TRANSACTIONS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 370, Number 5, May 2018, Pages 3487–3505
http://dx.doi.org/10.1090/tran/7060
Article electronically published on December 1, 2017

EXPLICIT DESCENT FOR JACOBIANS OF PRIME POWER CYCLIC COVERS OF THE PROJECTIVE LINE

EDWARD F. SCHAEFER

Abstract. The Jacobian of a cyclic cover of the projective line is isogenous to a product of abelian subvarieties, one for each positive divisor of the degree of the cover. In this article, we show how to compute a Selmer group that bounds the Mordell-Weil rank for each abelian subvariety corresponding to a non-trivial prime power divisor of the degree. In the case that the Chabauty condition holds for that abelian subvariety, we show how to bound the number of rational points on the curve.

1. Introduction

A classical Thue equation has the form $g(x, w) = h$ where h is an integer and $g(x, w)$ is an irreducible, homogeneous polynomial of degree $n \geq 3$, with integral coefficients. In [LT], Lorenzini and Tucker associate to that Thue equation the curve given by $hv^n = g(x, 1)$. They point out that the Jacobian of the curve is isogenous to a product of abelian subvarieties over $\mathbb{Q}$, one for each positive divisor of n. They then prove beautiful results using the method of Chabauty-Coleman. Some results depend on the Mordell-Weil rank of the Jacobian of the curve over $\mathbb{Q}$. This leads to the question of determining that rank, which is the sum of the ranks of the abelian subvarieties. The abelian subvariety of the Jacobian of $hv^n = g(x, 1)$, corresponding to a positive divisor $d|n$, is isogenous over $\mathbb{Q}$ to an abelian subvariety of the Jacobian of the curve $hy^d = g(x, 1)$.

A Selmer group for an endomorphism, a power of which is an associate of an integer greater than 1, can be used to give an upper bound on the Mordell-Weil rank. In fortunate cases, we can then provably determine the Mordell-Weil rank. The curve $hy^d = g(x, 1)$ has an automorphism τ given by $\tau(x, y) = (x, \zeta_d y)$, where ζ_d is a primitive d-th root of unity. We often denote a map and a map it induces with the same notation. We shall see that τ induces an automorphism of the abelian subvariety and in its endomorphism ring, τ acts like ζ_d. A method for computing the $(1 - \tau)$-Selmer group in the case that d is a prime is described in [PS] (in that case, the abelian subvariety corresponding to d is the entire Jacobian). A power of $1 - \zeta_d$ is an associate of an integer greater than 1 if and only if $d = p^r$ where p is a prime and $r \geq 1$. So the endomorphism $1 - \tau$ appears to be useful for bounding the Mordell-Weil rank in only this case. In this article, we describe a method for

Received by the editors July 29, 2015, and, in revised form, August 10, 2016.

2010 *Mathematics Subject Classification.* Primary 11G30; Secondary 11G10, 14G25, 14H40, 14H45.

The author is grateful for the hospitality of the Mathematisches Institut at the Universität Bayreuth, where much of this research was done, and to his host there, Michael Stoll, for many useful conversations. This article benefited from useful comments from the referees.

computing the $(1-\tau)$-Selmer group for the abelian subvariety, mentioned above, of the Jacobian of the curve $hy^{p^r} = g(x,1)$ with $r > 1$.

Typically when $r > 1$, the genus of $hy^{p^r} = g(x,1)$ is greater than 1. So by Faltings' Theorem, there is a finite number of rational points. Let us assume that the Chabauty condition, i.e., that the Mordell-Weil rank is less than the dimension, holds for the abelian subvariety mentioned above. For such a case we outline a method of doing a Chabauty computation to give an upper bound on the number of rational points on the curve $hy^{p^r} = g(x,1)$. With luck, this will equal the number of known rational points on the curve. As a corollary, this would give us the integer solutions to the Thue equation. Since most of the results in this article involve computing a Selmer group, we use a slightly different model for the curve, namely $y^{p^r} = f(x)$, in order to agree with the notation used in similar articles. Though the article of Lorenzini and Tucker [LT] is the inspiration for this work, we will no longer address Thue equations and instead will present our results in the context of rational points on cyclic covers of the projective line.

In Section 2, we define the abelian subvariety mentioned above, which we'll denote B, of the Jacobian J of the curve $y^{p^r} = f(x)$ and set the rest of the notation to be used throughout the article. In Section 3, we study the structures of and the relationship between the kernels of the isogenies $1-\tau$ on J and on B. In Section 4, we prove, under an assumption, that the $(1-\tau)$-Selmer group for B is isomorphic to a Selmer group for an isogeny to J. As described in [Sc2] and [BPS16], the computation of the latter kind of Selmer group can be practical. Since a convenient spanning set for the kernel of the isogeny to J leads to a fake descent setup (as described in [BPS16, §6]), we show in Section 5 how to get the Selmer group for the isogeny to J from the fake Selmer group. In Section 6, assuming we can find enough rational divisors whose images generate the fake Selmer group, we show how to determine the Mordell-Weil rank of B. In Section 7, we discuss conditions which imply part of the assumption made in Section 4.

In Section 8, we describe how to bound the number of rational points on $y^{p^r} = f(x)$ if the Chabauty condition holds for B. We give an example in Section 9 of the use of the techniques of the article to show that for $y^4 = 2x^4+x^3+1$ we have $B(\mathbb{Q}) \cong \mathbb{Z}$ and that the set of points with coordinates in $\mathbb{Q}$ is $\{(0,1),(0,-1),(-1/2,1),(-1/2,-1)\}$. In Appendix A, we prove the above claim that the subvarieties associated to d, as defined in the proof of [LT, Prop. 3.12], of the Jacobians of $v^n = f(x)$ and $y^d = f(x)$ are isogenous and the corresponding Mordell-Weil ranks are the same. We show in Appendix B that if p divides the multiplicity of a root of f, then the geometry can be more complicated, which is why we assume that p does not divide the multiplicity of any root of f.

2. Notation

Let p be a prime, let K be a field of characteristic different from p, and let K_s denote a separable closure. For an object Y over K, we use Y_s to denote its base extension to K_s. Let X be the curve over K (smooth, projective, and geometrically integral) with an affine model $y^{p^r} = f(x)$ for some $r > 1$, where f is a polynomial defined over K, of degree n. We assume K is sufficiently large so that we can assume that n is divisible by p^r. Let $f(x) = a_n \prod_{i=1}^{m} (x-\alpha_i)^{n_i}$, where the α_i are distinct elements of K_s. For simplicity, we add the restriction that p not divide

any n_i; otherwise the geometry becomes more complicated (see Section 12). Let $f_0(x) := \prod_{i=1}^{m}(x-\alpha_i) \in K[x]$ be the radical of f.

Let $\mathrm{Gal}(K) := \mathrm{Gal}(K_s/K)$ denote the absolute Galois group of K. For any place $\mathfrak{q}$ of K, let $K_{\mathfrak{q}}$ denote the completion. Let ζ_d denote a primitive d-th root of unity and $K' := K(\zeta_{p^r})$. We let $J := \mathrm{Alb}_X$ be the Jacobian of X. We can identify $\mathrm{Pic}^0(X_s)$ with $J_s(K_s)$. Where it will not lead to confusion, we also use X and J to denote the curve and its Jacobian over extension fields, e.g., $X \times_K K'$. We let $\mathcal{K}$ (respectively $\mathcal{K}'$) denote an arbitrary extension of K (respectively K'), for example when we want to prove a result for both K and $K_{\mathfrak{q}}$.

The curve X has an automorphism τ induced by $\tau(x,y) = (x, \zeta_{p^r} y)$ over K'. We also use τ to denote the automorphism it induces on J. For a degree 0 divisor D on X_s we use $[D]$ to denote its divisor class in $J_s(K_s)$. Let $\Phi(u) := (u^{p^r}-1)/(u-1)$ and $\Psi(u) := \Phi(u)/\Phi_{p^r}(u)$, where Φ_t denotes the t-th cyclotomic polynomial. Note that $\Psi(u) = \prod_{\ell \mid p^r, \ell \neq 1, p^r} \Phi_\ell(u)$. When we replace u by τ, we can evaluate any of these on divisors and, by extension, on $J_s(K_s)$. Let $\mathrm{End}(J)$ denote the endomorphism ring of the abelian variety J. We let $\Upsilon := \Psi(\tau) \in \mathrm{End}(J)$ and note that Υ maps surjectively to an abelian subvariety that we denote B. That B is defined over K follows from the argument in the proof of [LT, Prop. 3.12]. We have that Υ is the composition of a surjective morphism $\Upsilon_o : J \to B$ over K' with the embedding $\iota : B \hookrightarrow J$ over K. Let $X_{p^{r-1}}$ denote the curve given by $v^{p^{r-1}} = f(x)$ and $J_{p^{r-1}}$ denote its Jacobian. It follows from the results in Section 11 that J is isogenous over K to $J_{p^{r-1}} \oplus B$. We can identify $\iota(B_s(K_s))$ with the image of Υ on $\mathrm{Pic}^0(X_s)$. Since τ and Υ commute in $\mathrm{End}(J)$, we note that τ induces an automorphism of B, which we also denote by τ, except when adding a subscript will add clarity.

We denote the divisor on X that is the formal sum of the distinct points at infinity (with respect to the given affine model) by ∞. We use Δ to denote the $\mathrm{Gal}(K)$-subset of X_s that is $\{(\alpha_i, 0)\}$.

For a homomorphism of abelian varieties $g : A_1 \to A_2$, let $\hat{g} : \hat{A}_2 \to \hat{A}_1$ denote the dual homomorphism between dual abelian varieties. Let $\lambda : J \to \hat{J}$ be the canonical principal polarization of J coming from its being the Jacobian of X. For any homomorphism $h : A_3 \to A_4$ of abelian varieties or of groups, let $A_3[h]$ denote its kernel. For any $\mathrm{Gal}(K)$-module M, we use $H^1(K, M)$ to denote $H^1(\mathrm{Gal}(K), M)$, the first $\mathrm{Gal}(K)$-cohomology group of M. If g (defined above) is an isogeny defined over K, we let $\delta_g : A_2(K) \to H^1(K, A_1[g])$ denote the connecting homomorphism of cohomology. If G is a group, S is a G-set, and M is a G-module, let M^S denote the G-module of maps from S to M.

For a vector space V over $\mathbb{F}_p$, we let $\dim V$ denote its dimension. In the case that W is an algebraic variety, we use $\dim W$ to denote its dimension. For a finitely generated $\mathbb{Z}$-module M, let $\mathrm{rank}\, M$ denote its free $\mathbb{Z}$-rank.

