ACTA ARITHMETICA
191.2 (2019)

Arbitrarily large 2-torsion in Tate–Shafarevich groups of abelian varieties

by

E. V. Flynn (Oxford)

1. Introduction. There has been substantial research on arbitrarily large Tate–Shafarevich groups and Selmer groups on elliptic curves ([1], [3], [8], [11], [12], [13], [14], [15], [16]), which has mainly emphasised the p-torsion part of the Tate–Shafarevich group for $p \leq 13$. For higher dimension, Creutz [6] has shown that for any principally polarised 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 Sharif [5].

For higher dimension over $\mathbb{Q}$, Flynn [9] has recently shown that the Tate–Shafarevich groups of absolutely simple Jacobians of genus 2 curves over $\mathbb{Q}$ (in particular, their 2-torsion) can be arbitrarily large. This involved the examination of the quadratic twists of a genus 2 curve whose Jacobian has all of its 2-torsion defined over $\mathbb{Q}$, and then showing that the Selmer bounds for complete 2-descent and descent via Richelot isogeny can differ by an arbitrarily large amount.

Our desire here is to generalise this result to arbitrary genus. We shall show the following result.

Theorem 1. *For any $g \geq 1$, there exists a hyperelliptic curve of genus g over $\mathbb{Q}$, with absolutely simple Jacobian, such that the 2-torsion part of the Tate–Shafarevich groups is arbitrarily large amongst its quadratic twists.*

We shall make use of a recent elegant construction of Mestre [17] who describes, for any g, curves of genus g whose Jacobians admit a $(2, \ldots, 2)$ isogeny ϕ. Our broad principle is the same: we again wish to play the Selmer group information for complete 2-descent against the Selmer group infor-

2010 *Mathematics Subject Classification*: Primary 11G30; Secondary 11G10, 14H40.
Key words and phrases: Tate–Shafarevich group, abelian variety.
Received 18 November 2017; revised 3 November 2018.
Published online 5 September 2019.

DOI: 10.4064/aa171118-7-12

mation for descent via this isogeny. However, for general genus g, this is impractical, and we show how it is possible to focus on specific elements and just a small part of the information from the Selmer groups; our method also does not require any explicit models of the isogenous objects.

2. A construction of Mestre, generalising Richelot's isogeny. We summarise the recent construction of Mestre [17], which considers curves of genus g of the following form, in the variables x, y over the purely transcendental field $\mathbb{Q}(v, a_1, \ldots, a_g)$. We define $\mathcal{C}$ to be the smooth projective model of the following affine curve:

$$\mathcal{C} : y^2 = (x - v)(vx - 1)(x^2 - a_1) \cdots (x^2 - a_g). \tag{1}$$

Let $A = 2(v^2 + 1)(v^2 - a_1) \cdots (v^2 - a_g)$ and define $\widehat{\mathcal{C}}$ to be the smooth projective model of the following affine curve:

$$\widehat{\mathcal{C}} : y^2 = A(x - v)(vx - (-1)^g)(x^2 - b_1) \cdots (x^2 - b_g), \tag{2}$$

where $b_i = (a_i v^2 - 1)/(a_i - v^2)$ for each i. Note that in [17], the twisting factor A is placed on $\mathcal{C}$, and we have placed it here instead on $\widehat{\mathcal{C}}$ for later convenience. Of course, any specialisation to $v, a_1, \ldots, a_g \in \mathbb{Q}$ will give curves of genus g over $\mathbb{Q}$ provided that $0, v^2, 1/v^2, a_1, \ldots, a_g$ are distinct.

First consider the case when g is even. If we set

$$\begin{aligned} S(x, z) &= x^2 z^2 - v^2(x^2 + z^2) + 1, \\ M(x, z) &= \prod_{i=1}^{g/2} (v^2 - a_{2i})(x^2 - a_{2i-1})(z^2 - b_{2i}), \end{aligned} \tag{3}$$

then there is a correspondence Γ on $\mathcal{C} \times \widehat{\mathcal{C}}$ defined by

$$S(x, y) = 0, \qquad yt = M(x, z)(v^2 + 1)(1 - xv - zv + xz). \tag{4}$$

This induces an isogeny $\phi : J \to \widehat{J}$, where $J, \widehat{J}$ are the Jacobian varieties of $\mathcal{C}, \widehat{\mathcal{C}}$, respectively. Then ϕ is a $(2, \ldots, 2)$-isogeny, that is, an isogeny of degree 2^g, with kernel isomorphic to $(\mathbb{Z}/2\mathbb{Z})^g$; the kernel of ϕ is generated by the divisor classes $[(\sqrt{a_i}, 0) - (-\sqrt{a_i}, 0)]$. Similarly, the dual isogeny $\hat{\phi}$: $\widehat{J} \to J$ has kernel isomorphic to $(\mathbb{Z}/2\mathbb{Z})^g$, generated by the divisor classes $[(\sqrt{b_i}, 0) - (-\sqrt{b_i}, 0)]$. The composition $\hat{\phi}\phi$ is the multiplication by 2 map on J.

Mestre also shows (in [17, Section 2.4]) for odd genus that there is an isogeny $\phi : J \to \widehat{J}$ of degree 2^g and dual isogeny $\hat{\phi} : \widehat{J} \to J$ with kernels as described above.

When $g = 1$, this is the standard 2-isogeny on an elliptic curve (described in [20, Chapter X]); when $g = 2$, this is Richelot's isogeny (described in [2] and in [4, Chapter 9]).

Mestre concludes [17, Section 2.4] by showing that $\mathcal{C}$ generically has absolutely simple Jacobian J.

3. Descent via $(2,\ldots,2)$**-isogeny.** We now wish to take the isogeny ϕ described by Mestre and set up the machinery required to perform descent via this isogeny. From now onwards, we shall take $v, a_1, \ldots, a_g \in \mathbb{Q}$ such that $0, v^2, 1/v^2, a_1, \ldots, a_g$ are distinct, in order that the curves in (1), (2) are of genus g and defined over $\mathbb{Q}$, the isogenies ϕ and $\hat{\phi}$ are defined over $\mathbb{Q}$, and we may consider $\phi : J(\mathbb{Q}) \to \widehat{J}(\mathbb{Q})$ and $\hat{\phi} : \widehat{J}(\mathbb{Q}) \to J(\mathbb{Q})$.

