J. Inst. Math. Jussieu (2025), **24**(2), 481–502
doi:10.1017/S1474748024000392

ARBITRARILY LARGE p-TORSION IN TATE-SHAFAREVICH GROUPS

BY E. VICTOR FLYNN[1] AND ARI SHNIDMAN[2], WITH AN APPENDIX BY TOM FISHER[3]

[1] *Mathematical Institute, University of Oxford, Andrew Wiles Building, Radcliffe Observatory Quarter, Woodstock Road, Oxford OX2 6GG, United Kingdom*
(flynn@maths.ox.ac.uk)

[2] *Einstein Institute of Mathematics, Hebrew University of Jerusalem, Givat Ram. Jerusalem, 9190401, Israel*
(ari.shnidman@gmail.com)

[3] *University of Cambridge, DPMMS, Centre for Mathematical Sciences, Wilberforce Road, Cambridge CB3 0WB, UK*
(T.A.Fisher@dpmms.cam.ac.uk)

(Received 14 October 2023; revised 10 September 2024; accepted 16 September 2024; first published online 12 November 2024)

Abstract We show that, for any prime p, there exist absolutely simple abelian varieties over $\mathbb{Q}$ with arbitrarily large p-torsion in their Tate-Shafarevich groups. To prove this, we construct explicit μ_p-covers of Jacobians of curves of the form $y^p = x(x-1)(x-a)$ which violate the Hasse principle. In the appendix, Tom Fisher explains how to interpret our proof in terms of a Cassels-Tate pairing.

1. Introduction

An algebraic variety Y over $\mathbb{Q}$ *violates the Hasse principle* if $Y(\mathbb{Q}) = \emptyset$ despite the fact that $Y(\mathbb{Q}_p) \neq \emptyset$ for all completions $\mathbb{Q}_p$ of $\mathbb{Q}$, including the archimedean completion $\mathbb{Q}_\infty = \mathbb{R}$. The Hasse-Minkowski theorem shows that quadrics in $\mathbb{P}^n$ never violate the Hasse principle, but violations do exist in higher degree. Some early examples include the hyperelliptic curve $2y^2 = x^4 - 17$ studied by Lind and Reichardt [24, 33] and Selmer's plane cubic

Keywords: Tate-Shafarevich group; abelian variety

2020 Mathematics Subject Classification: Primary 11G30
Secondary 11G10; 14H40

$3x^3+4y^3+5z^3=0$ [35]. Each of these is a genus one curve C, and is therefore a torsor for its Jacobian, the elliptic curve $E=\mathrm{Pic}^0(C)$. The fact that C violates the Hasse principle means that it represents a nontrivial element $[C]$ in the Tate-Shafarevich group Ш(E) parameterizing locally trivial E-torsors. The order of $[C]$ in Ш(E) is, in these cases, equal to the minimum positive degree of an effective 0-cycle – hence 2 in the first example and 3 in the second.

There are by now many other examples of nontrivial elements of Tate-Shafarevich groups of elliptic curves. However, it is an open question whether for every prime p there exists an elliptic curve $E/\mathbb{Q}$ with a class of order p in Ш(E). Geometrically, such E-torsors are realized as genus one curves $C\subset\mathbb{P}^{p-1}_{\mathbb{Q}}$ contained in no hyperplane, which violate the Hasse principle. The lack of a systematic construction of order p elements is somewhat surprising, since heuristics of Delaunay predict that for a given prime p, the probability that a random elliptic curve E satisfies Ш$(E)[p]\neq 0$ should be positive [11].

More generally, for any abelian variety $A/\mathbb{Q}$, the group Ш(A) parameterizes A-torsors which violate the Hasse principle. Like the 1-dimensional case of elliptic curves, there are few examples with Ш$(A)[p]\neq 0$ for large primes p, beyond examples where $A=\mathrm{Res}^F_{\mathbb{Q}}B$ is the Weil restriction of an abelian variety B over a number field F with Ш$(B)[p]\neq 0$ (see, for example, [9, 18, 19]). However, the second author and Weiss [37] recently showed that for every prime p, there exist *absolutely simple* abelian varieties A over $\mathbb{Q}$ with Ш$(A)[p]\neq 0$. They prove such A exist among the quadratic twists of quotients of modular Jacobians $J_0(N)$ with prime level $N\equiv 1 \pmod p$, but the proof does not yield explicit examples.

1.1. Results

Our first main result is an explicit construction of A-torsors X which violate the Hasse principle. In our examples, both A and X have very simple equations. To state the theorem, recall the p-th power character $\left(\frac{q}{\ell}\right)_p$, which satisfies $\left(\frac{q}{\ell}\right)_p=1$ if and only if q is a p-th power in $\mathbb{Q}_\ell^\times$.

Theorem 1.1. *Let $p>5$ be a prime and let u,v be integers not divisible by 3. Let U be the set of primes dividing $3puv(u-3v)$. Let $t\geq 2$, and let $k=p_1p_2\cdots p_t$, where each p_i is a prime not in U satisfying*

(1) $\left(\frac{p_i}{p_j}\right)_p=1$, *for all $i\neq j$ in $\{1,\ldots,t\}$,*

(2) $\left(\frac{p_i}{q}\right)_p=1$, *for all $i\in\{1,\ldots,t\}$ and all $q\in U$,*

(3) $\left(\frac{q}{p_i}\right)_p=1$, *for all $i\in\{1,\ldots,t\}$ and all $q\in U\backslash\{3\}$,*

(4) $\left(\frac{3}{p_i}\right)_p\neq 1$, *for all $i\in\{1,\ldots,t\}$.*

Let $g=p-1$ and consider the variety $\tilde{A}\subset\mathbb{A}^{2g+1}_{\mathbb{Q}}$ defined by the equations

$$y_i^p=x_i(x_i-3uk)(x_i-9vk),\ \text{for } i=1,\ldots,g,\ \text{and } z^p=\prod_{i=1}^{g}x_i(x_i-3uk).$$

https://doi.org/10.1017/S1474748024000392 Published online by Cambridge University Press

The symmetric group S_g acts on $\tilde{A}$, and the quotient $\tilde{A}/S_g$ is birational to a unique g-dimensional abelian variety A over $\mathbb{Q}$. Let $I \subset \{1,\dots,t\}$ be a proper nonempty subset, and let $q = \prod_{i\in I} p_i$. Let $\tilde{X} \subset \mathbb{A}_{\mathbb{Q}}^{2g+1}$ be defined by the equations (with $i = 1,\dots,g$)

$$y_i^p = x_i(x_i - 3uk)(x_i - 9vk) \text{ and } qz^p = \prod_{i=1}^{g} x_i(x_i - 3uk).$$

Then $\tilde{X}/S_g$ is birational to an A-torsor X that violates the Hasse principle, and the class of X in $\text{Ш}(A)$ has order p.

Remark 1.2. Both A and X are μ_p-covers of the Jacobian J of the genus $p-1$ superelliptic curve $C\colon y^p = x(x-3uk)(x-9vk)$. Since J is birational to the symmetric power C^g/S_g, the μ_p-covers can be seen from the equations above as well.

Using the Cebotarev density theorem, we show in Proposition 6.1 that there exist primes $p_1,\dots,p_t$ satisfying the hypotheses of Theorem 1.1. Here is an example with $p = 29$.

Example 1.3. Let $\tilde{X} \subset \mathbb{A}_{\mathbb{Q}}^{28} \times \mathbb{A}_{\mathbb{Q}}^{28} \times \mathbb{A}_{\mathbb{Q}}^{1}$ be the variety defined by the 28 equations

$$y_i^{29} = x_i(x_i - 3\cdot 386029093\cdot 545622299)(x_i + 9\cdot 386029093\cdot 545622299)$$

for $i = 1,\dots,28$, as well as the additional equation

$$386029093z^{29} = \prod_{i=1}^{28} x_i(x_i - 3\cdot 386029093\cdot 545622299).$$

Then $\tilde{X}/S_g$ is birational to a torsor X for a 28-dimensional abelian variety A over $\mathbb{Q}$. Moreover, X violates the Hasse principle and represents an order 29 element of $\text{Ш}(A)$.

Remark 1.4. As a point of comparison, work of Radičević [32] gives a method to compute equations for order p torsors in the Tate-Shafarevich group of an elliptic curve E over $\mathbb{Q}$. Even for $p = 11$, the equations for these torsors are not so easy for humans to write down. As p grows, the computations quickly become intractable even for computers.

Since the hypotheses of Theorem 1.1 are always met, this gives a second proof of [37, Thm. 1], and moreover gives explicit examples for any prime p. Moreover, the flexibility of the index set I allows us to prove our second main result, that $\text{Ш}(A)[p]$ can be arbitrarily large.

Theorem 1.5. *For every prime p and every integer $k \geq 1$, there exists an absolutely simple abelian variety A over $\mathbb{Q}$ with $\#\text{Ш}(A)[p] \geq p^k$.*

The cases $p = 2,3,5$ not covered by Theorem 1.1 were proven by Bölling [3], Cassels [6] and Fisher [12], respectively. Indeed, it was previously known that the p-part of the Tate-Shafarevich group of absolutely simple abelian varieties over $\mathbb{Q}$ can be arbitrarily large only for certain small primes p. Our examples are special since they arise as μ_p-covers of a specific type of Jacobian, so we leave open the question of existence of order p elements in $\text{Ш}(A)[p]$ for 'generic' abelian varieties over $\mathbb{Q}$ (i.e., those such that the Mumford-Tate

https://doi.org/10.1017/S1474748024000392 Published online by Cambridge University Press

group is GSp_{2g} and $A[p]$ is irreducible as a $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$-module). In both this paper and [37], the abelian varieties are such that $\mathrm{rk}\,\mathrm{End}(A_{\bar{\mathbb{Q}}}) = \dim A$ and $A[p]$ is reducible.

Since we can control the dimension of our examples, we also conclude the following:

Corollary 1.6. *Suppose $g = p-1$ for some prime $p \geq 7$. Then the Tate-Shafarevich groups of absolutely simple abelian varieties A over $\mathbb{Q}$ of dimension g can be arbitrarily large. More precisely, the groups $Ш(A)[p]$ can be arbitrarily large.*

Our construction generalizes in an obvious way to any global field. We work over $\mathbb{Q}$ because it is the most interesting case and to keep the notation simple. The restriction $p \neq 5$ in our results is related to some quirky numerology (see Proposition A(*iii*) in the Appendix) that could probably be removed by tweaking the construction slightly.

