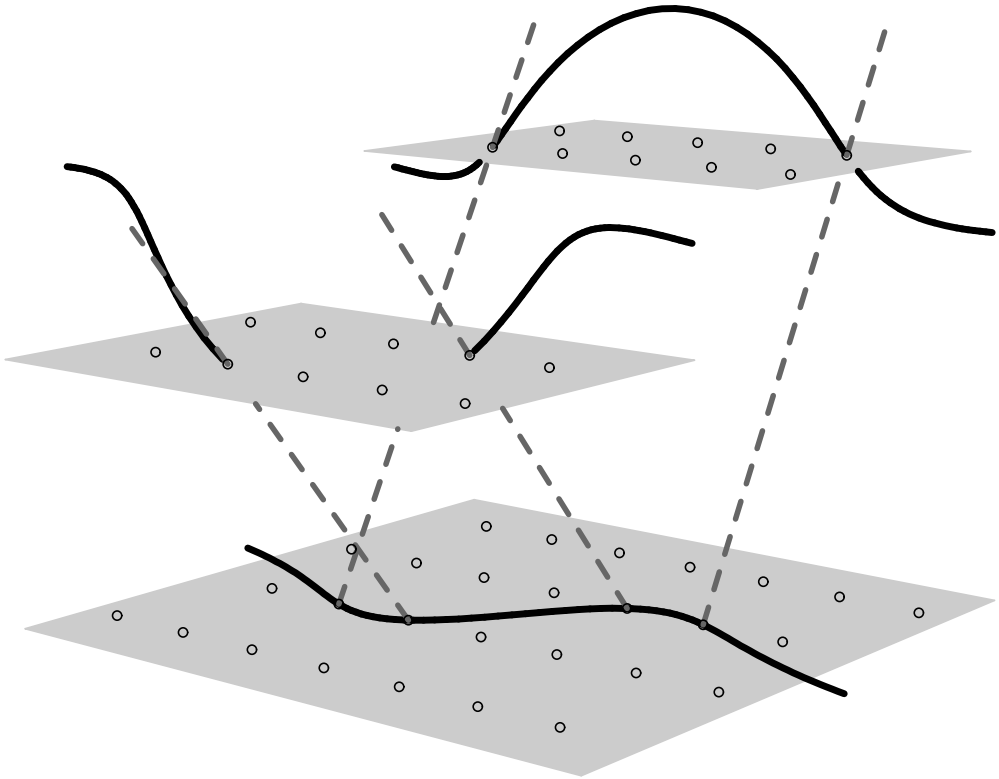
Chabauty methods and covering techniques applied to generalised Fermat equations



Nils Bruin

Chabauty methods and covering techniques applied to generalised Fermat equations

PROEFSCHRIFT

ter verkrijging van
de graad van Doctor aan de Universiteit Leiden,
op gezag van de Rector Magnificus Dr. W.A. Wagenaar,
hoogleraar in de faculteit der Sociale Wetenschappen,
volgens besluit van het College voor Promoties
te verdedigen op woensdag 6 oktober 1999
te klokke 15.15 uur

door

Nils Roald Bruin

geboren te Pijnacker in 1972

Samenstelling van de promotiecommissie:

promotor:	prof. dr. R. Tijdeman
copromotor:	dr. F. Beukers (Universiteit Utrecht)
referent:	prof. dr. E. F. Schaefer (Santa Clara University, USA)
overige leden:	prof. dr. G. van Dijk
	prof. dr. H. W. Lenstra Jr. (Univeristeit Leiden/UC Berkeley, USA)
	prof. dr. J. P. Murre
	dr. B. de Smit

Contents

Chapter 1

The generalised Fermat equation

1.1 Introduction

The roots of Diophantine geometry go back to at least the ancient Greeks. The Pythagoreans already knew that in every right triangle, the lengths of the sides satisfy a relation of the form $x^2 + y^2 = z^2$. They probably were not the first to be aware of this relation, but we do know that they were aware of the fact that it is not automatic (but true) that there are integral solutions to this equation, i.e. that not all right triangles with two sides of integral length have an integral length for their third side, but that there are some that do.

In Arithmetica, Diophantus formulated the related arithmetic question of writing a square as the sum of two other squares. Pierre de Fermat came across this and wondered if the 2 as exponent is essential to this equation, i.e. if $x^n + y^n = z^n$ has positive integer solutions for $n > 2$. The remark he scribbled in the margin of the book vexed mathematicians for 350 years, but as we now know (see [Wil95]), this equation admits no solutions.

Several generalisations spring to mind. One may wonder what integral solutions to $x_1^n + \cdots + x_m^n = 0$ exist. This is not the direction we will pursue. When we talk about the *generalised Fermat equation* we mean

$$Ax^r + By^s = Cz^t$$

with $r, s, t \in \mathbb{Z}_{>0}$ and $A, B, C \in \mathbb{Z}$, not all zero. Note that this equation is not homogeneous and thus, the argument that it suffices to look at $\gcd(x, y, z) = 1$ to describe all solutions is not valid. However, as Beukers points out, describing general solutions is often not a very interesting problem. For instance, if we take $U, V \in \mathbb{Z}$ and $W := U + V$, then $(U^5V^4W^3)^5 + (U^8V^7W^5)^3 = (U^{12}V^{10}W^8)^2$. For any solution $x^5 + y^3 = z^2$, we have that the solution resulting from $U = x^5$, $V = y^3$, $W = z^2$ is weighted homogeneously equivalent (as described below) to (x, y, z). Therefore, the given formula parametrises all solutions up to equivalence. We will restrict ourselves to $\gcd(x, y, z) = 1$ (or, more generally, $\gcd(x, y, z)$ composed of a given finite set of primes), which is a much more interesting problem.

Note that the described equation is *weighted homogeneous*: If (x, y, z) is a solution and $d = \operatorname{lcm}(r, s, t)$, then $(\lambda^{d/r}x, \lambda^{d/s}y, \lambda^{d/t}z)$ also satisfies the equation. We call two such solutions *weighted homogeneously equivalent*. Let $g = \gcd(r, s, t)$ and write $P(x, y, z) := (x^{r/g} : y^{s/g} : z^{t/g}) \in \mathbb{P}_2(\mathbb{Q})$. It follows that two equivalent solutions (x_1, y_1, z_1) and (x_2, y_2, z_2) have

$P(x_1, y_1, z_1) = P(x_2, y_2, z_2)$. Conversely, if two solutions (x_1, y_1, z_1) and (x_2, y_2, z_2) have $P(x_1, y_1, z_1) = P(x_2, y_2, z_2)$, then there is a $\lambda \in \mathbb{Q}$ such that

$$(x_1, y_1, z_1) = (\delta_x \lambda^{d/r} x_2, \delta_y \lambda^{d/s} y_2, \delta_z \lambda^{d/t} z_2),$$

where $\delta_x = 1$ if r/g is odd and $\delta_x = \pm 1$ otherwise and δ_y, δ_z are defined analogously. As a consequence, $P(x, y, z)$ does not necessarily distinguish between equivalence classes that are related by trivial transformations such as $x \mapsto -x$, but is faithful otherwise.

Let S be a finite set of primes. We call a solution *S-primitive* if $\gcd(x, y, z)$ contains only primes from S. We call an equivalence class of solutions S-primitive if it contains an S-primitive solution. If $S = \emptyset$ then we call such a class simply *primitive*.

1.2 Classification

The structure of the solution sets depends mainly on the quantity $\chi = \chi(r, s, t) := 1/r + 1/s + 1/t$. First we look at what is known for $\chi > 1$. In this case, we have $(r, s, t) = (2, 3, 3), (2, 3, 4), (2, 3, 5), (2, 2, t)$ (for any $t \geq 2$) or permutations of these. This is what we call the *spherical case*. Beukers showed that there exists a finite set of polynomial solutions such that the integral solutions can be obtained by specialising:

1.2.1. Theorem (Beukers). *Let $A, B, C \in \mathbb{Z}$, $ABC \neq 0$ and $r, s, t \in \mathbb{Z}_{\geq 2}$ such that $\chi > 1$. Then the equation $Ax^r + By^s = Cz^t$ has either zero or infinitely many solutions $x, y, z \in \mathbb{Z}$ with $\gcd(x, y, z) = 1$. Moreover, there is a finite set of triples $X, Y, Z \in \mathbb{Q}[U, V]$ with $\gcd(X, Y, Z) = 1$ and $AX^r + BY^s = CZ^t$ such that for every primitive integral solution (x, y, z), there is a triple (X, Y, Z) and $u, v \in \mathbb{Q}$ such that $x = X(u, v)$, $y = Y(u, v)$, $z = Z(u, v)$.*

(See [Beu98].) Beukers' proof is based on the fact that there are only finitely many number fields of bounded degree and ramification. In principle, this is an effective statement in the sense that this finite set of number fields can be enumerated. This enumeration process is not very efficient, however, so practical limitations become inhibitive. In Chapter 3 we will discuss some special cases where we can determine such a set of polynomials in practice.

A pair u, v, as in the theorem, represents a point $(u : v) \in \mathbb{P}_1(\mathbb{Q})$. The theorem basically says that there is a finite number of rational maps $\varphi : \mathbb{P}_1 \to \mathbb{P}_2$, defined over $\mathbb{Q}$, such that the representatives $(x^{r/g} : y^{s/g} : z^{t/g})$ of primitive classes of solutions in the $\mathbb{P}_2$ are covered by the images of $\mathbb{P}_1(\mathbb{Q})$ under the maps φ. We say that the solutions are *parametrised* by a finite set of $\mathbb{P}_1$'s.

If $\chi = 1$ then $(r, s, t) = (3, 3, 3), (4, 4, 2)$ or $(2, 3, 6)$. This is the *Euclidean case*. Here, solutions correspond to rational points on curves of genus 1. We find the curves $A(x/y)^3 + B = C(z/y)^3$, $A(x/y)^4 + B = C(z/y^2)^2$ and $A(x/z^3)^2 + B(y/z^2)^3 = C$ respectively. We basically see the same phenomenon. Primitive solution classes are parametrised by the rational points on finitely many algebraic curves. In this case, the curves are of genus 1 instead of genus 0. Depending on the curves, there will be zero, finitely many or infinitely many solutions. However, since the rational points on curves of genus 1 have a very special

structure (they form a finitely generated group, if there are any), we still have a fairly satisfactory description of the primitive solutions in this case.

For $\chi < 1$, the *hyperbolic case*, there is also a finite set of parametrising curves, but they are of genus > 1 and so, by Faltings' theorem (Theorem 2.3.3), there is only a finite number of primitive solutions:

1.2.2. Theorem (Darmon, Granville). *Let $A, B, C \in \mathbb{Z}$, $ABC \neq 0$ and $r, s, t \in \mathbb{Z}_{\geq 2}$ such that $\chi < 1$. Then the equation $Ax^r + By^s = Cz^t$ has only finitely many solutions $x, y, z \in \mathbb{Z}$ with $\gcd(x, y, z) = 1$.*

(See [DG95].) The proof is ineffective in two places. They use Riemann's Existence Theorem to obtain the parametrising curves and invoke Faltings' theorem to get finiteness of the set of rational points. The main part of this text deals with making this statement effective in a number of special cases.

The ABC-conjecture suggests an even stronger finiteness result.

1.2.3. Conjecture (ABC-Conjecture). *For every $\epsilon > 0$ there are only finitely many coprime positive integers a, b, c satisfying the relation $a + b = c$ such that*

$$\frac{\log c}{\log(\text{product of prime divisors of } abc)} > 1 + \epsilon.$$

The following argument comes from [Tij89]. Let r, s, t be positive integers. If $1/r + 1/s + 1/t < 1$, then $1/r + 1/s + 1/t \leq 41/42$. If we apply the ABC-conjecture with $\epsilon < 1/41$ to $(a, b, c) = (Ax^r, By^s, Cz^t)$ (possibly dividing out common factors to a, b, c), then we get for each $A, B, C \in \mathbb{Z}$, that there are only finitely many pairwise prime triples (x^r, y^s, z^t) with $\chi < 1$ such that $Ax^r + By^s = Cz^t$. Thus, finiteness should still hold if we allow r, s, t to vary under the restriction that $\chi < 1$, but fixing A, B, C.

From here on, we restrict ourselves to $A = B = C = 1$. In all spherical cases, we have infinitely many solutions and, apart from $x^2 + y^3 = z^5$, we have an efficient way of obtaining the parametrisations (see Chapter 3). In [Thi96], some bounds on the number of needed parametrisations for $x^2 + y^3 = z^5$ are derived which are better than the bounds following from the proof of Theorem 1.2.1, but are not guaranteed to be sharp. In the Euclidean cases, no nontrivial primitive solutions exist.

For the hyperbolic cases, we find that $(x, y, z) = (1, 0, 1), (0, 1, 1)$ are not the only positive primitive solutions, as can be seen in Table 1.1, copied from [Beu98]. One of the striking facts is that this table does not contain any example for which $r, s, t \geq 2$. This leads to the following bold conjecture.

1.2.4. Conjecture (Tijdeman, Zagier, Beal Prize Problem). *Let x, y, z, r, s, t be positive integers with $r, s, t > 2$. If $x^r + y^s = z^t$ then x, y, z have a factor in common.*

This conjecture was also posed by a Dallas banker named Beal, who awarded a prize for its proof or a counterexample (see [Mau97]).

$$
\begin{aligned}
1^r + 2^3 &= 3^2 \quad (r > 6)\\
13^2 + 7^3 &= 2^9\\
2^7 + 17^3 &= 71^2\\
2^5 + 7^2 &= 3^4\\
3^5 + 11^4 &= 122^2\\
17^7 + 76271^3 &= 21063928^2\\
1414^3 + 2213459^2 &= 65^7\\
33^8 + 1549034^2 &= 15613^3\\
43^8 + 96222^3 &= 30042907^2\\
9262^3 + 15312283^2 &= 113^7
\end{aligned}
$$

Table 1.1: Positive and primitive solutions to $x^r + y^s = z^t$; $\chi < 1$

1.3 Main results

Although the generalised Fermat equation (even with $A = B = C = 1$) seems well beyond present techniques for solving, some of the special cases are solved. For the remainder of this text, we put $A = B = C = 1$. As was pointed out in the previous section, the spherical and Euclidean cases are fairly well understood. In this section, we assume that $\chi < 1$.

The case $r = s = t$ is dealt with by Wiles. The equations $x^r + y^r = z^2$ and $x^r + y^r = z^3$ are proved not to have any nontrivial primitive solutions in [DM97] for $r \geq 7$ (assuming Shimura-Tanayama-Weil for the latter). There, they also deal with $x^r + y^r = 2z^r$, a special case of $x^p + 2^\alpha y^p + z^p$ investigated in [Rib97]. Poonen deals with $x^r + y^r = z^2$, $x^r + y^r = z^3$ and $x^r + y^r = 2z^r$ for $r < 7$ in [Poo98].

According to the ABC-conjecture, the complete list in Table 1.1 should be finite. In this thesis we shall show that, for some exponent triples (r, s, t), the list is complete.

1.3.1. Theorem. *If $x, y, z \in \mathbb{Z}$ satisfy $x^2 \pm y^4 = \pm z^6$ and $\gcd(x, y, z) = 1$ then $xyz = 0$.*

1.3.2. Theorem. *The only integer, pairwise prime, solutions to $x^2 + y^8 = z^3$ are*

$$(x, y, z) \in \{(\pm 1, 0, 1), (0, \pm 1, 1), (\pm 1549034, \pm 33, 15613)\}$$

1.3.3. Theorem. *The only integer, pairwise prime, solutions to $x^8 + y^3 = z^2$ are*

$$(x, y, z) \in \{(\pm 1, 0, \pm 1), (0, 1, \pm 1), (\pm 1, 2, \pm 3), (\pm 43, 96222, \pm 30042907)\}.$$

1.3.4. Theorem. *If $x, y, z \in \mathbb{Z}$ satisfy $x^2 + y^4 = z^5$ and $\gcd(x, y, z) = 1$ then $xyz = 0$.*

1.3.5. Theorem. *The only integer, pairwise prime solutions to $x^2 - y^4 = z^5$ are*

$$(x, y, z) \in \{(\pm 1, 0, 1), (0, \pm 1, -1), (\pm 122, \pm 11, 3), (\pm 7, \pm 3, -2)\}.$$

The main part of the rest of this text develops the machinery to prove these theorems. Upon inspection of Table 1.1, we see that the only r, s, t for which a nontrivial solution (other than $1 + 2^3 = 3^2$) not dealt with in one of the theorems above exist, are $2, 3, 9$ and $2, 3, 7$. While $2, 3, 9$ seems vulnerable to an attack along the lines presented in this text, the case $2, 3, 7$ seems well out of reach. See [Beu98] for details of what can be done.

Chapter 2

Basic definitions

In this chapter we fix some notation and review some standard results. The reader may prefer to skim through this chapter rather than read it thoroughly.

2.1 Number fields

Let K be a number field (i.e. a finite field extension of the field of rationals $\mathbb{Q}$). Then we write $\mathcal{O}_K$, or $\mathcal{O}$ if K is understood from the context, for the ring of integers of K (i.e. the ring of elements that are a root of a monic polynomial over $\mathbb{Z}$). Let $\mathfrak{p}$ be a prime ideal of $\mathcal{O}$. Then we write $\nu_\mathfrak{p} : K^* \to \mathbb{Z}$ for the normalised discrete valuation related to it (i.e. $\nu_\mathfrak{p}(K^*) = \mathbb{Z}$). Let $N_{\mathcal{O}/\mathbb{Z}}(\mathfrak{p}) := \#(\mathcal{O}/\mathfrak{p})$ denote the norm of $\mathfrak{p}$ over $\mathbb{Z}$. Then we define the normalised absolute value related to $\mathfrak{p}$ by $|x|_\mathfrak{p} := N_{\mathcal{O}/\mathbb{Z}}(\mathfrak{p})^{-\nu_\mathfrak{p}(x)}$ for $x \in K$. The field K is a topological field with respect to the metric topology induced by this absolute value and we write $K_\mathfrak{p}$ for the metric completion of K. We extend $|.|_\mathfrak{p}$ and $\nu_\mathfrak{p}$ to $K_\mathfrak{p}$. The completion of $\mathcal{O}$ is $\mathcal{O}_\mathfrak{p} := \{x \in K_\mathfrak{p} : \nu_\mathfrak{p}(x) \geq 0\}$. It is a local ring with maximal ideal $\mathfrak{p}\mathcal{O}_\mathfrak{p} = \{x \in K_\mathfrak{p} : \nu_\mathfrak{p}(x) \geq 1\}$. We choose a uniformiser $u_\mathfrak{p} \in \mathcal{O}$ at $\mathfrak{p}$, i.e. an element such that $(u_\mathfrak{p})\mathcal{O}_\mathfrak{p} = \mathfrak{p}\mathcal{O}_\mathfrak{p}$. Dividing out by any power of $\mathfrak{p}$ gives us a notion of reduction. We have the following exact sequence.

$$0 \longrightarrow \mathfrak{p}^e\mathcal{O}_\mathfrak{p} \longrightarrow \mathcal{O}_\mathfrak{p} \stackrel{\mathrm{mod}\,\mathfrak{p}^e}{\longrightarrow} \mathcal{O}/\mathfrak{p}^e \longrightarrow 0,$$

where we use that $\mathcal{O}_\mathfrak{p}/\mathfrak{p}^e\mathcal{O}_\mathfrak{p}$ is canonically isomorphic to $\mathcal{O}/\mathfrak{p}^e$. We induce this reduction map on polynomial rings $\mathcal{O}_\mathfrak{p}[X_1, \ldots, X_n]$ and free, finite $\mathcal{O}_\mathfrak{p}$-modules with basis by reducing the coefficients individually. Note that $\mathcal{O}/\mathfrak{p}$ is a finite field. We write $\mathrm{char}(\mathfrak{p})$ for the characteristic of this field, i.e. the rational prime that divides $N_{\mathcal{O}/\mathbb{Z}}(\mathfrak{p})$.

Field embeddings $\sigma : K \hookrightarrow \mathbb{C}$ give rise to Archimedean absolute values on K. If $\sigma(K) \subset \mathbb{R}$, we call σ a *real place* of K. In this case we define $|x|_\sigma = |\sigma(x)|$. Otherwise, σ is called a *complex place* and we write $|x|_\sigma = |\sigma(x)|^2$. These Archimedean places are called *primes at infinity*.

Let $\mathbb{Q} \subset K \subset L$ be a tower of number fields. We say that a prime $\mathfrak{p}$ of L lies above a prime p of K (notation $\mathfrak{p} \mid p$) if the topology on K induced by $|.|_\mathfrak{p}$ is that of $|.|_p$. Let S be a finite set of primes of subfields of K, containing the (unique) infinite prime of $\mathbb{Q}$. We say a prime $\mathfrak{p}$ of K lies *outside* S ($\mathfrak{p} \nmid S$) if $\mathfrak{p}$ does not lie above any prime in S. We define the ring of S-integers

$$(\mathcal{O}_K)_S = \mathcal{O}_S = \{x \in K : x \in \mathcal{O}_\mathfrak{p} \text{ for all } \mathfrak{p} \nmid S\}.$$

Suppose we have a tuple $(x_1, \ldots, x_n) \in K^n$. We call such a tuple *$S$-primitive* if we have that $\min(\nu_\mathfrak{p}(x_1), \ldots, \nu_\mathfrak{p}(x_n)) = 0$ for every $\mathfrak{p} \nmid S$.

Following [Sil86, Chapter X], we adopt the notation

$$K(S,m) := \{x \in K^*/(K^*)^m : \nu_\mathfrak{p}(x) \bmod m = 0 \text{ for all } \mathfrak{p} \nmid S\}.$$

We have that $K(S,m)$ is finite. We write $\delta \in K(S,m)$ as a shorthand for a representative $\delta \in K^*$ of an element of $K(S,m)$. If the m-torsion part of the ideal class group is a subgroup of the part generated by $\mathfrak{p} \mid S$, then $K(S,m) = \mathcal{O}_S^*/(\mathcal{O}_S^*)^m$ and then the representatives can be chosen to be m-th power free S-units (as far as m-th power freeness is defined for units). This is trivially the case if the class number (the order of the class group) $h(K)$ of K is prime to m.

If $K \subset L$ is a Galois extension (i.e. normal and separable), then we write $\mathrm{Gal}(L/K)$ for the group of field automorphisms of L that are the identity on K. We write $\bar{K}$ for an algebraic (separable) closure of K and $\mathrm{Gal}(K) := \mathrm{Gal}(\bar{K}/K)$ for the absolute Galois group of K, i.e. the Galois group of the extension $K \subset \bar{K}$.

2.2 Resultants

Let R be an integral domain and let $F, G \in R[X]$ be polynomials with $\deg(F) = n$ and $\deg(G) = m$. We write $F(X) = f_0X^n + \cdots + f_n$ and $G(X) = g_0X^m + \cdots + g_m$ and define

$$\mathrm{res}(F,G) := \det \underbrace{\begin{pmatrix} f_0 & \ldots & f_n & 0 & 0 & \ldots & 0 \\ 0 & f_0 & \ldots & f_n & 0 & \ldots & 0 \\ \vdots & & \ddots & & \ddots & & \\ 0 & \ldots & 0 & f_0 & f_1 & \ldots & f_n \\ g_0 & g_1 & \ldots & g_m & 0 & \ldots & 0 \\ & \ddots & & & \ddots & & \\ 0 & \ldots & 0 & g_0 & g_1 & \ldots & g_m \end{pmatrix}}_{n+m} \begin{matrix} \left.\vphantom{\begin{matrix}a\\a\\a\\a\end{matrix}}\right\}m \\ \left.\vphantom{\begin{matrix}a\\a\\a\\a\end{matrix}}\right\}n \end{matrix}.$$

Consequently, $\mathrm{res}(F,G)$ is a polynomial in the coefficients of F and G, and $\mathrm{res}(F,G) \bmod \mathfrak{p} = \mathrm{res}(F \bmod \mathfrak{p}, G \bmod \mathfrak{p})$, where the latter should be read as the resultant of a degree n and a degree m polynomial, with leading coefficients that are possibly 0. Suppose that

$$F(X) = f_0 \prod_{i=1}^{n} (X - \alpha_i), \quad G(X) = g_0 \prod_{j=1}^{m} (X - \beta_j)$$

over some extension of R. As shown in [Lan65, V,§10, Proposition 4], we have that $\mathrm{res}(F,G) = f_0^m g_0^n \prod_{i=1}^{n} \prod_{j=1}^{m} (\alpha_i - \beta_j)$. Consequently, two polynomials over a domain have a common root only if their resultant vanishes. This gives us the following lemma, which is the central principle of all the results in this text.

2.2.1. Lemma. *Let K be a number field, let $F, G \in \mathcal{O}_K[X,Y]$ be non-constant homogeneous polynomials and coprime over K. Let $m \in \mathbb{Z}_{>0}$ and $D \in \mathcal{O}_K$. Suppose that S is a set of primes such that $\mathrm{res}(F(X,1), G(X,1))$, $\mathrm{res}(F(1,Y), G(1,Y))$, $D \in \mathcal{O}_S^*$. If $x, y, z \in K$ with (x,y,z) S-primitive such that*

$$F(x,y)G(x,y) = Dz^m,$$

then there are $z_1, z_2 \in K$, with (z_1, z_2) S-primitive and $\delta_1, \delta_2 \in K(S,m)$ with $\delta_1\delta_2/D \in (K^*)^m$ such that

$$\begin{aligned} F(x,y) &= \delta_1 z_1^m, \\ G(x,y) &= \delta_2 z_2^m, \\ \frac{\delta_1\delta_2}{D} &= \left(\frac{z}{z_1 z_2}\right)^m. \end{aligned}$$

Proof: Let $\mathfrak{p}$ be a prime of K outside S. Note that since F and G have integral coefficients and $D \in \mathcal{O}_\mathfrak{p}^*$, we have that $m\nu_\mathfrak{p}(z) = \nu_\mathfrak{p}(F(x,y)G(x,y)/D) \geq \min(\nu_\mathfrak{p}(x), \nu_\mathfrak{p}(y))$. Therefore (x,y) is S-primitive as well. So, $x \bmod \mathfrak{p} \neq 0$ or $y \bmod \mathfrak{p} \neq 0$. Assume the latter. Since $\mathrm{res}(F(X,1), G(X,1)) \in \mathcal{O}_\mathfrak{p}^*$ we have that $F(X,1) \bmod \mathfrak{p}$ and $G(X,1) \bmod \mathfrak{p}$ have no common root. It follows that $\nu_\mathfrak{p}(F(x/y,1)) = 0$ or $\nu_\mathfrak{p}(G(x/y,1)) = 0$. By homogeneity, we have that $\nu_\mathfrak{p}(F(x,y)) = \nu_\mathfrak{p}(F(x/y,1)) + \deg(F)\nu_\mathfrak{p}(y) = \nu_\mathfrak{p}(F(x/y,1))$ and the same for G. Since

$$m\nu_\mathfrak{p}(z) = \nu_\mathfrak{p}(Dz^m) = \nu_\mathfrak{p}(F(x,y)G(x,y)) = \nu_\mathfrak{p}(F(x,y)) + \nu_\mathfrak{p}(G(x,y)),$$

we see that $\nu_\mathfrak{p}(F(x,y)), \nu_\mathfrak{p}(G(x,y)) \in m\mathbb{Z}$ for all $\mathfrak{p} \nmid S$. The case $x \bmod \mathfrak{p} \neq 0$ follows from symmetry. □

Furthermore, we define $\mathrm{disc}(F) = \mathrm{res}(F, (d/dX)(F))$. It is straightforward to check that $\mathrm{res}(F,G) \mid \mathrm{disc}(FG)$.

2.3 Algebraic curves

It is surprising to see how difficult it is to give a satisfactory elementary definition of an algebraic curve over a number field. Intuitively, we mean dimension 1 subsets of a vector space K^n over a field K, described by polynomial equations. However, we do want to be able to apply (non-linear) changes of coordinates and we want to look at points at infinity as well. Furthermore, we often use reduction mod $\mathfrak{p}$. This would lead us to consider schemes over the ring of integers. The language of schemes, although appropriate, is considered to be difficult by many people and, in fact, once a model of a curve is chosen, not really necessary for effective computations.

In this section, we define the concept of a curve (over number fields, completions of number fields, finite fields and over their algebraic closures) in terms of smooth projective models. The reduction map will only be dealt with in relation to a model of the curve over the ring of integers of a number field or a completion of it at a prime. It is in no way a complete treatment of the subject and we refer the reader to any basic text

on algebraic geometry for proofs and details. See for instance [Sil86, Chapter I,II] and [Har77, Chapter IV], although Hartshorne only considers algebraically closed fields. Our curves satisfy Hartshorne's definition if considered over the algebraic closure of their field of definition.

By an *algebraic curve* over a field K we mean a smooth projective, geometrically irreducible variety of dimension 1. Such a curve admits a smooth projective model $\mathcal{C}$ over K. This is given by an ideal $I(\mathcal{C}) \subset K[X_0, \ldots, X_n]$, generated by homogeneous polynomials $F_1, \ldots, F_m$. Let $\bar{K}$ be an algebraic closure of K. The $\bar{K}$-rational points form a non-empty set

$$\mathcal{C}(\bar{K}) = \left\{(x_0 : \ldots : x_n) \in \mathbb{P}_n(\bar{K}) : F_i(x_0, \ldots, x_n) = 0 \text{ for } i = 1, \ldots, m\right\}.$$

That the model represents a smooth variety of dimension 1, follows if $\mathcal{C}(\bar{K}) \neq \emptyset$, does not contain isolated points and for all $(x_0 : \ldots : x_n) \in \mathcal{C}(\bar{K})$ we have

$$\operatorname{rk}\left(\frac{\partial F_i}{\partial X_j}(x_0, \ldots, x_n)\right)_{i,j} = n - 1.$$

Geometrically irreducible means that $\mathcal{C}(\bar{K})$ is not the union of two strictly smaller sets $\mathcal{C}_1(\bar{K})$ and $\mathcal{C}_2(\bar{K})$, given by polynomials over $\bar{K}$. Let $P = (x_0 : \ldots : x_n) \in \mathcal{C}(\bar{K})$ and let L be a subfield of $\bar{K}$ containing K. Suppose that $x_0 \neq 0$. We call P *L-rational* if $x_1/x_0, \ldots, x_n/x_0 \in L$. We write $K(P)$ for the smallest subfield L of $\bar{K}$ such that P is L-rational. We write $\mathcal{C}(L)$ for the set of L-rational points of $\mathcal{C}$.

Note that $\mathrm{Gal}(L)$ acts on $\mathbb{P}_n(\bar{L})$. If $\mathcal{C}$ is defined over L and $P \in \mathcal{C}(\bar{L})$, then a point ${}^{\sigma}P$ conjugate to P over L will also satisfy the polynomial equations that define $\mathcal{C}$. Thus, $\mathrm{Gal}(L)$ acts on $\mathcal{C}(\bar{L})$. We can characterise $\mathcal{C}(L)$ as the $\mathrm{Gal}(L)$-invariant points $\mathcal{C}(\bar{L})^{\mathrm{Gal}(L)}$.

If K is a number field then we can choose $F_1, \ldots, F_m \in \mathcal{O}[X_0, \ldots, X_n]$. This gives us a notion of reduction at a prime $\mathfrak{p}$ of K for projective models

$$I(\mathcal{C} \bmod \mathfrak{p}) = (F_1 \bmod \mathfrak{p}, \ldots, F_m \bmod \mathfrak{p}) \subset (\mathcal{O}/\mathfrak{p})[X_0, \ldots, X_n].$$

We say $\mathcal{C}$ has good reduction at $\mathfrak{p}$ if $\mathcal{C} \bmod \mathfrak{p}$ is again a smooth projective model over $\mathcal{O}/\mathfrak{p}$.

Let $\varphi_0, \ldots, \varphi_m \in K[X_0, \ldots, X_n]$ be homogeneous polynomials of degree $d \geq 0$. Then the (partially defined) map

$$\begin{array}{rccc} \varphi & : & \mathbb{P}_n(\bar{K}) & \to & \mathbb{P}_m(\bar{K}) \\ & & (x_0 : \ldots : x_n) & \mapsto & (\varphi_0(x_0, \ldots, x_n) : \ldots : \varphi_m(x_0, \ldots, x_n)) \end{array}$$

is called a representative of a *rational map over K*. If φ' is another representative that agrees with φ where both are defined, then φ' is said to represent the same rational map. We denote the represented map with φ as well. A rational map is defined where one of its representatives is defined.

Let $\mathcal{C}$ and $\mathcal{D}$ be smooth projective models of curves over K. A non-constant map $\varphi : \mathcal{D} \to \mathcal{C}$ is called a *cover over K* if it is induced by rational maps over K from the ambient projective space of $\mathcal{D}$ to that of $\mathcal{C}$. As it turns out, such covers can always be extended to the whole of $\mathcal{D}(\bar{K})$ and are surjective on $\mathcal{C}(\bar{K})$. Being defined by polynomials,

the map $\varphi : \mathcal{D}(\bar{K}) \to \mathcal{C}(\bar{K})$ has finite fibres. We put $\deg(\varphi) := \max_{P \in \mathcal{C}(\bar{K})} \#\varphi^{-1}(\{P\})$. If $\deg(\varphi) = 1$, then φ is invertible and φ^{-1} is again a cover over K. In that case, $\mathcal{C}$ and $\mathcal{D}$ are called birationally equivalent. A curve over K can be defined as a birational equivalence class of smooth projective models over K. We will often not distinguish between a curve and a representing model.

The set of degree 1 covers $\mathcal{C} \to \mathcal{C}$ over K forms a group and is called the group of automorphisms $\mathrm{Aut}_K(\mathcal{C})$ of $\mathcal{C}$ over K. We write $\mathrm{Aut}(\mathcal{C}) := \mathrm{Aut}_{\bar{K}}(\mathcal{C})$. Suppose that $\varphi : \mathcal{D} \to \mathcal{C}$ is a cover over K. We write $\mathrm{Aut}(\mathcal{D}/\mathcal{C})$ for the subgroup of automorphisms $\tau \in \mathcal{D}$ such that $\varphi \circ \tau = \varphi$. If $\#\mathrm{Aut}(\mathcal{D}/\mathcal{C}) = \deg(\varphi)$, then φ is called a *Galois* cover and we write $\mathrm{Gal}(\mathcal{D}/\mathcal{C}) := \mathrm{Aut}(\mathcal{D}/\mathcal{C})$. As a shorthand, we sometimes write $(\mathrm{Gal}(\mathcal{D}/\mathcal{C})\backslash .) : \mathcal{D} \to \mathrm{Gal}(\mathcal{D}/\mathcal{C})\backslash\mathcal{D}$ for φ. Note that, although suppressed in this notation, the choice of φ is important in this construction, especially if $\mathrm{Gal}(\mathcal{D}/\mathcal{C}) \not\subset \mathrm{Aut}_K(\mathcal{D})$.