It will be more convenient to work with curves that are of odd degree and monic, so we shall first birationally transform $\mathcal{C}$ and $\widehat{\mathcal{C}}$ to this form. Let

$$P = (v^2-1)(v^2-a_1)\cdots(v^2-a_g) \in \mathbb{Q}^*, \tag{5}$$

and now map $(v,0)$ to infinity by replacing y by Py/x^{g+1} and replacing x by $(vx+P)/x$ in (1); we may then take $\mathcal{C}$ to be

$$\mathcal{C} : y^2 = \left(x + \frac{vP}{v^2-1}\right) f_1(x)\cdots f_g(x), \quad \text{where} \tag{6}$$
$$f_i(x) = x^2 + \frac{2vPx}{v^2-a_i} + \frac{P^2}{v^2-a_i}.$$

Similarly replace y by $2(v^2+1)^{\lfloor (g+3)/2\rfloor}(v^2-1)^{\lfloor (g+2)/2\rfloor} y/x^{g+1}$ and replace x by $(vx+2(v^4-1))/x$ in (2), and substitute the definitions of A and the b_i given immediately before and after (2); we may then take $\widehat{\mathcal{C}}$ to be

$$\begin{aligned} &\widehat{\mathcal{C}} : y^2 = \big(x + 2v(v^2+(-1)^g)\big)\hat{f}_1(x)\cdots\hat{f}_g(x), \quad \text{where} \\ &\hat{f}_i(x) = x^2 + 4v(v^2-a_i)x + 4(v^4-1)(v^2-a_i). \end{aligned} \tag{7}$$

A file which checks the above maps has been placed at [10]. We now describe the map which allows descent to be performed via this isogeny (sometimes referred to as the Cassels map for the descent). Let U consist of $2, \infty$ and the primes dividing the discriminants of $\mathcal{C}, \widehat{\mathcal{C}}$. Let $(\mathbb{Q}^*/(\mathbb{Q}^*)^2)^{\times g}$ denote the product $\mathbb{Q}^*/(\mathbb{Q}^*)^2 \times \cdots \times \mathbb{Q}^*/(\mathbb{Q}^*)^2$ (g times), and let M be the subgroup of $(\mathbb{Q}^*/(\mathbb{Q}^*)^2)^{\times g}$ generated by -1 and $U \setminus \{\infty\}$ in each factor. The recipe for finding the following maps is described in [19]. For descent via the above isogeny, we should find an injection on $\widehat{J}(\mathbb{Q})/\phi(J(\mathbb{Q}))$ by using functions whose divisors generate the kernel of $\hat{\phi}$, namely $\hat{f}_1(x), \ldots, \hat{f}_g(x)$. This is given by

$$\begin{aligned} &q^\phi : \widehat{J}(\mathbb{Q})/\phi(J(\mathbb{Q})) \to M \le (\mathbb{Q}^*/(\mathbb{Q}^*)^2)^{\times g}, \\ &\Big[\sum_{i=1}^{g}(x_i,y_i) - g\cdot\infty\Big] \mapsto \Big(\prod_{i=1}^{g}\hat{f}_1(x_i), \ldots, \prod_{i=1}^{g}\hat{f}_g(x_i)\Big). \end{aligned} \tag{8}$$

In the above definition, $x_i, y_i \in \overline{\mathbb{Q}}$ for each i, the divisor $\sum_{i=1}^{g}(x_i,y_i) - g\cdot\infty$ is

Galois stable, and the left hand side is its divisor class. The above definition applies when all $\hat{f}_j(x_i)$ are nonzero. When $\hat{f}_j(x_i) = 0$, it should be replaced by $(x_i + 2v(v^2 + (-1)^g))\hat{f}_1(x_i)\cdots\hat{f}_{j-1}(x_i)\hat{f}_{j+1}(x_i)\cdots\hat{f}_g(x_i)$; note that this is the evaluation at $x = x_i$ of the product of all factors except $\hat{f}_j(x)$ on the right hand side of (7). When (x_i, y_i) is the point at infinity, $\hat{f}_j(x_i)$ should be replaced by 1. Analogous adjustments apply to the maps $q^{\hat{\phi}}$ and q which will be defined below.

We should similarly find an injection on $J(\mathbb{Q})/\hat{\phi}(\widehat{J}(\mathbb{Q}))$ by using functions whose divisors generate the kernel of ϕ, namely $f_1(x), \ldots, f_g(x)$. This is given by

$$\begin{gathered} q^{\hat{\phi}} : J(\mathbb{Q})/\hat{\phi}(\widehat{J}(\mathbb{Q})) \to M \le (\mathbb{Q}^*/(\mathbb{Q}^*)^2)^{\times g}, \\ \Big[\sum_{i=1}^{g}(x_i, y_i) - g\cdot\infty\Big] \mapsto \Big(\prod_{i=1}^{g} f_1(x_i), \ldots, \prod_{i=1}^{g} f_g(x_i)\Big). \end{gathered} \tag{9}$$

We exploit the usual style of commutative diagram (of the type used, for example, in [4, Chapter 11] and in [18]):

$$\begin{array}{ccc} \widehat{J}(\mathbb{Q})/\phi(J(\mathbb{Q})) & \xrightarrow{q^{\phi}} & M \\ \downarrow{\scriptstyle i_p^{\phi}} & & \downarrow{\scriptstyle j_p} \\ \widehat{J}(\mathbb{Q}_p)/\phi(J(\mathbb{Q}_p)) & \xrightarrow{q_p^{\phi}} & M_p \end{array} \tag{10}$$

where q_p^{ϕ} and M_p are the local analogues of q^{ϕ} and M, and the maps i_p^{ϕ} and j_p are induced by the natural injection $\mathbb{Q} \hookrightarrow \mathbb{Q}_p$. We may then compute the Selmer group $\mathrm{Sel}^{\phi}(J/\mathbb{Q})$, using

$$\bigcap_{p\in U} j_p^{-1}(\operatorname{im} q_p^{\phi}) \cong \mathrm{Sel}^{\phi}(J/\mathbb{Q}), \tag{11}$$

which contains $\operatorname{im} q^{\phi}$, giving an upper bound on the order of $\widehat{J}(\mathbb{Q})/\phi(J(\mathbb{Q}))$.