For the remainder of this section, let K be a number field. We recall the definition of the Selmer group for an isogeny of abelian varieties $\epsilon : A_1 \to A_2$ over K. For any place $\mathfrak{q}$ of K, we denote the restriction map $r_{1,\mathfrak{q}} : H^1(K, A_1[\epsilon]) \to H^1(K_{\mathfrak{q}}, A_1[\epsilon])$. The Selmer group, denoted $S^{\epsilon}(A_1, K)$, is defined to be $\{\gamma \in H^1(K, A_1[\epsilon]) \mid r_{1,\mathfrak{q}}(\gamma) \in \delta_\epsilon(A_2(K_{\mathfrak{q}})/\epsilon A_1(K_{\mathfrak{q}})), \forall \mathfrak{q}\}$.

We recall the definition of the Shafarevich-Tate group for an abelian variety A_1 over K. For any place $\mathfrak{q}$ of K we denote the restriction map

$$r_{2,\mathfrak{q}} : H^1(K, A_1) \to H^1(K_{\mathfrak{q}}, A_1).$$

The Shafarevich-Tate group, denoted $Ш(A_1, K)$, is defined to be the kernel of

$$H^1(K, A_1) \overset{\prod r_{2,\mathfrak{q}}}{\to} \prod H^1(K_\mathfrak{q}, A_1), \tag{2.1}$$

where the products are taken over all places $\mathfrak{q}$ of K. We have the classic short exact sequence

$$0 \to A_2(K)/\epsilon A_1(K) \to S^\epsilon(A_1, K) \to Ш(A_1, K)[\epsilon] \to 0. \tag{2.2}$$

3. The isogenies $1 - \tau$ on J and on B

In this section, we want to describe $J[1-\tau]$ and $B[1-\tau]$. Let X_p be the curve with an affine model $w^p = f(x)$ and J_p be its Jacobian, which over K_s we associate to $\mathrm{Pic}^0(X_{p,s})$. Let $\pi : X \to X_p$ be the covering given by $\pi(x, y) = (x, y^{p^{r-1}})$; it induces $\pi^* : J_p \to J$ (see [Si, Remark 3.7]). We define an automorphism induced by $\tau_p(x, w) = (x, \zeta_{p^r}^{p^{r-1}} w)$ of X_p.

From the proof of [Sc2, Prop. 3.2], which was suggested by Michael Stoll, we have $J_s(K_s)[1-\tau] = \langle[(\alpha_j, 0) - (\alpha_i, 0)]\rangle$ (here each $(\alpha_k, 0) \in X_s(K_s)$) and $J_{p,s}(K_s)[1-\tau_p] = \langle[(\alpha_j, 0) - (\alpha_i, 0)]\rangle$ (here each $(\alpha_k, 0) \in X_{p,s}(K_s)$).

Lemma 3.1. *We have dim $J_{p,s}(K_s)[1-\tau_p] = m - 2$.*

Proof. This follows from [PS, Lem. 6.1]. □

Proposition 3.2. *The map π^* induces an isomorphism from $J_{p,s}(K_s)[1-\tau_p]$ to $p^{r-1}J_s(K_s)[1-\tau]$.*

Proof. That the image of $J_{p,s}(K_s)[1-\tau_p]$ is exactly $p^{r-1}J_s(K_s)[1-\tau]$ follows from the definition of π^* (see [Si, p. 33]). Assume $\sum_{i=1}^m \ell_i p^{r-1}(\alpha_i, 0) = \mathrm{div}(h)$ for some $h \in K_s(X_s)$ where each $\ell_i \in \mathbb{Z}$ and each $(\alpha_i, 0) \in X_s(K_s)$. To prove that π^* induces an injection on $J_{p,s}(K_s)[1-\tau_p]$, we need to prove that $h \in \pi^* K_s(X_{p,s})$.

We can consider τ^p to be a generator of $\mathrm{Gal}(K_s(X_s)/\pi^* K_s(X_{p,s}))$. Note that $\mathrm{div}(h) = \tau^p(\mathrm{div}(h)) = \mathrm{div}(\tau^p h)$. Thus there is a $\kappa \in K_s^\times$ such that $\tau^p h = \kappa h$. We expand both sides of the equation $\tau^p h = \kappa h$ on a power basis generated by y for the extension $K_s(X_s)/\pi^* K_s(X_{p,s})$. Then an easy exercise equating scalars shows that $\kappa = 1$ and thus $h \in \pi^* K_s(X_{p,s})$ or $h = g y^j$ for some $g \in \pi^* K_s(X_{p,s})^\times$ and $j \in \mathbb{Z}$.

In the latter case it suffices to prove that $y^j \in \pi^* K_s(X_{p,s})$. Since the supports of $\mathrm{div}(h)$ and $\mathrm{div}(y^j)$ are contained in Δ, the same is true of $\mathrm{div}(g)$. Since $g \in \pi^* K_s(X_{p,s})^\times$, the definition of π^* implies that $\mathrm{div}(g) = \sum_{i=1}^m \ell_i' p^{r-1}(\alpha_i, 0)$, where each $\ell_i' \in \mathbb{Z}$. Therefore $\mathrm{div}(y^j)$ is of this form as well. So $j = p^{r-1}d$ for some $d \in \mathbb{Z}$ and $y^j = \pi^*(w^d)$. □

Corollary 3.3. *We have dim $p^{r-1}J_s(K_s)[1-\tau] = m - 2$.*

Proof. This follows from Lemma 3.1 and Proposition 3.2. □

We will no longer consider X_p. The following lemma is a straightforward computation.

Lemma 3.4. *The p^r closed points at infinity for the affine model $y^{p^r} = f(x)$ of X_s are given by $(u, z) = (0, \zeta_{p^r}^i \sqrt[p^r]{a_n})$ for $0 \le i < p^r$, where a_n is the leading coefficient of f, $u := 1/x$, and $z := y/(x^{n/p^r})$.*

Over K_s, the divisor we denote ∞ is the formal sum of the p^r points listed in the above lemma.

Proposition 3.5. *We have* $J[1-\tau] \cong (\mathbb{Z}/p^r\mathbb{Z})^{m-2}$.

Proof. From above we know that $J_s(K_s)[1-\tau] = \langle[(\alpha_j,0)-(\alpha_i,0)]\rangle = \langle[(\alpha_i,0)-(\alpha_1,0)]\rangle$. Using Lemma 3.4 we can show that $\operatorname{div}(y) = \sum_{i=1}^{m} n_i(\alpha_i,0) - \frac{n}{p^r}\infty$ and $\operatorname{div}(x-\alpha_i) = p^r(\alpha_i,0)-\infty$. A straightforward computation using the above and the fact that $\gcd(n_m,p^r)=1$ shows that $[(\alpha_m,0)-(\alpha_1,0)] \in \langle[(\alpha_i,0)-(\alpha_1,0)] \mid 2 \le i \le m-1\rangle$. Since $J[1-\tau]$ can be generated by $m-2$ elements and $\dim p^{r-1}J_s(K_s)[1-\tau] = m-2$, the result follows. □

Lemma 3.6. *Considering* τ *as an automorphism of* B *the map* $\tau^i \mapsto \zeta_{p^r}^i$ *induces an isomorphism of the* $\mathrm{Gal}(K)$*-modules* $\langle\tau\rangle$ *and* μ_{p^r}.

Proof. We know that $J_s(K_s)$ is generated by divisor classes of the kind $[Q-R]$ where Q, R are closed points of X_s and Q, R are not points at infinity. Note that the image of the divisor $Q-R$ under $\Phi(\tau)$ is the divisor of the function $(x-x_Q)/(x-x_R)$. Thus $\Phi(\tau) = \Phi_{p^r}(\tau)\Upsilon = 0$ on J and $\Phi_{p^r}(\tau) = 0$ on $B = \Upsilon_o J$. Clearly the $\mathrm{Gal}(K)$-actions are the same. □

The following lemma comes from [LT, Lem. 3.13].

Lemma 3.7. *The dimension of* B *is* $\varphi(p^r)(m-2)/2$*, where* φ *denotes the Euler totient function.*

Proposition 3.8. *The endomorphism* $1-\tau$ *on* B *is an isogeny, defined over* K'*, whose kernel* $B[1-\tau]$ *is an* $\mathbb{F}_p$*-vector space of dimension* $m-2$.

Proof. Since $\iota B[1-\tau] \subset J[1-\tau]$, Proposition 3.5 tells us that the endomorphism $1-\tau$ of B is an isogeny. From Lemma 3.6, τ acts like ζ_{p^r} on B. Since $(1-\zeta_{p^r})^{\varphi(p^r)}$ is an associate of p, the kernel of $1-\tau$ on B is contained in $B[p]$. Since the dimension of B is $\varphi(p^r)(m-2)/2$ (from Lemma 3.7), we have $\dim B[p] = \varphi(p^r)(m-2)$ and $\dim B[1-\tau] = m-2$ as $\mathbb{F}_p$-vector spaces. □

Lemma 3.9. *We have* $\iota B[1-\tau] = p^{r-1}J[1-\tau] = J[1-\tau][p]$.

Proof. Since $\iota B \subset J$ we have $\iota B[1-\tau] \subseteq J[1-\tau]$. From Proposition 3.8, $\iota B[1-\tau] \subseteq J[p]$. So $\iota B[1-\tau] \subseteq J[1-\tau][p]$. From Proposition 3.5, $J[1-\tau][p] = p^{r-1}J[1-\tau]$. From Corollary 3.3 and Proposition 3.8, $\dim p^{r-1}J[1-\tau] = \dim \iota B[1-\tau]$. □

Proposition 3.10. *The map* Υ_o *induces a surjection from* $J[1-\tau]$ *to* $B[1-\tau]$*. When composed with the map induced by* ι *we get the* p^{r-1} *map on* $J[1-\tau]$.

Proof. Since τ acts trivially on $J[1-\tau]$, we see that $\Upsilon = \Phi(1)/\Phi_{p^r}(1) = p^{r-1}$ on $J[1-\tau]$. The result then follows from Lemma 3.9. □

4. An isomorphism of Selmer groups

For K a number field, we want to find a homomorphism on $B(K')/(1-\tau)B(K')$ to use for descent. However, the usual methods for explicitly computing a Selmer group ([Sc2], improved by [BPS16]) are for an isogeny from some abelian variety to a Jacobian. In this section, we describe (under a certain assumption) an isomorphism from the Selmer group associated to $(1-\tau)_B$ over K' to the Selmer group for an

isogeny from an abelian variety to J over K'. We begin this section by letting K be a field of characteristic different from p.

Recall that $\Delta := \{(\alpha_i, 0)\}$. In the notation and nomenclature of [BPS16, §6], we have that $(p, \Delta, p^{r-1}\Delta_{\mathrm{Diag}})$ is a fake descent setup for X over K'. Note that in the third coordinate, Δ_{Diag} is the diagonal embedding of Δ in $X \times \Delta$, and we give the divisor on $X \times \Delta$ representing the line bundle that should be in the third coordinate. To be a fake descent setup means that there is a divisor $D \in \mathrm{Div}(X)$, defined over K' (in our case $D = \infty$), such that $p(p^{r-1}\Delta_{\mathrm{Diag}}) - (D \times \Delta)$ is principal, i.e., the divisor of some $h \in K'(X \times \Delta)^\times$. In our case, at $K'(X \times (\alpha_i, 0))$, we have $h = x - \alpha_i$.

