PARTIAL DESCENT ON HYPERELLIPTIC CURVES AND THE GENERALIZED FERMAT EQUATION $x^3 + y^4 + z^5 = 0$

SAMIR SIKSEK AND MICHAEL STOLL

ABSTRACT. Let $C : y^2 = f(x)$ be a hyperelliptic curve defined over $\mathbb{Q}$. Let K be a number field and suppose f factors over K as a product of irreducible polynomials $f = f_1 f_2 \dots f_r$. We shall define a "Selmer set" corresponding to this factorization with the property that if it is empty then $C(\mathbb{Q}) = \emptyset$. We shall demonstrate the effectiveness of our new method by solving the generalized Fermat equation with signature $(3, 4, 5)$, which is unassailable via the previously existing methods.

1. Introduction

Let f be a separable polynomial with coefficients in $\mathbb{Z}$ and degree $d \geq 3$. Let C be the non-singular projective hyperelliptic curve with affine patch

$$C : y^2 = f(x).$$

One is interested in studying the set of rational points on $C(\mathbb{Q})$ and, in particular, deciding whether $C(\mathbb{Q})$ is empty or not. Several techniques have been developed to attack this problem [5], [6], [7], [8]. The easiest general method is the "two-cover descent" of Bruin and Stoll [7]. Let L be the étale algebra $L = \mathbb{Q}[x]/f$; this algebra is the direct sum of number fields. Bruin and Stoll define a map from $C(\mathbb{Q})$ to a group H which is either $L^\times/(L^\times)^2$ or $L^\times/(\mathbb{Q}^\times(L^\times)^2)$ depending on the parity of d.[1] They show how to compute a finite subset of H, which they call the "fake 2-Selmer set", that contains the image of $C(\mathbb{Q})$ in H. If this fake 2-Selmer set is empty then so is $C(\mathbb{Q})$.

The computation of the fake Selmer set requires explicit knowledge of the class and unit groups of the number fields that are the direct summands of L. If these number fields have large degrees or discriminants, then this computation is impractical. In this paper, we look at the situation where there is a number field K of relatively small degree such that f factors over K into a product $f = f_1 f_2 \cdots f_r$ of irreducible factors. We define an appropriate "Selmer set" whose computation demands the knowledge of the class group and units of K but not of larger number fields. This can be helpful either in proving the non-existence of rational points on our hyperelliptic curve, or in the construction of unramified covers that can help in the determination of the set of rational points. We call our method "partial descent" as the information it yields is usually weaker than the information given by the fake 2-Selmer set. We explain this in more detail in Section 2 below.

We shall demonstrate the effectiveness of our new method by solving the generalized Fermat equation with signature $(3, 4, 5)$.

Let p, q, $r \in \mathbb{Z}_{\geq 2}$. The equation

$$x^p + y^q = z^r \tag{1}$$

Date: July 4, 2011.

2000 *Mathematics Subject Classification.* Primary 11G30, Secondary 11G35, 14K20, 14C20.

Key words and phrases. Hyperelliptic curves, descent, Fermat-Catalan, generalized Fermat equation, Selmer set.

The first-named author is supported by an EPSRC Leadership Fellowship.

[1] $R^\times$ denotes the multiplicative group of an algebra R, and $(R^\times)^2$ denotes the subgroup of squares.

is known as the *generalized Fermat equation* (or the *Fermat-Catalan* equation) with signature (p, q, r). As in Fermat's Last Theorem, one is interested in non-trivial primitive integer solutions. An integer solution (x, y, z) is said to be *non-trivial* if $xyz \neq 0$, and *primitive* if x, y, z are coprime. Let $\chi = p^{-1} + q^{-1} + r^{-1}$. The parametrization of non-trivial primitive integer solutions for (p, q, r) with $\chi \geq 1$ has now been completed ([3], [14]). The generalized Fermat Conjecture [11], [12] is concerned with the case $\chi < 1$. It states that—up to sign and permutation—the only non-trivial primitive solutions to (1) with $\chi < 1$ are

$$1 + 2^3 = 3^2, \quad 2^5 + 7^2 = 3^4, \quad 7^3 + 13^2 = 2^9, \quad 2^7 + 17^3 = 71^2,$$
$$3^5 + 11^4 = 122^2, \quad 17^7 + 76271^3 = 21063928^2, \quad 1414^3 + 2213459^2 = 65^7,$$
$$9262^3 + 15312283^2 = 113^7, \quad 43^8 + 96222^3 = 30042907^2, \quad 33^8 + 1549034^2 = 15613^3.$$

The generalized Fermat Conjecture has been established for many signatures (p, q, r), including for several infinite families of signatures: Fermat's Last Theorem (p, p, p) by Wiles and Taylor [28], [26]; $(p, p, 2)$ and $(p, p, 3)$ by Darmon and Merel [13]; $(2, 4, p)$ by Ellenberg [15] and Bennett, Ellenberg and Ng [2]; $(2p, 2p, 5)$ by Bennett [1]. Recently, Chen and Siksek [9] have solved the generalized Fermat equation with signatures $(3, 3, p)$ for a set of prime exponents p having Dirichlet density 28219/44928. For exhaustive surveys see [10, Chapter 14] and [3]. An older but still very useful survey is [17]. An up-to-date list of partial results with references is found in [21]. It appears that the 'smallest' signature (p, q, r) for which the equation has not yet been resolved is $(3, 4, 5)$, in the sense that it is the only signature with $\max\{p, q, r\} \leq 5$ that is still open. In this paper we shall prove the following theorem.

Theorem 1.1. *The only primitive integer solutions to the equation*

$$x^3 + y^4 + z^5 = 0 \tag{2}$$

are the trivial solutions $(0, \pm 1, -1)$, $(-1, 0, 1)$, $(1, 0, -1)$, $(-1, \pm 1, 0)$.

Our proof proceeds as follows. Edwards [14] parametrized the primitive solutions to the generalized Fermat equation $x^2 + y^3 + z^5 = 0$. Using this parametrization, we reduce the resolution of (2) to the determination of the set of rational points on 49 hyperelliptic curves $C_i : y^2 = f_i(x)$ where the polynomial f_i has degree 30 (and so the curves are of genus 14). Of these 49 we can eliminate 26 using local considerations, which leaves 23 curves C_i. These include 13 'difficult' curves where the f_i are irreducible. An application of the method of Bruin and Stoll would require the computation of the class and unit groups of number fields of degree 30, which is impractical at present. However, in these 13 cases there are number fields K_i of degree 5 such that f_i becomes reducible over K_i; we shall show that an appropriate Selmer set corresponding to this factorization is empty, and deduce that $C_i(\mathbb{Q}) = \emptyset$. For the ten remaining cases, our Selmer sets are non-empty, but we use them to construct unramified covers of the C_i. It turns out that these unramified covers have low genus quotients for which it is easy to determine the rational points. In this way we can first determine the set of rational points on each of the unramified covers and then on the remaining curves C_i.

We are grateful to Don Zagier for suggesting to us that (2) is the 'next case' of the generalized Fermat conjecture. The first-named author would like to thank John Cremona, Sander Dahmen and Michael Mourao for helpful discussions.

2. Partial Descent on Hyperelliptic Curves

We will use $\mathcal{G}$ to denote the absolute Galois group of $\mathbb{Q}$.

It is convenient to adopt homogeneous coordinates for hyperelliptic curves. Let $f(u,v)$ be a squarefree binary form of even degree $2d \geq 4$ with rational integer coefficients. Let

$$C : y^2 = f(u,v) \tag{3}$$

be the hyperelliptic curve of genus $g = d-1$ associated to f in weighted projective space $\mathbb{P}_{(1,1,d)}$, where u, v, y are respectively given weights 1, 1 and d. Then C is covered by the two affine curves $y^2 = f(x,1)$ and $y^2 = f(1,x)$. To avoid having to deal with special cases, we will assume that $f(1,0) \neq 0$ (so that $f(x,1)$ has degree $2d$). If $f(1,0) = 0$, then we have to work with an extra factor v in the factorization of f below, and everything goes through in much the same way.

