ARBITRARILY LARGE TATE-SHAFAREVICH GROUP ON ABELIAN SURFACES

E.V. FLYNN

Abstract. We outline a method for demonstrating arbitrarily large Tate-Shafarevich groups which does not require explicit homogenous spaces, and we show that the Tate-Shafarevich groups over $\mathbb{Q}$ of absolutely simple Abelian surfaces (in particular, their 2-torsion) can be arbitrarily large.

1. Introduction

The 2-torsion and 3-torsion of the Tate-Shafarevich group of an elliptic curve over $\mathbb{Q}$ was shown to be arbitrarily large in work of Cassels [2], Bölling [1] and Kramer [9]; more recently, Fisher [6] showed that the 5-torsion can be arbitrarily large and Matsuno [12] that the 7-torsion and 13-torsion can be arbitrarily large. Lemmermeyer [10] showed that the 2-torsion of the Tate-Shafarevich group of an elliptic curve over $\mathbb{Q}$ is arbitrarily large amongst quadratic twists of a specific curve, and there is a similar result of Lemmermeyer and Molling in [11]. We note also the work of Kloosterman and Schaefer [8], that the p-Selmer groups of an elliptic curve over $\mathbb{Q}$ can be arbitrarily large for $p = 5, 7, 13$, and for any p over number fields of degree which is bounded for each p; Kloosterman [7] has also shown that, for any p, the p-torsion of the Tate-Shafarevich group can be made arbitrarily large for an elliptic curve over a number fiend of degree which is bounded for each p. For Abelian varieties, Creutz [5] 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, generalising work of Clark and Sherif [4].

Our interest here will be in finding arbitrarily large Tate-Shafarevich group over $\mathbb{Q}$ on something other than an elliptic curve, and a natural place to investigate is amongst absolutely simple abelian surfaces over $\mathbb{Q}$. The method of Creutz requires field extensions. The methods for elliptic curves over $\mathbb{Q}$ of Lemmermeyer, Mollin and Fisher use explicit models of homogeneous spaces and are difficult to generalise directly to higher genus. In the next section we shall initially give a summary of the method of Lemmermeyer and Mollin (for elliptic curves over $\mathbb{Q}$), in which they describe Selmer groups by careful attention to the homogeneous spaces; we give an alternative proof of their result which does not require homogeneous spaces, and so should be more amenable to generalisation to higher genus. In the final section we shall illustrate this by showing that the Tate-Shafarevich groups over $\mathbb{Q}$ of absolutely simple Jacobians of genus 2 curves (in particular, their 2-torsion) can be arbitrarily large.

Date: 25 September, 2017.

1991 *Mathematics Subject Classification.* Primary 11G30; Secondary 11G10, 14H40.

Key words and phrases. Tate-Shafarevich Group, Abelian Surface.

2. An Alternative Approach to an Example of Lemmermeyer and Mollin

We recall the example of Lemmermeyer and Mollin [11], which considers the family of elliptic curves

$$\mathcal{E}_k : y^2 = x(x+k)(x-k) = x(x^2-k^2), \tag{1}$$

with $k \in \mathbb{Q}^*$, which is 2-isogenous to

$$\widehat{\mathcal{E}}_k : y^2 = x(x^2+4k^2), \tag{2}$$

under the 2-isogeny $\phi : \mathcal{E}_k \longrightarrow \widehat{\mathcal{E}}_k : (x,y) \mapsto (y^2/x^2, y + k^2y/x^2)$, and dual isogeny $\hat{\phi}$. We take $k = p_1...p_t$, where t is odd, each prime $p_i \equiv 5 \pmod 8$ and each Legendre$(p_i,p_j) = 1$, for distinct i,j.

We recall also the standard injection (described in Chapter X of [14]) $q^\phi : \widehat{\mathcal{E}}_k(\mathbb{Q})/\phi(\mathcal{E}_k(\mathbb{Q})) \longrightarrow \mathbb{Q}^*/(\mathbb{Q}^*)^2 : (x,y) \mapsto x$ (together with the special cases that the point at infinity $\mathbf{o}$ maps to 1, and $(0,0)$ maps to $4k^2 = 1$ in $\mathbb{Q}^*/(\mathbb{Q}^*)^2$), whose image is given by squarefree integers r such that

$$W_r : r^2\ell^4 + 4k^2m^4 = rn^2, \text{ for some } \ell,m,n \in \mathbb{Z} \text{ with hcf}(\ell,m) = 1. \tag{3}$$

There is the corresponding injection $q^{\hat{\phi}} : \mathcal{E}_k(\mathbb{Q})/\hat{\phi}(\widehat{\mathcal{E}}_k(\mathbb{Q})) \longrightarrow \mathbb{Q}^*/(\mathbb{Q}^*)^2 : (x,y) \mapsto x$ (together with special cases that the point at infinity $\mathbf{o}$ maps to 1, and $(0,0)$ maps to $-k^2 = -1$ in $\mathbb{Q}^*/(\mathbb{Q}^*)^2$), whose image is given by squarefree integers r such that

$$\widehat{W}_r : r^2\ell^4 - k^2m^4 = rn^2, \text{ for some } \ell,m,n \in \mathbb{Z} \text{ with hcf}(\ell,m) = 1. \tag{4}$$

