J. Aust. Math. Soc. **102** (2017), 316–330
doi:10.1017/S1446788716000306

ON SELMER RANK PARITY OF TWISTS

MAJID HADIAN✉ and MATTHEW WEIDNER

(Received 25 November 2015; accepted 7 May 2016; first published online 28 September 2016)

Communicated by W. Zudilin

Abstract

In this paper we study the variation of the p-Selmer rank parities of p-twists of a principally polarized Abelian variety over an arbitrary number field K and show, under certain assumptions, that this parity is periodic with an explicit period. Our result applies in particular to principally polarized Abelian varieties with full K-rational p-torsion subgroup, arbitrary elliptic curves, and Jacobians of hyperelliptic curves. Assuming the Shafarevich–Tate conjecture, our result allows one to classify the rank parities of all quadratic twists of an elliptic or hyperelliptic curve after a finite calculation.

2010 *Mathematics subject classification*: primary 11G05; secondary 11G10.

Keywords and phrases: elliptic curves, Abelian varieties, Selmer rank parity, p-twist.

1. Introduction

In this paper we study the behaviour of the p-Selmer rank in families of p-twists of principally polarized Abelian varieties over arbitrary number fields. Our main result is that, under certain conditions on the Abelian variety, the parity of the p-Selmer rank is periodic with an explicit period (see Theorem 4.6, Corollary 4.7, and the following remarks). This is proved by using known results which write the variation of the p-Selmer rank under p-twist as a sum of local invariants and which evaluate those local invariants in certain cases (see Theorem 4.4).

Calculating arithmetic ranks of elliptic curves, and more generally Abelian varieties, is a very difficult problem in Diophantine geometry. As of today, this problem remains wide open in general, theoretically and computationally. In various forms, it is related to many long-standing open problems, such as the Birch and Swinnerton-Dyer conjecture. Many recent attempts at progress in this field have involved studying the Selmer rank and its parity. Given that the Selmer rank provides an upper bound for the arithmetic rank and, assuming the Shafarevich–Tate conjecture, in certain cases (see Remark 4.10) its parity differs by a simple factor from the parity of the arithmetic rank, any information on Selmer ranks and their parities can be used in the study of arithmetic ranks.

As an example, consider Goldfeld's conjecture about elliptic curves over $\mathbb{Q}$ (see [1, Conjecture B]). This predicts that among quadratic twists of a fixed elliptic curve E over $\mathbb{Q}$, half have rank 0 and half have rank 1. Assuming the Shafarevich–Tate conjecture, this would imply that half of the quadratic twists of E have even Selmer rank and half have odd Selmer rank. Now, it would be very interesting if one could prove statements like this concerning Selmer ranks without assuming big conjectures such as Goldfeld or Shafarevich–Tate.

In fact, there has been much recent interest in studying the variation of Selmer ranks and their parities. For example, Klagsbrun, Mazur and Rubin prove the above statement for 2-Selmer rank parities in [3]. As another example, Swinnerton-Dyer in [14] studies the size of 2-Selmer groups of quadratic twists of elliptic curves over $\mathbb{Q}$ with full rational 2-torsion subgroup. Several other mathematicians, including Kane, Kramer and Yu, have considered more general versions of this problem for p-Selmer groups of p-twists of elliptic curves and Jacobians of hyperelliptic curves (see [2, 4, 6, 7, 10, 16], for example). Our work in this paper is inspired by the above literature and gives uniform results that are finer than some of the existing ones. In particular, under certain conditions on the Abelian variety, the periodicity result of Section 4 reduces the problem of finding what portion of twists have even or odd p-Selmer rank to a finite calculation (see the examples given in Section 5). Under certain conditions when $p = 2$, assuming the Shafarevich–Tate conjecture, we can actually completely classify the rank parities of twists after a finite calculation (see Remark 4.10).

In Section 2 we set up some general notation that will be fixed throughout the paper. Section 3 is devoted to reviewing the necessary definitions and results on global metabolic structures, Selmer structures, twisting, and local conditions. This material is gathered from several references, including [3, 5, 6, 8, 10, 16], but in order to give a uniform treatment suitable for our applications we have included our version of it for the reader's convenience. In Section 4 we prove our main results, which imply the periodicity of the p-Selmer ranks together with an explicit period. Finally, in Section 5, we illustrate how our results can be applied to particular examples by calculating the 2-Selmer rank parities for all quadratic twists of two explicit elliptic curves over $\mathbb{Q}$.

2. General notation

Throughout this paper, p denotes a fixed rational prime and K a number field containing a primitive pth root of 1. Fix an algebraic closure $\bar{K}$ of K and let $G_K := \mathrm{Gal}(\bar{K}/K)$ be the absolute Galois group of K. Let $C(K) := \mathrm{Hom}(G_K, \mu_p)$ denote the group of characters of G_K with order dividing p. χ (respectively, 1_K) will denote a nontrivial (respectively, the trivial) character in $C(K)$. Note that by Kummer theory, we can identify $C(K)$ with $K^*/(K^*)^p$.

A will denote a principally polarized Abelian variety over K (i.e. A is defined over K and we have fixed a principal polarization of A over K), and when $\dim_K(A) = 1$ we use the more standard notation E. Let $e_p : A[p] \times A[p] \to \mu_p$ be the nondegenerate

https://doi.org/10.1017/S1446788716000306 Published online by Cambridge University Press

alternating Weil pairing of A. Let Σ denote a fixed finite set of places of K containing all primes of bad reduction for A, all primes above p, and all archimedean places.

For each place v of K, fix an embedding of $\bar{K}$ into the algebraic closure $\bar{K}_v$ of the completion K_v of K at v. This gives an embedding of the absolute Galois group $G_{K_v} := \mathrm{Gal}(\bar{K}_v/K_v)$ into G_K. If v is a finite place, O_v denotes the ring of integers of K_v, k_v the residue field, I_v the inertia subgroup of G_{K_v}, and $G_{k_v} = G_{K_v}/I_v$ the absolute Galois group of k_v.

For any G_K-module M which is a finite-dimensional $\mathbb{F}_p$-vector space and any place v of K, let $\mathrm{loc}_v : H^1(G_K, M) \to H^1(G_{K_v}, M)$ denote the localization map. If M is unramified at v, that is, if I_v acts trivially on M, we define $H^1_{\mathrm{ur}}(G_{K_v}, M)$ to be the unramified subgroup $H^1(G_{k_v}, M) \subset H^1(G_{K_v}, M)$, where the inclusion is induced by the inflation homomorphism. Finally, M^* denotes the Tate twist of the dual of M, i.e.

$$M^* := \mathrm{Hom}_{G_K}(M, \mu_p).$$

3. Preliminary notions and results

3.1. Global metabolic structures. A critical notion we will use in this paper is that of global metabolic structures as developed in [3]. For the reader's convenience, we briefly outline in this section what we will use.