Over $\bar{\mathbb{Q}}$, we can write

$$f(u,v) = c(u-\theta_1 v)\cdots(u-\theta_{2d}v)$$

where $c \in \mathbb{Q}^\times$ is the leading coefficient of $f(x,1)$ and the $\theta_j \in \bar{\mathbb{Q}}$ are the (pairwise distinct) roots of $f(x,1)$. Let $\Theta = \{\theta_1, \ldots, \theta_{2d}\}$; this is a set on which the absolute Galois group of $\mathbb{Q}$ acts. Denote by

$$L = \mathrm{Map}_{\mathbb{Q}}(\Theta, \bar{\mathbb{Q}}) \cong \mathbb{Q}[T]/(f(T,1))$$

the corresponding étale algebra (its elements are Galois-equivariant maps from Θ to $\bar{\mathbb{Q}}$). This algebra L decomposes as a product of number fields corresponding to the Galois orbits on Θ, or equivalently, to the irreducible factors of f in $\mathbb{Q}[u,v]$. Given elements $\alpha \in L^\times$ and $s \in \mathbb{Q}^\times$ such that $cN_{L/\mathbb{Q}}(\alpha) = s^2$, we can define a curve $D_{\alpha,s} \subset \mathbb{P}^{2d-1} \times C$ by declaring that

$$\big((z_1 : \ldots : z_{2d}), (u : v : y)\big) \in D_{\alpha,s}$$
$$\iff \exists a \neq 0 \text{ such that } \forall 1 \leq j \leq 2d : \alpha(T_j) z_j^2 = a(u - \theta_j v) \text{ and } s z_1 \cdots z_{2d} = a^d y\,.$$

(We consider $\alpha \in L$ as a map $\alpha : \Theta \to \bar{\mathbb{Q}}$.) It is clear that the condition is invariant under scaling and under the action of the Galois group $\mathcal{G}$, so that $D_{\alpha,s}$ is defined over $\mathbb{Q}$. Note that the hyperelliptic involution on C induces an isomorphism between $D_{\alpha,s}$ and $D_{\alpha,-s}$, and both curves are isomorphic to their common projection D_α to $\mathbb{P}^{2d-1}$. Projection to the second factor induces a covering map $\pi_{\alpha,s} : D_{\alpha,s} \to C$. It can be checked that this map is an unramified covering of C of degree $2^{2d-2} = 2^{2g}$; more precisely, $\pi_{\alpha,s}$ is a C-torsor under $J[2]$, the 2-torsion subgroup of the Jacobian variety J of C: a *2-covering* of C. Two such 2-coverings $\pi_{\alpha,s}$ and $\pi_{\beta,t}$ are isomorphic over $\mathbb{Q}$ as coverings of C if and only if there are $\gamma \in L^\times$ and $w \in \mathbb{Q}^\times$ such that $\beta = \alpha\gamma^2 w$ and $t = sN_{L/\mathbb{Q}}(\gamma)w^d$. The set of isomorphism classes of 2-coverings of C that have points everywhere locally is called the *2-Selmer set* $\mathrm{Sel}^{(2)}(C/\mathbb{Q})$ of C. Since it can be shown that every such 2-covering can be realized in the form $\pi_{\alpha,s}$, it follows that the 2-Selmer set can be identified with a subset of

$$H_c = \frac{\{(\alpha,s) \in L^\times \times \mathbb{Q}^\times : cN_{L/\mathbb{Q}}(\alpha) = s^2\}}{\{(\gamma^2 w, N_{L/\mathbb{Q}}(\gamma)w^d) : \gamma \in L^\times, w \in \mathbb{Q}^\times\}}\,.$$

(The group below acts on the set above by multiplication; the quotient is with respect to this group action.) It is known that the 2-Selmer set is finite. The image of $\mathrm{Sel}^{(2)}(C/\mathbb{Q})$ under the map to $L^\times/(\mathbb{Q}^\times(L^\times)^2)$ is known as the *fake 2-Selmer set* $\mathrm{Sel}^{(2)}_{\mathrm{fake}}(C/\mathbb{Q})$ of C. The map $\mathrm{Sel}^{(2)}(C/\mathbb{Q}) \to \mathrm{Sel}^{(2)}_{\mathrm{fake}}(C/\mathbb{Q})$ is either a bijection or two-to-one. There is a natural map $C(\mathbb{Q}) \to \mathrm{Sel}^{(2)}(C/\mathbb{Q})$ given on points with nonvanishing y-coordinate by

$$\delta : C(\mathbb{Q}) \ni (u_0 : v_0 : y_0) \longmapsto [u_0 - Tv_0, y_0] \in H_c$$

(where the square brackets denote the element represented by $(u_0 - Tv_0, y_0)$ and $T \in L$ is the identity map). If $y_0 = 0$, then we have $v_0 \neq 0$, and we can write

$$f(u,v) = c(u-\theta_0 v)\tilde{f}(u,v) \quad \text{with} \quad \tilde{f}(x,1) \text{ monic},$$

where $\theta_0 = u_0/v_0$. Then we set (compare [22] and [20])

$$\delta\big((u_0 : v_0 : 0)\big) = [\theta_0 - T + c\tilde{f}(T,1), c\tilde{f}(\theta_0,1)].$$

Therefore if the 2-Selmer set or the fake 2-Selmer set of C is empty, then C cannot have any rational points. The map δ above has the property that if the image of $P \in C(\mathbb{Q})$ under δ corresponds to $\pi_{\alpha,s}$, then $P = \pi_{\alpha,s}(Q)$ for some $Q \in D_\alpha(\mathbb{Q})$. Denoting the analogues of H_c and δ over $\mathbb{Q}_p$ by $H_{c,p}$ and δ_p, and writing $\rho_p : H_c \to H_{c,p}$ for the canonical map, we have that

$$\mathrm{Sel}^{(2)}(C/\mathbb{Q}) = \{h \in H_c : \rho_p(h) \in \operatorname{Im}\delta_p \text{ for all places } p \text{ of } \mathbb{Q}\}\,.$$

For a detailed account of the theory of 2-descent on hyperelliptic curves, see [7]. There it is shown how the fake 2-Selmer set can be computed if one can determine the class group of L (i.e., the class groups of the various number fields occurring as factors of L) and an odd-index subgroup of the group of units of L (dito). Now if the irreducible factors of f have large degree, then this information may be hard or next to impossible to get. So we would like to be able to compute some kind of intermediate Selmer set with less effort, at the price of potentially obtaining less information. This is the 'partial 2-descent' that we now describe.

We first define a different model of $D_{\alpha,s}$ that includes a lot of redundant variables. We denote by Π the set of all subsets of the set $\Theta = \{\theta_1, \ldots, \theta_{2d}\}$ of roots of f. We will frequently identify elements φ of Π with the corresponding factor $\prod_{\theta\in\varphi}(u - \theta v)$ of f. For any $\mathcal{G}$-invariant subset Y of Π, we let $\mathbb{P}_Y$ be the weighted projective space over $\mathbb{Q}$ whose coordinates correspond to the elements of Y, with weights given by their cardinality (as subsets of Θ) or degrees (as factors of f), and with twisted Galois action given by the $\mathcal{G}$-action on Y. We write z_φ for the coordinate corresponding to $\varphi \in Y$. Then we can define an embedding

$$\jmath : \mathbb{P}_\Theta \longrightarrow \mathbb{P}_\Pi\,, \quad (z_1 : \ldots : z_{2d}) \longmapsto (\ldots : \prod_{i:\theta_i\in\varphi} z_i : \ldots)$$

where the product gives the z_φ-coordinate of the image point. Now we let

$$\tilde{D}_{\alpha,s} = (\jmath \times \mathrm{id}_C)(D_{\alpha,s}) \subset \mathbb{P}_\Pi \times C\,.$$

For each $\mathcal{G}$-invariant subset $Y \subset \Pi$, there is a projection $\pi_Y : \mathbb{P}_\Pi \to \mathbb{P}_Y$. We obtain a commutative diagram

$$\begin{array}{ccc} \tilde{D}_{\alpha,s} & \xrightarrow{\ \tilde{\pi}_{\alpha,s}\ } & C \\ & {\scriptstyle \pi_Y\times\mathrm{id}} \searrow \quad \nearrow {\scriptstyle \pi_{\alpha,s,Y}} & \\ & D_{\alpha,s,Y} & \end{array}$$

We write $\pi_{\alpha,s,Y}$ for the restriction of the second projection $\mathrm{pr}_2 : \mathbb{P}_Y \times C \to C$ to the image $D_{\alpha,s,Y}$ of $\tilde{D}_{\alpha,s}$ under $\pi_Y \times \mathrm{id}_C$. With these notations, $D_{\alpha,s} = D_{\alpha,s,\Theta}$ and $\pi_{\alpha,s} = \pi_{\alpha,s,\Theta}$, and similarly $\tilde{D}_{\alpha,s} = D_{\alpha,s,\Pi}$, $\tilde{\pi}_{\alpha,s} = D_{\alpha,s,\Pi}$.

Let μ_2^Θ be the Galois module whose elements are the maps $\Theta \to \mu_2$, with pointwise multiplication and Galois action induced by that on Θ. Then $\mu_2^\Theta = \mu_2(\bar{L})$, where $\bar{L} = L \otimes_{\mathbb{Q}} \bar{\mathbb{Q}}$. It is well-known that

$$J[2] \cong \frac{\ker(N : \mu_2^\Theta \to \mu_2)}{\mu_2} = \frac{\ker(N_{\bar{L}/\bar{\mathbb{Q}}} : \mu_2(\bar{L}) \to \mu_2)}{\mu_2}$$

as Galois modules, where N maps an element of μ_2^Θ to the product of its entries. The elements of μ_2^Θ correspond to the subsets of Θ in a natural way by

$$\alpha \longmapsto \{\theta \in \Theta : \alpha(\theta) = -1\}\,. \tag{4}$$

The 2-torsion points therefore correspond to the partitions of Θ into two sets of even cardinality, and addition in $J[2]$ corresponds to taking symmetric differences. The action of $J[2]$ on a covering $D_{\alpha,s}$ is given in this setting by

$$P + \big((z_1 : \ldots : z_{2d}), Q\big) = \big((\alpha(\theta_1)z_1 : \ldots : \alpha(\theta_{2d})z_{2d}), Q\big)$$

where $P \in J[2]$ is represented by $\alpha \in \mu_2^\Theta$. Similarly, the action on $D_{\alpha,s,Y}$ is given by multiplying z_φ with $\prod_{\theta\in\varphi}\alpha(\theta)$, for all $\varphi \in Y$.

