J. reine angew. Math. **562** (2003), 27—49

Journal für die reine und angewandte Mathematik

Chabauty methods using elliptic curves

By *Nils Bruin* at Burnaby

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 $x^8 + y^3 = z^2$ and determine all solutions with coprime, integral x, y, z. To do this, we determine the rational points on several curves of genus 5 and 17.

1. Introduction

Since 1983 (see [13]), it is known that an algebraic curve of genus $g \geqq 2$ 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 [9]) does suggest a way of bounding the number of rational points.

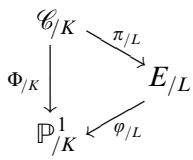
The proof applies to curves $\mathscr{C}$ of genus g over a number field K such that the rank of the Mordell-Weil group of the Jacobian variety $\mathrm{rk}\big(\mathrm{Jac}_{\mathscr{C}}(K)\big)$ is smaller than g. Let p be a finite prime of K. The proof is based on p-adic analytic geometry. It uses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

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

This intersection can often be determined explicitly and the number of points gives a bound on the size of $\mathscr{C}(K)$. Recently, Chabauty-methods have proved to be quite successful in giving sharp bounds on $\mathscr{C}(K)$. See for instance [15], [14], [8], [21] and [6]. These papers concentrate on the application of this argument to the simplest non-trivial case $g = 2$. Even then, the computations necessary on $\mathrm{Jac}_{\mathscr{C}}$ are quite involved.

The Abelian variety $\mathrm{Jac}_{\mathscr{C}}$ 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 [16], 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 $\mathrm{Jac}_{\mathscr{C}}$.

Let K be a number field. Suppose we have a cover $\Phi : \mathscr{C} \to \mathbb{P}^1$ 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:



To determine $\mathscr{C}(K)$, we can use the factorisation of covers $\Phi = \varphi \circ \pi$ in the following way. Suppose that $P \in \mathscr{C}(K)$. Then, clearly, $\pi(P) \in E(L)$ and $\varphi\big(\pi(P)\big) \in \mathbb{P}^1(K)$. Thus, $\Phi\big(\mathscr{C}(K)\big)$ is contained in $\varphi\big(E(L)\big) \cap \mathbb{P}^1(K)$. We treat the case where $\deg(\varphi) = 2$ in detail.

As an example, we prove the following three 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 [6] and [4]).

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 solutions to $x^2 - y^4 = z^5$ are*

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

Theorem 1.3. *The only integer, pairwise prime solutions to $x^8 + y^3 = z^2$ are*

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

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 [11], but we reformulate some of their results more explicitly. These lead to the problem of finding rational points on curves of genus 5 and 17.

2. Notation and terminology

For a number field K, we write $\mathcal{O}_K$ for its ring of integers. If p is a finite prime of K, we write K_p for the p-adic completion of K and $\mathcal{O}_p$ for the ring of local integers in K_p. We write $v_p : K_p \to \mathbb{Z}$ for the normalised valuation on K_p (normalised meaning that v_p is surjective). Let S be a finite set of primes of K containing all infinite primes and let L be a finite extension on K. If $\mathfrak{p}$ is a prime of L, then we write $\mathfrak{p} \mid S$ if $\mathfrak{p}$ lies over some prime in S. Otherwise, we write $\mathfrak{p} \nmid S$. Following [19], we write

$$L(S, m) := \{a \in L^* : v_{\mathfrak{p}}(a) \bmod m = 0 \text{ for all finite primes } \mathfrak{p} \nmid S \text{ of } L\}/L^{*m}.$$

Furthermore, we write

$$\mathcal{O}_{L,S} = \mathcal{O}_S = \{a \in L : v_\mathfrak{p}(a) \geqq 0 \text{ for all } \mathfrak{p} \not| S\}.$$

A tuple $(x_1, \ldots, x_n) \in (\mathcal{O}_L)^n$ is called *S-primitive* if $\min\{v_\mathfrak{p}(x_i) : i = 1, \ldots, n\} = 0$ for all $\mathfrak{p} \not| S$. If a tuple is S-primitive for $S = \emptyset$ then the tuple is called *primitive*. In particular, a tuple $(x_1, \ldots, x_n) \in \mathbb{Z}^n$ is primitive exactly if $\gcd(x_1, \ldots, x_n) = 1$.

In this article, we use *curve* for a smooth, projective, absolutely irreducible algebraic variety of dimension 1. In many cases we will represent them by an affine, singular model.

A *cover* is a nonconstant map $\varphi : \mathscr{D} \to \mathscr{C}$ between curves. Following algebraic geometric customs and contrary to topological convention, a cover can be ramified. For brevity, we will often refer to $\mathscr{D}$ as a *cover* of $\mathscr{C}$, and write $\mathscr{D}/\mathscr{C}$ if the map φ is obvious. We say two covers $\varphi_1 : \mathscr{D}_1 \to \mathscr{C}$ and $\varphi_2 : \mathscr{D}_2 \to \mathscr{C}$, defined over a field K, are *isomorphic*, if there is an isomorphism of curves $\psi : \mathscr{D}_1 \to \mathscr{D}_2$ over K such that $\varphi_1 = \varphi_2 \circ \psi$.

We write $\mathrm{Aut}_K(\mathscr{C})$ for the group of automorphisms of $\mathscr{C}$ over K. If $\overline{K}$ is an algebraic closure of the field of definition of $\mathscr{C}$, we write $\mathrm{Aut}(\mathscr{C}) = \mathrm{Aut}_{\overline{K}}(\mathscr{C})$. Similarly, we write $\mathrm{Aut}_K(\mathscr{D}/\mathscr{C})$ and $\mathrm{Aut}(\mathscr{D}/\mathscr{C})$ for the automorphisms of $\mathscr{D}$ as a cover of $\mathscr{C}$. We say a cover is *Galois* if $\#\mathrm{Aut}(\mathscr{D}/\mathscr{C}) = \deg(\mathscr{D}/\mathscr{C})$. We write the action of $\mathrm{Aut}(\mathscr{D})$ on $\mathscr{D}$ as a left action. If $H \subset \mathrm{Aut}(\mathscr{D})$ is a finite subgroup of automorphisms, we write $H\backslash. : \mathscr{D} \to H\backslash\mathscr{D}$ for the cover obtained by considering the curve that represents the orbits of $\mathscr{D}$ under H.

Due to the nature of the elliptic curves we encounter in this paper, we allow for an extra coefficient in Weierstrass-form:

$$E : \gamma Y^2 = X^3 + a_2X^2 + a_4X + a_6.$$

If E is defined over some number field K, then often we insist that $\gamma, a_2, a_4, a_6 \in \mathcal{O}_K$. Given a finite prime $\mathfrak{p}$ of $\mathcal{O}_K$, we consider the naive reduction $E \bmod \mathfrak{p}$, where we simply reduce the coefficients modulo $\mathfrak{p}$. We say the model of E has good reduction at $\mathfrak{p}$ if this reduced model defines an elliptic curve over $\mathcal{O}/\mathfrak{p}$. It is straightforward that if $\gamma, 2, \mathrm{disc}(X^3 + a_2X^2 + a_4X + a_6) \in \mathcal{O}_\mathfrak{p}^*$, then the model E has good reduction at $\mathfrak{p}$. In that case, we write $E^{(1)}(K_\mathfrak{p})$ for the kernel of $E(K_\mathfrak{p}) \to (E \bmod \mathfrak{p})(\mathcal{O}/\mathfrak{p})$.

It follows from [19], Chapter IV, that if $v_\mathfrak{p}(p) < p - 1$, where p is the characteristic of $\mathcal{O}/\mathfrak{p}$, then the *formal logarithm* induces a group isomorphism,

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

We write $\mathrm{Exp}_\mathfrak{p}$ for its inverse. Furthermore, this map can be normalised such that the induced homomorphism $E^{(1)}(K_\mathfrak{p}) \to \mathcal{O}/\mathfrak{p}^2$ coincides with the induced map from the function $Z = Y/X$.