A curve $\mathcal{D}$ over K that is birational to $\mathcal{C}$ over $\bar{K}$ by a cover $\psi : \mathcal{D} \to \mathcal{C}$ (but not necessarily over K) is called a *twist* of $\mathcal{C}$. Note that $\mathrm{Gal}(K)$ acts on $\mathrm{Aut}(\mathcal{C})$, induced by the action on $\mathcal{C}(\bar{K})$. We write $\mathrm{Twist}(\mathcal{C}/K)$ for the set of twists of $\mathcal{C}$ modulo isomorphisms over K. In terms of group cohomology (see [Ser79, Chapter VII] for instance), we have $\mathrm{Aut}_K(\mathcal{C}) = H^0(\mathrm{Gal}(K), \mathrm{Aut}(\mathcal{C}))$. Elements of $H^1(\mathrm{Gal}(K), \mathrm{Aut}(\mathcal{C}))$ can be represented by maps $\xi : \mathrm{Gal}(K) \to \mathrm{Aut}(\mathcal{C})$ satisfying the cocycle property $\xi(\sigma_1 \circ \sigma_2) = {}^{\sigma_1}(\xi(\sigma_2)) \circ \xi(\sigma_1)$. The following theorem links twists to 1-cocyles.

2.3.1. Theorem. *Let $\mathcal{C}$ be a curve over a field K of characteristic 0. Then the map*

$$\begin{array}{ccc} \mathrm{Twist}(\mathcal{C}/K) & \to & H^1(\mathrm{Gal}(K), \mathrm{Aut}(\mathcal{C})) \\ \psi & \mapsto & (\sigma \mapsto {}^{\sigma}\psi \circ \psi^{-1}) \end{array}$$

is a bijection.

(See [Sil86, Theorem X.2.2].)

Consider the affine part $\{X_0 \neq 0\} \subset \mathbb{P}_n$ with coordinate functions $Y_1 = X_1/X_0, \ldots, Y_n = X_n/X_0$. A projective model $\mathcal{C}$ leads to an affine model given by $I_{\mathcal{C}}^{\mathrm{aff}} = (F_i(1, Y_1, \ldots, Y_n))_{i=1\ldots m}$. Smoothness implies that for any $P_0 \in \mathcal{C}(\bar{K})$ there is an affine model and a coordinate function Y_i such that $Z(P) := Y_i(P) - Y_i(P_0)$ is a uniformiser at P_0, i.e. all coordinate functions can be uniquely expressed as formal power series in Z such that $P(Z) = (1 : Y_1(Z) : \ldots : Y_n(Z)) \in \mathcal{C}(K(P)[\![Z]\!])$ with $P(0) = P_0$ and $Y_i(P(Z)) = Z + Y_i(P_0)$.

Let $\varphi : \mathcal{D} \to \mathcal{C}$ be a cover of curves over K, let $P \in \mathcal{D}(\bar{K})$, Z be a uniformiser of $\mathcal{D}$ at P and $Y_1, \ldots, Y_n$ be coordinate functions of an affine part of $\mathcal{C}$ such that $Y_i(\varphi(P)) = 0$. We can express the Y_i uniquely as power series in Z. This gives us $e \in \mathbb{Z}_{>0}$ such that $Y_i(Z) = 0 \bmod Z^e$ and $Y_i(Z) \neq 0 \bmod Z^{e+1}$. We write $\mathrm{ord}_P(Y_i) := e$. We define the ramification index of φ at P as $e_P(\varphi) := \min\{\mathrm{ord}_P(Y_1 - Y_1(P)), \ldots, \mathrm{ord}_P(Y_n - Y_n(P))\}$ and we call φ ramified at P if $e_P(\varphi) > 1$. For fields of characteristic 0 we have that $\sum_{P \in \varphi^{-1}(\{Q\})} e_P(\varphi) = \deg(\varphi)$. Covers are ramified at only finitely many points.

We will not explicitly define the genus of a curve here. We will only need that $\mathrm{genus}(\mathcal{C}) \in \mathbb{Z}_{\geq 0}$ is a birational invariant and obeys the following lemma.

2.3.2. Theorem (Hurwitz). *Let $\varphi : \mathcal{D} \to \mathcal{C}$ be a finite cover of smooth curves over a*

field K of characteristic 0. Then

$$2(\text{genus}(\mathcal{D})-1) = 2\deg(\varphi)(\text{genus}(\mathcal{C})-1) + \sum_{P\in\mathcal{D}(\bar{K})}(e_P(\varphi)-1).$$

(See [Sil86, Theorem II.5.9] or [Har77, IV.2].)

We will often meet curves given as covers of the projective line. If such a cover is Galois with cyclic Galois group, we say that the curve is a *cyclic cover* of the projective line. We restrict ourselves to cyclic covers with an affine model $Y^m = F(X)$ where F is a square free polynomial. Such a model is smooth at all finite points. For $m = 2$, we have that with respect to $U = 1/X$ and $V = Y/X^{\lceil \deg(F)/2\rceil}$, we get the model $V^2 = U^{2\lceil\deg(F)/2\rceil}F(1/U)$. The points at infinity in the original model correspond to points with $U = 0$ and this model is smooth there. If $2 \mid n+1$, then there is only one such point and we denote it with ∞. Otherwise, there are 2 of those points. We denote these with ∞^+ and ∞^-. Instead of working with a smooth model of cyclic covers, we will work with this singular model and understand it to represent the smooth curve corresponding to it.

A motivating fact for the work in this thesis is that for a curve $\mathcal{C}$ over a number field K, the genus turns out to be crucial for the arithmetic properties of $\mathcal{C}$.

2.3.3. Theorem (Faltings). *Let $\mathcal{C}$ be a curve over a number field K with* $\text{genus}(\mathcal{C}) \geq 2$. *Then $\mathcal{C}(K)$ is finite.*

(See [Fal83] and [Fal84] or [Bom90].)

2.4 Elliptic curves

An *elliptic curve* E over K is an algebraic curve $\mathcal{E}$ over K with $\text{genus}(\mathcal{E}) = 1$, together with a point $O \in \mathcal{E}(K)$. The map $\mathcal{E} \to \text{Pic}^0(\mathcal{E})$ given by $P \to [P - O]$ induces an abelian group structure on $\mathcal{E}$, where O is the neutral element. This makes $\mathcal{E}$ a group variety, which we write additively (see [Sil86] for proofs and details). Such curves admit (in characteristic $\neq 2, 3$) what we will call a projective twisted Weierstrass model in $\mathbb{P}_2$ with coordinates $(X : Y : D)$

$$E : \gamma Y^2 D = X^3 + a_2X^2D + a_4XD^2 + a_6D^3,$$

sending O to the point $\infty = (0 : 1 : 0)$. This relates to the ordinary affine Weierstrass model

$$U^2 = V^3 + \gamma a_2V^2 + \gamma^2a_4V + \gamma^3a_6$$

via $(U, V) = (Y/(\gamma D), X/(\gamma D))$. The group law is characterised by the rules that ∞ is neutral and that $P_1 + P_2 + P_3 = \infty$ if and only if P_1, P_2, P_3 are collinear. We write E for an elliptic curve (given by a Weierstrass model) and $\mathcal{E}$ for the corresponding genus 1 curve. Naturally, if we consider non-constant maps $E_1 \to E_2$ between elliptic curves, we should insist that the distinguished point of E_1 lands on the distinguished point on E_2. Covers between elliptic curves with this property are called *isogenies*. They are automatically group homomorphisms.

We have the following theorem.

2.4.1. Theorem (Mordell-Weil theorem). *Let E be an elliptic curve over a number field K. Then the group $E(K)$ is finitely generated. Thus there is an $r \in \mathbb{Z}_{\geq 0}$ (the rank of $E(K)$) and a finite subgroup $E^{\mathrm{tor}}(K) \subset E(K)$ such that $E(K) \cong \mathbb{Z}^r \times E^{\mathrm{tor}}(K)$.*

(See [Sil86, Theorem VIII.6.7].)

Let E be a twisted Weierstrass model over a number field K with $\gamma, a_2, a_4, a_6 \in \mathcal{O}$ (so it is actually a model over $\mathcal{O}$). Let $\mathfrak{p}$ be a prime of good reduction of E. Then E is also a curve over $K_\mathfrak{p}$ and $E(K_\mathfrak{p}) \to (E \bmod \mathfrak{p})(\mathcal{O}/\mathfrak{p})$ is a surjective group homomorphism. We define the kernel of reduction $E^{(1)}(K_\mathfrak{p})$ to be the kernel of this map.

$$0 \longrightarrow E^{(1)}(K_\mathfrak{p}) \longrightarrow E(K_\mathfrak{p}) \stackrel{\bmod \mathfrak{p}}{\longrightarrow} (E \bmod \mathfrak{p})(\mathcal{O}/\mathfrak{p}) \longrightarrow 0.$$

We define the affine coordinates $Z = X/Y$, $W = D/Y$. The function Z is a uniformiser around ∞ and we have the equation

$$\gamma W = Z^3 + a_2 Z^2 W + a_4 Z W^2 + a_6 W^3.$$

Note that $P \in E^{(1)}(K_\mathfrak{p})$ implies $Z(P) \in \mathfrak{p}\mathcal{O}_\mathfrak{p}$. Let $E(\mathcal{O}[\gamma^{-1}][\![Z]\!])$ denote the collection of formal power series solutions to E, i.e. triples $X, Y, D \in \mathcal{O}[\gamma^{-1}][\![Z]\!]$ such that $\gamma Y^2 D = X^3 + a_2 X^2 D + a_4 X D^2 + a_6 D^3$ as formal power series. We consider $G(Z) \in E(\mathcal{O}[\gamma^{-1}][\![Z]\!])$ defined by $Z(G(Z)) = Z$ and $G(Z) \bmod (Z^2) = (Z : 1 : 0) \bmod Z^2$. We expand the group law in a power series $F(Z_1, Z_2) = Z(G(Z_1) + G(Z_2)) \in \mathcal{O}[\gamma^{-1}][\![Z_1, Z_2]\!]$. As is described in [Sil86, Chapter IV], this leads to a formal group $\mathcal{F}$ in one variable Z with coefficients in $\mathcal{O}[\gamma^{-1}]$. The group $E^{(1)}(K_\mathfrak{p})$ is isomorphic to $\mathcal{F}(\mathfrak{p}\mathcal{O}_\mathfrak{p})$ (good reduction implies $\gamma \in \mathcal{O}_\mathfrak{p}^*$). By [Sil86, Proposition IV.5.5] we have a power series $\mathrm{Log}_\mathcal{F}(Z) \in K[\![Z]\!]$ with $\mathrm{Log}_\mathcal{F}(Z) = Z \bmod (Z^2)$ and if $\nu_\mathfrak{p}(\mathrm{char}(\mathfrak{p})) < \mathrm{char}(\mathfrak{p}) - 1$, then by [Sil86, Theorem IV.6.4], $\mathrm{Log}_\mathcal{F} : \mathcal{F}(\mathfrak{p}\mathcal{O}_\mathfrak{p}) \to \mathfrak{p}\mathcal{O}_\mathfrak{p}$ is a group isomorphism. This induces a group isomorphism

$$\mathrm{Log}_\mathfrak{p} : E^{(1)}(K_\mathfrak{p}) \to \mathfrak{p}\mathcal{O}_\mathfrak{p},$$

with inverse $\mathrm{Exp}_\mathfrak{p}$. Furthermore, since for $z \in \mathfrak{p}\mathcal{O}_\mathfrak{p}$ we have $\mathrm{Log}_\mathcal{F}(z) \bmod \mathfrak{p}^2 = z \bmod \mathfrak{p}^2$, it follows that if $G_1, G_2 \in E^{(1)}(K_\mathfrak{p})$ then $Z(G_1 + G_2) \bmod \mathfrak{p}^2 = Z(G_1) + Z(G_2) \bmod \mathfrak{p}^2$.

Note that the concept of reduction is dependent on the chosen model E over $\mathcal{O}$. In that sense, the notation $E^{(1)}(K_\mathfrak{p})$ is misleading, since it suggests an object given over $K_\mathfrak{p}$. Writing $0 \to E^{(1)}(\mathcal{O}_\mathfrak{p}) \to E(\mathcal{O}_\mathfrak{p})$ would be even more misleading, since this would suggest we are looking at $\mathfrak{p}$-integral points, which most people would interpret as points with $\mathfrak{p}$-integral values for X/D and Y/D. As long as one remembers that $E^{(1)}(K_\mathfrak{p})$ is a set with a group structure which comes from a formal group $\mathcal{F}$ over $\mathcal{O}$ and that the object is really dependent on the chosen model, misunderstandings are unlikely to arise. As to whether the $^{(1)}$ should be a super- or a subscript, authors do not agree. In this text a superscript is chosen since subscripts are used to distinguish different curves. The parentheses are just ornaments to avoid confusion with an exponent. In some books, a ^{0} is used (see for instance [CF96]). This is not preferable, since the index 0 is widely used to indicate the

inverse image of the smooth part of $E \bmod \mathfrak{p}$ (which is not the whole of E in the case of bad reduction).

The inclusion $E(K) \hookrightarrow E(K_\mathfrak{p})$ splits the study of $E(K)$ in two subgroups of groups of which we have a better understanding.

$$\begin{array}{ccccccccc} 0 & \longrightarrow & E(K) \cap E^{(1)}(K_\mathfrak{p}) & \longrightarrow & E(K) & \longrightarrow & E(K) \bmod \mathfrak{p} & \longrightarrow & 0 \\ & & \uparrow & & \uparrow & & \uparrow & & \\ 0 & \longrightarrow & E^{(1)}(K_\mathfrak{p}) & \longrightarrow & E(K_\mathfrak{p}) & \xrightarrow{\bmod \mathfrak{p}} & (E \bmod \mathfrak{p})(\mathcal{O}/\mathfrak{p}) & \longrightarrow & 0 \end{array}$$

2.4.2. Theorem (Hasse). *Let E be an elliptic curve over a finite field F. Then*

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

(See [Sil86, Theorem V.1.1].)

We will use the following lemma to bound the size of the torsion subgroup of elliptic curves.

2.4.3. Lemma. *Let E be a Weierstrass model over a number field K with good reduction at $\mathfrak{p}$ and suppose that $\nu_\mathfrak{p}(\mathrm{char}(\mathfrak{p})) < \mathrm{char}(\mathfrak{p}) - 1$. Then*

$$E^{\mathrm{tor}}(K) \hookrightarrow (E(K) \bmod \mathfrak{p}) \subset (E \bmod \mathfrak{p})(\mathcal{O}/\mathfrak{p})$$

as groups.

Proof: Since $E(K) \subset E(K_\mathfrak{p})$ and $E^{(1)}(K_\mathfrak{p}) \cong \mathfrak{p}\mathcal{O}_\mathfrak{p}$, and thus free of torsion, we have that $E(K_\mathfrak{p}) \to E(K_\mathfrak{p})/E^{(1)}(K_\mathfrak{p})$ does not kill any torsion. Then the induced map on $E(K)$ is injective on torsion too. □

Chapter 3

Some spherical cases

In this chapter, we discuss an efficient way of determining a set of parametrising curves for some Fermat equations. The method utilises common factors in the exponents and yields a full parametrisation in all spherical cases except $x^2 + y^3 = z^5$. These parametrisations were first calculated by Zagier and published (without proof) in [Beu98].

The first section discusses the underlying principles that also apply to some nonspherical cases. These were first sketched in [DG95]. The second section applies the method to some spherical cases that are of interest to the rest of this thesis.

3.1 Parametrisation of $F(x, y) = Dz^m$

In this section we show how Lemma 2.2.1 leads to an effective and practical way to find the parametrising curves for the S-primitive solutions of a weighted homogeneous equation of the form $F(x, y) = Dz^n$ (where F is a square free homogeneous polynomial of degree $n \geq 2$) over a number field K. First we investigate the underlying geometry of the parametrising curves.

Let K be a number field and let $F(X, Y) \in \mathcal{O}_K[X, Y]$ and $D \in \mathcal{O}_K$. Let S be a set of primes such that $\mathrm{disc}(F(X, 1)), \mathrm{disc}(F(1, Y)), D \in \mathcal{O}_S^*$. The presence of D allows us to assume that F is monic in X. Let L be a splitting field of $F(X, 1)$ over K. We have $\alpha_1, \ldots, \alpha_n \in L$ such that $F(X, Y) = \prod_{i=1}^{n}(X - \alpha_i Y)$. Note that $\sigma \in \mathrm{Gal}(L/K)$ acts as a permutation on the α_i and use this to fix $\mathrm{Gal}(L/K) \hookrightarrow S_n$. We write ${}^{\sigma}\alpha_i = \alpha_{\sigma(i)}$. Suppose that x, y, z is an S-primitive solution in K. Lemma 2.2.1 gives that we have $\delta_1, \ldots, \delta_n \in L(S, m)$ with $(\delta_1 \cdots \delta_n)/D \in (K^*)^m$ and S-primitive $(z_1, \ldots, z_n) \in L^n$ such that

$$\begin{aligned} x - \alpha_i y &= \delta_i z_i^m \\ z &= \sqrt[m]{\tfrac{\delta_1 \cdots \delta_n}{D}}\, z_1 \cdots z_n. \end{aligned}$$

Since $x, y \in K$, we can assume, without loss of generality, that ${}^{\sigma}\delta_i = \delta_{\sigma(i)}$ and ${}^{\sigma}z_i = z_{\sigma(i)}$ for $\sigma \in \mathrm{Gal}(L/K)$. If F is irreducible over K then $\mathrm{Gal}(L/K)$ acts transitively on the α_i, so then δ_1 determines all δ_i. See Lemma 3.1.2 for details.

If we eliminate x and y from these equations, then we see that $(z_1, \ldots, z_n)$ must be a zero of the ideal

$$I_\delta := \{(\alpha_i - \alpha_j)(\delta_k Z_k^m - \delta_l Z_l^m) - (\alpha_k - \alpha_l)(\delta_i Z_i^m - \delta_j Z_j^m)\}_{i,j,k,l}$$

such that its image under $\varphi : (Z_1, \ldots, Z_n) \mapsto \frac{\alpha_j \delta_i Z_i^m - \alpha_i \delta_j Z_j^m}{\delta_i Z_i^m - \delta_j Z_j^m}$ is K-rational (corresponding to x/y), where the definition of φ is independent of the actual choice of i, j because of the relations generating I_δ. Also note that the zero-locus of I_δ does not intersect any $Z_i = Z_j = 0$, since the α_i are distinct.

We claim that the model $\mathcal{C}_\delta$ described by I_δ is a smooth projective model of a curve over L in $\mathbb{P}_{n-1}$. For $n = 2$ we have nothing to prove, since $I_\delta = 0$, so $\mathcal{C}_\delta = \mathbb{P}_1$, which is smooth. Otherwise, we have that, away from $Z_i = Z_k = 0$,

$$d\left(\frac{Z_i}{Z_k}\right) = \frac{(\alpha_k - \alpha_i)\delta_j}{(\alpha_k - \alpha_j)\delta_i} \frac{m Z_j^{m-1}}{m Z_i^{m-1}} d\left(\frac{Z_j}{Z_k}\right),$$

so Z_j/Z_k can be used as a uniformiser there.

Let ζ be a primitive m-th root of unity. The variety $\mathcal{C}_\delta$ has several automorphisms. Consider $\tau_i : \mathbb{P}_{n-1} \mapsto \mathbb{P}_{n-1}$ defined by $Z_i \mapsto \zeta Z_i$. Note that $\tau_n = (\tau_1 \circ \cdots \circ \tau_{n-1})^{-1}$. It is straightforward to check that $\varphi : \mathcal{C}_\delta \to \mathbb{P}_1$ is finite of degree m^{n-1} and Galois with Galois group $\langle \tau_1, \ldots, \tau_n \rangle$.

To conclude that $\mathcal{C}_\delta$ is actually geometrically irreducible, we consider the following argument. Since $\mathcal{C}_\delta$ is smooth, it is a disjoint union of components. Each τ_i has a fixed point, so the component containing that point is mapped to itself by τ_i. Since $\mathcal{C}_\delta$ is a Galois cover of the (connected) projective line, we have that the abelian Galois group $\langle \tau_1, \ldots, \tau_n \rangle$ acts transitively on the set of components of $\mathcal{C}_\delta$. Consequently, the τ_i act as the trivial permutation on the components, so there is only one.

Since ${}^\sigma I_\delta = I_\delta$ and ${}^\sigma \varphi = \varphi$ for $\sigma \in \mathrm{Gal}(L/K)$, we see that both are defined over K, so $\varphi : \mathcal{C}_\delta \to \mathbb{P}_1$ is in fact a model of a cover over K. Furthermore, $\mathcal{C}_\delta$ has good reduction at primes outside $S \cup \{p \mid m\}$.

We can now calculate the genus of $\mathcal{C}_\delta$ using Theorem 2.3.2. Note that $\#\varphi^{-1}(\{a\}) = m^{n-1}$ if $a \notin \{\alpha_1, \ldots, \alpha_n\}$ and $\#\varphi^{-1}(\{\alpha_i\}) = m^{n-2}$. As a consequence, $\sum_{P \in \mathcal{C}(\bar{K})} (e_P(\varphi) - 1) = n m^{n-2}(m-1)$. Since $\mathrm{genus}(\mathbb{P}_1) = 0$ we get

$$\mathrm{genus}(\mathcal{C}_\delta) = 1 + m^{n-2}\left(\tfrac{1}{2} n(m-1) - m\right).$$

Now suppose that x, y, z is an S-primitive K-rational solution to $F(x, y) = Dz^m$ and that $a = x/y$ (if $y = 0$, then a is the point $\infty \in \mathbb{P}_1(K)$). Suppose $P \in \varphi^{-1}(\{a\})$. If $\sigma \in \mathrm{Gal}(\bar{K}/K)$ then ${}^\sigma \varphi(P) = {}^\sigma a = a$. Since ${}^\sigma \varphi = \varphi$, it follows that there is a $\tau_\sigma \in \mathrm{Gal}(\mathcal{C}/\mathbb{P}_1)$ such that ${}^\sigma P = \tau_\sigma(P)$. It is easy to check that $\xi_P : \sigma \mapsto \tau_\sigma$ is a cocycle. By Theorem 2.3.1 there is a curve C_P over K and a degree 1 cover $\psi : \mathcal{C}_P \to \mathcal{C}_\delta$ (not necessarily over K) such that $\xi_P = (\sigma \mapsto {}^\sigma \psi \psi^{-1})$. Since

$${}^\sigma(\psi^{-1}(P)) = {}^\sigma \psi^{-1}(\tau_\sigma(P)) = {}^\sigma \psi^{-1} {}^\sigma \psi \psi^{-1}(P) = \psi^{-1}(P),$$

we see that $\psi^{-1}(P) \in \mathcal{C}_P(K)$. Furthermore, since φ is τ-invariant, $\varphi \circ \psi^{-1} : \mathcal{C}_P \to \mathbb{P}_1$ is a cover over K and $a \in \varphi \circ \psi^{-1}(\mathcal{C}_P(K))$. We see that the $\mathcal{C}_P$ form a parametrising set of curves for the S-primitive solutions. (Note that the $\mathcal{C}_\delta$ themselves are twists of each other). To see that we only need a finite number of $\mathcal{C}_P$, we need that $\mathcal{C}_P$ has again good

reduction outside S and that the number of twists with this property is finite. This follows from [Sil86, Lemma X.4.3]. Alternatively, finiteness follows from Lemma 2.2.1 together with Lemma 3.1.2. Summarising:

3.1.1. Theorem. *Let K, $F(x,y) = Dz^m$ and S be as above. Then there is a finite number of Galois-covers $\varphi_P : \mathcal{C}_P \to \mathbb{P}_1$ over K with $\mathrm{Gal}(\mathcal{C}_P/\mathbb{P}_1) \cong (\mathbb{Z}/m\mathbb{Z})^{n-1}$, where $\mathcal{C}_P$ is of genus $1 + \frac{1}{2}m^{n-2}(n(m-1)-m)$ and has good reduction outside $S \cup \{m\}$ such that*

$$\bigcup_{\mathcal{C}_P} \varphi_P(\mathcal{C}_P(K)) = \left\{(x:y) : F(x,y) = Dz^m \text{ with } x,y,z \in K \text{ and } (x,y,z) \text{ } S\text{-primitive}\right\}.$$

The $\mathcal{C}_P$ are all birationally equivalent over $\bar{K}$ and the φ_P are ramified exactly above the points $(x:y)$ for which $F(x,y) = 0$.

While the model $\mathcal{C}_\delta$ is well suited to analyse the underlying geometry of the problem, it is not very useful for explicitly determining a set of curves. This is partly because the model itself is a priori given over L and that we conclude that $\mathcal{C}_\delta$ is defined over K by Galois invariance. This means that even the question $P \in \mathcal{C}_\delta(K)$ is not easily answered. Furthermore, while by the correspondence proved in Theorem 2.3.1, determining the appropriate twists is effective, it is not a very practical procedure. We can do better.

First, note that if $F = F_1F_2$ with $F_1, F_2 \in \mathcal{O}_K[X,Y]$ then we can apply Lemma 2.2.1 to obtain a finite number of systems of equations over $\mathcal{O}_K$ of the form

$$\begin{cases} F_1(x,y) &= \delta z_1^m \\ F_2(x,y) &= D\delta^{m-1} z_2^m. \end{cases}$$

Therefore, it is enough to deal with the case that F is irreducible over K. Let α be a root of $F(X,1)$ and let $L = K(\alpha)$. Then, applying Lemma 2.2.1 over L we see that for an S-primitive solution x,y,z there exists a $\delta \in L(S,m)$ and $a_0, \ldots, a_{n-1} \in K$ such that

$$\begin{aligned} x - \alpha y &= \delta\left(a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1}\right)^m \\ z &= \sqrt[m]{\tfrac{N_{L/K}(\delta)}{D}}\, N_{L/K}\left(\textstyle\sum_{i=0}^{n-1} a_i\alpha^i\right). \end{aligned}$$

We have unique forms $b_{\delta,i} \in K[X_0, \ldots, X_{n-1}]$, homogeneous of degree m, such that

$$\sum_{i=0}^{n-1} b_{\delta,i}(a_0, \ldots, a_{n-1})\alpha^i = \delta\left(a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1}\right)^m.$$

Consequently, $(x:y) = (b_{\delta,0}(a_0, \ldots, a_{n-1}) : -b_{\delta,1}(a_0, \ldots, a_{n-1}))$ and $b_{\delta,i}(a_0, \ldots, a_{n-1})$ should vanish for $i = 2, \ldots, n-1$. This gives us

3.1.2. Lemma. *Let K, F, D and S be as above. Suppose that F is irreducible over K, that α is a root of $F(X,1)$ and that $L = K(\alpha)$. Suppose that $x,y,z \in K$ are S-primitive and satisfy $F(x,y) = Dz^m$. Then there are $a_0, \ldots, a_{n-1} \in K$ and $\delta \in L(S,m)$ with $N_{L/K}(\delta)/D \in (K^*)^m$ such that for the $b_{\delta,i}$ as defined above, we have*

$$\begin{aligned} (x:y) &= (b_{\delta,0}(a_0, \ldots, a_{n-1}) : -b_{\delta,1}(a_0, \ldots, a_{n-1})) \\ b_{\delta,i}(a_0, \ldots, a_{n-1}) &= 0 \quad \text{for } i = 2, \ldots, n-1. \end{aligned}$$

This shows that for irreducible F, models of the $\mathcal{C}_P$ mentioned in Theorem 3.1.1 are given by ideals of the form

$$I_P = (b_{\delta,2}(X_0, \ldots, X_{n-1}), \ldots, b_{\delta,n-1}(X_0, \ldots, X_{n-1}))$$

for appropriate values of $\delta \in L(S,m)$ and that φ_P takes the form $(b_{\delta,0}(X_0, \ldots, X_{n-1}) : -b_{\delta,1}(X_0, \ldots, X_{n-1}))$. These models have the advantage of being completely explicit, over K, and efficiently computable.

3.2 Solutions

In this section we apply the ideas of the previous section to several spherical equations. Note that, in each case, we are interested in *primitive* solutions x, y, z. Lemma 2.2.1 only tells us something about S-primitive solutions, where S contains some primes related to the equation. The complete primitivity yields congruences on the parameters s, t at the primes in S as well. In general, it is a rather laborious job to determine these. We will only say something about s, t at primes in S if we use this information later on.

3.2.1. Lemma. *Let x, y, z be coprime integers such that $x^2 + y^2 = z^2$. Possibly by interchanging x and y, we can assume that x is divisible by 2. Then there are coprime integers s and t, not both odd, such that*

$$\begin{cases} x &= 2st, \\ y &= s^2 - t^2, \\ \pm z &= s^2 + t^2. \end{cases}$$

Proof: This is a classical result. That x and y are not both odd can be seen mod 4. The polynomials can be obtained by observing that $y^2 = z^2 - x^2 = (z + x)(z - x)$. □

3.2.2. Lemma. *Let x, y, z be coprime integers such that $x^2 + y^2 = z^3$. Then there are coprime integers s, t such that*

$$\begin{cases} x &= s(s^2 - 3t^2), \\ y &= t(t^2 - 3s^2), \\ z &= s^2 + t^2. \end{cases}$$

Proof: This is a direct application of Lemma 3.1.2. Write $i = \sqrt{-1}$ and $L = \mathbb{Q}(i)$. Note that $S = \{2, 3\}$ and $L(S,3) = \langle 1 + i, 3 \rangle$ and that none has a norm that is a third power. That s and t must be integral and coprime, follows from the polynomials. □

To get a taste of the kind of arguments one meets when determining parametrisations in more complicated situations, we give the proof of the following lemma in detail. In other situations, one proceeds in a similar fashion.

3.2.3. Lemma (Zagier). *Let x, y, z be pairwise prime integers such that $x^2 + y^4 = z^3$. Then there are $s, t \in \mathbb{Z}_{\{2,3\}}$ such that one of the relations in Table 3.1 holds.*

$$\begin{array}{rcl}
x & = & 4st(s^2-3t^2)(s^4+6s^2t^2+81t^4)(3s^4+2s^2t^2+3t^4) \\
\pm y & = & (s^2+3t^2)(s^4-18s^2t^2+9t^4) \\
z & = & (s^4-2s^2t^2+9t^4)(s^4+30s^2t^2+9t^4) \\
\pm x & = & (s^4+12t^4)(s^8-408s^4t^4+144t^8) \\
y & = & 6st(s^4-12t^4) \\
z & = & s^8+168s^4t^4+144t^8 \\
\pm x & = & (3s^4+4t^4)(9s^8-408s^4t^4+16t^8) \\
y & = & 6st(3s^4-4t^4) \\
z & = & 9s^8+168s^4t^4+16t^8 \\
\pm x & = & (1/8)(s^4+3t^4)(s^8-102s^4t^4+9t^8) \\
y & = & (3/2)st(s^4-3t^4) \\
z & = & (1/4)(s^8+42s^4t^4+9t^8)
\end{array}$$

Table 3.1: Parametrisations of $x^2+y^4=z^3$

Proof: From Lemma 3.2.2 it follows that there are $s,t\in\mathbb{Z}$ such that y,s,t form a primitive solution to $t(t^2-3s^2)=\pm y^2$. First note that the sign of the left hand side can be controlled by the sign of t. It therefore suffices to look at $t(t^2-3s^2)=y^2$. By Lemma 2.2.1 we have $\delta\in\{1,-1,3,-3\}$ and $y_1,y_2\in\mathbb{Q}$ such that $t=\delta y_1^2$ and $t^2-3s^2=\delta y_2^2$. Modulo $3,9$ we see that only for $\delta=1,-3$ we have solutions. We treat these cases separately. First suppose $\delta=1$. Then $t^2-y_2^2=3s^2$. It follows that for some $\delta\in\{\pm1,\pm2,\pm3,\pm6\}$ (this need not be the δ we have used before), we have $s_1,s_2\in\mathbb{Q}$ such that

$$\begin{array}{rcl}
t & = & y_1^2=\frac{1}{2}\delta(s_1^2+3s_2^2) \\
y_2 & = & \frac{1}{2}\delta(s_1^2-3s_2^2) \\
s & = & \pm\delta s_1s_2
\end{array}$$

It follows that $\delta>0$ and, since 2 is inert in $\mathbb{Q}(\sqrt{-3})$, we have $2\mid\delta$. For $\delta=2$ we get $s_1^2+3s_2^2=y_1^2$ and for $\delta=6$ we get $3s_1^2+(3s_2)^2=y_1^2$. Therefore, by interchanging s_1 and s_2 we see that these cases are equivalent in the sense that both belong to the same parametric family. We restrict to $\delta=2$.

Again, we conclude that there is a $\delta\in\{\pm1,\pm2,\pm3,\pm6\}$ (not necessarily equal to any of the δs we have used before) and $u,v\in\mathbb{Q}$ such that

$$\begin{array}{rcl}
y_1 & = & \frac{1}{2}\delta(u^2+3v^2) \\
s_1 & = & \frac{1}{2}\delta(u^2-3v^2) \\
s_2 & = & \delta uv.
\end{array}$$

If we substitute these expressions back in the forms for s,t and remember that s,t are coprime integers, we see that $2\mid\delta$. Furthermore, the sign of δ only influences the sign of y. We obtain forms for x,y,z that are equivalent to the first parametrisation in Table 3.1 if we let u,v be rational multiples of the s,t in the table.

