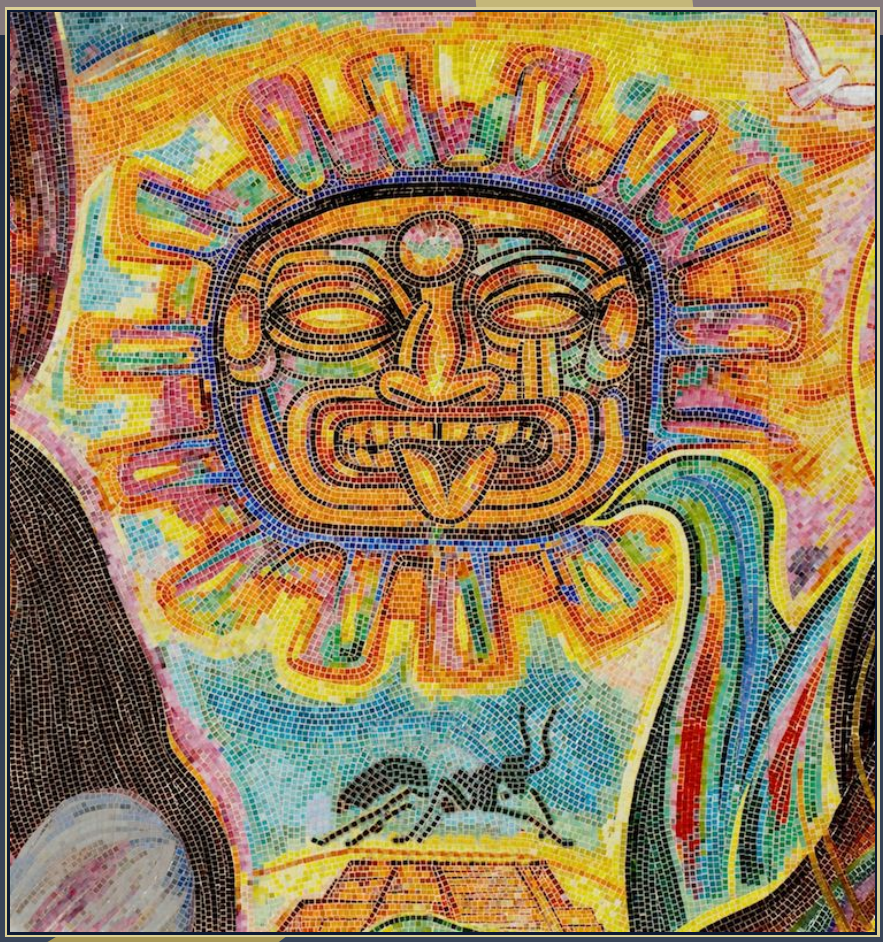
THE OPEN BOOK SERIES 1

ANTS X
Proceedings of the Tenth Algorithmic Number Theory Symposium

Explicit descent in the Picard group of a cyclic cover of the projective line

Brendan Creutz



msp

THE OPEN BOOK SERIES 1 (2013)
Tenth Algorithmic Number Theory Symposium
dx.doi.org/10.2140/obs.2013.1.295

Explicit descent in the Picard group of a cyclic cover of the projective line

Brendan Creutz

Given a curve X of the form $y^p = h(x)$ over a number field, one can use descents to obtain explicit bounds on the Mordell-Weil rank of the Jacobian or to prove that the curve has no rational points. We show how, having performed such a descent, one can easily obtain additional information which may rule out the existence of rational divisors on X of degree prime to p. This can yield sharper bounds on the Mordell-Weil rank by demonstrating the existence of nontrivial elements in the Shafarevich-Tate group. As an example we compute the Mordell-Weil rank of the Jacobian of a genus 4 curve over $\mathbb{Q}$ by determining that the 3-primary part of the Shafarevich-Tate group is isomorphic to $\mathbb{Z}/3 \times \mathbb{Z}/3$.

1. Introduction

Let k be a global field and J/k an abelian variety. Any separable isogeny $\varphi : J \to J$ gives rise to a short exact sequence of finite abelian groups,

$$0 \longrightarrow J(k)/\varphi(J(k)) \longrightarrow \mathrm{Sel}^{\varphi}(J/k) \longrightarrow Ш(J/k)[\varphi] \longrightarrow 0,$$

relating the finitely generated Mordell-Weil group $J(k)$ and the conjecturally finite Shafarevich-Tate group $Ш(J/k)$. Computation of the middle term, the *φ-Selmer group of J*, is typically referred to as a *φ-descent on J*. This produces an explicit upper bound for the Mordell-Weil rank which will only be sharp when $Ш(J/k)[\varphi]$ is trivial.

While descents on elliptic curves have a history stretching back as far as Fermat, the first examples for abelian varieties of higher dimension appear to have been computed in the 1990s by Gordon and Grant [10], though Cassels had suggested a method using his so-called $(x - T)$ map a decade earlier [6]. These first examples concerned Jacobians of genus 2 curves with rational Weierstrass points.

MSC2010: primary 11G10; secondary 11Y50.
Keywords: abelian variety, Mordell-Weil group, explicit descent.

Schaefer [16; 17] and Poonen and Schaefer [13] later developed a cohomological interpretation of Cassels' $(x-T)$ map which allowed them to generalize the method to Jacobians of all cyclic covers of the projective line. More recently Bruin and Stoll [5] and Mourao [12] have used a similar $(x-T)$ map to do a descent on the cyclic cover itself. This computes a finite set of everywhere locally solvable coverings of the curve which may be of use in determining its set of rational points. In particular, when this set is empty there are no rational points on the curve.

We show how, having performed a descent on the Jacobian J of a cyclic cover X, one can easily obtain additional information which may rule out the existence of k-rational divisors of degree 1 on X. When X is everywhere locally solvable (for instance) the scheme $\mathbf{Pic}^1(X)$, whose k-rational points parametrize k-rational divisor classes of degree 1 on X, represents an element of $Ш(J/k)$. So this can be used to show that $Ш(J/k)$ is nontrivial, and consequently to deduce sharper bounds for the Mordell-Weil rank. We show that this new information can be interpreted as a set parametrizing certain everywhere locally solvable coverings of $\mathbf{Pic}^1(X)$, so one might refer to the method as a *descent on* $\mathbf{Pic}^1(X)$. This interpretation allows us to relate the set in question to the divisibility properties of $\mathbf{Pic}^1(X)$ in $Ш(J/k)$ (see Theorem 4.5 and Corollary 4.6). Well known properties of the Cassels-Tate pairing then allow us to deduce a better lower bound for the size of $Ш(J/k)$ (unconditionally). We give several examples. In one we compute the Mordell-Weil rank of the Jacobian of a genus 4 curve over $\mathbb{Q}$ by determining that the 3-primary part of the Shafarevich-Tate group is isomorphic to $\mathbb{Z}/3\times\mathbb{Z}/3$. We also present empirical data suggesting better bounds are thus obtained rather frequently for hyperelliptic curves.

While one gets additional information on k-rational divisors of degree 1, this is unlikely to be of much additional use for determining the set of rational points on X when the genus is at least 2. When $X(k)\neq\varnothing$, the descent on $\mathbf{Pic}^1(X)$ yields no new information on the Mordell-Weil rank since $\mathbf{Pic}^1(X)\simeq J$. The obstruction to the existence of rational points on X provided by the descent on $\mathbf{Pic}^1(X)$ is weaker than that given by the descent on X, and only provides any new information when the descent on X actually gives an obstruction. That being said, descents on $\mathbf{Pic}^1(X)$ could be useful for computing large generators of the Mordell-Weil group or for finding a k-rational embedding of X into the Jacobian (see [4, Section 3.2] for some examples with genus 2 curves), both of which are relevant for tools such as the Mordell-Weil sieve or Chabauty's method. However, such benefits can only be reaped by constructing explicit models for the coverings parametrized by the descent, which is a topic which we will not address here.

1A. ***Notation.*** Throughout the paper p will be a prime number and k a field of characteristic different from p containing the p-th roots of unity. We use $\bar{k}$ to

denote a separable closure of k and $\mathfrak{g}_k$ to denote the absolute Galois group of k. When k is a global field we denote its completion at a prime v by k_v.

If G is a group, a *principal homogeneous space for* G is a set H on which G acts simply transitively. We make the convention that $\varnothing$ is a principal homogeneous space for any group. Suppose H and H' are principal homogeneous spaces for groups G and G', respectively, and that $i_0 : G \to G'$ is a homomorphism of groups. Then a map $i : H \to H'$ is said to be *affine* (with respect to i_0) if $i(g \cdot h) = i_0(g) \cdot i(h)$ for all $h \in H$ and $g \in G$. An *affine isomorphism* is an affine bijection with respect to an isomorphism of groups. When G is an abelian group and n is an integer, we use $G[n]$ and $G(n)$ to denote the n-torsion subgroup and the subgroup of elements killed by some power of n, respectively.

If L is a k-algebra we use $\bar{L}$ to denote $L \otimes_k \bar{k}$. If V is a projective variety over k and L is a commutative k-algebra we use V_L or $V \otimes_k L$ to denote the extension of scalars, $V \times_{\mathrm{Spec}(k)} \mathrm{Spec}(L)$. The group of k-rational divisors on V is denoted $\mathrm{Div}(V)$. The function field of V is denoted $\kappa(V)$. A divisor is called *principal* if it is the divisor of a function $f \in \kappa(V)$; the group of all such divisors is denoted $\mathrm{Princ}(V)$. The quotient of $\mathrm{Div}(V)$ by $\mathrm{Princ}(V)$ is denoted $\mathrm{Pic}(V)$. When V is a curve $\mathrm{Div}(V)$ is the free abelian group on the set of closed points of V, and there is a well defined notion of degree in $\mathrm{Div}(V)$. For a point $P \in V(\bar{k})$ we use $[P]$ to denote the corresponding element in $\mathrm{Div}(V_{\bar{k}})$. The degree of a principal divisor is 0, so there is also a well defined notion of degree for classes in $\mathrm{Pic}(V)$. We denote the subset consisting of classes of degree i by $\mathrm{Pic}^i(V)$.

