmic map Λ. Indeed, suppose α, β are nonzero elements of $\mathcal{O}_K$; letting $\Lambda(\alpha) = (x_1, \ldots, x_{r+1})$ and $\Lambda(\beta) = (y_1, \ldots, y_{r+1})$ we have

$$\log(N(\alpha, \beta)) + h_K(\alpha/\beta) = \sum_{i=1}^{r+1} \max\{x_i, y_i\}. \tag{6.3}$$

In view of this fact, throughout this section we will use the logarithmic height function h_K rather than H_K. From a computational standpoint, h_K is also more convenient because it is defined as a sum rather than a product.

To minimize the amount of time spent on height computations in step 5 of Algorithm 6.3.3, we make the following observation. Using (6.3), all of the heights required in that step can be computed from the data of the real vectors $\Lambda(\varepsilon_1), \ldots, \Lambda(\varepsilon_r)$ and the vectors $\Lambda(g_{\ell,i})$ for all indices ℓ, i:

- The height of a unit $u = \varepsilon_1^{n_1} \cdots \varepsilon_r^{n_r}$ can be found knowing only the tuple $(n_1, \ldots, n_r)$ — without actually computing u. Indeed, $h_K(u)$ can be computed from the vector $\Lambda(u)$, which is equal to $\sum_{j=1}^{r} n_j \Lambda(\varepsilon_j)$.
- The numbers $h_K(g_{\ell,i}/g_{\ell,j})$ required in step 5(b)(i) of Algorithm 6.3.3 can be computed from the vectors $\Lambda(g_{\ell,i})$ and $\Lambda(g_{\ell,j})$.
- Using the fact that $\Lambda(ug_{\ell,i}) = \Lambda(u) + \Lambda(g_{\ell,i})$, the number $h_K(u \cdot g_{\ell,i}/g_{\ell,j})$ in step 5(b)(ii) can be computed from the tuple $(n_1, \ldots, n_r)$ and the vectors $\Lambda(g_{\ell,i})$, $\Lambda(g_{\ell,j})$.

From these observations we conclude that the vectors $\Lambda(\varepsilon_1), \ldots, \Lambda(\varepsilon_r)$ and $\Lambda(g_{\ell,i})$ (for all appropriate indices ℓ, i) should be computed once and stored for later use; all height computations that take place within the algorithm can then make use of this precomputed data.

Step 5(b)(i) of Algorithm 6.3.3, in which we compute all units of height less than a given bound, must be performed many times — each time with a different height bound. It would be more efficient to let d be the largest height bound considered, and determine the list U of units u satisfying $h_K(u) \leq d$. This list will then contain all units needed throughout the algorithm. In particular, the units from step 4 can be obtained from U. Hence, step 4 should be carried out only after the list U has been computed. By making these changes, only one computation of units of bounded height will be required throughout the entire algorithm.

Similar remarks apply to step 5(a) of Algorithm 6.3.3: letting $N = \max_\ell N(\mathfrak{a}_\ell)$, we should list all principal ideals of $\mathcal{O}_K$ whose norms do not exceed $B \cdot N$. All of the ideals required in step 5(a) can then be found within this list. Thus, only one computation of principal ideals of bounded norm will be needed throughout the algorithm.

With all of the above modifications in mind we now give an improved version of our method.

Algorithm 6.3.10 (Algebraic numbers of bounded height)**.**
Input: A number field K and a bound $B \geq 1$.
Output: A list L of all elements $\gamma \in K$ satisfying $H_K(\gamma) \leq B$.

1. Find a complete set $\mathfrak{a}_1, \ldots, \mathfrak{a}_h$ of ideal class representatives.
2. Let $N = \max_\ell N(\mathfrak{a}_\ell)$ and make a list $\mathcal{P}$ of all nonzero principal ideals of $\mathcal{O}_K$ — each represented by a single generator g — having norm at most $B \cdot N$. Record $\Lambda(g)$ for each g.
3. For each ideal $\mathfrak{a}_\ell$, make a list $(g_{\ell,1}), \ldots, (g_{\ell,s_\ell})$ of all elements of $\mathcal{P}$ contained in $\mathfrak{a}_\ell$ whose norms are at most $B \cdot N(\mathfrak{a}_\ell)$.
4. For each index ℓ:
   (a) Make a list R_ℓ of pairs (i, j) such that $1 \leq i < j \leq s_\ell$ and $(g_{\ell,i}, g_{\ell,j}) = \mathfrak{a}_\ell$.
   (b) For each pair (i, j) in R_ℓ, use the data recorded in step (2) to compute $h_{\ell,i,j} = h_K(g_{\ell,i}/g_{\ell,j})$.
5. Let $d = \log B + \max_\ell \max_{(i,j)\in R_\ell} h_{\ell,i,j}$.
6. Compute a system $\boldsymbol{\varepsilon} = \{\varepsilon_1, \ldots, \varepsilon_r\}$ of fundamental units, and record their images under the logarithmic map Λ. Construct the matrix $S = S(\boldsymbol{\varepsilon})$ with column vectors $\Lambda'(\varepsilon_1), \ldots, \Lambda'(\varepsilon_r)$.
7. Construct a list U consisting of all integer vectors $(n_1, \ldots, n_r)$ in the polytope $S^{-1}([-d, d]^r)$.
8. Create a list L containing only the element 0, and create empty lists U_0 and L_0.
9. For each tuple $\boldsymbol{u} = (n_1, \ldots, n_r)$ in U:

```
    (a) Compute the vector $\Lambda_{\boldsymbol{u}} = \sum_{j=1}^{r} n_j \Lambda(\varepsilon_j)$ using the data from step (6).
    (b) Use $\Lambda_{\boldsymbol{u}}$ to compute $h_{\boldsymbol{u}} = h_K\left(\varepsilon_1^{n_1} \cdots \varepsilon_r^{n_r}\right)$.
    (c) If $h_{\boldsymbol{u}} \leq \log B$, then append $\boldsymbol{u}$ to $U_0$.
    (d) If $h_{\boldsymbol{u}} > d$, then remove $\boldsymbol{u}$ from $U$.
10. For each index $\ell$ :
        For each pair $(i,j) \in R_\ell$ :
            For each tuple $\boldsymbol{u} = (n_1, \ldots, n_r)$ in $U$:
                If $h_{\boldsymbol{u}} \leq \log B + h_{\ell,i,j}$, then:
                    i. Let $P$ be the packet $(\ell, (i,j), (n_1, \ldots, n_r))$.
                    ii. Use the data recorded in steps (2) and (9a) to compute $h_K(c(P))$.
                    iii. If $h_K(c(P)) \leq \log B$, then append the packet $P$ to $L_0$.
11. For each tuple $(n_1, \ldots, n_r)$ in $U_0$, append to $L$ all numbers of the form $\zeta\varepsilon_1^{n_1} \cdots \varepsilon_r^{n_r}$ with $\zeta \in \mu_K$.
12. For each packet $P$ in $L_0$, append to $L$ all numbers of the form $\zeta \cdot c(P)$ and $\zeta / c(P)$ with $\zeta \in \mu_K$.
13. Return the list $L$.
```

Note that several quantities appearing in Algorithm 6.3.10 involve real numbers, so that an implementation of the algorithm may require floating point arithmetic. For some applications this may not be an issue, but if one needs to know with certainty that all elements not exceeding the specified height bound have been found, then it is imperative to choose the precision for floating point calculations carefully. In the next section we will address this in detail.

6.4 Error analysis

There are two issues that must be considered in order to implement Algorithm 6.3.10 in such a way that the output is guaranteed to be complete and correct. These issues are due to the fact that in a computer we cannot work exactly with the real numbers that appear in the algorithm (heights of algebraic numbers, logarithms of real numbers, absolute values of algebraic numbers), so we must make do with rational approximations of them. We consider now the question of finding approximations that are good enough to guarantee correct results.

The first issue is that of computing the height of an algebraic number. In carrying out Algorithm 6.3.10 one must check inequalities of the form $h_K(x) \leq D$ for given $x \in K^*$ and $D \in \mathbb{R}$. In practice, one can only work with rational approximations $\tilde{h}$ of $h_K(x)$ and $\tilde{D}$ of D, and check whether $\tilde{h} \leq \tilde{D}$. However, it may happen that $h_K(x) \leq D$ even though $\tilde{h} > \tilde{D}$. To deal with this problem one must be able to find arbitrarily close rational approximations of $h_K(x)$.

The second issue is that of enumerating lattice points inside a polytope, which is needed in Algorithm 6.3.6. The polytopes considered are of the form $T(\mathcal{B})$, where $\mathcal{B} = [-d, d]^r$ is a box in $\mathbb{R}^r$ and $T : \mathbb{R}^r \longrightarrow \mathbb{R}^r$ is a linear isomorphism. In practice, the box $\mathcal{B}$ must be replaced by a box $\tilde{\mathcal{B}}$ with rational vertices, and the matrix of T must be approximated by a rational matrix corresponding to a map $\tilde{T}$. We will not necessarily have an equality $\mathbb{Z}^r \cap T(\mathcal{B}) = \mathbb{Z}^r \cap \tilde{T}(\tilde{\mathcal{B}})$, so lattice points may be lost in this approximation process. One must therefore take great care to ensure that good enough approximations are found so that at least there is a containment $\mathbb{Z}^r \cap T(\mathcal{B}) \subseteq \mathbb{Z}^r \cap \tilde{T}(\tilde{\mathcal{B}})$.

There are several ways of dealing with these issues, each one leading to a different implementation of the main algorithm. For concreteness, we describe in this section one way of solving these problems, and we give the corresponding modification of Algorithm 6.3.10.

We introduce the following terminology to be used throughout this section: if $\vec{x} = (x_1, \ldots, x_m)$ is a vector in the Euclidean space $\mathbb{R}^m$, we say that $\vec{y} = (y_1, \ldots, y_m) \in \mathbb{R}^m$ is a δ-*approximation* of $\vec{x}$ if $|x_i - y_i| < \delta$ for all $1 \le i \le m$.

6.4.1 The height function

Given an element $x \in K^*$ and a real number $\lambda > 0$, we wish to compute a rational number $\tilde{h}$ such that $|\tilde{h} - h_K(x)| < \lambda$. Writing $x = \alpha/\beta$ with $\alpha, \beta \in \mathcal{O}_K$ and using (6.3), we see that $h_K(x)$ can be approximated by first finding good approximations of the vectors $\Lambda(\alpha)$ and $\Lambda(\beta)$.

Lemma 6.4.1. *Fix $\lambda > 0$ and set $\delta = \lambda/(r+2)$. Let α, β be nonzero elements of $\mathcal{O}_K$. Let $\tilde{n}$, $(s_1, \ldots, s_{r+1})$, and $(t_1, \ldots, t_{r+1})$ be δ-approximations of $\log(N(\alpha, \beta))$, $\Lambda(\alpha)$, and $\Lambda(\beta)$, respectively. Then, with*

$$\tilde{h} = -\tilde{n} + \sum_{i=1}^{r+1} \max\{s_i, t_i\}$$

we have $|h_K(\alpha/\beta) - \tilde{h}| < \lambda$.

Proof. Let $\Lambda(\alpha) = (x_1, \ldots, x_{r+1})$ and $\Lambda(\beta) = (y_1, \ldots, y_{r+1})$. Using (6.3) we obtain

$$|h_K(\alpha/\beta) - \tilde{h}| \le |\tilde{n} - \log(N(\alpha, \beta))| + \sum_{i=1}^{r+1} |\max\{x_i, y_i\} - \max\{s_i, t_i\}| < (r+2)\delta = \lambda.$$

□

For a nonzero element $y \in K$, each entry of the vector $\Lambda(y)$ is of the form $n_v \log |y|_v$ for some place $v \in M_K^\infty$. Corresponding to v there is an embedding $\sigma : K \hookrightarrow \mathbb{C}$ such that $|y|_v = |\sigma(y)|$. Since $\sigma(y)$ is a complex root of the minimal polynomial of y, known methods (see [54], for instance) can be applied to approximate $\sigma(y)$ with any given accuracy. In this way, the vector $\Lambda(y)$ can be approximated to any required precision.