1.2. Previous work

Previous work on elliptic curves ([2, 3, 6, 12, 18, 19, 20, 22, 23, 26]) has found arbitrarily large p-torsion part of the Tate-Shafarevich group for $p \leqslant 7$ and $p = 13$. In higher dimension, Creutz [10] has shown that for any principally polarized abelian variety A over a number field K, the p-torsion in the Tate-Shafarevich group can be arbitrarily large over a field extension L of degree which is bounded in terms of p and the dimension of A, generalizing work of Clark and Sharif [9]. In higher dimension over $\mathbb{Q}$, the first author [14] has recently shown that the 2-torsion subgroup of Tate-Shafarevich groups of absolutely simple Jacobians of genus 2 curves over $\mathbb{Q}$ can be arbitrarily large, and then in [15] that the 2-torsion of the Tate-Shafarevich groups of absolutely simple Jacobians of curves of any genus over $\mathbb{Q}$ can be arbitrarily large. With Bruin, the authors recently showed in [5] that $Ш(A)[3]$ can be arbitrarily large among certain abelian surfaces $A/\mathbb{Q}$. Many of these works make use of Jacobians with an isogeny to another Jacobian, comparing the bound obtained using isogeny-descent against that of a complete p-descent.

1.3. Approach

Our method makes use of Jacobians with two independent $\mathbb{Q}$-rational p-torsion points, so we also make (implicit) use of isogenies. However, instead of bounding the Mordell-Weil rank, we construct locally soluble torsors and show directly that they have no rational points. Since our method does not require knowledge of L-functions nor any information related to the rank of $A(\mathbb{Q})$, it is more widely applicable. Our technique is similar in spirit to that of Cassels in [6] who used the Cassels-Tate pairing to show that the 3-part of the Tate-Shafarevich group of elliptic curves can be arbitrarily large. However, our approach is more direct. In the appendix by Tom Fisher, an alternative interpretation of our proof is given in terms of an appropriate Cassels-Tate pairing.

We construct our torsors purely geometrically, as μ_p-covers. In fact, we avoid the use of Galois cohomology in this paper, as a way of emphasizing the geometry. Experts will see that the proof can be interpreted cohomologically using standard descent techniques [8, 34], but the geometric point of view is the most direct way to understand the construction and will perhaps be more accessible to those less familiar with Selmer groups (though we do assume familiarity with the basics of abelian varieties).

1.4. Outline of proof

In Section 2 and 3, we prove some preliminary material on μ_p-covers and μ_p-descent. Most of this will be well known to experts, but we have customized the discussion to our needs and made it fairly self-contained. In Section 4, we specialize the discussion to μ_p-covers of Jacobians of superelliptic curves. In Section 5, we prove Theorem 1.1. We must show that the torsors have local points everywhere and yet have no rational points. For most primes ℓ, it is easy to see that the torsors have $\mathbb{Q}_\ell$-points using the fact that almost all of the primes in the set $\{p_1,\cdots,p_t\}\cup U$ are p-th powers modulo each other. The subtle case is where $\ell = p_i$, and in this case, we construct points explicitly using the torsion points $D_0 = (0,0) - \infty$ and $D_1 = (3uk,0) - \infty$ on J. The more interesting argument is the proof that the torsors have no global points. For this, we first show that the two global torsion divisors D_0 and D_1 generate a certain quotient of $J(\mathbb{Q}_{p_i})$, for each p_i. The presence of the powers of 3 in the model of the curve, and the fact that 3 is not a p-th power locally, then 'glues together' the localizations of the torsors in a certain way that makes it impossible for them to have a global point unless the parameter q is divisible by either all or none of the primes $p_1,\dots,p_t$. The particular choice of the prime 3 here is not special (we could replace it by 5 or 7, etc.), but the presence of this 'gluing prime' plays the crucial role in the argument.

In Section 6, we deduce Theorem 1.5 from Theorem 1.1. First, we use a Cebotarev argument to show that given p, the set U, and any $t \geq 1$, there exist primes $p_1,\dots,p_t$ satisfying the conditions of Theorem 1.1. Second, the flexibility in the choice of q allows us to generate a subgroup of $\mathbb{F}_p$-rank at least $t-1$ in $Ш(A)[p]$. Finally, we use a theorem of Masser to show that for 100% of integers u,v not divisible by 3, the corresponding abelian variety is geometrically simple. In the appendix, Tom Fisher recasts our proof in terms of a Cassels-Tate pairing.

2. μ_p-covers

2.1. Classifying μ_p-covers

Let X be a proper variety over a field F. Let μ_p be the F-group scheme of p-th roots of unity. A μ_p-cover of Y (or more formally, a μ_p-torsor over Y in the fppf topology) is a Y-scheme X together with a μ_p-action that is simply transitive on fibers over Y. The μ_p-covers of Y form a category $\mathcal{M}_p(Y)$ whose morphisms are μ_p-equivariant isomorphisms. The following proposition gives a concrete way to think about μ_p-covers.

Proposition 2.1. *There is an equivalence of categories between $\mathcal{M}_p(Y)$ and the category of pairs $(\mathcal{L},\eta)$ where $\mathcal{L}$ is an invertible sheaf on Y and $\eta\colon \mathcal{L}^{\otimes p} \simeq \mathcal{O}_Y$ is an isomorphism. Here, the morphisms $(\mathcal{L},\eta) \to (\mathcal{L}',\eta')$ are isomorphisms $g\colon \mathcal{L} \to \mathcal{L}'$ such that $\eta' \circ g^{\otimes p} = \eta$.*

Proof. This is well known (see [1] or [29, pg. 71]), so we just describe the functors in both directions. If $\pi\colon X \to Y$ is a μ_p-cover, then there is a $\mathbb{Z}/p\mathbb{Z}$-grading on the $\mathcal{O}_Y$-module

$$\pi_*\mathcal{O}_X = \mathcal{O}_Y \oplus \bigoplus_{i=1}^{p-1} \mathcal{L}_i$$

https://doi.org/10.1017/S1474748024000392 Published online by Cambridge University Press

where each $\mathcal{L}_i$ is the invertible subsheaf of $\pi_*\mathcal{O}_X$ on which μ_p acts by $\zeta \cdot s = \zeta^i s$. The algebra structure of $\pi_*\mathcal{O}_X$ gives isomorphisms $\mathcal{L}_i \otimes \mathcal{L}_j \simeq \mathcal{L}_{i+j}$, where indices are to be taken modulo p and where $\mathcal{L}_0 = \mathcal{O}_Y$. Thus, we obtain an isomorphism $\mathcal{L}_1^{\otimes p} \simeq \mathcal{O}_Y$. Conversely, starting with a pair $(\mathcal{L},\eta)$, we can define a sheaf of $\mathcal{O}_Y$-algebras $\mathcal{O}_Y \oplus \bigoplus_{i=1}^{p-1} \mathcal{L}^i$ using the given isomorphism η to define the multiplication $\mathcal{L}^i \otimes \mathcal{L}^j \simeq \mathcal{L}^{i+j} \simeq \mathcal{L}^{i+j-p}$ on the factors with $i+j \geq p$. The relative spectrum of this sheaf over Y is then naturally endowed with a μ_p-action making it a μ_p-cover. □

Remark 2.2. If $Y = \operatorname{Spec} F$, this recovers Kummer theory.

2.2. μ_p-covers of abelian varieties

Let us now specialize to the case where Y is an abelian variety over a field F of characteristic not p. We will think of a μ_p-cover $\pi\colon X \to Y$ in terms of the corresponding pair $(\mathcal{L},\eta)$. The isomorphism class of $\mathcal{L}$ is a well-defined element of $\operatorname{Pic}(Y) = \operatorname{Pic}_Y(F)$, called the *Steinitz class* of π. The existence of η means that $\mathcal{L}$ is p-torsion, so that $\mathcal{L} \in \widehat{Y}[p](F)$, where $\widehat{Y} = \operatorname{Pic}^0_Y \subset \operatorname{Pic}_Y$ is the dual abelian variety parameterizing algebraically trivial line bundles on Y.

From one μ_p-cover $(\mathcal{L},\eta)$, we may construct many more, simply by scaling $\eta\colon \mathcal{L}^{\otimes p} \to \mathcal{O}_Y$ by any $r \in F^*$. Two μ_p-covers $(\mathcal{L}, r\eta)$ and $(\mathcal{L}, s\eta)$ are isomorphic if and only if $r/s \in F^{*p}$. More generally, given two μ_p-covers $(\mathcal{L},\eta)$ and $(\mathcal{L}',\eta')$, the tensor product $(\mathcal{L}\otimes\mathcal{L}', \eta\otimes\eta')$ is another. Let $H^1(Y,\mu_p)$ denote the set of isomorphism classes of μ_p-covers of Y.

Proposition 2.3. *The set $H^1(Y,\mu_p)$ is naturally an abelian group and sits in a short exact sequence*

$$0 \to F^*/F^{*p} \to H^1(Y,\mu_p) \to \widehat{Y}[p](F) \to 0.$$

Proof. This follows from Proposition 2.1 and the discussion above. □

Remark 2.4. We use the notation $H^1(Y,\mu_p)$ since the étale cohomology group $H^1_{\text{et}}(Y,\mu_p)$ is also in bijection with isomorphism classes of μ_p-covers. From this point of view, one obtains Proposition 2.3 by applying the long exact sequence in cohomology to the short sequence of sheaves $0 \to \mu_p \to \mathbb{G}_m \to \mathbb{G}_m \to 0$.

Lemma 2.5. *The μ_p-cover $\pi\colon X \to Y$ corresponding to $(\mathcal{L},\eta)$ is geometrically connected if and only if $\mathcal{L} \not\simeq \mathcal{O}_X$.*

Proof. If $\mathcal{L} \simeq \mathcal{O}_X$, then η is scalar multiplication by some $r \in F^\times$. In this case, X is isomorphic to $Y \times_F F(\sqrt[p]{r})$ as an F-scheme, which is not geometrically connected. Conversely, if X is not geometrically connected, then the μ_p-cover $X_{\bar{F}} \to Y_{\bar{F}}$ induces an isomorphism on connected components, forcing $X_{\bar{F}}$ to be isomorphic to the trivial μ_p-torsor $Y_{\bar{F}} \times_{\bar{F}} \mu_p$. It follows that π is in $\ker(H^1(Y,\mu_p) \to H^1(Y_{\bar{F}},\mu_p)) \simeq F^*/F^{*p}$, and hence has trivial Steinitz class. □

Suppose now that $\pi\colon X \to Y$ is a geometrically connected μ_p-cover corresponding to $(\mathcal{L},\eta)$, so that $\mathcal{L} \not\simeq \mathcal{O}_Y$. Since every connected finite étale cover of the abelian variety $Y_{\bar{F}}$ is

https://doi.org/10.1017/S1474748024000392 Published online by Cambridge University Press

itself an abelian variety [29, §18], X becomes an abelian variety over the algebraic closure $\overline{F}$. It follows that X is a torsor for a certain abelian variety, which we will now identify.