Note that $2^{2+\text{rank}\mathcal{E}_k(\mathbb{Q})} = \#\widehat{\mathcal{E}}_k(\mathbb{Q})/\phi(\mathcal{E}_k(\mathbb{Q})) \cdot \#\mathcal{E}_k(\mathbb{Q})/\hat{\phi}(\widehat{\mathcal{E}}_k(\mathbb{Q}))$. The Selmer group $\text{Sel}^\phi(\mathcal{E}_k/\mathbb{Q})$ can be represented by those r for which $W_r(\mathbb{Q}_p)$ is nonempty for all $p \leqslant \infty$, and similarly for $\text{Sel}^{\hat{\phi}}(\widehat{\mathcal{E}}_k/\mathbb{Q})$. Any r for which W_r or $\widehat{W}_r$ violates the Hasse principle gives a member of the 2-part of $\text{Ш}(\mathcal{E}_k/\mathbb{Q})$. A brief summary of the argument of Lemmermeyer and Mollin in [11] (or at least the portion required to show that the 2-part of $\text{Ш}(\mathcal{E}_k/\mathbb{Q})$ can be arbitrarily large) is as follows. First they show that, for any $r \in \langle p_1,\dots,p_t\rangle$, $\widehat{W}_r$ has points in every $\mathbb{Q}_p$. They then show that, for any $r \in \langle p_1,\dots,p_t\rangle$ with $r \neq 1$, $r \neq k$, $\widehat{W}_r$ has no points over $\mathbb{Q}$, using a nonlocal argument which exploits the factorisation of the left hand side as $(r\ell^2 + km^2)(r\ell^2 - km^2)$.

If we wish to prove similar results in higher dimension, it is preferable to have a line of argument which avoids explicit homogeneous spaces, so we first give an alternative proof of the above result, in a style which does not require them. Note that, if we define $q_p^\phi : \widehat{\mathcal{E}}_k(\mathbb{Q}_p)/\phi(\mathcal{E}_k(\mathbb{Q}_p)) \longrightarrow {\mathbb{Q}_p}^*/({\mathbb{Q}_p}^*)^2 : (x,y) \mapsto x$ then, for any $r \in \mathbb{Q}^*/(\mathbb{Q}^*)^2$, we have $r \in \text{im } q_p^\phi \iff W_r(\mathbb{Q}_p) \neq \emptyset$ (where on the left hand side, we are identifying $r \in \mathbb{Q}^*/(\mathbb{Q}^*)^2$ with its natural image in ${\mathbb{Q}_p}^*/({\mathbb{Q}_p}^*)^2$), and we also note that it is sufficient to check $p = 2,\infty$ and each p_i (and the equivalent definition and statement applies for $q_p^{\hat{\phi}}$).

We first consider $\text{Sel}^\phi(\mathcal{E}_k/\mathbb{Q})$. For $r = p_i$, we have that p_i is square in $\mathbb{R}$ and in $\mathbb{Q}_{p_j}$, for any $j \neq i$, so that $p_i = q_\infty^\phi(\mathbf{o}) \in \text{im } q_\infty^\phi$ and $p_i = q_{p_j}^\phi(\mathbf{o}) \in \text{im } q_{p_j}^\phi$. Since $p_i \equiv 5 \pmod 8$, there exists $\alpha \in \mathbb{Q}_{p_i}^*$ such that $\alpha^2 = -1$ and $2\alpha \in \left(\mathbb{Q}_{p_i}^*\right)^2$. Then $(2\alpha k, 0) \in \widehat{\mathcal{E}}_k(\mathbb{Q}_{p_i})$ and $q_{p_i}^\phi : (2\alpha k, 0) \mapsto 2\alpha k = k = p_i$ in ${\mathbb{Q}_{p_i}}^*/({\mathbb{Q}_{p_i}}^*)^2$. Hence $p_i \in \text{im } q_{p_i}^\phi$. Furthermore, since $k \equiv 5 \pmod 8$, there exists $\beta \in \mathbb{Q}_2^*$ such that $\beta^2 = k(k^2+4k^2)$, and then: $q_2^\phi : (k,\beta) \mapsto k = p_i$ in ${\mathbb{Q}_2}^*/({\mathbb{Q}_2}^*)^2$ so $p_i \in \text{im } q_2^\phi$. We have now shown that any $p_i \in \text{Sel}^\phi(\mathcal{E}_k/\mathbb{Q})$ and so $\text{Sel}^\phi(\mathcal{E}_k/\mathbb{Q})$ contains $\langle p_1,\dots,p_t\rangle$.

We now consider $\mathrm{Sel}^{\hat{\phi}}(\widehat{\mathcal{E}}_k/\mathbb{Q})$. For $r = p_i$, as before, we have that p_i is square in $\mathbb{R}$ and in $\mathbb{Q}_{p_j}$, for any $j \neq i$, so that $p_i = q^{\hat{\phi}}_{\infty}(\mathbf{o}) \in \text{im } q^{\hat{\phi}}_{\infty}$ and $p_i = q^{\hat{\phi}}_{p_j}(\mathbf{o}) \in \text{im } q^{\hat{\phi}}_{p_j}$. Furthermore, $q^{\hat{\phi}}_{p_i} : (k, 0) \mapsto k = p_i$ in ${\mathbb{Q}_{p_i}}^*/({\mathbb{Q}_{p_i}}^*)^2$, so that $p_i \in \text{im } q^{\hat{\phi}}_{p_i}$. Also, $q^{\hat{\phi}}_{2} : (k, 0) \mapsto k = p_i$ in ${\mathbb{Q}_2}^*/({\mathbb{Q}_2}^*)^2$, so that $p_i \in \text{im } q^{\hat{\phi}}_{2}$. Hence $\mathrm{Sel}^{\hat{\phi}}(\widehat{\mathcal{E}}_k/\mathbb{Q})$ also contains $\langle p_1, \ldots, p_t\rangle$. At this stage, we see that the bound on the rank of $\mathcal{E}(\mathbb{Q})$ obtained from combining these two Selmer bounds is at least $2t - 2$.