Let A be an abelian variety defined over k. A *k-torsor under A* is a variety T over k, together with an algebraic group action of A on T defined over k such that the induced map $A \times T \ni (a, t) \mapsto (a + t, t) \in T \times T$ is an isomorphism. This means that geometrically A acts simply transitively on T. The k-isomorphism classes of k-torsors under A are parametrized by the torsion abelian group $H^1(k, A)$. The trivial class is represented by A acting on itself by translations, and a k-torsor under A is trivial if and only if it possesses a k-rational point. Thus when k is a global field with completions k_v, the Shafarevich-Tate group

$$Ш(A/k) := \ker\Big(H^1(k, A) \to \bigoplus H^1(k_v, A)\Big)$$

parametrizes isomorphism classes of everywhere locally solvable torsors.

We often refer to a variety as a k-torsor under A, taking the group action to be implicit. If T is a k-torsor under A, then any point $t_0 \in T$ gives rise to an isomorphism $T \simeq A$ defined over $k(t_0)$ sending a point $t \in T$ to the unique $a \in A$ such that $a + t_0 = t$. We say an isomorphism $\psi : T \simeq A$ is *compatible with the torsor structure on* T if it is of this type. The action of A on T can be recovered from such an isomorphism by the rule $a + t = \psi^{-1}(\psi(t) + a)$.

2. Coverings and divisibility in Ш

Definition 2.1. Let $\varphi : A' \to A$ be a separable isogeny of abelian varieties. Let T be a k-torsor under A and fix a $\bar{k}$-isomorphism $\psi_T : T \to A$ compatible with the torsor structure. A *φ-covering of T* is a k-variety S together with a morphism $S \xrightarrow{\pi} T$ defined over k such that there exists a $\bar{k}$-isomorphism $\psi_S : S \to A'$ such that $\varphi \circ \psi_S = \psi_T \circ \pi$. Two φ-coverings of T are k-isomorphic if they are k-isomorphic as T-schemes. We use $\mathrm{Cov}^{\varphi}(T/k)$ to denote the set of isomorphism classes of φ-coverings of T. If k is a global field we define the *φ-Selmer set of T* to be the subset $\mathrm{Sel}^{\varphi}(T/k) \subset \mathrm{Cov}^{\varphi}(T/k)$ consisting of those φ-coverings which are everywhere locally solvable.

We will see below that this definition generalizes the usual definition of the φ-Selmer group of an abelian variety. The definition does not depend on the choice for ψ_T, and the isomorphism ψ_S endows S with the structure of a k-torsor under A'.

Lemma 2.2. *Let (S, π) be a φ-covering of T. Then its group of $\bar{k}$-automorphisms is isomorphic to $A'[\varphi]$ as a Galois module.*

Proof. Suppose $\psi : S \to S$ is an isomorphism such that $\pi = \pi \circ \psi$ and consider the endomorphism $\tau = \psi_S \circ \psi \circ \psi_S^{-1} - 1 \in \mathrm{End}(A')$. Since $\pi = \varphi \circ \psi_S = \varphi \circ \psi_S \circ \psi$ we have that $\varphi \circ \tau$ is identically 0. Then τ is a continuous map from $A'(\bar{k})$, which is irreducible, to $A'[\varphi]$, which is discrete. Hence τ is constant. It follows that ψ is translation by a φ-torsion point. Conversely it is clear that translation by any φ-torsion point gives an automorphism of (S, π). □

By definition all φ-coverings of T are twists of one another. So by the twisting principle $\mathrm{Cov}^{\varphi}(T/k)$ is a principal homogeneous space for the group $H^1(k, A'[\varphi])$. In the special case $T = A$ (acting on itself by translations), the morphism $\varphi : A' \to A$ gives A' a canonical structure as a φ-covering of A. This gives a canonical identification of $H^1(k, A'[\varphi])$ and $\mathrm{Cov}^{\varphi}(A/k)$ and consequently endows $\mathrm{Cov}^{\varphi}(A/k)$ with a group structure in which $\varphi : A' \to A$ represents the identity. Under this identification the isomorphism classes of φ-coverings of A which possess k-rational points correspond to the kernel in the Kummer sequence

$$0 \longrightarrow A(k)/\varphi(A'(k)) \longrightarrow H^1(k, A'[\varphi]) \longrightarrow H^1(k, A')[\varphi] \longrightarrow 0. \quad (2\text{-}1)$$

When k is a global field one can deduce from this that $\mathrm{Sel}^{\varphi}(A/k)$ is identified with the kernel of the natural map $H^1(k, A'[\varphi]) \to \bigoplus_v H^1(k_v, A)$. In particular it is a subgroup and it sits in an exact sequence

$$0 \longrightarrow A(k)/\varphi(A'(k)) \longrightarrow \mathrm{Sel}^{\varphi}(A/k) \longrightarrow Ш(A'/k)[\varphi] \longrightarrow 0. \quad (2\text{-}2)$$

Remark. The reader is cautioned that our notation is nonstandard. Our $\mathrm{Sel}^{\varphi}(A/k)$ would typically be referred to as the φ-Selmer group of A' (with A' present in the notation).

More generally φ-Selmer sets are related to divisibility in the Shafarevich-Tate group as follows.

Proposition 2.3. *Suppose $\varphi : A' \to A$ is a separable isogeny of abelian varieties over k and that T is a k-torsor under A. Then $\mathrm{Cov}^{\varphi}(T/k) \neq \varnothing$ if and only if $T \in \varphi H^1(k, A')$. If k is a global field, then $\mathrm{Sel}^{\varphi}(T/k) \neq \varnothing$ if and only if $T \in \varphi Ш(A'/k)$.*

Proof. We will prove the second statement. The first can be proved using the same argument. We may assume $T \in Ш(A/k)$, otherwise the statement is trivial. Suppose T is killed by m and consider the following commutative and exact diagram:

$$\begin{array}{ccccc} \mathrm{Sel}^{m\circ\varphi}(A/k) & \longrightarrow & Ш(A'/k)[m\circ\varphi] & \longrightarrow & 0 \\ \downarrow{\scriptstyle \varphi_*} & & \downarrow{\scriptstyle \varphi} & & \\ \mathrm{Sel}^{m}(A/k) & \longrightarrow & Ш(A/k)[m] & \longrightarrow & 0. \end{array}$$

The torsor T admits a lift to an m-covering $T \xrightarrow{\pi} A$ in the m-Selmer group of A. Each choice of lift gives a map

$$\begin{aligned} \mathrm{Sel}^{\varphi}(T/k) &\longrightarrow \mathrm{Sel}^{(m\circ\varphi)}(A/k) \\ (S, \rho) &\longmapsto (S, \pi\circ\rho). \end{aligned}$$

The image of this map is exactly the fiber above (T, π) under the map denoted φ_* in the diagram above. From this one deduces the result from commutativity and the fact that the horizontal maps are surjective. □

We record here the following well known lemma which relates the condition in Proposition 2.3 to the Cassels-Tate pairing.

Lemma 2.4. *Let $\varphi : A' \to A$ be a separable isogeny of abelian varieties over a global field k with dual isogeny $\varphi^{\vee} : A^{\vee} \to A'^{\vee}$. An element of $Ш(A/k)$ is divisible by φ if and only if it pairs trivially with every element of $Ш(A^{\vee}/k)[\varphi^{\vee}]$ under the Cassels-Tate pairing.*

Proof. The compatibility of the Cassels-Tate pairing with isogenies (see [11, Remark I.6.10(a)]) shows that it induces a complex

$$\varphi Ш(A') \longrightarrow Ш(A) \longrightarrow \mathrm{Hom}\big(Ш(A^{\vee})[\varphi^{\vee}], \mathbb{Q}/\mathbb{Z}\big).$$

The statement is equivalent to claiming that this is exact. When φ is multiplication by an integer this result appears in the paragraph following the proof of [11, Lemma I.6.17]. The general statement can be deduced in exactly the same manner. □

3. Cyclic covers of $\mathbb{P}^1$

Let $\pi : X \to \mathbb{P}^1$ be a cyclic cover of degree p defined over k. By the Riemann-Hurwitz formula, X has genus $g = (d-2)(p-1)/2$, where d is the number of branch points of π. Provided $\mathbb{P}^1(k)$ has sufficiently many points we can make a change of variables to ensure that π is not ramified above $\infty \in \mathbb{P}^1$. As our present interest lies in infinite fields, there is no harm in assuming this to be the case. The pullback $\mathfrak{m} = \pi^*\infty$ is an effective k-rational divisor of degree p on X. Let $\Omega \subset X$ denote the set of ramification points of π. Then for any $\omega \in \Omega$ the divisor $p[\omega]$ is linearly equivalent to $\mathfrak{m}$, and $(2g-2)[\omega]$ is a canonical divisor.

3A. ***The isogeny ϕ.*** Since k contains the p-th roots of unity, the group of deck transformations of π may be identified with $\mu_p(\bar{k})$. The action of $\mu_p(\bar{k})$ on X extends linearly to give a Galois-equivariant action of the group ring $\mathbb{Z}[\mu_p]$ on $\mathrm{Div}(X_{\bar{k}})$. For any divisor D, the element $t = \sum_{\zeta \in \mu_p} \zeta \in \mathbb{Z}[\mu_p]$ sends D to a divisor linearly equivalent to $(\deg D)\mathfrak{m}$. Hence t sends $\mathrm{Div}^0(X_{\bar{k}})$ to $\mathrm{Princ}(X_{\bar{k}})$, so the induced actions of $\mathbb{Z}[\mu_p]$ on J and $\mathrm{Pic}^0(X)$ factor through $\mathbb{Z}[\mu_p]/t$, which is isomorphic to the cyclotomic subring of k generated by μ_p. Fix a generator $\zeta \in \mu_p$ and set $\phi = 1 - \zeta$. Then $\phi : J \to J$ is an isogeny of degree p^{d-2}. We note that the ratio of ϕ^{p-1} and p is a unit in $\mathrm{End}(J)$.

