Topological aspects of rational points on K3 surfaces

Proefschrift

ter verkrijging van
de graad van Doctor aan de Universiteit Leiden,
op gezag van Rector Magnificus prof. mr. C. J. J. M. Stolker,
volgens besluit van het College voor Promoties
te verdedigen op dinsdag 17 september 2013
klokke 13:45 uur
door

Rene Pannekoek

geboren te Apeldoorn
in 1981

Samenstelling van de promotiecommissie:

Promotor:	prof. dr. P. Stevenhagen
Copromotor:	dr. R. M. van Luijk
Overige leden:	prof. dr. S. J. Edixhoven
	prof. dr. A. N. Skorobogatov (Imperial College)
	prof. dr. J. Top (Rijksuniversiteit Groningen)
	dr. R. S. de Jong
	dr. A. Várilly-Alvarado (Rice University)

Universiteit Leiden

What Song the Syrens sang, or what name
Achilles assumed when he hid himself among
women, although puzzling Questions are not
beyond all conjecture.
Sir Thomas Browne

Contents

Introduction **ix**
0.1 Diophantine geometry ix
0.2 Topological aspects of rational points x
0.2.1 Completions of a number field x
0.2.2 The Hasse principle xi
0.2.3 Density of rational points xii
0.3 Obstructions to rational points xiii
0.4 Rational points on surfaces xv
0.5 Geometrically rational surfaces xv
0.6 K3 surfaces xvi
0.6.1 Existence of rational points xvii
0.6.2 Brauer group and density questions xvii
0.6.3 Elliptic fibrations on K3 surfaces xvii
0.6.4 Failure of weak approximation on K3 surfaces xviii
0.7 An open question about K3 surfaces xix
0.8 Contents of this thesis xix

1 Elliptic curves over p-adic fields **1**
1.1 Introduction 1
1.2 Preliminaries on Weierstrass curves 2
1.3 Extensions of topological abelian groups 5
1.3.1 The profinite topology 6
1.3.2 The extension problem 7
1.4 Weierstrass curves with additive reduction 12
1.5 Proof of the main theorem 15
1.5.1 The case $p = 2$ 16
1.5.2 The case $p = 3$ 17
1.5.3 The case $p = 5$ 18
1.5.4 The case $p = 7$ 19

1.5.5 The proof 19
1.6 Examples 20

2 Density results for quartic surfaces **23**
2.1 Some open subsets 24
2.1.1 Outline of the rest of the chapter 25
2.2 Elliptic fibrations 26
2.2.1 The level of a point on a Weierstrass curve 27
2.3 Weierstrass models for the fibres 27
2.3.1 The group structure on the fibres 30
2.3.2 The bad fibres 32
2.4 Using elliptic fibrations to prove density 35
2.4.1 One elliptic fibration 35
2.4.2 Two elliptic fibrations 36
2.5 Density in $\mathcal{C}_{c,1}$ 37
2.6 Density in $\mathcal{A}_c$ 40
2.7 Density in $\mathcal{B}_{c,n}$ for all n and in $\mathcal{C}'_{c,n}$ for $n \geq 2$ 43
2.8 Proof of the main theorem 47

3 Density results for Kummer surfaces **49**
3.1 Birational invariance of density results 50
3.2 Procyclic and topologically cyclic groups 52
3.3 Elliptic curves with good twists 55
3.3.1 Notation and definitions 55
3.3.2 Partition of the rational points of a Kummer surface 56
3.3.3 Elliptic curves with good twists 57
3.3.4 From good twists to density results 57
3.3.5 A partial converse to Theorem 3.20 58
3.4 Density results for Kummer surfaces 59
3.4.1 Topologically cyclic groups and density results 60
3.4.2 Proof of Theorems 3.1–3.2 63
3.5 Large product topologies 66
3.6 Proof of Theorem 3.4 71
3.7 Proof of Theorem 3.5 72

4 Refinements and computations **75**
4.1 Introduction 75
4.1.1 Goal of this chapter 75
4.1.2 Computer calculations 76

4.2 Definitions . . . 76
4.2.1 Mestre's construction . . . 77
4.2.2 An affine model for C . . . 78
4.3 Creating good twists . . . 79
4.4 Properties of the curve C . . . 80
4.5 Existence criteria for Mestre points . . . 86
4.5.1 Assumptions and definitions . . . 86
4.5.2 The case where p does not divide $\#\mathcal{E}(\mathbb{F}_p)$ . . . 87
4.5.3 The case of anomalous reduction . . . 88
4.5.4 Good points over ramified twists . . . 94
4.6 Existence criteria for good twists . . . 96
4.6.1 Unramified twists . . . 96
4.6.2 Ramified twists . . . 99
4.7 A computer experiment . . . 99
4.7.1 Results of the experiment . . . 101
4.8 `sage` code . . . 102
4.8.1 Looking for two-element sets of generators . . . 103
4.8.2 Finding pairs in the image of $\mathcal{C}(\mathbb{F}_p)$ . . . 104
4.8.3 The criteria involving anomalous reduction . . . 105
4.8.4 Wrapper code . . . 107

5 Descent on superelliptic curves **111**
5.1 Definitions and statement of results . . . 111
5.2 Properties of C and J . . . 112
5.3 Relating certain divisors on C . . . 113
5.4 The homomorphism $(x - T)$ . . . 114
5.4.1 Descent . . . 115
5.4.2 Some values of $(x - T)$ . . . 116
5.5 The image of $(x - T)$ . . . 118
5.6 An algebraic lemma . . . 119
5.7 Proof of the main theorem . . . 120

Bibliography **123**

Samenvatting **127**

Dankwoord **137**

Curriculum vitæ **139**

Introduction

This thesis is concerned with the arithmetic of K3 surfaces over number fields. A K3 surface over a field k is a smooth, projective, and geometrically integral surface over k such that the canonical divisor class of X is trivial and the first cohomology of the structure sheaf of X vanishes. We will prove various results about p-adic density of rational points on certain types of K3 surfaces defined over $\mathbb{Q}$. In particular, we prove that, for each prime number p, there exist infinitely many K3 surfaces X over $\mathbb{Q}$ such that the rational points on X are p-adically dense. A fuller summary of the results in this thesis can be found at the end of this Introduction.

0.1 Diophantine geometry

Broadly speaking, this thesis is concerned with the topic of Diophantine equations, which are polynomial equations with coefficients in a number field k, for which one is only interested in solutions defined over the same number field k. This thesis applies geometric methods to the study of solution sets of Diophantine equations. In this context, one often speaks of Diophantine geometry.

Given a number field k and a system of Diophantine equations

$$f_1 = 0, \ldots, f_n = 0, \tag{1}$$

where $f_1, \ldots, f_n$ are polynomials over k, one may consider the algebraic variety X defined by the $f_1, \ldots, f_n$. There are several ways to describe the variety X. The classical viewpoint is, having chosen an algebraically closed field extension F of k, for example the field $\mathbb{C}$ of complex numbers, to identify X with the set of F-valued solutions to (1). A more modern viewpoint is to view X as a scheme, which is a topological space equipped with a sheaf of commutative rings, that admits an open covering by so-called spectra of commutative rings. Both viewpoints are equally acceptable for

the purposes of this thesis, with the exception of some parts of chapter 4 which use scheme theory in an essential way. In both viewpoints, the variety X comes equipped with a topology, called the Zariski topology, in which the closed subsets are exactly the subsets Z of X that can be defined by imposing further polynomial equations

$$g_1 = 0, \ldots, g_m = 0 \tag{2}$$

on the points of Z.

We say that a variety is defined over a number field k if it arises from a set of polynomial equations whose coefficients lie in k. We also speak more simply of a variety over k. Note that the ground field k is often implicitly assumed to be part of the data of the variety.

Still writing X for the variety associated to the equations (1), the set of solutions over k to (1) is denoted by $X(k)$. The elements of $X(k)$ are called the rational points on X. For every field extension K of k, the set of solutions over K to (1) is denoted by $X(K)$.

Within the theory of Diophantine equations, the terminology afforded by the theory of algebraic varieties is considered to be so convenient that the central focus is often placed on the variety rather than its defining equations. Questions about Diophantine equations thus often take the following form: "Given a certain variety X defined over a number field k, what can one say about its set $X(k)$ of rational points?" In line with this, the results of this thesis are phrased in terms of varieties rather than their defining equations.

0.2 Topological aspects of rational points

0.2.1 Completions of a number field

It is possible to view $X(k)$ in a topological way, even leaving aside the Zariski topology for the moment. To this end, we will introduce the notion of completions of a number field k with respect to an (equivalence class of) absolute value(s) on k. Recall that an absolute value $|\cdot|$ on k is a function

$$|\cdot| : k \to \mathbb{R}$$

satisfying:

(i) for all $x \in k$ we have $|x| \geq 0$;
(ii) for all $x \in k$ we have $|x| = 0$ if and only if $x = 0$;

(iii) for all $x, y \in k$ we have $|xy| = |x|\,|y|$;
(iv) for all $x, y \in k$ we have $|x + y| \leq |x| + |y|$.

Note that property (iv) is known as the triangle inequality for $|\cdot|$. An absolute value $|\cdot|$ is called non-archimedean if in addition to (iv) it satisfies the stronger property

(iv') for all $x, y \in k$ we have $|x + y| \leq \max(|x|, |y|)$.

This last property is known as the ultrametric inequality for $|\cdot|$.

Two absolute values $|\cdot|_1$ and $|\cdot|_2$ of k are considered equivalent if there exists a non-zero real number e such that for all $x \in k$ we have $|x|_2 = |x|_1^e$. If v is a place of k, i.e. an equivalence class of absolute values on k, and $|\cdot|$ is an element of v, then the completion of k for v, often denoted by k_v, is obtained, analogously to the construction of $\mathbb{R}$ from $\mathbb{Q}$, by taking the Cauchy sequences in k for the metric $|\cdot|$ and identifying Cauchy sequences if their difference converges to 0. Note that this construction does not depend on the choice of $|\cdot|$. The set k_v is a field, with the addition and multiplication operations induced by the ones on k, and it is a metric space with the metric given by $|\cdot|$. If $|\cdot|$ is non-archimedean, then all elements of v are, and the field k_v is called a p-adic field.

By Ω_k we denote the set of all places of k. By Ostrowski's theorem, we have that the non-archimedean absolute values on k all arise from the valuations at the prime ideals of the ring of integers of k, whereas the archimedean absolute values on k are all obtained by composing the embeddings of k into the field $\mathbb{C}$ of complex numbers by the standard absolute value on $\mathbb{C}$. In particular, if we specialize to the case $k = \mathbb{Q}$, then all places of $\mathbb{Q}$ are given by either the standard absolue value on $\mathbb{Q}$, or the p-adic valuation for some prime number p

$$\begin{aligned} |\cdot| : \mathbb{Q} &\to \mathbb{R} \\ x &\mapsto p^{-v_p(x)} \\ 0 &\mapsto 0. \end{aligned}$$

Here v_p is the p-adic valuation on $\mathbb{Q}$: for every pair a, b of non-zero integers, we have that $v_p(a/b)$ is the number of prime factors p in a minus the number of prime factors p in b.

0.2.2 The Hasse principle

The sets $X(k_v)$, which we recall are the solution sets over k_v to (1), give a very useful tool for studying $X(k)$. Observe that $X(k)$ embeds in $X(k_v)$, by

considering a solution over k to (1) as a solution over k_v to (1). It follows that if, for some place v of k, we have that $X(k_v)$ is empty, then $X(k)$ must be empty too. This gives a very useful sufficient criterion for the emptiness of $X(k)$. Its usefulness derives from the fact that there is an algorithm that checks in finite time whether or not there exists a place v of k such that $X(k_v)$ is empty. (By Hensel's lemma and the Lang–Weil estimates [17] one reduces this last problem to deciding the non-emptiness of $X(k_v)$ for only finitely many places v, which can be done in finite time by the main result of [24].)

Conversely, one might ask: if for all places v of k the set $X(k_v)$ is non-empty, may we then conclude that $X(k)$ is also non-empty? As we shall see, this implication does not hold for general X. If X is such that the implication does hold, we say that X satisfies the Hasse principle; if it does not hold, then it is said that X violates the Hasse principle. Note that X violates the Hasse principle if and only if $X(k)$ is empty, but $X(k_v)$ is non-empty for all places v of k.

We have the following classical theorem.

Theorem 0.1 (Hasse, Minkowski)**.** *Let C be a smooth plane conic curve over a number field k. Then the Hasse principle holds for C; that is, if $C(k_v)$ is non-empty for all places v of k, then $C(k)$ is non-empty.*

There exist varieties X over number fields k (even over $\mathbb{Q}$) that violate the Hasse principle. We will see examples of this later in this introduction.

0.2.3 Density of rational points

This thesis deals with the topological aspects of the solution set $X(k)$. For instance, one may ask whether $X(k)$ is dense in X for the Zariski topology. This is sometimes abbreviated slightly by asking whether $X(k)$ is Zariski-dense in X.

Other topological aspects of $X(k)$ can be made visible as follows. If v is a place of k, then the set $X(k_v)$ inherits a topology from the one on k_v. By viewing $X(k)$ as a subset of $X(k_v)$, we may then ask: is $X(k)$ dense in $X(k_v)$? Similarly, for any non-empty set S of places of $X(k)$, the set $X(k)$ embeds diagonally into the product $\prod_{v\in S} X(k_v)$, which we consider as having the product topology, and one may ask if $X(k)$ has dense image under this embedding.

Let X be a variety defined over a number field k. The following are some questions one may ask about the topological nature of $X(k)$.

(D1) Is $X(k)$ Zariski-dense in X?
(D2) For a non-empty finite subset $S \subset \Omega_k$, is the closure of $X(k)$ open in $\prod_{v\in S} X(k_v)$?
(D3) For a non-empty finite subset $S \subset \Omega_k$, is $X(k)$ is dense in $\prod_{v\in S} X(k_v)$?
(D4) Does there exist a finite subset $T \subset \Omega_k$ such that $X(k)$ dense in $\prod_{v\notin T} X(k_v)$?
(D5) Is $X(k)$ dense in $\prod_{v\in\Omega_k} X(k_v)$?

If X satisfies property (D2) with respect to some finite set S of places of v, one says that X has S-openness. If X satisfies property (D4) for some finite set T of places of k, one says that X satisfies weak weak approximation. If X satisfies property (D5), one says that X satisfies weak approximation. (For this terminology, see [21].) We note that (D5) implies that (D4) holds for every T; (D4) for some T implies that (D3) holds for every S disjoint from T; (D3) for some S implies that (D2) holds for the same S; lastly, (D2) for some S implies that (D1) holds.

0.3 Obstructions to rational points

Before, we mentioned that $X(k)$ may be empty whereas $X(k_v)$ is non-empty for all places v of k. An example of this is given by the famous Reichardt–Lind curve, which is the curve T defined over $\mathbb{Q}$ that is given by the equation

$$2y^2 = x^4 - 17. \tag{3}$$

We have that $T(\mathbb{R}) \neq \emptyset$ as well as $T(\mathbb{Q}_p) \neq \emptyset$ for all prime numbers p. On the other hand, it is an easy application of the law of quadratic reciprocity to show that there are no solutions over $\mathbb{Q}$ to (3) (see [32, X.6.5(a)]), or equivalently, that we have $T(\mathbb{Q}) = \emptyset$. Hence, T provides an instance of a violation of the Hasse principle.

In 1970, Yuri Manin defined a framework that explains the failure of the Hasse principle in certain cases [19]. For this, we need to introduce some additional concepts and set some notation. Assume that X is a smooth, projective, and geometrically integral variety defined over a number field k. Let $\mathrm{Br}(X)$ be the Brauer group of X, which is defined as the étale cohomology group $\mathrm{H}^2_{\text{ét}}(X, \mathbb{G}_m)$. By functoriality, we have a map from $\mathrm{Br}(k)$, the Brauer group of the field k, to $\mathrm{Br}(X)$. The image of $\mathrm{Br}(k)$ in $\mathrm{Br}(X)$ is denoted by $\mathrm{Br}_0(X)$. Furthermore, one defines $\mathrm{Br}_1(X)$ as the subgroup of $\mathrm{Br}(X)$ consisting of the elements that become trivial over some finite

extension of k. The elements of $\mathrm{Br}_1(X)$ are called algebraic Brauer classes. Elements of $\mathrm{Br}(X)$ that are not algebraic are called transcendental. By the fact that X is projective, we may write

$$X(\mathbb{A}_k) = \prod_{v \in \Omega_k} X(k_v),$$

where $\mathbb{A}_k$ is the ring of adeles of k. We are now ready to describe Manin's theory. In [19], Manin defines a pairing

$$X(\mathbb{A}_k) \times \mathrm{Br}(X) \to \mathbb{Q}/\mathbb{Z}.$$

This pairing is continuous in the first variable, for the discrete topology on $\mathbb{Q}/\mathbb{Z}$, and it has the property that $((x_v)_v, \alpha)$ maps to 0 if $(x_v)_v \in X(\mathbb{A}_k)$ is the image of a rational point. The set of points $(x_v)_v \in X(\mathbb{A}_k)$ that pair to 0 with every $\alpha \in \mathrm{Br}(X)$ is customarily denoted by $X(\mathbb{A}_k)^{\mathrm{Br}}$. By these facts, we thus have the crucial property

$$X(k) \subset X(\mathbb{A}_k)^{\mathrm{Br}}. \tag{4}$$

The properties of Manin's pairing mentioned above imply that $X(\mathbb{A}_k)^{\mathrm{Br}}$ is a closed subset of $X(\mathbb{A}_k)$. Hence, if $\overline{X(k)}$ denotes the closure of the image of $X(k)$ in $X(\mathbb{A}_k)$, we have the following strengthening of (4):

$$\overline{X(k)} \subset X(\mathbb{A}_k)^{\mathrm{Br}}. \tag{5}$$

For a smooth, projective and geometrically integral variety over k, it may happen that $X(\mathbb{A}_k)$ is non-empty, but $X(\mathbb{A}_k)^{\mathrm{Br}}$ is empty, and, by (4), so is $X(k)$. Then X violates the Hasse principle, and Manin's pairing explains why this is true. In this case, one says that there is a Brauer–Manin obstruction to the Hasse principle on X. Similarly, if $X(\mathbb{A}_k)^{\mathrm{Br}}$ is a proper subset of $X(\mathbb{A}_k)$, then (5) shows that $X(k)$ is not dense in $X(\mathbb{A}_k)$, and one says that there is a Brauer–Manin obstruction to weak approximation on X.

In view of the inclusion (5), we may ask the following further question regarding the topological properties of $X(k)$.

(D4') Is $X(k)$ dense in $X(\mathbb{A}_k)^{\mathrm{Br}}$?

If the answer to (D5) is positive for X, then so is the answer to (D4'). Now assume that $\mathrm{Br}(X)/\mathrm{Br}_0(X)$ is finite, so that $X(\mathbb{A}_k)^{\mathrm{Br}}$ is open in $X(\mathbb{A}_k)$. Then if $X(k)$ is non-empty, and if the answer to (D4') is positive for X, then the answer to (D4) is also positive for some T.

0.4 Rational points on surfaces

By a surface X over a field k we will mean a smooth, projective, and geometrically integral variety X over k that has dimension 2. In the sequel, we again let k be a number field. The subject of this thesis mainly concerns the Diophantine geometry of surfaces over number fields, or, as is sometimes said, the arithmetic of surfaces. We will give an overview of what is known and conjectured about questions (D1)–(D5) for the case where X is a surface over a number field k.

0.5 Geometrically rational surfaces

One says that a variety X over k is rational if X is birational to $\mathbb{P}^n_k$ for some integer n. We say that X is geometrically rational if the base-change $X_{\overline{k}}$ of X to the algebraic closure of k is rational. Let X be a geometrically rational surface over a number field k.

It is well-known that, since X is geometrically rational, the quotient of $\mathrm{Br}(X)$ by $\mathrm{Br}_0(X)$ is finite, hence a positive answer to (D4') implies a positive answer to (D4) for some T. Moreover, we have that X is either a del Pezzo surface, which means that the anticanonical divisor $-K_X$ of X is ample, or X is a conic bundle, which means that there exists a surjective morphism $\pi\colon X \to C$, where C is a curve of genus 0 defined over k, such that the fibres of π are isomorphic to plane conics [16]. The degree d_X of X is defined as the self-intersection of K_X, where K_X is the canonical divisor of X.

The following conjecture is a special case of a conjecture by Colliot–Thélène [9, p. 319, Conjecture (d)]).

Conjecture 0.2. *Let X be a geometrically rational surface over a number field k. Then $X(k)$ is dense in $X(\mathbb{A}_k)^{\mathrm{Br}}$.*

We will discuss some of the known facts about Conjecture 0.2.

Suppose first that X is a del Pezzo surface. Then we have $d_X \geq 1$ by ampleness of $-K_X$. If $d_X \geq 5$, then we have by [20, Theorem 29.4] that X satisfies both the Hasse principle and weak approximation. It follows that if $d_X \geq 5$ and $X(k) \neq \emptyset$, then all questions (D1)–(D5) have positive answers. If $d_X = 4$, then X may violate the Hasse principle (see [1]). However, if $X(k)$ is non-empty, then $X(k)$ is dense in $X(\mathbb{A}_k)^{\mathrm{Br}}$ (see [27]). Hence if $d_X = 4$ and $X(k) \neq \emptyset$, then the questions (D1)–(D4') all have positive answers.

If $d_X = 3$, then the Hasse principle may fail (see [36]). Furthermore, if $d_X = 3$ and $X(k) \neq \emptyset$, then it is currently unknown in general whether any of the questions (D2)–(D5) have positive answers; however, it is known that if $X(k) \neq \emptyset$ then $X(k)$ is Zariski-dense in X, so that question (D1) does have a positive answer. Finally, if $d_X \leq 2$ and $X(k) \neq \emptyset$, we do not currently know the answers to any of the questions (D1)-(D5) in general; for the current state of the art in these cases, see [29] for $d_X = 2$ and [30] for $d_X = 1$.

If the geometrically rational surface X is not a del Pezzo surface, then it is shown in [16] that there exists a surjective morphism $\pi\colon X \to C$, where C is a curve of genus 0 defined over k, such that the fibres of π are isomorphic to plane conics.

By Theorem 0.1, the Hasse principle holds for C, hence a finite computation enables one to see whether $C(k)$ is non-empty. If $C(k) = \emptyset$, then we have $X(k) = \emptyset$. If $C(k) \neq \emptyset$, then C is isomorphic to $\mathbb{P}^1_k$. We assume that the latter is indeed the case, so that we have a surjective morphism $\pi\colon X \to \mathbb{P}^1_k$ whose fibres are isomorphic to plane conics. Then if the number of non-smooth fibres of π is at most 3, then X satisfies both the Hasse principle and weak approximation. Hence, if we are in this case and we have $X(k) \neq \emptyset$, the answers to the questions (D1)-(D5) are all positive. If the number of non-smooth fibres is 4 or 5, then we have that $X(k)$ is dense in $X(\mathbb{A}_k)^{\mathrm{Br}}$ (this follows from the results of [6], [7], [8], and [28] if the number of bad fibres is 4, and from [27] if the number of bad fibres is 5; see also the introduction to [4]). Finally, if the number of bad fibres is arbitrary, but every bad fibre is defined over $\mathbb{Q}$, then a very recent result [4, Theorem 1.1] says that $X(k)$ is always non-empty, and that $X(k)$ is dense in $X(\mathbb{A}_k)^{\mathrm{Br}}$.

0.6 K3 surfaces

Assume now that X is a K3 surface over a number field k, i.e., the class of the canonical divisor K_X in $\mathrm{Pic}(X)$ vanishes and we have $\mathrm{H}^1(X, \mathscr{O}_X) = 0$. In the case of K3 surfaces, the theory is far less complete than in the case for geometrically rational surfaces. We will describe some of the known results on the arithmetic of K3 surfaces, in particular the ones concerning density of rational points.

0.6.1 Existence of rational points

It is known that, in general, the Hasse principle fails for K3 surfaces over number fields. For example, Swinnerton-Dyer shows in [37] that the K3 surface over $\mathbb{Q}$ defined by

$$4x^4 + 9y^4 - 8z^4 - 8w^4 = 0$$

has points over $\mathbb{Q}_p$ for every prime number p, as well as over $\mathbb{R}$, but none over $\mathbb{Q}$.

0.6.2 Brauer group and density questions

By a remarkable result of Skorobogatov and Zarhin [34], one knows that $\mathrm{Br}_0(X)$ has finite index in $\mathrm{Br}(X)$, hence a positive answer to (D4') implies a positive answer to (D4) for some set of places T. In general, however, it is unknown whether any of the questions (D1)–(D5) has a positive answer. In fact, it is famously unknown whether $X(k) \neq \emptyset$ implies $X(k)$ to be even infinite!

0.6.3 Elliptic fibrations on K3 surfaces

It is known that K3 surfaces may admit fibrations into curves of genus 1. In this introduction, we will abuse terminology, and call such a fibration an elliptic fibration on X, even though the fibres are not elliptic curves since an identity for the group law is not specified.

Potential density

The presence of elliptic fibrations on a K3 surface is an important aid in proving density results. A seminal result by Bogomolov and Tschinkel [2, Theorem 1.1] says that if X possesses an elliptic fibration, then the rational points on X are potentially dense: there exists a finite field extension k'/k such that $X(k')$ is Zariski-dense in X.

If the rank of the abelian group $\mathrm{Pic}(X)$, which is free and finitely generated, is at least 5, then [13, Proposition 11.1] says that there exists a finite field extension k''/k such that the base-change of X to k'' possesses an elliptic fibration. From this and the result by Bogomolov and Tschinkel, it follows that if the rank of $\mathrm{Pic}(X_{\overline{k}})$ is at least 5, then the rational points on X are potentially dense.

Multiple elliptic fibrations

The result by Bogomolov and Tschinkel does not apply when one is solely interested in density over the ground field. We therefore turn to the case where X admits at least two elliptic fibrations. An example of a K3 surface over $\mathbb{Q}$ admitting at least two elliptic fibrations is the diagonal quartic surface

$$X_{a,b,c,d}\colon ax^4 + by^4 + cz^4 + dw^4 = 0,$$

where a, b, c, d are rational numbers such that $abcd \in \mathbb{Q}^{*2}$. It is a result by Logan, McKinnon, and Van Luijk [18, Theorem 1.1] that if $X_{a,b,c,d}$ contains a rational point that lies outside the coordinate planes and any of the 48 lines on $X_{a,b,c,d}$, then the rational points on $X_{a,b,c,d}$ lie dense in $X_{a,b,c,d}$ for the Zariski topology, as well as in $X_{a,b,c,d}(\mathbb{R})$ for the real-analytic topology.

The above is an example of a more general phenomenon. Assuming that X admits at least two elliptic fibrations, a result by Swinnerton-Dyer [38] provides sufficient conditions for $X(k)$ to be Zariski-dense in X. More precisely, under the assumption that every fibre belonging to one fibration is algebraically equivalent to none of the fibres belonging to the other fibration, Swinnerton-Dyer's result asserts the existence of an explicitly computable closed subset $Z \subsetneq X$ such that if X contains a rational point outside of Z, then $X(k)$ is Zariski dense in X.

0.6.4 Failure of weak approximation on K3 surfaces

We are still keeping the assumption that X is a K3 surface over a number field k. It is currently unknown whether or not it is true in general that $X(k)$ is dense in $X(\mathbb{A}_k)^{\mathrm{Br}}$. However, it is known that we may have $\overline{X(k)} \neq X(\mathbb{A}_k)$, even if $X(k)$ is non-empty. We give some examples of this. In [37, pp. 534–535], Swinnerton-Dyer shows that if X is the K3 surface over $\mathbb{Q}$ given by

$$7x^4 + 8y^4 - 9z^4 - 14w^4 = 0,$$

then $X(\mathbb{Q})$ does not lie dense in $X(\mathbb{Q}_3)$. In [41], Wittenberg shows that if X is the K3 surface over $\mathbb{Q}$ that is the minimal proper regular model of the elliptic surface

$$y^2 = x(x - 3(t-1)^3(t+3))(x - 3(t+1)^3(t-3))$$

over the projective line over $\mathbb{Q}$ with coordinate t, then $X(\mathbb{Q})$ is not dense in $X(\mathbb{Q}_2)$. In his PhD thesis [25], Preu shows that if X over $\mathbb{Q}$ is given by

$$x^4 + 3y^4 - 4z^4 - 9w^4 = 0,$$

then $X(\mathbb{Q})$ is not dense in $X(\mathbb{Q}_3)$. Finally, in [14], Hassett, Várilly-Alvarado, and Varilly construct a K3 surface with Picard rank equal to 1, for which weak approximation fails. In the last three cases, the failure of weak approximation is explained by a transcendental Brauer class.

0.7 An open question about K3 surfaces

In [34, p. 484], Skorobogatov and Zarhin ask the following question.

Question 0.3. Given a K3 surface X over a number field k, is $X(k)$ dense in $X(\mathbb{A}_k)^{\mathrm{Br}}$?

Question 0.3 thus asks whether the answer to question (D4') is positive for every K3 surface X. In other words: does the Brauer–Manin obstruction explain the failure of the Hasse principle or weak approximation for *all* K3 surfaces X? It is this question that has guided the research of this thesis. We have restricted to certain classes of K3 surfaces, and for none of these we have been able to give a full answer to Question 0.3. On the other hand, we believe that the results do suggest that the answer to Question 0.3 should be positive for at least certain K3 surfaces.

0.8 Contents of this thesis

We briefly describe the contents of this thesis.

In chapter 1, we answer the following question: if p is a prime, and E is an elliptic curve over $\mathbb{Q}_p$ that has additive reduction, what are the possible isomorphism types of $E(\mathbb{Q}_p)$ as a topological group? Let $E_0(\mathbb{Q}_p) \subset E(\mathbb{Q}_p)$ be the subgroup of points of good reduction. We will give an easy criterion to determine the isomorphism type of $E_0(\mathbb{Q}_p)$ in terms of the coefficients of a Weierstrass equation for E. In particular, we show that $E_0(\mathbb{Q}_p)$ is topologically isomorphic to either $\mathbb{Z}_p$ or $\mathbb{Z}_p \times \mathbb{Z}/p\mathbb{Z}$ as topological groups, where $\mathbb{Z}_p$ carries the p-adic topology, and $\mathbb{Z}/p\mathbb{Z}$ carries the discrete topology. If $p > 7$, then we find that $E_0(\mathbb{Q}_p)$ is always topologically isomorphic to $\mathbb{Z}_p$, and $E(\mathbb{Q}_p)$ is topologically isomorphic to the product of $\mathbb{Z}_p$ and a discrete finite group of order at most 4.

In chapter 2, we review, and slightly improve upon, a result by Sir Peter Swinnerton-Dyer [38]. This result concerns the 2-adic density of rational points on certain explicitly given diagonal quartic surfaces over $\mathbb{Q}$. We will mainly follow the proof of Swinnerton-Dyer, which employs the presence

of multiple elliptic fibrations. The argument also builds on the results of chapter 1 to determine the structure of the groups of 2-adic points on the fibres that have additive reduction. The work by Swinnerton-Dyer represents the first known result concerning p-adic density of rational points on a K3 surface for any prime number p.

In chapter 3, we move beyond the work of Swinnerton-Dyer, and construct, for each prime number p, infinitely many pairwise non-isomorphic K3 surfaces over $\mathbb{Q}$ whose rational points are p-adically dense. All K3 surfaces constructed in this chapter will be Kummer surfaces. We will give criteria, in terms of an elliptic curve E and a set of primes S, for the density of the rational points on the Kummer surface X of $E \times E$ in the topological space $\prod_{p \in S} X(\mathbb{Q}_p)$. We construct a K3 surface X over $\mathbb{Q}$ whose rational points lie dense in the space $\prod_{p \in S} X(\mathbb{Q}_p)$, where S is a set of 331 primes. We construct a K3 surface over $\mathbb{Q}$ whose rational points are p-adically dense for all p with $p > 7$ and $p \equiv 3 \pmod 4$. Finally, we give a simple not-too-strong condition, in terms of an elliptic curve E over $\mathbb{Q}$, for the p-adic density of the rational points on the Kummer surface of $E \times E$ for infinitely many p.

In chapter 4, we collect more conditions on an elliptic curve E and a prime number p that imply that the rational points on the Kummer surface of $E \times E$ are p-adically dense. We use these additional criteria to perform a computer experiment. A significant result of this experiment is that, for all elliptic curves E over $\mathbb{Q}$ given by $y^2 = x^3 + ax + b$, with $a, b \in \mathbb{Z}$ such that $-5 \leq a \leq 5$ with $a \neq 0$, and $0 < b \leq 5$, if X is the Kummer surface of $E \times E$, then $X(\mathbb{Q})$ is dense in $X(\mathbb{Q}_p)$ for all prime numbers p such that $109 < p < 2000$ and p is of good reduction for E.

In chapter 5, we treat a result of a different nature. At the AIM workshop "Cohomological Methods in Abelian Varieties", held in Palo Alto from 26–30 March 2012, a group of eight people, namely Lisa Berger, Chris Hall, Jennifer Park, Karl Rubin, Shahef Sharif, Alice Silverberg, Doug Ulmer, and the author of this thesis, worked on the task of extending the result [39, Theorem 12.1] to curves of higher genus. In this thesis, we will prove the following result, which is only one among many results obtained by our group. We let K and K_d be as above, we let C be the curve $y^r = x^{r-1}(x+1)(x+t)$ over K for an odd prime r, and we let J be the Jacobian of C. Then the rank of the abelian group $J(K_d)$ is unbounded, more precise, it is at least $d-2$ for infinitely many values of d. Moreover, for the d for which it is shown that the rank of $J(K_d)$ is at least $d-2$, explicit generators of a rank $d-2$ subgroup of $J(K_d)$ are given.

Chapter 1

Elliptic curves with additive reduction over p-adic fields

1.1 Introduction

In this chapter, we fix a prime p. If $E/\mathbb{Q}_p$ is an elliptic curve with additive reduction, and we choose a minimal Weierstrass equation over $\mathbb{Z}_p$ for it:

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \qquad a_i \in \mathbb{Z}_p \text{ for each } i,$$

then we denote by $E_0(\mathbb{Q}_p) \subset E(\mathbb{Q}_p)$ the open subgroup of points that reduce to a non-singular point of the reduced curve. As is well-known, this construction does not depend on the choice of minimal Weierstrass equation.

The purpose of this chapter is to investigate the structure of $E_0(\mathbb{Q}_p)$ as a topological group. We will prove the following theorem. It is slightly less general than the main result of this chapter (Theorem 1.28), but it has the advantage that its statement is more elementary.

Theorem 1.1. *Let $E/\mathbb{Q}_p$ be an elliptic curve with additive reduction, such that it can be given by a minimal Weierstrass equation over $\mathbb{Z}_p$:*

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

where the a_i are contained in $p\mathbb{Z}_p$ for each i. Then the group $E_0(\mathbb{Q}_p)$ is topologically isomorphic to $\mathbb{Z}_p$, except in the following four cases:

(i) $p = 2$ *and* $a_1 + a_3 \equiv 2 \pmod 4$*;*
(ii) $p = 3$ *and* $a_2 \equiv 6 \pmod 9$*;*
(iii) $p = 5$ *and* $a_4 \equiv 10 \pmod{25}$*;*

(iv) $p = 7$ *and* $a_6 \equiv 14 \pmod{49}$.

In each of the cases (i)-(iv), $E_0(\mathbb{Q}_p)$ *is topologically isomorphic to* $p\mathbb{Z}_p \times \mathbb{Z}/p\mathbb{Z}$*, where* $\mathbb{Z}/p\mathbb{Z}$ *has the discrete topology.*

The proof of Theorem 1.1 will be given in section 1.5.5. The case $p > 7$ of Theorem 1.1 was also mentioned in [38].

We will say a few words about the idea of the proof. It is a standard fact from the theory of elliptic curves over local fields [32, VII.6.3] that $E_0(\mathbb{Q}_p)$ admits a canonical filtration

$$E_0(\mathbb{Q}_p) \supset E_1(\mathbb{Q}_p) \supset E_2(\mathbb{Q}_p) \supset E_3(\mathbb{Q}_p) \supset \dots,$$

where for each $i \geq 1$ the quotient $E_i(\mathbb{Q}_p)/E_{i+1}(\mathbb{Q}_p)$ is isomorphic to $\mathbb{Z}/p\mathbb{Z}$. The quotient $E_0(\mathbb{Q}_p)/E_1(\mathbb{Q}_p)$ is also isomorphic to $\mathbb{Z}/p\mathbb{Z}$ by the fact that E has additive reduction. One has a natural isomorphism of topological groups $j\colon E_2(\mathbb{Q}_p) \xrightarrow{\sim} p^2\mathbb{Z}_p$ given by the theory of formal groups. If $p > 2$, the same theory even gives a natural isomorphism $j'\colon E_1(\mathbb{Q}_p) \xrightarrow{\sim} p\mathbb{Z}_p$ [32, IV.6.4(b)]. These isomorphisms identify $E_n(\mathbb{Q}_p)$ with $p^n\mathbb{Z}_p$ for all $n \geq 2$. The idea of the proof of theorem 1.1 is to start from j or j' and, by extending its domain, to build up an isomorphism between $E_0(\mathbb{Q}_p)$ and either $\mathbb{Z}_p$ or $p\mathbb{Z}_p \times \mathbb{Z}/p\mathbb{Z}$.

Rather than elliptic curves over $\mathbb{Q}_p$ with additive reduction, we consider the more general case of Weierstrass curves over $\mathbb{Z}_p$ whose generic fibre is smooth and whose special fibre is a cuspidal cubic curve. This allows more general results. Theorem 1.1 is derived as a special case.

In Section 1.6, we give examples for each prime $2 \leq p \leq 7$ of an elliptic curve $E/\mathbb{Q}$ with additive reduction at p such that $E_0(\mathbb{Q}_p)$ contains a p-torsion point defined over $\mathbb{Q}$.

1.2 Preliminaries on Weierstrass curves

All proofs of facts recalled in this section can be found in [32, Ch. IV, VII].

Let K be a finite field extension of $\mathbb{Q}_p$ for some prime p, and let $v_K\colon K \to \mathbb{Z} \cup \{\infty\}$ be its normalized valuation. Let $\mathcal{O}_K$ be the ring of integers, $\mathfrak{m}_K$ its maximal ideal and k its residue field. By a Weierstrass curve over $\mathcal{O}_K$ we mean a projective curve $\mathcal{E} \subset \mathbb{P}^2_{\mathcal{O}_K}$ defined by a Weierstrass equation

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6. \tag{1.1}$$

If moreover the generic fibre $\mathcal{E}_K$ of $\mathcal{E}$ is an elliptic curve over K with $(0:1:0)$ as the origin, then we call $\mathcal{E}$ a nice Weierstrass curve. The coefficients a_i are uniquely determined by $\mathcal{E}$. The discriminant of $\mathcal{E}$, denoted $\Delta_{\mathcal{E}}$, is defined as in [32, III.1]. The curve $\mathcal{E}$ is said to be minimal if $v_K(\Delta_{\mathcal{E}})$ is minimal among $v_K(\Delta_{\mathcal{E}'})$, where $\mathcal{E}'$ ranges over the Weierstrass curves such that $\mathcal{E}'_K \cong \mathcal{E}_K$.

We will say that a Weierstrass curve $\mathcal{E}/\mathcal{O}_K$ has good reduction when the special fibre $\mathcal{E}_k$ is smooth, multiplicative reduction when $\mathcal{E}_k$ is nodal (i.e. there are two distinct tangent directions to the singular point), and additive reduction when $\mathcal{E}_k$ is cuspidal (i.e. one tangent direction to the singular point). A non-minimal Weierstrass curve has additive reduction. The reduction type of an elliptic curve E over K is defined to be the reduction type of a minimal Weierstrass model of E over $\mathcal{O}_K$, which is a minimal Weierstrass curve $\mathcal{E}/\mathcal{O}_K$ such that $\mathcal{E}_K \cong E$. By the fact that the minimal Weierstrass model of E is unique up to $\mathcal{O}_K$-isomorphism, this is well-defined.

We have $E(K) = \mathcal{E}(K) = \mathcal{E}(\mathcal{O}_K)$ since $\mathcal{E}$ is projective. Therefore, we have a reduction map $E(K) \to \mathcal{E}(k)$ given by restricting an element of $\mathcal{E}(\mathcal{O}_K)$ to the special fibre. By $\mathcal{E}_0(K)$ we denote the subgroup $\mathcal{E}_0(K) \subset \mathcal{E}(K)$ of points reducing to a non-singular point of the special fibre $\mathcal{E}_k$. We define the subgroup $\mathcal{E}_1(K) \subset \mathcal{E}_0(K)$ as the kernel of reduction, i.e. the points that map to the identity of $\mathcal{E}(k)$ under the reduction map. A more explicit definition of $\mathcal{E}_1(K)$ is

$$\mathcal{E}_1(K) = \{(x,y) \in \mathcal{E}(K) : v_K(x) \leq -2, v_K(y) \leq -3\} \cup \{0\}. \tag{1.2}$$

More generally, one defines subgroups $\mathcal{E}_n(K) \subset \mathcal{E}_0(K)$ for $n \geq 1$ as follows:

$$\mathcal{E}_n(K) = \{(x,y) \in \mathcal{E}(K) : v_K(x) \leq -2n, v_K(y) \leq -3n\} \cup \{0\}.$$

We thus have an infinite filtration on the subgroup $\mathcal{E}_1(K)$:

$$\mathcal{E}_1(K) \supset \mathcal{E}_2(K) \supset \mathcal{E}_3(K) \supset \cdots \tag{1.3}$$

For an elliptic curve E/K and an integer $n \geq 0$, we define $E_n(K)$ to be the subgroups of $E(K)$ corresponding to $\mathcal{E}_n(K)$, where $\mathcal{E}$ is a minimal Weierstrass model of E over $\mathcal{O}_K$. The $E_n(K)$ are well-defined, again by the fact that the minimal Weierstrass model of E is unique up to $\mathcal{O}_K$-isomorphism.

Proposition 1.2. *For a nice Weierstrass curve $\mathcal{E}$ over $\mathbb{Z}_p$, there is an exact sequence*

$$0 \to \mathcal{E}_1(K) \to \mathcal{E}_0(K) \to \widetilde{\mathcal{E}}_{\mathrm{sm}}(k) \to 0,$$

where $\widetilde{\mathcal{E}}_{\mathrm{sm}}$ is the complement of the singular points in the special fibre $\widetilde{\mathcal{E}}$.

Proof. This comes down to Hensel's lemma. See [32, VII.2.1]. □

For a nice Weierstrass curve $\mathcal{E}$ over $\mathcal{O}_K$, we can consider its formal group $\widehat{\mathcal{E}}$ [32, IV.1–2]. This is a one-dimensional formal group over $\mathcal{O}_K$. Giving the data of this formal group is the same as giving a power series $F = F_{\widehat{\mathcal{E}}}$ in $\mathcal{O}_K[[X, Y]]$, called the formal group law. It satisfies

$$F(X, Y) = X + Y + (\text{terms of degree} \geq 2)$$

and

$$F(F(X, Y), Z)) = F(X, F(Y, Z)).$$

For $\mathcal{E}$ as in (1.1), the first few terms of F are given by

$$\begin{aligned} F(X,Y) &= X + Y - \\ &a_1XY - a_2(X^2Y + XY^2) - 2a_3(X^3Y + XY^3) + (a_1a_2 - 3a_3)X^2Y^2 - \\ &(2a_1a_3 + 2a_4)(X^4Y + XY^4) - (a_1a_3 - a_2^2 + 4a_4)(X^3Y^2 + X^2Y^3) + \dots \end{aligned}$$

Treating the Weierstrass coefficients a_i as unknowns, we may consider F as an element of $\mathbb{Z}[a_1, a_2, a_3, a_4, a_6][[X, Y]]$ called the generic formal group law. If we make $\mathbb{Z}[a_1, a_2, a_3, a_4, a_6]$ into a weighted ring with weight function wt, such that $\mathrm{wt}(a_i) = i$ for each i, then the coefficients of F in degree n are homogeneous of weight $n-1$ [32, IV.1.1]. For each $n \in \mathbb{Z}_{\geq 2}$, we define power series $[n]$ in $\mathcal{O}_K[[T]]$ by $[2](T) = F(T, T)$ and $[n](T) = F([n-1](T), T)$ for $n \geq 3$. Here also, we may consider each $[n]$ either as a power series in $\mathcal{O}_K[[T]]$ or as a power series in $\mathbb{Z}[a_1, a_2, a_3, a_4, a_6][[T]]$ called the generic multiplication by n law.

Lemma 1.3. *Let $[p] = \sum_n b_n T^n \in \mathbb{Z}[a_1, a_2, a_3, a_4, a_6][[T]]$ be the generic formal multiplication by p law. Then:*

(i) $p \mid b_n$ for all n not divisible by p;
(ii) $\mathrm{wt}(b_n) = n - 1$, considering $\mathbb{Z}[a_1, a_2, a_3, a_4, a_6]$ as a weighted ring as above.

Proof. Part (i) is proved in [32, IV.4.4]. Part (ii) follows from [32, IV.1.1] or what was said above. □

The series $F(u, v)$ converges to an element of $\mathfrak{m}_K$ for all $u, v \in \mathfrak{m}_K$. To $\mathcal{E}$ one associates the group $\widehat{\mathcal{E}}(\mathfrak{m}_K)$, the $\mathfrak{m}_K$-valued points of $\widehat{\mathcal{E}}$, which as a set is just $\mathfrak{m}_K$, and whose group operation $+$ is given by $u + v = F(u, v)$ for all $u, v \in \widehat{\mathcal{E}}(\mathfrak{m}_K)$. The identity element of $\widehat{\mathcal{E}}(\mathfrak{m}_K)$ is $0 \in \mathfrak{m}_K$. If $n \geq 1$ is an

integer, then by $\widehat{\mathcal{E}}(\mathfrak{m}_K^n)$ we denote the subset of $\widehat{\mathcal{E}}(\mathfrak{m}_K)$ corresponding to the subset $\mathfrak{m}_K^n \subset \mathfrak{m}_K$, where $\mathfrak{m}_K^n$ is the nth power of the ideal $\mathfrak{m}_K$ of $\mathcal{O}_K$. The groups $\widehat{\mathcal{E}}(\mathfrak{m}_K^n)$ are subgroups of $\widehat{\mathcal{E}}(\mathfrak{m}_K)$, and we have an infinite filtration of $\widehat{\mathcal{E}}(\mathfrak{m}_K)$:

$$\widehat{\mathcal{E}}(\mathfrak{m}_K) \supset \widehat{\mathcal{E}}(\mathfrak{m}_K^2) \supset \widehat{\mathcal{E}}(\mathfrak{m}_K^3) \supset \cdots \tag{1.4}$$

Proposition 1.4. *The map*

$$\begin{aligned} \psi_K \colon \mathcal{E}_1(K) &\xrightarrow{\sim} \widehat{\mathcal{E}}(\mathfrak{m}_K) \\ (x, y) &\mapsto -x/y \\ 0 &\mapsto 0 \end{aligned}$$

is an isomorphism of topological groups. Moreover, ψ_K respects the filtrations (1.3) and (1.4), i.e. it identifies the subgroups $\mathcal{E}_n(K)$ defined above with $\widehat{\mathcal{E}}(\mathfrak{m}_K^n)$.

Proof. See [32, VII.2.2]. □

It follows from the proof given in [32, VII.2.2] that there exists a power series $w \in \mathcal{O}_K[[T]]$, with the first few terms given by

$$w(T) = T^3 + a_1 T^4 + (a_1^2 + a_2)T^5 + (a_1^3 + 2a_1 a_2 + a_3)T^6 + \ldots,$$

such that the inverse to ψ_K is given by $z \mapsto (z/w(z), -1/w(z))$. Given a finite field extension $K \subset L$, we have an obvious commutative diagram

$$\begin{array}{ccc} \mathcal{E}_1(K) & \xrightarrow{\psi_K} & \widehat{\mathcal{E}}(\mathfrak{m}_K) \\ \Big\downarrow{\scriptstyle \text{incl}} & & \Big\downarrow{\scriptstyle \text{incl}} \\ \mathcal{E}_1(L) & \xrightarrow{\psi_L} & \widehat{\mathcal{E}_{\mathcal{O}_L}}(\mathfrak{m}_L) \end{array}$$

Here $\widehat{\mathcal{E}_{\mathcal{O}_L}}(\mathfrak{m}_L)$ is the set of $\mathfrak{m}_L$-valued points of the formal group of $\mathcal{E}_{\mathcal{O}_L}$, the base-change of $\mathcal{E}$ to $\mathrm{Spec}(\mathcal{O}_L)$.

1.3 Extensions of topological abelian groups

In this section, we investigate the following question. Suppose that d is a non-negative integer, that A and C are finite abelian groups considered

with the discrete topology, and that B is a topological abelian group sitting in a short exact sequence

$$0 \to \mathbb{Z}_p^d \times A \to B \to C \to 0$$

where the maps are continuous, and with the second map an embedding; determine which isomorphism types of topological abelian groups are possible for B. A partial answer, sufficient for the needs of this and later chapters, is given in Proposition 1.14.

1.3.1 The profinite topology

Definition 1.5. Let G be any group. The profinite topology on G is the coarsest topology such that, for all subgroups $H \subset G$ of finite index, the quotient map $G \to G/H$ is continuous.

Proposition 1.6. *Let G be a group. A base $\mathcal{B}$ for the profinite topology on G is obtained by letting $\mathcal{B}$ be the collection of all translates of finite index subgroups of G. Alternatively, a base $\mathcal{B}$ for the profinite topology on G is given by taking a set $\{H_i\}_{i\in I}$ of finite-index subgroups of G that is final among the set of all finite-index subgroups when ordered by inclusion, and letting $\mathcal{B}$ be the collection of the translates of each H_i.*

Proof. The first assertion is clear from the definition. The second one follows since we can write every subgroup H of G as a union of translates of an element H_i of the final set of subgroups $\{H_i\}_{i\in I}$ of G. □

Lemma 1.7. *Let $G = \mathbb{Z}_p$ considered with the p-adic topology.*

(i) The open subgroups of G are the subgroups $p^k\mathbb{Z}_p$ for $k \in \mathbb{Z}_{\geq 0}$.
(ii) The p-adic topology and the profinite topology on G are the same.