We use this description to find the group $\Gamma_Y \subset J[2]$ of deck transformations of the covering $\tilde{D}_{\alpha,s} \to D_{\alpha,s,Y}$. Its elements are represented by those $\alpha \in \mu_2^\Theta$ with $N(\alpha) = 1$ for which there is $\varepsilon \in \mu_2$ such that $\prod_{\theta\in\varphi}\alpha(\theta) = \varepsilon^{\#\varphi}$ for all $\varphi \in Y$. Since we can replace α by $\alpha\varepsilon$, we can take $\varepsilon = 1$. By Galois theory, it follows that $\pi_{\alpha,s,Y} : D_{\alpha,s,Y} \to C$ is (geometrically) Galois with Galois group $G_Y \cong J[2]/\Gamma_Y$. This group G_Y is dual to the annihilator of Γ_Y under the Weil pairing on $J[2]$. Recall that the Weil pairing is determined by the parity of the cardinality of the intersections of the sets in the partitions corresponding to two elements of $J[2]$. If we identify Y with a subset of μ_2^Θ via (4), then the dual group $G_Y^\vee$ is the image of $\langle Y\rangle \cap \ker N$ in $J[2] = (\ker N)/\mu_2$.

If $G_Y^\vee$ is neither trivial nor all of $J[2]$, then we obtain intermediate coverings. It should be noted that this is not possible in the generic case when the Galois group of f is the full symmetric group S_{2d}, since then the minimal $\mathcal{G}$-invariant subsets Y of Π contain all subsets of some fixed cardinality, and each such Y either generates all of $J[2]$ or the trivial group (when $Y = \{\Theta\}$ or $Y = \{\emptyset\}$). However, in many cases of interest, there are additional symmetries present that lead to smaller Galois groups, so that intermediate coverings may be available.

We want to generalize our setting for Selmer sets. To this end, we proceed similarly as above. We denote by L_Y the étale $\mathbb{Q}$-algebra corresponding to the $\mathcal{G}$-set Y (then $L = L_\Theta$). We have the subgroup

$$U_\Pi = \{\alpha \in L_\Pi^\times : \alpha(\varphi) = \prod_{\theta\in\varphi}\alpha(\{\theta\}) \text{ for all } \varphi \in \Pi\} \subset L_\Pi^\times$$

with an embedding

$$\iota_\Pi : \mathbb{Q}^\times \longrightarrow U_\Pi\,, \quad a \longmapsto (\varphi \mapsto a^{\#\varphi})\,,$$

the set

$$V_{c,\Pi} = \{(\alpha, s) \in U_\Pi \times \mathbb{Q}^\times : c\alpha(\Theta) = s^2\} \subset U_\Pi \times \mathbb{Q}^\times\,,$$

on which the group

$$W_\Pi = \{(\gamma^2\iota_\Pi(a), a^d\gamma(\Theta)) : \gamma \in U_\Pi, a \in \mathbb{Q}^\times\} \subset V_{1,\Pi}$$

acts, and the quotient set

$$H_{c,\Pi} = V_{c,\Pi}/W_\Pi\,.$$

We can extend the map $\delta : C(\mathbb{Q}) \to H_c$ to a map

$$\delta_\Pi : C(\mathbb{Q}) \longrightarrow H_{c,\Pi}\,, \quad (u_0 : v_0 : y_0) \longmapsto [\varphi \mapsto \varphi(u_0, v_0), y_0]$$

where $[\alpha, s]$ denotes the class of (α, s) and $\varphi(u, v) = \prod_{\theta\in\varphi}(u - \theta v)$. If $y_0 = 0$, the definition has to be changed suitably, see the definition of δ above.

For the following, we will assume that Y contains a partition X of Θ, and that for every $\varphi \in Y$, there is a partition of Θ contained in Y that has φ as an element. (If necessary, we can extend Y by adding the complements of its elements; this does not change the covering group G_Y nor the fields that occur as components of L_Y.) Then, using the obvious projections $\pi_Y : L_\Pi \to L_Y$, we can define a group $U_Y = \pi_Y(U_\Pi)$ with a map $\iota_Y : \mathbb{Q}^\times \to U_Y$, a set

$$V_{c,Y} = \{(\alpha, s) \in U_Y \times \mathbb{Q}^\times : c\prod_{\varphi\in X}\alpha(\varphi) = s^2\} \subset U_Y \times \mathbb{Q}^\times\,,$$

a group

$$W_Y = \{(\gamma^2 \iota_Y(a), a^d \prod_{\varphi \in X} \gamma(\varphi)) : \gamma \in U_Y, a \in \mathbb{Q}^\times\} \subset V_{1,Y}$$

and the quotient set

$$H_{c,Y} = V_{c,Y}/W_Y\,.$$

We get induced maps, which we denote again by π_Y, from the objects associated to Π to the corresponding objects associated to Y. We define $\delta_Y = \pi_Y \circ \delta_\Pi : C(\mathbb{Q}) \to H_{c,Y}$. Using notations $H_{c,Y,p}$, $\rho_{Y,p}$, $\delta_{Y,p}$ in analogy to $H_{c,p}$ etc., we define the *Y-Selmer set* of C to be

$$\mathrm{Sel}(C,Y) = \{h \in H_{c,Y} : \rho_{Y,p}(h) \in \operatorname{Im}\delta_{Y,p} \text{ for all places } p \text{ of } \mathbb{Q}\}\,.$$

Projecting to the first component, we obtain the *fake Y-Selmer set* $\mathrm{Sel}_{\mathrm{fake}}(C,Y)$. We write $H'_{c,Y} \subset U_Y/(U_Y^2 \iota_Y(\mathbb{Q}^\times))$ for the image of $H_{c,Y}$ under the map induced by projection of the product $U_Y \times \mathbb{Q}^\times$ to the first factor, and similarly δ'_Y for the composition $C(\mathbb{Q}) \xrightarrow{\delta_Y} H_{c,Y} \to H'_{c,Y}$. Using $H'_{c,Y,p}$, $\rho'_{Y,p}$, $\delta'_{Y,p}$ for the local equivalents, we have

$$\mathrm{Sel}_{\mathrm{fake}}(C,Y) = \{h \in H'_{c,Y} : \rho'_{Y,p}(h) \in \operatorname{Im}\delta'_{Y,p} \text{ for all places } p \text{ of } \mathbb{Q}\}\,.$$

It is clear that the covering $D_{\alpha,s,Y} \to C$ only depends on the image of (α, s) in $V_{c,Y}$; therefore we will write $\pi_{\beta,s,Y} : D_{\beta,s,Y} \to C$ instead, where (β, s) is the image of (α, s) in $V_{c,Y}$. As usual, we then have the following result.

Theorem 2.1. *We have* $\delta_Y\big(C(\mathbb{Q})\big) \subset \mathrm{Sel}(C,Y)$, *and*

$$C(\mathbb{Q}) = \bigcup_{[\beta,s] \in \mathrm{Sel}(C,X)} \pi_{\beta,s,Y}\big(D_{\beta,s,Y}(\mathbb{Q})\big)\,.$$

The curve $D_{\beta,s}$ is a connected component of the subscheme of $\mathbb{P}_Y \times C$ defined in terms of the coordinates z_φ and $(u : v : y)$ by

$$\exists a \neq 0 : \quad \beta(\varphi) z_\varphi^2 = a^{\deg\varphi}\varphi(u,v) \text{ for all } \varphi \in Y \quad \text{ and } \quad c\prod_{\varphi\in X} z_\varphi = a^d y\,.$$

(To select the appropriate component, one has to take into account possible relations between the z_φ — we can define $D_{\beta,s}$ as the closure of the set of all $(\mathbb{P}(z), Q)$ with $z \in \bar{U}_Y$ satisfying $(\beta z^2, c\prod_{\varphi\in X} z_\varphi) = (\bar{\iota}_Y(a), a^d)\bar{\delta}_Y(Q)$ for some $a \in \bar{\mathbb{Q}}^\times$. For this, we extend the objects and maps to their $\bar{\mathbb{Q}}$-counterparts.)

3. Computing Selmer sets

In this section, we explain how a set like $\mathrm{Sel}_{\mathrm{fake}}(C,Y)$ can be computed. The first step is to reduce the infinitely many local conditions to only a finite set of places.