Our strategy now, rather than attempting a direct argument on any homogenous space, is to find a bound on the rank using complete 2-descent, which differs from $2t-2$ by an arbitrarily large amount as t increases. We first recall the standard Cassels map for complete 2-descent (following Chapter X of [14]):

$$q : \mathcal{E}_k(\mathbb{Q})/2\mathcal{E}_k(\mathbb{Q}) \longrightarrow \mathbb{Q}^*/(\mathbb{Q}^*)^2 \times \mathbb{Q}^*/(\mathbb{Q}^*)^2 : (x, y) \mapsto [x, x+k], \tag{5}$$

whose image is contained in the group generated by the units and the bad finite primes:

$$\text{im } q \leqslant M := \langle -1, 2, p_1, \ldots, p_t\rangle \times \langle -1, 2, p_1, \ldots, p_t\rangle. \tag{6}$$

We exploit the usual commutative diagram (as described, for example, in Chapter 11 of [3] and in [13]).

$$\begin{tikzcd}
\mathcal{E}_k(\mathbb{Q})/2\mathcal{E}_k(\mathbb{Q}) \arrow[r, "q"] \arrow[d, "i_p"] & M \arrow[d, "j_p"] \\
\mathcal{E}_k(\mathbb{Q}_p)/2\mathcal{E}_k(\mathbb{Q}_p) \arrow[r, "q_p"] & M_p
\end{tikzcd} \tag{7}$$

where q_p and M_p are the local equivalents of q and M, and the maps i_p and j_p are induced by the natural injection $\mathbb{Q} \hookrightarrow \mathbb{Q}_p$. If we let $S = \{\infty, 2, p_1, \ldots, p_t\}$, the set of bad finite primes and ∞, we may then compute the 2-Selmer group using

$$\bigcap_{p \in \mathcal{S}} j_p^{-1}(\text{im } q_p) \cong \mathrm{Sel}^{(2)}(\mathcal{E}_k/\mathbb{Q}), \tag{8}$$

which contains im q, and so give an upper bound on the order of $\mathcal{E}_k(\mathbb{Q})/2\mathcal{E}_k(\mathbb{Q})$. We note that $q : (0, 0) \mapsto [-1, k]$ and $(-k, 0) \mapsto [-k, 2]$; for any i, these are independent in ${\mathbb{Q}_{p_i}}^*/({\mathbb{Q}_{p_i}}^*)^2 \times {\mathbb{Q}_{p_i}}^*/({\mathbb{Q}_{p_i}}^*)^2$, and so $\mathcal{E}_k(\mathbb{Q}_{p_i})/2\mathcal{E}_k(\mathbb{Q}_{p_i}) = \langle (0, 0), (-k, 0)\rangle$, using the result that $\mathcal{E}_k(\mathbb{Q}_p)/2\mathcal{E}_k(\mathbb{Q}_p) = \#\mathcal{E}_k(\mathbb{Q}_p)[2]$, when $p \neq 2, \infty$. We note that

$$\begin{aligned}\ker(j_{p_i}) = \langle &[1, -1], [1, p_1], \ldots, [1, p_{i-1}], [1, p_{i+1}], \ldots, [1, p_t], \\ &[-1, 1], [p_1, 1], \ldots, [p_{i-1}, 1], [p_{i+1}, 1], \ldots, [p_t, 1]\rangle,\end{aligned} \tag{9}$$

and so

$$\begin{aligned}j_{p_i}^{-1}(q_{p_i}(\mathcal{E}_k(\mathbb{Q}_{p_i})/2\mathcal{E}(\mathbb{Q}_{p_i})) = \langle &[1, -1], [1, p_1], \ldots, [1, p_t], \\ &[-1, 1], [p_1, 1], \ldots, [p_{i-1}, 1], [p_i, 2], [p_{i+1}, 1], \ldots, [p_t, 1]\rangle.\end{aligned} \tag{10}$$

We now intersect this information over all p_i, and we note that 2 divides the second component if and only if all p_i divide the first component, so that

$$\begin{aligned}\mathrm{Sel}^{(2)}(\mathcal{E}_k/\mathbb{Q}) &\leqslant \bigcap_{p_i} j_{p_i}^{-1}(\text{im } q_{p_i}) \\ &= \langle [1, -1], [1, p_1], \ldots, [1, p_t], [-1, 1], [k, 2]\rangle.\end{aligned} \tag{11}$$

If we had wished, we could also have used $\mathbb{R}$ to remove $[1, -1]$, but this is not needed, since we have already bounded $\#\mathcal{E}_k(\mathbb{Q})/2\mathcal{E}_k(\mathbb{Q})$ above by 2^{t+3} and so the rank of $\mathcal{E}_k(\mathbb{Q})$ by $t + 3 - 2 = t + 1$. The Selmer bound for the rank using descent via 2-isogeny was previously found to be at least $2t - 2$, and we have now shown the

Selmer bound using complete 2-descent is at most $t+1$; therefore the 2-part of $\text{Ш}(\widehat{\mathcal{E}}_k/\mathbb{Q})$ is at least $t-3$, which becomes arbitrarily large as t increases.

We briefly comment on what was needed in the above example in order to force the 2-part of $\text{Ш}(\widehat{\mathcal{E}}_k/\mathbb{Q})$ to become arbitrarily large. For both descent via 2-isogeny and complete 2-descent, there is an a priori bound on the rank of $\mathcal{E}_k(\mathbb{Q})$ of the form $2t+\text{constant}$. First note that for the Selmer bound using descent via 2-isogeny, it was not necessary to compute completely $\widehat{\mathcal{E}}_k(\mathbb{Q}_p)/\phi(\mathcal{E}_k(\mathbb{Q}_p))$ or $\mathcal{E}_k(\mathbb{Q}_p)/\hat{\phi}(\widehat{\mathcal{E}}_k(\mathbb{Q}_p))$, but only to find explicit elements which mapped to sufficiently many $r \in \mathbb{Q}^*/(\mathbb{Q}^*)^2$ that we could be sure the Selmer bound for descent via 2-isogeny was at least $2t+\text{constant}$. For the complete 2-descent, we used (7) and found $\mathcal{E}_k(\mathbb{Q}_{p_i})/2\mathcal{E}_k(\mathbb{Q}_{p_i})$ completely, in order to show that the Selmer bound for complete 2-descent was at most $t+\text{constant}$. Crucial was the role performed by the prime 2, which appeared explicitly when applying the map q to the points of order 2; the condition that 2 was not a quadratic residue mod p_i assisted in lowering the Selmer bound for complete 2-descent. On the other hand, the prime 2 did not appear when applying q^{ϕ} or $q^{\hat{\phi}}$ to $(0,0)$; this is not the entire story, as we still used the information at 2 in our 2-isogeny argument; but it turned out that there were congruence conditions on the p_i which allowed the Selmer bound for descent via 2-isogeny to remain $2t+\text{constant}$.