We have a similar commutative diagram for $\hat{\phi}$:

$$\begin{array}{ccc} J(\mathbb{Q})/\hat{\phi}(\widehat{J}(\mathbb{Q})) & \xrightarrow{q^{\hat{\phi}}} & M \\ \downarrow{\scriptstyle i_p^{\hat{\phi}}} & & \downarrow{\scriptstyle j_p} \\ J(\mathbb{Q}_p)/\hat{\phi}(\widehat{J}(\mathbb{Q}_p)) & \xrightarrow{q_p^{\hat{\phi}}} & M_p \end{array} \tag{12}$$

where $q_p^{\hat{\phi}}$ and M_p are the local analogues of $q^{\hat{\phi}}$ and M, and the maps $i_p^{\hat{\phi}}$ and j_p are induced by the natural injection $\mathbb{Q} \hookrightarrow \mathbb{Q}_p$. We may then compute the

Selmer group $\mathrm{Sel}^{\hat\phi}(\widehat{J}/\mathbb{Q})$, using

$$\bigcap_{p\in U} j_p^{-1}(\mathrm{im}\, q_p^{\hat\phi}) \cong \mathrm{Sel}^{\hat\phi}(\widehat{J}/\mathbb{Q}), \tag{13}$$

which contains $\mathrm{im}\, q^{\hat\phi}$, giving an upper bound on the order of $J(\mathbb{Q})/\hat\phi(J(\mathbb{Q}))$.

If one obtains bounds, as above, on the orders of $\widehat{J}(\mathbb{Q})/\phi(J(\mathbb{Q}))$ and $J(\mathbb{Q})/\hat\phi(\widehat{J}(\mathbb{Q}))$, one can deduce a bound on the order of $J(\mathbb{Q})/2J(\mathbb{Q})$ and a bound on the rank of $J(\mathbb{Q})$.

4. Arbitrarily large 2-torsion part of the Tate–Shafarevich group in any dimension. We aim to compare descent via the isogeny ϕ, as described in the last section, with complete 2-descent, so we shall take our curves to be in the form (6), (7), but with each a_i equal to α_i^2 for some $\alpha_i \in \mathbb{Q}^*$, and where we apply a quadratic twist by $k \in \mathbb{Q}^*$:

$$\mathcal{C}_k : y^2 = \Big(x + \frac{kvP}{v^2-1}\Big) h_1(x)\tilde h_1(x) \cdots h_g(x)\tilde h_g(x), \quad \text{where}$$
$$h_i(x) = x + \frac{kP}{v+\alpha_i} \quad \text{and} \quad \tilde h_i(x) = x + \frac{kP}{v-\alpha_i}, \tag{14}$$

and where

$$P = (v^2-1)(v+\alpha_1)(v-\alpha_1)\cdots(v+\alpha_g)(v-\alpha_g). \tag{15}$$

Similarly, we have

$$\widehat{\mathcal{C}}_k : y^2 = \big(x + 2kv(v^2+(-1)^g)\big)\hat h_1(x)\cdots \hat h_g(x), \quad \text{where}$$
$$\hat h_i(x) = x^2 + 4kv(v^2-\alpha_i^2)x + 4k^2(v^4-1)(v^2-\alpha_i^2). \tag{16}$$

Let T be the set of primes dividing k and let $S = T \cup U$. On $\widehat{J}_k(\mathbb{Q})/\phi(J_k(\mathbb{Q}))$, where $J_k, \widehat{J}_k$ are the Jacobians of $\mathcal{C}_k, \widehat{\mathcal{C}}_k$, the injection of (8) becomes

$$q^{\phi} : \widehat{J}_k(\mathbb{Q})/\phi(J_k(\mathbb{Q})) \to M' \le (\mathbb{Q}^*/(\mathbb{Q}^*)^2)^{\times g},$$
$$\Big[\sum_{i=1}^{g}(x_i,y_i) - g\cdot\infty\Big] \mapsto \Big(\prod_{i=1}^{g}\hat h_1(x_i), \ldots, \prod_{i=1}^{g}\hat h_g(x_i)\Big), \tag{17}$$

where M' is generated by -1 and $S\setminus\{\infty\}$ in each factor. The injection of (9) becomes

$$q^{\hat\phi} : J_k(\mathbb{Q})/\hat\phi(\widehat{J}_k(\mathbb{Q})) \to M' \le (\mathbb{Q}^*/(\mathbb{Q}^*)^2)^{\times g},$$
$$\Big[\sum_{i=1}^{g}(x_i,y_i) - g\cdot\infty\Big] \mapsto \Big(\prod_{i=1}^{g} h_1(x_i)\tilde h_1(x_i), \ldots, \prod_{i=1}^{g} h_g(x_i)\tilde h_g(x_i)\Big). \tag{18}$$

Since the Jacobian J_k of our curve $\mathcal{C}_k$ of (14) has all of its 2-torsion in $J_k(\mathbb{Q})$, we may also perform complete 2-descent. The relevant injection (using the method in [18]) is

$$\begin{aligned} &q : J_k(\mathbb{Q})/2J_k(\mathbb{Q}) \to M'' \le (\mathbb{Q}^*/(\mathbb{Q}^*)^2)^{\times 2g}, \\ &\Big[\sum_{i=1}^{g}(x_i,y_i) - g\cdot\infty\Big] \\ &\qquad\qquad \mapsto \Big(\prod_{i=1}^{g} h_1(x_i), \prod_{i=1}^{g} \tilde{h}_1(x_i), \ldots, \prod_{i=1}^{g} h_g(x_i), \prod_{i=1}^{g} \tilde{h}_g(x_i)\Big), \end{aligned} \tag{19}$$

where M'' is generated by -1 and $S\setminus\{\infty\}$ in each factor. We have our usual associated commutative diagram

$$\begin{array}{ccc} J_k(\mathbb{Q})/2J_k(\mathbb{Q}) & \xrightarrow{\ q\ } & M'' \\ {\scriptstyle i_p}\downarrow & & \downarrow{\scriptstyle j_p} \\ J_k(\mathbb{Q}_p)/2J_k(\mathbb{Q}_p) & \xrightarrow{\ q_p\ } & M''_p \end{array} \tag{20}$$

where q_p and M''_p are the local analogues of q and M'', and the maps i_p and j_p are induced by the natural injection $\mathbb{Q} \hookrightarrow \mathbb{Q}_p$. We may then compute the 2-Selmer group $\mathrm{Sel}^{(2)}(J_k/\mathbb{Q})$, using

$$\bigcap_{p\in S} j_p^{-1}(\operatorname{im} q_p) \cong \mathrm{Sel}^{(2)}(J_k/\mathbb{Q}), \tag{21}$$

which contains $\operatorname{im} q$, so gives an upper bound on the order of $J_k(\mathbb{Q})/2J_k(\mathbb{Q})$.

