Chabauty methods using elliptic curves

Nils Bruin

June 22, 1999

Abstract

In this article, we consider algebraic curves over $\mathbb{Q}$ that cover an elliptic curve over some extension of $\mathbb{Q}$. We show how we can use the arithmetic on that elliptic curve to obtain information on the rational points on the cover. We apply this method to curves arising from the diophantine equations $x^2 \pm y^4 = z^5$ and determine all solutions with coprime, integral x, y, z. To do this, we determine the rational points on several curves of genus 5.

1 Introduction

Since 1983 (see [Fal83]), it is known that an algebraic curve of genus $g \geq 2$ over a number field has only finitely many rational points. The proof of this theorem does not help in actually determining them, however. A much older, partial, proof by Chabauty (see [Cha41]) does suggest a way of bounding the number of rational points.

The proof applies to curves $\mathcal{C}$ of genus g over a number field K such that the rank of the Mordell-Weil group of the Jacobian variety $\mathrm{rk}(\mathrm{Jac}_{\mathcal{C}}(K))$ is smaller than g. Let p be a finite prime of K. The proof is based on p-adic analytic geometry. It uses that the dimension of the p-adic closure of a finitely generated group of rank r on a p-adic abelian variety has dimension $\leq r$. Therefore, the p-adic closure of the Mordell-Weil group is a proper submanifold of $\mathrm{Jac}_{\mathcal{C}}(K_p)$.

If we embed $\mathcal{C}$ in $\mathrm{Jac}_{\mathcal{C}}$ over K (assuming $\mathcal{C}(K) \neq \emptyset$), then $\mathcal{C}(K)$ will land in $\mathrm{Jac}_{\mathcal{C}}(K)$. As a consequence, the image of $\mathcal{C}(K)$ will be contained in the intersection of the image of $\mathcal{C}(K_p)$ and the p-adic closure of $\mathrm{Jac}_{\mathcal{C}}(K)$. The latter is an intersection of a p-adic curve and a manifold of codimension ≥ 1. Chabauty proves that the intersection will be 0-dimensional and, since $\mathrm{Jac}_{\mathcal{C}}(K_p)$ is compact, it is finite.

This intersection can often be determined explicitly and the number of points gives a bound on the size of $\mathcal{C}(K)$. Recently, Chabauty-methods have proved quite succesful in giving sharp bounds on $\mathcal{C}(K)$. See for instance [FPS97], [Fly97], [CF96], [Wet97] and [Bru97]. These papers concentrate on the application of this argument to the simplest non-trivial case $g = 2$. Even then, the computations necessary on $\mathrm{Jac}_{\mathcal{C}}$ are quite involved.

The variety $\mathrm{Jac}_{\mathcal{C}}$ need not be absolutely simple. A part of it might be isogenous to a product of elliptic curves (over an extension of the base field). In [FW99], it is described how this can be used for curves of genus 2 that cover an elliptic curve over the base field with degree 2. In this article, we describe a general way to take advantage of elliptic factors in $\mathrm{Jac}_{\mathcal{C}}$.

Let K be a number field. In our applications, we have $K = \mathbb{Q}$. Suppose we have a cover $\Phi : \mathcal{C} \to \mathbb{P}_1$ over K of genus $g > 1$ and suppose that there is an elliptic cover $\varphi : E \to \mathbb{P}_1$ over a finite extension L of K such that Φ factors through φ, as depicted in the following diagram.

$$\begin{tikzcd} \mathcal{C} \arrow[d, "\Phi"'] \arrow[dr, "\pi"] & \\ \mathbb{P}_1 & E \arrow[l, "\varphi"] \end{tikzcd}$$

If we want to determine $\mathcal{C}(K)$, then we can use this factorisation of covers in the following way. Suppose that $P \in \mathcal{C}(K)$. Then, clearly, $\pi(P) \in E(L)$ and $\varphi(\pi(P)) \in \mathbb{P}_1(K)$. Thus, $\Phi(\mathcal{C}(K))$ is contained in $\varphi(E(L)) \cap \mathbb{P}_1(K)$. We treat the case where $\deg(\varphi) = 2$ in detail.

As an example, we prove the following two theorems, that play a role in the ongoing analysis of the generalised Fermat equation $x^r + y^s = z^t$, $x, y, z \in \mathbb{Z}$, $\gcd(x, y, z) = 1$ (see [Bru97] and [Bru99]).