This leaves the case

$$\begin{aligned} t &= -3y_1^2 \\ t^2 - 3s^2 &= -3y_2^2 \\ \pm y &= 3y_1y_2. \end{aligned}$$

Then we have $\delta \in \{\pm 1, \pm 2, \pm 3, \pm 6\}$ and $t_1, t_2 \in \mathbb{Q}$ such that

$$\begin{aligned} s &= \tfrac{1}{2}\delta(t_1^2 + 3t_2^2), \\ y_2 &= \tfrac{1}{2}\delta(t_1^2 - 3t_2^2), \\ t &= -3y_1^2 = \pm 3\delta t_1 t_2. \end{aligned}$$

From the last equation, we conclude that there is an $\epsilon \in \{\pm 1, \pm 2, \pm 3, \pm 6\}$ and $u, v \in \mathbb{Q}$ such that

$$\begin{aligned} \pm t_1 &= \delta\epsilon u^2, \\ \pm t_2 &= \epsilon v^2. \end{aligned}$$

It follows that $t = \pm 3\epsilon^2\delta^2u^2v^2$ and $s = \frac{1}{2}\epsilon^2(\delta^3u^4 + 3\delta v^4)$. If s, t are to be coprime integers, then $3 \nmid \epsilon, \delta$. Upon inspection, one sees that the signs of ϵ and δ are only going to affect the signs of x, y, z. Furthermore, $\delta = 1, \epsilon = 2$ does not lead to any s, t that are integral and primitive at 2. The case $\delta = \epsilon = 2$ leads (up to rational scaling) to the second parametrisation in Table 3.1 and $\delta = 2, \epsilon = 1$ and $\delta = \epsilon = 1$ lead to the third and fourth parametrisation respectively. This concludes the proof. □

3.2.4. Lemma. *Let $x, y, z \in \mathbb{Z}$ be coprime integers satisfying $x^2 + y^2 = z^5$. Then there exist $s, t \in \mathbb{Z}_{\{2,5\}}$ with $(s, t) \bmod p \neq (0, 0)$ for any $p \nmid 10$ such that*

$$\begin{cases} x &= t(t^4 - 10t^2s^2 + 5t^4) \\ y &= s(s^4 - 10s^2t^2 + 5t^4) \\ z &= s^2 + t^2 \end{cases}$$

Proof: Let $i^2 = -1$. Then $x^2 + y^2 = (x + iy)(x - iy)$. Since x and y are coprime, we have $(x + iy, x - iy) \mid 2$. Consequently, $x + iy = \delta(s + it)^5$, where δ is some fifth power free 2-unit in $\mathbb{Z}[i]$ such that $N(\delta)$ is a fifth power. Since there $2 = -i(1 + i)^2$, it follows that δ is a unit. Since every unit in $\mathbb{Z}[i]$ is a fifth power, we can assume that $\delta = 1$. This is an application of Lemma 3.1.2 again. □

3.2.5. Lemma. *Let $x, y, z \in \mathbb{Z}$ be coprime integers satisfying $x^2 - y^2 = z^5$. Then there exist $s, t \in \mathbb{Z}_{\{2,5\}}$ with $(s, t) \neq (0, 0) \bmod p$ for any prime $p \nmid 10$ such that*

$$\begin{cases} \pm x &= \frac{1}{2}(s^5 + t^5) \\ y &= \frac{1}{2}(s^5 - t^5) \\ \pm z &= st \end{cases} \quad or \quad \begin{cases} \pm x &= s^5 + 8t^5 \\ y &= s^5 - 8t^5 \\ \pm z &= 2st \end{cases}$$

Proof: By factorisation, it follows that there are $s, t \in \mathbb{Z}_{\{2,5\}}$ and a fifth power free $\delta \in \mathbb{Z}$ such that, neglecting the sign of y, $x + y = \delta s^5$ and $x - y = \delta^4 t^5$. Since x and y are coprime, we can take $\delta \mid 2$. Note that $(\delta, s, t) \mapsto (-\delta, -s, t)$ corresponds to $(x, y, z) \mapsto (x, y, -z)$.

$$
\begin{aligned}
\pm x &= (s^2 - 3\,t^2)(s^4 + 18\,t^2s^2 + 9\,t^4)\\
y &= -(s^2 + 2\,ts + 3\,t^2)(s^2 - 2\,ts + 3\,t^2)(s^2 + 6\,ts + 3\,t^2)(s^2 - 6\,ts + 3\,t^2)\\
\pm z &= 4\,st(s^2 + 3\,t^2)(3\,s^4 - 2\,t^2s^2 + 3\,t^4)(s^4 - 6\,t^2s^2 + 81\,t^4)
\end{aligned}
$$

$$
\begin{aligned}
\pm x &= 6\,st(s^4 + 12\,t^4)\\
y &= (s^4 - 12\,t^2s^2 - 12\,t^4)(s^4 + 12\,t^2s^2 - 12\,t^4)\\
\pm z &= (s^4 - 12\,t^4)(s^8 + 408\,t^4s^4 + 144\,t^8)
\end{aligned}
$$

$$
\begin{aligned}
\pm x &= 6\,st(3\,s^4 + 4\,t^4)\\
y &= (3\,s^4 + 12\,t^2s^2 - 4\,t^4)(3\,s^4 - 12\,t^2s^2 - 4\,t^4)\\
\pm z &= (3\,s^4 - 4\,t^4)(9\,s^8 + 408\,t^4s^4 + 16\,t^8)
\end{aligned}
$$

$$
\begin{aligned}
\pm x &= s^6 + 40\,t^3s^3 - 32\,t^6\\
y &= -8\,ts(s^3 - 16\,t^3)(s^3 + 2\,t^3)\\
\pm z &= (s^6 + 32\,t^6)(s^6 - 176\,t^3s^3 - 32\,t^6)
\end{aligned}
$$

$$
\begin{aligned}
\pm x &= s^6 + 6\,s^5t - 15\,s^4t^2 + 20\,t^3s^3 + 15\,s^2t^4 + 30\,st^5 - 17\,t^6\\
y &= 2\,(s^4 - 4\,ts^3 - 6\,t^2s^2 + 4\,t^3s - 7\,t^4)(s^4 + 6\,t^2s^2 - 8\,t^3s - 3\,t^4)\\
\pm z &= 3\,s^{12} - 12\,ts^{11} + 66\,t^2s^{10} + 44\,t^3s^9 - 99\,t^4s^8 - 792\,t^5s^7 + 924\,t^6s^6\\
&\quad -2376\,t^7s^5 + 1485\,t^8s^4 + 1188\,t^9s^3 - 2046\,t^{10}s^2 + 156\,t^{11}s - 397\,t^{12}
\end{aligned}
$$

$$
\begin{aligned}
\pm x &= 9\,s^6 - 18\,ts^5 + 45\,t^2s^4 - 60\,t^3s^3 + 15\,t^4s^2 + 6\,t^5s - 5\,t^6\\
y &= -2\,(3\,s^4 - 6\,t^2s^2 + 8\,t^3s - t^4)(3\,s^4 - 12\,ts^3 + 6\,t^2s^2 - 4\,t^3s + 3\,t^4)\\
\pm z &= 27\,s^{12} + 324\,ts^{11} - 1782\,t^2s^{10} + 3564\,t^3s^9 - 3267\,t^4s^8 + 2376\,t^5s^7 - 2772\,t^6s^6\\
&\quad +3960\,t^7s^5 - 4059\,t^8s^4 + 2420\,t^9s^3 - 726\,t^{10}s^2 + 156\,t^{11}s - 29\,t^{12}
\end{aligned}
$$

Table 3.2: Parametrisations of $x^4 + y^3 = z^2$

So, if we neglect the sign of z, we can assume that δ is positive. Taking $\delta = 1, 2$ gives the relations mentioned above. The map $(s,t) \mapsto (-s,-t)$ induces $(x,y,z) \mapsto (-x,-y,z)$, so the mentioned relations also take into account the sign of y. □

We do not use the following lemma in the rest of this thesis, but for completeness we do include it here. Since the proof is along the same lines as the lemmas above, we do not give it here.

3.2.6. Lemma (Zagier). *Let $x, y, z \in \mathbb{Z}$ be coprime integers satisfying $x^3 + y^3 = z^2$. Then there exist $s, t \in \mathbb{Z}_{\{2,3\}}$ with $(s,t) \neq (0,0) \bmod p$ for any prime $p \nmid 6$ such that one of the following holds:*

$$
\begin{cases}
x \text{ or } y &= s^4 + 6s^2t^2 - 3t^4\\
y \text{ or } x &= -s^4 + 6s^2t^2 + 3t^4\\
z &= 6st(s^4 + 3t^4)
\end{cases}
\qquad
\begin{cases}
x \text{ or } y &= \tfrac{1}{4}(s^4 + 6s^2t^2 - 3t^4)\\
y \text{ or } x &= \tfrac{1}{4}(-s^4 + 6s^2t^2 + 3t^4)\\
z &= \tfrac{3}{4}st(s^4 + 3t^4)
\end{cases}
\qquad
\begin{cases}
x \text{ or } y &= s(s^3 + 8t^3)\\
y \text{ or } x &= 4t(t^3 - s^3)\\
\pm z &= s^6 - 20s^3t^3 - 8t^6
\end{cases}
$$

3.2.7. Lemma (Zagier). *Suppose x, y, z are coprime integers such that $x^4 + y^3 = z^2$. Then there are $s, t \in \mathbb{Z}_{\{2,3\}}$ such that one of the relations in Table 3.2 holds.*

(Completely analogous to Lemma 3.2.3 but, as can be seen from the table, a little more work.)

Chapter 4

Some hyperbolic cases

In this chapter we determine all primitive solutions to the hyperbolic generalised Fermat equations $x^2 \pm y^4 = \pm z^6$, $x^2 \pm y^8 = z^3$ and $x^2 \pm y^4 = z^5$. First we solve some cases that can be done using relatively elementary techniques. Then we develop some more general techniques and apply them to the remaining equations.

4.1 The equations $x^2 \pm y^4 = \pm z^6$

This section is part of [Bru97]. We solve the generalised Fermat equations with exponents 2, 4 and 6. These form very good examples for the more general methods that will be discussed in the next section because, as it turns out, the fundamental ideas can be applied to elliptic curves over $\mathbb{Q}$.

The strategy pursued is the following. First we observe that we have $x^2+(y^2)^2 = (\pm z^2)^3$ and thus that y^2 and z^2 satisfy relations given by Lemma 3.2.2, or that $x^2 \pm (y^2)^2 = \pm(z^3)^2$, so that y^2 and z^3 satisfy relations given by Lemma 3.2.1. In each case we obtain a finite number of Diophantine equations over $\mathbb{Q}$ in U, V, W of the form

$$DV^2 = U^6 + c_1 W^6 \text{ or } DV^2 = (U^2 + c_1 W^2)(U^4 + c_2 U^2 W^2 + c_3 W^4).$$

In both cases, we have that $(X, Y) = (U^2/W^2, V/W^3)$ gives an equation of the form $DY^2 = X^3 + a_2 X^2 + a_4 X + a_6$. This equation describes an elliptic curve, the rational points of which form an abelian group. If this group is finite, then there are only finitely many candidates for values of (X, Y) and thus for $(U : V : W)$.

For the second form, we can apply Lemma 2.2.1 to get a finite number of equations

$$U^2 + c_1 W^2 = D\delta V_1^2, \quad U^4 + c_2 U^2 W^2 + c_3 W^4 = \delta V_2^2.$$

If, for some value of δ, one of these equations has no solutions over $\mathbb{Q}_p$, then we will not get any solutions from that δ. Otherwise, we can try to find a rational solution to the second equation. By writing $X = U/W, Y = V_2/W^2$ we get $\delta Y^2 = X^4 + c_2 X^2 + c_3$. This describes a curve of genus 1 over $\mathbb{Q}$. If we have a rational point on that curve, we can use that point to make the curve into an elliptic curve. Again if the group of rational points on such a curve is finite, then only finitely many solutions to the original equation come from that curve. We have to consider all relevant values of δ, however.

In both constructions we start out with a curve given by a polynomial equation of the form $\mathcal{C} : D(V/W^3)^2 = F(U/W)$ of genus 2, the rational points of which give solutions to the Diophantine equation under consideration. The first construction realises a cover over $\mathbb{Q}$ from $\mathcal{C}$ to an elliptic curve E. Rational points of $\mathcal{C}$ necessarily map to rational points on E. If $E(\mathbb{Q})$ is finite, then simple enumeration gives us $\mathcal{C}(\mathbb{Q})$. The second construction is a bit more subtle. The geometric interpretation is explained in Section 5.2. This interpretation is not essential for applying the method.

4.1.1. Theorem. *If $x, y, z \in \mathbb{Z}$ are coprime such that $x^2 + y^4 = z^6$, then $xyz = 0$.*

Proof: Suppose we have a primitive solution x, y, z. Then, by applying Lemma 3.2.2 to $x^2 + (y^2)^2 = (z^2)^3$, we have coprime $a, b \in \mathbb{Z}$ such that

$$x = b(3a^2 - b^2) \tag{4.1}$$
$$y^2 = a(a^2 - 3b^2) \tag{4.2}$$
$$z^2 = a^2 + b^2. \tag{4.3}$$

Equation (4.3) implies that either $a = s^2 - t^2, b = 2st$ or $a = 2st, b = s^2 - t^2$. We treat each of the possibilities separately.

The case $a = s^2 - t^2, b = 2st$: By substitution in Equation (4.2), we get

$$y^2 = (s^2 - t^2)(s^4 - 14s^2t^2 + t^4).$$

Note that $t = 0$ implies that $b = 0$ and thus $x = 0$. We can therefore safely put $Y = y/t^3, X = s^2/t^2$. Solutions with $x \neq 0$ correspond to affine rational points on the elliptic curve

$$Y^2 = (X - 1)(X^2 - 14X + 1).$$

Using GP/Pari or Apecs, one can calculate the minimal model and the conductor of this curve. From this, we see that it is isomorphic to 144A2 from Cremona's tables [Cre92]. These tables show that this curve has only one affine rational point, namely $(1, 0)$. This corresponds to solutions with $y = 0$.

The case $a = 2st, b = s^2 - t^2$: Put $s - t = u, s + t = v$. This gives $a = (v^2 - u^2)/2, b = uv$. Substitution in Equation (4.2) yields

$$8y^2 = (v^2 - u^2)(v^4 - 14v^2u^2 + u^4).$$

Note that $u = 0$ implies that $b = 0$ and thus $x = 0$. By putting $Y = y/u^3$, $X = v^2/u^2$, other solutions correspond to affine rational points on the elliptic curve

$$8Y^2 = (X - 1)(X^2 - 14X + 1).$$

This curve is isomorphic to 576A2 in [Cre92] and has only one affine rational point, namely $(1, 0)$. This corresponds to solutions with $y = 0$. □

4.1.2. Theorem. *If $x, y, z \in \mathbb{Z}$ are coprime such that $x^2 = z^6 + y^4$, then $xyz = 0$.*

Proof: Suppose we have a primitive solution x, y, z. Then Lemma 3.2.1 states that there exist coprime s, t of distinct parity such that $y^2 = 2st, z^3 = s^2 - t^2$ or $y^2 = s^2 - t^2, z^3 = 2st$. We treat these cases separately.

The case $y^2 = 2st, z^3 = (s+t)(s-t)$: Since $\gcd(y, x) = 1$ and $s + t$ and $s - t$ are both odd, we have that $s + t$ and $s - t$ are coprime. Therefore, there exist $u, v \in \mathbb{Z}$ such that $u^3 = s - t$, $v^3 = s + t$. Rewriting y^2 in u, v gives

$$2y^2 = v^6 - u^6.$$

Note that $u = 0$ implies that $s = t$ and thus $z = 0$. Other solutions correspond to the affine rational points on the elliptic curve curve $2Y^2 = X^3 - 1$, which is isomorphic to 576E1 and has just (1,0) as affine rational point.

The case $y^2 = s^2 - t^2, z^3 = 2st$: Since y is odd, we have $y^2 = 1 \bmod 4$. Therefore, s is odd. From $z^3 = 2st$ we then conclude that $s = v^3, t = 4u^3$. Rewriting y^2 in u, v gives

$$y^2 = v^6 - 16u^6.$$

Note that $u = 0$ implies $t = 0$ and thus $z = 0$. Other solutions correspond to affine rational points on the elliptic curve $Y^2 = X^3 - 16$, which is 432A1 in [Cre92]. The curve has no affine rational points at all. □

4.1.3. Theorem. *If $x, y, z \in \mathbb{Z}$ are coprime such that $x^2 + z^6 = y^4$, then $xyz = 0$.*

Proof: Suppose we have a primitive solution x, y, z. If $z \neq 0$ then $y^4 - x^2 > 0$. Therefore, both $y^2 - x > 0$ and $y^2 + x > 0$. Since x and y are coprime, $\gcd(y^2 - x, y^2 + x) \mid 2$. Possibly after change of sign of x we have $y^2 - x = 2u^6, y^2 + x = 2^5 v^6$ or $y^2 - x = u^6, y^2 + x = v^6$. We treat these cases separately.

The case $y^2 - x = 2u^6, y^2 + x = 2^5 v^6$: Eliminating x gives

$$y^2 = u^6 + 16v^6.$$

Note that $v = 0$ implies that $z = 0$. Other solutions correspond to affine rational points on the elliptic curve $Y^2 = X^3 + 16$, which is isomorphic to 27A3 and has only the two affine rational points $(0, 4), (0, -4)$. The corresponding solutions have $u = z = 0$.

The case $y^2 - x = u^6, y^2 + x = v^6$: It follows that u and v are odd and coprime. Eliminating x gives $2y^2 = u^6 + v^6$. Proceeding as before does not work, as the elliptic curve $2Y^2 = X^3 + 1$ has infinitely many rational points. However, we remark that, by Lemma 2.2.1,

$$2y^2 = (u^2 + v^2)(u^4 - u^2v^2 + v^4)$$

implies that

$$\begin{aligned} u^2 + v^2 &= \alpha\, y_1^2, \\ u^4 - u^2v^2 + v^4 &= \beta\, y_2^2, \end{aligned}$$

where $\alpha\beta = 2y_0^2$ and α, β consist only of factors 2 and 3. Positivity shows that $\alpha, \beta > 0$ and modulo 3 we see that $3 \nmid \alpha$. Furthermore, the parity of u and v implies that $u^4 - u^2v^2 + v^4$ is odd. Therefore we have

$$u^2 + v^2 = 2y_1^2 \tag{4.4}$$
$$u^4 - u^2v^2 + v^4 = y_2^2 \tag{4.5}$$

Solutions of (4.5) correspond to rational points on the genus 1 curve $Y^2 = X^4 - X^2 + 1$, which is birational to 27A1 which has 8 rational points. These are $\{\infty^+, \infty^-, (0, \pm 1), (\pm 1, \pm 1)\}$ on our model. The points at infinity and $(0, \pm 1)$ correspond to solutions with $v = 0$ and $u = 0$ respectively. Equation (4.4) has no solution for those points. Solutions corresponding to $(\pm 1, \pm 1)$ have $u^6 = v^6$, which implies that $x = 0$. □

Proof of Theorem 1.3.1: Collect the results of Theorems 4.1.1, 4.1.2 and 4.1.3.

4.2 Overview of general method

In Section 4.1 we saw that a number of Diophantine equations can be solved by relating the solutions of the equation to the rational points on some elliptic curves of rank 0. For the other equations we treat in this thesis, these techniques do not apply. Either such elliptic curves do not exist or they are of positive rank.

In Sections 4.3 through 4.5 we develop the machinery to treat such more general cases. In Section 4.3 we consider an elliptic curve E over a number field K with a non-zero 2-torsion point defined over K. We describe a method of bounding $\#E(K)/2E(K)$, which in turn gives a bound on the rank of $E(K)$. This gives us the tools to get enough information about the Mordell-Weil group of E over K in the cases that we are interested in. At the end, we include a worked example to show how the method works in practice.

For $x^2 \pm y^4 = \pm z^6$, we could find elliptic curves over $\mathbb{Q}$ such that solutions to the equation correspond to rational points on the curves. In the more general cases, we find that solutions to the equation under consideration correspond to K-rational points G of some elliptic cover $\varphi : E \to \mathbb{P}_1$ over a number field K such that $\varphi(G) \in \mathbb{P}_1(\mathbb{Q})$. As it turns out, in each case we can get φ to be of degree 2. In Section 4.4 we investigate the structure of degree 2 elliptic covers of the projective line.

In Section 4.5 we put everything together to find a way of bounding $\varphi(E(K)) \cap \mathbb{P}_1(\mathbb{Q})$. First we use Section 4.3 to get an adequate description of $E(K)$. Then Section 4.4 gives us the structure of $\varphi : E \to \mathbb{P}_1$. An adaptation of Chabauty's technique (see for instance [Fly97]) for bounding the number of rational points on a curve of genus ≥ 2 gives the required results. A necessary condition for the method to work is that $\mathrm{rk}(E(K)) < [K : \mathbb{Q}]$. At the end we include a worked example to show how the method works in practice.

4.3 Descent on elliptic curves using 2-isogeny

In Section 4.1 we saw that knowledge of the structure of the set of rational points on an elliptic curve helps to solve some Diophantine equations. In the sequel, we meet elliptic curves E over number fields K. We will need the group structure of $E(K)$. As was pointed out in Theorem 2.4.1, $E(K)$ consists of a free part and a torsion part. Lemma 2.4.3 helps to bound $E^{\mathrm{tor}}(K)$. In this section, we discuss a method of bounding $\#E(K)/2E(K)$ for curves of a certain type. This gives a (hopefully sharp) bound on $\mathrm{rk}(E(K))$. This section basically describes [Sil86, Theorem X.4.9]. At some places, we use a somewhat different notation (for instance, we deal with twisted Weierstrass forms) and we discuss some enhancements which might help carrying out the procedure over number fields other than $\mathbb{Q}$.

Let K be a number field and consider an elliptic curve over K of the form

$$E : \gamma Y^2 = X^3 + AX^2 + BX.$$

Such a curve has a non-trivial 2-torsion point $T = (0,0)$. Dividing out the subgroup $\{O, T\}$ gives an isogeny of degree 2 to

$$E' : \gamma Y^2 = X^3 - 2AX^2 + (A^2 - 4B)X$$

given by

$$\begin{array}{rccc} \psi : & E & \to & E' \\ & (X,Y) & \mapsto & (\gamma\frac{Y^2}{X^2}, \frac{Y(B-X^2)}{X^2}) \end{array}$$

Analogously, there is an isogeny

$$\begin{array}{rccc} \psi' : & E' & \to & E \\ & (X,Y) & \mapsto & (\gamma\frac{Y^2}{4X^2}, \frac{Y(A^2-4B-X^2)}{8X^2}) \end{array}$$

We assume that γ, A, B are in $\mathcal{O}_K$. Let S be the set of primes dividing $2\gamma\,(A^2 - 4B)$ together with the infinite primes. The models E and E' have (possibly) bad reduction at the primes in S. Given some field $L \supset K$ (for instance a localisation of K), it is easy to check that the map

$$\begin{array}{rccccc} \mu_L^{(\psi')} : & E(L)/\psi'(E'(L)) & \to & L^*/(L^*)^2 & & \\ & (x,y) & \mapsto & \gamma x & & (x \neq 0, \infty) \\ & (0,0) & \mapsto & B & & \\ & \infty & \mapsto & 1 & & \end{array}$$

is an injective group homomorphism. We define $\mu_L^{(\psi)}$ analogously. For $L = K$, it is straightforward to check that $\mu_K^{(\psi')}(E(K)) \subset K(S,2)$. Note that a class represented by δ is in the image of $\mu_L^{(\psi')}$ if and only if

$$H_\delta : V^2 = \gamma^2\delta^3U^4 + \gamma\delta^2AU^2 + \delta B$$

has a point $(u, v) \in H_\delta(L)$. A corresponding point on $E(L)$ is $(\gamma\delta u^2, uv)$ for $u \neq 0, \infty$. Note that H_1 and H_B indeed contain points with $u = \infty$ and $u = 0$, respectively.

For every prime $\mathfrak{p}$ of K, we have the commutative diagram

$$\begin{array}{ccc} E(K)/\psi'(E'(K)) & \xrightarrow{\mu_K^{(\psi')}} & K(S,2) \\ \downarrow & & \downarrow \\ E(K_\mathfrak{p})/\psi'(E'(K_\mathfrak{p})) & \xrightarrow{\mu_{K_\mathfrak{p}}^{(\psi')}} & K_\mathfrak{p}^*/(K_\mathfrak{p}^*)^2 \end{array}$$

Consequently, if $H_\delta(K)$ is non-empty, then $H_\delta(K_\mathfrak{p})$ is non-empty for all primes $\mathfrak{p}$ of K. The set of δ for which H_δ has points everywhere locally, is called the *Selmer-group* of ψ',

$$S^{(\psi')}(E/K) := \left\{\delta \in K(S,2) \ : \ \delta \in \mu_{K_\mathfrak{p}}^{(\psi')}(E(K_\mathfrak{p})) \text{ for all } \mathfrak{p} \text{ of } \mathcal{O}_K\right\}.$$

This set contains the image of $E(K)/\psi'(E'(K))$ and we hope it is isomorphic to it.

Since H_δ will certainly have points locally at primes not in S, we can calculate $S^{(\psi')}$ by enumerating all δ and see if $H_\delta(K_\mathfrak{p})$ is non-empty for all $\mathfrak{p} \mid S$ (and for the real places of K). This method generally works well, but especially when working over a large degree extension of $\mathbb{Q}$, it is reassuring to have some certificate for the obtained bound. We can do so by taking the intersections of the pullbacks of $\mu_{K_\mathfrak{p}}^{(\psi')}(E(K_\mathfrak{p}))$ under $K(S,2) \to K_\mathfrak{p}^*/(K_\mathfrak{p}^*)^2$ for $\mathfrak{p} \in S$ and $\mathfrak{p} \mid \infty$, since, as it turns out, we can calculate $\#(E(K_\mathfrak{p})/\psi'(E'(K_\mathfrak{p})))\#(E'(K_\mathfrak{p})/\psi(E(K_\mathfrak{p})))$ beforehand.

Since the multiplication-by-2 on E factors as $\psi' \circ \psi$, we have Diagram 4.1 with exact rows and columns. For brevity, the designators (L) are left out. The diagram holds for the L-valued points for any field $L \supset K$. We see that

$$\#E(L)/2E(L) = \frac{\#E'(L)/\psi(E(L))\#E(L)/\psi'(E'(L))}{4/\#E[2](L)}. \tag{4.6}$$

Note that ψ is of degree 2, so $E[\psi](L) = \{(0,0), \infty\}$ regardless of L. Since $E(K_\mathfrak{p})$ is a Lie-group of dimension 1 over $K_\mathfrak{p}$ we have that, locally, the multiplication-by-2 map multiplies the Haar-measure with $|2|_\mathfrak{p}$ and, consequently,

$$\#E(K_\mathfrak{p})/2E(K_\mathfrak{p}) = \#E[2](K_\mathfrak{p})/|2|_\mathfrak{p}.$$

See [FPS97, page 451] for more information or [CF96, Chapter 7,§5, §6] for a more algebraic argument. These two formulas give the cardinalities of the images of $\mu_{K_\mathfrak{p}}^{(\psi)}$ and $\mu_{K_\mathfrak{p}}^{(\psi')}$. We get

$$\#E'(K_\mathfrak{p})/\psi(E(K_\mathfrak{p}))\#E(K_\mathfrak{p})/\psi'(E'(K_\mathfrak{p})) = 4/|2|_\mathfrak{p}.$$

With this, we can give a list of $\mathfrak{p}$-adic points on $E(K_\mathfrak{p})$ that provably generate $E(K_\mathfrak{p})/\psi'(E'(K_\mathfrak{p}))$. These determine a subspace of the $\mathbb{F}_2$-vector space $K(S,2)$ containing $\mu_K^{(\psi')}(E(K)/\psi'(E'(K)))$. The intersection of several such subspaces gives a (hopefully sharp) bound on $\#E(K)/\psi'(E(K))$.

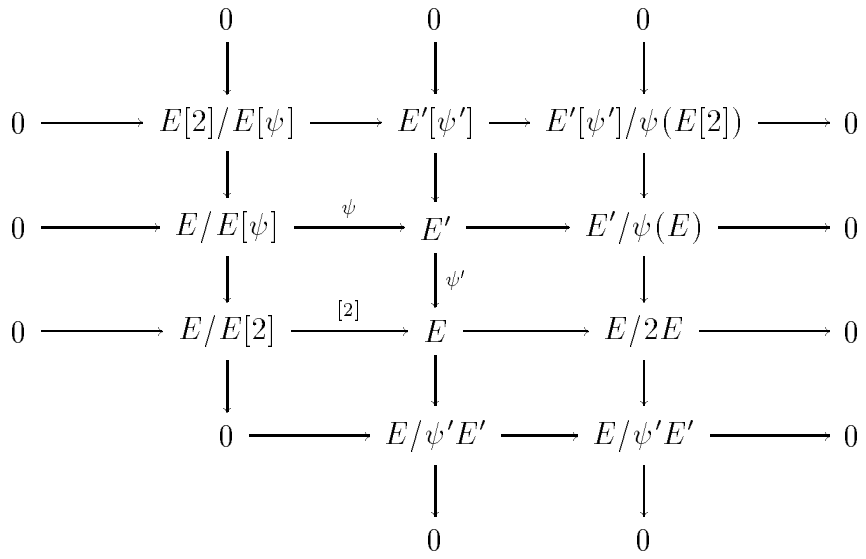


Diagram 4.1: The 2-isogeny for elliptic curves

Combining (4.6) with the fact that if r is the rank of the free part of $E(K)$, then

$$\#E(K)/2E(K) = 2^r \#E[2](K),$$

we get the (hopefully sharp) bound

$$2^r \leq \tfrac{1}{4}\#S^{(\psi')}(E/K)\#S^{(\psi)}(E'/K).$$

Now, if we have a subgroup $\langle G_1, \ldots, G_{r_1}\rangle \subset E(K)$ that maps onto $\mu_K^{(\psi')}(E(K)/\psi'(E(K)))$ and $\langle G'_1, \ldots, G'_{r_2}\rangle \subset E'(K)$ has the same property, then

$$\langle G_1, \ldots, G_{r_1}, \psi'(G'_1), \ldots, \psi'(G'_{r_2})\rangle \subset E(K)$$

is of odd index. To prove divisibility properties with respect to other primes, the following lemma is useful. We remind the reader of the definition $Z := X/Y$ in Section 2.4.

4.3.1. Lemma. *Let E be an elliptic curve over a number field L and let $p \in \mathbb{Z}$ be a prime > 2, unramified in $\mathcal{O}_L/\mathbb{Z}$, such that E has good reduction at $\mathfrak{p}_i \mid p$ and $\#(E \bmod \mathfrak{p}_i)(\mathcal{O}/\mathfrak{p}_i)$ is prime to p for $i = 1, \ldots, m$. Let $B_1, \ldots, B_r \in E(L)$ with $B_j = 0 \bmod \mathfrak{p}_i$ such that $\langle B_1, \ldots, B_r\rangle$ in $E(L)$ is of finite index divisible by p, then there are $n_1, \ldots, n_r \in \mathbb{Z}_p$ with $(n_1, \ldots, n_r) \neq (0, \ldots, 0) \bmod p$ such that $n_1 Z(B_1) + \cdots + n_r Z(B_r) = 0 \bmod \mathfrak{p}_i^2$ for $i = 1, \ldots, m$.*

Proof: The conditions in the lemma imply that there exists a $G \in E(L)$ and $n_1, \ldots, n_r \in \mathbb{Z}$, not all divisible by p, such that $n_1 B_1 + \cdots + n_r B_r = pG$. Let $i \in \{1, \ldots, m\}$. Note that $pG \in E(L) \cap E^{(1)}(L_{\mathfrak{p}_i})$. Since the reduction group has order prime to p, we have that $G = 0 \bmod \mathfrak{p}_i$. By the good reduction properties, we have $n_1 \mathrm{Log}_{\mathfrak{p}_i}(B_1) + \cdots +$

$n_r \mathrm{Log}_{\mathfrak{p}_i}(B_r) = p\mathrm{Log}_{\mathfrak{p}_i}(G)$. The statement follows by observing that $Z = \mathrm{Log}_{\mathfrak{p}_i} \bmod \mathfrak{p}_i^2$ and that $Z(E^{(1)}(L_{\mathfrak{p}_i})) = 0 \bmod \mathfrak{p}_i$. □

As an example, we prove the following lemma (which is chosen such that we can use the result later on in Section 4.6).

4.3.2. Lemma. *Let* $\alpha = \sqrt{3}$, $K = \mathbb{Q}(\alpha)$ *and*

$$E : 2Y^2 = X^3 - 2\alpha X.$$

Then $E^{\mathrm{tor}}(K) = \{\infty, G_2 := (0,0)\}$ *and* $\langle G_1 := (2, \alpha - 1), G_2\rangle$ *is a subgroup of* $E(K)$ *of odd index prime to* 23. *Let* $\mathfrak{p}, \mathfrak{q} \mid 23$ *such that* $\alpha \bmod \mathfrak{p} = 7$ *and* $\alpha \bmod \mathfrak{q} = -7$. *Then* $\langle G_1, G_2\rangle \bmod \mathfrak{p}$ *spans* $E(K) \bmod \mathfrak{p}$ *and the same for* $\mathfrak{q}$.

Proof: First, we describe the arithmetic structure of K. We have that $\mathcal{O}_K^* = \langle -1, \eta = 2 + \alpha\rangle$, $2\mathcal{O} = \mathfrak{p}_2^2$ and $3\mathcal{O} = \mathfrak{p}_3^2$, where $\mathfrak{p}_2 = (1+\alpha)\mathcal{O}$ and $\mathfrak{p}_3 = \alpha\mathcal{O}$. The ideal class group of $\mathcal{O}$ is trivial. E has good reduction outside $S = \{2, 3\}$ and $K(S, 2)$ is represented by elements of $\langle -1, \eta, \alpha, 1 + \alpha\rangle$.

We start with bounding $E^{\mathrm{tor}}(K)$. Let $\mathfrak{p}_{13}$ be the prime above 13 such that $\alpha \bmod \mathfrak{p}_{13} = 9$. Counting shows that $\#(E \bmod \mathfrak{p}_{13})(\mathcal{O}/\mathfrak{p}_{13}) = 10$, that $\#(\langle G_1, G_2\rangle \bmod \mathfrak{p}) = 12$ and that $\#(\langle G_1, G_2\rangle \bmod \mathfrak{q}) = 24$. By Theorem 2.4.2 we have $\#(E \bmod \mathfrak{p})(\mathcal{O}/\mathfrak{p}) = \#(E \bmod \mathfrak{q})(\mathcal{O}/\mathfrak{q}) = 24$. Applying Lemma 2.4.3 shows that $\#E_2^{\mathrm{tor}}(L) \mid 10, 24$. Since G_2 is 2-torsion point, we have $E^{\mathrm{tor}}(K)$ as stated in the lemma.

We use a 2-isogeny descent to determine the rank. Note that the size of $K(S, 2)$ gives an a priori bound $\mathrm{rk}(E) \leq 6$, since the Selmer groups are subgroups of $K(S, 2)$.

Let $E' : 2Y^2 = X^3 + 8\alpha X$ be the 2-isogenous curve to E. We have $G_1' = (2 + 2\alpha, 4 + 4\alpha) \in E'(K)$ and $\psi'(G_1') = G_1$. We start with $L = K_{\mathfrak{p}_2}$. Note that $|2|_{\mathfrak{p}_2} = 1/4$, so $\dim_{\mathbb{F}_2} E(L)/\psi'(E'(L)) + \dim_{\mathbb{F}_2} E'(L)/\psi(E(L)) = 4$. Since $K(S, 2) \to L^*/(L^*)^2$ is injective, this already gives $\mathrm{rk}(E) \leq 2$. Apart from G_1' and $(0, 0)$, we have a point with $X = 2 + 4\alpha$ in $E'(L)$. Computation modulo a sufficiently high power of $\mathfrak{p}_2$ shows that they are $\mathbb{F}_2$-independent in $E'(L)/\psi(E(L))$. In $E(L)$ we have G_2, which spans a 1-dimensional space in $E(L)/\psi'(E'(L))$. This shows that we have generators of the image of $\mu_L^{(\psi)}$ and $\mu_L^{(\psi')}$. Pulling back shows that $\mu_K^{(\psi)}(E'(K)) \subset \langle 8\alpha, \alpha - 1, -\alpha\rangle \subset K(S, 2)$ and $\mu_K^{(\psi')}(E(K)) \subset \langle -2\alpha\rangle \subset K(S, 2)$.

We combine this information with information at $L = K_{\mathfrak{p}_3}$. Here we have that $(0, 0)$ spans a 1-dimensional space in $E(L)/\psi'(E'(L))$ and $E'(L)/\psi(E(L))$ and by $|2|_{\mathfrak{p}_3} = 1$, it spans the whole space in both cases. Since $\alpha - 1$ is a non-square unit in $\mathcal{O}_{\mathfrak{p}_3}$, we see that $\alpha - 1 \notin S^{(\psi)}(E'/K)$. Consequently, $\mathrm{rk}(E(K)) < 2$ and G_1, G_2 span a subgroup of odd index.

From Hasse, we know that $15 \leq \#(E \bmod \mathfrak{p})(\mathcal{O}/\mathfrak{p}), \#(E \bmod \mathfrak{q})(\mathcal{O}/\mathfrak{q}) \leq 33$. Consequently, the subgroup generated by $\langle G_1, G_2\rangle \bmod \mathfrak{p}$ has index ≤ 2 in $E(L) \bmod \mathfrak{p}$ and $\langle G_1, G_2\rangle \bmod \mathfrak{q}$ index 1 in $E(L) \bmod \mathfrak{q}$. Since this index divides the odd number $[E(L) : \langle G_1, G_2\rangle]$, it follows that it is 1 in both cases.