Let V be a finite-dimensional vector space over $\mathbb{F}_p$. Recall that a quadratic form on V is a function $q : V \to \mathbb{F}_p$ such that:

- $q(av) = a^2 q(v)$ for every $a \in \mathbb{F}_p$ and $v \in V$;
- the map $(v, w)_q := q(v + w) - q(v) - q(w)$ is a bilinear form.

A subspace X of V is called a Lagrangian subspace if $q_{|X} = 0$ and $X^\perp = X$ with respect to the bilinear form $(,)_q$. The quadratic space (V, q) is called a metabolic space if V has a Lagrangian subspace and $(,)_q$ is nondegenerate.

All metabolic spaces relevant to our study arise in the following way. Let A be a principally polarized Abelian variety defined over K, and let $A[p]$ denote the p-torsion subgroup of A. Then for each place v of K, the cup product and the Weil pairing induce the local Tate pairing:

$$\langle , \rangle_v : H^1(G_{K_v}, A[p]) \times H^1(G_{K_v}, A[p]) \to H^2(G_{K_v}, \mu_p),$$

which is symmetric and nondegenerate (recall that local Tate duality states that for any Galois module M as above, the pairing $H^1(G_{K_v}, M) \times H^1(G_{K_v}, M^*) \to H^2(G_{K_v}, \mu_p)$ is nondegenerate). Note that if v is a finite place, then it is a well-known fact of local class field theory that $H^2(G_{K_v}, \mu_p) = \mathbb{F}_p$.

A global metabolic structure on $A[p]$ consists of a quadratic form q_v on $H^1(G_{K_v}, A[p])$ for every place v of K, such that:

(1) the quadratic space $(H^1(G_{K_v}, A[p]), q_v)$ is a metabolic space for every v;
(2) for every $v \notin \Sigma$, the unramified cohomology group $H^1_{\mathrm{ur}}(G_{K_v}, A[p])$ is an isotropic subspace with respect to q_v;

https://doi.org/10.1017/S1446788716000306 Published online by Cambridge University Press

(3) for any $c \in H^1(G_K, A[p])$, $\sum_v q_v(\mathrm{loc}_v(c)) = 0$;
(4) the bilinear form induced by q_v is the local Tate pairing $\langle , \rangle_v$ for every v.

We conclude our discussion of global metabolic structures with a result concerning their existence and uniqueness. For this result, if the fixed rational prime p happens to be 2, we need to assume that the Abelian variety A is the Jacobian of a hyperelliptic curve with affine equation $y^2 = f(x)$, where $f(x)$ is an odd-degree separable polynomial. Note that any such Abelian variety comes with a canonical principal polarization.

Proposition 3.1. *Let A be a principally polarized Abelian variety over K, which satisfies the above condition when $p = 2$. Then there is a canonical*[1] *global metabolic structure on $A[p]$.*

Proof. First assume that $p = 2$. In this case, we have assumed that A is the Jacobian of a hyperelliptic curve C, which is defined by an affine equation $y^2 = f(x)$ for a separable polynomial f of odd degree. Let O denote the unique point at infinity of C and consider the Abel–Jacobi map $j : C \to A$ that sends a point P of C to the class of $P - O$. There is a corresponding theta divisor and a Heisenberg group $\mathcal{H}$ that sits in a short exact sequence of group schemes over K_v (see [16, Section 5] and [10, Section 4]):

$$1 \to \mathbb{G}_m \to \mathcal{H} \to A[2] \to 1. \tag{3.1}$$

The desired quadratic form q_v is then induced by the connecting homomorphism

$$H^1(G_{K_v}, A[2]) \xrightarrow{\delta} H^2(G_{K_v}, \bar{K}_v^*) \subset \mathbb{Q}/\mathbb{Z}$$

corresponding to the short exact sequence (3.1). It is shown in [16, Lemma 5.8 and comment after Lemma 5.2] and [10, Proposition 4.9] that this construction defines a global metabolic structure on $A[2]$.

Now assume that $p > 2$ is an odd prime. For each place v of K, there is a unique quadratic form

$$q_v(x) := \tfrac{1}{2}\langle x, x\rangle_v$$

inducing the local Tate pairing. It follows from [9, Theorem I.2.6] that for $v \notin \Sigma$, $H^1_{\mathrm{ur}}(G_{K_v}, A[p])$ is a Lagrangian subspace of $H^1(G_{K_v}, A[p])$. For the third part of the definition, note that for any $c \in H^1(G_K, A[p])$, $\sum_v q_v(\mathrm{loc}_v(c)) = \frac{1}{2}\sum_v \langle \mathrm{loc}_v(c), \mathrm{loc}_v(c)\rangle_v$ is a multiple of the sum of local invariants of an element of $\mathrm{Br}(K)$, hence is zero. □

Remark 3.2. It follows from the proof of the above proposition that if p is odd, then there is in fact a unique global metabolic structure on $A[p]$.

[1] When $p = 2$, the global metabolic structure depends on our choice of rational Weierstrass point for A.

https://doi.org/10.1017/S1446788716000306 Published online by Cambridge University Press

3.2. Selmer structures. A Selmer structure $\mathcal{S}$ for $A[p]$ consists of an $\mathbb{F}_p$-subspace $H^1_{\mathcal{S}}(G_{K_v}, A[p])$ of $H^1(G_{K_v}, A[p])$ for every place v of K, such that $H^1_{\mathcal{S}}(G_{K_v}, A[p]) = H^1_{\mathrm{ur}}(G_{K_v}, A[p])$ for all but finitely many v. We say that $\mathcal{S}$ is Lagrangian if for every v, $H^1_{\mathcal{S}}(G_{K_v}, A[p])$ is a Lagrangian subspace of $H^1(G_{K_v}, A[p])$ with respect to the canonical global metabolic structure (see Proposition 3.1). The Selmer group associated to $\mathcal{S}$ is defined as

$$H^1_{\mathcal{S}}(G_K, A[p]) := \mathrm{Ker}\Big(H^1(G_K, A[p]) \to \bigoplus_v (H^1(G_{K_v}, A[p])/H^1_{\mathcal{S}}(G_{K_v}, A[p]))\Big),$$

where the sum runs over all places v of K. Note that the Selmer group is finite, since it consists of cocycles which are unramified outside of a finite set of places. The following result is taken from [3], although they only state and prove the claim when $A[p]$ has rank 2 over $\mathbb{F}_p$.