Theorem 1.1 *If $x, y, z \in \mathbb{Z}$ satisfy $x^2 + y^4 = z^5$ and $\gcd(x, y, z) = 1$ then $xyz = 0$.*

Theorem 1.2 *The only integer, pairwise prime integer solutions to $x^2 - y^4 = z^5$ are*

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

In order to reduce these theorems to the problem of finding rational points on algebraic curves, we examine primitive solutions to equations of the form $F(s, t) = Dy^m$. This kind of equations was already treated in [DG95], but we reformulate some of their results more explicitly. These lead to the problem of finding rational points on curves of genus 5.

This article contains material from [Bru99].

2 Preliminaries

Let L be a number field with ring of integers $\mathcal{O} = \mathcal{O}_L$. Let $\mathfrak{p}$ be a finite prime of L. Then we write $\nu_{\mathfrak{p}}$ for the $\mathfrak{p}$-adic logarithmic valuation and $\mathrm{char}(\mathfrak{p})$ for the rational prime lying below $\mathfrak{p}$. In this article, we consider elliptic curves E over L. In this section we fix some notation. See [Sil86] for a thorough treatment. We work with elliptic curves in twisted Weierstrass form

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

with $\gamma, a_2, a_4, a_6 \in \mathcal{O}$. The projective closure of this curve has a unique point ∞. The curve E is an abelian variety with a group law that is characterised by the fact that three points P_1, P_2, P_3 sum to 0 $(= \infty)$ if and only if they are collinear.

Take $\mathfrak{p} \nmid 2$ to be a finite prime of L. The curve E has good reduction at $\mathfrak{p}$ if the curve $E \bmod \mathfrak{p}$ over $\mathcal{O}/\mathfrak{p}$ defined by reducing E coefficient wise $\bmod \mathfrak{p}$, is again a curve of genus 1. We have a reduction map $E(L_\mathfrak{p}) \to (E \bmod \mathfrak{p})(\mathcal{O}/\mathfrak{p})$, which induces the short exact sequence of group homomorphisms

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

where $E^{(1)}(L_\mathfrak{p})$ is called the kernel of reduction. Consider the function $Z := X/Y$ on E. Then $E^{(1)}(L_\mathfrak{p}) = \{G \in E(L_\mathfrak{p}) : Z(G) \in \mathfrak{p}\mathcal{O}_\mathfrak{p}\}$. Suppose that $\mathfrak{p}$ is not too highly ramified (say, unramified). As described in [Sil86, Chapter IV], we have a group homomorphism $E^{(1)}(L_\mathfrak{p}) \to \mathfrak{p}\mathcal{O}_\mathfrak{p}$. This can be expanded as a power series in Z and we have $\mathrm{Log}_\mathfrak{p}(Z) = Z \bmod (Z^2)$. Furthermore, by [Sil86, Proposition IV.5.5] we have that $\mathrm{Log}_\mathfrak{p}(G) \bmod \mathfrak{p}^2 = Z(G) \bmod \mathfrak{p}^2$ for $G \in E^{(1)}(L_\mathfrak{p})$.

We will use

Lemma 2.1 *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 $i = 1, \dots, m$. Let $B_1, \dots, B_r \in E(L)$ with $B_j = 0 \bmod \mathfrak{p}_i$ such that $\langle B_1, \dots, B_r \rangle$ in $E(L)$ is of finite index divisible by p, then there are $n_1, \dots, n_r \in \mathbb{Z}_p$ with $(n_1, \dots, n_r) \neq (0, \dots, 0) \bmod p$ such that $n_1 Z(B_1) + \cdots + n_r Z(B_r) = 0 \bmod \mathfrak{p}_i^2$ for $i = 1, \dots, m$.*

Proof: The conditions in the lemma imply that there exists a $G \in E(L)$ and $n_1, \dots, n_r \in \mathbb{Z}$, not all divisible by p, such that $n_1 B_1 + \cdots + n_r B_r = pG$. Let $i \in \{1, \dots, m\}$. 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 $Z(E^{(1)}(L_{\mathfrak{p}_i})) = 0 \bmod \mathfrak{p}_i$. □

Furthermore, we apply

Lemma 2.2 *Let K be a number field, let $F, G \in \mathcal{O}_K[X, Y]$ be coprime homogeneous polynomials, $m \in \mathbb{Z}_{>0}$ and $D \in \mathcal{O}_K$. Suppose that S is a set of primes such that $\mathrm{res}(F(X,1), G(X,1))$, $D \in \mathcal{O}_S^*$. 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

$$\begin{aligned} F(x,y) &= \delta_1 z_1^m, \\ G(x,y) &= \delta_2 z_2^m, \\ z &= \sqrt[m]{\tfrac{\delta_1\delta_2}{D}}\, z_1 z_2. \end{aligned}$$