3B. ***The model $y^p = ch(x)$.*** By Kummer theory, X has a (possibly singular) affine model of the form $y^p = ch(x)$, where $c \in k^\times$ and $h(x) \in k[x]$ is a p-th-power-free polynomial with leading coefficient 1. In this model π is given by the x-coordinate and $\zeta \in \mu_p(\bar{k})$ acts via $(x, y) \mapsto (x, \zeta y)$. Our assumption that ∞ is not a branch point implies that the branch points are the roots of $h(x)$ and so we may assume p divides the degree of $h(x)$.

3C. ***The torsor $\mathscr{X}$.*** In what follows we consider the reduced scheme $\mathscr{X} = \mathbf{Pic}^1(X)$ classifying linear equivalence classes of divisors of degree 1 on X. This scheme is defined over k and its set of $\bar{k}$-points is $\mathscr{X}(\bar{k}) = \mathrm{Pic}^1(X_{\bar{k}})$. The obvious injection $\mathrm{Pic}^1(X) \to \mathrm{Pic}^1(X_{\bar{k}})^{\mathfrak{g}_k} = \mathscr{X}(k)$ is not always surjective. The obstruction to a k-rational divisor class being represented by a k-rational divisor can be interpreted as an element of the Brauer group; one has a well known exact sequence (see, for example, [2, Section 9.1])

$$0 \longrightarrow \mathrm{Pic}^1(X) \longrightarrow \mathscr{X}(k) \xrightarrow{\theta_X} \mathrm{Br}(k). \tag{3-1}$$

The obstruction θ_X vanishes identically when $\mathrm{Pic}^1(X)$ is nonempty. When k is a global field, the local-global principle for $\mathrm{Br}(k)$ can be used to show that $\mathrm{Pic}^1(X) = \mathscr{X}(k)$ if $\mathrm{Pic}^1(X_{k_v}) = \varnothing$ for at most one prime. Similarly if $\mathscr{X}(k_v) = \varnothing$ for at most one prime v, then $\mathrm{Pic}^0(X) = \mathrm{Pic}^0(X_{\bar{k}})^{\mathfrak{g}_k}$, which is equal to $J(k)$.

There is a $\bar{k}$-isomorphism $\mathscr{X} \simeq J$, sending a point $P \in \mathscr{X}$ corresponding to the divisor class of D to the class of the divisor $D - [\omega_0]$ in $\mathrm{Pic}^0(X_{\bar{k}}) = J(\bar{k})$. This endows $\mathscr{X}$ with the structure of a k-torsor under J (which does not depend on the choice for ω_0). The class of $\mathscr{X}$ in $H^1(k, J)$ is given by the class of the 1-cocycle sending $\sigma \in \mathfrak{g}_k$ to the class of $[\omega_0] - [\omega_0^\sigma]$ in $\mathrm{Pic}^0(X_{\bar{k}}) = J(\bar{k})$. As the difference of any two ramification points gives a ϕ-torsion point on J, we see that the class of $\mathscr{X}$ in $H^1(k, J)$ is killed by ϕ. In particular, this class has order p if and only if $\mathscr{X}(k) = \varnothing$. This is the case if and only if every k-rational divisor class on X has degree divisible by p.

4. The algebraic Selmer set

4A. ***The $(x - T, y)$ map.*** Let $H(x, z)$ be the binary form of degree $n = \deg(h(x))$ such that $H(x, 1) = h(x)$. Then X is birational to the curve $y^p = cH(x, z)$ in the weighted projective plane $\mathbb{P}^2(x : y : z)$ with weights $1, n/p, 1$. Writing $H(x, z)$ as $H(x, z) = H_1(x, z)^{n_1} \cdots H_e(x, z)^{n_e}$ with distinct irreducible factors $H_i(x, z)$, the radical of $H(x, z)$ is $H_{\mathrm{rad}}(x, z) = H_1(x, z) \cdots H_e(x, z)$. Let $L = \mathrm{Map}_k(\Omega, \bar{k}) \simeq k[x]/H_{\mathrm{rad}}(x, 1)$. This is the étale k-algebra associated to the finite $\mathfrak{g}_k$-set Ω. It splits as a product $L \simeq K_1 \times \cdots \times K_e$ of finite extensions of k corresponding to the irreducible factors $h_i(x)$ of $h(x)$. We have a *weighted norm map*

$$N : L \simeq K_1 \times \cdots \times K_e \to k, \quad (\alpha_1, \ldots, \alpha_e) \mapsto \prod_{i=1}^{e} N_{K_i/k}(\alpha_i)^{n_i}. \tag{4-1}$$

Let

$$\Omega' = \big\{p[\omega] : \omega \in \Omega\big\} \cup \Big\{\sum_{\omega \in \Omega} n_\omega [\omega]\Big\} \subset \mathrm{Div}(X_{\bar{k}}).$$

The first set appearing in the union above is isomorphic to Ω as a $\mathfrak{g}_k$-set. The divisor $\sum_{\omega \in \Omega} n_\omega[\omega]$ is the zero divisor of the function $y/z^{n/p} \in \kappa(X)^\times$. In particular it is invariant under the action of $\mathfrak{g}_k$. Thus Ω' is a disjoint union of $\mathfrak{g}_k$-sets, and the étale k-algebra corresponding to Ω' splits as $\mathrm{Map}_k(\Omega', \bar{k}) = M \simeq L \times k$. Since the action of $\mathfrak{g}_k$ on Ω' is induced from the action on Ω, we have an induced norm map

$$\partial : L = \mathrm{Map}_k(\Omega, \bar{k}) \to \mathrm{Map}_k(\Omega', \bar{k}) = M, \quad \alpha \mapsto \big(\omega' = \textstyle\sum c_\omega[\omega] \mapsto \prod \alpha(\omega)^{c_\omega}\big).$$

Concretely, this is the map

$$\alpha \mapsto (\alpha^p, N(\alpha)) \in L \times k, \tag{4-2}$$

where N is the weighted norm map defined in (4-1). We can embed k in M via the map $\iota : k \to M \simeq L \times k$ sending a to $(a, a^{n/p})$. The choice is such that $\partial(a) = \iota(a^p)$.

Let $f \in \mathrm{Map}_k(\Omega', \kappa(X_{\bar{k}})^\times)$ be the map

$$\omega' \longmapsto \begin{cases} (x - x(\omega)z)/z & \text{if } \omega' = p[\omega], \\ y/z^{n/p} & \text{if } \omega' = \sum_{\omega \in \Omega} n_\omega [\omega]. \end{cases}$$

Then f is a Galois-equivariant family of functions f_ω parametrized by Ω', whose divisors are supported on the union of Ω and the support of $\mathfrak{m}$. Moreover, if $[\boldsymbol{w}] \in \mathrm{Map}_k(\Omega, \mathrm{Div}(X_{\bar{k}}))$ denotes the map $(\omega \mapsto [\omega])$ and we interpret $\iota(\mathfrak{m})$ as the element

$$\omega' \longmapsto \begin{cases} \mathfrak{m} & \text{if } \omega' = p[\omega], \\ (n/p)\mathfrak{m} & \text{if } \omega' = \sum_{\omega \in \Omega} n_\omega [\omega] \end{cases}$$

of $\mathrm{Map}_k(\Omega', \mathrm{Div}(X_{\bar{k}}))$, then the family of divisors corresponding to f is

$$\mathrm{div}(f) = \partial[\boldsymbol{w}] - \iota(\mathfrak{m}) \in \mathrm{Map}_k\big(\Omega', \mathrm{Div}(X_{\bar{k}})\big).$$

Following the terminology in [13] we will say a divisor is *good* if its support is disjoint from Ω and $\mathfrak{m}$. For any good divisor, $D = \sum_P n_P [P] \in \mathrm{Div}(X_{\bar{k}})$, we may define

$$f(D) = \prod_P f(P)^{n_P} \in \overline{M}^\times.$$

Note that if $D \in \mathrm{Div}(X)$, then $f(D) \in M^\times$. Every k-rational divisor is linearly equivalent to a good k-rational divisor. Using this and applying Weil reciprocity one can prove the following proposition. For details we refer the reader to [7, Proposition 3.1], [13, Section 5] or [21, Section 4].

Proposition 4.1. *The function f induces a unique homomorphism*

$$f : \mathrm{Pic}(X) \to M^\times / \iota(k^\times)\partial(L^\times)$$

with the property that the image of the class of any good divisor $D \in \mathrm{Div}(X)$ is given by $f(D)$ as defined above.

Remark. The $(x - T, y)$ map of Stoll and van Luijk defined in [21] differs from ours slightly. The second factor of their map is defined using the function $\gamma y / z^{n/p}$ where γ is some p-th root of c. Hence their map and ours agree in degree 0 only. The projection $\mathrm{pr}_1 : M \simeq L \times k \to L$ induces a map $M^\times / \iota(k^\times)\partial(L^\times) \to L^\times / k^\times L^{\times p}$. Composing this with either f or the $(x - T, y)$ map defined in [21] one recovers the $(x - T)$ map defined in [13]. The main advantage of our definition over the others is that it defines a homomorphism on all of $\mathrm{Pic}(X)$ and not just the degree divisible by p part. The map used in [5; 12] to do a descent on X is the restriction of $\mathrm{pr}_1 \circ f$ to $X(k) \subset \mathrm{Pic}^1(X)$.