THEOREM 3.3. *Suppose that $\mathcal{S}$ and $\mathcal{S}'$ are Lagrangian Selmer structures for $A[p]$. Then*

$$\begin{aligned}&\dim_{\mathbb{F}_p}(H^1_{\mathcal{S}}(G_K, A[p])) - \dim_{\mathbb{F}_p}(H^1_{\mathcal{S}'}(G_K, A[p]))\\ &\quad\equiv \sum_v \dim_{\mathbb{F}_p}(H^1_{\mathcal{S}}(G_{K_v}, A[p])/(H^1_{\mathcal{S}}(G_{K_v}, A[p]) \cap H^1_{\mathcal{S}'}(G_{K_v}, A[p]))) \bmod 2, \quad (3.2)\end{aligned}$$

where the sum is taken over all places v of K.

PROOF. If necessary, enlarge Σ to a finite set of places Σ' outside of which $H^1_{\mathcal{S}}(G_{K_v}, A[p]) = H^1_{\mathcal{S}'}(G_{K_v}, A[p]) = H^1_{\mathrm{ur}}(G_{K_v}, A[p])$, and note that the right-hand sum in (3.2) is finite since we only have to sum across $v \in \Sigma'$. Let $V := \bigoplus_{v\in\Sigma'} H^1(G_{K_v}, A[p])$, let $\mathrm{loc}_{\Sigma'} : H^1(G_K, A[p]) \to V$ denote the direct sum of the localization maps, and define

$$H^1_{\Sigma'}(G_K, A[p]) := \mathrm{Ker}\Big(H^1(G_K, A[p]) \to \bigoplus_{v\notin\Sigma'} (H^1(G_{K_v}, A[p])/H^1_{\mathrm{ur}}(G_{K_v}, A[p]))\Big).$$

Now consider the following subspaces of the metabolic space $(V, \bigoplus_{v\in\Sigma'} q_v)$:

- $X := \bigoplus_{v\in\Sigma'} H^1_{\mathcal{S}}(G_{K_v}, A[p])$;
- $Y := \bigoplus_{v\in\Sigma'} H^1_{\mathcal{S}'}(G_{K_v}, A[p])$;
- $Z := \mathrm{loc}_{\Sigma'}(H^1_{\Sigma'}(G_K, A[p]))$.

In terms of these subspaces, the claim is equivalent to showing

$$\dim_{\mathbb{F}_p}(H^1_{\mathcal{S}}(G_K, A[p])) - \dim_{\mathbb{F}_p}(H^1_{\mathcal{S}'}(G_K, A[p])) \equiv \dim_{\mathbb{F}_p}(X/(X \cap Y)) \bmod 2.$$

First note that

$$\begin{aligned}B := \mathrm{Ker}\Big(&H^1(G_K, A[p]) \to \Big(\bigoplus_{v\notin\Sigma'} (H^1(G_{K_v}, A[p])/H^1_{\mathrm{ur}}(G_{K_v}, A[p]))\Big)\\ &\oplus\Big(\bigoplus_{v\in\Sigma'} H^1(G_{K_v}, A[p])\Big)\Big)\end{aligned}$$

https://doi.org/10.1017/S1446788716000306 Published online by Cambridge University Press

sits in short exact sequences of the form

$$0 \to B \to H^1_{\mathcal{S}}(G_K, A[p]) \xrightarrow{\mathrm{loc}_{\Sigma'}} X \cap Z \to 0,$$

$$0 \to B \to H^1_{\mathcal{S}'}(G_K, A[p]) \xrightarrow{\mathrm{loc}_{\Sigma'}} Y \cap Z \to 0.$$

Therefore, we have

$$\dim_{\mathbb{F}_p}(H^1_{\mathcal{S}}(G_K, A[p])) - \dim_{\mathbb{F}_p}(H^1_{\mathcal{S}'}(G_K, A[p])) = \dim_{\mathbb{F}_p}(Y \cap Z) - \dim_{\mathbb{F}_p}(X \cap Z). \quad (3.3)$$

So it suffices to show that the right-hand side of (3.3) is congruent modulo 2 to $\dim_{\mathbb{F}_p}(X/(X \cap Y))$. But, using [3, Proposition 2.4], this would be the case if all subspaces X, Y, and Z are Lagrangian in V. X and Y are Lagrangian by assumption, so it remains to show that Z is also Lagrangian. From the definition of Z, every element $z \in Z$ has the form $z = \mathrm{loc}_{\Sigma'}(x)$ for some $x \in H^1(G_K, A[p])$ that is unramified away from Σ'. Therefore,

$$\Big(\sum_{v \in \Sigma'} q_v\Big)(z) = \sum_{v \in \Sigma'} q_v(\mathrm{loc}_v(x)) = \sum_{\text{all } v} q_v(\mathrm{loc}_v(x)) = 0,$$

which shows that Z is an isotropic subspace of V. Finally, that Z is a maximal isotropic subspace (i.e. $Z = Z^{\perp}$) follows from global Poitou–Tate duality (see [12, Theorem 1.7.3(ii)]). □

3.3. Twisting. For any nontrivial element $\chi \in C(K)$, let F_χ be the cyclic degree p extension of K corresponding to χ, that is, $F_\chi = \bar{K}^{\mathrm{Ker}(\chi)}$. Following [8, Section 5], let $\mathrm{Res}(-)$ denote the Weil restriction functor, and define A_χ to be the kernel of the map

$$\mathrm{Res}^{F_\chi}_K(A_F) \to A,$$

induced by the trace element in the group ring $\mathbb{Z}[\mathrm{Gal}(F_\chi/K)]$. It is known that A_χ is an Abelian variety of dimension $(p-1)\cdot\dim(A)$ over K, which coincides with the quadratic twist of A by χ when $p = 2$.

Remark 3.4. Note that by Kummer theory, one can identify $C(K)$ with $K^*/(K^*)^p$, and therefore for any nontrivial $d \in K^*/(K^*)^p$, we can similarly define the twist A_d of A by d. In this section, we make all definitions and statements for twists by characters and omit the analogous definitions and statements for twists by elements of $K^*/(K^*)^p$.