Let $\widehat{\psi}\colon \widehat{Y} \to \widehat{Y}/\langle\mathcal{L}\rangle$ be the degree p isogeny obtained by modding out by $\mathcal{L}$. Let $\psi\colon A_{\mathcal{L}} \to Y$ be the dual isogeny, which is also of degree p. Then ψ can itself be given the structure of μ_p-cover. Indeed, we have

$$\ker(\psi) \simeq \widehat{\ker(\widehat{\psi})} \simeq \widehat{\mathbb{Z}/p\mathbb{Z}} = \mathrm{Hom}(\mathbb{Z}/p\mathbb{Z},\mathbb{G}_m) \simeq \mu_p.$$

Note that there are $p-1$ different isomorphisms $\ker(\psi) \simeq \mu_p$, corresponding to the different $\mathbb{Z}/p\mathbb{Z}$-gradings we can put on $\psi_*\mathcal{O}_{A_{\mathcal{L}}}$. Exactly one of them will have the property that the corresponding μ_p-cover has Steinitz class $\mathcal{L}_1 \subset \psi_*\mathcal{O}_{A_{\mathcal{L}}}$ isomorphic to $\mathcal{L}$. We choose this μ_p-cover structure for ψ.

Lemma 2.6. *Let $\pi\colon X \to Y$ be a μ_p-cover with nontrivial Steinitz class $\mathcal{L} \in \widehat{Y}[p](F)$. Then π is a twist of the μ_p-cover $\psi\colon A_{\mathcal{L}} \to Y$ and X is a torsor for $A_{\mathcal{L}}$.*

Proof. If $\psi\colon A_{\mathcal{L}} \to Y$ corresponds to $(\mathcal{L},\eta)$, then $\pi\colon X \to Y$ corresponds to $(\mathcal{L},s\eta)$ for some scalar $s \in F^*$. Over $\bar{F}$ there is an isomorphism $\rho\colon (A_{\mathcal{L}})_{\bar{F}} \to X_{\bar{F}}$ of μ_p-covers, which satisfies

$$\rho^g(P) = \sqrt[p]{s}^{\,g}/\sqrt[p]{s} + \rho(P)$$

for all $g \in \mathrm{Gal}(\bar{F}/F)$ and $P \in A_{\mathcal{L}}(\bar{F})$; here, $\sqrt[p]{s}^{\,g}/\sqrt[p]{s} \in \mu_p$ and $+$ is the torsor action. The torsor structure $A_{\mathcal{L}} \times X \to X$ is given by $(P,Q) \mapsto \rho(P+\rho^{-1}(Q))$. Using the formula for ρ^g, we see that this torsor is indeed defined over F. □

We have seen that for each nonzero $\mathcal{L} \in \widehat{Y}[p](F)$, there is, in fact, a distinguished μ_p-cover with Steinitz class $\mathcal{L}$ – namely, the cover $A_{\mathcal{L}} \to Y$. This means there must be a distinguished isomorphism $\eta\colon \mathcal{L}^p \simeq \mathcal{O}_Y$. We will describe this isomorphism η in Lemma 3.6, in the context of rational points. For simplicity, we will specialize to the case where Y is a Jacobian, and in particular principally polarized (so that $\widehat{Y} \simeq Y$). However, most of what we prove can be generalized to arbitrary abelian varieties in a straightforward way.

2.3. μ_p-covers of Jacobians

Let C be a smooth projective geometrically integral curve over F, and let $J = \mathrm{Pic}^0(C)$ be its Jacobian. Let g be the genus of C, and hence also the dimension of the abelian variety J. Let $D \in J[p](F)$ be a divisor class of order p. Let $J \to J/\langle D\rangle$ be the quotient and let $\psi\colon A_D \to \widehat{J}$ be the corresponding dual isogeny, where A_D is the dual of $J/\langle D\rangle$. Then ψ is a μ_p-cover of $\widehat{J}$ corresponding to a pair $(\mathcal{L},\eta)$, as in the previous section.

Remark 2.7. As before, we may choose the μ_p-cover structure on ψ so that $\mathcal{L} \in \mathrm{Pic}^0(\widehat{J})(F)$ is mapped to D under the isomorphism $\hat{\hat{J}} \simeq J$.

From now on, we identify J and $\widehat{J}$ via the principal polarization $\lambda\colon J \to \widehat{J}$ coming from the theta divisor of the curve C. To make this explicit, we assume that C contains a rational point $\infty \in C(F)$. The theta divisor $\Theta \subset J$ is the subvariety of degree 0 divisor

https://doi.org/10.1017/S1474748024000392 Published online by Cambridge University Press

classes of the form $E-(g-1)\infty$, where E is an effective divisor of degree $g-1$. The isomorphism $J \to \widehat{J}$ sends P to $t_P^*\mathcal{O}_J(\Theta)\otimes\mathcal{O}_J(\Theta)^{-1}$, where $t_P\colon J\to J$ is translation by P. We can also describe $\lambda(P)$ as the line bundle on J associated to the divisor $[\Theta-P]-[\Theta]$.

After making the identification $J\simeq\widehat{J}$, we may view ψ as a μ_p-cover of J and η as an isomorphism $\mathcal{L}^{\otimes p}\to\mathcal{O}_J$. By Proposition 2.3, we have the exact sequence

$$0\to F^*/F^{*p}\to H^1(J,\mu_p)\to J[p](F)\to 0.$$

3. μ_p-descent

We continue with our assumptions on $J=\mathrm{Pic}^0(C)$. We have seen that to each $D\in J[p](F)$ of order p, there is a corresponding μ_p-cover $\psi\colon A_D\to J$ giving rise to the data $(\mathcal{L},\eta)$. These particular μ_p-covers are by construction abelian varieties, but general μ_p-covers corresponding to pairs $(\mathcal{L},r\eta)$, for $r\in F^\times$, may only be torsors for abelian varieties. We characterize those which are abelian varieties, or equivalently, those which have rational points.

3.1. Descent over general fields

Fix $D\in J[p](F)$ and $(\mathcal{L},\eta)$, as above. Given $P\in J(F)$, we may consider the μ_p-cover $\psi_P=t_P\circ\psi\colon A_D\to J$, where $t_P\colon J\to J$ is translation by P. The μ_p-cover ψ_P is endowed with the same μ_p-action as ψ, but different structure map to J. Since the Steinitz class is in $\mathrm{Pic}^0(J)$, it is invariant under translation, and hence, ψ_P and ψ have isomorphic Steinitz classes. If $\psi_P=(\mathcal{L}',\eta')$, then we can choose an isomorphism $\mathcal{L}'\simeq\mathcal{L}$, and under this isomorphism, we have $\eta'=r_P\eta$ for some $r_P\in F^*$. Any other choice of isomorphism $\mathcal{L}'\simeq\mathcal{L}$ differs by a scalar, so the element r_P is well defined up to F^{*p}.

Lemma 3.1. *The map $P\mapsto r_P$ induces an injective map $\partial^D\colon J(F)/\psi(A_D(F))\to F^*/F^{*p}$.*

Proof. Note that $r_P\in F^{*p}$ if and only if ψ_P is isomorphic as a μ_p-cover to ψ. But any isomorphism of μ_p-covers induces an isomorphism of A_D-torsors, and hence must be given by translation by Q for some $Q\in A_D(F)$. Translation by Q gives an isomorphism between these two μ_p-covers if and only if $P=\psi(Q)$. □

For completeness, we state the following result, connecting the map ∂^D to a boundary map in Galois cohomology:

Lemma 3.2. *The map ∂^D is the boundary map $J(F)\to H^1(F,\mu_p)\simeq F^*/F^{*p}$ in the long exact sequence in group cohomology for the short exact sequence of* $\mathrm{Gal}(\bar F/F)$*-modules*

$$0\to\mu_p\to A_D(\bar F)\xrightarrow{\psi}J(\bar F)\to 0.$$

Proof. The boundary map $J(F)\to H^1(F,\mu_p)$ sends $P\in J(F)$ to the cocycle $c\colon\mathrm{Gal}(\bar F/F)\to\mu_p\simeq A_D[\psi]$ given by $g\mapsto Q^g-Q$, where $Q\in A_D$ is such that $\psi(Q)=P$. We must show that this cocycle agrees with the cocycle $g\mapsto\sqrt[p]{r}^g/\sqrt[p]{r}$, where $r=r_P$. From the proof of Lemma 2.6, we see that the A_D-torsors $(\mathcal{L},r\eta)$ and $(\mathcal{L},\eta)$ are isomorphic

https://doi.org/10.1017/S1474748024000392 Published online by Cambridge University Press

(over $\bar{F}$) via translation by Q. By the explicit formula given there, this exactly means that $Q^g - Q$ is equal to the element $\sqrt[p]{r}^g / \sqrt[p]{r} \in \mu_p$. □

Lemma 3.3. *The image of ∂^D is the set of $r \in F^*/F^{*p}$ such that the μ_p-cover $(\mathcal{L}, r\eta)$ has a rational point.*

Proof. Every torsor in the image clearly has a rational point since it is isomorphic to A_D as a variety. Conversely, if a μ_p-cover $X \to J$ of the form $(\mathcal{L}, r\eta)$ has a rational point, then the underlying A_D-torsor is isomorphic to the trivial A_D-torsor up to translation by a point P. Hence, $\partial^D(-P) = r$. □

Remark 3.4. It follows that for a μ_p-cover $\pi\colon X \to J$ with Steinitz class $\mathcal{L}$, X is isomorphic to A_D (as varieties) if and only if π corresponds to $(\mathcal{L}, r\eta)$, with r in the image of ∂^D.

The following lemma is immediate from the definitions and can be used to give an explicit formula for the homomorphism ∂^D.

Lemma 3.5. *Let $F(J)$ be the function field of J and view $\eta^{-1}\colon \mathcal{O}_J \to \mathcal{L}^p$ as a global section of $\mathcal{L}^p$. Fix an embedding of $\mathcal{L}$ as a subsheaf of $F(J)$, so that η^{-1} is a nonzero element f of $F(J)$. Let Q be such that Q and $Q+P$ are in a domain of definition for f. Then $\partial^D(P) = r_P = f(P+Q)/f(Q)$, up to p-th powers.*

Thinking of η^{-1} as a function on J allows us to distinguish the unique μ_p-cover $(\mathcal{L}, \eta)$ corresponding to $\psi\colon A_D \to J$ among all μ_p-covers with Steinitz class $\mathcal{L}$, as promised.

