Algebra & Number Theory

Volume 7

2013

No. 4

Explicit Chabauty over number fields

Samir Siksek

msp

ALGEBRA AND NUMBER THEORY 7:4 (2013)
dx.doi.org/10.2140/ant.2013.7.765

Explicit Chabauty over number fields

Samir Siksek

Let C be a smooth projective absolutely irreducible curve of genus $g \geq 2$ over a number field K of degree d, and let J denote its Jacobian. Let r denote the Mordell–Weil rank of $J(K)$. We give an explicit and practical Chabauty-style criterion for showing that a given subset $\mathcal{H} \subseteq C(K)$ is in fact equal to $C(K)$. This criterion is likely to be successful if $r \leq d(g-1)$. We also show that the only solution to the equation $x^2 + y^3 = z^{10}$ in coprime nonzero integers is $(x, y, z) = (\pm 3, -2, \pm 1)$. This is achieved by reducing the problem to the determination of K-rational points on several genus-2 curves where $K = \mathbb{Q}$ or $\mathbb{Q}(\sqrt[3]{2})$ and applying the method of this paper.

1. Introduction

Let C be a smooth projective absolutely irreducible curve of genus $g \geq 2$ defined over a number field K, and write J for the Jacobian of C. Suppose that the rank of the Mordell–Weil group $J(K)$ is at most $g-1$. In a pioneering paper, Chabauty [1941] proved the finiteness of the set of K-rational points on C. This has since been superseded by the proof of Faltings [1983] of the Mordell conjecture, which gives the finiteness of $C(K)$ without any assumption on the rank of $J(K)$. Chabauty's approach, where applicable, does however have two considerable advantages:

(a) Chabauty's method can be refined to give explicit bounds for the cardinality of $C(K)$ as shown by Coleman [1985a]. Coleman's bounds are realistic and occasionally even sharp; see for example [Grant 1994; Flynn 1995b]. Coleman's approach has been adapted to give bounds (assuming some reasonable conditions) for the number of solutions of Thue equations [Lorenzini and Tucker 2002], the number of rational points on Fermat curves [McCallum 1992; 1994], the number of points on curves of the form $y^2 = x^5 + A$ [Stoll 2006b], and the number of rational points on twists of a given curve [Stoll 2006a].

(b) The Chabauty–Coleman strategy can often be adapted to compute $C(K)$ as in [Bruin 2002; 2003; Flynn 1997; Flynn and Wetherell 1999; 2001; McCallum

The author is supported by an EPSRC Leadership Fellowship.
MSC2010: primary 11G30; secondary 14K20, 14C20.
Keywords: Chabauty, Coleman, jacobian, divisor, abelian integral, Mordell–Weil sieve, generalized Fermat, rational points.

and Poonen 2010; Wetherell 1997] and even the K-rational points on the symmetric powers of C [Siksek 2009].

This paper is inspired by a talk[1] given by Joseph Wetherell at the MSRI on December 11, 2000. In that talk, Wetherell suggested that it should be possible to adapt the Chabauty strategy to compute the set of K-rational points on C provided the rank r of the Mordell–Weil group $J(K)$ satisfies $r \le d(g-1)$, where $d = [K : \mathbb{Q}]$. Wetherell has never published details of his method, which we believe is similar to ours.

In this paper, we give a practical Chabauty-style method for determining $C(K)$ that should succeed if the inequality $r \le d(g-1)$ holds (but see the discussion at the end of Section 2). We suppose that we have been supplied with a basis $D_1, \dots, D_r$ for a subgroup of $J(K)$ of full rank and hence finite index; the elements of this basis are represented as degree-0 divisors on C (modulo linear equivalence). Obtaining a basis for a subgroup of full rank is often the happy outcome of a successful descent calculation [Cassels and Flynn 1996; Flynn 1994; Poonen and Schaefer 1997; Schaefer 1995; Schaefer and Wetherell 2005; Stoll 1998; 2001; 2002a]. Obtaining a basis for the full Mordell–Weil group is often time-consuming for genus-2 curves [Flynn 1995a; Flynn and Smart 1997; Stoll 1999; 2002b] and simply not feasible in the present state of knowledge for curves of genus at least 3. We also assume the knowledge of at least one rational point $P_0 \in C(K)$. If a search for rational points on C does not reveal any points, then experience suggests that $C(K) = \varnothing$ and that some combination of descent and Mordell–Weil sieving [Bruin and Stoll 2008; 2009; 2010] is likely to prove this.

This paper is organized as follows. Section 2 gives a heuristic explanation of why Chabauty's approach should be applicable when the rank r of the Mordell–Weil group satisfies $r \le g(d-1)$. Section 3 gives a quick summary of basic facts regarding υ-adic integration on curves and Jacobians. In Section 4, for $Q \in C(K)$ and a rational prime p, we define a certain neighborhood of Q in $\prod_{\upsilon|p} C(K_\upsilon)$ that we call the p-unit ball around Q and give a Chabauty-style criterion for Q to be the unique K-rational point belonging to this neighborhood. In Section 5, we explain how to combine our Chabauty criterion with the Mordell–Weil sieve and deduce a practical criterion for a given set $\mathcal{H} \subseteq C(K)$ to be equal to $C(K)$. In Section 6, we use our method to prove the following theorem:

Theorem 1. *The only solutions to the equation*

$$x^2 + y^3 = z^{10} \tag{1}$$

in coprime integers x, y, and z are

$$(\pm 3, -2, \pm 1), \quad (\pm 1, 0, \pm 1), \quad (\pm 1, -1, 0), \quad \text{and} \quad (0, 1, \pm 1).$$

[1] http://msri.org/publications/ln/msri/2000/arithgeo/wetherell/1/banner/01.html

We note that Dahmen [2008, Chapter 3.3.2] has solved the equation $x^2+z^{10}=y^3$ using Galois representations and level-lowering. We have been unable to solve (1) by using Galois representations; the difficulty arises from the additional "nontrivial" solution $(x, y, z)=(\pm 3, -2, \pm 1)$, which is not present for the equation $x^2+z^{10}=y^3$. We solve (1) by reducing the problem to determining the K-rational points on several genus-2 curves where K is either $\mathbb{Q}$ or $\mathbb{Q}(\sqrt[3]{2})$. For all these genus-2 curves, the inequality $r \le d(g-1)$ is satisfied and we are able to determine the K-rational points using the method of this paper.

Recently, David Brown [2012] has given an independent and entirely different proof of Theorem 1. Brown's method is rather intricate and makes use of elliptic-curve Chabauty, mod-5 level-lowering, and number-field enumeration.

2. A heuristic explanation of Wetherell's idea

In this section, we explain the heuristic idea behind Chabauty's method and then how the heuristic can be modified for curves over number fields. Let C be a smooth projective curve of genus $g \ge 2$ defined over K. Let J be the Jacobian of C and r the rank of the Mordell–Weil group $J(K)$. Fix a rational point $P_0 \in C(K)$, and let $\jmath : C \hookrightarrow J$ be the Abel–Jacobi map with base point P_0. We use $\jmath$ to identify C as a subvariety of J.

To explain the usual Chabauty method, it is convenient to assume that $K=\mathbb{Q}$. Choose a finite prime p. Inside $J(\mathbb{Q}_p)$, it is clear that

$$C(\mathbb{Q}) \subseteq C(\mathbb{Q}_p) \cap J(\mathbb{Q}) \subseteq C(\mathbb{Q}_p) \cap \overline{J(\mathbb{Q})},$$

where $\overline{J(\mathbb{Q})}$ is the closure of $J(\mathbb{Q})$ in the p-adic topology. Now $J(\mathbb{Q}_p)$ is a $\mathbb{Q}_p$-Lie group of dimension g, and $\overline{J(\mathbb{Q})}$ is a $\mathbb{Q}_p$-Lie subgroup of dimension at most r. Moreover, $C(\mathbb{Q}_p)$ is a one-dimensional submanifold of $J(\mathbb{Q}_p)$. If $r+1 \le g$, then we expect that the intersection $C(\mathbb{Q}_p) \cap \overline{J(\mathbb{Q})}$ is finite. It turns out that this intersection is indeed finite if $r \le g-1$, and Coleman [1985a] gives a bound for the cardinality of this intersection under some further (but mild) hypotheses. Moreover, in practice, this intersection can be computed to any desired p-adic accuracy.

Now we return to the general setting by letting K be a number field of degree d. Define the Weil restrictions

$$V = \mathrm{Res}_{K/\mathbb{Q}} C \quad \text{and} \quad A = \mathrm{Res}_{K/\mathbb{Q}} J. \tag{2}$$

Then V is a variety of dimension d and A an abelian variety of dimension gd, both defined over $\mathbb{Q}$. The Weil restriction of the morphism $\jmath : C \hookrightarrow J$ is a morphism $V \hookrightarrow A$ defined over $\mathbb{Q}$ that we use to identify V as a subvariety of A. This Weil restriction defines a bijection between $C(K)$ and $V(\mathbb{Q})$, and

$$\mathrm{rank}\, A(\mathbb{Q}) = \mathrm{rank}\, J(K) = r.$$

Mimicking the previous argument,

$$V(\mathbb{Q}) \subseteq V(\mathbb{Q}_p) \cap \overline{A(\mathbb{Q})}.$$

Now $\overline{A(\mathbb{Q})}$ is at most r-dimensional, $V(\mathbb{Q}_p)$ is d-dimensional, and the intersection is taking place in the $\mathbb{Q}_p$-Lie group $A(\mathbb{Q}_p)$ of dimension gd. If $r + d \leq gd$, we expect that the intersection is finite.

Remark. As Wetherell points out, even if $r + d \leq gd$, it is possible for the intersection $V(\mathbb{Q}_p) \cap \overline{A(\mathbb{Q})}$ to be infinite. For example, let C be a curve defined over $\mathbb{Q}$ with Mordell–Weil rank at least g. One normally expects that $\overline{J(\mathbb{Q})}$ is g-dimensional. Assume that this is the case. Then the intersection

$$C(\mathbb{Q}_p) \cap \overline{J(\mathbb{Q})}$$

will contain a neighborhood in $C(\mathbb{Q}_p)$ of the base point P_0 and so will be infinite. Now let V and A be obtained from C and J by first base-extending to number field K and then taking Weil restriction back to $\mathbb{Q}$. One has a natural injection

$$C(\mathbb{Q}_p) \cap \overline{J(\mathbb{Q})} \hookrightarrow V(\mathbb{Q}_p) \cap \overline{A(\mathbb{Q})}$$

proving that the latter intersection is infinite. This is true regardless of whether the inequality $r \leq d(g-1)$ is satisfied. However, for a random curve C defined over a number field K, on the basis for the above heuristic argument, we expect the intersection $V(\mathbb{Q}_p) \cap \overline{A(\mathbb{Q})}$ to be finite when the inequality $r \leq d(g-1)$ is satisfied. We are led to the following open question:

Open question. *Let C be a smooth projective curve of genus $g \geq 2$ over a number field K of degree d. Suppose, for every smooth projective curve D defined over a subfield $L \subseteq K$ and satisfying $D \times_L K \cong_K C$, that the inequality*

$$\operatorname{rank} J_D(L) \leq [L : \mathbb{Q}](g-1)$$

holds, where J_D denotes the Jacobian of D. Let V and A be given by (2). Is $V(\mathbb{Q}_p) \cap \overline{A(\mathbb{Q})}$ necessarily finite?