We wish to show arbitrarily large 2-torsion part of the Tate–Shafarevich group for arbitrary genus by finding elements of $\mathrm{Sel}^{\hat{\phi}}(\widehat{J}/\mathbb{Q})$ which can be shown to violate the Hasse principle by using $\mathrm{Sel}^{(2)}(J/\mathbb{Q})$. Note that if $(r_1, r_2, r_3, r_4, \ldots, r_{2g-1}, r_{2g}) \in \operatorname{im} q$ then $(r_1r_2, r_3r_4, \ldots, r_{2g-1}r_{2g})$ is the corresponding member of $\operatorname{im} q^{\hat{\phi}}$, so the map q refines $q^{\hat{\phi}}$. Our approach will not require finding entire Selmer groups, nor will it even require the explicit model for $\widehat{\mathcal{C}}_k$, since we work entirely on specific elements $\mathbf{r} \in M'$, showing $\mathbf{r} \in \mathrm{Sel}^{\hat{\phi}}(\widehat{J}/\mathbb{Q})$ by proving directly, for all $p \in S$, the existence of $D \in J_k(\mathbb{Q}_p)$ such that $q_p^{\hat{\phi}}(D) = \mathbf{r}$ and by showing $\mathbf{r} \notin \operatorname{im} q^{\hat{\phi}}$ by local arguments on the q_p.

Specifically, our strategy will be to fix a small prime; we shall use 7. Then congruence conditions on v and the α_i will ensure that, for $\mathcal{C}_1 = \mathcal{C}$, the prime 7 will, in a certain sense (which will be apparent in the details of the next result), be relevant for local constraints on $\operatorname{im} q$ but not on $\operatorname{im} q^{\hat{\phi}}$. If we twist by $k = p_1 \cdots p_t$ where, for all i, the p_i are chosen such that all members of $U \setminus \{7, \infty\}$ (with U defined just after (7)) and all p_j (for $j \ne i$) are squares in $\mathbb{Q}^*_{p_i}$, but also such that 7 is nonsquare in $\mathbb{Q}^*_{p_i}$, then the prime 7 will create constraints due to local arguments on $\operatorname{im} q$ more severe than those obtained by local arguments on $\operatorname{im} q^{\hat{\phi}}$.

THEOREM 2. *Let* $v, \alpha_1, \ldots, \alpha_g \in \mathbb{Z}$, *with* $0, v, -v, 1/v, -1/v, \alpha_1, \ldots, \alpha_g$ *distinct, satisfy* $7^1 \parallel \alpha_1$, $v \equiv \pm 2 \pmod 7$ *and* $\alpha_i \equiv \pm 1 \pmod 7$ *for each* $i \geq 2$. *Let* U *consist of* $2, \infty$ *and the primes dividing the discriminants of* $\mathcal{C}_1, \widehat{\mathcal{C}}_1$ *(as in* (14), (16), *with* $k = 1$*). Now let* $k = p_1 \ldots p_t$, *where* $t \in \mathbb{N}$ *is arbitrary, satisfy* $\left(\frac{p_i}{p_j}\right) = 1$ *for distinct* i, j, $p_i \equiv 1 \pmod 8$ *for each* i, $\left(\frac{7}{p_i}\right) = -1$ *for each* i, *and* $\left(\frac{\pi}{p_i}\right) = 1$ *for each* $\pi \in U \setminus \{7, \infty\}$ *and each* i. *Let* $\mathcal{C}_k$ *be as in* (14), $\widehat{\mathcal{C}}_k$ *be as in* (16), J_k *be the Jacobian of* $\mathcal{C}_k$, *and* $\widehat{J}_k$ *be the Jacobian of* $\widehat{\mathcal{C}}_k$. *Then* J_k *and* $\widehat{J}_k$ *are of dimension* g, *and* $Ш(\widehat{J}_k/\mathbb{Q})[\hat{\phi}]$ *becomes arbitrarily large as* t *increases.*

Proof. The given conditions force $\mathcal{C}_k, \widehat{\mathcal{C}}_k$ to have genus g, so $J_k, \widehat{J}_k$ have dimension g. The conditions also imply that, for any prime $\pi \in U \setminus \{7, \infty\}$ and any i, we have $\pi \in (\mathbb{Q}_{p_i}^*)^2$ and $p_i \in (\mathbb{Q}_\pi^*)^2$; furthermore, $p_j \in (\mathbb{Q}_{p_i}^*)^2$ for any $j \neq i$; finally, $7 \notin (\mathbb{Q}_{p_i}^*)^2$ and $p_i \notin (\mathbb{Q}_7^*)^2$ by quadratic reciprocity. By the Chinese Remainder Theorem and Dirichlet's Theorem, we can find an arbitrarily large set of such primes $p_1, \ldots, p_t$, so t is arbitrarily large.

Let $T = \{p_1, \ldots, p_t\}$ and let $S = T \cup U$. The given conditions force $7 \nmid P$, where P is defined in (15). Let

(22)
$$\beta_0 = \frac{-kvP}{v^2 - 1}, \quad \beta_1 = \frac{-kP}{v + \alpha_1}, \quad \beta_2 = \frac{-kP}{v - \alpha_1}, \ldots,$$
$$\beta_{2g-1} = \frac{-kP}{v + \alpha_g}, \quad \beta_{2g} = \frac{-kP}{v - \alpha_g}, \quad \text{all in } \mathbb{Z},$$

be the roots of the polynomial on the right hand side of (14). Also define

(23)
$$\beta_{i,j} = \beta_i - \beta_j \in \mathbb{Z} \quad \text{when } i \neq j,$$
$$\beta_{i,i} = (\beta_i - \beta_0)(\beta_i - \beta_1) \ldots (\beta_i - \beta_{i-1})(\beta_i - \beta_{i+1}) \ldots (\beta_i - \beta_{2g}) \in \mathbb{Z}.$$

The discriminant of the polynomial on the right hand side of C_1 (given by (14) with $k = 1$) is

(24)
$$2^{2g}((v^2 - 1))^{2g(2g-1)} \Big(\prod_{i=1}^{g} \alpha_i^2 \big((v^2 - \alpha_i^2)\big)^{2g(2g-1)} (v^2\alpha_i^2 - 1)^2 \Big) \prod_{i<j} (\alpha_i^2 - \alpha_j^2)^4,$$

so $v+1, v-1$ and each $\alpha_i, v \pm \alpha_i, v\alpha_i \pm 1, \alpha_i \pm \alpha_j$ is divisible only by the primes in $U \setminus \{\infty\}$. The congruence conditions in the hypotheses of the theorem give $7^1 \parallel \alpha_1$,

(25)
$$7 \nmid v+1, v-1, v \pm \alpha_i, v\alpha_i \pm 1 \quad \text{for } i = 1, \ldots, g,$$

and

$$7 \nmid \alpha_j, \alpha_1 \pm \alpha_j \quad \text{for } j = 2, \ldots, g, \tag{26}$$

so each expression in (25), (26) is divisible only by the primes in $U \setminus \{7, \infty\}$. For any $j \in \{0, \ldots, 2g\}$,

$$\beta_{0,j} = \begin{cases} -k(v\alpha_{(j+1)/2} + 1)(v - \alpha_{(j+1)/2}) \displaystyle\prod_{\substack{1 \le i \le g \\ i \ne (j+1)/2}} (v^2 - \alpha_i^2) & \text{for } j \text{ odd}, \\ k(v\alpha_{j/2} - 1)(v + \alpha_{j/2}) \displaystyle\prod_{\substack{1 \le i \le g \\ i \ne j/2}} (v^2 - \alpha_i^2) & \text{for } j \text{ even}, \end{cases} \tag{27}$$

which shows, by using (25), that

(28) $\beta_{0,j}/k \in \mathbb{Z}$ is divisible only by the primes in $U \setminus \{7, \infty\}$ for $j \in \{1, \ldots, 2g\}$.