Let $E := (\mathbb{Z}/p\mathbb{Z})^{\Delta}_{\deg 0}$ be the $\mathrm{Gal}(K')$-module of maps from Δ to $\mathbb{Z}/p\mathbb{Z}$ with the property that the sum of the images is 0. There is a homomorphism $\hat{\alpha} : E \to \hat{J}_s(K_s)[p]$ induced by the divisor $p^{r-1}\Delta_{\mathrm{Diag}}$. Specifically, if $e \in E$ and $e((\alpha_i, 0)) = \overline{m}_i$, then $\hat{\alpha}(e) = \lambda[\sum_{i=1}^{m} m_i p^{r-1}(\alpha_i, 0)]$, where the m_i are integers summing to 0 and each m_i reduces mod p to $\overline{m}_i$. From Lemma 3.9, we have $\hat{\alpha}(E) = \lambda\iota(B[1-\tau])$. Define $\hat{\phi} : \hat{J} \to \hat{A}$, where $\hat{A} := \hat{J}/\hat{\alpha}(E)$. Then $\phi : A \to J$ is an isogeny, defined over K', whose kernel has dimension $m-2$ (from Proposition 3.8). We proceed to clarify the relation between ϕ and $(1-\tau)_J$.

Proposition 4.1. *We have* $\lambda(J[1-\tau]) = \hat{J}[1 \hat{-} \tau]$.

Proof. By the definition of the Rosati involution, diagram (4.1) commutes:

$$\begin{array}{ccc} J & \xrightarrow{(1-\tau)^\dagger} & J \\ {\scriptstyle\lambda}\downarrow & & \downarrow{\scriptstyle\lambda} \\ \hat{J} & \xrightarrow{1\hat{-}\tau} & \hat{J} \end{array} \tag{4.1}$$

Since τ is an automorphism of X it induces an automorphism of the pair (J, λ). From the proof of [Mi1, Prop. 17.5] we have $\tau^\dagger = \tau^{-1}$. So $(1-\tau)^\dagger = 1 - \tau^{-1} = -\tau^{-1}(1-\tau)$, which is an associate of $1-\tau$. □

Corollary 4.2. *We have* $\hat{J}[\hat{\phi}] = \lambda\iota(B[1-\tau]) = (\hat{J}[1 \hat{-} \tau])[p]$.

Proof. This follows from Lemma 3.9 and Proposition 4.1. □

From Corollary 4.2 there is an isogeny $\hat{\eta}$, over K', such that $\hat{\eta}\hat{\phi} = (1 \hat{-} \tau)_{\hat{J}}$. Thus there is an isogeny η, over K', such that $\phi\eta = (1-\tau)_J$.

Lemma 4.3. *We have* $J[\eta] = p(J[1-\tau])$.

Proof. This follows from Proposition 3.5 and Corollary 4.2. □

As Υ and $1-\tau$ commute in $\mathrm{End}(J)$, diagram (4.2) commutes:

$$\begin{array}{ccccc} J & \xrightarrow{\eta} & A & \xrightarrow{\phi} & J \\ {\scriptstyle\Upsilon_o}\downarrow & & & & \downarrow{\scriptstyle\Upsilon_o} \\ B & & \xrightarrow{1-\tau} & & B \end{array} \tag{4.2}$$

Proposition 4.4. *We have* $J[\eta] \subseteq J[\Upsilon]$.

Proof. Since τ acts trivially on $J[\eta] \subset J[1-\tau]$, we see that Υ acts as p^{r-1} on $J[\eta]$ from Proposition 3.10. From Lemma 4.3, we have $\Upsilon(J_s(K_s)[\eta]) = \langle p^r[(\alpha_i, 0) - (\alpha_1, 0)]\rangle = 0$. □

Recall that $J[\Upsilon] = J[\Upsilon_o]$ and $\eta : J \to A$ is surjective. So from Proposition 4.4, the map $\Upsilon'_o := \Upsilon_o \eta^{-1}$ is a well-defined homomorphism of abelian varieties from A to B over K'.

Corollary 4.5. *Diagram* (4.3) *commutes:*

$$\begin{array}{ccc} A & \xrightarrow{\phi} & J \\ {\scriptstyle \Upsilon'_o}\downarrow & & \downarrow{\scriptstyle \Upsilon_o} \\ B & \xrightarrow{1-\tau} & B \end{array} \tag{4.3}$$

Proposition 4.6. *The homomorphism of abelian varieties $\Upsilon'_o : A \to B$ induces an isomorphism of groups $\Upsilon'_o : A[\phi] \to B[1-\tau]$ over K'.*

Proof. Let $\bar{q} : J[1-\tau] \to J[1-\tau]/pJ[1-\tau]$ be the quotient map. By Lemma 4.3, there is an isomorphism $\nu : A[\phi] \to J[1-\tau]/pJ[1-\tau]$ over K' making the upper-right parallelogram of diagram (4.4) commute. From Proposition 3.10, the lower-left parallelogram of diagram (4.4) commutes:

$$\begin{array}{ccccc} J[1-\tau] & & \xrightarrow{\eta} & & A[\phi] \\ {\scriptstyle \Upsilon_o}\downarrow & \searrow^{=} & & \swarrow_{\nu} & \\ B[1-\tau] & & J[1-\tau] & \xrightarrow{\bar{q}} & J[1-\tau]/pJ[1-\tau] \\ & \searrow_{\iota} & \downarrow{\scriptstyle p^{r-1}} & & \\ & & p^{r-1}J[1-\tau] & & \end{array} \tag{4.4}$$

From Proposition 3.5, $p^{r-1}(\bar{q})^{-1} : J[1-\tau]/pJ[1-\tau] \to p^{r-1}J[1-\tau]$ is an isomorphism over K', as are ι (see Lemma 3.9) and ν. Thus $\Upsilon'_o = \Upsilon_o \eta^{-1} : A[\phi] \to B[1-\tau]$ induces an isomorphism over K'. □

Corollary 4.7. *The isomorphism $\Upsilon'_o : A[\phi] \to B[1-\tau]$ induces an isomorphism $\Upsilon'_o : H^1(\mathcal{K}', A[\phi]) \to H^1(\mathcal{K}', B[1-\tau])$.*

From Corollary 4.5 and Proposition 4.6, diagram (4.5) is a commutative diagram of $\mathrm{Gal}(\mathcal{K}')$-modules:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A[\phi] & \longrightarrow & A(\mathcal{K}'_s) & \xrightarrow{\phi} & J(\mathcal{K}'_s) & \longrightarrow & 0 \\ & & {\scriptstyle \Upsilon'_o}\downarrow & & {\scriptstyle \Upsilon'_o}\downarrow & & {\scriptstyle \Upsilon_o}\downarrow & & \\ 0 & \longrightarrow & B[1-\tau] & \longrightarrow & B(\mathcal{K}'_s) & \xrightarrow{1-\tau} & B(\mathcal{K}'_s) & \longrightarrow & 0 \end{array} \tag{4.5}$$

Taking $\mathrm{Gal}(\mathcal{K}')$-invariants gives us the following.

Lemma 4.8. *Diagram* (4.6) *commutes:*

$$\begin{array}{ccc} J(\mathcal{K}')/\phi A(\mathcal{K}') & \xrightarrow{\delta_\phi} & H^1(\mathcal{K}', A[\phi]) \\ {\scriptstyle \Upsilon_o}\downarrow & & \downarrow{\scriptstyle \Upsilon'_o} \\ B(\mathcal{K}')/(1-\tau)B(\mathcal{K}') & \xrightarrow{\delta_{1-\tau}} & H^1(\mathcal{K}', B[1-\tau]) \end{array} \tag{4.6}$$

Proposition 4.9. *The map* $\Upsilon_o : J(\mathcal{K}')/\phi A(\mathcal{K}') \to B(\mathcal{K}')/(1-\tau)B(\mathcal{K}')$ *is an injection.*

Proof. This follows from Corollary 4.7 and Lemma 4.8 and the fact that δ_ϕ is an injection. □

For the remainder of this article, K is a number field. Let S be any finite set of finite places of K', which includes the places of bad reduction of J and places lying over p. If $\mathfrak{q}$ is a finite place of K', not lying over p, at which the coefficients of f are integral and $\mathfrak{q}$ does not divide the discriminant of f or the leading coefficient of f, then J has good reduction at $\mathfrak{q}$.

Assumption 1. *For all places* $\mathfrak{q} \in S$*, the map*

$$\Upsilon_o : J(K'_\mathfrak{q})/\phi A(K'_\mathfrak{q}) \to B(K'_\mathfrak{q})/(1-\tau)B(K'_\mathfrak{q})$$

is a surjection.

We are unaware of whether there is a counterexample to Assumption 1.

Proposition 4.10. *Under Assumption* 1*, the map*

$$\Upsilon_o : J(K'_\mathfrak{q})/\phi A(K'_\mathfrak{q}) \to B(K'_\mathfrak{q})/(1-\tau)B(K'_\mathfrak{q})$$

induces an isomorphism for all finite places $\mathfrak{q}$ *of* K'*.*

Proof. From Proposition 4.9, the map is always injective. The result follows for places in S from Assumption 1. From [Sc1, Lem. 3.8], for finite places outside S, we have $\#J(K'_\mathfrak{q})/\phi A(K'_\mathfrak{q}) = \#A(K'_\mathfrak{q})[\phi]$ and $\#B(K'_\mathfrak{q})/(1-\tau)B(K'_\mathfrak{q}) = \#B(K'_\mathfrak{q})[1-\tau]$. From Proposition 4.6, we have $\#A(K'_\mathfrak{q})[\phi] = \#B(K'_\mathfrak{q})[1-\tau]$. □

Theorem 4.11. *Under Assumption* 1*, the map* Υ'_o *induces an isomorphism of* $S^\phi(A, K')$ *and* $S^{1-\tau}(B, K')$*.*

Proof. Consider diagram (4.7):

(4.7)

$$\begin{array}{ccccc}
 & & H^1(K', A[\phi]) & & \\
 & & \downarrow{\scriptstyle r_{1,\mathfrak{q}}} \quad \searrow{\scriptstyle \Upsilon'_o} & & \\
J(K'_\mathfrak{q})/\phi A(K'_\mathfrak{q}) & \xrightarrow{\delta_\phi} & H^1(K'_\mathfrak{q}, A[\phi]) & & H^1(K', B[1-\tau]) \\
 & \searrow{\scriptstyle \Upsilon_o} & & \searrow{\scriptstyle \Upsilon'_o} & \downarrow{\scriptstyle r_{1,\mathfrak{q}}} \\
 & & B(K'_\mathfrak{q})/(1-\tau)B(K'_\mathfrak{q}) & \xrightarrow{\delta_{1-\tau}} & H^1(K'_\mathfrak{q}, B[1-\tau])
\end{array}$$

That the upper parallelogram commutes is trivial. That the lower parallelogram commutes is Lemma 4.8. From Corollary 4.7, the two maps induced by Υ'_o are isomorphisms. Since K' contains ζ_{p^r} and $p^r \geq 4$, the completion of K' with respect to any infinite place is isomorphic to $\mathbb{C}$. So for infinite places, the groups $J(K'_\mathfrak{q})/\phi A(K'_\mathfrak{q})$ and $B(K'_\mathfrak{q})/(1-\tau)B(K'_\mathfrak{q})$ are trivial, hence isomorphic. From Proposition 4.10, the map induced by Υ_o on $J(K'_\mathfrak{q})/\phi A(K'_\mathfrak{q})$ is an isomorphism for all finite places. Since all maps in the commutative diagram induced by Υ_o and Υ'_o are isomorphisms, the result follows. □

5. The fake Selmer group

Let us describe an explicit way to compute $S^{\phi}(A, K')$; we primarily follow [BPS16] and [Sc2]. Though K denotes a number field, the results of this section up to and including Proposition 5.3 hold for any field of characteristic different from p.