3. Preliminaries

In this section, we summarize various results on p-adic integration that we need. The definitions and proofs can be found in [Coleman 1985b; Colmez 1998]. For an introduction to the ideas involved in Chabauty's method, we warmly recommend the thesis [Wetherell 1997] and the survey paper [McCallum and Poonen 2010] as well as [Coleman 1985a].

Integration. Let p be a (finite) rational prime. Let K_υ be a finite extension of $\mathbb{Q}_p$ and $\mathcal{O}_\upsilon$ the ring of integers in K_υ. Let $\mathcal{W}$ be a smooth proper connected scheme of finite type over $\mathcal{O}_\upsilon$, and write W for the generic fiber. Coleman [1985b, Section II] describes how to integrate "differentials of the second kind" on W. We shall however only be concerned with global 1-forms (i.e., differentials of the first kind) and so shall restrict our attention to these. Among the properties of integration [Coleman 1985b, Section II] that we shall need are the following, where P, Q, R lie in $W(K_\upsilon)$, while ω and ω' are global 1-forms on W, and α is an element of K_υ:

(i) $$\int_P^Q \omega = -\int_Q^P \omega.$$

(ii) $$\int_Q^P \omega + \int_P^R \omega = \int_Q^R \omega.$$

(iii) $$\int_Q^P (\omega + \omega') = \int_Q^P \omega + \int_Q^P \omega'.$$

(iv) $$\int_Q^P \alpha\omega = \alpha \int_Q^P \omega.$$

We shall also need a change of variables formula [Coleman 1985b, Theorem 2.7]: if $\mathcal{W}_1$ and $\mathcal{W}_2$ are smooth proper connected schemes of finite type over $\mathcal{O}_\upsilon$ and $\varrho : W_1 \to W_2$ is a morphism of their generic fibers, then

$$\int_Q^P \varrho^*\omega = \int_{\varrho(Q)}^{\varrho(P)} \omega$$

for all global 1-forms ω on W_2 and $P, Q \in W_1(K_\upsilon)$.

Now let A be an abelian variety of dimension g over K_υ, and write Ω_A for the K_υ-space of global 1-forms on A. Consider the pairing

$$\Omega_A \times A(K_\upsilon) \to K_\upsilon, \quad (\omega, P) \mapsto \int_0^P \omega. \tag{3}$$

This pairing is bilinear. It is K_υ-linear on the left by (iii) and (iv). It is $\mathbb{Z}$-linear on the right; this is a straightforward consequence [Coleman 1985b, Theorem 2.8] of the "change of variables formula". The kernel on the left is 0, and on the right is the torsion subgroup of $A(K_\upsilon)$ [Bourbaki 1989, III.7.6].

Notation. Henceforth, we shall be concerned with curves over number fields and their Jacobians. We fix once and for all the following notation:

K is a number field,

C is a smooth projective absolutely irreducible curve defined over K of genus at least 2,

J is the Jacobian of C,

υ is a non-Archimedean prime of K of good reduction for C,
K_υ is the completion of K at υ,
k_υ is the residue field of K at υ,
$\mathbb{O}_\upsilon$ is the ring of integers in K_υ,
$x \mapsto \tilde{x}$ is the natural map $\mathbb{O}_\upsilon \to k_\upsilon$,
$\mathscr{C}_\upsilon$ is a minimal regular proper model for C over $\mathbb{O}_\upsilon$,
$\tilde{C}_\upsilon$ is the special fiber of $\mathscr{C}_\upsilon$ at υ, and
Ω_{C/K_υ} is the K_υ-vector space of global 1-forms on C.

Integration on curves and Jacobians. For any field extension M/K (not necessarily finite), we shall write $\Omega_{C/M}$ and $\Omega_{J/M}$ for the M-vector spaces of global 1-forms on C/M and J/M, respectively. We shall assume the existence of some $P_0 \in C(K)$. The point P_0 gives rise to an Abel–Jacobi map

$$\jmath : C \hookrightarrow J, \quad P \mapsto [P - P_0].$$

It is well known that the pull-back $\jmath^* : \Omega_{J/K} \to \Omega_{C/K}$ is an isomorphism of K-vector spaces [Milne 1986, Proposition 2.2]. Clearly any two Abel–Jacobi maps differ by a translation on J. As 1-forms on J are translation invariant, the map $\jmath^*$ is independent of the choice of P_0 [Wetherell 1997, Section 1.4]. Let υ be a non-Archimedean place for K. The isomorphism $\jmath^*$ extends to an isomorphism $\Omega_{J/K_\upsilon} \to \Omega_{C/K_\upsilon}$, which we shall also denote $\jmath^*$. For any global 1-form $\omega \in \Omega_{J/K_\upsilon}$ and any two points $P, Q \in C(K_\upsilon)$, we have

$$\int_Q^P \jmath^*\omega = \int_{\jmath Q}^{\jmath P} \omega = \int_0^{[P-Q]} \omega$$

using the properties of integration above. We shall henceforth use $\jmath^*$ to identify Ω_{C/K_υ} with Ω_{J/K_υ}. With this identification, the pairing (3) with $J = A$ gives the bilinear pairing

$$\Omega_{C/K_\upsilon} \times J(K_\upsilon) \to K_\upsilon, \quad \left(\omega, \left[\sum P_i - Q_i\right]\right) \mapsto \sum \int_{Q_i}^{P_i} \omega, \tag{4}$$

whose kernel on the right is 0 and on the left is the torsion subgroup of $J(K_\upsilon)$. We ease notation a little by defining, for divisor class $D = \sum P_i - Q_i$ of degree 0, the integral

$$\int_D \omega = \sum \int_{Q_i}^{P_i} \omega.$$

Note that this integral depends on the equivalence class of D and not on its decomposition as $D = \sum P_i - Q_i$.

Uniformizers. The usual Chabauty approach when studying rational points in a residue class is to work with a local coordinate (defined shortly) and create power-series equations in terms of the local coordinate whose solutions, roughly speaking, contain the rational points. In our case, we find it more convenient to shift the local coordinate so that it becomes a uniformizer at a rational point in the residue class.

Fix a non-Archimedean place υ of good reduction for C and a minimal regular proper model $\mathscr{C}_\upsilon$ for C over υ. Since our objective is explicit computation, we point out that in our case of good reduction, such a model is simply a system of equations for the nonsingular curve that reduces to a nonsingular system modulo υ. Let $Q \in C(K_\upsilon)$, and let $\tilde{Q}$ be its reduction on the special fiber $\tilde{C}_\upsilon$; as we are considering a regular model, $\tilde{Q}$ is a smooth point. Choose a rational function $s_Q \in K_\upsilon(C)$ so that the maximal ideal in $\mathbb{O}_{\mathscr{C}_\upsilon,\tilde{Q}}$ is (s_Q, π), where π is a uniformizing element for K_υ. The function s_Q is called [Lorenzini and Tucker 2002, Section 1] a *local coordinate* at Q. Let $t_Q = s_Q - s_Q(Q)$. We shall refer to t_Q, constructed as above, as a *well behaved uniformizer* at Q. A uniformizer at a smooth point Q means a local coordinate that vanishes with multiplicity 1 at Q. The reason for the adjective "well behaved" will be clear from Lemma 3.1 below.

Before stating the lemma, we define the *υ-unit ball around Q* to be

$$\mathcal{B}_\upsilon(Q) = \{\, P \in C(K_\upsilon) : \tilde{P} = \tilde{Q} \,\}. \tag{5}$$

Lemma 3.1.

(i) *t_Q is a uniformizer at Q.*

(ii) *$\tilde{t}_Q$ is a uniformizer at $\tilde{Q}$.*

(iii) *t_Q defines a bijection*

$$\mathcal{B}_\upsilon(Q) \to \pi\mathbb{O}_\upsilon, \quad P \mapsto t_Q(P),$$

where π is any uniformizing element for K_υ. In particular, for $P \in \mathcal{B}_\upsilon(Q)$, we have $t_Q(P) = 0$ if and only if $P = Q$.

Proof. Parts (i) and (ii) are clear from the construction. Part (iii) is standard; see [Lorenzini and Tucker 2002, Section 1; Wetherell 1997, Sections 1.7 and 1.8] for example. □

Estimating integrals on curves.

Lemma 3.2. *Let p be an odd rational prime that does not ramify in K. Let υ be a place of K above p. Let $Q \in C(K_\upsilon)$, and let $t_Q \in K_\upsilon(C)$ be a well behaved uniformizer at Q. Let $\omega \in \Omega_{\mathscr{C}_\upsilon/\mathbb{O}_\upsilon}$. Then there is a power series*

$$\phi(x) = \alpha_1 x + \alpha_2 x^2 + \alpha_3 x^3 + \cdots \in K_\upsilon[[x]] \tag{6}$$

that converges for $x \in \pi\mathbb{O}_v$ such that

$$\int_Q^P \omega = \phi(z)$$

for all $P \in \mathcal{B}_v(Q)$, where $z = t_Q(P)$. Moreover, the coefficient α_1 is given by

$$\alpha_1 = \Big(\frac{\omega}{dt_Q}\Big)(Q) \in \mathbb{O}_v, \tag{7}$$

where we interpret ω/dt_Q as an element of $K_v(C)$, and

$$\phi(z) = \int_Q^P \omega \equiv \alpha_1 z \pmod{z^2\mathbb{O}_v}. \tag{8}$$

Proof. We can expand ω (after viewing it as an element in $\Omega_{\hat{\mathbb{O}}_Q}$) as a formal power series

$$\omega = (\gamma_0 + \gamma_1 t_Q + \gamma_2 t_Q^2 + \cdots)dt_Q,$$

where the coefficients γ_i belong to $\mathbb{O}_v$ (see [Lorenzini and Tucker 2002, Proposition 1.6; Wetherell 1997, Chapters 1.7 and 1.8] for example); here we have not used the assumption that $t_Q(Q) = 0$, merely that t_Q is a local coordinate at Q. We note that $(\omega/dt_Q)(Q) = \gamma_0$ and is hence integral.

Let $P \in \mathcal{B}_v(Q)$ and $z = t_Q(P)$. Then (see [Lorenzini and Tucker 2002, Proposition 1.3] for example)

$$\int_Q^P \omega = \sum_{j=0}^{\infty} \frac{\gamma_j}{j+1} z^{j+1}. \tag{9}$$

Thus, in (6), we take the coefficients $\alpha_i = \gamma_{i-1}/i$. The power series $\phi(x)$ converges for $x \in \pi\mathbb{O}_v$ as the γ_i are integral. In particular, $\phi(z)$ converges since $\mathrm{ord}_v(z) \geq 1$ by Lemma 3.1(iii). To complete the proof, observe that

$$\phi(z) - \alpha_1 z = z^2\Big(\frac{\gamma_1}{2} + \frac{\gamma_2}{3}z + \frac{\gamma_3}{4}z^2 + \cdots\Big).$$

We must show the sum in brackets belongs to $\mathbb{O}_v$. Thus, it is sufficient to show that

$$\mathrm{ord}_v(j+2) \leq j$$

for all $j \geq 0$. But $K_v/\mathbb{Q}_p$ is unramified, and so $\mathrm{ord}_v(j+2) = \mathrm{ord}_p(j+2)$. Hence, we need to show that $\mathrm{ord}_p(j+2) \leq j$ for all $j \geq 0$ and all odd primes p. This is now an easy exercise. □

4. Chabauty in a single unit ball

Let C be a smooth projective curve over a number field K. Let J be the Jacobian of C, and write r for the rank of the Mordell–Weil group $J(K)$. Let $D_1, \dots, D_r$ be a basis for a free subgroup of finite index in $J(K)$.