It is known that the ring of integers $\mathbb{Z}[\mu_p]$ of $\mathbb{Q}(\mu_p)$ acts on A_χ (see, for example, [8, Lemma 5.4 and Theorem 5.5]). In particular, if $\mathfrak{p}$ denotes the unique prime of $\mathbb{Z}[\mu_p]$ lying above p, then any uniformizer π of $\mathfrak{p}$ acts on A_χ. Let $\mathrm{Sel}^\pi(A_\chi)$ denote the π-Selmer group of A_χ, and put

$$d_p(A_\chi) := \dim_{\mathbb{F}_p}(\mathrm{Sel}^\pi(A_\chi)).$$

There is a canonical G_K-isomorphism $A[p] \cong A_\chi[\pi]$. Indeed, for $p = 2$, where A is supposed to be the Jacobian of a hyperelliptic curve $C : y^2 = f(x)$, it follows from the

https://doi.org/10.1017/S1446788716000306 Published online by Cambridge University Press

fact that $A[2]$ is generated by classes $\{(x_i, 0) - O\}$ where x_i runs through roots of $f(x)$ and O is the point at infinity of C, and for $p > 2$ it is shown in [6, Section 4]. This leads to a canonical identification:

$$H^1(G_{K_v}, A[p]) \xrightarrow{\sim} H^1(G_{K_v}, A_\chi[\pi]). \tag{3.4}$$

Now we will associate a Selmer structure $\mathcal{S}_\chi$ to any character $\chi \in C(K)$ as follows. For any place v, let $H^1_{\mathcal{S}_\chi}(G_{K_v}, A[p])$ be the image under the Kummer map of $A_\chi(K_v)/\pi A_\chi(K_v)$, where we have used the identification (3.4) to identify $H^1(G_{K_v}, A_\chi[\pi])$ with $H^1(G_{K_v}, A[p])$. The following result shows that the resulting Selmer structure $\mathcal{S}_\chi$ is Lagrangian.

Lemma 3.5. *For any character χ in $C(K)$, the Selmer structure $\mathcal{S}_\chi$ defined above is Lagrangian.*

Proof. First assume that $p = 2$. Then each $A_\chi(K_v)/2A_\chi(K_v)$ maps to a Lagrangian subspace of $H^1(G_{K_v}, A_\chi[2])$ by [10, Propositions 4.9 and 4.11]. Then the G_K-isomorphism $A[2] \cong A_\chi[2]$ identifies the canonical global metabolic structures on $A[2]$ and $A_\chi[2]$ by [16, Theorem 5.10], so that the image of $A_\chi(K_v)/2A_\chi(K_v)$ maps isomorphically to a Lagrangian subspace of $H^1(G_{K_v}, A[2])$.

Now assume that $p > 2$ is an odd prime. For each place v, $H^1_{\mathcal{S}_{1_K}}(G_{K_v}, A[p])$ is its own orthogonal complement in $H^1(G_{K_v}, A[p])$ by Tate's local duality, while if $\chi \neq 1_K$, then $H^1_{\mathcal{S}_\chi}(G_{K_v}, A[p])$ is its own orthogonal complement by [6, Proposition 4.4]. They are then Lagrangian subspaces by the definition of the unique global metabolic structure on $A[p]$. □

For any place v of K and any character $\chi \in C(K)$, define the local invariant $\delta_v(A, \chi)$ as

$$\delta_v(A, \chi) := \dim_{\mathbb{F}_p}(H^1_{\mathcal{S}_{1_K}}(G_{K_v}, A[p])/(H^1_{\mathcal{S}_{1_K}}(G_{K_v}, A[p]) \cap H^1_{\mathcal{S}_\chi}(G_{K_v}, A[p]))).$$

Applying Theorem 3.3 to this situation gives the following result.

Theorem 3.6. *For any character $\chi \in C(K)$,*

$$d_p(A) - d_p(A_\chi) \equiv \sum_v \delta_v(A, \chi) \bmod 2,$$

where the sum is taken over all places v of K.

3.4. Local conditions. In this final preliminary part, we will list a number of results that allow us to compute the local invariants $\delta_v(A, \chi)$ in certain situations. Fix a nontrivial character χ in $C(K)$ and a place v of K. Let $F := \bar{K}^{\mathrm{Ker}(\chi)}$ be the associated extension of K and F_w be the localization of F at a place w lying above v.

Lemma 3.7. *Let $N : A(F_w) \to A(K_v)$ be the norm map. Then the identification $H^1_{\mathcal{S}_{1_K}}(G_{K_v}, A[p]) \cong A(K_v)/pA(K_v)$ identifies*

$$H^1_{\mathcal{S}_{1_K}}(G_{K_v}, A[p]) \cap H^1_{\mathcal{S}_\chi}(G_{K_v}, A[p]) = N(A(F_w))/pA(K_v).$$

https://doi.org/10.1017/S1446788716000306 Published online by Cambridge University Press

Proof. This is shown in [16, Proposition 2.17] for $p = 2$ and in [6, Proposition 5.2] for odd p. □

Lemma 3.8. *Let v be a finite place of K not lying above p at which A has good reduction and F/K is unramified. Then $H^1_{S_{1_K}}(G_{K_v}, A[p]) = H^1_{S_\chi}(G_{K_v}, A[p])$ and thus $\delta_v(A,\chi) = 0$.*

Proof. It is known that the norm map $N : A(F_w) \to A(K_v)$ is surjective under our assumptions (see [5, Corollary 4.4]). The claim then follows from Lemma 3.7. □

Lemma 3.9. *Let v be a finite place of K not lying above p at which A has good reduction and F/K is ramified. Then $H^1_{S_{1_K}}(G_{K_v}, A[p]) \cap H^1_{S_\chi}(G_{K_v}, A[p]) = 0$ and thus $\delta_v(A,\chi) = \dim_{\mathbb{F}_p}(A(K_v)[p])$.*

Proof. The natural map $A(K_v)/pA(K_v) \to A(F_w)/pA(F_w)$ is an isomorphism by [16, Lemma 2.11(ii)] when $p = 2$ and by [6, Lemma 5.5(ii)] when $p > 2$. Hence $N(A(F_w)) = pA(K_v)$, so that $\delta_v(A,\chi) = \dim_{\mathbb{F}_p}(H^1_{S_{1_K}}(G_{K_v}, A[p]))$ by Lemma 3.7. The claim then follows by [16, Lemma 2.11(i)] when $p = 2$ and by [6, Lemma 5.4] when $p > 2$. □

4. Periodicity of Selmer rank parity

In this section we use the preliminary results of the above section to show that the p-Selmer rank parities of certain p-twists of the Abelian variety A are periodic with an explicit period. Recall from the previous section that for any character $\chi \in C(K)$ or any element $d \in K^*/(K^*)^p$, A_χ or A_d denotes the corresponding twist, respectively. For any place v of K, the local invariants $\delta_v(A,\chi)$ or $\delta_v(A,d)$ are defined as in Section 3.3.