Lemma 3.6. *The μ_p-cover corresponding to $(\mathcal{L}, \eta)$, which is isomorphic to the μ_p-cover $A_{\mathcal{L}} = A_D \to J$, is characterized among all μ_p-covers with Steinitz class $\mathcal{L}$ by the fact that the value $f(0_J)$ of the function $f = \eta^{-1} \in F(J)$ at 0_J is a p-th power in F^*. (Here we assume that $\mathcal{L}$ is chosen within its isomorphism class so that $f(0_J) \in F^\times$.)*

Proof. The μ_p-cover $A_D \to J$ is distinguished among μ_p-covers with Steinitz class $\mathcal{L}$ by the fact that the fiber above 0 has a rational point. Indeed, if $\pi\colon X \to J$ is a μ_p-cover of type $(\mathcal{L}, r\eta)$ with a rational point $Q \in X(F)$ above $0 \in J(F)$, then $\pi = \psi_P$ for some $P \in J(F)$, and $\pi^{-1}(0) = \psi^{-1}(-P)$. It follows that $P \in \psi(A_D(F))$, and hence, r is a p-th power, or in other words, π is isomorphic to ψ as μ_p-covers.

However, the pullback of the μ_p-cover $(\mathcal{L}, \eta)$ on J to $\operatorname{Spec} F$, via the inclusion $\{0_J\} \hookrightarrow J$, is $\operatorname{Spec} k[z]/(z^p - h)$ where $h = f(0_J)$. This has an F-rational point if and only if h is a p-th power. □

Let $\operatorname{Sym}^g C = C^g/S_g$ be the g-th symmetric power of C. Points of $\operatorname{Sym}^g C$ correspond to effective degree g divisors E on C. Recall that the map $\operatorname{Sym}^g C \to J$ sending $E \mapsto E - g\infty$ is birational [27, Thm. 5.1], and hence induces an isomorphism of function fields $F(\operatorname{Sym}^g C) \simeq F(J)$.

Lemma 3.7. *Suppose $pD = \operatorname{div}(\tilde{f})$ for some $\tilde{f} \in F(C)$. Then $\mathcal{L} \simeq \mathcal{O}_J(\tilde{D})$ for a divisor $\tilde{D}$ on J such that $p\tilde{D} = \operatorname{div}(f)$, where $f \in F(J) \simeq F(\operatorname{Sym}^g C)$ is the rational function $f(\sum_{i=1}^g (x_i, y_i) - g\infty) = \prod_{i=1}^g \tilde{f}(x_i, y_i)$.*

https://doi.org/10.1017/S1474748024000392 Published online by Cambridge University Press

Proof. Assume, for simplicity, that $D = \infty - Q$ for some $Q \in C(F)$. Under the polarization $J \to \widehat{J}$, the point D gets sent to the divisor $[\Theta - D] - [\Theta]$. Note that

$$\Theta - D = \{E + Q - g\infty \colon E \text{ effective of degree } g-1\}$$

is the locus of poles of the function f. Similarly, Θ is the zero locus. Taking into account multiplicities, the divisor of f is $p[\Theta - D] - p[\Theta]$, as claimed. The general case where $D = \sum_j (\infty - Q_j)$ is similar. □

Finally, we will use a generalization of the map ∂ and Lemma 3.1. Let $H = \{D_1, \ldots, D_m\} \subset J[p](F)$ be a subset of $\mathbb{F}_p$-linearly independent elements. For each $i = 1, \ldots, m$, let $\psi_i \colon A_i \to J$ be the μ_p-covers corresponding to D_i. Let $A_H = \widehat{J/\langle H \rangle}$ and let $\psi_H \colon A_H \to J$ be the isogeny dual to $J \to J/\langle H \rangle$. Then we have a homomorphism

$$\tilde{\partial}^H \colon J(F) \longrightarrow \prod_{i=1}^{m} F^*/F^{*p}$$

sending P to $(\partial^{D_1}(P), \ldots, \partial^{D_m}(P))$.

Lemma 3.8. *The map $\tilde{\partial}^H$ induces an injection $\partial^H \colon J(F)/\psi_H(A_H(F)) \hookrightarrow \bigoplus_{i=1}^m F^*/F^{*p}$.*

Proof. We prove this in the case $m = 2$, which is the only case we will use. The general case follows by an inductive argument. Suppose $\tilde{\partial}^{D_1}(P) = 0$ and $\tilde{\partial}^{D_2}(P) = 0$, so that $P = \psi_i(Q_i)$ for some $Q_i \in A_i(F)$ by Lemma 3.1. Let $g_i \colon A_H \to A_i$ be the natural maps, of degree p; note that $\psi_1 g_1 = \psi_2 g_2$. The fiber diagram

$$\begin{array}{ccc} A_H & \longrightarrow & A_2 \\ \downarrow & & \downarrow \\ A_1 & \longrightarrow & J \end{array} \tag{3.1}$$

shows that there is a unique point Q in $A_H(\bar{F})$ such that $g_i(Q) = Q_i$ for $i = 1,2$. The uniqueness of Q implies that it is $\mathrm{Gal}(\bar{F}/F)$-stable, and so we have $P = \psi_H(Q)$ with $Q \in A_H(F)$. This shows that ∂^H is injective. □

3.2. Descent over global fields

Suppose now that C is a curve over $\mathbb{Q}$. The preceding discussion applies for $F = \mathbb{Q}$, but also for $F = \mathbb{Q}_\ell$ for any prime $\ell \leq \infty$. Having fixed $D \in J[p](\mathbb{Q})$, let

$$\mathrm{Sel}(A_D) \subset \mathbb{Q}^*/\mathbb{Q}^{*p}$$

be the subgroup of classes r with the property that for every prime ℓ, the class of r in $\mathbb{Q}_\ell^*/\mathbb{Q}_\ell^{*p}$ is in the image of $\partial^D \colon J(\mathbb{Q}_\ell)/\psi(A_D(\mathbb{Q}_\ell)) \to \mathbb{Q}_\ell^*/\mathbb{Q}_\ell^{*p}$. In other words, an element of $\mathrm{Sel}(A_D)$ is a μ_p-cover $X \to J$ with Steinitz class D and such that $X(\mathbb{Q}_\ell) \neq \emptyset$ for every prime ℓ.

https://doi.org/10.1017/S1474748024000392 Published online by Cambridge University Press

Recall that if A is an abelian variety over $\mathbb{Q}$, then $\text{Ш}(A)$ is the group of A-torsors which are trivial over $\mathbb{Q}_\ell$, for all primes $\ell \leq \infty$.

Proposition 3.9. *Let $\text{Ш}(A_D)$ be the Tate-Shafarevich group of A_D. There is an exact sequence*

$$0 \to J(\mathbb{Q})/\psi(A_D(\mathbb{Q})) \to \mathrm{Sel}(A_D) \to \text{Ш}(A_D)[\psi] \to 0$$

where $\text{Ш}(A_D)[\psi]$ is the kernel of the map $\text{Ш}(A_D) \to \text{Ш}(J)$ induced by ψ.

Proof. The map $\mathrm{Sel}(A_D) \to \text{Ш}(A_D)[\psi]$ sends the μ_p-cover $X \to J$ to the underlying A_D-torsor (c.f. Lemma 2.6). The cocycle $c\colon \mathrm{Gal}(\bar{F}/F) \to A_D(\bar{F})$ with $c(g) = \sqrt[p]{s}^g/\sqrt[p]{s}$ determines this torsor and has image in $\mu_p \simeq \ker(\psi)$, so the cocycle indeed becomes trivial in $\text{Ш}(J)$. The exactness of the sequence in the middle follows from Lemma 3.3. The exactness on the right can be proved using direct geometric arguments but is most easily seen using Lemma 3.2. Since we will not actually use the exactness on the right, we omit the proof. □

The group $\mathrm{Sel}(A_D)$ is isomorphic to the usual Selmer group

$$\mathrm{Sel}_\psi(A_D) \subset H^1(F, A_D[\psi]) \simeq H^1(F, \mu_p) \simeq F^*/F^{*p}.$$

In particular, it is finite. This can also be seen from the following proposition.

Proposition 3.10. *Suppose $\ell \neq p$ is a prime of good reduction for J. Then the image of $\partial^D\colon J(\mathbb{Q}_\ell) \to \mathbb{Q}_\ell^*/\mathbb{Q}_\ell^{*p}$ is the subgroup $\mathbb{Z}_\ell^*/\mathbb{Z}_\ell^{*p}$.*

Proof. This well-known fact follows from [7, Prop. 2.7(d)] if we grant Lemma 3.2, but we will give a more geometric proof in the spirit of this paper. The classes in $\mathbb{Z}_\ell^*/\mathbb{Z}_\ell^{*p}$ represent μ_p-covers $X \to J$ which are trivialized by an unramified field extension; hence, the corresponding A_D-torsor X is also trivialized by an unramified field extension. Since A_D has good reduction at ℓ, the torsor X has a Néron model $\mathcal{X}$ over $\mathbb{Z}_\ell$, which is a torsor for the Néron model $\mathcal{A}$ of A_D [4, 6.5. Cor. 4]. Since any torsor for a smooth proper group scheme over $\mathbb{Z}_\ell$ has a $\mathbb{Z}_\ell$-point, it follows that such classes are in the image of ∂^D by Lemma 3.3. Conversely, any element r in the image of ∂^D corresponds to a μ_p-cover (and A_D-torsor) X which is abstractly isomorphic to A_D, and hence has good reduction over $\mathbb{Q}_\ell$. By the Néron mapping property, X extends to a μ_p-cover and even an $\mathcal{A}$-torsor over $\mathbb{Z}_\ell$. It follows that $r \in \mathbb{Z}_\ell^*$, since we can interpret this scalar as an automorphism of a line bundle on an abelian scheme $\mathcal{J}$ over $\mathbb{Z}_\ell$ (well-defined up to p-th powers). □

We will also consider more general Selmer groups. Given a subset $H = \{D_1, \ldots, D_m\} \subset J[p](F)$ of linearly independent elements, we can define an analogous Selmer group $\mathrm{Sel}(A_H) \subset \prod_{i=1}^m F^*/F^{*p}$ which sits in an exact sequence

$$0 \to J(\mathbb{Q})/\psi_H(A_H(\mathbb{Q})) \to \mathrm{Sel}(A_H) \to \text{Ш}(A_H)[\psi_H] \to 0$$

and which is isomorphic to the usual Selmer group $\mathrm{Sel}_{\psi_H}(A_H)$.

https://doi.org/10.1017/S1474748024000392 Published online by Cambridge University Press

4. Jacobians of curves of the form $y^p = x(x-e_1)(x-e_2)$

4.1. A special family of curves

Let $p > 5$ be a prime and let e_0, e_1, e_2 be distinct integers. Let C be the smooth projective curve over $\mathbb{Q}$ with affine model

$$y^p = (x-e_0)(x-e_1)(x-e_2). \tag{4.1}$$

There is no loss in generality in assuming $e_0 = 0$, so we will do so. The affine model is itself smooth, and its complement in C is a single rational point we call ∞. The genus of C is $g = p-1$. For more details on such curves, see [30].