To see that $\langle G_1, G_2\rangle$ is of index prime to 23, we prove that $\langle 12G_1\rangle$ has the same property. This follows from applying Lemma 4.3.1 using that $Z(12G_1) = 23 \cdot 21 \bmod \mathfrak{p}$ and $Z(12G_1) = 23 \cdot 16 \bmod \mathfrak{q}$. □

4.4 Elliptic covers of degree 2

Let E be an elliptic curve over a number field L. In this section we determine what degree 2 covers $\varphi : E \to \mathbb{P}_1$ look like. Suppose that E is a twisted Weierstrass model over the ring of integers $\mathcal{O}_L$ of a number field L.

$$E : \gamma Y^2 D = X^3 + a_2 X^2 D + a_4 X D^2 + a_6 D^3$$

Suppose that φ is a degree 2 cover $E \to \mathbb{P}_1$ over L. Then we can choose a model $(\varphi_1(X,Y,D) : \varphi_2(X,Y,D))$, with $\varphi_1, \varphi_2 \in \mathcal{O}_L[X,Y,D]$ homogeneous polynomials of equal degree. By choosing affine coordinates on $\mathbb{P}_1$, we write $\varphi = \varphi_1/\varphi_2$. Since $\deg(\varphi) = 2$, there are at most two points $G_1, G_2 \in E(\bar{L})$ such that $\varphi(G_1) = \varphi(G_2) = 0$. These two points determine the intersection of $\varphi_1(X,Y,D) = 0$ with E in $\mathbb{P}_2$. If $G_1 = G_2$, then $\varphi_1(X,Y,D) = 0$ should be tangent to E in G_1. Along the same lines, there are two points G_3, G_4 with $\varphi(G_3) = \varphi(G_4) = \infty$. Up to scalar multiplication, φ is determined by the lines through G_1 and G_2 and through G_3 and G_4. We can assume $\varphi_1 = c_{11}X + c_{12}Y + c_{13}D$ and $\varphi_2 = c_{21}X + c_{22}Y + c_{23}D$, with $c_{ij} \in \mathcal{O}_L$. Note that $\varphi_1(X,Y,D) = 0$ has 3 points of intersection with E and so has $\varphi_2(X,Y,D) = 0$. For φ to have degree 2, we must have that the unique point G_φ with $\varphi_1(G_\varphi) = \varphi_2(G_\varphi) = 0$ lies on E. If we define

$$\begin{aligned} G_{\varphi,1} &= c_{12}c_{23} - c_{13}c_{22} \\ G_{\varphi,2} &= c_{13}c_{21} - c_{11}c_{23} \\ G_{\varphi,3} &= c_{11}c_{22} - c_{12}c_{21} \end{aligned}$$

then we have $G_\varphi = (G_{\varphi,1} : G_{\varphi,2} : G_{\varphi,3})$. The map $\tau = \tau_\varphi : E \to E$ that interchanges the elements of the fibres of φ is an *involution*, i.e. $\tau \in \mathrm{Aut}(\mathcal{E})$ (where $\mathcal{E}$ is the algebraic curve corresponding to E) and $\tau \circ \tau = \mathrm{id}$. From [Sil86, Corollary III.10.2] we know that $\mathrm{Aut}(E)[2] = \{[1], [-1]\}$ and from [Sil86, Example III.4.7] that an automorphism of E as a curve is the composition of an automorphism of E as an elliptic curve with a translation. Translations over 2-torsion points are involutions, but they give unramified covers (see Section 4.3). Thus, there is a $G_\tau \in E(\bar{L})$ such that $\tau(G) = G_\tau - G$. Note that $G_2 = \tau(G_1) = G_\tau - G_1$. Therefore G_1, G_2 and $-G_\tau$ are collinear. Note however that G_φ is collinear with G_1 and G_2 as well. It follows that $G_\tau = -G_\varphi$ and thus that τ is defined over L. We will either assume that $G_\tau \neq G_\varphi$ or that $G_\tau = G_\varphi = \infty$. If $G_\varphi = G_\tau$, then we can take $G_\varphi = \infty$ by choosing the distinguished point on the algebraic curve corresponding to E.

We now derive some expressions that allow us to calculate $\mathfrak{p}$-adic approximations to φ. Let $\mathfrak{p}$ be a prime of $\mathcal{O}_L$. We call $\mathfrak{p}$ a *good prime* with respect to $\varphi : E \to \mathbb{P}_1$ if

- E has good reduction at $\mathfrak{p}$
- $\varphi_1 \bmod \mathfrak{p}$ and $\varphi_2 \bmod \mathfrak{p}$ have degree 1 and are linearly independent
- if $G_\varphi \neq -G_\varphi$, then $G_\varphi \bmod \mathfrak{p} \neq -G_\varphi \bmod \mathfrak{p}$
- $\nu_\mathfrak{p}(\mathrm{char}(\mathfrak{p})) < \mathrm{char}(\mathfrak{p}) - 1$.

Suppose that $\mathfrak{p}$ is such a prime. Then $\mathrm{Exp}_{\mathfrak{p}} : \mathfrak{p}\mathcal{O}_{\mathfrak{p}} \to E^{(1)}(L_{\mathfrak{p}})$ is a group isomorphism with the property that $Z(\mathrm{Exp}_{\mathfrak{p}}(z)) = z \bmod \mathfrak{p}^2$. Let $G \in E(L_{\mathfrak{p}})$ with $G \bmod \mathfrak{p} \neq G_\tau \bmod \mathfrak{p}$. Then, by choosing coordinates on $\mathbb{P}_1$ (i.e., by interchanging φ_1 and φ_2 if necessary), we can assume that $\varphi(G) \bmod \mathfrak{p} \neq \infty$. Then $\varphi(G + \mathrm{Exp}_{\mathfrak{p}}(z))$ is a power series with coefficients in L and convergent on $\mathfrak{p}\mathcal{O}_{\mathfrak{p}}$ with values in $\mathcal{O}_{\mathfrak{p}}$. We derive some approximations to these power series. Suppose that $z \in \mathfrak{p}\mathcal{O}_{\mathfrak{p}}$. If $G = \infty$ and $G_\tau \neq G_\varphi$ then

$$\varphi(\mathrm{Exp}_{\mathfrak{p}}(z)) = \varphi(\infty) + \frac{G_{\varphi,3}}{c_{22}^2} z \bmod \mathfrak{p}^2.$$

Put $F'(x) = 3x^2 + 2a_2x + a_4$. If $G = (x, y)$ and $G \bmod \mathfrak{p} \neq \infty$, then

$$\varphi((x,y) + \mathrm{Exp}_{\mathfrak{p}}(z)) = \varphi(x,y) + \frac{F'(x)(xG_{\varphi,3} - G_{\varphi,1}) - 2\gamma y(yG_{\varphi,3} - G_{\varphi,2})}{\gamma(c_{21}x + c_{22}y + c_{23})^2} z \bmod \mathfrak{p}^2.$$

Now suppose that $G_\tau = G_\varphi = \infty$. Then $\varphi(X : Y : D) = (c_{11}X + c_{13}D)/(c_{21}X + c_{23}D)$ and $\tau = [-1]$. Consequently, $\varphi(\mathrm{Exp}_{\mathfrak{p}}(Z))$ and $\varphi((x,0) + \mathrm{Exp}_{\mathfrak{p}}(Z))$ will be power series in Z^2. Using higher order terms, we derive

$$\begin{aligned} \varphi(\mathrm{Exp}_{\mathfrak{p}}(z)) &= \frac{c_{11}}{c_{21}} + \frac{G_{\varphi,2}}{\gamma c_{21}} z^2 \bmod \mathfrak{p}^3, \\ \varphi((x,0) + \mathrm{Exp}_{\mathfrak{p}}(z)) &= \varphi(x,0) - \frac{F'(x)G_{\varphi,2}}{\gamma(c_{21}x + c_{23})^2} z^2 \bmod \mathfrak{p}^3. \end{aligned}$$

4.5 Rationality restrictions on elliptic covers

Let $\mathbb{Q} \subset K \subset L$ be number fields and let $\varphi : E \to \mathbb{P}_1$ be an elliptic cover defined over L. In this section we propose a method for determining the L-rational points G on E such that $\varphi(G)$ is K-rational. Note that, although φ is just defined over L, the answer to this question requires $\mathbb{P}_1$ to be viewed as a curve over K and not over L. The method we explain here might give a sharp bound on the number of such G if $\mathrm{rk}(E(L)) < [L : K]$. In Proposition 4.5.3 as well as in Sections 4.6, 4.7 and 4.8, we will only deal with cases where $K = \mathbb{Q}$.

By Theorem 2.4.1, $E(L)$ is a finitely generated abelian group. Suppose that $E(L) = \langle G_1, \ldots, G_r, G_{r+1}, \ldots, G_{r+t} \rangle$, where $\langle G_1, \ldots, G_r \rangle \simeq \mathbb{Z}^r$ and $\langle G_{r+1}, \ldots, G_{r+t} \rangle$ is finite.

We choose a prime p of $\mathcal{O}_K$ such that all $\mathfrak{p} \mid p$ of $\mathcal{O}_L$ are unramified in $\mathcal{O}_L/\mathcal{O}_K$, $\nu_{\mathfrak{p}}(\mathrm{char}(\mathfrak{p})) < \mathrm{char}(\mathfrak{p}) - 1$, E has good reduction at $\mathfrak{p}$ and $\varphi \bmod \mathfrak{p} : (E \bmod \mathfrak{p}) \to \mathbb{P}_1$ is again a cover.

Choose $B_1, \ldots, B_r \subset E(L)$ such that

$$\langle B_1, \ldots, B_r \rangle = \bigcap_{\mathfrak{p} \mid p} \left(E^{(1)}(L_{\mathfrak{p}}) \cap E(L) \right).$$

Since $E(L)/\langle B_1, \ldots, B_r \rangle$ is finite, we need only finitely many $G_0 \in E(L)$ to cover $E(L)$ with translates $G_0 + \langle B_1, \ldots, B_r \rangle$.

We fix G_0 and try to determine how many points G of the form $G = G_0 + n_1B_1 + \cdots + n_rB_r$ exist such that $\varphi(G) \in \mathbb{P}_1(K)$. Note that $\varphi(G)$ is K-rational if and only if $1/\varphi(G)$ is. If $\mathfrak{p}, \mathfrak{q} \mid p$ such that $\varphi(G_0) \bmod \mathfrak{p} = \infty$ and $\varphi(G_0) \bmod \mathfrak{q} \neq \infty$, then there is no $G = G_0 + n_1B_1 + \cdots n_rB_r$ with $\varphi(G) \in \mathbb{P}_1(K)$, as this would imply $\varphi(G_0) \bmod \mathfrak{p} = \varphi(G_0) \bmod \mathfrak{q}$. Therefore, by changing from φ to $1/\varphi$ if necessary, which corresponds to a K-rational coordinate transformation on $\mathbb{P}_1$, we can assume that $\varphi(G_0) \bmod \mathfrak{p} \neq \infty$ for any $\mathfrak{p} \mid p$. Since $B_1, \ldots, B_r \in E^{(1)}(L_\mathfrak{p})$ for all $\mathfrak{p} \mid p$, we have

$$n_1B_1 + \cdots + n_rB_r = \mathrm{Exp}_\mathfrak{p}(n_1\mathrm{Log}_\mathfrak{p}(B_1) + \cdots + n_r\mathrm{Log}_\mathfrak{p}(B_r)).$$

Consequently, we can write

$$\theta_\mathfrak{p}^{G_0}(n_1, \ldots, n_r) = \varphi\left(G_0 + \mathrm{Exp}_\mathfrak{p}\left(\sum n_i\mathrm{Log}_\mathfrak{p}(B_i)\right)\right) \in L[\![n_1, \ldots, n_r]\!],$$

which is convergent for $(n_1, \ldots, n_r) \in (\mathcal{O}_\mathfrak{p})^r$ and has values in $\mathcal{O}_\mathfrak{p}$. If $\varphi(G_0 + \sum n_iB_i) \in \mathbb{P}_1(K)$, then, identifying $\mathbb{P}_1(L) \setminus \{\infty\}$ with L, we have $\theta_\mathfrak{p}^{G_0}(n_1, \ldots, n_r) \in \mathcal{O}_p \subset \mathcal{O}_\mathfrak{p}$. If $\mathfrak{q} \mid p$ as well then $\theta_\mathfrak{p}^{G_0}(n_1, \ldots, n_r) = \theta_\mathfrak{q}^{G_0}(n_1, \ldots, n_r)$. These requirements can be expressed in power series over K in the following way. Let $I = [L_\mathfrak{p} : K_p]$ and let $1, \alpha, \ldots, \alpha^{I-1}$ be an $\mathcal{O}_p$-basis of $\mathcal{O}_\mathfrak{p}$. Then there are unique $\theta_{\mathfrak{p},i}^{G_0} \in K_p[\![n_1, \ldots, n_r]\!]$ such that

$$\theta_\mathfrak{p}^{G_0} = \theta_{\mathfrak{p},0}^{G_0} + \alpha\theta_{\mathfrak{p},1}^{G_0} + \cdots + \alpha^{I-1}\theta_{\mathfrak{p},I-1}^{G_0}.$$

The statement $\varphi(G_0 + \sum n_iB_i) \in \mathbb{P}_1(K)$ translates into $\theta_{\mathfrak{p},i}^{G_0}$ and $\theta_{\mathfrak{p},0}^{G_0} - \theta_{\mathfrak{q},0}^{G_0}$ having a simultaneous zero in $(n_1, \ldots, n_r)$ for all $\mathfrak{p}, \mathfrak{q} \mid p$ and $i \geq 1$. Taking all these conditions together, this corresponds to some $\theta^{G_0} \in K_p[\![n_1, \ldots, n_r]\!]^{[L:K]-1}$ vanishing in $(n_1, \ldots, n_r)$. If p splits completely (i.e. $L_\mathfrak{p} = K_p$ for all $\mathfrak{p} \mid p$) then it is particularly easy to express this power series. Suppose that $\mathfrak{p}_1, \ldots, \mathfrak{p}_m \mid p$. Then

$$\theta^{G_0}(n_1, \ldots, n_r) = \begin{pmatrix} \theta_{\mathfrak{p}_2}^{G_0}(n_1, \ldots, n_r) - \theta_{\mathfrak{p}_1}^{G_0}(n_1, \ldots, n_r) \\ \vdots \\ \theta_{\mathfrak{p}_m}^{G_0}(n_1, \ldots, n_r) - \theta_{\mathfrak{p}_1}^{G_0}(n_1, \ldots, n_r) \end{pmatrix}.$$

It is often possible to give a bound on the number of zeros that such a power series has if $r < m$. The following lemma is an example of the kind of arguments that might apply.

4.5.1. Lemma. *Let $\mathcal{O}_\mathfrak{p}$ be a complete local ring with maximal ideal $\mathfrak{p}$ and*

$$f = (f_1, \ldots, f_m) \in (\mathcal{O}_\mathfrak{p}[\![X_1, \ldots, X_r]\!])^m,$$

convergent on $\mathcal{O}_\mathfrak{p}^r$. Write $X = (X_1, \ldots, X_r)$. If one of the following conditions holds,

- *$f(X_1, \ldots, X_r) = b + A\,X \bmod \mathfrak{p}$, where A is an $m \times r$ matrix over $\mathcal{O}_\mathfrak{p}$ such that $A \bmod \mathfrak{p}$ has rank r,*
- *$f_i(0, \ldots, 0) = 0$, $\frac{\partial f_i}{\partial X_j}(0, \ldots, 0) = 0$ and $f_i(X_1, \ldots, X_r) = X^t\,A_i\,X \bmod \mathfrak{p}$ for all i, j, where the $A_1, \ldots, A_m$ are symmetric $r \times r$ matrices such that the projective variety in $\mathbb{P}_{r-1}$ described by $\{X^t(A_i \bmod \mathfrak{p})X = 0\}_{i=1,\ldots,m}$ has no points over $\mathcal{O}_\mathfrak{p}/\mathfrak{p}$,*

then f has at most one zero in $\mathcal{O}_{\mathfrak{p}}^r$.

Proof: Let u be a uniformiser of $\mathcal{O}_{\mathfrak{p}}$. Consider the first case. Note that $g(X) = f(X) - b - A\,X \in (\mathfrak{p}\mathcal{O}_{\mathfrak{p}}[\![X_1, \ldots, X_r]\!])^m$. If $x \in (\mathcal{O}_{\mathfrak{p}})^r$ and $f(x) = 0$ then we have that $A\,x = -b \bmod \mathfrak{p}$. By assumption, there is at most one such $x \bmod \mathfrak{p}$. It remains to show that f cannot have two zeros reducing to the same vector mod $\mathfrak{p}$. Suppose that there is an $e \geq 1$ and $x, y \in (\mathcal{O}_{\mathfrak{p}})^r$, $y \not\equiv 0 \bmod \mathfrak{p}$, such that $f(x) = f(x + u^e y) = 0$. Subtraction yields $0 = -u^e A\,y + g(x) - g(x + u^e y)$. By the assumption on the rank of A and $y \not\equiv 0 \bmod \mathfrak{p}$, it follows that $-u^e A\,y \not\equiv 0 \bmod \mathfrak{p}^{e+1}$, but since all coefficients of g are divisible by $\mathfrak{p}$, we have that $g(x) = g(x + u^e y) \bmod \mathfrak{p}^{e+1}$. It follows that such y, e cannot exist.

For the second case, suppose that there is a $y \in \mathcal{O}_{\mathfrak{p}}^r$ with $y \bmod \mathfrak{p} \neq 0$ and an $e \geq 0$ such that $f(u^e y) = 0$. Then $0 = f_i(y) = u^{2e} y^t A_i y \bmod \mathfrak{p}^{2e+1}$. It follows that y reduces to a point on $\{X^t (A_i \bmod \mathfrak{p}) X = 0\}_{i=1,\ldots,m}$. □

We apply these ideas to the case where $\deg(\varphi) = 2$. We adopt the notation from Section 4.4 and we assume that the $\mathfrak{p} \mid p$ are good with respect to $\varphi : E \to \mathbb{P}_1$. If we stay away from $G_\varphi \bmod \mathfrak{p}$ then the formulas given there lead to

$$\begin{aligned}
\theta_{\mathfrak{p}}^{\infty} &= \varphi(\infty) + \frac{G_{\varphi,3}}{c_{22}^2} \sum_{i=1}^{r} n_i Z(B_i) \bmod \mathfrak{p}^2, \\
\theta_{\mathfrak{p}}^{(x,y)} &= \varphi(x,y) + \frac{F'(x)(xG_{\varphi,3} - G_{\varphi,1}) - 2\gamma y(yG_{\varphi,3} - G_{\varphi,2})}{\gamma(c_{21}x + c_{22}y + c_{23})^2} \sum_{i=1}^{r} n_i Z(B_i) \bmod \mathfrak{p}^2,
\end{aligned}$$

which enables us to compute $\theta^{\infty} \bmod p^2$ and $\theta^{(x,y)} \bmod p^2$. For the case $G_\varphi = G_\tau = \infty$ we have

$$\begin{aligned}
\theta_{\mathfrak{p}}^{\infty} &= \frac{c_{11}}{c_{21}} + \frac{G_{\varphi,2}}{\gamma c_{21}} \sum_{i,j=1}^{r} n_i n_j Z(B_i) Z(B_j) \bmod \mathfrak{p}^3, \\
\theta_{\mathfrak{p}}^{(x,0)} &= \varphi(x,0) - \frac{F'(x) G_{\varphi,2}}{\gamma(c_{21}x + c_{23})^2} \sum_{i,j=1}^{r} n_i n_j Z(B_i) Z(B_j) \bmod \mathfrak{p}^3.
\end{aligned}$$

which enable us to compute $\theta^{\infty} \bmod p^3$ and $\theta^{(x,0)} \bmod p^3$ in these cases. Note that the fact that φ is even in this case, guarantees that only monomials of even degree occur in θ^{∞} and $\theta^{(x,0)}$. Furthermore, since $\nu_{\mathfrak{p}}(Z(B_i)) \geq 1$, we only need $Z(B_i) \bmod \mathfrak{p}^2$ to compute any of these approximations. We summarise this information in

$$Z(B)/u_p = \begin{pmatrix} Z(B_1)/u_p \bmod \mathfrak{p}_1 & \cdots & Z(B_r)/u_p \bmod \mathfrak{p}_1 \\ \vdots & \ddots & \vdots \\ Z(B_1)/u_p \bmod \mathfrak{p}_m & \cdots & Z(B_r)/u_p \bmod \mathfrak{p}_m \end{pmatrix}$$

where u_p is some fixed uniformiser for p in K. (Since the $\mathfrak{p}_i$ are unramified over p, u_p is also a uniformiser for $\mathfrak{p}_i$ in L).

For simplicity, we assumed that we have generators of $E(L)$. Note that $E^{(1)}(L_\mathfrak{p})$ is isomorphic to $\mathfrak{p}\mathcal{O}_\mathfrak{p}$ and as such has an $\mathcal{O}_\mathfrak{p}$-module structure. In particular, it is an $\mathcal{O}_p$-module. In fact, instead of *generators* of $E(L)$, we only need $E(L) \bmod \mathfrak{p}$ and a set $\{B_1, \ldots, B_r\} \in E(L)$ that generates an $\mathcal{O}_p$-module in $E^{(1)}(L_\mathfrak{p})$ containing $\bigcap(E^{(1)}(L_\mathfrak{p}) \cap E(L))$. This means that we only have to prove that

$$\operatorname{char}(p) \nmid \left[\bigcap_{\mathfrak{p}|p} \left(E^{(1)}(L_\mathfrak{p}) \cap E(L)\right) : \langle B_1, \ldots, B_r \rangle \right],$$

which is much easier to establish. For instance, this follows from Lemma 4.3.1 if all $L_\mathfrak{p} = K_p$ and $Z(B)/u_p \bmod p$ has rank r. If $E(L) \bmod \mathfrak{p} = \langle G_1, \ldots, G_{r+t} \rangle$, then representatives of $E(L) \bmod \mathfrak{p}$ are easily generated.

We assumed that we used the information at all primes of L above p. The argument might already work if we just use the information at $\mathfrak{p}_1, \ldots, \mathfrak{p}_m \mid p$ with $\sum_{i=1}^m [L_\mathfrak{p} : K_p] > r$. Then, it is sufficient to take $B_1, \ldots, B_r$ to generate a subgroup of $\bigcap_{i=1}^m (E^{(1)}(L_{\mathfrak{p}_i}) \cap E(L))$ of index prime to $\operatorname{char}(p)$. Thus, we can bound the number of $G \in E(L)$ with K-rational image under φ in a p-adic neighbourhood by bounding the number of zeros of θ^{G_0}. This can be done using Lemma 4.5.1. We have the following.

4.5.2. Lemma. *Let $K, L, p, \mathfrak{p}_1, \ldots, \mathfrak{p}_m$ and $\varphi : E \to \mathbb{P}_1$ be defined as above. Let $G \in E(L)$.*

- *If $\theta^G \bmod p \neq 0$, then $\varphi(G) \bmod p$ is not hit by $\varphi(E(L)) \cap \mathbb{P}_1(K)$.*
- *If $\varphi(G) \in \mathbb{P}_1(L)$ and θ^G/p satisfies the first condition in Lemma 4.5.1, then G and $\tau_\varphi(G)$ are the only $G' \in E(L)$ such that $\varphi(G') \in \mathbb{P}_1(K)$ and $\varphi(G) \bmod p = \varphi(G') \bmod p$.*
- *If $G = G_\varphi = G_\tau = (0:1:0)$ and θ^G/p^2 satisfies the second condition in Lemma 4.5.1, then G is the only $G' \in E(L)$ such that $\varphi(G') \in \mathbb{P}_1(K)$ and $\varphi(G) \bmod p = \varphi(G') \bmod p$.*

As an example we prove the following proposition. The example is chosen such that the result can be used later on.

4.5.3. Proposition. *Let $\alpha = \sqrt{3}$ and let $L = \mathbb{Q}(\alpha)$. Let $E : 2Y^2 = X^3 - 2\alpha X$ and let $\varphi : E \to \mathbb{P}_1$ be the cover $(X, Y) \to X$. Then $\varphi(E(L)) \cap \mathbb{P}_1(\mathbb{Q}) = \{\infty, 0, 2\}$.*

Proof: We refer to Lemma 4.3.2 for notation. We have $E \bmod \mathfrak{p} : Y^2 = X^3 + 9X$ and $E \bmod \mathfrak{q} : Y^2 = X^3 + 14X$. The following describes $\langle G_1, G_2 \rangle \bmod \mathfrak{p}$ (clearly $6G_1 + G_2 \bmod \mathfrak{p} = \infty$).

n	0	1	2	3	4	5
nG_1	∞	$(2,6)$	$(4,21)$	$(3,21)$	$(8,19)$	$(16,2)$
$nG_1 + G_2$	$(0,0)$	$(16,21)$	$(8,4)$	$(3,2)$	$(4,2)$	$(2,17)$

We do the same for $\langle G_1, G_2 \rangle \bmod \mathfrak{q}$ (we see that $12G_1 \bmod \mathfrak{q} = \infty$).

n	0	1	2	3	4	5	6
nG_1	∞	$(2,15)$	$(9,18)$	$(18,11)$	$(6,9)$	$(8,17)$	$(3,0)$
$nG_1 + G_2$	$(0,0)$	$(7,5)$	$(22,2)$	$(11,15)$	$(10,8)$	$(19,20)$	$(20,0)$

$$\begin{array}{lll} \mathcal{C}_1 & : & Y^2 = -(X^2+3)(X^4-18X^2+9) \\ \mathcal{C}_2 & : & Y^2 = (X^2+3)(X^4-18X^2+9) \\ \mathcal{C}_3 & : & Y^2 = 6X(X^4-12) \\ \mathcal{C}_4 & : & Y^2 = 6X(3X^4-4) \\ \mathcal{C}_5 & : & Y^2 = 6X(X^4-3) \end{array}$$

Table 4.2: Parametrising curves for $x^2 + y^8 = z^3$

Now, if $\varphi(G) = X(G) \in \mathbb{P}_1(\mathbb{Q})$ then in particular, $X(G) \bmod \mathfrak{p} = X(G) \bmod \mathfrak{q}$. Since G_1, G_2 span $E(L) \bmod \mathfrak{p}$ and $E(L) \bmod \mathfrak{q}$, we can find $k_1, k_2 \in \mathbb{Z}$ and $B \in (E(L) \cap E^{(1)}(L_\mathfrak{p})) \cap E^{(1)}(L_\mathfrak{q})$ such that $G = k_1 G_1 + k_2 G_2 + B$. A priori, we get $X(G) \bmod 23 \in \{\infty, 0, 2, 3, 8\}$, since other values do not occur in both tables. Note that $X(G) = X(k_1 G_1 + k_2 G_2) \bmod \mathfrak{p}$ and $X(G) = X(k_1 G_1 + k_2 G_2) \bmod \mathfrak{q}$. For instance, if $X(G) \in \mathbb{P}_1(\mathbb{Q})$ and $X(G) = 8 \bmod 23$, then at $\mathfrak{p}$ it follows that $k_1 G_1 + k_2 G_2 \in \{4G_1, 2G_1 + G_2\} + \langle 6G_1 + G_2 \rangle$ and at $\mathfrak{q}$ we get that $k_1 G_1 + k_2 G_2 \in \{5G_1, 7G_1\} + \langle 12G_1 \rangle$. These contradict each other and we conclude that $X(G) = 8 \bmod 23$ does not happen. For $X(G) = 3 \bmod 23$ we proceed similarly. Note that for the remaining values, we have $X(\infty) = \infty$, $X(G_1) = 2$ and $X(G_2) = 0$, so these values really do occur. It remains to prove that for each of these values x, we have that if $X(G) \in \mathbb{P}_1(\mathbb{Q})$ and $X(G) = x \bmod \mathfrak{p}$ and $X(G) = x \bmod \mathfrak{q}$, then $X(G) = x$.

For that, we have to find a subgroup of $\langle G_1, G_2 \rangle$ that generates a $\mathbb{Z}_{23}$-submodule containing $(E(L) \cap E^{(1)}(L_\mathfrak{p})) \cap E^{(1)}(L_\mathfrak{q})$. The cyclic group generated by $B_1 = 12G_1$ is one. To check this we can calculate $Z(B_1) = (X/Y)(B_1) \bmod \mathfrak{p}^2$ and $\bmod \mathfrak{q}^2$. This gives $23 \cdot 21$ and $23 \cdot 16$ respectively. These values can be obtained by computing $Z(12G_1)$ globally and then reducing using $\alpha = 306 \bmod \mathfrak{p}^2$ and $\alpha = 223 \bmod \mathfrak{q}^2$, but it is much more efficient to only calculate an approximation of $12G_1$. Since $Z : E^{(1)}(L_\mathfrak{p}) \bmod \mathfrak{p}^2 \to \mathfrak{p}\mathcal{O}/\mathfrak{p}^2$ is a group homomorphism, we see that $12G_1$ indeed is not divisible by 23 in $E^{(1)}(L_\mathfrak{p})$ (as was already pointed out in Lemma 4.3.2 by the same argument). The same group homomorphism shows that $Z(n_1 B_1) \bmod \mathfrak{p}^2 = n_1 Z(B_1) \bmod \mathfrak{p}^2$ for $n_1 \in \mathbb{Z}_{23}$, and the same for $\mathfrak{q}$. This information enables us to compute $1/(\theta_\mathfrak{p}^\infty(n_1)) = \frac{1}{2} n_1^2 \cdot 23^2 21^2 \bmod \mathfrak{p}^3$ and $1/(\theta_\mathfrak{q}^\infty(n_1)) = \frac{1}{2} n_1^2 \cdot 23^2 16^2 \bmod \mathfrak{q}^3$. If $\varphi(n_1 B_1) \in \mathbb{P}_1(\mathbb{Q})$, then these values should agree, so the equation $23^2 \cdot 11 n_1^2 \bmod 23$ should hold. This (truncated) power series satisfies the second criterion in Lemma 4.5.2, so $n_1 = 0$ is the only solution. We proceed similarly for $G_2 + n_1 B_1$ and $G_1 + n_1 B_1$. Note that if $\varphi(G_1 + n_1 B_1) \in \mathbb{P}_1(\mathbb{Q})$, then the same holds for $\varphi(-G_1 - n_1 B_1)$, so we only have to look around one of $G_1, -G_1$. We find $\theta^{G_2}(n_1) = 23^2(3n_1^2) \bmod 23^3$ and $\theta^{G_1}(n_1) = 23(2n_1) \bmod 23^2$. In all cases we can use Lemma 4.5.2 to obtain the desired result. □

4.6 The equation $x^2 + y^8 = z^3$

This section provides an alternative proof to that in [Bru97]. Throughout this section, we write $\alpha := \sqrt{3}$ and $\beta := \sqrt[4]{3}$. First we determine parametrising curves for the primitive

integral solutions to the equation.

4.6.1. Lemma. *Let x, y, z be pairwise coprime integers such that $x^2+y^8 = z^3$. Then there is a $\mathcal{C}_i$ from Table 4.2, $t \in \mathbb{Q}$ and $P \in \mathcal{C}_i(\mathbb{Q})$ such that $Y(P) = y/t^3$ for $i = 1, \ldots, 4$ and $Y(P) = 2y/t^3$ for $i = 5$.*

Proof: First consider $x^2 + (y^2)^4 = z^3$. Then, by Lemma 3.2.3, we have $s, t \in \mathbb{Z}_{\{2,3\}}$ and a homogeneous degree 6 polynomial $F \in \mathbb{Q}[S, T]$ such that $y^2 = F(s, t)$. If $t \neq 0$, this leads to $(y/t^3)^2 = F(s/t, 1)$, i.e. a finite rational point on the curve $Y^2 = F(X, 1)$. If $t = 0$, then this leads to one of the infinite points on the curve. The curves in Table 4.2 are exactly those, except $\mathcal{C}_5$, where the model has been made integral. □

The rational points on $\mathcal{C}_1$ and $\mathcal{C}_2$ are easily determined.

4.6.2. Proposition. $\mathcal{C}_1(\mathbb{Q}) = \{\infty^+, \infty^-\}$.

Proof: The curve $\mathcal{C}_1$ is a double cover of the elliptic curve $Y^2 = -(X + 3)(X^2 - 18X + 9)$ by the map $X \mapsto X^2$. The elliptic curve is of conductor 2304 and has rank 0, which can be verified by performing a 2-isogeny descent as described in Section 4.3. The only affine torsion-point is $(-3, 0)$, which lifts to $(\pm\sqrt{-3}, 0)$ on $\mathcal{C}_1$. □

4.6.3. Proposition. $\mathcal{C}_2(\mathbb{Q}) = \{(0, 0), \infty\}$.

Proof: Unfortunately, by applying the map $X \mapsto X^2$ we get an elliptic curve of rank 1. We observe that, because $(X^2+3)(X^4-18X^2+9)$ has no rational roots and $\mathrm{res}(X^2+3, X^4 - 18X^2 + 9) = 2^6 3^4$, every rational solution must satisfy

$$\mu Y_1^2 = X^2 + 3 \tag{4.7}$$
$$\mu Y_2^2 = X^4 - 18X^2 + 9 \tag{4.8}$$

for one $\mu \in \{\pm 1, \pm 2, \pm 3, \pm 6\}$. Equation (4.7) shows that $\mu \geq 0$. A simple computer search shows that there are no solutions to $\mu Y_2^2 = X^4 - 18X^2Z^2 + 9Z^4 \bmod 128$ for $\mu = 2, 3, 6$ with $(X, Z) \in \mathbb{Z}^2$, $(X, Z) \neq (0, 0) \bmod 2$, which only leaves $\mu = 1$. For $\mu = 1$, (4.8) is isomorphic to 288D1, which is a curve with 4 rational points. For our model, these are $\infty^+, \infty^-, (0, 3), (0, -3)$. The affine points clearly do not satisfy (4.7). □

Although the technique used in Proposition 4.6.3 in principle does apply to $\mathcal{C}_3, \mathcal{C}_4, \mathcal{C}_5$, in each case we come across a genus 1 curve with infinitely many rational points. Therefore, we find other elliptic curves that describe $\mathcal{C}_i(\mathbb{Q})$ in some way. The following lemmas make this precise.