Since $\beta_{i,0} = -\beta_{0,i}$ for each i, it follows that

(29) $\beta_{i,0}/k \in \mathbb{Z}$ is divisible only by the primes in $U \setminus \{7, \infty\}$ for $i \in \{1, \ldots, 2g\}$.

Also

$$\beta_{1,2} = 2k\alpha_1(v^2 - 1) \prod_{i=2}^{g} (v^2 - \alpha_i^2), \tag{30}$$

so, by (25) and the fact that $7^1 \parallel \alpha_1$,

(31) $\beta_{1,2}/(7k) \in \mathbb{Z}$ is divisible only by the primes in $U \setminus \{7, \infty\}$.

For any $j \in \{3, \ldots 2g\}$, $\beta_{1,j}$ is

$$\begin{cases} k(v^2 - 1)(\alpha_1 - \alpha_{(j+1)/2})(v - \alpha_1)(v - \alpha_{(j+1)/2}) \displaystyle\prod_{\substack{2 \le i \le g \\ i \ne (j+1)/2}} (v^2 - \alpha_i^2) & \text{for } j \text{ odd}, \\ k(v^2 - 1)(\alpha_1 + \alpha_{j/2})(v - \alpha_1)(v + \alpha_{j/2}) \displaystyle\prod_{\substack{2 \le i \le g \\ i \ne j/2}} (v^2 - \alpha_i^2) & \text{for } j \text{ even}, \end{cases} \tag{32}$$

which gives, in view of (25), (26),

(33) $\beta_{1,j}/k \in \mathbb{Z}$ is divisible only by the primes in $U \setminus \{7, \infty\}$ for $j \in \{3, \ldots, 2g\}$.

Since $\beta_{1,1} = \beta_{1,0}\beta_{1,2}\beta_{1,3} \ldots \beta_{1,2g}$ it follows from (29) with $i = 1$, and from (31), (33), that

(34) $\beta_{1,1}/(7k^{2g}) \in \mathbb{Z}$ is divisible only by the primes in $U \setminus \{7, \infty\}$.

Hence, combining (28), (31), (33), (34), we see that

(35) $\beta_{1,1}\beta_{0,1}/(7k^{2g+1}), \beta_{1,2}\beta_{0,2}/(7k^2) \in \mathbb{Z}$ and $\beta_{1,j}\beta_{0,j}/k^2 \in \mathbb{Z}$ for each $j \in \{3,\dots,2g\}$ are divisible only by the primes in $U \setminus \{7,\infty\}$.

Similarly

(36) $\beta_{2,1}\beta_{0,1}/(7k^2), \beta_{2,2}\beta_{0,2}/(7k^{2g+1}) \in \mathbb{Z}$ and $\beta_{2,j}\beta_{0,j}/k^2 \in \mathbb{Z}$ for each $j \in \{3,\dots,2g\}$ are divisible only by the primes in $U \setminus \{7,\infty\}$,

and

(37) for any distinct $i,j \in \{3,\dots,2g\}$, $\beta_{i,1}\beta_{0,1}/k^2, \beta_{i,2}\beta_{0,2}/k^2 \in \mathbb{Z}$ are divisible only by the primes in $U \setminus \{7,\infty\}$, and $\beta_{i,i}\beta_{0,i}/k^{2g+1}, \beta_{i,j}\beta_{0,j}/k^2 \in \mathbb{Z}$ are divisible only by the primes in $U \setminus \{\infty\}$.

For any $i \in \{1,\dots,2g\}$, $[(\beta_i,0)-(\beta_0,0)] = [(\beta_i,0)+(\beta_0,0)-2\infty]$ is taken by the map q of (19) to $(\beta_{i,1}\beta_{0,1}, \beta_{i,2}\beta_{0,2},\dots,\beta_{i,2g}\beta_{0,2g})$, where now each $\beta_{i,j}\beta_{0,j}$ represents a member of $\mathbb{Q}^*/(\mathbb{Q}^*)^2$; by (35)–(37), the subset

(38) $$\{[(\beta_1,0)-(\beta_0,0)],\ [(\beta_2,0)-(\beta_0,0)],\dots,[(\beta_{2g},0)-(\beta_0,0)]\}$$

of $J_k(\mathbb{Q})$ is mapped by q of (19) to a set of members of $(\mathbb{Q}^*/(\mathbb{Q}^*)^2)^{\times 2g}$ of the following form, where each entry is represented by a squarefree integer:

(39) $$\begin{aligned} H = \{&(7kw_1^{(1)}, 7w_2^{(1)}, w_3^{(1)}, w_4^{(1)},\dots,w_{2g-1}^{(1)}, w_{2g}^{(1)}),\\ &(7w_1^{(2)}, 7kw_2^{(2)}, w_3^{(2)}, w_4^{(2)},\dots,w_{2g-1}^{(2)}, w_{2g}^{(2)}),\\ &(w_1^{(3)}, w_2^{(3)}, ku_3^{(3)}, u_4^{(3)},\dots,u_{2g-1}^{(3)}, u_{2g}^{(3)}),\\ &(w_1^{(4)}, w_2^{(4)}, u_3^{(4)}, ku_4^{(4)},\dots,u_{2g-1}^{(4)}, u_{2g}^{(4)}),\dots,\\ &(w_1^{(2g-1)}, w_2^{(2g-1)}, u_3^{(2g-1)}, u_4^{(2g-1)},\dots,ku_{2g-1}^{(2g-1)}, u_{2g}^{(2g-1)}),\\ &(w_1^{(2g)}, w_2^{(2g)}, u_3^{(2g)}, u_4^{(2g)},\dots,u_{2g-1}^{(2g)}, ku_{2g}^{(2g)})\}, \end{aligned}$$

where each $u_i^{(j)}$ is divisible only by the primes in $U \setminus \{\infty\}$, and each $w_i^{(j)}$ is divisible only by the primes in $U \setminus \{7,\infty\}$. In (39) the symbol k only appears in the diagonal entries.