Let p a rational prime such that

(p1) p is odd,

(p2) p is unramified in K, and

(p3) every prime υ of K above p is a prime of good reduction for the curve C.

Let $Q \in C(K)$. For $\upsilon \mid p$, let $\mathcal{B}_\upsilon(Q)$ be as in (5), and define the *p-unit ball around* Q to be

$$\mathcal{B}_p(Q) = \prod_{\upsilon \mid p} \mathcal{B}_\upsilon(Q). \tag{10}$$

We will shortly give a criterion for a point $Q \in C(K)$ to be the unique K-rational point in its own p-unit ball. Our criterion and its proof are rather involved. As motivation, we first explain the case $K = \mathbb{Q}$.

Motivation. Suppose $K = \mathbb{Q}$. Let $P \in C(\mathbb{Q}) \cap \mathcal{B}_p(Q)$. We will write down equations that give information about P and which, with appropriate assumptions, allow us to show that $P = Q$.

Let m be the index

$$m := [J(\mathbb{Q}) : \langle D_1, \dots, D_r \rangle].$$

There are integers $n_1', \dots, n_r'$ such that

$$m(P - Q) = n_1' D_1 + \cdots + n_r' D_r, \tag{11}$$

where the equality takes place in $\mathrm{Pic}^0(C)$. Let $\omega_1, \dots, \omega_g$ be a $\mathbb{Z}_p$ basis for $\Omega_{\mathscr{C}_p/\mathbb{Z}_p}$. By the properties of integration explained in Section 3,

$$m \int_Q^P \omega_i = n_1' \tau_{i,1} + \cdots + n_r' \tau_{i,r}, \quad i = 1, \dots, g,$$

where the $\tau_{i,j}$ are given by

$$\tau_{i,j} = \int_{D_j} \omega_i, \quad j = 1, \dots, r.$$

Let $n_i = n_i'/m \in \mathbb{Q}$. Thus,

$$\int_Q^P \omega_i = n_1 \tau_{i,1} + \cdots + n_r \tau_{i,r}.$$

Let t_Q be a well behaved uniformizer at Q as defined on page 771, and write $z = t_Q(P)$. By Lemma 3.1, we know that $z \in p\mathbb{Z}_p$. By Lemma 3.2, there are power series ϕ_i with coefficients in $\mathbb{Q}_p$, converging on $p\mathbb{Z}_p$, such that

$$\int_Q^P \omega_i = \phi_i(z) = \alpha_i z + \alpha_i' z^2 + \alpha_i'' z^2 + \cdots .$$

Then

$$n_1\tau_{i,1} + \cdots + n_r\tau_{i,r} = \phi_i(z), \quad i = 1, \ldots, g. \tag{12}$$

This is a system of g equations in $r+1$ unknowns, $n_1, n_2, \ldots, n_r, z$. If $r \le g-1$, we can use linear algebra to eliminate $n_1, n_2, \ldots, n_r$ to obtain $g-r$ equations

$$\theta_1(z) = \theta_2(z) = \cdots = \theta_{g-r}(z) = 0,$$

where the $\theta_i(z)$ are power series with coefficients in $\mathbb{Q}_p$, converging on $p\mathbb{Z}_p$. In practical computations, it is usual at this point to use Newton polygons and other techniques to bound the number of solutions to this system with $z \in p\mathbb{Z}_p$. By Lemma 3.1(iii), the map $\mathcal{B}_p(Q) \to p\mathbb{Z}_p$ given by $P \mapsto t_Q(P) = z$ is bijective; thus, we also obtain a bound on the number of $P \in C(\mathbb{Q}) \cap \mathcal{B}_p(Q)$.

Now we want a practical criterion for Q to be the unique rational point in its p-unit ball or equivalently that $z = 0$. The system of equations (12) is easier to analyze if we consider only the linear terms of the power series ϕ_i. By (8),

$$n_1\tau_{i,1} + \cdots + n_r\tau_{i,r} \equiv \alpha_i z \pmod{z^2\mathbb{Z}_p},$$

where $\alpha_i = (\omega_i/dt_Q)(Q) \in \mathbb{Z}_p$. Let T be the $g \times r$ matrix $(\tau_{i,j})$ — this has entries in $\mathbb{Q}_p$. Let A be the column vector (α_i). We can rewrite this linear system of congruences in matrix form

$$T\boldsymbol{n} \equiv Az \pmod{z^2\mathbb{Z}_p},$$

where $\boldsymbol{n}$ is the column vector (n_i). Choose a non-negative integer a such that p^aT has entries in $\mathbb{Z}_p$. Let U be a unimodular matrix with entries in $\mathbb{Z}_p$ so that $U \cdot p^aT$ is in Hermite normal form (HNF) (see [Cohen 2000, Section 1.4.2] for the theory of HNF). Let h be the number of zero rows of $U \cdot p^aT$; as $U \cdot p^aT$ is in HNF, these are the last h rows. Let $M_p(Q)$ be the vector in $\mathbb{Z}_p^h$ formed by the last h elements of UA.

Lemma 4.1. *With the above assumptions and notation, suppose $h > 0$ and let $\tilde{M}_p(Q) \in \mathbb{F}_p^h$ denote the vector obtained by reducing $M_p(Q)$ mod p. If $\tilde{M}_p(Q) \neq \mathbf{0}$, then $C(\mathbb{Q}) \cap \mathcal{B}_p(Q) = \{Q\}$.*

Proof. From the above, we know that

$$M_p(Q)z \equiv 0 \pmod{z^2\mathbb{Z}_p}$$

and that $M_p(Q)$ has entries in $\mathbb{Z}_p$. Suppose β is some entry of $M_p(Q)$ such that $\beta \not\equiv 0 \pmod{p}$. Then $\beta z \equiv 0 \pmod{z^2\mathbb{Z}_p}$. As $z \in p\mathbb{Z}_p$, we must have that $z = 0$. By the above discussion, this forces $P = Q$. □

We do not take any credit for this lemma; the ideas involved can found in [Coleman 1985a]. We have however expressed our lemma and the ideas leading up to it in a way that motivates our generalization to the case where $[K : \mathbb{Q}] > 1$.

The general case. We return to the general case where K is a number field. The p-unit ball $\mathcal{B}_p(Q)$ is defined in (10). We would like to give a criterion for Q to be the unique K-rational point in its p-unit ball. Again, let $P \in C(K) \cap \mathcal{B}_p(Q)$. We will write equations that give information about P and devise a Chabauty-style criterion that forces $P = Q$. In the case $K = \mathbb{Q}$, the variable $z = t_Q(P)$ measured the "distance from P to Q along $C(\mathbb{Q}_p)$". Now the field K has several embeddings K_υ with $\upsilon \mid p$. We will need to replace z by a vector whose entries "measure the distances from P to Q along $\prod_{\upsilon|p} C(K_\upsilon)$".

To state our criterion — Theorem 2 below — we need to define a pair of matrices T and A. The matrix T depends on the basis $D_1, \ldots, D_r$. The matrix A depends on the point $Q \in C(K)$. Let $\upsilon_1, \ldots, \upsilon_n$ be the places of K above p. For each place υ above p, we fix once and for all a $\mathbb{Z}_p$-basis $\theta_{\upsilon,1}, \ldots, \theta_{\upsilon,d_\upsilon}$ for $\mathbb{O}_\upsilon$, where $d_\upsilon = [K_\upsilon : \mathbb{Q}_p]$. Of course, $d_\upsilon = [\mathbb{O}_\upsilon : \mathbb{Z}_p] = [k_\upsilon : \mathbb{F}_p]$ as p is unramified in K. We also choose an $\mathbb{O}_\upsilon$-basis $\omega_{\upsilon,1}, \ldots, \omega_{\upsilon,g}$ for $\Omega_{\mathscr{C}_\upsilon/\mathbb{O}_\upsilon}$.

Now fix υ above p, and let $\omega \in \Omega_{\mathscr{C}_\upsilon/\mathbb{O}_\upsilon}$. Let

$$\tau_j = \int_{D_j} \omega, \quad j = 1, \ldots, r. \tag{13}$$

Write

$$\tau_j = \sum_{i=1}^{d_\upsilon} t_{ij}\theta_{\upsilon,i}, \quad t_{ij} \in \mathbb{Q}_p. \tag{14}$$

Let

$$T_{\upsilon,\omega} = (t_{ij})_{i=1,\ldots,d_\upsilon,\ j=1,\ldots,r}; \tag{15}$$

that is, $T_{\upsilon,\omega}$ is the $d_\upsilon \times r$ matrix with entries t_{ij}. Recall that $\omega_{\upsilon,1}, \ldots, \omega_{\upsilon,g}$ is a basis for $\Omega_{\mathscr{C}_\upsilon/\mathbb{O}_\upsilon}$. Let

$$T_\upsilon = \begin{pmatrix} T_{\upsilon,\omega_{\upsilon,1}} \\ T_{\upsilon,\omega_{\upsilon,2}} \\ \vdots \\ T_{\upsilon,\omega_{\upsilon,g}} \end{pmatrix}; \tag{16}$$

this is a $gd_\upsilon \times r$ matrix with entries in $\mathbb{Q}_p$. We now define the matrix T needed for our criterion below:

$$T = \begin{pmatrix} T_{\upsilon_1} \\ T_{\upsilon_2} \\ \vdots \\ T_{\upsilon_n} \end{pmatrix}. \tag{17}$$

Note that T is a $gd \times r$ matrix with entries in $\mathbb{Q}_p$, where $d = [K : \mathbb{Q}] = d_{\upsilon_1} + \cdots + d_{\upsilon_n}$.

Let $Q \in C(K)$. We now define the second matrix A (depending on Q) needed to state our criterion for $C(K) \cap \mathcal{B}_p(Q) = \{Q\}$. For each place υ of K above p, we have chosen a minimal proper regular model $\mathscr{C}_\upsilon$. Let t_Q be a well behaved uniformizer at Q as defined in Section 3. Let $\omega \in \Omega_{\mathscr{C}_\upsilon/\mathbb{O}_\upsilon}$, and let α be given by (7). By Lemma 3.2, $\alpha \in \mathbb{O}_\upsilon$. Recall we have fixed a basis $\theta_{\upsilon,1}, \ldots, \theta_{\upsilon,d_\upsilon}$ for $\mathbb{O}_\upsilon/\mathbb{Z}_p$. Write

$$\alpha \cdot \theta_{\upsilon,j} = \sum_{i=1}^{d_\upsilon} a_{ij}\theta_{\upsilon,i}, \quad j = 1, \ldots, d_\upsilon, \tag{18}$$

with $a_{ij} \in \mathbb{Z}_p$. Let

$$A_{\upsilon,\omega} = (a_{ij})_{i,j=1,\ldots,d_\upsilon}. \tag{19}$$

Let

$$A_\upsilon = \begin{pmatrix} A_{\upsilon,\omega_1} \\ A_{\upsilon,\omega_2} \\ \vdots \\ A_{\upsilon,\omega_g} \end{pmatrix}; \tag{20}$$

this is a $d_\upsilon g \times d_\upsilon$ matrix with entries in $\mathbb{Z}_p$. Let

$$A = \begin{pmatrix} A_{\upsilon_1} & \mathbf{0} & \cdots & \mathbf{0} \\ \mathbf{0} & A_{\upsilon_2} & \cdots & \mathbf{0} \\ \vdots & \vdots & \ddots & \vdots \\ \mathbf{0} & \mathbf{0} & \cdots & A_{\upsilon_n} \end{pmatrix}. \tag{21}$$

Then A is a $dg \times d$ matrix with entries in $\mathbb{Z}_p$.