Let $Y/\mathcal{G}$ be the set of Galois-orbits of Y. For each orbit $O \in Y/\mathcal{G}$, we select a representative $\varphi_O \in O$. Then $L_Y \cong \prod_O K_O$, where K_O is the field of definition of φ_O (i.e., the subfield of $\bar{\mathbb{Q}}$ consisting of elements fixed by the stabilizer of φ_O in $\mathcal{G}$). Let p be a (finite) prime of $\mathbb{Q}$, and let $\beta \in U_Y$ be an element such that there is $s \in \mathbb{Q}^\times$ with $[\rho_{Y,p}(\beta), s] \in \operatorname{Im}\delta_{Y,p}$. Let $\beta_O \in K_O$ be the O-component of β, and let $\mathfrak{p}$ be a place of K_O above p. Let $\varphi'(u,v) = f/\varphi(u,v)$ be the cofactor of $\varphi(u,v)$. By assumption, there are $u_0, v_0, y_0 \in \mathbb{Q}_p$ such that $\varphi(u_0,v_0) = \beta_O$ and $f(u_0,v_0) = y_0^2$. If p does not divide the leading coefficient c of f and $\mathfrak{p}$ does not divide the resultant $R_O = \mathrm{Res}(\varphi(u,v), \varphi'(u,v))$, then the valuation $v_\mathfrak{p}(\beta_O)$ must be even. We therefore define S_O to be the (finite) set of places $\mathfrak{p}$ of K_O such that $\mathfrak{p} \mid \infty$ or $v_\mathfrak{p}(c) \neq 0$ or $v_\mathfrak{p}(R_O) \neq 0$. Write $\mathcal{S}$ for the family $(S_O)_{O \in Y/\mathcal{G}}$. As usual, if K is a number field and S is a set of places of K containing the infinite places, we define

$$K(S,2) = \{\alpha(K^\times)^2 \in K^\times/(K^\times)^2 : v_\mathfrak{p}(\alpha) \text{ is even for all } \mathfrak{p} \notin S\}\,.$$

Then we can define

$$L_Y(\mathcal{S},2) = \prod_O K_O(S_O,2) \subset L_Y^\times/(L_Y^\times)^2\,.$$

From the discussion above, it follows that elements of the fake Selmer set $\mathrm{Sel}_{\mathrm{fake}}(C,Y)$ are represented by elements β of $L_Y(\mathcal{S},2)$. Since the groups $K(S,2)$ are finite when S is finite, this gives the Selmer set as a subset of a finite group. We have to determine the image of this finite group in the quotient group $K_Y^\times/((K_Y^\times)^2\iota_Y(\mathbb{Q}^\times))$.

The map $\iota_Y : \mathbb{Q}^\times \to L_Y^\times$ induces a map again denoted ι_Y from $\mathbb{Q}^\times/(\mathbb{Q}^\times)^2$ to $L_Y^\times/(L_Y^\times)^2$. By standard results from algebra, we have that the image of $L_Y(\mathcal{S},2)$ in $K_Y^\times/((K_Y^\times)^2\iota_Y(\mathbb{Q}^\times))$ is given by $L_Y(\mathcal{S},2)/(L_Y(\mathcal{S},2)\cap\iota_Y(\mathbb{Q}^\times/(\mathbb{Q}^\times)^2))$. So we have to determine the intersection $L_Y(\mathcal{S},2)\cap\iota_Y(\mathbb{Q}^\times/(\mathbb{Q}^\times)^2)$. We write $e_{\mathfrak{p}/p}$ for the ramification index of the extension $K_{O,\mathfrak{p}}/\mathbb{Q}_p$.

Lemma 3.1. *Let T be the following set of rational primes p:*

$$T = \{p : \textit{for all } O \textit{ such that } \#\varphi_O \textit{ is odd: } \forall \mathfrak{p} \mid p, \textit{ either } \mathfrak{p} \in S_O \textit{ or } 2 \mid e_{\mathfrak{p}/p}\}\,.$$

Then

$$L_Y(\mathcal{S},2) \cap \operatorname{Im}\iota_Y = \iota_Y(\mathbb{Q}(T,2))\,.$$

Proof. First we show that $\iota_Y(\mathbb{Q}(T,2)) \subset L_Y(\mathcal{S},2)$. Suppose $a \in \mathbb{Q}(T,2)$ and $\mathfrak{p}$ is a finite place of K_O, where $\#\varphi_O$ is odd (in the other case, there is nothing to show). Let p be the rational prime below $\mathfrak{p}$. Now

$$v_{\mathfrak{p}}(a) = e_{\mathfrak{p}/p}\cdot v_p(a)\,. \tag{5}$$

Suppose $v_{\mathfrak{p}}(a)$ is odd. Thus $v_p(a)$ is odd and $e_{\mathfrak{p}/p}$ is odd. As $a \in \mathbb{Q}(T,2)$ and $v_p(a)$ is odd, we see that $p \in T$. By definition of T we deduce that $\mathfrak{p} \in S_O$. This shows that $\iota_Y(a) \in L_Y(\mathcal{S},2)$ as required.

Now we want to show that $L_Y(\mathcal{S},2)\cap\operatorname{Im}\iota_Y \subset \iota_Y(\mathbb{Q}(T,2))$. Suppose $\alpha \in L_Y(\mathcal{S},2)$ is also in $\operatorname{Im}\iota_Y$. Then there is some $a \in \mathbb{Q}^\times$ and some $\beta \in L_Y^\times$ such that $\alpha_O\beta_O^2 = a^{\#\varphi_O}$ for all $O \in Y/\mathcal{G}$. We want to show that $a \in \mathbb{Q}(T,2)$. Suppose $p \notin T$. Then there is some place $\mathfrak{p}$ of some K_O with $\#\varphi_O$ odd such that $\mathfrak{p} \mid p$, $\mathfrak{p} \notin S_O$ and $e_{\mathfrak{p}/p}$ is odd. As $\mathfrak{p} \notin S_O$, we know that $v_{\mathfrak{p}}(\alpha_O)$ is even. This implies that $v_{\mathfrak{p}}(a)$ is even. By (5), we see that $v_p(a)$ is even. As this is true for all $p \notin T$, we have that $a \in \mathbb{Q}(T,2)$ as required. □

We have already remarked that the group $L_Y(\mathcal{S},2)$ is finite; it is also computable. Its computation [23] requires knowledge of the class groups of the fields K_O and of a subgroup of the unit group of each K_O of full rank and odd index.

Lemma 3.2. *The fake Selmer set $\mathrm{Sel}_{\mathrm{fake}}(C,Y)$ is contained in the intersection $H'_{c,Y}$ of $L_Y(\mathcal{S},2)/\iota_Y(\mathbb{Q}(T,2))$ with the image of $H_{c,Y}$ under the projection to $L_Y^\times/((L_Y^\times)^2\iota_Y(\mathbb{Q}^\times))$. If $\beta \in L_Y(\mathcal{S},2)$ represents an element of this intersection, then the covering curve $D_{\beta,s,Y}$ (for both possible choices of s) has good reduction at all odd primes p not dividing the discriminant or the leading coefficient of f.*

Proof. The first assertion follows from the preceding discussion.

If p is an odd prime not dividing the discriminant or the leading coefficient of f, then β can be represented by a tuple $(\beta_O)_O$ such that β_O is a $\mathfrak{p}$-adic unit for all $\mathfrak{p} \mid p$. The whole construction of covering curves can then be carried out over $\mathbb{F}_p$. In particular, we obtain an unramified Galois covering of $C/\mathbb{F}_p$ that is the reduction of $D_{\beta,s,Y}$ mod p, which must therefore be smooth. □

Let $\mathcal{A}$ be any set of (finite or infinite) places of $\mathbb{Q}$. We denote by $\mathrm{Sel}_{\mathrm{fake}}(C,Y,\mathcal{A})$ the subset of $H'_{c,Y}$ consisting of elements that satisfy the local conditions for the fake Selmer

set at all places in $\mathcal{A}$. Then

$$\mathrm{Sel}_{\mathrm{fake}}(C,Y) = \mathrm{Sel}_{\mathrm{fake}}(C,Y,\{\text{all places of } \mathbb{Q}\}) \subset \mathrm{Sel}_{\mathrm{fake}}(C,Y,\mathcal{A})\,.$$

By definition, $\mathrm{Sel}(C,Y)$ maps to $\mathrm{Sel}_{\mathrm{fake}}(C,Y)$. So by Theorem 2.1, we see that $C(\mathbb{Q})$ must be empty if $\mathrm{Sel}_{\mathrm{fake}}(C,Y,\mathcal{A}) = \emptyset$.

This definition will be useful, since we will see that we would need to check the local conditions at very many primes if we want to compute the fake Selmer set exactly. Using a smaller number of primes can already give a very useful upper bound, which is much easier to compute.

The next result shows that we only need to consider a finite set of places when we want to compute a (fake) Selmer set.

Theorem 3.3. *Let $\mathcal{T}$ be a set of rational primes containing the following primes p:*

- *$p = \infty$,*
- *$p < 4g_D^2$ where $g_D = \#G_Y(g-1)+1$ is the genus of the covering curves $D_{\beta,s,Y}$.*
- *p dividing the discriminant or the leading coefficient of f.*

Then $\mathrm{Sel}_{\mathrm{fake}}(C,Y) = \mathrm{Sel}_{\mathrm{fake}}(C,Y,\mathcal{T})$.

Proof. We have to show that for a prime p outside $\mathcal{T}$, the local condition is automatically satisfied. So assume that $p \notin \mathcal{T}$. Then $p \ge 4g_D^2$ and p does not divide the discriminant or leading coefficient of f. Let $\beta \in L_Y(\mathcal{S},2)$ represent an element of $H'_{c,Y}$. The latter two conditions on p imply by Lemma 3.2 that $D_{\beta,s,Y}$ has good reduction at p. The first condition then implies by the Hasse-Weil bounds that the reduction of $D_{\beta,s,Y}$ mod p has (smooth) $\mathbb{F}_p$-points; then Hensel's Lemma shows that $D_{\beta,s,Y}(\mathbb{Q}_p)$ is non-empty. This in turn means that the element represented by β is in the image of $\mathrm{pr}_1 \circ \delta_{Y,p}$. The theorem follows. □

One convenient way of obtaining a suitable set Y is the following. We fix some number field K and let X be the partition of Θ corresponding to the factorization of f into irreducible factors over K. Then Y can be taken to be the union of the $\mathcal{G}$-orbits of the elements of X. In this case, all the fields occurring as components of the algebra L_Y will be (isomorphic to) subfields of K. We will denote the corresponding (fake) Selmer sets also by $\mathrm{Sel}(C,K)$, $\mathrm{Sel}(C,K,\mathcal{A})$, $\mathrm{Sel}_{\mathrm{fake}}(C,K)$ and $\mathrm{Sel}_{\mathrm{fake}}(C,K,\mathcal{A})$.