Lemma 6.4.1 provides a way of approximating the height of any element of K by using the map Λ. However, in practice a slightly different method will be needed for computing heights of units. As mentioned in §6.3.3, in order to avoid costly arithmetic with fundamental units we do not work directly with units u when carrying out Algorithm 6.3.10. Hence, we cannot approximate the vector $\Lambda(u)$ by computing $|u|_v$ for every place v. Instead, a unit $u = \varepsilon_1^{n_1} \cdots \varepsilon_r^{n_r}$ is encoded by the tuple $(n_1, \ldots, n_r)$, so we need a way of approximating $h_K(u)$ given only this tuple. Since $\Lambda(u) = \sum_{j=1}^{r} n_j \Lambda(\varepsilon_j)$, it is enough to approximate the vectors $\Lambda(\varepsilon_i)$ sufficiently well; we make this precise in the following lemma.

Lemma 6.4.2. *Fix $\lambda, M > 0$ and set $\delta = \lambda/(r(r+1)M)$. Let $\{\varepsilon_1, \ldots, \varepsilon_r\}$ be a system of fundamental units for $\mathcal{O}_K^\times$, and for each j let $(s_{1,j}, \ldots, s_{r+1,j})$ be a rational δ-approximation of $\Lambda(\varepsilon_j) = (x_{1,j}, \ldots, x_{r+1,j})$. Suppose $u = \varepsilon_1^{n_1} \cdots \varepsilon_r^{n_r}$ is a unit with $|n_1|, \ldots, |n_r| \leq M$. Then, with*

$$\tilde{h} = \sum_{i=1}^{r+1} \max \left\{ \sum_{j=1}^{r} n_j s_{i,j} \ , 0 \right\}$$

we have

$$|h_K(u) - \tilde{h}| < \lambda.$$

Proof. Since $\Lambda(u) = \sum_{j=1}^{r} n_j \Lambda(\varepsilon_j)$, the i-th coordinate of $\Lambda(u)$ is given by $\sum_{j=1}^{r} n_j x_{i,j}$. Applying (6.3) to $u = u/1$ yields

$$h_K(u) = \sum_{i=1}^{r+1} \max \left\{ \sum_{j=1}^{r} n_j x_{i,j} \ , 0 \right\}.$$

Therefore,

$$\begin{aligned} |h_K(u) - \tilde{h}| &= \left| \sum_{i=1}^{r+1} \left(\max \left\{ \sum_{j=1}^{r} n_j x_{i,j}, 0 \right\} - \max \left\{ \sum_{j=1}^{r} n_j s_{i,j}, 0 \right\} \right) \right| \\ &\leq \sum_{i=1}^{r+1} \sum_{j=1}^{r} |n_j| \cdot |x_{i,j} - s_{i,j}| < r(r+1)M\delta = \lambda. \end{aligned}$$

□

6.4.2 Units of bounded height

We use here the notation from §3.2. Let $d = \log D$ and let $\mathcal{B} = [-d, d]^r$. Algorithm 6.3.6 requires that we enumerate all integer lattice points in the polytope $S^{-1}(\mathcal{B})$. In practice, the matrix S must be replaced by a rational approximation $\tilde{S}$, and the box $\mathcal{B}$ by a rational box $\tilde{\mathcal{B}}$. We show here how to choose these approximations so that $S^{-1}(\mathcal{B}) \subseteq \tilde{S}^{-1}(\tilde{\mathcal{B}})$. For the purpose of enumerating integer lattice points, we may then replace $\mathcal{B}$ with $\tilde{\mathcal{B}}$ and S with $\tilde{S}$, thus avoiding errors arising from floating-point arithmetic.

For a vector $v \in \mathbb{R}^r$ we denote by $|v|$ the usual Euclidean norm of v, and for a linear map $L : \mathbb{R}^r \longrightarrow \mathbb{R}^r$ we let $\|L\|$ denote the operator norm,

$$\|L\| = \sup_{|x| \leq 1} |Lx| \ .$$

We also denote by L the matrix of L with respect to the standard basis for $\mathbb{R}^r$. Recall that the supremum norm of L is given by $\|L\|_{\sup} := \max_{i,j} |L_{i,j}|$, and that there is an inequality

$$\|L\| \leq r\sqrt{r} \cdot \|L\|_{\sup}. \tag{6.4}$$

We begin with two results which will be useful for approximating the inverse of a matrix.

Lemma 6.4.3. *Let V be an $r \times r$ invertible matrix over the real numbers, and let $\tilde{V}$ be a matrix such that*

$$\|\tilde{V} - V\| \cdot \|V^{-1}\| < 1.$$

Then $\tilde{V}$ is invertible and

$$\|\tilde{V}^{-1} - V^{-1}\| \leq \frac{\|\tilde{V} - V\| \cdot \|V^{-1}\|^2}{1 - \|\tilde{V} - V\| \cdot \|V^{-1}\|}.$$

Proof. See the proof of Theorem 9.8 in [63]. □

Using (6.4) we obtain:

Corollary 6.4.4. *With V as in the lemma, let m be a constant with $m \geq r^2 \cdot \|V^{-1}\|_{\sup}$. Given $\lambda > 0$, let $\tilde{V}$ be a matrix such that $\|\tilde{V} - V\|_{\sup} < \frac{\lambda}{r^2(m^2+m\lambda)}$. Then $\tilde{V}$ is invertible and $\|\tilde{V}^{-1} - V^{-1}\| < \lambda$.*

We can now give the required accuracy in approximating the matrix S.

Proposition 6.4.5. *Let S be an invertible $r \times r$ matrix over the real numbers, and let d be a positive real number. Given $\eta > 0$, define $\tilde{\mathcal{B}} = [-d-\eta, d+\eta]^r$. Let m be a real number such that*

$$m \geq r^2 \cdot \max\{\|S\|_{\sup}, \|S^{-1}\|_{\sup}\}.$$

Define constants

$$\lambda := \frac{\eta}{dr(1+m)} \;\; \textit{and} \;\; \delta := \min\left\{\frac{\lambda}{r^2(m^2+m\lambda)}, \frac{1}{r^2}\right\}.$$

If $\tilde{S}$ is any $r \times r$ matrix such that $\|\tilde{S} - S\|_{\sup} < \delta$, then $\tilde{S}$ is invertible and $S^{-1}(\mathcal{B}) \subseteq \tilde{S}^{-1}(\tilde{\mathcal{B}})$.

Proof. It follows from Corollary 6.4.4 that $\tilde{S}$ is invertible and $\|\tilde{S}^{-1} - S^{-1}\| < \lambda$. For any $x \in \mathcal{B}$ we then have

$$|\tilde{S}(S^{-1}x) - x| = |\tilde{S}(S^{-1}x) - \tilde{S}(\tilde{S}^{-1}x)| \leq \|\tilde{S}\| \cdot \|S^{-1} - \tilde{S}^{-1}\| \cdot |x| < \eta.$$

Hence, we see that $\tilde{S}(S^{-1}x) \in \tilde{\mathcal{B}}$, so $S^{-1}x \in \tilde{S}^{-1}(\tilde{\mathcal{B}})$ and this completes the proof. □

Proposition 6.4.5 reduces the problem of finding an adequate approximation of S to finding upper bounds for $\|S\|_{\sup}$ and $\|S^{-1}\|_{\sup}$. The former can be easily done using any approximation of S. One way of finding an upper bound for $\|S^{-1}\|_{\text{sup}}$ is to use the fact that $S^{-1} = \frac{1}{\det(S)} \cdot A$, where A is the adjugate matrix of S. By approximating S one can obtain a lower bound for $\det(S)$ and an upper bound for the entries of A.

6.4.3 Revised algorithm

Using the methods described above we give a new version of Algorithm 6.3.10 which takes precision issues into account. We assume here that $r > 0$; the case $r = 0$ is treated in §6.4.4 for imaginary quadratic fields, and is trivial when $K = \mathbb{Q}$.

Algorithm 6.4.6 (Algebraic numbers of bounded height).
Input: A number field K, a bound $B \geq 1$, and a tolerance $\theta \in (0, 1]$, with $B, \theta \in \mathbb{Q}$.
Output: Two lists, L and L', such that:

- If $x \in K$ satisfies $H_K(x) \leq B$, then x is in either L or L'.

- For every $x \in L$, $H_K(x) < B$.

- For every $x \in L'$, $|H_K(x) - B| < \theta$.

1. Set $t = \theta/(3B)$ and let $\delta_1 = t/(6r + 12)$. Find a complete set $\mathfrak{a}_1, \ldots, \mathfrak{a}_h$ of ideal class representatives, and for each index ℓ compute a rational δ_1-approximation of $\log(N(\mathfrak{a}_\ell))$.

2. Let $N = \max_\ell N(\mathfrak{a}_\ell)$ and make a list $\mathcal{P}$ of all nonzero principal ideals of $\mathcal{O}_K$ — each represented by a single generator g — having norm at most $B \cdot N$. For each g, find a δ_1-approximation of $\Lambda(g)$.

3. For each ideal $\mathfrak{a}_\ell$, make a list $(g_{\ell,1}), \ldots, (g_{\ell,s_\ell})$ of all elements of $\mathcal{P}$ contained in $\mathfrak{a}_\ell$ whose norms are at most $B \cdot N(\mathfrak{a}_\ell)$.

4. For each index ℓ:

   (a) Make a list R_ℓ of pairs (i, j) such that $1 \leq i < j \leq s_\ell$ and $(g_{\ell,i}, g_{\ell,j}) = \mathfrak{a}_\ell$.

   (b) For each pair (i, j) in R_ℓ:

   Use Lemma 6.4.1 and data from steps (1) and (2) to find a rational approximation of $h_K(g_{\ell,i}/g_{\ell,j})$.

   The result will be a rational number $r_{\ell,i,j}$ such that $|r_{\ell,i,j} - h_K(g_{\ell,i}/g_{\ell,j})| < t/6$.

5. Find a rational number b such that $\frac{t}{12} < b - \log(B) < \frac{t}{4}$ and set $\tilde{d} = b + \frac{t}{6} + \max_\ell \max_{(i,j)\in R_\ell} r_{\ell,i,j}$.

6. Compute a system of fundamental units $\boldsymbol{\varepsilon} = \{\varepsilon_1, \ldots, \varepsilon_r\}$ and find a constant m such that

$$m \geq r^2 \cdot \max\{\|S(\boldsymbol{\varepsilon})\|_{\sup}, \|S(\boldsymbol{\varepsilon})^{-1}\|_{\sup}\}.$$

7. Define constants

$$\tilde{\lambda} = \frac{t/12}{\tilde{d}r(1+m)},\ \tilde{\delta} = \min\left\{\frac{\tilde{\lambda}}{r^2(m^2+m\tilde{\lambda})}, \frac{1}{r^2}\right\},\ M = \lceil \tilde{d}(m+\tilde{\lambda}\sqrt{r})\rceil,\ \delta_2 = \min\left\{\tilde{\delta}, \frac{t/6}{r(r+1)M}\right\}.$$

8. Compute δ_2-approximations $v_1, \ldots, v_r$ of the vectors $\Lambda(\varepsilon_1), \ldots, \Lambda(\varepsilon_r)$, and construct the $r \times r$ matrix $\tilde{S}$ whose j-th column is the vector v_j with its last coordinate deleted.