Choose a non-negative integer a such that $p^a T$ has entries in $\mathbb{Z}_p$. Let U be a unimodular matrix with entries in $\mathbb{Z}_p$ such that $U \cdot p^a T$ is in HNF. Let h be the number of zero rows of $U \cdot p^a T$; these are the last h rows. Let $M_p(Q)$ be the $h \times d$ matrix (with entries in $\mathbb{Z}_p$) formed by the last h rows of UA.

Theorem 2. *With the assumptions and notation above, let $\tilde{M}_p(Q)$ denote the matrix with entries in $\mathbb{F}_p$ obtained by reducing $M_p(Q)$ modulo p. If $\tilde{M}_p(Q)$ has rank d, then $C(K) \cap \mathcal{B}_p(Q) = \{Q\}$.*

Remarks. (i) Let $\boldsymbol{u}_1, \ldots, \boldsymbol{u}_h$ be a $\mathbb{Z}_p$-basis for the kernel of the homomorphism of $\mathbb{Z}_p$-modules $\mathbb{Z}_p^{gd} \to \mathbb{Z}_p^r$ given by $p^a T$. Then $\boldsymbol{u}_1 A, \ldots, \boldsymbol{u}_h A$ span the same $\mathbb{Z}_p$-module as the rows of $M_p(Q)$, showing that the rank of $\tilde{M}_p(Q)$ is independent of the choice of U.

(ii) Since the matrix T is $gd \times r$, it is evident that $h \geq \max(gd - r, 0)$ and, very likely, $h = \max(gd - r, 0)$. Now the matrix $\tilde{M}_p(Q)$ is $h \times d$, and so a necessary condition for the criterion to hold is that $h \geq d$. Thus, it is sensible to apply the theorem when $gd - r \geq d$ or equivalently when $r \leq d(g-1)$.

(iii) In practice, we do not compute the matrix T exactly, merely an approximation to it. Thus, we won't be able to provably determine h unless $h = \max(gd - r, 0)$.

Proof of Theorem 2. Suppose that $P \in C(K) \cap \mathcal{B}_p(Q)$. We need to show $P = Q$.

Let m be the index

$$m := [J(K) : \langle D_1, \ldots, D_r \rangle].$$

There are integers $n_1', \ldots, n_r'$ such that (11) holds, where the equality takes place in $\mathrm{Pic}^0(C)$.

Let υ be one of the places $\upsilon_1, \ldots, \upsilon_n$ above p. Recall that we have chosen a well behaved uniformizer t_Q at Q. Write $z = t_Q(P)$. By Lemma 3.1(iii), $\mathrm{ord}_\upsilon(z) \geq 1$. We will show that $z = 0$, and so again by Lemma 3.1(iii), $P = Q$, which is what we want to prove.

We write

$$z = z_{\upsilon,1}\theta_{\upsilon,1} + \cdots + z_{\upsilon,d_\upsilon}\theta_{\upsilon,d_\upsilon},$$

where $z_{\upsilon,i} \in \mathbb{Z}_p$. As $\tilde{\theta}_{\upsilon,1}, \ldots, \tilde{\theta}_{\upsilon,d_\upsilon}$ is a basis for $k_\upsilon/\mathbb{F}_p$ and $\mathrm{ord}_\upsilon(z) \geq 1$, we see that $\mathrm{ord}_\upsilon(z_{\upsilon,i}) \geq 1$ for $i = 1, \ldots, d_\upsilon$. Let

$$s_\upsilon = \min_{1 \leq i \leq d_\upsilon} \mathrm{ord}_p(z_{\upsilon,i}). \tag{22}$$

We will show that $s_\upsilon = \infty$, which implies that $z_{\upsilon,i} = 0$ for $i = 1, \ldots, d_\upsilon$, and so $z = 0$ as required. For now, we note that $s_\upsilon \geq 1$.

Now fix an $\omega \in \Omega_{\mathcal{C}_\upsilon/\mathbb{C}_\upsilon}$, and let $\alpha \in \mathbb{C}_\upsilon$ be as in Lemma 3.2; by that lemma,

$$\int_Q^P \omega = \alpha z + \beta z^2$$

for some $\beta \in \mathbb{C}_\upsilon$. However, by (11) and the properties of integration explained in Section 3,

$$m \int_Q^P \omega = n_1'\tau_1 + \cdots + n_r'\tau_r,$$

where the τ_j are given in (13). Let $n_i = n_i'/m \in \mathbb{Q}$. Thus,

$$\int_Q^P \omega = n_1\tau_1 + \cdots + n_r\tau_r.$$

Hence,

$$n_1\tau_1 + \cdots + n_r\tau_r = \alpha(z_{\upsilon,1}\theta_{\upsilon,1} + \cdots + z_{\upsilon,d_\upsilon}\theta_{\upsilon,d_\upsilon}) + \beta(z_{\upsilon,1}\theta_{\upsilon,1} + \cdots + z_{\upsilon,d_\upsilon}\theta_{\upsilon,d_\upsilon})^2.$$

From this and (22), we obtain

$$n_1\tau_1 + \cdots + n_r\tau_r \equiv z_{\upsilon,1}(\alpha\theta_{\upsilon,1}) + \cdots + z_{\upsilon,d_\upsilon}(\alpha\theta_{\upsilon,d_\upsilon}) \pmod{p^{2s_\upsilon}\mathbb{O}_\upsilon}. \tag{23}$$

Write

$$\boldsymbol{n} = \begin{pmatrix} n_1 \\ n_2 \\ \vdots \\ n_r \end{pmatrix} \quad \text{and} \quad \boldsymbol{z}_\upsilon = \begin{pmatrix} z_{\upsilon,1} \\ z_{\upsilon,2} \\ \vdots \\ z_{\upsilon,d_\upsilon} \end{pmatrix}, \tag{24}$$

and note that the entries of $\boldsymbol{n}$ are in $\mathbb{Q}$ and the entries of $\boldsymbol{z}_\upsilon$ are in $p^{s_\upsilon}\mathbb{Z}_p$. Recall that we have expressed $\tau_j = \sum t_{ij}\theta_{\upsilon,i}$ in (14) and $\alpha \cdot \theta_{\upsilon,j} = \sum a_{ij}\theta_{\upsilon,i}$ in (18), where t_{ij} are in $\mathbb{Q}_p$ and the a_{ij} are in $\mathbb{Z}_p$. Substituting in (23) and comparing the coefficients for $\theta_{\upsilon,i}$, we obtain

$$T_{\upsilon,\omega}\boldsymbol{n} \equiv A_{\upsilon,\omega}\boldsymbol{z}_\upsilon \pmod{p^{2s_\upsilon}},$$

where $T_{\upsilon,\omega}$ and $A_{\upsilon,\omega}$ are respectively given in (15) and (19).

Let T_υ and A_υ be as given in (16) and (20), respectively. Then

$$T_\upsilon\boldsymbol{n} \equiv A_\upsilon\boldsymbol{z}_\upsilon \pmod{p^{2s_\upsilon}}.$$

Now let

$$\boldsymbol{z} = \begin{pmatrix} \boldsymbol{z}_{\upsilon_1} \\ \boldsymbol{z}_{\upsilon_2} \\ \vdots \\ \boldsymbol{z}_{\upsilon_n} \end{pmatrix}.$$

Then $\boldsymbol{z}$ is of length $d = [K : \mathbb{Q}]$ with entries in $p\mathbb{Z}_p$. Write

$$s = \min_{\upsilon=\upsilon_1,\ldots,\upsilon_n} s_\upsilon = \min_{i,j} \operatorname{ord}_{\upsilon_j}(z_{i,\upsilon_j}), \tag{25}$$

where the s_υ are defined in (22). Clearly $s \geq 1$. It is sufficient to show that $s = \infty$ since then all of the $z_{i,\upsilon_j} = 0$, implying that $P = Q$.

Let T and A be as given in (17) and (21). Then

$$T\boldsymbol{n} \equiv A\boldsymbol{z} \pmod{p^{2s}}, \tag{26}$$

where we note once again that T is $dg \times r$ with entries in $\mathbb{Q}_p$ and A is $dg \times d$ with entries in $\mathbb{Z}_p$.

Let U, $M_p(Q)$, and h be as in the paragraph preceding the statement of the theorem. Suppose that $\tilde{M}_p(Q)$ has rank d. Suppose $s < \infty$, and we will derive a contradiction. Recall that the last h rows of UT are zero. From (26), we have that $M_p(Q)\boldsymbol{z} \equiv 0 \pmod{p^{2s}}$ since, by definition, $M_p(Q)$ is the matrix formed by the last h rows of UA. In particular, $M_p(Q)$ has entries in $\mathbb{Z}_p$ since both U and A have entries in $\mathbb{Z}_p$. From the definition of s in (25), we can write $\boldsymbol{z} = p^s\boldsymbol{w}$, where the entries of $\boldsymbol{w}$ are in $\mathbb{Z}_p$ and $\boldsymbol{w} \not\equiv \boldsymbol{0} \pmod{p}$. However, $M_p(Q)\boldsymbol{w} \equiv 0 \pmod{p^s}$, and as $s \geq 1$, we have that $M_p(Q)\boldsymbol{w} \equiv 0 \pmod{p}$. Since $\boldsymbol{w} \in \mathbb{Z}_p^d$, if $\tilde{M}_p(Q)$ has rank d, then $\boldsymbol{w} \equiv \boldsymbol{0} \pmod{p}$, giving the desired contradiction. □

Remark. In the above, we are only considering the linear terms of the power series $\phi(z)$, and this is enough for our criterion for $C(K) \cap \mathcal{B}_p(Q) = \{Q\}$. Of course, if there is another rational point sharing the same p-unit ball as Q, then our criterion will fail. It may then be possible to obtain an upper bound for the number of rational points in the p-unit ball by writing out higher terms of the power series and eliminating the n_i. This is likely to be technical, and we have not attempted it in practice. However, we note that we can always choose a large enough prime p so that no two known rational points share the same p-unit ball. If our necessary condition $r \leq d(g-1)$ is satisfied, then we expect to be able to find a prime p so that our Chabauty criterion succeeds in showing $C(K) \cap \mathcal{B}_p(Q) = \{Q\}$ for all known rational points Q. We then expect to be able to complete our determination of the rational points using the Mordell–Weil sieve as explained below.