3. Application in Genus 2

Our strategy in this section will be to play descent via Richelot isogeny against complete 2-descent. There have been a number of examples in the literature which have performed such descents in detail, so the aim here is to give a brief summary. However, it will be necessary to set up the relevants maps in order to convey the keys steps which force the Tate-Shafarevic group to be arbitrarily large. So, we begin with a brief summary of the generalities, following Chapter 11 of [3].

For a curve of genus 2 given by $\mathcal{C} : y^2 = f(x)$, where $f(x) \in \mathbb{Q}[x]$, we let ∞^+, ∞^- denote the points on the non-singular curve that lie over the singular point at infinity on $\mathcal{C}$ when $f(x)$ is sextic; when $f(x)$ is quintic we let ∞ denote the unique such point. We denote members of the Mordell-Weil group of the Jacobian $J(\mathbb{Q})$ by $\{(x_1,y_1),(x_2,y_2)\}$, as a shorthand notation for the divisor class $[(x_1,y_1)+(x_2,y_2)-\infty^+-\infty^-]$, where either $(x_1,y_1),(x_2,y_2) \in \mathcal{C}(\mathbb{Q})$ or they are in some $\mathcal{C}\big(\mathbb{Q}(\sqrt{d})\big)$ and conjugate.

Suppose our curve is of the form

$$\mathcal{C} : y^2 = F(x) = G_1(x)G_2(x)G_3(x), \text{ where } G_j(x) = g_{j2}x^2 + g_{j1}x + g_{j0}, \tag{12}$$

and where each $g_{ji} \in \mathbb{Q}$. Then there is a Richelot isogeny ϕ from J, the Jacobian of $\mathcal{C}$, to $\widehat{J}$, the Jacobian of the following curve.

$$\widehat{\mathcal{C}} : \Delta y^2 = H(X) = L_1(x)L_2(x)L_3(x), \tag{13}$$

where each $L_i(x) = G_j'(x)G_k(x) - G_j(x)G_k'(x)$ (for $[i,j,k] = [1,2,3],[2,3,1],[3,1,2]$), and where $\Delta = \det(g_{ij})$, which we assume to be nonzero. The kernel of ϕ consists of the identity $\mathcal{O}$ and the three divisors of order 2 given by $G_j = 0$. Similarly for the dual isogeny $\hat{\phi} : \widehat{J} \to J$. We have the injections

$$\begin{aligned} q^{\phi} &: \widehat{J}(\mathbb{Q})/\phi\big(J(\mathbb{Q})\big) \longrightarrow M^{\phi} \leqslant \mathbb{Q}^*/(\mathbb{Q}^*)^2 \times \mathbb{Q}^*/(\mathbb{Q}^*)^2 \\ &: \{(x_1,y_1),(x_2,y_2)\} \mapsto [L_1(x_1)L_1(x_2), L_2(x_1)L_2(x_2)], \\ q^{\hat{\phi}} &: J(\mathbb{Q})/\hat{\phi}\big(\widehat{J}(\mathbb{Q})\big) \longrightarrow M^{\hat{\phi}} \leqslant \mathbb{Q}^*/(\mathbb{Q}^*)^2 \times \mathbb{Q}^*/(\mathbb{Q}^*)^2 \\ &: \{(x_1,y_1),(x_2,y_2)\} \mapsto [G_1(x_1)G_1(x_2), G_2(x_1)G_2(x_2)], \end{aligned} \tag{14}$$

where $M^{\phi}, M^{\hat{\phi}}$ are generated by the units and the bad finite primes. Note the following special cases: when x_j is a root of G_i then $G_i(x_j)$ should be taken to be $\prod_{\ell \in \{1,2,3\}\setminus\{i\}} G_\ell(x_j)$; when x_j is a root of L_i then $L_i(x_j)$ should be taken to be $\Delta \prod_{\ell \in \{1,2,3\}\setminus\{i\}} L_\ell(x_j)$; when $F(x)$ has odd degree and $(x_j, y_j) = \infty$ then $G_i(x_j)$ should be taken to be 1; when $H(x)$ has odd degree and $(x_j, y_j) = \infty$ then $L_i(x_j)$ should be taken to be 1 (there are further special cases for when $F(x)$ or $H(x)$ has even degree, but we shall not require these). We also let q_p^{ϕ} and $q_p^{\hat{\phi}}$ denote the analagous maps on $\widehat{J}(\mathbb{Q}_p)/\phi\big(J(\mathbb{Q}_p)\big)$ and $J(\mathbb{Q}_p)/\hat{\phi}\big(\widehat{J}(\mathbb{Q}_p)\big)$, respectively. This provides the maps used in performing descent via Richelot isogeny.