Proof. Let $H \subset \mathbb{Z}_p$ be an open subgroup of G. Since G is compact, it is of finite index; let the index of H be n. We write $n = mp^k$ with m not divisible by p. Then we have $p^k\mathbb{Z}_p = n\mathbb{Z}_p \subset H$, so H contains $p^k\mathbb{Z}_p$. The image of H in $\mathbb{Z}_p/p^k\mathbb{Z}_p = \mathbb{Z}/p^k\mathbb{Z}$ must have index n as well: therefore we have $n = p^k$ and $H = p^k\mathbb{Z}_p$. Conversely, it is clear that the subgroups $p^k\mathbb{Z}_p$ of G are open. This proves (i).

The proof of (i) shows that any finite index subgroup of G is of the form $p^k\mathbb{Z}_p$, and therefore open. Hence a base for the profinite topology on G is given by the $p^k\mathbb{Z}_p$ and their translates. The same is true for the p-adic topology. □

Lemma 1.8. *If G_1 and G_2 are topological groups such that their topologies coincide with the profinite topologies, then the same is true for the topological group $G_1 \times G_2$, considered with the product topology.*

Proof. Let $G = G_1 \times G_2$. A base $\mathcal{B}$ for the product topology on G is given by taking bases $\mathcal{B}_1$ and $\mathcal{B}_2$ for the topologies on G_1 and G_2, and defining $\mathcal{B}$ to be the collection of products $U_1 \times U_2$ with $U_i \in \mathcal{B}_i$ for $i \in \{1, 2\}$.

Now we describe the profinite topology on G. Clearly, the set $\mathcal{S}$ of subgroups of the form $H_1 \times H_2$, with H_1 of finite index in G_1 and H_2 of finite index in G_2, is final among the set of all finite-index subgroups of G. By Proposition 1.6, the collection $\mathcal{B}'$ consisting of all translates of elements of $\mathcal{S}$ is a basis for the profinite topology on G. It is now clear that $\mathcal{B}$ and $\mathcal{B}'$ are the same. □

Lemma 1.9. *Let G be a topological group and let $H \subset G$ be an open subgroup of finite index. Assume that the induced topology on H is the profinite one. Then the topology on G is the profinite one.*

Proof. A base $\mathcal{B}$ for the topology on G is given by letting $\mathcal{B}$ consist of all possible translates of a base for the topology of H. If G' has finite index in G, then $G' \cap H$ has finite index in H. Conversely, clearly every finite-index subgroup H' of H is of the form $G' \cap H$ for G' of finite index in G: one can just take $G' = H'$. Subgroups of G of the form $G' \cap H$, with G' of finite index in G, are final among the set of all finite-index subgroups of G. Hence, by Proposition 1.6, if $\mathcal{B}'$ is defined as the union of all translates of subgroups of the form $G' \cap H$ of G, then $\mathcal{B}'$ gives a base for the profinite topology on G. But it is clear that $\mathcal{B}$ and $\mathcal{B}'$ are the same. □

Corollary 1.10. *Let d be a non-negative integer, and let G be a topological group containing $\mathbb{Z}_p^d$, equipped with the p-adic topology, as an open subgroup of finite index. Then G has the profinite topology.*

Proof. By Lemmas 1.7(ii) and 1.8, we have that $\mathbb{Z}_p^d$ has the profinite topology. Lemma 1.9 shows that the same is true for G. □

1.3.2 The extension problem

Lemma 1.11. *Let d be a non-negative integer and let G be $\mathbb{Z}_p^d$. Let $H \subset G$ be a subgroup of finite index. Then H is isomorphic to $\mathbb{Z}_p^d$ as a $\mathbb{Z}_p$-submodule.*

Proof. We use the properties of G as a topological group. Since H is of finite index, it contains $p^n\mathbb{Z}_p^d$ as an open subgroup for some n, and therefore it is open in G. Hence H is also closed in G, which shows that it is actually a $\mathbb{Z}_p$-submodule of G. Since H is finitely generated (since it is the kernel of the map $G \to G/H$ between finitely generated modules over a Noetherian ring) and torsion-free over the local ring $\mathbb{Z}_p$, it is a free $\mathbb{Z}_p$-module, i.e. it is isomorphic to $\mathbb{Z}_p^r$ for some non-negative integer r. Since H contains an isomorphic image of $p^n\mathbb{Z}_p^d$ as a finite-index subgroup, we must have $r = d$. □

Lemma 1.12. *Let p be a prime, d a non-negative integer, and B a finite abelian group. Let $G = \mathbb{Z}_p^d \times B$ and let $H \subset G$ be a subgroup of finite index. Then the following statements are true.*

(i) There exists a subgroup $B' \subset B$ such that H is isomorphic to $\mathbb{Z}_p^d \times B'$.

(ii) Suppose that p does not divide $\#B$. Let $\pi_1 \colon G \to \mathbb{Z}_p^d$ and $\pi_2 \colon G \to B$ be the projections to the first and second factors. Then

$$\begin{aligned} H &\to \pi_1(H) \times \pi_2(H) \\ h &\mapsto (\pi_1(h), \pi_2(h)) \end{aligned}$$

is an isomorphism.

Proof. First we prove (i). Let $\pi_1 \colon G \to \mathbb{Z}_p^d$ be the projection to the first coordinate. Since H has finite index in G, the subgroup $\pi_1(H)$ of $\mathbb{Z}_p^d$ has finite index. By Lemma 1.11, we have that $\pi_1(H)$ is isomorphic to the free $\mathbb{Z}_p$-module $\mathbb{Z}_p^d$, which implies the existence of a section $\sigma \colon \pi_1(H) \to H$ of the restricted map $\pi_1|_H : H \to \pi_1(H)$. We define a map $\pi_2' \colon H \to B$ by $h \mapsto h - \sigma(\pi_1(h)) \in \{0\} \times B$. We claim that

$$\begin{aligned} H &\to \pi_1(H) \times \pi_2'(H) \\ h &\mapsto (\pi_1(h), \pi_2'(h)) \end{aligned}$$

is an isomorphism. Indeed, injectivity is clear, and the surjectivity follows from the fact that π_2' sends an element of the form $h_1 + b$, with $h_1 \in (\sigma \circ \pi_1)(H)$ and $b \in \{0\} \times B$, to b.

To establish (ii), we claim that if p does not divide $\#B$, the map π_2' constructed above is the restriction of the projection $\pi_2 \colon G \to B$ to H. Since $\pi_2|_H$ and π_2' coincide on $\{0\} \times B$, the two maps differ by an element of $\mathrm{Hom}(\pi_1(H), B) \cong \mathrm{Hom}(\mathbb{Z}_p^d, B)$, which is zero by the assumption on B, so the claim follows. Hence $\pi_2' = \pi_2$. Since the argument from the previous paragraph showed that $(\pi_1, \pi_2') \colon H \to \pi_1(H) \times \pi_2'(H)$ is an isomorphism, we are done. □

Lemma 1.13. *Let $0 \to A \to B \xrightarrow{g} C \to 0$ be a short exact sequence of abelian groups, and let $A = A_1 \times A_2$. If we set $B_1 = B/A_2$ and $B_2 = B/A_1$, then for i equal to 1 or 2 we have short exact sequences $0 \to A_i \to B_i \to C \to 0$, and B sits inside the short exact sequence $0 \to B \to B_1 \times B_2 \to C \to 0$, where $B \to B_1 \times B_2$ is the diagonal map.*

Proof. Dividing out $0 \to A \to B \to C \to 0$ by A_i we get,

$$0 \to A_i \to B_i \to C \to 0. \tag{1.5}$$

Taking the sum over the exact sequences (1.5) for $i \in \{1, 2\}$, we get,

$$0 \to A \to B_1 \times B_2 \to C \times C \to 0,$$

with B sitting in the short exact sequence

$$\begin{aligned} 0 \to B \to B_1 \times B_2 \to C \to 0 \\ (b_1, b_2) \mapsto g(b_1) - g(b_2) \end{aligned}$$

This proves the lemma. □

With the next proposition, we answer the question posed at the start of this section. Note that, if B' is a finite abelian group, and $G = \mathbb{Z}_p^d \times B'$ for some non-negative integer d, then B' is uniquely determined by G up to isomorphism, since we have $B' \cong G_{\text{tors}}$.

Proposition 1.14. *Let A and C be finite abelian groups considered with the discrete topology. Let d be a positive integer, let B be a topological abelian group, and let*

$$0 \to \mathbb{Z}_p^d \times A \to B \to C \to 0$$

be a short exact sequence, with continuous maps and with the second map an embedding. Then the following statements are true.

- *(i) We have $B \cong \mathbb{Z}_p^d \times B'$ as topological groups, where B' is a finite abelian group carrying the discrete topology.*
- *(ii) If $A = \{0\}$, then B' is isomorphic to a subgroup of C.*
- *(iii) If $A = \{0\}$ and $C \cong \mathbb{Z}/p\mathbb{Z}$, then B' is isomorphic to $\{0\}$ or to $\mathbb{Z}/p\mathbb{Z}$.*
- *(iv) If p divides neither $\#A$ nor $\#C$, then B' fits inside a short exact sequence $0 \to A \to B' \to C \to 0$.*

Proof. We will show existence of a finite abelian group B'' such that, as a group, B can be embedded as a finite index subgroup of $\mathbb{Z}_p^d \times B''$. By Lemma 1.12, it then follows that B is isomorphic as a group to $\mathbb{Z}_p^d \times B'$ for some subgroup B' of B''. Then, since the topological groups B and $\mathbb{Z}_p^d \times B'$ both have $\mathbb{Z}_p^d$ as a finite-index open subgroup, and since they are isomorphic as groups, by Lemma 1.10 they are isomorphic as topological groups. The existence of B'' thus proves (i).

By Lemma 1.13, there exist groups B_1 and B_2 such that B sits inside a short exact sequence of abelian groups

$$0 \to B \to B_1 \times B_2 \to C \to 0 \tag{1.6}$$

and such that there are further short exact sequences

$$0 \to \mathbb{Z}_p^d \xrightarrow{i} B_1 \xrightarrow{\pi} C \to 0 \tag{1.7}$$

and

$$0 \to A \to B_2 \xrightarrow{\rho} C \to 0. \tag{1.8}$$

Since A and C are finite abelian groups and since B is abelian, we have that B_2 is finite abelian. Furthermore, we may embed B_1 in $\mathbb{Z}_p^d \times C$ by

$$\begin{aligned} f\colon B_1 &\to \mathbb{Z}_p^d \times C \\ b &\mapsto (i^{-1}(nb), \pi(b)) \end{aligned}$$

where $n = \#C$. For the image of $\mathbb{Z}_p^d \subset B_1$ we have $f(\mathbb{Z}_p^d) = n\mathbb{Z}_p^d \times \{0\}$, so $f(B_1)$ has finite index in $\mathbb{Z}_p^d \times C$. Together with (1.6), this shows that B has finite index in $\mathbb{Z}_p^d \times B_2 \times C$. We may thus take B'' to be $B_2 \times C$, which proves (i).

If $A = \{0\}$, then in addition to (1.7),

$$0 \to \mathbb{Z}_p^d \to B_1 \xrightarrow{\pi} C \to 0$$

we have that (1.8) becomes

$$0 \to 0 \to C \xrightarrow{\mathrm{id}} C \to 0.$$

By Lemma 1.13, we have that B sits inside the exact sequence

$$0 \to B \to B_1 \times C \to C \to 0$$

where the map $B_1 \times C \to C$ is given by $(b, c) \mapsto \pi(b) - c$ by Lemma 1.13. This map is split by the obvious section $c \mapsto (0, c)$; hence we have $B \cong B_1$,

which by the previous paragraph is isomorphic to a subgroup of $\mathbb{Z}_p^d \times C$. Part (ii) now follows from Lemma 1.12(i).

Assertion (iii) follows from (ii).

Now the proof of (iv). Since p does not divide $\#C$, Lemma 1.12(ii) shows that B_1 is isomorphic to $\mathbb{Z}_p^d \times C$, and that, moreover, this isomorphism can be chosen in such a way that π corresponds to the projection $\mathbb{Z}_p^d \times C \to C$ to the second factor. From (1.6), we see that B is obtained as the kernel of the surjective map

$$\mathbb{Z}_p^d \times C \times B_2 \to C$$

that sends (x, c, b) to $c - \rho(b)$ by Lemma 1.13. This map has the obvious section $c \mapsto (0, c, 0)$; hence the kernel B is isomorphic to $\mathbb{Z}_p^d \times B_2$. This proves (iv). □

Remark 1.15. By repeatedly applying Proposition 1.14, we see that if we have a finite filtration

$$\mathbb{Z}_p^d = B_n \subset B_{n-1} \subset \ldots \subset B_1$$

of topological groups, in which all quotients are finite abelian groups, then B_1 is torsion-free if and only if it is topologically isomorphic to $\mathbb{Z}_p^d$.

The following is a strengthening of Proposition 1.14 in the case $d = 1$, which will be important for us.

Corollary 1.16. *Suppose we have a short exact sequence*

$$0 \to p\mathbb{Z}_p \xrightarrow{i} X \to \mathbb{Z}/p\mathbb{Z} \to 0$$

of topological abelian groups where the second arrow is a topological embedding. Then the following statements are true.

(i) If X is topologically isomorphic to $\mathbb{Z}_p$, then $v_p(i^{-1}(px)) = 1$ for all $x \in X - i(p\mathbb{Z}_p)$, where v_p is the p-adic valuation.

(ii) If X is not topologically isomorphic to $\mathbb{Z}_p$, it is topologically isomorphic to $p\mathbb{Z}_p \times \mathbb{Z}/p\mathbb{Z}$, and we have $v_p(i^{-1}(px)) > 1$ for all $x \in X - i(p\mathbb{Z}_p)$.

Proof. If X is topologically isomorphic to $\mathbb{Z}_p$, the map i is given by multiplication by some unit $\alpha \in \mathbb{Z}_p^*$ followed by the inclusion $p\mathbb{Z}_p \subset \mathbb{Z}_p$. Assertion (i) follows.

If X is not topologically isomorphic to $\mathbb{Z}_p$, then by Proposition 1.14(iii) we must have $X \cong p\mathbb{Z}_p \times \mathbb{Z}/p\mathbb{Z}$. But then if $x = (y, c)$, we have $v_p(i^{-1}(px)) = v_p(py) > 1$, proving (ii). □

Corollary 1.17. *Suppose that we have an inclusion $H \subset G$ of topological groups, that*

$$0 \to H \xrightarrow{i} G \to \mathbb{Z}/p\mathbb{Z} \to 0$$

is an exact sequence with continuous maps, with i being the inclusion of H in G and $\mathbb{Z}/p\mathbb{Z}$ carrying the discrete topology, and that H is topologically isomorphic to $\mathbb{Z}/p\mathbb{Z}$. If G is topologically isomorphic to $\mathbb{Z}_p$, then $pG = H$, and any topological isomorphism $\phi\colon H \xrightarrow{\sim} p\mathbb{Z}_p$ extends to a topological isomorphism $\widetilde{\phi}\colon G \xrightarrow{\sim} \mathbb{Z}_p$.

Proof. If G is isomorphic to $\mathbb{Z}_p$, then it follows from Corollary 1.16 that $pG = H$. Furthermore, fixing topological isomorphisms $\phi\colon H \xrightarrow{\sim} p\mathbb{Z}_p$ and $\phi'\colon G \xrightarrow{\sim} \mathbb{Z}_p$, we get a commutative diagram

$$\begin{array}{ccc} H & \xrightarrow{\phi} & p\mathbb{Z}_p \\ \downarrow & & \vdots\, a \\ G & \xrightarrow{\phi'} & \mathbb{Z}_p \end{array}$$

where the dotted map is defined as $a = \phi^{-1} \circ i \circ \phi'$, making the diagram commute. Since a is continuous, there is $\alpha \in \mathbb{Z}_p^*$ such that for all $x \in p\mathbb{Z}_p$ we have $a(x) = \alpha x \in \mathbb{Z}_p$. Then $\widetilde{\phi} = \alpha^{-1}\phi'$ is the desired lift of ϕ. □

1.4 Weierstrass curves with additive reduction

Let K be a finite extension of $\mathbb{Q}_p$. Let $\mathcal{O}_K$ again be the ring of integers of K, with maximal ideal $\mathfrak{m}_K$ and residue field k.

In this section, we gather some general properties of nice Weierstrass curves over $\mathcal{O}_K$ with additive reduction.

Lemma 1.18. *Let $\mathcal{E}/\mathcal{O}_K$ be a Weierstrass curve with additive reduction. Then $\mathcal{E}$ is $\mathcal{O}_K$-isomorphic to a Weierstrass curve of the form*

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

where all a_i lie in $\mathfrak{m}_K$.

Proof. We construct an automorphism $\alpha \in \mathrm{PGL}_3(\mathcal{O}_K)$ that maps $\mathcal{E}$ to a Weierstrass curve of the desired form. Consider a translation $\alpha_1 \in$

$\mathrm{PGL}_3(\mathcal{O}_K)$ moving the singular point of the special fibre $\mathcal{E}_k$ to $(0:0:1)$. The image $\mathcal{E}_1 = \alpha_1(\mathcal{E})$ is a Weierstrass curve with coefficients satisfying a_3, a_4, a_6 in $\mathfrak{m}_K$. There exists a second automorphism $\alpha_2 \in \mathrm{PGL}_3(\mathcal{O}_K)$, of the form $x' = x, y' = y + cx$, such that in the special fibre of $\alpha_2(\mathcal{E}_1)$ the unique tangent at $(0:0:1)$ is given by $y' = 0$. The Weierstrass curve $\mathcal{E}_2 = \alpha_2(\mathcal{E}_1)$ now has all its coefficients a_1, a_2, a_3, a_4, a_6 in $\mathfrak{m}_K$. One may thus take $\alpha = \alpha_2 \circ \alpha_1$. □

Suppose that $\mathcal{E}/\mathcal{O}_K$ is a nice Weierstrass curve given by (1.1), and suppose that the a_i are contained in $\mathfrak{m}_K$. In particular, $\mathcal{E}$ has additive reduction. If we let F denote the formal group law of $\mathcal{E}$, then the assumption on the a_i implies that $F(u, v)$ converges to an element of $\mathcal{O}_K$ for all $u, v \in \mathcal{O}_K$. Hence F can be seen to induce a group structure on $\mathcal{O}_K$, extending the group structure on $\widehat{\mathcal{E}}(\mathfrak{m}_K)$. The same statement holds true when we replace K by a finite field extension L.

Definition 1.19. Let $\mathcal{E}/\mathcal{O}_K$ be a nice Weierstrass curve given by (1.1), and assume that the a_i are contained in $\mathfrak{m}_K$. For any finite field extension $K \subset L$, we denote by $\widehat{\mathcal{E}}(\mathcal{O}_L)$ the topological group obtained by endowing the space $\mathcal{O}_L$ with the group structure induced by F.

The following proposition will be fundamental in determining the structure of $\mathcal{E}_0(\mathbb{Q}_p)$ as a topological group for nice Weierstrass curves with additive reduction.

Proposition 1.20. *Let $\mathcal{E}/\mathcal{O}_K$ be a nice Weierstrass curve given by (1.1), and assume that the a_i are contained in $\mathfrak{m}_K$.*

(i) The map $\Psi\colon \mathcal{E}_0(K) \to \widehat{\mathcal{E}}(\mathcal{O}_K)$ that sends (x, y) to $-x/y$ is an isomorphism of topological groups.

(ii) If $6e(K/\mathbb{Q}_p) < p - 1$, where e denotes the ramification degree, then $\mathcal{E}_0(K)$ is also topologically isomorphic to $\mathcal{O}_K$ equipped with the usual group structure.

Proof. Let π be a uniformizer for $\mathcal{O}_K$. Consider the field extension $L = K(\rho)$ with $\rho^6 = \pi$. Then define the Weierstrass curve $\mathcal{D}$ over $\mathcal{O}_L$ by

$$y^2 + \alpha_1 xy + \alpha_3 y = x^3 + \alpha_2 x^2 + \alpha_4 x^4 x + \alpha_6,$$

where $\alpha_i = a_i/\rho^i$. There is a birational map $\phi\colon \mathcal{E} \times_{\mathcal{O}_K} \mathcal{O}_L \dashrightarrow \mathcal{D}$, given by $\phi(x, y) = (x/\rho^2, y/\rho^3)$. The birational map ϕ induces an isomorphism on generic fibres, and hence a homeomorphism between $\mathcal{E}(L)$ and $\mathcal{D}(L)$. Using

(1.2) and the fact that we have $(x, y) \in \mathcal{E}_0(L)$ if and only if $v_L(x), v_L(y)$ are both not greater than zero, one sees that ϕ induces a bijection $\mathcal{E}_0(L) \xrightarrow{\sim} \mathcal{D}_1(L)$, that all maps (*a priori* just of sets) in the following diagram are well-defined, and that the diagram commutes:

$$\begin{array}{ccccccc} \mathcal{E}_1(K) & \xrightarrow{\text{incl}} & \mathcal{E}_0(K) & \xrightarrow{\text{incl}} & \mathcal{E}_0(L) & \xrightarrow{\phi} & \mathcal{D}_1(L) \\ \downarrow{\scriptstyle \psi_K} & & \downarrow{\scriptstyle \Psi} & & \downarrow{\scriptstyle \Psi_L} & & \downarrow{\scriptstyle \psi_L} \\ \widehat{\mathcal{E}}(\mathfrak{m}_K) & \xrightarrow{\text{incl}} & \widehat{\mathcal{E}}(\mathcal{O}_K) & \xrightarrow{\text{incl}} & \widehat{\mathcal{E}}(\mathcal{O}_L) & \xrightarrow{\cdot\rho} & \widehat{\mathcal{D}}(\mathfrak{m}_L) \end{array}$$

Here the map $\Psi_L \colon \mathcal{E}_0(L) \to \mathcal{O}_L$ is defined by $(x, y) \mapsto -x/y$, the rightmost lower horizontal arrow is multiplication by ρ, and the maps labeled incl are the obvious inclusions. Note that the horizontal and vertical outer maps are all continuous. Since ψ_L, ϕ and multiplication by ρ are homeomorphisms (for ψ_L one uses Proposition 1.4), so is Ψ_L. Hence Ψ must be a homeomorphism onto its image. By Galois theory, Ψ is surjective, so it is itself a homeomorphism.

Let $F_{\widehat{\mathcal{D}}}$ be the formal group law of $\mathcal{D}$. One calculates that

$$\rho F(X, Y) = F_{\widehat{\mathcal{D}}}(\rho X, \rho Y).$$

Hence all maps in the diagram are group homomorphisms. This proves the first part of the proposition.

Now assume $6e(K/\mathbb{Q}_p) < p - 1$, so that $v_L(p) = 6v_K(p) = 6e(K/\mathbb{Q}_p) < p - 1$. Now [32, IV.6.4(b)] implies that $\mathcal{E}_1(K)$ is topologically isomorphic to $\mathfrak{m}_K$, and $\mathcal{D}_1(L)$ to $\mathfrak{m}_L$. Since $\mathcal{E}$ has additive reduction, we have $\widetilde{\mathcal{E}}_{\text{sm}}(k) \cong k^+ \cong (\mathbb{Z}/p\mathbb{Z})^f$, where $f = f(K/\mathbb{Q}_p)$ is the inertia degree of $K/\mathbb{Q}_p$ and $\widetilde{\mathcal{E}}_{\text{sm}}$ is the smooth locus of the special fibre of $\mathcal{E}$. Proposition 1.2 shows we have a short exact sequence

$$0 \to \mathfrak{m}_K \to \mathcal{E}_0(K) \to (\mathbb{Z}/p\mathbb{Z})^f \to 0.$$

In the diagram above, the topological group $\mathcal{E}_0(K)$ is mapped homomorphically into the torsion-free group $\mathcal{D}_1(L)$, hence it is itself torsion-free. It follows from Remark 1.15 that $\mathcal{E}_0(K)$ is topologically isomorphic to $\mathcal{O}_K$. This proves the second part. □

The following corollary is worth noting, but will not be used in what follows.

Corollary 1.21. *Let $\mathcal{E}/\mathcal{O}_K$ be a nice Weierstrass curve with additive reduction. If $6e(K/\mathbb{Q}_p) < p-1$, then $\mathcal{E}_0(K)$ is topologically isomorphic to $\mathcal{O}_K$.*

Proof. The statement that $\mathcal{E}_0(K)$ is topologically isomorphic to $\mathcal{O}_K$ only depends on the $\mathcal{O}_K$-isomorphism class of $\mathcal{E}$. By Lemma 1.18, there exists a Weierstrass curve $\mathcal{E}'$ with $a_i \in \mathfrak{m}_K$ that is $\mathcal{O}_K$-isomorphic to $\mathcal{E}$. Now apply Proposition 1.20 to $\mathcal{E}'$. □

1.5 Proof of the main theorem

In this section, we gather some general properties of nice Weierstrass curves over $\mathbb{Z}_p$ with additive reduction and finish the proof of Theorem 1.1.

Lemma 1.22. *Let $\mathcal{E}/\mathbb{Z}_p$ be a nice Weierstrass curve with additive reduction. Then there exists a topological isomorphism $\chi\colon \widehat{\mathcal{E}}(p\mathbb{Z}_p) \xrightarrow{\sim} p\mathbb{Z}_p$ that, for all $n \in \mathbb{Z}_{\geq 1}$, identifies $\widehat{\mathcal{E}}(p^n\mathbb{Z}_p)$ with $p^n\mathbb{Z}_p$.*

Proof. For $p > 2$, this is standard; the proof may be found in [32, IV.6.4(b)]. We now treat the case $p = 2$. By Lemma 1.18, we may assume that the Weierstrass coefficients a_i of $\mathcal{E}$ all lie in $2\mathbb{Z}_2$. The multiplication by 2 on $\widehat{\mathcal{E}}(2\mathbb{Z}_2)$ is given by the power series

$$[2](T) = F_{\widehat{\mathcal{E}}}(T,T) = 2T - a_1T^2 - 2a_2T^3 + (a_1a_2 - 7a_3)T^4 - \dots, \qquad (1.9)$$

where $F_{\widehat{\mathcal{E}}}$ is the formal group law of $\mathcal{E}$. By [32, IV.3.2(a)], $\widehat{\mathcal{E}}(2\mathbb{Z}_2)/\widehat{\mathcal{E}}(4\mathbb{Z}_2)$ is cyclic of order 2. By [32, IV.6.4(b)], there exists a topological isomorphism $\widehat{\mathcal{E}}(4\mathbb{Z}_2) \xrightarrow{\sim} 4\mathbb{Z}_2$. Hence there exists an extension

$$0 \to 4\mathbb{Z}_2 \xrightarrow{i} \widehat{\mathcal{E}}(2\mathbb{Z}_2) \to \mathbb{Z}/2\mathbb{Z} \to 0.$$

From Proposition 1.14 we see that $\widehat{\mathcal{E}}(2\mathbb{Z}_2)$ is topologically isomorphic either to $2\mathbb{Z}_2$ or to $4\mathbb{Z}_2 \times \mathbb{Z}/2\mathbb{Z}$. Assume that the latter is the case, then there is an element z of order 2 in $\widehat{\mathcal{E}}(2\mathbb{Z}_2)$ that is not contained in $\widehat{\mathcal{E}}(4\mathbb{Z}_2)$. For such a z we have $v_2(z) = 1$, where $v_2\colon \widehat{\mathcal{E}}(2\mathbb{Z}_2) \to \mathbb{Z}_{\geq 1} \cup \{\infty\}$ is the 2-adic valuation on the underlying set $2\mathbb{Z}_2$ of $\widehat{\mathcal{E}}(2\mathbb{Z}_2)$. Using that in the duplication power series (1.9) we have $a_i \in 2\mathbb{Z}_2$ for each i, it follows that $v_2([2](z)) = 2$, so $[2](z) \neq 0$. This is a contradiction, so there exists an isomorphism $\chi\colon \widehat{\mathcal{E}}(2\mathbb{Z}_2) \xrightarrow{\sim} 2\mathbb{Z}_2$ as topological groups. From this, and from the fact that $\widehat{\mathcal{E}}(2^n\mathbb{Z}_2)/\widehat{\mathcal{E}}(2^{n+1}\mathbb{Z}_2) \cong \mathbb{Z}/2\mathbb{Z}$ for all $n \in \mathbb{Z}_{\geq 1}$ [32, IV.3.2(a)], we see that χ necessarily respects the filtrations on either side. □

Corollary 1.23. *Let $\mathcal{E}/\mathbb{Z}_p$ be a nice Weierstrass curve with additive reduction. Then there exists an isomorphism $\mathcal{E}_1(\mathbb{Q}_p) \xrightarrow{\sim} p\mathbb{Z}_p$ which for $n \in \mathbb{Z}_{\geq 1}$ identifies $\mathcal{E}_n(\mathbb{Q}_p)$ with $p^n\mathbb{Z}_p$.*

Proof. Such an isomorphism can be obtained by composing the isomorphism χ from Lemma 1.22 with the isomorphism $\psi_{\mathbb{Q}_p}$ from Proposition 1.4. □

1.5.1 The case $p = 2$

Proposition 1.24. *Let $\mathcal{E}/\mathbb{Z}_2$ be a nice Weierstrass curve with its coefficients a_i in $2\mathbb{Z}_2$. Then $\mathcal{E}_0(\mathbb{Q}_2)$ is topologically isomorphic to $\mathbb{Z}_2$ if $a_1+a_3 \equiv 0 \pmod 4$, and to $2\mathbb{Z}_2 \times \mathbb{Z}/2\mathbb{Z}$ otherwise.*

Proof. Proposition 1.2 shows that there is a short exact sequence

$$0 \to \mathcal{E}_1(\mathbb{Q}_2) \to \mathcal{E}_0(\mathbb{Q}_2) \to \mathbb{Z}/2\mathbb{Z} \to 0.$$

By Lemma 1.22, we have $\mathcal{E}_1(\mathbb{Q}_2) \cong 2\mathbb{Z}_2$, so Proposition 1.14 implies that $\mathcal{E}_0(\mathbb{Q}_2)$ is topologically isomorphic either to $\mathbb{Z}_2$ or to $2\mathbb{Z}_2 \times \mathbb{Z}/2\mathbb{Z}$.

Let $[2](T) \in \mathcal{O}_K[[T]]$ be the formal duplication formula (1.9) on $\mathcal{E}$. Let Ψ be the map from Proposition 1.20. Since Ψ is an isomorphism of topological groups, we have for all $P \in \mathcal{E}_0(\mathbb{Q}_2)$:

$$\Psi(2P) = [2](\Psi(P)). \tag{1.10}$$

By Corollary 1.16, we have $\mathcal{E}_0(\mathbb{Q}_2) \cong \mathbb{Z}_2$ if and only if for all $P \in \mathcal{E}_0(\mathbb{Q}_2) - \mathcal{E}_1(\mathbb{Q}_2)$ we have $2P \in \mathcal{E}_1(\mathbb{Q}_2) - \mathcal{E}_2(\mathbb{Q}_2)$, which by (1.10) is true if and only if for all $z \in \widehat{\mathcal{E}}(\mathbb{Z}_2) - \widehat{\mathcal{E}}(2\mathbb{Z}_2)$ we have $v_2([2](z)) = 1$, where $v_2\colon \widehat{\mathcal{E}}(\mathbb{Z}_2) \to \mathbb{Z}_{\geq 0} \cup \{\infty\}$ is the 2-adic valuation on the underlying set $\mathbb{Z}_2$ of $\widehat{\mathcal{E}}(\mathbb{Z}_2)$. This condition may be checked using the duplication power series

$$[2](T) = 2T - a_1T^2 - 2a_2T^3 + (a_1a_2 - 7a_3)T^4 - \ldots = \sum_{i=1}^{\infty} b_iT^i.$$

In deciding whether $v_2([2](z)) = 1$ for $z \in \widehat{\mathcal{E}}(\mathbb{Z}_2) - \widehat{\mathcal{E}}(2\mathbb{Z}_2)$, we do not need to consider those parts of terms whose coefficients have valuation ≥ 2. The non-linear parts of each coefficient b_i will contribute only terms with valuation ≥ 2, so may ignore these and keep only the linear parts. The terms b_iz^i with i odd and greater than 1 we may discard altogether; by Lemma 1.3, all their coefficients have valuation ≥ 2. Finally, we may discard all terms b_iz^i with i even and ≥ 6: a polynomial in $\mathbb{Z}[a_1, \ldots, a_6]$ whose weight

is odd and at least 5 does not contain a linear term (there being no a_5), so the terms involving $z^6, z^8, z^{10}, \ldots$ will have valuation ≥ 2.

We thus get that, if $z \in \widehat{\mathcal{E}}(\mathbb{Z}_2) - \widehat{\mathcal{E}}(2\mathbb{Z}_2)$,

$$v_2([2](z)) = 1 \quad \Leftrightarrow \quad v_2(2z - a_1 z^2 - 7a_3 z^4) = 1.$$

The last statement is true for all $z \in \widehat{\mathcal{E}}(\mathbb{Z}_2) - \widehat{\mathcal{E}}(2\mathbb{Z}_2)$ if and only if

$$v_2\left(z - \frac{a_1}{2}z^2 - \frac{7a_3}{2}z^4\right) = 0 \Leftrightarrow a_1 + 7a_3 \equiv 0 \bmod 4 \Leftrightarrow a_1 + a_3 \equiv 0 \bmod 4$$

since $z \equiv z^2 \equiv z^4 \pmod 2$. This proves the proposition. □

1.5.2 The case $p = 3$

Proposition 1.25. *Let $\mathcal{E}/\mathbb{Z}_3$ be a nice Weierstrass curve with its coefficients a_i in $3\mathbb{Z}_3$. Then $\mathcal{E}_0(\mathbb{Q}_3)$ is topologically isomorphic to $\mathbb{Z}_3$ if $a_2 \not\equiv 6 \pmod 9$, and to $3\mathbb{Z}_3 \times \mathbb{Z}/3\mathbb{Z}$ otherwise.*

Proof. We proceed as in the proof of Proposition 1.24, using the formal triplication formula:

$$[3](T) = 3T - 3a_1T^2 + (a_1^2 - 8a_2)T^3 + (12a_1a_2 - 39a_3)T^4 + \ldots = \sum_{i=1}^{\infty} b_i T^i. \tag{1.11}$$

We consider the usual exact sequence for $\mathcal{E}_0(\mathbb{Q}_3)$:

$$0 \to \mathcal{E}_1(\mathbb{Q}_3) \to \mathcal{E}_0(\mathbb{Q}_3) \to \mathbb{Z}/3\mathbb{Z} \to 0.$$

We see from $\mathcal{E}_1(\mathbb{Q}_3) \cong 3\mathbb{Z}_3$ and Corollary 1.16 that $\mathcal{E}_0(\mathbb{Q}_3)$ is topologically isomorphic to $3\mathbb{Z}_3 \times \mathbb{Z}/3\mathbb{Z}$ if and only if for all elements $z \in \widehat{\mathcal{E}}(\mathbb{Z}_3) - \widehat{\mathcal{E}}(3\mathbb{Z}_3)$, $[3](z)$ has valuation greater than 1. On the other hand, $\mathcal{E}_0(\mathbb{Q}_3)$ is topologically isomorphic to $\mathbb{Z}_3$ if for all such z, the valuation of $[3](z)$ is 1. Reasoning as in the proof of Proposition 1.24, we see that we may ignore all terms whose degree is not 1 and not a multiple of 3, since these have coefficients divisible by 3 and of positive weight. Also we may ignore the terms of degree both equal to a multiple of 3 and greater than 3, since their coefficients do not contain parts that are linear in $a_1, \ldots, a_6$. Finally, we may ignore the non-linear part of the term of degree 3. We see that for $z \in \widehat{\mathcal{E}}(\mathbb{Z}_3) - \widehat{\mathcal{E}}(3\mathbb{Z}_3)$, we have

$$v_3([3](z)) = 1 \quad \Leftrightarrow \quad v_3(3z - 8a_2z^3) = 1.$$

The last statement is true for all such z if and only if

$$v_3\left(z - \frac{8a_2}{3}z^3\right) = 0 \Leftrightarrow 1 - \frac{8a_2}{3} \not\equiv 0 \bmod 3 \Leftrightarrow a_2 \not\equiv 6 \bmod 9$$

since $z \equiv z^3 \pmod 3$. This proves the proposition. □

1.5.3 The case $p = 5$

Proposition 1.26. *Let $\mathcal{E}/\mathbb{Z}_5$ be a nice Weierstrass curve with its coefficients a_i in $5\mathbb{Z}_5$. Then $\mathcal{E}_0(\mathbb{Q}_5)$ is topologically isomorphic to $\mathbb{Z}_5$ if $a_4 \not\equiv 10 \pmod{25}$, and to $5\mathbb{Z}_5 \times \mathbb{Z}/5\mathbb{Z}$ otherwise.*

Proof. For simplicity, we give the formal multiplication by 5 power series in the case where a_1, a_2, a_3 are zero:

$$[5](T) = 5T - 1248a_4T^5 + \ldots = \sum_{i=1}^{\infty} b_iT^i \tag{1.12}$$

This formula suffices for our purposes, since the same arguments as in the proofs of Propositions 1.24 and 1.25 show that the terms that are canceled by setting $a_1 = a_2 = a_3 = 0$ could have been ignored anyway.

We apply Corollary 1.16 to:

$$0 \to 5\mathbb{Z}_5 \to \mathcal{E}_0(\mathbb{Q}_5) \to \mathbb{Z}/5\mathbb{Z} \to 0.$$

In (1.12) we may ignore terms of degree not equal to 1 or 5, by the same reasoning as in the proofs of Propositions 1.24 and 1.25. We see that for $z \in \widehat{\mathcal{E}}(\mathbb{Z}_5) - \widehat{\mathcal{E}}(5\mathbb{Z}_5)$ we have

$$v_5([5](z)) = 1 \quad \Leftrightarrow \quad v_5(5z - 1248a_4z^5) = 1.$$

The last statement is true for all such z if and only if

$$v_5\left(z - \frac{1248a_4}{5}z^5\right) = 0 \Leftrightarrow 1 - \frac{1248a_4}{5} \not\equiv 0 \bmod 5 \Leftrightarrow a_4 \not\equiv 10 \bmod 25$$

since $z \equiv z^5 \pmod 5$. This proves the proposition. □

1.5.4 The case $p = 7$

Proposition 1.27. *Let $\mathcal{E}/\mathbb{Z}_7$ be a nice Weierstrass curve with its coefficients a_i in $7\mathbb{Z}_7$. Then $\mathcal{E}_0(\mathbb{Q}_7)$ is topologically isomorphic to $\mathbb{Z}_7$ if $a_6 \not\equiv 14 \pmod{49}$, and to $7\mathbb{Z}_7 \times \mathbb{Z}/7\mathbb{Z}$ otherwise.*

Proof. For simplicity, we give the formal multiplication by 7 power series with a_1, a_2, a_3 set to zero:

$$[7](T) = 7T - 6720a_4T^5 - 352944a_6T^7 + \dots \tag{1.13}$$

As before, the terms that have disappeared as a result could have been ignored anyway.

We apply Corollary 1.16 to:

$$0 \to 7\mathbb{Z}_7 \to \mathcal{E}_0(\mathbb{Q}_7) \to \mathbb{Z}/7\mathbb{Z} \to 0,$$

In (1.13) we may ignore terms of degree not equal to 1 or 7, by the same reasoning as in the proofs of Propositions 1.24 and 1.25. We see that for $z \in \widehat{\mathcal{E}}(\mathbb{Z}_7) - \widehat{\mathcal{E}}(7\mathbb{Z}_7)$ we have

$$v_7([7](z)) = 1 \quad \Leftrightarrow \quad v_7(7z - 352944a_6z^7) = 1.$$

The last statement is true for all such z if and only if

$$v_7\left(z - \frac{352944a_6}{7}z^7\right) = 0 \Leftrightarrow 1 - \frac{352944a_6}{7} \not\equiv 0 \bmod 7 \Leftrightarrow a_6 \not\equiv 14 \bmod 49$$

since $z \equiv z^7 \pmod 7$. This proves the proposition. □

1.5.5 The proof

We are now ready to derive Theorem 1.1 from our previous results. In fact, we state a more general version of that theorem, since it is also valid for non-minimal Weierstrass equations.

Theorem 1.28. *Let $\mathcal{E}/\mathbb{Z}_p$ be a nice Weierstrass curve given by*

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

where the a_i are contained in $p\mathbb{Z}_p$ for each i. Then there is a topological isomorphism between $\mathcal{E}_0(\mathbb{Q}_p)$ and $\mathbb{Z}_p$, except in the following four cases:

(i) $p = 2$ *and* $a_1 + a_3 \equiv 2 \pmod 4$*;*
(ii) $p = 3$ *and* $a_2 \equiv 6 \pmod 9$*;*
(iii) $p = 5$ *and* $a_4 \equiv 10 \pmod{25}$*;*
(iv) $p = 7$ *and* $a_6 \equiv 14 \pmod{49}$*.*

Moreover, every isomorphism between $\mathcal{E}_0(\mathbb{Q}_p)$ *and* $\mathbb{Z}_p$ *identifies* $\mathcal{E}_n(\mathbb{Q}_p)$ *with* $p^n\mathbb{Z}_p$ *for all* $n \in \mathbb{Z}_{\geq 0}$*. In each of the cases (i)-(iv),* $\mathcal{E}_0(\mathbb{Q}_p)$ *is topologically isomorphic to* $p\mathbb{Z}_p \times \mathbb{Z}/p\mathbb{Z}$*, where* $\mathbb{Z}/p\mathbb{Z}$ *has the discrete topology.*

Proof. The isomorphism type of $\mathcal{E}_0(\mathbb{Q}_p)$ follows from applying part (ii) of Proposition 1.20 if $p > 7$, or one of Propositions 1.24–1.27 if $p \leq 7$.

We claim that, if $\mathcal{E}_0(\mathbb{Q}_p) \cong \mathbb{Z}_p$, then the isomorphism can be chosen in such a way that $\mathcal{E}_n(\mathbb{Q}_p)$ is identified with $p^n\mathbb{Z}_p$ for all $n \in \mathbb{Z}_{\geq 0}$. For this, we choose the topological isomorphism $\chi\colon \mathcal{E}_1(\mathbb{Q}_p) \xrightarrow{\sim} p\mathbb{Z}_p$ from Lemma 1.22. By Corollary 1.17, the map χ extends to a topological isomorphism

$$\widetilde{\chi}\colon \mathcal{E}_0(\mathbb{Q}_p) \xrightarrow{\sim} \mathbb{Z}_p$$

and we have $p\mathcal{E}_0(\mathbb{Q}_p) = \mathcal{E}_1(\mathbb{Q}_p)$. It follows from Lemma 1.22 that $p^n\mathcal{E}_0(\mathbb{Q}_p)$ equals $\mathcal{E}_n(\mathbb{Q}_p)$; hence *every* group isomorphism $\mathcal{E}_0(\mathbb{Q}_p) \xrightarrow{\sim} \mathbb{Z}_p$ will identify $\mathcal{E}_n(\mathbb{Q}_p)$ with $p^n\mathbb{Z}_p$. This concludes the proof. □

Proof of Theorem 1.1. Theorem 1.1 follows by applying Theorem 1.28 to a minimal Weierstrass equation of E

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

where the a_i are contained in $p\mathbb{Z}_p$ for each i. Such an equation exists by Lemma 1.18. □

1.6 Examples

In this section, we have collected some examples of elliptic curves over $\mathbb{Q}_p$ with additive reduction, such that their points of good reduction contains a p-torsion point. All curves and torsion points in these examples are defined over $\mathbb{Q}$. The fact that they possess a p-torsion point of good reduction can be verified using the appropriate result from the previous section.

Example 1.29. The elliptic curve

$$E_2\colon y^2 - 2y = x^3 - 2$$

has additive reduction at 2, and its 2-torsion point $(1, 1)$ is of good reduction.

Example 1.30. The elliptic curve

$$E_3 \colon y^2 = x^3 - 3x^2 + 3x$$

has additive reduction at 3, and its 3-torsion point $(1, 1)$ is of good reduction.

Example 1.31. The elliptic curve

$$E_5 \colon y^2 - 5y = x^3 + 20x^2 - 15x$$

has additive reduction at 5, and its 5-torsion point $(1, -1)$ is of good reduction.

Example 1.32. The elliptic curve

$$E_7 \colon y^2 + 7xy - 28y = x^3 + 7x - 35$$

has additive reduction at 7, and its 7-torsion point $(2, 1)$ is of good reduction.

Chapter 2

Density results for diagonal quartic surfaces

For $c \in \mathbb{Q}^*$, let V_c be the smooth quartic surface in $\mathbb{P}^3_{\mathbb{Q}}$ given by

$$x_0^4 + cx_1^4 = x_2^4 + cx_3^4. \tag{2.1}$$

Let $\mathbb{Q}_2$ denote the field of 2-adic numbers, let $\mathbb{Z}_2 \subset \mathbb{Q}_2$ denote the ring of 2-adic integers, and let $v\colon \mathbb{Q}_2 \to \mathbb{Z} \cup \{\infty\}$ denote the 2-adic valuation, using the convention $v(0) = \infty$. We will call a 2-adic integer a odd if $v(a) = 0$; otherwise we will call it even.

The main result discussed in this chapter is the following theorem, due to Sir Peter Swinnerton-Dyer.

Theorem 2.1 (Swinnerton-Dyer, 2010)**.** *Let c be 2 or 4. The set $V_c(\mathbb{Q})$ lies dense in $V_c(\mathbb{Q}_2)$, when this set is equipped with the 2-adic topology.*

The reasons for including a discussion of Swinnerton-Dyer's theorem in this thesis are twofold. Since this thesis is concerned with results concerning p-adic density of rational points on K3 surfaces, and since Swinnerton-Dyer's result was the first such result to appear for any K3 surface and for any p, it provides an important example of how such a result is arrived at. Secondly, we have striven to provide more details in our proof, and incorporate some minor improvements over the proof of Swinnerton-Dyer. For example, most of our results are stated for arbitrary values of c, whereas Swinnerton-Dyer restricts to $c \in \{2, 4, 8\}$ (although his methods clearly would have allowed him to go beyond this). Using this, we prove Theorem 2.1 for more values of c than Swinnerton-Dyer.

In our proof of Theorem 2.1, we will follow the arguments of Swinnerton-Dyer [38] in the main. The proof will be given in section 2.8.

2.1 Some open subsets of $V_c(\mathbb{Q}_2)$

We start by defining some open sets of $V_c(\mathbb{Q}_2)$. We use them to reduce the proof of density of $V_c(\mathbb{Q})$ in $V_c(\mathbb{Q}_2)$ to the proof of density of $V_c(\mathbb{Q})$ in many smaller open subsets.

Definition 2.2. For any $c \in \mathbb{Q}^*$, let $\mathcal{U}_c \subset V_c(\mathbb{Q}_2)$ be the open subset of 2-adic points that have representatives $(a_0 : a_1 : a_2 : a_3)$ where the a_i are 2-adic integers such that a_0 and a_2 are both odd.

Proposition 2.3. *Let $c \in \mathbb{Q}$ be such that $1 \leq v(c) \leq 3$. If the rational points on V_c lie dense in $\mathcal{U}_c$ and the rational points on $V_{16/c}$ lie dense in $\mathcal{U}_{16/c}$, then $V_c(\mathbb{Q})$ lies dense in $V_c(\mathbb{Q}_2)$ and $V_{16/c}(\mathbb{Q})$ lies dense in $V_{16/c}(\mathbb{Q}_2)$.*

Proof. Suppose that $(a_0 : a_1 : a_2 : a_3)$ defines a point in $V_c(\mathbb{Q}_2)$, where the a_i are 2-adic integers that do not all have positive valuation. Then it follows from (2.1) and the assumption on c that either a_0, a_2 are both odd, or a_0, a_2 are both even and a_1, a_3 are both odd. Moreover, there is an isomorphism between V_c and $V_{16/c}$ defined as follows

$$\begin{aligned} \psi_c \colon V_c &\to V_{16/c} \\ (x_0 : x_1 : x_2 : x_3) &\mapsto (x_1 : \frac{x_0}{2} : x_3 : \frac{x_2}{2}) \end{aligned}$$

We see from this that either a_0 and a_2 are both odd, or we have that $\psi_c(a_0 : a_1 : a_2 : a_3) \in V_{16/c}(\mathbb{Q}_2)$ has a representative $(a_0' : a_1' : a_2' : a_3')$ where the a_i' are 2-adic integers such that a_0' and a_2' are both odd. So for $P \in V_c(\mathbb{Q}_2)$ we have either $P \in \mathcal{U}_c$ or $\psi_c(P) \in \mathcal{U}_{16/c}$. This establishes the proposition. □

We partition the sets $\mathcal{U}_c$ into open subsets

$$\mathcal{U}_c' \cup \bigcup_{n=1}^{\infty} \mathcal{U}_{c,n}'' \cup \bigcup_{n=1}^{\infty} \mathcal{U}_{c,n}''',$$

with the definition of these subsets included in the following definition.

Definition 2.4. We define various open subsets of $\mathcal{U}_c$.

– Let $\mathcal{U}_c' \subset \mathcal{U}_c$ be the open subset of 2-adic points that have representatives $(a_0 : a_1 : a_2 : a_3)$ such that the a_i are all odd 2-adic integers.

- Let $\mathcal{A}_c \subset \mathcal{U}'_c$ be the open subset of points $(a_0 : a_1 : a_2 : a_3)$ where the a_i additionally satisfy $v(a_0+a_2) = v(a_1-a_3) = 1$. Let $\mathcal{A}'_c \subset \mathcal{U}'_c$ be the open subset where instead the a_i satisfy $v(a_0 - a_2) = v(a_1 + a_3) = 1$.
- For $n \in \mathbb{Z}_{\geq 1}$, let $\mathcal{U}''_{c,n} \subset \mathcal{U}_c$ be the set of 2-adic points that have representatives $(a_0 : a_1 : a_2 : a_3)$ where the a_i are 2-adic integers such that a_0 and a_2 are both odd and $v(a_1) = v(a_3) = n$.
- For $n \in \mathbb{Z}_{\geq 1}$, let $\mathcal{B}_{c,n} \subset \mathcal{U}''_{c,n}$ be the open subset of points $(a_0 : a_1 : a_2 : a_3)$ where the a_i additionally satisfy $v(a_0 - a_2) = 1$ and $v(a_1 - a_3) = n + 1$.
- For $n \in \mathbb{Z}_{\geq 1}$, let $\mathcal{U}'''_{c,n} \subset \mathcal{U}_c$ be the open subset of 2-adic points that have representatives $(a_0 : a_1 : a_2 : a_3)$ where the a_i are 2-adic integers such that a_0 and a_2 are both odd, and either $v(a_1) > v(a_3) = n$ or $v(a_3) > v(a_1) = n$.
- For $n \in \mathbb{Z}_{\geq 1}$, let $\mathcal{C}_{c,n} \subset \mathcal{U}'''_{c,n}$ be the open subset of points $(a_0 : a_1 : a_2 : a_3)$ where the a_i additionally satisfy $v(a_0+a_2) = 1$, and let $\mathcal{C}'_{c,n} \subset \mathcal{U}'''_{c,n}$ be the open subset of points $(a_0 : a_1 : a_2 : a_3)$ where the a_i additionally satisfy $v(a_0 - a_2) = 1$.