Recall that $c \in k^\times$ is the leading coefficient of the polynomial defining X. For $r \in \mathbb{Z}$ define

$$\boldsymbol{H}_k^r = \frac{\{(\alpha, s) \in L^\times \times k^\times : c^r \cdot N(\alpha) = s^p\}}{\{(\gamma\alpha^p, \gamma^{n/p} N(\alpha)) \in L^\times \times k^\times : \alpha \in L^\times, \gamma \in k^\times\}} \subset M^\times/\iota(k^\times)\partial(L^\times).$$

Lemma 4.2. *For $r \in \mathbb{Z}$,*

$$\boldsymbol{H}_k^r = \big(f(D)\partial(\bar{L}^\times)\big)^{\mathfrak{g}_k}\big/\iota(k^\times)\partial(L^\times),$$

where $D \in \mathrm{Pic}^r(X_{\bar{k}})$ is any divisor class of degree r. In particular,

$$\boldsymbol{H}_k^0 = \big(\partial(\bar{L}^\times)\big)^{\mathfrak{g}_k}\big/\iota(k^\times)\partial(L^\times).$$

Proof. First we claim that

$$\partial(\bar{L}^\times) = \big\{(\alpha, s) \in \bar{L}^\times \times \bar{k}^\times : N(\alpha) = s^p\big\}.$$

By definition $\partial(\bar{L}^\times) = \{(\alpha^p, N(\alpha)) : \alpha \in \bar{L}^\times\}$, so clearly

$$\partial(\bar{L}^\times) \subset \big\{(\alpha, s) \in \bar{L}^\times \times \bar{k}^\times : N(\alpha) = s^p\big\}.$$

For the other inclusion, suppose $(a, s) \in \bar{L}^\times \times \bar{k}^\times$ is such that $N(\alpha) = s^p$. Then for any p-th root $\beta \in \bar{L}^\times$ of α we have $N(\beta)^p = s^p$. Hence $N(\beta) = \nu s$ for some $\nu \in \mu_p(\bar{k})$. Since $h(x)$ is p-th-power-free, the weighted norm map $N : \mu_p(\bar{L}) \to \mu_p(\bar{k})$ is surjective. Hence there must exist $\nu' \in \mu_p(\bar{L})$ such that $\nu'\beta \in \bar{L}^\times$ satisfies $\partial\beta = ((\nu'\beta)^p, N(\nu'\beta)) = (\alpha, s)$. This establishes the claim.

For $i = 1, 2$, let pr_i denote the projection of $M \simeq L \times k$ onto the i-th factor. For every point $P = (x_0, y_0) \in X$ we have

$$cN(\mathrm{pr}_1 \circ f(P)) = c \prod_{\omega \in \Omega} (x_0 - x(\omega))^{n_\omega} = ch(x_0) = y_0^p = \mathrm{pr}_2(f(P))^p,$$

where n_ω denotes the multiplicity of ω as a root of $h(x)$. So for any good divisor D of degree r we have $c^r N(\mathrm{pr}_1 \circ f(D)) = \mathrm{pr}_2(f(D))^p$, and, in light of the claim above, we have

$$f(D)\partial(\bar{L}^\times) = \big\{(\alpha, s) \in \bar{L}^\times \times \bar{k}^\times : c^r \cdot N(\alpha) = s^p\big\}.$$

In particular, the coset $f(D)\partial(\bar{L}^\times)$ depends only on the degree of D. The same is then true of its Galois-invariant subset. The lemma now follows easily. □

Corollary 4.3. *If $\boldsymbol{H}_k^1 = \varnothing$, then $\mathrm{Pic}^1(X) = \varnothing$.*

Proof. The image of $f : \mathrm{Pic}^r(X) \to M^\times/\iota(k^\times)\partial(L^\times)$ is contained in $\boldsymbol{H}_k^r$. □

4B. ***The algebraic Selmer set.*** Over a global field one can combine the information from the various local versions of the map f to obtain a finite subset of $\boldsymbol{H}^r_k$ which contains the image of $\mathrm{Pic}^r(X)$.

Definition 4.4. For a global field k with completions k_v, define *algebraic ϕ-Selmer sets*:

$$\mathrm{Sel}^{\phi}_{\mathrm{alg}}(J/k) = \left\{\delta \in \boldsymbol{H}^0_k : \text{ for all primes } v,\ \mathrm{res}_v(\delta) \in f(\mathrm{Pic}^0(X_{k_v}))\right\},$$
$$\mathrm{Sel}^{\phi}_{\mathrm{alg}}(X/k) = \left\{\delta \in \boldsymbol{H}^1_k : \text{ for all primes } v,\ \mathrm{res}_v(\delta) \in f(X(k_v))\right\},$$
$$\mathrm{Sel}^{\phi}_{\mathrm{alg}}(\mathscr{X}/k) = \left\{\delta \in \boldsymbol{H}^1_k : \text{ for all primes } v,\ \mathrm{res}_v(\delta) \in f(\mathrm{Pic}^1(X_{k_v}))\right\}.$$

Recall that the projection $\mathrm{pr}_1 : M \simeq L \times k \to L$ induces a map

$$\mathrm{pr}_1 : M^\times/\iota(k^\times)\partial(L^\times) \to L^\times/k^\times L^{\times p}.$$

The *fake ϕ-Selmer group* considered in [13] is equal to $\mathrm{pr}_1(\mathrm{Sel}^{\phi}_{\mathrm{alg}}(J/k))$. The *unfaked ϕ-Selmer group* considered in [21] is equal to $\mathrm{Sel}^{\phi}_{\mathrm{alg}}(J/k)$. From [21, Theorem 5.1] we see that if X has divisors of degree 1 everywhere locally, then we can identify $\mathrm{Sel}^{\phi}_{\mathrm{alg}}(J/k)$ with the ϕ-Selmer group of J. In particular, $\mathrm{Sel}^{\phi}_{\mathrm{alg}}(J/k)$ is finite. If the set $\mathrm{Sel}^{\phi}_{\mathrm{alg}}(\mathscr{X}/k)$ is nonempty, it is a coset of $\mathrm{Sel}^{\phi}_{\mathrm{alg}}(J/k)$ inside $M^\times/\iota(k^\times)\partial(L^\times)$. This implies that $\mathrm{Sel}^{\phi}_{\mathrm{alg}}(\mathscr{X}/k)$ is also finite. If, in addition, $\delta \in \mathrm{Sel}^{\phi}_{\mathrm{alg}}(X/k) \neq \varnothing$, then $\mathrm{Sel}^{\phi}_{\mathrm{alg}}(\mathscr{X}/k) = \delta \cdot \mathrm{Sel}^{\phi}_{\mathrm{alg}}(J/k)$, and, in particular, $\mathrm{Sel}^{\phi}_{\mathrm{alg}}(X/k) \subset \mathrm{Sel}^{\phi}_{\mathrm{alg}}(\mathscr{X}/k)$. The set $\mathrm{pr}_1\left(\mathrm{Sel}^{\phi}_{\mathrm{alg}}(X/k)\right)$ is equal to the *fake ϕ-Selmer set* considered in [5; 12] where it is shown to be a quotient of the ϕ-Selmer set of X (see Definition 5.1). As we shall see in Corollary 5.5, $\mathrm{Sel}^{\phi}_{\mathrm{alg}}(X/k)$ is in one-to-one correspondence with ϕ-Selmer set of X.

One motivation for considering this set is that it can explain the failure of the Hasse principle for X. Similarly, one can easily deduce the implication

$$\left(\mathrm{Sel}^{\phi}_{\mathrm{alg}}(\mathscr{X}/k) = \varnothing\right) \implies \left(\mathrm{Pic}^1(X) = \varnothing\right).$$

When X has points everywhere locally we can say even more.

Theorem 4.5. *Suppose k is a global field and X is everywhere locally solvable. Then $\mathrm{Sel}^{\phi}_{\mathrm{alg}}(\mathscr{X}/k)$ is nonempty if and only if the torsor $\mathscr{X}$ is divisible by ϕ in $Ш(J/k)$.*

In light of Proposition 2.3, to prove the theorem it will suffice to show that when X is everywhere locally solvable $\mathrm{Sel}^{\phi}(\mathscr{X}/k)$ and $\mathrm{Sel}^{\phi}_{\mathrm{alg}}(\mathscr{X}/k)$ are in one-to-one correspondence. This will be accomplished with Proposition 6.2 below.

Corollary 4.6. *Suppose k is a global field and X is everywhere locally solvable. If $\mathrm{Sel}^{\phi}_{\mathrm{alg}}(\mathscr{X}/k)$ is empty, then $\dim_{\mathbb{F}_p} Ш(J/k)[\phi] \geq 2$. If in addition $\dim_{\mathbb{F}_p} Ш(J/k)[\phi] \leq 2$, then $Ш(J/k)(p) \simeq \mathbb{Z}/p \times \mathbb{Z}/p$.*

Proof. Under the assumptions the theorem implies that $\mathscr{X}$ represents a nontrivial class in the finite abelian group $G = Ш(J/k)[\phi]/\phi Ш(J/k)[\phi^2]$. Under the canonical identification of J with its dual, ϕ is self dual (up to a unit). It then follows from Lemma 2.4 and [14, Corollary 12] that the Cassels-Tate pairing induces a nondegenerate alternating pairing on G. Hence the order of G is a positive even power of p. This establishes the first statement. For the second, note that the assumptions imply that $\phi Ш(J/k)[\phi^2] = 0$, and use that $\phi^{p-1} = p$ up to a unit. □

Remark. To show G has square order it is enough to assume that p is odd or that X has a k_v-rational divisor of degree 1 for each prime v. We use the assumption that X is everywhere locally solvable to ensure that $\mathscr{X}$ represents a nontrivial element of G. Indeed this assumption is used in our proof of Theorem 4.5 when we apply Lemma 6.1 in the proof of Proposition 6.2. While it may be possible to relax this hypothesis, some assumption on the existence of k_v-rational divisors of degree 1 is required. For the curve $X : y^2 = 3x^6 + 3$, one can show that $\mathrm{Pic}^1(X_{\mathbb{Q}_2}) = \varnothing$, while $\mathscr{X}(\mathbb{Q}) \neq \varnothing$. So the algebraic Selmer set is empty, but $\mathscr{X} \in 2Ш(J/\mathbb{Q})$.

Remark. It is not generally true that $Ш(J/k)[\phi]$ has square order. Well known examples with $p = 2$ are given in [13] and are necessarily explained by the fact that X fails to have a k_v-rational divisor of degree 1 at an odd number of primes. An example with $p = 3$ where X has a rational point is given in [8].