Let K be a ring and let $F, G \in K[X, Y]$ be homogeneous polynomials. We write $\mathrm{res}(F, G)$ for the resultant of F and G as forms. If $F(X, 0)$ and $G(X, 0)$ are non-zero, then this is just equal to the resultant of $F(X, 1)$ and $G(X, 1)$ as polynomials.

3. A motivating problem

3.1. Generalised Fermat equations. In [11] and [2], the generalised Fermat equation

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

is considered. All the variables $A, B, C, x, y, z, r, s, t$ are considered unknown integers, with A, B, C non-zero and r, s, t positive. We are mainly interested in solutions such that (x, y, z) is primitive or, more generally, for a finite set of primes S, such that (x, y, z) is S-primitive.

If we fix $A, B, C \in \mathbb{Z}_{>0}$ and $r, s, t \in \mathbb{Z}_{\geqq 2}$, and $x, y, z \in \mathbb{Z}$ and then [11] shows that if $1/r + 1/s + 1/t < 1$, we have only finitely many primitive solutions. Furthermore, the ABC-conjecture would imply only finitely many solutions x, y, z if r, s, t are allowed to vary while still under the condition $1/r + 1/s + 1/t < 1$ (see [20]). In particular, taking $A = B = C = 1$, one would expect only finitely many primitive solutions x, y, z to

$$x^r + y^s = z^t, \quad \frac{1}{r} + \frac{1}{s} + \frac{1}{t} < 1.$$

Amazingly, the above equation has some quite large solutions (see [2]). However, apart from $2^3 + 1^s = 3^2$, the only exponent triples r, s, t for which primitive solutions with $xyz \neq 0$ are known, are

$$\{2, 3, 7\}, \quad \{2, 3, 8\}, \quad \{2, 3, 9\}, \quad \{2, 4, 5\}.$$

In [6], all primitive solutions to $x^2 + y^8 = z^3$ are determined, or rather, it is shown that the previously known solutions are the only ones. In the present article, we do the same for the equations $x^2 + y^3 = z^8$ and $x^2 \pm y^4 = z^5$. We determine a finite set of curves such that the rational points on those curves correspond to a set of solutions that contains all primitive solutions. Then we determine the rational points on each of these curves.

3.2. Parametrisation of $F(x, y) = Dz^m$. In this section we show how the following lemma 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 $F(x, y) = Dz^m$ (where F is a square free homogeneous polynomial of degree $n \geqq 2$) over a number field K.

Lemma 3.1. *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 $\operatorname{res}\big(F(X, Y), G(X, Y)\big)$, $D \in \mathcal{O}_S^*$. 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

$$F(x, y) = \delta_1 z_1^m,$$

$$G(x, y) = \delta_2 z_2^m,$$

$$z = \sqrt[m]{\frac{\delta_1\delta_2}{D}} z_1 z_2.$$

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 $mv_{\mathfrak{p}}(z) = v_{\mathfrak{p}}\big(F(x, y)G(x, y)/D\big) \geqq \min\big(v_{\mathfrak{p}}(x), v_{\mathfrak{p}}(y)\big)$. Therefore (x, y) is S-primitive as well. So, $(x, y) \bmod \mathfrak{p} \neq (0, 0)$. Since

$$\operatorname{res}\big(F(X, Y), G(X, Y)\big) \bmod \mathfrak{p} \neq 0,$$

it follows that $v_{\mathfrak{p}}\big(F(x,y)\big) = 0$ or $v_{\mathfrak{p}}\big(G(x,y)\big) = 0$. By homogeneity, we have

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

we see that $v_{\mathfrak{p}}\big(F(x,y)\big), v_{\mathfrak{p}}\big(G(x,y)\big) \in m\mathbb{Z}$ for all $\mathfrak{p} \nmid S$. $\square$

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 $\operatorname{disc}\big(F(X,Y)\big)$, $D \in \mathcal{O}_S^*$. For ease of exposition, we assume that F is monic in X. Using an appropriate change of variables, one can always obtain this form. Let L be a splitting field of $F(X,1)$ over K. We have $\alpha_1, \dots, \alpha_n \in L$ such that $F(X,Y) = \prod_{i=1}^{n}(X - \alpha_i Y)$. Note that $\sigma \in \operatorname{Gal}(L/K)$ acts as a permutation on the α_i and we 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 3.1 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

$$x - \alpha_i y = \delta_i z_i^m,$$

$$z = \sqrt[m]{\frac{\delta_1 \cdots \delta_n}{D}} z_1 \cdots z_n.$$

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 and δ_1 determines all δ_i. See Lemma 3.3 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

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

such that its image under $\Phi_\delta : (Z_1, \dots, Z_n) \mapsto (\alpha_j \delta_i Z_i^m - \alpha_i \delta_j Z_j^m)/(\delta_i Z_i^m - \delta_j Z_j^m)$ is K-rational (corresponding to x/y), where the definition of Φ_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 $\mathscr{C}_\delta$ 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 $\mathscr{C}_\delta = \mathbb{P}^1$, 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 $\mathscr{C}_\delta$ 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 $\Phi_\delta : \mathscr{C}_\delta \to \mathbb{P}^1$ is finite of degree m^{n-1} and Galois with $\operatorname{Aut}(\mathscr{C}_\delta/\mathbb{P}^1) = \langle \tau_1, \dots, \tau_n \rangle$.

To conclude that $\mathscr{C}_\delta$ is actually geometrically irreducible, we consider the following argument. Since $\mathscr{C}_\delta$ 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 $\mathscr{C}_\delta$ 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 $\mathscr{C}_\delta$. Consequently, the τ_i act as the trivial permutation on the components, so there is only one.

To see that $\mathscr{C}_\delta$ can in fact be defined over K, we twist the action of $\mathrm{Gal}(L/K)$ on $L[Z_1, \dots, Z_n]$. For $\sigma \in \mathrm{Gal}(L/K)$, we define ${}^\sigma Z_i = Z_{\sigma(i)}$. Under this action, $L[Z_1, \dots, Z_n]$ is a $\mathrm{Gal}(L/K)$-module and $I_\delta \subset L[Z_1, \dots, Z_n]$ and Ψ_δ are invariant. This shows that $\mathscr{C}_\delta/\mathbb{P}^1$ is in fact a model of a cover over K. Furthermore, $\mathscr{C}_\delta$ has good reduction at primes outside $S \cup \{p \mid m\}$.

We can now calculate the genus of $\mathscr{C}_\delta$ using Riemann-Hurwitz (see [19], 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, $\sum_{P \in \mathscr{C}(\bar{K})} \big(e_P(\Phi_\delta) - 1\big) = nm^{n-2}(m-1)$. Since $\mathrm{genus}(\mathbb{P}^1) = 0$ we get

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

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 $\tau_\sigma \in \mathrm{Gal}(\mathscr{C}/\mathbb{P}^1)$ such that ${}^\sigma P = \tau_\sigma(P)$. It is easy to check that $\xi_P : \sigma \mapsto \tau_\sigma$ is a cocycle. By [19], Theorem X.2.2, there is a curve C_P over K and an isomorphism $\psi : \mathscr{C}_P \to \mathscr{C}_\delta$ (not necessarily over K) such that $\xi_P = (\sigma \mapsto {}^\sigma\psi\psi^{-1})$. Since

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

we see that $\psi^{-1}(P) \in \mathscr{C}_P(K)$. Furthermore, since Φ_δ is τ-invariant, $\Phi_P := \Phi_\delta \circ \psi^{-1} : \mathscr{C}_P \to \mathbb{P}^1$ is a cover over K and $a \in \Phi_P\big(\mathscr{C}_P(K)\big)$. We see that the $\mathscr{C}_P$ form a parametrising set of curves for the S-primitive solutions. (Note that the $\mathscr{C}_\delta$ themselves are twists of each other.) To see that we only need a finite number of $\mathscr{C}_P$, we need that $\mathscr{C}_P$ has again good reduction outside S and that the number of twists with this property is finite. This follows from [19], Lemma X.4.3. Alternatively, finiteness follows from Lemma 3.1 together with Lemma 3.3. Summarising:

Theorem 3.2. *Let K, $F(x, y) = Dz^m$ and S be as above. Then there is a finite number of Galois-covers $\Phi_P : \mathscr{C}_P \to \mathbb{P}^1$ over K with $\mathrm{Gal}(\mathscr{C}_P/\mathbb{P}^1) \cong (\mathbb{Z}/m\mathbb{Z})^{n-1}$, where $\mathscr{C}_P$ is of genus $1 + m^{n-2}\left(\frac{1}{2}n(m-1) - m\right)$ and has good reduction outside $S \cup \{\mathfrak{p} : \mathfrak{p} \mid m\}$ such that*

$$\bigcup_{\mathscr{C}_P} \Phi_P\big(\mathscr{C}_P(K)\big) = \{(x : y) \in \mathbb{P}^1(K) \mid \exists z \in K : F(x, y) = Dz^m \text{ and } (x, y, z) \text{ } S\text{-primitive}\}.$$

The $\mathscr{C}_P$ 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 $\mathscr{C}_\delta$ 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 $\mathscr{C}_\delta$ is defined over K by Galois invariance. Furthermore, while by the correspondence proved in [19], 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 3.1 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 3.1 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

$$x - \alpha y = \delta(a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1})^m,$$

$$z = \sqrt[m]{\frac{N_{L/K}(\delta)}{D}} N_{L/K}\left(\sum_{i=0}^{n-1} a_i\alpha^i\right).$$

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

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

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

Lemma 3.3. *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*

$$(x : y) = \big(b_{\delta,0}(a_0, \ldots, a_{n-1}) : -b_{\delta,1}(a_0, \ldots, a_{n-1})\big),$$

$$b_{\delta,i}(a_0, \ldots, a_{n-1}) = 0 \quad \text{for } i = 2, \ldots, n-1.$$

This shows that for irreducible F, models of the $\mathscr{C}_P$ mentioned in Theorem 3.2 are given by ideals of the form

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

for appropriate values of $\delta \in L(S, m)$ and that Φ_P takes the form

$$\big(b_{\delta,0}(X_0, \ldots, X_{n-1}) : -b_{\delta,1}(X_0, \ldots, X_{n-1})\big).$$

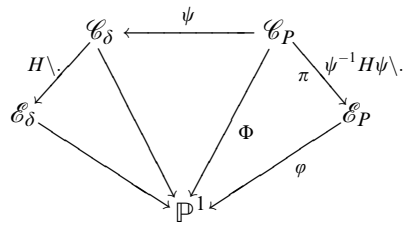
These models have the advantage of being completely explicit, over K, and efficiently computable.

3.3. Elliptic subcovers for $F(x, y) = Dz^2$. Consider the situation of Section 3.2 with $m = 2$. In principle, Theorem 3.2 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 $\mathscr{C}_P$ over K. If the genus of those curves is >1, in which case $\deg(F) \geqq 5$, then it may be possible to determine $\mathscr{C}_P(K)$ for each of these using an effective Chabauty-method. Since the genus of $\mathscr{C}_P$ may be quite high, this would involve computations on high dimensional Abelian varieties. We follow another approach.

We use the notation of Section 3.2 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 $\mathrm{Gal}(\mathscr{C}_\delta/\mathbb{P}^1)$ of index 2. Consequently, $\Phi : \mathscr{C}_P \to \mathbb{P}^1$ splits in $\mathscr{C}_P \to \mathscr{E}_P \xrightarrow{\varphi} \mathbb{P}^1$, induced by the map $H\backslash. : \mathscr{C}_\delta \to \mathscr{E}_\delta$. In general, dividing out a variety by a finite group of automorphisms gives a variety again. See [19], Exercise 3.13 or [18], §7. This is quite a deep result. In this special case, observe that $H\backslash.$ is induced by the map $(Y_1 : \cdots : Y_n) \mapsto (Y_1^2 Y_4 : Y_2^2 Y_4 : Y_1 Y_2 Y_3 : Y_4^3)$, which can be seen from the fact that it is invariant under H and induces a map of degree 2^{n-2} on $\mathscr{C}_\delta$. The curve $\mathscr{E}_\delta$ is the image of $\mathscr{C}_\delta$ 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 $\varphi : \mathscr{E}_P \to \mathbb{P}^1$ 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

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

where $\varphi = X$. This model is not smooth at ∞. We denote the branches at infinity by ∞^+ and ∞^-, separated by the two branches of Y/X^2. Which of the two branches is labeled ∞^+ is arbitrary, but fixed. 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 $\Phi(P) = X\big(\pi(P)\big) \in \mathbb{P}^1(K)$, then $\gamma Y\big(\pi(P)\big)^2 \in K(R)$. 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 $P \in \mathscr{C}_P(K)$ leads to a point $G = \pi(P) \in \mathscr{E}_P\big(K(R)\big)$ with $\varphi(G) = \Phi(P) \in \mathbb{P}^1(K)$. If $\mathscr{E}_P$ has a $K(R)$-rational point, then we can make it into an elliptic curve. This places us in the situation of Section 4.2.

Lemmas 3.6, 3.7 and 3.8 apply this procedure to some equations where $\deg(F) = 5$. In those cases, $\mathrm{genus}(\mathscr{C}_\delta) = 5$. For a more general treatment of curves of genus 5 admitting maps to curves of genus 1, see [1], exercise section VI.F.

3.4. Application to covering collections of a hyperelliptic curve. Another interesting

subcover exists if $m = 2$ and n is even, say $n = 2g + 2$. We consider the same construction as in Section 3.3, but now we consider the subgroup $H = \langle \tau_1 \circ \tau_2, \tau_1 \circ \tau_3, \ldots, \tau_1 \circ \tau_{2g+2} \rangle$. The map $H\backslash . : \mathscr{C}_\delta \to \mathscr{D}_\delta$ induces a subcover $\mathscr{C}_\delta \to \mathscr{D}_\delta \to \mathbb{P}^1$. From degree and ramification behaviour, it follows that $\varphi : \mathscr{D}_\delta \to \mathbb{P}^1$ is a double cover that is ramified exactly above $\alpha_1, \ldots, \alpha_{2g+2}$. It follows that $\mathscr{D}_\delta$ is a hyperelliptic curve of genus g and has a model of the form

$$\mathscr{D}_\delta : \gamma Y^2 = F(X, 1).$$

Consequently, the cover $\mathscr{C}_\delta \to \mathscr{D}_\delta$ is unramified and Abelian Galois with $\mathrm{Aut}(\mathscr{C}_\delta/\mathscr{D}_\delta) = (\mathbb{Z}/2\mathbb{Z})^{2g}$. It follows from [17], Proposition 9.1, that $\mathscr{C}_\delta$ is isomorphic to a pullback along the multiplication-by-two map of an embedding of $\mathscr{D}_\delta$ in its Jacobian. The techniques described here to find the primitive solutions to an equation $F(x, y) = Dz^2$ can be used to find the rational points on a hyperelliptic curve. See [3] for a more detailed analysis of this approach.

3.5. Parametrising curves for $x^8 + y^3 = z^2$ and $x^2 \pm y^4 = z^5$. We determine parametrising curves for $x^2 \pm y^4 = z^5$ by first parametrising the primitive solutions to $x^2 \pm u^2 = z^5$ using Theorem 3.2. For each of these parametrisations, we impose $y^2 = u$. This leads to an equation of the type $y^2 = U(s, t)$, so we can again apply Theorem 3.2.