4.6.4. Lemma. *For points $P \in \mathcal{C}_3(\mathbb{Q})$ there exists an elliptic cover $\varphi : \mathcal{E} \to \mathbb{P}_1$ over a number field L and a point $Q \in \mathcal{E}(L)$ such that $\varphi(Q) = X(P)$. The curves $\mathcal{E}_1, \mathcal{E}_2$ from Table 4.3 suffice.*

Proof: Suppose we have $(x, y) \in \mathcal{C}_3(\mathbb{Q})$. Then we can write

$$\begin{aligned} 6x &= \delta_1 y_1^2 \\ x^2 - 2\alpha &= \delta_2 y_2^2 \\ y^2 &= \delta_1 y_1^2 N_{\mathbb{Q}(\alpha)/\mathbb{Q}}(\delta_2 y_2^2) \end{aligned}$$

j	$\mathcal{E}_j$	$\varphi(X,Y)$	L
1	$-3Y^2 = X^4 - 12$	X	$\mathbb{Q}$
2	$2Y^2 = X(X^2 - 2\alpha)$	X	$\mathbb{Q}(\alpha)$
3	$3Y^2 = 3X^4 - 4$	X	$\mathbb{Q}$
4	$\alpha Y^2 = X^3 - 2\alpha X$	X	$\mathbb{Q}(\alpha)$
5	$Y^2 = X^4 - 3$	X	$\mathbb{Q}$
6	$-3Y^2 = X^4 - 3$	X	$\mathbb{Q}$
7	$-(\beta^3 - \beta^2 - \beta + 1)Y^2 = (X - \beta)(X^2 + \beta^2)$	X	$\mathbb{Q}(\beta)$

$$\alpha^2 - 3 = 0; \quad \beta^4 - 3 = 0$$

L	$\mathbb{Z}$-basis of $\mathcal{O}_L$	$\mathrm{disc}(\mathcal{O}_L/\mathbb{Z})$	$\mathcal{O}_L^*$	$\mathrm{reg}(\mathcal{O}_L^*)$	$h(\mathcal{O}_L)$
$\mathbb{Q}(\alpha)$	$1, \alpha$	12	$\langle -1, 2+\alpha \rangle$	1.3170	1
$\mathbb{Q}(\beta)$	$1, \beta, \beta^2, \beta^3$	$-2^8 3^3$	$\langle -1, 2+\beta^2, 1+\beta-\beta^3 \rangle$	5.2459	1

L	p	$\mathfrak{p}$	defining relation
$\mathbb{Q}(\alpha)$	2	$\mathfrak{p}_2$	$\mathfrak{p}_2 = (1+\alpha)\mathcal{O};\ 2\mathcal{O} = \mathfrak{p}_2^2$
	3	$\mathfrak{p}_3$	$\mathfrak{p}_3 = \alpha\mathcal{O};\ 3\mathcal{O} = \mathfrak{p}_3^2$
	23	$\mathfrak{p}_{23,1}$	$\alpha - 7 \bmod \mathfrak{p}_{23,1} = 0$
		$\mathfrak{p}_{23,2}$	$\alpha + 7 \bmod \mathfrak{p}_{23,1} = 0$

L	p	$\mathfrak{p}$	defining relation
$\mathbb{Q}(\beta)$	2	$\mathfrak{p}_2$	$\mathfrak{p}_2 = (1+\beta)\mathcal{O};\ 2\mathcal{O} = \mathfrak{p}_2^4$
	3	$\mathfrak{p}_3$	$\mathfrak{p}_3 = \beta\mathcal{O};\ 3\mathcal{O} = \mathfrak{p}_3^4$
	13	$\mathfrak{p}_{13,1}$	$\beta - 3 \bmod \mathfrak{p}_{13,1} = 0$
		$\mathfrak{p}_{13,2}$	$\beta + 2 \bmod \mathfrak{p}_{13,2} = 0$
		$\mathfrak{p}_{13,3}$	$\beta + 3 \bmod \mathfrak{p}_{13,3} = 0$
		$\mathfrak{p}_{13,4}$	$\beta - 2 \bmod \mathfrak{p}_{13,4} = 0$

Table 4.3: Elliptic covers related to $\mathcal{C}_3, \mathcal{C}_4, \mathcal{C}_5$ with their fields of definition

If $y \neq 0, \infty$, then we can take δ_2 to be a square free $\{2,3\}$-unit in $\mathbb{Q}(\alpha)$ and $\delta_1 = N_{\mathbb{Q}(\alpha)/\mathbb{Q}}(\delta_2)$. The $\{2,3\}$-units are generated by $-1, 2+\alpha, 1-\alpha, \alpha$, of norms $1, 1, -2, -3$ respectively. Thus, the possible values for δ_1 are $1, -2, -3, 6$. Note that for $y_3 = y/(\delta_1 y_1)$ we have $x^4 - 12 = \delta_1 y_3^2$. This equation only has solutions over $\mathbb{Q}_2$ for $\delta_1 = 1, -3$. For $\delta_1 = -3$ we have $\mathcal{E}_1$. For $\delta_1 = N(\delta_2) = 1$ we get a curve of rank 1. The curve $x^2 - 2\alpha = \delta_2 y_2^2$, with δ_2 a square free unit, only has points locally at the prime above 2 for $\delta_2 = 1$. This corresponds to $\mathcal{E}_2$ by observing that $6x(x^2 - 2\alpha) = (y_1 y_2)^2$. Solutions with $y = 0$ correspond with $X = 0$ on $\mathcal{E}_1$ and $y = \infty$ with $X = \infty$ on $\mathcal{E}_2$. □

4.6.5. Lemma. *For points $P \in \mathcal{C}_4(\mathbb{Q})$ there exists an elliptic cover $\varphi : \mathcal{E} \to \mathbb{P}_1$ over a number field L and a point $Q \in \mathcal{E}(L)$ such that $\varphi(Q) = X(P)$. The curves $\mathcal{E}_3, \mathcal{E}_4$ from Table 4.3 suffice.*

Proof: Suppose $(x, y) \in \mathcal{C}_4(\mathbb{Q})$. If $y \neq 0, \infty$, then we can write

$$\begin{aligned} 6x &= \delta_1 y_1^2 \\ 2 - \alpha x^2 &= \delta_2 y_2^2 \\ y^2 &= -\delta_1 y_1^2 N_{\mathbb{Q}(\alpha)/\mathbb{Q}}(\delta_2 y_2^2) \end{aligned}$$

with δ_2 a square-free $\{2,3\}$-unit in $\mathbb{Q}(\alpha)$ and $\delta_1 = -N(\delta_2)$. As we saw in Lemma 4.6.4, this means that $\delta_1 = -1, 2, 3, -6$. We should have $3x^4 - 4 = \delta_1 N(y_2)^2$. This equation has

no solutions over $\mathbb{Q}_2$ for $\delta_1 = 2, -6$. For $\delta_1 = 3$, we get $\mathcal{E}_3$. For $\delta_1 = -1$, the corresponding curve over $\mathbb{Q}$ would have rank 1, so we examine this case in more detail. We have that $N(\delta_2) = 1$. Locally at the prime above 2, we have that $2 - \alpha X^2 = \delta_2 Y^2$ only has points for $\delta_2 = 2 + \alpha$. This leads to the equation $6X(2 - \alpha X^2) = -(2 + \alpha)Y^2$. This describes $\mathcal{E}_4$, which is E_4 in Table 4.4 if considered as an elliptic curve. □

4.6.6. Lemma. *For points $P \in \mathcal{C}_5(\mathbb{Q})$ there exists an elliptic cover $\varphi : \mathcal{E} \to \mathbb{P}_1$ over a number field L and a point $Q \in \mathcal{E}(L)$ such that $\varphi(Q) = X(P)$. The curves $\mathcal{E}_5, \mathcal{E}_6, \mathcal{E}_7$ from Table 4.3 suffice. The curve $\mathcal{E}_7$ is birational to the curve E_7 in Table 4.4 over L.*

Proof: Suppose we have $(x, y) \in \mathcal{C}_5(\mathbb{Q})$. Then there are $y_1 \in \mathbb{Q}$ and $y_2 \in \mathbb{Q}(\alpha)$ such that

$$\begin{aligned} 6x &= \delta_1 y_1^2 \\ x^2 - \alpha &= \delta_2 y_2^2 \\ y^2 &= \delta_1 N_{\mathbb{Q}(\alpha)/\mathbb{Q}}(\delta_2 y_2^2) y_1^2, \end{aligned}$$

where δ_2 is a square free $\{2,3\}$-unit in $\mathbb{Q}(\alpha)$ and $\delta_1 = N_{\mathbb{Q}(\alpha/\mathbb{Q}}(\delta_2)$. Taking norms gives $x^4 - 3 = \delta_1 y_3^2$ for $y_3 = N(y_2)$. We are thus led to consider the equation $X^4 - 3 = \delta_1 Y^2$ for $\delta_1 = 1, -2, -3, 6$. For $\delta_1 = 1, -3$, we get $\mathcal{E}_5$ and $\mathcal{E}_6$ respectively. For $\delta_1 = 6$ there are no solutions over $\mathbb{Q}_2$. We study the case $\delta_1 = -2$ in more detail. We put $L := \mathbb{Q}(\beta)$. We have $x^2 - \alpha = N_{L/\mathbb{Q}(\alpha)}(x - \beta)$ for some appropriate embedding $\mathbb{Q}(\alpha) \hookrightarrow \mathbb{Q}(\beta)$. Therefore, we can take $y_3 \in L$ and $\delta_3 \in L(\{2,3\}, 2)$ with $N_{L/\mathbb{Q}}(\delta_3) = N_{\mathbb{Q}(\alpha)/\mathbb{Q}}(\delta_2) = -2$ and

$$\begin{aligned} x - \beta &= \delta_4 y_4^2 \\ y^2 &= -2 y_1^2 N_{L/\mathbb{Q}}(\delta_4 y_4^2). \end{aligned}$$

We substitute $6x = -2y_1^2$, which leads to $y_1^2 + 3\beta = -\delta_4(\beta^2 y_4)^2$. A local argument at the prime above 2 shows that, up to squares, $\delta_4 = (2 + \beta^2)(1 - \beta)$ must hold for this equation to have solutions with $y_1 \in \mathbb{Q}_2$. Now we use that $(X^4 - 3)/(X + \beta) = (X - \beta)(X^2 + \beta^2)$ and we see that $(x - \beta)(x^2 + \beta^2) = (2 + \beta^2)(1 - \beta)(1 + \beta^2) y_5^2$ for some $y_5 \in L$. This leads to $\mathcal{E}_7$. The model E_7 only differs by a linear transformation. □

In order to apply the method described in Section 4.5, we need some data on the Mordell-Weil groups of the curves we have obtained.

4.6.7. Lemma. *Let E_4 be the elliptic curve described in Table 4.4 and $L = \mathbb{Q}(\alpha)$. We have $E_4^{\mathrm{tor}}(L) = \langle G_2 \rangle$. The group $\langle G_1, G_2 \rangle$ is a subgroup of odd finite index in $E_4(L)$, prime to 23. The group $\langle G_1, G_2 \rangle \bmod \mathfrak{p}_{23,i}$ spans $E_4(L) \bmod \mathfrak{p}_{23,i}$.*

Proof: The proof follows the same lines as that of Lemma 4.3.2. The following data give the necessary ingredients. Let $\mathfrak{p}_{13} \mid 13$ such that $\alpha \bmod \mathfrak{p}_{13} = 4$ and $E = E_4$.

$$\begin{array}{ll} \#(E \bmod \mathfrak{p}_{13})(\mathcal{O}/\mathfrak{p}_{11}) = 10 & G_1' = (6 + 6\alpha, 24 + 16\alpha);\ G_1 = \psi'(G_1') \\ \#(E \bmod \mathfrak{p}_{23,1})(\mathcal{O}/\mathfrak{p}_{23,1}) = 24 & E'(L_{\mathfrak{p}_2}/\psi(E(L_{\mathfrak{p}_2})) = \langle G_1', (10, ?), (0,0) \rangle \\ \#(\langle G_1, G_2 \rangle \bmod \mathfrak{p}_{23,1}) = 6 & E(L_{\mathfrak{p}_2}/\psi'(E'(L_{\mathfrak{p}_2})) = \langle G_3 \rangle \\ \#(\langle G_1, G_2 \rangle \bmod \mathfrak{p}_{23,2}) = 24 & E'(L_{\mathfrak{p}_2}/\psi(E(L_{\mathfrak{p}_2})) = \langle (0,0) \rangle \end{array}$$

$\langle G_1, G_2 \rangle \cap E^{(1)}(L_{\mathfrak{p}_{23,1}}) \cap E^{(1)}(L_{\mathfrak{p}_{23,2}}) = \langle 12G_1 \rangle$. See Table 4.4 for values of Z. □

j	G_i	p	M^t	$Z(B)/p$
2	$(2, \alpha - 1)$ $(0, 0)$	23	$\begin{pmatrix} 12 \\ 0 \end{pmatrix}$	$\begin{pmatrix} 21 \\ 16 \end{pmatrix}$
4	$(2 + \frac{4}{3}\alpha, -\frac{8}{3} - 2\alpha)$ $(0, 0)$	23	$\begin{pmatrix} 12 \\ 0 \end{pmatrix}$	$\begin{pmatrix} 13 \\ 15 \end{pmatrix}$
7	$(-3 - 2\beta - 2\beta^2 - \frac{1}{3}\beta^3, 2 + 5\beta + \frac{5}{3}\beta^2 + 2\beta^3)$ $(-\frac{3}{4} - \frac{3}{4}\beta - \frac{1}{4}\beta^2 - \frac{1}{12}\beta^3, -\frac{1}{4} - \frac{1}{2}\beta - \frac{1}{3}\beta^2)$ $(0, 0)$	13	$\begin{pmatrix} 2 & 0 \\ 12 & 24 \\ 0 & 0 \end{pmatrix}$	$\begin{pmatrix} 9 & 7 \\ 11 & 11 \\ 7 & 7 \\ 1 & 7 \end{pmatrix}$

$$\begin{array}{lllll} E_2 & : & 2Y^2 = X^3 - 2\alpha X & ; & \varphi_2(X,Y) = X \\ E_4 & : & \alpha Y^2 = X^3 - 2\alpha X & ; & \varphi_4(X,Y) = X \\ E_7 & : & -(\beta^2+\beta)Y^2 = X^3 + 2X^2 + 2 & ; & \varphi_7(X,Y) = \beta X + \beta \end{array}$$

Table 4.4: Curves E_j and data on Mordell-Weil group

4.6.8. Lemma. *Let E_7 be the elliptic curve described in Table 4.4 and $L = \mathbb{Q}(\beta)$. We have $E_7^{\mathrm{tor}}(L) = \langle G_2 \rangle$. The group $\langle G_1, G_2 \rangle$ is a subgroup of odd finite index in $E_7(L)$, prime to 13. The group $\langle G_1, G_2 \rangle \bmod \mathfrak{p}_{13,i}$ spans $E_7(L) \bmod \mathfrak{p}_{13,i}$.*

Proof: Proof as that of Lemma 4.3.2. Let $\mathfrak{p}_{11} \mid 11$ such that $\alpha \bmod \mathfrak{p}_{11} = 4$ and $E = E_7$.

$$\begin{array}{l} \#(E \bmod \mathfrak{p}_{11})(\mathcal{O}/\mathfrak{p}_{11}) = 10 \\ \#(\langle G_1, G_2, G_3 \rangle \bmod \mathfrak{p}_{13,i}) = 16, 12, 12, 12 \\ G_2' = (-2\beta - 2\beta^2, 2 + 4\beta + 2\beta^2);\ G_2 = \psi'(G_2) \\ E(L_{\mathfrak{p}_2}/\psi'(E'(L_{\mathfrak{p}_2})) = \langle G_1, G_3, (2 + \beta + \beta^2, ?), (2 + 3\beta + 3\beta^2, ?) \rangle \\ E'(L_{\mathfrak{p}_2}/\psi(E(L_{\mathfrak{p}_2})) = \langle G_2', (0,0) \rangle \\ E(\mathbb{R})/\psi' E'(\mathbb{R}) = \{0\} \text{ (for both real primes)} \\ E'(\mathbb{R})/\psi E(\mathbb{R}) = \langle (0,0) \rangle \text{ (for both real primes)} \\ \bigcap_{i=1}^{4} \langle G_1, G_2, G_3 \rangle \cap E^{(1)}(L_{\mathfrak{p}_{13,i}}) = \langle 2G_1 + 12G_2, 24G_2 \rangle \end{array}$$

See Table 4.4 for values of Z. □

Now we can put the information together and determine the rational points on the remaining curves.

4.6.9. Proposition. $\mathcal{C}_3(\mathbb{Q}) = \{\infty, (0,0)\}$.

Proof: Lemma 4.6.4 shows that we can obtain $\mathcal{C}_3(\mathbb{Q})$ if we determine which L-valued points have rational image under $\varphi_i : \mathcal{E} \to \mathbb{P}_1$ for $i = 1, 2$. It is straightforward to show that $\mathcal{E}_1$ is birational to $Y^2 = X^3 + 27X$. This is 288E1 in [Cre92] and has only 2 rational points. On $\mathcal{E}_1$, these are $(0, \pm 6)$. Proposition 4.5.3 gives us that $\varphi_2(E_2(\mathbb{Q}(\alpha))) \cap \mathbb{P}_1(\mathbb{Q}) = \{0, \infty, 2\}$. Together, this shows that $Q \in \mathcal{C}_3(\mathbb{Q})$ has $X(Q) \in \{0, \infty, 2\}$. For $X(Q) = 2$ we get $Q = (2, \pm 4\sqrt{3})$, which are not rational points. This proves the statement. □

4.6.10. Proposition. $\mathcal{C}_4(\mathbb{Q}) = \{(0,0), \infty\}$.

j	G	$\varphi(G)$	$\theta^G(n_1, \ldots, n_r)$
2	∞	∞	$23^2\left(11n_1^2\right) \bmod 23^3$
	G_2	0	$23^2\left(3n_1^2\right) \bmod 23^3$
	G_1	2	$23\left(2n_1\right) \bmod 23^2$
4	∞	∞	$23^2\left(16n_1^2\right) \bmod 23^3$
	G_2	0	$23^2\left(3n_1^2\right) \bmod 23^3$
7	∞	∞	$13^2\begin{pmatrix} 2n_2^2 - n_1n_2 \\ n_1^2 + n_1n_2 + 3n_2^2 \\ -2n_2^2 + n_1n_2 \end{pmatrix} \bmod 13^3$
	$G_1 - G_2$	$-\frac{1}{3}$	$13\begin{pmatrix} 5n_1 - 3n_2 \\ 7n_1 - n_2 \\ -n_1 + 3n_2 \end{pmatrix} \bmod 13^2$

Table 4.5: Fibres of rational points

Proof: By Lemma 4.6.5, it suffices to analyse $\mathcal{E}_3$ and E_4 as in the proof of Proposition 4.6.9. The curve $\mathcal{E}_3$ is birational to 288E1 in [Cre92] and has only 2 rational points, being $\infty^{\pm}$. These give $X(\infty^{\pm}) = \infty$. Similar to Proposition 4.5.3, we find $\varphi_4(E_4(L)) \cap \mathbb{P}_1(\mathbb{Q}) = \{0, \infty\}$. See Table 4.5 for relevant data. It follows that if $Q \in \mathcal{C}_4(\mathbb{Q})$, then we have $X(Q) = 0, \infty$, which gives the points stated in the proposition. □

4.6.11. Proposition. $\mathcal{C}_5(\mathbb{Q}) = \{(0,0), (-\frac{1}{3}, \pm\frac{22}{9}), \infty\}$.

Proof: The curve $\mathcal{E}_5$ is birational to $Y^2 = X^3 + 12X$, which is 576F2 in [Cre92] and has only 2 rational points, which are $\infty^{\pm}$ on $\mathcal{E}_5$. The curve $\mathcal{E}_6$ is birational to $Y^2 = X^3 + 108X$, which is 576G2 in [Cre92]. It also has only 2 rational points, being $(0, \pm 1)$ on $\mathcal{E}_6$. Similar to Proposition 4.5.3, we find $\varphi_7(E_7(L)) \cap \mathbb{P}_1(\mathbb{Q}) = \{0, -\frac{1}{3}\}$. See Table 4.5 for relevant data. This shows that the list stated is complete. □

Proof of Theorem 1.3.2: This is really just a matter of combining Lemma 4.6.1 and the Propositions 4.6.2 through 4.6.11. The points $(-\frac{1}{3}, \pm\frac{22}{9}) \in \mathcal{C}_5(\mathbb{Q})$ give rise to the nontrivial solutions.

4.7 The equation $x^8 + y^3 = z^2$

We can apply exactly the same methods as in the previous section to determine all primitive solutions to $x^8 + y^3 = z^2$. As it turns out, the computations are a lot more involved in this case, though. We refer to Table 4.7 for algebraic number theoretic data and notational conventions used throughout this section. We start by determining a set of parametrising curves.

4.7.1. Lemma. *Let $x, y, z \in \mathbb{Z}$ be a primitive solution to $x^8 + y^3 = z^2$. Then there is a $\mathcal{C} = \mathcal{C}_i$ from Table 4.6 with $P \in \mathcal{C}(\mathbb{Q})$ and $t \in \mathbb{Q}$ such that $x = t^3Y(P)$.*

$$
\begin{aligned}
\mathcal{C}_1 &: Y^2 = (X^2-3)(X^4+18\,X^2+9)\\
\mathcal{C}_2 &: Y^2 = -(X^2-3)(X^4+18\,X^2+9)\\
\mathcal{C}_3 &: Y^2 = 6X(X^4+12)\\
\mathcal{C}_4 &: Y^2 = 6X(3X^4+4)\\
\mathcal{C}_5 &: Y^2 = X^6+40X^3-32\\
\mathcal{C}_6 &: Y^2 = -X^6-40X^3+32\\
\mathcal{C}_7 &: Y^2 = X^6+6\,X^5-15\,X^4+20\,X^3+15\,X^2+30\,X-17\\
\mathcal{C}_8 &: Y^2 = -X^6-6\,X^5+15\,X^4-20\,X^3-15\,X^2-30\,X+17\\
\mathcal{C}_9 &: Y^2 = X^6-6\,X^5+45\,X^4-180\,X^3+135\,X^2+162\,X-405\\
\mathcal{C}_{10} &: Y^2 = -X^6+6\,X^5-45\,X^4+180\,X^3-135\,X^2-162\,X+405
\end{aligned}
$$

Table 4.6: Parametrising curves for $x^8+y^3=z^2$

Proof: Let x,y,z be such a solution. Then, by Lemma 3.2.7, we have some homogeneous $F\in\mathbb{Z}[S,T]$ of degree 6 as in Table 3.2 and $s,t\in\mathbb{Q}$ such that $\pm x^2=F(s,t)$ This leads to a point $P=(s/t,x/t^3)$ on $\pm Y^2=F(X,1)$. These curves are given in Table 4.6. Note that, for the curves $\mathcal{C}_3$ and $\mathcal{C}_4$, we can control the sign of $F(s,t)$ with the sign of t. Therefore, we only need one of $\pm Y^2=F(X,1)$. The curves $\mathcal{C}_9$ and $\mathcal{C}_{10}$ have undergone a small transformation to make $F(X,1)$ monic. □

For most of these curves, arguments using elliptic curves over $\mathbb{Q}$ suffice. For $\mathcal{C}_5$, $\mathcal{C}_7$ and $\mathcal{C}_9$ we need Section 4.5. The following lemma establishes the elliptic covers we need to consider. The models given in the lemma follow naturally from the models of the $\mathcal{C}_i$, whereas the models given in Table 4.9 are in twisted Weierstrass form and therefore are more suitable for computational purposes.

4.7.2. Lemma. *The $\mathbb{Q}$-rational points on $\mathcal{C}_5$, $\mathcal{C}_7$ and $\mathcal{C}_9$ correspond to L-rational points G on the genus 1 covers $\varphi=X:\mathcal{E}_j\to\mathbb{P}_1$ with $\varphi(G)\in\mathbb{P}_1(\mathbb{Q})$. The following choices for $\mathcal{E}_j$ and L suffice:*

$\mathcal{C}_j$	L	$\mathcal{E}_j$
$\mathcal{C}_5$	$\mathbb{Q}(\beta)$	$\mathcal{E}_5: Y^2=X^4-2\beta X^3+6\beta^2X^2+8X+8\beta$
$\mathcal{C}_7$	$\mathbb{Q}(\alpha)$	$\mathcal{E}_7: Y^2=(X^2+[2,-2,-2,0,0,-4,0,0,2,2,0,0]X+[-1,0,0,0,0,2,0,0,0,0,0,0])\cdot$ $(X^2+[2,0,0,-1,1,3,1,0,-2,0,-1,-3]X+[-1,0,4,3,5,-1,1,2,0,0,-1,-1])$
$\mathcal{C}_9$	$\mathbb{Q}(\alpha)$	$\mathcal{E}_9: Y^2=(X^2+[-2,2,2,0,0,0,0,0,-2,-2,0,0]X+[3,0,0,0,0,6,0,0,0,0,0,0])\cdot$ $(X^2+[-2,-2,0,-1,-1,1,-3,-2,0,2,-3,1]X+[3,12,6,3,3,-9,9,0,0,0,-3,3])$

These covers are birational to the ones given in Table 4.9 with given maps φ.

Proof: Let $\mathcal{C}:Y^2=F(X)$ be a hyperelliptic model of the genus 2 curve we consider. Let L be an extension of $\mathbb{Q}$ such that $F=R\cdot Q$ with $R,Q\in L[X]$. If $(x,y)\in\mathcal{C}(\mathbb{Q})$, then there are $\delta,y_1,y_2\in L$ such that $R(x)=\delta y_1^2$ and $Q(x)=\delta y_2^2$. Without loss of generality, we can take δ square-free S-unit, where S contains the places dividing $2\mathrm{disc}(F)$. We then see for which of those δ there exist $x\in\mathbb{Q}$ such that $\delta R(x)$ and $\delta Q(x)$ are squares simultaneously, everywhere locally. As it turns out, in all three cases, this only happens for $\delta=1$. Note that for $\mathcal{C}_7$ and $\mathcal{C}_9$, we can also find R and Q over $\mathbb{Q}(\beta)$ but the resulting elliptic curves turn out to have rank 3, which means that the described methods cannot be applied. Checking

$$\beta^3 - 2 = 0\,; \quad \alpha^{12} + 6\alpha^{10} + 39\alpha^8 + 64\alpha^6 + 15\alpha^4 - 6\alpha^2 - 3 = 0$$

L	$\mathbb{Z}$ basis of $\mathcal{O}_L$	$\mathrm{disc}(\mathcal{O}_L/\mathbb{Z})$	$\mathcal{O}_L^*$	$\mathrm{reg}(\mathcal{O}_L^*)$	$h(\mathcal{O}_L)$
$\mathbb{Q}(\beta)$	$1, \beta, \beta^2$	-108	$\langle -1, 1-\beta \rangle$	1.3474	1
$\mathbb{Q}(\alpha)$	$b_1, \ldots, b_{12}$	$-2^{26}3^{13}$	$\langle -1, \eta_1, \ldots, \eta_6 \rangle$	321.19	1

$$\begin{pmatrix} b_1 \\ b_2 \\ b_3 \\ b_4 \\ b_5 \\ b_6 \\ b_7 \\ b_8 \\ b_9 \\ b_{10} \\ b_{11} \\ b_{12} \end{pmatrix}^T = \begin{pmatrix} 1 \\ \alpha \\ \alpha^2 \\ \alpha^3 \\ \alpha^4 \\ \alpha^5 \\ \alpha^6 \\ \alpha^7 \\ \alpha^8 \\ \alpha^9 \\ \alpha^{10} \\ \alpha^{11} \end{pmatrix}^T \begin{pmatrix} 1 & 0 & -1 & 0 & -7 & 0 & 49 & 0 & 33 & 0 & -1641 & 0 \\ 0 & 0 & 1 & 0 & 1 & 8 & -28 & -38 & 66 & -88 & 613 & 1496 \\ 0 & 0 & -1 & -4 & 5 & 17 & 24 & 47 & -270 & -692 & 379 & 1290 \\ 0 & 1 & 0 & 0 & 0 & -27 & 0 & 96 & 0 & 455 & 0 & -4742 \\ 0 & 0 & 0 & -1 & 8 & 1 & -38 & 30 & -88 & -158 & 1496 & -273 \\ 0 & 0 & 0 & 0 & -7 & -8 & 33 & 38 & 64 & 88 & -1226 & -1496 \\ 0 & 0 & 0 & 3 & 0 & -8 & 0 & -55 & 0 & 446 & 0 & -67 \\ 0 & 0 & 0 & -4 & 0 & -2 & 0 & 150 & 0 & -564 & 0 & -2276 \\ 0 & 0 & 1 & 1 & -1 & -16 & -30 & 41 & 158 & 310 & 273 & -2449 \\ 0 & 0 & 1 & -1 & -1 & 16 & -30 & -41 & 158 & -310 & 273 & 2449 \\ 0 & 0 & 0 & 1 & 0 & -12 & 0 & 35 & 0 & 198 & 0 & -1797 \\ 0 & 0 & 0 & -3 & 0 & 24 & 0 & -21 & 0 & -622 & 0 & 3059 \end{pmatrix}^{-1}$$

Elements of $\mathbb{Q}(\alpha)$ are given with respect to the basis $b_1, \ldots, b_{12}$.

$$\begin{array}{l|l} \eta_1 = [0,1,0,0,0,0,0,0,0,0,0,0,0] & \eta_2 = [0,1,0,0,0,0,0,1,0,-1,0,0,0] \\ \eta_3 = [0,0,1,0,1,0,0,0,0,0,0,-1,0] & \eta_4 = [0,0,0,0,0,0,0,0,0,0,0,1,0] \\ \eta_5 = [0,-1,-1,0,0,0,0,0,1,1,0,1,-1] & \eta_6 = [0,1,-1,0,0,0,1,-1,0,0,0,0,0] \end{array}$$

L	p	$\mathfrak{p}$	defining relation	$\mathbb{F}_p$-basis of $\mathcal{O}/\mathfrak{p}$
$\mathbb{Q}(\beta)$	2	$\mathfrak{p}_2$	$\mathfrak{p}_2 = \beta\mathcal{O}\,;\ 2\mathcal{O} = \mathfrak{p}_2^3$	
	3	$\mathfrak{p}_3$	$\mathfrak{p}_3 = (1+\beta)\mathcal{O}\,;\ 3\mathcal{O} = \mathfrak{p}_3^3$	
	5	$\mathfrak{p}_{5,1}$	$\beta + 2 \bmod \mathfrak{p}_{5,1} = 0$	1
		$\mathfrak{p}_{5,2}$	$\beta^2 - 2\beta - 1 \bmod \mathfrak{p}_{5,2} = 0$	$1, \beta$
$\mathbb{Q}(\alpha)$	2	$\mathfrak{p}_2$	$\mathfrak{p}_2 = [0,1,0,0,1,0,1,0,0,0,0,0]\mathcal{O};\ 2\mathcal{O} = \mathfrak{p}_2^{12}$	
	3	$\mathfrak{p}_3$	$\mathfrak{p}_3 = [1,0,1,0,0,0,0,0,0,0,-1,0]\mathcal{O}$	
		$\mathfrak{q}_3$	$\mathfrak{q}_3 = [1,0,0,0,0,-1,0,0,1,1,0,0]\mathcal{O};\ 3\mathcal{O} = \mathfrak{p}_3^6\mathfrak{q}_3^3$	
	31	$\mathfrak{p}_{31,1}$	$\alpha - 5 \bmod \mathfrak{p}_{31,1} = 0$	1
		$\mathfrak{p}_{31,2}$	$\alpha + 12 \bmod \mathfrak{p}_{31,2} = 0$	1
		$\mathfrak{p}_{31,3}$	$\alpha + 5 \bmod \mathfrak{p}_{31,3} = 0$	1
		$\mathfrak{p}_{31,4}$	$\alpha - 12 \bmod \mathfrak{p}_{31,4} = 0$	1
		$\mathfrak{p}_{31,5}$	$\alpha^2 - 5\alpha + 13 \bmod \mathfrak{p}_{31,5} = 0$	$1, b_2$

Table 4.7: Data regarding number fields

j	G_i
5	$(-2,1)$
	$((-4-2\beta-\beta^2)/6,(1+\beta^2)/6)$
	$(1,0)$
	$(0,0)$
7	$([0,-1,6,-4,0,-1,-2,0,-4,0,-1,4],[8,-2,23,-12,-2,0,-6,7,-18,0,-6,14])$
	$([-1,-1,0,0,0,1,-1,1,0,0,0,-1],[0,0,0,1,1,-1,1,0,0,0,-1,-1])$
	$([1,0,0,-1,0,0,1,-1,-1,1,0,-1],[0,0,0,2,0,2,0,0,0,-4,0,-2])$
	$([-11,-1,-7,-2,-3,-10,0,-1,5,3,3,2]/12,-[4,-5,5,0,3,6,-10,4,-2,1,-5,1]/12)$
	$(0,0)$
9	$([1,-2,-4,-1,0,2,-1,1,1,1,2,-3]/3,[-4,-2,0,0,0,2,4,-2,-4,2,0,4]/3)$
	$([-7,1,-12,2,-2,2,2,-5,2,2,5,-6]/3,[28,-6,16,36,-2,-6,2,26,30,-12,-12,2]/3)$
	$([-1,2,0,0,-1,-2,1,-1,-1,1,0,1],[0,-4,-2,-1,-5,1,-5,2,4,-2,5,-1])$
	$([1,5,-3,-2,-1,-4,0,-7,-3,7,-5,6]/4,[5,2,-4,0,0,1,6,2,3,-6,5,-5]/4])$
	$(0,0)$

Table 4.8: Mordell-Weil pseudo-generators

that the covers in Table 4.9 are indeed birational to the ones mentioned in the lemma is tedious and straightforward. □

We examine the Mordell-Weil groups of the curves in Table 4.9.

4.7.3. Lemma. *Let E_5 be the elliptic curve described in Table 4.9 and the let the G_i be as in Table 4.8. We have $E_5^{\mathrm{tor}}(L) = \langle G_3, G_4\rangle$. The group $\langle G_1,\dots,G_4\rangle$ is a subgroup of odd finite index in $E_5(L)$ prime to 5. The group $\langle G_1,\dots,G_4\rangle \bmod \mathfrak{p}_{5,k}$ spans $E_5(L) \bmod \mathfrak{p}_{5,k}$ for $k = 1, 2$.*

Proof: Proof as that of Lemma 4.3.2. Let $E = E_5$ and $\mathfrak{p}_{11} \mid 11$ such that $\beta = 7 \bmod \mathfrak{p}$.

$$\begin{aligned}
&\#(E \bmod \mathfrak{p}_{11})(\mathcal{O}/\mathfrak{p}_{11}) = 12;\ \#(\langle G_1,\dots,G_4\rangle \bmod \mathfrak{p}_{5,i}) = 8, 16\\
&G_2' = (-2-2\beta, (4+2\beta+4\beta^2)/3);\ G_2 = \psi'(G_2')\\
&E(L_{\mathfrak{p}_2})/\psi'(E'(L_{\mathfrak{p}_2})) = \langle G_1, G_3, G_4\rangle\\
&E(L_{\mathfrak{p}_2})/\psi'(E'(L_{\mathfrak{p}_2})) = \langle G_2', (2+\beta, ?)\rangle \text{ (latter does not lift to } L(S,2))\\
&\langle G_1,\dots,G_4\rangle \cap E^{(1)}(L_{\mathfrak{p}_{5,1}}) \cap E^{(1)}(L_{\mathfrak{p}_{5,2}}) = \langle 2G_1 + G_4, 4G_2\rangle
\end{aligned}$$

See Table 4.10 for values of Z. □

4.7.4. Lemma. *Let E_7 be the elliptic curve described in Table 4.9 and the G_i as in Table 4.8. We have $E_7^{\mathrm{tor}}(L) = \langle G_5\rangle$. The group $\langle G_1,\dots,G_5\rangle$ is a subgroup of odd finite index in $E_7(L)$ prime to 31. The group $\langle G_1,\dots,G_5\rangle \bmod \mathfrak{p}_{31,k}$ spans $E_7(L) \bmod \mathfrak{p}_{31,k}$ for $k = 1,\dots,5$.*

j	E_j	c
5	$-6Y^2 = X^3 - X$	$\begin{pmatrix} \beta & -6\beta & \beta \\ 2 & 0 & -1 \end{pmatrix}$
7	$[0,0,0,-1,-1,0,-1,0,0,0,1,0]Y^2 = X^3 + 2X^2 + 2X$	C_7
9	$[0,0,0,1,1,-1,1,1,0,-1,1,-1]Y^2 = X^3 + 2X^2 + 2X$	C_9

$$C_7 = \begin{pmatrix} [4,-4,-4,-2,0,6,-2,8,4,-6,10,-8] & -12 & [2,1,2,5,2,-2,1,0,1,-3,-1,-3] \\ [0,4,0,4,0,0,0,-4,4,0,0,4] & 0 & [4,-3,0,5,2,-8,-1,-4,3,5,-5,5] \end{pmatrix}$$

$$C_9 = \begin{pmatrix} [0,2,6,0,-6,10,-10,6,-2,-10,2,2] & -12 & [0,7,2,1,-2,2,-3,2,1,-7,3,-1] \\ [-4,0,0,0,-4,0,0,0,0,-4,4,4] & 0 & [0,3,2,-1,0,2,-1,0,-1,-3,1,-1] \end{pmatrix}$$

$$\varphi(X,Y) = \frac{c_{11}X + c_{12}Y + c_{13}}{c_{21}X + c_{22}Y + c_{23}}$$

Table 4.9: Weierstrass models of covers

Proof: Proof is as that of Lemma 4.3.2. Let $E = E_7$ and $\mathfrak{p}_{43} \mid 43$ such that $\alpha = 6 \bmod \mathfrak{p}_{43}$.