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 $\operatorname{res}(F(X,1),G(X,1)) \in \mathcal{O}_{\mathfrak{p}}^*$ we have that $F(X,1) \bmod \mathfrak{p}$ and $G(X,1) \bmod \mathfrak{p}$ cannot both be zero. 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 by symmetry and the fact that $\operatorname{res}(F(X,1),G(X,1)) = \pm\operatorname{res}(F(1,X),G(1,Y))$. □

3 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 fibers of φ is an *involution*, i.e. $\tau \in \operatorname{Aut}(\mathcal{E})$ (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 $\operatorname{Aut}(E)[2] = \{[1], [-1]\}$ 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. 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 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 $\mathrm{rk}(E(L)) < [L : K]$. We remind the reader that not much is lost by the assumption $K = \mathbb{Q}$.

By the Mordell-Weil theorem ([Sil86, VIII]), $E(L)$ 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 $B_1, \dots, B_r \subset E(L)$ such that

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

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

We fix G_0 and try to determine how many points G of the form $G = G_0 + n_1 B_1 + \cdots + n_r B_r$ 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 $G = G_0 + n_1 B_1 + \cdots n_r B_r$ 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 $B_1, \dots, B_r \in E^{(1)}(L_\mathfrak{p})$ for all $\mathfrak{p} \mid p$, we have

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

Consequently, we can write

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

which is convergent for $(n_1, \dots, n_r) \in (\mathcal{O}_\mathfrak{p})^r$ and has values in $\mathcal{O}_\mathfrak{p}$. If $\varphi(G_0 + \sum n_i B_i) \in \mathbb{P}_1(K)$, then, identifying $\mathbb{P}_1(L) \setminus \{\infty\}$ with L, we have $\theta_\mathfrak{p}^{G_0}(n_1, \dots, n_r) \in \mathcal{O}_p \subset \mathcal{O}_\mathfrak{p}$. If $\mathfrak{q} \mid p$ as well then $\theta_\mathfrak{p}^{G_0}(n_1, \dots, n_r) = \theta_\mathfrak{q}^{G_0}(n_1, \dots, n_r)$. These requirements can be expressed in power series over K in the following way. Let $I = [L_\mathfrak{p} : K_p]$ and let $1, \alpha, \dots, \alpha^{I-1}$ be an $\mathcal{O}_p$-basis of $\mathcal{O}_\mathfrak{p}$. Then there are unique $\theta_{\mathfrak{p},i}^{G_0} \in K_p[\![n_1, \dots, n_r]\!]$ 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 $\varphi(G_0 + \sum n_i B_i) \in \mathbb{P}_1(K)$ 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 $(n_1, \dots, n_r)$ for all $\mathfrak{p}, \mathfrak{q} \mid p$ and $i \geq 1$. Taking all these conditions together, this corresponds to some $\theta^{G_0} \in K_p[\![n_1, \dots, n_r]\!]^{[L:K]-1}$ vanishing in $(n_1, \dots, n_r)$. If p splits completely (i.e. $L_\mathfrak{p} = K_p$ for all $\mathfrak{p} \mid p$) then it is particularly easy to this power series. Suppose that $\mathfrak{p}_1, \dots, \mathfrak{p}_m \mid p$. Then

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

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.

Lemma 4.1 *Let $\mathcal{O}_\mathfrak{p}$ be a complete local ring with maximal ideal $\mathfrak{p}$ and*

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

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

- *$f(X_1, \dots, X_r) = b + A\,X \bmod \mathfrak{p}$, where A is an $m \times r$ matrix over $\mathcal{O}_\mathfrak{p}$ such that $A \bmod \mathfrak{p}$ has rank r*
- *$f_i(0, \dots, 0) = 0$, $\frac{\partial f_i}{\partial X_j}(0, \dots, 0) = 0$ and $f_i(X_1, \dots, X_r) = X^t\,A_i\,X \bmod \mathfrak{p}$ for all i, j, where the $A_1, \dots, A_m$ are symmetric $r \times r$ matrices such that the projective variety in $\mathbb{P}_{r-1}$ described by $\{X^t(A_i \bmod \mathfrak{p})X = 0\}_{i=1,\dots,m}$ 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 $g(X) = f(X) - b - A\,X \in (\mathfrak{p}\mathcal{O}_\mathfrak{p}[\![X_1, \dots, X_r]\!])^m$. 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 $\bmod \mathfrak{p}$. Suppose that there is an $e \geq 1$ and $x, y \in (\mathcal{O}_\mathfrak{p})^r$, $y \neq 0 \bmod \mathfrak{p}$, 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 $y \neq 0 \bmod \mathfrak{p}$, it follows that $-u^e A\,y \neq 0 \bmod \mathfrak{p}^{e+1}$, 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 $\{X^t(A_i \bmod \mathfrak{p})X = 0\}_{i=1,\dots,m}$. □