For any i, the hypotheses imply that -1 and all primes of $S \setminus \{7, p_i, \infty\}$ are squares in $\mathbb{Q}_{p_i}^*$, and that the images of 7 and p_i in $\mathbb{Q}_{p_i}^*/(\mathbb{Q}_{p_i}^*)^2$ are $\mathbb{F}_2$-independent, so $\langle -1, S \setminus \{\infty\}\rangle \cap (\mathbb{Q}_{p_i}^*)^2 = \langle -1, U \setminus \{7,\infty\}, (p_\ell)_{\text{all } \ell\neq i}\rangle$. This implies that the above elements of H map to $\mathbb{F}_2$-independent elements of $(\mathbb{Q}_{p_i}^*/(\mathbb{Q}_{p_i}^*)^2)^{\times 2g}$, and since $\#J_k(\mathbb{Q}_{p_i})/2J_k(\mathbb{Q}_{p_i}) = \#J_k(\mathbb{Q}_{p_i})[2] = 2^{2g}$ (see [18, Section 4]), it follows that the elements of H are mapped by q_{p_i} to an $\mathbb{F}_2$-basis of $\operatorname{im} q_{p_i}$. Hence

$$(40)\qquad j_{p_i}^{-1}(\operatorname{im} q_{p_i}) = \langle H, (-1,1,\ldots,1,1), (1,-1,\ldots,1,1), \ldots, (1,1,\ldots,-1,1), (1,1,\ldots,1,-1), (w,1,\ldots,1,1)_{\text{all } w\in U\setminus\{7,\infty\}}, (1,w,\ldots,1,1)_{\text{all } w\in U\setminus\{7,\infty\}}, \ldots, (1,1,\ldots,w,1)_{\text{all } w\in U\setminus\{7,\infty\}}, (1,1,\ldots,1,w)_{\text{all } w\in U\setminus\{7,\infty\}}, (p_\ell,1,\ldots,1,1)_{\text{all } \ell\neq i}, (1,p_\ell,\ldots,1,1)_{\text{all } \ell\neq i}, \ldots, (1,1,\ldots,p_\ell,1)_{\text{all } \ell\neq i}, (1,1,\ldots,p_\ell)_{\text{all } \ell\neq i}\rangle.$$

Recall that $T = \{p_1, \ldots, p_t\}$; consider an arbitrary member $(r_1, \ldots, r_{2g})$ of the 2-Selmer group $\mathrm{Sel}^{(2)}(J_k/\mathbb{Q})$ of (21), where each r_i is a squarefree integer representing an element of $\mathbb{Q}^*/(\mathbb{Q}^*)^2$.

Let

$$t_1 = \prod_{\substack{p\in T\\ p\mid r_1}} p \quad \text{and} \quad t_2 = \prod_{\substack{p\in T\\ p\mid r_2}} p.$$

Consider the case where there does not exist any p_i dividing either r_1 or r_2. Then $t_1 = t_2 = 1$.

Consider the case where some p_i divides r_1 and r_2. From (21), (39), (40) we see that $7 \nmid r_1$ and $7 \nmid r_2$. This case can only arise if the expression of $(r_1, \ldots, r_{2g})$ as a product of generators on the right hand side of (40) involves the first two elements of H. Hence, for all j, the expression of $(r_1, \ldots, r_{2g})$ as a product of generators on the right hand side of (40) with $i = j$ must involve both or neither of the first two elements of H, and no other generator can contribute a factor of p_j to r_1 or r_2. Hence, for all j, $p_j \mid r_1 \Leftrightarrow p_j \mid t_2$, so $t_1 = t_2$.

Consider the case where some p_i divides r_1 but does not divide r_2. From (21), (39), (40) we see that $7 \mid r_1$ and $7 \mid r_2$. This case can only arise if the expression of $(r_1, \ldots, r_{2g})$ as a product of generators on the right hand side of (40) involves the first and not the second element of H. Hence, for all j, the expression of $(r_1, \ldots, r_{2g})$ as a product of generators on the right hand side of (40) with $i = j$ must involve exactly one of the first two elements of H, and no other generator can contribute a factor of p_j to r_1 or r_2. Hence, for all j, $p_j|r_1 \Leftrightarrow p_j \nmid t_2$, so $t_1 t_2 = k$.

The remaining case, where there exists some p_i which divides r_2 but does not divide r_1, similarly gives $t_1 t_2 = k$.

It now follows that for $(r_1, \ldots, r_{2g})$ in the 2-Selmer group $\mathrm{Sel}^{(2)}(J_k/\mathbb{Q})$, the squarefree integer representing $r_1 r_2$ in $\mathbb{Q}^*/(\mathbb{Q}^*)^2$ must be divisible either by no members of T or by all members of T. Since $\operatorname{im} q \subseteq \mathrm{Sel}^{(2)}(J_k/\mathbb{Q})$, the same must be true of any member of $\operatorname{im} q$. Furthermore, as we have previously observed, for any $D \in J_k(\mathbb{Q})$, if $q(D) = (r_1, r_2, r_3, r_4, \ldots, r_{2g-1}, r_{2g})$ then $q^{\hat{\phi}}(D) = (r_1r_2, r_3r_4, \ldots, r_{2g-1}r_{2g})$. Hence

$$(41) \qquad (\gamma_1, \ldots, \gamma_g) \in \operatorname{im} q^{\hat{\phi}} \implies (\forall i, p_i | \gamma_1) \text{ or } (\nexists i,\ p_i \mid \gamma_1),$$

where each γ_i is a squarefree integer representing an element of $\mathbb{Q}^*/(\mathbb{Q}^*)^2$. If we now merge pairs of entries in (39), we see that

$$(42) \qquad q^{\hat{\phi}}([(\beta_1, 0) - (\beta_0, 0)]) = (kw_1^{(1)}w_2^{(1)}, w_3^{(1)}w_4^{(1)}, \ldots, w_{2g-1}^{(1)}w_{2g}^{(1)}),$$

after removing the factor of 7^2 from the first entry since, as usual, all entries are modulo squares. Recall that the prime factors of $w_1^{(1)}, \ldots, w_{2g}^{(1)}$ come entirely from $U \setminus \{7, \infty\}$, and our conditions imply that all members of $U \setminus \{7, \infty\}$ are in every $(\mathbb{Q}_{p_i}^*)^2$. Recall also that for any distinct i, ℓ, our conditions show that $p_\ell \in (\mathbb{Q}_{p_i}^*)^2$.