For any finite place v of K, let m_v be defined as

$$m_v := \begin{cases} \dfrac{e_{v/p}}{p-1}p + 1 & \text{if } v|p, \\ 1 & \text{otherwise,} \end{cases}$$

where $e_{v/p}$ is the ramification index of v over p. Note that m_v is an integer as $\mathbb{Q}(\mu_p) \subset K$ implies $(p-1)|e_{v/p}$. It can be easily checked that $\prod_{v|p} v^{m_v}$ divides 8 (respectively, p^2) when $p = 2$ (respectively, $p > 2$).

Lemma 4.1. *Let v be a finite prime of K. Then a nonzero element α in O_v is a pth power provided that $\mathrm{ord}_v(\alpha - 1) \geq m_v$.*

Proof. For v not lying over p this follows from Hensel's lemma. So let $v|p$ and consider an element $\alpha = 1 + \beta\pi^n$, where π is a uniformizer for v, $n \in \mathbb{N}$ and $\beta \in O_v$. Then we have the binomial expansion

$$\alpha^{1/p} = (1 + \beta\pi^n)^{1/p} = \sum_{i=0}^{\infty} \binom{1/p}{i} \beta^i \pi^{in}.$$

https://doi.org/10.1017/S1446788716000306 Published online by Cambridge University Press

This series converges in K_v so long as the valuations of the terms appearing in the right-hand series tend to infinity. Now, by definition we have

$$\binom{1/p}{i} = \frac{1(1-p)(1-2p)\dots(1-(i-1)p)}{p^i i!}.$$

Using Legendre's formula, we can bound the valuation of this term by

$$\begin{aligned}\operatorname{ord}_v\left(\frac{1(1-p)(1-2p)\dots(1-(i-1)p)}{p^i i!}\right) &\geq -\left(i + \frac{i-1}{p-1}\right)\operatorname{ord}_v(p)\\ &= -\frac{ip-1}{p-1}e_v.\end{aligned}$$

Hence, we want

$$\lim_{i\to\infty}\left(in - \frac{ip-1}{p-1}e_v\right) \to \infty.$$

But this holds precisely when $n \geq m_v$. □

Remark 4.2. The above statement can be proven using local class field theory, but the given proof is direct and easy!

Corollary 4.3. *Let v be a finite place of K. Then two units $c, d \in O_v^*$ have a pth power ratio if and only if they project to the same element in $(O_v/(\pi_v)^{m_v})^*/((O_v/(\pi_v)^{m_v})^*)^p$.*

Proof. One direction is trivial. For the other, first suppose that c and d project to the same element in $O_v/(\pi_v)^{m_v}$. Then $\operatorname{ord}_v(c/d-1) \geq m_v$ and thus the ratio c/d is a pth power by Lemma 4.1. The general case then follows as every pth power in $(O_v/(\pi_v)^{m_v})^*$ has a pth power preimage in O_v, hence all of its preimages are pth powers by the previous case. □

We are now ready to prove the following theorem, which leads to the periodicity of p-Selmer rank parities. For ease of notation, we first introduce a function as follows. For two integers a and b, $(a \,?|\, b)$ takes the value 0 if b is divisible by a and the value 1 otherwise.

Theorem 4.4. *Let $c, d \in K^*$ be such that, for all finite places v in Σ:*

- $\operatorname{ord}_v(c) \equiv \operatorname{ord}_v(d) \bmod p$;
- *$c/(\pi_v^{\operatorname{ord}_v(c)})$ and $d/(\pi_v^{\operatorname{ord}_v(d)})$ have the same projection in $(O_v/(\pi_v)^{m_v})^*/((O_v/(\pi_v)^{m_v})^*)^p$.*

If $p = 2$, assume further that c and d have the same signs at all real embeddings. Then

$$d_p(A_c) - d_p(A_d) \equiv \sum_{v|cd, v\notin\Sigma} ((p \,?|\, \operatorname{ord}_v(c)) + (p \,?|\, \operatorname{ord}_v(d)))\dim_{\mathbb{F}_p}(A(K_v)[p]) \bmod 2. \quad (4.1)$$

https://doi.org/10.1017/S1446788716000306 Published online by Cambridge University Press

Proof. As $d_p(A_c) - d_p(A_d) = (d_p(A) - d_p(A_d)) - (d_p(A) - d_p(A_c))$, it suffices by Theorem 3.6 to compute

$$\sum_v (\delta_v(A, d) - \delta_v(A, c)).$$

For v in Σ, the assumptions on c and d allow us to apply Corollary 4.3 and deduce that $c = x^p d$ for $x \in K_v^*$. Therefore, for every $v \in \Sigma$, we have $A_c \cong A_d$ over K_v and hence $\delta_v(A, c) = \delta_v(A, d)$.

For $v \notin \Sigma$, A has good reduction at v. On the other hand, v is unramified in $K_v(\sqrt[p]{c})$ if and only if $p|\mathrm{ord}_v(c)$. Therefore, using Lemmas 3.8 and 3.9, we have

$$\delta_v(A, c) = (p \,?|\, \mathrm{ord}_v(c))\dim_{\mathbb{F}_p}(A(K_v)[p]).$$

Applying the above equality for all v, and the same equalities with c replaced by d, we get

$$\sum_v (\delta_v(A, d) - \delta_v(A, c)) \equiv \sum_{v \notin \Sigma} ((p \,?|\, \mathrm{ord}_v(c)) + (p \,?|\, \mathrm{ord}_v(d)))\dim_{\mathbb{F}_p}(A(K_v)[p]) \bmod 2.$$

But $(p \,?|\, \mathrm{ord}_v(c)) = (p \,?|\, \mathrm{ord}_v(d)) = 0$ when v does not divide cd. So we can restrict the right-hand sum to $v|cd$, which completes the proof. □