Now Δ, considered as a finite étale $\mathcal{K}'$-scheme, is equal to Spec $L_{\mathcal{K}'}$ for the algebra $L_{\mathcal{K}'} := \mathcal{K}'[T]/(f_0(T))$. We can identify $L_{\mathcal{K}',s}$ with $\prod_{i=1}^{m} \mathcal{K}'_s$, where the image of T corresponds to $(\alpha_1, \dots, \alpha_m)$. If $\ell = (\ell_1, \dots, \ell_m) \in L_{\mathcal{K}',s}$, we define $N : L_{\mathcal{K}',s} \to \mathcal{K}'_s$ by $N(\ell) = \prod_{i=1}^{m} \ell_i^{n_i}$. Note that N is a $\mathrm{Gal}(\mathcal{K}')$-equivariant map.

The function $h \in \mathcal{K}'(X \times \Delta)$, described in the second paragraph of Section 4, is then $x - T$. We define a divisor of X to be *good* if it has degree 0, is $\mathcal{K}'$-rational, and its support does not intersect the supports of the divisors of the functions $x - \alpha_i$. Over $\mathcal{K}'_s$ we can write a good divisor as a sum of closed points $D' := \sum n_P P$, with $n_P \in \mathbb{Z}$. We define $(x - T)(D') = \prod (x(P) - T)^{n_P} \in L^{\times}_{\mathcal{K}'}$. Let $J(\mathcal{K}')/\phi A(\mathcal{K}')_0$ denote the subgroup of $J(\mathcal{K}')/\phi A(\mathcal{K}')$ that is represented by good divisors.

Proposition 5.1. *The map $x - T$ induces a well-defined homomorphism from $J(\mathcal{K}')/\phi A(\mathcal{K}')_0$ to the kernel of the norm $N : L^{\times}_{\mathcal{K}'}/(L^{\times p}_{\mathcal{K}'}\mathcal{K}'^{\times}) \to \mathcal{K}'^{\times}/\mathcal{K}'^{\times p}$.*

Proof. That $x - T$ factors through principal divisors and through $\phi A(\mathcal{K}')$ is proven in [BPS16, Cor. 6.6 and Cor. 6.15]. The proof that the image is in the kernel of $N : L^{\times}_{\mathcal{K}'}/(L^{\times p}_{\mathcal{K}'}\mathcal{K}'^{\times}) \to \mathcal{K}'^{\times}/\mathcal{K}'^{\times p}$ is essentially the same as the proof in [PS, §5 and Prop. 12.1]. □

Now let us give a cohomological interpretation of the $x - T$ map. Recall the notation in the third paragraph of Section 4. Dualizing $\hat{\alpha} : (\mathbb{Z}/p\mathbb{Z})^{\Delta}_{\deg 0} \to \hat{A}[\hat{\phi}]$ gives $\alpha : A[\phi] \to \mu_p^{\Delta}/\mu_p$. We have a short exact sequence of $\mathrm{Gal}(\mathcal{K}')$-modules, $1 \to \mu_p \to \mu_p^{\Delta} \to \mu_p^{\Delta}/\mu_p \to 1$, which leads to the long exact sequence of $\mathrm{Gal}(\mathcal{K}')$-cohomology, part of which is $\mathcal{K}'^{\times}/\mathcal{K}'^{\times p} \to L^{\times}_{\mathcal{K}'}/L^{\times p}_{\mathcal{K}'} \to H^1(\mathcal{K}', \mu_p^{\Delta}/\mu_p)$. This induces an injection $k : L^{\times}_{\mathcal{K}'}/(L^{\times p}_{\mathcal{K}'}\mathcal{K}'^{\times}) \to H^1(\mathcal{K}', \mu_p^{\Delta}/\mu_p)$.

Proposition 5.2. *Diagram* (5.1) *commutes:*

$$\begin{array}{ccc} J(\mathcal{K}')/\phi A(\mathcal{K}')_0 & \xrightarrow{x-T} & L^{\times}_{\mathcal{K}'}/(L^{\times p}_{\mathcal{K}'}\mathcal{K}'^{\times}) \\ \downarrow{\scriptstyle \delta_\phi} & & \downarrow{\scriptstyle k} \\ H^1(\mathcal{K}', A[\phi]) & \xrightarrow{\alpha} & H^1(\mathcal{K}', \mu_p^{\Delta}/\mu_p) \end{array} \tag{5.1}$$

Proof. This follows from Proposition 5.1 and [BPS16, Prop. 6.10]. □

To use diagram (5.1), we need to understand the kernel of the $x - T$ map. The proof of the following proposition can be adapted mutatis mutandis from the proof of [PS, Thm. 11.3].

Proposition 5.3. *Assume that X has a $\mathcal{K}'$-rational divisor class $\mathcal{D}$ of degree 1. Then the kernel of the $x - T$ map on $J(\mathcal{K}')/\phi A(\mathcal{K}')_0$ is generated by $(1 - \tau)(\mathcal{D})$. This kernel has order 1 if Δ has a $\mathrm{Gal}(\mathcal{K}')$-orbit of size relatively prime to p or $p = 2$, $m \equiv 2 \pmod 4$, and Δ is the disjoint union of two sets, each of size $m/2$, which, as a pair, are $\mathrm{Gal}(\mathcal{K}')$-stable. This kernel has order p otherwise.*

Let $H^1(K', A[\phi]; S)$ denote the finite subgroup of $H^1(K', A[\phi])$, unramified at places outside S. From the proof of Theorem 4.11, the completion of K' with respect to an infinite place is isomorphic to $\mathbb{C}$ and $H^1(\mathbb{C}, A[\phi]) = 0$. So we need not consider infinite places. We have

$$S^{\phi}(A, K') = \{\gamma \in H^1(K', A[\phi]; S) \mid r_{1,\mathfrak{q}}(\gamma) \in \delta_{\phi} J(K'_{\mathfrak{q}})/\phi A(K'_{\mathfrak{q}}),\ \forall \mathfrak{q} \in S\}$$

(see [Mi3, p. 92]). We now make a standard assumption for descent using divisors and functions on a curve.

Assumption 2. *The curve X has a $K'_{\mathfrak{q}}$-rational divisor class of degree 1 for each $\mathfrak{q} \in S$.*

For discussions of Assumption 2, see [BPS16, Lem. 10.2] and [Sc2, Prop. 2.7]. Note that if $X(K')$ is non-empty, then Assumption 2 holds. From [La, Lem. 3, p. 166] (and see [PS, Prop. 32]), it follows from Assumption 2 that every element of $J(K'_{\mathfrak{q}})/\phi A(K'_{\mathfrak{q}})$ is represented by a good divisor with respect to $K'_{\mathfrak{q}}$ (i.e., $J(K'_{\mathfrak{q}})/\phi A(K'_{\mathfrak{q}})_0 = J(K'_{\mathfrak{q}})/\phi A(K'_{\mathfrak{q}})$).

Let $\mathfrak{L}$ denote the subgroup of the kernel of $N : L^{\times}_{K'}/(L^{\times p}_{K'} K'^{\times}) \to K'^{\times}/K'^{\times p}$ that is unramified outside S, as described in [BPS16, §7]. For an algorithm for determining generators of $\mathfrak{L}$, see [PS, §12]. Let $r_{\mathfrak{q}} : \mathfrak{L} \to L^{\times}_{K'_{\mathfrak{q}}}/(L^{\times p}_{K'_{\mathfrak{q}}} K_{\mathfrak{q}}'^{\times})$ denote the "restriction" map that comes from the canonical embeddings of number fields into their localizations. Define $S^{\text{fake}}(A, K') := \{\ell \in \mathfrak{L} \mid r_{\mathfrak{q}}(\ell) \in (x-T)(J(K'_{\mathfrak{q}})/\phi A(K'_{\mathfrak{q}})),\ \forall \mathfrak{q} \in S\}$.

In practice, if Assumption 2 holds, then to compute $(x - T)(J(K'_{\mathfrak{q}})/\phi A(K'_{\mathfrak{q}}))$, we usually search for divisors on X, good with respect to $K'_{\mathfrak{q}}$, and compute their images in $L^{\times}_{K'_{\mathfrak{q}}}/(L^{\times p}_{K'_{\mathfrak{q}}} K_{\mathfrak{q}}'^{\times})$, where it is easiest to determine whether they are independent. Let us discuss the issue of finding enough independent good divisors. There are two ways, which have been described in the literature, for determining the size of $J(K'_{\mathfrak{q}})/\phi A(K'_{\mathfrak{q}})$, and neither is especially practical. The first is the formula $\#J(K'_{\mathfrak{q}})/\phi A(K'_{\mathfrak{q}}) = c_J \# A(K'_{\mathfrak{q}})[\phi] I / c_A$, where c_J and c_A are the Tamagawa numbers of J and A over $K'_{\mathfrak{q}}$ and I is essentially the index of the image of ϕ on formal groups. For a more precise formulation of I and a proof see [Sc1, Lem. 3.8]. The second is the algorithm described in [BPS16, §11], which also finds generators.

However, with luck, our naïve search will succeed at both determining $(x - T)(J(K'_{\mathfrak{q}})/\phi A(K'_{\mathfrak{q}}))$ and also verifying that Assumption 1 holds. First we use Proposition 5.3 to determine the dimension $d_{\ker,\mathfrak{q}}$ of the kernel of the $x - T$ map on $J(K'_{\mathfrak{q}})/\phi A(K'_{\mathfrak{q}})$. Second, we use Propositions 5.4 and 5.5 below to determine $d_{B,\mathfrak{q}} := \dim B(K'_{\mathfrak{q}})/(1-\tau)B(K'_{\mathfrak{q}})$. Recall that $\Upsilon_o : J(K'_{\mathfrak{q}})/\phi A(K'_{\mathfrak{q}}) \to B(K'_{\mathfrak{q}})/(1-\tau)B(K'_{\mathfrak{q}})$ is injective from Proposition 4.9. So if for each place $\mathfrak{q} \in S$ we can find $d_{B,\mathfrak{q}} - d_{\ker,\mathfrak{q}}$ good divisors with independent images under the $x - T$ map, then Assumption 1 holds and we have generators for each $(x-T)(J(K'_{\mathfrak{q}})/\phi A(K'_{\mathfrak{q}}))$. If our naïve search does not succeed, we can start the algorithm of [BPS16, §11] and quit when we find enough generators. Otherwise we finish the algorithm without finding enough generators and thus prove that Assumption 1 does not hold.