Hence, for any distinct i, j, the above equals $(p_ip_j, 1, \ldots, 1)$ in both of $(\mathbb{Q}_{p_i}^*/(\mathbb{Q}_{p_i}^*)^2)^{\times g}$ and $(\mathbb{Q}_{p_j}^*/(\mathbb{Q}_{p_j}^*)^2)^{\times g}$, so $(p_ip_j, 1, \ldots, 1)$ is in $j_{p_i}^{-1}(\operatorname{im} q_{p_i}^{\hat{\phi}})$ and $j_{p_j}^{-1}(\operatorname{im} q_{p_j}^{\hat{\phi}})$. Also, $(p_ip_j, 1, \ldots, 1) = (1, \ldots, 1)$ in $(\mathbb{Q}_{p_\ell}^*/(\mathbb{Q}_{p_\ell}^*)^2)^{\times g}$ for all $\ell \notin \{i, j\}$ and in $(\mathbb{Q}_\pi^*/(\mathbb{Q}_\pi^*)^2)^{\times g}$ for all $\pi \in U$ (including $\pi = 7$), so in all of these cases is the image of the identity under q_{p_ℓ} and q_π. Hence $(p_ip_j, 1, \ldots, 1)$ is in $j_{p_\ell}^{-1}(\operatorname{im} q_{p_\ell}^{\hat{\phi}})$ for all $\ell \notin \{i, j\}$, and in $j_\pi^{-1}(\operatorname{im} q_\pi^{\hat{\phi}})$ for all $\pi \in U$.

In summary, for any distinct i, j and for any $p \in S$, $(p_ip_j, 1, \ldots, 1)$ is in $j_p^{-1}(\operatorname{im} q_p^{\hat{\phi}})$, so in $\mathrm{Sel}^{\hat{\phi}}(\widehat{J}_k/\mathbb{Q})$. These elements span a $(t-1)$-dimensional $\mathbb{F}_2$-subspace V of $\mathrm{Sel}^{\hat{\phi}}(\widehat{J}_k/\mathbb{Q})$. By (41), $(\operatorname{im} q^{\hat{\phi}}) \cap V$ is contained in the 1-dimensional subspace spanned by $(p_1 \ldots p_t, 1, 1, \ldots, 1)$. The intersection is the kernel of the composition $V \hookrightarrow \mathrm{Sel}^{\hat{\phi}}(\widehat{J}_k/\mathbb{Q}) \twoheadrightarrow \text{Ш}(\widehat{J}_k/\mathbb{Q})[\hat{\phi}]$ so the image of $V \to \text{Ш}(\widehat{J}_k/\mathbb{Q})[\hat{\phi}]$ has dimension at least $(t-1) - 1 = t - 2$. It follows that, for each g, $\text{Ш}(\widehat{J}_k/\mathbb{Q})[\hat{\phi}]$ can be arbitrarily large. ∎

We note here the following standard result.

Lemma 1. *The following is an exact sequence:*

$$(43) \qquad 0 \to \text{Ш}(\widehat{J}_k/\mathbb{Q})[\hat{\phi}] \to \text{Ш}(\widehat{J}_k/\mathbb{Q})[2] \to \text{Ш}(J_k/\mathbb{Q})[\phi],$$

so $\text{Ш}(\widehat{J}_k/\mathbb{Q})[\hat{\phi}]$ *injects into* $\text{Ш}(\widehat{J}_k/\mathbb{Q})[2]$.

Proof. The analogous result for elliptic curves appears in the bottom row of the commutative diagram in [14, Section 5], and the same argument applies here. ∎

It remains to show that, for each genus g, there exists an example for which the Jacobian is absolutely simple. We first state the following result, which is [7, Theorem 8].

Lemma 2. *Let K be an infinite field of finite type over the prime field, for instance a number field. Let $g \geq 1$ be an integer, and let $f(x) \in K[x]$ be a squarefree polynomial of degree $2g$. Let A_s be the Jacobian of the hyperelliptic curve of genus g over $K(s)$ with the affine model $y^2 = (x - s)f(x)$. Then there are only finitely many $s \in K$ such that A_s is not absolutely simple.*

We use this to show the following result.

Lemma 3. *There exist $v, \alpha_1, \ldots, \alpha_g \in \mathbb{Z}$, with $0, v, -v, 1/v, -1/v, \alpha_1, \ldots, \alpha_g$ distinct, satisfying $7^1 \parallel \alpha_1$, $v \equiv 2 \pmod 7$ and $\alpha_i \equiv 1 \pmod 7$ for all $i \geq 2$, such that $\mathcal{C}_1$ (as in (14) with $k = 1$) has absolutely simple Jacobian.*

Proof. Let $d_1, \ldots, d_g$ be any choice of distinct integers satisfying $7^1 \parallel d_1$ and $d_i \equiv 4 \pmod 7$ for all $i \geq 2$ (for example, take $d_1 = 7$ and $d_i = 4 + 7i$ for $i \geq 2$). Now an application of Lemma 2, with $K = \mathbb{Q}$, to the polynomial

$$f(x) = ((x+1)^2 - d_1^2x^2) \ldots ((x+1)^2 - d_g^2x^2) \tag{44}$$

shows that there are only finitely many $s \in \mathbb{Q}$ for which the Jacobian of $y^2 = (x-s)f(x)$ is not absolutely simple. For any $s \in \mathbb{Q}$ there are at most two values of $v \in \mathbb{Q}$ such that $v^2/(1-v^2) = s$, so there must also be only a finite set of values of $v \in \mathbb{Q}$ for which the Jacobian of $y^2 = (x - v^2/(1-v^2))f(x)$ is not absolutely simple. Hence there exists $v \in \mathbb{Z}$, with $v \equiv 2 \pmod 7$ which is outside this finite set. Define $\alpha_i = vd_i \in \mathbb{Z}$ for all i, so $7^1 \parallel \alpha_1$ and $\alpha_i \equiv 1 \pmod 7$ for all $i \geq 2$. Hence the Jacobian of the following curve is absolutely simple:

$$y^2 = \left(x - \frac{v^2}{1-v^2}\right)\left((x+1)^2 - \left(\frac{\alpha_1}{v}\right)^2 x^2\right) \ldots \left((x+1)^2 - \left(\frac{\alpha_g}{v}\right)^2 x^2\right). \tag{45}$$

Replacing y by $y\sqrt{v/(v^2-1)}/(x-v)^{g+1}$ and x by $v/(x-v)$ takes this to (1) with $a_i = \alpha_i^2$ for each i (a check of the above map has been included in [10]), so these are birationally equivalent over $\mathbb{C}$. We have already seen that (1), with $a_i = \alpha_i^2$ for each i, is birationally equivalent to $\mathcal{C}_1$ (as in (14) with $k = 1$), so $\mathcal{C}_1$ must also have absolutely simple Jacobian. ■

We are now in a position to prove the main theorem, which was stated in the introduction.