9. Construct a list U consisting of all integer vectors $(n_1, \ldots, n_r)$ in the polytope $\tilde{S}^{-1}([-\tilde{d}, \tilde{d}]^r)$.

10. Create a list L containing only the element 0, and create empty lists U_0, U_0' and L_0, L_0'.

11. For each tuple $\boldsymbol{u} = (n_1, \ldots, n_r)$ in U:

    (a) Compute the vector $\tilde{\Lambda}_{\boldsymbol{u}} = \sum_{j=1}^r n_j v_j$.

    (b) Using $\tilde{\Lambda}_{\boldsymbol{u}}$ and Lemma 6.4.2, find a rational approximation of $h_K\left(\varepsilon_1^{n_1} \cdots \varepsilon_r^{n_r}\right)$. The result will be a rational number $r_{\boldsymbol{u}}$ such that $\left|r_{\boldsymbol{u}} - h_K\left(\varepsilon_1^{n_1} \cdots \varepsilon_r^{n_r}\right)\right| < t/6$.

```
    (c) If $r_{\boldsymbol{u}} + \frac{5}{12}t < b$, then append $\boldsymbol{u}$ to $U_0$.
    (d) If $b - \frac{5}{12}t \le r_{\boldsymbol{u}} < b + \frac{1}{12}t$, then append $\boldsymbol{u}$ to $U_0'$.
    (e) If $r_{\boldsymbol{u}} - t/12 > \tilde{d}$, then remove $\boldsymbol{u}$ from $U$.
12. For each index $\ell$ :
        For each pair $(i, j) \in R_\ell$ :
          For each tuple $\boldsymbol{u} = (n_1, \ldots, n_r)$ in $U$:
            If $r_{\boldsymbol{u}} < b + r_{\ell,i,j} + \frac{1}{4}t$, then:
              (a) Let $P$ be the packet $(\ell, (i, j), (n_1, \ldots, n_r))$.
              (b) Use the data from steps (1), (2), and (11a), together with (6.3), to find
                  a rational approximation of $h_K(c(P))$. The result will be a rational
                  number $r_P$ with $|r_P - h_K(c(P))| < t/3$.
              (c) If $r_P + \frac{7}{12}t \le b$, then append the packet $P$ to $L_0$.
              (d) If $b - \frac{7}{12}t < r_P < b + \frac{1}{4}t$, then append the packet $P$ to $L_0'$.
13. For each tuple $(n_1, \ldots, n_r)$ in $U_0$, append to $L$ all numbers of the form $\zeta\varepsilon_1^{n_1} \cdots \varepsilon_r^{n_r}$ with
    $\zeta \in \mu_K$, and similarly for $U_0'$ and $L'$.
14. For each packet $P$ in $L_0$, append to $L$ all numbers of the form $\zeta \cdot c(P)$ and $\zeta/c(P)$ with
    $\zeta \in \mu_K$, and similarly for $L_0'$ and $L'$.
15. Return the lists $L$ and $L'$.
```

We make the following comments regarding various steps of Algorithm 6.4.6:

- Let $S = S(\boldsymbol{\varepsilon})$. With d as in step (5) of Algorithm 6.3.10 we have $\tilde{d} > d + t/12$. Therefore, if we set $\eta = t/12$ and let λ and δ be defined as in Proposition 6.4.5, then

$\tilde{\lambda} < \lambda$ and $\tilde{\delta} \leq \delta$. By construction, $\|\tilde{S} - S\|_{\sup} < \tilde{\delta} \leq \delta$, so that by Proposition 6.4.5 we have

$$S^{-1}([-d, d]^r) \subseteq \tilde{S}^{-1}([-d - \eta, d + \eta]^r) \subseteq \tilde{S}^{-1}([-\tilde{d}, \tilde{d}]^r).$$

- In order to use Lemma 6.4.2 in step 11(b) we must know that $|n_i| \leq M$ for all $1 \leq i \leq r$. Since $\boldsymbol{u} \in \tilde{S}^{-1}([-\tilde{d}, \tilde{d}]^r)$, we clearly have the upper bound $|n_i| \leq \tilde{d}\sqrt{r}\|\tilde{S}^{-1}\|$. By Corollary 6.4.4, $\|\tilde{S}^{-1} - S^{-1}\| < \tilde{\lambda}$, so applying (6.4) we have $\|\tilde{S}^{-1}\| \leq r\sqrt{r}\|S^{-1}\|_{\sup} + \tilde{\lambda}$. It follows that $|n_i| \leq \tilde{d}(m + \tilde{\lambda}\sqrt{r}) \leq M$.

- The condition $r_{\boldsymbol{u}} + \frac{5}{12}t < b$ from step (11)c implies that $h_{\boldsymbol{u}} < \log B$; the condition $b - \frac{5}{12}t \leq r_{\boldsymbol{u}} < b + \frac{1}{12}t$ from step (11)d implies $|h_{\boldsymbol{u}} - \log B| < t$. Moreover, every $\boldsymbol{u} = (n_1, \ldots, n_r)$ for which $h_K(\varepsilon_1^{n_1} \cdots \varepsilon_r^{n_r}) \leq \log B$ is in U_0 or U_0', since $h_{\boldsymbol{u}} \leq \log B$ implies $r_{\boldsymbol{u}} < b + \frac{1}{12}t$.

- The condition $r_{\boldsymbol{u}} - t/12 > \tilde{d}$ from step (11)e implies that $h_{\boldsymbol{u}} > d$.

- The condition $r_P + \frac{7}{12}t \leq b$ from step (12)c implies that $h_K(c(P)) < \log B$; the condition $b - \frac{7}{12}t < r_P < b + \frac{1}{4}t$ from step (12)d implies that $|h_K(c(P)) - \log B| < t$. Moreover, every packet P with $h(c(P)) \leq \log B$ is in either L_0 or L_0', since $h_K(c(P)) \leq \log B$ implies that $r_P < b + \frac{t}{4}$.

- Elements $x \in L$ satisfy $H_K(x) < B$, since they come from tuples in U_0 and packets in L_0. Elements $x \in L'$ satisfy $|h_K(x) - \log B| < t$, which implies that $|H_K(x) - B| < \theta$ by the Mean Value Theorem.

Note that the list L' of Algorithm 6.4.6 consists of elements $x \in K$ whose heights are so close to B that it is not possible to decide whether $H_K(x) \leq B$ with the tolerance specified as input. In particular, L' might contain elements of height exactly B. For general number fields K we cannot prevent this from occurring; however, for quadratic fields we can prevent it, as explained below.

6.4.4 Case of quadratic fields

We give here a way to shorten the list L' from Algorithm 6.4.6 in the case of real quadratic fields, and to eliminate it altogether in the case of imaginary quadratic fields.

Proposition 6.4.7. *Let K be a quadratic field and let $x \in K^*$. Let σ be the generator of* $\mathrm{Gal}(K/\mathbb{Q})$.

1. *If K is an imaginary field, then $H_K(x)$ is an integer.*
2. *If K is a real field, then $H_K(x) \in \mathbb{Q}$ if and only if $\max\{|x|, |\sigma(x)|\} \leq 1$ or $\min\{|x|, |\sigma(x)|\} \geq 1$. Moreover, if $H_K(x) \in \mathbb{Q}$, then $H_K(x) \in \mathbb{Z}$.*

Proof. Write $x = a/b$ with $a, b \in \mathcal{O}_K$, and let $\mathfrak{a} = (a, b)$ be the ideal generated by a and b in $\mathcal{O}_K$. Then $H_K(x) = N(\mathfrak{a})^{-1} \prod_{v \in M_K^\infty} \max\{|a|_v^{n_v}, |b|_v^{n_v}\}$. There are coprime ideals I and J of $\mathcal{O}_K$ such that $(a) = \mathfrak{a} \cdot I$ and $(b) = \mathfrak{a} \cdot J$. We then have $H_K(x) = N(J) \prod_{v \in M_K^\infty} \max\{|x|_v^{n_v}, 1\}$.

1. If K is an imaginary field, then

$$H_K(x) = N(\mathfrak{a})^{-1} \max\{N_{K/\mathbb{Q}}(a), N_{K/\mathbb{Q}}(b)\} = \max\{N(I), N(J)\} \in \mathbb{Z}.$$

2. If K is a real field, then $H_K(x) = N(J) \max\{|x|, 1\} \cdot \max\{|\sigma(x)|, 1\}$. If $\max\{|x|, |\sigma(x)|\} \leq 1$, then $H_K(x) = N(J) \in \mathbb{Z}$. If $\min\{|x|, |\sigma(x)|\} \geq 1$, then

$$H_K(x) = N(J)|N_{K/\mathbb{Q}}(x)| = N(J)N(a)/N(b) = N(I) \in \mathbb{Z}.$$

Now suppose that $\max\{|x|, |\sigma(x)|\} > 1$ and $\min\{|x|, |\sigma(x)|\} < 1$. Then, without loss of generality we may assume that $|x| < 1 < |\sigma(x)|$. It follows that $x \notin \mathbb{Q}$, so $H_K(x) = N(J)|\sigma(x)| \notin \mathbb{Q}$.

□

In the case of real quadratic fields it is possible to detect some elements of the list L' from Algorithm 6.4.6 which should be in the list L: if $x \in L'$ has height $H_K(x) \in \mathbb{Q}$ — a condition which can be determined using Proposition 6.4.7 — then by construction of L' it must be the case that $H_K(x)$ is the unique integer closest to B (assuming the tolerance θ from Algorithm 6.4.6 was chosen to be less than 1/2). If the nearest integer is $\lfloor B \rfloor$, then x can then be deleted from L' and appended to L. Otherwise, x can be deleted from L'. At the end of this process the list L' will only contain elements of K whose heights are irrational and very close to B.

For imaginary quadratic fields K there is a modification of Algorithm 6.3.10 that allows us to determine elements of bounded height without doing any height computations. Thus, for such fields we avoid the need for a list L' as in Algorithm 6.4.6.

With the notation and terminology of §6.3.1 we have:

Theorem 6.4.8. *Let K be an imaginary quadratic field. Then*

$$\{\gamma \in K^* : H_K(\gamma) \leq B\} = \mu_K \cup \bigcup_{B\text{-packets } P} F(P).$$

Proof. One containment follows from Theorem 6.3.1. It is therefore enough to show that $H_K(c(P)) \leq B$ for every packet P. Letting $P = (\ell, (i,j))$ we have

$$N(\mathfrak{a}_\ell)H_K(c(P)) = \prod_{v \in M_K^\infty} \max\{|g_{\ell,i}|_v^{n_v}, |g_{\ell,j}|_v^{n_v}\} = \max\{N_{K/\mathbb{Q}}(g_{\ell,i}), N_{K/\mathbb{Q}}(g_{\ell,j})\} \leq B \cdot N(\mathfrak{a}_\ell).$$

Hence, $H_K(c(P)) \leq B$. □

Theorem 6.4.8 leads to the following algorithm.

Algorithm 6.4.9 (Numbers of bounded height in an imaginary quadratic field)**.**

Input: An imaginary quadratic field K and a bound $B \geq 1$.

Output: A list of all elements $x \in K$ satisfying $H_K(x) \leq B$.

1. Create a list L containing 0 and all elements of μ_K.

2. Find a complete set $\mathfrak{a}_1, \ldots, \mathfrak{a}_h$ of ideal class representatives.

3. Let $N = \max_\ell N(\mathfrak{a}_\ell)$ and make a list $\mathcal{P}$ of all nonzero principal ideals of $\mathcal{O}_K$ — each represented by a single generator g — having norm at most $B \cdot N$.