In the following, we will assume that we are in this situation and would like to compute $\mathrm{Sel}_{\mathrm{fake}}(C,K,\mathcal{A})$ for some finite set $\mathcal{A}$ of primes. For simplicity, we will assume in addition that none of the factors in the factorization of f over K is actually defined over a smaller field and that no two of the factors are in the same $\mathcal{G}$-orbit. Since it is advantageous for the computation, we will remove the requirement that the factors are monic and instead consider a factorization

$$f(u,v) = c f_1(u,v) f_2(u,v) \cdots f_r(u,v)$$

with $c \in \mathbb{Z}$ and polynomials $f_1,\dots,f_r$ with coefficients in $\mathcal{O}$, the ring of integers of K. (It may be necessary to scale f by an integral square to make this possible.) Then $L_Y \cong K^r$, and if we let S be the union of the sets S_j corresponding to the orbit of f_j, then $L_Y(\mathcal{S},2) \subset K(S,2)^r$.

Testing the local conditions. Let $h \in H'_{c,Y}$, and let p be a rational prime. To be able to compute $\mathrm{Sel}_{\mathrm{fake}}(C,K,\mathcal{A})$, we need an algorithm for determining whether $\rho_p(h) \in \mathrm{Im}(\delta'_{Y,p})$ (for all $p \in \mathcal{A}$). Let us deal first with the case $p = \infty$ which is certainly easier. In this case we actually compute the image of $\delta'_{Y,\infty} : C(\mathbb{R}) \to H'_{c,Y,\infty}$. Note that this is a continuous map from $C(\mathbb{R})$ to a discrete set, so it must be constant on connected components. We can therefore proceed as follows. Let $I_1,\dots,I_k$ be the open

intervals on which $f(u,1)$ is positive. For each j choose $u_j \in I_j$ and $y_j \in \mathbb{R}$ such that $y_j^2 = f(u_j,1)$. Then $\mathrm{Im}(\delta'_{Y,\infty})$ is simply $\{\delta'_{Y,\infty}(u_j : 1 : y_j) : 1 \le j \le k\}$.

We now let p be a finite prime. We shall suppose that h is represented by $(\alpha_1, \dots, \alpha_r)$ in $K(S,2)^r$. We denote the degree of f_j by d_j and shall also suppose that $d_1, \dots, d_s$ are odd and $d_{s+1}, \dots, d_r$ are even. Then $\rho_p(h) \in \mathrm{Im}(\delta'_{Y,p})$ if and only if there is some $(u : v) \in \mathbb{P}^1(\mathbb{Q}_p)$ and $a \in \mathbb{Q}_p^\times/(\mathbb{Q}_p^\times)^2$ such that $a\alpha_i F_i(u,v) \in K_p^2$ for $1 \le i \le s$ and $\alpha_i F_i(u,v) \in K_p^2$ for $s+1 \le i \le r$ and $f(u,v) \in \mathbb{Q}_p^2$. Now $\mathbb{Q}_p^\times/(\mathbb{Q}_p^\times)^2$ is finite, and we choose rational integers a representing its cosets. Moreover $(u : v) = (x : 1)$ or $(1 : px)$ for some $x \in \mathbb{Z}_p$. Thus we can decide whether h maps into the local image st p if we can decide the following question: given a polynomial $f \in \mathbb{Z}[x]$ and polynomials $f_i \in \mathcal{O}[x]$, is there $x \in \mathbb{Z}_p$ such that $f(x) \in \mathbb{Q}_p^2$ and $f_i(x) \in K_p^2$ for $1 \le i \le r$. Equivalently, is there $x \in \mathbb{Z}_p$ satisfying the following property

$$\begin{cases} f(x) \text{ is a square in } \mathbb{Q}_p \text{ and} \\ f_i(x) \text{ is a square in } K_{\mathfrak{p}} & \text{for each place } \mathfrak{p} \text{ above } p \text{ and for } 1 \le i \le r. \end{cases} \tag{6}$$

We shall restrict to the case where

$$f \text{ is separable} \qquad \text{and} \qquad f/\prod f_i \text{ is a constant in } (K^\times)^2. \tag{7}$$

This is certainly true for the f and f_i in our situation.

We shall need the following pair of lemmas.

Lemma 3.4. *Let $g = \sum a_i x^i \in \mathbb{Z}[x]$, $x_0 \in \mathbb{Z}$, and $n \ge 1$. Let $c = \min v_p(a_i)$ and $m = v_p(g'(x_0))$. Write $\lambda = \min\{m+n, c+2n\}$. Let $k = v_p(g(x_0))$. Suppose $k < \lambda$. If either of the following two conditions holds,*

- *k is odd, or*
- *k is even and $g(x_0)/p^k$ is not a square modulo $p^{\lambda-k}$,*

then $g(x)$ is not a square in $\mathbb{Q}_p$ for all $x \in x_0 + p^n\mathbb{Z}_p$.

Lemma 3.5. *Let $g = \sum a_i x^i \in \mathcal{O}[x]$, $x_0 \in \mathbb{Z}$, and $n \ge 1$. Let $\mathfrak{p}$ be a place above p having ramification index e and let $\pi \in \mathcal{O}$ be a uniformizing element for $\mathfrak{p}$. Let $c = \min v_{\mathfrak{p}}(a_i)$ and $m = v_{\mathfrak{p}}(g'(x_0))$. Write $\lambda = \min\{m+ne, c+2ne\}$. Let $k = v_{\mathfrak{p}}(g(x_0))$. Suppose $k < \lambda$. If either of the following two conditions holds,*

- *k is odd, or*
- *k is even and $g(x_0)/\pi^k$ is not a square modulo $\pi^{\lambda-k}$,*

then $g(x)$ is not a square in $K_{\mathfrak{p}}$ for all $x \in x_0 + p^n\mathbb{Z}_p$.

We shall prove Lemma 3.5, with the proof of Lemma 3.4 being an easy simplification.

Proof. Suppose $x \in x_0 + p^n\mathbb{Z}_p \subset x_0 + \pi^{ne}\mathcal{O}_\pi$. Let $g_1 = g/\pi^c \in \mathcal{O}_\pi[x]$. By Taylor's Theorem

$$g_1(x) = g_1(x_0) + (x - x_0)g_1'(x_0) + O(\pi^{2ne}).$$

Thus

$$g(x) = g(x_0) + (x - x_0)g'(x_0) + O(\pi^{c+2ne}).$$

It follows that

$$g(x) \equiv g(x_0) \pmod{\pi^\lambda},$$

where λ is given in the statement of the lemma. The lemma follows. □

We return to our question: given $f \in \mathbb{Z}[x]$ and $f_i \in \mathcal{O}[x]$ satisfying (7), is there $x \in \mathbb{Z}_p$ satisfying (6)? Our algorithm for answering this question produces a sequence of finite sets of integers $\mathcal{B}_0, \mathcal{B}_1, \mathcal{B}_2, \dots$ satisfying

$$\{x \in \mathbb{Z}_p : x \text{ satisfies (6)}\} \subset \bigcup_{x_0 \in \mathcal{B}_n} (x_0 + p^n\mathbb{Z}_p). \tag{8}$$

We start with $\mathcal{B}_0 = \{0\}$. To produce $\mathcal{B}_n$ from $\mathcal{B}_{n-1}$ we initially let

$$\mathcal{B}_n = \{x_0 + p^n a : x_0 \in \mathcal{B}_{n-1} \text{ and } 0 \le a \le p-1\}.$$

If any $x_0 \in \mathcal{B}_n$ satisfies (6) then we have answered our question positively and our algorithm terminates. Otherwise, for each $x_0 \in \mathcal{B}_n$, we apply the tests in Lemmas 3.4 and 3.5. If the hypotheses of Lemma 3.4 apply to $g = f$ with the current choices of x_0 and n then we eliminate x_0 from $\mathcal{B}_n$. Likewise if there is some $1 \le i \le r$, and some $\mathfrak{p}$ above p such that $g = f_i$ satisfies the hypotheses of Lemma 3.5. We see that once this process is complete, $\mathcal{B}_n$ still satisfies (8). At any stage of the algorithm, if $\mathcal{B}_n$ is empty then we have answered our question negatively.

Lemma 3.6. *The above algorithm terminates in finite time.*

Proof. Suppose otherwise.

Suppose first that there is some $x^* \in \mathbb{Z}_p$ that satisfies property (6) and $f(x^*) \neq 0$. By (7) this forces $f_i(x^*) \neq 0$. Now by (8) there is, for each n, an $x_n \in \mathcal{B}_n$ such that $x_n \equiv x^* \pmod{p^n}$. However, for n large enough it is clear that x_n satisfies (6) and so the algorithm would have stopped at the n-th step, and we have a contradiction.