Clearly, to prove density of a certain subset of $\mathcal{U}_c$ it suffices to prove its density in each of the sets $\mathcal{U}'_c$, $\mathcal{U}''_{c,n}$ and $\mathcal{U}'''_{c,n}$. However, if we use some of the automorphisms of V_c, it suffices to restrict our attention to smaller open subsets $\mathcal{A}_c$, $\mathcal{A}'_c$, $\mathcal{B}_{c,n}$, $\mathcal{C}_{c,n}$ and $\mathcal{C}'_{c,n}$.

Throughout the chapter, we make frequent use of the following automorphisms of V_c.

Definition 2.5. For $0 \leq i \leq 3$, let ϕ_i denote the automorphism of V_c that acts on $(x_0 : x_1 : x_2 : x_3)$ by multiplying the x_i-coordinate by -1.

We observe that $\mathcal{U}'_c$ is the union of the images of $\mathcal{A}_c$ under the subgroup of $\mathrm{Aut}(V_c)$ generated by the ϕ_i. Note also that we have $\mathcal{A}'_c = \phi_2(\phi_3(\mathcal{A}_c))$ and $\mathcal{C}'_{c,n} = \phi_2(\mathcal{C}_{c,n})$ for each n. Also, each $\mathcal{U}''_{c,n}$ is the union of the images of $\mathcal{B}_{c,n}$ under the said subgroup of $\mathrm{Aut}(V_c)$ and each $\mathcal{U}'''_{c,n}$ is the union of the images of $\mathcal{C}_{c,n}$. Therefore, to prove density of the set of $V_c(\mathbb{Q})$ in $\mathcal{U}_c$, it suffices to prove its density in the sets $\mathcal{A}_c$, $\mathcal{B}_{c,n}$ for all integers $n \geq 1$ and in either $\mathcal{C}_{c,n}$ or $\mathcal{C}'_{c,n}$ for all integers $n \geq 1$.

2.1.1 Outline of the rest of the chapter

In sections 2.2 and 2.3, we introduce elliptic fibrations on V_c, and we investigate the fibres of these fibrations. In section 2.4, we explain the strategy of

proving density of rational points using elliptic fibrations. Sections 2.5–2.7 form the core of the proof. We will prove in section 2.5 that the existence of any rational point on V_c that is in $\mathcal{C}_{c,1}$ implies the density of $V_c(\mathbb{Q})$ in $\mathcal{C}_{c,1}$; that the same fact implies the density of $V_c(\mathbb{Q})$ in $\mathcal{A}_c$ will be proven in section 2.6. In section 2.7, we will show that density of $V_c(\mathbb{Q})$ in $\mathcal{A}'_c = \phi_2(\phi_3(\mathcal{A}_c))$ implies the density of $V_c(\mathbb{Q})$ in $\mathcal{B}_{c,n}$ for all integers $n \geq 1$ and in $\mathcal{C}'_{c,n}$ for all integers $n \geq 2$. Therefore, in view of the arguments of the previous paragraph, sections 2.5–2.7 show that the existence of a rational point of V_c that is in $\mathcal{C}_{c,1}$ implies the density of $V_c(\mathbb{Q})$ in the set $\mathcal{U}_c$ defined at the start of this section. Furthermore, if we combine this with Proposition 2.3, we find that the existence of both a rational point of V_c that is in $\mathcal{C}_{c,1}$ and a rational point of $V_{16/c}$ that is in $\mathcal{C}_{16/c,1}$ implies the density of $V_c(\mathbb{Q})$ in $V_c(\mathbb{Q}_2)$.

2.2 Elliptic fibrations on V_c

We define rational maps $f, g\colon V_c \dashrightarrow \mathbb{P}^1$ as follows:

$$f(x_0 : x_1 : x_2 : x_3) = \frac{x_0 - x_2}{x_1 - x_3}, \quad g(x_0 : x_1 : x_2 : x_3) = \frac{x_0 + x_2}{x_1 - x_3}.$$

We observe that $g = f \circ \phi_2$. By considering the identities

$$-\frac{x_0 \pm x_2}{x_1 - x_3} = c\,\frac{(x_1 + x_3)(x_1^2 + x_3^2)}{(x_0 \mp x_2)(x_0^2 + x_2^2)}$$

in the function field of V_c, we see that f and g are actually morphisms from V_c to $\mathbb{P}^1$. For $\lambda \in \mathbb{P}^1$, the preimage $f^{-1}(\lambda)$ is the intersection of the cubic surface

$$(x_0 + x_2)(x_0^2 + x_2^2) = -\frac{c}{\lambda}(x_1 + x_3)(x_1^2 + x_3^2) \tag{2.2}$$

with the plane $x_0 - x_2 = \lambda(x_1 - x_3)$, with the understanding that the left-hand side is equated to zero if $\lambda = 0$, and the right-hand side is equated to zero if $\lambda = \infty$, with λ replaced by any finite value. For $\mu \in \mathbb{P}^1$, the preimage $g^{-1}(\mu)$ is the intersection of the cubic surface

$$(x_0 - x_2)(x_0^2 + x_2^2) = -\frac{c}{\mu}(x_1 + x_3)(x_1^2 + x_3^2),$$

with the plane $x_0 + x_2 = \mu(x_1 - x_3)$, with the understanding that the left-hand side is equated to zero if $\mu = 0$, and the right-hand side is equated to zero if $\mu = \infty$, with μ replaced by any finite value.

The morphisms $f, g\colon V_c \to \mathbb{P}^1$ endow the surface V_c with a fibration in curves of genus one (which is often abusively called an elliptic fibration). Note that f has the section $\lambda \mapsto P_\lambda$, where $P_\lambda = (\lambda : 1 : -\lambda : -1)$. The point P_λ is the intersection of $f^{-1}(\lambda)$ with the line $x_0 + x_2 = x_1 + x_3 = 0$. Applying ϕ_2, we see that g likewise has a section given by $\mu \mapsto P'_\mu$, where $P'_\mu = (\mu : 1 : \mu : -1)$. By taking P_λ to be the identity for the group law on $f^{-1}(\lambda)$, and P'_μ for the one on $g^{-1}(\mu)$, we may (and will) regard f and g as elliptic fibrations, i.e. fibrations whose generic fibres are elliptic curves.

2.2.1 The level of a point on a Weierstrass curve

Let $P \in V_c(\mathbb{Q}_2)$ and let $E = e^{-1}(e(P))$ be a fibre of an elliptic fibration $e\colon V_c \to \mathbb{P}^1$ passing through P. Then E is an elliptic curve over $\mathbb{Q}_2$. Suppose we are given a nice Weierstrass curve $\mathcal{E}$ over $\mathbb{Z}_2$ together with a morphism $i\colon E \to \mathcal{E}$ that is an isomorphism on generic fibres. On $\mathcal{E}(\mathbb{Q}_2)$, we have a filtration (see section 1.2)

$$\mathcal{E}(\mathbb{Q}_2) \supset \mathcal{E}_0(\mathbb{Q}_2) \supset \mathcal{E}_1(\mathbb{Q}_2) \supset \mathcal{E}_2(\mathbb{Q}_2) \supset \dots,$$

inducing an exhaustive filtration $\{E_n(\mathbb{Q}_2)\}_{n=0}^{\infty}$ on the subgroup of $E(\mathbb{Q}_2)$ that maps isomorphically to $\mathcal{E}_0(\mathbb{Q}_2)$. If P is not the identity of $E(\mathbb{Q}_2)$, and P lies in $E_0(\mathbb{Q}_2)$, then there exists a largest integer $n \geq 0$ such that $P \in E_n(\mathbb{Q}_2)$; we will call n the level of P on $\mathcal{E}$. If the image of P does not lie in $\mathcal{E}_0(\mathbb{Q}_2)$, we will say that the level of P is -1: this is the same as saying that the image of P has singular reduction. The choice of i is suppressed from the terminology; it is always clear from the context. Usually the choices of both i and $\mathcal{E}$ are clear: we will then speak of the level of P on E or along e, or write $\mathrm{level}_E(P)$.

2.3 Weierstrass models for the fibres of f

This section consists mainly of calculations, of which the aim is to find Weierstrass models for the fibres of f. We do this in order to be able to apply the results of chapter 1, which deal with Weierstrass curves. Moreover, with a Weierstrass equation at hand it is easier to compute j-invariants and division polynomials, as is done in the proof of Proposition 2.10. The Weierstrass models and the changes of variables from which they result are summarized in Propositions 2.6–2.8.

Throughout section 2.3, we assume $1 \leq v(c) \leq 3$. By $\overline{\mathbb{Z}}_2$ we denote the integral closure of $\mathbb{Z}_2$ in $\overline{\mathbb{Q}}_2$.

Proposition 2.6. *Let $\lambda \in \mathbb{P}^1(\overline{\mathbb{Q}}_2) - \{0, \infty\}$ be such that $\lambda^8 \neq c^2$ and $v(\lambda) \geq 0$. Then there exists an isomorphism from $f^{-1}(\lambda)$ to the generic fibre of the Weierstrass curve in $\mathbb{P}^2_{\overline{\mathbb{Z}}_2}$ with homogeneous coordinates x, y, z given by*

$$\mathcal{E}_\lambda \colon y^2 z = x^3 - 3\lambda^6 x^2 z - 3\lambda^4 (c^2 - \lambda^8) x z^2 - \lambda^2 (c^2 - \lambda^8)^2 z^3, \tag{2.3}$$

where this isomorphism is given by

$$x = -\frac{x_0 + x_2}{2c}, y = \frac{x_1 - x_3}{2}, z = \frac{x_1 + x_3 + \frac{\lambda^3}{c}(x_0 + x_2)}{2\lambda(c^2 - \lambda^8)}. \tag{2.4}$$

Proof. Let λ be as in the proposition. The preimage $f^{-1}(\lambda)$ of λ under the morphism $f \colon V_c \to \mathbb{P}^1$ is the cubic curve over $\overline{\mathbb{Q}}_2$

$$(x_0 + x_2)(x_0^2 + x_2^2) = -\frac{c}{\lambda}(x_1 + x_3)(x_1^2 + x_3^2), \quad x_0 - x_2 = \lambda(x_1 - x_3).$$

Note that it has the point P_λ defined in the previous section, which we take to be the identity for the group law, endowing $f^{-1}(\lambda)$ with the structure of an elliptic curve. We map $f^{-1}(\lambda)$ isomorphically to the cubic curve in $\mathbb{P}^3_{\overline{\mathbb{Q}}_2}(s_0, s_1, v_0, v_1)$ given by

$$s_0(s_0^2 + v_0^2) = -\frac{c}{\lambda} s_1 (s_1^2 + v_1^2), \quad v_0 = \lambda v_1 \tag{2.5}$$

with the maps given by

$$s_0 = x_0 + x_2, \quad v_0 = x_0 - x_2, \quad s_1 = x_1 + x_3, \quad v_1 = x_1 - x_3. \tag{2.6}$$

If we project the image of $f^{-1}(\lambda)$ to $\mathbb{P}^2_{\mathbb{Q}_2}(s_0, s_1, v_1)$, by eliminating v_0 in (2.5), its isomorphic copy in $\mathbb{P}^2_{\overline{\mathbb{Q}}_2}(s_0, s_1, v_1)$ is given by

$$s_0(s_0^2 + \lambda^2 v_1^2) = -\frac{c}{\lambda} s_1 (s_1^2 + v_1^2). \tag{2.7}$$

The point P_λ maps to the flex point $(s_0 : v_1 : s_1) = (0 : 1 : 0)$, whose tangent is given by $\lambda^3 s_0 = -c s_1$. We introduce the variable

$$s_2 = s_1 + \frac{\lambda^3}{c} s_0.$$

With this substitution we arrive at the curve in $\mathbb{P}^2_{\overline{\mathbb{Q}}_2}(s_0, v_1, s_2)$

$$s_0^3 = \frac{c}{\lambda}\left(\frac{\lambda^9}{c^3} s_0^3 - 3\frac{\lambda^6}{c^2} s_0^2 s_2 + 3\frac{\lambda^3}{c} s_0 s_2^2 - s_2^3 - v_1^2 s_2\right),$$

isomorphic to the one given by (2.7). The effect of this last step is that the image of the point P_λ is $(s_0 : v_1 : s_2) = (0 : 1 : 0)$, with the tangent now given by $s_2 = 0$. Rearranging, we get

$$-\frac{c}{\lambda}v_1^2 s_2 = \left(1 - \frac{\lambda^8}{c^2}\right) s_0^3 + 3\frac{\lambda^5}{c} s_0^2 s_2 - 3\lambda^2 s_0 s_2^2 + \frac{c}{\lambda} s_2^3.$$

Finally, since $\lambda^8 \neq c^2$, we may define an isomorphism from the curve defined by the equation above to the Weierstrass curve given by

$$y^2 z = x^3 - 3\lambda^6 x^2 z - 3\lambda^4(c^2 - \lambda^8) x z^2 - \lambda^2 (c^2 - \lambda^8)^2 z^3,$$

by setting

$$x = -\frac{s_0}{2c} = -\frac{x_0 + x_2}{2c}, y = \frac{v_1}{2} = \frac{x_1 - x_3}{2},$$
$$z = \frac{s_2}{2\lambda(c^2 - \lambda^8)} = \frac{x_1 + x_3 + \frac{\lambda^3}{c}(x_0 + x_2)}{2\lambda(c^2 - \lambda^8)}.$$

Here, the factors 2 in the denominators are introduced for our convenience at a later stage in this chapter. This ends the proof. □

Proposition 2.7. *Let $\lambda \in \mathbb{P}^1(\overline{\mathbb{Q}}_2) - \{0, \infty\}$ be such that $\lambda^8 \neq c^2$ and $v(\lambda) \geq v(c)$. There exists an isomorphism from $f^{-1}(\lambda)$ to the generic fibre of the Weierstrass curve in $\mathbb{P}^2_{\overline{\mathbb{Z}}_2}$ with homogeneous coordinates $\widetilde{x}, \widetilde{y}, \widetilde{z}$ given by*

$$\widetilde{\mathcal{E}}_\lambda \colon \widetilde{y}^2\widetilde{z} = \widetilde{x}^3 - \frac{3\lambda^6}{c^2}\widetilde{x}^2\widetilde{z} - \frac{3\lambda^4(c^2 - \lambda^8)}{c^4}\widetilde{x}\widetilde{z}^2 - \frac{\lambda^2(c^2 - \lambda^8)^2}{c^6}\widetilde{z}^3. \tag{2.8}$$

where this isomorphism is given by

$$\widetilde{x} = -\frac{x_0 + x_2}{2c^3}, \widetilde{y} = \frac{x_1 - x_3}{2c^3}, \widetilde{z} = \frac{x_1 + x_3 + \frac{\lambda^3}{c}(x_0 + x_2)}{2\lambda(c^2 - \lambda^8)}. \tag{2.9}$$

Proof. The new variables $\widetilde{x}, \widetilde{y}, \widetilde{z}$ are related to the x, y, z from Proposition 2.6 by $\widetilde{x} = x/c^2, \widetilde{y} = y/c^2, \widetilde{z} = z$. □

Proposition 2.8. *Let $\lambda \in \mathbb{P}^1(\overline{\mathbb{Q}}_2) - \{0, \infty\}$ be such that $\lambda^8 \neq c^2$ and $v(\lambda) < 0$. There exists an isomorphism from $f^{-1}(\lambda)$ to the generic fibre of the Weierstrass curve in $\mathbb{P}^2_{\overline{\mathbb{Z}}_2}$ with homogeneous coordinates $\widehat{x}, \widehat{y}, \widehat{z}$ given by*

$$\widehat{\mathcal{E}}_\lambda \colon \widehat{y}^2\widehat{z} = \widehat{x}^3 - 3\lambda^{-4}c^2\widehat{x}\widehat{z}^2 - \lambda^{-2}c^2(c^2\lambda^{-8} + 1)\widehat{z}^3. \tag{2.10}$$

where this isomorphism is given by

$$\widehat{x} = -\frac{x_0+x_2}{2\lambda^4 c} - \frac{\lambda(x_1+x_3)+\frac{\lambda^4}{c}(x_0+x_2)}{2(c^2-\lambda^8)}, \widehat{y} = \frac{x_1-x_3}{2\lambda^6},$$
$$\widehat{z} = \frac{x_1+x_3+\frac{\lambda^3}{c}(x_0+x_2)}{2\lambda(c^2-\lambda^8)}. \tag{2.11}$$

Proof. Resuming the notation of Proposition 2.6, we set

$$u = x - \lambda^6 z = -\frac{x_0+x_2}{2c} - \frac{\lambda^5(x_1+x_3)+\frac{\lambda^8}{c}(x_0+x_2)}{2(c^2-\lambda^8)},$$

we get a morphism from $f^{-1}(\lambda)$ to the curve given by the short Weierstrass equation

$$y^2 z = u^3 - 3\lambda^4 c^2 u z^2 - \lambda^2 c^2 (c^2+\lambda^8) z^3. \tag{2.12}$$

If we put $\widehat{z} = z$, and define scalings of u and y as follows

$$\widehat{x} = u/\lambda^4, \quad \widehat{y} = y/\lambda^6,$$

this defines an isomorphism from $f^{-1}(\lambda)$ to the curve (2.10). □

Remark 2.9. The above propositions can of course be used to give Weierstrass models for fibres of other elliptic fibrations on V_c. Let ϕ be any automorphism of V_c. Then $e = f \circ \phi$ is an elliptic fibration of V_c. For $\lambda \in \mathbb{P}^1(\overline{\mathbb{Q}}_2) - \{0, \infty\}$ such that $v(\lambda) \geq 0$, Proposition 2.6 can be used to give an embedding of $e^{-1}(\lambda)$ into the Weierstrass curve $E_\lambda \subset \mathbb{P}^2_{\overline{\mathbb{Z}}_2}$ as defined by (2.3). This embedding is obtained by precomposing the morphism (2.4) with ϕ. Similarly, Propositions 2.7 and 2.8 can be used to obtain embeddings of $e^{-1}(\lambda)$ into the Weierstrass curves $\widetilde{E}_\lambda$ and $\widehat{E}_\lambda$ given by (2.8) and (2.10) for the appropriate values of $\lambda \in \mathbb{P}^1(\overline{\mathbb{Q}}_2) - \{0, \infty\}$.

2.3.1 The group structure on the fibres

It will be important for us in what follows to know the structure of the topological groups $\mathcal{E}_\lambda(\mathbb{Q}_2)$, $\widetilde{\mathcal{E}}_\lambda(\mathbb{Q}_2)$, and $\widehat{\mathcal{E}}_\lambda(\mathbb{Q}_2)$, where the notation is as in Propositions 2.6–2.8, or at least the parts consisting of the points of good reduction.

Proposition 2.10. *Assume that* $1 \leq v(c) \leq 3$. *We have the following isomorphisms of topological groups.*

(i) For all $\lambda \in \mathbb{P}^1(\mathbb{Q}_2) - \{0, \infty\}$ *with* $v(\lambda) = 0$*, we have*

$$(\mathcal{E}_\lambda)_0(\mathbb{Q}_2) \cong \mathbb{Z}_2,$$

and the isomorphism can be chosen in such a way that $(\mathcal{E}_\lambda)_n(\mathbb{Q}_2)$ *is identified with* $2^n\mathbb{Z}_2$ *for all* $n \in \mathbb{Z}_{\geq 0}$*.*

(ii) For all $\lambda \in \mathbb{P}^1(\mathbb{Q}_2) - \{0, \infty\}$ *with* $v(\lambda) \geq v(c)$*, we have*

$$(\widetilde{\mathcal{E}}_\lambda)_0(\mathbb{Q}_2) \cong \mathbb{Z}_2,$$

and the isomorphism can be chosen in such a way that $(\widetilde{\mathcal{E}}_\lambda)_n(\mathbb{Q}_2)$ *is identified with* $2^n\mathbb{Z}_2$ *for all* $n \in \mathbb{Z}_{\geq 0}$*.*

(iii) For all $\lambda \in \mathbb{P}^1(\mathbb{Q}_2) - \{0, \infty\}$ *with* $v(\lambda) < 0$*, we have*

$$(\widehat{\mathcal{E}}_\lambda)_0(\mathbb{Q}_2) \cong \mathbb{Z}_2,$$

and the isomorphism can be chosen in such a way that $(\widehat{\mathcal{E}}_\lambda)_n(\mathbb{Q}_2)$ *is identified with* $2^n\mathbb{Z}_2$ *for all* $n \in \mathbb{Z}_{\geq 0}$*.*

(iv) For all $\lambda \in \mathbb{P}^1(\mathbb{Q}_2) - \{0, \infty\}$ *with* $v(\lambda) = v(c) + 1$*, we have*

$$\widetilde{\mathcal{E}}_\lambda(\mathbb{Q}_2) \cong 2^{-1}\mathbb{Z}_2,$$

where $2^{-1}\mathbb{Z}_2$ *is seen as an open subset of* $\mathbb{Q}_2$*, and the isomorphism can be chosen in such a way that* $(\widetilde{\mathcal{E}}_\lambda)_n(\mathbb{Q}_2)$ *is identified with* $2^n\mathbb{Z}_2$ *for all* $n \in \mathbb{Z}_{\geq 0}$*.*

Proof. For (i)–(iii), it suffices to apply Theorem 1.28 of Chapter 1. Now part (iv). In view of (ii) and Corollary 1.17, it is enough to show that $\widetilde{\mathcal{E}}_\lambda(\mathbb{Q}_2) \cong 2^{-1}\mathbb{Z}_2$. Let $\lambda \in \mathbb{P}^1 - \{\infty\}$ be such that $v(\lambda) = v(c) + 1$. The j-invariant of the generic fibre of $\widetilde{\mathcal{E}}_\lambda$ equals

$$12^3 \cdot \frac{4\lambda^8 c^2}{4\lambda^8 c^2 - \lambda^8 - c^2},$$

which has positive 2-adic valuation. Therefore $\widetilde{\mathcal{E}}_\lambda$ has either good or additive reduction. However, the reduction must in fact be additive: the discriminant of $\widetilde{\mathcal{E}}_\lambda$ is equal to

$$16 \cdot 27 \cdot \lambda^4 c^{-8}(4\lambda^8 c^2 - (c^2 + \lambda^8)^2),$$

and so has valuation 8, hence $\widetilde{\mathcal{E}}_\lambda$ is minimal. We thus have a short exact sequence

$$0 \to (\widetilde{\mathcal{E}}_\lambda)_0(\mathbb{Q}_2) \to \widetilde{\mathcal{E}}_\lambda(\mathbb{Q}_2) \to G \to 0$$

where G is a group of order at most 4 [32, C.15]. It follows from Proposition 1.14(ii) that $\widetilde{\mathcal{E}}_\lambda(\mathbb{Q}_2)$ is isomorphic to $\mathbb{Z}_2$ if and only if it has no elements of order 2 or 3. We may prove that the 2- and 3-torsion of $\widetilde{\mathcal{E}}_\lambda(\mathbb{Q}_2)$ is trivial using the 2- and 3-division polynomials of $(\widetilde{\mathcal{E}}_\lambda)_{\mathbb{Q}_2}$. However, we may equally well work with the 2- and 3-division polynomials $\Phi_2, \Phi_3 \in \mathbb{Q}_2[u]$ of the generic fibre of the Weierstrass curve (2.12), which is isomorphic to $(\widetilde{\mathcal{E}}_\lambda)_{\mathbb{Q}_2}$; we will do this since this makes the computation easier. The polynomial Φ_2 is just the right-hand side of (2.12):

$$\Phi_2 = u^3 - 3\lambda^4 c^2 u - \lambda^2 c^2 (c^2 + \lambda^8).$$

For Φ_3 we have [32, III, Exercise 3.7]:

$$\Phi_3 = 3u^4 - 18\lambda^4 c^2 u^2 - 12\lambda^2 c^2 (c^2 + \lambda^8) u - 9\lambda^8 c^4.$$

We find the valuation of the three zeros of Φ_2 by inspecting its Newton polygon. The coefficient of u^0 has valuation $6v(c) + 2$, that of u^1 has valuation $6v(c) + 4$, and that of u^3 has valuation 0: each zero of Φ_2 therefore has valuation $2v(c) + \frac{2}{3}$, and therefore does not lie in $\mathbb{Q}_2$. We consider the Newton polygon of Φ_3: the coefficient of u^0 has valuation $12v(c) + 8$, that of u^1 has valuation $6v(c) + 4$, that of u^2 has valuation $6v(c) + 5$, and that of u^4 has valuation 0. From this, we see that Φ_3 has a unique root in $\mathbb{Q}_2$, and this root has valuation $6v(c) + 4$. However, there is no 2-adic point (u_0, y_0) on the curve (2.12) such that $v(u_0) = 6v(c) + 4$, since then it would follow from (2.12) and from the valuations of the coefficients of Φ_2 we have just computed that we would have

$$y_0^2 \equiv -\lambda^2 c^2 (c^2 + \lambda^8) \pmod{2^{12v(c)+8}}.$$

However, the right-hand side cannot be a square in $\mathbb{Q}_2$, since $\lambda^2 c^2 (c^2 + \lambda^8) = \lambda^2 c^4 (1 + \lambda^8/c^2)$ is a square in $\mathbb{Q}_2$. Therefore $\widetilde{\mathcal{E}}_\lambda(\mathbb{Q}_2)$ has no 2- or 3-torsion. This concludes the proof. □

Section 2.3.2 will illustrate how Proposition 2.10 can be used to prove that, locally in $V_c(\mathbb{Q}_2)$, one has 2-adic density of rational points.

2.3.2 The bad fibres

We will describe the bad (non-smooth) fibres of f.

Lemma 2.11. *The geometric fibre of $f\colon V_c \to \mathbb{P}^1$ above $\lambda = 0$ is the union of the line*

$$x_0 - x_2 = x_1 + x_3 = 0$$

and two lines whose field of definition contains a square root of -1. The geometric fibre of f above $\lambda = \infty$ is the union of the line

$$x_0 + x_2 = x_1 - x_3 = 0$$

and two lines whose field of definition contains a square root of -1. The fibres of f above $\lambda = 0$ and $\lambda = \infty$ both consist of three lines meeting in one point.

Proof. If $\lambda = 0$, then from (2.2) we get that the fibre $f^{-1}(\lambda)$ is given by

$$(x_1 + x_3)(x_1^2 + x_3^2) = 0,\ x_0 - x_2 = 0.$$

If $\lambda = \infty$, then the fibre $f^{-1}(\lambda)$ is given by

$$(x_0 + x_2)(x_0^2 + x_2^2) = 0,\ x_1 - x_3 = 0.$$

The last assertion is clear from these equations. □

Lemma 2.12. *Let $\lambda \in \overline{\mathbb{Q}}$ be such that $\lambda^8 = c^2$. The geometric fibres of $f\colon V_c \to \mathbb{P}^1$ above λ are unions of a line and a smooth conic.*

Proof. Let λ be as in the statement of the lemma. From (2.2) we get that the fibre $f^{-1}(\lambda)$ is given by

$$(x_0 + x_2)(x_0^2 + x_2^2) = \pm\lambda^3(x_1 + x_3)(x_1^2 + x_3^2),\ x_0 - x_2 = \lambda(x_1 - x_3),$$

for some change of sign. Changing variables to

$$s_0 = x_0 + x_2,\ v_0 = x_0 - x_2,\ s_1 = \lambda(x_1 + x_3),\ v_1 = \lambda(x_1 - x_3),$$

we find that $f^{-1}(\lambda)$ is isomorphic to the curve given by

$$s_0(s_0^2 + v_0^2) = \pm s_1(s_1^2 + v_1^2),\ v_0 = v_1.$$

By projecting onto the coordinates (s_0, s_1, v_1), and slightly rearranging the resulting equation, we get that $f^{-1}(\lambda)$ is isomorphic to the curve given by

$$(s_0 \mp s_1)(s_0^2 + s_1^2 \pm s_0 s_1 + v_1^2) = 0.$$

This clearly consists of a line and a non-singular conic. □

We will show that there are no other bad fibres than the ones described in Lemmas 2.11–2.12.

Proposition 2.13. *The non-smooth fibres of $f\colon V_c \to \mathbb{P}^1$ are exactly the fibres above $\lambda = 0$, $\lambda = \infty$ and the λ with $\lambda^8 = c^2$.*

Proof. Let $\lambda \in \mathbb{P}^1(\overline{\mathbb{Q}}_2) - \{0, \infty\}$ be such that $\lambda^8 \neq c^2$. We will see that $f^{-1}(\lambda)$ is an elliptic curve. It follows from the proof of Proposition 2.8 that (2.11) defines an isomorphism from $f^{-1}(\lambda)$ to the curve E_λ over $\overline{\mathbb{Q}}_2$ defined by

$$\widehat{y}^2\widehat{z} = \widehat{x}^3 - 3\lambda^{-4}c^2\widehat{x}\widehat{z}^2 - \lambda^{-2}c^2(c^2\lambda^{-8} + 1)\widehat{z}^3.$$

(The restriction $v(\lambda) < 0$ in Proposition 2.8 is there just to ensure that (2.10) defines a Weierstrass curve over $\overline{\mathbb{Z}}_2$.) We claim that the Weierstrass curve E_λ is non-singular. In order to see this, it suffices to check that its discriminant, which is

$$16 \cdot 27 \cdot \lambda^{20}c^{-8}(4c^2\lambda^{-8} - (c^2\lambda^{-8} + 1)^2) = -16 \cdot 27 \cdot \lambda^{20}c^{-8}(c^2\lambda^{-8} - 1)^2,$$

is non-zero, which is clearly the case. The proposition now follows from Lemmas 2.11–2.12. □

Corollary 2.14. *Let $P \in V_c(\mathbb{Q}_2)$ be a point lying on a bad fibre of f.*

(i) We have $f(P) = 0$ or $f(P) = \infty$, and P lies on the line $x_0 - x_2 = x_1 + x_3 = 0$ if $f(P) = 0$, and on the line $x_0 + x_2 = x_1 - x_3 = 0$ if $f(P) = \infty$.

(ii) Assume that $P \in \mathcal{U}_c$. If $f(P) = 0$, then $P \in \mathcal{A}_c$ or $P \in \phi_3(\mathcal{B}_{c,n})$ for some $n \geq 1$. If $f(P) = \infty$, then $P \in \mathcal{A}'_c$ or $P \in \phi_2(\mathcal{B}_{c,n})$ for some $n \geq 1$.

Proof. Let P be as in the statement, and let $\lambda = f(P) \in \mathbb{P}^1(\mathbb{Q}_2)$. The point P is defined over $\mathbb{Q}_2$, so we cannot have $\lambda^8 = c^2$, since the valuation of c is not a multiple of four. Hence λ is either 0 or ∞ by Proposition 2.13.

Assuming that $f(P) = 0$, then by Lemma 2.11, the point P lies on the line $x_0 - x_2 = x_1 + x_3 = 0$. Assume moreover $P \in \mathcal{U}_c$. Then if P is given by $(a_0 : a_1 : a_2 : a_3)$ with the a_i in $\mathbb{Z}_2$ and $v(a_0) = v(a_2) = 0$, we have $v(a_0 - a_2) = \infty$ and $v(a_0 + a_2) = v(2a_0) = 1$, and $v(a_1 + a_3) = \infty$ and $v(a_1 - a_3) = v(2a_1)$. Hence, if $v(a_1) = 0$, then P lies in $\mathbb{A}_c$, if $v(a_1) > 0$, then P lies in $\phi_2(\mathcal{B}_{c,n})$ with $n = v(a_1)$.

Assuming that $f(P) = \infty$, then by Lemma 2.11, the point P lies on the line $x_0 + x_2 = x_1 - x_3 = 0$. Assume moreover $P \in \mathcal{U}_c$. Then if P is

given by $(a_0 : a_1 : a_2 : a_3)$ with the a_i in $\mathbb{Z}_2$ and $v(a_0) = v(a_2) = 0$, we have $v(a_0 + a_2) = \infty$ and $v(a_0 - a_2) = v(2a_0) = 1$, and $v(a_1 - a_3) = \infty$ and $v(a_1 + a_3) = v(2a_1)$. Hence, if $v(a_1) = 0$, then P lies in $\mathbb{A}'_c$; if $v(a_1) > 0$, then P lies in $\phi_3(\mathcal{B}_{c,n})$ with $n = v(a_1)$. □

2.4 Using elliptic fibrations to prove density

We will show how the elliptic fibrations on V_c can be exploited to show that, locally around a certain point in $V_c(\mathbb{Q}_2)$, the rational points lie dense. The main result of this section, Lemma 2.16, is almost trivial, but it neatly captures the basic ideas of this chapter.

2.4.1 One elliptic fibration

Assume that $e\colon V_c \to \mathbb{P}^1$ is an elliptic fibration. Let P and P' be elements of $V_c(\mathbb{Q}_2)$ lying on the same smooth fibre of e, and let $E = e^{-1}(e(P))$. Assume that we have a Weierstrass curve $\mathcal{E}$ over $\mathbb{Z}_2$, and an isomorphism $i\colon E \to \mathcal{E}_{\mathbb{Q}_2}$ of elliptic curves over $\mathbb{Q}_2$. Suppose furthermore that we have an isomorphism $\phi\colon \mathcal{E}_n(\mathbb{Q}_2) \xrightarrow{\sim} 2^n\mathbb{Z}_2$ for some $n \geq -1$, where we write $\mathcal{E}_{-1}(\mathbb{Q}_2) = \mathcal{E}(\mathbb{Q}_2)$, and that ϕ identifies $\mathcal{E}_k(\mathbb{Q}_2)$ with $2^k\mathbb{Z}_2$ for all $k \geq n$. (Note that Proposition 2.10 asserts that there (many) triples (e, P, P') for which these conditions are all satisfied.) In this setup, we have the following lemma.

Lemma 2.15. *Suppose that we have*

$$\operatorname{level}_E(P') \geq \operatorname{level}_E(P) \geq n.$$

Then the multiples of P on E lie dense around P'. Moreover, if there exists a sequence $\{Q_i\}_{i=0}^{\infty}$ of rational points converging to P, then there exists a sequence $\{Q'_i\}_{i=0}^{\infty}$ of rational points converging to P'.

Proof. Let $k = \operatorname{level}_E(P)$ and $k' = \operatorname{level}_E(P')$. Then $\phi(i(P)) \in 2^n\mathbb{Z}_2$ has valuation k and $\phi(i(P')) \in 2^n\mathbb{Z}_2$ has valuation $k' \geq k$. Hence the multiples of $\phi(i(P))$ are dense around $\phi(i(P'))$. Since $\phi \circ i$ is a homeomorphism from $\mathcal{E}_n(\mathbb{Q}_2)$ to $2^n\mathbb{Z}_2$, the multiples of P are dense around P'. For any integer m, we have the rational map $[m]\colon V_c \dashrightarrow V_c$ that is multiplication by m along fibres of e; it is a morphism when restricted to the smooth locus of e. Let $\{Q_i\}_{i=0}^{\infty}$ be as in the statement of the lemma. If $\{m_i\}_{i=0}^{\infty}$ is a sequence of integers such that $[m_i]P$ converges to P', then $\{[m_i]Q_i\}_{i=0}^{\infty}$ converges to P', by continuity of $[m_i]$ near smooth fibres. We may thus take $Q'_i = [m_i]Q_i$ for all i. □

2.4.2 Two elliptic fibrations

We continue with the assumptions of section 2.4.1. If we employ not just one elliptic fibration e, but also a second one e', we obtain a method for proving density in an open subset of $V_c(\mathbb{Q}_2)$. Let $e'\colon V_c \to \mathbb{P}^1$ be an elliptic fibration, and suppose that P'' is an element of $V_c(\mathbb{Q}_2)$ such that P' and P'' lie on the same smooth fibre of e'. Let us denote $E' = (e')^{-1}(e'(P'))$.

Assume, analogously to what we assumed for E, that we have a Weierstrass curve $\mathcal{E}'$ over $\mathbb{Z}_2$, and an isomorphism $i'\colon E' \to \mathcal{E}'_{\mathbb{Q}_2}$ of elliptic curves over $\mathbb{Q}_2$. Suppose furthermore that we have an isomorphism $\phi'\colon \mathcal{E}'_m(\mathbb{Q}_2) \xrightarrow{\sim} 2^m\mathbb{Z}_2$ for some $m \geq -1$, where we again write $\mathcal{E}'_{-1}(\mathbb{Q}_2) = \mathcal{E}'(\mathbb{Q}_2)$, and that ϕ' identifies $\mathcal{E}'_k(\mathbb{Q}_2)$ with $2^k\mathbb{Z}_2$ for all $k \geq m$.

Lemma 2.16. *Suppose that we have both*

$$\operatorname{level}_E(P') \geq \operatorname{level}_E(P) \geq n$$

and

$$\operatorname{level}_{E'}(P'') \geq \operatorname{level}_{E'}(P') \geq m.$$

Then if there exists a sequence $\{Q_i\}_{i=0}^{\infty}$ of rational points converging to P, then there exists a sequence $\{Q''_i\}_{i=0}^{\infty}$ of rational points converging to P''. In particular, the rational points are dense around P''.

Proof. For any integer m, we have the rational maps $[m]_e\colon V_c \dashrightarrow V_c$ and $[m]_{e'}\colon V_c \dashrightarrow V_c$ that are multiplication by m along fibres of e and e'; the rational maps $[m]_e$ and $[m]_{e'}$ give morphisms when restricted to the smooth loci of e and e'. Lemma 2.15 applied to P and P' yields the existence of a sequence $\{m_i\}_{i=0}^{\infty}$ of integers such that $([m_i]_e P)_i$ converges to P'. By restricting to a subsequence if necessary, we can assume that all $[m_i]_e P$ lie on smooth fibres of e'. Applying Lemma 2.15 to P' and P'', we get the existence of a sequence $\{m'_i\}_{i=0}^{\infty}$ of integers such that $([m'_i]_{e'} P')_i$ converges to P''. If we put

$$Q''_i = [m'_i]_{e'}[m_i]_e Q_i,$$

then $\{Q''_i\}_{i=0}^{\infty}$ is a sequence of rational points converging to P''. □

Lemma 2.16 shows the strategy that we will follow to prove density of $V_c(\mathbb{Q})$ in $V_c(\mathbb{Q}_2)$. Continuing with the assumptions on e and e' and the notation established earlier in this section, one starts from a point $P \in V_c(\mathbb{Q}_2)$ and a sequence $\{Q_i\}_{i=0}^{\infty}$ of rational points converging to P (this is especially easy if P is itself rational), then one looks for an open subset U of

$V_c(\mathbb{Q}_2)$ such that, for all $P'' \in U$, there exists an auxiliary point $P' \in V_c(\mathbb{Q}_2)$ with $e(P') = e(P)$ and $e'(P') = e'(P'')$ such that both

$$\text{level}_E(P') \geq \text{level}_E(P) \geq n$$

and

$$\text{level}_{E'}(P'') \geq \text{level}_{E'}(P') \geq m.$$

It follows from Lemma 2.16 that the rational points are then dense in U.

This is the strategy that will be followed in sections 2.5 and 2.6, where density in $\mathcal{C}_{c,1}$ and $\mathcal{A}_c$ is established. The roles of e and e' will be taken by the elliptic fibrations f, g and $f \circ \phi_3$. The arguments in section 2.7, which covers density in $\mathcal{B}_{c,n}$ for $n \geq 1$ and $\mathcal{C}_{c,n}$ for $n \geq 2$, are similar, but apply Lemma 2.15 instead of Lemma 2.16.

2.5 Density in $\mathcal{C}_{c,1}$

From this point in the chapter on, we will assume that $c \in \mathbb{Q}^*$ is such that $1 \leq v(c) \leq 3$.

We will show that the rational points on V_c are dense in $\mathcal{C}_{c,1}$. In this section and the next, we will frequently use the fact that the equation (2.1) defining V_c can be rewritten as

$$(x_0 - x_2)(x_0 + x_2)(x_0^2 + x_2^2) = -c(x_1 - x_3)(x_1 + x_3)(x_1^2 + x_3^2). \qquad (2.13)$$

Lemma 2.17. *Let $P = (a_0 : a_1 : a_2 : a_3)$ be a point in $\mathcal{C}_{c,1}$, where the a_i are 2-adic integers at least one of which is a unit. Write $\lambda = f(P)$ and $\pi = (f \circ \phi_3)(P)$. Then the following statements are true.*

(i) We have

$$v(a_0 + a_2) = 1, v(a_0 - a_2) = v(c) + 2, v(a_0^2 + a_2^2) = 1$$

as well as

$$v(a_1 + a_3) = 1, v(a_1 - a_3) = 1, v(a_1^2 + a_3^2) = 2.$$

(ii) We have $v(\lambda) = v(\pi) = v(c) + 1$.

Proof. The first equality is by definition of $\mathcal{C}_{c,1}$. The third equality follows from the fact that the square of an element $a \in \mathbb{Z}_2^*$ is $1 \pmod 8$. The second

row of equalities all follow from the definition of $\mathcal{C}_{c,1}$. Now from (2.13), we get

$$v(a_0 - a_2) = v(c) + v(a_1 - a_3) + v(a_1 + a_3) + v(a_1^2 + a_3^2) \\ - v(a_0 + a_2) - v(a_0^2 + a_2^2) = v(c) + 2, \tag{2.14}$$

which concludes the proof of (i). Part (ii) is a direct consequence of part (i). □

We have the following converse of Lemma 2.17(ii).

Lemma 2.18. *Let $\lambda_0, \pi_0 \in \mathbb{Q}_2$ satisfy $v(\lambda_0) = v(\pi_0) = v(c) + 1$. Then there exists a unique point $P \in \mathcal{C}_{c,1}$ such that $f(P) = \lambda_0$ and $(f \circ \phi_3)(P) = \pi_0$. Moreover, the dependence of P on λ_0 and π_0 is continuous.*

Proof. We rewrite (2.13) in terms of the homogeneous coordinates $s_0 = x_0 + x_2, v_0 = x_0 - x_2, s_1 = x_1 + x_3, v_1 = x_1 - x_3$:

$$s_0 v_0 (s_0^2 + v_0^2) = -c s_1 v_1 (s_1^2 + v_1^2). \tag{2.15}$$

The hypotheses imply that in (2.15) we have $v_0 = \lambda_0 v_1$ and $v_0 = \pi_0 s_1$. If we set $w = s_0/v_0$, we obtain the following equation for w:

$$w^3 + w + b_0 = 0,$$

where

$$b_0 = c \frac{\lambda_0^2 + \pi_0^2}{\lambda_0^3 \pi_0^3}.$$

The conditions on the valuations of λ_0 and π_0 give $v(b_0) = -3v(c) - 3$. (Here, we use that if $\kappa \in \mathbb{Z}_2$, then $\kappa^2 \equiv 2^{2v(\kappa)} \pmod{2^{2v(\kappa)+3}}$.) Setting $w = w'/2c$, we find that w' satisfies

$$w'^3 + 4c^2 w' + 8 b_0 c^3 = 0. \tag{2.16}$$

By Hensel's lemma, this has a solution $w_0' \in \mathbb{Q}_2$ with $v(w_0') = 0$. Moreover, the three roots w_0', w_1', w_2' of (2.16) in $\overline{\mathbb{Q}}_2$ reduce to the three zeros of $X^3 + 1$ in $\overline{\mathbb{F}}_2$, only one of which lies in $\mathbb{F}_2$; therefore, w_0' is the unique solution to (2.16) in $\mathbb{Q}_2$. It gives rise to the point

$$P_0 = P(\lambda_0, \pi_0) = (w_0' + 2c : 2c/\lambda_0 + 2c/\pi_0 : w_0' - 2c : -2c/\lambda_0 + 2c/\pi_0),$$

of which one checks that it indeed lies in $\mathcal{C}_{c,1}$. For the P whose existence was asserted in the lemma we may thus take $P = P_0$.

Finally, we check that $P(\lambda_0, \pi_0)$ depends on λ_0 and π_0 in a continuous way. This comes down to the claim that if $((\lambda_i, \pi_i))_{i=1}^{\infty} \subset \mathbb{Q}_2^2$ is a sequence of pairs converging to (λ_0, μ_0), then if w_i' is a solution to

$$w'^3 + 4c^2 w' + 8b_i c^3 = 0 \tag{2.17}$$

where

$$b_i = c\frac{\lambda_i^2 + \pi_i^2}{\lambda_i^3 \pi_i^3}.$$

then the sequence $(w_i')_i$ tends to w_0'. We now prove this claim. From (2.17) we deduce

$$\begin{aligned} 8(b_i - b_{i-1})c^3 &= (w_{i-1}'^3 + 4c^2 w_{i-1}') - (w_i'^3 + 4c^2 w_i') \\ &= -(w_i' - w_{i-1}')(w_i'^2 + w_i' w_{i-1}' + w_{i-1}'^2 + 4c^2). \end{aligned}$$

As i tends to infinity, we have that $b_i - b_{i-1}$ tends to 0, while $v(w_i'^2 + w_i' w_{i-1}' + w_{i-1}'^2 + 4c^2) = 0$ since $v(w_{i-1}') = v(w_i') = 0$. Hence $w_i' - w_{i-1}'$ tends to 0, and we are done. □

For each $P \in \mathcal{C}_{c,1}$, we will identify the fibre through P of f with the generic fibre of the curve $\widetilde{\mathcal{E}}_{f(P)}$ given by (2.8) via (2.9); the fibre through P of $f \circ \phi_3$ we will identify with the generic fibre of the curve $\widetilde{\mathcal{E}}_{(f\circ\phi_3)(P)}$ in the same way. It follows from Lemma 2.17(ii) that these identifications can be made. With these conventions, it makes sense to speak of the levels of the points in $\mathcal{C}_{c,1}$ along f and $f \circ \phi_3$.

Lemma 2.19. *Let P be a point in $\mathcal{C}_{c,1}$. The level of P along f is equal to -1. The level of P along $f \circ \phi_3$ is equal to -1.*

Proof. The proof uses Lemma 2.17 throughout. We write $P = (a_0 : a_1 : a_2 : a_3)$ and $\lambda = f(P)$. We obtain a representative $(\widetilde{\xi} : \widetilde{\eta} : \widetilde{\zeta})$ of the image of P on $\widetilde{E}_\lambda$ by substituting $x_i = a_i$ into the equations (2.9). Using (2.9), we get

$$v(\widetilde{\xi}) = v(a_0 + a_2) - 3v(c) - 1 = -3v(c), \;\; v(\widetilde{\eta}) = v(a_1 - a_3) - 3v(c) - 1 = -3v(c),$$

where we have used the definition of $\mathcal{C}_{c,1}$. To compute the valuation of

$$\widetilde{\zeta} = \frac{a_1 + a_3 + \frac{\lambda^3}{c}(a_0 + a_2)}{2\lambda(c^2 - \lambda^8)} \tag{2.18}$$

note that Lemma 2.17(i) implies $v(a_1+a_3) = 1 < 2v(c)+4 = v(\frac{\lambda^3}{c}(a_0+a_2))$; hence the valuation of the numerator is equal to 1. Therefore

$$v(\widetilde{\zeta}) = 1 - v(2\lambda(c^2 - \lambda^8)) = 1 - (1 + v(c) + 1 + 2v(c)) = -3v(c) - 1.$$

It follows that we have $v(\widetilde{\xi}/\widetilde{\zeta}) = v(\widetilde{\eta}/\widetilde{\zeta}) = 1$. Therefore the point P reduces to the singular point on the special fibre of $\widetilde{E}_\lambda$. Thus we have shown that the level of P along f is -1.

The calculations for the level along $f \circ \phi_3$ go in exactly the same way as the calculations for the level along f. □

Proposition 2.20. *Assume that there exists a rational point $P_0 \in \mathcal{C}_{c,1}$. Then $V_c(\mathbb{Q})$ is dense in $\mathcal{C}_{c,1}$.*

Proof. Let $P_2 \in \mathcal{C}_{c,1}$ be an arbitrary 2-adic point. Define $\lambda_0 = f(P_0)$ and $\pi_2 = (f \circ \phi_3)(P_2)$. It follows from Lemma 2.17(ii) and 2.18 that there exists a unique $P_1 \in \mathcal{C}_{c,1}$ such that $f(P_1) = \lambda_0$ and $(f \circ \phi_3)(P_1) = \pi_2$. These conditions express exactly that P_1 lies on the same f-fibre as P_0, and on the same $(f \circ \phi_3)$-fibre as P_2. The levels of P_0 and P_1 along f are both equal to -1 by Lemma 2.19. The levels of P_1 and P_2 along $f \circ \phi_3$ are both equal to -1 by Lemma 2.19. By Corollary 2.14, the points P_0 and P_1 lie on a smooth fibre of f, and P_1 and P_2 lie on a smooth fibre of $f \circ \phi_3$. By Lemma 2.16, the rational points lie dense around P_2. □

2.6 Density in $\mathcal{A}_c$

Assuming there is a rational point in $\mathcal{C}_{c,1}$, we will show density of the rational points in $\mathcal{A}_c$.

Lemma 2.21. *Let $P = (a_0 : a_1 : a_2 : a_3)$ be a point in $\mathcal{A}_c$. Write $\lambda = f(P)$ and $\mu = g(P)$. Then the following statements are true.*

(i) We have

$$v(a_0 + a_2) = 1, v(a_0 - a_2) = v(\lambda) + 1, v(a_0^2 + a_2^2) = 1,$$

as well as

$$v(a_1 + a_3) = v(\lambda) + 1 - v(c), v(a_1 - a_3) = 1, v(a_1^2 + a_3^2) = 1.$$

(ii) We have $v(\lambda) \geq v(c) + 1$ and $v(\mu) = 0$.