In the previous paragraph, we saw that we need $\dim B(K'_{\mathfrak{q}})/(1-\tau)B(K'_{\mathfrak{q}})$ for each $\mathfrak{q} \in S$.

Proposition 5.4. *Let $K'_{\mathfrak{q}}$ be a finite extension of $\mathbb{Q}_q$, $t := \operatorname{ord}_p(q)$, and let d be the dimension of B. As an $\mathbb{F}_p$-vector space we have* $\dim B(K'_{\mathfrak{q}})/(1-\tau)B(K'_{\mathfrak{q}}) = dt[K'_{\mathfrak{q}} : \mathbb{Q}'_q] + \dim B(K'_{\mathfrak{q}})[1-\tau]$.

Proof. This proof can be adapted mutatis mutandis from that for [Sc2, Cor. 3.6]. □

The proof of the following can be adapted mutatis mutandis from that for [PS, Lem. 12.9].

Proposition 5.5. *Let ℓ denote the number of distinct irreducible factors of $f_0(x)$ over $\mathcal{K}'$. Suppose that one of these factors has degree prime to p. We have* $\dim A(\mathcal{K}')[\phi] = \dim B(\mathcal{K}')[1-\tau] = \ell - 2$.

If all factors of $f(x)$ have degree divisible by p, then it is usually a straightforward computation using the Galois action on Δ to determine $\dim B(\mathcal{K}')[1-\tau]$.

Now that we can determine the group $S^{\text{fake}}(A, K')$ (under the two assumptions), we want to understand its relation to $S^{\phi}(A, K')$. The proof of the following proposition can be adapted mutatis mutandis from the proof of [PS, Thm. 13.2]. Note that k induces an injection from $S^{\text{fake}}(A, K')$ to $H^1(K', \mu_p^{\Delta}/\mu_p)$.

Proposition 5.6. *Under Assumption 2, α maps $S^{\phi}(A, K')$ onto $k(S^{\text{fake}}(A, K'))$. The kernel has order 1 if Δ has a $\mathrm{Gal}(K')$-orbit of size relatively prime to p or $p = 2$, $m \equiv 2 (\mathrm{mod}\, 4)$, and Δ is the disjoint union of two sets, each of size $m/2$, which as a pair are $\mathrm{Gal}(K')$-stable. This kernel has order p otherwise.*

Thus, given the two assumptions and Theorem 4.11, if we can compute the size of $S^{\text{fake}}(A, K')$ and the $\mathrm{Gal}(K')$-action on Δ, then we can compute the sizes of $S^{\phi}(A, K')$ and $S^{1-\tau}(B, K')$.

6. Determining the rank of $B(K)$

The following proposition tells us what follows if we can find good divisors, with respect to K', whose images under the $x - T$ map generate $S^{\text{fake}}(A, K')$.

Proposition 6.1. *Assume that X has a K'-rational degree 1 divisor class. Assume that $x - T$ is a surjective map from $J(K')$ to $S^{\text{fake}}(A, K')$. Then under Assumption 1, we have* $\dim B(K')/(1-\tau)B(K') = \dim S^{\phi}(A, K')$ *and* $\dim Ш(A, K')[\phi] = \dim Ш(B, K')[1-\tau] = 0$.

Proof. Using Propositions 5.3 and 5.6 (and see diagram (5.1)), we know that $\delta_\phi : J(K')/\phi A(K') \to S^{\phi}(A, K')$ is a surjection. So from equation (2.2), we have $Ш(A, K')[\phi] = 0$ and δ_ϕ is an isomorphism. From Lemma 4.8 and Theorem 4.11, diagram (6.1) commutes, and the map induced by Υ'_o on Selmer groups is an isomorphism:

$$\begin{array}{ccc} J(K')/\phi A(K') & \xrightarrow{\delta_\phi} & S^{\phi}(A, K') \\ \downarrow{\scriptstyle \Upsilon_o} & & \downarrow{\scriptstyle \Upsilon'_o} \\ B(K')/(1-\tau)B(K') & \xrightarrow{\delta_{1-\tau}} & S^{1-\tau}(B, K') \end{array} \tag{6.1}$$

We know that $\delta_{1-\tau}$ is injective and from Proposition 4.9 that the map induced by Υ_o is injective. So all four maps in diagram (6.1) are isomorphisms; the result follows. □

Regardless of whether $x - T : J(K')/\phi A(K') \to S^{\text{fake}}(A, K')$ is a surjective map, let us assume that we have somehow managed to determine $\dim S^{1-\tau}(B, K')$ and $\dim Ш(B, K')[1-\tau]$, and thus $\dim B(K')/(1-\tau)B(K')$ (see equation (2.2)). The

proofs of the next two propositions can be adapted, mutatis mutandis, from the proofs of [Sc2, Cor. 3.7] and [PS, Lem. 13.4], respectively (the second was suggested independently by Armand Brumer and Michael Stoll).

Proposition 6.2. *We have*

$$\operatorname{rank} B(K') = \varphi(p^r)(\dim B(K')/(1-\tau)B(K') - \dim B(K')[1-\tau]).$$

Proposition 6.3. *We have* $\operatorname{rank} B(K) = (\operatorname{rank} B(K'))/[K' : K]$.

7. Conditions implying Assumption 1

In the case that the place $\mathfrak{q} \in S$ does not lie over p, we present two conditions implying that the map $\Upsilon_o : J(K'_\mathfrak{q})/\phi A(K'_\mathfrak{q}) \to B(K'_\mathfrak{q})/(1-\tau)B(K'_\mathfrak{q})$ is a surjection.

Proposition 7.1. *Assume that $\mathfrak{q} \in S$ and does not lie over p. Let c_J and c_A be the Tamagawa numbers of J and A over $K'_\mathfrak{q}$. If $c_J \geq c_A$, then the map $\Upsilon_o : J(K'_\mathfrak{q})/\phi A(K'_\mathfrak{q}) \to B(K'_\mathfrak{q})/(1-\tau)B(K'_\mathfrak{q})$ is a surjection.*

Proof. From Proposition 5.4 we have $\#B(K'_\mathfrak{q})/(1-\tau)B(K'_\mathfrak{q}) = \#B(K'_\mathfrak{q})[1-\tau]$. We have $\#B(K'_\mathfrak{q})[1-\tau] = \#A(K'_\mathfrak{q})[\phi]$ from Proposition 4.6. From [Sc1, Lem. 3.8] we have $\#J(K'_\mathfrak{q})/\phi A(K'_\mathfrak{q}) = c_J(\#A(K'_\mathfrak{q})[\phi])/c_A$. So since $c_J \geq c_A$ we have

$$\#J(K'_\mathfrak{q})/\phi A(K'_\mathfrak{q}) \geq B(K'_\mathfrak{q})/(1-\tau)B(K'_\mathfrak{q}).$$

Since $\Upsilon_o : J(K'_\mathfrak{q})/\phi A(K'_\mathfrak{q}) \to B(K'_\mathfrak{q})/(1-\tau)B(K'_\mathfrak{q})$ is an injection from Proposition 4.9, the result follows. □

Note that if $\mathfrak{q} \in S$ does not lie over p, then from [Sc1, Lem. 3.8] we have that the finite groups $J(K'_\mathfrak{q})/(1-\tau)J(K'_\mathfrak{q})$ and $J(K'_\mathfrak{q})[1-\tau]$ have the same size.

Proposition 7.2. *Assume that $\mathfrak{q} \in S$ and does not lie over p. If $J(K'_\mathfrak{q})/(1-\tau)J(K'_\mathfrak{q}) \cong J(K'_\mathfrak{q})[1-\tau]$, then the map $\Upsilon_o : J(K'_\mathfrak{q})/\phi A(K'_\mathfrak{q}) \to B(K'_\mathfrak{q})/(1-\tau)B(K'_\mathfrak{q})$ is a surjection.*

Proof. We first want to show that $\eta(J(K'_\mathfrak{q})[1-\tau]) = A(K'_\mathfrak{q})[\phi]$. Let

$$w := \dim B(K'_\mathfrak{q})[1-\tau].$$

Note that w is determined by the $\operatorname{Gal}(K'_\mathfrak{q})$-action on Δ. Clearly $\eta(J(K'_\mathfrak{q})[1-\tau]) \cong J(K'_\mathfrak{q})[1-\tau]/J(K'_\mathfrak{q})[\eta]$. We then see from Proposition 3.5, Lemma 3.9, and the definition of η in Section 4 that $J(K'_\mathfrak{q})[1-\tau] \cong (\mathbb{Z}/p^r\mathbb{Z})^w$ and $J(K'_\mathfrak{q})[\eta] = pJ(K'_\mathfrak{q})[1-\tau] \cong (p\mathbb{Z}/p^r\mathbb{Z})^w$. Thus $\dim \eta(J(K'_\mathfrak{q})[1-\tau]) = w$. From Proposition 4.6 we have $\dim A(K'_\mathfrak{q})[\phi] = w$.

From [Sc1, Prop. 2.6] we have the following exact sequence:

$$0 \to \frac{A(K'_\mathfrak{q})[\phi]}{\eta J(K'_\mathfrak{q})[1-\tau]} \to \frac{A(K'_\mathfrak{q})}{\eta J(K'_\mathfrak{q})} \xrightarrow{\phi} \frac{J(K'_\mathfrak{q})}{(1-\tau)J(K'_\mathfrak{q})} \to \frac{J(K'_\mathfrak{q})}{\phi A(K'_\mathfrak{q})} \to 0. \tag{7.1}$$

From the previous paragraph we see that $A(K'_\mathfrak{q})[\phi]/\eta J(K'_\mathfrak{q})[1-\tau] = 0$. Since $A(K'_\mathfrak{q})/\eta J(K'_\mathfrak{q})$ has exponent p^{r-1} and injects into $J(K'_\mathfrak{q})/(1-\tau)J(K'_\mathfrak{q})$, which is isomorphic to $(\mathbb{Z}/p^r\mathbb{Z})^w$, we see that $\#A(K'_\mathfrak{q})/\eta J(K'_\mathfrak{q}) \leq p^{w(r-1)}$. From [Sc1, Lem. 3.8] we have $\#A(K'_\mathfrak{q})/\eta J(K'_\mathfrak{q}) = c_A(\#J(K'_\mathfrak{q})[\eta])/c_J = p^{w(r-1)}c_A/c_J$. Thus $c_A \leq c_J$, and the result follows from Proposition 7.1. □

8. Chabauty computations

Assume that X has a K-rational degree 1 divisor, namely D_1. If $\operatorname{rank} J(K) < \dim J$, then we can do a straightforward Chabauty computation (described in [PSS, §12.2] and [MP]), possibly combined with a Mordell-Weil sieve (described in [BE] and [ES], and more fully in [PSS, §12.1]). With luck, the upper bound it gives on $\#X(K)$ is realized by known rational points. It is possible that $\operatorname{rank} J(K) \geq \dim(J)$, but $\operatorname{rank} B(K) < \dim(B)$. In this section, we assume that $\operatorname{rank} B(K) < \dim B$. We would like to adapt a Chabauty argument to this situation. We describe only what differs from standard Chabauty computations.