4C. ***Computing the algebraic Selmer set.*** Before carrying on with the proof of Theorem 4.5 we briefly discuss how $\mathrm{Sel}^{\phi}_{\mathrm{alg}}(\mathscr{X}/k)$ can be computed in practice. For an extension K/k set $\mathfrak{L}(K) = (L \otimes_k K)^\times / K^\times (L \otimes_k K)^{\times p}$, and use res_K to denote the canonical map $\mathfrak{L}(k) \to \mathfrak{L}(K)$. The weighted norm $N : L \to k$ induces a map $N : \mathfrak{L}(k) \to k^\times/k^{\times p}$. If k is a local field, an element of $\mathfrak{L}(k)$ is said to be *unramified* if its image under res_{k^u} is trivial, where k^u denotes the maximal unramified extension of k. If k is a global field, an element $\delta \in \mathfrak{L}(k)$ is said to be *unramified at a prime* v of k if $\mathrm{res}_{k_v}(\delta)$ is unramified.

Now suppose k is a global field and let S denote the set of primes of k consisting of all primes of bad reduction, all nonarchimedean primes dividing cp and all archimedean primes.[1] Let $\mathfrak{L}(k)_S$ denote the subgroup of $\mathfrak{L}(k)$ consisting of elements which are unramified at all primes outside of S. This is a finite group which can be computed from the S-unit group and class group of each of the constituent fields of L (see Propositions 12.5 and 12.6, Corollary 12.7, and Proposition 12.8 of [13]). For an element $a \in k^\times$, let $\mathfrak{L}(k)_{S,a}$ denote the subset of $\mathfrak{L}(k)_S$ consisting of elements α such that $aN(\alpha) \in k^{\times p}$.

[1] Actually, one can get away with using a smaller set of primes. Compare with [20, Corollary 4.7 and Proposition 5.12], [5, Lemma 4.3], and [12, Lemma 2.6].

Computable descriptions of $\mathrm{pr}_1(\mathrm{Sel}^{\phi}_{\mathrm{alg}}(J/k))$ and $\mathrm{pr}_1(\mathrm{Sel}^{\phi}_{\mathrm{alg}}(X/k))$ are given in [13, Theorem 13.2], [5, Section 6] and [12, Corollary 3.12]. They are the subsets of $\mathfrak{L}(k)_{S,1}$ and $\mathfrak{L}(k)_{S,c}$ cut out by certain local conditions. The former is the subgroup of elements which restrict into $\mathrm{pr}_1 \circ f(\mathrm{Pic}^0(X_{k_v}))$ for all $v \in S$ while the latter is the subset which restricts into $\mathrm{pr}_1 \circ f(X(k_v))$ for all primes with norm up to some explicit bound. For explicit descriptions of how to compute these local images, see [5; 12; 20].

Proposition 4.7. *Suppose that $D_v \in X(k_v)$ for each $v \in S$. Then*

$$\mathrm{pr}_1\big(\mathrm{Sel}^{\phi}_{\mathrm{alg}}(\mathscr{X}/k)\big) = \big\{\delta \in \mathfrak{L}(k)_{S,c} : \mathrm{res}_{k_v}(\delta) \in \mathrm{pr}_1(f(D_v)) \cdot \mathrm{pr}_1\big(f(\mathrm{Pic}^0(X_{k_v}))\big) \text{ for all } v \in S\big\}.$$

Proof. This follows from the descriptions of $\mathrm{pr}_1(\mathrm{Sel}^{\phi}_{\mathrm{alg}}(J/k))$ and $\mathrm{pr}_1(\mathrm{Sel}^{\phi}_{\mathrm{alg}}(X/k))$ above and the fact that $\mathrm{pr}_1 \circ f$ is a homomorphism. □

Remark. This shows that while doing a ϕ-descent on J — that is, computing $\mathrm{pr}_1(\mathrm{Sel}^{\phi}_{\mathrm{alg}}(J/k))$ — one can determine whether $\mathrm{Sel}^{\phi}_{\mathrm{alg}}(\mathscr{X}/k)$ is empty or not with virtually no extra effort.

5. ϕ-coverings of X

Our proof of Theorem 4.5 will involve relating $\mathrm{Sel}^{\phi}_{\mathrm{alg}}(\mathscr{X}/k)$ and $\mathrm{Sel}^{\phi}(\mathscr{X}/k)$. To do this we first relate $\mathrm{Sel}^{\phi}_{\mathrm{alg}}(X/k)$ to a certain set of coverings of X which we now define.

Definition 5.1. A *ϕ-covering of X* is a covering $Y \to X$ which arises as the pullback of some ϕ-covering $\mathcal{Y} \to \mathscr{X}$ along the canonical map $X \to \mathscr{X}$ sending a point P to the class of the divisor $[P]$. We use $\mathrm{Cov}^{\phi}(X/k)$ to denote the set of k-isomorphism classes of ϕ-coverings of X. If k is a global field, the *ϕ-Selmer set of X* is defined to be the subset $\mathrm{Sel}^{\phi}(X/k) \subset \mathrm{Cov}^{\phi}(X/k)$ consisting of those coverings that are everywhere locally solvable.

It follows that any ϕ-covering of X is an X-torsor under $J[\phi]$ and that all ϕ-coverings of X are twists of one another. Hence $\mathrm{Cov}^{\phi}(X/k)$ is also a principal homogeneous space for $H^1(k, J[\phi])$. The action of twisting is compatible with base change, so the obvious map $\mathrm{Cov}^{\phi}(\mathscr{X}/k) \to \mathrm{Cov}^{\phi}(X/k)$ is an affine isomorphism.

Our next goal is to relate $\boldsymbol{H}^1_k$ with a certain subset of $\mathrm{Cov}^{\phi}(X/k)$ and use this to show that $\mathrm{Sel}^{\phi}_{\mathrm{alg}}(X/k)$ and $\mathrm{Sel}^{\phi}(X/k)$ are in one-to-one correspondence. While we work with $\mathrm{Sel}^{\phi}_{\mathrm{alg}}(X/k)$ rather than its image under pr_1, this result was essentially established in [5; 12]. The only new ingredient here is to clarify the affine structure of these sets. This interpretation is, however, crucial to our proof of Theorem 4.5.

We have an exact sequence

$$1 \longrightarrow \mu_p \longrightarrow J_{\mathfrak{m}}[\phi] \xrightarrow{q} J[\phi] \longrightarrow 0, \tag{5-1}$$

where $J_{\mathfrak{m}}$ is the generalized Jacobian associated to the modulus $\mathfrak{m} \in \mathrm{Div}(X)$ (see [13, Section 2] or [19, Chapter 5]). Applying Galois cohomology gives an exact sequence

$$H^1(k, \mu_p) \longrightarrow H^1(k, J_{\mathfrak{m}}[\phi]) \longrightarrow H^1(k, J[\phi]) \xrightarrow{\Upsilon} H^2(k, \mu_p). \tag{5-2}$$

The description of $J_{\mathfrak{m}}[\phi]$ in [13, Section 6] identifies $J_{\mathfrak{m}}[\phi]$ with the kernel of $\partial : \bar{L}^\times \to \overline{M}^\times$. This allows us to interpret the cocycle in the following proposition as taking values in $J[\phi]$.

Proposition 5.2. *There is an isomorphism $\boldsymbol{H}_k^0 \simeq \ker \Upsilon$ which sends the class of $\partial(\alpha) \in \partial(\bar{L}^\times)^{\mathfrak{g}_k}$ to the class of the 1-cocycle $\sigma \mapsto q(\sigma(\alpha)/\alpha)$ in $H^1(k, J[\phi])$.*

Proof. This can be found in [21] (see Proposition 3.1 and Remark 4.3). □

Definition 5.3. Define

$$\mathrm{Cov}_0^\phi(X/k) = \left\{ (Y, \pi) \in \mathrm{Cov}^\phi(X/k) : \begin{array}{l} \pi^*[\omega_0] \text{ is linearly equivalent} \\ \text{to a } k\text{-rational divisor} \end{array} \right\}.$$

The pullbacks of the ramification points are all linearly equivalent, so $\pi^*[\omega_0]$ represents a k-rational divisor class. If k is a global field and Y is everywhere locally solvable, then every k-rational divisor class contains a k-rational divisor. Thus we see that $\mathrm{Sel}^\phi(X/k) \subset \mathrm{Cov}_0^\phi(X/k)$.

Proposition 5.4. *The action of $H^1(k, J[\phi])$ on $\mathrm{Cov}^\phi(X/k)$ restricts to a simply transitive action of $\ker(\Upsilon) \simeq \boldsymbol{H}_k^0$ on $\mathrm{Cov}_0^\phi(X/k)$. The function f induces an affine isomorphism*

$$\mathfrak{f} : \mathrm{Cov}_0^\phi(X/k) \to \boldsymbol{H}_k^1$$

with the property that for any $(Y, \pi) \in \mathrm{Cov}_0^\phi(X/k)$ and any extension K/k, we have

$$f(\pi(Q)) = \mathfrak{f}((Y, \pi)) \text{ in } \boldsymbol{H}_K^1$$

for every point $Q \in Y(K)$.

Corollary 5.5. *Suppose k is a global field. Then $\mathfrak{f}$ restricts to give a bijection $\mathfrak{f} : \mathrm{Sel}^\phi(X/k) \to \mathrm{Sel}^\phi_{\mathrm{alg}}(X/k)$.*

Proof of Proposition 5.4. Let $(Y, \pi) \in \mathrm{Cov}_0^\phi(X/k)$. The complete linear system associated to $\pi^*[\omega_0]$ gives an embedding in $\mathbb{P}^N$ (for some N) with the property that for $\omega \in \Omega$, the divisor $\pi^*[\omega]$ is a hyperplane section defined by the vanishing of some linear form l_ω. Recall that $[\boldsymbol{w}]$ is the map $(\omega \mapsto [\omega]) \in \mathrm{Map}_K(\Omega, \mathrm{Div}(X_{\bar{k}}))$.