Suppose now that our genus 2 curve has the form

$$\mathcal{C} : y^2 = \lambda(x-e_1)(x-e_2)(x-e_3)(x-e_4)(x-e_5), \text{ with } \lambda \in \mathbb{Q} \text{ and each } e_i \in \mathbb{Q}. \tag{15}$$

Then we have the standard injection

$$\begin{aligned} q :& J(\mathbb{Q})/2J(\mathbb{Q}) \longrightarrow M \leqslant \mathbb{Q}^*/(\mathbb{Q}^*)^2 \times \mathbb{Q}^*/(\mathbb{Q}^*)^2 \times \mathbb{Q}^*/(\mathbb{Q}^*)^2 \times \mathbb{Q}^*/(\mathbb{Q}^*)^2 \\ :& \{(x_1,y_1),(x_2,y_2)\} \mapsto [(x_1-e_1)(x_2-e_1), (x_1-e_2)(x_2-e_2), (x_1-e_3)(x_2-e_3), (x_1-e_4)(x_2-e_4)], \end{aligned} \tag{16}$$

where M is generated by the units and the bad finite primes. Note the following special cases which are not covered by the above definition: when $(x_j, y_j) = \infty$ then $x_j - e_i$ should be taken to be λ; when $(x_j, y_j) = (e_i, 0)$ then $x_j - e_i$ should be taken to be $\lambda \prod_{\ell \in \{1,\dots,5\}\setminus\{i\}} (e_i - e_\ell)$. We have the standard commutative diagram:

$$\begin{tikzcd} J(\mathbb{Q})/2J(\mathbb{Q}) \arrow[r, "q"] \arrow[d, "i_p"] & M \arrow[d, "j_p"] \\ J(\mathbb{Q}_p)/2J(\mathbb{Q}_p) \arrow[r, "q_p"] & M_p \end{tikzcd} \tag{17}$$

where q_p and M_p are the local equivalents of q and M, and the maps i_p and j_p are induced by the natural injection $\mathbb{Q} \hookrightarrow \mathbb{Q}_p$. If we let S consist of $2, \infty$ and all primes dividing the discriminant of $\mathcal{C}$, then we may then compute the 2-Selmer group using

$$\bigcap_{p \in \mathcal{S}} j_p^{-1}(\text{im } q_p) \cong \text{Sel}^{(2)}(J/\mathbb{Q}), \tag{18}$$

which contains im q, and so give an upper bound on the order of $J(\mathbb{Q})/2J(\mathbb{Q})$; one can then deduce an upper bound on the rank r of $J(\mathbb{Q})$, since $2^{4+\text{rank} J(\mathbb{Q})} = \#J(\mathbb{Q})/2J(\mathbb{Q})$. This gives the Selmer bound on the rank using complete 2-descent. In order to determine each im q_p, it is helpful to use the following (equation (11.2.3) of [3]) to know when all of $J(\mathbb{Q}_p)/2J(\mathbb{Q}_p)$ has been found:

$$\#J(\mathbb{Q}_p)/2J(\mathbb{Q}_p) = J(\mathbb{Q}_p)[2]/|2|_p^2. \tag{19}$$

Our aim is to force these bounds to differ by an arbitrarily large amount. The search for likely examples was conducted amongst curves of the form (15), so that both descent via Richelot isogeny and complete

2-descent would be possible working entirely over $\mathbb{Q}$; it turns out to be helpful if $\widehat{\mathcal{C}}$ also completely splits. We also placed the restriction that the prime 3 should appear amongst the components of the images of the points of order 2 under the map q, but should not appear when the map q^{ϕ} is applied to the three points of order 2 given by $L_j = 0$ and similarly for $q^{\hat{\phi}}$. When we apply a quadratic twist by $k = p_1 \ldots p_t$, the a priori bound on the rank is of the form $4t +$ constant, regardless of which method is applied. However, we can hope that, by including a congruence condition on the p_i that forces Legendre$(3, p_i) = -1$, we can reduce this bound for complete 2-descent; by making our other congruence conditions as nice as possible (in the sense of making as many bad primes be quadratic residues modulo other bad primes), we can hope to keep the bound using descent via Richelot isogeny of the form $4t +$ constant.

After some searching, a successful example was found, namely

$$y^2 = F(x) = (x+2)x(x-6)(x+1)(x-7), \tag{20}$$

for which, if we apply the Richelot isogeny using $G_1(x) = x+2, G_2(x) = x(x-6), G_3(x) = (x+1)(x-7)$, then the curve with isogenous Jacobian is $y^2 = 2F(x)$, so that there is real multiplication by $\sqrt{2}$. We also see that 3 performs exactly the desired role (in particular, $q : \{(0,0),(7,0)\} \mapsto [2,3,-6,2]$). We now show our desired result that, if we apply a quadratic twist by $k = p_1 \ldots p_t$, for suitably chosen congruence conditions on the p_i, then we can force our bounds to be arbitrarily far apart.

Theorem 1. *Let $\mathcal{C}_k : y^2 = F_k(x) = (x+2k)x(x-6k)(x+k)(x-7k)$, where $k = p_1 \ldots p_t$ and where $t \in \mathbb{N}$ is arbitrary, each p_i is prime, each Legendre$(p_i, p_j) = 1$, for i, j distinct, each $p_i \equiv 1 \pmod 8$, each $p_i \equiv 2 \pmod 3$ and each $p_i \equiv 1, 2$ or $4 \pmod 7$, and let J_k be the Jacobian of $\mathcal{C}_k$. Then J_k and $\widehat{J}_k$ are absolutely simple, and $\text{Ш}(\widehat{J}_k/\mathbb{Q})[2]$ becomes arbitrarily large as t increases.*

Proof We first note that, using the technique in [15] (also described in Chapter 14 of [3]) at the prime 17 shows J_k and $\widehat{J}_k$ to be absolutely simple.

The set of bad primes is $S = \{\infty, 2, 3, 7, p_1, \ldots, p_t\}$; define also $S' = \{-1, 2, 3, 7, p_1, \ldots, p_t\}$. By Dirichlet's theorem on primes in arithmetic progressions, there exist $p_1, \ldots, p_t$ satisfying the given conditions, for arbitrary $t \in \mathbb{N}$. The congruence conditions give that $-1, 2, 7, p_j$ are squares and $3, p_i$ are nonsquares in $\mathbb{Q}_{p_i}^*$ (for $i \neq j$); they also give that p_i is square in $\mathbb{Q}_2^*, \mathbb{Q}_7^*, \mathbb{Q}_{p_j}^*$ (for $i \neq j$), but p_i is nonsquare in $\mathbb{Q}_3^*, \mathbb{Q}_{p_i}^*$.