4. For each ideal $\mathfrak{a}_\ell$, make a list $(g_{\ell,1}), \ldots, (g_{\ell,s_\ell})$ of all elements of $\mathcal{P}$ contained in $\mathfrak{a}_\ell$ whose norms are at most $B \cdot N(\mathfrak{a}_\ell)$.

5. For each index ℓ:
   - For each pair of indices (i, j) such that $1 \leq i < j \leq s_\ell$ and $(g_{\ell,i}, g_{\ell,j}) = \mathfrak{a}_\ell$:
     - Let $c = g_{\ell,i}/g_{\ell,j}$ and append to L all elements of the form $\zeta \cdot c$ and ζ/c with $\zeta \in \mu_K$.

6. Return the list L.

By Theorem 6.3.1, the list L will not contain duplicate elements.

6.5 Efficiency of the algorithm

We discuss in this section a measure of the efficiency of Algorithm 6.3.10 — henceforth abbreviated A3 — and of the algorithm of Pethő and Schmitt — abbreviated PS — proposed in [56]. Given a number field K and a height bound B, both methods begin by computing some basic data attached to K: an integral basis for $\mathcal{O}_K$ in the case of PS; the ideal class group and a set of fundamental units in the case of A3. After this step, both methods construct a set of elements of K which is known to contain the desired set of numbers of bounded height; this larger set will be called the *search space* of the method and denoted by $\mathcal{S}_{\mathrm{PS}}(B)$ or $\mathcal{S}_{\mathrm{A3}}(B)$. Once a search space is known, the two methods proceed to compute the height of each element in this set and check whether it is smaller than B. We will measure the efficiency of a method by comparing the size of the search space to the size of the set of elements of height $\leq B$. Thus, we define the *search ratio* of PS to be the number

$$\sigma_{\mathrm{PS}}(B) := \frac{\#\mathcal{S}_{\mathrm{PS}}(B)}{\#\{P \in K : H_K(P) \leq B\}} \,,$$

and similarly for A3.

Recall the result on which PS is based:

Theorem 6.5.1 (Pethő, Schmitt)**.** *Let K be a number field of degree n over $\mathbb{Q}$. Let $B \in \mathbb{R}, B \geq 1$. Denote by r_2 the number of complex places of K. Let $\omega_1, \ldots, \omega_n$ be an LLL-reduced integral basis for $\mathcal{O}_K$. Then every element $x \in K$ with $H_K(x) \leq B$ can be written in the form*

$$x = \frac{a_1\omega_1 + \cdots + a_n\omega_n}{c} \,,$$

where $a_1, \ldots, a_n, c$ are integers satisfying

$$1 \leq c \leq B \quad \text{and} \quad |a_i| \leq 2^{n(n+1)/4 - r_2} Bc \,.$$

Proof. See the proof of Theorem 2 in [56]. □

This leads to the following algorithm:

Algorithm 6.5.2 (PS)**.**

Input: A number field K and a bound $B \geq 1$.

Output: A list of all elements $x \in K$ satisfying $H_K(x) \leq B$.

1. Compute an LLL-reduced integral basis $\omega_1, \ldots, \omega_n$ for $\mathcal{O}_K$.

2. Create an empty list L.

3. For $c = 1$ to $\lfloor B \rfloor$:

```
    (a) Let $D = \lfloor 2^{n(n+1)/4 - r_2} Bc \rfloor$ .
    (b) For every integer tuple $(a_1, \ldots, a_n) \in [-D, D]^n$ :
        i. Let $x = \dfrac{a_1\omega_1 + \cdots + a_n\omega_n}{c}$ .
        ii. If $H_K(x) \leq B$, then append $x$ to $L$.
4. Return the list $L$.
```

We now give our main result comparing the efficiency of PS with that of A3.

Theorem 6.5.3. *Let K be a number field of degree n. The search ratios of* PS *and* A3 *satisfy*

$$\sigma_{\mathrm{PS}}(B) \gg B^{2n-2} \quad \text{and} \quad \sigma_{\mathrm{A3}}(B) \ll (\log B)^r,$$

where r is the rank of the unit group $\mathcal{O}_K^\times$.

Proof. By Schanuel's formula [64] we know that there is a constant C_K such that

$$\#\{P \in K : H_K(P) \leq B\} \sim C_K B^2.$$

A simple calculation shows that the size of the search space in PS satisfies $\#\mathcal{S}_{\mathrm{PS}}(B) > B^{2n} 2^{n^2(n-1)/4+n}$; the first statement in the theorem then follows easily. Now let $\boldsymbol{\mathfrak{a}} = \{\mathfrak{a}_1, \ldots, \mathfrak{a}_h\}$ be a complete set of ideal class representatives for $\mathcal{O}_K$ and $\boldsymbol{\varepsilon} = \{\varepsilon_1, \ldots, \varepsilon_r\}$ a system of fundamental units. For each index ℓ let $g_{\ell,1}, \ldots, g_{\ell,s_\ell}$ be generators for all nonzero principal ideals contained in $\mathfrak{a}_\ell$ whose norms are at most $B \cdot N(\mathfrak{a}_\ell)$. By [4, p. 123] we may assume that

$$|g_{\ell,i}|_v^{n_v} \leq E_K(B \cdot N(\mathfrak{a}_\ell))^{1/(r+1)} \tag{6.5}$$

for every place $v \in M_K^\infty$ and all indices ℓ, i. Here E_K is a constant which depends on $\boldsymbol{\varepsilon}$ but not on B.

Let $P(B) = \sum_{\ell=1}^{h} s_\ell$. Using the bound given in [50, Thm. 1] we find that $P(B) \ll B$. Using Theorem 6.3.1 we see that the size of the search space considered in A3 satisfies

$$\#\mathcal{S}_{\mathrm{A3}}(B) \leq 1 + \#\{u \in \mathcal{O}_K^\times : H_K(u) \leq D\} \cdot \left(1 + 2 \cdot P(B)^2\right) \ll B^2 \cdot \#\{u \in \mathcal{O}_K^\times : H_K(u) \leq D\}, \tag{6.6}$$

where D is any number such that $D \geq B \cdot \max_{\ell,i,j} H_K(g_{\ell,i}/g_{\ell,j})$. By (6.5) we have

$$H_K(g_{\ell,i}/g_{\ell,j}) \leq \frac{\prod_{v \in M_K^\infty} \max\{|g_{\ell,i}|_v^{n_v}, |g_{\ell,j}|_v^{n_v}\}}{N(\mathfrak{a}_\ell)} \leq \frac{\prod_{v \in M_K^\infty} E_K(B \cdot N(\mathfrak{a}_\ell))^{1/(r+1)}}{N(\mathfrak{a}_\ell)} = F_K B$$

for all ℓ, i, j and for some constant F_K independent of B. Hence, we may take $D = F_K B^2$. By Corollary 6.3.9,

$$\#\{u \in \mathcal{O}_K^\times : H_K(u) \leq D\} \ll (\log B)^r.$$

Therefore, by (6.6), the size of the search space in A3 satisfies $\#\mathcal{S}_{\mathrm{A3}}(B) \ll B^2(\log B)^r$. The second statement in the theorem follows from this inequality and Schanuel's asymptotic estimate. □

Theorem 6.5.3 shows that, for a fixed field K, the method A3 is asymptotically (as $B \longrightarrow \infty$) much more efficient than PS. However, the search ratio is not the only factor determining total computation time: the initial step of computing basic data for K can be very time-consuming. If K is a field for which the cost of this initial step is high, then PS may perform better than A3. An example of this phenomenon may be seen in the next section.

6.6 Performance of the algorithm

Having done a theoretical analysis of the methods PS and A3 in the previous section, we show in this section how the methods perform in practice. Both algorithms have been implemented in Sage [68]. All computations below have been done on a Mac Pro with a Quad-Core 2.26 GHz processor and 8 GB of memory. In all examples, the embeddings of the number field K are computed using 100 bits of precision. When K is imaginary quadratic, Algorithm 6.4.9 (henceforth abbreviated A5) is used instead of A3.

The computations presented in this section are intended to make a comparison of the performances of A3, A5, and PS in practice. We will first determine the range within which PS can operate (in terms of number field degrees and height bounds); next, we compare A3 and A5 with PS within this range. Finally, we show that A3 and A5 can run efficiently on many examples that are well beyond the range of applicability of PS. In order to be able to give a substantial amount of examples, we will only consider number fields K and height bounds B for which the computation of the set $\{x \in K : H_K(x) \leq B\}$ requires at most 10 hours using A3, A5 or PS.

6.6.1 Limits of PS

Table 6.1 below lists the time required for computing the set $\{x \in K : H_K(x) \leq B\}$ for three number fields K and bounds B using PS. The field is specified by its defining polynomial in the variable t. In each case the field was chosen so that, among all number fields of equal degree, it has minimal absolute discriminant and maximal number of complex embeddings (such data may be found in Jones's number field database [30]). This choice minimizes the amount of time spent on steps 1 and 3 of PS, therefore minimizing total computation time. Thus, for any bound B and for number fields of fixed degree, the fields given in the table represent a best-case scenario for PS. However, even with the small values of B chosen here, the computation times exceed our set limit of 10 hours.

In view of these times, we will not carry out any computations using PS over fields of degree larger than 3. Moreover, for quadratic fields we will only consider height bounds

Number field K	Height bound B	PS time
$t^4 - t^3 - t^2 + t + 1$	2	33.64 hours
$t^3 - t^2 + 1$	5	20.84 hours
$t^2 - t + 1$	25	16.27 hours

Table 6.1: Sample computations with PS

$B \leq 20$, and for cubic fields only bounds $B \leq 4$.

6.6.2 Comparing A3 and A5 with PS

The four tables below contain the results of computations done using both PS and A3/A5 over quadratic and cubic fields, and are meant to give representative examples of the efficiency of the methods. Number fields are chosen to have nontrivial class group so that computing time for A3/A5 will not be optimal. In the tables, a number field K is specified by giving a defining polynomial for it in the variable t. The class number of K is given, then the height bound used for the particular computation, and then the computing times and search ratios of the two methods. Note that, by Theorem 6.4.8, the search ratio of A5 is always 1.

Field K	$\#\mathrm{Cl}(K)$	Bound B	PS time	A5 time	$\sigma_{\mathrm{PS}}(B)$	$\sigma_{\mathrm{A5}}(B)$
$t^2 + 61$	6	20	5.41 hours	0.38 seconds	96,233	1
$t^2 + 9026$	160	20	5.39 hours	4.50 seconds	330,540	1
$t^2 + 49661$	424	20	4.83 hours	25.24 seconds	330,540	1
$t^2 + 312311$	1001	20	4.88 hours	50.30 seconds	330,540	1

Table 6.2: PS and A5 over imaginary quadratic fields

As mentioned in §6.5, PS may be faster than A3 if the discriminant of K is very large and B is very small. For example, the computation of all elements of height ≤ 5 in the quadratic field $K = \mathbb{Q}(\sqrt{359612476105})$ with class number 53,936 took 2.47 minutes using

Field K	#Cl(K)	Bound B	PS time	A3 time	$\sigma_{\mathrm{PS}}(B)$	$\sigma_{\mathrm{A3}}(B)$
$t^2 - 36865$	52	15	9.95 hours	3 seconds	495,268	3.13
$t^2 - 254017$	124	15	9.95 hours	13 seconds	495,268	1.0
$t^2 - 627265$	206	15	9.28 hours	29 seconds	495,268	1.0
$t^2 - 705601$	254	15	10.25 hours	34 seconds	495,268	1.0

Table 6.3: PS and A3 over real quadratic fields

Field K	#Cl(K)	Bound B	PS time	A3 time	$\sigma_{\mathrm{PS}}(B)$	$\sigma_{\mathrm{A3}}(B)$
$t^3 - t^2 + 21t - 1$	13	4	4.26 hours	0.48 seconds	10^6	1.0
$t^3 - t^2 + 45t - 93$	53	4	4.95 hours	16.63 seconds	10^6	1.0
$t^3 - 141t - 1004$	87	4	4.54 hours	1.89 minutes	3×10^6	1.0
$t^3 - t^2 + 194t - 944$	123	4	4.56 hours	1.95 minutes	3×10^6	1.0

Table 6.4: PS and A3 over cubic fields with one real embedding

Field K	#Cl(K)	Bound B	PS time	A3 time	$\sigma_{\mathrm{PS}}(B)$	$\sigma_{\mathrm{A3}}(B)$
$t^3 - t^2 - 17t - 16$	4	2.7	2 hours	0.1 seconds	219,501	1.0
$t^3 - t^2 - 25t + 24$	8	2.7	2 hours	0.49 seconds	219,501	1.0
$t^3 - t^2 - 55t - 77$	13	2.7	2 hours	12 seconds	219,501	1.0
$t^3 - t^2 - 49t + 48$	16	2.7	1.88 hours	1.66 seconds	219,501	1.0

Table 6.5: PS and A3 over totally real cubic fields

PS, but using A3 the computation did not terminate within 10 hours. This difference is due to the expense of computing ideal class representatives.