Remark 4.5. In this remark, we show that the right-hand side of (4.1) can actually be effectively computed. Indeed, for any $v|cd$ outside of Σ, A has good reduction at v and so we get a commutative diagram with exact rows as follows:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \hat{A}((\pi_v)) & \longrightarrow & A(K_v) & \longrightarrow & \tilde{A}(k_v) & \longrightarrow & 0 \\ & & \downarrow p & & \downarrow p & & \downarrow p & & \\ 0 & \longrightarrow & \hat{A}((\pi_v)) & \longrightarrow & A(K_v) & \longrightarrow & \tilde{A}(k_v) & \longrightarrow & 0 \end{array}$$

where $\hat{A}$ is the formal group associated to A, $\tilde{A}$ is the reduction of A at v, and k_v is the residue field $O_v/(\pi_v)$. Since p is a unit at v, multiplication by p on $\hat{A}$ is an isomorphism. The snake lemma then implies that $A(K_v)[p] \cong \tilde{A}(k_v)[p]$, and so

$$\begin{aligned} &\sum_{v|cd, v \notin \Sigma} ((p \,?|\, \mathrm{ord}_v(c)) + (p \,?|\, \mathrm{ord}_v(d)))\dim_{\mathbb{F}_p}(A(K_v)[p]) \\ &\quad = \sum_{v|cd, v \notin \Sigma} ((p \,?|\, \mathrm{ord}_v(c)) + (p \,?|\, \mathrm{ord}_v(d)))\dim_{\mathbb{F}_p}(\tilde{A}(k_v)[p]). \end{aligned}$$

But for each of the finitely many v in the latter sum, calculating $\tilde{A}(k_v)[p]$ requires a finite amount of calculation.

For $p = 2$ and a one-dimensional Abelian variety A over $\mathbb{Q}$ (i.e. an elliptic curve over $\mathbb{Q}$), we can pursue this even further as follows. Let $y^2 = f(x)$ be a Weierstrass equation for A, where f is a nondegenerate cubic polynomial with integer coefficients. Then for any prime of good reduction l, $\dim_{\mathbb{F}_2}(A(\mathbb{F}_l)[2])$ is odd if and only if f has exactly one solution modulo l. But this happens if and only if $(\Delta \mid l) = -1$, where Δ is the discriminant of f.

https://doi.org/10.1017/S1446788716000306 Published online by Cambridge University Press

THEOREM 4.6. *Let* $G := \mathrm{Gal}(K(A[p])/K)$ *and* $S := \{\sigma \in G : \dim_{\mathbb{F}_p}(A[p]^{\sigma=1})$ *is even*$\}$. *Suppose that either*

(1) $S = G$, *or*
(2) $p = 2$ *and* $[G : S] = 2$.

Then for all c *and* d *satisfying the hypotheses of Theorem 4.4,* $d_p(A_c)$ *and* $d_p(A_d)$ *have the same parity.*

PROOF. First note that, for $v \notin \Sigma$, $K(A[p])/K$ is unramified at v and $A(K_v)[p] = A[p]^{\mathrm{Frob}_v=1}$. Thus, $\dim_{\mathbb{F}_p}(A(K_v)[p])$ is even if and only if $\mathrm{Frob}_v \in S$. So, if condition (1) holds, $\dim_{\mathbb{F}_p}(A(K_v)[p])$ is even for all v outside of Σ and we are done by Theorem 4.4.

Now assume that condition (2) holds, and let $K(\sqrt{\alpha})$ be the fixed field of S, where $\alpha \in K$. For each $v \notin \Sigma$, define $\beta_v := \alpha/(\pi_v^{\mathrm{ord}_v(\alpha)})$. Since $K(A[2])$ is unramified outside of Σ, $K(\sqrt{\alpha})/K$ is unramified outside of Σ as well, so $\beta_v \equiv \alpha \bmod (K_v^*)^2$. Then for any $v \notin \Sigma$, $\dim_{\mathbb{F}_p}(A(K_v)[p])$ is even if and only if Frob_v acts trivially on $\sqrt{\alpha}$, which is if and only if $(\beta_v \mid v) = 1$. We have

$$\begin{aligned}
&\sum_{v \mid cd, v \notin \Sigma} ((2 \mid \mathrm{ord}_v(c)) + (2 \mid \mathrm{ord}_v(d))) \dim_{\mathbb{F}_2}(A(K_v)[2]) \equiv 0 \bmod 2 \\
&\quad\Longleftrightarrow \sum_{v \mid cd, v \notin \Sigma} \mathrm{ord}_v(cd) \dim_{\mathbb{F}_2}(A(K_v)[2]) \equiv 0 \bmod 2 \\
&\quad\Longleftrightarrow \prod_{v \notin \Sigma} \left(\frac{\beta_v}{v}\right)^{\mathrm{ord}_v(cd)} = 1.
\end{aligned}$$

Now for each place v of K, let

$$\rho_v : K_v^* \to \mathrm{Gal}(K_v(\sqrt{cd})/K_v) \hookrightarrow \{\pm 1\}$$

be the local reciprocity map for the extension $K_v(\sqrt{cd})/K_v$. For all $v \notin \Sigma$, we have $\rho_v(\alpha) = \rho_v(\beta_v)$ because the image of ρ_v has exponent dividing 2, and

$$\rho_v(\beta_v) = \left(\frac{\beta_v}{v}\right)^{\mathrm{ord}_v(cd)}$$

because the Legendre symbol is the only nontrivial quadratic character of $(O_K/v)^*$. Hence

$$\begin{aligned}
\prod_{v \notin \Sigma} \left(\frac{\beta_v}{v}\right)^{\mathrm{ord}_v(cd)} &= \prod_{v \notin \Sigma} \rho_v(\alpha) \\
&= \prod_{v} \rho_v(\alpha) \\
&= 1
\end{aligned}$$

where ρ_v is trivial for all $v \in \Sigma$ because then $K_v(\sqrt{cd}) = K_v(\sqrt{c/d}) = K_v$, and where the last line follows by the Artin reciprocity law. □

https://doi.org/10.1017/S1446788716000306 Published online by Cambridge University Press

Corollary 4.7. *If A satisfies the hypotheses of Theorem 4.6, then for nonzero $d \in O_K$ such that $\mathrm{ord}_v(d) < p$ for all primes $v \in \Sigma$, the parity of $d_p(A_d)$ depends only on the signs of d at all real embeddings (if $p = 2$) and the residue class of d modulo*

$$\Big(\prod_{v|p} v^{m_v+p-1}\Big)\Big(\prod_{v\in\Sigma, v\nmid\infty p} v^p\Big).$$

Remark 4.8. If $A[p] \subset A(K)$, then hypothesis (1) of Theorem 4.6 is satisfied.