We apply these ideas to the case where $\deg(\varphi) = 2$. We adopt the notation from Section 3 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 $\{B_1,\dots,B_r\} \in E(L)$ 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

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

which is much easier to establish. For instance, This follows from Lemma 2.1 if all $L_{\mathfrak{p}} = K_p$ and $Z(B)/u_p \bmod p$ has rank r. If $E(L) \bmod \mathfrak{p} = \langle G_1,\dots,G_{r+t}\rangle$, 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 $\mathfrak{p}_1,\dots,\mathfrak{p}_m \mid p$ with $\sum_{i=1}^m [L_{\mathfrak{p}} : K_p] > r$. Then, it is sufficient to take $B_1,\dots,B_r$ to generate a subgroup of $\bigcap_{i=1}^m (E^{(1)}(L_{\mathfrak{p}_i}) \cap E(L))$ of index prime to $\mathrm{char}(p)$. 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 4.1. We have the following.

Lemma 4.2 *Let $K, L, p, \mathfrak{p}_1,\dots,\mathfrak{p}_m$ 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 4.1, 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 4.1, then G is the only $G' \in E(L)$ such that $\varphi(G') \in \mathbb{P}_1(K)$ and $\varphi(G) \bmod p = \varphi(G') \bmod p$.*

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

In this section we show how Lemma 2.2 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 $\operatorname{disc}(F(X,1)),\operatorname{disc}(F(1,Y)),D\in\mathcal{O}_S^*$. 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 $\alpha_1,\dots,\alpha_n\in L$ such that $F(X,Y)=\prod_{i=1}^n(X-\alpha_iY)$. Note that $\sigma\in\operatorname{Gal}(L/K)$ acts as a permutation on the α_i and use this to fix $\operatorname{Gal}(L/K)\hookrightarrow S_n$. We write ${}^\sigma\alpha_i=\alpha_{\sigma(i)}$. Suppose that x,y,z is an S-primitive solution in K. Lemma 2.2 gives that we have $\delta_1,\dots,\delta_n\in L(S,m)$ with $(\delta_1\cdots\delta_n)/D\in(K^*)^m$ and S-primitive $(z_1,\dots,z_n)\in L^n$ such that

$$\begin{aligned} x-\alpha_iy &= \delta_iz_i^m\\ z &= \sqrt[m]{\tfrac{\delta_1\cdots\delta_n}{D}}z_1\cdots z_n. \end{aligned}$$

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 $\sigma\in\operatorname{Gal}(L/K)$. If F is irreducible over K then $\operatorname{Gal}(L/K)$ acts transitively on the α_i, so then δ_1 determines all δ_i. See Lemma 5.2 for details.

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

$$I_\delta:=\{(\alpha_i-\alpha_j)(\delta_kZ_k^m-\delta_lZ_l^m)-(\alpha_k-\alpha_l)(\delta_iZ_i^m-\delta_jZ_j^m)\}_{i,j,k,l}$$

such that its image under $\Phi_\delta:(Z_1,\dots,Z_n)\mapsto\frac{\alpha_j\delta_iZ_i^m-\alpha_i\delta_jZ_j^m}{\delta_iZ_i^m-\delta_jZ_j^m}$ is K-rational (corresponding to x/y), where the definition of Φ_δ 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 the $\mathbb{P}_{n-1}$. 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 $Z_i=Z_k=0$,

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

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 $\Phi_\delta:\mathcal{C}_\delta\to\mathbb{P}_1$ is finite of degree m^{n-1} and galois with galois group $\langle\tau_1,\dots,\tau_n\rangle$.