These linear forms l_ω may be chosen so as to give a linear form l with coefficients in L defining the $\mathfrak{g}_k$-equivariant family of divisors

$$\big(\pi^*[\boldsymbol{w}] : \omega \mapsto \pi^*[\omega]\big) \in \mathrm{Map}_K(\Omega, \mathrm{Div}(Y_{\bar{k}})).$$

Since the divisor of f is $\partial[\boldsymbol{w}] - \iota(\mathfrak{m}) \in \mathrm{Map}_k(\Omega', \mathrm{Div}(X_{\bar{k}}))$, we see that there is some $\Delta \in M^\times$ such that

$$\pi^* f = \Delta \frac{\partial(l)}{\iota(z \circ \pi)} \in \mathrm{Map}_k(\Omega', \kappa(Y_{\bar{k}})^\times).$$

Define $\mathfrak{f}((Y, \pi)) = \Delta$. A different choice of model for Y or a different choice for the linear form l would serve to modify Δ by an element of $\iota(k^\times)\partial(L^\times)$. So the class of Δ in $\boldsymbol{H}^1_k$ is well defined. For any point $Q \in Y(K)$ not lying above a Weierstrass point or some point at above ∞ on X, the defining property stated in the proposition is immediate. For the finitely many remaining points the result follows by application of the moving lemma.

Given $(\delta, s) \in L^\times \times k^\times$ representing an element of $\boldsymbol{H}^1_k$ one can construct a ϕ-covering of X as follows. Let $\mathbb{P}_\Omega$ be the projective space with coordinates parametrized by Ω. Define a curve $Y_{\delta,s} \subset \mathbb{P}_\Omega \times X$ by declaring that

$$\big((u_\omega)_{\omega\in\Omega}, (x : y : z)\big) \in Y_{\delta,s}$$

if and only if there exists some $a \in k^\times$ such that

$$\delta(\omega) u_\omega^p = a(x - x(\omega)z) \text{ for all } \omega \in \Omega, \quad \text{and} \quad s \prod_\omega u_\omega^{n_\omega} = a^d y. \tag{5-3}$$

Recall that $\delta \in L$ can be interpreted as a map $\delta : \Omega \to \bar{k}$ and that n_ω denotes the weight associated to ω in the weighted norm map $N : L \to k$. Projection onto the second factor gives $Y_{\delta,s}$ the structure of an X-torsor under $J[\phi]$. It is easy to see that the isomorphism class of $Y_\delta \to X$ depends only on the class of (δ, s) in $\boldsymbol{H}^1_k$. Suppose $(Y, \pi) \in \mathrm{Cov}^\phi_0(X/k)$ and $\mathfrak{f}(Y, \pi) = (\epsilon, t)$. Then (with notation as above) we can find a projective embedding $Y \to \mathbb{P}^N$ and linear forms l_ω which cut out the divisors $\pi^*[\omega]$. The rational map $\mathbb{P}^N \to \mathbb{P}_\Omega$ given by $(l_\omega)_{\omega\in\Omega}$ gives an isomorphism (of X-schemes) $Y \to Y_{\epsilon,t}$. This shows that the $Y_{\delta,s}$ are ϕ-coverings. It is evident from the construction that the pullback of any ramification point $\omega \in X$ is the hyperplane section of $Y_{\delta,s}$ cut out by $u_\omega = 0$. So this covering represents an element of $\mathrm{Cov}^\phi_0(X/k)$. Moreover, it is clear that the image of $(Y_\delta, \pi_{\delta,s})$ under $\mathfrak{f}$ is represented by (δ, s). This shows that $\mathfrak{f}$ is surjective.

Now we show that the map is affine with respect to the action of

$$\boldsymbol{H}^0_k \simeq (\partial(\bar{L}^\times))^{\mathfrak{g}_k} / \iota(k^\times)\partial(L^\times).$$

For this suppose $\alpha \in \bar{L}^\times$ with $\partial\alpha = (\alpha^p, N(\alpha)) \in (\partial(\bar{L}^\times))^{\mathfrak{g}_k}$. Multiplication by α induces a $\bar{k}$-automorphism of $\mathbb{P}_\Omega$. It is evident from (5-3) that this induces an isomorphism of X-schemes $\alpha : (Y_{\alpha^p\delta, N(\alpha)s}, \pi_{\alpha^p\delta, N(\alpha)s}) \longrightarrow (Y_{\delta,s}, \pi_{\delta,s})$. The cocycle $\xi \in H^1(k, J[\phi])$ corresponding to this twist sends $\sigma \in \mathfrak{g}_k$ to

$$\alpha^\sigma \circ \alpha^{-1} \in \mathrm{Aut}((Y_\delta, \pi_{\delta,s})) \simeq J[\phi].$$

Under the isomorphism $(\partial(\bar{L}^\times))^{\mathfrak{g}_k}/k^\times\partial(L^\times) \simeq \ker(\Upsilon) \subset H^1(k, J_{\mathfrak{m}}[\phi])$ from Proposition 5.2, the class of $\partial\alpha$ corresponds to the class of the cocycle η that sends $\sigma \in \mathfrak{g}_k$ to $q(\alpha^\sigma/\alpha) \in J[\phi]$, where $q : J_{\mathfrak{m}}[\phi] \to J[\phi]$ is the quotient map in the exact sequence (5-1). It is then clear that ξ and η give the same class in $H^1(k, J[\phi])$. This proves that $\mathfrak{f}$ is affine. □

6. A descent map for coverings of $\mathscr{X}$

We consider the subset $\mathrm{Cov}^\phi_{\mathrm{good}}(\mathscr{X}/k) \subset \mathrm{Cov}^\phi(\mathscr{X}/k)$ consisting of ϕ-coverings of $\mathscr{X}$ such that the corresponding ϕ-covering of X lies in $\mathrm{Cov}^\phi_0(X/k)$, and we define a map

$$\mathfrak{F} : \mathrm{Cov}^\phi_{\mathrm{good}}(\mathscr{X}/k) \to \mathrm{Cov}^\phi_0(X/k) \xrightarrow{\mathfrak{f}} \boldsymbol{H}^1_k.$$

Proposition 5.4 implies that $\mathfrak{F}$ is an affine isomorphism.

Lemma 6.1. *Suppose $X(k) \neq \varnothing$.*

(1) *If $(\mathscr{Y}, \pi) \in \mathrm{Cov}^\phi(\mathscr{X}/k)$ and $\mathscr{Y}(k) \neq \varnothing$, then $(\mathscr{Y}, \pi) \in \mathrm{Cov}^\phi_{\mathrm{good}}(\mathscr{X}/k)$.*

(2) *If $(\mathscr{Y}, \pi) \in \mathrm{Cov}^\phi_{\mathrm{good}}(\mathscr{X}/k)$ and $Q \in \mathscr{Y}(K)$ for some extension K/k, then*

$$f(\pi(Q)) = \mathfrak{F}((\mathscr{Y}, \pi)) \text{ in } \boldsymbol{H}^1_K.$$

Proof. By assumption there is some point $R \in X(k) \neq \varnothing$. Then there exists $(Y, \pi) \in \mathrm{Cov}^\phi_0(X/k)$ and $R' \in Y(k)$ such that $\pi(R') = R$. Let $(\mathscr{Y}, \widetilde{\pi}) \in \mathrm{Cov}^\phi_{\mathrm{good}}(\mathscr{X}/k)$ be the corresponding covering and $i_Y : Y \to \mathscr{Y}$ the base change of $i_X : X \to \mathscr{X}$. Clearly $i_Y(R') \in \mathscr{Y}(k) \neq \varnothing$.

The set B of isomorphism classes of ϕ-coverings of $\mathscr{X}$ which contain a k-rational point is a principal homogeneous space for the image of $J(k)$ under the connecting homomorphism in the Kummer sequence (2-2). This image is contained in $\ker(\Upsilon)$, so $B \subset (\mathscr{Y}, \pi) \cdot \ker(\Upsilon) = \mathrm{Cov}^\phi_{\mathrm{good}}(\mathscr{X}/k)$. This proves statement (1).

For statement (2), consider the map $d : \mathrm{Pic}^1(X) \to \mathrm{Cov}^\phi(\mathscr{X}/k)$ sending a point $P \in \mathrm{Pic}^1(X) = \mathscr{X}(k)$ to the unique covering to which P lifts. This map is affine, since $f : \mathrm{Pic}^0(X) \to \boldsymbol{H}^0_k \simeq \ker(\Upsilon) \subset H^1(k, J[\phi])$ can be identified with the connecting homomorphism in the Kummer sequence [21, Theorem 1.1]. Moreover its image lands in $\mathrm{Cov}^\phi_{\mathrm{good}}(\mathscr{X}/k)$ by statement (1).

It suffices to prove the statement for $K = k$, which amounts to showing that $f(D) = \mathfrak{F}(d(D))$ for every $D \in \mathrm{Pic}^1(X)$. The point $i_Y(R') \in \mathcal{Y}(k)$ is a lift of $[R] \in \mathcal{X}(k)$, so $\mathcal{Y} = d([R])$. From the definition of $\mathfrak{F}$ and the defining property of $\mathfrak{f}$ we have

$$\mathfrak{F}((\mathcal{Y}, \widetilde{\pi})) = \mathfrak{f}((Y, \pi)) = f([\pi(R')]) = f([R]) \in \boldsymbol{H}^1_k.$$

Hence $f([R]) = \mathfrak{F}(d([R]))$.

Now suppose $D \in \mathrm{Pic}^1(X)$. Since d is affine, $d(D)$ is the twist of $d([R])$ by the cocycle $f(D - [R]) \in \boldsymbol{H}^0_k \simeq \ker(\Upsilon)$. Since $\mathfrak{F}$ is affine, we have

$$\mathfrak{F}(d(D)) = \mathfrak{F}(d[R]) \cdot f(D - [R]) = f(D)\mathfrak{F}(d[R])/f([R]) = f(D).$$

This completes the proof. □

We have the following analogue of Corollary 5.5, which, with Proposition 2.3, implies Theorem 4.5.