Remark 4.9. Let $p = 2$. Then by assumption, A is the Jacobian of a curve C defined by an affine equation of the form $y^2 = f(x)$, where $f(x)$ is an odd-degree separable polynomial. Then hypotheses (1) and (2) of Theorem 4.6 are always satisfied. Indeed, let $\deg(f) = 2g + 1$. We know that $A[2]$ is a $2g$-dimensional $\mathbb{F}_2$-vector space spanned by divisors of the form $[(a_i, 0) - O]$ for a_i a root of $f(x)$ and O the point at infinity of C, subject to the constraint

$$\sum_{i=1}^{2g+1} [(a_i, 0) - O] = 0.$$

Hence $K(A[2]) = K(a_1, a_2, \ldots, a_{2g+1})$ is the splitting field for $f(x)$ over K, so that there is a canonical inclusion $\mathrm{Gal}(K(A[2])/K) \subset \mathfrak{S}_{2g+1}$. By [16, Lemma 2.12], $\dim_{\mathbb{F}_p}(A[2]^{\sigma=1})$ is even if and only if $\sigma \in \mathfrak{S}_{2g+1}$ consists of an odd number of orbits. Since $\deg(f)$ is odd, this is the case if and only if $\sigma \in \mathfrak{A}_{2g+1}$. Hence, in the notation of Theorem 4.6, $S = \mathrm{Gal}(K(A[2])/K) \cap \mathfrak{A}_{2g+1}$, which is a subgroup of index 1 or 2.

Remark 4.10. In the situation of Remark 4.9, we additionally gain information about the rank parity of twists. Indeed, the Cassels–Tate pairing on the Shafarevich–Tate group is alternating (see [11, Corollaries 4 and 7], noting that A has a K-rational point at infinity). Hence assuming the Shafarevich–Tate conjecture,

$$\mathrm{rank}(A_d/K) \equiv d_2(A_d) - \dim_{\mathbb{F}_2}(A(K)[2]) \bmod 2.$$

Now $\dim_{\mathbb{F}_2}(A(K)[2])$ is computable, using the above description of $A[2]$. Then since the conditions of Theorem 4.4 partition the $d \in K^*$ into finitely many classes, we can, assuming the Shafarevich–Tate conjecture, classify the rank parity of A_d/K as a function of d after a finite calculation.

Example 4.11. When hypotheses (1) and (2) of Theorem 4.6 are not satisfied, it is possible for its conclusion to fail. For example, let $p = 3$, $K = \mathbb{Q}(\mu_3)$, and E/K be the elliptic curve $y^2 = x^3 - 7x + 3$. Using SAGE [13, 15], we find that E has bad reduction at 2, $-35\zeta_3 - 32$, and $-35\zeta_3 - 3$. Also, $\prod_{v|p} v^{m_v}$ divides 9, so $c = 1$ and $d = (1 + \zeta_3) \cdot 9 \cdot 2 \cdot (-35\zeta_3 - 32) \cdot (-35\zeta_3 - 3) + 1$ satisfy the hypotheses of Theorem 4.4. By Theorem 4.4 and Remark 4.5, $d_3(E) - d_3(E_d) \equiv \sum_{v|d} \dim_{\mathbb{F}_3}(\tilde{E}(k_v)[3]) \bmod 2$. But using SAGE again, we find that $\sum_{v|d} \dim_{\mathbb{F}_3}(\tilde{E}(k_v)[3]) = 1$.

https://doi.org/10.1017/S1446788716000306 Published online by Cambridge University Press

TABLE 1. 2-Selmer rank parities for positive squarefree twists of $y^2 = x^3 - x$.

$d \bmod 8$	1	2	3	5	6	7
$d_2(E_d) \bmod 2$	0	0	0	1	1	1

5. Some examples

In this final section, we give two examples to demonstrate our results when $p = 2$ and A is an elliptic curve, which will be denoted by E. Note that hypotheses (1) and (2) of Theorem 4.6 are always satisfied in this case by Remark 4.9.

EXAMPLE 5.1. Let $K = \mathbb{Q}$, and let $E/\mathbb{Q} : y^2 = x^3 - x$ be the congruent number curve. We wish to classify the 2-Selmer rank parities of twists by positive squarefree d. The only prime of bad reduction is 2, so by Corollary 4.7, the parity of $d_2(E_d)$ for positive squarefree d depends only on the residue class of d modulo 16. In fact, Theorem 4.6 shows that when d is also odd, $d_2(E_d)$ only depends on the residue class of d modulo 8. By explicit computation using SAGE [13, 15], $d_2(E) \equiv d_2(E_3) \equiv 0$ modulo 2 and $d_2(E_5) \equiv d_2(E_7) \equiv 1$ modulo 2, so all twists by 1 or 3 modulo 8 have even 2-Selmer rank while all twists by 5 or 7 modulo 8 have odd 2-Selmer rank. Similarly, $d_2(E_2) \equiv d_2(E_{10}) \equiv 0$ modulo 2 and $d_2(E_6) \equiv d_2(E_{14}) \equiv 1$ modulo 2, so all twists of E by 2 or 10 modulo 16 have even 2-Selmer rank while all twists by 6 or 14 modulo 16 have odd 2-Selmer rank. In summary, we have Table 1.

Note that because $d_2(E_2) \equiv d_2(E_{10})$ modulo 2 and $d_2(E_6) \equiv d_2(E_{14})$ modulo 2, the 2-Selmer rank parities have period 8 instead of 16. In particular, this gives a new proof that, assuming the Shafarevich–Tate conjecture, all positive $d \equiv 5, 6, 7$ modulo 8 are congruent numbers.

EXAMPLE 5.2. Let $K = \mathbb{Q}(\sqrt{-2})$, and let $E/K : y^2 + xy + y = x^3 + x^2 - 3x - 1$ be the elliptic curve in [3, Example 7.11]. The finite primes of bad reduction for E are $\sqrt{-2}$ and 29, with $m_{\sqrt{-2}} = 5$ and $m_{29} = 1$. Then the conditions of Theorem 4.6 divide the elements d of K^* into 64 classes, indexed by a choice of:

- $\operatorname{ord}_{\sqrt{-2}}(d) \bmod 2 \in \{0, 1\}$;
- $\operatorname{ord}_{29}(d) \bmod 2 \in \{0, 1\}$;
- $\frac{d}{(\sqrt{-2})^{\operatorname{ord}_{\sqrt{-2}}(d)}} \in \frac{(O_{\sqrt{-2}}/(\sqrt{-2})^5)^*}{((O_{\sqrt{-2}}/(\sqrt{-2})^5)^*)^2} = \{\pm 1, \pm 3, \pm(1 - \sqrt{-2}), \pm(3 + \sqrt{-2})\}$; and
- $\frac{d}{29^{\operatorname{ord}_{29}(d)}} \in \frac{(O_{29}/(29))^*}{((O_{29}/(29))^*)^2} = \{1, 7 + 12\sqrt{-2}\}$.