Proof. Since P is in $\mathcal{A}_c$ we have $v(a_0 + a_2) = v(a_1 - a_3) = 1$ by definition of $\mathcal{A}_c$, and this implies

$$v(a_0^2 + a_2^2) = v(a_1^2 + a_3^2) = 1,$$

since the square of the 2-adic unit a_i is 1 (mod 8) for each i. This shows (i) except for the second and fourth equality. Using (2.13) as in the proof of Lemma 2.17, we get

$$v(a_0 - a_2) = v(a_1 + a_3) + v(c), \tag{2.19}$$

which shows that $v(\lambda) = v((a_0 - a_2)/(a_1 - a_3)) = v(a_0 - a_2) - 1$, which shows the second equality. If we combine this with (2.19), we get $v(\lambda) = v(a_1 + a_3) + v(c) - 1$. This concludes the proof of the fourth equality and therefore that of (i). Part (ii) is a direct consequence of part (i). □

We have the following converse of Lemma 2.21(ii).

Lemma 2.22. *Let $\lambda_0, \mu_0 \in \mathbb{Q}_2$ satisfy $v(\lambda_0) \geq v(c)+1$ and $v(\mu_0) = 0$. Then there exists a unique point $P \in \mathcal{A}_c$ such that $f(P) = \lambda_0$ and $g(P) = \mu_0$. Moreover, the dependence of P on λ_0 and μ_0 is continuous.*

Proof. We rewrite (2.13) in terms of the homogeneous coordinates $s_0 = x_0 + x_2, v_0 = x_0 - x_2, s_1 = x_1 + x_3, v_1 = x_1 - x_3$:

$$s_0 v_0 (s_0^2 + v_0^2) = -c s_1 v_1 (s_1^2 + v_1^2).$$

We are looking for a point with $f(P) = \lambda_0$ and $g(P) = \mu_0$. We thus have $v_0 = \lambda_0 v_1$ and $s_0 = \mu_0 v_1$. In terms of $w = s_1/v_1$ we have to solve the equation

$$\lambda_0 \mu_0 (\lambda_0^2 + \mu_0^2) = -cw(1 + w^2).$$

Defining

$$a = \frac{\lambda_0 \mu_0}{c} (\lambda_0^2 + \mu_0^2),$$

we can rewrite the equation as

$$w^3 + w + a = 0.$$

Given a solution $w_0 \in \mathbb{Q}_2$ to this equation, we get the point in $V_c(\mathbb{Q}_2)$ represented by the four-tuple

$$P_0 = (\lambda_0 + \mu_0 : w_0 + 1 : -\lambda_0 + \mu_0 : w_0 - 1). \tag{2.20}$$

Note that we have $v(a) > 0$. By considering the Newton polygon of $w^3 + w + a$, we see that two of its zeros in $\overline{\mathbb{Q}}_2$ have valuation 0. These do not give rise to points in $\mathcal{U}_c'$. The remaining zero w_0 has positive valuation. By Galois theory, we have $w_0 \in \mathbb{Q}_2$. By the assumptions on λ_0, μ_0 and the fact that $v(w_0) > 0$, the four-tuple (2.20) represents a point in $\mathcal{U}_c'$. One can check that it in fact lies in $\mathcal{A}_c$. For the P whose existence was asserted in the lemma we may thus take $P = P_0$. Finally, the fact that P depends continuously on λ_0 and μ_0 is shown exactly as in the proof of Lemma 2.18. □

For each $P \in \mathcal{A}_c$, we will identify $f^{-1}(f(P))$ with the generic fibre of (2.8) via (2.9). Note that this is the same choice that we made in section 2.5 for $P \in \mathcal{C}_{c,1}$, so that it makes sense to compare levels along f of points in $\mathcal{A}_c$ and $\mathcal{C}_{c,1}$. We will identify the fibre $g^{-1}(g(P))$ with the generic fibre of (2.3) via (2.4). It follows from Lemma 2.21(ii) that these identifications can be made. With these conventions, it makes sense to speak of the levels of the points in $\mathcal{A}_c$ along f and g.

Lemma 2.23. *Let P be a point in $\mathcal{A}_c$ and write $\lambda = f(P)$. The level of P along f is equal to 0. The level of P along g is equal to $v(\lambda) - v(c)$.*

Proof. We write $P = (a_0 : a_1 : a_2 : a_3)$. We obtain a representative $(\widetilde{\xi} : \widetilde{\eta} : \widetilde{\zeta})$ of the image of P on $\widetilde{\mathcal{E}}_\lambda$ by substituting $x_i = a_i$ into the equations (2.9). Using (2.9), we get

$$v(\widetilde{\xi}) = v(a_0+a_2)-3v(c)-1 = -3v(c), \;\; v(\widetilde{\eta}) = v(a_1-a_3)-3v(c)-1 = -3v(c),$$

where we have used the definition of $\mathcal{A}_c$. To compute the valuation of

$$\widetilde{\zeta} = \frac{a_1 + a_3 + \frac{\lambda^3}{c}(a_0 + a_2)}{2\lambda(c^2 - \lambda^8)}, \tag{2.21}$$

note that Lemma 2.21(i) implies $v(a_1 + a_3) = v(\lambda) + 1 - v(c) < 3v(\lambda) + 1 - v(c) = v(\frac{\lambda^3}{c}(a_0 + a_2))$; hence the valuation of the numerator is equal to $v(a_1 + a_3)$. Therefore

$$v(\widetilde{\zeta}) = v(a_1+a_3)-v(2\lambda(c^2-\lambda^8)) = (v(\lambda)+1-v(c))-(v(\lambda)+1+2v(c)) = -3v(c).$$

It follows that we have $v(\widetilde{\xi}/\widetilde{\zeta}) = v(\widetilde{\eta}/\widetilde{\zeta}) = 0$. Therefore the point P reduces to a non-singular point different from the identity on the special fibre of $\widetilde{E}_\lambda$. Thus we have shown that the level of P along f is 0.

Set $\mu = g(P)$. We obtain a representative $(\xi : \eta : \zeta)$ of the image of P on $\mathcal{E}_\mu$ by substituting $x_i = a_i$ for $i \neq 2$ and $x_2 = -a_2$ into the equations (2.4), and replacing λ by μ. We get

$$v(\xi) = v(a_0 - a_2) - 1 - v(c) = v(\lambda) - v(c) \geq 1$$

and

$$v(\eta) = v(a_1 - a_3) - 1 = 0.$$

From $v(\mu) = 0$ and (2.19) we deduce

$$v(a_1 + a_3) = v\left(\frac{\mu^3}{c}(a_0 - a_2)\right),$$

hence we have, by formula (2.4),

$$v(\zeta) > v(a_1 + a_3) - v(2\mu(c^2 - \mu^8)) = v(a_1 + a_3) - 1 > 0.$$

Since $v(\eta) < v(\zeta)$, the point P is mapped to $(\mathcal{E}_\mu)_1(\mathbb{Q}_p)$, and its level is therefore $v(\xi/\eta) = v(\lambda) - v(c)$. □

Proposition 2.24. *Assume that there is a rational point $P_0 \in V_c(\mathbb{Q})$ such that $P_0 \in \mathcal{C}_{c,1}$. Then $V_c(\mathbb{Q})$ is dense in $\mathcal{A}_c$.*

Proof. Let P_0 be as in the statement of the proposition, and let $P_2 \in \mathcal{A}_c$ be an arbitrary 2-adic point. Define $\lambda_0 = f(P)$ and $\mu_2 = g(P_2)$. We have $v(\lambda_0) = v(c) + 1$ by Lemma 2.17(ii) and $v(\mu_2) = 0$ by Lemma 2.21(ii). It follows from Lemma 2.22 that there exists a unique $P_1 \in \mathcal{A}_c$ such that $f(P_1) = \lambda_0$ and $g(P_1) = \mu_2$.

By Lemma 2.19 we have that the level of P along f is -1 and, by Lemma 2.23, the level of P_1 along f is 0. Also by Lemma 2.23, the level of P_1 along g equals $v(f(P_1)) - v(c) = 1$ and level of P_2 along g is $v(f(P_2)) - v(c)$, which is at least 1 by Lemma 2.21. The f-fibre through P_1 is smooth since it equals the f-fibre through P_0, which is smooth by Corollary 2.14. Moreover, we may assume that the g-fibre through P_1 is smooth, since we may otherwise replace P_2 by a point lying arbitrarily close to it by Lemma 2.22. By Lemma 2.16, the rational points lie dense around P_2. □

2.7 Density in $\mathcal{B}_{c,n}$ for all n and in $\mathcal{C}'_{c,n}$ for $n \geq 2$

Assuming density of $V_c(\mathbb{Q})$ in $\mathcal{A}'_c$, we show that the rational points on V_c are dense in $\mathcal{B}_{c,n}$ for all $n \geq 1$ and in $\mathcal{C}'_{c,n}$ for all $n \geq 2$.

Lemma 2.25. *The following statements are true.*

(i) Let $P = (a_0 : a_1 : a_2 : a_3)$ be a point in $\mathcal{A}'_c$, where the a_i are 2-adic integers at least one of which is a unit. Write $\lambda = f(P)$. We have

$$v(a_0 + a_2) = v(c) + 1 - v(\lambda), v(a_0 - a_2) = 1, v(a_0^2 + a_2^2) = 1$$

as well as

$$v(a_1 + a_3) = 1, v(a_1 - a_3) = 1 - v(\lambda), v(a_1^2 + a_3^2) = 1.$$

(ii) Let $P \in \mathcal{A}'_c$ and write $\lambda = f(P), \mu = g(P)$. Then we have $v(\lambda) < 0$ and $v(\mu) = v(c)$.

(iii) Let $P = (a_0 : a_1 : a_2 : a_3)$ be a point in $\mathcal{B}_{c,n}$ for some integer $n \geq 1$, where the a_i are 2-adic integers at least one of which is a unit. We have

$$v(a_0 - a_2) = 1, v(a_0^2 + a_2^2) = 1$$

as well as

$$v(a_1+a_3) = v(a_0+a_2)-3n-v(c), v(a_1-a_3) = n+1, v(a_1^2+a_3^2) = 2n+1.$$

(iv) Let $P \in \mathcal{B}_{c,n}$ for some integer $n \geq 1$. Write $\lambda = f(P)$. Then we have $v(\lambda) = -n$.

(v) Let $P = (a_0 : a_1 : a_2 : a_3) \in \mathcal{C}'_{c,n}$ for some integer $n \geq 2$, where the a_i are 2-adic integers at least one of which is a unit. We have

$$v(a_0 + a_2) = v(c) + 4n - 2, v(a_0 - a_2) = 1, v(a_0^2 + a_2^2) = 1$$

as well as

$$v(a_1 + a_3) = n, v(a_1 - a_3) = n, v(a_1^2 + a_3^2) = 2n.$$

(vi) Let $P \in \mathcal{C}'_{c,n}$ for some integer $n \geq 2$. Write $\lambda = f(P)$. Then we have $v(\lambda) = 1 - n$.

Proof. Part (i) follows directly from Lemma 2.21(i). Part (ii) follows from part (i). In part (iii), the first and fourth equality follow directly from the definition of $\mathcal{B}_{c,n}$. For the second and fifth, one uses that if $a \in \mathbb{Z}_2$, then $a^2 \equiv 2^{2v(a)} \pmod{2^{2v(a)+3}}$. The third equality follows from the others and from (2.13). Part (iv) follows from part (iii). In part (v), the only non-obvious equation is the first one: it follows from the others and (2.13). Part (vi) follows from part (v). □

We have the following converse of Lemma 2.25(ii).

Lemma 2.26. *Let $\lambda_0, \mu_0 \in \mathbb{Q}_2$ satisfy $v(\lambda_0) < 0$ and $v(\mu_0) = v(c)$. Then there exists a unique point $P \in \mathcal{A}'_c$ such that $f(P) = \lambda_0$ and $g(P) = \mu_0$. Moreover, the dependence of P on λ_0 and μ_0 is continuous.*

Proof. As in the proof of Lemma 2.22, we define

$$a = \frac{\lambda_0\mu_0}{c}(\lambda_0^2 + \mu_0^2).$$

Still as in the proof of Lemma 2.22, given a solution w_0 to the equation

$$w^3 + w + a = 0, \tag{2.22}$$

we get the point in $V_c(\mathbb{Q}_2)$ represented by the four-tuple

$$(\lambda_0 + \mu_0 : w_0 + 1 : -\lambda_0 + \mu_0 : w_0 - 1). \tag{2.23}$$

Under the assumptions of the lemma, we have $v(a) = 3v(\lambda_0) < 0$. If we put $w = \lambda_0 w'$, equation (2.22) transforms to

$$w'^3 + \lambda_0^{-2} w' + a\lambda_0^{-3} = 0, \tag{2.24}$$

where $a\lambda_0^{-3} \in \mathbb{Z}_2^*$. By Hensel's lemma, this has a solution $w'_0 \in \mathbb{Z}_2^*$. Moreover, the three roots w'_0, w'_1, w'_2 of (2.24) in $\overline{\mathbb{Q}}_2$ reduce to the three zeros of $X^3 + 1$ in $\overline{\mathbb{F}}_2$, only one of which lies in $\mathbb{F}_2$; therefore, w'_0 is the unique solution to (2.24) in $\mathbb{Q}_2$. We then have $w_0 = \lambda_0 w'_0$ with $v(w_0) = v(\lambda_0) < 0$. The four-tuple (2.23) that we obtain has non-integral coordinates. Scaling by λ_0^{-1}, we obtain the four-tuple

$$(\mu_0/\lambda_0 + 1 : w'_0 + \lambda_0^{-1} : \mu_0/\lambda_0 - 1 : w'_0 - \lambda_0^{-1}),$$

which defines a point in $\mathcal{U}'_c$, and one checks that it lies in $\mathcal{A}'_c$. For the P whose existence was asserted in the lemma we may thus take $P = P_0$. Finally, the fact that P depends continuously on λ_0 and μ_0 follows as in the proof of Lemma 2.18. □

For a point $P \in V_c(\mathbb{Q}_2)$ that is contained in $\mathcal{A}'_c$, in $\mathcal{B}_{c,n}$ for some $n \geq 1$, or in $\mathcal{C}_{c,n}$ for some $n \geq 2$, we will identify $f^{-1}(f(P))$ with the generic fibre of the curve $\widehat{\mathcal{E}}_{f(P)}$ given by (2.10) via (2.11). Since Lemma 2.25 shows that $v(f(P)) < 0$ in each case, these identifications may be made. Accordingly, the level along f of such a point P is well-defined.

Lemma 2.27. *Let $P = (a_0 : a_1 : a_2 : a_3) \in V_c(\mathbb{Q}_2)$ be a point, where the a_i are 2-adic integers at least one of which is a unit.*

(i) Assume that $P \in \mathcal{A}'_c$. The level of P along f is equal to 0.
(ii) Assume that $P \in \mathcal{B}_{c,n}$ for some $n \geq 1$. The level of P along f is equal to $v(a_1 + a_3) - 1$, which is an integer at least 2.
(iii) Assume that $P \in \mathcal{C}'_{c,n}$ for some $n \geq 2$. The level of P along f is equal to $n - 1$.

Proof. We write $\lambda = f(P)$. In all cases (i)–(iii), we obtain a representative $(\widehat{\xi} : \widehat{\eta} : \widehat{\zeta})$ of the image of P on $\widehat{\mathcal{E}}_\lambda$ by substituting $x_i = a_i$ into the equations (2.11). We have

$$v(\widehat{\xi}) = v\left(-\frac{a_0 + a_2}{2\lambda^4 c} - \frac{\lambda(a_1 + a_3) + \frac{\lambda^4}{c}(a_0 + a_2)}{2(c^2 - \lambda^8)}\right). \tag{2.25}$$

We will only need to compute this valuation for case (ii). We have $v\left(-\frac{a_0+a_2}{2\lambda^4 c}\right) = v(a_0 + a_2) - 1 - v(c) + 4n = v(a_1 + a_3) + 7n - 1$ by Lemma 2.25(iii)–(iv). Both the terms $\lambda(a_1 + a_3)$ and $\frac{\lambda^4}{c}(a_0 + a_2)$ have valuation equal to $v(a_1 + a_3) - n$ by Lemma 2.25(iii)–(iv). Hence the second fraction in (2.25) has valuation greater than or equal to $v(a_1 + a_3) + 7n$. Hence in case (ii) we have $v(\widehat{\xi}) = v(a_1 + a_3) + 7n - 1$.

For

$$v(\widehat{\eta}) = v\left(\frac{a_1 - a_3}{2\lambda^6}\right),$$

we have in case (i) that $v(\widehat{\eta}) = -7v(\lambda)$. In case (ii) we find $v(\widehat{\eta}) = n + 1 - (1 - 6n) = 7n$. In case (iii) we get $v(\widehat{\eta}) = n - (1 + 6(1 - n)) = 7n - 7$.

Finally, we consider

$$v(\widehat{\zeta}) = v\left(\frac{a_1 + a_3 + \frac{\lambda^3}{c}(a_0 + a_2)}{2\lambda(c^2 - \lambda^8)}\right).$$

In case (i), we have $v(a_1 + a_3) = 1$ and $v(\frac{\lambda^3}{c}(a_0 + a_2)) = 2v(\lambda) + 1 < 1$; therefore, we have that $v(\widehat{\zeta}) = 2v(\lambda) + 1 - (1 + 9v(\lambda)) = -7v(\lambda)$. In case (ii), both the terms $a_1 + a_3$ and $\frac{\lambda^3}{c}(a_0 + a_2)$ have valuation equal to $v(a_1 + a_3)$, hence we have that $v(\widehat{\zeta}) \geq v(a_1 + a_3) + 9n$. In case (iii), we have $v(a_1 + a_3) = n$ and $v(\frac{\lambda^3}{c}(a_0 + a_2)) = 3(1 - n) - v(c) + v(c) + 4n - 2 = n + 1$; therefore, we have that $v(\widehat{\zeta}) = n - (10 - 9n) = 10n - 10$.

We finish the proof for case (i) by observing that, in that case, we have $v(\widehat{\eta}/\widehat{\zeta}) = 0$. Therefore, in view of equation (2.10), we must have that the level of P is 0. In case (ii) we see that $v(\widehat{\eta}/\widehat{\zeta}) \leq -2n - v(a_1 + a_3)$, which implies that the level of P is equal to $v(\widehat{\xi}/\widehat{\zeta}) = v(a_1 + a_3) - 1 \geq 2$, where the last inequality follows from $v(a_1 + a_3) \geq 3$. Finally, in case (iii), we have $v(\widehat{\eta}/\widehat{\zeta}) = -3n + 3$, which shows that the level of P is equal to $n - 1$. □

Proposition 2.28. *Assume the density of $V_c(\mathbb{Q})$ in $\mathcal{A}'_c$. The rational points on V_c are dense in $\mathcal{B}_{c,n}$ for all integers $n \geq 1$ and in $\mathcal{C}'_{c,n}$ for all integers $n \geq 2$.*

Proof. Let P_1 be any point in either $\mathcal{B}_{c,n}$ or $\mathcal{C}'_{c,n}$, where n is as in the proposition. Then if $\lambda_1 = f(P_1)$, we have $v(\lambda_1) < 0$ by Lemma 2.25(iv)+(vi). By Lemma 2.26, there exists $P_0 \in \mathcal{A}'_c$ such that $f(P_0) = \lambda_1$ and $g(P_0) = c$. Note that P_0 and P_1 lie on the same fibre of f. Since the rational points on V_c are dense in $\mathcal{A}'_c$, there is a sequence $\{P'_i\}_{i=0}^{\infty} \subset V_c(\mathbb{Q})$ that converges to P_0. By Lemma 2.27, the level of P_0 along f is 0 and the level of P_1 along f is at least 1. By Corollary 2.14, the f-fibre through P_0 and P_1 is smooth. Hence we are done by Lemma 2.15. □

2.8 Proof of the main theorem

Theorem 2.29. *Let c be an element of the set*

$$S = \{2, 4, 6, 10, 12, 14, 18, 20, 22, 2/3, 2/5, 2/7, 2/9, 2/11\}.$$

Then the set $V_c(\mathbb{Q})$ lies dense in the set $V_c(\mathbb{Q}_2)$, when this set is equipped with the 2-adic topology.

Proof. In view of the discussion in section 2.1, it suffices to exhibit an element $P_c \in V_c(\mathbb{Q})$ that lies in $\mathcal{C}_{c,1}$ for each c such that either c or $16/c$ lies in S. This is done in the table below.

Value of c	Point P_c in $V_c(\mathbb{Q}) \cap \mathcal{C}_{c,1}$
2	$P_2 = (489 : 684 : 577 : 662)$
4	$P_4 = (61 : 168 : 237 : 58)$
6	$P_6 = (67 : 16 : -37 : 42)$
8	$P_8 = (257 : 22 : -223 : 124)$
10	$P_{10} = (1 : 4 : -7 : 2)$
12	$P_{12} = (359 : 112 : -361 : 106)$
14	$P_{14} = (11 : 4 : 3 : 6)$
18	$P_{18} = (9 : 16 : 33 : 2)$
20	$P_{20} = (309 : 132 : 37 : 166)$
22	$P_{22} = (347 : 76 : -269 : 146)$
24	$P_{24} = (11 : 308 : -533 : 274)$
40	$P_{40} = (29 : 12 : -3 : 14)$
56	$P_{56} = (43 : 68 : 139 : 62)$
72	$P_{72} = (269 : 52 : 109 : 94)$
88	$P_{88} = (1333 : 172 : 1109 : 374)$
2/3	$P_{2/3} = (39 : 4 : 31 : 38)$
2/5	$P_{2/5} = (31 : 8 : -25 : 34)$
2/7	$P_{2/7} = (349 : 124 : -347 : 194)$
2/9	$P_{2/9} = (3 : 16 : 11 : 2)$
2/11	$P_{2/11} = (179 : 76 : -53 : 274)$
4/3	$P_{4/3} = (171 : 88 : -101 : 158)$
4/5	$P_{4/5} = (79 : 452 : 415 : 262)$
8/3	$P_{8/3} = (19 : 4 : -13 : 14)$
8/5	$P_{8/5} = (5 : 24 : -27 : 2)$
8/7	$P_{8/7} = (599 : 2732 : 1591 : 2662)$
8/9	$P_{8/9} = (269 : 156 : 109 : 282)$
8/11	$P_{8/11} = (391 : 152 : -281 : 394)$

□

Proof of Theorem 2.1. This follows from Theorem 2.29. □

Chapter 3

Density results for Kummer surfaces

In the preprint [38], Sir Peter Swinnerton-Dyer has given two non-singular diagonal quartic surfaces over $\mathbb{Q}$ together with a proof that their rational points lie dense in the space of 2-adic points. A detailed proof of Swinnerton-Dyer's theorem was given in chapter 2. To the author's best knowledge, Swinnerton-Dyer's result provides the first proof of p-adic density of rational points on any K3 surface over $\mathbb{Q}$, for any prime number p. The goal of this chapter is to extend the results of Swinnerton-Dyer to all prime numbers p, giving for each p an infinite number of K3 surfaces over $\mathbb{Q}$ on which the rational points form a p-adically dense set.

The K3 surfaces for which we will obtain p-adic density results are Kummer surfaces. For an abelian variety B over a field of characteristic different from 2, let $\mathrm{Km}(B)$ denote the Kummer variety of B. It is the blow-up of the quotient $B/\langle -1\rangle$ in the image of the 2-torsion of B. When B is an abelian variety of dimension 2, the surface $\mathrm{Km}(B)$ is a K3 surface.

We will establish the following results.

Theorem 3.1. *Let p be a prime number. Then there exist infinitely many pairwise non-isomorphic Kummer surfaces X of the form $\mathrm{Km}(E \times E)$, with E an elliptic curve over $\mathbb{Q}$, such that $X(\mathbb{Q})$ is dense in $X(\mathbb{Q}_p) \times X(\mathbb{R})$.*

Theorem 3.2. *Let p and q be distinct prime numbers not equal to 3. Then there exist infinitely many pairwise non-isomorphic Kummer surfaces X of the form $\mathrm{Km}(E \times E)$, with E an elliptic curve over $\mathbb{Q}$, such that $X(\mathbb{Q})$ is dense in $X(\mathbb{Q}_p) \times X(\mathbb{Q}_q) \times X(\mathbb{R})$.*

Theorem 3.3. *There exists an elliptic curve E over $\mathbb{Q}$ and a set S of 331 prime numbers, such that, if X is the Kummer surface $\mathrm{Km}(E \times E)$, we have $X(\mathbb{Q})$ dense in $\prod_{p \in S} X(\mathbb{Q}_p)$.*

Theorem 3.4. *There exists an elliptic curve E over $\mathbb{Q}$ such that the set of rational points of $\mathrm{Km}(E \times E)$ lies dense in the space of p-adic points for all prime numbers p with $p \equiv 3 \pmod 4$ and $p > 7$.*

Theorem 3.5. *For an elliptic curve E over $\mathbb{Q}$ such that $\#E(\mathbb{Q})[2] = 2$, the set of rational points of $\mathrm{Km}(E \times E)$ lies dense in the space of p-adic points for infinitely many p.*

The proofs will be given in the present chapter. The proofs of Theorems 3.1 and 3.2 are given at the end of Section 3.4. Theorem 3.3 is proven in Section 3.5. Theorem 3.4 is proven in Section 3.6. Theorem 3.5 is proven in Section 3.7.

We will treat the archimedean completion $\mathbb{R}$ of $\mathbb{Q}$ as well as the non-archimedean completions $\mathbb{Q}_p$ for every prime p. Our terminology will be such that, for every number field k, we will take a prime of k to mean a place of k, i.e. an equivalence class of absolute values on $\mathbb{Q}$, two absolute values $|\cdot|_1$ and $|\cdot|_2$ being considered equivalent if and only if there exists a real number e such that $|x|_1 = |x|_2^e$ for all $x \in k$. We will take a prime to mean either a prime of $\mathbb{Q}$, in the sense defined above, or a prime number $p \in \mathbb{Z}_{\geq 0}$.

3.1 Birational invariance of density results

By a variety over a field k we shall mean a scheme that is separated and of finite type over k. For a number field k and a prime v of k, we denote by k_v the completion of k at v. If X is a variety over a number field k and S is a set of primes of k, we write $X(S) = \prod_{v \in S} X(k_v)$ to shorten notation. Unless stated otherwise, we will consider $X(k_v)$ as endowed with the analytic topology and $X(S)$ with the product topology.

Lemma 3.6. *Let X be a smooth geometrically integral variety over a number field k and let $Y \subset X$ be a non-empty Zariski open subset. If S is a finite set of primes of k and $U \subset X(S)$ is a non-empty open subset, then $U \cap Y(S)$ is non-empty.*

Proof. By definition of the product topology, the set U must contain a set $\prod_{v \in S} U_v$ with the $U_v \subset X(k_v)$ non-empty open sets. It is therefore enough

to show that if $U \subset X(k_v)$ is a non-empty open subset for some fixed v, then U cannot be contained in $Z(k_v)$, where we define Z as the complement of Y in X.

Suppose that $U \subset Z(k_v)$. We choose a point $z_0 \in U \cap Z(k_v)$. Let $t_1, \ldots, t_d$ denote a set of local parameters of X at z_0, where d is the dimension of X. By smoothness of X and the implicit function theorem, there exists a neighborhood U' of z_0 contained in U so that the map

$$\begin{aligned} \phi\colon U' &\to k_v^d \\ u &\mapsto (t_1(u), \ldots, t_d(u)) \end{aligned}$$

is a diffeomorphism onto its image. Since Z is a proper closed subset of X, there exists a function $g \in k(X)$ defined at z_0 that vanishes on Z. We view g as an element of the power series ring $k[[t_1, \ldots, t_d]]$ via the embedding of the local ring $\mathcal{O}_{X,z_0}$ into its completion $k[[t_1, \ldots, t_d]]$. We have that g converges on an open neighborhood of z_0 and by assumption, it must vanish on the non-empty open set $\phi(U')$ of k_v^d. But a power series that vanishes on an open neighborhood of $(0, \ldots, 0) \in k_v^d$ must be zero, which is a contradiction. □

If $f\colon Y \dashrightarrow X$ is a rational map between varieties over a number field k and $\Delta \subset Y(S)$ is some subset for some set S of primes of k, then we define the subset $f(\Delta)$ of $X(S)$ as

$$f(\Delta) = \{f(t) : \text{all } t \in \Delta \text{ for which } f(t) \text{ is defined}\}.$$

Proposition 3.7. *Let X and Y be geometrically integral varieties over a number field k and let S be a finite set of primes of k. Assume that $f\colon Y \dashrightarrow X$ is a birational map, and that $\Gamma \subset X(S)$ and $\Delta \subset Y(S)$ are subsets such that $f(\Delta) \subset \Gamma$ and $f^{-1}(\Gamma) \subset \Delta$. Then Γ is dense in $X(S)$ if and only if Δ is dense in $Y(S)$.*

Proof. The proof proceeds in four steps.

Step 0. By restricting the domain of f, we may assume that f is the inclusion of a non-empty Zariski open subset Y of X. The conditions $f(\Delta) \subset \Gamma$ and $f^{-1}(\Gamma) \subset \Delta$ now mean that f identifies Δ with a subset of Γ whose complement lies outside $f(Y(S))$.

Step 1. We claim that if $\Gamma \subset X(S)$ is dense, then $\Delta \subset Y(S)$ is dense. Since the v-adic topology is finer than the Zariski topology, the map $f\colon Y(S) \to X(S)$ is the inclusion of an open subset. Therefore if Γ is dense in $X(S)$, then $\Delta = \Gamma \cap Y(S)$ is dense in $Y(S)$.

Step 2. We claim that, under the assumption that X is smooth over k, the following is true: if $\Delta \subset Y(S)$ is dense, then $\Gamma \subset X(S)$ is dense. Let $U \subset X(S)$ be a non-empty open subset. We want to show that it contains the image of an element of Δ. By Lemma 3.6, the open subset $U \cap f(Y(S))$ of $f(Y(S))$ is non-empty, and by the assumption that $\Delta \subset Y(S)$ is dense it must contain the image of an element of Δ. This proves the claim.

Step 3. We claim that if $\Delta \subset Y(S)$ is dense, then $\Gamma \subset X(S)$ is dense, now without the smoothness assumption on X. For this step we combine the results of Step 1 and 2. By step 1, we may shrink Y if necessary; in particular, we may assume that Y is smooth over k. Now by resolution of singularities, there exists a smooth variety $\widetilde{X}$ over k, a morphism $\pi\colon \widetilde{X} \to X$, and an embedding $\widetilde{f}\colon Y \hookrightarrow \widetilde{X}$, such that the diagram

$$\begin{array}{ccc} Y & \xhookrightarrow{\widetilde{f}} & \widetilde{X} \\ \| & & \downarrow{\scriptstyle \pi} \\ Y & \xhookrightarrow{f} & X \end{array}$$

is commutative. So if $U \subset X(S)$ is a non-empty open subset, then $\pi^{-1}(U) \subset \widetilde{X}(S)$ is also a non-empty open subset. By the argument of the previous paragraph, the open subset $U \cap \widetilde{f}(Y(S))$ of $\widetilde{f}(Y(S))$ is then non-empty. It follows from the diagram that $U \cap f(Y(S))$ is also non-empty. Now arguing as in Step 2, we finish the proof. □

Corollary 3.8. *Let S be a set of primes and let X and Y be geometrically integral varieties over $\mathbb{Q}$ that are birational to each other. Then $X(\mathbb{Q})$ is dense in $\prod_{p\in S} X(\mathbb{Q}_p)$ if and only if $Y(\mathbb{Q})$ is dense in $\prod_{p\in S} Y(\mathbb{Q}_p)$.*

3.2 Procyclic and topologically cyclic groups

In this section, we recall the definitions of profinite and procyclic groups, and gather some facts about these. We will also introduce "topologically cyclic" groups (Definition 3.10). This term is non-standard, but will be very useful to us.

Definition 3.9. A topological group G is called profinite if it is an inverse limit

$$G = \varprojlim_{i\in I} G_i,$$

where the G_i are finite, and the topology on G is the coarsest topology such that the quotient maps $G \to G_i$ are continuous. A topological group G is called procyclic if it is an inverse limit

$$G = \varprojlim_{i \in I} C_i,$$

where the C_i are finite cyclic, and the topology on G is the coarsest topology such that the quotient maps $G \to C_i$ are continuous.

Definition 3.10. If G is a topological group, we call a set $V \subset G$ a generator set of G if the closure of $\langle V \rangle$ is equal to G. We will call $g \in G$ a topological generator of G if $\{g\}$ is a generator set of G. If G has a topological generator, then we call G topologically cyclic.

Lemma 3.11. *A profinite group is procyclic if and only if it is topologically cyclic.*

Proof. Let G be a profinite group. By Corollary 1.1.8(a) of [26], we may assume that G is the limit of an inverse system (G_i, t_{ji}) where the G_i are finite and the transition maps $t_{ji} \colon G_j \to G_i$ are surjective. The result now follows from Lemma 2.5.3 of [26]. □

In general, the topologically cyclic groups do not define the same class of topological groups as the procyclic groups. This is shown by the example of the circle $\mathbb{R}/\mathbb{Z}$, which is generated topologically by the class of any irrational real number. It does not have any non-trivial finite quotients, since it is divisible. Hence it is certainly not profinite.

It is very easy to give a complete classification of procyclic groups. We define a supernatural number to be a formal product

$$\prod_p p^{n(p)},$$

where the product is taken over all prime numbers p, and where $0 \leq n(p) \leq \infty$ for each p. The natural numbers (not counting zero) are those supernatural numbers $\prod_p p^{n(p)}$ with $n(p) < \infty$ for each p and $n(p) = 0$ for almost all p. Note that with this definition, there is an obvious division relation on the set of supernatural numbers that extends the ordinary one on the natural numbers. We may therefore take greatest common divisors and least common multiples of supernatural numbers, and it makes sense to describe two supernatural numbers as being coprime or not.

Definition 3.12. The order of a profinite group G is the least common multiple of the finite supernatural numbers $(G : H)$, where H runs through the open normal subgroups of G.

Note that if G_1 is profinite of order n_1 and G_2 is profinite of order n_2, then $G_1 \times G_2$ is profinite of order $n_1 n_2$. A procyclic group is determined up to isomorphism by its order.

Proposition 3.13. *The following statements are true.*

(i) For each integer $n \in \mathbb{Z}_{\geq 0}$, the discrete group $\mathbb{Z}/p^n\mathbb{Z}$ is the unique procyclic group of order p^n, and the group $\mathbb{Z}_p$ equipped with the p-adic topology is the unique procyclic group of order p^∞.

(ii) For any supernatural number $\sigma = \prod_p p^{n(p)}$, there is a unique procyclic group G of order σ. Moreover, the group G is the direct product $\prod_p G_p$, where the product is taken over all prime numbers p, and where G_p is the unique procyclic group of order $p^{n(p)}$.

Proof. This follows from Theorem 2.7.1 from [26] and the discussion following immediately afterwards. □

As a corollary, we note:

Corollary 3.14. *Let G_1 be procyclic of order n_1 and let G_2 be procyclic of order n_2. If n_1 and n_2 are coprime, then $G_1 \times G_2$ is again procyclic.*

Proof. We can write G_1 and G_2 as products of procyclic groups of order p^n. Since n_1 and n_2 are coprime, the set of primes appearing in the product for G_1 is disjoint from the set of primes appearing in the product for G_2 by Proposition 3.13(ii). Again by Proposition 3.13(ii), the product of G_1 and G_2 is procyclic. □

In the rest of the chapter, we will be mainly concerned with topologically cyclic groups. The following result complements Corollary 3.14.

Proposition 3.15. *The following statements are true.*

(i) Let G_1 be procyclic and let G_2 be $\mathbb{R}/\mathbb{Z}$. Then $G_1 \times G_2$ is topologically cyclic.

(ii) Let G_1 be procyclic of order coprime to 2, and let G_2 be $\mathbb{R}/\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Then $G_1 \times G_2$ is topologically cyclic.

Proof. For part (i), we let g_i be a topological generator of G_i for $i \in \{1, 2\}$. Write $G = G_1 \times G_2$ and $g = (g_1, g_2)$. We prove that if $U \subset G$ is an open subset, then some multiple of g lies in U. By shrinking U we may suppose it is of the form $U = U_1 \times U_2$ with $U_i \subset G_i$ open for $i \in \{1, 2\}$. Furthermore, U_1 contains a translate of some open subgroup $H \subset G_1$. Therefore, it is enough to see that the quotient map

$$G \to G_1/H \times G_2$$

has dense image, where the first factor is a group of finite order n carrying the discrete topology. Since g_1 is a topological generator of G_1, for every coset c in G_1/H there exists an $m \in \mathbb{Z}$ such that $(m + kn)g_1$ maps to c for all $k \in \mathbb{Z}$. But the set

$$\{(m + kn)g_2 : k \in \mathbb{Z}\}$$

lies dense in G_2. Hence the image of the set of multiples of g is a dense set in G.

Part (ii) follows from part (i) by taking $G_1' = G_1 \times \mathbb{Z}/2\mathbb{Z}$ and $G_2' = \mathbb{R}/\mathbb{Z}$. We have $G_1 \times G_2 = G_1' \times G_2'$, and G_1' is procyclic by Corollary 3.14. Now apply part (i) to G_1' and G_2'. □

3.3 Elliptic curves with good twists

3.3.1 Notation and definitions

For the rest of this chapter, we fix an elliptic curve E over $\mathbb{Q}$. Most of our results will therefore be of the form "Assume that E satisfies (some list of properties), then (some conclusion) holds." We assume that E is given by the affine equation $y^2 = f(x)$, with $f(x)$ a separable polynomial of degree 3. Let us denote the complement of $E[2]$ in E by E°. If $c \in k^*$, then by E^c we denote the quadratic twist of E by c, and we assume that it is given by the equation $cy^2 = f(x)$.

The inversion -1 on each twist E^c restricts to an involution of $(E^c)^\circ$, which we will also denote by -1. For c in a field $\ell \supset k$, we let A^c be the variety $(E^c)^\circ \times (E^c)^\circ$ over ℓ. We set $A = A^1$. The A^c are thus non-empty Zariski open subsets of the abelian surfaces $E^c \times E^c$. The quotient $A/\langle -1 \rangle$, where -1 acts diagonally, is a smooth subvariety Y of $X = \mathrm{Km}(E \times E)$. We will identify the variety Y with the subvariety of $\mathbb{A}^3_{\mathbb{Q}}$, with coordinates (x_1, x_2, z), given by

$$z^2 = f(x_1)f(x_2), \quad z \neq 0. \tag{3.1}$$

With this choice of model, the maps q_c defined by

$$q_c \colon A^c \to Y$$
$$((x_1, y_1), (x_2, y_2)) \mapsto (x_1, x_2, cy_1y_2)$$

are the quotient maps for the involution -1 on A_c. Note that $q_1 \colon A \to Y$ is obtained by restricting the quotient rational map $E \times E \dashrightarrow X$ to A.

3.3.2 Partition of the rational points of a Kummer surface

The role played by the varieties A^c, the morphisms q_c and the open subset $Y \subset X$ is explained by the following lemma. It is stated very generally, but we will only apply it for $k = \mathbb{Q}$ and ℓ equal either to $\mathbb{Q}_p$ for some prime number p or to $\mathbb{R}$.

Lemma 3.16. *Let k be a field containing $\mathbb{Q}$, and let $k \subset \ell$ be a field extension.*

(i) For every set $\Gamma(\ell)$ of coset representatives of ℓ^*/ℓ^{*2}, we have

$$Y(\ell) = \coprod_{c \in \Gamma(\ell)} q_c(A^c(\ell)).$$

Moreover, a point $(\xi_1, \xi_2, \zeta) \in Y(\ell)$ lies in $q_c(A^c(\ell))$ if and only if $c \in f(\xi_1)\ell^{*2}$.

(ii) The maps q_c induce a natural bijection

$$\coprod_{c \in \Gamma(\ell)} q_c : \coprod_{c \in \Gamma(\ell)} A^c(\ell)/\langle -1 \rangle \xrightarrow{\sim} Y(\ell).$$

Proof. The second assertion follows from the first, since

$$q_c \colon A^c \to Y$$

is the quotient map for the involution -1 on A^c. For the first assertion, it suffices to show the following: for every $P \in Y(\ell)$, there exists a $c \in \ell^*$ such that $P \in q_c(A^c(\ell))$, and moreover c is unique up to multiplication by a square in ℓ^*. Let $P = (\xi_1, \xi_2, \zeta)$ be an element of $Y(\ell)$. There is a unique element $c \in \Gamma(\ell)$ such that $f(\xi_1)/c = \alpha^2$ for some $\alpha \in \ell^*$. Then (ξ_1, α) and $(\xi_2, \alpha\zeta/f(\xi_1))$ are elements of $(E^c)^\circ(\ell)$; furthermore the point

$$((\xi_1, \alpha), (\xi_2, \alpha\zeta/f(\xi_1)) \in A^c(\ell)$$

maps to P under q_c. Now for the uniqueness of c up to squares: an element in $A^c(\ell)$ that maps to P by q_c is of the form $((\xi_1, \eta_1), (\xi_2, \eta_2))$, and from $(\xi_1, \eta_1) \in (E^c)^\circ(\ell)$ it follows that $c\eta_1^2 = f(\xi_1)$, so we have $c \in f(\xi_1)\ell^{*2}$. This ends the proof. □

Remark 3.17. Since A has a natural structure of $\mathbb{Z}/2\mathbb{Z}$-torsor over Y, part (i) of Lemma 3.16 is a special case of [33, eq. (2.12)].

3.3.3 Elliptic curves with good twists

We begin by stating the most important definition of this chapter.

Definition 3.18. Let S be a set of primes.

(i) For $(d_p) \in \prod_{p\in S} \mathbb{Q}_p^*$ and $c \in \mathbb{Q}^*$, we call E^c a good twist of E with respect to (d_p) and S if for each $p \in S$ we have $c \in d_p\mathbb{Q}_p^{*2}$, and $E^c(\mathbb{Q})$ is dense in $\prod_{p\in S} E^c(\mathbb{Q}_p)$.

(ii) We say E has good twists if, for all $(d_p) \in \prod_{p\in S} \mathbb{Q}_p^*$, there is $c \in \mathbb{Q}^*$ such that E^c is a good twist of E with respect to (d_p) and S.

If $S = \{p\}$ for some prime p, and if E has good twists with respect to (d_p) and S, we will also say that E has good twists with respect to d_p and p, and if E has good twists with respect to $S = \{p\}$, we will also say that E has good twists with respect to p.

Theorem 3.20 will show: if the elliptic curve E over $\mathbb{Q}$ has good twists with respect to S, and we have $X = \mathrm{Km}(E \times E)$, then $X(\mathbb{Q})$ is dense in $\prod_{p\in S} X(\mathbb{Q}_p)$. For all primes p, we will give many examples of elliptic curves with good twists with respect to p.

Remark 3.19. The condition $c \in d_p\mathbb{Q}_p^{*2}$ appearing in Definition 3.18 is equivalent to the twists E^c and E^{d_p}, considered as elliptic curves over $\mathbb{Q}_p$, being isomorphic over $\mathbb{Q}_p$. We may thus rephrase the fact of E having good twists with respect to S as follows: for all collections of twists $\{E^{d_p}\}_{p\in S}$ of E over $\mathbb{Q}_p$, there exists a twist E^c of E over $\mathbb{Q}$ that is isomorphic over $\mathbb{Q}_p$ to E^{d_p} for each $p \in S$, for which $E^c(\mathbb{Q})$ is dense in $\prod_{p\in S} E^c(\mathbb{Q}_p)$.

3.3.4 From good twists to density results

Theorem 3.20. *Let S be a set of primes and let E be an elliptic curve over $\mathbb{Q}$ that has good twists with respect to S. Let $X = \mathrm{Km}(E \times E)$. Then $X(\mathbb{Q})$ is dense in $\prod_{p\in S} X(\mathbb{Q}_p)$.*

Proof. Let $P = (P_p)_{p\in S}$ be a point of $\prod_{p\in S} Y(\mathbb{Q}_p)$. Since E has good twists with respect to S, there exists a $c \in \mathbb{Q}^*$ such that $c \in f(x_1(P_p))\mathbb{Q}_p^{*2}$ for each $p \in S$ and $E^c(\mathbb{Q})$ is dense in $\prod_{p\in S} E^c(\mathbb{Q}_p)$. By Lemma 3.16, we have that for each $p \in S$, the point P_p is in the image of the map

$$q_c \colon A^c(\mathbb{Q}_p) \to Y(\mathbb{Q}_p),$$

hence P is in the image of the map

$$q_{c,S} \colon \prod_{p\in S} A^c(\mathbb{Q}_p) \to \prod_{p\in S} Y(\mathbb{Q}_p).$$

Since $A^c(\mathbb{Q})$ lies dense in $\prod_{p\in S} A^c(\mathbb{Q}_p)$, the set $q_{c,S}(A^c(\mathbb{Q}))$ lies dense around P. □

3.3.5 A partial converse to Theorem 3.20

In this section, we provide a converse to Theorem 3.20 in the case where $S = \{p\}$ and $p > 2$ (see Proposition 3.23). We need a lemma first.

Lemma 3.21. *Let p be a prime and let $\mathscr{E}$ be an elliptic curve over $\mathbb{Q}_p$. Then $\mathscr{E}(\mathbb{Q}_p)$ can be generated topologically by three elements. If $p > 2$, then $\mathscr{E}(\mathbb{Q}_p)$ can be generated topologically by two elements.*

Proof. By Proposition 1.14(i), we have a topological isomorphism

$$\mathscr{E}(\mathbb{Q}_p) \cong \mathbb{Z}_p \times G$$

for some finite abelian group G. It follows from [32, Theorem VI.6.1] that, for every prime ℓ, the ℓ-torsion subgroup $G[\ell] = \mathscr{E}(\mathbb{Q}_p)[\ell]$ is generated by at most 2 elements. Hence by the structure theorem for finitely generated abelian groups we have $G \cong C_1 \times C_2$, with C_1 and C_2 cyclic groups for which the order of C_1 divides that of C_2. It is clear that the elements $(1,0,0)$, $(0,1,0)$ and $(0,0,1)$ are topological generators of $\mathbb{Z}_p \times C_1 \times C_2$.

For the second part, note that $G[p] = \mathscr{E}(\mathbb{Q}_p)[p]$ cannot equal $\mathscr{E}(\overline{\mathbb{Q}}_p)[p]$, since $\mathbb{Q}_p(\mathscr{E}[p])$ contains a primitive p-th root of unity $\zeta_p \notin \mathbb{Q}_p$ by the existence of the Weil pairing. Therefore, the order of C_1 is coprime to p. Then if we define the elements P and Q in $\mathbb{Z}_p \times C_1 \times C_2$ to be $P = (1,1,0)$ and $Q = (0,0,1)$, the elements P and Q correspond to topological generators of $\mathscr{E}(\mathbb{Q}_p)$. □

Remark 3.22. We give an example showing that the second part of Lemma 3.21 fails for $p = 2$. Take the elliptic curve $\mathscr{E}$ over $\mathbb{Q}_2$ defined by $y^2 = x^3 - x$. It has CM over $\mathbb{Q}_2(\sqrt{-1})$, so has potentially good reduction. Since the reduction is bad, it must be additive. We have $\mathscr{E}_0(\mathbb{Q}_2) \cong \mathbb{Z}_2$ by Theorem 1.1, and clearly $\mathscr{E}(\mathbb{Q}_2)[2]$ is isomorphic to the Klein four-group. Hence by Proposition 1.14(ii) we have

$$\mathscr{E}(\mathbb{Q}_2) \cong \mathbb{Z}_2 \times C_1 \times C_2,$$

where C_1 and C_2 are cyclic groups of even order. Hence $\mathscr{E}(\mathbb{Q}_2)$ needs 3 elements to generate it topologically.

Proposition 3.23. *If $X(\mathbb{Q})$ is dense in $X(\mathbb{Q}_p)$ for some prime p greater than 2, then E has good twists with respect to p.*

Proof. Let $d \in \mathbb{Q}_p^*$ be arbitrary, we will show that E has a good twist with respect to d and p. By Lemma 3.21, we may choose elements $P, Q \in E^d(\mathbb{Q}_p)$ such that $\langle P, Q\rangle$ is dense in $E^d(\mathbb{Q}_p)$. We may assume that P and Q are not contained in $E^d(\mathbb{Q}_p)[2]$. Let $R \in X(\mathbb{Q}_p)$ be the image of the point (P, Q) under the map

$$q_d \colon A^d \to Y.$$

If $X(\mathbb{Q})$ is dense in $X(\mathbb{Q}_p)$, then by Corollary 3.8 there exists a sequence $\{R_i\}_{i=1}^{\infty} \subset Y(\mathbb{Q})$ converging to R. By Lemma 3.16 there are $c_i \in \mathbb{Q}^*$ and $(P_i, Q_i) \in A^{c_i}(\mathbb{Q})$ such that $R_i = q_{c_i}((P_i, Q_i))$. Again by Lemma 3.16, we have $c_i \in f(x_1(R_i))\mathbb{Q}_p^{*2}$ and $d \in f(x_1(R))\mathbb{Q}_p^{*2}$, so we have $c_i \equiv d \pmod{\mathbb{Q}_p^{*2}}$ for i sufficiently large. We claim that for these values of i, we have that $\langle P_i, Q_i\rangle$ is dense in $E^{c_i}(\mathbb{Q}_p)$, and therefore that $E^{c_i}(\mathbb{Q})$ is dense in $E^{c_i}(\mathbb{Q}_p)$. For these values of i, we fix isomorphisms over $\mathbb{Q}_p$

$$\phi_i \colon E^{c_i} \xrightarrow{\sim} E^d$$

The images of P_i and Q_i under $\pm\phi_i$ converge to $\pm P$ and $\pm Q$. Since P and Q are topological generators of $E^c(\mathbb{Q}_p)$, we have that P_i and Q_i are topological generators of $E^{c_i}(\mathbb{Q}_p)$. □

3.4 Density results for Kummer surfaces

In this section, we give sufficient conditions on E to have good twists with respect to a prime p, and we show that there are many cases in which these conditions are satisfied. Secondly, we give sufficient criteria for E and a set of primes S that imply that E has good twists with respect to S. At the end of this section, we will derive Theorems 3.1 and 3.2 from these results.