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 $\langle\tau_1,\dots,\tau_n\rangle$ 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 ${}^{\sigma}\Phi_\delta = \varphi_\delta$ for $\sigma \in \mathrm{Gal}(L/K)$, we see that both are defined over K, so $\Phi_\delta : \mathcal{C}_\delta \to \mathbb{P}_1$ 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 Riemann-Hurwitz (see [Sil86, Theorem II.5.9]. Note that $\#\Phi_\delta^{-1}(\{a\}) = m^{n-1}$ if $a \notin \{\alpha_1, \dots, \alpha_n\}$ and $\#\Phi_\delta^{-1}(\{\alpha_i\}) = m^{n-2}$. As a consequence, $\sum_{P \in \mathcal{C}(\bar{K})}(e_P(\Phi_\delta) - 1) = nm^{n-2}(m-1)$. 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 $P \in \Phi_\delta^{-1}(\{a\})$. If $\sigma \in \mathrm{Gal}(\bar{K}/K)$ then ${}^{\sigma}\Phi_\delta(P) = {}^{\sigma}a = a$. Since ${}^{\sigma}\Phi_\delta = \Phi_\delta$, 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 [Sil86, Theorem X.2.2] 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_δ is τ-invariant, $\Phi_P := \Phi_\delta \circ \psi^{-1} : \mathcal{C}_P \to \mathbb{P}_1$ is a cover over K and $a \in \Phi_P(\mathcal{C}_P(K))$. 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 together with Lemma 5.2. Summarising:

Theorem 5.1 *Let K, $F(x,y) = Dz^m$ and S be as above. Then there is a finite number of galois-covers $\Phi_P : \mathcal{C}_P \to \mathbb{P}_1$ 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*

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

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 [Sil86, Theorem X.2.2], 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 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 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

Lemma 5.2 *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*

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

This shows that for irreducible F, models of the $\mathcal{C}_P$ mentioned in Theorem 5.1 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.

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

Consider the situation of Section 5 with $m = 2$. In principle, Theorem 5.1 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 these 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 5 and we will put $n = 2$ and write $\Phi = \Phi_P$. 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 $H\backslash. : \mathcal{C}_\delta \to \mathcal{E}_\delta$. 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.

$$\begin{tikzcd}
 & \mathcal{C}_\delta \arrow[dl, "H\backslash."'] \arrow[ddr] & & \mathcal{C}_P \arrow[ll, "\psi"'] \arrow[ddl, "\Phi"] \arrow[dr, "\psi^{-1}H\psi\backslash."] \arrow[dr, "\pi"'] & \\
\mathcal{E}_\delta \arrow[drr] & & & & \mathcal{E}_P \arrow[dll, "\varphi"] \\
 & & \mathbb{P}_1 & &
\end{tikzcd}$$

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.

Lemmas 7.3, 7.4 and 7.5 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].

7 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 7.1 and 7.2 show that we have to determine $\{2, 5\}$-primitive solutions fo equations of the form $y^2 = F(s, t)$, where F is a homogeneous form of degree 5.

Lemma 7.1 *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 $\mathrm{Norm}(\delta)$ 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 $\delta = 1$. □

Lemma 7.2 *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*

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

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 $(x, y, z) \mapsto (x, y, -z)$. 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. □

According to Theorem 5.1, solutions to equations as mentioned in the lemmas above, are parametrised by the rational points on genus 5 curves. By Section 6, these curves cover elliptic curves. The next three lemmas determine these elliptic curves including the induced cover of the projective line.

Lemma 7.3 *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 1.*

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 5.2, it follows that with $S = \{2,5\}$, we have

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

where $\delta \in L(S,2)$. It follows that $(s/t)^4 - 10(s/t)^2 + 5 = \mathrm{Norm}(\delta)(y/(a_4t^2))^2$ as well. As is easily checked, the curve $X^4 - 10X^2 + 5 = DY^2$ has no $\mathbb{Q}$-rational points for

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 $\mathcal{O}_L$	$\operatorname{disc}(\mathcal{O}_L/\mathbb{Z})$	$\mathcal{O}_L^*$	$\operatorname{reg}(\mathcal{O}_L^*)$	$h(\mathcal{O}_L)$
$\mathbb{Q}(\beta)$	$1, \beta, \beta^2, \beta^3$	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

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

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 1: Parametrising curves and their fields of definition

$D = 2, 10, -2, -5, -10$. 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 $-\operatorname{Norm}(\delta)$ 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 should exist a solution $(a_0, \ldots, a_4) \in \mathbb{Z}_p^5$ with $(a_0, \ldots, a_4) \not\equiv (0, \ldots, 0) \bmod p$ for any prime p as well. 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. □