$\#((E \bmod \mathfrak{p}_{43})(\mathcal{O}/\mathfrak{p}_{43})) = 38$
$\#(\langle G_1, \ldots, G_5 \rangle \bmod \mathfrak{p}_{31,i}) = 32, 32, 32, 32, 1024$
$G'_4 = ([1,-1,-1,0,1,-2,0,1,1,1,-1,0],[0,-2,0,0,0,0,-4,0,0,2,-2,2])$
$G_4 = \psi'(G'_4)$
$E(L_{\mathfrak{p}_2})/\psi'(E'(L_{\mathfrak{p}_2})) = \langle G_1, G_2, G_3, G_5, ([0,0,-7,-1,8,8,-4,-2,5,1,4,2],?),$
$([1,1,-5,0,3,6,2,-5,5,3,-3,2],?), ([-7,2,-4,5,-2,2,13,-7,-5,-3,2,-5],?),$
$([11,12,4,3,-6,-6,9,-5,1,-7,6,5],?), ([3,-4,6,5,0,6,1,7,-7,-1,4,-5],?),$
$([-15,8,-6,-5,-6,2,-15,7,5,1,-4,-3],?)\rangle$
$E'(L_{\mathfrak{p}_2})/\psi(E(L_{\mathfrak{p}_2})) = \langle G'_4, (0,0),$
$([18,-58,-48,-14,20,-28,-86,-20,-56,56,-2,54],?),$
$([-78,-74,-8,-54,-28,-8,90,56,-28,48,6,26],?)\rangle$

$E(L_{\mathfrak{q}_3})/\psi'(E'(L_{\mathfrak{q}_3})) = \langle G_2 \rangle$; $E'(L_{\mathfrak{q}_3})/\psi(E(L_{\mathfrak{q}_3})) = \langle G'_4 \rangle$
$E'(\mathbb{R})/\psi(E(\mathbb{R})) = \langle (0,0) \rangle$; $E(\mathbb{R})/\psi'(E'(\mathbb{R})) = \{1\}$ (for both real primes)
$\bigcap_{i=1}^{5} \langle G_1, \ldots, G_4 \rangle \cap E^{(1)}(L_{\mathfrak{p}_{31,i}}) = \langle 16G_1 + 8G_4 + G_5, 16G_2 + 8G_4, 32G_3, 16G_4 \rangle$

See Table 4.10 for values of Z. □

4.7.5. Lemma. *Let E_9 be the elliptic curve described in Table 4.9 and the G_i as in Table 4.8. We have $E_9^{\mathrm{tor}}(L) = \langle G_5 \rangle$. The group $\langle G_1, \ldots, G_5 \rangle$ is a subgroup of odd finite index in $E_9(L)$ prime to 31. The group $\langle G_1, \ldots, G_5 \rangle \bmod \mathfrak{p}_{31,k}$ spans $E_9(L) \bmod \mathfrak{p}_{31,k}$ for $k = 1, \ldots, 5$.*

j	p	M	$Z(B)/p \bmod p$
5	5	$\begin{pmatrix} 2 & 0 & 0 & 1 \\ 0 & 4 & 0 & 0 \end{pmatrix}$	$\begin{pmatrix} 4 & 4 \\ 4 & 1+4\beta \end{pmatrix}$
7	31	$\begin{pmatrix} 16 & 0 & 0 & 8 & 1 \\ 0 & 16 & 0 & 8 & 0 \\ 0 & 0 & 32 & 0 & 0 \\ 0 & 0 & 0 & 16 & 0 \end{pmatrix}$	$\begin{pmatrix} 23 & 21 & 1 & 19 \\ 12 & 30 & 28 & 21 \\ 21 & 11 & 4 & 20 \\ 26 & 27 & 25 & 30 \\ 23\alpha+7 & 11+\alpha & 22\alpha+1 & 19\alpha+8 \end{pmatrix}$
9	31	$\begin{pmatrix} 4 & 4 & 368 & 88 & 0 \\ 0 & 32 & 320 & 16 & 0 \\ 0 & 0 & 480 & 0 & 0 \\ 0 & 0 & 0 & 240 & 0 \end{pmatrix}$	$\begin{pmatrix} 25 & 4 & 17 & 29 \\ 27 & 4 & 28 & 29 \\ 12 & 23 & 26 & 0 \\ 7 & 15 & 17 & 13 \\ 11\alpha+13 & 21+8\alpha & 17\alpha+23 & 19\alpha+25 \end{pmatrix}$

For E_7 and E_9, only $\bigcap_{k=1}^{5}(E(L) \cap E^{(1)}(L_{\mathfrak{p}_{31,k}}))$ is considered.

Table 4.10: kernels of reduction

Proof: Proof is as that of Lemma 4.3.2. Let $E = E_7$ and $\mathfrak{p}_{43} \mid 43$ such that $\alpha = 6 \bmod \mathfrak{p}_{43}$.

$\#((E \bmod \mathfrak{p}_{43})(\mathcal{O}/\mathfrak{p}_{43})) = 50$
$\#(\langle G_1, \ldots, G_5\rangle \bmod \mathfrak{p}_{31,i}) = 32, 32, 32, 16, 900$
$G_4' = ([2,-2,0,0,0,2,-2,2,0,0,0,-2],[-2,0,-4,2,-4,0,-2,2,4,-4,4,-2])$
$G_4 = 2G_1 + 2G_2 - \psi'(G_4')$
$E(L_{\mathfrak{p}_2})/\psi'(E'(L_{\mathfrak{p}_2})) = \langle G_1, G_2, G_3, G_5, ([-6,6,6,-1,-3,-7,5,-6,4,4,5,-1],?),$
$([3,-1,5,0,-5,-4,-6,7,7,1,-3,-2],?),([1,-15,2,0,-6,4,16,7,-4,0,7,0],?),$
$([3,-7,6,-4,0,6,6,-7,-6,8,-1,4],?),([1,1,-2,6,-6,8,-6,-3,8,6,3,-4],?),$
$([-1,-13,4,6,0,-4,-6,3,6,-4,5,8],?)\rangle$
$E'(L_{\mathfrak{p}_2})/\psi(E(L_{\mathfrak{p}_2})) = \langle G_4', (0,0),$
$([50,46,-32,22,36,20,110,-32,-60,-4,-38,-46],?),$
$([-114,-30,40,10,48,-12,2,16,16,52,-6,-22],?)$
$E(L_{\mathfrak{p}_3})/\psi'(E'(L_{\mathfrak{p}_3})) = \langle(1/[1,0,0,1,0,0,0,0,0,0,0,0],?)\rangle$
$E'(L_{\mathfrak{p}_3})/\psi(E(L_{\mathfrak{p}_3})) = \langle G_4'\rangle$
$E'(\mathbb{R})/\psi(E(\mathbb{R})) = \langle(0,0)\rangle$; $E(\mathbb{R})/\psi'(E'(\mathbb{R})) = \{1\}$ (for both real primes)
$\bigcap_{i=1}^{5}\langle G_1, \ldots, G_4\rangle \cap E^{(1)}(L_{\mathfrak{p}_{31,i}}) = \langle 4G_1 + 4G_2 + 368G_3 + 88G_4,$
$32G_2 + 320G_3 + 16G_4, 480G_3, 240G_4\rangle$

See Table 4.10 for values of Z. □

4.7.6. Proposition. $\mathcal{C}_1(\mathbb{Q}) = \{\infty^+, \infty^-\}$.

Proof: The curve is a double cover of an elliptic curve by the map $X \mapsto X^2$. The elliptic curve $Y^2 = (X-3)(X^2+18X+9)$ is of rank 0 and has 2 rational points: ∞ and $(3,0)$. The first is covered by ∞^+ and ∞^-, which are indeed rational points of $\mathcal{C}_1$. The second is covered by $(\pm\sqrt{3}, 0)$, which are quadratic conjugate points. □

4.7.7. Proposition. $\mathcal{C}_2(\mathbb{Q}) = \emptyset$.

Proof: The curve is a double cover of an elliptic curve by the map $X \mapsto 1/X^2$. The elliptic curve $Y^2 = (3\,X - 1)(9\,X^2 + 18\,X + 1)$ is of rank 0 and has 2 rational points: $(1/3, 0)$ and ∞. Neither of these points lifts to rational points. □

4.7.8. Proposition. $\mathcal{C}_3(\mathbb{Q}) = \{\infty, (0,0)\}$.

Proof: We see that for solutions with $X \neq 0, \infty$, we have $X^4 + 12 = \delta\,Y_1^2$ with δ in the set $\{\pm 1, \pm 2, \pm 3, \pm 6\}$. It is clear that $\delta \geq 0$ from real considerations and that $2 \nmid \delta$ from considerations locally at 2. Both $X^4 + 12 = Y_1^2$ and $X^4 + 12 = 3\,Y_1^2$ are genus 1 curves of rank 0 with only 2 rational points: the two branches at infinity and the two points with $X = 0$ respectively. □

4.7.9. Proposition. $\mathcal{C}_4(\mathbb{Q}) = \{\infty, (0,0)\}$.

Proof: We see that for solutions with $X \neq 0, \infty$, we have $3\,X^4 + 4 = \delta\,Y_1^2$ with δ in the set $\{\pm 1, \pm 2, \pm 3, \pm 6\}$. It is clear that $\beta \geq 0$ from real considerations and that $2 \nmid \beta$ from considerations locally at 2. Both $3\,X^4 + 4 = 3\,Y_1^2$ and $3\,X^4 + 4 = Y_1^2$ are genus 1 curves of rank 0 with only 2 rational points: the two branches at infinity and the two points with $X = 0$ respectively. □

4.7.10. Proposition. $\mathcal{C}_5(\mathbb{Q}) = \{\infty^+, \infty^-, (1,3), (1,-3)\}$

Proof: Similar to Proposition 4.5.3, we find $\varphi_5(E_5(L)) \cap \mathbb{P}_1(\mathbb{Q}) = \{\infty, 0, 1\}$. By Lemma 4.7.2 this bounds $\mathcal{C}_5(\mathbb{Q})$. See Table 4.11 for relevant data. It is easy to check that $X = 0$ does not lead to a rational point. □

4.7.11. Proposition. $\mathcal{C}_6(\mathbb{Q}) = \emptyset$

Proof: It is easy to check that $\mathcal{C}_6(\mathbb{Q}_3) = \emptyset$. □

4.7.12. Proposition. $\mathcal{C}_7(\mathbb{Q}) = \{\infty^{\pm}, (1/2, \pm 15/8)\}$.

Proof: Similar to Proposition 4.5.3, we find $\varphi_7(E_7(L)) \cap \mathbb{P}_1(\mathbb{Q}) = \{\infty, \frac{1}{2}\}$. See Table 4.11 for relevant data. By Lemma 4.7.2 this bounds $\mathcal{C}_7(\mathbb{Q})$. □

4.7.13. Proposition. $\mathcal{C}_8(\mathbb{Q}) = \emptyset$

Proof: It is easy to check that $\mathcal{C}_8(\mathbb{Q}_2) = \emptyset$. □

4.7.14. Proposition. $\mathcal{C}_9(\mathbb{Q}) = \{\infty^{\pm}, (9/2, \pm 387/8\}$.

Proof: Similar to Proposition 4.5.3, we find $\varphi_9(E_9(L)) \cap \mathbb{P}_1(\mathbb{Q}) = \{\infty, \frac{9}{2}\}$. See Table 4.11 for relevant data. By Lemma 4.7.2 this bounds $\mathcal{C}_9(\mathbb{Q})$. □

4.7.15. Proposition. $\mathcal{C}_{10}(\mathbb{Q}) = \emptyset$

Proof: It is easy to check that $\mathcal{C}_{10}(\mathbb{Q}_3) = \emptyset$. □

Proof of Theorem 1.3.3 We now complete our proof by checking to which solutions the rational points on $\mathcal{C}_1, \ldots, \mathcal{C}_{10}$ correspond. Since at least one of the forms for x, y, z in Lemma 3.2.7, corresponding to $\mathcal{C}_1, \ldots, \mathcal{C}_6$, is divisible by s and t, points with $X = 0, \infty$

j	G	$\varphi(G)$	$\theta^G(n_1,\dots,n_r)$
5	∞	∞	$5\begin{pmatrix}2n_1+2n_2\\2n_1+3n_2\end{pmatrix} \bmod 5^2$
	G_3-G_1	0	$5\begin{pmatrix}3n_1+2n_2\\4n_1+4n_2\end{pmatrix} \bmod 5^2$
	G_2	1	$5\begin{pmatrix}4n_1+0n_2\\n_1+n_2\end{pmatrix} \bmod 5^2$
7	∞	∞	$31\begin{pmatrix}13&0&0&24\\4&4&4&21\\13&19&23&24\\20&16&11&1\\30&15&18&28\end{pmatrix}\begin{pmatrix}n_1\\n_2\\n_3\\n_4\end{pmatrix} \bmod 31^2$
	G_4	$\frac{1}{2}$	$31\begin{pmatrix}30&20&29&26\\24&15&18&13\\21&18&1&18\\27&26&4&3\\6&0&21&17\end{pmatrix}\begin{pmatrix}n_1\\n_2\\n_3\\n_4\end{pmatrix} \bmod 31^2$
9	∞	∞	$31\begin{pmatrix}16&24&16&19\\26&24&4&9\\29&4&28&26\\26&5&13&23\\4&23&11&15\end{pmatrix}\begin{pmatrix}n_1\\n_2\\n_3\\n_4\end{pmatrix} \bmod 31^2$
	$-G_4$	$\frac{9}{2}$	$31\begin{pmatrix}28&14&19&24\\18&19&29&11\\0&18&19&25\\15&29&17&6\\30&28&24&9\end{pmatrix}\begin{pmatrix}n_1\\n_2\\n_3\\n_4\end{pmatrix} \bmod 31^2$

Table 4.11: Fibres of rational points

correspond to solutions with $xyz = 0$. This only leaves $(1, \pm 3)$ on $\mathcal{C}_5$. The corresponding solutions are $(x, y, z) = (\pm 3, 2^3 \cdot 3^2 \cdot 5, \pm 3^3 \cdot 11 \cdot 23)$. Being a remarkable relation in itself, it does not satisfy the condition that $(x, y, z) = 1$. Furthermore, it cannot be transformed into such a solution using a weighted multiplication $(x, y, z) \mapsto (\lambda^3 x, \lambda^8 y, \lambda^{12} z)$ either.

On $\mathcal{C}_7$, the points $\infty^{\pm}$ correspond to $(\pm 1, 2, \pm 3)$ and the points $(1/2, \pm 15/8)$ correspond (after clearing denominators) to $(\pm 3 \cdot 5, 2 \cdot 3^2 \cdot 29 \cdot 37, \pm 3^3 \cdot 99431)$. On $\mathcal{C}_9$, $\infty^{\pm}$ correspond to $(\pm 3, -2 \cdot 3^2, \pm 3^3)$ and $(9/2, \pm 387/8)$ (after clearing denominators) to $(\pm 43, 2 \cdot 3 \cdot 7 \cdot 29 \cdot 79, \pm 109 \cdot 275623)$. We conclude that the list stated in the theorem is complete. □

4.8 The equations $x^2 \pm y^4 = z^5$

In this section we determine the primitive solutions to $x^2 + y^4 = z^5$ and $x^2 - y^4 = z^5$. We use the same methods as in the previous sections. Lemmas 3.2.4 and 3.2.5 show that we have to determine $\{2, 5\}$-primitive solutions to equations of the form $y^2 = F(s, t)$, where F is a homogeneous form of degree 5. According to Theorem 3.1.1, solutions to such equations are parametrised by the rational points on genus 5 curves. As it turns out, these curves cover elliptic curves. See Section 5.2 for a systematic approach to this. The next two lemmas determine these elliptic curves including the induced cover of the projective line.

4.8.1. Lemma. *The $\{2, 5\}$-primitive solutions to $y^2 = s(s^4 - 10s^2t^2 + 5t^4)$ have $s/t = \varphi(P)$, where $\varphi : \mathcal{E}_P \to \mathbb{P}_1$ is a double cover of genus 1 over a field L and $P \in \mathcal{E}_P(L)$. It suffices to take $\mathcal{E}_1, \ldots, \mathcal{E}_4$ as described in Table 4.12.*

Proof: Let $\beta^4 - 5\beta^2 + 5 = 0$. The field $\mathbb{Q}(\beta)$ is Galois and

$$X^4 - 10X^2 + 5X = (X + 2\beta - \beta^3)(X - 2\beta + \beta^3)(X - 4\beta + \beta^3)(X + 4\beta - \beta^3).$$

Put $\alpha = \beta^3 - 2\beta$. Using Lemma 3.1.2, it follows that with $S = \{2, 5\}$, we have

$$\begin{aligned} s &= N(\delta) a_4^2 \\ s - \alpha t &= \delta(a_0 + a_1\beta + a_2\beta^2 + a_3\beta^3)^2 \end{aligned}$$

where $\delta \in L(S, 2)$. It follows that $(s/t)^4 - 10(s/t)^2 + 5 = N(\delta)(y/(a_4 t^2))^2$ as well. As is easily checked, the curve $X^4 - 10X^2 + 5 = DY^2$ has no $\mathbb{Q}$-rational points for $D = 2, 10, -2, -5, -10$. For $D = 1, 5$, the curves are mentioned in the lemma. For $D = -1$, however, we get an elliptic curve of rank 1, which is not usable if we want a finite bound on the number of solutions. Therefore, we examine the case where $-N(\delta)$ is a square in more detail. As it turns out, all units in $\mathcal{O}$ have positive norm. Generators of the prime ideal $\mathfrak{p}_2 \mid 2$, for instance $1 + \beta - \beta^2$, have norm -4. Since $5\mathcal{O} = \mathfrak{p}_5^4$, we can take δ to be $1 + \beta - \beta^2$ times a square-free unit. This gives 16 possibilities. For each δ, we write out the 5 equations for s, t with respect to the basis $1, \ldots, \beta^3$ and we eliminate s, t from them. This leaves us with 3 quadratic forms in $a_0, \ldots, a_4$. By homogeneity, if they have a common rational zero, then there also is a solution $(a_0, \ldots, a_4) \in \mathbb{Z}^5$ with $\gcd(a_0, \ldots, a_4) = 1$. Thus, there

j	$\mathcal{E}_j$	$\varphi_j(X,Y)$	L
1	$Y^2{=}X^4-10X^2+5$	X	$\mathbb{Q}$
2	$5Y^2{=}X^4-10X^2+5$	X	$\mathbb{Q}$
3	$(8\beta-2\beta^3-6)Y^2{=}\beta^3X^3+(4\beta^2-5)X^2+(\beta^3-4\beta)X-1$	$1/X$	$\mathbb{Q}(\beta)$
4	$(2\beta^3-8\beta-6)Y^2{=}\beta^3X^3+(4\beta^2-5)X^2+(\beta^3-4\beta)X-1$	$1/X$	$\mathbb{Q}(\beta)$
5	$5Y^2{=}X^4+X^3+X^2+X+1$	X	$\mathbb{Q}$
6	$2(\zeta-\zeta^2-1)Y^2{=}X^4-\zeta X^3+\zeta^2X^2-\zeta^3X+\zeta^4$	X	$\mathbb{Q}(\zeta)$
7	$2(1-\zeta+\zeta^2)Y^2{=}X^4-\zeta X^3+\zeta^2X^2-\zeta^3X+\zeta^4$	X	$\mathbb{Q}(\zeta)$
8	$Y^2{=}X^4+\alpha^3X^3+2\alpha X^2+2\alpha^4X+4\alpha^2$	X	$\mathbb{Q}(\alpha)$
9	$(\alpha^3+\alpha^2-1)Y^2{=}X^4+\alpha^3X^3+2\alpha X^2+2\alpha^4X+4\alpha^2$	X	$\mathbb{Q}(\alpha)$

L	$\mathbb{Z}$-basis of $\mathcal{O}_L$	$\mathrm{disc}(\mathcal{O}_L/\mathbb{Z})$	$\mathcal{O}_L^*$	$\mathrm{reg}(\mathcal{O}_L^*)$	$h(\mathcal{O}_L)$
$\mathbb{Q}(\beta)$	$1,\beta,\beta^2,\beta^3$	2000	$\langle -1,\eta_1,\eta_2,\eta_3\rangle$	1.8528	1
$\mathbb{Q}(\zeta)$	$1,\zeta,\zeta^2,\zeta^3$	125	$\langle \zeta, 1-\zeta\rangle$	0.9624	1
$\mathbb{Q}(\alpha)$	$1,\alpha,\alpha^2,\alpha^3,\alpha^4$	50000	$\langle -1, 1-\alpha, \alpha^4-\alpha^3+\alpha^2-1\rangle$	4.8349	1

$$\begin{array}{rcl|l} \beta^4-5\beta^2+5 & = & 0 & \eta_1 = 2-\beta^2 \\ \zeta^4-\zeta^3+\zeta^2-\zeta+1 & = & 0 & \eta_2 = 2+\beta-\beta^2 \\ \alpha^5-2 & = & 0 & \eta_3 = -3+3\beta+\beta^2-\beta^3 \end{array}$$

L	p	defining relation
$\mathbb{Q}(\beta)$	41	$\beta = 3 \bmod \mathfrak{p}_{p,1}$
		$\beta = 18 \bmod \mathfrak{p}_{p,2}$
		$\beta = 23 \bmod \mathfrak{p}_{p,3}$
		$\beta = 38 \bmod \mathfrak{p}_{p,4}$
	2	$2\mathcal{O}_L = (1+\beta-\beta^2)\mathcal{O}_L^2 = \mathfrak{p}_2^2$
	5	$5\mathcal{O}_L = \beta\mathcal{O}_L^5 = \mathfrak{p}_5^4$
$\mathbb{Q}(\zeta)$	31	$\zeta = 15 \bmod \mathfrak{p}_{p,1}$
		$\zeta = 23 \bmod \mathfrak{p}_{p,2}$
		$\zeta = 27 \bmod \mathfrak{p}_{p,3}$
		$\zeta = 29 \bmod \mathfrak{p}_{p,4}$

L	p	defining relation
$\mathbb{Q}(\zeta)$	2	$2\mathcal{O}_L = \mathfrak{p}_2$
	5	$5\mathcal{O}_L = (1+\zeta+\zeta^2+\zeta^3)\mathcal{O}_L^4 = \mathfrak{p}_5^4$
$\mathbb{Q}(\alpha)$	151	$\alpha = 22 \bmod \mathfrak{p}_{p,1}$
		$\alpha = 25 \bmod \mathfrak{p}_{p,2}$
		$\alpha = 49 \bmod \mathfrak{p}_{p,3}$
		$\alpha = 90 \bmod \mathfrak{p}_{p,4}$
		$\alpha = 116 \bmod \mathfrak{p}_{p,5}$
	2	$2\mathcal{O}_L = \alpha\mathcal{O}_L^5 = \mathfrak{p}_2^5$
	5	$5\mathcal{O}_L = (\alpha+1)\mathcal{O}_L^5 = \mathfrak{p}_5^5$

Table 4.12: Parametrising curves and their fields of definition

should exist a solution $(a_0,\ldots,a_4)\in\mathbb{Z}_p^5$ with $(a_0,\ldots,a_4)\neq(0,\ldots,0) \bmod p$ for any prime p as well. See Appendix A.2 for an algorithm to check for local solutions. If we test this for both $p=2$ and $p=5$, we see that only for $\delta = 3\beta^3+6\beta^2-4\beta-9, -3\beta^3+6\beta^2+4\beta-9$ do we have solutions locally. If we combine this with our original relations on s,t and choose appropriate representatives of $L(S,2)$, we get that for some $y_1\in\mathbb{Q}(\beta)$ and $x=s/t$, we have

$$x(x^4-10x^2+5)/(x+\beta^3-4\beta) = 6\pm 2\beta(\beta^2-4)y_1^2.$$

This leads to the remaining two curves. □

$$
\begin{aligned}
E_j : \gamma_j Y^2 &= X^3 - 5X^2 + 5X \\
\gamma_3 &= 1 + \beta - \beta^2 \\
\varphi_3(X,Y) &= \frac{(6\beta - 2\beta^3)X + 3\beta^3 - 10\beta}{5} \\
\gamma_6 &= 2(\zeta^2 - \zeta) \\
\varphi_6(X,Y) &= \frac{X - 2\zeta^2 + \zeta - 2}{X + \zeta^3 + \zeta^2 - \zeta - 1} \\
\gamma_7 &= -2(\zeta^2 - \zeta) \\
\varphi_7(X,Y) &= \frac{X - 2\zeta^2 + \zeta - 2}{X + \zeta^3 + \zeta^2 - \zeta - 1} \\
\gamma_8 &= 1 \\
\varphi_8(X,Y) &= \frac{-\alpha^3 X + 2\alpha^3 Y}{4X - 5} \\
\gamma_9 &= \alpha^3 + \alpha^2 - 1 \\
\varphi_9(X,Y) &= \frac{2(6\alpha^4 - 4\alpha^3 + 5\alpha^2 + 11\alpha - 13)X + 12Y - 10(3\alpha^4 - \alpha^3 + 4\alpha - 6)}{(-4\alpha^3 + 2\alpha^2 + 2\alpha + 2)X - 12Y - 5(3\alpha^4 - 3\alpha^3 + \alpha^2 - 4)}
\end{aligned}
$$

Table 4.13: Description of covers with respect to models E_j

4.8.2. Lemma. *The $\{2,5\}$-primitive solutions to $2y^2 = s^5 - t^5$ have $s/t = \varphi(P)$, where $\varphi : \mathcal{E}_P \to \mathbb{P}_1$ is a double cover of genus 1 over a field L and $P \in \mathcal{E}_P(L)$. It suffices to take $\mathcal{E}_5, \mathcal{E}_6, \mathcal{E}_7$ as in Table 4.12.*

Proof: Let $\zeta^4 - \zeta^3 + \zeta^2 - \zeta + 1 = 0$. Then

$$X^5 - 1 = (X-1)(X+\zeta)(X-\zeta^2)(X+\zeta^3)(X-\zeta^4).$$

Put $\alpha = -\zeta$. It follows that

$$
\begin{aligned}
s - t &= 2N(\delta)a_4^2 \\
s + \zeta t &= \delta(a_0 + a_1\zeta + a_2\zeta^2 + a_3\zeta^3)^2
\end{aligned}
$$

where $\delta \in L(S,2)$. It follows that $(s/t)^4 + (s/t)^3 + (s/t)^2 + (s/t) + 1 = (y/a_4t^2))^2/N(\delta)$ as well. As is easily checked, the curve $X^4 + X^3 + X^2 + X + 1 = DY^2$ has $\mathbb{Q}$-rational points for $D = 1, 5$ only. For $D = 5$, the curve is mentioned in the lemma. For $D = 1$ we find a curve of positive rank, so we examine the case where $N(\delta)$ is a square in more detail. We can take δ to be a multiplicative combination of $\{2, \zeta^3 + \zeta - 1, \zeta\}$. Filtering at 2 and 5 gives that, without loss of generality, $\delta = \zeta^3 - 1, 1 - \zeta^3$. It follows that for some $y_1 \in \mathbb{Q}(\zeta)$ and $x = s/t$, we have

$$(x^5 - 1)/(x + \zeta) = 2N(\delta)/\delta y_1^2.$$

This leads to the remaining two curves. □

4.8.3. Lemma. *The $\{2,5\}$-primitive solutions to $y^2 = s^5 - 8t^5$ have $s/t = \varphi(P)$, where $\varphi : \mathcal{E}_P \to \mathbb{P}_1$ is a double cover of genus 1 over a field L and $P \in \mathcal{E}_P(L)$. It suffices to take $\mathcal{E}_8, \mathcal{E}_9$ as in Table 4.12.*

j	G_i	p	M^t	$Z(B)/p$
3	$(10+5\beta-2\beta^2-\beta^3, 20+15\beta-5\beta^2-4\beta^3)$ $(\beta^3, 0)$ $(0,0)$	41	$\begin{pmatrix} 110 \\ 0 \\ 0 \end{pmatrix}$	$\begin{pmatrix} 21 \\ 35 \\ 2 \\ 18 \end{pmatrix}$
6	$(1-3\zeta^2+3\zeta^3, 1+3\zeta-2\zeta^2+\zeta^3)$ $(1-1\zeta^2+\zeta^3, \zeta^3)$ $(2-\zeta^2+\zeta^3, 0)$ $(0,0)$	31	$\begin{pmatrix} 4 & 0 \\ 8 & 16 \\ 0 & 0 \\ 0 & 0 \end{pmatrix}$	$\begin{pmatrix} 3 & 3 \\ 12 & 29 \\ 12 & 15 \\ 0 & 17 \end{pmatrix}$
7	$(2+\zeta^2-\zeta^3, 1-\zeta-\zeta^3)$ $(-1+3\zeta^2-3\zeta^3, 1-7\zeta+8\zeta^2-4\zeta^3)$ $(2-\zeta^2+\zeta^3, 0)$ $(0,0)$	31	$\begin{pmatrix} 8 & 0 \\ 4 & 8 \\ 0 & 0 \\ 0 & 0 \end{pmatrix}$	$\begin{pmatrix} 21 & 8 \\ 2 & 2 \\ 0 & 15 \\ 22 & 27 \end{pmatrix}$
8	$(1-2\alpha+\alpha^3, 3-2\alpha^2-2\alpha^3+\alpha^4)$ $(4,2)$ $(0,0)$	151	$\begin{pmatrix} 80 & 0 \\ 0 & 20 \\ 0 & 1 \end{pmatrix}$	$\begin{pmatrix} 51 & -1 \\ 43 & -1 \\ 146 & -1 \\ 127 & -1 \\ 92 & -1 \end{pmatrix}$
9	$(1+\alpha+\alpha^2-\alpha^3+\alpha^4, 1-5\alpha+6\alpha^2-4\alpha^3+2\alpha^4)$ $(3+5\alpha+4\alpha^2+2\alpha^3, 9+13\alpha+7\alpha^2+5\alpha^3+2\alpha^4)$ $(0,0)$	151	$\begin{pmatrix} 120 & 0 \\ 120 & 720 \\ 0 & 0 \end{pmatrix}$	$\begin{pmatrix} 49 & 64 \\ 78 & 22 \\ 47 & 145 \\ 57 & 135 \\ 94 & 60 \end{pmatrix}$

Table 4.14: Curves E_j and data on the Mordell-Weil groups

Proof: Let $\alpha^5 - 2 = 0$. Then

$$X^5 - 8 = (X - \alpha^3)(X^4 + \alpha^3 X^3 + 2\alpha X^2 + 2\alpha^4 X + 4\alpha^2).$$

It follows that

$$\begin{aligned} s - \alpha^3 t &= \delta(a_0 + a_1\alpha + a_2\alpha^2 + a_3\alpha^3 + a_4\alpha^4)^2 \\ y^2 &= N(\delta)N(a_0 + a_1\alpha + a_2\alpha^2 + a_3\alpha^3 + a_4\alpha^4)^2 \end{aligned}$$

where $\delta \in L(S, 2)$. From the second equation, it follows that δ is of square norm. Since 2 and 5 completely ramify, this leaves $\delta \in \{1, \alpha - 1, 1 + \alpha + \alpha^3, \alpha^4 - \alpha^3 + \alpha^2 - 1\}$. Filtering at 2 only leaves $\delta = 1, \alpha^4 - \alpha^3 + \alpha^2 - 1$. For $x = s/t$ and some $y_1 \in \mathbb{Q}(\alpha)$ we have

$$(x^5 - 8)/(x - \alpha^3) = N(\delta)/\delta y_1^2.$$

This leads to the curves in the lemma. □

4.8.4. Lemma. *The covers $\mathcal{E}_3, \mathcal{E}_6, \ldots, \mathcal{E}_9$ in Table 4.12 are birational to the covers E_j : $\gamma Y^2 = X^3 - 5X^2 + 5X$ described in Table 4.13.*

Proof: It is straightforward to check this. □

Having established elliptic covers that parametrise $\{2,5\}$-primitive solutions in some way, we now determine their Mordell-Weil groups (up to finite index).