Lemma 3.4. *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 3.5. *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. □

Using Lemmas 3.4 and 3.5 we see that the primitive solutions to $x^2 \pm y^2 = z^5$ can be obtained from the $\{2, 5\}$-primitive solutions to one of the equations

$$y^2 = s(s^4 - 10s^2t^2 + 5t^2),$$

$$y^2 = \frac{1}{2}(s^5 - t^5),$$

$$y^2 = s^5 - 8t^5.$$

According to Theorem 3.2, solutions to equations as mentioned in the lemmas above, are parametrised by the rational points on genus 5 curves. By Section 3.3, these curves cover elliptic curves. The next three lemmas determine these elliptic curves including the induced cover of the projective line. We only give the proof of Lemma 3.7. The proofs for the other lemmas are similar.

Lemma 3.6. *The* $\{2,5\}$*-primitive solutions to* $y^2 = s(s^4 - 10s^2t^2 + 5t^4)$ *have* $s/t = \varphi(P)$*, where* $\varphi : \mathscr{E}_P \to \mathbb{P}^1$ *is a double cover of genus* 1 *over a field* L *and* $P \in \mathscr{E}_P(L)$*. It suffices to take* $\mathscr{E}_1, \ldots, \mathscr{E}_4$ *as described in Table* 1.

j	$\mathscr{E}_j$	$\varphi_j(X, Y)$	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	$Y^2 = X^4 + \rho_5^3X^3 + 2\rho_5X^2 + 2\rho_5^4X + 4\rho_5^2$	X	$\mathbb{Q}(\rho_5)$
9	$(\rho_5^3 + \rho_5^2 - 1)Y^2 = X^4 + \rho_5^3X^3 + 2\rho_5X^2 + 2\rho_5^4X + 4\rho_5^2$	X	$\mathbb{Q}(\rho_5)$
10	$Y^2 = X^4 - 2\rho_3X^3 + 6\rho_3^2X^2 + 8X + 8\rho_3$	X	$\mathbb{Q}(\rho_3)$
11	$Y^2 = R_{11}(X)$	X	$\mathbb{Q}(\alpha)$
12	$Y^2 = R_{12}(X)$	X	$\mathbb{Q}(\alpha)$

$R_{11}, R_{12} \in \mathbb{Q}(\alpha)$ of degree 4. Their coefficients are too large to display here.
Defining relations:

$$\alpha^{12} + 6\alpha^{10} + 39\alpha^8 + 64\alpha^6 + 15\alpha^4 - 6\alpha^2 - 3 = 0,$$
$$\beta^4 - 5\beta^2 + 5 = 0,$$
$$\zeta^4 - \zeta^3 + \zeta^2 - \zeta + 1 = 0,$$
$$\rho_5^5 - 2 = 0,$$
$$\rho_3^3 - 2 = 0.$$

Table 1. Parametrising curves and their fields of definition.

Lemma 3.7. *The* $\{2,5\}$*-primitive solutions to* $2y^2 = s^5 - t^5$ *have* $s/t = \varphi(P)$*, where* $\varphi : \mathscr{E}_P \to \mathbb{P}^1$ *is a double cover of genus* 1 *over a field* L *and* $P \in \mathscr{E}_P(L)$*. It suffices to take* $\mathscr{E}_5, \mathscr{E}_6, \mathscr{E}_7$ *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

$$s - t = 2\,\mathrm{Norm}(\delta)a_4^2,$$

$$s + \zeta t = \delta(a_0 + a_1\zeta + a_2\zeta^2 + a_3\zeta^3)^2$$

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 $\{2, \zeta^3 + \zeta - 1, \zeta\}$. Local arguments at 2 and 5 show 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 3.8. *The $\{2,5\}$-primitive solutions to $y^2 = s^5 - 8t^5$ have $s/t = \varphi(P)$, where $\varphi : \mathscr{E}_P \to \mathbb{P}^1$ is a double cover of genus 1 over a field L and $P \in \mathscr{E}_P(L)$. It suffices to take $\mathscr{E}_8, \mathscr{E}_9$ as in Table 1.*

For the equation $x^8 + y^3 = z^2$, we could proceed in a similar way. First find parametrisations of $u^2 - z^2 = -y^3$, which would express u as a cubic form $U(s,t)$. For each of those forms, we could obtain parametrising curves for $x^4 = U(s,t)$. However, work by Beukers, Edwards and Zagier have already determined parametrisations of $v^4 + y^3 = z^2$.

Lemma 3.9 (Zagier, Edwards)**.** *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 2 holds.*

The first 6 parametrisations in Table 2 were computed by Zagier and first appeared in [2]. The last parametrisation has been found by Edwards [12]. This last parametrisation generates solutions that are weighted homogeneously equivalent to those of the first. If (x_0, y_0, z_0) is a solution to $x^4 + y^3 = z^2$ that can be obtained by specialising s, t in the first parametrisation, then $(2^3x_0, 2^4y_0, 2^6z_0)$ can be obtained from the last parametrisation by taking the same values for s, t. Therefore, if one is only interested in generating weighted homogeneous equivalence classes containing primitive solutions, which is the goal in [2], then the first six parametrisations suffice. However, taking $s = t = 1/2$ in the last parametrisation yields the primitive solution $(x, y, z) = (-7, 15, 76)$. Of course, the equivalence class of this solution is hit by the first parametrisation by taking $s = t = 1$, yielding $(-2^3 \cdot 7, 2^4 \cdot 15, 2^6 \cdot 76)$, but the primitive solution itself cannot be obtained from the first parametrisation. The proof of Lemma 3.9 can be found in [12].

We can use Lemma 3.9 to get a set of equations $x^2 =$ sextic form, whose $\{2,3\}$-primitive solutions contain the primitive solutions to $x^8 + y^3 = z^2$. According to Theorem 3.2, we obtain a finite set of curves of genus 17 that parametrise those solutions. However, if we apply the remark made in Section 3.4, we get an intermediate set of curves. These

$$
\begin{aligned}
\pm x &= (s^2 - 3t^2)(s^4 + 18t^2s^2 + 9t^4),\\
y &= -(s^2 + 2ts + 3t^2)(s^2 - 2ts + 3t^2)(s^2 + 6ts + 3t^2)(s^2 - 6ts + 3t^2),\\
\pm z &= 4st(s^2 + 3t^2)(3s^4 - 2t^2s^2 + 3t^4)(s^4 - 6t^2s^2 + 81t^4),\\
\pm x &= 6st(s^4 + 12t^4),\\
y &= (s^4 - 12t^2s^2 - 12t^4)(s^4 + 12t^2s^2 - 12t^4),\\
\pm z &= (s^4 - 12t^4)(s^8 + 408t^4s^4 + 144t^8),\\
\pm x &= 6st(3s^4 + 4t^4),\\
y &= (3s^4 + 12t^2s^2 - 4t^4)(3s^4 - 12t^2s^2 - 4t^4),\\
\pm z &= (3s^4 - 4t^4)(9s^8 + 408t^4s^4 + 16t^8),\\
\pm x &= s^6 + 40t^3s^3 - 32t^6,\\
y &= -8ts(s^3 - 16t^3)(s^3 + 2t^3),\\
\pm z &= (s^6 + 32t^6)(s^6 - 176t^3s^3 - 32t^6),\\
\pm x &= s^6 + 6s^5t - 15s^4t^2 + 20t^3s^3 + 15s^2t^4 + 30st^5 - 17t^6,\\
y &= 2(s^4 - 4ts^3 - 6t^2s^2 + 4t^3s - 7t^4)(s^4 + 6t^2s^2 - 8t^3s - 3t^4),\\
\pm z &= 3s^{12} - 12ts^{11} + 66t^2s^{10} + 44t^3s^9 - 99t^4s^8 - 792t^5s^7 + 924t^6s^6\\
&\quad - 2376t^7s^5 + 1485t^8s^4 + 1188t^9s^3 - 2046t^{10}s^2 + 156t^{11}s - 397t^{12},\\
\pm x &= 9s^6 - 18ts^5 + 45t^2s^4 - 60t^3s^3 + 15t^4s^2 + 6t^5s - 5t^6,\\
y &= -2(3s^4 - 6t^2s^2 + 8t^3s - t^4)(3s^4 - 12ts^3 + 6t^2s^2 - 4t^3s + 3t^4),\\
\pm z &= 27s^{12} + 324ts^{11} - 1782t^2s^{10} + 3564t^3s^9 - 3267t^4s^8 + 2376t^5s^7 - 2772t^6s^6\\
&\quad + 3960t^7s^5 - 4059t^8s^4 + 2420t^9s^3 - 726t^{10}s^2 + 156t^{11}s - 29t^{12},\\
\pm x &= 2^3(s^2 - 3t^2)(s^4 + 18t^2s^2 + 9t^4),\\
y &= -2^4(s^2 + 2ts + 3t^2)(s^2 - 2ts + 3t^2)(s^2 + 6ts + 3t^2)(s^2 - 6ts + 3t^2),\\
\pm z &= 2^8st(s^2 + 3t^2)(3s^4 - 2t^2s^2 + 3t^4)(s^4 - 6t^2s^2 + 81t^4).
\end{aligned}
$$