Lemma 7.4 *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 1.*

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

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

where $\delta \in L(S, 2)$. It follows that $(s/t)^4 + (s/t)^3 + (s/t)^2 + (s/t) + 1 = (y/a_4t^2))^2/\mathrm{Norm}(\delta)$ 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 $\mathrm{Norm}(\delta)$ 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

$$(x^5 - 1)/(x + \zeta) = 2\mathrm{Norm}(\delta)/\delta y_1^2.$$

This leads to the remaining two curves. □

Lemma 7.5 *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 1.*

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

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

It follows that

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

$$\begin{aligned}
E_j : \gamma_j Y^2 &= X^3 - 5X^2 + 5X \\
\gamma_3 &= 8\beta - 2\beta^3 - 6 \\
\varphi_3(X,Y) &= \frac{(6\beta - 2\beta^3)X + 3\beta^3 - 10\beta}{5} \\
\gamma_6 &= 2(\zeta^2 - \zeta) \\
\varphi_6(X,Y) &= \frac{X - 2\zeta^2 + \zeta - 2}{X + \zeta^3 + \zeta^2 - \zeta - 1} \\
\gamma_7 &= -2(\zeta^2 - \zeta) \\
\varphi_7(X,Y) &= \frac{X - 2\zeta^2 + \zeta - 2}{X + \zeta^3 + \zeta^2 - \zeta - 1} \\
\gamma_8 &= 1 \\
\varphi_8(X,Y) &= \frac{-\alpha^3 X + 2\alpha^3 Y}{4X - 5} \\
\gamma_9 &= \alpha^3 + \alpha^2 - 1 \\
\varphi_9(X,Y) &= \frac{2(6\alpha^4 - 4\alpha^3 + 5\alpha^2 + 11\alpha - 13)X + 12Y - 10(3\alpha^4 - \alpha^3 + 4\alpha - 6)}{(-4\alpha^3 + 2\alpha^2 + 2\alpha + 2)X - 12Y - 5(3\alpha^4 - 3\alpha^3 + \alpha^2 - 4)}
\end{aligned}$$

Table 2: Description of covers with respect to models E_j

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

$$(x^5 - 8)/(x - \alpha^3) = \mathrm{Norm}(\delta)/\delta y_1^2.$$

This leads to the curves in the lemma. $\square$

Lemma 7.6 *The covers $\mathcal{E}_3, \mathcal{E}_6, \ldots, \mathcal{E}_9$ in Table 1 are birational to the covers $E_j : \gamma Y^2 = X^3 - 5X^2 + 5X$ described in Table 2.*

Proof: It is straightforward to check this. $\square$

Having established elliptic covers that parametrise $\{2,5\}$-primitive solutions in some way, we now determine their Mordell-Weil groups (up to finite index). We do this using a 2-isogeny-descent (see [Sil86, Proposition X.4.9] or [Bru99, Section 4.3]). We only give results. For more detailed information, see [Bru99, Section 4.8] and the electronic references given there.

Lemma 7.7 *Let $j = 3, 6, 7, 8, 9$. Consider E_j, G_i, p and M be as given in Table 2 and let L be the field of definition of E_j. then the group spanned by the G_i span a subgroup of finite index prime to 2 and p in $E_j(L)$, containing $E_j^{\mathrm{tor}}(L)$. Let $\mathfrak{p}$ be a prime of L above p. Then the reduction of the G_i span $E_j(L) \bmod \mathfrak{p}$. The rows of M form linear combinations of the G_i that span the intersections of the kernels of reduction mod $\mathfrak{p} \mid p$.*

Proof: We get that the index is finite and prime to 2 by doing a 2-isogeny-descent (see [Sil86, Proposition X.4.9] or [Bru99, Section 4.3]). For more detailed information, see

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 3: Curves E_j and data on the Mordell-Weil groups

[Bru99, Section 4.8] and the electronic references given there. The torsion can be bounded by using that, under mild conditions, reduction modulo a prime is injective on torsion. Therefore, the torsion is a subgroup of the group of rational points over the residue field of most primes.

The matrix M gives us a subgroup of $\bigcap_{\mathfrak{p}|p}(E_j(L) \cap E_j^{(1)}(L_\mathfrak{p}))$. Applying Lemma 2.1 to $Z(B)/p$ (the matrix of Z-coordinates of generators of that group) gives that the index is prime to p as well. That the G_i span $E_j(L) \bmod \mathfrak{p}$ can be checked by computing the index of the reduction of the G_i in the finite group $(E_j \bmod \mathfrak{p})(\mathcal{O}/\mathfrak{p})$. $\square$

Having established knowledge of the appropriate Mordell-Weil groups, we can proceed and apply the method described in Section 4.

Proposition 7.8 $\mathcal{E}_1(\mathbb{Q}) = \{\infty^+, \infty^-\}$.