Next we shall suppose that x^* satisfies property (6) and $f(x^*) = 0$. Hence precisely one of the $f_i(x^*)$ is zero. Without loss of generality suppose that $f_1(x^*) = 0$. Now $f'(x^*) \neq 0$ as f is separable. Let $x^{**} = x^* + p^{2u} f'(x^*)$ where u is a large positive integer that will be chosen later. By Taylor's Theorem

$$f(x^{**}) \equiv \left(p^u f'(x^*)\right)^2 \pmod{p^{4u}}.$$

This forces $f(x^{**})$ to be a non-zero square for u large enough. Moreover, for u large enough, $f_i(x^{**})$ is a non-zero square in $K_{\mathfrak{p}}$ for $2 \le i \le r$, since $f_i(x^*)$ is a non-zero square. By (7), $f_1(x^{**})$ must also be a square. Thus $f(x^{**}) \neq 0$ and x^{**} satisfies (6). This reduces us to the previous case and we have a contradiction.

We deduce that no $x^* \in \mathbb{Z}_p$ satisfies (6). Now choose $x_n \in \mathcal{B}_n$ for $n = 0, 1, 2, \ldots$ such that $x_{n+1} \equiv x_n \pmod{p^n}$. Let $x^* = \lim x_n \in \mathbb{Z}_p$. In particular $x^* \equiv x_n \pmod{p^n}$. Now either $f(x^*)$ is a non-square in $\mathbb{Q}_p$, or $f_i(x^*)$ is a non-square in $K_{\mathfrak{p}}$ for some $\mathfrak{p}$ above p and some $1 \le i \le r$.

Suppose that $f(x^*)$ is a non-square in $\mathbb{Q}_p$. Let $k = v_p(f(x^*)) < \infty$. Suppose $n > k$. Then $k = v_p(f(x_n))$. Now either k is odd, or $f(x_n)/p^k$ is not a square modulo p^{n-k}, for large enough n. In either case, x_n satisfies the hypotheses of Lemma 3.4, and cannot belong to $\mathcal{B}_n$ giving a contradiction. Likewise we obtain a contradiction if $f_i(x^*)$ is a non-square in $K_{\mathfrak{p}}$. □

4. Edwards' Parametrization

The remainder of this paper is devoted to the proof of Theorem 1.1. In this section, we use Edwards' parametrization of the generalized Fermat equation with signature $(2, 3, 5)$. This allows us to reduce the resolution of (2) to the determination of rational points on 49 hyperelliptic curves of genus 14; in determining the rational points on these curves our partial descent will play a major rôle. All our computations are carried out using the package `MAGMA` [4].

In the following, the notation $h = [\alpha_0, \alpha_1, \ldots, \alpha_{12}]$ means that h is the binary form

$$h(u, v) = \sum_{i=0}^{12} \binom{12}{i} \alpha_i u^i v^{12-i}.$$

We define binary forms $h_1, \ldots, h_{27}$ as given in Table 1 on page 11.

$h_1 = [0, 1, 0, 0, 0, 0, -144/7, 0, 0, 0, 0, -20736, 0]$,
$h_2 = [-1, 0, 0, -2, 0, 0, 80/7, 0, 0, 640, 0, 0, -102400]$,
$h_3 = [-1, 0, -1, 0, 3, 0, 45/7, 0, 135, 0, -2025, 0, -91125]$,
$h_4 = [1, 0, -1, 0, -3, 0, 45/7, 0, -135, 0, -2025, 0, 91125]$,
$h_5 = [-1, 1, 1, 1, -1, 5, -25/7, -35, -65, -215, 1025, -7975, -57025]$,
$h_6 = [3, 1, -2, 0, -4, -4, 24/7, 16, -80, -48, -928, -2176, 27072]$,
$h_7 = [-10, 1, 4, 7, 2, 5, 80/7, -5, -50, -215, -100, -625, -10150]$,
$h_8 = [-19, -5, -8, -2, 8, 8, 80/7, 16, 64, 64, -256, -640, -5632]$,
$h_9 = [-7, -22, -13, -6, -3, -6, -207/7, -54, -63, -54, 27, 1242, 4293]$,
$h_{10} = [-25, 0, 0, -10, 0, 0, 80/7, 0, 0, 128, 0, 0, -4096]$,
$h_{11} = [6, -31, -32, -24, -16, -8, -144/7, -64, -128, -192, -256, 256, 3072]$,
$h_{12} = [-64, -32, -32, -32, -16, 8, 248/7, 64, 124, 262, 374, 122, -2353]$,
$h_{13} = [-64, -64, -32, -16, -16, -32, -424/7, -76, -68, -28, 134, 859, 2207]$,
$h_{14} = [-25, -50, -25, -10, -5, -10, -235/7, -50, -49, -34, 31, 614, 1763]$,
$h_{15} = [55, 29, -7, -3, -9, -15, -81/7, 9, -9, -27, -135, -459, 567]$,
$h_{16} = [-81, -27, -27, -27, -9, 9, 171/7, 33, 63, 141, 149, -67, -1657]$,
$h_{17} = [-125, 0, -25, 0, 15, 0, 45/7, 0, 27, 0, -81, 0, -729]$,
$h_{18} = [125, 0, -25, 0, -15, 0, 45/7, 0, -27, 0, -81, 0, 729]$,
$h_{19} = [-162, -27, 0, 27, 18, 9, 108/7, 15, 6, -51, -88, -93, -710]$,
$h_{20} = [0, 81, 0, 0, 0, 0, -144/7, 0, 0, 0, 0, -256, 0]$,
$h_{21} = [-185, -12, 31, 44, 27, 20, 157/7, 12, -17, -76, -105, -148, -701]$,
$h_{22} = [100, 125, 50, 15, 0, -15, -270/7, -45, -36, -27, -54, -297, -648]$,
$h_{23} = [192, 32, -32, 0, -16, -8, 24/7, 8, -20, -6, -58, -68, 423]$,
$h_{24} = [-395, -153, -92, -26, 24, 40, 304/7, 48, 64, 64, 0, -128, -512]$,
$h_{25} = [-537, -205, -133, -123, -89, -41, 45/7, 41, 71, 123, 187, 205, -57]$,
$h_{26} = [359, 141, -1, -21, -33, -39, -207/7, -9, -9, -27, -81, -189, -81]$,
$h_{27} = [295, -17, -55, -25, -25, -5, 31/7, -5, -25, -25, -55, -17, 295]$.

TABLE 1. Definition of the forms h_i, $1 \le i \le 27$.

For $i = 1, \ldots, 27$, let

$$g_i = \frac{1}{132^2}\left(\frac{\partial^2 h_i}{\partial u^2}\frac{\partial^2 h_i}{\partial v^2} - \frac{\partial^2 h_i}{\partial u \partial v}\frac{\partial^2 h_i}{\partial u \partial v}\right), \qquad f_i = \frac{1}{240}\left(\frac{\partial h_i}{\partial u}\frac{\partial g_i}{\partial v} - \frac{\partial h_i}{\partial v}\frac{\partial g_i}{\partial u}\right).$$

Let

$$\begin{aligned}
(f_i, g_i, h_i) &= (-f_{i-27}, g_{i-27}, h_{i-27}), && i = 28, 29,\\
(f_i, g_i, h_i) &= (-f_{i-25}, g_{i-25}, h_{i-25}), && i = 30, \ldots, 41,\\
(f_i, g_i, h_i) &= (-f_{i-23}, g_{i-23}, h_{i-23}), && i = 42, \ldots, 49.
\end{aligned}$$

Note that the f_i, g_i and h_i are binary forms with integral coefficients, of degrees 30, 20 and 12 respectively.

Theorem 4.1. *(Edwards* [14]*) Suppose a, b, c are coprime rational integers satisfying $a^2 + b^3 + c^5 = 0$. Then for some $i = 1, \ldots, 49$, there is a pair of coprime rational integers u, v such that*

$$a = f_i(u, v), \qquad b = g_i(u, v), \qquad c = h_i(u, v).$$

Proof. See pages 235–236 of [14], particularly the last paragraph on page 236. □

5. Local Solubility

Lemma 5.1. *Suppose x, y, z are coprime integers satisfying equation (2). Then, for some i in*

$$I = \{2, 3, 5, 6, 15, 16, 17, 23, 24, 27, 28, 29, 31, 32, 36, 37, 38, 40, 41, 43, 44, 47, 49\} \tag{9}$$

there is a pair of coprime integers u, v, such that

$$y^2 = f_i(u, v), \qquad x = g_i(u, v), \qquad z = h_i(u, v). \tag{10}$$

Proof. From Edwards' Theorem, the conclusion certainly holds for some $1 \le i \le 49$. It turns out that for all i the form f_i is square-free and so the equation $y^2 = f_i(u, v)$ defines a hyperelliptic curve

$$C_i : y^2 = f_i(u, v)$$

in weighted projective space, where we give u, v and y the weights 1, 1 and 15. This hyperelliptic curve has genus $g = 14$ since the binary form f_i has degree 30. We tested each C_i for everywhere local solubility using our implementation of the algorithm in [19]. By the Hasse-Weil bounds, it is only necessary to test for local solubility at ∞, the primes dividing the discriminant of f_i, and those $< 4g^2$. We find that for i in the set

$$\{1, 4, 9, 10, 11, 13, 14, 18, 25, 26, 33, 35, 39, 45, 46, 48\}$$

the curve C_i has no 2-adic points and for $i = 20$, 42, it has no 3-adic points.