Let J be the Jacobian of C. Note that $J(\mathbb{Q})$ has p-torsion of rank at least 2, generated by the three divisor classes $D_i = [(e_i, 0) - \infty]$, for $i \in \{0,1,2\}$. The equality of divisors $D_0 + D_1 + D_2 = \operatorname{div}(y)$ means that $D_0 + D_1 + D_2 = 0$ in J. Let $D = D_0 + D_1$ and define the abelian varieties

$$\widehat{A} = J/\langle D_0, D_1\rangle \tag{4.2}$$

$$\widehat{B} = J/\langle D\rangle \tag{4.3}$$

and the corresponding quotient isogenies $\widehat{\phi} : J \to \widehat{A}$ and $\widehat{\psi} \colon J \to \widehat{B}$. As before, we identify J with its dual via the canonical principal polarization, so that we may write $\phi : A \to J$ and $\psi \colon B \to J$ for the dual isogenies. We also define A_{D_i} to be the dual of $J/\langle D_i\rangle$ for $i = 0,1,2$ with isogenies $\psi_i \colon A_{D_i} \to J$. We have $B \simeq A_{D_2}$ since $D = -D_2$.

Let $H = \langle D_0, D_1\rangle$, and define the map

$$\begin{aligned} \partial^H : & J(\mathbb{Q})/\phi\big(A(\mathbb{Q})\big) \longrightarrow \mathbb{Q}^*/\mathbb{Q}^{*p} \times \mathbb{Q}^*/\mathbb{Q}^{*p}, \\ & \left[\sum_{j=1}^{g} (x_j, y_j) - g \cdot \infty\right] \mapsto \Big(\prod_{j=1}^{g} x_j,\ \prod_{j=1}^{g} (x_j - e_1)\Big) \end{aligned} \tag{4.4}$$

as in Lemmas 3.5 and 3.7 of Section 2.3. In the above definition, each $x_j, y_j \in \overline{\mathbb{Q}}$, the divisor $\sum_{j=1}^{g} (x_j, y_j) - g \cdot \infty$ is Galois stable, and the left-hand side is its divisor class. That such representatives exist follows from the fact that $C(\mathbb{Q}) \neq \emptyset$ [34, Prop. 2.7]. The above description of ∂^H applies whenever it makes sense – that is, when all x_j and $x_j - e_1$ are nonzero. Every class in $J(\mathbb{Q})/\phi\big(A(\mathbb{Q})\big)$ can be represented by such a divisor [21, pg.166].

For $i \in \{1,2,3\}$, we have similar homomorphisms

$$\begin{aligned} \partial^{D_i} : & J(\mathbb{Q})/\psi_i\big(A_{D_i}(\mathbb{Q})\big) \longrightarrow \mathbb{Q}^*/\mathbb{Q}^{*p}, \\ & \left[\sum_{j=1}^{g} (x_j, y_j) - g \cdot \infty\right] \mapsto \prod_{j=1}^{g} \Big(x_j - e_i\Big), \end{aligned} \tag{4.5}$$

https://doi.org/10.1017/S1474748024000392 Published online by Cambridge University Press

as well as the homomorphism

$$\begin{aligned} \partial^D : & J(\mathbb{Q})/\psi\big(B(\mathbb{Q})\big) \longrightarrow \mathbb{Q}^*/\mathbb{Q}^{*p}, \\ & \left[\sum_{j=1}^{g}(x_j,y_j) - g\cdot\infty\right] \mapsto \prod_{j=1}^{g}\Big(x_j(x_j-e_1)\Big). \end{aligned} \tag{4.6}$$

As before, the description of these maps is for representative divisors for which it makes sense. However, note that by the equation for the curve, we have $\partial^{D_0}\cdot\partial^{D_1}\cdot\partial^{D_2}=1$. This allows us to describe the maps ∂^{D_i} even on points where the formula above is not well defined. For example,

Lemma 4.1. *We have*

$$\partial^H([(0,0)-\infty]) = [e_1^{-1}e_2^{-1}, -e_1]$$

and

$$\partial^H([(e_1,0)-\infty]) = [e_1, e_1^{-1}(e_1-e_2)^{-1}].$$

In the next section, we will make critical use of the following commutative diagram

$$\begin{array}{ccc} J(\mathbb{Q})/\phi\big(A(\mathbb{Q})\big) & \xrightarrow{\partial^H} & \mathbb{Q}^*/\mathbb{Q}^{*p}\times\mathbb{Q}^*/\mathbb{Q}^{*p} \\ \downarrow & & \downarrow \\ J(\mathbb{Q})/\psi\big(B(\mathbb{Q})\big) & \xrightarrow{\partial^D} & \mathbb{Q}^*/\mathbb{Q}^{*p}, \end{array} \tag{4.7}$$

whose right vertical map is $[r_1,r_2]\mapsto r_1r_2$.

4.2. Models

There are simple birational models for the μ_p-covers of J with a given Steinitz class. For concreteness, assume that the Steinitz class is $D=D_0+D_1$. The distinguished μ_p-cover with this Steinitz class is the cover $B\to J$. A birational model for J is given by the equations

$$y_i^p = x_i(x_i-e_1)(x_i-e_2)$$

for $i=1,\ldots,g$, modulo the action of S_g. By Lemmas 3.5, 3.6 and 3.7, a birational model for B is given by the same g equations above along with the additional equation

$$z^p = \prod_{i=1}^{g} x_i(x_i-e_1),$$

all modulo the action of S_g. Similarly, if $r\in\mathbb{Q}^\times$, then the μ_p-cover corresponding to $(\mathcal{L},r\eta)$ is given by the same equations, with the last one twisted by r:

$$y_i^p = x_i(x_i-e_1)(x_i-e_2)$$

https://doi.org/10.1017/S1474748024000392 Published online by Cambridge University Press

for $i = 1, \ldots, g$ and

$$rz^p = \prod_{i=1}^{g} x_i(x_i - e_1),$$

again modulo the action of S_g.

5. Arbitrarily large p-torsion part of the Tate-Shafarevich group

We wish to produce examples of arbitrarily large p-torsion subgroups in the Tate-Shafarevich group $Ш(B)[p]$, by finding elements of $\mathrm{Sel}(B)$ which can be shown to violate the Hasse principle by using $\mathrm{Sel}(A)$. We will choose fairly generic curves of the form $y^p = x(x-e_1)(x-e_2)$, but then we will twist them in a carefully chosen way to produce our examples.

Let

$$C = C_{u,v} : y^p = x(x-3u)(x-9v),$$

where $p > 5$ is prime and where $u, v \in \mathbb{Z}$ are not divisible by 3. Let J be the Jacobian of C and let A be the isogenous abelian variety, as in the previous section.

Lemma 5.1. *Suppose q is a prime such that $q \equiv 1 \pmod{p}$. Then $J(\mathbb{Q}_q)/\phi\big(A(\mathbb{Q}_q)\big)$ has order p^2.*

Proof. The congruence condition on q implies $\mathbb{Q}_q^*$ contains a primitive p-th root of unity ζ. Over any field containing ζ, the automorphism $(x,y) \mapsto (x, \zeta y)$ of C induces a ring embedding $\iota\colon \mathbb{Z}[\zeta] \hookrightarrow \mathrm{End}(J)$. The degree of $\iota(\alpha)$ is equal to $\mathrm{Nm}(\alpha)^2 = \#(\mathbb{Z}[\zeta]/\alpha)^2$. Indeed, the degree function restricted to $\mathbb{Z}[\zeta]$ is a power of the norm [29, §19], and we have $\deg([n]) = n^{2g} = n^{2[\mathbb{Q}(\zeta)\colon \mathbb{Q}]}$, so it is the square of the norm in this case. The kernel of $\widehat{\phi}\colon J \to \widehat{A}$ is then equal to the kernel of the endomorphism $1 - \iota(\zeta)$. It follows that $\widehat{\phi}$ agrees with $1 - \iota(\zeta)$ up to post-composition with an automorphism (since they have the same degree and one factors through the other); hence, the abelian varieties A and $\widehat{A}$ are isomorphic to J (over any field containing ζ, and in particular over $\mathbb{Q}_q$). However, we have [36, Cor. 3.2]

$$\frac{\#J(\mathbb{Q}_q)/\phi\big(A(\mathbb{Q}_q)\big)}{\#A(\mathbb{Q}_q)[\phi]} = c_q(J)/c_q(A),$$

where the right-hand side is the ratio of Tamagawa numbers over $\mathbb{Q}_q$. Since $J \simeq A$ over $\mathbb{Q}_q$, this ratio is 1. We also have $\#A(\mathbb{Q}_q)[\phi] = p^2$, which shows that $\#J(\mathbb{Q}_q)/\phi\big(A(\mathbb{Q}_q)\big) = p^2$. □

For each integer k, we will consider the curve

$$C_k = C_{u,v,k}\colon y^p = x(x-3uk)(x-9vk).$$

Another model for C_k is $k^{-3}y^p = x(x-3u)(x-9v)$, which shows that C_k is a μ_p-twist of the original curve $C = C_{u,v}$. Let J_k, A_k and B_k be the corresponding abelian varieties for the curve C_k. These are μ_p-twists of J, A and B, respectively.

https://doi.org/10.1017/S1474748024000392 Published online by Cambridge University Press

For two primes q and ℓ, set $\left(\frac{q}{\ell}\right)_p = 1$ if and only if q is a p-th power in $\mathbb{Q}_\ell^\times$. Recall the exact sequence

$$0 \to J_k(\mathbb{Q})/\psi(B_k(\mathbb{Q})) \xrightarrow{\partial^D} \mathrm{Sel}(B_k) \to \text{Ш}(B_k)[\psi] \to 0$$

from Proposition 3.9.