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. $\square$

Proposition 7.9 $\mathcal{E}_2(\mathbb{Q}) = \{(0,1),(0,-1)\}$.

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. □

Proposition 7.10 $\mathcal{E}_5(\mathbb{Q}) = \{\infty^+, \infty^-\}$.

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. □

Proposition 7.11 *The following statements are true.*

- *The points* $P \in \mathcal{E}_3(\mathbb{Q}(\beta))$ *with* $X(P) \in \mathbb{P}_1(\mathbb{Q})$ *have* $X(P) = 0$.
- *The points* $P \in \mathcal{E}_4(\mathbb{Q}(\beta))$ *with* $X(P) \in \mathbb{P}_1(\mathbb{Q})$ *have* $X(P) = 0$.
- *The points* $P \in \mathcal{E}_6(\mathbb{Q}(\zeta))$ *with* $X(P) \in \mathbb{P}_1(\mathbb{Q})$ *have* $X(P) = \pm 1$.
- *The points* $P \in \mathcal{E}_7(\mathbb{Q}(\zeta))$ *with* $X(P) \in \mathbb{P}_1(\mathbb{Q})$ *have* $X(P) \in \{1, \frac{1}{3}, 3\}$.
- *The points* $P \in \mathcal{E}_8(\mathbb{Q}(\alpha))$ *with* $X(P) \in \mathbb{P}_1(\mathbb{Q})$ *have* $X(P) \in \{\infty, 0, -2\}$.
- *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: We apply the method proposed in Section 4 to each of the curves individually. We work with the twisted Weierstrass models E_i from Table 2 instead of the models $\mathcal{E}_i$. The map $X : \mathcal{E}_i \to \mathbb{P}_1$ corresponds to $\varphi_i : E_i \to \mathbb{P}_1$. Note that the map $(X, Y, \beta) \to (-X, Y, -\beta)$ gives a map between the covers $\varphi_4 : \mathcal{E}_4 \to \mathbb{P}_1$ and $\varphi_3 : \mathcal{E}_3 \to \mathbb{P}_1$. Consequently, the statement on $\mathcal{E}_4$ follows from the one on $\mathcal{E}_3$. The method is almost automatic, so we only give the argument for E_7, which illustrates the different facets of the method nicely. The arguments for the other curves are similar. Many of the computational steps cannot be reproduced here on paper. Instead, a program is available that does the computations for you. It is written for KASH 2.0 (see [DFK+97]) and is available from the preprint server of the Mathematical Institute of Leiden University or through the author's homepage.

We have $K = \mathbb{Q}$, $L = \mathbb{Q}(\zeta)$, $E = E_7$ and $\varphi = \varphi_7$. According to Lemma 7.7, we have that $\langle G_1, \ldots, G_4\rangle$ generate a subgroup of $E(L)$ with appropriate properties. For the sake of simplicity of the argument, we pretend that they actually generate the whole of $E(L)$.

We choose $p = 31$ and $\mathfrak{p}_1, \ldots, \mathfrak{p}_4 = \mathfrak{p}_{31,1}, \ldots, \mathfrak{p}_{31,4}$. It is straightforward to compute that $\langle G_1, \ldots, G_4\rangle \cap E^{(1)}(L_{\mathfrak{p}_i}) = \langle 2G_1 + G_2 + G_4, 4G_2 + G_4\rangle$, $\langle 2G_1 + 3G_2 + G_4, 4G_2 + G_1 + G_2\rangle$, $\langle 2G_1 + G_2 + G_3, 4G_2 + G_3 + G_4\rangle$, $\langle 2G_1 + 3G_2, 4G_2 + G_4\rangle$ for $i = 1, 2, 3, 4$ respectively. Consequently, $B_1 = 8G_1 + 4G_2, B_2 = 8G_2$ generate the intersection of the kernels of reduction.

In order to determine $\varphi(E(L)) \cap \mathbb{P}_1(\mathbb{Q})$, we first look at the reduction mod 31. If $P \in \varphi(E(L)) \cap \mathbb{P}_1(\mathbb{Q})$, then certainly $P \bmod 31 \in \varphi(E(L)) \bmod \mathfrak{p}_i$. The latter is something

j	G	$\varphi(G)$	$\theta^G(n_1,\dots,n_r)$
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: Fibers of rational points

we can compute explicitly. We find

$$\begin{aligned}
\varphi(E(L)) \bmod \mathfrak{p}_1 &= \{0,1,2,3,4,8,9,13,15,16,17,21,24,25,26,27,29,\infty\}\\
\varphi(E(L)) \bmod \mathfrak{p}_2 &= \{1,2,3,4,5,6,7,9,10,11,14,15,16,18,19,21,25,27\}\\
\varphi(E(L)) \bmod \mathfrak{p}_3 &= \{1,2,3,5,7,8,9,16,17,18,19,20,21,23,25,26,28,29\}\\
\varphi(E(L)) \bmod \mathfrak{p}_4 &= \{0,1,2,3,4,5,6,7,8,11,12,15,16,21,22,23,29,\infty\}.
\end{aligned}$$