Using SAGE again, we find that the four classes in Table 2 have 2-Selmer rank parity 0, while the rest have 2-Selmer rank parity 1.

In summary, for squarefree $d \in O_K$, $d_2(E_d) \equiv 0 \bmod 2$ if and only if d is a unit at $\sqrt{-2}$ and a square modulo $(\sqrt{-2})^5$.

This agrees with the distribution results of [3, Example 7.11], as follows. For real numbers $X > 0$, let

$$C(K, X) := \{d \in O_K : d \text{ is squarefree and divisible only by primes } \mathfrak{q} \text{ with } \mathbf{N}\mathfrak{q} \le X\}.$$

https://doi.org/10.1017/S1446788716000306 Published online by Cambridge University Press

TABLE 2. Classes of twists of $E/\mathbb{Q}(\sqrt{-2}) : y^2 + xy + y = x^3 + x^2 - 3x - 1$ with even 2-Selmer rank.

$\operatorname{ord}_{\sqrt{-2}}(d) \bmod 2$	0	0	0	0
$\operatorname{ord}_{29}(d) \bmod 2$	0	0	1	1
$\dfrac{d}{(\sqrt{-2})^{\operatorname{ord}_{\sqrt{-2}}(d)}} \in \dfrac{(O_{\sqrt{-2}}/(\sqrt{-2})^5)^*}{((O_{\sqrt{-2}}/(\sqrt{-2})^5)^*)^2}$	1	1	1	1
$\dfrac{d}{29^{\operatorname{ord}_{29}(d)}} \in \dfrac{(O_{29}/(29))^*}{((O_{29}/(29))^*)^2}$	1	$7 + 12\sqrt{-2}$	1	$7 + 12\sqrt{-2}$

For $X \geq 2$, half of the $d \in C(K, X)$ are units at $\sqrt{-2}$. To count how many of these units are squares modulo $(\sqrt{-2})^5$, let L be the ray class group of $(\sqrt{-2})^5$ over K, so that $(O_K/(\sqrt{-2})^5)^* \cong \operatorname{Gal}(L/K)$ via the Artin map. Since $|((O_{\sqrt{-2}}/(\sqrt{-2})^5)^*)^2| = 2$ and $|(O_{\sqrt{-2}}/(\sqrt{-2})^5)^*| = 16$, it follows from the Chebotarev density theorem applied to L/K that

$$\lim_{X\to\infty} \frac{|\{d \in C(K, X) : d \text{ is a unit at } \sqrt{-2} \text{ and } d \in ((O_{\sqrt{-2}}/(\sqrt{-2})^5)^*)^2\}|}{|\{d \in C(K, X) : d \text{ is a unit at } \sqrt{-2}\}|} = \frac{1}{8}.$$

Hence,

$$\lim_{X\to\infty} \frac{|\{d \in C(K, X) : d_2(E_d) \text{ is even}\}|}{|C(K, X)|} = \frac{1}{16},$$

as expected.

Acknowledgements

We would like to thank the referee for making useful comments. The second author would like to thank the Caltech SFP office for supporting his research on this project.

References

[1] D. Goldfeld, *Conjectures on Elliptic Curves over Quadratic Fields*, Lecture Notes in Mathematics 751 (Springer, New York, 1979), 108–118.
[2] D. M. Kane, 'On the ranks of the 2-Selmer groups of twists of a given elliptic curve', *Algebra & Number Theory* **5** (2013), 1253–1297.
[3] Z. Klagsbrun, B. Mazur and K. Rubin, 'Disparity in Selmer ranks of quadratic twists of elliptic curves', *Ann. of Math.* (2) **178**(1) (2013), 287–320.
[4] K. Kramer, 'Arithmetic of elliptic curves upon quadratic extensions', *Trans. Amer. Math. Soc.* **264** (1981), 121–135.
[5] B. Mazur, 'Rational points of abelian varieties with values in towers of number fields', *Invent. Math.* **18**(3–4) (1972), 183–266.
[6] B. Mazur and K. Rubin, 'Finding large Selmer rank via an arithmetic theory of local constants', *Ann. of Math.* (2) **166**(2) (2007), 579–612.
[7] B. Mazur and K. Rubin, 'Ranks of twists of elliptic curves and Hilbert's tenth problem', *Invent. Math.* **181**(3) (2010), 541–575.

https://doi.org/10.1017/S1446788716000306 Published online by Cambridge University Press

[8] B. Mazur, K. Rubin and A. Silverberg, 'Twisting commutative algebraic groups', *J. Algebra* **314**(1) (2007), 419–438.
[9] J. S. Milne, *Arithmetic Duality Theorems*, Perspectives in Mathematics 1 (Academic Press, Boston, 1986).
[10] B. Poonen and E. Rains, 'Random maximal isotropic subspaces and Selmer groups', *J. Amer. Math. Soc.* **25**(1) (2012), 245–269.
[11] B. Poonen and M. Stoll, 'The Cassels–Tate pairing on polarized Abelian varieties', *Ann. of Math.* (2) **150**(3) (1999), 1109–1149.
[12] K. Rubin, *Euler Systems*, Annals of Mathematics Studies (Princeton University Press, Princeton, NJ, 2000).
[13] W. A. Stein *et al.*, *Sage Mathematics Software (Version 6.4.1). The Sage Developement Team (2014)*, http://www.sagemath.org.
[14] P. Swinnerton-Dyer, 'The effect of twisting on the 2-Selmer group', *Math. Proc. Cambridge Philos. Soc.* **145**(3) (2008), 513–526.
[15] The PARI Group, *Bordeaux (Version 2.7.0) (2014)*, http://pari.math.u-bordeaux.fr/.
[16] M. Yu, 'Selmer ranks of twists of hyperelliptic curves and superelliptic curves'. PhD Thesis, UC Irvine.

MAJID HADIAN, California Institute of Technology,
Department of Mathematics, Pasadena, CA 91125, USA
e-mail: hadian@caltech.edu

MATTHEW WEIDNER, California Institute of Technology,
Department of Mathematics, Pasadena, CA 91125, USA
e-mail: mweidner@caltech.edu

https://doi.org/10.1017/S1446788716000306 Published online by Cambridge University Press