5. Chabauty and the Mordell–Weil sieve

For the complete determination of the set of rational points on a curve of genus at least 2, it is often necessary to combine Chabauty with the Mordell–Weil sieve. Before giving details of how this works in our case, we sketch the idea behind the Mordell–Weil sieve.

We continue with the notation of the previous sections. In particular, C is a smooth curve defined over a number field K and P_0 is a fixed K-rational point on C. Let $\mathcal{K}$ be the subset of known K-rational points on C, and suppose that we would like to prove that $C(K) = \mathcal{K}$. Using our Theorem 2, it may be possible to show, for some prime p, that $C(K) \cap \mathcal{B}_p(Q) = \{Q\}$ for every $Q \in \mathcal{K}$. In this situation, Chabauty tells us that to show that $C(K) = \mathcal{K}$, all you have to do is show that every $P \in C(K)$ belongs to the p-unit ball $\mathcal{B}_p(Q)$ for some $Q \in \mathcal{K}$. This is where we turn to the Mordell–Weil sieve.

Let υ be a place of K of good reduction for C. Let red denote the natural maps

$$\mathrm{red} : C(K) \to C(k_\upsilon) \quad \text{and} \quad \mathrm{red} : J(K) \to J(k_\upsilon).$$

Let $\jmath$ denote the Abel–Jacobi maps

$$C(K) \hookrightarrow J(K) \quad \text{and} \quad C(k_\upsilon) \hookrightarrow J(k_\upsilon)$$

respectively associated to P_0 and $\tilde{P}_0$. A glance at the commutative diagram

$$\begin{array}{ccc} C(K) & \xrightarrow{\jmath} & J(K) \\ \Big\downarrow{\scriptstyle \text{red}} & & \Big\downarrow{\scriptstyle \text{red}} \\ C(k_\upsilon) & \xrightarrow{\jmath} & J(k_\upsilon) \end{array}$$

shows that $\jmath(C(K)) \subseteq W_\upsilon + L_\upsilon$, where $L_\upsilon := \ker(J(K) \to J(k_\upsilon))$ is a subgroup of finite index in $J(K)$ and W_υ is a set of coset representatives for $\text{red}^{-1}\jmath(C(k_\upsilon))$. In practice, if one knows a Mordell–Weil basis for $J(K)$, then W_υ and L_υ are straightforward to compute. Now let S be a finite set of places υ of K, all of good reduction for C. We can write

$$\bigcap_{\upsilon \in S} (W_\upsilon + L_\upsilon) = W_S + L_S, \tag{27}$$

where W_S is a finite subset of $J(K)$ and $L_S = \cap_{\upsilon \in S} L_\upsilon$ (of course, the elements of W_S are unique up to translation by elements of L_S). Clearly $\jmath(C(K)) \subseteq W_S + L_S$. With a judicious choice of places S, it is sometimes possible to show that

$$\jmath(\mathcal{H}) + L_S = W_S + L_S \supseteq \jmath(C(K)),$$

where the index $[J(K) : L_S]$ is large. In other words, any rational point is "close" to a known rational point in the profinite topology on the Mordell–Weil group. Suppose next that there is some rational prime p satisfying assumptions (p1)–(p3) on page 773 and that L_S is contained in the kernel of the diagonal map

$$J(K) \to \prod_{\upsilon | p} J(k_\upsilon).$$

It then follows that, for every $P \in C(K)$, there is some $Q \in \mathcal{H}$ (one of the known rational points) such that $P \in \mathcal{B}_p(Q)$. We may then attempt to apply Theorem 2 to show that $C(K) \cap \mathcal{B}_p(Q) = \{Q\}$ for all $Q \in \mathcal{H}$; if we can show this, then we will have shown that $C(K) = \mathcal{H}$.

The standard references for the Mordell–Weil sieve, e.g., [Bruin and Elkies 2002; Bruin and Stoll 2008; 2010; Bugeaud et al. 2008], as well as the above sketch assume full knowledge of the Mordell–Weil group. For reasons that we now explain, we need to adapt the Mordell–Weil sieve to work with a subgroup of the Mordell–Weil group of finite (but unknown) index. Let L_0 be a subgroup of $J(K)$ of finite index containing the free subgroup L generated by $D_1, \ldots, D_r$ of the previous section. We can take $L_0 = L$, but for our purpose, it is preferable to

include the torsion subgroup of $J(K)$ in L_0. The usual p-saturation method [Siksek 1995b; 1995a; Flynn and Smart 1997] shows how to enlarge L_0 so that its index in $J(K)$ is not divisible by any given small prime p. One expects, after checking p-saturation for all small primes p up to some large bound, that L_0 is in fact equal to $J(K)$. However, proving that $J(K) = L_0$ requires an explicit theory of heights on the Jacobian J. This is not yet available for Jacobians of curves of genus at least 3. For Jacobians of curves of genus 2, there is an explicit theory of heights [Flynn 1995a; Flynn and Smart 1997; Stoll 1999; 2002b] though the bounds over number fields other than the rationals are likely to be impractically large.

Before we give the details, we point out that substantial improvements can be made to the version of the Mordell–Weil sieve outlined below. It has certainly been sufficient for the examples we have computed so far (including the ones detailed in the next section). But we expect that for some other examples it will be necessary (though not difficult) to incorporate the improvements to the Mordell–Weil sieve found in [Bruin and Stoll 2008; 2010].

Lemma 5.1 (Mordell–Weil sieve). *Let L_0 be a subgroup of $J(K)$ of finite index $n = [J(K) : L_0]$. Let $P_0 \in C(K)$, and let $\jmath$ denote the Abel–Jacobi maps associated to P_0 as above. Let $\upsilon_1, \dots, \upsilon_s$ be places of K such that each $\upsilon = \upsilon_i$ satisfies the following two conditions*:

(υ1) *υ is a place of good reduction for C and*

(υ2) *the index n is coprime to $\#J(k_\upsilon)$.*

To ease notation, write k_i for the residue field k_{υ_i}. Define inductively a sequence of subgroups

$$L_0 \supseteq L_1 \supseteq L_2 \supseteq L_3 \supseteq \cdots \supseteq L_s$$

and finite subsets $W_0, W_1, \dots, W_s \subseteq L_0$ as follows. Let $W_0 = \{\mathbf{0}\}$. Suppose we have defined L_i and W_i, where $i \le s-1$. Let L_{i+1} be the kernel of the composition

$$L_i \hookrightarrow J(K) \to J(k_{i+1}).$$

To define W_{i+1}, choose a complete set $\mathcal{Q}$ of coset representatives for L_i/L_{i+1} and let

$$W'_{i+1} = \{\, \boldsymbol{w} + \boldsymbol{q} : \boldsymbol{w} \in W_i \text{ and } \boldsymbol{q} \in \mathcal{Q} \,\}.$$

Let

$$W_{i+1} = \{\, \boldsymbol{w} \in W'_{i+1} : \mathrm{red}(\boldsymbol{w}) \in \jmath(C(k_{i+1})) \,\}.$$

Then, for every $i = 0, \dots, s$ and every $Q \in C(K)$, there is some $\boldsymbol{w} \in W_i$ such that

$$n(\jmath(Q) - \boldsymbol{w}) \in L_i. \tag{28}$$

Remark. If $L_0 = J(K)$, there is no difference between the usual Mordell–Weil sieve sketched at the beginning of this section and the Mordell–Weil sieve of the lemma. However, we have expressed the Mordell–Weil sieve in the lemma iteratively as this reflects how it is used in practice; we compute the intersection (27) gradually rather than all at once.

Proof of Lemma 5.1. The proof is by induction on i. Since L_0 has index n in $J(K)$, (28) is true with $\boldsymbol{w} = 0$. Let $i \leq s-1$. Suppose $Q \in C(K)$, $\boldsymbol{w}' \in W_i$, and $\boldsymbol{l}' \in L_i$ satisfy

$$n(\jmath(Q) - \boldsymbol{w}') = \boldsymbol{l}'. \tag{29}$$

By definition of L_{i+1}, the quotient group L_i/L_{i+1} is isomorphic to a subgroup of $J(k_{i+1})$. It follows from assumption ($\upsilon 2$) that n is coprime to the order of L_i/L_{i+1}. Recall that $\mathfrak{Q}$ was defined as a complete set of coset representatives for L_i/L_{i+1}. Thus, $n\mathfrak{Q}$ is also a set of coset representatives. Hence, we may express $\boldsymbol{l}' \in L_i$ as

$$\boldsymbol{l}' = n\boldsymbol{q} + \boldsymbol{l},$$

where $\boldsymbol{q} \in \mathfrak{Q}$ and $\boldsymbol{l} \in L_{i+1}$. Let $\boldsymbol{w} = \boldsymbol{w}' + \boldsymbol{q}$. Then $\boldsymbol{w} \in W'_{i+1}$. By (29), we see that

$$n(\jmath(Q) - \boldsymbol{w}) = \boldsymbol{l}' - n\boldsymbol{q} = \boldsymbol{l} \in L_{i+1}.$$

To complete the inductive argument, all we need to show is that $\boldsymbol{w} \in W_{i+1}$ or equivalently that $\mathrm{red}(\boldsymbol{w}) \in \jmath(C(k_{i+1}))$. However, since L_{i+1} is contained in the kernel of $\mathrm{red} : J(K) \to J(k_{i+1})$, we see that

$$n(\jmath(\tilde{Q}) - \mathrm{red}(\boldsymbol{w})) = 0 \quad \text{in } J(k_{i+1}).$$

Using the fact that n is coprime to $\#J(k_{i+1})$ once again gives $\mathrm{red}(\boldsymbol{w}) = \jmath(\tilde{Q})$ as required. □

The following theorem puts together the Mordell–Weil sieve with Theorem 2 to give a criterion for $C(K) = \mathcal{K}$. It is precisely the argument sketched before Lemma 5.1 but adapted to take account of the possibility that the index n may not be 1.

Theorem 3 (Chabauty with the Mordell–Weil sieve). *We continue with the above notation and assumptions. Let $L_0 \supseteq L_1 \supseteq \cdots \supseteq L_s$ and $W_0, \ldots, W_s$ be the sequences constructed in Lemma 5.1. Let $\mathcal{K}$ be a subset of $C(K)$. Let $P_0 \in \mathcal{K}$, and let $\jmath$ denote the maps associated to P_0 as above. Suppose that for every $\boldsymbol{w} \in W_s$, there is a point $Q \in \mathcal{K}$ and a prime p such that the following conditions hold*:

(a) *p satisfies conditions (p1)–(p3) on page 773.*

(b) *In the notation of the previous section, the matrix $\tilde{M}_p(Q)$ has rank d.*

(c) *The kernel of the homomorphism*

$$J(K) \longrightarrow \prod_{\upsilon \mid p} J(k_\upsilon) \tag{30}$$

contains both the group L_s and the difference $\jmath(Q) - \boldsymbol{w}$.

(d) *The index $n = [J(K) : L_0]$ is coprime to the orders of the groups $J(k_\upsilon)$ for $\upsilon \mid p$.*

Then $C(K) = \mathcal{H}$.