4.8.5. Lemma. *Let E_3 be the elliptic curve described in Table 4.14 and $L = \mathbb{Q}(\beta)$. We have $E_3^{\mathrm{tor}}(L) = \langle G_2, G_3 \rangle$. The group $\langle G_1, G_2, G_3 \rangle$ is a subgroup of odd finite index in $E_3(L)$, prime to 41. The group $\langle G_1, G_2, G_3 \rangle \bmod \mathfrak{p}_{41,i}$ spans $E_3(L) \bmod \mathfrak{p}_{41,i}$.*

Proof: The proof follows the same lines as that of Lemma 4.3.2. Let $E = E_3$. The following data give the necessary ingredients.

$$
\begin{aligned}
&\#(\langle G_1, G_2, G_3 \rangle \bmod \mathfrak{p}_{41,i} = 44, 44, 20, 20\\
&G_3' = (5 - 4\beta^3, 0); \quad G_3 = \psi'(G_3')\\
&E(L_{\mathfrak{p}_2})/\psi'(E'(L_{\mathfrak{p}_2})) = \langle G_1, G_2, (2 - \beta + \beta^2 + \beta^3, ?),\\
&\quad (-4 + 6\beta - 6\beta^2 + 6\beta^3, ?), (6 - 2\beta + 2\beta^2, ?) \rangle\\
&E'(L_{\mathfrak{p}_2})/\psi(E(L_{\mathfrak{p}_2})) = \langle G_3' \rangle\\
&E(L_{\mathfrak{p}_5}/\psi'(E'(L_{\mathfrak{p}_5})) = \langle G_1 \rangle;\ E'(L_{\mathfrak{p}_5})/\psi(E(L_{\mathfrak{p}_5})) = \langle (2\beta^2 - 2\beta^3, ?) \rangle\\
&E(\mathbb{R})/\psi'(E'(\mathbb{R})) = \{1\};\ E'(\mathbb{R})/\psi(E(\mathbb{R})) = \langle (-2\mathrm{sign}(\gamma), ?) \rangle \text{ (for all real primes)}\\
&\textstyle\bigcap_{i=1}^{4} (\langle G_1, G_2, G_3 \rangle \cap E^{(1)}(L_{\mathfrak{p}_{41,i}})) = \langle 110 G_1 \rangle
\end{aligned}
$$

See Table 4.14 for values of Z. □

4.8.6. Lemma. *Let E_6 be the elliptic curve described in Table 4.14 and $L = \mathbb{Q}(\zeta)$. We have $E_6^{\mathrm{tor}}(L) = \langle G_3, G_4 \rangle$. The group $\langle G_1, \ldots, G_4 \rangle$ is a subgroup of odd finite index in $E_6(L)$, prime to 31. The group $\langle G_1, \ldots, G_4 \rangle \bmod \mathfrak{p}_{31,i}$ spans $E_6(L) \bmod \mathfrak{p}_{31,i}$.*

Proof: The proof follows the same lines as that of Lemma 4.3.2. Let $E = E_6$ and $\mathfrak{p}_{41} \mid 41$ with $\zeta = 4 \bmod 41$. The following data give the necessary ingredients.

$$
\begin{aligned}
&\#(\langle G_1, \ldots, G_4 \rangle \bmod \mathfrak{p}_{31,i} = 32, 32, 32, 32\\
&\#(E \bmod \mathfrak{p}_{41})(\mathcal{O}/\mathfrak{p}_{41}) = 44\\
&G_4' = (-3 + 4\zeta^2 - 4\zeta^3, 0); \quad G_4 = \psi'(G_4')\\
&E(L_{\mathfrak{p}_2})/\psi'(E'(L_{\mathfrak{p}_2})) = \langle G_1, G_2, G_3, (4 - 2\zeta, ?), (4 - 2\zeta^2, ?) \rangle\\
&E'(L_{\mathfrak{p}_2})/\psi(E(L_{\mathfrak{p}_2})) = \langle G_4' \rangle\\
&E(L_{\mathfrak{p}_5}/\psi'(E'(L_{\mathfrak{p}_5})) = \langle G_4 \rangle;\ E'(L_{\mathfrak{p}_5})/\psi(E(L_{\mathfrak{p}_5})) = \langle (4 - 12\zeta^2 + 12\zeta^3, ?) \rangle\\
&\textstyle\bigcap_{i=1}^{4} (\langle G_1, \ldots, G_4 \rangle \cap E^{(1)}(L_{\mathfrak{p}_{31,i}})) = \langle 4G_1 + 8G_2, 16G_2 \rangle
\end{aligned}
$$

See Table 4.14 for values of Z. □

4.8.7. Lemma. *Let E_7 be the elliptic curve described in Table 4.14 and $L = \mathbb{Q}(\zeta)$. We have $E_7^{\mathrm{tor}}(L) = \langle G_3, G_4 \rangle$. The group $\langle G_1, \ldots, G_4 \rangle$ is a subgroup of odd finite index in $E_7(L)$, prime to 31. The group $\langle G_1, \ldots, G_4 \rangle \bmod \mathfrak{p}_{31,i}$ spans $E_7(L) \bmod \mathfrak{p}_{31,i}$.*

Proof: The proof follows the same lines as that of Lemma 4.3.2. Let $E = E_7$ and $\mathfrak{p}_{41} \mid 41$ with $\zeta = 4 \bmod 41$. The following data give the necessary ingredients.

$$\begin{aligned}
&\#(\langle G_1, \dots, G_4\rangle \bmod \mathfrak{p}_{31,i} = 32, 32, 32, 32\\
&\#(E \bmod \mathfrak{p}_{41})(\mathcal{O}/\mathfrak{p}_{41}) = 44\\
&G_4' = (-3 + 4\zeta^2 - 4\zeta^3, 0); \quad G_4 = \psi'(G_4')\\
&E(L_{\mathfrak{p}_2})/\psi'(E'(L_{\mathfrak{p}_2})) = \langle G_1, G_2, G_3, (4 + 10\zeta + 8\zeta^2 + 8\zeta^3, ?), (-4 + 2\zeta^2 + 8\zeta^3, ?)\rangle\\
&E'(L_{\mathfrak{p}_2})/\psi(E(L_{\mathfrak{p}_2})) = \langle G_4'\rangle\\
&E(L_{\mathfrak{p}_5}/\psi'(E'(L_{\mathfrak{p}_5})) = \langle G_2\rangle;\ E'(L_{\mathfrak{p}_5})/\psi(E(L_{\mathfrak{p}_5})) = \langle(-4 + 12\zeta^2 - 12\zeta^3, ?)\rangle\\
&\textstyle\bigcap_{i=1}^{4}(\langle G_1, \dots, G_4\rangle \cap E^{(1)}(L_{\mathfrak{p}_{31,i}})) = \langle 8G_1 + 4G_2, 8G_2\rangle
\end{aligned}$$

See Table 4.14 for values of Z. □

4.8.8. Lemma. *Let E_8 be the elliptic curve described in Table 4.14 and $L = \mathbb{Q}(\alpha)$. We have $E_8^{\mathrm{tor}}(L) = \langle G_3\rangle$. The group $\langle G_1, G_2, G_3\rangle$ is a subgroup of odd finite index in $E_8(L)$, prime to 151. We have $\langle G_1, G_2, G_3\rangle \bmod \mathfrak{p}_{151,i} = E_8(L) \bmod \mathfrak{p}_{151,i}$.*

Proof: The proof follows the same lines as that of Lemma 4.3.2. Let $E = E_8$ and $\mathfrak{p}_3 \mid 3$ with $\alpha = 2 \bmod \mathfrak{p}_3$. The following data give the necessary ingredients.

$$\begin{aligned}
&\#(\langle G_1, G_2, G_3\rangle \bmod \mathfrak{p}_{151,i} = 80, 80, 40, 80, 40\\
&\#(E \bmod \mathfrak{p}_3)(\mathcal{O}/\mathfrak{p}_3) = 6\\
&G_2' = (5, -20);\ G_2 = \psi'(G_2')\\
&E(L_{\mathfrak{p}_2})/\psi'(E'(L_{\mathfrak{p}_2})) = \langle G_1, G_3, (4 + 4\alpha + 12\alpha^2 + 9\alpha^4, ?), (4 + 8\alpha^2 + 18\alpha^3 + 12\alpha^4)\rangle\\
&E'(L_{\mathfrak{p}_2})/\psi(E(L_{\mathfrak{p}_2})) = \langle G_2', (3, ?), (9 + 8\alpha^2 - 22\alpha^3 + 12\alpha^4)\rangle\\
&E(L_{\mathfrak{p}_5}/\psi'(E'(L_{\mathfrak{p}_5})) = \langle G_3\rangle;\ E'(L_{\mathfrak{p}_5})/\psi(E(L_{\mathfrak{p}_5})) = \langle G_2'\rangle\\
&\textstyle\bigcap_{i=1}^{5}(\langle G_1, G_2, G_3\rangle \cap E^{(1)}(L_{\mathfrak{p}_{151,i}})) = \langle 80G_1, 20G_2 + G_3\rangle
\end{aligned}$$

See Table 4.14 for values of Z. □

4.8.9. Lemma. *Let E_9 be the elliptic curve described in Table 4.14 and $L = \mathbb{Q}(\alpha)$. We have $E_9^{\mathrm{tor}}(L) = \langle G_3\rangle$. The group $\langle G_1, G_2, G_3\rangle$ is a subgroup of odd finite index in $E_9(L)$, prime to 151. We have $\langle G_1, G_2, G_3\rangle \bmod \mathfrak{p}_{151,i} = E_9(L) \bmod \mathfrak{p}_{151,i}$.*

Proof: The proof follows the same lines as that of Lemma 4.3.2. Let $E = E_9$ and $\mathfrak{p}_3 \mid 3$ with $\alpha = 2 \bmod \mathfrak{p}_3$. The following data give the necessary ingredients.

$$\begin{aligned}
&\#(\langle G_1, G_2, G_3\rangle \bmod \mathfrak{p}_{151,i} = 144, 72, 80, 40, 80\\
&\#(E \bmod \mathfrak{p}_3)(\mathcal{O}/\mathfrak{p}_3) = 2\\
&G_2' = (1 + 8\alpha - 4\alpha^3, 8\alpha^4 - 8\alpha^3 - 4\alpha^2 - 4\alpha + 20);\ G_2 = \psi'(G_2') - G_1\\
&E(L_{\mathfrak{p}_2})/\psi'(E'(L_{\mathfrak{p}_2})) = \langle G_1, G_3, (6 - 3\alpha^2 + 3\alpha^4, ?), (5 + 3\alpha + 5\alpha^2 + 7\alpha^3 + 6\alpha^4, ?)\rangle\\
&E'(L_{\mathfrak{p}_2})/\psi(E(L_{\mathfrak{p}_2})) = \langle G_2', (0, 0), (13 + 10\alpha + 2\alpha^2 - \alpha^3 + 3\alpha^4)\rangle\\
&E(L_{\mathfrak{p}_5}/\psi'(E'(L_{\mathfrak{p}_5})) = \langle G_3\rangle;\ E'(L_{\mathfrak{p}_5})/\psi(E(L_{\mathfrak{p}_5})) = \langle(0, 0)\rangle\\
&\textstyle\bigcap_{i=1}^{5}(\langle G_1, G_2, G_3\rangle \cap E^{(1)}(L_{\mathfrak{p}_{151,i}})) = \langle 120G_1 + 120G_2, 720G_2\rangle
\end{aligned}$$

See Table 4.14 for values of Z. □

Having established knowledge of the appropriate Mordell-Weil groups, we can proceed and apply the method described in Section 4.5.

4.8.10. Proposition. $\mathcal{E}_1(\mathbb{Q}) = \{\infty^+, \infty^-\}$.

Proof: Obviously, the points mentioned are rational. It is straightforward to show that this curve is birational to the elliptic curve 400D1 in [Cre92]. This elliptic curve has only 2 rational points, which shows that the list is complete. □

4.8.11. Proposition. $\mathcal{E}_2(\mathbb{Q}) = \{(0,1),(0,-1)\}$.

Proof: Obviously, the points mentioned are rational. It is straightforward to show that this curve is birational to the elliptic curve 400F1 in [Cre92]. This elliptic curve has only 2 rational points, which shows that the list is complete. □

4.8.12. Proposition. *The points* $P \in \mathcal{E}_3(\mathbb{Q}(\beta))$ *with* $X(P) \in \mathbb{P}_1(\mathbb{Q})$ *have* $X(P) = 0$.

Proof: Similar to Proposition 4.5.3. Note that $\varphi : E_3 \to \mathbb{P}_1$ and $X : \mathcal{E}_3 \to \mathbb{P}_1$ represent the same cover. See Table 4.15 for relevant data. □

4.8.13. Proposition. *The points* $P \in \mathcal{E}_4(\mathbb{Q}(\beta))$ *with* $X(P) \in \mathbb{P}_1(\mathbb{Q})$ *have* $X(P) = 0$.

Proof: The map $(X, Y, \beta) \mapsto (-X, Y, -\beta)$ gives a map between the covers $\varphi_4 : \mathcal{E}_4 \to \mathbb{P}_1$ and $\varphi_3 : \mathcal{E}_3 \to \mathbb{P}_1$. This reduces the proposition to Proposition 4.8.12. □

4.8.14. Proposition. $\mathcal{E}_5(\mathbb{Q}) = \{\infty^+, \infty^-\}$.

Proof: Obviously, the points mentioned are rational. It is straightforward to show that this curve is birational to the elliptic curve 200D1 in [Cre92]. This elliptic curve has only 2 rational points, which shows that the list is complete. □ The next propositions are completely analogous to Proposition 4.5.3. See Table 4.15 for relevant data.

4.8.15. Proposition. *The points* $P \in \mathcal{E}_6(\mathbb{Q}(\zeta))$ *with* $X(P) \in \mathbb{P}_1(\mathbb{Q})$ *have* $X(P) = \pm 1$.

4.8.16. Proposition. *The points* $P \in \mathcal{E}_7(\mathbb{Q}(\zeta))$ *with* $X(P) \in \mathbb{P}_1(\mathbb{Q})$ *have* $X(P) \in \{1, \frac{1}{3}, 3\}$.

4.8.17. Proposition. *The points* $P \in \mathcal{E}_8(\mathbb{Q}(\alpha))$ *with* $X(P) \in \mathbb{P}_1(\mathbb{Q})$ *have* $X(P) \in \{\infty, 0, -2\}$.

4.8.18. Proposition. *The points* $P \in \mathcal{E}_9(\mathbb{Q}(\alpha))$ *with* $X(P) \in \mathbb{P}_1(\mathbb{Q})$ *have* $X(P) \in \{\infty\}$.

Proof of Theorem 1.3.4: Consider $x^2+y^4 = z^5$. Lemma 3.2.4 together with Lemma 4.8.1 show that the curves $\mathcal{E}_1, \ldots, \mathcal{E}_4$ from Table 4.12 parametrise the primitive solutions and in what way the parameter values s/t can be recovered from the points $P \in \mathcal{E}_i(L)$ with $\varphi_i(P) \in \mathbb{P}_1(\mathbb{Q})$. Propositions 4.8.10 through 4.8.13 give those points. We see all points must have $s/t = 0, \infty$, so we have that either $s = 0$ or $t = 0$ which leads to $y = 0$ or $x = 0$.

Proof of Theorem 1.3.5: Consider $x^2 - y^4 = z^5$. Lemmas 3.2.5, 4.8.2 and 4.8.3 show that $\mathcal{E}_5, \ldots, \mathcal{E}_9$ determine all possible solutions. Propositions 4.8.14 through 4.8.18 give the possible candidates and the values of s/t belonging to them. The values $s/t = \infty, 1, -1$

in Lemma 4.8.2 lead to solutions with $z = 0$, $y = 0$ or $x = 0$. The values $s/t = 3, \frac{1}{3}$ lead to $x = \pm 122, y = \pm 11, z = 3$.

The points on $\mathcal{E}_8(L)$ lead to $s/t = 1, \infty, -2$. These correspond to $(x, y, z) = (0, \pm 1, -1)$ and $(\pm 16, \pm 4, 0)$. While $(-2, 2(\alpha - \alpha^2 - \alpha^3))$ is a genuine point on $\mathcal{E}_8(L)$, we have that $\lambda(2 + \alpha^3)$ is not a square in L for any $\lambda \in \mathbb{Q}^*$. We therefore see that no rational s, t with $s/t = -2$ exist that satisfy Lemma 4.8.3. The point on $\mathcal{E}_9(L)$ leads to $(x, y, z) = (\pm 7, \pm 3, -2)$.

j	G	$\varphi(G)$	$\theta^G(n_1, \ldots, n_r)$
3	∞	∞	$41^2 \begin{pmatrix} 23n_1^2 \\ n_1^2 \\ 36n_1^2 \end{pmatrix} \bmod 41^3$
6	∞	1	$31^2 \begin{pmatrix} n_1^2 + 8n_1n_2 + 19n_2^2 \\ 27n_1^2 + 17n_1n_2^2 + 28n_2^2 \\ 8n_1^2 + 16n_1n_2 + 16n_2^2 \end{pmatrix} \bmod 31^3$
	$G_1 + G_3 + G_4$	-1	$31 \begin{pmatrix} 9n_1 + 22n_2 \\ 11n_1 + 22n_2 \\ 29n_1 \end{pmatrix} \bmod 31^2$
7	∞	1	$31^2 \begin{pmatrix} 10n_1n_2 + n_2^2 \\ 11n_1^2 + n_1n_2 + 23n_2^2 \\ 2n_1^2 + 24n_1n_2 + 24n_2^2 \end{pmatrix} \bmod 31^3$
	$G_1 + G_2 + G_4$	$\frac{1}{3}$	$31 \begin{pmatrix} 26n_1 + 22n_2 \\ 16n_1 + 18n_2 \\ 5n_1 + 14n_2 \end{pmatrix} \bmod 31^2$
	$G_1 - G_2 + G_4$	3	$31 \begin{pmatrix} 30n_1 + 5n_2 \\ 7n_1 + 10n_2 \\ 12n_1 + 29n_2 \end{pmatrix} \bmod 31^2$
8	∞	∞	$151 \begin{pmatrix} 77n_1 + 10n_2 \\ 4n_1 + 46n_2 \\ 17n_1 + 85n_2 \\ 134n_1 + 14n_2 \end{pmatrix} \bmod 151^2$
	G_2	0	$151 \begin{pmatrix} 103n_1 + 139n_2 \\ 2n_1 + 35n_2 \\ 119n_1 + 90n_2 \\ 109n_1 + 13n_2 \end{pmatrix} \bmod 151^2$
	$-2G_1$	-2	$151 \begin{pmatrix} 78n_1 + 29n_2 \\ 79n_1 + 3n_2 \\ 44n_1 + 45n_2 \\ 28n_1 + 2n_2 \end{pmatrix} \bmod 151^2$
9	∞	-1	$151 \begin{pmatrix} 147n_1 + 57n_2 \\ 31n_1 + 84n_2 \\ 16n_1 + 42n_2 \\ 24n_1 + 119n_2 \end{pmatrix} \bmod 151^2$

Table 4.15: Fibres of rational points

Chapter 5

Chabauty methods

In this chapter we place the constructions used in Sections 4.6, 4.7 and 4.8 in a wider, geometric context. We use the notion of the *jacobian variety* of a curve (see [Mil86b] or [CF96] for a more explicit treatment of the genus 2 case). In fact, we only need that it is an abelian variety (a complete, connected, non-singular variety with a geometric group law, see [Mil86a]) of dimension equal to the genus of the curve and with the same field of definition as the curve. If a curve has a point over its field of definition, then the curve can be embedded (using the Abel-Jacobi map) in its jacobian over the field of definition.

5.1 General idea

Let $\mathcal{C}$ be an algebraic curve over a number field K with a K-rational point and let $\mathcal{J}$ denote its jacobian $\mathrm{Jac}(\mathcal{C})$. Let $\mathfrak{p}$ be a finite prime of $\mathcal{O}_K$. In [Cha41], C. Chabauty proved Theorem 2.3.3 for curves that have $\mathrm{rk}(\mathrm{Jac}(\mathcal{C})(K)) < \mathrm{genus}(\mathcal{C})$. The proof is based on the fact that the $\mathfrak{p}$-adic topological closure of a finitely generated subgroup ($\mathcal{J}(K)$ in our case) of rank r in $\mathcal{J}(K_\mathfrak{p})$ has dimension $\leq r$. We write $\overline{\mathcal{J}(K)}$ for the topological closure of $\mathcal{J}(K)$ in $\mathcal{J}(K_\mathfrak{p})$. If we consider $\mathcal{C}$ (via the Abel-Jacobi embedding) as a subvariety of $\mathcal{J}$, then we have $\mathcal{C}(K) \subset \mathcal{C}(K_\mathfrak{p}) \cap \overline{\mathcal{J}(K)}$. Thus, if $\mathrm{rk}(\mathcal{J}(K)) < \mathrm{genus}(\mathcal{C})$ then we see that $\mathcal{C}(K)$ is contained in the intersection of a $\mathfrak{p}$-adic subvariety of dimension 1 and one of codimension ≥ 1. Since $\mathcal{C}(K_\mathfrak{p})$ generates $\mathcal{J}(K_\mathfrak{p})$ as a group, it cannot be contained in a subgroup. Using vanishing properties of differentials of the first kind, Chabauty proceeds to proving that $\mathcal{C}(K_\mathfrak{p})$ cannot have an analytic component in $\overline{\mathcal{J}(K)}$. It follows that the intersection is a 0-dimensional $\mathfrak{p}$-adic analytic subvariety of $\mathcal{J}(K_\mathfrak{p})$. Since $\mathcal{J}(K_\mathfrak{p})$ is compact, it follows that $\mathcal{C}(K_\mathfrak{p}) \cap \overline{\mathcal{J}(K)}$ is finite and thus that $\mathcal{C}(K)$ is finite.

The result itself is superseded by the proof of Faltings, who proved finiteness independent of $\mathrm{rk}(\mathcal{J}(K))$. However, no effective proof is known for Theorem 2.3.3 while intersections of $\mathfrak{p}$-adic varieties can be approximated effectively. This means that, if we can effectively compute on $\mathcal{J}$ (both as a group and as a $\mathfrak{p}$-adic variety), determine the subgroup $\mathcal{J}(K)$, find a point $P \in \mathcal{C}(K)$ and have $\mathrm{rk}(\mathcal{J}(K)) < \mathrm{genus}(\mathcal{C})$, then we can carry out the procedure described by Chabauty explicitly. This gives both an upper bound for $\#\mathcal{C}(K)$ and $\mathfrak{p}$-adic approximations for all elements of $\mathcal{C}(K)$.

Methods based on this idea are quite commonly referred to as *effective Chabauty methods*. For curves of genus 1 this idea is trivial, since $\mathrm{rk}(\mathcal{J}(K)) < \mathrm{genus}(\mathcal{C})$ implies that

$\mathcal{J}(K)$ is finite itself. For genus 2, there are some examples where this method has been successful. See for instance [Col85], [FPS97], [Fly97] and [Bru97].

If $\mathrm{rk}(\mathcal{J}(K))$ is high, then a different method is needed. If we have a finite number of covers $\mathcal{D}_\delta \to \mathcal{C}$ over K such that the images of $\mathcal{D}_\delta(K)$ cover $\mathcal{C}(K)$, then we can try to determine $\mathcal{D}_\delta(K)$ through the same process. In general, $\mathrm{genus}(\mathcal{D}_\delta) > \mathrm{genus}(\mathcal{C})$ and $\mathrm{rk}(\mathrm{Jac}(\mathcal{D}_\delta)(K)) \geq \mathrm{rk}(\mathrm{Jac}(\mathcal{C})(K))$. Therefore, it is possible Chabauty methods are applicable to the $\mathcal{D}_\delta$. This idea is worked out in [Wet97] for bi-elliptic curves of genus 2 and applied to a curve of rank 2.

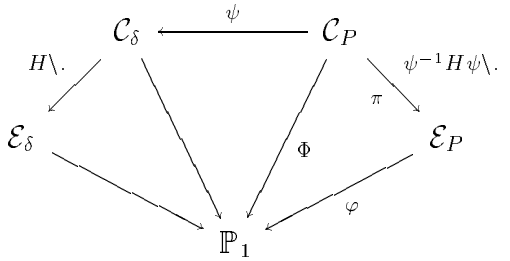
In the rest of this chapter, we show how the methods described in preceding chapters can be interpreted in terms of these ideas.

5.2 Subcovers for $F(x, y) = Dz^2$

Consider the situation of Section 3.1 with $m = 2$. In principle, Theorem 3.1.1 guarantees that primitive solutions of the equation $F(x, y) = Dz^2$ over a number field K are parametrised by a finite number of curves $\mathcal{C}_P$ over K. If the genus of those curves is > 1, in which case $\deg(F) \geq 5$, then it may be possible to determine $\mathcal{C}_P(K)$ for each of them using an effective Chabauty-method. Since the genus of $\mathcal{C}_P$ may be quite high, this would involve computations on high dimensional abelian varieties. We follow another approach.

We use the notation of Section 3.1 and we will put $n = 2$ and we write $\Phi : \mathcal{C}_P \to \mathbb{P}_1$ for the map previously denoted by $\varphi \circ \psi^{-1}$. Recall that Φ is Galois with Galois group $\langle \tau_1, \ldots, \tau_n \rangle$. Furthermore, note that $H := \langle \tau_1 \circ \tau_2, \tau_2 \circ \tau_3, \tau_5, \ldots, \tau_n \rangle$ is a normal subgroup of $\mathrm{Gal}(\mathcal{C}_\delta/\mathbb{P}_1)$ of index 2. Consequently, $\Phi : \mathcal{C}_P \to \mathbb{P}_1$ splits in $\mathcal{C}_P \to \mathcal{E}_P \xrightarrow{\varphi} \mathbb{P}_1$, induced by the map $H\backslash . : \mathcal{C}_\delta \to \mathcal{E}_\delta$. Note that this φ is different from the one in Section 3.1 and agrees with the maps φ in Sections 4.6 through 4.8. In general, dividing out a variety by a group of automorphisms gives a variety again. See [Sil86, Exercise 3.13] or [Mum70, §7]. This is quite a deep result. In this special case, observe that $H\backslash .$ is induced by the map $(Y_1 : \ldots : Y_n) \mapsto (Y_1^2 Y_4 : Y_2^2 Y_4 : Y_1 Y_2 Y_3 : Y_4^3)$, which can be seen from the fact that it is invariant under H and induces a map of degree 2^{n-1} on $\mathcal{C}_\delta$. The curve $\mathcal{E}_\delta$ is the image of $\mathcal{C}_\delta$ under this map. That the image gives a smooth model is not important for our purposes and is left to the reader.

This construction is nicely summarised in the following commutative diagram.



From degree and ramification behaviour, it follows that $\varphi : \mathcal{E}_P \to \mathbb{P}_1$ is a double cover, which is ramified exactly above $\alpha_1, \ldots, \alpha_4$. Therefore it is of genus 1 and has a model of

the form

$$\mathcal{E}_P : \gamma Y^2 = (X-\alpha_1)(X-\alpha_2)(X-\alpha_3)(X-\alpha_4) = R(X),$$

where $\varphi = X$. This model is not smooth at ∞. We denote the branches at infinity by ∞^+ and ∞^-, classified by Y/X^2. It does have good reduction at primes outside $S \cup \{2\}$ in the sense that the locally regular charts (X, Y) and $(1/X, Y/X^2)$ in reduction cover the curve with locally regular charts again.

Let $K(R)$ denote the field of definition of $R(X)$. If $\Phi(P) = X(\pi(P)) \in \mathbb{P}_1(K)$, then $\gamma Y(\pi(P))^2 \in K(R)$, the field of definition of R. Therefore, it suffices to consider only γ that are representatives of $K(R)(S, 2)$. Note that the choices of δ are absorbed in γ.

Now $P \in \mathcal{C}_P(K)$ leads to a point $G = \pi(P) \in \mathcal{E}_P(K(R))$ with $\varphi(G) = \Phi(P) \in \mathbb{P}_1(K)$. If $\mathcal{E}_P$ has a $K(R)$-rational point, then we can make it into an elliptic curve. This places us in the situation of Section 4.5.

Lemmas 4.8.1, 4.8.2 and 4.8.3 apply this procedure to some equations where $\deg(F) = 5$. In those cases, $\text{genus}(\mathcal{C}_\delta) = 5$. For a more general treatment of curves of genus 5 admitting maps to curves of genus 1, see [ACGH85, exercise section VI.F].

5.3 Multiplication-by-two cover on genus 2

We can apply the construction from Section 5.2 directly to the equation $F(X, Y) = DZ^2$ with $\deg(F) = 6$. However, by writing $F(X/Y, 1) = D(Z/Y^3)^2$, we see that solutions are in fact parametrised by a single genus 2 curve, instead of several genus 17 curves. This approach is taken in [Bru97]. Note that the curves $\mathcal{C}_7$ and $\mathcal{C}_9$ in Section 4.7 turn out to have Jacobians of rank 2 over $\mathbb{Q}$, so a Chabauty-argument cannot be applied to them directly.

In this section, we examine what the relation is between such a genus 2 curve $\mathcal{C}$ and the genus 17 curves $\mathcal{D}$. It turns out that there is a beautiful geometric construction for it. The curve $\mathcal{D}$ is a degree 16 unramified cover of $\mathcal{C}$. In [Wet97] Wetherell already constructed a degree 4 unramified cover of genus 2 curves that are a degree 2 cover of an elliptic curve over the field of definition. This construction is a generalisation of that idea and applies to any hyperelliptic curve but is only described for genus 2.

Let K be a number field and let $\mathcal{C}$ be a curve over K of genus 2, given by a model

$$\mathcal{C} : Y^2 = F(X) = f_6(X-t_1)(X-t_2)\cdots(X-t_6)$$

where $F \in \mathcal{O}_K[X]$ is a square-free polynomial of degree 5 or 6. If $\deg(F) = 5$ then we write $t_i = \infty$ for one i. The map $(X, Y) \mapsto (X, -Y)$ defines an involution on $\mathcal{C}$ and is denoted by $P \mapsto \hat{P}$. The fixed points of this involution are exactly the $T_i = (t_i, 0)$. If $\deg(F) = 5$, then we have that one of the $T_i = \infty$. Otherwise, $\mathcal{C}$ has two points corresponding to the singular point ∞ of the model, denoted by ∞^+ and ∞^-. These can be distinguished by the value of Y/X^3.

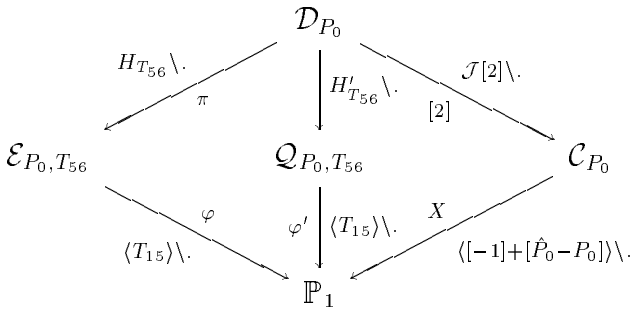
Let $\mathcal{J}$ denote the jacobian variety of $\mathcal{C}$. We fix some notation for some morphisms $\mathcal{J} \to \mathcal{J}$ as a variety. Since $\mathcal{J}$ is an abelian variety, we have that $\mathbb{Z}$ acts on $\mathcal{J}$ by multiplication. We denote this with $[n] : \mathcal{J} \to \mathcal{J}$. Any $D_0 \in \mathcal{J}(\bar{K})$ can be identified with the translation $D \mapsto D + D_0$.

We refer to [CF96] for an explanation of the arithmetic on $\mathcal{J}$. We just recall that points of $\mathcal{J}(\bar{K})$ can be represented by formal finite linear combinations $\sum_{P\in\mathcal{C}(\bar{K})} n_P P$ with $n_P \in \mathbb{Z}$ and $\sum n_P = 0$. We have that $[-1](\sum n_P P) = \sum n_P \hat{P}$. We see that the points $T_{ij} = [T_i - T_j]$ are 2-torsion points. One further relation is that $T_{12} + T_{34} + T_{56} = 0$. As a consequence, $\mathcal{J}[2](\bar{K})$ consists of 16 elements and the 15 non-zero elements give involutions $T_{ij} : \mathcal{J} \to \mathcal{J}$ given by $D \mapsto D + T_{ij}$.

Suppose we have $P_0 \in \mathcal{C}(K)$. Then we can embed $\mathcal{C}(K)$ in $\mathcal{J}(K)$ using the Abel-Jacobi map $P \mapsto [P - P_0]$. The image of this map constitutes the curve $\mathcal{C}_{P_0} \subset \mathcal{J}$. Note that the hyperelliptic involution on $\mathcal{C}_{P_0}$ is induced by $[\hat{P}_0 - P_0] \circ [-1]$.

Define $\mathcal{D}_{P_0}$ to be the inverse image of $\mathcal{C}_{P_0}$ under the [2]-map. Thus, $\mathcal{D}_{P_0}$ is an unramified degree 16 cover of a genus 2 curve which, by Theorem 2.3.2, is of genus 17. Note that $\mathcal{D}_{P_0}(K)$ need not cover the whole of $\mathcal{C}_{P_0}(K)$, since fibres of rational points might consist of conjugate points. However, $\mathcal{D}_{P_0}(K)$ certainly does cover P_0. For another point $P_1 \in \mathcal{C}(K)$, we have that $\mathcal{C}_{P_1}$ is isomorphic to $\mathcal{C}_{P_0}$ over K by the translation $[P_0 - P_1]$. Similarly, $\mathcal{D}_{P_1}$ is isomorphic to $\mathcal{D}_{P_0}$ over $\bar{K}$ via the translation over some point D such that $2D = [P_0 - P_1]$. Thus, we see that $\mathcal{D}_{P_1}$ is a twist of $\mathcal{D}_{P_0}$, classified by the class of $[P_0 - P_1]$ in $\mathcal{J}(K)/2\mathcal{J}(K)$. Since, by the Mordell-Weil theorem, $\mathcal{J}(K)$ is finitely generated, we only need a finite number of twists of $\mathcal{D}_{P_0}$ to cover all rational points of $\mathcal{C}(K)$ (this is a special case of [Wet97, Theorem 2.3.3]). Thus, the problem of determining the rational points of a genus 2 curve is transformed to finding the rational points on several curves of genus 17. This would not be progress if we did not have some additional structure.

The involution $[\hat{P}_0 - P_0] \circ [-1]$ can be pulled back under [2] to $\tau_{T_i} = [-1] + [T_i - P_0]$. Note that $\mathcal{D}_{P_0}$ comes equipped with a degree 32 cover of $\mathbb{P}_1$, namely $X \circ [2]$. This $\mathbb{P}_1$ corresponds to $\langle \mathcal{J}[2], \tau_{T_6} \rangle \backslash \mathcal{D}_{P_0}$. By factoring out subgroups of involutions, we get intermediate covers. For instance, take $H_{T_{56}} = \langle T_{12}, T_{13}, T_{14}, \tau_{T_6} \rangle$. It is straightforward to check that τ_{T_5} is also in this group and that $T_{15} \notin H_{T_{56}}$. Put $\mathcal{E}_{P_0} = \mathcal{E}_{P_0,T_{56}} = H_{T_{56}} \backslash \mathcal{D}_{P_0}$. It follows that T_{15} induces a non-trivial involution on $\mathcal{E}_{P_0}$ and that the quotient is $\langle \hat{\cdot} \rangle \backslash \mathcal{C}$. This gives a double cover $\varphi : \mathcal{E}_{P_0} \to \mathbb{P}_1$.



To determine the genus of $\mathcal{E}_{P_0}$, we look at the ramification of this double cover. It can only be ramified above the t_i's. We have that $\varphi^{-1}(\{t_i\}) = H_{T_{56}} \backslash (X \circ [2])^{-1}(\{t_i\})$. If $2D = [T_i - P_0]$, then $\tau_{T_6}(D) = D + T_{i6}$. So, for $i = 1, 2, 3, 4$ we see that $H_{T_{56}}$ works transitively on the fibre. Therefore, φ is ramified above $t_1, \ldots t_4$. By Theorem 2.3.2, $\mathcal{E}_{P_0}$ is of genus 1.

Note that we can only guarantee that $\mathcal{E}_{P_0}$ is defined over $L = K(T_{56})$ and that $\pi(\mathcal{D}_{P_0}(K)) \subset \mathcal{E}_{P_0}(L)$. However, since φ comes from factoring $X \circ [2]$, which is defined over K, we know that such points map to K-rational points under φ. Thus, we are interested in determining the set $\mathbb{P}_1(K) \cap \varphi(\mathcal{E}_{P_0}(L))$. Taking X^{-1} of this set gives a superset of $C_{P_0}(K) \cap [2](\mathcal{D}_{P_0}(K))$.

In order to make this procedure effective, we have to determine which twists of $\mathcal{E}_{P_0}$ we need. The ramification information of φ completely determines the geometry of $\mathcal{E}_{P_0}$. A double cover of the projective line, ramified above t_1, t_2, t_3, t_4 is of the form

$$\mathcal{E}_\delta : \delta Y_1^2 = R_{T_{56}}(X) = (X - t_1)(X - t_2)(X - t_3)(X - t_4).$$

where $\delta = \delta_{P_0}$ represents an element of $L^*/(L^*)^2$, depending on P_0. We can identify $X : \mathcal{E}_\delta \to \mathbb{P}_1$ with φ.

If we repeat this procedure with $H'_{T_{56}} = \langle T_{12}, T_{13}, T_{14}, \tau_{T_1} \rangle$, we get a double cover of $\mathbb{P}_1$ that is ramified above t_5, t_6. By Theorem 2.3.2, it is of genus 0 and has a model of the form

$$\mathcal{Q}_{\delta'} : \delta' Y_2^2 = Q_{T_{56}}(X) = f_6(X - t_5)(X - t_6).$$

Again, $X : \mathcal{Q}_{\delta'} \to \mathbb{P}_1$ is the double cover of $\mathbb{P}_1$ induced by $X \circ [2]$ on $\mathcal{D}_{P_0}$.