6.6.3 Performance of A3 and A5

We end by giving a series of examples showing how A3 and A5 perform over number fields of various degrees and with several different height bounds.

Bound B	A5 time	$\sigma_{\text{A5}}(B)$	Elements found
200	0.84 seconds	1	15,275
1,000	19.06 seconds	1	393,775
3,000	2.78 minutes	1	3,523,651
7,000	15.25 minutes	1	19,124,179

Table 6.6: Computing times for A5 over the field $K = \mathbb{Q}(\sqrt{-107})$

Bound B	A3 time	$\sigma_{\text{A3}}(B)$	Elements found
200	8.45 seconds	11.98	14,331
1,000	2.02 minutes	14.94	366,395
3,000	17 minutes	18.28	3,315,767
5,000	49 minutes	19.86	9,161,731

Table 6.7: Computing times for A3 over the field $K = \mathbb{Q}(\sqrt{91})$

Bound B	A3 time	$\sigma_{\text{A3}}(B)$	Elements found
200	37 seconds	121.89	6,819
1,000	7.09 minutes	197.66	166,751
2,000	26 minutes	234.11	667,651
4,000	1.75 hours	270.43	2,671,227

Table 6.8: Computing times for A3 over the field $K : t^3 - 43t - 66$

Bound B	A3 time	$\sigma_{\text{A3}}(B)$	Elements found
200	12 seconds	68.08	75,027
500	1.44 minutes	125.76	528,459
1,000	6 minutes	149.93	2,073,303
3,000	1 hour	186.94	18,261,363

Table 6.9: Computing times for A3 over the sextic cyclotomic field $K = \mathbb{Q}(\zeta_7)$

Appendix A

Graphs of preperiodic points

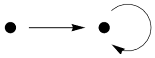
This appendix contains figures, in the first section, and data in the second, corresponding to sets of preperiodic points for quadratic polynomials over quadratic number fields.

A.1 Figures

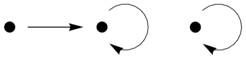
We give here a list of 46 graphs representing preperiodic structures for quadratic polynomials over quadratic number fields, discovered via the methods described in §4.5. The label of each graph is in the form $N(\ell_1, \ell_2, \ldots)$, where N denotes the number of vertices in the graph, and $\ell_1, \ell_2, \ldots$ are the lengths of the directed cycles in the graph in nonincreasing order. If more than one isomorphism class of graphs with this data was observed, we add a lowercase roman letter to distinguish them. For example, the labels 5(1,1)a and 5(1,1)b correspond to the two isomorphism classes of graphs observed that have five vertices and two fixed points. In all figures below we omit the connected component corresponding to the point at infinity.

0

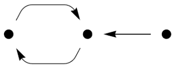
2(1)



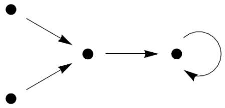
3(1,1)



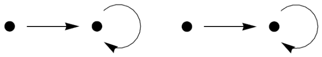
3(2)



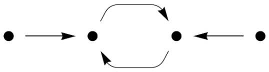
4(1)



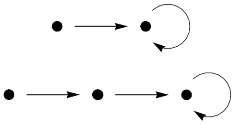
4(1,1)



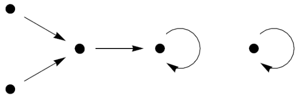
4(2)



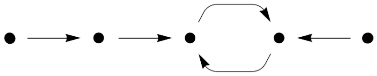
5(1,1)a



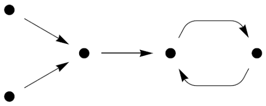
5(1,1)b



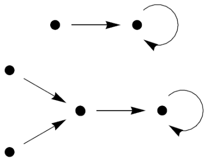
5(2)a



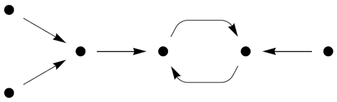
5(2)b



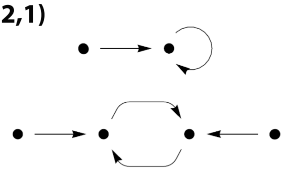
6(1,1)



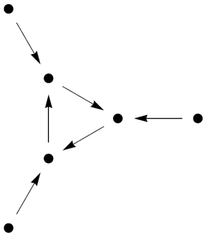
6(2)



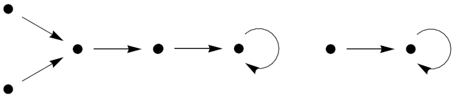
6(2,1)

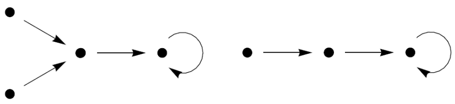
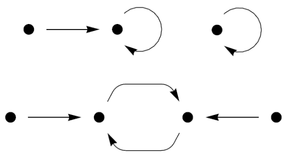
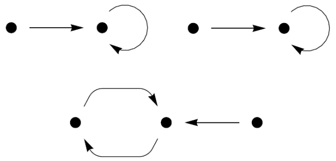
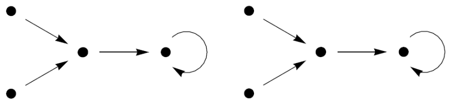
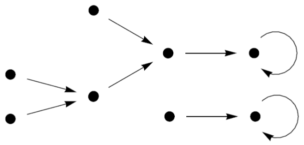
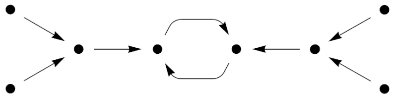
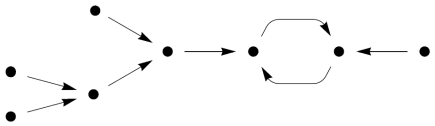
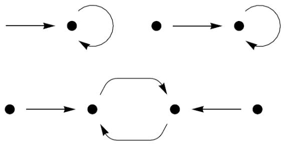
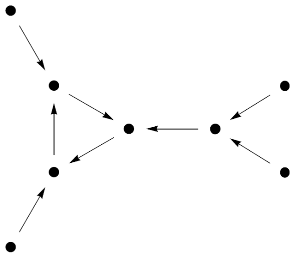
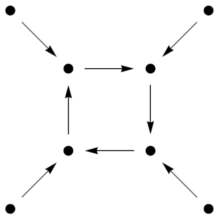
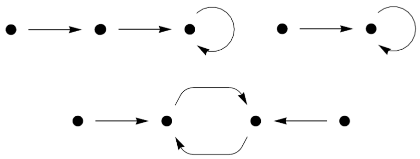
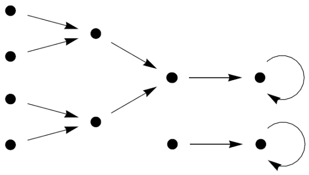


6(3)

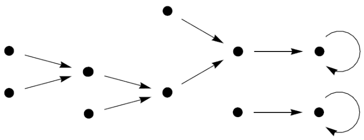


7(1,1)a

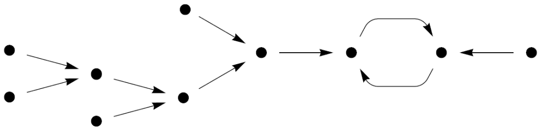


7(1,1)b 	**7(2,1,1)a** 
7(2,1,1)b 	**8(1,1)a** 
8(1,1)b 	**8(2)a** 
8(2)b 	**8(2,1,1)** 
8(3) 	**8(4)** 
9(2,1,1) 	**10(1,1)a** 

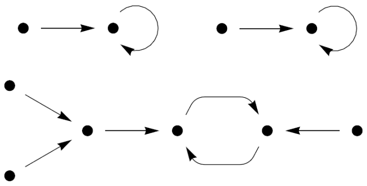
10(1,1)b



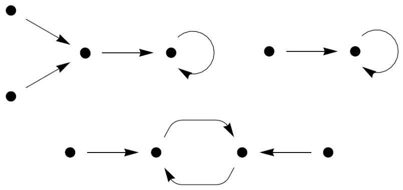
10(2)



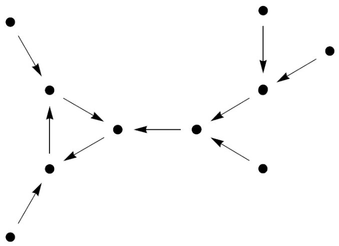
10(2,1,1)a



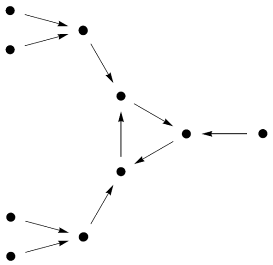
10(2,1,1)b



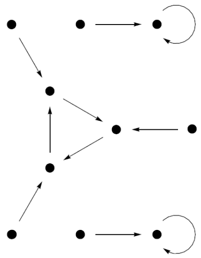
10(3)a



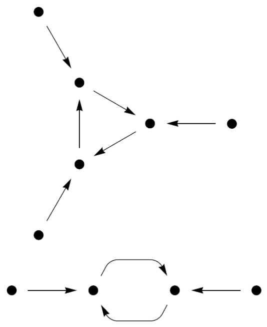
10(3)b



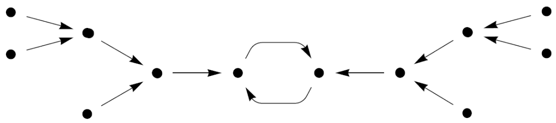
10(3,1,1)



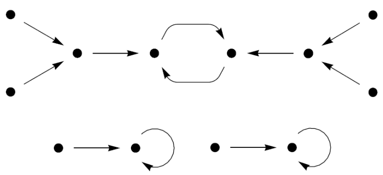
10(3,2)



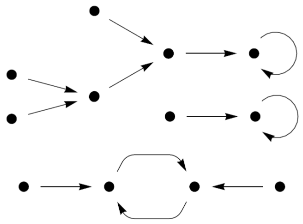
12(2)