Proof of Theorem 1. For any g, let $v, \alpha_1, \ldots, \alpha_g \in \mathbb{Z}$ be as in Lemma 3, so $\mathcal{C}_1$ has absolutely simple Jacobian J_1. Then $\widehat{J}_1$, the Jacobian of $\widehat{\mathcal{C}}_1$, must also be absolutely simple, since it is isogenous to J_1. Note that $v, \alpha_1, \ldots, \alpha_g \in \mathbb{Z}$ then also satisfy the conditions of Theorem 2, and let k be as described in the statement of that theorem. By Theorem 2, $Ш(\widehat{J}_k/\mathbb{Q})[\hat{\phi}]$ is arbitrarily large, so, by Lemma 1, $Ш(\widehat{J}_k/\mathbb{Q})[2]$ is arbitrarily large. Hence $\widehat{\mathcal{C}}_1$ is a hyperelliptic curve of genus g over $\mathbb{Q}$, with absolutely simple Jacobian, such that the 2-torsion part of the Tate–Shafarevich groups is arbitrarily large amongst its quadratic twists. ∎

The congruence conditions modulo 7 in Theorem 2 hold for a positive density set of $(v, \alpha_1, \ldots, \alpha_g) \in \mathbb{Z}^{g+1}$. For $s = a/b \in \mathbb{Q}$ with $a, b \in \mathbb{Z}$ coprime, let $H(s) = \max(|a|, |b|)$. Let $n \in \mathbb{N}$; for $z = (z_1, \ldots, z_n) \in \mathbb{Q}^n$, let $H(z) = \max(H(z_1), \ldots, H(z_n))$. For any subsets W_1, W_2 of $\mathbb{Q}^n$ with $W_1 \subseteq W_2$, if the limit of $|\{z \in W_1 : H(z) \le B\}|/|\{z \in W_2 : H(z) \le B\}|$ exists as $B \to \infty$, then we call this the *density* of W_1 in W_2. The proof of Theorem 2 might be modified to apply to a positive density set of the $(v, \alpha_1, \ldots, \alpha_g)$ in $\mathbb{Q}^{g+1}$; if one varies the theorem to conditions modulo q for other $q \ge 7$, and combines these, then one might aim to show that there are density 1 of these in $\mathbb{Q}^{g+1}$. We may similarly define the density of a given set of hyperelliptic curves of genus g over $\mathbb{Q}$, given by $y^2 = f(x)$, where $f(x)$ is a polynomial of degree $2g+1$ or $2g+2$ with no repeated roots, by regarding both the given set and the set of all hyperelliptic curves of genus g over $\mathbb{Q}$ as subsets of $\mathbb{Q}^{2g+2}$ by identifying each curve $y^2 = f(x)$ with the sequence of coefficients of $f(x)$. One might hope for the following to be true.

CONJECTURE 1. *For any $g \ge 1$, density 1 of hyperelliptic curves $\mathcal{C} : y^2 = f(x)$ of genus g over $\mathbb{Q}$ have the property that the 2-part of the Tate–Shafarevich group of the Jacobian is arbitrarily large amongst quadratic twists $\mathcal{C}_k : y^2 = kf(x)$ with $k \in \mathbb{Q}$.*

It is also possible that the above conjecture holds for all hyperelliptic curves over $\mathbb{Q}$.

References

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

[2] J.-B. Bost et J.-F. Mestre, *Moyenne arithmético-géometrique et périodes de courbes de genre 1 et 2*, Gaz. Math. 38 (1988), 36–64.

[3] J. W. S. Cassels, *Arithmetic on curves of genus 1, VI. The Tate–Šafarevič group can be arbitrarily large*, J. Reine Angew. Math. 214/215 (1964), 65–70.

[4] J. W. S. Cassels and E. V. Flynn, *Prolegomena to a Middlebrow Arithmetic of Curves of Genus 2*, London Math. Soc. Lecture Note Ser. 230, Cambridge Univ. Press, Cambridge, 1996.

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

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

[7] J. S. Ellenberg, C. Elsholtz, C. Hall and E. Kowalski, *Non-simple abelian varieties in a family: geometric and analytic approaches*, J. London Math. Soc. 80 (2009), 135–154.

[8] T. Fisher, *Some examples of 5 and 7 descent for elliptic curves over* $\mathbb{Q}$, J. Eur. Math. Soc. 3 (2001), 169–201.
[9] E. V. Flynn, *Arbitrarily large Tate–Shafarevich group on abelian surfaces*, J. Number Theory 186 (2018), 248–258.
[10] E. V. Flynn, https://people.maths.ox.ac.uk/flynn/genus2/maple/maple38.
[11] R. Kloosterman, *The p-part of the Tate–Shafarevich groups of elliptic curves can be arbitrarily large*, J. Théor. Nombres Bordeaux 17 (2005), 787–800.
[12] R. Kloosterman and E. F. Schaefer, *Selmer groups of elliptic curves that can be arbitrarily large*, J. Number Theory 99 (2003), 148–163.
[13] K. Kramer, *A family of semistable elliptic curves with large Tate–Shafarevich groups*, Proc. Amer. Math. Soc. 89 (1983), 379–386.
[14] F. Lemmermeyer, *On Tate–Shafarevich groups of some elliptic curves*, in: Algebraic Number Theory and Diophantine Analysis (Graz, 1998), de Gruyter, Berlin, 2000, 277–291.
[15] 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.
[16] K. Matsuno, *Construction of elliptic curves with large Iwasawa* λ*-invariants and large Tate–Shafarevich groups*, Manuscripta Math. 122 (2007), 289–304.
[17] J.-F. Mestre, *Une généralisation d'une construction de Richelot*, J. Algebraic Geom. 22 (2013), 575–580.
[18] E. F. Schaefer, *2-descent on the Jacobians of hyperelliptic curves*, J. Number Theory 51 (1995), 219–232.
[19] E. F. Schaefer, *Computing a Selmer group of a Jacobian using functions on the curve*, Math. Ann. 310 (1998), 447–471.
[20] J. H. Silverman, *The Arithmetic of Elliptic Curves*, Grad. Texts in Math. 106, Springer, New York, 2009.

E. V. Flynn
Mathematical Institute
University of Oxford
Andrew Wiles Building
Radcliffe Observatory Quarter, Woodstock Road
Oxford OX2 6GG
United Kingdom
E-mail: flynn@maths.ox.ac.uk