Note that $F(X) = Q_{T_{56}}(X) R_{T_{56}}(X)$, so for a point $P \in \mathcal{C}(K)$ covered by $\mathcal{D}_{P_0}(K)$ we have a $\delta = \delta_{P_0}$ and a pair of points $(X(P), Y_1) \in \mathcal{E}_\delta(L)$ and $(X(P), Y_2) \in \mathcal{Q}_{\delta'}(L)$ with $Y(P)^2 = \delta\delta' Y_1^2 Y_2^2$. It follows that if $\mathcal{D}_{P_0}(K)$ is non-empty, then δ' should represent the same class as δ_{P_0}. So without loss of generality, we can put $\delta' = \delta_{P_0}$ and we have $Y(P) = \pm\delta Y_1 Y_2$.

The point P_0 is certainly covered by $\mathcal{D}_{P_0}(K)$. Therefore, δ_{P_0} should represent the quadratic class of $R_{T_{56}}(X(P_0))$. For $X(P_0) \in \{t_1, \ldots, t_4\}$, we can determine δ_{P_0} by noticing that δ_{P_0} should also represent the quadratic class of $Q_{T_{56}}(X(P_0))$. It follows that δ_{P_0} will be a square locally at primes where $\mathrm{disc}(F)$ is a unit. Therefore δ_{P_0} is a representative of the finite set $L(S, 2)$, where S is the set of primes dividing $\mathrm{disc}(F)$.

Twists of $\mathcal{E}_\delta$ that have points that correspond to K-rational points of $\mathcal{C}$ are called *productive*. To narrow down the number of $\mathcal{E}_\delta$ that might be productive, we can proceed in the following manner. We let δ run through a set of representatives of $L(S, 2)$, choose a prime p of K together with a prime $\mathfrak{p} \mid p$ of L and see whether there exist $X \in K_p$ such that $R_{T_{56}}(X), Q_{T_{56}}(X) \in \delta \cdot (L_\mathfrak{p}^*)^2 \cup \{0\}$. If representatives of $\mathcal{J}(K)/2\mathcal{J}(K)$ are available, then they can give information that helps to reduce the number of candidates for δ as well.

Now we are again in the situation where we have a finite number of degree 2 elliptic covers $\varphi : E \to \mathbb{P}^1$ over a number field L such that for any point $P \in \mathcal{C}(K)$ there is one such cover and a point $G \in E(L)$ such that $\varphi(G) = X(P)$. We are thus led to determine the L-rational points of E with K-rational image under φ. This is discussed in Section 4.5.

5.4 Weil restriction

In both Sections 5.2 and 5.3 we get a cover $\Phi : \mathcal{C} \to \mathbb{P}_1$ over a number field K that splits as $\mathcal{C} \xrightarrow{\pi} \mathcal{E} \xrightarrow{\varphi} \mathbb{P}_1$ over an extension L. In Section 4.5 we deal with the problem of determining

$\mathcal{C}(K)$ in the following way. We observe that $\Phi(\mathcal{C}(K)) = \varphi(\mathcal{E}(L)) \cap \mathbb{P}_1(K)$ and we determine the latter. We refer to this method as a Chabauty-style argument. In this section we briefly sketch why this is justified.

Let E be an elliptic curve over a number field L and let K be a subfield. We need the Weil restriction of E from L to K. For affine objects, one obtains the Weil restriction by writing out the equations and variables with respect to a K-basis of L. See [BLR90, §7.6] for a proper definition. Let $\mathcal{A}$ denote the Weil-restriction of E from L to K. Then, [BLR90, Proposition 7.6.5] assures that $\mathcal{A}$ is a smooth complete variety such that $\mathcal{A}(K) \cong E(L)$ as sets. The group law on E induces a group law on $\mathcal{A}$ (over K), which implies that $\mathcal{A}(K) \cong E(L)$ as groups. For $\mathcal{A}$ to be an abelian variety, it should be geometrically connected. This follows from the fact that, as varieties over $\bar{L}$, $\mathcal{A}$ is covered by $E \times \cdots \times E$ ($[L : K]$ times). The latter is connected since it is connected over $\mathbb{C}$.

The map $\pi : \mathcal{C} \to E$ induces a map $\mathcal{C} \to \mathcal{A}$ over K (also denoted by π). This is the situation of a Chabauty argument. If p is a prime of $\mathcal{O}_K$, and $\pi(\mathcal{C}(K_p))$ and the p-adic closure of $\mathcal{A}(K)$ do not share a component of dimension 1, then $\pi(\mathcal{C}(K_p)) \cap \overline{\mathcal{A}(K)}$ is finite (because $\mathcal{A}(K_p)$ is compact).

When constructing the power series θ in Section 4.5, we do in fact write out $\mathcal{C} \xrightarrow{\pi} \mathcal{E} \xrightarrow{\varphi} \mathbb{P}_1$ with respect to a K-basis of L locally. It is just convenient to do most computations on E over L instead of on $\mathcal{A}$ over K, since with the current state of computational machinery, simple geometry over a field with complicated arithmetic is to be preferred over complicated geometry over a field with simple arithmetic.

That we work with $\varphi : E \to \mathbb{P}_1$ instead of $\pi : \mathcal{C} \to E$ is just because $\deg(\varphi) = 2$ and we have a fairly complete description of such covers in Section 4.4. In other situations, it may be preferable to work with $\pi : \mathcal{C} \to E$. In that case, one is interested in those $G \in E(L)$ such that $\pi^{-1}(\{G\})$ hits $\mathcal{C}(K)$. One may proceed in the following way. Choose a $P_0 \in \mathcal{C}(K_p)$ and a local map $z \mapsto P(z)$ that parametrises the p-adic neighbourhood of P_0 (i.e. $P(p\mathcal{O}_p)$ is the part of $\mathcal{C}(K_p)$ that reduces to $P_0 \bmod p$). Then $\pi(P(z)) - \pi(P_0) \in E^{(1)}(L_\mathfrak{p})$ for all $\mathfrak{p} \mid p$ and $z \in p\mathcal{O}_p$. Given that $E(L) \cap E^{(1)}(L_\mathfrak{p}) = \langle B_1, \ldots, B_r \rangle$ and $\pi(P_0) \in E(L)$, it follows that if $\pi(P(z)) \in E(L)$, then there are $n_1, \ldots, n_r \in \mathbb{Z}$ such that $\mathrm{Log}_\mathfrak{p}(\pi(P(z)) - \pi(P_0)) - n_1 \mathrm{Log}_\mathfrak{p}(B_1) - \cdots - n_r \mathrm{Log}_\mathfrak{p}(B_r) = 0$ for all $\mathfrak{p} \mid p$. The number of such $z, n_1, \ldots, n_r$ can be bounded using the same techniques as in Lemma 4.5.2.

Appendix A

Algorithms

A.1 Computations in local fields

In this text, we frequently used that if a variety has a point over a number field K, then it also has points over localisations $K_\mathfrak{p}$. Whether a variety has a point over a local field is a question which is easier to answer. In this chapter we describe how. Note that if $\mathfrak{p}$ is an infinite prime, then $K_\mathfrak{p} = \mathbb{R}$ or $K_\mathfrak{p} = \mathbb{C}$. Since $\mathbb{C}$ is algebraically closed, any non-trivial variety will have points over $\mathbb{C}$. For $\mathbb{R}$, it is also quite easy to find points, or show that there are none. We will not deal with these cases here, so we assume that $\mathfrak{p} \mid p$ for some prime p of $\mathbb{Z}$.

Suppose that $K = \mathbb{Q}(\alpha)$, where α is a zero of a given monic irreducible polynomial $F(X) \in \mathbb{Z}[X]$. Let the prime $\mathfrak{p}$ be given as an ideal of $\mathcal{O}_K$. Note that for any $x \in K_\mathfrak{p}^*$, we have $x/u_\mathfrak{p}^{\nu_\mathfrak{p}(x)} \in \mathcal{O}_\mathfrak{p}^*$. Therefore, we can approximate elements in $K_\mathfrak{p}^*$ by elements

$$(v, \tilde{x}) \in \mathbb{Z} \times (\mathcal{O}_\mathfrak{p}/(\mathfrak{p}\mathcal{O}_\mathfrak{p})^e)^* = \mathbb{Z} \times (\mathcal{O}/\mathfrak{p}^e)^*$$

such that $x = u_\mathfrak{p}^e \tilde{x} \bmod \mathfrak{p}^{v+e}$. Representation of 0 is not very difficult either.

Since $(\mathcal{O}/\mathfrak{p}^e)^*$ is a finite abelian group, it is isomorphic to a product of cyclic groups, of sizes $m_1, \ldots, m_t$, say. The map

$$\mu_{\mathfrak{p}^e} : (\mathcal{O}/\mathfrak{p}^e)^* \xrightarrow{\sim} \mathbb{Z}/m_1\mathbb{Z} \times \cdots \times \mathbb{Z}/m_t\mathbb{Z}$$

is effectively computable. It is available as EltRayResidueRingRep in KASH (see [DFK+97]) and as IdealLog in PARI-GP (see [BBB+]).

The map $\bar{\mu}_{\mathfrak{p}^e}$ defined by taking every component of $\mu_{\mathfrak{p}^e}$ modulo $\gcd(2, m_i)$ clearly has $((\mathcal{O}_\mathfrak{p}^e)^*)^2$ as kernel. Let c denote the number of m_i that are divisible by 2. To determine if $x \in K$ is a $\mathfrak{p}$-adic square, it is sufficient to test if $v = \nu_\mathfrak{p}(x) = 0 \bmod 2$ and if $\bar{\mu}_{\mathfrak{p}^{\nu_\mathfrak{p}(4)+1}}(x) = 0$. Thus

$$\begin{array}{rcl} K_\mathfrak{p}^*/(K_\mathfrak{p}^*)^2 & \to & \mathbb{F}_2 \oplus (\mathbb{F}_2)^c \\ x & \mapsto & \left(\nu_\mathfrak{p}(x) \bmod 2, \bar{\mu}_{\mathfrak{p}^{\nu_\mathfrak{p}(4)+1}}\left(x/u_\mathfrak{p}^{\nu_\mathfrak{p}(x)}\right)\right) \end{array}$$

is a group isomorphism. Note that if $x \in \mathcal{O}_\mathfrak{p}^*$, $e > \nu_\mathfrak{p}(4)$, then by Newton approximation, we have that $x \in (\mathcal{O}_\mathfrak{p}^*)^2$ if and only if $x \bmod \mathfrak{p}^e = y^2 \bmod \mathfrak{p}^e$ for some $y \in \mathcal{O}_\mathfrak{p}^*$.

A.2 Proving local unsolvability

Let $I = (F_1, \ldots, F_m) \subset \mathcal{O}_K[X_0, \ldots, X_n]$ be a homogeneously generated ideal, let $\mathfrak{p}$ be a prime of $\mathcal{O}$ and let R be a set of representatives of $\mathcal{O}/\mathfrak{p}$ in $\mathcal{O}$. In this section we present a little algorithm that tests if the variety determined by I has no points over $K_\mathfrak{p}$.

Test($\mathfrak{p}, I, (y_0, \ldots, y_n), e, B$):

1. If $F_i(y_0, \ldots, y_n) \bmod \mathfrak{p}^e \neq 0$ for any $i \in \{1, \ldots, m\}$ then return($true$).
2. else if $e \geq B$ then return($false$).
3. else for all $(x_0, \ldots, x_n) \in R \times \cdots \times R$ do
4. if Test($\mathfrak{p}, I, (y_0 + u_\mathfrak{p}^e x_0, \ldots, y_n + u_\mathfrak{p}^e x_n), e+1, B) = false$ then return($false$)
5. if done with for then return($true$).

HasNoLocalPoint($\mathfrak{p}, I, B$):

1. for all $(y_0, \ldots, y_n) \in \{1\} \times R \times \cdots \times R \cup \cdots \cup \{(0, \ldots, 0, 1)\}$ do
2. if Test($\mathfrak{p}, I, (y_0, \ldots, y_n), 1, B) = false$ then return($unknown$)
3. if done with for then return($true$)

If HasNoLocalPoint returns $true$ for some value of B, then the variety described by I does not have points over $K_\mathfrak{p}$ since $\mathbb{P}_n(\mathcal{O}_\mathfrak{p}) = \mathbb{P}_n(K_\mathfrak{p})$. By Hensel's lemma, there is a value for B, effectively computable from I, such that, if $unknown$ is returned for that value, then in fact I does have a point over $K_\mathfrak{p}$. For hyperelliptic curves, we can use this idea to make a more efficient algorithm. Let $F \in \mathcal{O}_K[X]$ be a square free polynomial (not necessarily monic). Consider the curve $\mathcal{C} : Y^2 = F(X)$. If $\deg(F)$ is odd or F has a zero over $K_\mathfrak{p}$, then $\mathcal{C}$ certainly has a point over $K_\mathfrak{p}$, so we assume this is not the case. Note that, if $\mathcal{C}$ has a $K_\mathfrak{p}$-valued point, then one of $Y^2 = F(X)$ and $Y^2 = X^{\deg(F)}F(1/X)$ has a solution with $X \in \mathcal{O}_\mathfrak{p}$. Therefore, it is enough to consider only points with integral X.

HasLocalPointWithIntX($\mathfrak{p}, F, x_0, e$):

1. $v := \nu_\mathfrak{p}(F(x_0))$.
2. if $v < e$ and $v \bmod 2 \neq 0$ then return($false$)
3. else if $v < e$ and $\bar{\mu}_{\mathfrak{p}^{e-v}}(F(x_0)/u_\mathfrak{p}^v) \neq 0$ then return($false$)
4. else if $e - v > \nu_\mathfrak{p}(4)$ then return(x_0)
5. else for all $x_1 \in R$ do
6. $t :=$ HasLocalPointWithIntX($\mathfrak{p}, F, x_0 + u_\mathfrak{p}^e x_1, e+1$)
7. if $t \neq false$ then return(t)
8. if done with for then return($false$)

If HasLocalPointWithIntX($\mathfrak{p}, F(X), 0, 0$) returns $false$, then $\mathcal{C}$ has no $K_\mathfrak{p}$ with $X \in \mathcal{O}_\mathfrak{p}$, otherwise it returns an $x \in \mathcal{O}$ for which $F(x)$ is a square in $K_\mathfrak{p}$. To search for non-integral X it suffices to call HasLocalPointWithIntX($\mathfrak{p}, X^{\deg(F)}F(1/X), 0, 1$).

In line 3 we use that $x \bmod \mathfrak{p}^e$ determines the value of $F(x) \bmod \mathfrak{p}^e$. For specific F we can do better. For instance, for descents as described in Section 4.3 we often need to search for local points on $Y^2 = F(X) = f_0X^4 + f_2X^2 + f_4$. As is easily checked, for $x_0, x_1 \in \mathcal{O}_\mathfrak{p}$ we have

$$\nu_\mathfrak{p}(F(x_0) - F(x_0 + u_\mathfrak{p}^e x_1)) \geq e + \min\{\nu_\mathfrak{p}(4f_0), \nu_\mathfrak{p}(6f_0) + e, \nu_\mathfrak{p}(f_0) + 3e, \nu_\mathfrak{p}(2f_2), \nu_\mathfrak{p}(f_2) + e\}$$

which is better if $\mathfrak{p} \mid 2$, especially if it is highly ramified.

Furthermore, in Section 5.2, we want to test if there are local solutions to $Y^2 = F(X)$ with *rational* X. Let p be the prime of $\mathbb{Z}$ below $\mathfrak{p}$. Instead of taking R to be representatives of $\mathcal{O}/\mathfrak{p}$, we take R to represent $\mathbb{Z}/p$. In line 6, we can replace $e + 1$ by $e + \nu_\mathfrak{p}(p)$.

A.3 Sieving for rational points

In Section 4.3 we described how to bound the rank of an elliptic curve over a number field, but we did not say how generators may be found. There is no efficient solution for this and especially if we want generators of a curve over a number field of high degree, then searching for points can be a difficult task. In this section we present an algorithm which does not improve theoretically on brute force searching, but is very efficient to implement.

Let K be a number field of degree n over $\mathbb{Q}$ and let $b_1, \ldots, b_n$ be a $\mathbb{Z}$-basis of $\mathcal{O}_K$. Consider a hyperelliptic curve $\mathcal{C} : Y^2 = F(X)$, with $F \in \mathcal{O}_K[X]$. We present an algorithm that searches for rational points with integral X-coordinate. To search for points with non-integral X with prescribed denominator, just rewrite the model of $\mathcal{C}$. We select N primes $\mathfrak{p}_1, \ldots, \mathfrak{p}_N$ of $\mathcal{O}_K$ above rational primes $p_1, \ldots, p_N$ unequal to 2 such that $\mathcal{O}/\mathfrak{p}_i = \mathbb{F}_{p_i}$. We use the property that if $x, y \in \mathcal{O}_K$ such that $y^2 = F(x)$, then $F(x) \bmod \mathfrak{p}_i$ is a square in $\mathbb{F}_{p_i}$.

Sieve($F, b_1, \ldots, b_n, \mathfrak{p}_1, \ldots, \mathfrak{p}_N, B$):

1. for $i = 1, \ldots, N$ do
2. $\quad F_i := F \bmod \mathfrak{p}_i \in \mathbb{F}_{p_i}[X]$
3. $\quad$ for all $x \in \mathbb{F}_{p_i}$ do
4. $\quad\quad$ if $\sqrt{F_i(x)} \in \mathbb{F}_{\mathfrak{p}_i}$ then $V_i[x] = \mathit{true}$ else $V_i[x] = \mathit{false}$
5. $\quad$ for $j = 1, \ldots, n$ do $b_j^{(i)} := b_j \bmod \mathfrak{p}_i \in \mathbb{F}_{p_i}$
6. for all $(c_1, \ldots, c_n) \in \{-B, \ldots, B\} \times \cdots \times \{-B, \ldots, B\}$ do
7. $\quad f := \mathit{true}$
8. $\quad$ for $i = 1, \ldots, N$ do
9. $\quad\quad$ if $V_i\left[\sum_{j=1}^n c_j b_j^{(i)}\right] = \mathit{false}$ then $f := \mathit{false}$; goto 10
10. $\quad$ if $f = \mathit{true}$ then report$(c_1b_1 + \cdots + c_nb_n)$

Note that, if N is large, i.e. $2^N > (2B+1)^n$, then it is likely that a reported x-coordinate does indeed belong to a rational point, which may be checked by factoring $Y^2 - F(x)$ over

$\mathcal{O}_K$. It is clearly a good idea to first test at primes $\mathfrak{p}_i$ for which it is unlikely that $F_i(x)$ is a square. Thus, the $\mathfrak{p}_i$ should be ordered such that $\#\{x \in \mathbb{F}_{p_i} : V_i[x] = true\}/p_i$ increases with i. Furthermore, each time line 9 is executed, we need to compute n multiplications and $n-1$ additions in $\mathbb{F}_{p_i}$ to determine the index in V_{p_i}. This can be quite expensive. Note that indices belonging to consecutive vectors $(c_1, \ldots, c_n)$ have a difference of $b_1^{(i)}$ or $b_{j+1}^{(i)} - 2Bb_j^{(i)}$. It is a great time saver to precompute these differences for small i ($i < C$, say) and update $\sum_{j=1}^{n} c_j b_j^{(i)}$ for every candidate. This will cost (apart from a lookup of the appropriate increment) only one addition in $\mathbb{F}_{p_i}$. This cost will be made for *every* candidate though, regardless of whether the candidate was already shown not to be the X of a rational point due to other primes. Heuristically, the i-th prime will be used once every 2^{i-1} candidates. The optimal value of C depends on n and the relative cost of multiplication.

A.4 Electronic verification

Many of the proofs in Chapter 4 require computations that are extensive to represent on paper. To facilitate the verification of those calculations (and to help people who want to do this kind of calculations themselves), the author developed a computer package that automates these computations to a considerable degree. The files are packaged as "thesis.sh" and can be found in the preprint archive of the Mathematical Institute of Leiden University as "W99-14.sh", accompanying [Bru99]. Alternatively, the reader can consult the home-page of the author (no permanent address can be given) or contact the author directly.

The package is written for use with KASH 2.0, a freely available shell for the KANT library (see [DFK+97]). Any future user should make sure that KASH is available to him or her. The package consists of the following files

index.txt a file describing the contents of the package

matalg.g linear algebra extension to the standard functions

array.g arbitrary dimensional arrays

domain.g functions facilitating writing generic code

latcalc.g functions to work with sublattices of $\mathbb{Z}^r$

loccalc.g finite precision arithmetic in localisations of number fields

ellcalc.g basic arithmetic of elliptic curves over number fields as well as Chabauty method as described in Section 4.5

isogdesc.g 2-isogeny descent on elliptic curve over number field as described in Section 4.3

eq283E2.g computations for 4.3.2 and 4.5.3

eq283E4.g computations for 4.6.7 and 4.6.10

eq283E7.g computations for 4.6.8 and 4.6.11

eq238E5.g computations for 4.7.3 and 4.7.10

eq238E7.g computations for 4.7.4 and 4.7.12

eq238E9.g computations for 4.7.5 and 4.7.14

eq245E3.g computations for 4.8.5 and 4.8.12

eq245E6.g computations for 4.8.6 and 4.8.15

eq245E7.g computations for 4.8.7 and 4.8.16

eq245E8.g computations for 4.8.8 and 4.8.17

eq245E9.g computations for 4.8.9 and 4.8.18

powseries.mpl Maple V script for computing the approximations given in Section 4.4

sieve.c C source of a program called from the Sieve implementation in loccalc.g.

The algorithms HasLocalPointWithIntX (also with the modification for *rational* integer X) and Sieve are implemented in loccalc.g. Therefore, the proofs of lemmas like Lemma 4.6.4 can be checked quite easily using these routines. The proof of for instance Lemma 4.8.4 is a straightforward exercise in algebra. A particularly convenient description of the construction used for obtaining a Weierstrass model from a quartic model can be found in [Cas91].

Bibliography

[ACGH85] E. Arbarello, M. Cornalba, P. A. Griffiths, and J. Harris. *Geometry of algebraic curves. Vol. I.* Springer-Verlag, New York, 1985.

[BBB+] C. Batut, K. Belabas, D. Bernardi, H. Cohen, and M. Olivier. PARI-GP. Available from `ftp://megrez.math.u-bordeaux.fr/pub/pari`.

[Beu98] Frits Beukers. The Diophantine equation $Ax^p + By^q = Cz^r$. *Duke Math. J.*, 91:61–88, 1998.

[BLR90] Siegfried Bosch, Werner Lütkebohmert, and Michel Raynaud. *Néron models.* Springer-Verlag, Berlin, 1990.

[Bom90] Enrico Bombieri. The Mordell conjecture revisited. *Ann. Scuola Norm. Sup. Pisa Cl. Sci. (4)*, 17:615–640, 1990.

[Bru97] Nils Bruin. The diophantine equations $x^2 \pm y^4 = \pm z^6$ and $x^2 + y^8 = z^3$. Technical Report W97-21, University of Leiden, 1997. To appear in Compositio Math.

[Bru99] Nils Bruin. Chabauty methods using elliptic curves. Technical Report W99-14, University of Leiden, 1999.

[Cas91] J. W. S. Cassels. *Lectures on Elliptic Curves.* LMS-ST 24. University Press, Cambridge, 1991.

[CF96] J.W.S. Cassels and E.V. Flynn. *Prolegomena to a Middlebrow Arithmetic of Curves of Genus 2.* LMS–LNS 230. Cambridge University Press, Cambridge, 1996.

[Cha41] Claude Chabauty. Sur les points rationnels des variétés algébriques dont l'irrégularité est supérieure à la dimension. *C. R. Acad. Sci. Paris*, 212:1022–1024, 1941.

[Col85] Robert F. Coleman. Effective Chabauty. *Duke Math. J.*, 52:765–770, 1985.

[Cre92] J.E. Cremona. *Algorithms for Modular Elliptic Curves.* Cambridge University Press, 1992.

[DFK+97] M. Daberkow, C. Fieker, J. Klüners, M. Pohst, K. Roegner, M. Schörnig, and K. Wildanger. KANT V4. *J. Symbolic Comput.*, 24:267–283, 1997. Available from `ftp://ftp.math.tu-berlin.de/pub/algebra/Kant/Kash`.

[DG95] Henri Darmon and Andrew Granville. On the equations $z^m = F(x, y)$ and $Ax^p + By^q = Cz^r$. *Bull. London Math. Soc.*, 27:513–543, 1995.

[DM97] Henri Darmon and Loïc Merel. Winding quotients and some variants of Fermat's last theorem. *J. Reine Angew. Math.*, 490:81–100, 1997.

[Fal83] G. Faltings. Endlichkeitssätze für abelsche Varietäten über Zahlkörpern. *Invent. Math.*, 73:349–366, 1983.

[Fal84] G. Faltings. Erratum: "Finiteness theorems for abelian varieties over number fields". *Invent. Math.*, 75:381, 1984.

[Fly97] E.V. Flynn. A flexible method for applying Chabauty's theorem. *Compositio Math.*, 105:79–94, 1997.

[FPS97] E. V. Flynn, Bjorn Poonen, and Edward F. Schaefer. Cycles of quadratic polynomials and rational points on a genus-2 curve. *Duke Math. J.*, 90:435–463, 1997.

[Har77] Robin Hartshorne. *Algebraic Geometry.* GTM 52. Springer-Verlag, 1977.

[Lan65] Serge Lang. *Algebra.* Addison-Wesley, Reading, Mass., 1965.

[Mau97] R. Daniel Mauldin. A generalization of Fermat's last theorem: the Beal conjecture and prize problem. *Notices Amer. Math. Soc.*, 44:1436–1437, 1997.

[Mil86a] J. S. Milne. Abelian varieties. In *Arithmetic geometry (Storrs, Conn., 1984)*, pages 103–150. Springer, New York, 1986. Eds. G. Cornell and J.H. Silverman.

[Mil86b] J. S. Milne. Jacobian varieties. In *Arithmetic geometry (Storrs, Conn., 1984)*, pages 167–212. Springer, New York, 1986. Eds. G. Cornell and J.H. Silverman.

[Mum70] David Mumford. *Abelian varieties.* Tata Institute of Fundamental Research, Bombay, 1970.

[Poo98] Bjorn Poonen. Some Diophantine equations of the form $x^n + y^n = z^m$. *Acta Arith.*, 86:193–205, 1998.

[Rib97] Kenneth A. Ribet. On the equation $a^p + 2^\alpha b^p + c^p = 0$. *Acta Arith.*, 79:7–16, 1997.

[Ser79] Jean-Pierre Serre. *Local fields.* Springer-Verlag, New York, 1979.

[Sil86] Joseph H. Silverman. *The Arithmetic of Elliptic Curves*. GTM 106. Springer-Verlag, 1986.

[Thi96] Steve Thiboutot. Courbes elliptiques, représentations galoisiennes et l'équation $x^2 + y^3 = z^5$. Master's thesis, Université McGill, Montréal, 1996.

[Tij89] R. Tijdeman. Diophantine equations and Diophantine approximations. In *Number theory and applications (Banff, AB, 1988)*, pages 215–243. Kluwer Acad. Publ., Dordrecht, 1989.

[Wet97] Joseph L. Wetherell. *Bounding the number of rational points on certain curves of high rank*. PhD thesis, U.C. Berkeley, 1997.

[Wil95] Andrew Wiles. Modular elliptic curves and Fermat's last theorem. *Ann. of Math. (2)*, 141:443–551, 1995.

Samenvatting

Chabauty-methoden en overdekkingstechnieken toegepast op gegeneraliseerde Fermat-vergelijkingen

Al in de klassieke oudheid werden bijzondere eigenschappen van getallen bestudeerd. De Pythagoreeërs (ong. 400 v.C.) kenden al oneindig veel oplossingen van $x^2 + y^2 = z^2$ in gehele getallen, in de vorm van rechthoekige driehoeken waarvan alle zijden een gehele lengte hebben. Een van de meest invloedrijke werken in de getaltheorie is *Arithmetica* van Diophantus (ong. 250 n.C.). In dit boek worden vragen behandeld over vergelijkingen in positieve gebroken getallen. Eén van de vragen die hij beschouwt, is of een gegeven kwadraat te schrijven is als de som van twee andere kwadraten. Hij slaagt erin om dit voor een voorbeeld te doen. Het is bij deze vraag dat Pierre de Fermat (1601-1665) een kanttekening maakte over de vraag of de som van twee hogere machten weer eenzelfde macht kan zijn. Vertaald in moderne notatie, beschouwde hij de vraag of er voor $n \geq 3$ oplossingen zijn van

$$x^n + y^n = z^n, \quad x, y, z \in \mathbb{Z}_{>0}.$$

Hij beweerde dat er geen oplossingen zijn, maar gaf daar geen bewijs voor. Het heeft tot 1995 geduurd totdat Wiles met hulp van Taylor bewees dat Fermat gelijk had.

De grote hoeveelheid wiskundige literatuur die geïnspireerd is door Fermat's bewering en de opzienbarende strukturen die daarin zijn blootgelegd, geven aan dat dit soort vergelijkingen raken aan het wezen van de gehele getallen. Het ligt dan ook voor de hand om een meer algemene vergelijking te beschouwen, de *gegeneraliseerde Fermat-vergelijking*

$$x^r + y^s = z^t, \quad r, s, t \in \mathbb{Z}_{>1}, \quad x, y, z \in \mathbb{Z}_{>0}, \quad \mathrm{ggd}(x, y, z) = 1.$$

Specifieke gevallen zijn al veel vroeger beschouwd.

Het blijkt dat de struktuur van de oplossingsverzameling van deze vergelijking voor gegeven r, s, t voornamelijk wordt geregeerd door de grootheid $\chi = 1/r + 1/s + 1/t$. Als $\chi > 1$, dan zijn er oneindig veel oplossingen. In al deze gevallen, behalve $x^2 + y^3 = z^5$, beschikken we over een bevredigende beschrijving van de oplossingsverzameling, dankzij het werk van Darmon en Granville en Beukers en Zagier. Deze resultaten worden in hoofdstuk 3 van dit proefschrift beschreven.

Voor $\chi = 1$ blijken er helemaal geen oplossingen te zijn. Voor $\chi < 1$ hebben Darmon en Granville bewezen dat er maar eindig veel oplossingen zijn. Wiskundigen vermoeden zelfs dat alle oplossingsverzamelingen voor deze gevallen samengenomen slechts een eindige

verzameling vormen. We weten echter wel dat dit *geen* lege verzameling is. We kennen (dankzij Beukers en Zagier) de volgende oplossingen:

$$\begin{array}{rcl@{\quad}rcl} 1^r + 2^3 &=& 3^2 & (r > 6) & 17^7 + 76271^3 &=& 21063928^2 \\ 13^2 + 7^3 &=& 2^9 & & 1414^3 + 2213459^2 &=& 65^7 \\ 2^7 + 17^3 &=& 71^2 & & 33^8 + 1549034^2 &=& 15613^3 \\ 2^5 + 7^2 &=& 3^4 & & 43^8 + 96222^3 &=& 30042907^2 \\ 3^5 + 11^4 &=& 122^2 & & 9262^3 + 15312283^2 &=& 113^7. \end{array}$$

Het is interessant om te weten of er nog meer voorbeelden aan de lijst kunnen worden toegevoegd. Als deelprobleem kan men zich afvragen of er nog meer voorbeelden zijn voor de gegeven waarden (r, s, t) die in de tabel voorkomen. In Hoofdstuk 4 van dit proefschrift wordt bewezen dat de vergelijkingen $x^2 \pm y^8 = z^3$, $x^2 \pm y^4 = z^5$ en $x^2 \pm y^4 = \pm z^6$ geen primitieve oplossingen hebben buiten de oplossingen die in de bovenstaande lijst staan.

De oplossingsmethode bestaat uit het concreet maken van de abstracte methode die Darmon en Granville gebruiken om eindigheid van het aantal oplossingen vast te stellen. Zij bewijzen dat oplossingen in correspondentie staan met zogenaamde *rationale punten op algebraïsche krommen*. Eerst bewijzen ze dat er maar eindig veel van dat soort krommen nodig zijn en vervolgens laten ze zien dat die krommen van een bijzonder type zijn: ze zijn van *geslacht* ≥ 2. Zulke krommen hebben, zoals Faltings in 1984 bewees, slechts eindig veel rationale punten.

De eerste stap is de krommen expliciet te bepalen. Daartoe worden in Hoofdstuk 4 de technieken uit Hoofdstuk 3 toegepast. Hierbij dient wel opgemerkt te worden dat deze niet in alle gevallen werken (bijvoorbeeld voor $x^2 + y^3 = z^7$). Vervolgens moet voor ieder van die krommen aangetoond worden dat daarop geen andere rationale punten liggen dan welke corresponderen met bekende oplossingen. Voor $x^2 \pm y^4 = z^6$ blijkt dat relatief eenvoudig te zijn. In andere gevallen is het echt nodig de stelling van Faltings concreet te maken. Dat lukt niet via het bewijs dat Faltings zelf gaf, maar een eerdere constructie van Chabauty uit 1941, waarmee hij een beperkte versie van Faltings' stelling bewees, is wel bruikbaar. Sommige van de krommen voldoen echter niet aan de extra conditie die Chabauty stelt. Voor deze krommen moet eerst via overdekkingstechnieken een aantal andere krommen geconstrueerd worden die wel aan Chabauty's conditie voldoen, zodat de rationale punten op de oorspronkelijke kromme corresponderen met de rationale punten op de nieuwe krommen.

In hoofdstuk 5 wordt een meer algemeen kader voor deze methoden geschetst. Door eerdere auteurs zijn voornamelijk krommen van geslacht 2 onderzocht op toepasbaarheid van Chabauty-methoden. Coleman, Flynn, en anderen hebben dit voor krommen van geslacht 2 gedaan. Wetherell heeft overdekkingstechnieken toegepast op speciale krommen van geslacht 2, hetgeen hem bracht tot het bestuderen van Chabauty-methoden voor krommen van geslacht 3. In dit proefschrift worden overdekkingstechnieken besproken die toepasbaar zijn op hyperelliptische krommen in het algemeen (krommen van geslacht 2 zijn hyperelliptisch). Bovendien wordt aangetoond dat uitgebreide berekeningen op ingewikkelde wiskundige strukturen in deze situaties kunnen worden vervangen door berekeningen op elliptische krommen over uitbreidingen van het grondlichaam. Dat is vanuit computationeel

oogpunt een bijzonder aantrekkelijke optie. Deze mogelijkheid bestaat voor iedere kromme die meetkundig een overdekking is van een elliptische kromme.

Curriculum vitae

De schrijver van dit proefschrift is geboren op 5 mei 1972 in Pijnacker. In 1990 behaalde hij het V.W.O.-diploma aan de Christelijke Scholengemeenschap 't Loo te Voorburg. Vervolgens begon hij met de studie Wiskunde aan de Rijksuniversiteit Leiden (thans Universiteit Leiden) en legde in 1991 het propedeutisch examen af. In juni 1995 rondde hij zijn studie af met een afstudeerproject Getaltheorie met als titel "Generalisations of the ABC-conjecture" onder leiding van prof. dr. R. Tijdeman. Van 1 juli 1995 tot 1 juli 1999 was hij werkzaam als assistent in opleiding aan de Universiteit Leiden. Het onderzoek waarvan de resultaten in dit proefschrift beschreven staan, werd begeleid door dr. F. Beukers en prof. dr. R. Tijdeman. Vanaf 1 september 1999 werkt hij als postdoc aan de Universiteit Utrecht.