Proposition 8.1. *The curve X has genus $\frac{1}{2}(p^r-1)(m-2)$. A basis for the holomorphic differentials is $U := \{\frac{x^i dx}{y^j} \mid 1 \leq j \leq p^r-1,\ 0 \leq i \leq \frac{mj}{p^r}-2\}$. A basis for the set of holomorphic differentials in the kernel of $\Phi_{p^r}(\tau)^*$, and in the image of Υ^*, is $U_B := \{\frac{x^i dx}{y^j} \in U \mid p \nmid j\}$. A basis for the set of holomorphic differentials in the kernel of Υ^*, and in the image of $\Phi_{p^r}(\tau)^*$, is $\{\frac{x^i dx}{y^j} \in U \mid p|j\}$.*

Proof. Straightforward computations show that $\operatorname{div}(dx) = (\sum_{\ell=1}^m (p^r-1)(\alpha_\ell, 0)) - 2\infty$, $\operatorname{div}(x) = D' - \infty$ (for an effective divisor D' of degree p^r) and $\operatorname{div}(y) = (\sum_{\ell=1}^m n_\ell(\alpha_\ell, 0)) - \frac{n}{p^r}\infty$. The genus can be computed from the degree of the canonical divisor $\operatorname{div}(dx)$. The basis for the holomorphic differentials can be computed from the three divisors above using techniques found in [Si, §II.4] (these are not original results). A straightforward computation with roots of unity and cyclotomic polynomials gives the results for the images and kernels of $\Phi_{p^r}(\tau)^*$ and Υ^*. □

To do a Chabauty computation, we would like a map from X to B over K. Define $\iota_{D_1} : X \hookrightarrow J$ by $P \mapsto [P - D_1]$. We can compose this with Υ_o, but Υ_o is not, in general, defined over K. Michael Stoll suggested that we use $\tilde{B} := J/(J[\Upsilon])$ instead. Since the image of Υ is defined over K, so is its kernel. Thus $\tilde{B}$ is defined over K (it is a twist of B).

Proposition 8.2. *We have* $\operatorname{rank} B(K) = \operatorname{rank} \tilde{B}(K)$.

Proof. Since both B/K and $\tilde{B}/K$, when base extended to K', are isomorphic to B/K', the proof of Proposition 6.3 shows that both $B(K)$ and $\tilde{B}(K)$ have rank equal to $(\operatorname{rank} B(K'))/[K' : K]$. □

Let $\tilde{\Upsilon}_o : J \to \tilde{B}$ be the quotient map. We note that ι_{D_1} and $\tilde{\Upsilon}_o$ are both defined over K. Their composition gives a map $\tilde{\Upsilon}_o \iota_{D_1} : X \to \tilde{B}$ that is defined over K. In addition, if the Chabauty condition holds for B, then it also does for $\tilde{B}$, as shown in Proposition 8.2. So $\tilde{\Upsilon}_o \iota_{D_1}$ can be used for a Chabauty computation.

Now let us explain which differentials should be used for the Chabauty computation. Note that $\Phi_{p^r}(\tau) \in (\operatorname{End}(J))(K)$.

Lemma 8.3. *The abelian variety $\Phi_{p^r}(\tau)J$ has finite index in $J[\Upsilon]$.*

Proof. From the proof of Lemma 3.6, we have that $\Upsilon \Phi_{p^r}(\tau) = 0$ on J, so $\Phi_{p^r}(\tau)J \subseteq J[\Upsilon]$. From Proposition 8.1, we have $\dim \Phi_{p^r}(\tau)J = \dim J[\Upsilon]$. □

For a variety W, let $\Omega^1(W)$ denote the space of holomorphic differentials on W.

Proposition 8.4. *The vector space $\Omega^1(\tilde{B})$ is isomorphic under the induced map $\tilde{\Upsilon}_o^*$ to the kernel of the map $\Phi_{p^r}(\tau)^*$ on $\Omega^1(J)$ over K.*

Proof. From Lemma 8.3, the image of $\Phi_{p^r}(\tau) : J \to J$ has finite index in the kernel of the quotient map $\tilde{\Upsilon}_o : J \to \tilde{B}$. Both of these maps are defined over K, and so are the maps they induce on differentials. Thus we have an exact sequence $0 \to \Omega^1(\tilde{B}) \xrightarrow{\tilde{\Upsilon}_o^*} \Omega^1(J) \xrightarrow{\Phi_{p^r}(\tau)^*} \Omega^1(J)$ of $\mathrm{Gal}(K)$-modules. □

The injection $\iota_{D_1} : X \to J$ induces an isomorphism $\iota_{D_1}^* : \Omega^1(J) \to \Omega^1(X)$ (see [Mi2, Prop. 2.2]).

Corollary 8.5. *The differentials in U_B (described in Proposition 8.1) form a basis for $\iota_{D_1}^* \tilde{\Upsilon}_o^* \Omega^1(\tilde{B})$.*

So to do a Chabauty computation, we need a subgroup of finite index in any subgroup of $J(K)$ that maps onto $\tilde{B}(K)$ and use only the differentials in U_B. From there, we can use the techniques described in [PSS, §12] and [MP]. We do an example at the end of Section 9.

9. Example

All computations were done with Magma (see [BCP]) and GP-PARI. In this section we use i to denote a choice of $\sqrt{-1}$.

Proposition 9.1. *Let $X/\mathbb{Q}$ be the curve with an affine model $y^4 = 2x^4 + x^3 + 1$. Let J be its Jacobian and let B be the 2-dimensional abelian variety $(1+\tau)J$ where τ is induced by $(x, y) \mapsto (x, iy)$. We have $B(\mathbb{Q}) \cong \mathbb{Z}$, $J(\mathbb{Q}) \cong \mathbb{Z}^3$, and*

$$X(\mathbb{Q}) = \{(0, -1), (0, 1), (-1/2, -1), (-1/2, 1)\}.$$

These results could probably be determined by combining the Chabauty computation with the techniques found in [BPS16, §12] as well (though our result is unconditional). This is just an example, however, and it is clear that our techniques would be much simpler than those found in [BPS16] for most prime power cyclic covers of the projective line.

Proof. The curve X is a double cover of the genus 1 curve E given by $v^2 = 2x^4 + x^3 + 1$. With the base point $(x, v) = (0, 1)$, we see that E is an elliptic curve, and Magma shows that $E(\mathbb{Q}) \cong \mathbb{Z}^2$. From Lemma 3.7, B has dimension 2. From the results in Section 11, we have that J is isogenous over $\mathbb{Q}$ to $E \oplus B$.

We have $\mathbb{Q}' = \mathbb{Q}(i)$. Since $X(\mathbb{Q}(i))$ is not empty, Assumption 2 holds and X has a degree 1 divisor class defined over $\mathbb{Q}(i)$. We have $L(= L_{\mathbb{Q}(i)}) = \mathbb{Q}(i)[T]/(2T^4 + T^3 + 1)$, which is isomorphic to a degree 8 number field over $\mathbb{Q}$. The discriminant of $2x^4 + x^3 + 1$ is $43 \cdot 47$; both places 43 and 47 are inert in $\mathbb{Q}(i)$, so we take $S = \{1 + i, 43, 47\}$. We need to find a basis for $\mathfrak{L}$, the subgroup of the kernel of $N : L^\times/(L^{\times 2}\mathbb{Q}(i)^\times) \to \mathbb{Q}(i)^\times/\mathbb{Q}(i)^{\times 2}$ that is unramified outside S. We let t be a generator of L with minimal polynomial $z^8 + 4z^4 + z^2 + 4$ over $\mathbb{Q}$.

The field L has class number 1 and unit group isomorphic to $(\mathbb{Z}/4\mathbb{Z}) \oplus \mathbb{Z}^3$, generated by $i = -\frac{1}{2}t^7 - t^3 - \frac{1}{2}t$, $u_2 = t^6 + t^2 - 1$, $u_3 = -t^7 + t^6 + t^5 - t^4 - 3t^3 + 3t^2 - 3$, and $u_4 = -\frac{3}{2}t^7 - 2t^6 - t^5 + t^4 - 3t^3 - 5t^2 - \frac{9}{2}t$, and their norms in $\mathbb{Q}(i)$ are 1, i, 1, and 1, respectively.

The prime ideal $\langle 1 + i \rangle$ of $\mathbb{Z}[i]$ splits into three prime ideals of L with $(e, f) = (1, 1)$, $(1, 1)$ and $(1, 2)$ (this is the standard notation from algebraic number theory and abuses our earlier notation f). They are generated by $\alpha_{2,1} = -t^5 - 2t - 1$,

$\alpha_{2,2} = \frac{1}{2}t^7 + t^3 + \frac{3}{2}t + 1$, and $\alpha_{2,3} = \frac{1}{2}t^7 - t^5 + t^4 + t^3 - \frac{3}{2}t + 2$, and their norms in $\mathbb{Q}(i)$ are $-1+i$, $-1-i$, and 2, respectively.

The prime ideal $\langle 43\rangle$ of $\mathbb{Z}[i]$ splits into three prime ideals of L with $(e,f) = (1,1)$, $(1,1)$ and $(2,1)$. They are generated by $\alpha_{43,1} = -\frac{1}{2}t^7 - t^5 - \frac{1}{2}t$, $\alpha_{43,2} = -t^6 + 2t^4 - t^2 + 3$, and $\alpha_{43,3} = -\frac{1}{2}t^7 - t^5 - \frac{5}{2}t$, respectively. All three have norm 43 in $\mathbb{Q}(i)$.

The prime ideal $\langle 47\rangle$ of $\mathbb{Z}[i]$ splits into three prime ideals of L with $(e,f) = (1,1)$, $(1,1)$ and $(2,1)$. They are generated by $\alpha_{47,1} = -\frac{1}{2}t^7 + t^6 - t^4 - t^3 + t^2 + \frac{5}{2}t - 4$, $\alpha_{47,2} = \frac{1}{2}t^7 + \frac{3}{2}t$, and $\alpha_{47,3} = \frac{1}{2}t^7 - t^6 + t^5 + t^4 + t^3 - 2t^2 + \frac{3}{2}t + 4$, and their norms in $\mathbb{Q}(i)$ are $-47i$, 47, and 47, respectively.