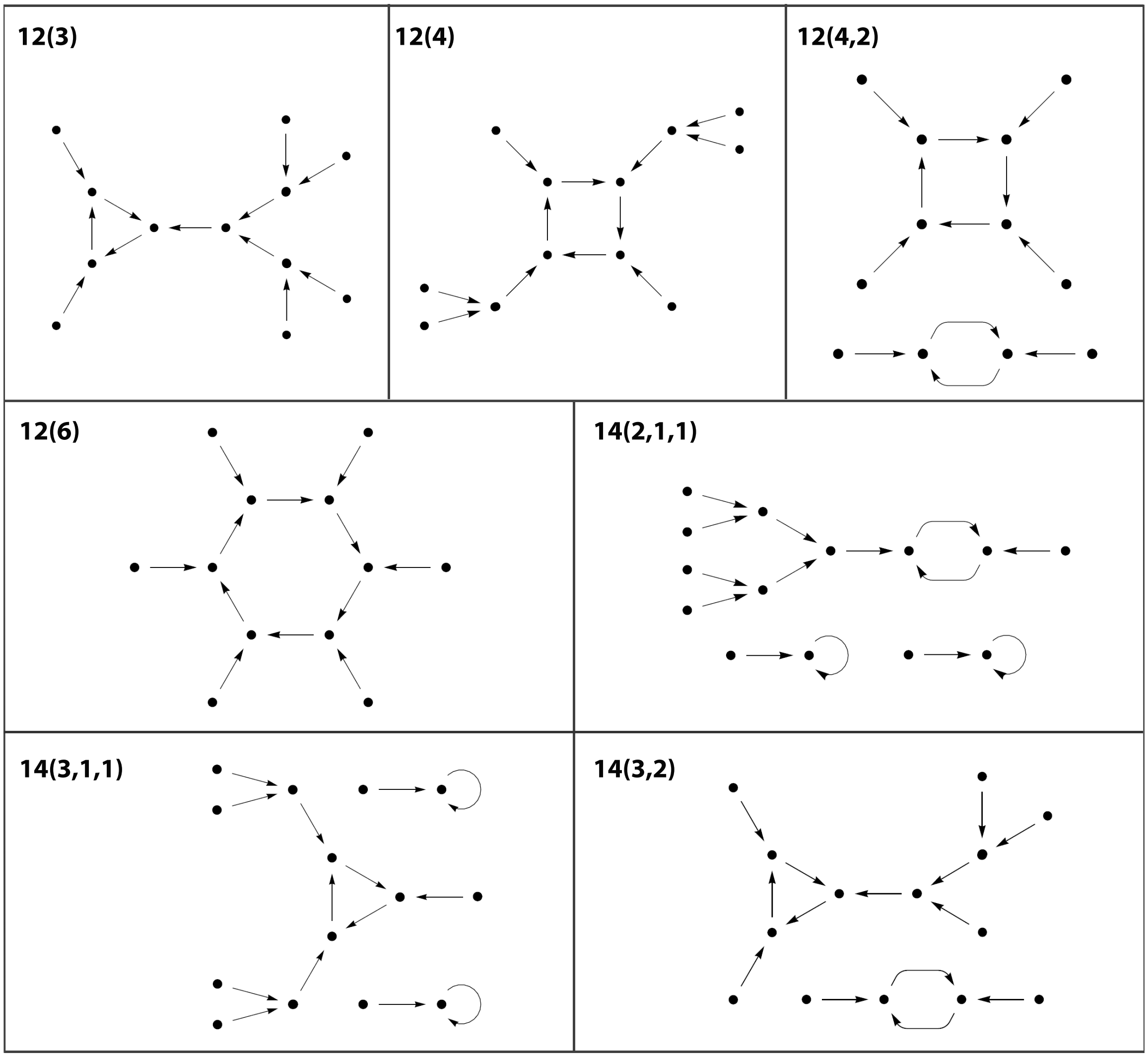


12(2,1,1)a



12(2,1,1)b




12(3)
12(4)
12(4,2)
12(6)
14(2,1,1)
14(3,1,1)
14(3,2)

A.2 Data

We now give, for each graph shown in the previous section, a representative example of a map f_c and a quadratic field K such that the set $\mathrm{PrePer}(f_c, K)$ has the given graph structure. The data below is presented in the form

$$K, p(t), c, \mathrm{PrePer}(f_c, K)'.$$

Here $K = \mathbb{Q}(\sqrt{D})$ is a quadratic field over which this preperiodic structure was observed; $p(t)$ is a defining polynomial for K with a root $g \in K$; c is an element of K such that the set $\mathrm{PrePer}(f_c, K)\backslash\{\infty\}$, when endowed with the structure of a directed graph, is isomorphic to the given graph; and $\mathrm{PrePer}(f_c, K)'$ is an abbreviated form of the full set of finite K-rational preperiodic points for f_c: since $x \in \mathrm{PrePer}(f_c, K)$ if and only if $-x \in \mathrm{PrePer}(f_c, K)$, we list only one of x and $-x$ in the set $\mathrm{PrePer}(f_c, K)'$. If a particular graph was observed over both real and imaginary quadratic fields, we give a representative set of data for each case.

0.

$\mathbb{Q}(\sqrt{5}),\ \ t^2 - t - 1,\ \ 1,\ \ \emptyset$

$\mathbb{Q}(\sqrt{-3}),\ \ t^2 - t + 1,\ \ 2,\ \ \emptyset$

2(1).

$\mathbb{Q}(\sqrt{5}),\ \ t^2 - t - 1,\ \ \frac{1}{4},\ \ \{\frac{1}{2}\}$

$\mathbb{Q}(\sqrt{-7}),\ \ t^2 - t + 2,\ \ \frac{1}{4},\ \ \{\frac{1}{2}\}$

3(1,1).

$\mathbb{Q}(\sqrt{5}),\ \ t^2-t-1,\ \ 0,\ \ \{0,1\}$

$\mathbb{Q}(\sqrt{-7}),\ \ t^2-t+2,\ \ 0,\ \ \{0,1\}$

3(2).

$\mathbb{Q}(\sqrt{3}),\ \ t^2-3,\ \ -1,\ \ \{0,1\}$

$\mathbb{Q}(\sqrt{-3}),\ \ t^2-t+1,\ \ -1,\ \ \{0,1\}$

4(1). $\mathbb{Q}(\sqrt{-3}),\ \ t^2-t+1,\ \ \frac{1}{4},\ \ \left\{\frac{1}{2}, g-\frac{1}{2}\right\}$

4(1,1).

$\mathbb{Q}(\sqrt{5}),\ \ t^2-t-1,\ \ \frac{1}{5},\ \ \left\{\frac{1}{5}g+\frac{2}{5}, \frac{1}{5}g-\frac{3}{5}\right\}$

$\mathbb{Q}(\sqrt{-3}),\ \ t^2-t+1,\ \ 1,\ \ \{g, g-1\}$

4(2).

$\mathbb{Q}(\sqrt{5}),\ \ t^2-t-1,\ \ -\frac{4}{5},\ \ \left\{\frac{1}{5}g+\frac{2}{5}, \frac{1}{5}g-\frac{3}{5}\right\}$

$\mathbb{Q}(\sqrt{-3}),\ \ t^2-t+1,\ \ -\frac{2}{3},\ \ \left\{\frac{1}{3}g-\frac{2}{3}, \frac{1}{3}g+\frac{1}{3}\right\}$

5(1,1)a.

$\mathbb{Q}(\sqrt{13}),\ \ t^2-t-3,\ \ -2,\ \ \{0,2,1\}$

$\mathbb{Q}(\sqrt{-3}),\ \ t^2-t+1,\ \ -2,\ \ \{0,2,1\}$

5(1,1)b. $\mathbb{Q}(\sqrt{-1})$, t^2+1, 0, $\{0,1,g\}$

5(2)a. $\mathbb{Q}(\sqrt{-1})$, t^2+1, g, $\{0,g,g-1\}$

5(2)b. $\mathbb{Q}(\sqrt{2})$, t^2-2, -1, $\{0,1,g\}$

6(1,1).

$\mathbb{Q}(\sqrt{5})$, t^2-t-1, $-\frac{3}{4}$, $\left\{\frac{1}{2},g-\frac{1}{2},\frac{3}{2}\right\}$

$\mathbb{Q}(\sqrt{-3})$, t^2-t+1, $-\frac{3}{4}$, $\left\{\frac{1}{2},\frac{3}{2},g-\frac{1}{2}\right\}$

6(2).

$\mathbb{Q}(\sqrt{5})$, t^2-t-1, -3, $\{1,2,2g-1\}$

$\mathbb{Q}(\sqrt{-3})$, t^2-t+1, $-\frac{13}{9}$, $\left\{\frac{1}{3},\frac{4}{3},\frac{5}{3}\right\}$

6(2,1). $\mathbb{Q}(\sqrt{-1})$, t^2+1, $\frac{1}{4}$, $\left\{\frac{1}{2},g-\frac{1}{2},g+\frac{1}{2}\right\}$

6(3).

$\mathbb{Q}(\sqrt{33})$, t^2-t-8, $-\frac{301}{144}$, $\left\{\frac{5}{12},\frac{19}{12},\frac{23}{12}\right\}$

$\mathbb{Q}(\sqrt{-67})$, t^2-t+17, $-\frac{301}{144}$, $\left\{\frac{5}{12},\frac{19}{12},\frac{23}{12}\right\}$

7(1,1)a. $\mathbb{Q}(\sqrt{2})$, t^2-2, -2, $\{0,1,2,g\}$

7(1,1)b. $\mathbb{Q}(\sqrt{3})$, t^2-3, -2, $\{0,1,2,g\}$

7(2,1,1)a. $\mathbb{Q}(\sqrt{-3})$, t^2-t+1, 0, $\{0,1,g,g-1\}$

7(2,1,1)b. $\mathbb{Q}(\sqrt{5})$, t^2-t-1, -1, $\{0,1,g,g-1\}$

8(1,1)a.

$\mathbb{Q}(\sqrt{13}),\ \ t^2-t-3,\ \ -\frac{289}{144},\ \ \left\{\frac{5}{6}g+\frac{1}{12},\frac{1}{2}g-\frac{13}{12},\frac{1}{2}g+\frac{7}{12},\frac{5}{6}g-\frac{11}{12}\right\}$

$\mathbb{Q}(\sqrt{-15}),\ \ t^2-t+4,\ \ -\frac{5}{16},\ \ \left\{\frac{1}{4},\frac{3}{4},\frac{5}{4},\frac{1}{2}g-\frac{1}{4}\right\}$

8(1,1)b.

$\mathbb{Q}(\sqrt{13}),\ \ t^2-t-3,\ \ -\frac{40}{9},\ \ \left\{\frac{4}{3},\frac{8}{3},\frac{5}{3},\frac{4}{3}g-\frac{2}{3}\right\}$

$\mathbb{Q}(\sqrt{-2}),\ \ t^2+2,\ \ -\frac{10}{9},\ \ \left\{\frac{2}{3},\frac{1}{3}g,\frac{4}{3},\frac{5}{3}\right\}$

8(2)a.

$\mathbb{Q}(\sqrt{10}),\ \ t^2-10,\ \ -\frac{13}{9},\ \ \left\{\frac{1}{3},\frac{1}{3}g,\frac{4}{3},\frac{5}{3}\right\}$

$\mathbb{Q}(\sqrt{-3}),\ \ t^2-t+1,\ \ -\frac{5}{12},\ \ \left\{\frac{2}{3}g-\frac{5}{6},\frac{2}{3}g+\frac{1}{6},\frac{1}{3}g+\frac{5}{6},\frac{1}{3}g-\frac{7}{6}\right\}$

8(2)b.

$\mathbb{Q}(\sqrt{13}),\ \ t^2-t-3,\ \ -\frac{37}{9},\ \ \left\{\frac{4}{3},\frac{5}{3},\frac{7}{3},\frac{4}{3}g-\frac{2}{3}\right\}$

$\mathbb{Q}(\sqrt{-7}),\ \ t^2-t+2,\ \ -\frac{13}{16},\ \ \left\{\frac{1}{4},\frac{3}{4},\frac{1}{2}g-\frac{1}{4},\frac{5}{4}\right\}$

8(2,1,1).