Proposition 6.2. *Suppose k is a global field and X is everywhere locally solvable. Then $\mathfrak{F}$ restricts to an affine isomorphism $\mathrm{Sel}^{\phi}(\mathcal{X}/k) \to \mathrm{Sel}^{\phi}_{\mathrm{alg}}(\mathcal{X}/k)$.*

Proof. First off, let us show that $\mathrm{Sel}^{\phi}(\mathcal{X}/k) \subset \mathrm{Cov}^{\phi}_{\mathrm{good}}(\mathcal{X}/k)$. Suppose that $(\mathcal{Y}, \pi) \in \mathrm{Sel}^{\phi}(\mathcal{X}/k)$ and that X is everywhere locally solvable. Consider the covering $\widetilde{\pi} : Y \to X$ obtained by pulling back. We want to show that the pullback to Y of some ramification point on X is linearly equivalent to a k-rational divisor. The obstruction to a k-rational divisor class being represented by a k-rational divisor is an element of the Brauer group of k. Since the Brauer group of a global field satisfies the local-global principle it suffices to show that $(Y, \widetilde{\pi})$ gives a class in $\mathrm{Cov}^{\phi}_0(X/k_v)$ for every prime v. This follows from Lemma 6.1(1) since we have assumed both X and $\mathcal{Y}$ are everywhere locally solvable.

Now let us show that $\mathfrak{F}$ maps the ϕ-Selmer set to the algebraic ϕ-Selmer set. Let $(\mathcal{Y}, \pi) \in \mathrm{Sel}^{\phi}(\mathcal{X}/k)$ and set $\delta = \mathfrak{F}((\mathcal{Y}, \pi))$. For every completion k_v of k, $X(k_v) \neq \varnothing$, so we may apply Lemma 6.1(2) over k_v. This shows that $\mathrm{res}_v(\delta) \in f(\mathrm{Pic}^1(X_{k_v}))$ for every v. Consequently, δ lies in the algebraic ϕ-Selmer set.

It now suffices to show that the map in the statement is surjective, as it is the restriction of an affine isomorphism. For this let δ be an element in the algebraic ϕ-Selmer set. Then $\delta \in \boldsymbol{H}^1_k$, so $\delta = \mathfrak{F}((\mathcal{Y}, \pi))$ for some $(\mathcal{Y}, \pi) \in \mathrm{Cov}^{\phi}_{\mathrm{good}}(\mathcal{X}/k)$. We need to show that $\mathcal{Y}$ is everywhere locally solvable. For each prime v we can find $P_v \in \mathrm{Pic}^1(X_{k_v}) \subset \mathcal{X}(k_v)$ such that $\mathrm{res}_v(\delta) = f(P_v)$. The point P_v lifts to a k_v-point on some ϕ-covering $(\mathcal{Y}_v, \pi_v)$ defined over k_v. Moreover $(\mathcal{Y}_v, \pi_v) \in \mathrm{Cov}^{\phi}_{\mathrm{good}}(\mathcal{X}/k_v)$ by Lemma 6.1(1) and $\mathfrak{F}((\mathcal{Y}_v, \pi_v)) = \mathrm{res}_v(\delta)$ by Lemma 6.1(2). Since $\mathfrak{F}$ is injective we have that $\mathcal{Y} \otimes k_v$ and $\mathcal{Y}_v$ are isomorphic, for each prime v. This implies that $\mathcal{Y}$ is everywhere locally solvable as required. □

7. Examples

We have implemented the algorithm described in Section 4C in the computer algebra system Magma [3] for degree p cyclic covers of $\mathbb{P}^1$ defined over the p-th cyclotomic field. As a test of the algorithm (and the correctness of the implementation) we performed computations for a large sample of hyperelliptic curves. When at all possible we checked our results for consistency with rank bounds obtained by other means (for example, different implementations of descent on elliptic curves and Jacobians of hyperelliptic curves, points of small height on the Jacobian, information obtained assuming standard conjectures, and so on). Some of the resulting data is presented at the end of this section. In addition to this we offer the following examples.

Example 7.1. The two hyperelliptic curves

$$X_1: \ y^2 + (x^3 + x + 1)y = x^6 + 5x^5 + 12x^4 + 12x^3 + 6x^2 - 3x - 4,$$
$$X_2: \ y^2 + (x^3 + x + 1)y = -2x^6 + 7x^5 - 2x^4 - 19x^3 + 2x^2 + 18x + 7$$

over $\mathbb{Q}$ have Mordell-Weil rank 0, and the 2-primary parts of their Shafarevich-Tate groups are isomorphic to $\mathbb{Z}/2 \times \mathbb{Z}/2$.

Proof. Let J_i denote the Jacobian of X_i and $\mathscr{X}_i$ denote $\mathbf{Pic}^1(X_i)$. The X_i are everywhere locally solvable double covers of $\mathbb{P}^1$. Using Magma we computed that $\mathrm{Sel}^2(J_i/\mathbb{Q})$ has $\mathbb{F}_2$-dimension 2 and that the 2-Selmer set of $\mathbf{Pic}^1(X_i)$ is empty for $i = 1, 2$. The result then follows from Theorem 4.5 and its corollary. □

Remark. These curves were taken from [9] (where they were labeled $C_{125,B}$ and $C_{133,A}$), where it is shown that the order of the 2-torsion subgroup of Ш is equal to the order of Ш predicted by the Birch and Swinnerton-Dyer conjectural formula for several modular Jacobian surfaces. In particular, it is proved in [9] that the formula holds for those Jacobians considered if and only if $2\text{Ш} = 0$. For the curves considered one can determine the rank (unconditionally) by analytic means, so a 2-descent on the Jacobian determines Ш[2], but it only determines Ш(2) when $\dim_{\mathbb{F}_2} \text{Ш}[2] \leq 1$. Apart from the two curves above, all curves considered in [9] had $\dim_{\mathbb{F}_2} \text{Ш}[2] \leq 1$. So from the example above one can now conclude for the curves considered in [9] that the conjectural formula holds if and only if Ш has no elements of odd order.

Example 7.2. Let $X/\mathbb{Q}$ be the genus 4 cyclic cover of $\mathbb{P}^1$ with affine equation

$$X: y^3 = 3(x^6 + x^4 + 4x^3 + 2x^2 + 4x + 3).$$

Then X is everywhere locally solvable, yet has no $\mathbb{Q}$-rational divisors of any degree prime to 3. Moreover, the Jacobian J of X has Mordell-Weil rank 1 and the 3-primary part of its Shafarevich-Tate group is isomorphic to $\mathbb{Z}/3 \times \mathbb{Z}/3$.

Proof. We first note that X is everywhere locally solvable. In order to apply the results of this paper, we work over the field $k = \mathbb{Q}(\zeta_3)$ obtained by adjoining a primitive cube root of unity ζ_3. To prove the result we do ϕ-descents on J_k and $\mathbf{Pic}^1(X_k)$, for $\phi = 1 - \zeta_3$. Using Magma we computed that the ϕ-Selmer group of J_k has $\mathbb{F}_3$-dimension 3. From the exact sequence (2-2) it follows that

$$\dim_{\mathbb{F}_3} \frac{J(k)}{\phi J(k)} + \dim_{\mathbb{F}_3} Ш(J/k)[\phi] = 3.$$

We then computed $\mathrm{Sel}^{\phi}_{\mathrm{alg}}(\mathbf{Pic}^1(X_k)/k)$ and found it to be empty. Using Corollary 4.6 this lowers the upper bound for the dimension of $J(k)/\phi J(k)$ to 1.

The divisor on $\mathbb{P}^1$ defined by $x^3 - x^2 + 4x + 4 = 0$ lifts to a degree 3 $\mathbb{Q}$-rational divisor D on X. One can check that the image of the class of $D - \mathfrak{m}$ under $f : \mathrm{Pic}^0(X_k) \to \boldsymbol{H}^0_k$ is nontrivial. So we find that $J(k)/\phi J(k)$ has dimension 1. This gives an upper bound of 2 for the dimension of $Ш(J/k)[\phi]$, so by Corollary 4.6, $Ш(J/k)(3) \simeq Ш(J/k)[\phi] \simeq \mathbb{Z}/3 \times \mathbb{Z}/3$. On the other hand, $\mathbf{Pic}^1(X)$ represents an element of $Ш(J/\mathbb{Q})[3]$ which is not divisible by 3 (since it is not divisible by 3 over k). On the other hand the dimension of $Ш(J/\mathbb{Q})[3]$ is even [14], so it is at least 2. Now the map $Ш(J/\mathbb{Q})(3) \to Ш(J/k)(3)$ obtained by extension of scalars is injective since $[k : \mathbb{Q}] = 2$ is prime to 3, so we must have $Ш(J/\mathbb{Q})(3) \simeq \mathbb{Z}/3 \times \mathbb{Z}/3$.

It remains to compute the rank. The Galois group acts on the ramification points as the full symmetric group, from which it follows that there is no nontrivial k-rational ϕ-torsion in $J(k)$. By [17, Corollary 3.7 and Proposition 3.8] it follows that

$$\mathrm{rank}(J(k)) = [k : \mathbb{Q}] \cdot \left(\dim \frac{J(k)}{\phi J(k)} - \dim J(k)[\phi] \right) = 2, \quad \text{and}$$

$$\mathrm{rank}(J(\mathbb{Q})) = \frac{\mathrm{rank}(J(k))}{[k : \mathbb{Q}]} = 1.$$

In fact, $D - \mathfrak{m}$ represents a point of infinite order in $J(\mathbb{Q})$. □

Remark. From a ϕ-descent on J alone, one is only able to conclude that $1 \leq \dim_{\mathbb{F}_3} J(k)/\phi J(k) \leq 3$, giving $1 \leq \mathrm{rank}(J(\mathbb{Q})) \leq 3$.