3.4.1 Topologically cyclic groups and density results

Recall that E is given by $y^2 = f(x)$, with f separable and of degree 3.

Lemma 3.24. *Assume that $f(x) = x^3 + ax + b$. Let p be a prime number.*

(i) Assume $p = 2$, $v_2(a) > 0$, and $v_2(b) = 1$. Then for all $d \in \mathbb{Q}_2^*$, the topological group $E^d(\mathbb{Q}_2)$ is procyclic of order 2^∞.

(ii) Assume $p = 3$, $v_3(a) = 1$, and $v_3(b) > 1$. Then for all $d \in \mathbb{Q}_3^*$, the topological group $E^d(\mathbb{Q}_3)$ is procyclic of order $2 \cdot 3^\infty$.

(iii) Assume $p > 3$, $v_p(a) > 0$, $v_p(b) = 1$. If $p = 5$, assume $a \not\equiv \pm 10 \pmod{25}$; if $p = 7$, assume $b \not\equiv \pm 14 \pmod{49}$. Then for all $d \in \mathbb{Q}_p^*$, the topological group $E^d(\mathbb{Q}_p)$ is procyclic of order p^∞ or $3 \cdot p^\infty$. Both orders occur for some d.

(iv) Assume $p > 3$, $v_p(a) = 1$, $v_p(b) > 1$. If $p = 5$, assume $a \not\equiv \pm 10 \pmod{25}$. Then for all $d \in \mathbb{Q}_p^*$, the topological group $E^d(\mathbb{Q}_p)$ is procyclic of order $2 \cdot p^\infty$.

(v) Assume $p > 3$, $v_p(a) > 1$, $v_p(b) = 2$. Then for all $d \in \mathbb{Q}_p^*$, the topological group $E^d(\mathbb{Q}_p)$ is procyclic of order p^∞ or $3 \cdot p^\infty$. Both orders occur for some d.

Proof. Without loss of generality, we assume that d satisfies $v_p(d) \in \{0, 1\}$. For the j-invariant $j(E)$ of E, we have

$$j(E) = 2^8 \cdot 3^3 \cdot \frac{a^3}{4a^3 + 27b^2}, \tag{3.2}$$

and the discriminant Δ_d of the model $\mathcal{E}^d$ of E^d over $\mathbb{Z}_p$ given by $y^2 = x^3 + ad^2x + bd^3$ is

$$\Delta_d = -16d^6(4a^3 + 27b^2).$$

In all cases, we have $v_p(j(E)) \geq 0$ and $v_p(\Delta_d) > 0$. This implies that the reduction type of E at p is potentially good, hence either good or additive; moreover, if $\mathcal{E}^d$ is a minimal model of E at p, then the reduction of E must be additive. In case (i), Tate's algorithm gives the following: firstly, $\mathcal{E}^d$ is a minimal model of E^d for all d; secondly, if $v_2(d) = 0$ then E^d has Kodaira type II, if $v_2(d) = 1$ and $v_2(a) = 1$ then E^d has Kodaira type III*, if $v_2(d) = 1$ and $v_2(a) > 1$ then E^d has Kodaira type II*. In cases (ii)-(v), we have that $v_p(\Delta_d)$ is strictly less than 12. Hence in each case, the Weierstrass curve $\mathcal{E}^d$ is a minimal model of E^d, so E^d has additive reduction in all cases.

Since E^d has additive reduction for all d, it follows from [32, Theorem C.15.1] that $\Phi = E^d(\mathbb{Q}_p)/E_0^d(\mathbb{Q}_p)$, the component group of the special fibre

of the Néron model, is a group of order at most 4. It follows from Theorem 1.1 that $E_0^d(\mathbb{Q}_p)$ is topologically isomorphic to $\mathbb{Z}_p$ in each of the cases (i)-(v) and for all d. We have the tautological exact sequence

$$0 \to E_0^d(\mathbb{Q}_p) \to E^d(\mathbb{Q}_p) \to \Phi \to 0. \tag{3.3}$$

Applying Proposition 1.14(ii) to (3.3) gives that $E^d(\mathbb{Q}_p)$ is topologically isomorphic to a subgroup of $\mathbb{Z}_p \times \Phi'$ with Φ' a subgroup of Φ. To determine Φ', the following strategy may be followed: first one determines the Kodaira type of E^d at p to get an upper bound for Φ, leaving only a finite number of possibilities for Φ', and then one uses the division polynomials of E^d to identify the isomorphism type of Φ'.

We prove part (i). By the fact that the Kodaira type of E^d is II, III* or II*, the group Φ is of order at most 2. Hence we are done if we can show $E^d(\mathbb{Q}_2)[2] = 0$ for all d. We do this with the 2-division polynomial ψ_2 of E^d, which is $\psi_2 = x^3 + ad^2x + bd^3$, whose Newton polygon has vertices $(0, 1 + 3v_p(d))$, $(1, v_p(a) + 2v_p(d))$, and $(3, 0)$, which shows that its three roots in $\overline{\mathbb{Q}}_2$ have valuation $1/3 + v_p(d)$, so do not lie in $\mathbb{Q}_2$.

We prove part (ii). Tate's algorithm gives that the Kodaira type of E^d is III if $v_3(d) = 0$ and III* if $v_3(d) = 1$. Hence Φ is of order at most 2. We use the 2-division polynomial $\psi_2 = x^3 + ad^2x + bd^3$ of E^d to prove that $E^d(\mathbb{Q}_3)[2] \cong \mathbb{Z}/2\mathbb{Z}$ for all d. The Newton polygon of ψ_2 shows that two of its roots in $\overline{\mathbb{Q}}_3$ have valuation $1/2 + v_p(d)$, so do not lie in $\mathbb{Q}_3$. The third one is the unique one with valuation $v_p(b) + v_p(d) - 1$, so by Galois theory it must lie in $\mathbb{Q}_3$.

In parts (iii)-(v) we have $p > 3$. Since E^d has potentially good reduction, and p is different from 2 and 3, the table from [32, C.15] enables us to determine the Kodaira type of E^d at p, and hence an upper bound for Φ, just by knowing $v_p(\Delta_d)$.

In case (iii), we have to show that $E^d(\mathbb{Q}_p)[2] = 0$ for all d, while both $E^d(\mathbb{Q}_p)[3] = 0$ for some d and $E^d(\mathbb{Q}_p)[3] \cong \mathbb{Z}/3\mathbb{Z}$ for some d. We find from the table in [32, C.15] that the curve E^d has Kodaira type II if $v_p(d) = 0$ and Kodaira type IV* if $v_p(d) = 1$. In the first case, the component group is trivial, so $E^d(\mathbb{Q}_p) = E_0^d(\mathbb{Q}_p) \cong \mathbb{Z}_p$ is procyclic of order p^∞ as claimed. In the second case, the group Φ has order 1 or 3, so $E^d(\mathbb{Q}_p)$ is isomorphic to either $\mathbb{Z}_p$ or $\mathbb{Z}_p \times \mathbb{Z}/3\mathbb{Z}$, so indeed procyclic of order p^∞ or $3 \cdot p^\infty$. We show that both possibilities occur. We therefore investigate the 3-division polynomial ψ_3^d of E^d. Its Newton polygon shows that ψ_3^d has a unique zero $x_d \in \overline{\mathbb{Q}}_2$ of valuation $2v_p(a) + v_p(d) - 1$, which is therefore defined over $\mathbb{Q}_p$, while the remaining three roots have valuation $1/3 + v_p(d)$, so lie outside of $\mathbb{Q}_p$. We

conclude: if $x_d^3 + ad^2x_d + bd^3$ is a square in $\mathbb{Q}_p^*$, we have $E^d(\mathbb{Q}_p)[3] \cong \mathbb{Z}/3\mathbb{Z}$; otherwise we have $E^d(\mathbb{Q}_p)[3] = 0$. Note that there indeed exists $d \in \mathbb{Q}_p^*$ such that we have $x_d^3 + ad^2x_d + bd^3 \in \mathbb{Q}_p^{*2}$, since we have

$$x_d^3 + ad^2x_d + bd^3 = d^3(x_1^3 + ax_1 + b),$$

where $x_1 \in \mathbb{Q}_p^*$ is the unique zero of ψ_3^1 in $\mathbb{Q}_p$.

In case (iv), the curve E^d has Kodaira type III if $v_p(d) = 0$ and Kodaira type III* if $v_p(d) = 1$. In both cases, we find from the table in [32, C.15] that Φ has order 1 or 2, and that therefore $E^d(\mathbb{Q}_p)$ is isomorphic to either $\mathbb{Z}_p$ or $\mathbb{Z}_p \times \mathbb{Z}/2\mathbb{Z}$. To show that only the latter possibility occurs, we use the 2-division polynomial $x^3 + ad^2x + bd^3$ of E^d. We find from the Newton polygon that there are two roots with valuation $1/2 + v_p(d)$, and one with valuation $v_p(b) + v_p(d) - 1$, which therefore lies in $\mathbb{Q}_p$.

In case (v), the curve E^d has Kodaira type IV if $v_p(d) = 0$ and Kodaira type II* if $v_p(d) = 1$. As in case (iii), we find from the table that Φ has order 1 or 2 if $v_p(d) = 0$, and order 1 if $v_p(d) = 1$, which implies that $E^d(\mathbb{Q}_p)$ is isomorphic to $\mathbb{Z}_p$ or $\mathbb{Z}_p \times \mathbb{Z}/3\mathbb{Z}$ if $v_p(d) = 0$ and to $\mathbb{Z}_p$ if $v_p(d) = 1$. As in case (iii), we use the Newton polygon of the 3-division polynomial of E^d to show that it has a unique zero $x_d \in \overline{\mathbb{Q}}_2$ of valuation $2v_p(a)+v_p(d)-1$, which is therefore defined over $\mathbb{Q}_p$, while the remaining three roots have valuation $1/3 + v_p(d)$, so lie outside of $\mathbb{Q}_p$. The same argument as the one given for case (iii) shows that both $E^d(\mathbb{Q}_p) \cong \mathbb{Z}_p$ and $E^d(\mathbb{Q}_p) \cong \mathbb{Z}_p \times \mathbb{Z}/3\mathbb{Z}$ occur for suitable d. □

Lemma 3.25. *For all $d \in \mathbb{R}$, the group $E^d(\mathbb{R})$ is topologically isomorphic to $\mathbb{R}/\mathbb{Z} \times (\mathbb{Z}/2\mathbb{Z})^e$, where $e \in \{0, 1\}$. Furthermore, we have $e = 0$ if and only if f has only one real root.*

Proof. The first assertion is proven in [31, V.2.3.1]. The second one is standard. □

Lemma 3.26. *Let S be a finite set of primes and let $(d_p) \in \prod_{p\in S} \mathbb{Q}_p^*$. For all $p \in S$, let (ξ_p, η_p) be in $E^{d_p}(\mathbb{Q}_p)$ and let γ_p and ϵ_p be real numbers. Then there exists a non-zero rational number c, such that for all $p \in S$ we have $v_p(c - d_p) > \gamma_p$, and such that there exists a point $(\xi, \eta) \in E^c(\mathbb{Q})$ satisfying $v_p(\xi - \xi_p) > \epsilon_p$ for all $p \in S$.*

Proof. We may assume that $\eta_p \neq 0$ for all $p \in S$. By the approximation theorem, there exist ξ and η with $\eta \neq 0$ in $\mathbb{Q}$ such that, for all $p \in S$, we have $v_p(\xi - \xi_p) > \epsilon_p$ and $v_p(\eta - \eta_p) > \epsilon_p$. Define $c = f(\xi)/\eta^2$. Since for all

$p \in S$ we have $f(\xi_p)/\eta_p^2 = d_p$, we may assume that c satisfies $v_p(c-d_p) > \gamma_p$ for all $p \in S$ by choosing both ξ closer to ξ_p and η closer to η_p if necessary. Now the twist E^c of E, given by the equation $(f(\xi)/\eta^2)y^2 = f(x)$, trivially contains the point (ξ, η), and both c and ξ satisfy the requirements. □

Proposition 3.27. *Let E be an elliptic curve over $\mathbb{Q}$ and let S be a finite set of primes. Assume that $\prod_{p\in S} E^{d_p}(\mathbb{Q}_p)$ is topologically cyclic for all tuples $(d_p)_p \in \prod_{p\in S} \mathbb{Q}_p^*$. Then E has good twists with respect to S.*

Proof. It suffices to show that for all $(d_p) \in \prod_{p\in S} \mathbb{Q}_p^*$, there exists $c \in \mathbb{Q}^*$, such that for each $p \in S$ we have $c \in d_p\mathbb{Q}_p^{*2}$, and $E^c(\mathbb{Q})$ is dense in $\prod_{p\in S} E^c(\mathbb{Q}_p)$.

We choose $(d_p) \in \prod_{p\in S} \mathbb{Q}_p^*$. Let $P = ((\xi_p, \eta_p))_p$ be a topological generator of $\prod_{p\in S} E^{d_p}(\mathbb{Q}_p)$. By the previous proposition, there exists a twist E^c of E, with c arbitrarily close to each of the d_p, such that there exists a point $(\xi, \eta) \in E^c(\mathbb{Q})$ with ξ arbitrarily close to each of the ξ_p. If c is sufficiently close to each of the d_p, we have $c \in d_p\mathbb{Q}_p^{*2}$; we may therefore assume that we can choose $\alpha_p \in \mathbb{Q}_p^{*2}$ such that $\alpha_p^2 = c/d_p$ for each p.

We now claim that, if ξ is sufficiently close to each of the ξ_p, then (ξ, η) is a topological generator of $\prod_{p\in S} E^c(\mathbb{Q}_p)$, and hence $E^c(\mathbb{Q})$ lies dense in $\prod_{p\in S} E^c(\mathbb{Q}_p)$. For each $p \in S$, there is an isomorphism defined over $\mathbb{Q}_p$

$$\begin{aligned} \psi_p \colon E^c &\to E^{d_p} \\ (x, y) &\mapsto (x, \alpha_p y) \end{aligned}$$

Hence the ψ_p combine to give an isomorphism of topological groups

$$\psi \colon \prod_{p\in S} E^c(\mathbb{Q}_p) \xrightarrow{\sim} \prod_{p\in S} E^{d_p}(\mathbb{Q}_p).$$

Under ψ, the point $((\xi, \eta))_p$ maps to a point $P' = ((\xi, \eta'_p))_p$, for certain $(\eta'_p) \in \prod_{p\in S} \mathbb{Q}_p$. If ξ is sufficiently close to the ξ_p, we can make P' as close as we want to the image of P under an automorphism of $\prod_{p\in S} E^{d_p}(\mathbb{Q}_p)$ that acts on the η_p by multiplication by ± 1; hence for ξ sufficiently close to the ξ_p, the point P' is a topological generator of $\prod_{p\in S} E^{d_p}(\mathbb{Q}_p)$, and so (ξ, η) is a topological generator of $\prod_{p\in S} E^c(\mathbb{Q}_p)$. □

3.4.2 Proof of Theorems 3.1–3.2

Lemma 3.28. *If E_1 and E_2 are elliptic curves over $\mathbb{Q}$ that do not admit complex multiplication over $\mathbb{Q}$, and for which $\mathrm{Km}(E_1 \times E_1)$ is $\overline{\mathbb{Q}}$-isomorphic to $\mathrm{Km}(E_2 \times E_2)$, then E_1 and E_2 are isogenous over $\overline{\mathbb{Q}}$.*

Proof. Let E_1 and E_2 be as in the statement of the lemma. By [34, eq. (10)], we have that $\mathrm{NS}(E_1 \times E_1)$ has rank 3, and is generated by the classes of $D_1 = E_1 \times \{0\}$, $D_2 = \{0\} \times E_1$, and D_3, which is the diagonal copy of E_1 inside $E_1 \times E_1$. The discriminant of $\mathrm{NS}(E_1 \times E_1)$ equals

$$\det \begin{pmatrix} D_1^2 & D_1D_2 & D_1D_3 \\ D_1D_2 & D_2^2 & D_2D_3 \\ D_1D_3 & D_2D_3 & D_3^2 \end{pmatrix} = \det \begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix} = 2.$$

Theorem 0.1 of [15] says that if B_1 and B_2 are abelian surfaces over $\overline{\mathbb{Q}}$ such that $\mathrm{NS}(B_1)$ has rank 3 and has square-free discriminant, and such that $\mathrm{Km}(B_1) \cong \mathrm{Km}(B_2)$, then B_2 is isomorphic to either B_1 or its dual. If we apply this result with B_i equal to $E_i \times E_i$ base-changed to $\overline{\mathbb{Q}}$ for $i \in \{1, 2\}$, and use that the $E_i \times E_i$ are their own duals, we find that $E_1 \times E_1$ is isomorphic to $E_2 \times E_2$ over $\overline{\mathbb{Q}}$. The Poincaré Complete Reducibility Theorem [23, p. 173] implies that E_1 is isogenous to E_2 over $\overline{\mathbb{Q}}$. □

Lemma 3.29. *Let E_1 be an elliptic curve over $\mathbb{Q}$ that does not admit complex multiplication over $\overline{\mathbb{Q}}$. Then there are only finitely many elliptic curves E_2 over $\mathbb{Q}$ up to $\overline{\mathbb{Q}}$-isomorphism such that E_1 and E_2 are isogenous over $\overline{\mathbb{Q}}$.*

Proof. Let E_1 be as in the statement of the lemma. The proof is an application of [32, Corollary IX.6.2], which says that there are only finitely many elliptic curves E_2 over $\mathbb{Q}$ up to $\mathbb{Q}$-isomorphism such that E_1 and E_2 are isogenous over $\mathbb{Q}$.

Let E_2 be an elliptic curve over $\mathbb{Q}$ and let $\phi\colon E_1 \to E_2$ be a $\overline{\mathbb{Q}}$-isogeny. By [32, Corollary IX.6.2], it suffices to show that there exists a quadratic twist E_2' of E_2 over $\mathbb{Q}$ such that E_1 and E_2' are isogenous over $\mathbb{Q}$. Let $\overline{\phi}\colon E_2 \to E_1$ be the dual isogeny to ϕ. Then there exists an integer n with $\phi \circ \overline{\phi} = [n]_{E_2}$, where $[n]_{E_i}$ is multiplication by n on E_i for $i \in \{1, 2\}$. We construct a cocycle

$$c\colon \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \{\pm 1\}$$

as follows: for every $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, we have that $c'_\sigma\colon E_2 \to E_2$ defined by $c'_\sigma = {}^\sigma\phi \circ \overline{\phi}$ is an endomorphism of degree n^2. Since E_1 does not admit complex multiplication over $\overline{\mathbb{Q}}$, the same holds for E_2, and we have $c'_\sigma = \pm[n]_{E_2}$. We define $c_\sigma \in \{\pm 1\}$ to be such that $c'_\sigma = c_\sigma[n]_{E_2}$. It is a trivial verification that c_σ is a cocycle.

By the theory of quadratic twists, there exists a quadratic twist E_2' of E_2 and a $\overline{\mathbb{Q}}$-isomorphism

$$\psi\colon E_2 \to E_2'$$

such that for every $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ we have ${}^{\sigma}(\psi^{-1}) \circ \psi = c_\sigma$. Let $\chi\colon E_1 \to E_2'$ be the $\overline{\mathbb{Q}}$-isogeny $\psi \circ \phi$, and let $\overline{\chi} = \overline{\phi} \circ \psi^{-1}$. We have $\overline{\chi} \circ \chi = [n]_{E_1}$, so $\overline{\chi}$ is the dual isogeny to χ. For every $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, we have

$$ {}^{\sigma}\overline{\chi} \circ \chi = {}^{\sigma}\overline{\phi} \circ {}^{\sigma}\psi^{-1} \circ \psi \circ \phi = [n]_{E_1}. $$

Hence χ is defined over $\mathbb{Q}$. This concludes the proof. □

Corollary 3.30. *Let $\mathcal{C}$ be a collection of elliptic curves over $\mathbb{Q}$, representing infinitely many $\overline{\mathbb{Q}}$-isomorphism classes of elliptic curves. Then the collection of Kummer surfaces*

$$ \{\mathrm{Km}(E' \times E') : E' \in \mathcal{C}\} $$

contains infinitely many pairwise non-$\overline{\mathbb{Q}}$-isomorphic surfaces.

Proof. Since there are only a finite number of $\overline{\mathbb{Q}}$-isomorphism classes of elliptic curves over $\mathbb{Q}$ that admit complex multiplication over $\overline{\mathbb{Q}}$, we may assume that $\mathcal{C}$ does not contain any such elliptic curves. By Lemma 3.28, if the Kummer surfaces $\mathrm{Km}(E_1 \times E_1)$ and $\mathrm{Km}(E_2 \times E_2)$ are $\overline{\mathbb{Q}}$-isomorphic, then E_1 and E_2 are $\overline{\mathbb{Q}}$-isogenous. But by Lemma 3.29, for every $E_1 \in \mathcal{C}$, there are only finitely many $E_2 \in \mathcal{C}$ up to $\overline{\mathbb{Q}}$-isomorphism such that E_1 and E_2 are $\overline{\mathbb{Q}}$-isogenous. Since the elliptic curves in $\mathcal{C}$ represent infinitely many $\overline{\mathbb{Q}}$-isomorphism classes, we are done. □

We use the results obtained so far to give the proofs of Theorems 3.1 and 3.2.

Proof of Theorem 3.1. Assume that the elliptic curve E is given by $y^2 = x^3 + ax + b$ with $a, b \in \mathbb{Q}$. We give conditions on a and b implying that, if $X = \mathrm{Km}(E \times E)$, then $X(\mathbb{Q})$ is dense in $X(\mathbb{Q}_p) \times X(\mathbb{R})$. We treat the case $p = 3$ separately.

First, assume $p = 3$. Assume that $a > 0$, $v_3(a) = 1$, and $v_3(b) > 1$. Then according to Lemma 3.24(ii), we have that $E^d(\mathbb{Q}_3)$ is a procyclic group of order $2 \cdot 3^\infty$ for all $d \in \mathbb{Q}_p^*$. Since $x^3 + ax + b$ has only one real root by the positivity of a, we have $E^d(\mathbb{R}) \cong \mathbb{R}/\mathbb{Z}$ for all $d \in \mathbb{R}$ by Lemma 3.25. Now Proposition 3.15 yields that $E^{d_3}(\mathbb{Q}_3) \times E^{d_\infty}(\mathbb{R})$ is topologically cyclic for all $d_3 \in \mathbb{Q}_3$ and $d_\infty \in \mathbb{R}$. Finally, Proposition 3.27 implies that E has good twists with respect to $\{3, \infty\}$, so $X(\mathbb{Q})$ is dense in $X(\mathbb{Q}_3) \times X(\mathbb{R})$ by Theorem 3.20.

Now assume $p \neq 3$. We assume that a and b in $\mathbb{Q}$ are such that $v_p(a) > 0$, and $v_p(b) = 1$; if $p = 2$ we require additionally that $a > 0$, if $p = 5$ we require

additionally that $a \not\equiv \pm 10 \pmod{25}$, and if $p = 7$, we require additionally that $b \not\equiv \pm 14 \pmod{49}$. Lemma 3.24(i)+(iii) gives that $E^{d_p}(\mathbb{Q}_p)$ is a procyclic group of order p^∞ or $3 \cdot p^\infty$ for all $d \in \mathbb{Q}_p^*$. Our assumptions on a and b together with Lemma 3.25 imply that, for all $d_\infty \in \mathbb{R}$, the group $E^{d_\infty}(\mathbb{R})$ is isomorphic to $\mathbb{R}/\mathbb{Z}$ or $\mathbb{R}/\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$; moreover, if $p = 2$, then, for all $d_\infty \in \mathbb{R}$, the group $E^{d_\infty}(\mathbb{R})$ is isomorphic to $\mathbb{R}/\mathbb{Z}$. Proposition 3.15 yields that $E^{d_p}(\mathbb{Q}_p) \times E^{d_\infty}(\mathbb{R})$ is topologically cyclic for all $d_p \in \mathbb{Q}_p$ and $d_\infty \in \mathbb{R}$. As in the previous case, we find that $X(\mathbb{Q})$ is dense in $X(\mathbb{Q}_p) \times X(\mathbb{R})$.

Finally, it follows from equation (3.2) that the conditions on a and b given above correspond to infinitely many $\overline{\mathbb{Q}}$-isomorphism classes of elliptic curves. The theorem thus follows from Corollary 3.30. □

Proof of Theorem 3.2. Assume that the elliptic curve E is given by $y^2 = x^3 + ax + b$ with $a, b \in \mathbb{Q}$. For p and q as in the theorem, we give conditions on a and b implying that, if $X = \mathrm{Km}(E \times E)$, then $X(\mathbb{Q})$ is dense in $X(\mathbb{Q}_p) \times X(\mathbb{Q}_q) \times X(\mathbb{R})$. We may assume that $p < q$.

We assume that a and b in $\mathbb{Q}^*$ are such that they satisfy the following conditions: $a > 0$, $v_p(a) = 1$, $v_p(b) > 1$, $v_q(a) > 0$, and $v_q(b) = 1$; if one of p and q equals 5, we require additionally that $a \not\equiv \pm 10 \pmod{25}$, and if $q = 7$, we require additionally that $b \not\equiv \pm 14 \pmod{49}$. According to parts (i), (iii) and (iv) of Lemma 3.24 and Corollary 3.14, the group $E^{d_p}(\mathbb{Q}_p) \times E^{d_q}(\mathbb{Q}_q)$ is procyclic for all $d_p \in \mathbb{Q}_p$ and $d_q \in \mathbb{Q}_q$. Observe that $E^d(\mathbb{R})$ is isomorphic to $\mathbb{R}/\mathbb{Z}$ for all $d \in \mathbb{R}$ by the fact that $a > 0$. Then by Proposition 3.15, we get that $E^{d_p}(\mathbb{Q}_p) \times E^{d_q}(\mathbb{Q}_q) \times E^{d_\infty}(\mathbb{R})$ is topologically cyclic for all choices of $d_p \in \mathbb{Q}_p$, $d_q \in \mathbb{Q}_q$, and $d_\infty \in \mathbb{R}$. By Proposition 3.27 and Theorem 3.20, we have that $X(\mathbb{Q})$ is dense in $X(\mathbb{Q}_p) \times X(\mathbb{Q}_q) \times X(\mathbb{R})$.

As in the proof of Theorem 3.1, the conditions on a and b given above correspond to infinitely many $\overline{\mathbb{Q}}$-isomorphism classes of elliptic curves. Hence, again by Corollary 3.30, we are done. □

3.5 Large product topologies

Lemma 3.31. *Let $p > 3$ be a prime number and let $\mathscr{E}$ be an elliptic curve over $\mathbb{Q}_p$ with good reduction. Assume that the groups $\widetilde{\mathscr{E}}(\mathbb{F}_p)$ and $\widetilde{\mathscr{E}^t}(\mathbb{F}_p)$ are both cyclic of order coprime to p, where $\widetilde{\mathscr{E}}$ is the reduction modulo p of $\mathscr{E}$ and $\widetilde{\mathscr{E}^t}$ its unique non-trivial quadratic twist. Then $\mathscr{E}^d(\mathbb{Q}_p)$ is a procyclic*

group for all $d \in \mathbb{Q}_p^*$. Moreover, its order is equal to

$$\#\mathscr{E}^d(\mathbb{Q}_p) = \begin{cases} \#\widetilde{\mathscr{E}}(\mathbb{F}_p) \cdot p^\infty & \text{if } d \in \mathbb{Q}_p^{*2} \\ \#\widetilde{\mathscr{E}^t}(\mathbb{F}_p) \cdot p^\infty & \text{if } d \notin \mathbb{Q}_p^{*2} \text{ and } v_p(d) \text{ is even} \\ \#\widetilde{\mathscr{E}}(\mathbb{F}_p)[2] \cdot p^\infty & \text{if } v_p(d) \text{ is odd} \end{cases}$$

Proof. By changing to a $\mathbb{Q}_p$-isomorphic curve if necessary, it suffices to restrict to the case where $d \in \mathbb{Q}_p^*$ satisfies $v_p(d) = 0$ or $v_p(d) = 1$. First assume that we have $v_p(d) = 0$. Since p is a prime of good reduction for $\mathscr{E}^d$, by [32, VII.2.1] we have a short exact sequence

$$0 \to \mathscr{E}_1^d(\mathbb{Q}_p) \to \mathscr{E}^d(\mathbb{Q}_p) \to C \to 0 \tag{3.4}$$

where $\mathscr{E}_1^d(\mathbb{Q}_p)$ is the kernel of reduction of $\mathscr{E}^d$, which is topologically isomorphic to $\mathbb{Z}_p$ by [32, IV.6.4(b)], and C is $\widetilde{\mathscr{E}}(\mathbb{F}_p)$ if $d \in \mathbb{Z}_p^{*2}$ and $\widetilde{\mathscr{E}^t}(\mathbb{F}_p)$ otherwise. By assumption, the order of C is coprime to p. By Proposition 1.14(iv), then we must have

$$\mathscr{E}^d(\mathbb{Q}_p) \cong \mathscr{E}_1^d(\mathbb{Q}_p) \times C, \tag{3.5}$$

with C as above. Therefore, the group $\mathscr{E}^d(\mathbb{Q}_p)$ is a procyclic topological group by Corollary 3.14. Since $\mathscr{E}^d(\mathbb{Q}_p)$ is a direct product, its order is the product of the orders of $\mathscr{E}_1^d(\mathbb{Q}_p)$ and C. This proves the lemma in the case $v_p(d) = 0$.

Now we assume that $v_p(d) = 1$. The minimal discriminant of the twist $\mathscr{E}^d$ has valuation 6, and from the table in [32, C.15] we see that $\mathscr{E}^d$ is of reduction type I_0^*, and the component group of the special fibre of its Néron model is isomorphic to a subgroup of the Klein four-group. Hence $\mathscr{E}^d(\mathbb{Q}_p)$ sits in a short exact sequence of topological groups

$$0 \to \mathscr{E}_0^d(\mathbb{Q}_p) \to \mathscr{E}^d(\mathbb{Q}_p) \to \Phi \to 0, \tag{3.6}$$

where Φ is isomorphic to a subgroup of the Klein four-group. Since $\mathscr{E}^d$ can be given of an equation $y^2 = x^3 + ad^2x + bd^3$ with a and b in $\mathbb{Z}_p$, the group $\mathscr{E}_0^d(\mathbb{Q}_p)$ is topologically isomorphic to $\mathbb{Z}_p$ by Theorem 1.1. We conclude that $\mathscr{E}^d(\mathbb{Q}_p)$ is an extension of a finite abelian 2-group by $\mathbb{Z}_p$, and hence must be isomorphic to the direct product by Proposition 1.14(iv). We have then that $\Phi = \Phi[2] = \mathscr{E}^d(\mathbb{Q}_p)[2]$, and this is isomorphic to $\mathscr{E}(\mathbb{Q}_p)[2]$ since the twisting does not affect the 2-torsion. We have $\mathscr{E}(\mathbb{Q}_p)[2] = \widetilde{\mathscr{E}}(\mathbb{F}_p)[2]$ by (3.6) and Proposition 1.14(iv). Since $\widetilde{\mathscr{E}}(\mathbb{F}_p)$ is cyclic, so is $\widetilde{\mathscr{E}}(\mathbb{F}_p)[2]$, and therefore $\mathscr{E}^d(\mathbb{Q}_p) \cong \mathscr{E}_0^d(\mathbb{Q}_p) \times \widetilde{\mathscr{E}}(\mathbb{F}_p)[2]$ is procyclic by Corollary 3.14. The assertion about the order follows as in the first part. □

The following corollary will be used to prove Theorem 3.3.

Corollary 3.32. *Let S be a set of prime numbers > 3 such that:*

(i) for all $p \in S$, the elliptic curve E has good reduction at p;

(ii) for all $p \in S$ and all $\delta \in \mathbb{F}_p^*$, the group $\widetilde{E}^\delta(\mathbb{F}_p)$ is cyclic, where $\widetilde{E}$ denotes the reduction of E modulo p;

(iii) for all $(\delta_p)_p \in \prod_{p\in S} \mathbb{F}_p^*$, the numbers $\#\widetilde{E}^{\delta_p}(\mathbb{F}_p)$ are pairwise coprime, and are coprime to $\log_2 \#E(\mathbb{R})[2]$ and the elements of S.

Then if $X = \mathrm{Km}(E \times E)$, then $X(\mathbb{Q})$ is dense in $X(\mathbb{R}) \times \prod_{p\in S} X(\mathbb{Q}_p)$.

Proof. Lemma 3.31 shows that, for all $p \in S$, the prime numbers dividing the orders of the groups $E^d(\mathbb{Q}_p)$, as d runs through $\mathbb{Q}_p^*$, are equal to p and the primes dividing $\#\widetilde{E}^\delta(\mathbb{F}_p)$, where δ runs through $\mathbb{F}_p^*$. Lemma 3.14 and assumptions (i)-(iii) then imply that, for all $(d_p)_p \in \prod_{p\in S} \mathbb{Q}_p^*$, the topological groups $E^{d_p}(\mathbb{Q}_p)$ are procyclic and pairwise of coprime order.

By Proposition 3.15 and the fact that the numbers $\#\widetilde{E}^{\delta_p}(\mathbb{F}_p)$ are coprime to $\log_2 \#E(\mathbb{R})[2]$ for all $p \in S$ and $\delta_p \in \mathbb{F}_p^*$, the groups $E^{d_\infty}(\mathbb{R}) \times \prod_{p\in S} E^{d_p}(\mathbb{Q}_p)$ are topologically cyclic for all $(d_p)_p \in \prod_{p\in S} \mathbb{Q}_p^*$ and $d_\infty \in \mathbb{R}$. The result now follows from Proposition 3.27 and Theorem 3.20. □

Theorem 3.33. *Assume that E is given by $y^2 = x^3 + x + 1$. Let S be the following set of 331 primes:* $S = \{$467, 1033, 1289, 1823, 2081, 2221, 2591, 2887, 3163, 3229, 4691, 4751, 6047, 7103, 7883, 8069, 8663, 9221, 11909, 12149, 12211, 13451, 13567, 14207, 14419, 14557, 15299, 15959, 18089, 18233, 19889, 20201, 20857, 21379, 21803, 24509, 25031, 26711, 27091, 28477, 28607, 29333, 29723, 32309, 37139, 38791, 39359, 39953, 40519, 41957, 42179, 44867, 45233, 45757, 47501, 48767, 49711, 50581, 51563, 52379, 53699, 55487, 56951, 57089, 57413, 63659, 64153, 64217, 66347, 68927, 71597, 71987, 72139, 72869, 73061, 73583, 73613, 73849, 76679, 77377, 78179, 78889, 79531, 81197, 81953, 82883, 82997, 84299, 85061, 85259, 87407, 87641, 88741, 89909, 90373, 90499, 92699, 98519, 98801, 102533, 104831, 105563, 108161, 108877, 110237, 112403, 116131, 117659, 122051, 125399, 125899, 125941, 126397, 131321, 131507, 131797, 133769, 135851, 135887, 136531, 137239, 137867, 138869, 139921, 140269, 144299, 145139, 145829, 146801, 147083, 148157, 148663, 149533, 149731, 149921, 151637, 154849, 157019, 157901, 159899, 164581, 164617, 165713, 166949, 167879, 169859, 170953, 173501, 174413, 175361, 182687, 184187, 185599, 186583, 187373, 187787, 187931, 188171, 190409, 192233, 194891,

195103, 196709, 197441, 198959, 199313, 199603, 199783, 202031, 203531, 204557, 204973, 205129, 205441, 209123, 210907, 212081, 214507, 214559, 219251, 220771, 221261, 221411, 222109, 225371, 228601, 228913, 230389, 230999, 231109, 232607, 234989, 238181, 238213, 239119, 240319, 241727, 242083, 242453, 245753, 251171, 251879, 251969, 253109, 254369, 263489, 263849, 265091, 265711, 266089, 266129, 267749, 268253, 270329, 271619, 272549, 273281, 274831, 276323, 278819, 278917, 280061, 280963, 281893, 283837, 287003, 287501, 289343, 289607, 290767, 291371, 291559, 292133, 293071, 297191, 297589, 306781, 308003, 310087, 311237, 314407, 315461, 315527, 315899, 317459, 319031, 320611, 322079, 322583, 324983, 325229, 327517, 328589, 330439, 332851, 333791, 337327, 337907, 339517, 342389, 342527, 344429, 347993, 350159, 352309, 353401, 353963, 354337, 361789, 364853, 365929, 370067, 371737, 371873, 372397, 376039, 376577, 379913, 380189, 381209, 381527, 390703, 393299, 393539, 402419, 408461, 409391, 414077, 414893, 419599, 419789, 421703, 422407, 423221, 424601, 427169, 429887, 431521, 433859, 439661, 440983, 442333, 443759, 447257, 450847, 453569, 456553, 456679, 457381, 460099, 462311, 466061, 467651, 470279, 471923, 472057, 475793, 476137, 477409, 478679, 480463, 481097, 486449, 487717, 491149, 491327, 493291, 494699, 495449, 495947, 495973 }. *Then* $E(\mathbb{Q})$ *is dense in* $E(\mathbb{R}) \times \prod_{p\in S} E(\mathbb{Q}_p)$.

Proof. One proves this by taking the list S and verifying (for example with the help of `sage`) that E and S as in the theorem satisfy the hypotheses of Corollary 3.32.

The assertion about the cardinality of S is left to the reader. □

Proof of Theorem 3.3. Theorem 3.3 follows from Theorem 3.33. □

Remark 3.34. The list S in Theorem 3.33 was found by defining the following procedure in `sage` [35]. The prime numbers that are to be included in S are contained in the set `greedyList`; this set is only added to while the procedure runs. The set `primeList` keeps track of the prime numbers p whose inclusion in S still has to be decided; it is equal to the set of prime numbers between `min_p` and `max_p` at the start of the procedure, and every time a new prime number p is added to S, the prime divisors of $\#\widetilde{E}^{\delta}(\mathbb{F}_p)$ are removed from it, where δ runs over the elements of $\mathbb{F}_p^*$. The set `greedyBlacklist` contains the primes in `greedyList` as well as the set of prime divisors of $\widetilde{E}^{\delta}(\mathbb{F}_p)$, where p runs over the elements of `greedyList` and δ runs over the elements of $\mathbb{F}_p^*$. If $E(\mathbb{R})[2] = 4$, the initial value of `greedyBlacklist` is $\{2\}$, otherwise its initial value is $\emptyset$.

```
def findPrimes(E,min_p,max_p):
    Disc = E.discriminant()
    min_p = max(min_p,5)

    primeList = set([p for p in prime_range(min_p,max_p)])
    greedyList = set([])
    greedyBlacklist = set([])
    phi_2 = (E.division_polynomial(2)).change_ring(RR)
    if len(phi_2.roots()) == 3:
        greedyBlacklist.add(2)

    while primeList != set([]):
        p = primeList.pop()
        if (Disc % p) != 0 and p not in greedyBlacklist:
            Ep = E.base_extend(GF(p))
            A = Ep.abelian_group()
            B = Ep.quadratic_twist().abelian_group()
            if A.is_cyclic() == true:
                if B.is_cyclic() == true:
                    S = set(A.order().prime_divisors())
                    T = set(B.order().prime_divisors())
                    U = S.union(T)
                    greedyList.add(p)
                    for s in U:
                        if s == p or s in greedyBlacklist:
                            greedyList.remove(p)
                            break
            if p in greedyList:
                Up = U.union([p])
                greedyBlacklist = greedyBlacklist.union(Up)
                primeList = primeList.difference(U)
    return(greedyList);
```

One gets the list S in Theorem 3.33 by running the commands

```
E = EllipticCurve([1,1]); min_p = 5; max_p = 500000
findPrimes(E,min_p,max_p)
```

3.6 Proof of Theorem 3.4

We keep our notation and assumptions as explained in section 3.3.1.

Theorem 3.35. *Assume that $E/\mathbb{Q}$ is given by $y^2 = x^3 + x$. Then $X(\mathbb{Q})$ is dense in $X(\mathbb{Q}_p)$ for all p with $p \equiv 3 \pmod 4$ and $p > 7$.*

Proof. Let p be a prime congruent to 3 mod 4. For $d \in \mathbb{Q}_p^*$, the twist E^d of E is given by the equation $y^2 = x^3 + d^2x$. By Lemma 3.27 and Theorem 3.20, it suffices to show that $E^d(\mathbb{Q}_p)$ is procyclic for all $d \in \mathbb{Q}_p^*$. By changing to a $\mathbb{Q}_p$-isomorphic curve if necessary, it suffices to restrict to the case of $d \in \mathbb{Q}_p^*$ with $v_p(d)$ equal to 0 or 1.

First assume $v_p(d) = 0$. Let $\widetilde{E^d}$ be the reduction of E^d modulo p. Then $\#\widetilde{E^d}(\mathbb{F}_p) = p + 1$. This follows from the fact that $\widetilde{E^d}$ is supersingular [32, V.4.5] and the fact that $p > 3$. We claim that $\widetilde{E^d}(\mathbb{F}_p)$ is cyclic. Suppose that $(\mathbb{Z}/\ell\mathbb{Z})^2 \subset \widetilde{E^d}(\mathbb{F}_p)$ for some prime ℓ. Then p must split completely in $\mathbb{Q}(\zeta_\ell)$, giving $\ell \mid p-1$. On the other hand ℓ must certainly divide $\#\widetilde{E^d}(\mathbb{F}_p) = p+1$; therefore we must have $\ell = 2$. But since x^3+d^2x has a linear and a quadratic irreducible factor over $\mathbb{F}_p$, we must have $\#\widetilde{E^d}(\mathbb{F}_p)[2] = 2$. This gives a contradiction, proving the claim.

By [32, VII.2.1] and the fact that E^d has good reduction at p, we have a short exact sequence:

$$0 \to E_1^d(\mathbb{Q}_p) \to E^d(\mathbb{Q}_p) \to \widetilde{E^d}(\mathbb{F}_p) \to 0,$$

where the kernel of reduction $E_1^d(\mathbb{Q}_p)$ of E^d is isomorphic to $\mathbb{Z}_p$ by [32, IV.6.4(b)]. We conclude that $E^d(\mathbb{Q}_p)$ is topologically isomorphic to the direct product of $\mathbb{Z}_p$ and a cyclic group of order $p + 1$. By Proposition 1.14(iv), the group $E^d(\mathbb{Q}_p)$ is procyclic.

Now assume $v_p(d) = 1$. Then E^d has additive reduction with Kodaira type IV [32, C.15]. Hence we have a short exact sequence

$$0 \to E_0^d(\mathbb{Q}_p) \to E^d(\mathbb{Q}_p) \to G \to 0,$$

where $E_0^d(\mathbb{Q}_p)$ is topologically isomorphic to $\mathbb{Z}_p$ by Theorem 1.1, and G is isomorphic to a subgroup of the Klein four-group. Again by Proposition 1.14(iv), the group $E^d(\mathbb{Q}_p)$ is topologically isomorphic to the direct product of $\mathbb{Z}_p$ and G. Hence G is isomorphic to $E^d(\mathbb{Q}_p)[2] = E(\mathbb{Q}_p)[2]$, which we already knew to be isomorphic to $\mathbb{Z}/2\mathbb{Z}$. Hence by Corollary 3.14, the group $E^d(\mathbb{Q}_p)$ is procyclic. □

Proof of Theorem 3.4. Theorem 3.4 follows from Theorem 3.35. □

3.7 Proof of Theorem 3.5

In this section, we will now prove Theorem 3.5. The core of the proof of this theorem is a slight modification of the proof of Theorem 1 of [11] by Rajiv Gupta and M. Ram Murty. We will need the following lemma, which is reasonably standard.

Lemma 3.36. *Let p be a prime. Let E be an elliptic curve over $\mathbb{Q}$ and $\widetilde{E}$ its reduction modulo p. If $\widetilde{E}(\mathbb{F}_p)[\ell]$ is not cyclic for some prime ℓ, then $p \equiv 1 \pmod{\ell}$.*

Proof. If $\widetilde{E}(\mathbb{F}_p)[\ell]$ is not cyclic for some prime ℓ, the prime p must split completely in $\mathbb{Q}(E[\ell])$. By the existence of the Weil pairing, we have $\mathbb{Q}(\zeta_\ell) \subset \mathbb{Q}(E[\ell])$. Hence p splits completely in $\mathbb{Q}(\zeta_\ell)$. Now the theory of cyclotomic fields implies that $p \equiv 1 \pmod{\ell}$. □

Theorem 3.37. *For every elliptic curve E over $\mathbb{Q}$ such that $\#E(\mathbb{Q})[2] = 2$, the set of rational points of $\mathrm{Km}(E \times E)$ lies dense in the space of its p-adic points for infinitely many primes p.*

Proof. Take an elliptic curve E as in the statement of the theorem. Whenever we write $\widetilde{E}$, we will mean the reduction of E modulo the prime p under consideration and $\widetilde{E}^t$ for its non-trivial quadratic twist.

In this proof, we will call a prime p "good" for an elliptic curve E if the groups $\widetilde{E}(\mathbb{F}_p)$ and $\widetilde{E}^t(\mathbb{F}_p)$ are both cyclic, and "bad" otherwise. Applying Lemma 3.31, Proposition 3.27 and Theorem 3.20 in turn, one sees that it suffices to prove that there exist infinitely many primes p that are good for E. (Note that, since $\#E(\mathbb{Q})[2] = 2$, the condition in Lemma 3.31 that the order of both groups be different from p is automatically satisfied if p is not equal to 2 and is a prime of good reduction.)

We will restrict to a set of primes among which the primes that are good for E are easier to count. Following Gupta and Murty, we define the following set of primes for each pair of positive real numbers ϵ and x:

$$S_\epsilon(x) = \left\{ p \leq x \text{ prime } : \begin{array}{l} E \text{ has good reduction at } p, \text{ each odd prime} \\ \text{divisor of } p-1 \text{ is } \geq x^{1/4+\epsilon} \text{ and divides} \\ p-1 \text{ only once, and } p \text{ is non-split in } \mathbb{Q}(E[2]) \end{array} \right\}$$

In [11, Lemma 3], Gupta and Murty prove, using a result from sieve theory by Fouvry and Iwaniec [10], that there exists an $\epsilon > 0$ such that

$$\#S_\epsilon(x) \gg \frac{x}{\log^2 x}. \tag{3.7}$$

We choose an ϵ such that (3.7) holds, and we define $S(x) = S_\epsilon(x)$. For every integer a we let $S(a,x) \subset S(x)$ be the subset of primes p such that a_p is equal to a, where $a_p = p + 1 - \#\widetilde{E}(\mathbb{F}_p)$ is the trace of the Frobenius of E at p. By the Hasse–Weil bound, we have

$$S(x) = \coprod_{|a| \leq 2x^{1/2}} S(a,x).$$

We claim that if $x \in \mathbb{R}$ is large enough, then for every integer a with $|a| \leq 2x^{1/2}$, there are primes ℓ_a and ℓ_a^t, both greater than or equal to $x^{1/4+\epsilon}$, such that, for all $p \in S(a,x)$, we have that $\widetilde{E}(\mathbb{F}_p)[\ell]$ is cyclic for all primes $\ell \neq \ell_a$ and $\widetilde{E}^t(\mathbb{F}_p)[\ell']$ is cyclic for all primes $\ell' \neq \ell_a^t$. Choose an integer a such that $|a| \leq 2x^{1/2}$. First, assume that $p \in S(a,x)$ and $\widetilde{E}(\mathbb{F}_p)[\ell]$ is not cyclic. Then ℓ must be odd, since p does not split in $\mathbb{Q}(E[2])$. Then we must have

$$\ell^2 \mid \#\widetilde{E}(\mathbb{F}_p) = p + 1 - a. \tag{3.8}$$

We also have

$$\ell \mid p - 1 \tag{3.9}$$

by Lemma 3.37. This last fact implies, by the definition of $S(x)$ and the fact that ℓ is odd, that we have

$$\ell \geq x^{1/4+\epsilon} \tag{3.10}$$

Together, (3.8) and (3.9) imply $\ell \mid a - 2$. If x is large enough, then the integer a, whose absolute value is less than $2x^{1/2}$, has at most one prime divisor that is greater than or equal to $x^{1/4+\epsilon}$. Hence, if there is such a prime divisor ℓ_a, we have $\ell = \ell_a$. If there is no such prime divisor, we may set ℓ_a equal to any prime we want. For the other part, we assume that $p \in S(a,x)$ and $\widetilde{E}^t(\mathbb{F}_p)[\ell']$ is not cyclic. Now we use that $\ell^2 \mid \#\widetilde{E}^t(\mathbb{F}_p) = p + 1 + a$. Reasoning as before, we find that ℓ' must be an odd prime divisor of $a + 2$ that is greater than or equal to $x^{1/4+\epsilon}$. Again, there is at most one such a prime divisor for x large enough: if there exists one we will call it ℓ_a^t, and then we must have $\ell' = \ell_a^t$; if not, we let ℓ_a^t be arbitrary. This proves the claim made at the start of the paragraph.

Assuming that x is large enough as in the previous paragraph, we can now give a lower bound in terms of x on the number of primes p in $S(a,x)$ such that p is good for E in the sense defined earlier. If $p \in S(a,x)$ is bad for E, then we must have either $\ell_a^2 \mid p + 1 - a$ or $(\ell_a^t)^2 \mid p + 1 + a$. Since

both ℓ_a and ℓ_a^t are greater than or equal to $x^{1/4+\epsilon}$, and we have $p \leq x$, the number of $p \in S(a,x)$ that are bad for E is bounded above by

$$\frac{x}{\ell_a^2} + \frac{x}{(\ell_a^t)^2} + O(1) \leq \frac{x}{x^{1/2+2\epsilon}} + \frac{x}{x^{1/2+2\epsilon}} + O(1) = 2x^{1/2-2\epsilon} + O(1).$$

Summing the above over all integers a with $|a| \leq 2x^{1/2}$, we find that the total number of p in $S(x)$ that is bad for E is at most

$$4x^{1/2} \cdot \left(2x^{1/2-2\epsilon} + O(1)\right) = 8x^{1-2\epsilon} + O(x^{1/2}).$$

Comparing this with (3.7), we see that, for x large enough, the number of good primes in $S(x)$ grows at least as fast asymptotically as $\frac{x}{\log^2 x}$ times a constant. □

Proof of Theorem 3.5. Theorem 3.5 coincides with Theorem 3.37. □

Chapter 4

Refinements and computations

4.1 Introduction

We recall the following definition from chapter 3.