We first examine the Selmer bound using descent via Richelot isogeny. Taking $G_1(x) = (x+2k)$, $G_2(x) = x(x-6k)$ and $G_3(x) = (x+k)(x-7k)$, and applying the formula (13), we find that $L_1(x) = -14k^2(x-3k)$, $L_2(x) = (x-k)(x+5k)$, $L_3(x) = -(x-2k)(x+6k)$ and $\Delta = -7k^2$; therefore $\widehat{\mathcal{C}}$ is birationally equivalent over $\mathbb{Q}$ (as can be seen by replacing x with $-x+k$) to $y^2 = 2F_k(x)$, so that J_k is isogenous to a twist of itself.

Let p_i, p_j be distinct. Since $q^{\phi} : \{(-k,0),\infty\} \mapsto [2k, 7] = [p_i p_j, 1]$ in both $\mathbb{Q}_{p_i}^*/(\mathbb{Q}_{p_i}^*)^2 \times \mathbb{Q}_{p_i}^*/(\mathbb{Q}_{p_i}^*)^2$ and $\mathbb{Q}_{p_j}^*/(\mathbb{Q}_{p_j}^*)^2 \times \mathbb{Q}_{p_j}^*/(\mathbb{Q}_{p_j}^*)^2$, and since also $p_i p_j = 1 \bmod (\mathbb{Q}_2^*)^2$, $(\mathbb{Q}_3^*)^2$, $(\mathbb{Q}_7^*)^2$, $(\mathbb{R}^*)^2$ and any $(\mathbb{Q}_{p_k}^*)^2$ (for $k \notin \{i,j\}$), we see that any $[p_i p_j, 1] \in \text{Sel}^{\phi}(J_k/\mathbb{Q})$. Similarly, since $q^{\phi} : \{(0,0),(-k,0)\} \mapsto [2,-k] = [1, p_i p_j]$

in both $\mathbb{Q}_{p_i}^*/(\mathbb{Q}_{p_i}^*)^2 \times \mathbb{Q}_{p_i}^*/(\mathbb{Q}_{p_i}^*)^2$ and $\mathbb{Q}_{p_j}^*/(\mathbb{Q}_{p_j}^*)^2 \times \mathbb{Q}_{p_j}^*/(\mathbb{Q}_{p_j}^*)^2$, and since also $p_ip_j = 1 \bmod (\mathbb{Q}_2^*)^2$, $(\mathbb{Q}_3^*)^2$, $(\mathbb{Q}_7^*)^2$, $(\mathbb{R}^*)^2$ and any $(\mathbb{Q}_{p_k}^*)^2$ (for $k \notin \{i,j\}$), we see that any $[1, p_ip_j] \in \mathrm{Sel}^{\phi}(J_k/\mathbb{Q})$.

It follows that there are at least $2t-2$ independent members of $\mathrm{Sel}^{\phi}(J_k/\mathbb{Q})$; for example, the following are independent: $[p_1p_2, 1], [p_1p_3, 1], \ldots, [p_1p_t, 1]$ and $[1, p_1p_2], [1, p_1p_3], \ldots, [1, p_1p_t]$.

We can now use $q^{\hat{\phi}} : \{(-k, 0), \infty\} \mapsto [k, 7]$, $q^{\hat{\phi}} : \{(0, 0), (-k, 0)\} \mapsto [2, -2k]$ and a virtually identical argument to see that the same elements represent $2t-2$ independent members of $\mathrm{Sel}^{\hat{\phi}}(\widehat{J}_k/\mathbb{Q})$. So, the Selmer bound via Richelot isogeny on the rank of $J_k(\mathbb{Q})$ is at least $2t-2+2t-2-4 = 4t-8$. We have not found the bound precisely, but we have already done enough to see that it grows at rate $4t +$ constant, the same rate as the a priori bound. Note that the prime 3 did not appear in any of the images under q^{ϕ} or $q^{\hat{\phi}}$ which we needed to consider.

We now examine the Selmer bound via complete 2-descent. Under the map q of (16) with $e_1 = -2k$, $e_2 = 0$, $e_3 = 6k$, $e_4 = -k$, we see that $\{(-2k, 0), (7k, 0)\}$, $\{(0, 0), (7k, 0)\}$, $\{(6k, 0), (7k, 0)\}$, $\{(-k, 0), (7k, 0)\}$ map, respectively, to

$$H = \{[k, -14, -2, -2], [2, 3k, -6, 2], [2, 42, -21k, 14], [1, -7, -7, -7k]\}. \tag{21}$$

First consider im q_{p_i}. Note that $\langle S' \rangle \cap (\mathbb{Q}_{p_i}^*)^2 = \langle -1, 2, 7, (p_\ell)_{\text{all } \ell \neq i} \rangle$. We see that the members of H are locally independent and, since $\#J(\mathbb{Q}_{p_i})/2J(\mathbb{Q}_{p_i}) = \#J(\mathbb{Q}_{p_i})[2] = 2^4$, it follows that these give all of im q_{p_i}. Hence

$$\begin{aligned} &j_{p_i}^{-1}\Big(q_{p_i}\big(J(\mathbb{Q}_{p_i})/2J(\mathbb{Q}_{p_i})\big)\Big) \\ &\quad = \langle H, [-1,1,1,1], [1,-1,1,1], [1,1,-1,1], [1,1,1,-1], \\ &\qquad [2,1,1,1], [1,2,1,1], [1,1,2,1], [1,1,1,2], \\ &\qquad [7,1,1,1], [1,7,1,1], [1,1,7,1], [1,1,1,7], \\ &\qquad [p_\ell,1,1,1]_{\text{all } \ell\neq i}, [1,p_\ell,1,1]_{\text{all } \ell\neq i}, [1,1,p_\ell,1]_{\text{all } \ell\neq i}, [1,1,1,p_\ell]_{\text{all } \ell\neq i} \rangle. \end{aligned} \tag{22}$$