Proof. Suppose that $P \in C(K)$. We would like to show that $P \in \mathcal{H}$. By Lemma 5.1, there is some $\boldsymbol{w} \in W_s$ such that $n(\jmath(P) - \boldsymbol{w}) \in L_s$. Let $Q \in \mathcal{H}$ and prime p satisfy conditions (a)–(d) of the theorem. By (c), L_s is contained in the kernel of (30), and hence,

$$n(\jmath(\tilde{P}) - \mathrm{red}(\boldsymbol{w})) = 0$$

in $J(k_\upsilon)$ for all $\upsilon \mid p$. Since p satisfies assumption (d), it follows that

$$\jmath(\tilde{P}) - \mathrm{red}(\boldsymbol{w}) = 0$$

in $J(k_\upsilon)$ for all $\upsilon \mid p$. But by assumption (c) again,

$$\jmath(\tilde{Q}) - \mathrm{red}(\boldsymbol{w}) = 0$$

in $J(k_\upsilon)$ for all $\upsilon \mid p$. It follows that $\tilde{P} = \tilde{Q}$ in $C(k_\upsilon)$ for all $\upsilon \mid p$. Hence, $P \in \mathcal{B}_p(Q)$, where $\mathcal{B}_p(Q)$ is the p-unit ball around Q defined in (10). By assumption (b) and Theorem 2, we see that $P = Q \in \mathcal{H}$, completing the proof. □

6. The generalized Fermat equation with signature (2, 3, 10)

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

$$x^p + y^q = z^r \tag{31}$$

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 integer solutions x, y, and z. Such a solution is called *nontrivial* if $xyz \neq 0$ and *primitive* if x, y, and z are coprime. Let $\chi = p^{-1} + q^{-1} + r^{-1}$. The parametrization of nontrivial primitive solutions for (p, q, r) with $\chi \geq 1$ has now been completed [Edwards 2004]. The generalized Fermat conjecture [Darmon 1997; Darmon and Granville 1995] is concerned with the case $\chi < 1$. It states that the only nontrivial primitive solutions to (31) with $\chi < 1$ are those shows in Table 1.

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 [Wiles 1995; Taylor and Wiles 1995], $(p, p, 2)$ and $(p, p, 3)$ by Darmon and Merel [1997], $(2, 4, p)$ by Ellenberg [2004] and Bennett

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

Table 1. Known (and conjecturally only) primitive solutions to $x^p+y^q=z^r$ with $p^{-1}+q^{-1}+r^{-1}<1$.

et al. [2010], and $(2p, 2p, 5)$ by Bennett [Bennett 2006]. Recently, Chen and Siksek [2009] have solved the generalized Fermat equation with signatures $(3, 3, p)$ for a set of prime exponents p having Dirichlet density 28219/44928. For an exhaustive survey, see the book of Cohen [2007, Chapter 14]. An older but still very useful survey is [Kraus 1999].

There is an abundance of solutions for generalized Fermat equations with signatures $(2, 3, n)$ [Edwards 2004; Cohen 2007, Chapter 14], and so this subfamily is particularly interesting. The condition $\chi > 1$ within this subfamily coincides with the condition $n \geq 7$. The cases $n = 7, 8, 9$ are solved respectively in [Poonen et al. 2007; Bruin 2003; 2005]. The case $n = 10$ appears to be the first hitherto unresolved case within this subfamily, and this of course corresponds to Equation (1).

In this section, we solve Equation (1) in coprime integers x, y, and z, thereby proving Theorem 1. Equation (1) does not define a curve in $\mathbb{P}^3$; however, using standard factorization arguments, we will reduce its resolution to the determination of K-rational points on a family of genus-2 curves where $K = \mathbb{Q}(\sqrt[3]{2})$. One of these curves has Jacobian Mordell–Weil rank 2, and two others have Jacobian Mordell–Weil rank 3. Classical Chabauty is inapplicable as these curves defy the bound $r \leq g-1$. However, they do satisfy the weaker bound $r \leq d(g-1)$, which is a necessary condition for the applicability of our method. In what follows, we sketch how we successfully applied the method of this paper to determine the K-rational points on these curves. We used Magma [Bosma et al. 1997] for all our calculations. It includes implementations by Nils Bruin and Michael Stoll of 2-descent on Jacobians of hyperelliptic curves over number fields; the algorithm is detailed in [Stoll 2001]. Magma also includes an implementation of Chabauty for genus-2 curves over $\mathbb{Q}$.

Case I (y is odd). From (1), we immediately see that

$$x+z^5=u^3 \quad \text{and} \quad x-z^5=v^3,$$

where u and v are coprime and odd. Hence, $2z^5=u^3-v^3$.

Case I.1 ($3 \nmid z$). Then

$$u - v = 2a^5 \quad \text{and} \quad u^2 + uv + v^2 = b^5,$$

where a and b are coprime integers with $z = ab$. We now use the identity

$$(u - v)^2 + 3(u + v)^2 = 4(u^2 + uv + v^2) \tag{32}$$

to obtain $4a^{10} + 3c^2 = 4b^5$, where $c = u + v$. Dividing by $4a^{10}$, we obtain a rational point $(X, Y) = (b/a^2, 3c/2a^5)$ on the genus-2 curve

$$C : Y^2 = 3(X^5 - 1).$$

Using Magma, we are able to show that the Jacobian of this genus-2 curve C has Mordell–Weil rank 0 and torsion subgroup isomorphic to $\mathbb{Z}/2\mathbb{Z}$. It is immediate that $C(\mathbb{Q}) = \{\infty, (1, 0)\}$.

Working backwards, we obtain the solutions $(x, y, z) = (0, 1, \pm 1)$ to (1).

Case I.2 ($3 \mid z$). Recall that $2z^5 = u^3 - v^3$ and u and v are odd and coprime. Thus,

$$u - v = 2 \cdot 3^4 a^5 \quad \text{and} \quad u^2 + uv + v^2 = 3b^5,$$

where $z = 3ab$. Now we use identity (32) to obtain $4 \cdot 3^8 a^{10} + 3c^2 = 12b^5$, where $c = u + v$. Hence, we obtain a rational point $(X, Y) = (b/a^2, c/2a^5)$ on the genus-2 curve

$$C : Y^2 = X^5 - 3^7.$$

Let J be the Jacobian of C. Using Magma, we can show that $J(\mathbb{Q})$ is free of rank 1 with generator

$$\left(\frac{-9 + 3\sqrt{-3}}{2}, \frac{81 + 27\sqrt{-3}}{2}\right) + \left(\frac{-9 - 3\sqrt{-3}}{2}, \frac{81 - 27\sqrt{-3}}{2}\right) - 2\infty.$$

Using Magma's built-in Chabauty command, we find that $C(\mathbb{Q}) = \{\infty\}$. Working backwards, we obtain $(x, y, z) = (\pm 1, -1, 0)$.

Case II (y is even). We would now like to solve (1) with y even and x and y coprime. Replacing x by $-x$ if necessary, we obtain $x \equiv z^5 \pmod 4$. Thus,

$$x + z^5 = 2u^3 \quad \text{and} \quad x - z^5 = 4v^3,$$

where $y = -2uv$. Hence,

$$u^3 - 2v^3 = z^5 \quad \text{with } u \text{ and } v \text{ coprime and } u \text{ and } z \text{ odd.} \tag{33}$$

If $3 \mid z$, then this equation is impossible modulo 9. Hence, $3 \nmid z$.

Let $\theta = \sqrt[3]{2}$. We shall work in the number field $K = \mathbb{Q}(\theta)$. This has ring of integers $\mathbb{O}_K = \mathbb{Z}[\theta]$ with class number 1. The unit group is isomorphic to $\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ with $\epsilon = 1 - \theta$ a fundamental unit.

Observe that

$$(u - v\theta)(u^2 + uv\theta + v^2\theta^2) = z^5,$$

where the two factors on the left-hand side are coprime as u and v are coprime and z is neither divisible by 2 nor 3. Hence,

$$u - v\theta = \epsilon^s \alpha^5 \quad \text{and} \quad u^2 + uv\theta + v^2\theta^2 = \epsilon^{-s}\beta^5, \tag{34}$$

where $-2 \le s \le 2$ and $\alpha, \beta \in \mathbb{Z}[\theta]$ satisfy $z = \alpha\beta$. We now use the identity

$$(u - v\theta)^2 + 3(u + v\theta)^2 = 4(u^2 + uv\theta + v^2\theta^2)$$

to obtain

$$\epsilon^{2s}\alpha^{10} + 3(u + v\theta)^2 = 4\epsilon^{-s}\beta^5.$$

Let C_s be the genus-2 curve defined over K given by

$$C_s : Y^2 = 3(4\epsilon^{-s}X^5 - \epsilon^{2s}).$$

We see that

$$(X, Y) = \left(\frac{\beta}{\alpha^2}, \frac{3(u + v\theta)}{\alpha^5}\right) \tag{35}$$

is a K-rational point on C_s. To complete our proof of Theorem 1, we need to determine $C_s(K)$ for $-2 \le s \le 2$. Let J_s be the Jacobian of C_s. Using reduction at various places of K, we easily showed that the torsion subgroup of $J_s(K)$ is trivial in all cases. The 2-Selmer ranks of $J_s(K)$ are respectively 1, 3, 2, 3, and 0 for $s = -2, -1, 0, 2, 1$. We searched for K-rational points on each J_s by first searching for points on the associated Kummer surface. We are fortunate to have found enough independent points in $J_s(K)$ in each case to show that the Mordell–Weil rank is equal to the 2-Selmer rank. In other words, we have determined a basis for a subgroup of $J_s(K)$ of finite index, and this is given in Table 2.

In each case, the rank r is at most $3 = d(g - 1)$, where $d = [K : \mathbb{Q}] = 3$ and $g = 2$ is the genus. We note that the bound $r \le g - 1$ needed to apply classical Chabauty fails for $s = -1, 0, 1$.