Definition 4.1. Let S be a set of primes.

(i) For $(d_p) \in \prod_{p\in S} \mathbb{Q}_p^*$ and $c \in \mathbb{Q}^*$, we call E^c a good twist of E with respect to (d_p) and S if for each $p \in S$ we have $c \in d_p\mathbb{Q}_p^{*2}$, and $E^c(\mathbb{Q})$ is dense in $\prod_{p\in S} E^c(\mathbb{Q}_p)$.

(ii) We say E has good twists if, for all $(d_p) \in \prod_{p\in S} \mathbb{Q}_p^*$, there is $c \in \mathbb{Q}^*$ such that E^c is a good twist of E with respect to (d_p) and S.

As before, if $S = \{p\}$ for some prime p, and if E has good twists with respect to (d_p) and S, we will also say that E has good twists with respect to d_p and p. If E has good twists with respect to S, we will also say that E has good twists with respect to p.

4.1.1 Goal of this chapter

In this chapter we will establish criteria for an elliptic curve E over $\mathbb{Q}$ to have good twists with respect to a prime p. In view of Theorem 3.20, the existence of good twists of E with respect to p implies that the rational points on $\mathrm{Km}(E \times E)$ lie p-adically dense. The crucial idea underlying all criteria established in this chapter is a construction of Jean-François Mestre [22], to be introduced in section 4.2.1. In section 4.7, we will use these criteria to perform a computer search for pairs (E, p) for which it is true that the rational points on $\mathrm{Km}(E \times E)$ lie p-adically dense.

4.1.2 Computer calculations

For an elliptic curve E over $\mathbb{Q}$ whose j-invariant is different from 0 and 1728, we will introduce the notion of a lucky prime number p for E in Definition 4.34. Prime numbers that are not lucky for E are called unlucky for E. The unlucky prime numbers include the prime numbers less than or equal to 7, and the primes for which E has bad reduction. It will be very easy to verify, using a Computer Algebra System, whether or not a prime number p is lucky for E. We will show in Proposition 4.35 that if p is lucky for E, and if $X = \mathrm{Km}(E \times E)$, then $X(\mathbb{Q})$ lies dense in $X(\mathbb{Q}_p)$. We have also created computer code (described in section 4.7) that computes the lucky prime numbers < 2000 for all elliptic curves E over $\mathbb{Q}$ given by $y^2 = x^3 + ax + b$, where a and b are integers such that $-5 \leq a \leq 5$ with $a \neq 0$, and $0 < b \leq 5$. Doing this, we have obtained the following result.

Theorem 4.2. *Let $S_{5,5}$ be the set of elliptic curves E over $\mathbb{Q}$ given by $y^2 = x^3 + ax + b$, where a and b are integers such that $-5 \leq a \leq 5$ with $a \neq 0$, and $0 < b \leq 5$. Then for all $E \in S_{5,5}$ there are at most 8 prime numbers p with $7 < p < 2000$ which are unlucky for E. Furthermore, for all prime numbers p such that $109 < p < 2000$ and all $E \in S_{5,5}$ we have that if p is unlucky for E, then p is a prime of bad reduction for E. If $E \in S_{5,5}$, and $X = \mathrm{Km}(E \times E)$, and p is a prime with $109 < p < 2000$ for which E has good reduction, then $X(\mathbb{Q})$ is dense in $X(\mathbb{Q}_p)$.*

The proof of Theorem 4.2 will be given at the end of section 4.7.

4.2 Definitions

Let k be a field of characteristic not equal to 2. Let a and b be elements of k such that

$$ab(4a^3 + 27b^2) \neq 0 \tag{4.1}$$

and define $f(x) = x^3 + ax + b$. Then the curve E over k given by $y^2 = f(x)$ is an elliptic curve with j-invariant not equal to 0 or 1728.

Remark 4.3. The assumption (4.1) also implies:

$$f(-b/a) = (-b/a)^3 + a(-b/a) + b = (-b/a)^3 \neq 0 \tag{4.2}$$

and

$$f(3b/a) = (3b/a)^3 + a(3b/a) + b = a^{-3}b\left(27b^2 + 4a^3\right) \neq 0; \tag{4.3}$$

in other words, $-b/a$ and $3b/a$ are not the x-coordinate of any 2-torsion point on E.

4.2.1 Mestre's construction

We now come to the construction by Mestre [22], which is of fundamental importance to the rest of this chapter. We shall denote

$$\phi(u) = -\frac{b}{a}\frac{u^4+u^2+1}{u^4+u^2}. \tag{4.4}$$

We will mostly interpret ϕ as a rational expression in whatever argument is given to it, but we will sometimes regard it as a morphism $\mathbb{P}^1_k \to \mathbb{P}^1_k$. Note that

$$u^2\phi(u) = \phi(u^{-1}).$$

For each $d \in k$, we define the smooth projective curve C^d over k as

$$C^d\colon dv^2 = f(\phi(u)).$$

For each $d \in k$, we have a morphism $\pi_1^d\colon C^d \to E^d$ sending (u,v) to $(\phi(u),v)$. It is clear from (4.4) that ϕ satisfies

$$a\phi(u)(u^4+u^2) = -b(u^4+u^2+1).$$

Multiplying both sides with (u^2-1), we get

$$a\phi(u)u^2(u^4-1) = b(1-u^6).$$

Rearranging this, we obtain

$$au^2\phi(u)+b = u^6(a\phi(u)+b).$$

Finally, from this it follows that we have

$$\begin{aligned} f(\phi(u^{-1})) = f(u^2\phi(u)) &= u^6\phi(u)^3 + au^2\phi(u) + b \\ &= u^6(\phi(u)^3 + a\phi(u) + b) = u^6 f(\phi(u)). \end{aligned}$$

For each $d \in k$ therefore, there exists the involution τ^d of C^d defined by

$$\begin{aligned} \tau^d\colon C^d &\to C^d \\ (u,v) &\mapsto (u^{-1}, u^3v) \end{aligned}$$

We define a second morphism $\pi_2^d\colon C^d \to E^d$ for each $d \in k$, by setting $\pi_2^d = \pi_1^d \circ \tau^d$. The morphism π_2^d sends (u, v) to $(u^2\phi(u), u^3 v)$.

Summarizing, we have two morphisms for each $d \in k$

$$\begin{aligned} \pi_1\colon C^d &\to E^d & \qquad \pi_2\colon C^d &\to E^d \\ (u,v) &\mapsto (\phi(u), v) & \qquad (u,v) &\mapsto (u^2\phi(u), u^3 v) \end{aligned}$$

as well as the following diagram

$$\begin{array}{ccc} C^d & \xrightarrow{\tau^d} & C^d \\ & {\scriptstyle \pi_1} \searrow \quad \swarrow {\scriptstyle \pi_2} & \\ & E^d & \end{array}$$

For brevity, we denote the curve C^1 by C, the automorphism τ^1 by τ, and the morphisms π_1^1 and π_2^1 from C to E by π_1 and π_2. This concludes the discussion of Mestre's construction.

Remark 4.4. Unless stated otherwise, when write (u_0, v_0) for a point on C, we will mean u_0 to be its u-coordinate, and v_0 to be its v-coordinate.

4.2.2 An affine model for C

We create an affine model for C that is smooth away from infinity. We introduce the change of variables $v' = u^3(u^2+1)^2 v$, resulting in a model for C of the form

$$v'^2 = g(u), \tag{4.5}$$

with $g(u)$ a polynomial of degree 14 equal to

$$g(u) = (u^2+1)\left(\left(-\frac{b}{a}\right)^3 (u^4+u^2+1)^3 - b(u^4+u^2+1)(u^4+u^2)^2 + b(u^4+u^2)^3 \right). \tag{4.6}$$

We will show that (4.5) defines a smooth affine curve in Proposition 4.8(ii). We have $g(0) = (-b/a)^3 \neq 0$. Relative to the model $v'^2 = g(u)$, the curve C has two points ∞_1 and ∞_2 at infinity. The maps $\pi_1\colon C \to E$ and $\pi_2\colon C \to E$ are now given by

$$\begin{aligned} \pi_1\colon C &\to E & \qquad \pi_2\colon C &\to E \\ (u, v') &\mapsto (\phi(u), u^{-3} v'(u^2+1)^{-2}) & \qquad (u, v') &\mapsto (u^2\phi(u), v'(u^2+1)^{-2}) \end{aligned}$$

while the automorphism $\tau\colon C \to C$ is given by

$$\begin{aligned} \tau\colon C &\to C \\ (u, v') &\mapsto (u^{-1}, u^{-7}v'). \end{aligned}$$

4.3 Creating good twists

In this section, we take $k = \mathbb{Q}$. The conditions on a and b, which are now elements of $\mathbb{Q}$, are as in the previous section, and the rest of the notation introduced there remains valid. The lemmas 4.5 and 4.6 in this subsection will explain the relevance of the curves C^d and the morphisms π_i^d. They will be used to construct good twists of E.

Lemma 4.5. *Take $k = \mathbb{Q}$. Let $\alpha, \beta \in k$ with $\beta \neq 0$, and write $c = f(\phi(\alpha))/\beta^2$. The point*

$$(\alpha, \beta)$$

lies on the curve C^c, and the points

$$(\phi(\alpha), \beta) \quad \text{and} \quad (\alpha^2\phi(\alpha), \alpha^3\beta)$$

lie on the elliptic curve E^c.

Proof. It is obvious that (α, β) lies on C^c. The two points $(\phi(a), \beta)$ and $(\alpha^2\phi(\alpha), \alpha^3\beta)$ are its images on E^c under π_1^c and π_2^c. □

Lemma 4.6. *Suppose that there exists $P \in C^d(\mathbb{Q}_p)$ such that $\pi_1^d(P)$ and $\pi_2^d(P)$ generate $E^d(\mathbb{Q}_p)$ topologically. Then there exists a good twist of E with respect to d and p.*

Proof. By perturbing P if necessary, we may assume that $u_0 = u(P)$ and $v_0 = v(P)$ are both finite, and that v_0 is non-zero. Choose u_0' and $v_0' \in \mathbb{Q}$ with $v_0' \neq 0$ such that u_0' is close to u_0 and v_0' is close to v_0. Define $c = f(\phi(u_0'))/v_0'^2$; by possibly taking u_0' and v_0' closer to u_0 and v_0, we may assume that $c/d \in \mathbb{Q}_p^{*2}$. By Lemma 4.5, the curve C^c contains the rational point (u_0', v_0'), and E^c contains the rational points

$$Q_1' = (\phi(u_0'), v_0')) \quad \text{and} \quad Q_2' = (u_0'^2\phi(u_0'), u_0'^3 v_0')).$$

Under the isomorphism defined over $\mathbb{Q}_p$

$$\begin{aligned} E^c &\to E^d \\ (x, y) &\mapsto (x, y\sqrt{c/d}) \end{aligned}$$

the points $\pm Q_1'$ and $\pm Q_2'$ map to points lying arbitrarily close to $\pm Q_1$ and $\pm Q_2$, where $Q_1 = \pi_1^d(P)$ and $Q_2 = \pi_2^d(P)$. Hence, possibly after taking u_0' and v_0' closer to u_0 and v_0, we get that Q_1' and Q_2' are topological generators of $E^c(\mathbb{Q}_p)$. □

Lemma 4.6 provides the implication going from a purely p-adic statement to a statement about rational points. Therefore, after establishing some elementary properties of the curves C^d, we will restrict to $k = \mathbb{Q}_p$. Later on, in section 4.6, we will go back to assuming $k = \mathbb{Q}$, and we will use Lemma 4.6 to draw conclusions about the existence of good twists. In fact, the hypothesis of Lemma 4.6 is so important in this chapter, that we will make it into a definition.

Definition 4.7. We will say that $P \in C^d(\mathbb{Q}_p)$ is a Mestre point if the points $\pi_1^d(P)$ and $\pi_2^d(P)$ generate $E^d(\mathbb{Q}_p)$ topologically.

4.4 Properties of the curve C

In this section, the field k is an arbitrary field of characteristic not equal to 2. We will collect some information on C (defined in section 4.2.1) and its maps to E. Let the assumptions and notation on the ground field k, the curve E, the curve C, and the maps π_1,π_2 and τ be as in section 4.2.

Proposition 4.8. *The following statements are true.*

(i) The branch locus of π_1 consists of the points on E with x equal to $-b/a$ or $3b/a$. The ramification loci of π_1 and π_2 are disjoint.

(ii) The polynomial g is separable. The genus of C is equal to 6.

Proof. We let C' be the smooth projective curve defined by

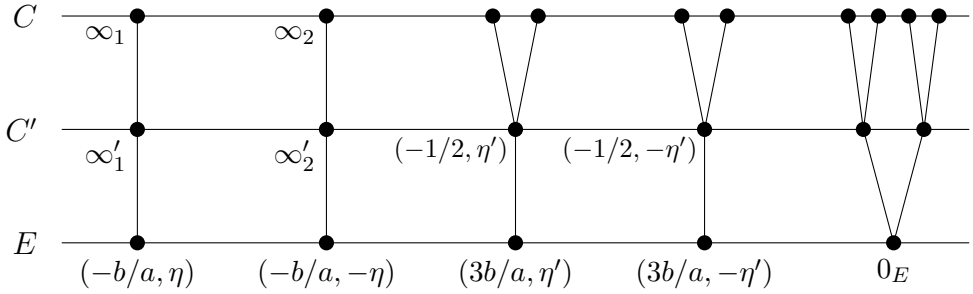
$$C' \colon v^2 = f\left(-\frac{b}{a}\frac{w^2+w+1}{w^2+w}\right).$$

Putting $v'' = v(w^2+w)^2$, we obtain for C' an affine model of the form $v''^2 = h(w)$ with $h(w)$ a polynomial of degree 8 with a simple zero at 0. Note that, relative to this model, the curve C' has two points ∞_1', ∞_2' at infinity. In terms of the coordinates (u, v') on C, and the coordinates (w, v'') on C', we define the maps

$$\begin{aligned} &\pi_1' \colon C \to C' && \pi_1'' \colon C' \to E \\ &(u, v') \mapsto (u^2, uv') && (w, v'') \mapsto \left(-\frac{b}{a}\frac{w^2+w+1}{w^2+w}, v''(w^2+w)^{-2}\right) \end{aligned}$$

With these definitions, we have factored the map π_1 as $\pi_1'' \circ \pi_1'$.

In view of (4.2) and (4.3), the points on E with x-coordinates $-b/a$ or $3b/a$ do not belong to the 2-torsion on E, and hence there are two of both.



We analyze the ramification of the degree-two map $\pi_1'' \colon C' \to E$. It is unramified above the identity 0_E of E, since the points with $w = 0$ or $w = -1$ map to 0_E. It is ramified at the two points (w, v) where $w = \infty$, which map to the points with $x = -b/a$. If w is finite, not equal to 0 or -1, and π_1'' is ramified at (w, v), then the equation

$$-\frac{b}{a}\frac{T^2+T+1}{T^2+T} = -\frac{b}{a}\frac{w^2+w+1}{w^2+w} =: x_0$$

must have a unique solution $T = w$; equivalently, the polynomial

$$T^2 + T + \frac{b}{ax_0 + b}$$

has its unique zero at $T = w$. Hence we must have $b/(ax_0 + b) = 1/4$. In that case, we must therefore have $x_0 = 3b/a$ and $w = -1/2$. Summarizing, we have found that π_1'' is ramified at the points (w, v) lying above the points where $x = -b/a$, which have $w = \infty$, and at the points (w, v) lying above the points where $x = 3b/a$, which have $w = -1/2$.

Next, we analyze the ramification of the degree-two map $\pi_1' \colon C \to C'$ that, in terms of the models constructed at the start of the proof, sends (u, v') to (u^2, uv'). It is certainly unramified above points where w is not 0 or ∞. It is also unramified above points where $w = 0$; indeed, there is a single point on C' where $w = 0$, which corresponds to the smooth point $(0, 0)$ on the model $v''^2 = h(w)$ for C' obtained before, whereas on C there are two points with $u = 0$. We claim further that π_1' is ramified above the points at infinity ∞_1' and ∞_2'. Indeed, it is clear that the preimage of $\{\infty_1', \infty_2'\}$ under π_1' is $\{\infty_1, \infty_2\}$.

Summarizing, we have shown, firstly, that π_1'' ramifies at ∞_1' and ∞_2', which map to the two points where $x = -b/a$, and at the two points where w equals $-1/2$, which map to the points where $x = 3b/a$; secondly, that π_1' ramifies at the two points ∞_1 and ∞_2, which map to ∞_1' and ∞_2'. This shows that π_1 is ramified at ∞_1 and ∞_2, each with ramification index 4, and at the four points where $u^2 = -1/2$, each with ramification index 2. Applying the automorphism τ, we get that π_2 is ramified at the two points where $u = 0$ with ramification index 4, and at the four points where $u^2 = -2$, each with ramification index 2. This shows that the ramification loci are disjoint.

Now we prove (ii). From (4.6), we see that the set of zeros of g is the union of the set of zeros of $u^2 + 1$, and the set of u with $u^4 + u^2 \neq 0$ such that

$$f(\phi(u)) = f\left(-\frac{b}{a}\frac{u^4 + u^2 + 1}{u^4 + u^2}\right) \tag{4.7}$$

is zero. We see from (4.2) and (4.3) that $f(\phi(u)) = 0$ implies $\phi(u) \neq -b/a$ and $\phi(u) \neq 3b/a$, hence π_1 is unramified above $E[2]$. This shows that there are exactly 12 values of u for which (4.7) vanishes. Hence g has 14 distinct zeros, and therefore it can have no repeated roots. This shows that C has genus 6, and ends the proof. □

Remark 4.9. Part (ii) of Proposition 4.8 was mentioned by Mestre [22].

We define the map

$$i\colon C \to E \times E \tag{4.8}$$

as the map given by (π_1, π_2). Also, we will use the letter Z to denote the (reduced) closed subscheme of C consisting of the points (u, v) with

$$u^4 + u^2 + 1 = 0 \quad \text{or} \quad v = 0.$$

Using (4.5) and (4.6), we see that $Z \times_k \overline{k}$ consists of the 8 points where $u^4 + u^2 + 1 = 0$, and the 14 points where $v = 0$, hence 22 points in total.

Proposition 4.10. *The restriction of i to $C - Z$ is an embedding.*

Proof. We resume the notation of the proof of Proposition 4.8. We first claim that $i|_{C-Z}$ is injective, and that $i(C - Z)$ and $i(Z)$ are disjoint; from this we will deduce that $i|_{C-Z}$ is a homeomorphism onto its image. Let P be a point on $C - Z$ and write (Q_1, Q_2) for the point on $E \times E$ that is the image of P under i. By definition of i, we have $Q_1 = \pi_1(P)$ and $Q_2 = \pi_2(P)$. We distinguish three pairwise exclusive possibilities for (Q_1, Q_2).

Case (a): we have $Q_1 = 0_E$ or $Q_2 = 0_E$. First suppose $P \notin Z$. If $Q_1 = 0_E$, we have that $u(P) = 0$ or $u(P)^2 + 1 = 0$; since $P \notin Z$, we must have $u(P) = 0$. We get that $u(\tau(P)) = u(P)^{-1} = \infty$, hence $\tau(P) = \infty_1$ or $\tau(P) = \infty_2$, and we have $Q_2 = \pi_1(\tau(P)) = (-b/a, \pm\eta)$, where $\eta^2 = f(-b/a)$. If $Q_2 = 0_E$, we can apply τ to the result of the previous calculation to find that $Q_1 = (-b/a, \pm\eta)$. Hence, there are four possibilities for P: the two points with $u(P) = 0$ and the two points with $u(P) = \infty$. The first pair maps to the two points $(0_E, (-b/a, \pm\eta))$, the second pair maps to the two points $((-b/a, \pm\eta), 0_E)$. Now suppose $P \in Z$. Reasoning as before, we find that $Q_1 = 0_E$ or $Q_2 = 0_E$ implies $u(P)^2 + 1 = 0$. One checks that i sends the points satisfying $u^2 + 1 = 0$ to $(0_E, 0_E)$.

Case (b): we have $x(Q_1) = 0$ or $x(Q_2) = 0$. Then we have either $\phi(u(P)) = 0$ or $u(P)^2\phi(u(P)) = 0$. In either case we have $u(P)^4 + u(P)^2 + 1 = 0$. Hence P lies in Z. Conversely, if P is such that $u(P)^4+u(P)^2+1 = 0$, then we have both $x(Q_1) = 0$ and $x(Q_2) = 0$.

Case (c): we have that $x_1 = x(Q_1)$ and $x_2 = x(Q_2)$ are both finite and non-zero. By the discussion of the previous case, we have $u(P)^4+u(P)^2+1 \neq 0$. Then since $x_1 = \phi(u(P))$ and $x_2 = u(P)^2\phi(u(P))$, we have that $u(P)$ is also finite and non-zero. If we further put $y_1 = y(Q_1)$ and $y_2 = y(Q_2)$, then from $y_1 = v(P)$ we get that y_1 is also finite. First assume that $y_1 = v(P)$ is zero. Then $P \in Z$. Assuming that $y_1 = v(P)$ is non-zero, then since we also had $u(P)^4 + u(P)^2 + 1 \neq 0$, we must have $P \notin Z$. Since we have $y_2 = u(P)^3v(P) = u(P)^3y_1$, we can find back $u(P)$ from x_1, x_2, y_1, y_2 as $u(P) = x_2y_2/(x_1y_1)$, and we can find $v(P)$ back as $v(P) = y_1$. Hence P is determined by Q_1 and Q_2 in case (c).

Clearly, cases (a) through (c) exhaust the possibilities for the pair (Q_1, Q_2). The discussion of the three cases above then establishes the claim that the restriction to $C - Z$ of i is injective, and that $i(C - Z)$ is disjoint from $i(Z)$. Since i is proper, it is closed and since $i(C - Z)$ is disjoint from $i(Z)$, we must have that the map $i|_{C-Z}$ is closed onto its image. Since $i|_{C-Z}$ is moreover injective and continuous, we get that it is a homeomorphism onto its image.

To prove that $i|_{C-Z}$ is an embedding in the sense of algebraic geometry, it is enough by the proof of [12, Lemma II.7.4] to show that it separates tangent vectors, i.e., that, for each $P \in C$, the map

$$T_PC \to T_{i(P)}(E \times E) = T_{\pi_1(P)}(E) \times T_{\pi_2(P)}(E)$$

induced by i is an injection. By dualizing, this is equivalent to showing that

the pull-back map

$$i_P^*\colon T^*_{\pi_1(P)}(E) \times T^*_{\pi_2(P)}(E) \to T_P^*C \tag{4.9}$$

on cotangent spaces is surjective for all $P \in C$. Let ω be the invariant differential

$$\omega = \frac{dx}{y} \in H^0(E, \Omega^1_E)$$

on E. Since T_P^*C is a one-dimensional k-vector space, it suffices to check that for each $P \in C$, at least one of the everywhere-regular differential forms $\pi_1^*\omega$ and $\pi_2^*\omega$ on C is non-zero at P. One easily computes that

$$\pi_1^*\omega = \frac{1}{v} d\left(-\frac{b}{a}\frac{u^4+u^2+1}{u^4+u^2}\right) = \frac{2b}{a}\frac{2u^2+1}{u^3v(u^2+1)^2}du = \frac{2b}{a}\frac{2u^2+1}{v'}du$$

and

$$\pi_2^*\omega = \frac{1}{v} d\left(-\frac{b}{a}\frac{u^4+u^2+1}{u^2+1}\right) = -\frac{2b}{a}\frac{u^2+2}{(u^2+1)^2v}du = -\frac{2b}{a}\frac{u^3(u^2+2)}{v'}du.$$

One computes that the zero-locus of $\pi_1^*\omega$ consists of $\{\infty_1, \infty_2\}$ as well as the points where $u^2 = -1/2$, while the zero-locus of $\pi_2^*\omega$ consists of the points where $u^2 = 0$ or $u^2 = -2$. Hence (4.9) is surjective for all $P \in C$, and so $i\colon C \to E \times E$ separates tangent vectors. This concludes the proof of the proposition. □

The following lemma will be used in the proof of Proposition 4.12. We keep the assumption that k is a field of characteristic not equal to 2.

Lemma 4.11. *Let e_1, e_2, e_3 be the roots of $f = x^3 + ax + b$ in $\overline{k}$, and let $\{\lambda, \mu, \nu\} = \{1, 2, 3\}$. Then the roots in $\overline{k}$ of the polynomial*

$$T^2 + T + \frac{b}{ae_\lambda + b} \tag{4.10}$$

are e_μ/e_λ and e_ν/e_λ. If furthermore k is a p-adic field with $p \neq 2$, and e_1, e_2 and e_3 are of equal valuation in k, then one of the elements

$$\frac{e_1}{e_2}, \frac{e_2}{e_3}, \text{ and } \frac{e_3}{e_1}$$

is a square in $k(e_1, e_2, e_3)$.

Proof. Without loss of generality, we assume that we have $\lambda = 1, \mu = 2, \nu = 3$. Long division gives $f = (x - e_1)g$ with

$$g = (x^2 + e_1 x + a + e_1^2),$$

so that we have

$$(x-e_2/e_1)(x-e_3/e_1) = e_1^{-2} g(e_1 x) = x^2+x+\frac{a+e_1^2}{e_1^2} = x^2+x+\frac{-b/e_1}{(-ae_1-b)/e_1},$$

from which the first claim follows. The second one is clear. □

Proposition 4.12. *Let ϕ_1 denote ϕ and let ϕ_2 denote the function $u \mapsto u^2\phi(u)$. Let k be a finite extension of $\mathbb{Q}_p$ for some prime number p with $p \neq 2$, and assume that the zeros of f in $\overline{k}$ have the same valuation.*

(i) Let i be either 1 or 2. If f has three roots in k, then at least two of the roots of f are contained in $\phi_i(\mathbb{P}^1(k))$.

(ii) Let e_1, e_2, e_3 be the roots of f in $\overline{k}$, and let $\{\lambda, \mu, \nu\} = \{1, 2, 3\}$. Then

$$\phi_2(\phi_1^{-1}(e_\lambda)) = \{e_\mu, e_\nu\}.$$

Proof. We first prove assertion (i) for $i = 1$. For any $e \in k$, we have $e \in \phi_1(\mathbb{P}^1(k))$ if and only if there exists $u \in k$ such that

$$\phi_1(u) = -\frac{b}{a}\frac{u^4+u^2+1}{u^4+u^2} = e. \tag{4.11}$$

Let e_1, e_2, e_3 be the zeros of f. If for example $e = e_1$, Lemma 4.11 shows that the solutions to this equation are $u = \pm\sqrt{e_2/e_1}$ and $u = \pm\sqrt{e_3/e_1}$. For the cases where $e = e_2$ and $e = e_3$, the solutions follow from this by symmetry.

By the identity $(e_1/e_2)\cdot(e_2/e_3)\cdot(e_3/e_1) = 1$ and the fact that e_1, e_2, e_3 have equal valuation in k, we can choose λ, μ and ν such that $\{\lambda, \mu, \nu\} = \{1, 2, 3\}$ in such a way that e_λ/e_μ is a square in k. Therefore equation (4.11) has the solution $u_\lambda = \sqrt{e_\mu/e_\lambda}$ in k if $e = e_\lambda$, and the solution $u_\mu = 1/u_\lambda$ in k if $e = e_\mu$. Hence we find that u_λ is a preimage in k of e_λ under ϕ_1, and u_μ is a preimage in k of e_μ under ϕ_1. Hence assertion (i) is proven for $i = 1$. For $i = 2$, we need only observe

$$\phi_2(u_\lambda) = u_\lambda^2\phi(u_\lambda) = (e_\mu/e_\lambda)\cdot e_\lambda = e_\mu \tag{4.12}$$

and

$$\phi_2(u_\mu) = u_\mu^2 \phi(u_\mu) = (e_\lambda/e_\mu) \cdot e_\mu = e_\lambda.$$

We now prove (ii). We define $u'_\lambda = \sqrt{e_\nu/e_\lambda}$. The preimages of e_λ under ϕ_1 are $\pm u_\lambda$ and $\pm u'_\lambda$. We get $\phi_2(\pm u_\lambda) = e_\mu$ by (4.12), as well as

$$\phi_2(\pm u'_\lambda) = (e_\nu/e_\lambda) \cdot \phi(\pm u'_\lambda) = (e_\nu/e_\lambda) \cdot e_\lambda = e_\nu.$$

This concludes the proof of (ii). □

4.5 Existence criteria for Mestre points

In this section we will establish various criteria for the existence of Mestre points on C in the sense of Definition 4.7.

Definition 4.13. By a smooth curve (resp. surface) over $\mathbb{Z}_p$ we shall mean a scheme equipped with a smooth morphism to $\mathbb{Z}_p$ whose fibres are of dimension one (resp. two).

4.5.1 Assumptions and definitions

For the rest of this section, we assume that $p > 2$ is a prime, that $k = \mathbb{Q}_p$ and that a and b are elements of $\mathbb{Z}_p$ such that

$$ab(4a^3 + 27b^2) \in \mathbb{Z}_p^*. \tag{4.13}$$

The elliptic curve E over $\mathbb{Q}_p$ is defined as at the start of section 4.2, and we let $\mathcal{E}$ be the Weierstrass model of E defined by $y^2 = x^3 + ax + b$. By (4.13), we have that $\mathcal{E}$ is a smooth curve over $\mathbb{Z}_p$. In particular, the elliptic curve E has good reduction, and $\mathcal{E}$ is a minimal Weierstrass model of it. By $\mathcal{C}$ we denote the closure of $i(C)$ in $\mathcal{E} \times \mathcal{E}$, where i is as in (4.8), and by $\mathcal{Z}$ we denote the closure of $i(Z)$ in $\mathcal{E} \times \mathcal{E}$, both considered with their reduced subscheme structures. We further define $\mathcal{C}^\circ = \mathcal{C} - \mathcal{Z}$. We have that $\mathcal{C}$ is a proper curve over $\mathbb{Z}_p$. Moreover, since $\mathcal{C}$ is the scheme-theoretic image of the morphism $C \to \mathcal{E} \times \mathcal{E}$ by [12, ex. II.3.11(d)], it is flat over $\mathbb{Z}_p$ by [3, 1.1]. Since $\mathcal{C}^\circ \subset \mathcal{C}$ is an open subscheme of the proper flat scheme $\mathcal{C}$ over $\mathbb{Z}_p$, and its fibres over $\mathbb{Z}_p$ are smooth, it is itself smooth over $\mathbb{Z}_p$. The automorphism of $\mathcal{E} \times \mathcal{E}$ that interchanges both factors will be denoted by τ. On $i(C)$, the map τ induces the same map as the automorphism τ of C. The maps π_1 and π_2 from C to E extend to morphisms $\mathcal{C} \to \mathcal{E}$, which we will denote by the same symbols.

By $\Gamma_n \subset \mathcal{E} \times \mathcal{E}$, we denote the graph of multiplication by n, in the following sense

$$\Gamma_n = \{(e, ne) : e \in \mathcal{E}\}.$$

We have that the curve $\Gamma_n \subset \mathcal{E} \times \mathcal{E}$ is smooth over $\mathbb{Z}_p$ for all n. By the valuative criterion of properness, we have

$$E(\mathbb{Q}_p) = \mathcal{E}(\mathbb{Q}_p) = \mathcal{E}(\mathbb{Z}_p), \quad C(\mathbb{Q}_p) = \mathcal{C}(\mathbb{Q}_p) = \mathcal{C}(\mathbb{Z}_p)$$

and via these identifications the subgroups $E_n(\mathbb{Q}_p)$ and $\mathcal{E}_n(\mathbb{Q}_p)$, as defined in section 1.2, coincide for all integers $n \geq 0$.

4.5.2 The case where p does not divide $\#\mathcal{E}(\mathbb{F}_p)$

The following proposition shows that if $\#\mathcal{E}(\mathbb{F}_p)$ is coprime to p, we may reduce the problem of finding a P as in Lemma 4.6 to a problem involving only the reductions $\mathcal{C}_{\mathbb{F}_p}$ and $\mathcal{E}_{\mathbb{F}_p}$.

Proposition 4.14. *Assume that the order of $\mathcal{E}(\mathbb{F}_p)$ is coprime to p. Let $\overline{P} \in \mathcal{C}(\mathbb{F}_p)$. Then the following conditions are equivalent.*

(i) The points $\pi_1(\overline{P})$ and $\pi_2(\overline{P})$ generate $\mathcal{E}(\mathbb{F}_p)$.
(ii) There exists a Mestre point $P \in \mathcal{C}(\mathbb{Q}_p)$ with $P_{\mathbb{F}_p} = \overline{P}$.

Proof. The implication (ii) ⇒ (i) is clear: if $P \in \mathcal{C}(\mathbb{Q}_p)$ is such that $P_{\mathbb{F}_p} = \overline{P}$, and $\pi_1(\overline{P})$ and $\pi_2(\overline{P})$ do not generate $\mathcal{E}(\mathbb{F}_p)$, then certainly $\pi_1(P)$ and $\pi_2(P)$ do not generate $E(\mathbb{Q}_p)$ topologically.

Since the ramification loci of the π_i are disjoint by Proposition 4.8(i), without loss of generality we may assume $(\pi_1)_{\mathbb{F}_p}$ to be unramified, and hence étale, at $\overline{P}$. Write $\overline{Q} = \pi_1(\overline{P})$.

Denote the set of points in $C(\mathbb{Q}_p)$ that reduce to $\overline{P}$ with $C(\mathbb{Q}_p)_{\overline{P}}$. If $P' \in C(\mathbb{Q}_p)_{\overline{P}}$, then by the assumption of the proposition, the points $Q'_1 = \pi_1(P')$ and $Q'_2 = \pi_2(P')$ together with $E_1(\mathbb{Q}_p)$ generate $E(\mathbb{Q}_p)$. Therefore it suffices to show that we can choose P' in such a way that some $\mathbb{Z}$-linear combination of Q'_1 and Q'_2 lies in $E_1(\mathbb{Q}_p) - E_2(\mathbb{Q}_p)$. By the fact that π_1 is étale at $\overline{P}$ and by Hensel's lemma, the restriction of π_1 to $C(\mathbb{Q}_p)_{\overline{P}}$ surjects to the set $E(\mathbb{Q}_p)_{\overline{Q}}$ of points $Q' \in E(\mathbb{Q}_p)$ such that $(Q')_{\mathbb{F}_p} = \overline{Q}$. We have $E(\mathbb{Q}_p)_{\overline{Q}} = \pi_1(P') + E_1(\mathbb{Q}_p)$ for any $P' \in C(\mathbb{Q}_p)_{\overline{P}}$. Hence, for any $P' \in C(\mathbb{Q}_p)_{\overline{P}}$, there exists $P'' \in C(\mathbb{Q}_p)_{\overline{P}}$ with $\pi_1(P') - \pi_1(P'') \notin E_2(\mathbb{Q}_p)$.

Now we use the fact that the order of $\mathcal{E}(\mathbb{F}_p)$ is coprime to p. We have $\ell\pi_1(\overline{P}) = 0$ for some integer ℓ coprime to p. Let $P' \in C(\mathbb{Q}_p)_{\overline{P}}$ be arbitrary.

The fact $\ell\pi_1(\overline{P}) = 0$ implies that $\ell\pi_1(P') \in E_1(\mathbb{Q}_p)$. If $\ell\pi_1(P') \notin E_2(\mathbb{Q}_p)$, we are done. Otherwise, there exists $P'' \in C(\mathbb{Q}_p)_{\overline{P}}$ such that $\pi_1(P') - \pi_1(P'') \notin E_2(\mathbb{Q}_p)$. We have $\ell\pi_1(P') - \ell\pi_1(P'') \notin E_2(\mathbb{Q}_p)$, since $E_2(\mathbb{Q}_p)$ has index p in $E_1(\mathbb{Q}_p)$, and $p \nmid \ell$, and therefore $\ell\pi_1(P'') \notin E_2(\mathbb{Q}_p)$. Hence in this case we can take P'' instead of P', and we are again done. □

4.5.3 The case of anomalous reduction

The most notable case to which Proposition 4.14 does not apply is the case where $\mathcal{E}(\mathbb{F}_p)$ has order p. Indeed, when we have $p > 5$ the Hasse–Weil bound implies that if $\mathcal{E}(\mathbb{F}_p)$ is divisible by p, then it must be equal to p.

Definition 4.15. We say that E has anomalous reduction if $\mathcal{E}(\mathbb{F}_p)$ is cyclic of order p.

In this section, we establish two criteria for the existence of Mestre points on C in the anomalous reduction case.

Remark 4.16. Assume that E has anomalous reduction at p, and that $p > 7$. We have the usual short exact sequence

$$0 \to E_1(\mathbb{Q}_p) \to E(\mathbb{Q}_p) \to \mathcal{E}(\mathbb{F}_p) \to 0$$

as well as the topological isomorphism $E_1(\mathbb{Q}_p) \cong \mathbb{Z}_p$ [32, IV.6.4(b)]. Then according to Proposition 1.14(iii), we have either $E(\mathbb{Q}_p) \cong \mathbb{Z}_p$ or $E(\mathbb{Q}_p) \cong \mathbb{Z}_p \times \mathbb{Z}/p\mathbb{Z}$. In the first case, we have that $E(\mathbb{Q}_p)$ is procyclic, and the results of chapter 3 give that E has good twists. Therefore, the results from this section are only needed in the second case.

Lemma 4.17. *Assume that E has anomalous reduction. Let P_1 and P_2 be elements of $\mathcal{E}(\mathbb{Q}_p)$. Consider the following three statements.*

(i) The points P_1 and P_2 generate $\mathcal{E}(\mathbb{Q}_p)$ topologically.
(ii) The points P_1 are P_2 are not both contained in $\mathcal{E}_1(\mathbb{Q}_p)$.
(iii) There exists $n \in \mathbb{Z}$ such that $(P_1, P_2)_{\mathbb{F}_p}$ is contained in $\Gamma_n(\mathbb{F}_p)$, but $(P_1, P_2)_{\mathbb{Z}/p^2\mathbb{Z}}$ is not contained in $\Gamma_n(\mathbb{Z}/p^2\mathbb{Z})$.

Then (ii)+(iii) implies (i).

Proof. Assume that assumption (ii) and (iii) hold. In view of (ii), we only have to prove that $\langle P_1, P_2 \rangle$ lies dense in $\mathcal{E}_1(\mathbb{Q}_p)$. Since we had assumed $p > 2$, we have $\mathcal{E}_1(\mathbb{Q}_p) \cong \mathbb{Z}_p$; therefore it suffices to show that some integer linear combination of P_1 and P_2 lies in $\mathcal{E}_1(\mathbb{Q}_p) - \mathcal{E}_2(\mathbb{Q}_p)$. We let n be as in (iii). Then we have $P_2 - nP_1 \in \mathcal{E}_1(\mathbb{Q}_p) - \mathcal{E}_2(\mathbb{Q}_p)$. □

Anomalous reduction: a transversality criterion

To establish the first criterion for the existence of a Mestre point on C in the case of anomalous reduction, we reinterpret condition (iii) of Lemma 4.17 as the statement that a certain intersection is transversal.

Proposition 4.18. *Let $\mathcal{S}$ be a smooth surface over $\mathbb{Z}_p$, and let $\mathcal{D}_1, \mathcal{D}_2 \subset \mathcal{S}$ be smooth curves over $\mathbb{Z}_p$. Let $P \in \mathcal{S}(\mathbb{Z}_p)$. The following conditions are equivalent.*

(i) We have the following equality between subsets of $\mathcal{S}(\mathbb{Z}/p^2\mathbb{Z})$:

$$\left\{P' \in \mathcal{D}_1(\mathbb{Z}/p^2\mathbb{Z}) : (P')_{\mathbb{F}_p} = P_{\mathbb{F}_p}\right\} = \left\{P' \in \mathcal{D}_2(\mathbb{Z}/p^2\mathbb{Z}) : (P')_{\mathbb{F}_p} = P_{\mathbb{F}_p}\right\}.$$

(ii) The curves $(\mathcal{D}_1)_{\mathbb{F}_p}$ and $(\mathcal{D}_2)_{\mathbb{F}_p}$ are tangent to each other in $P_{\mathbb{F}_p}$.

Proof. The result can be seen as a variant of the multi-variable Hensel's lemma. A difference here is that we are only interested in lifting $\mathbb{F}_p$-points to $\mathbb{Z}/p^2\mathbb{Z}$-points.

By the fact that $\mathcal{S}$ is locally of finite type, we have that $\mathcal{S}$ is of the following form locally around $P_{\mathbb{F}_p}$

$$\operatorname{Spec} \mathbb{Z}_p[x_1, \ldots, x_n]/(f_1, \ldots, f_r)$$

for $f_1, \ldots, f_r \in \mathbb{Z}_p[x_1, \ldots, x_n]$, where we may identify P with the section $\mathbf{0} = (0, \ldots, 0)$. Let $i \in \{1, 2\}$. Since $\mathcal{D}_i$ is smooth along P of relative dimension 1, there exist

$$g_{1,1}, \ldots, g_{1,n-1}, g_{2,1}, \ldots, g_{2,n-1} \in \mathbb{Z}_p[x_1, \ldots, x_n]$$

such that $\mathcal{D}_i$ is given as the zero-set $\mathcal{V}_i$ of

$$g_{i,1}, \ldots, g_{i,n-1}$$

locally around $\mathbf{0}$, where the $g_{i,j}$ are such that the matrix

$$\mathbf{T}_i = \begin{pmatrix} \frac{\partial g_{i,1}}{\partial x_1} & \cdots & \frac{\partial g_{i,1}}{\partial x_n} \\ \vdots & \ddots & \vdots \\ \frac{\partial g_{i,n-1}}{\partial x_1} & \cdots & \frac{\partial g_{i,n-1}}{\partial x_n} \end{pmatrix}_{(0,\ldots,0)}$$

has an $(n-1)$-by-$(n-1)$ minor whose determinant is contained in $\mathbb{Z}_p^*$. As usual, the tangent space of $(\mathcal{D}_i)_{\mathbb{F}_p}$ at $\mathbf{0}_{\mathbb{F}_p}$ may be identified with the kernel of the matrix

$$\mathbf{T}_{i,\mathbb{F}_p}\big|_{(0,\ldots,0)}$$

where $\mathbf{T}_{i,\mathbb{F}_p}$ denotes the entry-wise reduction modulo p of the matrix $\mathbf{T}_i$.

Since $\mathbb{Z}/p^2\mathbb{Z}$ is a local ring and $\mathcal{D}_i$ and $\mathcal{V}_i$ agree on open subsets containing P and $\mathbf{0}$ respectively, the $\mathbb{Z}/p^2\mathbb{Z}$-points of $\mathcal{D}_i$ reducing to $P_{\mathbb{F}_p}$ are in bijection with the $\mathbb{Z}/p^2\mathbb{Z}$-points of $\mathcal{V}_i$ reducing to $\mathbf{0}_{\mathbb{F}_p}$. It thus suffices to show that equality

$$\{P' \in \mathcal{V}_1(\mathbb{Z}/p^2\mathbb{Z}) : P'_{\mathbb{F}_p} = \mathbf{0}_{\mathbb{F}_p}\} = \{P' \in \mathcal{V}_2(\mathbb{Z}/p^2\mathbb{Z}) : P'_{\mathbb{F}_p} = \mathbf{0}_{\mathbb{F}_p}\} \tag{4.14}$$

is equivalent to

$$\ker(\mathbf{T}_{1,\mathbb{F}_p}) = \ker(\mathbf{T}_{2,\mathbb{F}_p}). \tag{4.15}$$

Let $Z_i = \{P' \in \mathcal{V}_i(\mathbb{Z}/p^2\mathbb{Z}) : P'_{\mathbb{F}_p} = \mathbf{0}_{\mathbb{F}_p}\}$. We can describe Z_i explicitly in terms of $\mathbf{T}_{i,\mathbb{F}_p}$: any $P' \in Z_i$ must be of the form

$$(\delta_1 p, \ldots, \delta_n p)$$

with $\delta_1, \ldots, \delta_n \in \mathbb{F}_p$. Let $P' = (\delta_1 p, \ldots, \delta_n p)$. By expanding the equations

$$g_{i,1}(\delta_1 p, \ldots, \delta_n p) = \ldots = g_{i,n-1}(\delta_1 p, \ldots, \delta_n p) = 0,$$

we find that for P' to be contained in Z_i, it is necessary and sufficient that

$$\mathbf{T}_i|_{(0,\ldots,0)} \cdot \begin{pmatrix} \delta_1 p \\ \vdots \\ \delta_n p \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix} \quad \text{in } (\mathbb{Z}/p^2\mathbb{Z})^{n-1}.$$

This shows that (4.14) and (4.15) are indeed equivalent. This finishes the proof. □

In order to be able to keep track of tangent directions on $(\mathcal{E} \times \mathcal{E})_{\mathbb{F}_p}$, we introduce the following definition.

Definition 4.19. Let κ be $\mathbb{Q}_p$ or $\mathbb{F}_p$, and denote by $\mathcal{E}_\kappa$ the base-change of $\mathcal{E}$ to κ. Let $\omega = \frac{dx}{y}$ be the standard invariant differential on $\mathcal{E}_\kappa$. Let D be a smooth curve on $(\mathcal{E} \times \mathcal{E})_\kappa$. If $P \in D(\kappa)$, then the tangent direction to D at P is

$$\left(\frac{i_2^*\omega}{i_1^*\omega}\right)(P) \in \mathbb{P}^1(\kappa), \tag{4.16}$$

where

$$(i_1, i_2)\colon D \to (\mathcal{E} \times \mathcal{E})_\kappa, \tag{4.17}$$

is the closed embedding of D into $(\mathcal{E} \times \mathcal{E})_\kappa$, and where the left-hand side of (4.16) denotes the value of the function $\frac{i_2^*\omega}{i_1^*\omega} \in \kappa(D)$ at P.

The above definition can be given in a dual form that is a little more involved, but shows more clearly the relationship between Definition 4.19 and tangent vectors.

Lemma 4.20. *Let κ be $\mathbb{Q}_p$ or $\mathbb{F}_p$, and denote by $\mathcal{E}_\kappa$ the base-change of $\mathcal{E}$ to κ. Let $\omega = \frac{dx}{y}$ as in Definition 4.19. For every $Q \in \mathcal{E}(\kappa)$, there is a unique tangent vector $\omega_Q^* \in T_Q\mathcal{E}_\kappa$ such that $\omega(\omega_Q^*) = 1$. Let D, i_1 and i_2 be as in Definition 4.19, and let $P \in D(\kappa)$ be a smooth point with $i_1(P) = Q_1$ and $i_2(P) = Q_2$. Choose a non-zero element $\eta \in T_P D$. Then the tangent direction to D at P is the image of η under the composite map*

$$T_P D \xrightarrow{(i_1,i_2)_*} T_{Q_1}\mathcal{E}_\kappa \times T_{Q_2}\mathcal{E}_\kappa \dashrightarrow \mathbb{P}^1(\kappa),$$

where the last arrow is the partially-defined map that sends $(t_1\omega_{Q_1}, t_2\omega_{Q_2})$ to $(t_2 : t_1)$ for all $t_1, t_2 \in \kappa$ that are not both zero.

Proof. We have that ω is a basis for the cotangent space $T_Q^*\mathcal{E}_\kappa$ for every $Q \in \mathcal{E}_\kappa$, so for each $Q \in \mathcal{E}(\kappa)$ there exists a unique tangent vector $\omega_Q^* \in T_Q\mathcal{E}_\kappa$ such that $\omega(\omega_Q^*) = 1$. Furthermore, ω_Q^* is a basis of $T_Q\mathcal{E}_\kappa$ for each Q, which shows that the map $T_{Q_1}\mathcal{E}_\kappa \times T_{Q_2}\mathcal{E}_\kappa \dashrightarrow \mathbb{P}^1(\kappa)$ is defined everywhere except at 0. Suppose that $t_1, t_2 \in \kappa$ are such that $(i_1, i_2)_*(\eta) = (t_1\omega_{Q_1}, t_2\omega_{Q_2})$. Then we have $i_1^*(\omega)(\eta) = \omega(i_{1*}(\eta)) = \omega(t_1\omega_{Q_1}) = t_1$, and likewise $i_2^*(\omega)(\eta) = t_2$. This shows that $i_2^*(\omega)/i_1^*(\omega)$ evaluated at P gives t_2/t_1, which is what we had to show. □

The following lemma is due to J. F. Voloch, to whom I am very grateful for mentioning it to me in a discussion about this chapter.

Lemma 4.21. *Assume that $\mathcal{E}(\mathbb{F}_p)$ is cyclic of order p. Write*

$$f(x)^{(p-1)/2} = U(x) + Ax^{p-1} + x^p V(x)$$

for some $U(x)$ of degree at most $p-2$ and $V(x)$ of degree $(p-3)/2$. Then the map

$$\begin{aligned} \mathcal{E}(\mathbb{F}_p) &\to \mathbb{F}_p \\ (x, y) &\mapsto yV(x) \end{aligned}$$

is an isomorphism of groups.

Proof. Let $\phi\colon \mathcal{E}'_{\mathbb{F}_p} \to \mathcal{E}_{\mathbb{F}_p}$ the isogeny dual to the Frobenius. Since $\mathcal{E}(\mathbb{F}_p)[p] \neq 0$, we have that ϕ is separable and its image equals $p\mathcal{E}(\mathbb{F}_p) = 0$. The result now follows from Proposition 1.3 in [40]. □

The proof of the following proposition makes essential use of the smoothness of $\mathcal{C}^\circ$.

Proposition 4.22. *Suppose that E has anomalous reduction. Write*

$$f(x)^{(p-1)/2} = U(x) + Ax^{p-1} + x^p V(x) \tag{4.18}$$

for some $U(x)$ of degree at most $p-2$ and $V(x)$ of degree $(p-3)/2$. Write $\omega = dx/y$ for the standard invariant differential on $\mathcal{E}_{\mathbb{F}_p}$. Assume that there exists a point $P \in \mathcal{C}^\circ(\mathbb{F}_p)$ such that

$$\left(\frac{\pi_2^*\omega}{\pi_1^*\omega}\right)(P) \neq \left(\frac{\pi_2^* yV(x)}{\pi_1^* yV(x)}\right)(P), \tag{4.19}$$

where the value infinity is allowed for both sides. Then C has a Mestre point.