Proposition 5.2. *Let U be the set of primes that divide $3puv(u-3v)$. Suppose k is a product of distinct primes $k = p_1 p_2 \cdot \ldots \cdot p_t$, where $t \geq 2$ and each prime p_i is not in U, and satisfies*

(1) $\left(\frac{p_i}{p_j}\right)_p = 1$, *for all $i \neq j$ in $\{1,\ldots,t\}$,*

(2) $\left(\frac{p_i}{q}\right)_p = 1$, *for all $i \in \{1,\ldots,t\}$ and all $q \in U$,*

(3) $\left(\frac{q}{p_i}\right)_p = 1$, *for all $i \in \{1,\ldots,t\}$ and all $q \in U \backslash \{3\}$,*

(4) $\left(\frac{3}{p_i}\right)_p \neq 1$, *for all $i \in \{1,\ldots,t\}$.*

Then, for all i, we have $p_i \in \mathrm{Sel}(B_k)$ but $p_i \notin \partial^D(J_k(\mathbb{Q}))$. More generally, if $q = \prod_{i \in I} p_i^{a_i}$, where I is any nonempty proper subset of $\{1,\ldots,t\}$ and $1 \leq a_i \leq p-1$, then $q \in \mathrm{Sel}(B_k)$ but $q \notin \partial^D(J_k(\mathbb{Q}))$.

Note that condition (4) implies that $p_i \equiv 1 \pmod p$ for all i.

Proof. By Lemma 4.1, we have

$$\partial^H([(0,0) - \infty]) = [3^{-3}u^{-1}v^{-1}k^{-2}, -3uk]$$

and

$$\partial^H([(3uk,0) - \infty]) = [3uk, 3^{-2}u^{-1}(u-3v)^{-1}k^{-2}].$$

For $i = 1,\ldots,t$, the images of these two elements in $\mathbb{Q}_{p_i}^*/(\mathbb{Q}_{p_i}^*)^p \times \mathbb{Q}_{p_i}^*/(\mathbb{Q}_{p_i}^*)^p$ are $[3^{-3}p_i^{-2}, 3p_i]$ and $[3p_i, 3^{-2}p_i^{-2}]$, respectively, by our assumptions on the p_i. These two elements are linearly independent, and hence generate all of $\partial^H\big(J_k(\mathbb{Q}_{p_i})/\phi(A_k(\mathbb{Q}_{p_i}))\big)$, by Lemma 5.1.

Let $[r_1, r_2]$ be in $\partial^H\big(J_k(\mathbb{Q})/\phi(A_k(\mathbb{Q}))\big)$. We shall consider elements of $\mathbb{Q}^*/\mathbb{Q}^{*p}$ as pth-power-free integers. Note that by Proposition 3.10, the integers r_1 and r_2 can only be divisible by primes in the set $\{p_1,\ldots,p_t\} \cup U$.

If there is no i such that $\mathrm{ord}_{p_i}(r_1) \equiv \mathrm{ord}_{p_i}(1/r_2) \pmod p$, then $\mathrm{ord}_{p_i}(r_1 r_2) \not\equiv 0 \pmod p$ for every p_i, and so $r_1 r_2$ cannot be of the form $\prod_{i \in I} p_i^{a_i}$, for a nonempty proper subset of indices I, and any tuple of exponents a_i with $1 \leq a_i \leq p-1$.

Suppose there exists i such that $\mathrm{ord}_{p_i}(r_1) \equiv \mathrm{ord}_{p_i}(1/r_2) \pmod p$. Since $[3^{-3}p_i^{-2}, 3p_i]$ and $[3p_i, 3^{-2}p_i^{-2}]$ generate all of $\partial^H\big(J_k(\mathbb{Q}_{p_i})/\phi(A_k(\mathbb{Q}_{p_i}))\big)$, considering only the p_i-adic valuation, we have

$$[r_1, r_2] \equiv [p_i^{-2a}, p_i^a] \cdot [p_i^b, p_i^{-2b}] \equiv [p_i^{b-2a}, p_i^{a-2b}]$$

https://doi.org/10.1017/S1474748024000392 Published online by Cambridge University Press

for integers a and b. So

$$r_1 r_2 \equiv p_i^{b-2a+a-2b} = p_i^{-b-a}$$

and we must have $b \equiv -a \pmod{p_i}$. In other words, the image of $[r_1, r_2]$ in $\mathbb{Q}_{p_i}^*/(\mathbb{Q}_{p_i}^*)^p \times \mathbb{Q}_{p_i}^*/(\mathbb{Q}_{p_i}^*)^p$ must be a power of the quotient of these generators. Thus, in $\mathbb{Q}_{p_i}^*/(\mathbb{Q}_{p_i}^*)^p \times \mathbb{Q}_{p_i}^*/(\mathbb{Q}_{p_i}^*)^p$, we have

$$[r_1, r_2] = [3^{-4} p_i^{-3}, 3^3 p_i^3]^m = [3^{-4m} p_i^{-3m}, 3^{3m} p_i^{3m}],$$

for some $0 \le m < p$. Thus, in $\mathbb{Q}_{p_i}^*/(\mathbb{Q}_{p_i}^*)^p$, we have

$$r_1^3 r_2^4 = 3^{-12m+12m} p_i^{-9m+12m} = p_i^{3m}.$$

Since 3 is not a p-th power modulo p_i, this implies that 3 divides r_1^3 and $1/r_2^4$ to the same power. Since, for any j, the elements $[3^{-3} p_j^{-2}, 3p_j]$ and $[3p_j, 3^{-2} p_j^{-2}]$ generate all of $\partial^H((J_k(\mathbb{Q}_{p_j})/\phi(A_k(\mathbb{Q}_{p_j}))))$, and since we have already shown that 3 divides r_1^3 and $1/r_2^4$ to the same power, we deduce that the image of $[r_1, r_2]$ in $\mathbb{Q}_{p_j}^*/(\mathbb{Q}_{p_j}^*)^p \times \mathbb{Q}_{p_j}^*/(\mathbb{Q}_{p_j}^*)^p$ must be a power of the quotient of these generators, and so p_j must divide r_1 and $1/r_2$ to the same power. This applies for all j; hence, no p_j will appear in $r_1 r_2$. So again we have that $r_1 r_2$ cannot be of the form $\prod_{i \in I} p_i^{a_i}$ with $0 < \#I < t$.

Since $\partial^H\big(J_k(\mathbb{Q})/\phi(A_k(\mathbb{Q}))\big)$ maps surjectively onto $\partial^D\big(J_k(\mathbb{Q})/\psi(B_k(\mathbb{Q}))\big)$, it follows that each element of the form $\prod_{i \in I} p_i^{a_i}$ with $0 < \#I < t$ and $0 < a_i < p$ is not in $\partial^D\big(J_k(\mathbb{Q})/\psi(B_k(\mathbb{Q}))\big)$.

However, we show that each p_i is in $\partial^D(J_k(\mathbb{Q}_\ell)/\psi(B_k(\mathbb{Q}_\ell)))$ for every prime ℓ, as follows. First, note that for every prime $\ell \in U \cup \{p_1, \ldots, p_t\}$ except p_i itself, p_i is a pth power in $\mathbb{Q}_\ell^*$, and so p_i is in $\partial^D\big(J_k(\mathbb{Q}_\ell)/\psi(B_k(\mathbb{Q}_\ell))\big)$ by virtue of being ∂^D of the identity. If $\ell \notin U \cup \{p_1, \ldots, p_t\}$, we have $p_i \in \partial^D(J_k(\mathbb{Q}_\ell)/\psi(B_k(\mathbb{Q}_\ell)))$, by Proposition 3.10. For the remaining case $\ell = p_i$, note that $\partial^D([(0,0) - \infty]) = [-3^{-2} v^{-1} k^{-1}]$ and $\partial^D([(3uk, 0) - \infty]) = [3^{-1}(u - 3v)^{-1} k^{-1}]$, and so the first divided by the square of the second gives p_i, since all other factors are pth powers in $\mathbb{Q}_{p_i}$. Hence, p_i is in the image everywhere locally. □

As a corollary, we deduce the first theorem from the introduction.

Proof of Theorem 1.1. The Theorem follows from Lemma 3.3 and Proposition 5.2, together with the discussion of models in Section 4.2. □

As a second corollary, we have the following:

Corollary 5.3. *Let $C_{u,v,k}$ be as in Proposition 5.2. Then $\#\text{Ш}(B_{u,v,k})[p] \ge p^{t-1}$.*

Proof. Let $B_k = B_{u,v,k}$. We have the exact sequence

$$0 \longrightarrow J_k(\mathbb{Q})/\psi(B_k(\mathbb{Q})) \longrightarrow \mathrm{Sel}(B_k) \longrightarrow \text{Ш}(B_k)[\psi] \longrightarrow 0. \tag{5.1}$$

Moreover, we have seen that any element of the form $\prod_{i \in I} p_i^{a_i}$, for some proper subset $I \subset \{1, \ldots, t\}$ is contained in $\mathrm{Sel}(B_k)$ but does not lie in the subgroup $J_k(\mathbb{Q})/\psi(B_k(\mathbb{Q})$. Thus, these elements must map nontrivially to $\text{Ш}(B_k/\mathbb{Q})[\psi]$. In fact, we see that the intersection of $J_k(\mathbb{Q})/\psi(B_k(\mathbb{Q}))$ with the subgroup of $\mathrm{Sel}(B_k)$ generated by the elements

https://doi.org/10.1017/S1474748024000392 Published online by Cambridge University Press

$p_1,\ldots,p_t$ is at most one dimensional as an $\mathbb{F}_p$-vector space. Indeed, any two linearly independent elements in this subgroup can be scaled so that they are divisible exactly once by p_1, and hence, their ratio is nonzero and not divisible by p_1, which would be a contradiction. It follows that the image of the subgroup $\langle p_1,\ldots,p_t\rangle$ in $Ш(B_k)[\psi]$ has dimension at least $t-1$. Since $\deg(\psi)=p$, we have $Ш(B_k)[\psi]\subset Ш(B_k)[p]$, which finishes the proof. □

6. Proof of Theorem 1.5

To deduce Theorem 1.5 from the results of the previous section, we need two extra ingredients.

Proposition 6.1. *For any u,v as above, and for any $t\geq 0$, there are primes $p_1,\ldots,p_t$ satisfying the conditions of Proposition 5.2.*

Proof. Let $K=\mathbb{Q}(\zeta)=\mathbb{Q}(\mu_p)$. We prove this by induction on t. If $t=0$, then there is nothing to prove.

Now let $t>0$ and suppose we have found primes $p_1,\cdots,p_{t-1}$ satisfying the conditions. Let $k=p_1\cdots p_{t-1}$. Let N be the product of the primes dividing $puv(u-3v)k$, and let ζ_{pN} be a primitive pN-th root of unity. Let L be the compositum inside $\bar{\mathbb{Q}}$ of $\mathbb{Q}(\zeta_{pN})$ with all of the fields $\mathbb{Q}(\sqrt[p]{q})$, with q a prime dividing N. Then L is an abelian extension of K and a Galois extension of $\mathbb{Q}$. Finally, let $E=\mathbb{Q}(\sqrt[p]{3})$ and let $F=EL$ be the compositum of E and L, which is again a Galois extension of $\mathbb{Q}$.