We can eliminate a further eight indices i as follows. Let $S = \{\overline{w}^2 : \overline{w} \in \mathbb{Z}/2^8\mathbb{Z}\}$ and $T = \{2\overline{w} : \overline{w} \in \mathbb{Z}/2^8\mathbb{Z}\}$ be subsets of $\mathbb{Z}/2^8\mathbb{Z}$. Let

$$U_i = \{(\overline{u}, \overline{v}) \in (\mathbb{Z}/2^8\mathbb{Z})^2 : f_i(\overline{u}, \overline{v}) \in S, \quad (f_i(\overline{u}, \overline{v}), g_i(\overline{u}, \overline{v}), h_i(\overline{u}, \overline{v})) \notin T^3\}.$$

If $U_i = \emptyset$ then for any pair of integers u, v, if $f_i(u, v)$ is a square then the integers $f_i(u, v)$, $g_i(u, v)$, $h_i(u, v)$ must all be even and so cannot be coprime. It turns out that $U_i = \emptyset$ for $i = 7, 8, 12, 19, 21, 22, 30, 34$, and so we can eliminate these indices from consideration. This leaves us with the set I in the statement of the theorem.

Our attempts to eliminate other indices using the corresponding trick with other prime powers were unsuccessful. □

Remark. In what follows we will determine the rational points on the curves C_i for the 23 values of $i \in I$. There are various relations between these 23 curves which are helpful to bear in mind, even though we shall not use them explicitly. First, the curves C_3, C_{17} and C_{47} are isomorphic. Secondly, if we write $i \sim j$ to mean that C_i is a quadratic twist of C_j then we have

$$5 \sim 31 \sim 49, \qquad 6 \sim 32, \qquad 15 \sim 16,$$
$$23 \sim 24, \qquad 27 \sim 28 \sim 37 \sim 38, \qquad 43 \sim 44.$$

6. Factorization Types

Let $G \in \mathbb{Q}[u, v]$ be a binary form, and let K be a number field. We say G has *factorization type* $[d_1, d_2, \ldots, d_n]$ over K if it factors as a product $G = G_1 G_2 \ldots G_n$ where $G_j \in K[u, v]$ is irreducible over K of degree d_j. The following table records the factorization types of f_i over $\mathbb{Q}$ for the 23 values of $i \in I$.

factorization type of f_i over $\mathbb{Q}$	$i \in I$
$[30]$	$15, 16, 23, 24, 27, 28, 29, 37, 38, 40, 41, 43, 44$
$[10, 20]$	$2, 36$
$[6, 12, 12]$	$3, 17, 47$
$[1, 1, 4, 4, 4, 8, 8]$	$5, 6, 31, 32, 49$

We implemented our partial descent in MAGMA, and used it to deal with the remaining f_i as we now explain.

6.1. **Dealing with factorization type** $[30]$**.** Here the f_i are irreducible and it is impractical to compute the class group and units of the degree 30 number fields $\mathbb{Q}[x]/f_i$. It follows from Edwards' construction that the Galois group of the splitting field of any of the f_i (or g_i or h_i) must be isomorphic to a subgroup of $\mathrm{GL}_2(\mathbb{F}_5)/\{\pm I\}$. In these 13 cases where f_i is irreducible, it turns out that the Galois group is isomorphic to $\mathrm{GL}_2(\mathbb{F}_5)/\{\pm I\}$, which has order 240. Now $\mathrm{GL}_2(\mathbb{F}_5)/\{\pm I\}$ has a subgroup of order 48 and hence index 5. By the Galois correspondence, the splitting field of f_i must contain a subfield K_i of degree 5. It is possible to determine for these fields K_i the class group and unit information needed for the Selmer set computation. Recall that $\mathrm{Sel}_{\mathrm{fake}}(C, K, \mathcal{A})$ was defined (following Theorem 3.3) to be the Selmer set corresponding to the $\mathcal{G}$-set obtained from a factorization over K. It turns out that $\mathrm{Sel}_{\mathrm{fake}}(C_i, K_i, \mathcal{A}_i) = \emptyset$ where $\mathcal{A}_i$ is the set consisting of the primes < 100, infinity and the primes dividing the leading coefficient of f_i. This shows that $C_i(\mathbb{Q}) = \emptyset$ for $i = 15, 16, 23, 24, 27, 28, 29, 37, 38, 40, 41, 43, 44$. We briefly indicate in this table the choice of K_i. In all these cases, f_i has factorization type $[6, 24]$ over K_i. (It can be checked that the Galois group of the coverings one would obtain is isomorphic to μ_2^4, so we have $g_D = 16(g-1)+1 = 209$.)

$i \in I$	Defining polynomial for K_i
$15, 16, 23, 24$	$x^5 - 10x^2 - 15x - 6$
$27, 28, 37, 38, 43, 44$	$x^5 + 20x^2 + 30x + 60$
29	$x^5 + 30x^2 + 45x + 18$
40	$x^5 + 20x^2 + 30x + 6$
41	$x^5 + 30x^3 + 60x^2 + 45x + 12$

For the remaining factorization types we let $K = \mathbb{Q}$ and computed the Selmer set $\mathrm{Sel}_{\mathrm{fake}}(C_i, \mathbb{Q}, \mathcal{A}_i)$ where again $\mathcal{A}_i$ is the set consisting of the primes < 100, infinity and the primes dividing the leading coefficient of f_i. In all these cases the Selmer set is non-empty. However, it turns out that each unramified cover D_h corresponding to an element h of these Selmer sets has at least one quotient $D_h \to D'/\mathbb{Q}$ such that:

(i) D' is a curve of genus 1, and its Jacobian has rank 0, or
(ii) D' is a curve of genus 2, and its Jacobian has rank at most 1.

In either case we have been able determine $D'(\mathbb{Q})$ (where for (ii) we use Chabauty's method, see [8], [16], [18], [25], [27]). This allows us to determine the rational points on the D_h, and hence on the C_i. We give some details below.

6.2. **Dealing with factorization type** $[10, 20]$**.** Here $i = 2$ or 36. We explain the details for $i = 2$; those for $i = 36$ are practically identical. Here $f_2 = F_1 F_2$ where

$$F_1 = 20736u^{10} + v^{10}$$
$$F_2 = 429981696u^{20} + 1558683648u^{15}v^5 - 207484416u^{10}v^{10} - 75168u^5v^{15} + v^{20}.$$

The Selmer set is

$$\mathrm{Sel}_{\mathrm{fake}}(C_2, \mathbb{Q}, \mathcal{A}_2) = \left\{ \left(1 \cdot (\mathbb{Q}^\times)^2, 1 \cdot (\mathbb{Q}^\times)^2\right) \right\}.$$

Thus if $(u : v : y) \in C_2(\mathbb{Q})$ then $F_1(u, v)$ and $F_2(u, v)$ are both squares. In other words, every rational point $(u : v : y) \in C_2(\mathbb{Q})$ lifts to a rational point $(u : v : y_1 : y_2)$ on the

curve

$$D : \begin{cases} F_1(u,v) = y_1^2, \\ F_2(u,v) = y_2^2, \end{cases}$$

via the map

$$\phi : D \to C_2, \qquad (u : v : y_1 : y_2) \mapsto (u : v : y_1 y_2).$$

However, the curve D covers the genus 2 curve (given here in affine coordinates)

$$D' : Y^2 = X^5 + 20736,$$

via

$$\psi : (u : v : y_1 : y_2) \mapsto (X, Y) = \left(\frac{v}{u}, \frac{y_1}{u^5}\right).$$

To determine $D(\mathbb{Q})$ and hence $C_2(\mathbb{Q})$ it is enough to determine $D'_2(\mathbb{Q})$. Write J for the Jacobian of D'. Using the in-built `MAGMA` routines for descent on Jacobians of genus 2 curves (based on [24]) we were able to show that $J(\mathbb{Q}) \cong \mathbb{Z}/5\mathbb{Z}$. From this one can easily conclude that $D'(\mathbb{Q}) = \{\infty, (0, \pm 144)\}$. Thus

$$\begin{aligned} D(\mathbb{Q}) &= \{(0 : 1 : \pm 1 : \pm 1), (1 : 0 : \pm 144 : \pm 20736)\}, \\ C_2(\mathbb{Q}) &= \{(0 : 1 : \pm 1), (1 : 0 : \pm 2985984)\}. \end{aligned}$$

From (10) we obtain the following solutions to (2)

$$(x, y, z) = (-1, \pm 1, 0), \qquad (-429981696, \pm 2985984, 0).$$

We can exclude the latter pair since we are only interested in solutions where x, y, z are coprime.

In this case, we obtain double covers of genus $g_D = 2 \cdot 13 + 1 = 27$, so $4g_D^2 = 2916$, and the exact computation of the fake Selmer sets would be feasible.