Proof. Recall that we denote by τ the automorphism of $\mathcal{E} \times \mathcal{E}$ that interchanges both factors. Replacing P by $\tau(P)$ amounts to replacing both sides of (4.19) by their inverses. Possibly after replacing P by $\tau(P)$, we may assume that $\pi_1(P) \neq 0$, so there exists an integer n such that $\pi_2(P) = n\pi_1(P)$, which is equivalent to $P \in \Gamma_n(\mathbb{F}_p)$.

The left-hand side of (4.19) is the tangent direction to $\mathcal{C}^\circ_{\mathbb{F}_p} \subset (\mathcal{E} \times \mathcal{E})_{\mathbb{F}_p}$ at P. For the right-hand side, we have

$$\left(\frac{\pi_2^* yV(x)}{\pi_1^* yV(x)}\right)(P) = n$$

by Proposition 4.21 and the definition of n. We claim that the tangent direction to $(\Gamma_n)_{\mathbb{F}_p}$ at P is n. The curve Γ_n arises as the image of the closed immersion

$$(i_1, i_2)\colon \mathcal{E} \to \mathcal{E} \times \mathcal{E}$$

defined on points by $e \mapsto (e, ne)$. Using Definition 4.19, we see that the tangent direction to $(\Gamma_n)_{\mathbb{F}_p}$ at any point P' is

$$\left(\frac{i_2^*\omega}{i_1^*\omega}\right)(P') = n.$$

(This uses the fact that $[n]^*\omega = n\omega$, where $[n]\colon \mathcal{E}_{\mathbb{F}_p} \to \mathcal{E}_{\mathbb{F}_p}$ is multiplication by n; see [32, III.5.3].) Hence the statement (4.19) is equivalent to the tangent direction to $\mathcal{C}^\circ$ at P not being equal to the tangent direction to Γ_n at P. Then by Proposition 4.18, there exists a point $P' \in \mathcal{C}^\circ(\mathbb{Z}/p^2\mathbb{Z})$

with $(P')_{\mathbb{F}_p} = P$, but $P' \notin \Gamma_n(\mathbb{Z}/p^2\mathbb{Z})$. By Hensel's lemma, there exists $P'' \in \mathcal{C}^\circ(\mathbb{Z}_p) \subset C(\mathbb{Q}_p)$ so that P'' satisfies $(P'')_{\mathbb{Z}/p^2\mathbb{Z}} = P'$. Let $Q_1 = \pi_1(P'')$ and $Q_2 = \pi_2(P'')$. The condition $(P'')_{\mathbb{Z}/p^2\mathbb{Z}} \notin \Gamma_n(\mathbb{Z}/p^2\mathbb{Z})$ implies that $Q_2 - nQ_1 \in E_1(\mathbb{Q}_p) - E_2(\mathbb{Q}_p)$, and hence by Lemma 4.17 we have that Q_1 and Q_2 are topological generators of $E(\mathbb{Q}_p)$. This concludes the proof. □

Remark 4.23. By expanding, we can make the inequality (4.19) more explicit. It says that, for a point $P = (u_0, v_0) \in \mathcal{C}(\mathbb{F}_p)$, we have

$$-\frac{u_0^3(u_0^2+2)}{2u_0^2+1} \neq \frac{u_0^3 V(-b/a \cdot (u_0^4+u_0^2+1)/(u_0^2+1))}{V(-b/a \cdot (u_0^4+u_0^2+1)/(u_0^4+u_0^2)))}$$

with V defined as in (4.18). It seems difficult in general to prove that there exists a point $P = (u_0, v_0) \in \mathcal{C}(\mathbb{F}_p)$ for which this inequality is satisfied. For instance, the degree of the rational function on the right-hand side grows linearly with p, so that the naive estimate comparing the number of zeros of a rational function on $\mathcal{C}$ with the number of points in $\mathcal{C}(\mathbb{F}_p)$ will not work.

Anomalous reduction: an explicit criterion

Proposition 4.24. *Suppose that E has anomalous reduction. Assume that $-ab \in \mathbb{Q}_p^{*2}$. Then C has a Mestre point.*

Proof. We assume $-ab \in \mathbb{Q}_p^{*2}$. We will prove the existence of $P \in C(\mathbb{Q}_p)$ such that $Q_1 = \pi_1(P)$ is contained in $E_1(\mathbb{Q}_p) - E_2(\mathbb{Q}_p)$ and $Q_2 = \pi_2(P)$ is contained in $E(\mathbb{Q}_p) - E_1(\mathbb{Q}_p)$. Since $E(\mathbb{Q})$ is isomorphic to either $\mathbb{Z}_p$ or $\mathbb{Z}_p \times \mathbb{Z}/p\mathbb{Z}$, where in the latter case the subgroup $\mathbb{Z}_p$ corresponds to $E_1(\mathbb{Q}_p)$, the points Q_1 and Q_2 generate $E(\mathbb{Q}_p)$ topologically.

Let $Q_1 = (x_0, y_0) \in E_1(\mathbb{Q}_p) - E_2(\mathbb{Q}_p)$ be arbitrary. Observe that we have $v_p(x_0) = -2$. Also, since $y_0^2 = x_0^3 + ax_0 + b$, we have $x_0 \in \mathbb{Q}_p^{*2}$. Then, for $u_0 \in \mathbb{Q}_p$, the statement that $P = (u_0, y_0)$ is contained in $C(\mathbb{Q}_p)$ and is such that $\pi_1(P) = Q_1$ is equivalent to

$$x_0 = \phi(u_0) = -\frac{b}{a}\frac{w_0^2 + w_0 + 1}{w_0^2 + w_0}, \tag{4.20}$$

where we have put $w_0 = u_0^2$. Solving this equation for w_0, we get

$$w_+ = -\frac{1}{2} + \frac{1}{2}\sqrt{1 - \frac{4b}{ax_0 + b}} \quad \text{and} \quad w_- = -\frac{1}{2} - \frac{1}{2}\sqrt{1 - \frac{4b}{ax_0 + b}} \tag{4.21}$$

Since $v_p(4b/(ax_0+b)) = 2$, we have $w_+ \in \mathbb{Q}_p$. Moreover, by p-adically expanding the square roots in the expressions (4.21), we obtain

$$w_+ = -\frac{1}{2} + \frac{1}{2}\left(1 - \frac{1}{2}\frac{4b}{ax_0+b} + O(p^4)\right) = -\frac{b}{ax_0+b} + O(p^4) \qquad (4.22)$$

and

$$w_- = -\frac{1}{2} - \frac{1}{2}\left(1 - \frac{1}{2}\frac{4b}{ax_0+b} + O(p^4)\right) = -1 + \frac{b}{ax_0+b} + O(p^4)$$

We have that x_0 and $-b/a$ are both contained in $\mathbb{Q}_p^{*2}$, so that w_+ is a p-adic square. Therefore, there exists $u_0 \in \mathbb{Q}_p$ that satisfies (4.20), and equation (4.22) shows that $v_p(w_+) = -v_p(x_0) = 2$. We have that $P = (u_0, y_0)$ maps to $Q_1 \in E_1(\mathbb{Q}_p)$. Moreover, $Q_2 = \pi_2(u_0, y_0)$ is equal to $Q_2 = (u_0^2\phi(u_0), u_0^3 y_0) = (u_0^2 x_0, u_0^3 y_0)$, which is obviously contained in $E(\mathbb{Q}_p) - E_1(\mathbb{Q}_p)$. This proves the proposition. (Note that we couldn't have used w_- even if $-1 \in \mathbb{Q}_p^{*2}$, since in that case both $\pi_1(\sqrt{w_-}, y_0)$ and $\pi_2(\sqrt{w_-}, y_0)$ would lie in $E_1(\mathbb{Q}_p)$.) □

4.5.4 Good points over ramified twists

For $d \in \mathbb{Q}_p^*$, recall that a twist E^d of E is called ramified if the valuation of d is odd. For such d, the existence of Mestre points on C^d is guaranteed by Proposition 4.26 in the case where E^d has the full 2-torsion over $\mathbb{Q}_p$. (In the other cases we will have that $E^d(\mathbb{Q}_p)$ is procyclic, so we can apply the results of the previous chapter.)

Lemma 4.25. *Let $d \in \mathbb{Q}_p^*$ be an element of valuation 1. Then the quadratic twist E^d of E has Kodaira type I_0^*, and $E^d(\mathbb{Q}_p)[2]$ contains no non-zero points of good reduction.*

Proof. The 2-torsion of E^d is defined over any extension of $\mathbb{Q}_p$ that contains the roots of the polynomial

$$x^3 + ad^2x + bd^3 = d^3 f(x/d). \qquad (4.23)$$

As (4.23) shows, the same is true over any extension of $\mathbb{Q}_p$ that contains the roots of f. Since $f \pmod p$ is separable over $\mathbb{F}_p$, the roots of f are contained in an unramified extension of $\mathbb{Q}_p$. The 2-torsion of E^d is therefore defined over the maximal unramified extension $\mathbb{Q}_p^{\mathrm{un}}$ of $\mathbb{Q}_p$. Equation (4.23) shows that for any $x_0 \in \mathbb{Q}_p^{\mathrm{un}}$, we have that x_0 is a root of f if and only

if $(dx_0, 0)$ is a point in $E^d(\mathbb{Q}_p^{\mathrm{un}})$. Since $y^2 = x^3 + ad^2x + bd^3$ defines a minimal Weierstrass model of E^d, the non-trivial 2-torsion of $E^d(\mathbb{Q}_p^{\mathrm{un}})$ is of bad reduction, which shows that $E^d(\mathbb{Q}_p^{\mathrm{un}})/E_0^d(\mathbb{Q}_p^{\mathrm{un}})$ contains the Klein four-group. The only Kodaira type for which the component group contains the Klein four-group is I_0^* (see [32, C.15]), so this must be the Kodaira type of E^d. □

Proposition 4.26. *Let $d \in \mathbb{Q}_p^*$ be an element of valuation 1. Assume furthermore that either $p > 7$ or $E_0^d(\mathbb{Q}_p) \cong \mathbb{Z}_p$, and assume furthermore that $\#E^d(\mathbb{Q}_p)[2] = 4$. Then there exists a Mestre point $P \in C^d(\mathbb{Q}_p)$.*

Proof. The assumption that either $p > 7$ or $E_0^d(\mathbb{Q}_p) \cong \mathbb{Z}_p$ is there to guarantee $E_0^d(\mathbb{Q}_p) \cong \mathbb{Z}_p$. (See Theorem 1.1; note that E^d has additive reduction.) Putting $\Phi = E^d(\mathbb{Q}_p)/E_0^d(\mathbb{Q}_p)$, we have the usual short exact sequence

$$0 \to \mathbb{Z}_p \to E^d(\mathbb{Q}_p) \to \Phi \to 0,$$

with Φ isomorphic to $(\mathbb{Z}/2\mathbb{Z})^2$ by Lemma 4.25. Proposition 1.14(iv) shows that $E^d(\mathbb{Q}_p)$ is topologically isomorphic to $\mathbb{Z}_p \times (\mathbb{Z}/2\mathbb{Z})^2$.

When denoting points on E^d, we shall be using the equation $dy^2 = f(x)$ for it. By performing Tate's algorithm on a Weierstrass model for E^d, we find that the three non-trivial cosets of $E_0^d(\mathbb{Q}_p)$ in $E^d(\mathbb{Q}_p)$ are of the following form:

$$S_e = \left\{(x_0, y_0) \in E^d(\mathbb{Q}_p) : x_0 \equiv e \pmod{p}\right\},$$

where $e \in \mathbb{Z}_p^*$ is one of the three roots of f. We may apply Proposition 4.12 to $\overline{f}$, using $\phi_2(u) = \phi_1(u^{-1})$, to find that there exist two distinct roots e_1 and e_2 of f, such that if we put $\alpha_1 = \overline{e_1}$ and $\alpha_2 = \overline{e_2}$, there exist elements β_1 and β_2 of $\mathbb{F}_p$ such that

$$\overline{\phi}(\beta_1) = \alpha_1, \quad \overline{\phi}(\beta_2) = \alpha_2$$

and

$$\overline{\phi}(\beta_1^{-1}) = \alpha_2, \quad \overline{\phi}(\beta_2^{-1}) = \alpha_1,$$

where we use $\overline{\cdot}$ to denote reduction modulo p. These identities imply that for any point $P' = (u_1, v_1)$ in $C^d(\mathbb{Q}_p)$ such that $\overline{u_1} = \beta_1$, if we write $\pi_1(P') = (x_1, y_1)$ and $\pi_2(P') = (x_2, y_2)$, then we have $\overline{x_1} = \alpha_1$ and $\overline{x_2} = \alpha_2$ in $\mathbb{F}_p$.

Let $Q_1 = (x_1, y_1)$ be an arbitrary point in $E^d(\mathbb{Q}_p) - E_0^d(\mathbb{Q}_p)$ with $x_1 \equiv e_1 \pmod{p}$. We will construct a point $P = (u_1, v_1)$ in $C^d(\mathbb{Q}_p)$ such that $\pi_1(P) = Q_1$. Such a P may be constructed from a solution $u = u_1$ to the equation

$$-\frac{b}{a}\frac{u^4 + u^2 + 1}{u^4 + u^2} = x_1, \tag{4.24}$$

since for a solution u_1 to (4.24), the morphism π_1 maps $P = (u_1, y_1)$ to Q_1. Over $\mathbb{F}_p$, the reduction modulo p of (4.24) has 4 distinct solutions, since the right-hand side reduces to α_1, and we know from Proposition 4.8(i) that π_1 is unramified above the point $(\alpha_1, 0)$ on the smooth curve $\mathcal{E}_{\mathbb{F}_p}$. We may thus apply Hensel's lemma to find a solution u_1 such that $\overline{u_1} = \beta_1$. We define $P = (u_1, y_1)$. Then we have $\pi_1(P) = Q_1$, as desired. Moreover, by the previous paragraph, we also have $\pi_2(P) = (x_2, y_2)$, with x_2 an element of $\mathbb{Z}_p$ such that $\overline{x_2} = \alpha_2$.

Now take $Q_1 = (x_1, y_1)$ to be a point in $E^d(\mathbb{Q}_p)$ such that $x_1 \equiv e_1 \pmod{p}$ and such that some multiple of Q_1 lies in $E_0^d(\mathbb{Q}_p) - E_1^d(\mathbb{Q}_p)$. (We know that such a Q_1 exists by the fact that the points (x_1, y_1) satisfying $x_1 \equiv e_1 \pmod{p}$ make up a coset of $E_0^d(\mathbb{Q}_p) \cong \mathbb{Z}_p$ in $E^d(\mathbb{Q}_p) \cong \mathbb{Z}_p \times (\mathbb{Z}/2\mathbb{Z})^2$.) Then by the previous paragraph, there exists P in $C^d(\mathbb{Q}_p)$ such that $Q_1 = \pi_1(P)$ and $Q_2 = \pi_2(P)$ lie in different non-trivial cosets of $E_0^d(\mathbb{Q}_p)$ in $E^d(\mathbb{Q}_p)$. Since in addition some multiple of Q_1 lies in $E_0^d(\mathbb{Q}_p) - E_1^d(\mathbb{Q}_p)$, it is clear that Q_1 and Q_2 generate $E^d(\mathbb{Q}_p)$ topologically. □

4.6 Existence criteria for good twists

We let $p > 2$ be a prime number and a and b rational numbers of non-negative p-adic valuation such that

$$ab(4a^3 + 27b^2)$$

is a p-adic unit. We let E be the elliptic curve over $\mathbb{Q}$ given by $y^2 = x^3 + ax + b$. In this section, we will combine the results of section 4.5 with Lemma 4.6 to give existence results on good twists, given $d \in \mathbb{Q}_p^*$, of E with respect to d and p.

4.6.1 Unramified twists

The following definitions are made in order to apply the results of section 4.5 to (unramified) twists E^d of E, instead of just E itself. Instead of the curves E^d, given by $dy^2 = x^3 + ax + b$, we consider the curves E'^d, which are given by $y^2 = x^3 + ad^2x + bd^3$. The curves E^d and E'^d are isomorphic for each d, but the E'^d have the advantage that they are given by Weierstrass equations.

Definition 4.27. For $d \in \mathbb{Z}_p^*$, we let E'^d be the elliptic curve given by $y^2 = x^3 + ad^2x + bd^3$ and $\mathcal{E}'^d$ the smooth Weierstrass curve over $\mathbb{Z}_p$ given

by the same equation. Note that E'^d is isomorphic to E^d and that $\mathcal{E}'^d$ is a smooth Weierstrass model of E'^d. We let C'^d be the curve arising from the construction in section 4.2.1 applied to the case where E is replaced by the elliptic curve E'^d. Note that C'^d is isomorphic to C^d as defined in section 4.2.1. We define $Z'^d \subset C'^d$ in the same way as we defined Z for C (see the start of section 4.4). As in section 4.2.1, we have maps

$$\pi_1'^d \colon C'^d \to E'^d, \quad \pi_2'^d \colon C'^d \to E'^d,$$

and we define the notion of a Mestre point on C'^d in the same way we did for C^d. We denote by $i'^d \colon C'^d \to E'^d \times E'^d$ the map $i'^d = (\pi_1'^d, \pi_2'^d)$. We let $\mathcal{C}'^d \subset \mathcal{E}'^d \times \mathcal{E}'^d$ be the closure of $i'^d(C'^d)$. The morphisms $\pi_1'^d$ and $\pi_2'^d$ extend to morphisms $\pi_1'^d, \pi_2'^d \colon \mathcal{C}'^d \to \mathcal{E}'^d$. We let $\mathcal{Z}'^d \subset \mathcal{E}'^d \times \mathcal{E}'^d$ be the closure of $i'^d(Z'^d)$. Finally, the smooth subscheme $\mathcal{C}'^d - \mathcal{Z}'^d$ of $\mathcal{E}'^d \times \mathcal{E}'^d$ we will denote by $\mathcal{C}'^d_{\mathrm{smooth}}$.

Remark 4.28. One checks that the isomorphisms between E'^d and E^d and between C^d and C'^d can be chosen in such a way that, for $d \in \mathbb{Z}_p^*$ and $i \in \{1, 2\}$, the diagram

$$\begin{array}{ccc} C^d & \xrightarrow{\sim} & C'^d \\ \downarrow{\scriptstyle \pi_i^d} & & \downarrow{\scriptstyle \pi_i'^d} \\ E^d & \xrightarrow{\sim} & E'^d \end{array}$$

commutes. Thus C'^d has a Mestre point if and only if C^d does.

Unramified twists: the non-anomalous reduction case

Let $d \in \mathbb{Q}_p^*$ be an element with $v_p(d) = 0$.

Proposition 4.29. *Assume that the order of $\mathcal{E}'^d(\mathbb{F}_p)$ is coprime to p. Let $P \in \mathcal{C}'^d(\mathbb{F}_p)$. If the points $\pi_1'^d(P)$ and $\pi_2'^d(P)$ generate $\mathcal{E}'^d(\mathbb{F}_p)$, then there exists a good twist of E with respect to d and p.*

Proof. Proposition 4.14, with E replaced by E'^d, implies that C'^d has a Mestre point. By Remark 4.28, so does C^d. The result now follows from Lemma 4.6. □

The following proposition deals with the special case of cyclic non-anomalous reduction. It is partly a corollary of the results from the previous chapter.

Proposition 4.30. *Assume that $\mathcal{E}'^d(\mathbb{F}_p)$ is cyclic of order coprime to p. Then there exists a good twist of E with respect to d and p.*

Proof. We have that $E'^d(\mathbb{Q}_p)$ sits inside a short exact sequence with continuous maps, and with the second map an embedding

$$0 \to E_1'^d(\mathbb{Q}_p) \to E'^d(\mathbb{Q}_p) \to \mathcal{E}'^d(\mathbb{F}_p) \to 0,$$

where $E_1'^d(\mathbb{Q}_p)$ is procyclic and $\mathcal{E}'^d(\mathbb{F}_p)$ is cyclic of order coprime to p. By Proposition 1.14(ii), we have that $E'^d(\mathbb{Q}_p)$ is procyclic, and therefore so is $E^d(\mathbb{Q}_p)$. By Proposition 3.27 we find that E has a good twist with respect to d and p. □

Unramified twists: the anomalous reduction case

Again, we let $d \in \mathbb{Q}_p^*$ be an element with $v_p(d) = 0$.

Proposition 4.31. *Assume that the order of $\mathcal{E}'^d(\mathbb{F}_p)$ is equal to p. Write*

$$\left(x^3 + ad^2x + bd^3\right)^{(p-1)/2} = U(x) + Ax^{p-1} + x^pV(x) \tag{4.25}$$

for some $U(x)$ of degree at most $p-2$ and $V(x)$ of degree $(p-3)/2$. Write

$$\omega = \frac{dx}{y} \tag{4.26}$$

for the standard invariant differential on $(\mathcal{E}'^d)_{\mathbb{F}_p}$. Assume that there exists a point $P \in \mathcal{C}_{\mathrm{smooth}}'^d(\mathbb{F}_p)$ such that

$$\left(\frac{\pi_2^*\omega}{\pi_1^*\omega}\right)(P) \neq \left(\frac{\pi_2^* yV(x)}{\pi_1^* yV(x)}\right)(P), \tag{4.27}$$

where the value infinity is allowed for both sides. Then E has a good twist with respect to d and p.

Proof. From Proposition 4.22, with E replaced by E'^d, it follows that C'^d has a Mestre point. By Remark 4.28, so does C^d. The result follows from Lemma 4.6. □

Proposition 4.32. *Suppose that E^d has anomalous reduction at p. Assume that $-abd \in \mathbb{Q}_p^{*2}$. Then E has a good twist with respect to d and p.*

Proof. From Proposition 4.24, with E replaced by E'^d, it follows that C'^d has a Mestre point. By Remark 4.28, so does C^d. The result follows from Lemma 4.6. □

4.6.2 Ramified twists

If $d \in \mathbb{Q}_p^*$ is such that $v_p(d) = 1$, and p is greater than 7, it is very easy to prove that E has good twists with respect to d and p.

Proposition 4.33. *Let $d \in \mathbb{Q}_p^*$ be an element of valuation one. Assume also that either $p > 7$ or $E_0^d(\mathbb{Q}_p)$ is topologically isomorphic to $\mathbb{Z}_p$. Then E has a good twist with respect to d and p.*

Proof. We know from Lemma 4.25 that E^d has Kodaira type I_0^*, so that $E^d(\mathbb{Q}_p)$ fits inside an exact sequence

$$0 \to E_0^d(\mathbb{Q}_p) \to E^d(\mathbb{Q}_p) \to \Phi \to 0,$$

with $E_0^d(\mathbb{Q}_p)$ topologically isomorphic to $\mathbb{Z}_p$, and Φ isomorphic to a subgroup of $(\mathbb{Z}/2\mathbb{Z})^2$. Proposition 1.14(iv) shows that we have

$$E^d(\mathbb{Q}_p) \cong \mathbb{Z}_p \times \Phi \tag{4.28}$$

as topological groups. By (4.28) and since Φ is isomorphic to a subgroup of $(\mathbb{Z}/2\mathbb{Z})^2$, we have that Φ is isomorphic to the torsion subgroup of $E^d(\mathbb{Q}_p)[2]$. If Φ is not isomorphic to the full $(\mathbb{Z}/2\mathbb{Z})^2$, then $E^d(\mathbb{Q}_p)$ is a product of two procyclic groups of coprime order, hence procyclic, and we may apply Proposition 3.27 to find that E has good twists with respect to d and p. If $\Phi \cong (\mathbb{Z}/2\mathbb{Z})^2$, we may apply Proposition 4.26 to find that C^d has a Mestre point, and the result follows from Lemma 4.6 again. □

4.7 A computer experiment

Propositions 4.29–4.33 provide five criteria implying the existence of good twists of E, and hence the p-adic density of rational points on $\mathrm{Km}(E \times E)$ by Theorem 3.20. These criteria are all formulated in terms of elliptic curves over finite fields, and hence are well-suited to do a computer search. In this section, we list the results of a computer search we have performed using the open-source Computer Algebra System `sage` [35].

For the purpose of this section only, we will introduce the notion of a lucky prime for E. Very loosely speaking, a prime p will be called lucky for E if we can deduce from Propositions 4.29–4.33 and Theorem 3.20 that E has good twists with respect to p. We keep the notation introduced in Definition 4.27.

Definition 4.34. We will call a prime p lucky (for E) if p is greater than 7, the elliptic curve E can be given by a short Weierstrass equation

$$y^2 = x^3 + ax + b \tag{4.29}$$

with a and b in $\mathbb{Q}^*$ such that $v_p(a) = v_p(b) = v_p(ab(4a^3 + 27b^2)) = 0$, and for all $d \in \mathbb{Q}_p^*$ with $v_p(d) \in \{0, 1\}$ at least one of the following criteria is satisfied:

(C1) we have $v_p(d) = 0$, the order of $\mathcal{E}'^d(\mathbb{F}_p)$ is coprime to p, and there exists $\overline{P} \in \mathcal{C}'^d(\mathbb{F}_p)$ such that $\pi_1'^d(\overline{P})$ and $\pi_2'^d(\overline{P})$ generate $\mathcal{E}'^d(\mathbb{F}_p)$;
(C2) we have $v_p(d) = 0$, and $\mathcal{E}'^d(\mathbb{F}_p)$ is cyclic of order coprime to p;
(C3) we have $v_p(d) = 0$, the order of $\mathcal{E}'^d(\mathbb{F}_p)$ is equal to p, and for some $\overline{P} \in \mathcal{C}'^d_{\mathrm{smooth}}(\mathbb{F}_p)$ we have

$$\left(\frac{\pi_2^*\omega}{\pi_1^*\omega}\right)(P) \neq \left(\frac{\pi_2^* yV(x)}{\pi_1^* yV(x)}\right)(P), \tag{4.30}$$

where ω is as in (4.26) and V is as in (4.25);
(C4) we have $v_p(d) = 0$, the order of $\mathcal{E}'^d(\mathbb{F}_p)$ equals p, and $-abd \in \mathbb{Q}_p^{*2}$;
(C5) we have $v_p(d) = 1$.

If p is not lucky for E, then we will call it unlucky (for E). Note that the set of primes that are unlucky for E include the primes p for which E has bad reduction.

The ultimate use of the above definition is recorded in the following proposition.

Proposition 4.35. *Let p be a lucky prime for E. If $X = \mathrm{Km}(E \times E)$, then $X(\mathbb{Q})$ is dense in $X(\mathbb{Q}_p)$.*

Proof. By Theorem 3.20, it suffices to show that if $d \in \mathbb{Q}_p^*$, then E has a good twist with respect to d and p. Obviously, we may assume that $v_p(d) = 0$ or $v_p(d) = 1$. Choose an arbitrary d with $v_p(d) = 0$ or $v_p(d) = 1$. One proceeds in a manner depending on d: if (C1) is satisfied, apply Proposition 4.29; if (C2) is satisfied, apply Proposition 4.30; if (C3) is satisfied, apply Proposition 4.31; if (C4) is satisfied, apply Proposition 4.32; if (C5) is satisfied, apply Proposition 4.33. □

Remark 4.36. In fact, to verify whether p is a lucky prime for E, we only need to check the conditions (C1)–(C5) for d running through a set of coset representatives of $\mathbb{Q}_p^{*2}$ in $\mathbb{Q}_p^*$, which has only four elements. In fact, since (C5) automatically holds for the two coset representatives for which $v_p(d) = 1$, it suffices to check the conditions (C1)–(C4) for a single d such that $d \in \mathbb{Z}_p^{*2}$, and a single d for which $d \in \mathbb{Z}_p^* - \mathbb{Z}_p^{*2}$.

4.7.1 Results of the experiment

In our search, we consider the set $S_{5,5}$ of all elliptic curves $E_{a,b}$ over $\mathbb{Q}$ given by a short Weierstrass equation

$$E_{a,b}\colon y^2 = x^3 + ax + b$$

with $-5 \leq a \leq 5$, where $a \neq 0$, and $0 < b \leq 5$, as well as the 299 prime numbers p such that $7 < p < 2000$. For each of the curves $E_{a,b}$ and each prime p in the sets just described, we have let the computer decide the question whether p is lucky for $E_{a,b}$.

From the results of our experiments, it seems that the criteria developed in this thesis always seem to yield the existence of good twists with respect to p, roughly speaking, once p is large enough. The following table shows this more precisely. For each of the 49 elliptic curves E in our search space, we list the set of unlucky primes p with $7 < p < 2000$, along with its cardinality $N_{a,b}$. The asterisks denote primes of bad reduction.

(a,b)	Set of unlucky primes for $E_{a,b}$	$N_{a,b}$
$(-5,1)$	$\{11^*, 43^*, 73\}$	3
$(-5,2)$	$\{17, 23, 47\}$	3
$(-5,3)$	$\{257^*\}$	1
$(-5,4)$	$\{13, 17^*, 19, 43, 53, 67\}$	6
$(-5,5)$	$\{53\}$	1
$(-4,1)$	$\{37, 229^*\}$	2
$(-4,2)$	$\{37^*\}$	1
$(-4,3)$	$\{13^*, 17, 23, 29, 43\}$	5
$(-4,4)$	$\{11^*, 47\}$	2
$(-4,5)$	$\{43, 419^*\}$	2
$(-3,1)$	$\{17, 19, 37\}$	3
$(-3,3)$	$\emptyset$	0
$(-3,4)$	$\{13, 53, 67\}$	3
$(-3,5)$	$\{23, 29\}$	2
$(-2,1)$	$\{11, 19, 29, 41\}$	4
$(-2,2)$	$\{19^*, 23\}$	2
$(-2,3)$	$\{11, 53, 109, 211^*\}$	4
$(-2,4)$	$\{13, 17, 29, 37\}$	4
$(-2,5)$	$\{643^*\}$	1
$(-1,1)$	$\{23^*\}$	1
$(-1,2)$	$\{13^*\}$	1
$(-1,3)$	$\{239^*\}$	1

(a, b)	set of unlucky primes for $E_{a,b}$	$N_{a,b}$
$(-1, 4)$	$\{13, 29, 107^*\}$	3
$(-1, 5)$	$\{11^*, 17, 43, 61^*\}$	4
$(1, 1)$	$\{31^*\}$	1
$(1, 2)$	$\{11, 23, 37, 43\}$	4
$(1, 3)$	$\{13^*, 17, 19^*\}$	3
$(1, 4)$	$\{109^*\}$	1
$(1, 5)$	$\{11, 97^*\}$	2
$(2, 1)$	$\{17, 59^*\}$	2
$(2, 2)$	$\{17\}$	1
$(2, 3)$	$\{11^*, 23, 31, 37, 47, 53, 67, 71\}$	8
$(2, 4)$	$\{19, 29^*\}$	2
$(2, 5)$	$\{101^*\}$	1
$(3, 1)$	$\{47, 73\}$	2
$(3, 2)$	$\{11, 29, 79\}$	3
$(3, 3)$	$\{11, 13^*, 41\}$	3
$(3, 4)$	$\{17, 19, 23, 53\}$	4
$(3, 5)$	$\{29^*\}$	1
$(4, 1)$	$\{71, 283^*\}$	1
$(4, 2)$	$\{13^*\}$	1
$(4, 3)$	$\{499^*\}$	1
$(4, 4)$	$\{11, 13, 43^*, 47\}$	4
$(4, 5)$	$\{11, 17, 19^*, 23, 43, 47, 61\}$	7
$(5, 1)$	$\{11, 17^*, 19, 29, 31^*\}$	5
$(5, 2)$	$\{19^*, 37, 47\}$	3
$(5, 3)$	$\{37, 743^*\}$	2
$(5, 4)$	$\{11, 233^*\}$	2
$(5, 5)$	$\{37, 47^*, 53, 61\}$	4

Proof of Theorem 4.2. This follows from the table above. □

4.8 sage code

This section lists the `sage` source code that was used to perform the computations described in section 4.7.

4.8.1 Looking for two-element sets of generators

This procedure takes as input two elements of an abelian group isomorphic to $\mathbb{Z}/mZ \oplus \mathbb{Z}/n\mathbb{Z}$ with $m \mid n$, and decides whether or not they generate it.

```
# Given a list of two elements P, Q of an abelian group A
# isom. to Z/m + Z/n, with m | n, check whether <P,Q> = A.

def isSetOfGenerators(A,elements):
    P = elements[0]; Q = elements[1]
    m = A.invariants()[0]; n = A.invariants()[1]
    # we take n to be at least m
    if m > n:
        r = m
        m = n
        n = r

    # if ord(P) < ord(Q), switch P and Q.
    if P.order() != n:
        R = P
        P = Q
        Q = R

    # if ord(P) < n still holds, then <P,Q> != A.
    if P.order() != n:
        return false

    # order of Q has to be multiple of m.
    Q_order = Q.order()
    if Q_order % m != 0:
        return false

    P_multiples = set([i*P for i in range(n)])
    Q_multiples = set([j*Q for j in range(1,m)])

    # check if {i*P} and {j*Q : 0<j<m} have empty int'n
    return (P_multiples.intersection(Q_multiples) == set([]))
```

4.8.2 Finding pairs in the image of $\mathcal{C}(\mathbb{F}_p)$

The following procedure takes an elliptic curve over $\mathbb{F}_p$ as input, and finds the pairs $(Q_1, Q_2) \in \mathcal{E}(\mathbb{F}_p) \times \mathcal{E}(\mathbb{F}_p)$ such that $Q_1 = \pi_1(P)$ and $Q_2 = \pi_2(P)$ for some $P \in \mathcal{C}(\mathbb{F}_p)$.

```
# given an elliptic curve E over F_p as input
# find the elements in the image of C(F_p) -> E(F_p) x E(F_p).

def findPairs(E):
    a = E.a4(); b = E.a6()

    K = a.base_ring()
    R.<u> = PolynomialRing(K)
    S.<x> = PolynomialRing(K)

    p = K.characteristic()
    alpha = K.multiplicative_generator()

    gamma = -b/a
    phi = gamma*(u^4+u^2+1)/(u^4+u^2)
    f = x^3+a*x+b

    # don't need to consider u with u^4 + u^2 = 0
    # (maps to infinity)
    # also use the fact that u, u^-1, -u, -u^-1 all
    # give the same pair of points on E: therefore
    # u only needs to range up to (p-1)/4.

    alpha_range = range(1,(p-1)/4)
    u_list = [alpha^i for i in alpha_range]
    pairsList = []

    for u_0 in u_list:

        x_0 = phi(u_0)
        # is x_0 the x-coordinate of a point in E(F_p)?
        f_0 = f(x_0)
        if f_0.is_square() == false:
            continue
```

```
        y_0 = f_0.sqrt()

        # append the pair of points that was found
        pairsList.append([[E.point([x_0,y_0]),E.point(
        [u_0^2*x_0,u_0^3*y_0])],u_0])

    return pairsList
```

4.8.3 The criteria involving anomalous reduction

The procedure `checkAnomalousCurve` takes an elliptic curve over $\mathbb{F}_p$ as input, and determines whether either of Propositions 4.31–4.32 applies to it. It returns 2 if this is the case, and 3 otherwise. The procedure `computeV` computes the polynomial V from Lemma 4.21.

```
# given f in F_p[x], compute V
# such that x^p*V + A*x^(p-1) + U(x) = f(x)^((p-1)/2)
# with deg(U) < p-1

def computeV(f):

    K = f.base_ring()
    R.<x> = PolynomialRing(K)
    p = K.characteristic()

    g = f^((p-1)/2)
    coeff_list = g.coeffs()

    V = 0
    for i in range(p,len(coeff_list)):
        V += coeff_list[i]*x^(i-p)

    return V

# input: elliptic curve E over GF(p) with j != 0 or 1728 and
# E.order() == p
# output: 2 if a good twist was found, 3 otherwise

def checkAnomalousCurve(E):
```

```
a = E.a4(); b = E.a6()
K = a.base_ring()
p = K.characteristic()

if E.order() != p:
    print("Number of points is wrong:",E.order())
    return False

if a*b == 0:
    return False

gamma = -b/a

# explicit criterion
if (gamma).is_square():
    return 2

# Voloch's criterion: need to enumerate points on C

R.<x> = PolynomialRing(K)
f = x^3 + a*x + b
phi = gamma*(x^4+x^2+1)/(x^4+x^2)

V = computeV(f)

alpha = K.multiplicative_generator()
alpha_range = range(1,(p-1)/4)
if (p-1) % 6 == 0 and p > 7:
    alpha_range.remove((p-1)/6)

u_list = [alpha^i for i in alpha_range]

for u_0 in u_list:
    x_0 = phi(u_0)

    # is x_0 the x-coordinate of a point in E(F_p)?
    # if yes, see if Voloch's criterion holds there.
```

```
        if f(x_0).is_square():

            # we have found a point, namely (u_0,v_0):

            v_0 = f(x_0).sqrt()

            # now check to see if (5.27) holds:

            num_1   = u_0^3*(u_0^6 - 3*u_0^2 + 2)
            denom_1 = -2*u_0^6 + 3*u_0^4 - 1
            num_2   = u_0^3*v_0*V(u_0^2*phi(u_0))
            denom_2 = v_0*V(phi(u_0))

            if num_1*denom_2 != num_2*denom_1:
                if not(num_1 == 0 and denom_1 == 0) and not(
                num_2 == 0 and denom_2 == 0):
                    return 2

    return 3
```

4.8.4 Wrapper code

The rest of the procedures are mainly non-mathematical in nature. The procedure `checkManyPrimes` takes as input an elliptic curve E over $\mathbb{Q}$ and upper and lower prime bounds `max_p` and `min_p`, and outputs a table listing, among others, the primes of anomalous reduction that are lucky for E, the primes of anomalous reduction that are lucky for the twist of E, the set of primes that are unlucky for E, and the set of primes that are unlucky for its twist.

```
# return e with
# e = 0 if E has bad reduction;
# e = 1 if E(F_p) has order 1;
# e = 2 if E is anomalous and satisfies C3 or C4;
# e = 3 if E is anomalous and can't be dealt
# with by one of these criteria;
# e = 5 if E is non-anomalous and satisfies C1
# e = 6 if E is non-anomalous and can't be dealt
# with by that criterion;
```

```
# e = 7 if E(F_p) is cyclic non-anomalous (C2).

def checkSingleCurve(Ep,p):

    A = Ep.abelian_group()
    gen_orders = A.generator_orders()

    if len(gen_orders) == 0:
        return 1

    n = gen_orders[0]

    if len(gen_orders)==1:
        if n == p:
            return checkAnomalousCurve(Ep)
        if (n % p) == 0 and n != p:
            return 4
        if (n % p) != 0:
            return 7

    pairsList = findPairs(Ep)

        # check whether some pair is a set of generators;
        # keep track of how many pairs

    if pairsList == false:
        return 8

    else:
        for pair in pairsList:
            if isSetOfGenerators(A,pair[0]):
                return 5
        return 6


def checkManyPrimes(E,min_p,max_p):

    counter   = [0,0,0,0,0,0,0,0,0]
    counter_t = [0,0,0,0,0,0,0,0,0]
```

```
results   = [range(1,500) for i in range(0,9)]
results_t = [range(1,500) for i in range(0,9)]

# p <= 7 is not allowed
min_p = max(11,min_p)

Delta = E.discriminant()*E.a4()*E.a6()

for p in prime_range(min_p,max_p):

    F = GF(p)
    alpha = F.multiplicative_generator()

    if (Delta % p) == 0:
        results[0][counter[0]] = p
        counter[0] += 1
        continue

    Ep = E.change_ring(GF(p))
    e = checkSingleCurve(Ep,p)
    results[e][counter[e]] = p
    counter[e] += 1

    Ept = Ep.quadratic_twist(alpha)
    e_t = checkSingleCurve(Ept,p)
    results_t[e_t][counter_t[e_t]] = p
    counter_t[e_t] += 1

badList = results[0][0:counter[0]]
oneList = results[1][0:counter[1]]
pGoodList = results[2][0:counter[2]]
pBadList = results[3][0:counter[3]]
two_pList = results[4][0:counter[4]]
lGoodList = results[5][0:counter[5]]
lBadList = results[6][0:counter[6]]
cyclicList = results[7][0:counter[7]]

oneList_t = results_t[1][0:counter_t[1]]
pGoodList_t = results_t[2][0:counter_t[2]]
```

```
pBadList_t = results_t[3][0:counter_t[3]]
two_pList_t = results_t[4][0:counter_t[4]]
lGoodList_t = results_t[5][0:counter_t[5]]
lBadList_t = results_t[6][0:counter_t[6]]
cyclicList_t = results_t[7][0:counter_t[7]]

print(str([E.a4(),E.a6()])+":")
print("Primes of 'bad reduction': "+str(badList))
print("Good anomalous primes: "+str(pGoodList))
print("Good anom. primes (twist): "+str(pGoodList_t))
print("Bad anomalous primes: "+str(pBadList))
print("Bad non-anomalous primes: "+str(lBadList))
print("Bad anom. primes (twist): "+str(pBadList_t))
print("Bad non-anom. primes (twist): "+str(lBadList_t))

badSet = list(set(badList).union(set(pBadList))
.union(set(lBadList)).union(set(pBadList_t))
.union(set(lBadList_t)))
badSet.sort()
howManyBad = len(badSet)

print("Set of bad primes / total number of primes: ")
print("("+E.a4().str()+","+E.a6().str()+") &"),
if howManyBad > 0:
    print("\\{"),
    for i in range(0,howManyBad-1):
        print(str(badSet[i])+","),
    print(badSet[howManyBad-1]),
    print("\\}"),
else:
    print("\\emptyset"),
print("& "+str(howManyBad)+" \\\\")
print(RR(100*(1-howManyBad/164)))
```

Chapter 5

Descent on a family of superelliptic curves

Let q be a power of a prime p and let K be the rational function field $\mathbb{F}_q(t)$. For each integer $d > 1$, define $K_d = K(\zeta_d, t^{1/d})$, where ζ_d is a primitive d-th root of unity. When d is clear from the context, we sometimes write u for $t^{1/d}$. The results in this chapter, notably Theorem 5.1, generalize results of the paper [39] by Douglas Ulmer. The idea that the results in this paper could be generalized is also due to Douglas Ulmer. The results in this chapter are part of a larger, joint work together with Lisa Berger, Chris Hall, Jennifer Park, Karl Rubin, Shahed Sharif, Alice Silverberg, and Doug Ulmer. The people in this group have also contributed significantly to the work presented in this chapter. The entire project was initiated at the AIM conference "Cohomological Methods in Abelian Varieties", which was held in Palo Alto from 26–30 March 2012.

5.1 Definitions and statement of results

Choose an odd prime r different from p. Choose an integer ν and set $d = q^\nu + 1$. Assume that r divides d. We will consider the smooth projective curve C over K defined by the affine equation

$$y^r = x^{r-1}(x+1)(x+t). \tag{5.1}$$

Let $Q_\infty \in C(K)$ denote the point at infinity. We define

$$P_{i,j} = \left(\zeta_d^i t^{1/d}, \zeta_d^{jd/r+i} t^{1/d} (\zeta_d^i t^{1/d} + 1)^{d/r}\right).$$

for $0 \le i \le d-1$ and $0 \le j \le r-1$. We verify that $P_{0,j}$ is an element of $C(K_d)$ for each j. Using repeatedly that $d = q^\nu + 1$, and writing $u = t^{1/d}$, we have that

$$\begin{aligned}\left(\zeta_d^{jd/r} u(u+1)^{d/r}\right)^r &= u^r(u+1)^d \\ &= u^r(u+1)^{q^\nu+1} \\ &= u^r(u+1)(u+1)^{q^\nu} \\ &= u^r(u+1)(u^{d-1}+1) \\ &= u^{r-1}(u+1)(u+t).\end{aligned}$$

Hence we have $P_{0,j} \in C(K_d)$ for all j. Observe that $P_{i,j}$ is a $\mathrm{Gal}(K_d/K)$-conjugate of $P_{0,j}$ for all i and j, hence this computation shows that we have $P_{i,j} \in C(K_d)$ for all i and j.

Let J be the Jacobian of C. In this chapter, we will prove the following result.

Theorem 5.1. *The divisor classes $[P_{i,j}] - [Q_\infty]$ generate a subgroup of $J(K_d)$ of rank $(r-1)(d-2)$. Moreover, we have $J(K_d)[r^\infty] \cong (\mathbb{Z}/r\mathbb{Z})^3$.*

Remark 5.2. We will show that our assumption that r divides d gives a non-empty condition, in other words, that for all q there exists ν such that $d = q^\nu + 1$ is divisible by r. For such a ν to exist, it is necessary and sufficient that r is an odd prime divisor of $q^\mu + 1$ for some integer μ; if μ is the smallest such integer, we must have $\nu = \mu\ell$ for some odd integer ℓ. There are infinitely many r that satisfy this condition, as can be seen by observing that $q^{2^a} + 1$ and $q^{2^b} + 1$ are coprime integers for all distinct positive integers a and b. Since $q^a + 1$ divides $q^{a\ell} + 1$ for any odd integer ℓ, there exist infinitely many integers ν such that $d = q^\nu + 1$ is divisible by r.

5.2 Properties of C and J

We will use the projective model for C in $\mathbb{P}^2_K$ defined by

$$C' \colon Y^r Z = X^{r-1}(X+Z)(X+tZ).$$

The curve C' is non-singular at the unique point at infinity $Q_\infty = (0:1:0)$. The normalization map $C \to C'$ is bijective on $\overline{K}$-points; we will use this fact to identify $C(\overline{K})$ and $C'(\overline{K})$. Let $Q_0 = (0,0)$, $Q_1 = (-1,0)$, and

$Q_t = (-t, 0)$ be points on C. Note that Q_0 is the only singular point on C'. We write $\Delta = \{Q_0, Q_1, Q_t\}$. We consider the covering

$$\pi\colon C \to \mathbb{P}^1$$

of degree r induced by the function x. The ramification points of π are Q_0, Q_1, Q_t and Q_∞, each with ramification index r. Applying Riemann–Hurwitz gives that the genus of C is $r-1$. Note that C_{K_d} has an automorphism given by $(x, y) \mapsto (x, \zeta_d^{d/r} y)$; we denote this automorphism by ζ_r. The automorphism ζ_r of C_{K_d} induces an automorphism ζ_r of J_{K_d}. The Rosati-involution $\alpha \mapsto \alpha^\dagger$ on $\mathrm{End}(J_{K_d})$ sends ζ_r to its inverse: this simply restates the fact that ζ_r respects the polarization on J_{K_d}, which it does, coming from an automorphism of C_{K_d}. We let $\phi\colon J_{K_d} \to J_{K_d}$ be the endomorphism $1 - \zeta_r$.

Proposition 5.3. *The endomorphism ϕ is a separable isogeny of degree r^2. Its kernel is generated by $[Q_0] - [Q_\infty]$ and $[Q_1] - [Q_\infty]$.*

Proof. Let $g = r - 1$ be the genus of C. We claim that the endomorphism $(1-\zeta_r)^{r-1}$ and the separable isogeny $[r]\colon J \to J$ factor through each other. This follows from the well-known fact from algebraic number theory that the ideal (r) of the Dedekind domain $\mathbb{Z}[\zeta_r]$ decomposes as $(1-\zeta_r)^{r-1}$. It follows that:

$$\deg(1-\zeta_r)^{r-1} = \deg[r] = r^{2g} = r^{2(r-1)},$$

which proves that $\deg(1-\zeta_r) = r^2$.

For the final assertion, one easily verifies that the divisor classes $D_0 = [Q_0] - [Q_\infty]$ and $D_1 = [Q_1] - [Q_\infty]$ are contained in the kernel of ϕ. To see that the $mD_0 + nD_1$ are distinct elements of $J(K_d)$ for all pairs (m, n) with $m, n \in \{0, 1, \ldots, r-1\}$, and hence that $\ker(\phi)$ is generated by D_0 and D_1, it suffices to show that $x^m(x+1)^n$ is not an r-th power in $K_d(C)$ unless $r \mid m$ and $r \mid n$. This is a routine exercise in field theory. □

Lemma 5.4. *We have $J[\phi] = J[\phi^\dagger]$, as group schemes.*

Proof. The equality comes down to the observation that the endomorphisms $\phi = 1 - \zeta_r$ and $\phi^\dagger = 1 - \zeta_r^{-1}$ factor through each other. This follows from the fact that $(1-\zeta_r)/(1-\zeta_r^{-1}) \in \mathbb{Z}[\zeta_r]^*$. □

5.3 Relating certain divisors on C

By $\sim$ we denote linear equivalence in $\mathrm{Div}(C_{K_d})$.

Lemma 5.5. *We have the following relations in* $\mathrm{Div}(C_{K_d})$*:*

$$(r+1)Q_\infty \sim (r-1)Q_0 + Q_1 + Q_t, \tag{5.2}$$

$$\sum_{i=0}^{d-1}(P_{i,0} - Q_\infty) \sim Q_0 - Q_1, \tag{5.3}$$

and

$$\sum_{i=0}^{d-1}(P_{i,0} - P_{i,-i}) \sim Q_0 - Q_\infty. \tag{5.4}$$

Proof. Equation (5.2) follows from considering $\mathrm{div}(y) \sim 0$. We define $f, g \in K_d(C)$ as follows: $f = y - x(x+1)^{d/r}$ and $g = yx^{d/r-1} - u^{d/r}(x+1)^{d/r}$. Then (5.3) follows from considering $\mathrm{div}(f/x) \sim 0$ and (5.4) follows from $\mathrm{div}(f/xg) \sim 0$. □

Lemma 5.6. *Define* $D \in \mathrm{Div}(C_{K_d})$ *by*

$$D = \sum_{i=0}^{d-1}\sum_{j=0}^{[-1-i]}(P_{i,j} - Q_\infty),$$

where $[-1-i] \in \{0, \ldots, r-1\}$ *is congruent to* $-1-i$ *modulo* r*, then*

$$(1-\zeta_r)(D) \sim Q_0 - Q_\infty.$$

Hence the class of D *is a* $(1-\zeta_r)^2$*-torsion element of* $J(K_d)$*.*

Proof. A straightforward calculation shows $(1-\zeta_r)(\sum_{j=0}^{[-1-i]} P_{i,j}) = P_{i,0} - P_{i,-i}$; this uses that $\zeta_r(P_{i,j}) = P_{i,[j+1]}$ for all i and j with $0 \le i \le d-1$ and $0 \le j \le r-1$, where $[j+1]$ denotes $j+1$ if $j < r-1$, and 0 if $j = r-1$. Hence $(1-\zeta_r)(D) \sim Q_0 - Q_\infty$ follows from (5.4) and the fact that $\zeta_r(Q_\infty) = Q_\infty$. The last statement follows from $(1-\zeta_r)[Q_0 - Q_\infty] = 0$, as noted in Lemma 5.3. □

5.4 The homomorphism $(x - T)$

For any curve $\mathcal{C}$, we will denote by $\mathrm{Div}(\mathcal{C})$ the group of Weil divisors on $\mathcal{C}$, and by $\mathrm{Div}^0(\mathcal{C}) \subset \mathrm{Div}(\mathcal{C})$ its subgroup of degree-zero divisors. We will define the pivotal homomorphism

$$(x-T)\colon \mathrm{Div}^0(C_{K_d}) \to \prod_{Q \in \Delta} K_d^*/K_d^{*r}.$$

Its properties are described in Proposition 5.7. For an element v of the product $\prod_{Q\in\Delta} K_d^*/K_d^{*r}$, we conveniently write $v=(v_0,v_1,v_t)$, where v_i is the coordinate corresponding to Q_i.