Note that the fields E and L are linearly disjoint over $\mathbb{Q}$. Indeed, $E/\mathbb{Q}$ is totally ramified at 3, whereas L is unramified at 3. Thus, we have an exact sequence

$$0\to(\mathbb{Z}/p\mathbb{Z})\to\mathrm{Gal}(F/\mathbb{Q})\to\mathrm{Gal}(L/\mathbb{Q})\to 0.$$

By the Cebotarev density theorem, there exists a prime p_t (in fact, infinitely many such primes) whose Frobenius conjugacy class in $\mathrm{Gal}(F/\mathbb{Q})$ is not trivial but restricts to the trivial class in $\mathrm{Gal}(L/\mathbb{Q})$. Let us check that p_t satisfies all the desired properties.

By construction, p_t splits completely in any subfield of L. In particular, p_t splits completely in $\mathbb{Q}(\zeta_{pN})$ and hence is a p-th power in $\mathbb{Q}_q^*$ for any prime q dividing $3pN$. For $q\nmid 3p$, this is because $p_t\equiv 1 \pmod{q}$, and hence, p_t is a p-th power in $\mathbb{Q}_q^*$ by Hensel's lemma. For $q=p$, this is because $p^2\mid pN$, and hence $p_t\equiv 1 \pmod{p^2}$, and hence is a p-th power, again by Hensel's lemma. For $q=3$, this is because every unit in $\mathbb{Z}_3$ is a p-th power. Similarly, p_t splits completely in $\mathbb{Q}(\sqrt[p]{q})$ for all $q\mid N$, so all such primes q are p-th powers modulo p_t.

Finally, we check that 3 is not a p-th power in $\mathbb{Q}_{p_t}^*$. It is enough to show that the prime p_t does not have a degree 1 prime above it in E. If it did, then because $\zeta\in\mathbb{Q}_{p_t}^*$, once the polynomial x^p-3 has one root in $\mathbb{Q}_{p_t}^*$, it necessarily has all of its roots in $\mathbb{Q}_{p_t}^*$. Therefore, p_t would split completely in E. Since p_t splits completely in L, this would mean that p_t splits completely in $F=EL$. But by construction, the Frobenius at p_t is nontrivial, so p_t does not split completely. □

It remains to show that, for each prime p, there exist examples for which $J_{u,v,k}$ is absolutely simple, and hence $B_{u,v,k}$ as well.

https://doi.org/10.1017/S1474748024000392 Published online by Cambridge University Press

Lemma 6.2. *For each $p>5$, there exist $u,v\in\mathbb{Z}$ as in Proposition 5.2 such that $B_{u,v,k}$ is absolutely simple for all k.*

Proof. The Jacobian of the curve $y^p=x(x-1)(x-t)$ over $\mathbb{Q}(t)$ is absolutely simple since there is a value of $t\in\mathbb{C}$ – namely, $t=\frac{1}{2}+\frac{\sqrt{3}}{2}i$ – which makes the curve isomorphic over $\mathbb{C}$ to $y^p=x^3-1$, and the Jacobian of the latter is known to be absolutely simple [16, 17]. By a result of Masser [25], for an abelian variety over $\mathbb{Q}(t)$, the geometric endomorphism ring for 100% of specializations of $t\in\mathbb{Q}$ (ordered by height) is the same as the generic geometric endomorphism ring. Since the generic abelian variety is geometrically simple, this endomorphism ring is a division ring, and hence, 100% of specializations are simple as well. But for $t=a/b\in\mathbb{Q}$, a positive proportion has 3 exactly dividing a and 3 not dividing b. So, there are many curves $y^p=x(x-1)(x-3v/u)$ with $u,v\in\mathbb{Z}$, not divisible by 3, with absolutely simple Jacobian. This is a twist of the curve $\mathcal{C}_{u,v,1}:y^p=x(x-3u)(x-3^2v)$, so there are curves of this form with absolutely simple Jacobian, giving that $B_{u,v,1}$ is also absolutely simple. Since each $B_{u,v,k}$ is a twist of $B_{u,v,1}$, it follows that $B_{u,v,k}$ is absolutely simple for all k. □

Proof of Theorem 1.5. This follows from Corollary 5.3, Proposition 6.1 and Lemma 6.2. □

Appendix: The Cassels-Tate pairing for p-coverings of Jacobians

by Tom Fisher

The purpose of this appendix is to interpret the proof of Proposition 5.2 in terms of a certain Cassels-Tate pairing. Let $J/\mathbb{Q}$ be a Jacobian, and identify $J=\widehat{J}$ in the usual way.

Let $p>5$ be a prime. Suppose that $J(\mathbb{Q})$ contains subgroups $\mathbb{Z}/p\mathbb{Z}$ and $(\mathbb{Z}/p\mathbb{Z})^2$ that we take to be the kernels of isogenies $\widehat{\psi}:J\to\widehat{B}$ and $\widehat{\phi}:J\to\widehat{A}$. We further suppose that $\ker\widehat{\psi}\subset\ker\widehat{\phi}$, so that $\widehat{\phi}$ factors via $\widehat{\psi}$ to give a commutative diagram

$$\begin{array}{ccc} J & \xrightarrow{\ \widehat{\phi}\ } & \widehat{A}\,. \\ & {\scriptstyle\widehat{\psi}}\searrow \quad \nearrow{\scriptstyle\widehat{\nu}} & \\ & \widehat{B} & \end{array}$$

There is then a commutative diagram

$$\begin{array}{ccccc} A(\mathbb{Q}) & \xrightarrow{\ \nu\ } & B(\mathbb{Q}) & \xrightarrow{\ \delta_\nu\ } & \mathbb{Q}^*/(\mathbb{Q}^*)^p \\ \| & & \downarrow{\scriptstyle\psi} & & \downarrow{\scriptstyle\iota} \\ A(\mathbb{Q}) & \xrightarrow{\ \phi\ } & J(\mathbb{Q}) & \xrightarrow{\ \delta_\phi\ } & \mathbb{Q}^*/(\mathbb{Q}^*)^p\times\mathbb{Q}^*/(\mathbb{Q}^*)^p \\ \downarrow{\scriptstyle\nu} & & \| & & \downarrow{\scriptstyle\pi} \\ B(\mathbb{Q}) & \xrightarrow{\ \psi\ } & J(\mathbb{Q}) & \xrightarrow{\ \delta_\psi\ } & \mathbb{Q}^*/(\mathbb{Q}^*)^p \end{array}$$

where $\iota(s) = (s, s^{-1})$ and $\pi(r_1, r_2) = r_1 r_2$. We now give the Weil pairing definition of the Cassels-Tate pairing (see [28, Chapter 1, Proposition 6.9], [31, Section 12.2] or [13]) simplified by the fact that π has an obvious section given by $r \mapsto (r, 1)$. The Cassels-Tate pairing

$$\langle\ ,\ \rangle_{\mathrm{CT}} : S^{(\psi)}(B/\mathbb{Q}) \times S^{(\widehat{\nu})}(\widehat{B}/\mathbb{Q}) \to \mathbb{Q}/\mathbb{Z}$$

is defined as follows. We start with

$$r \in S^{(\psi)}(B/\mathbb{Q}) \subset \mathbb{Q}^*/(\mathbb{Q}^*)^p \quad \text{and} \quad s \in S^{(\widehat{\nu})}(\widehat{B}/\mathbb{Q}) \subset H^1(\mathbb{Q}, \mathbb{Z}/p\mathbb{Z}).$$

For each prime ℓ, we pick $P_\ell \in J(\mathbb{Q}_\ell)$ with $\delta_{\psi,\ell}(P_\ell) \equiv r \mod (\mathbb{Q}_\ell^*)^p$. Then $\delta_{\phi,\ell}(P_\ell) = (r\xi_\ell, \xi_\ell^{-1})$ for some $\xi_\ell \in \mathbb{Q}_\ell^*/(\mathbb{Q}_\ell^*)^p$. We define

$$\langle r, s\rangle_{\mathrm{CT}} = \sum_\ell (\xi_\ell, \mathrm{res}_\ell\, s)_\ell,$$

where

$$(\ ,\ )_\ell : H^1(\mathbb{Q}_\ell, \mu_p) \times H^1(\mathbb{Q}_\ell, \mathbb{Z}/p\mathbb{Z}) \to \mathbb{Q}/\mathbb{Z} \tag{6.1}$$

is the local pairing given by cup product and the local invariant map. Since the sum of the local invariants of an element in $H^2(\mathbb{Q}, \mu_p)$ is 0, we have $\langle r, s\rangle_{\mathrm{CT}} = 0$ for all $r \in \delta_\psi(J(\mathbb{Q}))$.

Proposition A. *With the notation and assumptions of Proposition 5.2 (noting that δ_ϕ, δ_ψ and $S^{(\psi)}(B/\mathbb{Q})$ are there called ∂^H, ∂^D and $\mathrm{Sel}(B_k)$), we have*

(i) $p_i \in S^{(\psi)}(B/\mathbb{Q}) \subset \mathbb{Q}^*/(\mathbb{Q}^*)^p$ *for all* $1 \leqslant i \leqslant t$.

(ii) *Let* $\chi_i \in H^1(\mathbb{Q}, \mathbb{Z}/p\mathbb{Z}) = \mathrm{Hom}(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}), \mathbb{Z}/p\mathbb{Z})$ *be the unique continuous character that factors via* $\mathrm{Gal}(\mathbb{Q}(\zeta_{p_i})/\mathbb{Q})$ *and satisfies* $\chi_i(\mathrm{Frob}_3) = 1$ *(this is possible by assumption (4)). Then*

$$\chi_i - \chi_j \in S^{(\widehat{\nu})}(\widehat{B}/\mathbb{Q}) \subset H^1(\mathbb{Q}, \mathbb{Z}/p\mathbb{Z})$$

for all $1 \leqslant i, j, \leqslant t$.

(iii) *For* $a_1, \ldots, a_t, b_1, \ldots, b_t \in \{0, 1, \ldots, p-1\}$ *with* $\sum b_j \equiv 0 \pmod p$, *we have*

$$\left\langle \prod_{i=1}^t p_i^{a_i}, \sum_{j=1}^t b_j \chi_j \right\rangle_{\mathrm{CT}} = \frac{-5}{p} \sum_{i=1}^t a_i b_i.$$

In particular, since $p > 5$, if $q = \prod_{i=1}^t p_i^{a_i}$, and the $a_i \in \{0, 1, \ldots, p-1\}$ are not all equal, then $q \notin \delta_\psi(J(\mathbb{Q}))$.