$\mathbb{Q}(\sqrt{5}),\ \ t^2-t-1,\ \ -12,\ \ \{3,3g-1,3g-2,4\}$

$\mathbb{Q}(\sqrt{-3}),\ \ t^2-t+1,\ \ \frac{7}{12},\ \ \left\{\frac{2}{3}g+\frac{1}{6},\frac{2}{3}g-\frac{5}{6},\frac{4}{3}g-\frac{7}{6},\frac{4}{3}g-\frac{1}{6}\right\}$

8(3).

$\mathbb{Q}(\sqrt{5}),\ \ t^2-t-1,\ \ -\frac{29}{16},\ \ \left\{\frac{1}{4},\frac{5}{4},\frac{3}{4},\frac{7}{4}\right\}$

$\mathbb{Q}(\sqrt{-3}),\ \ t^2-t+1,\ \ -\frac{29}{16},\ \ \left\{\frac{1}{4},\frac{5}{4},\frac{3}{4},\frac{7}{4}\right\}$

8(4).

$\mathbb{Q}(\sqrt{10})$, $t^2 - 10$, $-\frac{155}{72}$, $\left\{\frac{1}{4}g - \frac{1}{6}, \frac{1}{4}g + \frac{1}{6}, \frac{1}{12}g - \frac{3}{2}, \frac{1}{12}g + \frac{3}{2}\right\}$

$\mathbb{Q}(\sqrt{-455})$, $t^2 - t + 114$, $\frac{199}{720}$, $\left\{\frac{1}{10}g + \frac{17}{60}, \frac{1}{15}g - \frac{47}{60}, \frac{1}{10}g - \frac{23}{60}, \frac{1}{15}g + \frac{43}{60}\right\}$

9(2,1,1). $\mathbb{Q}(\sqrt{5})$, $t^2 - t - 1$, -2, $\{0, 1, 2, g, g - 1\}$

10(1,1)a. $\mathbb{Q}(\sqrt{-7})$, $t^2 - t + 2$, $\frac{3}{16}$, $\left\{\frac{1}{4}, \frac{1}{2}g + \frac{1}{4}, \frac{1}{2}g - \frac{1}{4}, \frac{1}{2}g - \frac{3}{4}, \frac{3}{4}\right\}$

10(1,1)b. $\mathbb{Q}(\sqrt{17})$, $t^2 - t - 4$, $-\frac{1}{2}g - \frac{13}{16}$, $\left\{\frac{1}{4}, \frac{1}{2}g + \frac{3}{4}, \frac{3}{4}, \frac{1}{2}g - \frac{1}{4}, \frac{1}{2}g + \frac{1}{4}\right\}$

10(2).

$\mathbb{Q}(\sqrt{73})$, $t^2 - t - 18$, $\frac{1}{9}g - \frac{205}{144}$, $\left\{\frac{1}{6}g + \frac{1}{12}, \frac{1}{6}g - \frac{11}{12}, \frac{1}{6}g + \frac{7}{12}, \frac{1}{3}g - \frac{7}{12}, \frac{1}{3}g - \frac{1}{12}\right\}$

$\mathbb{Q}(\sqrt{-7})$, $t^2 - t + 2$, $-\frac{1}{2}g - \frac{5}{16}$, $\left\{\frac{1}{4}, \frac{1}{2}g - \frac{1}{4}, \frac{1}{2}g + \frac{1}{4}, \frac{3}{4}, \frac{1}{2}g + \frac{3}{4}\right\}$

10(2,1,1)a.

$\mathbb{Q}(\sqrt{17})$, $t^2 - t - 4$, $-\frac{273}{64}$, $\left\{\frac{11}{8}, \frac{13}{8}, \frac{19}{8}, \frac{5}{4}g - \frac{5}{8}, \frac{21}{8}\right\}$

$\mathbb{Q}(\sqrt{-1})$, $t^2 + 1$, $\frac{3}{8}g - \frac{1}{4}$, $\left\{\frac{3}{4}g + \frac{1}{4}, \frac{3}{4}g - \frac{3}{4}, \frac{1}{4}g - \frac{1}{4}, \frac{1}{4}g + \frac{3}{4}, \frac{1}{4}g - \frac{5}{4}\right\}$

10(2,1,1)b.

$\mathbb{Q}(\sqrt{13})$, $t^2 - t - 3$, $-\frac{10}{9}$, $\left\{\frac{2}{3}, \frac{4}{3}, \frac{5}{3}, \frac{1}{3}g - \frac{2}{3}, \frac{1}{3}g + \frac{1}{3}\right\}$

$\mathbb{Q}(\sqrt{-7})$, $t^2 - t + 2$, $-\frac{21}{16}$, $\left\{\frac{1}{4}, \frac{7}{4}, \frac{1}{2}g - \frac{1}{4}, \frac{3}{4}, \frac{5}{4}\right\}$

10(3)a. $\mathbb{Q}(\sqrt{41})$, $t^2 - t - 10$, $-\frac{29}{16}$, $\left\{\frac{1}{4}, \frac{5}{4}, \frac{3}{4}, \frac{1}{2}g - \frac{1}{4}, \frac{7}{4}\right\}$

10(3)b. $\mathbb{Q}(\sqrt{57})$, $t^2 - t - 14$, $-\frac{29}{16}$, $\left\{\frac{1}{4}, \frac{3}{4}, \frac{5}{4}, \frac{7}{4}, \frac{1}{2}g - \frac{1}{4}\right\}$

10(3,1,1) $\mathbb{Q}(\sqrt{337})$, t^2-t-84, $-\frac{301}{144}$, $\left\{\frac{5}{12}, \frac{19}{12}, \frac{23}{12}, \frac{1}{6}g+\frac{5}{12}, \frac{1}{6}g-\frac{7}{12}\right\}$

10(3,2). $\mathbb{Q}(\sqrt{193})$, t^2-t-48, $-\frac{301}{144}$, $\left\{\frac{5}{12}, \frac{19}{12}, \frac{23}{12}, \frac{1}{6}g+\frac{5}{12}, \frac{1}{6}g-\frac{7}{12}\right\}$

12(2). $\mathbb{Q}(\sqrt{2})$, t^2-2, $-\frac{15}{8}$, $\left\{\frac{3}{4}g+\frac{1}{2}, \frac{3}{4}g-\frac{1}{2}, \frac{1}{4}g+\frac{1}{2}, \frac{1}{4}g-\frac{3}{2}, \frac{1}{4}g-\frac{1}{2}, \frac{1}{4}g+\frac{3}{2}\right\}$

12(2,1,1)a. $\mathbb{Q}(\sqrt{17})$, t^2-t-4, $-\frac{13}{16}$, $\left\{\frac{1}{4}, \frac{3}{4}, \frac{5}{4}, \frac{1}{2}g+\frac{1}{4}, \frac{1}{2}g-\frac{3}{4}, \frac{1}{2}g-\frac{1}{4}\right\}$

12(2,1,1)b.

$\mathbb{Q}(\sqrt{33})$, t^2-t-8, $-\frac{45}{16}$, $\left\{\frac{3}{4}, \frac{9}{4}, \frac{5}{4}, \frac{1}{2}g-\frac{3}{4}, \frac{1}{2}g+\frac{1}{4}, \frac{1}{2}g-\frac{1}{4}\right\}$

$\mathbb{Q}(\sqrt{-7})$, t^2-t+2, $-\frac{5}{16}$, $\left\{\frac{1}{4}, \frac{3}{4}, \frac{5}{4}, \frac{1}{2}g+\frac{1}{4}, \frac{1}{2}g-\frac{3}{4}, \frac{1}{2}g-\frac{1}{4}\right\}$

12(3). $\mathbb{Q}(\sqrt{73})$, t^2-t-18, $-\frac{301}{144}$, $\left\{\frac{1}{6}g-\frac{1}{12}, \frac{5}{12}, \frac{19}{12}, \frac{1}{3}g+\frac{1}{12}, \frac{1}{3}g-\frac{5}{12}, \frac{23}{12}\right\}$

12(4). $\mathbb{Q}(\sqrt{105})$, $t^2{-}t{-}26$, $-\frac{95}{48}$, $\left\{\frac{1}{6}g-\frac{13}{12}, \frac{1}{6}g+\frac{11}{12}, \frac{1}{3}g-\frac{5}{12}, \frac{1}{6}g+\frac{5}{12}, \frac{1}{6}g-\frac{7}{12}, \frac{1}{3}g+\frac{1}{12}\right\}$

12(4,2). $\mathbb{Q}(\sqrt{-15})$, $t^2{-}t{+}4$, $-\frac{31}{48}$, $\left\{\frac{1}{3}g+\frac{1}{12}, \frac{1}{6}g-\frac{13}{12}, \frac{1}{3}g-\frac{5}{12}, \frac{1}{6}g+\frac{5}{12}, \frac{1}{6}g-\frac{7}{12}, \frac{1}{6}g+\frac{11}{12}\right\}$

12(6). $\mathbb{Q}(\sqrt{33})$, $t^2{-}t{-}8$, $-\frac{71}{48}$, $\left\{\frac{1}{6}g-\frac{13}{12}, \frac{1}{6}g-\frac{7}{12}, \frac{1}{3}g-\frac{5}{12}, \frac{1}{6}g+\frac{5}{12}, \frac{1}{3}g+\frac{1}{12}, \frac{1}{6}g+\frac{11}{12}\right\}$

14(2,1,1). $\mathbb{Q}(\sqrt{17})$, t^2-t-4, $-\frac{21}{16}$, $\left\{\frac{1}{4}, \frac{3}{4}, \frac{5}{4}, \frac{7}{4}, \frac{1}{2}g-\frac{1}{4}, \frac{1}{2}g-\frac{3}{4}, \frac{1}{2}g+\frac{1}{4}\right\}$

14(3,1,1). $\mathbb{Q}(\sqrt{33})$, t^2-t-8, $-\frac{29}{16}$, $\left\{\frac{1}{4}, \frac{5}{4}, \frac{3}{4}, \frac{1}{2}g-\frac{3}{4}, \frac{1}{2}g+\frac{1}{4}, \frac{1}{2}g-\frac{1}{4}, \frac{7}{4}\right\}$

14(3,2). $\mathbb{Q}(\sqrt{17})$, t^2-t-4, $-\frac{29}{16}$, $\left\{\frac{1}{4}, \frac{5}{4}, \frac{3}{4}, \frac{1}{2}g-\frac{1}{4}, \frac{1}{2}g-\frac{3}{4}, \frac{1}{2}g+\frac{1}{4}, \frac{7}{4}\right\}$

Bibliography

[1] Houria Baaziz. “Equations for the modular curve $X_1(N)$ and models of elliptic curves with torsion points”. *Math. Comp.* 79.272 (2010), pp. 2371–2386.

[2] Alexander I. Barvinok. “A Polynomial Time Algorithm for Counting Integral Points in Polyhedra When the Dimension Is Fixed”. *Mathematics of Operations Research* 19.4 (1994), pp. 769–779.

[3] Daniel Berend and Yuri Bilu. “Polynomials with roots modulo every integer”. *Proc. Amer. Math. Soc.* 124.6 (1996), pp. 1663–1671.

[4] A. I. Borevich and I. R. Shafarevich. *Number theory.* Pure and Applied Mathematics, Vol. 20. Academic Press, 1966.

[5] Nils Bruin and Michael Stoll. “Deciding existence of rational points on curves: an experiment”. *Experiment. Math.* 17.2 (2008), pp. 181–189.

[6] Nils Bruin and Michael Stoll. “Two-cover descent on hyperelliptic curves”. *Math. Comp.* 78.268 (2009), pp. 2347–2370.

[7] David G. Cantor. “Computing in the Jacobian of a hyperelliptic curve”. *Math. Comp.* 48.177 (1987), pp. 95–101.