6.3. **Dealing with factorization type** $[6, 12, 12]$**.** Here $i = 3$, 17 or 47. The Selmer sets for all have size 1. It is unsurprising that all three have the same size Selmer set since, as we have observed before, the curves C_3, C_{17} and C_{47} are isomorphic. We give the details for $i = 3$ here; the other cases are almost identical. We can write $f_3 = F_1 F_2 F_3$ where

$$\begin{aligned} F_1 &= 320u^6 + v^6, \\ F_2 &= 102400u^{12} + 32000u^9v^3 + 16440u^6v^6 - 100u^3v^9 + v^{12}, \\ F_3 &= 102400u^{12} + 896000u^9v^3 - 140160u^6v^6 - 2800u^3v^9 + v^{12}. \end{aligned}$$

The Selmer set is

$$\mathrm{Sel}_{\mathrm{fake}}(C_3, \mathbb{Q}, \mathcal{A}_3) = \left\{\left(1 \cdot (\mathbb{Q}^\times)^2, 1 \cdot (\mathbb{Q}^\times)^2, 1 \cdot (\mathbb{Q}^\times)^2\right)\right\}.$$

As before, every rational point $(u : v : y) \in C_3(\mathbb{Q})$ lifts to a rational point $(u : v : y_1 : y_2 : y_3)$ on the curve

$$D : \begin{cases} F_1(u,v) = y_1^2, \\ F_2(u,v) = y_2^2, \\ F_3(u,v) = y_3^2, \end{cases}$$

via the map

$$\phi : D \to C_3, \qquad (u : v : y_1 : y_2 : y_3) \mapsto (u : v : y_1 y_2 y_3).$$

However, the curve D covers the elliptic curve

$$E : Y^2 = X^3 + 25$$

via

$$\psi : D \to E, \qquad (u : v : y_1 : y_2 : y_3) \mapsto \left(\frac{20u^2}{v^2}, \frac{5y_1}{v^3}\right).$$

The curve E has rank 0 and the Mordell–Weil group is

$$E(\mathbb{Q}) = \{O, (0,5), (0,-5)\}.$$

We deduce that the only rational points on C_3 are $(u:v:y) = (0:1:\pm 1)$. These give the solution $(0,1,-1)$ to equation (2).

6.4. **Dealing with factorization type** $[1,1,4,4,4,8,8]$**.** Here $i = 5, 6, 31, 32, 49$. In all these cases the Selmer set has exactly two elements. We give the details for $i = 5$; the other cases are similar. Now $f_5 = 2F_1F_2F_3F_4F_5F_6F_7$ where

$$\begin{aligned}
&F_1 = v, \qquad F_2 = u, \qquad F_3 = 45u^4 - v^4,\\
&F_4 = 405u^4 + 30u^2v^2 + v^4, \qquad F_5 = 15u^4 + 10u^2v^2 + 3v^4,\\
&F_6 = 405u^8 - 540u^6v^2 + 846u^4v^4 - 60u^2v^6 + 5v^8,\\
&F_7 = 50625u^8 - 13500u^6v^2 + 4230u^4v^4 - 60u^2v^6 + v^8.
\end{aligned}$$

The Selmer set has representatives $(3,2,5,5,15,5,1)$ and $(5,-6,-1,1,3,5,1)$. If $(u:v:y)$ is a rational point on C_5 mapping to the first element of the Selmer set then there are rational numbers a, $y_1, \ldots, y_7$, with $a \neq 0$, such that

$$\begin{aligned}
&F_1 = 3ay_1^2, \qquad F_2 = 2ay_2^2, \qquad F_3 = 5y_3^2,\\
&F_4 = 5y_4^2, \qquad F_5 = 15y_5^2, \qquad F_6 = 5y_6^2, \qquad F_7 = y_7^2.
\end{aligned}$$

Consider the curve

$$D' : F_3(u,v) = 5y_3^2.$$

The Jacobian of this genus 1 curve is the elliptic curve

$$E : y^2 = x^3 + 4500x,$$

which has rank 0 and Mordell–Weil group $E(\mathbb{Q}) = \{O, (0,0)\}$. It follows that $D'(\mathbb{Q}) = \{(1:0:3), (1:0:-3)\}$. This gives us the solution $(184528125, 0, -91125)$ to (2) which we can exclude since we are only interested in primitive solutions. We deal with the second element of the Selmer set in a similar way.

References

[1] M. Bennett, *On the equation* $x^{2n} + y^{2n} = z^5$, J. Théor. Nombres Bordeaux **18** (2006), 315–321.

[2] M.A. Bennett, J.S. Ellenberg and N.C. Ng, *The Diophantine equation* $A^4 + 2^\delta B^2 = C^n$, International Journal of Number Theory, **6** (2010), no. 2, 311338.

[3] F. Beukers, *The Diophantine equation* $Ax^p + By^q = Cz^r$, Lectures held at Institut Henri Poincaré, September 2004, `http://www.math.uu.nl/people/beukers/Fermatlectures.pdf`

[4] W. Bosma, J. Cannon and C. Playoust: *The Magma Algebra System I: The User Language*, J. Symb. Comp. **24** (1997), 235–265. (See also `http://magma.maths.usyd.edu.au/magma/`)

[5] N. Bruin and E.V. Flynn, *Towers of* 2*-covers of hyperelliptic curves*, Trans. Amer. Math. Soc. **357** (2005), 4329–4347.

[6] N. Bruin and M. Stoll, *Deciding existence of rational points on curves: an experiment*, Experimental Mathematics **17** (2008), 181–189.

[7] N. Bruin and M. Stoll, *Two-cover descent on hyperelliptic curves*, Mathematics of Computations **78** (2009), 2347–2370.

[8] N. Bruin and M. Stoll, *The Mordell-Weil sieve: Proving non-existence of rational points on curves*, LMS J. Comput. Math. **13** (2010), 272–306.

[9] I. Chen and S. Siksek, *Perfect powers expressible as sums of two cubes*, Journal of Algebra **322** (2009), 638–656.

[10] H. Cohen, *Number Theory, Volume II: Analytic and Modern Tools*, GTM **240**, Springer-Verlag, 2007.

[11] H. Darmon, *Faltings plus epsilon, Wiles plus epsilon, and the generalized Fermat equation*, C. R. Math. Rep. Acad. Sci. Canada **19** (1997), no. 1, 3–14.

[12] H. Darmon and A. Granville, *On the Equation* $z^m = F(x,y)$ *and* $Ax^p + By^q = Cz^r$, Bull. London Math. Society, **27** (1995), no. 6, 513–543.

[13] H. Darmon and L. Merel, *Winding quotients and some variants of Fermat's Last Theorem*, J. reine angew. Math. **490** (1997), 81–100.
[14] J. Edwards, *A complete solution to* $X^2+Y^3+Z^5=0$, J. reine angew. Math. **571** (2004), 213–236.
[15] J. Ellenberg, *Galois representations attached to* $\mathbb{Q}$*-curves and the generalized Fermat equation* $A^4+B^2=C^p$, Amer. J. Math. **126** (2004), 763–787.
[16] E.V. Flynn, *A flexible method for applying Chabauty's Theorem*, Compositio Math. **105** (1997), 79–94.
[17] A. Kraus, *On the Equation* $x^p+y^q=z^r$*: A Survey*, Ramanujan Journal **3** (1999), 315–333.
[18] W. McCallum and B. Poonen, *The method of Chabauty and Coleman*, preprint, 14 June 2010, `http://www-math.mit.edu/ poonen/papers/chabauty.pdf`
[19] J.R. Merriman, S. Siksek and N.P. Smart, Explicit 4-descents on elliptic curves, Acta Arithmetica **LXXVII.4** (1996), 358-404.
[20] B. Poonen and E.F. Schaefer, *Explicit descent on cyclic covers of the projective line*, J. reine angew. Math. **488** (1997), 141–188.
[21] B. Poonen, E.F. Schaefer and M. Stoll, *Twists of* $X(7)$ *and primitive solutions to* $x^2+y^3=z^7$, Duke Math. J. **137** (2007), 103–158.
[22] E.F. Schaefer, 2*–descent on the Jacobians of hyperelliptic curves*, J. Number Theory **51** (1995), 219–232.
[23] S. Siksek and N.P. Smart, *On the complexity of computing the* 2*-Selmer group of an elliptic curve*, Glasgow Mathematical Journal **39** (1997), 251–258.
[24] M. Stoll, *Implementing 2-descent for Jacobians of hyperelliptic curves*, Acta Arith. **98** (2001), 245–277.
[25] M. Stoll, *Independence of rational points on twists of a given curve*, Compositio Math. **142** (2006), 1201–1214.
[26] R. Taylor and A. Wiles, *Ring-theoretic properties of certain Hecke algebras*, Annals of Mathematics **141** (1995), no. 3, 553–572.
[27] J.L. Wetherell, *Bounding the Number of Rational Points on Certain Curves of High Rank*, Ph.D. dissertation, University of California at Berkeley, 1997.
[28] A. Wiles, *Modular elliptic curves and Fermat's Last Theorem*, Annals of Mathematics **141** (1995), no. 3, 443–551.

Mathematics Institute, University of Warwick, Coventry, CV4 7AL, United Kingdom
E-mail address: `s.siksek@warwick.ac.uk`

Mathematisches Institut, Universität Bayreuth, 95440 Bayreuth, Germany.
E-mail address: `Michael.Stoll@uni-bayreuth.de`