Proof. (i) See the final paragraph of the proof of Proposition 5.2.
(ii) The restriction $\mathrm{res}_\ell(\chi_i)$ is unramified for all $\ell \neq p_i$, and trivial for all $\ell \in U \setminus \{3\}$ by assumption (3). So we only need to check the local conditions at $p_1, \ldots, p_t$ and 3. By Lemmas 4.1 and 5.1, we know that $\mathrm{im}\,\delta_{\phi,p_i}$ has order p^2, and the natural map $\mathrm{im}\,\delta_{\phi,p_i} \to \mathrm{im}\,\delta_{\psi,p_i}$ is an isomorphism. Chasing around (the local analogue of) the above diagram shows that $\mathrm{im}\,\delta_{\nu,p_i}$ is trivial. It follows by Tate local duality that $\mathrm{im}\,\delta_{\widehat{\nu},p_i}$ is

https://doi.org/10.1017/S1474748024000392 Published online by Cambridge University Press

all of $H^1(\mathbb{Q}_{p_i},\mathbb{Z}/p\mathbb{Z})$. In other words, in the definition of $S^{(\widehat{\nu})}(\widehat{B}/\mathbb{Q})$, there are no local conditions at $p_1,\ldots,p_t$. It is the local condition at 3 that forces us to take differences.
(iii) We take $r=p_i$ in the above description of the pairing. The only primes ℓ that can contribute to the pairing are those in $\{p_1,\ldots,p_t\}\cup U$. For all such primes $\ell\neq p_i$ we have that r is trivial in $\mathbb{Q}_\ell^\times/(\mathbb{Q}_\ell^\times)^p$ by assumptions (1) and (2). Taking $P_\ell=0$ and $\xi_\ell=1$, we see that these primes make no contribution to the pairing. It remains to compute the contribution at $\ell=p_i$. By Lemma 4.1, we have

$$\delta_{\phi,\ell}(P_\ell)=((3^{-3}p_i^{-2})^a(3p_i)^b,(3p_i)^a(3^{-2}p_i^{-2})^b)$$

for some $a,b\in\mathbb{Z}/p\mathbb{Z}$. We know that $(r_1,r_2)\mapsto r_1r_2$ maps this to $r=p_i\in\mathbb{Q}_{p_i}^*/(\mathbb{Q}_{p_i}^*)^p$, and that $\mathbb{Q}_{p_i}^*/(\mathbb{Q}_{p_i}^*)^p$ is generated by 3 and p_i. Therefore, $-2a-b\equiv 0 \pmod p$ and $-a-b\equiv 1 \pmod p$. We solve these to give $a=1$ and $b=-2$. Therefore,

$$\delta_{\phi,\ell}(P_\ell)=(3^{-5}p_i^{-4},3^5p_i^5).$$

and $\xi_\ell=3^{-5}p_i^{-5}$. Therefore,

$$\langle p_i,\sum b_j\chi_j\rangle_{\mathrm{CT}}=\sum b_j((3p_i)^{-5},\mathrm{res}_{p_i}\chi_j)_{p_i}=\frac{-5b_i}{p}.$$

Notice that, since $p_i\equiv 1 \pmod p$, evaluating the local pairing (6.1) reduces to a computation of Hilbert symbols. The formula in the statement of the proposition follows by linearity in the first argument. □

Acknowledgements. The authors thank Michael Stoll for his comments and for organizing Rational Points 2022, where they began working together on this problem. The second author was supported by the Israel Science Foundation (grant No. 2301/20). The authors also thank Ariyan Javanpeykar, Jef Laga and Ariel Weiss for comments on an earlier draft. Finally, we thank Tom Fisher for his suggestions and for letting us include his appendix.

Competing interest. The authors have no competing interest to declare.

References

[1] A. Arsie and A. Vistoli, Stacks of cyclic covers of projective spaces. *Compos. Math.* **140**(3) (2004), 647–666.
[2] M. Bhargava, Z. Klagsbrun, R. J. Lemke Oliver and A. Shnidman, Elements of given order in Tate-Shafarevich groups of abelian varieties in quadratic twist families. *Algebra Number Theory* **15**(3) (2021), 627–655.
[3] R. Bölling, Die Ordnung der Schafarewitsch-Tate-Gruppe kann beliebig gross werden. *Math. Nachr.* **67** (1975), 157–179.
[4] S. Bosch, *Néron Models*, vol. 21. Ergebnisse der Mathematik und ihrer Grenzgebiete (3) [Results in Mathematics and Related Areas (3)]. (Berlin: Springer-Verlag, 1990).
[5] N. Bruin, E. V. Flynn and A. Shnidman, Genus two curves with full $\sqrt{3}$-level structure and Tate-Shafarevich groups. *Sel. Math. New Ser.* **29** (2023), 42.
[6] J. W. S. Cassels, Arithmetic on curves of genus 1, VI. The Tate-Shafarevich group can be arbitrarily large. *J. Reine Angew. Math.* **214** / 215 (1964), 65–70.

https://doi.org/10.1017/S1474748024000392 Published online by Cambridge University Press

[7] K. Česnavičius, Selmer groups as flat cohomology groups. *J. Ramanujan Math. Soc.* **31**(1) (2016), 31–61.
[8] J. W. S. Cassels and E. V. Flynn, *Prolegomena to a Middlebrow Arithmetic of Curves of Genus 2*, vol. 230. LMS–LNS. (Cambridge: Cambridge University Press, 1996).
[9] P. L. Clark and S. Sharif, Period, index and potential Ш. *Algebra Number Theory* **4** (2010), 151–174.
[10] B. Creutz, Potential Ш for abelian varieties. *J. Number Theory* **131** (2011), 2162–2174.
[11] C. Delaunay, Heuristics on class groups and on Tate-Shafarevich groups: the magic of the Cohen-Lenstra heuristics. In *Ranks of Elliptic Curves and Random Matrix Theory*, vol. 341. (London Math. Soc. Lecture Note Ser. Cambridge: Cambridge Univ. Press, 2007), 323–340.
[12] T. Fisher, Some examples of 5 and 7 descent for elliptic curves over Q. *J. Eur. Math. Soc.* **3** (2001), 169–201.
[13] T. A. Fisher, The Cassels-Tate pairing and the Platonic solids. *J. Number Theory* **98**(1) (2003), 105–155.
[14] E. V. Flynn, Arbitrarily large Tate-Shafarevich group on abelian surfaces. *J. Number Theory* **186** (2018), 248–258.
[15] E. V. Flynn, Arbitrarily large 2-torsion in Tate-Shafarevich groups of abelian varieties. *Acta Arith.* **191** (2019), 101–114.
[16] F. Hazama, Hodge cycles on the Jacobian variety of the Catalan curve. *Compos. Math.* **107** (1997), 339–353.
[17] T. Jedrzejak, A note on the torsion of the jacobians of superelliptic curves $y^q = x^p + a$. *Banach Center Publications* **108** (2016), 143–149.
[18] R. Kloosterman, The p-part of the Tate-Shafarevich groups of elliptic curves can be arbitrarily large. *J. Thér. Nombres Bordeaux* **17** (2005), 787–800.
[19] R. Kloosterman and E. F. Schaefer, Selmer groups of elliptic curves that can be arbitrarily large. *J. Number Theory* **99** (2003), 148–163.
[20] K. Kramer, A family of semistable elliptic curves with large Tate-Shafarevich groups. *Proc. Am. Math. Soc.* **89** (1983), 379–386.
[21] S. Lang, *Abelian Varieties*, no. 7. Interscience Tracts in Pure and Applied Mathematics. New York: Interscience Publishers, Inc.; (London: Interscience Publishers Ltd, 1959).
[22] F. Lemmermeyer, On Tate-Shafarevich groups of some elliptic curves. In *Algebraic Number Theory and Diophantine Analysis (Graz, 1998)*. (Berlin: de Gruyter, 2000), 277–291.
[23] F. Lemmermeyer and R. Mollin, On Tate-Shafarevich groups of $y^2 = x(x^2 - k^2)$. *Acta Math. Univ. Comenian.* **72** (2003), 73–80.
[24] C. E. Lind, *Untersuchungen über die rationalen Punkte der ebenen kubischen Kurven vom Geschlecht Eins*. PhD dissertation, (Univ. Uppsala, 1940).
[25] D. W. Masser, Specialization of endomorphism rings of abelian varieties. *Bulletin de la S.M.F.* **124** (1996), 457–476.
[26] K. Matsuno, Construction of elliptic curves with large Iwasawa λ-invariants and large Tate-Shafarevich groups. *Manuscripta Math.* **122** (2007), 289–304.
[27] J. S. Milne, Jacobian varieties. In G. Cornell and J. H. Silverman (eds), *Arithmetic Geometry*. (New York: Springer-Verlag, 1986).
[28] J. S. Milne *Arithmetic Duality Theorems*, second edition. (Charleston, SC: BookSurge, LLC, 2006).
[29] D. Mumford, *Abelian Varieties*, vol. 5. Tata Institute of Fundamental Research Studies in Mathematics. (London: Oxford University Press, 1970).

[30] B. Poonen and E. Schaefer, Explicit descent for Jacobians of cyclic covers of the projective line. *J. Reine Angew. Math.* **488** (1997), 141–188.

[31] B. Poonen and M. Stoll, The Cassels-Tate pairing on polarized abelian varieties. *Ann. of Math. (2)* **150**(3) (1999), 1109–1149.

[32] L. Radičević, Explicit realization of elements of the Tate-Shafarevich group constructed from Kolyvagin classes. *Res. Number Theory* **8**(4), Paper No. 72, (2022), 25 pp.

[33] H. Reichardt, Einige im Kleinen überall lösbare, im Grossen unlösbare diophantische Gleichun-gen. *J. Reine Angew. Math.* **184** (1942), 12–18.

[34] E. F. Schaefer, Computing a Selmer group of a Jacobian using functions on the curve. *Math. Ann.* **310** (1998), 447–471.

[35] E. S. Selmer, The Diophantine equation $ax^3 + by^3 + cz^3 = 0$. *Acta Math.* **85** (1951), 203–362.

[36] A. Shnidman, Quadratic twists of abelian varieties with real multiplication. *Int. Math. Res. Not.* **2021**(5) (2021), 3267–3298.

[37] A. Shnidman and A. Weiss, Elements of prime order in Tate-Shafarevich groups of abelian varieties over Q. *Forum Math. Sigma* **10**, Paper No. e98, (2022), 10 pp.