[8] Henri Cohen. *A course in computational algebraic number theory.* Vol. 138. Graduate Texts in Mathematics. Springer-Verlag, 1993.

[9] Robert F. Coleman. “Effective Chabauty”. *Duke Math. J.* 52.3 (1985), pp. 765–770.

[10] Henri Darmon. “Note on a polynomial of Emma Lehmer”. *Math. Comp.* 56.194 (1991), pp. 795–800.

[11] Jesús A. De Loera et al. “Effective lattice point counting in rational convex polytopes”. *J. Symbolic Comput.* 38.4 (2004), pp. 1273–1302.

[12] Fred Diamond and Jerry Shurman. *A first course in modular forms.* Vol. 228. Graduate Texts in Mathematics. Springer-Verlag, 2005.

[13] John R. Doyle, Xander Faber, and David Krumm. *Computation of preperiodic structures for quadratic polynomials over number fields.* Submitted.

[14] John R. Doyle, Xander Faber, and David Krumm. *Preperiodic points for quadratic polynomials over quadratic fields.* In preparation.

[15] John R. Doyle and David Krumm. *Computing algebraic numbers of bounded height.* In revision.

[16] U. Fincke and M. Pohst. “A procedure for determining algebraic integers of given norm”. *Computer algebra (London, 1983).* Vol. 162. Lecture Notes in Comput. Sci. Springer, 1983, pp. 194–202.

[17] E. V. Flynn, Bjorn Poonen, and Edward F. Schaefer. “Cycles of quadratic polynomials and rational points on a genus-2 curve”. *Duke Math. J.* 90.3 (1997), pp. 435–463.

[18] Michael D. Fried and Moshe Jarden. *Field arithmetic.* Third. Springer-Verlag, 2008.

[19] Steven D. Galbraith, Michael Harrison, and David J. Mireles Morales. “Efficient hyperelliptic arithmetic using balanced representation for divisors”. *Algorithmic number theory.* Vol. 5011. Lecture Notes in Comput. Sci. Springer, 2008, pp. 342–356.

[20] Jean Gillibert and Aaron Levin. “Pulling back torsion line bundles to ideal classes”. *Mathematical Research Letters* (To appear).

[21] Robin Hartshorne. *Algebraic geometry.* Graduate Texts in Mathematics, No. 52. Springer-Verlag, 1977.

[22] Everett W. Howe, Kristin E. Lauter, and Jaap Top. "Pointless curves of genus three and four". *Arithmetic, geometry and coding theory (AGCT 2003).* Vol. 11. Sémin. Congr. Soc. Math. France, pp. 125–141.

[23] Benjamin Hutz. *Determination of all rational preperiodic points for morphisms of* $\mathbb{P}^N$. Preprint.

[24] Benjamin Hutz and Patrick Ingram. "On Poonen's conjecture concerning rational preperiodic points of quadratic maps". *Rocky Mountain J. Math.* (To appear).

[25] Kenneth Ireland and Michael Rosen. *A classical introduction to modern number theory.* Second. Vol. 84. Graduate Texts in Mathematics. Springer-Verlag, 1990.

[26] Nobuhiko Ishida and Noburo Ishii. "Generators and defining equation of the modular function field of the group $\Gamma_1(N)$". *Acta Arith.* 101.4 (2002), pp. 303–320.

[27] Daeyeol Jeon and Chang Heon Kim. "On the arithmetic of certain modular curves". *Acta Arith.* 130.2 (2007), pp. 181–193.

[28] Daeyeol Jeon, Chang Heon Kim, and Euisung Park. "On the torsion of elliptic curves over quartic number fields". *J. London Math. Soc. (2)* 74.1 (2006), pp. 1–12.

[29] Daeyeol Jeon, Chang Heon Kim, and Andreas Schweizer. "On the torsion of elliptic curves over cubic number fields". *Acta Arith.* 113.3 (2004), pp. 291–301.

[30] John Jones. *Number Fields.* URL: `http://hobbes.la.asu.edu/NFDB/`.

[31] S. Kamienny. "Torsion points on elliptic curves and q-coefficients of modular forms". *Invent. Math.* 109.2 (1992), pp. 221–229.

[32] S. Kamienny and F. Najman. "Torsion groups of elliptic curves over quadratic fields". *Acta Arith.* 152 (2012), pp. 291–305.

[33] Nicholas M. Katz and Barry Mazur. *Arithmetic moduli of elliptic curves.* Vol. 108. Annals of Mathematics Studies. Princeton University Press, 1985.

[34] M. A. Kenku. “Certain torsion points on elliptic curves defined over quadratic fields”. *J. London Math. Soc. (2)* 19.2 (1979), pp. 233–240.

[35] M. A. Kenku and F. Momose. “Torsion points on elliptic curves defined over quadratic fields”. *Nagoya Math. J.* 109 (1988), pp. 125–149.

[36] Anthony W. Knapp. *Elliptic curves.* Vol. 40. Mathematical Notes. Princeton University Press, 1992.

[37] Neal Koblitz. “Hyperelliptic cryptosystems”. *J. Cryptology* 1.3 (1989), pp. 139–150.

[38] Serge Lang. *Algebraic number theory.* Second. Vol. 110. Graduate Texts in Mathematics. Springer-Verlag, 1994.

[39] Odile Lecacheux. “Unités d’une famille de corps cycliques réeles de degré 6 liés à la courbe modulaire $X_1(13)$”. *J. Number Theory* 31.1 (1989), pp. 54–63.

[40] Dino Lorenzini. “Torsion and Tamagawa numbers”. *Ann. Inst. Fourier* 61.5 (2011), pp. 1995–2037.

[41] Dino Lorenzini and Thomas J. Tucker. “Thue equations and the method of Chabauty-Coleman”. *Invent. Math.* 148.1 (2002), pp. 47–77.

[42] Daniel Maisner and Enric Nart. “Abelian surfaces over finite fields as Jacobians”. *Experiment. Math.* 11.3 (2002), pp. 321–337.

[43] B. Mazur. “Modular curves and the Eisenstein ideal”. *Inst. Hautes Études Sci. Publ. Math.* 47 (1977), 33–186 (1978).

[44] B. Mazur and J. Tate. “Points of order 13 on elliptic curves”. *Invent. Math.* 22 (1973/74), pp. 41–49.

[45] J. S. Milne. “Jacobian varieties”. *Arithmetic geometry (Storrs, Conn., 1984)*. Springer, 1986, pp. 167–212.

[46] Fumiyuki Momose. “p-torsion points on elliptic curves defined over quadratic fields”. *Nagoya Math. J.* 96 (1984), pp. 139–165.

[47] Patrick Morton. “Arithmetic properties of periodic points of quadratic maps, II”. *Acta Arith.* 87 (1998), pp. 89–102.

[48] Patrick Morton and Joseph H. Silverman. “Rational periodic points of rational functions”. *Int. Math. Res. Not.* 1994.2 (1994), pp. 97–110.

[49] David Mumford. *Tata lectures on theta. II.* Modern Birkhäuser Classics. Birkhäuser Boston Inc., 2007.

[50] M. Ram Murty and Jody Esmonde. *Problems in algebraic number theory.* Second. Vol. 190. Graduate Texts in Mathematics. Springer-Verlag, 2005.

[51] Filip Najman. “Complete classification of torsion of elliptic curves over quadratic cyclotomic fields”. *J. Number Theory* 130.9 (2010), pp. 1964–1968.

[52] Filip Najman. “Torsion of elliptic curves over quadratic cyclotomic fields”. *Math. J. Okayama Univ.* 53 (2011), pp. 75–82.

[53] D. G. Northcott. “Periodic points on an algebraic variety”. *Ann. of Math.* 51.1 (1950), pp. 167–177.

[54] Victor Y. Pan. “Univariate polynomials: nearly optimal algorithms for numerical factorization and root-finding”. *J. Symbolic Comput.* 33.5 (2002). Computer algebra (London, ON, 2001), pp. 701–733.

[55] Pierre Parent. “No 17-torsion on elliptic curves over cubic number fields”. *J. Théor. Nombres Bordeaux* 15.3 (2003), pp. 831–838.

[56] A. Pethő and S. Schmitt. “Elements with bounded height in number fields”. *Period. Math. Hungar.* 43.1-2 (2001), pp. 31–41.

[57] Bjorn Poonen. “Computing torsion points on curves”. *Experiment. Math.* 10.3 (2001), pp. 449–465.

[58] Bjorn Poonen. “The classification of rational preperiodic points of quadratic polynomials over $\mathbb{Q}$: a refined conjecture”. *Math. Z.* 228.1 (1998), pp. 11–29.

[59] F. Patrick Rabarison. “Structure de torsion des courbes elliptiques sur les corps quadratiques”. *Acta Arith.* 144.1 (2010), pp. 17–52.

[60] Markus A. Reichert. “Explicit determination of nontrivial torsion structures of elliptic curves over quadratic number fields”. *Math. Comp.* 46.174 (1986), pp. 637–658.

[61] David E. Rohrlich. “Modular curves, Hecke correspondence, and L-functions”. *Modular forms and Fermat’s last theorem (Boston, MA, 1995).* Springer, 1997, pp. 41–100.

[62] Hans-Georg Rück. “A note on elliptic curves over finite fields”. *Math. Comp.* 49.179 (1987), pp. 301–304.

[63] Walter Rudin. *Principles of mathematical analysis.* Third. International Series in Pure and Applied Mathematics. McGraw-Hill Book Co., 1976.

[64] Stephen Hoel Schanuel. “Heights in number fields”. *Bull. Soc. Math. France* 107.4 (1979), pp. 433–449.

[65] Goro Shimura. *Introduction to the arithmetic theory of automorphic functions.* Vol. 11. Publications of the Mathematical Society of Japan. Princeton University Press, 1994.

[66] Joseph H. Silverman. *The arithmetic of dynamical systems.* Vol. 241. Graduate Texts in Mathematics. Springer, 2007.

[67] Joseph H. Silverman. *The arithmetic of elliptic curves.* Second. Vol. 106. Graduate Texts in Mathematics. Springer, 2009.

[68] W. A. Stein et al. *Sage Mathematics Software (Version 4.7.1)*. `http://www.sagemath.org`. The Sage Development Team. 2011.

[69] Michael Stoll. “Implementing 2-descent for Jacobians of hyperelliptic curves”. *Acta Arith.* 98.3 (2001), pp. 245–277.

[70] Michael Stoll. “Rational 6-cycles under iteration of quadratic polynomials”. *LMS J. Comput. Math.* 11 (2008), pp. 367–380.

[71] Michael Stoll. “Rational points on curves”. *J. Théor. Nombres Bordeaux* 23.1 (2011), pp. 257–277.

[72] Andrew V. Sutherland. “Constructing elliptic curves over finite fields with prescribed torsion”. *Math. Comp.* 81 (2012), pp. 1131–1147.

[73] Paul Vojta. “A generalization of theorems of Faltings and Thue-Siegel-Roth-Wirsing”. *J. Amer. Math. Soc.* 5.4 (1992), pp. 763–804.

[74] R. Walde and P. Russo. “Rational periodic points of the quadratic function $Q_c(x) = x^2 + c$”. *Amer. Math. Monthly* 101 (1994), pp. 318–331.

[75] Lawrence C. Washington. “A family of cyclic quartic fields arising from modular curves”. *Math. Comp.* 57.196 (1991), pp. 763–775.

[76] William C. Waterhouse. “Abelian varieties over finite fields”. *Ann. Sci. École Norm. Sup. (4)* 2 (1969), pp. 521–560.

[77] Yifan Yang. “Defining equations of modular curves”. *Adv. Math.* 204.2 (2006), pp. 481–508.