We implemented our method in Magma. Our program succeeded in determining $C_s(K)$ for all $-2 \le s \le 2$, and the results are given in Table 2. The entire computation took approximately 2.5 hours on a 2.8 GHz dual-core AMD Opteron; this includes the time taken for computing Selmer groups and searching for points on the Kummer surfaces. It is appropriate to give more details, and we do this for the case $s = 1$. Let $C = C_1$, and write J for its Jacobian. Let

$$\mathcal{H} = \{\infty, P_0, P_0', P_1, P_1'\},$$

s	basis for subgroup of $J_s(K)$ of finite index	$C_s(K)$
-2	$(\theta^2+\theta+1, \theta^2+2\theta+1)-\infty$	∞, $(\theta^2+\theta+1, \pm(\theta^2+2\theta+1))$
-1	$(-\theta^2-\theta-1, 11\theta^2+13\theta+17)-\infty$, $\sum_{i=1,2}(\Phi_i, (2\theta^2+2\theta+3)\Phi_i+2\theta^2+3\theta+4)-2\infty$, $\sum_{i=3,4}(\Phi_i, (4\theta^2+6\theta+10)\Phi_i+9\theta^2+11\theta+13)-2\infty$	∞, $(\frac{-\theta^2-2\theta-1}{3}, \frac{\pm(\theta^2-\theta+1)}{3})$,$(-\theta^2-\theta-1, \pm(11\theta^2+13\theta+17))$
0	$(1, 3)-\infty$, $(\frac{\theta^2+2\theta+1}{3}, \frac{10\theta^2+8\theta+13}{3})-\infty$	∞, $(\frac{\theta^2+2\theta+1}{3}, \frac{\pm(10\theta^2+8\theta+13)}{3})$, $(1, \pm 3)$
1	$D_1 = (-\theta^2-\theta-1, -40\theta^2-53\theta-67)-\infty$, $D_2 = (-1, 3\theta+3)-\infty$, $D_3 = \sum_{i=5,6}(\Phi_i, (2\theta-2)\Phi_i-\theta+1)-2\infty$	∞, $(-\theta^2-\theta-1, \pm(40\theta^2+53\theta+67))$, $(-1, \pm(3\theta+3))$
2	$\varnothing$	∞

Table 2. Notation: Φ_1 and Φ_2 are the roots of $2\Phi^2+(\theta^2+\theta+2)\Phi+(\theta^2+\theta+2)=0$; Φ_3 and Φ_4 are the roots of $3\Phi^2+(4\theta^2+5\theta+4)\Phi+(4\theta^2+5\theta+7)=0$; Φ_5 and Φ_6 are the roots of $3\Phi^2+(\theta^2-\theta-2)\Phi+(-2\theta^2+2\theta+1)=0$.

where

$$P_0 = (-\theta^2-\theta-1, 40\theta^2+53\theta+67), \quad P_1 = (-1, 3\theta+3),$$

and P_0' and P_1' are respectively the images of P_0 and P_1 under the hyperelliptic involution. Let D_1, D_2, D_3 be the basis given in Table 2 for a subgroup of $J(K)$ of finite index. Let $L_0 = \langle D_1, D_2, D_3\rangle$. Our program verified that the index of L_0 in $J(K)$ is not divisible by any prime less than 75. Our program used the point

$$P_0 = (-\theta^2-\theta-1, 40\theta^2+53\theta+67)$$

as the base point for the Abel–Jacobi map $\jmath$. The image of $\mathcal{H}$ under $\jmath$ is

$$\jmath(\mathcal{H}) = \{D_1, 0, 2D_1, D_1+D_2, D_1-D_2\},$$

where we have listed the elements of $\jmath(\mathcal{H})$ so that they correspond to the above list of points of $\mathcal{H}$. Next our program applied the Mordell–Weil sieve as in Lemma 5.1. The program chose twenty-two places υ that are places of good reduction for C

with $\#J(k_\upsilon)$ divisible only by primes less than 75. In the notation of Lemma 5.1,

$$L_{22} = \langle 1386000D_1 + 16632000D_2 + 18018000D_3,\ 24948000D_2,\ 24948000D_3\rangle$$

and

$$\begin{aligned} W_{22} = \{0,\ & D_1 - D_2,\ D_1,\ D_1 + D_2,\ 2D_1,\ D_1 + 12474000D_2 + 87318000D_3,\\ & 277201D_1 + 5821200D_2 + 51004800D_3,\ 277201D_1 - 6652800D_2 - 36313200D_3,\\ & -277199D_1 + 6652800D_2 + 36313200D_3,\\ & -277199D_1 - 5821200D_2 - 51004800D_3\}. \end{aligned}$$

Next we would like to apply Theorem 3, and so we need primes p satisfying conditions (a)–(d) of that theorem. In particular, our program searches for odd primes p, unramified in K, so that every place $\upsilon \mid p$ is a place of good reduction for C, $\#J(k_\upsilon)$ is divisible only by primes less than 75, and L_{22} is contained in the kernel of the homomorphism (30). The smallest prime satisfying these conditions is $p = 109$, which splits completely in K, and so there are three degree-1 places υ_1, υ_2, and υ_3 above 109. It turns out that

$$J(k_\upsilon) \cong (\mathbb{Z}/110)^2$$

for $\upsilon = \upsilon_1, \upsilon_2, \upsilon_3$. The reader can easily see that

$$L_{22} \subset 110L_0 \subseteq 110J(K),$$

and so clearly L_{22} is in the kernel of (30) with $p = 109$. Moreover, the reader will easily see that every $\boldsymbol{w} \in W_{22}$ is equivalent modulo $110L_0$ to some element of $\jmath(\mathcal{H})$. Hence, conditions (a), (c), and (d) of Theorem 3 are satisfied for each $\boldsymbol{w} \in W_{22}$ with $p = 109$. To show that $C(K) = \mathcal{H}$, it is enough to show that $\tilde{M}_{109}(Q)$ has rank 3 for all $Q \in \mathcal{H}$.

It is convenient to take

$$\omega_1 = \frac{dx}{y} \quad \text{and} \quad \omega_2 = \frac{x\,dx}{y}$$

as basis for the 1-forms on C. With this choice, we computed the matrices $\tilde{M}_{109}(Q)$ for $Q \in \mathcal{H}$. For example, we obtained

$$\tilde{M}_{109}(\infty) = \begin{pmatrix} 79 & 64 & 0 \\ 31 & 0 & 0 \\ 104 & 0 & 82 \end{pmatrix} \pmod{109};$$

this matrix of course depends on our choice of U used to compute the HNF on page 776 though, as observed in the remarks after Theorem 2, its rank is independent of this choice of U. The matrix $\tilde{M}_{109}(\infty)$ clearly has nonzero determinant and so

rank 3. It turns out that the four other $\tilde{M}_{109}(Q)$ also have rank 3. This completes the proof that $C(K) = \mathcal{H}$.

We now return to the general case where $-2 \le s \le 2$ and would like to recover the coprime integer solutions u and v to Equation (33) from the K-rational points on C_s and hence the solutions (x, y, z) to (1) with y even and $x \equiv z^5 \pmod 4$. From (35) and (34), we see that

$$Y = \frac{3(u + v\theta)}{\alpha^5} = 3\epsilon^s\Big(\frac{u + v\theta}{u - v\theta}\Big).$$

Thus,

$$\frac{u}{v} = \theta \cdot \Big(\frac{Y + 3\epsilon^s}{Y - 3\epsilon^s}\Big).$$

Substituting in here the values of Y and s from the K-rational points on the curves C_s, the only $\mathbb{Q}$-*rational* values for u/v we obtain are -1, 2, 0, 5/4, and 1; these come from the points $(\theta^2 + \theta + 1, -\theta^2 - 2\theta - 1)$, $(-\theta^2 - \theta - 1, -11\theta^2 - 13\theta - 17)$, $(1, -3)$, $(-\theta^2 - \theta - 1, 40\theta^2 + 53\theta + 67)$, and $(-1, 3\theta + 3)$, respectively. This immediately allows us to complete the proof of Theorem 1.

The reader can find the Magma code for verifying the above computations at http://www.warwick.ac.uk/staff/S.Siksek/progs/chabnf/.

Remarks. (i) Although our approach solves Equation (1) completely, we point out that it is possible to eliminate some cases by using Galois representations and level-lowering as Dahmen [2008] does for the equation $x^2 + z^{10} = y^3$. Indeed, by mimicking Dahmen's approach and making use of the work of Darmon and Merel [1997] and the so called "method for predicting the exponents of constants" [Cohen 2007, Section 15.7], we were able to reduce to the case $s = 1$, and it is this case that corresponds to our nontrivial solution $(x, y, z) = (\pm 3, -2, \pm 1)$. It seems however that the approach via Galois representations cannot in the current state of knowledge deal with case $s = 1$.

(ii) Note that to solve our original problem (1), we did not need all K-rational points on the curves C_s, merely those $(X, Y) \in C_s(K)$ with

$$\theta \cdot \Big(\frac{Y + 3\epsilon^s}{Y - 3\epsilon^s}\Big) \in \mathbb{Q}.$$

Mourao [2013] has recently developed a higher-dimensional analogue of elliptic curve Chabauty that is applicable in such situations, and this may provide an alternative approach to (1).

Acknowledgments

I am indebted to Tim Dokchitser for useful discussions and Sander Dahmen for corrections. I am grateful to the referees for many improvements and useful comments.

References

[Bennett 2006] M. A. Bennett, "The equation $x^{2n} + y^{2n} = z^5$", *J. Théor. Nombres Bordeaux* **18**:2 (2006), 315–321. MR 2007i:11048 Zbl 1138.11009

[Bennett et al. 2010] M. A. Bennett, J. S. Ellenberg, and N. C. Ng, "The Diophantine equation $A^4 + 2^\delta B^2 = C^n$", *Int. J. Number Theory* **6**:2 (2010), 311–338. MR 2011k:11045 Zbl 1218.11035

[Bosma et al. 1997] W. Bosma, J. Cannon, and C. Playoust, "The Magma algebra system, I: The user language", *J. Symbolic Comput.* **24**:3-4 (1997), 235–265. MR 1484478 Zbl 0898.68039

[Bourbaki 1989] N. Bourbaki, *Elements of Mathematics: Lie groups and Lie algebras, Chapters 1–3*, Springer, Berlin, 1989. MR 89k:17001 Zbl 0672.22001

[Brown 2012] D. Brown, "Primitive integral solutions to $x^2 + y^3 = z^{10}$", *Int. Math. Res. Not.* **2012**:2 (2012), 423–436. MR 2012k:11036 Zbl 06013326

[Bruin 2002] N. R. Bruin, *Chabauty methods and covering techniques applied to generalized Fermat equations*, Ph.D. thesis, University of Leiden, Amsterdam, 2002. MR 2003i:11042 Zbl 1043.11029

[Bruin 2003] N. Bruin, "Chabauty methods using elliptic curves", *J. Reine Angew. Math.* **562** (2003), 27–49. MR 2004j:11051 Zbl 1135.11320

[Bruin 2005] N. Bruin, "The primitive solutions to $x^3 + y^9 = z^2$", *J. Number Theory* **111**:1 (2005), 179–189. MR 2006e:11040 Zbl 1081.11019

[Bruin and Elkies 2002] N. Bruin and N. D. Elkies, "Trinomials $ax^7 + bx + c$ and $ax^8 + bx + c$ with Galois groups of order 168 and $8 \cdot 168$", pp. 172–188 in *Algorithmic number theory* (Sydney, 2002), edited by C. Fieker and D. R. Kohel, Lecture Notes in Computer Science **2369**, Springer, Berlin, 2002. MR 2005d:11094 Zbl 1058.11044

[Bruin and Stoll 2008] N. Bruin and M. Stoll, "Deciding existence of rational points on curves: an experiment", *Experiment. Math.* **17**:2 (2008), 181–189. MR 2009d:11100 Zbl 1218.11065

[Bruin and Stoll 2009] N. Bruin and M. Stoll, "Two-cover descent on hyperelliptic curves", *Math. Comp.* **78**:268 (2009), 2347–2370. MR 2010e:11059 Zbl 1208.11078

[Bruin and Stoll 2010] 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. MR 2011j:11118 Zbl 05947723

[Bugeaud et al. 2008] Y. Bugeaud, M. Mignotte, S. Siksek, M. Stoll, and S. Tengely, "Integral points on hyperelliptic curves", *Algebra Number Theory* **2**:8 (2008), 859–885. MR 2010b:11066 Zbl 1168.11026

[Cassels and Flynn 1996] J. W. S. Cassels and E. V. Flynn, *Prolegomena to a middlebrow arithmetic of curves of genus 2*, London Math. Soc. Lecture Note Ser. **230**, Cambridge University Press, 1996. MR 97i:11071 Zbl 0857.14018