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

curves are only of genus 2 and they are considerably less in number. In order to structure the considerable computations we have to do to determine the rational points on the parametrising curves, we formulate the following lemma.

Lemma 3.10. *Let $x, y, z \in \mathbb{Z}$ be a primitive solution to $x^8 + y^3 = z^2$. Then there is a $\mathscr{C} = \mathscr{C}_i$ from Table 3 with $P \in \mathscr{C}(\mathbb{Q})$ and $t \in \mathbb{Q}$ such that $x = t^3 Y(P)$.*

$$
\begin{aligned}
\mathscr{C}_1 &: Y^2 = (X^2 - 3)(X^4 + 18X^2 + 9),\\
\mathscr{C}_2 &: Y^2 = -(X^2 - 3)(X^4 + 18X^2 + 9),\\
\mathscr{C}_3 &: Y^2 = 6X(X^4 + 12),\\
\mathscr{C}_4 &: Y^2 = 6X(3X^4 + 4),\\
\mathscr{C}_5 &: Y^2 = X^6 + 40X^3 - 32,\\
\mathscr{C}_6 &: Y^2 = -X^6 - 40X^3 + 32,\\
\mathscr{C}_7 &: Y^2 = X^6 + 6X^5 - 15X^4 + 20X^3 + 15X^2 + 30X - 17,\\
\mathscr{C}_8 &: Y^2 = -X^6 - 6X^5 + 15X^4 - 20X^3 - 15X^2 - 30X + 17,\\
\mathscr{C}_9 &: Y^2 = X^6 - 6X^5 + 45X^4 - 180X^3 + 135X^2 + 162X - 405,\\
\mathscr{C}_{10} &: Y^2 = -X^6 + 6X^5 - 45X^4 + 180X^3 - 135X^2 - 162X + 405,\\
\mathscr{C}_{11} &: Y^2 = 2(X^2 - 3)(X^4 + 18X^2 + 9),\\
\mathscr{C}_{12} &: Y^2 = -2(X^2 - 3)(X^4 + 18X^2 + 9).
\end{aligned}
$$

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

Proof. Let x, y, z be such a solution. Then, by Lemma 3.9, we have some homogeneous $F \in \mathbb{Z}[S,T]$ of degree 6 as in Table 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 3. Note that, for the curves $\mathscr{C}_3$ and $\mathscr{C}_4$, 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 $\mathscr{C}_9$ and $\mathscr{C}_{10}$ have undergone a small transformation to make $F(X,1)$ monic. □

For some of the curves in Lemma 3.10, it is easy to determine their rational points.

Lemma 3.11. $\mathscr{C}_1(\mathbb{Q}) = \{\infty^+, \infty^-\}$.

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 $\mathscr{C}_1$. The second is covered by $(\pm\sqrt{3}, 0)$, which are quadratic conjugate points. □

Lemma 3.12. *The curves $\mathscr{C}_2$, $\mathscr{C}_6$, $\mathscr{C}_8$, $\mathscr{C}_{10}$, $\mathscr{C}_{11}$ and $\mathscr{C}_{12}$ have no $\mathbb{Q}$-rational points.*

Proof. Each of the curves has no points over $\mathbb{Q}_2$ or $\mathbb{Q}_3$. □

For $\mathscr{C}_3$ and $\mathscr{C}_4$ we consider a curve $\mathscr{C} : y^2 = F(x)$, where $F(x) = Q(x)R(x)$, with $R(x)$ of degree 4. Using this factorisation, we recover an elliptic subcover as in Section 3.3 of the multiplication-by-two cover of the curve $\mathscr{C}$ as in Section 3.4. In Section 4, we develop a method to use elliptic subcovers defined over an extension of the base field for finding the rational points on a curve. If the elliptic subcover is defined over the base field, the method becomes particularly straightforward. It is instructive to see how that method (also used in [6]) works in that case.

Lemma 3.13. $\mathscr{C}_3(\mathbb{Q}) = \{\infty, (0,0)\}$ *and* $\mathscr{C}_4(\mathbb{Q}) = \{\infty, (0,0)\}$.

Proof. We prove the statement for $\mathscr{C}_3(\mathbb{Q})$, the argument for the other curve being similar.

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 $\delta \geqq 0$ from real considerations and that $2 \nmid \delta$ from considerations locally at 2. Both $X^4 + 12 = Y_1^2$ and $X^4 + 12 = 3Y_1^2$ 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. □

For the curves $\mathscr{C}_5$, $\mathscr{C}_7$, $\mathscr{C}_9$, we apply the same argument. We need a non-trivial extension of the base field for that. Since the elliptic curves have positive rank, we need the more refined method developed in the next section. Here, we suffice in giving the elliptic subcovers. Note that, for $\mathscr{C}_7$ and $\mathscr{C}_9$, there is another choice that would yield elliptic curves over a cubic extension. Those elliptic curves have rank 3, which is too high for the method to work.

Lemma 3.14. *The $\mathbb{Q}$-rational points on $\mathscr{C}_5$, $\mathscr{C}_7$ and $\mathscr{C}_9$ correspond to L-rational*

points G on the genus 1 covers $\varphi = X : \mathscr{E}_j \to \mathbb{P}^1$. The choices $\mathscr{E}_{10}$, $\mathscr{E}_{11}$ and $\mathscr{E}_{12}$ respectively, as indicated in Table 1 suffice.

Proof. Let $\mathscr{C} : Y^2 = F(X)$ 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 $(x, y) \in \mathscr{C}(\mathbb{Q})$, 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 to represent one of the finitely many classes in $L(S, 2)$. 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 $\mathscr{C}_7$ and $\mathscr{C}_9$, 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 that the covers in Table 4 are indeed birational to the ones mentioned in the lemma is tedious and straightforward. □

$$
\begin{aligned}
E_3 :\ & (1+\beta-\beta^2)Y^2 = X^3 - 5X^2 + 5X,\\
& \varphi_3(X,Y) = \frac{(6\beta - 2\beta^3)X + 3\beta^3 - 10\beta}{5},\\
E_6 :\ & (\zeta^2-\zeta)Y^2 = X^3 - 5X^2 + 5X,\\
& \varphi_6(X,Y) = \frac{X - 2\zeta^2 + \zeta - 2}{X + \zeta^3 + \zeta^2 - \zeta - 1},\\
E_7 :\ & (\zeta^2-\zeta)Y^2 = X^3 - 5X^2 + 5X,\\
& \varphi_7(X,Y) = \frac{X - 2\zeta^2 + \zeta - 2}{X + \zeta^3 + \zeta^2 - \zeta - 1},\\
E_8 :\ & Y^2 = X^3 - 5X^2 + 5X,\\
& \varphi_8(X,Y) = \frac{-\rho_5^3 X + 2\rho_5^3 Y}{4X - 5},\\
E_9 :\ & (\rho_5^3 + \rho_5^2 - 1)Y^2 = X^3 - 5X^2 + 5X,\\
& \varphi_9(X,Y) = \frac{2(6\rho_5^4 - 4\rho_5^3 + 5\rho_5^2 + 11\rho_5 - 13)X + 12Y - 10(3\rho_5^4 - \rho_5^3 + 4\rho_5 - 6)}{(-4\rho_5^3 + 2\rho_5^2 + 2\rho_5 + 2)X - 12Y - 5(3\rho_5^4 - 3\rho_5^3 + \rho_5^2 - 4)},\\
E_{10} :\ & -6Y^2 = X^3 - X,\\
& \varphi_{10}(X,Y) = \frac{\rho_3 X - 6\rho_3 Y + \rho_3}{2X - 1},\\
E_{11} :\ & \gamma_{11} Y^2 = X^3 + 2X^2 + 2X,\\
E_{12} :\ & \gamma_{12} Y^2 = X^3 + 2X^2 + 2X.
\end{aligned}
$$

The constants γ_{11} and γ_{12} and the maps φ_{11} and φ_{12} are too large to display here.