Example 7.3 (Data for hyperelliptic curves). For $g \in \{2, 3, 4\}$ we tested our algorithm on various samples of hyperelliptic curves of genus g. For varying values of N, we randomly chose 10,000 separable polynomials $h(x) = \sum_{i=1}^{2g+2} h_i x^i$ of degree at least $2g + 1$ and with integer coefficients h_i bounded in absolute value by N. For each of the genus g curves X defined by $y^2 = h(x)$, we computed $\mathrm{Sel}^2_{\mathrm{alg}}(J/\mathbb{Q})$ and $\mathrm{Sel}^2_{\mathrm{alg}}(\mathscr{X}/\mathbb{Q})$, assuming the generalized Riemann hypothesis for reasons of efficiency. If the latter set was empty, we noted whether or not this was because $\mathrm{Pic}^1(X_{\mathbb{Q}_p})$ was empty for some prime $p \leq \infty$. The resulting data

g	N	$\mathrm{Sel}^2(\mathscr{X}/\mathbb{Q}) = \varnothing$	Rank	Rank*	Improvement	Improvement*
2	5	2146	7873	9819	29%	84%
		981	**848**	**977**		
2	10	3088	5315	9346	22%	73%
		1778	**1295**	**1752**		
2	20	3787	3411	8392	17%	59%
		2420	**1350**	**2317**		
2	50	4297	2156	6955	15%	46%
		2916	**1350**	**2637**		
3	5	2101	2540	7573	8%	32%
		1228	**645**	**1164**		
3	10	2801	1477	5840	8%	29%
		1857	**786**	**1619**		
4	5	1991	1717	6031	6%	22%
		1278	**484**	**1127**		
4	10	2687	1296	5145	8%	25%
		1952	**726**	**1644**		

Table 1. Data for hyperelliptic curves. For reasons of efficiency, all computations summarized in this table were made under the assumption of the generalized Riemann hypothesis; furthermore, in the columns marked by asterisks, we also assumed that $Ш_{\mathrm{div}} = 0$. The first two columns indicate the genus g and the coefficient height bound N of the examples considered in a given row. The third column counts the number of curves (out of 10,000 randomly chosen hyperelliptic curves of the given genus and coefficient height bound) for which $\mathrm{Sel}^2(\mathscr{X}/\mathbb{Q}) = \varnothing$; the bold figures give the number of times the explanation was *not* simply that $\mathrm{Pic}^1(X_{\mathbb{Q}_p})$ is empty for some prime $p \leq \infty$. The "Rank" columns give the number of curves for which the rank could be computed (under the assumptions indicated), with the numbers in bold giving the number of curves for which information from our algorithm was needed to complete the computation. The final two columns give the "improvement factor" in the rank computations: of the sample curves whose ranks could not be determined by earlier methods, the fraction whose ranks could be determined using our algorithm (under the assumptions indicated).

is summarized in Table 1. The boldfaced entries correspond to curves where our algorithm provided information that would not otherwise have been obtained.

It is also interesting to consider how often the combined information yields a sharp upper bound for the Mordell-Weil rank. This will be the case if (i) $\mathscr{X}$ is either trivial or not divisible by 2 in $Ш(J/\mathbb{Q})$; (ii) the number of primes where X fails to have divisors of degree 1 locally is at most one (respectively, not even and positive when the genus is even); and (iii) $Ш(J/\mathbb{Q})[2]$ contains at most two elements

linearly independent from $\mathscr{X}$. The assumptions (i) and (ii) imply, respectively, that in order for $\mathscr{X}(\mathbb{Q})$ to be empty it is necessary and sufficient that $\mathrm{Sel}^2_{\mathrm{alg}}(\mathscr{X}/\mathbb{Q})$ be empty, while (iii) guarantees that determining whether $\mathscr{X}(\mathbb{Q})$ is empty is sufficient to deduce a sharp bound.

With this in mind we used a point search to compute a lower bound for the rank for each curve, both with and without assuming that the divisible subgroup of $Ш(J/\mathbb{Q})$ is trivial (the assumption allows us to determine the parity of the rank). When this matched the upper bound it means we computed the rank, and in such cases we counted the number of curves where the additional information provided by $\mathrm{Sel}^2_{\mathrm{alg}}(\mathscr{X}/\mathbb{Q})$ was needed. We then computed the proportion of curves for which the rank could be determined with the additional information provided by our algorithm among those for which the rank could not be determined by descent on the Jacobian alone.

For example, in the sample of genus 2 curves with $N = 10$ the method yielded new information for about 17% of the curves, which (assuming $Ш_{\mathrm{div}} = 0$) increased our success rate from about 76% to about 93%, handling about 73% of the curves left previously undecided by the descent on the Jacobian.

References

[1] Michael Artin and John Tate (eds.), *Arithmetic and geometry*, *vol. I*, Progress in Mathematics, no. 35, Birkhäuser, Boston, 1983. MR 84j:14005a

[2] Siegfried Bosch, Werner Lütkebohmert, and Michel Raynaud, *Néron models*, Ergebnisse der Mathematik und ihrer Grenzgebiete (3), no. 21, Springer, Berlin, 1990. MR 91i:14034

[3] Wieb Bosma, John Cannon, and Catherine Playoust, *The Magma algebra system, I: The user language*, J. Symbolic Comput. **24** (1997), no. 3–4, 235–265. MR 1484478

[4] Nils Bruin and Michael Stoll, *Deciding existence of rational points on curves: An experiment*, Experiment. Math. **17** (2008), no. 2, 181–189. MR 2009d:11100

[5] ———, *Two-cover descent on hyperelliptic curves*, Math. Comp. **78** (2009), no. 268, 2347–2370. MR 2010e:11059

[6] J. W. S. Cassels, *The Mordell-Weil group of curves of genus* 2, in Artin and Tate [1], 1983, pp. 27–60. MR 84k:14032

[7] Brendan Matthew Creutz, *Explicit second p-descent on elliptic curves*, Ph.D. thesis, Jacobs University, Bremen, Germany, 2010. http://www.jacobs-university.de/phd/files/1283816493.pdf

[8] Tom Fisher, *A counterexample to a conjecture of Selmer*, in Reid and Skorobogatov [15], 2003, pp. 119–131. MR 2005a:11077

[9] E. Victor Flynn, Franck Leprévost, Edward F. Schaefer, William A. Stein, Michael Stoll, and Joseph L. Wetherell, *Empirical evidence for the Birch and Swinnerton-Dyer conjectures for modular Jacobians of genus 2 curves*, Math. Comp. **70** (2001), 1675–1697. MR 2002d:11072

[10] Daniel M. Gordon and David Grant, *Computing the Mordell-Weil rank of Jacobians of curves of genus two*, Trans. Amer. Math. Soc. **337** (1993), no. 2, 807–824. MR 93h:11057

[11] J. S. Milne, *Arithmetic duality theorems*, 2nd ed., BookSurge, LLC, Charleston, SC, 2006. MR 2007e:14029

[12] Michael Mourao, *Descent on superelliptic curves*, 2011. arXiv 1010.2360v3 [math.NT]

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

[14] Bjorn Poonen and Michael Stoll, *The Cassels-Tate pairing on polarized abelian varieties*, Ann. of Math. (2) **150** (1999), no. 3, 1109–1149. MR 2000m:11048

[15] Miles Reid and Alexei Skorobogatov (eds.), *Number theory and algebraic geometry*, London Mathematical Society Lecture Note Series, no. 303, Cambridge University Press, 2003. MR 2004k:00024

[16] Edward F. Schaefer, *2-descent on the Jacobians of hyperelliptic curves*, J. Number Theory **51** (1995), no. 2, 219–232. MR 96c:11066

[17] ———, *Computing a Selmer group of a Jacobian using functions on the curve*, Math. Ann. **310** (1998), no. 3, 447–471, erratum: [18]. MR 99h:11063

[18] ———, *Erratum: "Computing a Selmer group of a Jacobian using functions on the curve" [Math. Ann. **310** (1998), no. 3, 447–471]*, Math. Ann. **339** (2007), no. 1, 1. MR 2008f:11063

[19] Jean-Pierre Serre, *Algebraic groups and class fields*, 2nd ed., Graduate Texts in Mathematics, no. 117, Springer, New York, 1998. MR 88i:14041

[20] Michael Stoll, *Implementing 2-descent for Jacobians of hyperelliptic curves*, Acta Arith. **98** (2001), no. 3, 245–277. MR 2002b:11089

[21] Michael Stoll and Ronald van Luijk, *Unfaking the fake Selmer group*, 2011. arXiv 1108.3364 [math.AG]

BRENDAN CREUTZ: brendan.creutz@sydney.edu.au
School of Mathematics and Statistics, University of Sydney, Sydney, NSW 2006, Australia

VOLUME EDITORS

Everett W. Howe
Center for Communications Research
4320 Westerra Court
San Diego, CA 92121-1969
United States

Kiran S. Kedlaya
Department of Mathematics
University of California, San Diego
9500 Gilman Drive #0112
La Jolla, CA 92093-0112

Front cover artwork based on a detail of
Chicano Legacy 40 Años ©2010 Mario Torero.

ISSN: 2329-9061 (print), 2329-907X (electronic)

ISBN: 978-1-935107-00-2 (print), 978-1-935107-01-9 (electronic)

First published 2013.

MATHEMATICAL SCIENCES PUBLISHERS
798 Evans Hall #3840, c/o University of California, Berkeley CA 94720-3840
contact@msp.org **http://msp.org**

THE OPEN BOOK SERIES 1

Tenth Algorithmic Number Theory Symposium

The Algorithmic Number Theory Symposium (ANTS), held biennially since 1994, is the premier international forum for research in computational number theory. ANTS is devoted to algorithmic aspects of number theory, including elementary, algebraic, and analytic number theory, the geometry of numbers, arithmetic algebraic geometry, the theory of finite fields, and cryptography.

This volume is the proceedings of the tenth ANTS meeting, held July 9–13, 2012, at the University of California, San Diego. It includes revised and edited versions of the 25 refereed papers presented at the conference, together with extended abstracts of two of the five invited talks.

TABLE OF CONTENTS