Note that $\langle S' \rangle \cap (\mathbb{Q}_2^*)^2 = \langle -7, (p_\ell)_{\text{all } \ell} \rangle$. We see that only three members of H are locally independent and, since $\#J(\mathbb{Q}_2)/2J(\mathbb{Q}_2) = \#J(\mathbb{Q}_2)[2]/|2|_2^2 = 2^6$, it follows that we are still missing three generators, namely $\{(5k, \beta_1), \infty\}$, $\{(-3k, \beta_2), \infty\}$ and $\{(-5k, \beta_3), \infty\}$, where $\beta_1, \beta_2, \beta_3 \in \mathbb{Q}_2^*$ are such that $\beta_1^2, \beta_2^2, \beta_3^2$ equal $F_k(5k), F_k(-3k), F_k(-5k)$, respectively. These map under q_2, respectively, to $[-1,-3,-1,6]$, $[-1,-3,-1,-2]$, $[-3,3,-3,-1]$ so that

$$\begin{aligned} j_2^{-1}\Big(q_2\big(J(\mathbb{Q}_2)/2J(\mathbb{Q}_2)\big)\Big) = \langle H, &[-1,-3,-1,6], [-1,-3,-1,-2], [-3,3,-3,-1], \\ &[-7,1,1,1], [1,-7,1,1], [1,1,-7,1], [1,1,1,-7], \\ &[p_\ell,1,1,1]_{\text{all } \ell}, [1,p_\ell,1,1]_{\text{all } \ell}, [1,1,p_\ell,1]_{\text{all } \ell}, [1,1,1,p_\ell]_{\text{all } \ell} \rangle. \end{aligned} \tag{23}$$

Note that $\langle S' \rangle \cap (\mathbb{Q}_3^*)^2 = \langle -2, 7, (-p_\ell)_{\text{all } \ell} \rangle$. We see that only three members of H are locally independent and, since $\#J(\mathbb{Q}_3)/2J(\mathbb{Q}_3) = \#J(\mathbb{Q}_3)[2] = 2^4$, it follows that we are still missing one generator. When t is odd, this is $\{(k, \gamma_1), \infty\}$, where $\gamma_1 \in \mathbb{Q}_3^*$ is such that $\gamma_1^2 = F_k(k)$. This is mapped by q_3 to $[-3,-1,-1,1]$. When t is even, this is $\{(k(2+i), \gamma_2), (k(2-i), \bar{\gamma}_2)\}$, where $\gamma_2 \in \mathbb{Q}_3(i)^*$ is such that $\gamma_2^2 = F_k(k(2+i))$ and

$\bar{\gamma}_2$ is its conjugate. This is mapped by q_3 to $[-1,-1,-1,1]$. Hence

$$\begin{aligned}j_3^{-1}\Big(q_3\big(J(\mathbb{Q}_3)/2J(\mathbb{Q}_3)\big)\Big) = \langle H, &\{[-3,-1,-1,1] \text{ (when t odd) OR } [-1,-1,-1,1] \text{ (when t even)}\},\\ &[-2,1,1,1],[1,-2,1,1],[1,1,-2,1],[1,1,1,-2],\\ &[7,1,1,1],[1,7,1,1],[1,1,7,1],[1,1,1,7],\\ &[-p_\ell,1,1,1]_{\text{all } \ell},[1,-p_\ell,1,1]_{\text{all } \ell},[1,1,-p_\ell,1]_{\text{all } \ell},[1,1,1,-p_\ell]_{\text{all } \ell}\rangle.\end{aligned} \tag{24}$$

Note that $\langle S'\rangle \cap (\mathbb{Q}_7^*)^2 = \langle 2,-3,(p_\ell)_{\text{all } \ell}\rangle$. We see that the members of H are locally independent and, since $\#J(\mathbb{Q}_7)/2J(\mathbb{Q}_7) = \#J(\mathbb{Q}_7)[2] = 2^4$, it follows that these give all of im q_7. Hence

$$\begin{aligned}j_7^{-1}\Big(q_7\big(J(\mathbb{Q}_7)/2J(\mathbb{Q}_7)\big)\Big) = \langle H, &[2,1,1,1],[1,2,1,1],[1,1,2,1],[1,1,1,2],\\ &[-3,1,1,1],[1,-3,1,1],[1,1,-3,1],[1,1,1,-3],\\ &[p_\ell,1,1,1]_{\text{all } \ell},[1,p_\ell,1,1]_{\text{all } \ell},[1,1,p_\ell,1]_{\text{all } \ell},[1,1,1,p_\ell]_{\text{all } \ell}\rangle.\end{aligned} \tag{25}$$

Finally note that $\langle S'\rangle \cap (\mathbb{R}^*)^2 = \langle 2,3,7,(p_\ell)_{\text{all } \ell}\rangle$. We see that two members of H are locally independent and, since $\#J(\mathbb{R})/2J(\mathbb{R}) = \#J(\mathbb{Q}_7)[2]/|2|_\infty^2 = 2^2$, it follows that these give all of im q_∞. Hence

$$\begin{aligned}j_\infty^{-1}\Big(q_\infty\big(J(\mathbb{Q}_\infty)/2J(\mathbb{Q}_\infty)\big)\Big) = \langle H, &[2,1,1,1],[1,2,1,1],[1,1,2,1],[1,1,1,2],\\ &[3,1,1,1],[1,3,1,1],[1,1,3,1],[1,1,1,3],\\ &[7,1,1,1],[1,7,1,1],[1,1,7,1],[1,1,1,7],\\ &[p_\ell,1,1,1]_{\text{all } \ell},[1,p_\ell,1,1]_{\text{all } \ell},[1,1,p_\ell,1]_{\text{all } \ell},[1,1,1,p_\ell]_{\text{all } \ell}\rangle.\end{aligned} \tag{26}$$

The intersection of (22), (23), (24), (25) and (26) gives the 2-Selmer group; it is straightforward to check that this intersection is contained inside

$$\langle H,[p_\ell,1,1,1]_{\text{all } \ell},[1,p_\ell,1,1]_{\text{all } \ell},[1,1,p_\ell,1]_{\text{all } \ell},[1,1,1,p_\ell]_{\text{all } \ell}\rangle. \tag{27}$$

This still only gives a bound of the form $4t+\text{constant}$, so we aim now to prove a further restriction that will reduce the $4t$ to $3t$. Let $T=\{p_1,\ldots,p_t\}$. Consider an arbitrary member $[a_1,a_2,a_3,a_4]$ of the 2-Selmer group.