By factoring $1+i$, 43, and 47 over L, we note that the subgroup of the kernel of $N : L^\times/L^{\times 2} \to \mathbb{Q}(i)^\times/\mathbb{Q}(i)^{\times 2}$, represented by elements in $\mathbb{Q}(i)^\times$, is generated by i, $\alpha_{2,1}\alpha_{2,2}\alpha_{2,3}$, $u_3\alpha_{43,1}\alpha_{43,2}$, and $u_2u_4\alpha_{47,1}\alpha_{47,2}$. So $\mathfrak{L} = \langle u_3,\ u_4,\ u_2\alpha_{2,1}\alpha_{2,2},\ \alpha_{43,1}\alpha_{43,3},\ \alpha_{47,2}\alpha_{47,3}\rangle$.

By Propositions 5.4 and 5.5 we have $\dim B(\mathbb{Q}_2(i))/(1-\tau)B(\mathbb{Q}_2(i)) = 3$, $\dim B(\mathbb{Q}_{43}(i))/(1-\tau)B(\mathbb{Q}_{43}(i)) = 1$, and $\dim B(\mathbb{Q}_{47}(i))/(1-\tau)B(\mathbb{Q}_{47}(i)) = 1$.

For $q = 2$, 43, and 47, let $L_q\ (= L_{\mathbb{Q}_q(i)}) = \mathbb{Q}_q(i)[T]/(2T^4 + T^3 + 1)$. There are points in $X(\mathbb{Q}_2(i))$ with x-coordinates $x_{2,1} := 4$, $x_{2,2} := 2i - 6$, and $x_{2,3} := -148988195836032i + 838728979062199118312846942 93$. The images of $[(x_{2,j}, y_{2,j}) - (0,1)]$ for $1 \le j \le 3$ by the map $x - T$ are independent in $L_2^\times/(L_2^{\times 2}\mathbb{Q}_2(i)^\times)$. From Proposition 5.3, the kernel of $x - T$ on $J(\mathbb{Q}_2(i))/\phi A(\mathbb{Q}_2(i))$ is trivial. Since $\dim B(\mathbb{Q}_2(i))/(1-\tau)B(\mathbb{Q}_2(i)) = 3$, the part of Assumption 1 for the place over 2 holds (see the discussion before Proposition 5.4).

Similarly for each place $q \in \{43, 47\}$, the kernel of $x - T$ on $J(\mathbb{Q}_q(i))/\phi A(\mathbb{Q}_q(i))$ is trivial. Since $\dim B(\mathbb{Q}_q(i))/(1-\tau)B(\mathbb{Q}_q(i)) = 1$ in both cases, from Proposition 4.10 we need to find single generators for each $J(\mathbb{Q}_q(i))/\phi A(\mathbb{Q}_q(i))$. There is a point in $X(\mathbb{Q}_{43}(i))$ with x-coordinate $18i + 34$. The image of $[(18i + 34, y_{43}) - (0,1)]$ by the map $x - T$ is non-trivial in $L_{43}^\times/(L_{43}^{\times 2}\mathbb{Q}_{43}(i)^\times)$. There is a point in $X(\mathbb{Q}_{47}(i))$ with x-coordinate 25. The image of $[(25, y_{47}) - (0,1)]$ by the map $x - T$ is non-trivial in $L_{47}^\times/(L_{47}^{\times 2}\mathbb{Q}_{47}(i)^\times)$. Thus Assumption 1 holds, and we have found the local images of $x - T$ for all relevant places.

A computation shows that only the trivial element of $\mathfrak{L}$ restricts to the image of $J(\mathbb{Q}_q(i))/\phi A(\mathbb{Q}_q(i))$ by $x - T$ for all three places. So we have $\dim S^{\mathrm{fake}}(A, \mathbb{Q}(i)) = 0$, and from Proposition 5.6 and Theorem 4.11 we have

$$\dim S^{\phi}(A, \mathbb{Q}(i)) = \dim S^{1-\tau}(B, \mathbb{Q}(i)) = 1.$$

In addition, from Proposition 6.1, $\dim Ш(B, \mathbb{Q}(i))[1-\tau] = \dim Ш(A, \mathbb{Q}(i))[\phi] = 0$ and $\dim B(\mathbb{Q}(i))/(1-\tau)B(\mathbb{Q}(i)) = 1$. We have $\dim B(\mathbb{Q}(i))[1-\tau] = 0$, so from Proposition 6.2, the rank of $B(\mathbb{Q}(i))$ is 2. From Proposition 6.3, the rank of $B(\mathbb{Q})$ is 1.

We have $\#J(\mathbb{F}_5) = 7 \cdot 37$ and $\#J(\mathbb{F}_{11}) = 2^5 \cdot 3^4$, so the torsion subgroups of $J(\mathbb{Q})$ and of $B(\mathbb{Q})$ are trivial. Thus $B(\mathbb{Q}) \cong \mathbb{Z}$ and $J(\mathbb{Q}) \cong \mathbb{Z}^3$.

Let $X(\mathbb{Q})_k := \{(0,1), (0,-1), (-1/2, 1), (-1/2, -1)\}$ be the set of known rational points on X. We cannot determine the set $X(\mathbb{Q})$ from $E(\mathbb{Q})$, since $E(\mathbb{Q})$ is not finite, nor from a Chabauty argument using $J(\mathbb{Q})$ alone, with no consideration of its factors, since $J(\mathbb{Q})$ has rank 3 and J has dimension 3. We can do Chabauty computations using the fact that the rank of $\tilde{B}(\mathbb{Q})$ is 1 (from Proposition 8.2) and the dimension of $\tilde{B}$ is 2. We have four known points in $X(\mathbb{Q})$, and the Chabauty computation using $\mathbb{Q}_3$ shows that $\#X(\mathbb{Q}) \le 6$. So we try another local field.

It turns out that a Mordell-Weil sieve computation combined with a Chabauty computation using $\mathbb{Q}_7$ proves that $\#X(\mathbb{Q}) \leq 4$. We outline these computations.

Let $J(\mathbb{Q})_k$ denote the subgroup of $J(\mathbb{Q})$ generated by points in $X(\mathbb{Q})_k$. We do a Mordell-Weil sieve construction to prove that 5 does not divide the index of $\tilde{\Upsilon}_0(J(\mathbb{Q})_k)$ in $\tilde{B}(\mathbb{Q})$. For readability, for any abelian group G and positive integer m, we denote G/mG by G/m.

For any appropriate field F, there is an isomorphism β over $F' = F(i)$ making diagram (9.1) commute:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & J[\Upsilon] & \longrightarrow & J & \xrightarrow{\tilde{\Upsilon}_0} & \tilde{B} & \longrightarrow & 0 \\ & & \Big\downarrow{\scriptstyle =} & & \Big\downarrow{\scriptstyle =} & & \Big\downarrow{\scriptstyle \beta} & & \\ 0 & \longrightarrow & J[\Upsilon] & \longrightarrow & J & \xrightarrow{\Upsilon_o} & B & \longrightarrow & 0 \end{array} \tag{9.1}$$

Now $5 \not| \, \#J(\mathbb{F}_{13})$, so $5 \not| \, \#B(\mathbb{F}_{13})$, and thus $B(\mathbb{Q}(i))[5] = \tilde{B}(\mathbb{Q}(i))[5] = 0$. So $\tilde{B}(\mathbb{Q})[5] = 0$. Since $\tilde{B}(\mathbb{Q})$ has rank 1, we see that $\tilde{B}(\mathbb{Q})/5$ is 1-dimensional as an $\mathbb{F}_5$-vector space.

We have $J(\mathbb{F}_9) \cong \mathbb{Z}/40 \times \mathbb{Z}/40$. The image of

$$\Upsilon_o[(0,-1) - (0,1)] = (1+\tau)[(0,-1) - (0,1)]$$

in $J(\mathbb{F}_9)/5$, and hence in $B(\mathbb{F}_9)/5$, is non-trivial. From diagram (9.1), the image of $\tilde{\Upsilon}_0([(0,-1) - (0,1)])$ is non-trivial in $\tilde{B}(\mathbb{F}_9)/5$, and hence in $\tilde{B}(\mathbb{F}_3)/5$. We have homomorphisms $\tilde{\Upsilon}_0(J(\mathbb{Q})_k)/5 \to \tilde{B}(\mathbb{Q})/5 \to \tilde{B}(\mathbb{F}_3)/5$, which are induced by inclusion and reduction, respectively. From the above, the image of $\tilde{\Upsilon}_0([(0,-1) - (0,1)])$ is then non-trivial in $\tilde{\Upsilon}_0(J(\mathbb{Q})_k)/5$ and $\tilde{B}(\mathbb{Q})/5$. Since $\tilde{B}(\mathbb{Q})/5$ is 1-dimensional as an $\mathbb{F}_5$-vector space, we see that 5 does not divide the index of $\tilde{\Upsilon}_0(J(\mathbb{Q})_k)$ in $\tilde{B}(\mathbb{Q})$.

The following is a commutative diagram:

$$\begin{array}{ccccccccccc} X(\mathbb{Q}) & \xrightarrow{\iota_{(0,1)}} & J(\mathbb{Q}) & \xrightarrow{\tilde{\Upsilon}_0} & \tilde{B}(\mathbb{Q}) & \longrightarrow & \tilde{B}(\mathbb{Q}(i)) & \xrightarrow{\beta} & B(\mathbb{Q}(i)) & & \frac{\mathbb{Z}}{600} \times \frac{\mathbb{Z}}{200} \longrightarrow \frac{\mathbb{Z}}{5} \\ \Big\downarrow & & \Big\downarrow & & \Big\downarrow & & \Big\downarrow & & \Big\downarrow & & \Big\uparrow \\ X(\mathbb{F}_7) & \xrightarrow{\iota_{(0,1)}} & J(\mathbb{F}_7) & \xrightarrow{\tilde{\Upsilon}_0} & \tilde{B}(\mathbb{F}_7) & \longrightarrow & \tilde{B}(\mathbb{F}_{49}) & \xrightarrow{\beta} & B(\mathbb{F}_{49}) & \xrightarrow{\iota} & J(\mathbb{F}_{49}) \end{array} \tag{9.2}$$

where all arrows pointing down are reduction maps, the maps on $\tilde{B}(\mathbb{Q})$ and $\tilde{B}(\mathbb{F}_7)$ are the obvious inclusion maps, the map on $J(\mathbb{F}_{49})$ is an isomorphism that Magma chose, and the map on $\mathbb{Z}/600 \times \mathbb{Z}/200$ is a surjective homomorphism that we chose. Note that all arrows in diagram (9.2) are homomorphisms except for the leftmost three. The four points in $X(\mathbb{Q})_k$ reduce to four distinct points in $X(\mathbb{F}_7)$, which we denote $X(\mathbb{F}_7)_k$. We use $X(\mathbb{F}_7)_u$ to denote the other eight points in $X(\mathbb{F}_7)$. A computation shows, in diagram (9.2), that the image of the subset $X(\mathbb{F}_7)_k$ of $X(\mathbb{F}_7)$ in $\mathbb{Z}/5$ is 0. Therefore the image of the subgroup $J(\mathbb{Q})_k$ of $J(\mathbb{Q})$ in $\mathbb{Z}/5$ is 0. Since 5 does not divide the index of $\tilde{\Upsilon}_0(J(\mathbb{Q})_k)$ in $\tilde{B}(\mathbb{Q})$, the image of $\tilde{B}(\mathbb{Q})$, and therefore of $X(\mathbb{Q})$, is also 0. The image of the subset $X(\mathbb{F}_7)_u$ of $X(\mathbb{F}_7)$ in $\mathbb{Z}/5$ does not contain 0. Thus, any point $R \in X(\mathbb{Q})$ reduces, modulo 7, to a point in $X(\mathbb{F}_7)_k$.