Table 4. Description of covers with respect to models E_j.

For each of the curves $\mathscr{E}_i$ in Table 1 we have that there is a point $P \in \mathscr{E}_i(L)$ such that $\varphi(P) \in \mathbb{P}^1(\mathbb{Q})$. In particular, we can represent those curves by Weierstrass-models over L. In Table 4 we give these models E_i, together with the transformed covers $\varphi_i : E_i \to \mathbb{P}^1$. See, for instance, [7] for a recipe for obtaining a Weierstrass-model from a quartic together with a rational point.

Lemma 3.15. *The covers $\varphi_i : \mathscr{E}_i \to \mathbb{P}^1$ in Table 1 are isomorphic to the covers $\varphi_i : E_i \to \mathbb{P}^1$ in Table 4.*

4. Chabauty methods using elliptic curves

4.1. 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. Let E be given by a homogeneous 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 $\big(\varphi_1(X, Y, D) : \varphi_2(X, Y, D)\big)$, 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

$$G_{\varphi,1} = c_{12}c_{23} - c_{13}c_{22},$$

$$G_{\varphi,2} = c_{13}c_{21} - c_{11}c_{23},$$

$$G_{\varphi,3} = c_{11}c_{22} - c_{12}c_{21},$$

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. $\tau \in \mathrm{Aut}(\mathscr{E})$ (where $\mathscr{E}$ is the algebraic curve corresponding to E) and $\tau \circ \tau = \mathrm{id}$. From [19], Corollary III.10.2, we know that $\mathrm{Aut}(E)[2] = \{[1], [-1]\}$ and from [19], 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 $G_\varphi \bmod \mathfrak{p} \neq -G_\varphi \bmod \mathfrak{p}$,
- $v_\mathfrak{p}\big(\mathrm{char}(\mathcal{O}/\mathfrak{p})\big) < \mathrm{char}(\mathcal{O}/\mathfrak{p}) - 1$.

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 $Z\big(\mathrm{Exp}_\mathfrak{p}(z)\big) = z \bmod \mathfrak{p}^2$, where $Z = Y/X$. Let $G \in E(L_\mathfrak{p})$ with

$G \bmod \mathfrak{p} \neq G_\tau \bmod \mathfrak{p}$. Then, by choosing coordinates on $\mathbb{P}^1$ (e.g., by interchanging φ_1 and φ_2 if necessary), we can assume that $\varphi(G) \bmod \mathfrak{p} \neq \infty$. Then $\varphi\big(G + \mathrm{Exp}_{\mathfrak{p}}(z)\big)$ 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

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

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

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

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, $\varphi\big(\mathrm{Exp}_{\mathfrak{p}}(Z)\big)$ and $\varphi\big((x,0) + \mathrm{Exp}_{\mathfrak{p}}(Z)\big)$ will be power series in Z^2. Using higher order terms, we derive

$$\varphi\big(\mathrm{Exp}_{\mathfrak{p}}(z)\big) = \frac{c_{11}}{c_{21}} + \frac{G_{\varphi,2}}{\gamma c_{21}} z^2 \bmod \mathfrak{p}^3,$$

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

4.2. Rationality restrictions on elliptic curves. 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 $\mathrm{rk}\big(E(L)\big) < [L : K]$.

By the Mordell-Weil theorem ([19], 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 $\mathcal{O}_L/\mathcal{O}_K$, $v_{\mathfrak{p}}\big(\mathrm{char}(\mathcal{O}/\mathfrak{p})\big) < \mathrm{char}(\mathcal{O}/\mathfrak{p}) - 1$, 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

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

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

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

Consequently, we can write

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

which is convergent for $(n_1, \ldots, n_r) \in (\mathcal{O}_\mathfrak{p})^r$ and has values in $\mathcal{O}_\mathfrak{p}$. If $\varphi(G_0 + \sum n_i B_i) \in \mathbb{P}^1(K)$, then, identifying $\mathbb{P}^1(L)\backslash\{\infty\}$ 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 $\varphi(G_0 + \sum n_i B_i) \in \mathbb{P}^1(K)$ 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 $(n_1, \ldots, n_r)$ for all $\mathfrak{p}, \mathfrak{q} \mid p$ and $i \geqq 1$. 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 $\mathfrak{p}|p$) then it is particularly easy to compute 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.

Lemma 4.1. *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:

- *$f(X_1, \ldots, X_r) = b + AX \bmod \mathfrak{p}$, where A is an $m \times r$ matrix over $\mathcal{O}_\mathfrak{p}$ such that $A \bmod \mathfrak{p}$ has rank r,*

- *$f_i(0, \ldots, 0) = 0$, $\dfrac{\partial f_i}{\partial X_j}(0, \ldots, 0) = 0$ 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 $g(X) = f(X) - b - AX \in (\mathfrak{p}\mathcal{O}_\mathfrak{p}[\![X_1, \ldots, X_r]\!])^m$. If $x \in (\mathcal{O}_\mathfrak{p})^r$ and $f(x) = 0$ then we have that $Ax = -b \bmod \mathfrak{p}$. 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 $e \geqq 1$ 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 $0 = -u^e Ay + g(x) - g(x + u^e y)$. By the assumption on the rank of A and $y \not\equiv 0 \bmod \mathfrak{p}$, it follows that $-u^e Ay \not\equiv 0 \bmod \mathfrak{p}^{e+1}$, 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 $e \geqq 0$ such that $f(u^e y) = 0$. Then $0 = f_i(u^e y) = u^{2e} y^t A_i y \bmod \mathfrak{p}^{2e+1}$. 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 4.1 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

$$\theta_\mathfrak{p}^\infty = \varphi(\infty) + \frac{G_{\varphi,3}}{c_{22}^2} \sum_{i=1}^r n_i Z(B_i) \bmod \mathfrak{p}^2,$$

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

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

$$\theta_\mathfrak{p}^\infty = \frac{c_{11}}{c_{21}} + \frac{G_{\varphi,2}}{\gamma c_{21}} \sum_{i,j=1}^r n_i n_j Z(B_i) Z(B_j) \bmod \mathfrak{p}^3,$$

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

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 $v_\mathfrak{p}\big(Z(B_i)\big) \geqq 1$, 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 $\{B_1, \ldots, B_r\} \subset E(L)$ that generates an $\mathcal{O}_p$-module in $E^{(1)}(L_\mathfrak{p})$ containing $\bigcap\big(E^{(1)}(L_\mathfrak{p}) \cap E(L)\big)$. This means that we only have to prove that

$$\operatorname{char}(\mathcal{O}/p) \nmid \Big[\bigcap_{\mathfrak{p} \mid p} \big(E^{(1)}(L_\mathfrak{p}) \cap E(L)\big) : \langle B_1, \ldots, B_r \rangle\Big],$$

which is much easier to establish. The following lemma is a useful tool.