Consider the case where there does not exist any p_i dividing either a_2 or a_3. Then the product of all members of T which divide a_2 is 1, and the product of all members of T which divide a_3 is 1,

Consider the case where there exists some p_i which divides both a_2 and a_3. Then from (22) we see that $3 \nmid a_2$ and $3 \nmid a_3$. Hence, for all j, using (22) but with $i=j$, we see that $p_j|a_2 \iff p_j|a_3$. Hence the product of all members of T which divide a_2 is the same as the product of all members of T which divide a_3.

Consider the case where there exists some p_i which divides a_2 but does not divide a_3. Then from (22) we see that $3|a_2$ and $3|a_3$. Hence, for all j, using (22) but with $i=j$, we see that $p_j|a_2 \iff p_j \nmid a_3$. Hence the product of all members of T which divide a_2 times the product of all members of T which divide a_3 gives k.

The remaining case, where there exists some p_i which divides a_3 but does not divide a_2, similarly gives that the product of all members of T which divide a_2 times the product of all members of T which divide a_3 gives k.

It now follows that the 2-Selmer group is at most

$$\langle H, [p_\ell, 1, 1, 1]_{\text{all } \ell}, [1, p_\ell, p_\ell, 1]_{\text{all } \ell}, [1, 1, k, 1], [1, 1, 1, p_\ell]_{\text{all } \ell}\rangle. \tag{28}$$

Hence the Selmer bound on the rank of $J_k(\mathbb{Q})$ using complete 2-descent is at most $3t + 5 - 4 = 3t + 1$.

In summary, the Selmer bound on the rank of $J_k(\mathbb{Q})$ using descent via Richelot isogeny is at least $4t - 8$ and the Selmer bound using complete 2-descent is at most $3t + 1$, so that the 2-part of $Ш(\widehat{J}_k/\mathbb{Q})$ becomes arbitrarily large as t increases. □

We conclude by suggesting the following conjecture.

Conjecture 1. *Let $f(x) \in \mathbb{Q}[x]$. Then there is arbitrarily large 2-part of $Ш(J_k/\mathbb{Q})$ amongst the Jacobians J_k of the hyperelliptic curves $C_k : y^2 = kf(x)$, for $k \in \mathbb{Q}$.*

It is hard to see how to prove this in general, but the above argument makes it seem plausible at least when $f(x)$ is of degree at most 6, with all roots $e_i \in \mathbb{Q}$, subject to certain requirements on the roots. For example, in the genus 2 case, it seems plausible that the above style of argument could typically be used when all roots are in $\mathbb{Q}$ for both C_k and $\widehat{\mathcal{C}}_k$, and there exists a prime ρ which divides some difference of the roots to an odd power, but which does not divide to an odd power the resultant of any $x - e_i$ and any quadratic $(x - e_j)(x - e_k)$ that corresponds to a member of the kernel of the Richelot isogeny.

References

[1] R. Bölling. *Die Ordnung der Schafarewitsch-Tate-Gruppe kann beliebig gross werden.* Math. Nachr. **67** (1975), 157-179.

[2] 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.

[3] J.W.S. Cassels and E.V. Flynn. *Prolegomena to a Middlebrow Arithmetic of Curves of Genus 2.* LMS–LNS **230**. Cambridge University Press, Cambridge (1996).

[4] P.L. Clark and S. Sharif. *Period, index and potential Ш.* Algebra Number Theory **4** (2010) 151-174.

[5] B. Creutz. *Potential Ш for abelian varieties.* J. Number Theory **131** (2011), 2162-2174.

[6] T. Fisher. *Some examples of 5 and 7 descent for elliptic curves over $\mathbb{Q}$.* J. Eur. Math. Soc. **3** (2001), 169-201.

[7] 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.

[8] R. Kloosterman and E.F. Schaefer. *Selmer groups of elliptic curves that can be arbitrarily large.* J. Number Theory **99** (2003), 148–163.

[9] K. Kramer. *A family of semistable elliptic curves with large Tate-Shafarevich groups.* Proc. Am. Math. Soc. **89** (1983), 379-386.

[10] F. Lemmermeyer. *On Tate-Shafarevich groups of some elliptic curves.* Algebraic number theory and Diophantine analysis (Graz, 1998), 277-291, de Gruyter, Berlin (2000).

[11] 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.

[12] K. Matsuno. *Construction of elliptic curves with large Iwasawa λ-invariants and large Tate-Shafarevich groups.* Manuscripta Math. **122** (2007), 289-304.

[13] E.F. Schaefer. *2-descent on the Jacobians of Hyperelliptic Curves.* J. Number Theory **51** (1995), 219–232.

[14] J.H. Silverman. *The Arithmetic of Elliptic Curves.* Graduate Texts in Mathematics **106**, Springer-Verlag, 2009.

[15] M. Stoll. *Two simple 2-dimensional abelian varieties defined over $\mathbb{Q}$ with Mordell-Weil rank at least* 19. C. R. Acad. Sci. Paris, Série I, **321** (1995), 1341–1344.

Mathematical Institute, University of Oxford, 24–29 St. Giles, Oxford OX1 3LB, United Kingdom
E-mail address: flynn@maths.ox.ac.uk