It follows that $\varphi(E(L)) \cap \mathbb{P}_1(\mathbb{Q}) \bmod 31 \subset \{1,2,3,16,21\}$. Upon closer inspection, we see that if $G \in E(L)$ and $\varphi(G) \bmod \mathfrak{p}_1 = 2$, then $G \in \{G_3\} + E^{(1)}(L_{\mathfrak{p}_1})$. Similarly, for $\varphi(G) \bmod \mathfrak{p}_4 = 2$, we get $G \in \{2G_2, 2G_2+G_4\} + E^{(1)}(L_{\mathfrak{p}_4})$. But then we have that $2G_2 - G_3$ or $2G_2+G_4-G_3$ is in $E^{(1)}(L_{\mathfrak{p}_1}) \cap E^{(1)}(L_{\mathfrak{p}_4}) = \langle 2G_1+G_2, G_2, G_4\rangle$. This is clearly not the case. A similar argument rules out 16. Thus we see that $\varphi(E(L) \cap \mathbb{P}_1(\mathbb{Q})) \bmod 31 \subset \{1,3,1/3\}$. We know that equality holds, since $G = 0, G_1 - G_2 + G_4, G_1 + G_2 + G_4$ realise these values.

It remains to show that these are the only points (apart from the points $G_\tau - G$) with rational image under φ. We can do so by applying Lemma 4.2. For this, we need $Z(B_1), Z(B_2) \bmod \mathfrak{p}_i^2$. We can compute these either by performing the group addition with exact precision and then reduce $\bmod\, \mathfrak{p}_i^2$ or (more efficiently), do the group operations with finite $\mathfrak{p}_i$-adic precision. Either way, we find the values mentioned in Table 3. By applying Lemma 2.1 to these, we get that $\langle G_1, \dots, G_4\rangle$ has index prime to 31 in $E(L)$, as stated in Lemma 7.7.

Using these values we can compute approximations to $\theta^{G_0}(n_1, n_2)$, as shown in Table 4. In is easily checked that in each case, one of the criteria in Lemma 4.2 applies. We conclude that $P \in \varphi(E(L)) \cap \mathbb{P}_1(\mathbb{Q})$ with $P \bmod 31 \in \{1,3,21\}$ are $P = 1, 3, 1/3$. □

Proof of Theorem 1.1: Consider $x^2 + y^4 = z^5$. Lemma 7.1 together with Lemma 7.3 show that the curves $\mathcal{E}_1, \dots, \mathcal{E}_4$ from Table 1 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 7.8 through 7.11 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 1.2: Consider $x^2 - y^4 = z^5$. Lemmas 7.2, 7.4 and 7.5 show that $\mathcal{E}_5, \dots, \mathcal{E}_9$ determine all possible solutions. Propositions 7.10 through 7.11 give the possible candidates and the values of s/t belonging to them. The values $s/t = \infty, 1, -1$ in Lemma 7.4 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 7.5. The point on $\mathcal{E}_9(L)$ leads to $(x,y,z) = (\pm 7, \pm 3, -2)$. □

Acknowledgements

The results presented in this article are part of [Bru99], which is a thesis resulting from 4 years of research at Leiden University under supervision of F. Beukers and R. Tijdeman, who helped with valuable discussions. Furthermore, E. Schaefer and H. W. Lenstra Jr. offered many useful comments. The many computations made heavy use of the freely available computer algebra package KASH/KANT ([DFK+97]). The maintaining group was of great help with their quick responses to bug reports and requests for new features.

References

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

[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 and Covering Techniques applied to Generalised Fermat Equations.* PhD thesis, Universiteit Leiden, 1999.

[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.

[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.

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

[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.

[FW99] E. V. Flynn and J. L. Wetherell. Finding rational points on bielliptic genus 2 curves. to appear in Man. Math., 1999.

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

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

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

Address for correspondence: Nils Bruin, Math. Institute, Leiden University, P.O. Box 9512, 2300 RA Leiden, The Netherlands; e-mail: nbruin@wi.leidenuniv.nl