Lemma 4.2. *Let E be an elliptic curve over a number field L and let $p > 2$ be a rational prime, unramified in $\mathcal{O}_L/\mathbb{Z}$. Suppose that $\mathfrak{p}_1, \ldots, \mathfrak{p}_m$ are the primes of $\mathcal{O}_L$ above p and that for $i = 1, \ldots, m$, we have that E has good reduction at $\mathfrak{p}_i \mid p$ and that $\#(E \bmod \mathfrak{p}_i)(\mathcal{O}/\mathfrak{p}_i)$ 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 $(n_1, \ldots, n_r) \not\equiv (0, \ldots, 0) \bmod p$ 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 $n_1 \operatorname{Log}_{\mathfrak{p}_i}(B_1) + \cdots + n_r \operatorname{Log}_{\mathfrak{p}_i}(B_r) = p \operatorname{Log}_{\mathfrak{p}_i}(G)$. The statement follows by observing that $Z = \operatorname{Log}_{\mathfrak{p}_i} \bmod \mathfrak{p}_i^2$ and that $Z\big(E^{(1)}(L_{\mathfrak{p}_i})\big) = 0 \bmod \mathfrak{p}_i$. □

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 $\bigcap_{i=1}^{m} \big(E^{(1)}(L_{\mathfrak{p}_i}) \cap E(L)\big)$ of index prime to $\operatorname{char}(\mathcal{O}/p)$.

By bounding the number of zeroes of θ^{G_0}, for instance, by using Lemma 4.1, we obtain a bound on the number of $G \in E(L)$ with a K-rational image under φ, with G and G_0 reducing to the same point modulo $\mathfrak{p}_1, \ldots, \mathfrak{p}_m$. This yields the following lemma.

Lemma 4.3. *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 $\theta^G \bmod p \not\equiv 0$, then $\varphi(G) \bmod p$ is not hit by $\varphi\big(E(L)\big) \cap \mathbb{P}^1(K)$.*
- *If $\varphi(G) \in \mathbb{P}^1(K)$ 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. Sketch of proof of Theorems 1.1, 1.2 and 1.3

In Section 3.5, we have reduced the problem of finding the primitive solutions to $x^2 \pm y^4 = z^5$ and $x^8 + y^3 = z^2$ to determining the sets $\varphi_i\big(\mathscr{E}_i(L)\big) \cap \mathbb{P}^1(\mathbb{Q})$ for the covers $\varphi_i : \mathscr{E}_i \to \mathbb{P}^1$ given in Table 1. Here we use the method introduced in Section 4.2 to accomplish this.

Proposition 5.1. *For each of the curves $\mathscr{E}_i$ in Table 1 we have*

i	$\varphi_i(\mathscr{E}_i(L)) \cap \mathbb{P}^1(\mathbb{Q})$	i	$\varphi_i(\mathscr{E}_i(L)) \cap \mathbb{P}^1(\mathbb{Q})$
1	$\{\infty\}$	7	$\{1, 1/3, 3\}$
2	$\{0\}$	8	$\{0, -2, \infty\}$
3	$\{0\}$	9	$\{\infty\}$
4	$\{0\}$	10	$\{0, 1, \infty\}$
5	$\{\infty\}$	11	$\{1/2, \infty\}$
6	$\{1, -1\}$	12	$\{\infty, 9/2\}$

Proof. We apply the method proposed in Section 4.2 to each of the curves individually. We work with the twisted Weierstrass models E_i from Table 4 instead of the models $\mathscr{E}_i$. The map $X : \mathscr{E}_i \to \mathbb{P}^1$ 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 $\varphi_4 : \mathscr{E}_4 \to \mathbb{P}^1$ and $\varphi_3 : \mathscr{E}_3 \to \mathbb{P}^1$. Consequently, the statement on $\mathscr{E}_4$ follows from the one on $\mathscr{E}_3$. 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 [10]) and is available via [5] from the preprint server of the Mathematical Institute of Leiden University or through the author's homepage.

We put $K = \mathbb{Q}$, $L = \mathbb{Q}(\zeta)$, $E = E_7$ and $\varphi = \varphi_7$. Consider the points

$$G_1 = (1 - 3\zeta^2 + 3\zeta^3, 1 + 3\zeta - 2\zeta^2 + \zeta^3),$$
$$G_2 = (1 - 1\zeta^2 + \zeta^3, \zeta^3),$$
$$G_3 = (2 - \zeta^2 + \zeta^3, 0),$$
$$G_4 = (0, 0).$$

From a 2-isogeny descent, it follows that $\langle G_1, \ldots, G_4 \rangle \subset E(L)$ is a subgroup of odd index. One would expect that $G_1, \ldots, G_4$ in fact generate $E(L)$, but we don't need to prove that. As we will see, it is sufficient to show that the index is coprime to $2 \cdot 31$.

We choose $p = 31$ and we consider the four primes $\mathfrak{p}_1, \ldots, \mathfrak{p}_4$ above 31 characterised by

$$\zeta \bmod \mathfrak{p}_1 = 15, \quad \zeta \bmod \mathfrak{p}_3 = 27,$$
$$\zeta \bmod \mathfrak{p}_2 = 23, \quad \zeta \bmod \mathfrak{p}_4 = 29.$$

Since $\#(E \bmod \mathfrak{p}_i)(\mathscr{O}/\mathfrak{p}_i) = 32$, we see that $[E(L) \bmod \mathfrak{p}_i : \langle G_1, \ldots, G_4 \rangle \bmod \mathfrak{p}_i]$ is a power of 2. We know that $[E(L) : \langle G_1, \ldots, G_4 \rangle]$ is odd, so we have $E(L) \bmod \mathfrak{p}_i = \langle G_1, \ldots, G_4 \rangle \bmod \mathfrak{p}_i$.

It is straightforward to compute that

$$\begin{aligned}\langle G_1,\dots,G_4\rangle \cap E^{(1)}(L_{\mathfrak{p}_i}) = \langle &2G_1+G_2+G_4, 4G_2+G_4\rangle,\\ &\langle 2G_1+3G_2+G_4, 4G_2+G_1+G_2\rangle,\\ &\langle 2G_1+G_2+G_3, 4G_2+G_3+G_4\rangle,\\ &\langle 2G_1+3G_2, 4G_2+G_4\rangle \quad \text{for } i=1,2,3,4\end{aligned}$$

respectively. Consequently, $B_1 = 8G_1 + 4G_2$, $B_2 = 8G_2$ generate the intersection of the kernels of reduction.

In order to determine $\varphi\big(E(L)\big) \cap \mathbb{P}^1(\mathbb{Q})$, we first look at the reduction mod 31. If $P \in \varphi\big(E(L)\big) \cap \mathbb{P}^1(\mathbb{Q})$, then certainly $P \bmod 31 \in \varphi\big(E(L)\big) \bmod \mathfrak{p}_i$. The latter is something we can compute explicitly. We find

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

It follows that $\varphi\big(E(L)\big) \cap \mathbb{P}^1(\mathbb{Q}) \bmod 31 \subset \{1,2,3,16,21\}$. 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

$$\varphi\big(E(L) \cap \mathbb{P}^1(\mathbb{Q})\big) \bmod 31 \subset \{1,3,1/3\}.$$

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 4.3. If $\varphi(G) \in \mathbb{P}^1(\mathbb{Q})$, we know that $G \in G_0 + \bigcap_i E^{(1)}(L_{\mathfrak{p}_i}) \cap E(L)$, for G_0 or $G_\tau - G_0$ a member of $\{0, G_1 - G_2 + G_4, G_1 + G_2 + G_4\}$. We would expect $\langle B_1, B_2\rangle$ to be the intersection of the kernels of reduction, but we only need that

$$\langle B_1, B_2\rangle \otimes \mathbb{Z}_{31} = \Big(\bigcap_i E^{(1)}(L_{\mathfrak{p}_i}) \cap E(L)\Big) \otimes \mathbb{Z}_{31}.$$