[Chabauty 1941] C. Chabauty, "Sur les points rationnels des variétés algébriques dont i'irrégularité est supérieure à la dimension", *C. R. Acad. Sci. Paris* **212** (1941), 1022–1024. MR 6,102e Zbl 0025.24903

[Chen and Siksek 2009] I. Chen and S. Siksek, "Perfect powers expressible as sums of two cubes", *J. Algebra* **322**:3 (2009), 638–656. MR 2011d:11070 Zbl 1215.11026

[Cohen 2000] H. Cohen, *Advanced topics in computational number theory*, Graduate Texts in Mathematics **193**, Springer, New York, 2000. MR 2000k:11144 Zbl 0977.11056

[Cohen 2007] H. Cohen, *Number theory, II: Analytic and modern tools*, Graduate Texts in Mathematics **240**, Springer, New York, 2007. MR 2008e:11002 Zbl 1119.11002

[Coleman 1985a] R. F. Coleman, "Effective Chabauty", *Duke Math. J.* **52**:3 (1985), 765–770. MR 87f:11043 Zbl 0588.14015

[Coleman 1985b] R. F. Coleman, "Torsion points on curves and p-adic abelian integrals", *Ann. of Math.* (2) **121**:1 (1985), 111–168. MR 86j:14014 Zbl 0578.14038

[Colmez 1998] P. Colmez, *Intégration sur les variétés p-adiques*, Astérisque **248**, 1998. MR 2000e:14026 Zbl 0930.14013

[Dahmen 2008] S. R. Dahmen, *Classical and modular methods applied to Diophantine equations*, Ph.D. thesis, Universiteit Utrecht, 2008, Available at http://igitur-archive.library.uu.nl/dissertations/2008-0820-200949/dahmen.p% df.

[Darmon 1997] H. Darmon, "Faltings plus epsilon, Wiles plus epsilon, and the generalized Fermat equation", *C. R. Math. Rep. Acad. Sci. Canada* **19**:1 (1997), 3–14. MR 98h:11034a Zbl 0932.11022

[Darmon and Granville 1995] H. Darmon and A. 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. MR 96e:11042 Zbl 0838.11023

[Darmon and Merel 1997] H. Darmon and L. Merel, "Winding quotients and some variants of Fermat's last theorem", *J. Reine Angew. Math.* **490** (1997), 81–100. MR 98h:11076 Zbl 0976.11017

[Edwards 2004] J. Edwards, "A complete solution to $X^2 + Y^3 + Z^5 = 0$", *J. Reine Angew. Math.* **571** (2004), 213–236. MR 2005e:11035 Zbl 1208.11045

[Ellenberg 2004] J. S. Ellenberg, "Galois representations attached to $\mathbb{Q}$-curves and the generalized Fermat equation $A^4 + B^2 = C^p$", *Amer. J. Math.* **126**:4 (2004), 763–787. MR 2005g:11089 Zbl 1059.11041

[Faltings 1983] G. Faltings, "Endlichkeitssätze für abelsche Varietäten über Zahlkörpern", *Invent. Math.* **73**:3 (1983), 349–366. MR 85g:11026a Zbl 0588.14026

[Flynn 1994] E. V. Flynn, "Descent via isogeny in dimension 2", *Acta Arith.* **66**:1 (1994), 23–43. MR 95g:11057 Zbl 0835.14009

[Flynn 1995a] E. V. Flynn, "An explicit theory of heights", *Trans. Amer. Math. Soc.* **347**:8 (1995), 3003–3015. MR 95j:11052 Zbl 0864.11033

[Flynn 1995b] E. V. Flynn, "On a theorem of Coleman", *Manuscripta Math.* **88**:4 (1995), 447–456. MR 97b:11082 Zbl 0865.14012

[Flynn 1997] E. V. Flynn, "A flexible method for applying Chabauty's theorem", *Compositio Math.* **105**:1 (1997), 79–94. MR 97m:11083 Zbl 0882.14009

[Flynn and Smart 1997] E. V. Flynn and N. P. Smart, "Canonical heights on the Jacobians of curves of genus 2 and the infinite descent", *Acta Arith.* **79**:4 (1997), 333–352. MR 98f:11066 Zbl 0895.11026

[Flynn and Wetherell 1999] E. V. Flynn and J. L. Wetherell, "Finding rational points on bielliptic genus 2 curves", *Manuscripta Math.* **100**:4 (1999), 519–533. MR 2001g:11098 Zbl 1029.11024

[Flynn and Wetherell 2001] E. V. Flynn and J. L. Wetherell, "Covering collections and a challenge problem of Serre", *Acta Arith.* **98**:2 (2001), 197–205. MR 2002b:11088 Zbl 1049.11066

[Grant 1994] D. Grant, "A curve for which Coleman's effective Chabauty bound is sharp", *Proc. Amer. Math. Soc.* **122**:1 (1994), 317–319. MR 94k:14019 Zbl 0834.14015

[Kraus 1999] A. Kraus, "On the equation $x^p + y^q = z^r$: a survey", *Ramanujan J.* **3**:3 (1999), 315–333. MR 2001f:11046 Zbl 0939.11016

[Lorenzini and Tucker 2002] D. Lorenzini and T. J. Tucker, "Thue equations and the method of Chabauty–Coleman", *Invent. Math.* **148**:1 (2002), 47–77. MR 2003d:11088 Zbl 1048.11023

[McCallum 1992] W. G. McCallum, "The arithmetic of Fermat curves", *Math. Ann.* **294**:3 (1992), 503–511. MR 93j:11037 Zbl 0766.14013

[McCallum 1994] W. G. McCallum, "On the method of Coleman and Chabauty", *Math. Ann.* **299**:3 (1994), 565–596. MR 95c:11079 Zbl 0824.14017

[McCallum and Poonen 2010] W. McCallum and B. Poonen, "The method of Chabauty and Coleman", preprint, 2010, Available at http://www-math.mit.edu/~poonen/papers/chabauty.pdf.

[Milne 1986] J. S. Milne, "Jacobian varieties", pp. 167–212 in *Arithmetic geometry* (Storrs, CT, 1984), edited by G. Cornell and J. H. Silverman, Springer, New York, 1986. MR 861976 Zbl 0604.14018

[Mourao 2013] M. Mourao, "Extending elliptic curve Chabauty to higher genus curves", *Manusc. Math.* (2013). arXiv 1111.5506

[Poonen and Schaefer 1997] B. Poonen and E. F. Schaefer, "Explicit descent for Jacobians of cyclic covers of the projective line", *J. Reine Angew. Math.* **488** (1997), 141–188. MR 98k:11087 Zbl 0888.11023

[Poonen et al. 2007] 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**:1 (2007), 103–158. MR 2008i:11085 Zbl 1124.11019

[Schaefer 1995] E. F. Schaefer, "2-descent on the Jacobians of hyperelliptic curves", *J. Number Theory* **51**:2 (1995), 219–232. MR 96c:11066 Zbl 0832.14016

[Schaefer and Wetherell 2005] E. F. Schaefer and J. L. Wetherell, "Computing the Selmer group of an isogeny between abelian varieties using a further isogeny to a Jacobian", *J. Number Theory* **115**:1 (2005), 158–175. MR 2006g:11116 Zbl 1095.11033

[Siksek 1995a] S. Siksek, *Descents on curves of genus* 1, Ph.D. thesis, University of Exeter, 1995, Available at http://homepages.warwick.ac.uk/~maseap/papers/phdnew.pdf.

[Siksek 1995b] S. Siksek, "Infinite descent on elliptic curves", *Rocky Mountain J. Math.* **25**:4 (1995), 1501–1538. MR 97g:11053 Zbl 0852.11028

[Siksek 2009] S. Siksek, "Chabauty for symmetric powers of curves", *Algebra Number Theory* **3**:2 (2009), 209–236. MR 2010b:11069 Zbl 05566607

[Stoll 1998] M. Stoll, "On the arithmetic of the curves $y^2 = x^l + A$ and their Jacobians", *J. Reine Angew. Math.* **501** (1998), 171–189. MR 99h:11069 Zbl 0902.11024

[Stoll 1999] M. Stoll, "On the height constant for curves of genus two", *Acta Arith.* **90**:2 (1999), 183–201. MR 2000h:11069 Zbl 0932.11043

[Stoll 2001] M. Stoll, "Implementing 2-descent for Jacobians of hyperelliptic curves", *Acta Arith.* **98**:3 (2001), 245–277. MR 2002b:11089 Zbl 0972.11058

[Stoll 2002a] M. Stoll, "On the arithmetic of the curves $y^2 = x^l + A$, II", *J. Number Theory* **93**:2 (2002), 183–206. MR 2003d:11090 Zbl 1004.11038

[Stoll 2002b] M. Stoll, "On the height constant for curves of genus two, II", *Acta Arith.* **104**:2 (2002), 165–182. MR 2003f:11093 Zbl 1139.11318

[Stoll 2006a] M. Stoll, "Independence of rational points on twists of a given curve", *Compos. Math.* **142**:5 (2006), 1201–1214. MR 2007m:14025 Zbl 1128.11033

[Stoll 2006b] M. Stoll, "On the number of rational squares at fixed distance from a fifth power", *Acta Arith.* **125**:1 (2006), 79–88. MR 2007g:11039 Zbl 1162.11326

[Taylor and Wiles 1995] R. Taylor and A. Wiles, "Ring-theoretic properties of certain Hecke algebras", *Ann. of Math.* (2) **141**:3 (1995), 553–572. MR 96d:11072 Zbl 0823.11030

[Wetherell 1997] J. L. Wetherell, *Bounding the number of rational points on certain curves of high rank*, Ph.D. thesis, University of California, Berkeley, 1997, Available at www.williamstein.org/swc/notes/files/99WetherellThesis.pdf. MR 2696280

[Wiles 1995] A. Wiles, "Modular elliptic curves and Fermat's last theorem", *Ann. of Math.* (2) **141**:3 (1995), 443–551. MR 96d:11071 Zbl 0823.11029

Communicated by Bjorn Poonen
Received 2010-07-06 Revised 2012-07-23 Accepted 2012-10-31

s.siksek@warwick.ac.uk *Department of Mathematics, University of Warwick, Coventry, CV4 7AL, United Kingdom*
http://www.warwick.ac.uk/~maseap/

Algebra & Number Theory

msp.org/ant

See inside back cover or msp.org/ant for submission instructions.

The subscription price for 2013 is US $200/year for the electronic version, and $350/year (+$40, if shipping outside the US) for print and electronic. Subscriptions, requests for back issues and changes of subscribers address should be sent to MSP.

Algebra & Number Theory (ISSN 1944-7833 electronic, 1937-0652 printed) at Mathematical Sciences Publishers, 798 Evans Hall #3840, c/o University of California, Berkeley, CA 94720-3840 is published continuously online. Periodical rate postage paid at Berkeley, CA 94704, and additional mailing offices.

ANT peer review and production are managed by EditFLOW® from Mathematical Sciences Publishers.

PUBLISHED BY

mathematical sciences publishers

nonprofit scientific publishing

http://msp.org/

Algebra & Number Theory

Volume 7 No. 4 2013