From Proposition 8.1 and Corollary 8.5, the set $\{\frac{dx}{y^3}, \frac{xdx}{y^3}\}$ is a basis for $\iota_{(0,1)}^* \tilde{\Upsilon}_0^* \Omega^1(\tilde{B})$. We integrated each differential from $(0,-1)$ to $(0,1)$ over $\mathbb{Q}_7$ and found that the differential $\frac{(3+O(7)+x)dx}{y^3}$ kills the Mordell-Weil group $\tilde{B}(\mathbb{Q})$. Using

this differential, we were able to show that there is at most one x-coordinate for a point of $X(\mathbb{Q})$ in the modulo 7 residue class of each of the four known points in $X(\mathbb{Q})$. □

10. Directions for future work

(1) Generalize the results of this article to curves of the form $y^{p^r} = f(x)$, where p divides the multiplicity of some roots of f. See Section 12 for a discussion.

(2) Adapt the results of [SvL] to the curves in this article so that functions on the curve can be used to determine the entire Selmer group, not just the fake Selmer group.

11. Appendix A - Isogenous subabelian varieties

In this section, we consider more than one curve, so we make the notation more specific. Assume d, e, n are positive integers with $d|e$ and $e|n$. Let K be a field of characteristic not dividing e. Define X_e/K as $y^e = f(x)$ where f is a polynomial over K of degree n. Assume $f(x) = a_n \prod_{i=1}^{m}(x-\alpha_i)^{n_i}$ with $\gcd(e, n_i) = 1$ for each i. Let J_e be the Jacobian of X_e. Let $\tau_e(x, y) = (x, \zeta_e y)$, $\Upsilon_{e,d} := \prod_{\ell|e,\ell\neq 1,d} \Phi_\ell(\tau_e)$, and $B_{e,d} := \Upsilon_{e,d} J_e$. By replacing e by d everywhere we can define X_d, J_d, τ_d (where we choose $\zeta_d = \zeta_e^{e/d}$), $\Upsilon_{d,d}$, and $B_{d,d}$. (For improved notation, we could use a different variable instead of y in the equation for X_d.) In this appendix, we show that $B_{e,d}$ and $B_{d,d}$ are isogenous over K.

Let $\pi : X_e \to X_d$ by $\pi(x, y) = (x, y^{e/d})$, which induces $\pi_* : J_e \to J_d$ and $\pi^* : J_d \to J_e$.

Lemma 11.1. *The map π^* has finite kernel.*

Proof. Let D be a degree 0 divisor on X_d with the property that $\pi^*([D]) = 0$. Thus $\pi_*\pi^*([D]) = \frac{e}{d}[D] = 0$ and $[D] \in J_d[\frac{e}{d}]$. (This is not an original result.) □

Lemma 11.2. *We have $\pi^*(B_{d,d}) \subseteq B_{e,d}$.*

Proof. We first consider how π^* acts on a divisor. Let D be a divisor on X_d. Let $\pi^{-1}(D)$ denote a divisor on X_e such that $\pi_*\pi^{-1}(D) = D$. Define $\gamma := (1+\tau_e^d+\tau_e^{2d}+\ldots+\tau_e^{e-d})$. We note that $\pi^*(D) = \gamma\pi^{-1}(D)$. Clearly $\gamma(1+\tau_e+\ldots+\tau_e^{d-1}) = (1+\tau_e+\ldots+\tau_e^{e-1})$, i.e., $\gamma \prod_{\ell|d,\ell\neq 1} \Phi_\ell(\tau_e) = \prod_{\ell|e,\ell\neq 1} \Phi_\ell(\tau_e)$. Thus $\gamma = \prod_{\ell|e,\ell\nmid d} \Phi_\ell(\tau_e)$.

Next we consider how π^* acts on divisors in the image of $\Upsilon_{d,d}$. Let E be a degree 0 divisor on X_d. Make a choice for $\pi^{-1}(E)$. Since $\pi_*\tau_e = \tau_d\pi_*$ we can then take $\pi^{-1}\Upsilon_{d,d}(E)$ to be $(\prod_{\ell|d,\ell\neq 1,d} \Phi_\ell(\tau_e))\pi^{-1}(E)$ (recall that $\pi_*\pi^{-1}(D) = D$). Therefore $\pi^*\Upsilon_{d,d}(E) = \gamma\pi^{-1}\Upsilon_{d,d}(E) = (\prod_{\ell|e,\ell\nmid d} \Phi_\ell(\tau_e))(\prod_{\ell|d,\ell\neq 1,d} \Phi_\ell(\tau_e))\pi^{-1}(E)$ $= (\prod_{\ell|e,\ell\neq 1,d}(\tau_e))\pi^{-1}(E) = \Upsilon_{e,d}\pi^{-1}(E)$. □

Lemma 11.3. *We have* $\dim B_{d,d} = \dim B_{e,d} = \frac{\varphi(d)(m-2)}{2}$.

Proof. See [LT, Lem. 3.13]. □

Theorem 11.4. *The map $\pi^* : B_{d,d} \to B_{e,d}$ induces an isogeny of abelian varieties over K.*

Proof. This follows from Lemmas 11.1, 11.2, 11.3, and the fact that π is defined over K. □

Corollary 11.5. *The ranks of $B_{d,d}(K)$ and $B_{e,d}(K)$ are the same.*

Consider the curve X_{p^t} for some integer $t > 1$. From the proof of [LT, Prop. 3.12], we have that J_{p^t} is isogenous over K to $\bigoplus_{r=1}^{t} B_{p^t,p^r}$. From Theorem 11.4 we see that J_{p^t} is isogenous over K to $\bigoplus_{r=1}^{t} B_{p^r,p^r}$. So the rank of $J_{p^t}(K)$ is the sum of the ranks of the $B_{p^r,p^r}(K)$, which, with this article, we now have some hope of determining.

12. Appendix B - Roots of $f(x)$ of multiplicity a multiple of p

If p divides the multiplicity of a root of $f(x)$ it can lead to significant geometric differences. For example, the curve $X/\mathbb{Q}$ given by $y^8 = x^4 + x + 1$ is isomorphic to the curve $v^8 = u^8 + u^7 + u^4$, where the right hand side has a root of multiplicity 4. Magma shows that $J[1-\tau] \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z}$, and not $(\mathbb{Z}/8\mathbb{Z})^3$.

References

[BCP] Wieb Bosma, John Cannon, and Catherine Playoust, *The Magma algebra system. I. The user language*, Computational algebra and number theory (London, 1993), J. Symbolic Comput. **24** (1997), no. 3-4, 235–265, DOI 10.1006/jsco.1996.0125. MR1484478

[BE] Nils Bruin and Noam D. Elkies, *Trinomials $ax^7 + bx + c$ and $ax^8 + bx + c$ with Galois groups of order 168 and $8 \cdot 168$*, Algorithmic number theory (Sydney, 2002), Lecture Notes in Comput. Sci., vol. 2369, Springer, Berlin, 2002, pp. 172–188, DOI 10.1007/3-540-45455-1_14. MR2041082

[BPS16] Nils Bruin, Bjorn Poonen, and Michael Stoll, *Generalized explicit descent and its application to curves of genus 3*, Forum Math. Sigma **4** (2016), e6, 80, DOI 10.1017/fms.2016.1. MR3482281

[ES] Dennis Eriksson and Victor Scharaschkin, *On the Brauer-Manin obstruction for zero-cycles on curves*, Acta Arith. **135** (2008), no. 2, 99–110, DOI 10.4064/aa135-2-1. MR2453526

[La] Serge Lang, *Abelian varieties*, Springer-Verlag, New York-Berlin, 1983. Reprint of the 1959 original. MR713430

[LT] Dino Lorenzini and Thomas J. Tucker, *Thue equations and the method of Chabauty-Coleman*, Invent. Math. **148** (2002), no. 1, 47–77, DOI 10.1007/s002220100186. MR1892843

[MP] William McCallum and Bjorn Poonen, *The method of Chabauty and Coleman* (English, with English and French summaries), Explicit methods in number theory, Panor. Synthèses, vol. 36, Soc. Math. France, Paris, 2012, pp. 99–117. MR3098132

[Mi1] J. S. Milne, *Abelian varieties*, Arithmetic geometry (Storrs, Conn., 1984), Springer, New York, 1986, pp. 103–150. MR861974

[Mi3] J. S. Milne, *Arithmetic duality theorems*, Perspectives in Mathematics, vol. 1, Academic Press, Inc., Boston, MA, 1986. MR881804

[Mi2] J. S. Milne, *Jacobian varieties*, Arithmetic geometry (Storrs, Conn., 1984), Springer, New York, 1986, pp. 167–212. MR861976

[PS] 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. MR1465369

[PSS] Bjorn Poonen, Edward F. Schaefer, and Michael Stoll, *Twists of $X(7)$ and primitive solutions to $x^2+y^3 = z^7$*, Duke Math. J. **137** (2007), no. 1, 103–158, DOI 10.1215/S0012-7094-07-13714-1. MR2309145

[Sc1] Edward F. Schaefer, *Class groups and Selmer groups*, J. Number Theory **56** (1996), no. 1, 79–114, DOI 10.1006/jnth.1996.0006. MR1370197

[Sc2] Edward F. Schaefer, *Computing a Selmer group of a Jacobian using functions on the curve*, Math. Ann. **310** (1998), no. 3, 447–471, DOI 10.1007/s002080050156. MR1612262

[Si] Joseph H. Silverman, *The arithmetic of elliptic curves*, Graduate Texts in Mathematics, vol. 106, Springer-Verlag, New York, 1986. MR817210

[SvL] Michael Stoll and Ronald van Luijk, *Explicit Selmer groups for cyclic covers of $\mathbb{P}^1$*, Acta Arith. **159** (2013), no. 2, 133–148, DOI 10.4064/aa159-2-4. MR3062912

Department of Mathematics and Computer Science, Santa Clara University, Santa Clara, California 95053

Email address: eschaefer@scu.edu