We compute $Z(B_1), Z(B_2) \bmod \mathfrak{p}_i^2$. We do that either by performing the group addition with exact precision and then reduce mod $\mathfrak{p}_i^2$ or (more efficiently), do the group operations with finite $\mathfrak{p}_i$-adic precision. Either way, we find the values

$$\begin{pmatrix} Z(B_1)/31 \bmod \mathfrak{p}_1 & Z(B_2)/31 \bmod \mathfrak{p}_1\\ Z(B_1)/31 \bmod \mathfrak{p}_2 & Z(B_2)/31 \bmod \mathfrak{p}_2\\ Z(B_1)/31 \bmod \mathfrak{p}_3 & Z(B_2)/31 \bmod \mathfrak{p}_3\\ Z(B_1)/31 \bmod \mathfrak{p}_4 & Z(B_2)/31 \bmod \mathfrak{p}_4 \end{pmatrix} = \begin{pmatrix} 21 & 8\\ 2 & 2\\ 0 & 15\\ 22 & 27 \end{pmatrix}.$$

By applying Lemma 4.2 to these, we get that $\langle G_1, \ldots, G_4 \rangle$ has index prime to 31 in $E(L)$. This implies B_1, B_2 indeed generate the intersections of the kernels of reduction as $\mathbb{Z}_{31}$-modules.

Using these values we can compute approximations to $\theta^{G_0}(n_1, n_2)$, as described in Section 4.2. It is easily checked that in each case, one of the criteria in Lemma 4.3 applies. We conclude that $a \in \varphi\big(E(L)\big) \cap \mathbb{P}^1(\mathbb{Q})$ with $a \bmod 31 \in \{1, 3, 21\}$ are $a = 1, 3, 1/3$. □

Proof of Theorem 1.1. Consider $x^2 + y^4 = z^5$. Lemma 3.4 together with Lemma 3.6 show that the curves $\mathscr{E}_1, \ldots, \mathscr{E}_4$ from Table 1 parametrise the primitive solutions and in what way the parameter values s/t can be recovered from the points $P \in \mathscr{E}_i(L)$ with $\varphi_i(P) \in \mathbb{P}_1(\mathbb{Q})$. Proposition 5.1 gives 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 3.5, 3.7 and 3.8 show that $\mathscr{E}_5, \ldots, \mathscr{E}_9$ determine all possible solutions. Proposition 5.1 gives the possible candidates and the values of s/t belonging to them. The values $s/t = \infty, 1, -1$ in Lemma 3.7 lead to solutions with $z = 0$, $y = 0$ or $x = 0$. The values $s/t = 3, 1/3$ lead to $x = \pm 122$, $y = \pm 11$, $z = 3$.

The points on $\mathscr{E}_8(L)$ lead to $s/t = 1, \infty, -2$. These correspond to $(x, y, z) = (0, \pm 1, -1)$ and $(\pm 16, \pm 4, 0)$. While $\big(-2, 2(\alpha - \alpha^2 - \alpha^3)\big)$ is a genuine point on $\mathscr{E}_8(L)$, 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 3.8. The point on $\mathscr{E}_9(L)$ leads to $(x, y, z) = (\pm 7, \pm 3, -2)$. □

Proof of Theorem 1.3. Lemma 3.10 shows that the primitive solutions to $x^8 + y^3 = z^2$ can be obtained from rational points on the curves $\mathscr{C}_i$ in Table 3. For most curves, we already determined the rational points. Lemma 3.14 establishes that the rational points on $\mathscr{C}_5$, $\mathscr{C}_7$ and $\mathscr{C}_9$ can be obtained from $\mathscr{E}_{10}$, $\mathscr{E}_{11}$ and $\mathscr{E}_{12}$. Proposition 5.1 gives the necessary information to do that.

We now complete our proof by checking to which solutions the rational points on $\mathscr{C}_1, \ldots, \mathscr{C}_{10}$ correspond. Since at least one of the forms for x, y, z in Lemma 3.9, corresponding to $\mathscr{C}_1, \ldots, \mathscr{C}_6$, is divisible by s and t, points with $X = 0, \infty$ correspond to solutions with $xyz = 0$. This only leaves $(1, \pm 3)$ on $\mathscr{C}_5$. 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 $\mathscr{C}_7$, 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 $\mathscr{C}_9$, $\infty^{\pm}$ 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. □

References

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

[2] *Frits Beukers*, The Diophantine equation $Ax^p + By^q = Cz^r$, Duke Math. J. **91**(1) (1998), 61–88.
[3] *Nils Bruin* and *E. Victor Flynn*, Towers of 2-covers of hyperelliptic curves, Technical Report PIMS-01-12, PIMS, 2001, http://www.pims.math.ca/publications/#preprints.
[4] *Nils Bruin*, Chabauty Methods and Covering Techniques applied to Generalised Fermat Equations, PhD thesis, Universiteit Leiden, 1999.
[5] *Nils Bruin*, Chabauty methods using elliptic curves, Technical Report W99-14, University of Leiden, 1999, http://www.math.leidenuniv.nl/reports/1999-14.shtml.
[6] *Nils Bruin*, The diophantine equations $x^2 \pm y^4 = \pm z^6$ and $x^2 + y^8 = z^3$, Compos. Math. **118** (1999), 305–321.
[7] *J. W. S. Cassels*, Lectures on Elliptic Curves, LMS-ST 24, University Press, Cambridge 1991.
[8] *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.
[9] *Claude Chabauty*, Sur les points rationnels des variétés algébriques dont l'irrégularité est supérieure à la dimension, C. R. Acad. Sci. Paris **212** (1941), 1022–1024.
[10] *M. Daberkow*, *C. Fieker*, *J. Klüners*, *M. Pohst*, *K. Roegner*, *M. Schörnig*, and *K. Wildanger*, KANT V4, J. Symbolic Comput. **24**(3–4) (1997), 267–283, ftp://ftp.math.tu-berlin.de/pub/algebra/Kant/Kash.
[11] *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**(6) (1995), 513–543.
[12] *Johnny Edwards*, A complete solution of $x^2 + y^3 + z^5 = 0$, http://www.math.uu.nl/people/edwards/icosahedron.ps, 2001.
[13] *G. Faltings*, Endlichkeitssätze für abelsche Varietäten über Zahlkörpern, Invent. Math. **73**(3) (1983), 349–366.
[14] *E. V. Flynn*, A flexible method for applying Chabauty's theorem, Compos. Math. **105** (1997), 79–94.
[15] *E. V. Flynn*, *Bjorn Poonen*, and *Edward F. Schaefer*, Cycles of quadratic polynomials and rational points on a genus-2 curve, Duke Math. J. **90**(3) (1997), 435–463.
[16] *E. V. Flynn* and *J. L. Wetherell*, Finding rational points on bielliptic genus 2 curves, Man. Math., to appear.
[17] *J. S. Milne*, Jacobian varieties, in: Arithmetic geometry (Storrs, Conn., 1984), G. Cornell and J. H. Silverman, eds., Springer, New York (1986), 167–212.
[18] *David Mumford*, Abelian varieties, Tata Inst. Fund. Res. Stud. Math. **5** (1970).
[19] *Joseph H. Silverman*, The Arithmetic of Elliptic Curves, GTM 106, Springer-Verlag, 1986.
[20] *R. Tijdeman*, Diophantine equations and Diophantine approximations, in: Number theory and applications (Banff, AB, 1988), Kluwer Acad. Publ., Dordrecht (1989), 215–243.
[21] *Joseph L. Wetherell*, Bounding the number of rational points on certain curves of high rank, PhD thesis, U.C. Berkeley, 1997.

Department of Mathematics, Simon Fraser University, Burnaby BC V5A 1S6, Canada
e-mail: bruin@member.ams.org

Eingegangen 6. November 2000, in revidierter Fassung 30. April 2002