Let $C^\circ_{K_d}\subset C_{K_d}$ be the complement of $\Delta\cup\{Q_\infty\}$. We define the homomorphism

$$(x-T)'\colon \operatorname{Div}(C^\circ_{K_d})\to\prod_{Q\in\Delta} K_d^*/K_d^{*r}$$

by defining it on a closed point $P\in C^\circ_{K_d}$ as follows

$$P\mapsto (x(P)-x(Q))_{Q\in\Delta}\,,$$

followed by taking the norm if the residue field of P is a proper field extension of K_d.

We now define the homomorphism

$$(x-T)\colon \operatorname{Div}^0(C_{K_d})\to\prod_{Q\in\Delta} K_d^*/K_d^{*r}$$

as follows: let $D\in\operatorname{Div}^0(C_{K_d})$ be a degree-zero divisor on C_{K_d}, then choose $D'\in\operatorname{Div}(C^\circ_{K_d})$ in such a way that D is linearly equivalent to D'. We define $(x-T)(D)$ to be $(x-T)'(D')$. For a proof that $(x-T)$ is well-defined, see [5, 6.2.2].

5.4.1 Descent

We fix a separable closure K_d^{sep} of K_d, and we let $\mathcal{G}$ be the absolute Galois group $\operatorname{Gal}(K_d^{\mathrm{sep}}/K_d)$ of K_d. For a finite $\mathcal{G}$-module M of cardinality coprime to p, we denote by $M^\vee$ the dual $\mathcal{G}$-module $\operatorname{Hom}(M,K_d^{\mathrm{sep}\,*})$, and we will abbreviate the Galois cohomology groups $H^i(\mathcal{G},M)$ by $H^i(M)$ for every integer $i\geq 0$.

Proposition 5.7. *There exists a homomorphism α from $H^1(J[\phi])$ to the group $\prod_{Q\in\Delta} K_d^*/K_d^{*r}$ such that the following diagram is commutative with exact bottom row.*

$$\begin{array}{ccccccccc}
 & & \operatorname{Div}^0(C_{K_d}) & & & & & & \\
 & & \downarrow & \searrow^{(x-T)} & & & & & \\
 & & J(K_d)/\phi J(K_d) & & & & & & \\
 & & \downarrow{\scriptstyle\partial} & & & & & & \\
0 & \longrightarrow & H^1(J[\phi]) & \xrightarrow{\alpha} & \prod_{Q\in\Delta} K_d^*/K_d^{*r} & \xrightarrow{\mathcal{N}} & K_d^*/K_d^{*r} & \longrightarrow & 0
\end{array}$$

Here ∂ is induced by the Galois cohomology coboundary map for the isogeny ϕ, and $\mathcal{N}$ is the map sending (a_0, a_1, a_t) to $a_1 a_t / a_0$.

Proof. The proof is based on arguments from the paper [5], where the theory of descent is developed in great generality.

Let E be $(\mathbb{Z}/r\mathbb{Z})^{\Delta}$, the $\mathcal{G}$-module of $\mathbb{Z}/r\mathbb{Z}$-valued functions on Δ. Note that the $\mathcal{G}$-action on Δ as well as E is trivial. There is a $\mathcal{G}$-module map $\alpha^\vee \colon E \to J[\phi]$ defined by $h \mapsto \sum_{Q \in \Delta} h(Q) \cdot [Q - Q_\infty]$. Proposition 5.3 shows that $\alpha^\vee$ is surjective. Its kernel R is the $\mathbb{Z}/r\mathbb{Z}$-submodule of E generated by the map ρ defined by $Q_0 \mapsto -1, Q_1 \mapsto 1, Q_t \mapsto 1$. The resulting short exact sequence of $\mathcal{G}$-modules

$$0 \to R \to E \xrightarrow{\alpha^\vee} J[\phi] \to 0 \tag{5.5}$$

is split-exact, since it consists of modules that are free as $\mathbb{Z}/r\mathbb{Z}$-modules and have trivial $\mathcal{G}$-action. Dualizing (5.5) and taking Galois cohomology, we obtain a split-exact sequence

$$0 \to H^1(J[\phi^\dagger]) \to H^1(E^\vee) \to H^1(R^\vee) \to 0. \tag{5.6}$$

By Lemma 5.4, $H^1(J[\phi^\dagger])$ is the same as $H^1(J[\phi])$. We compute that $H^1(E^\vee) = H^1(\mu_r^\Delta) = \prod_{Q \in \Delta} K_d^*/K_d^{*r}$, where the last step is Hilbert 90. Choosing the isomorphism $\mathbb{Z}/r\mathbb{Z} \xrightarrow{\sim} R$ given by $1 \mapsto \rho$, we identify $H^1(R^\vee)$ with $H^1(\mu_r) = K_d^*/K_d^{*r}$, where the last step is again Hilbert 90. With these identifications, the short exact sequence (5.6) becomes the bottom row in the diagram, and the map $H^1(E^\vee) \to H^1(R^\vee)$ corresponds to the $\mathcal{N}$ from the statement of the proposition.

The fact that the diagram is commutative is the content of Proposition 6.4 in [5]. □

It follows from Proposition 5.7 that $(x - T)$ induces a map $J(K_d) \to \prod_{Q \in \Delta} K_d^*/K_d^{*r}$. We will also denote this map by $(x - T)$. The map $(x - T)$ can be seen as a computation-friendly substitute for the coboundary map $\delta \colon J(K_d) \to H^1(J[\phi])$, since we have $(x - T) = \alpha \circ \delta$, where α is the injective map from Proposition 5.7. Moreover, Proposition 5.7 shows that the image of $(x - T)$ is contained in the kernel of $\mathcal{N}$, with $\mathcal{N}$ as in the statement of the proposition.

5.4.2 Some values of $(x - T)$

The rest of this subsection is devoted to the computation of $(x - T)(Q - Q_\infty)$ for $Q \in \Delta$.

Lemma 5.8. *Let $D \in \mathrm{Div}(C^\circ_{K_d})$. Then if $(x-T)'(D) = (v_0, v_1, v_t)$, we have $v_1 v_t / v_0 = v_0^{r-1} v_1 v_t = 1$.*

Proof. From equation (5.1) it follows that, if $P \in C^\circ_{K_d}$ is a closed point, then (the $\kappa(P)/K_d$-norm of) $x(P)^{r-1}(x(P)+1)(x(P)+t)$ is contained in K_d^{*r}. □

The following lemma states that $(x - T)$ can be "evaluated on the coordinates on which it makes sense".

Lemma 5.9. *Let $D \in \mathrm{Div}(C_{K_d})$ be a divisor supported outside of Q_∞. If $Q \in \Delta$ is such that D is also supported outside of Q, then we have*

$$(x-T)(D)_Q = \prod_P (x(P) - x(Q))^{\mathrm{ord}_P(D)}.$$

Proof. Choose a divisor $D' \in \mathrm{Div}(C^\circ_{K_d})$ that is linearly equivalent to D. Choose $g \in K_d(C)^*$ such that $D' = D + \mathrm{div}(g)$. Observe that $\mathrm{div}(g)$ is supported outside Q and Q_∞. Then

$$\begin{aligned}(x-T)(D)_Q &= (x-T)'(D')_Q \\ &= \prod_P (x(P) - x(Q))^{\mathrm{ord}_P(D')} \\ &= \prod_P (x(P) - x(Q))^{\mathrm{ord}_P(D + \mathrm{div}(g))} \\ &= \prod_P (x(P) - x(Q))^{\mathrm{ord}_P(D)} \prod_P (x(P) - x(Q))^{\mathrm{ord}_P(g)}.\end{aligned}$$

In the last expression however, the contribution of the second product is trivial:

$$\prod_P (x(P) - x(Q))^{\mathrm{ord}_P(g)} = \prod_P g(P)^{\mathrm{ord}_P(x - x(Q))} = g(Q)^r g(\infty)^{-r} = 1,$$

where the first equality is due to Weil reciprocity and the second one rests on the fact that for $Q \in \Delta$ we have $\mathrm{div}(x - x(Q)) = r \cdot Q - r \cdot Q_\infty$, as is shown by direct calculation. □

For future use, we apply Lemmas 5.8 and 5.9 to the computation of the images under $(x - T)$ of the divisors $Q_1 - Q_\infty$ and $P_i - Q_\infty$.

Proposition 5.10. *We have $(x-T)(Q_1 - Q_\infty) = (-1, 1/(1-t), t-1)$ and $(x-T)(P_{i,j} - Q_\infty) = (\zeta_d^i u, \zeta_d^i u + 1, \zeta_d^i u + t)$.*

Proof. For $\bullet \in \{0, 1, t, \infty\}$, let $D_\bullet \in \mathrm{Div}(C^\circ_{K_d})$ be a divisor that is linearly equivalent to $Q_\bullet$. Using Lemmas 5.8 and 5.9, one gets $(x-T)'(D_0) = (t, 1, t)$, $(x-T)'(D_1) = (-1, 1/(1-t), t-1)$, and $(x-T)'(D_t) = (-t, 1-t, t/(t-1))$. Applying (5.2), we then find $(x-T)'(D_\infty) = (1, 1, 1)$. Hence $(x-T)(Q_1 - Q_\infty) = (x-T)'(D_1 - D_\infty) = (-1, 1/(1-t), t-1)$.

Finally, we have $(x-T)(P_{i,j} - Q_\infty) = (x-T)(P_{i,j} - D_\infty) = (x-T)'(P_{i,j}) - (x-T)'(D_\infty) = (\zeta_d^i u, \zeta_d^i u + 1, \zeta_d^i u + t)$. □

5.5 The image of $(x - T)$

For this section, let $N \subset J(K_d)$ be the subgroup generated by the divisor classes $[P_{i,j} - Q_\infty]$, where $i \in \{0, \ldots, d-1\}$ and $j \in \{0, \ldots, r-1\}$. Observe that the known torsion elements $[Q_0 - Q_\infty]$, $[Q_1 - Q_\infty]$, $[Q_t - Q_1]$ and $[D] = [\sum_{i=0}^{d-1} \sum_{j=0}^{[-1-i]} (P_{i,j} - Q_\infty)]$ (the D is as in Lemma 5.6) are all contained in N by Lemmas 5.5 and 5.6. Therefore N contains all elements of $J(K_d)$ described so far.

Proposition 5.11. *We have* $\dim_{\mathbb{F}_r}(x-T)(N) = d$.

Proof. Since $(x-T)(P_{i,j} - Q_\infty) = (x-T)(\zeta_r^j(P_{i,0} - Q_\infty)) = (x-T)(P_{i,0} - Q_\infty)$, the dimension certainly cannot be larger than d. To show that it is precisely d, we project down from $\prod_{Q \in \Delta} K_d^*/K_d^{*r}$ to a finite-dimensional quotient space of dimension d, and conclude by showing that the projection is surjective.

For an irreducible polynomial π inside K_d, the valuation it induces on K_d^* is denoted $\mathrm{val}_\pi \colon K_d^* \to \mathbb{Z}$. We define the following map:

$$\begin{aligned} \mathrm{pr} \colon \prod_{Q \in \Delta} K_d^*/K_d^{*r} &\to \mathbb{F}_r^d \\ (v_0, v_1, v_t) &\mapsto (\mathrm{val}_{u+1}(v_1), \mathrm{val}_{u+\zeta_d^{-1}}(v_1), \mathrm{val}_{u+\zeta_d^{-2}}(v_1), \ldots, \mathrm{val}_{u+\zeta_d}(v_1)) \end{aligned}$$

By Proposition 5.10, we have $(x-T)(P_{i,j} - Q_\infty) = (\zeta_d^i u, \zeta_d^i u + 1, \zeta_d^i u + t)$. We see that pr maps the image of $P_{i,j} - Q_\infty$ to the i-th basis vector. Hence pr maps $(x-T)(N)$ surjectively onto $\mathbb{F}_r^d$. This establishes the proposition. □

Lemma 5.12. *The image under* $(x - T)$ *of the subgroup generated by* $[D]$ *and* $[Q_1 - Q_\infty]$ *has* $\mathbb{F}_r$*-dimension* 2.

Proof. Since $(x-T)(P_{i,j} - Q_\infty) = (x-T)(P_{i,0} - Q_\infty)$, as noted in the proof of Proposition 5.11, we see that the image of $D = \sum_{i=0}^{d-1} \sum_{j=0}^{[-1-i]} P_{i,j}$ is the same

as that of $\sum_{i=0}^{d-1}(d-i)(P_{i,0}-Q_\infty)$. If we resume the notation of the proof of Proposition 5.11, we find $\mathrm{pr}((x-T)(D)) = (0,-1,-2,\ldots,-d+1) \in \mathbb{F}_r^d$.

Proposition 5.10 gives $(x-T)(Q_1-Q_\infty) = (-1, 1/(1-t), t-1)$. Since in K_d we have the factorization $1-t = \prod_{i=0}^{d-1}(1-\zeta_d^i u)$, we get $\mathrm{pr}((x-T)(Q_1-Q_\infty)) = (-1,-1,-1,\ldots,-1)$. The lemma now follows. □

5.6 An algebraic lemma

We consider $\mathbb{F}_r$ as a $\mathbb{Z}[\zeta_r]$-module via the unique ring homomorphism $\mathbb{Z}[\zeta_r] \to \mathbb{F}_r$, whose kernel is the maximal ideal generated by $1-\zeta_r$. Then ζ_r acts as the identity on $\mathbb{F}_r$.

Lemma 5.13. *Let $R = \mathbb{Z}[\zeta_r]$ and $\phi = 1-\zeta_r$. Let M and N be R-modules with $N \subset M$.*

(i) There are positive integers e_i such that

$$M[r^\infty] = M[\phi^\infty] \cong \bigoplus_{i=1}^{t} R/(\phi^{e_i})$$

as R-modules, where $t = \dim_{\mathbb{F}_r} M[\phi]$.

(ii) There is an exact sequence

$$0 \to N[\phi] \to M[\phi] \to (M/N)[\phi] \to N \otimes_R \mathbb{F}_r \to M \otimes_R \mathbb{F}_r \to (M/N) \otimes_R \mathbb{F}_r \to 0,$$

where the middle map sends $m+N$ to $\phi m \otimes 1$.

Let $\rho = \dim_{\mathbb{Q}(\zeta_r)} N \otimes_{\mathbb{Z}} \mathbb{Q}$ be the rank of N as R-module, and let $V \subset M \otimes_R \mathbb{F}_r$ be the image of the map $N \to M \otimes_R \mathbb{F}_r$.

(iii) We have

$$\rho = \dim_{\mathbb{F}_r} V + \dim_{\mathbb{F}_r}(M/N)[\phi] - \dim_{\mathbb{F}_r} M[\phi].$$

Proof. Since the elements r and ϕ^{r-1} of $\mathbb{Z}[\zeta_r]$ generate the same ideal, they differ by a unit, and hence we have $M[r^\infty] = M[\phi^\infty]$. Localizing at the prime ideal (ϕ), we find, by the structure theorem for finitely generated modules over principal ideal domains:

$$M_{(\phi)} \cong R_{(\phi)}^s \oplus \bigoplus_{i=1}^{t} R/(\phi^{e_i}),$$

for some choice of non-negative integers s, t and e_i. Since localizing at (ϕ) does not affect ϕ-power torsion, we find $M[\phi^\infty] \cong \bigoplus_{i=1}^{t} R/(\phi^{e_i})$. From the isomorphism, it is clear that $t = \dim_{\mathbb{F}_r} M[\phi]$. This proves part (i).

The exact sequence given in part (ii) is the long exact sequence that results from applying $- \otimes_R \mathbb{F}_r$ to $0 \to N \to M \to M/N \to 0$.

Truncating the exact sequence of part (ii) at the fifth term, we get the exact sequence

$$0 \to N[\phi] \to M[\phi] \to (M/N)[\phi] \to N \otimes_R \mathbb{F}_r \to V \to 0. \tag{5.7}$$

Using

$$\dim_{\mathbb{F}_r} N \otimes_R \mathbb{F}_r = \dim_{\mathbb{F}_r} N_{(\phi)} \otimes_{R_{(\phi)}} \mathbb{F}_r = \rho + \dim_{\mathbb{F}_r} N[\phi],$$

and the fact that the $\mathbb{F}_r$-dimensions of the terms of (5.7) add up to zero, we obtain part (iii). This concludes the proof. □

5.7 Proof of the main theorem

As in section 5.6, we consider $\mathbb{F}_r$ as a $\mathbb{Z}[\zeta_r]$-module. Since the isogeny ϕ was defined as $1 - \zeta_r$, we may write $J(K_d)/\phi J(K_d) = J(K_d) \otimes_{\mathbb{Z}[\zeta_r]} \mathbb{F}_r$. By Proposition 5.7, we have a commutative diagram

$$\begin{array}{ccc} J(K_d) & \longrightarrow & J(K_d) \otimes_{\mathbb{Z}[\zeta_r]} \mathbb{F}_r \\ & \searrow^{(x-T)} & \downarrow \\ & & \prod_{Q \in \Delta} K_d^*/K_d^{*r} \end{array}$$

Let N be a $\mathbb{Z}[\zeta_r]$-submodule of $J(K_d)$. Then the image of N under $(x - T)$ can be identified with the image of the map $N \to J(K_d) \otimes_{\mathbb{Z}[\zeta_r]} \mathbb{F}_r$.

We conclude by giving the proof of Theorem 5.1.

Proof of Theorem 5.1. First, we determine $J(K_d)[r^\infty]$. By Proposition 5.3 and Lemma 5.13(i) we find that

$$J(K_d)[r^\infty] \cong \mathbb{Z}[\zeta_r]/(1 - \zeta_r)^{e_1} \oplus \mathbb{Z}[\zeta_r]/(1 - \zeta_r)^{e_2}$$

for some positive integers e_1, e_2. By Lemma 5.12, the classes of $[D]$ and $[Q_1 - Q_\infty]$ generate $J(K_d)[r^\infty] \otimes_{\mathbb{Z}[\zeta_r]} \mathbb{F}_r$, so by Nakayama's lemma $[D]$ and $[Q_1 - Q_\infty]$ generate $J(K_d)[r^\infty]$.

Let $N \subset J(K_d)$ be the subgroup generated by the divisor classes $[P_{i,j} - Q_\infty]$, for $0 \leq i \leq d-1$ and $0 \leq j \leq r-1$. From Proposition 5.11 and Lemma 5.13(iii) applied with $M = J(K_d)$ we find:

$$\mathrm{rank}_{\mathbb{Z}[\zeta_r]}(N) = d - 2 + \dim_{\mathbb{F}_r}(J(K_d)/N)[1-\zeta_r].$$

Since $N \otimes_{\mathbb{Z}[\zeta_r]} \mathbb{F}_p$ has dimension d, it follows from Proposition 5.11 that $N \otimes_{\mathbb{Z}[\zeta_r]} \mathbb{F}_p$ injects into $J(K_d) \otimes_{\mathbb{Z}[\zeta_r]} \mathbb{F}_p$, which by Lemma 5.13(ii) implies

$$\dim_{\mathbb{F}_r}(J(K_d)/N)[1-\zeta_r] = 0$$

Therefore, the $\mathbb{Z}$-rank of N is equal to $(r-1)(d-2)$. □

Bibliography

[1] B. J. Birch and H. P. F. Swinnerton-Dyer. The Hasse problem for rational surfaces. *J. Reine Angew. Math.*, 274/275:164–174, 1975.

[2] F. Bogomolov and Y. Tschinkel. Density of rational points on elliptic K3 surfaces. *Asian J. of Math.*, 4:351–368, 2000.

[3] Siegfried Bosch, Werner Lütkebohmert, and Michel Raynaud. *Néron Models*. Springer-Verlag, Berlin-Heidelberg, 1990.

[4] T. D. Browning, L. Matthiesen, and A. N. Skorobogatov. Rational points on pencils of conics and quadrics with many degenerate fibres. Preprint, 2012. `http://arxiv.org/abs/1209.0207`.

[5] Nils Bruin, Bjorn Poonen, and Michael Stoll. Generalized explicit descent and its application to curves of genus 3. Preprint, 2012. arXiv:1205.4456v1.

[6] J-L. Colliot-Thélène, J-J. Sansuc, and H. P. F. Swinnerton-Dyer. Intersections of two quadrics and Châtelet surfaces I. *J. reine angew. Math.*, 373:37–107, 1987.

[7] J-L. Colliot-Thélène, J-J. Sansuc, and H. P. F. Swinnerton-Dyer. Intersections of two quadrics and Châtelet surfaces II. *J. reine angew. Math.*, 374:72–168, 1987.

[8] Jean-Louis Colliot-Thélène. Surfaces rationnelles fibrées en coniques de degré 4. In *Séminaire de théorie des nombres, Paris 1988-1989*, volume 91 of *Progr. Math.*, pages 43–55. Birkhäuser, 1990.

[9] Jean-Louis Colliot-Thélène. L'arithmétique des variétés rationnelles. *Ann. Fac. Sci. Toul.*, 54(2):375–492, 1992.

[10] E. Fouvry and H. Iwaniec. Primes in arithmetic progressions. *Acta Arith.*, 42(2):197–218, 1983.

[11] Rajiv Gupta and M. Ram Murty. Cyclicity and generation of points mod p on elliptic curves. *Invent. Math.*, 101:225–235, 1990.

[12] Robin Hartshorne. *Algebraic Geometry*. Springer-Verlag, New York, 1977.

[13] Brendan Hassett. Potential Density of Rational Points on Algebraic Varieties. In *Higher Dimensional Varieties and Rational Points*. Springer, 2003.

[14] Brendan Hassett, Anthony Várilly-Alvarado, and Patrick Varilly. Transcendental obstructions to weak approximation on general K3 surfaces. *Adv. Math.*, 228:1377–1404, 2011.

[15] Shinobu Hosono, Bong H. Lian, Keiji Oguiso, and Shing-Tung Yau. Kummer structures on a K3 surface: an old question of T. Shioda. *Duke Math. J.*, 120(3):635–647, 2003.

[16] V. A. Iskovskikh. Minimal models of rational surfaces over arbitrary fields. *Izv. Akad. Nauk SSSR Ser. Math.*, 43(1):19–43, 237, 1979.

[17] S. Lang and A. Weil. Number of points of varieties in finite fields. *Amer. J. Math.*, 76:819–827, 1954.

[18] Adam Logan, David McKinnon, and Ronald van Luijk. Density of rational points on diagonal quartic surfaces. *Algebra and Number Theory*, 4(1):1–20, 2010.

[19] Yu. I. Manin. Le groupe de Brauer–Grothendieck en géométrie diophantienne. In *Actes Congrès Int. Math. Nice*, volume 1, pages 401–411, 1970.

[20] Yu. I. Manin. *Cubic Forms: Algebra, Geometry, Arithmetic*. North-Holland Publishing Co., Amsterdam, 2nd edition, 1986.

[21] Barry Mazur. The Topology of Rational Points. *Experimental Mathematics*, 1(1):35–45, 1992.

[22] Jean-François Mestre. Rang de courbes elliptiques d'invariant donné. *C. R. Acad. Sci. Paris Sér. I Math.*, 314:919–922, 1992.

[23] David Mumford. *Abelian varieties*. Oxford University Press, Oxford, 2nd edition, 1974.

[24] A. Nerode. A decision method for p-adic integral zeros of diophantine equations. *Bull. Amer. Math. Soc.*, 69:513, 1963.

[25] Thomas Preu. *Transcendental Brauer–Manin obstruction for a diagonal quartic surface*. PhD thesis, Universität Zürich, 2010.

[26] Luis Ribes and Pavel Zalesskii. *Profinite Groups*. Springer-Verlag, Berlin-Heidelberg, 2010.

[27] P. Salberger and A. N. Skorobogatov. Weak approximation for surfaces defined by two quadratic forms. *Duke Math. J.*, 63(2):517–536, 1991.

[28] Per Salberger. Sur l'arithmétique de certaines surfaces de del Pezzo. *C. R. Acad. Sci. Paris*, 303:273–276, 1986.

[29] Cecília Salgado, Damiano Testa, and Anthony Várilly-Alvarado. On the unirationality of del Pezzo surfaces of degree two. Preprint, 2013. `http://arxiv.org/abs/1304.6798`.

[30] Cecília Salgado and Ronald van Luijk. Density of rational points on del Pezzo surfaces of degree one. Preprint, 2012. `http://arxiv.org/abs/1212.2364`.

[31] Joseph H. Silverman. *Advanced Topics in the Arithmetic of Elliptic Curves*. Springer-Verlag, New York, 1994.

[32] Joseph H. Silverman. *The Arithmetic of Elliptic Curves, Second Edition*. Springer-Verlag, New York, 2009.

[33] Alexei Skorobogatov. *Torsors and rational points*. Cambridge University Press, Cambridge, 2001.

[34] A. N. Skorobogatov and Yu. G. Zarhin. A finiteness theorem for the Brauer group of abelian varieties and K3 surfaces. *J. Alg. Geom.*, 17:481–502, 2008.

[35] W. A. Stein et al. *Sage Mathematics Software (Version 5.4.1)*. The Sage Development Team, 2013. `http://www.sagemath.org`.

[36] H. P. F. Swinnerton-Dyer. Two special cubic surfaces. *Mathematika*, 9:54–56, 1962.

[37] Sir Peter Swinnerton-Dyer. Arithmetic of diagonal quartic surfaces, II. *Proc. London Math. Soc*, 80(3):513–544, 2000.

[38] Sir Peter Swinnerton-Dyer. Density of rational points on certain surfaces. 2010. Preprint.

[39] Doug Ulmer. Explicit points on the Legendre curve. Preprint, 2012. `http://arxiv.org/abs/1002.3313v2`.

[40] J. F. Voloch. Explicit p-descent for elliptic curves in characteristic p. *Compos. Math.*, 74:247–258, 1990.

[41] Olivier Wittenberg. Transcendental Brauer–Manin obstruction on a pencil of elliptic curves. In B. Poonen et Yu. Tschinkel, editor, *Arithmetic of higher-dimensional varieties*, volume 226 of *Progress in Mathematics*, pages 259–267, 2004.

Samenvatting

Mijn proefschrift gaat over *rationale punten*. Voordat ik daaraan toekom moet ik het echter eerst hebben over *rationale getallen*.

Rationale getallen

Als je leert te tellen, begin je met de *natuurlijke getallen*:

$$1, 2, 3, \ldots.$$

Later leer je van het bestaan van nul en de negatieve getallen. Samen met de positieve getallen vormen deze de *gehele getallen*:

$$\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots.$$

Maar lang niet alle getallen die je in het dagelijks leven tegenkomt zijn geheel. Een treinkaartje met korting van Den Haag naar Leiden kost bijvoorbeeld €1,90. Op de basisschool leer je dan ook dat er naast de gehele getallen *breuken* bestaan, die door wiskundigen ook wel *rationale getallen* worden genoemd. Voorbeelden van rationale getallen zijn:

$$\frac{1}{2}, -\frac{1}{3}, \frac{6}{7}, \frac{22}{7}.$$

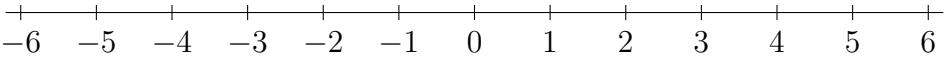
De gehele getallen zijn zelf ook rationale getallen, want het gehele getal 3 bijvoorbeeld kun je ook als een breuk schrijven:

$$3 = \frac{3}{1}.$$

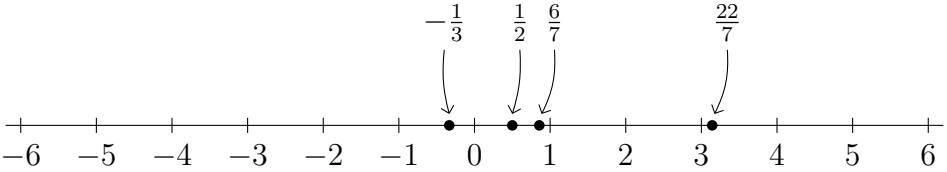
Alle soorten getallen die we hierboven besproken hebben zijn dus voorbeelden van rationale getallen.

Irrationale getallen

Op de middelbare school leer je dat alle getallen die je tot dan toe kent een plekje hebben op de *getallenlijn*:



Je moet je de getallenlijn voorstellen alsof hij zich oneindig ver naar links en rechts uitstrekt. Hieronder geven we een aantal getallen op de getallenlijn aan.



Wiskundigen hebben het niet vaak over de getallenlijn, maar ze hebben wel een naam voor de getallen die je erop aantreft, namelijk *reële getallen*. Het feit dat alle rationale getallen een plekje op de getallenlijn hebben zouden wiskundigen liever als volgt formuleren: alle rationale getallen zijn reële getallen.

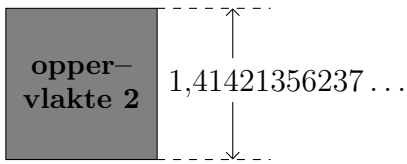
Is het omgekeerd ook waar dat alle reële getallen rationaal zijn? Nee! Hier is een reëel getal dat niet rationaal is:

$$\sqrt{2} = 1{,}41421356237\ldots.$$

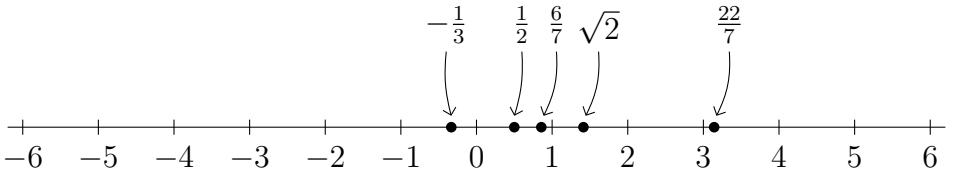
Bovenstaand getal, de *wortel van* 2 genaamd, heeft de eigenschap dat als je het met zichzelf vermenigvuldigt, je de uitkomst 2 krijgt. In een formule:

$$\sqrt{2} \times \sqrt{2} = 1{,}41421356237\ldots \times 1{,}41421356237\ldots = 2.$$

Anders gezegd, $\sqrt{2}$ is de lengte van een zijde van een vierkant met oppervlakte 2. In een plaatje:



De oude Grieken wisten al dat er geen enkele *breuk* is met bovenstaande eigenschap. Het getal $\sqrt{2}$ is dus niet rationaal. Niettemin is $\sqrt{2}$ wel gewoon een reëel getal: het heeft een plekje op de getallenlijn.



Reële getallen die niet rationaal zijn, zoals $\sqrt{2}$, noemen we ook wel *irrationale getallen*.

Intermezzo: de irrationaliteit van $\sqrt{2}$

In deze paragraaf bewijzen we dat $\sqrt{2}$ een irrationaal getal is. Deze paragraaf kan zonder problemen worden overgeslagen.

Het bewijs dat $\sqrt{2}$ irrationaal is, is een klassiek geval van een *bewijs uit het ongerijmde*. Dit gaat zo. We nemen eerst aan dat $\sqrt{2}$ wél rationaal is, om daarna op een tegenstrijdigheid uit te komen. De tegenstrijdigheid laat zien dat onze aanname fout was; dus is $\sqrt{2}$ niet rationaal.

Stel dat $\sqrt{2}$ rationaal is. Dan zijn er gehele getallen m en n zodanig dat

$$\sqrt{2} = \frac{m}{n}.$$

Zoals je op de basisschool leert kun je sommige breuken *vereenvoudigen*, door de teller en noemer door hetzelfde getal te delen. We mogen dus aannemen dat $\frac{m}{n}$ niet meer verder vereenvoudigd kan worden. In het bijzonder zijn m en n niet allebei *even* – waren ze dat wel, dan konden we ze allebei door 2 delen, waardoor de breuk vereenvoudigd zou worden.

We gaan nu met bovenstaande vergelijking aan de slag, eerst maar eens door van beide leden het kwadraat te nemen:

$$2 = \frac{m^2}{n^2}.$$

Vervolgens vermenigvuldigen we beide leden met n^2 en krijgen dan

$$2n^2 = m^2. \tag{1}$$

Merk nu op: als m even is, dan is m^2 ook even; als m oneven is, dan is m^2 ook oneven. Hetzelfde geldt uiteraard als we m vervangen door n. Omdat m en n niet allebei even waren, zijn m^2 en n^2 dus ook niet allebei even. Uit bovenstaande vergelijking zien we dat m^2 gelijk is aan $2n^2$, dus m^2 is even, en dus is m zelf even. We kunnen dus

$$m = 2k$$

schrijven, waarbij k weer een zeker geheel getal is. Als we bovenstaande invullen in vergelijking (1), dan krijgen we

$$2n^2 = (2k)^2,$$

oftewel, als we de haakjes wegwerken,

$$2n^2 = 4k^2.$$

Delen we de laatste vergelijking door 2, dan staat er

$$n^2 = 2k^2.$$

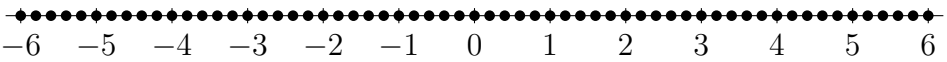
Hieruit volgt dat n^2 even is, en dus n zelf ook. Maar dan zijn m en n dus beide even. Dit is in tegenstrijdigheid met de eerdere opmerking dat $\frac{m}{n}$ een vereenvoudigde breuk was. Dus $\sqrt{2}$ is irrationaal.

Dichtheid

We weten nu dus dat niet alle reële getallen rationaal zijn. Het is zelfs nog erger dan dat: in de 19e eeuw bewees Georg Cantor dat bijna alle reële getallen *ir*rationaal zijn! Aan de andere kant, als je alle rationale getallen op de getallenlijn zou aanstippen, dan zou je de hele getallenlijn met stipjes bedekken. Als voorbeeld hebben we hieronder de rationale getallen

$$-\frac{60}{10}, -\frac{58}{10}, -\frac{56}{10}, \ldots, \frac{56}{10}, \frac{58}{10}, \frac{60}{10}$$

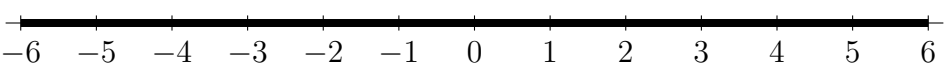
aangestipt:



In bovenstaand plaatje zie je de afzonderlijke stipjes nog wel, maar als je bijvoorbeeld de rationale getallen

$$-\frac{600}{100}, -\frac{599}{100}, -\frac{598}{100}, \ldots, \frac{598}{100}, \frac{599}{100}, \frac{600}{100}$$

aanstipt, dan krijg je dit:

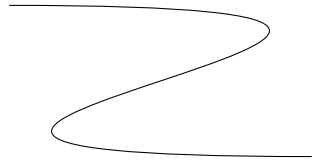


Hoe klein je de stipjes ook maakt – als je *alle* rationale getallen zou aanstippen, dan zou de hele getallenlijn ingekleurd raken. We zeggen ook wel dat de rationale getallen *dicht* liggen op de getallenlijn.

Het verschijnsel dichtheid staat centraal in dit proefschrift. Daarin wordt echter niet meer gekeken naar de dichtheid van de rationale getallen op de getallenlijn, maar naar de dichtheid van rationale *punten* op meetkundige voorwerpen als *krommen* en *oppervlakken*.

Krommen

Een *kromme* is grofweg gesproken iets wat eruitziet als een uit de vrije hand getekende (niet noodzakelijk rechte) lijn op papier. Bijvoorbeeld:



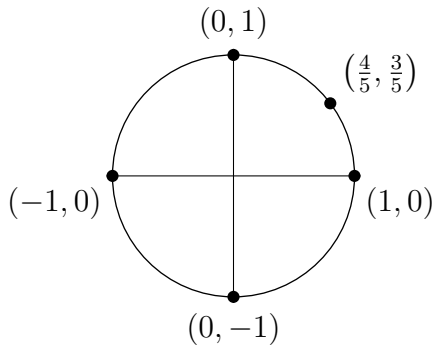
In dit proefschrift wordt met een kromme altijd een kromme bedoeld die gedefinieerd is door algebraïsche vergelijkingen. Voor het gemak zullen we ons in deze samenvatting verder beperken tot krommen in het platte vlak. Een punt in het platte vlak wordt aangegeven met (a, b), waarbij a de x-coördinaat is, en b de y-coördinaat.

Voorbeeld: een cirkel

Als voorbeeld van een kromme bekijken we de cirkel C in het platte vlak met straal 1 en middelpunt $(0, 0)$. Deze heeft als vergelijking

$$x^2 + y^2 = 1.$$

De cirkel C bestaat dus uit alle punten (x, y) in het platte vlak die voldoen aan bovenstaande vergelijking. Hieronder is C getekend en zijn enkele punten op C aangegeven.



Een *rationaal punt* op de cirkel C is een punt (a, b) dat op C ligt, en waarvoor a en b rationale getallen zijn. Voorbeelden van rationale punten op C zijn de punten $(1, 0)$, $(0, 1)$, $(-1, 0)$, $(0, -1)$ en $\left(\frac{4}{5}, \frac{3}{5}\right)$ die boven aangegeven staan. Andere rationale punten op C zijn $\left(\frac{7}{13}, \frac{12}{13}\right)$, $\left(\frac{9}{25}, \frac{24}{25}\right)$ en $\left(\frac{20}{29}, \frac{21}{29}\right)$, zoals de lezer door een berekening zou kunnen nagaan.

Pythagoras

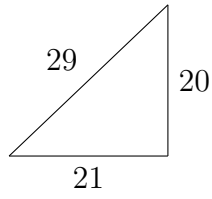
Er is iets grappigs aan de hand met de cirkel C en zijn rationale punten. Neem het laatstgenoemde punt $\left(\frac{20}{29}, \frac{21}{29}\right)$. Dat het op C ligt betekent

$$\left(\frac{20}{29}\right)^2 + \left(\frac{21}{29}\right)^2 = 1.$$

Als we dit met 29^2 vermenigvuldigen, dan staat er

$$20^2 + 21^2 = 29^2.$$

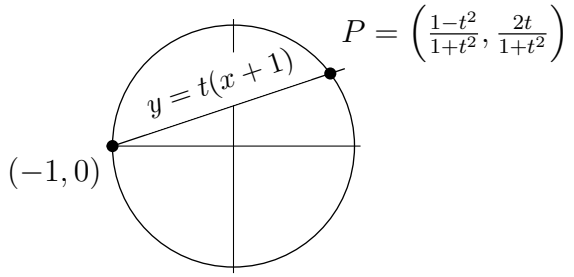
Degenen die de stelling van Pythagoras kennen zullen zich nu realiseren dat de driehoek met zijden 20, 21 en 29 rechthoekig is:



Op dezelfde manier leidt het punt $\left(\frac{4}{5}, \frac{3}{5}\right)$ tot de bekende rechthoekige driehoek met zijdelengten 3-4-5, leidt het punt $\left(\frac{7}{13}, \frac{12}{13}\right)$ tot de rechthoekige driehoek met zijdelengten 7-12-13 en leidt het punt $\left(\frac{9}{25}, \frac{24}{25}\right)$ tot de rechthoekige driehoek met zijdelengten 9-24-25.

Dichtheid van de rationale punten op de cirkel

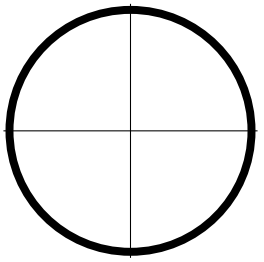
We zullen laten zien dat C oneindig veel rationale punten heeft. Beschouw de cirkel C, en laat L_t de lijn zijn door het punt $(-1, 0)$ en met richtingscoëfficiënt t. De vergelijking van deze lijn is $y = t(x + 1)$.



Zoals aangegeven snijdt de lijn de cirkel in het punt

$$P = \left(\frac{1 - t^2}{1 + t^2}, \frac{2t}{1 + t^2}\right).$$

Als t een rationaal getal is, dan laat bovenstaande formule zien dat P een rationaal punt is op C. Omdat je voor t oneindig veel verschillende rationale getallen kunt invullen, liggen er oneindig veel rationale punten op C. Meer is waar, want de rationale punten liggen zelfs *dicht* op C: als je elk rationaal punt op C zou aangeven met een stipje, dan bedek je de hele cirkel met stipjes:



Krommen in het algemeen

Een kromme Γ in het platte vlak wordt gegeven door een vergelijking

$$f(x, y) = 0,$$

waarbij f een *polynoom met rationale coëfficiënten* is, dat wil zeggen dat $f(x, y)$ een som is van termen van de vorm cx^iy^j, waarbij c een rationaal

getal is en waarbij i en j niet-negatieve gehele getallen zijn. De rationale punten op Γ zijn weer die punten op Γ waarvan de x- en y-coördinaten rationale getallen zijn. We noemen Γ verder *irreducibel* wanneer f niet te schrijven is als het product van twee niet-constante polynomen.

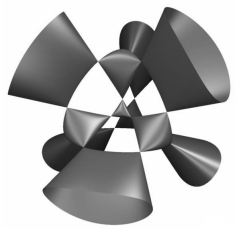
We kunnen irreducibele krommen indelen naargelang hun *geslacht*. Het geslacht van een kromme is een niet-negatief geheel getal, dat nauw verbonden is met zijn meetkundige eigenschappen.

- De krommen van geslacht 0 zijn de *kegelsneden*, zoals de cirkel C van eerder. Als een kromme Γ geslacht 0 heeft, en Γ bezit tenminste één rationaal punt, dan liggen de rationale punten dicht op Γ.
- Als een kromme Γ van geslacht 1 een rationaal punt heeft, is het een zogenaamde *elliptische kromme*. Op sommige elliptische krommen liggen de rationale punten dicht, op andere niet.
- Een kromme Γ van geslacht groter dan 1 heeft *eindig* veel rationale punten volgens een beroemd resultaat van Faltings uit 1983. De rationale punten liggen dus nooit dicht op een dergelijke kromme.

Of de rationale punten op een kromme Γ dicht liggen of niet wordt dus in belangrijke mate bepaald door het geslacht van Γ.

Oppervlakken

De cirkel C van hierboven was gedefinieerd door middel van de vergelijking $x^2 + y^2 = 1$. Als we in plaats van vergelijkingen in x en y kijken naar vergelijkingen in x, y en z, dan komen we uit bij de zogenaamde *oppervlakken* in de driedimensionale ruimte. Als je een oppervlak zou tekenen zou je bijvoorbeeld het volgende plaatje kunnen krijgen.



Rationale punten op oppervlakken

Ook bij een oppervlak kunnen we weer kijken naar zijn *rationale punten*. Net zoals de rationale punten op de cirkel aanleiding gaven tot rechthoekige

driehoeken met gehele zijdelengten, vinden ook rationale punten op oppervlakken vele toepassingen binnen de getaltheorie.

De vragen die ten grondslag liggen aan mijn onderzoek zijn vooral de volgende twee. Voor welke typen oppervlakken mogen we verwachten dat de rationale punten dicht liggen, en voor welke mogen we het juist niet verwachten? Zijn er net als voor krommen eenvoudige meetkundige criteria die voorspellen of de rationale punten al dan niet dicht liggen? Dit zijn zeer veelomvattende vragen, en ik verwacht dat er zeker nog jarenlang onderzoek voor nodig is om ze echt op te lossen.

Dichtheid van rationale punten op K3-oppervlakken

Met de resultaten uit mijn proefschrift kun je onder meer de volgende uitspraak bewijzen. Als a en b rationale getallen zijn waarbij a bovendien positief is, en K is het oppervlak gegeven door

$$z^2 = (x^3 + ax + b)(y^3 + ay + b),$$

dan liggen de rationale punten dicht op K. Het oppervlak K is een voorbeeld van een *K3-oppervlak*, zo genoemd naar de meetkundigen Kähler, Kodaira en Kummer.

Dankwoord

Ten eerste dank ik mijn promotor, Peter Stevenhagen, zowel voor het uitstekende onderzoeksklimaat aan het Mathematisch Instituut, waarvoor hij als wetenschappelijk directeur verantwoordelijk is, als voor de vele antwoorden die hij gegeven heeft op mijn wiskundige vragen. Daarnaast wil ik graag mijn copromotor Ronald van Luijk bedanken. Zijn inhoudelijke vakkundigheid, zijn persoonlijke betrokkenheid en zijn onfeilbare oog voor detail hebben mij gedurende de laatste vier jaar zowel geholpen als geïnspireerd. Beste Ronald, ontzettend bedankt.

Verder ben ik dank verschuldigd aan Jaap Top, die mij op het spoor bracht van de constructie van Mestre die ten grondslag ligt aan hoofdstuk 4, en aan Bas Edixhoven, Lenny Taelman en Peter Bruin, die mijn vragen over meetkunde altijd met eindeloos geduld en goed humeur beantwoord hebben. Het is voorts onmogelijk om vier jaar op dezelfde universiteit te werken als Hendrik Lenstra en niet van hem te leren; ik wil hem daarvoor dan ook hartelijk danken.

I would like to thank Bas Edixhoven, Alexei Skorobogatov, Jaap Top, Robin de Jong, and Tony Várilly-Alvarado for agreeing to serve on my *promotiecommissie* and for carefully reading this thesis. I would further like to thank Sir Peter Swinnerton-Dyer, for his great insights and for the pleasure that I derived from his work, and Alexei Skorobogatov, for his wonderful encouragement. Special thanks go to Felipe Voloch, whose remarks have greatly contributed to some of the results in Chapter 4, to Doug Ulmer, without whom Chapter 5 would never have existed, and to my other collaborators on the AIM project, Lisa Berger, Chris Hall, Jennifer Park, Karl Rubin, Shahed Sharif, and Alice Silverberg. I would like to thank Hélène Esnault, Andrew Kresch, Bjorn Poonen, and Alexei Skorobogatov for organizing and giving me the opportunity to participate in the great *Rational Points and Algebraic Cycles* semester in Lausanne. I would also like to thank David Holmes, for some very agreeable collaborative efforts, and Martin Bright, Kęstutis Česnavičius, Altan Erdoğan, Rachel Newton,

Cecília Salgado, Damiano Testa, and Bianca Viray for stimulating discussions on several topics.

I would further like to say thanks to all the people working at the *Mathematisch Instituut*, for having made working there such a great pleasure. In particular, I would like to mention my office mates Gabriele, Bien, Alberto, and Julio, and my other (former or current) fellow PhD students: Andrea, Ariyan, Athanasios, Chao, Dino, Frits, Jeanine, Krzysztof, Michiel, Miek, Samuele, and Wei Dong.

Dan wil ik graag mijn vader en moeder bedanken, alsmede mijn lieve zusje Manon en haar kersverse man Teun, voor de morele steun die ze me altijd geboden hebben. Ook Jan en Corrie, die er altijd voor me waren, wil ik op deze plek graag heel hartelijk bedanken.

Tenslotte dank ik mijn vrienden, Allard, David, Henri, Jasper, Jeroen, Marijke, Marijn, Meike, Michal, Michiel, Olga, Peter, Roy en Vincent. Wiskunde doen is een veeleisende activiteit. Het is belangrijk om nooit, nooit te vergeten dat er daarnaast nog andere dingen in het leven zijn. Bedankt dat jullie me hieraan blijven herinneren.

Curriculum vitæ

Rene Pannekoek werd in 1981 geboren te Apeldoorn. Zijn jeugd bracht hij door in het Veluwse dorp Epe, waar hij ook de Gildeschool bezocht. In groep zes raakte hij gefascineerd door de Griekse mythologie, waarna hij besloot zijn scholing voort te zetten aan het Gymnasium Apeldoorn. Op die school deed hij mee aan diverse landelijke wiskundewedstrijden, waaronder de Kangoeroewedstrijd, waarbij hij in 1995 de eerste prijs behaalde in de categorie tweede klas voorbereidend wetenschappelijk onderwijs, en de Nederlandse Wiskunde Olympiade, waarbij hij in 1998 de zevende prijs behaalde. In 1999 deed hij achtereenvolgens eindexamen en vertegenwoordigde hij Nederland samen met vijf andere jongeren bij de Internationale Wiskunde Olympiade in Boekarest.

In datzelfde jaar begon Rene aan de studies wiskunde en natuurkunde aan de Universiteit Utrecht. Na enkele academische uitstapjes, onder meer naar de studie assyriologie aan de Universiteit Leiden, besloot hij zijn bachelor- en mastertitels in de wiskunde te behalen aan de Rijksuniversiteit Groningen. Aan deze universiteit studeerde hij in 2009 cum laude af op een onderzoek getiteld "Parametrizations over $\mathbb{Q}$ of cubic surfaces", uitgevoerd onder leiding van prof. dr. Jaap Top.

Na de voltooiing van zijn studie vervolgde Rene zijn wiskundige carrière als promovendus aan de Universiteit Leiden. Hier voerde hij onder supervisie van dr. Ronald van Luijk een promotieonderzoek uit naar de getaltheorie van K3-oppervlakken. Verder was hij aan de Universiteit Leiden werkzaam in het onderwijs. In 2013 hoopt hij te promoveren op het proefschrift "Topological aspects of rational points on K3 surfaces", waarover hij voordrachten gaf in Londen, Lausanne, Bristol, Hannover en Leuven. Een voordracht over zijn onderzoek bij het Nederlands Mathematisch Congres van 2013 in Nijmegen leverde hem de Philips-wiskundeprijs voor promovendi op.

Vanaf oktober 2013 zal Rene twee jaar als postdoctoraal onderzoeker verbonden zijn aan Imperial College in Londen.