JOURNAL
de Théorie des Nombres
de BORDEAUX

anciennement Séminaire de Théorie des Nombres de Bordeaux

Anna ARNTH-JENSEN et E. Victor FLYNN

Non-trivial Ш in the Jacobian of an infinite family of curves of genus 2

Tome 21, n^o 1 (2009), p. 1-13.

<http://jtnb.cedram.org/item?id=JTNB_2009__21_1_1_0>

Journal de Théorie des Nombres
de Bordeaux **21** (2009), 1-13

Non-trivial Ш in the Jacobian of an infinite family of curves of genus 2

par Anna ARNTH-JENSEN et E. Victor FLYNN

Résumé. Nous donnons une famille infinie de courbes de genre 2 dont la Jacobienne possède des éléments non triviaux du groupe de Tate-Shafarevich pour une descente via l'isogénie de Richelot. Nous le prouvons en effectuant une descente via l'isogénie de Richelot et une 2-descente complète sur la Jacobienne isogène. Nous donnons également un modèle explicite d'une famille associée de surfaces qui violent le principe de Hasse.

Abstract. We give an infinite family of curves of genus 2 whose Jacobians have non-trivial members of the Tate-Shafarevich group for descent via Richelot isogeny. We prove this by performing a descent via Richelot isogeny and a complete 2-descent on the isogenous Jacobian. We also give an explicit model of an associated family of surfaces which violate the Hasse principle.

1. Introduction

Let $\mathcal{C} : y^2 = F(x)$, where $F(x)$ is a polynomial of degree 5 or 6, denote a curve of genus 2 over $\mathbb{Q}$ and let $\mathcal{J}$ denote its Jacobian.

In connection with computing the rank of the finitely generated Mordell-Weil group $\mathcal{J}(\mathbb{Q})$ it is relevant to determine the size of $\mathcal{J}(\mathbb{Q})/2\mathcal{J}(\mathbb{Q})$. This is bounded by the size of the Selmer group $S^{(2)}(\mathcal{J}/\mathbb{Q})$ which is effectively computable. The size of the 2-part of the Tate-Shafarevich group $Ш(\mathcal{J}/\mathbb{Q})[2]$ measures the deviation of the Selmer group from $\mathcal{J}(\mathbb{Q})/2\mathcal{J}(\mathbb{Q})$, since

$$0 \to \mathcal{J}(\mathbb{Q})/2\mathcal{J}(\mathbb{Q}) \to S^{(2)}(\mathcal{J}/\mathbb{Q}) \to Ш(\mathcal{J}/\mathbb{Q})[2] \to 0.$$

The group $S^{(2)}(\mathcal{J}/\mathbb{Q})$ can be determined by means of descent methods. The method of complete 2-descent [11] makes possible a determination of the 2-Selmer group $S^{(2)}(\mathcal{J}/\mathbb{Q})$ in the case where $F(X)$ has degree 5. In the case where the equation of $\mathcal{C}$ is in sextic form the method of descent via isogeny [5],[7] often proves useful. More precisely, this method can be applied if $F(x)$ is of the form $F(x) = G_1(x)G_2(x)G_3(x)$, where each $G_i(x) \in \mathbb{Q}[x]$ is of degree 2. Both methods avoid the use of homogeneous spaces and

The first author thanks EPSRC for support: postgraduate studentship. The second author thanks EPSRC for support: grant number EP/F060661/1.

so are well suited for explicit computations. Section 2 briefly reviews the main points of these methods.

No known algorithm for computing $Ш(\mathcal{J}/\mathbb{Q})[2]$ exists. However, it is sometimes possible to demonstrate non-trivial members of this group; [2] contains a specific numerical example of a pair of curves of genus 2, $\mathcal{C}$ and $\mathcal{D}$, over $\mathbb{Q}$ with Richelot isogenous Jacobians $\mathrm{Jac}(\mathcal{C})$ and $\mathrm{Jac}(\mathcal{D})$, where complete 2-descents on each Jacobian result in the rank bounds $\mathrm{rank}(\mathrm{Jac}(\mathcal{C})(\mathbb{Q})) \leq 4$ and $\mathrm{rank}(\mathrm{Jac}(\mathcal{D})(\mathbb{Q})) = 0$, thereby proving the existence of non-trivial members of $Ш(\mathrm{Jac}(\mathcal{C})/\mathbb{Q})[2]$. In Section 3 we take this idea of demonstrating non-trivial members of the Tate-Shafarevich group by playing off two descents against each other a step further: we give an example where non-trivial members of the ϕ-part of the Tate-Shafarevich group of a Jacobian can be demonstrated by performing a 2-descent as well as a descent via isogeny where ϕ is a 2-isogeny. Furthermore, our example will be for a familiy of curves, whereas the Richelot example in [2] is only for a specific numerical example (there is also a family of examples in [2] using instead the Brauer-Manin obstruction on a related degree 4 del Pezzo surface, as is also the case in [3],[10]).

2. Descent methods

First, we outline the method of complete 2-descent [8],[11],[12]; we shall do this for the quintic case, but note that there are also algorithms described for the general sextic case, for example, in [4],[9],[14]. We let $\mathcal{C} : y^2 = F(x)$ denote a curve of genus 2 defined over $\mathbb{Q}$ and assume that $\deg(F(x)) = 5$. Let $\mathcal{J}$ denote its Jacobian. Furthermore, let $F(x) = F_1(x) \cdot \ldots \cdot F_n(x)$, $n \leq 5$, denote the irreducible factorization of $F(x)$ and let α_i denote a root of $F_i(x)$, $1 \leq i \leq n$. We define $L_i := \mathbb{Q}(\alpha_i)$. There exists an injective homomorphism

$$(2.1) \qquad \mu' : \quad \mathcal{J}(\mathbb{Q})/2\mathcal{J}(\mathbb{Q}) \to L_1^*/(L_1^*)^2 \times \ldots \times L_n^*/(L_n^*)^2$$

given by

$$(2.2) \quad \{(x_1, y_1), (x_2, y_2)\} \mapsto [(x_1 - \alpha_1)(x_2 - \alpha_1), \ldots, (x_1 - \alpha_n)(x_2 - \alpha_n)],$$

where $\{(x_1, y_1), (x_2, y_2)\}$ is a shorthand notation for the divisor class containing $(x_1, y_1) + (x_2, y_2) - 2\infty$. We let $\mathcal{S}$ denote the finite set of primes in $\mathbb{Q}$ consisting of the prime ∞, the prime 2 and the primes of bad reduction for $\mathcal{J}$. The image of μ' is a subgroup of the finite group M generated by the elements $[c_1, \ldots, c_n]$ with the following property: The field extensions $L_1(\sqrt{c_1}) : L_1, \ldots, L_n(\sqrt{c_n}) : L_n$ are ramified only at primes lying over primes of $\mathcal{S}$. Let $p \in \mathcal{S}$ and let $\mathbb{Q}_p$ denote the p-adic numbers. We have a commutative diagram

(2.3)
$$\begin{tikzcd} \mathcal{J}(\mathbb{Q})/2\mathcal{J}(\mathbb{Q}) \arrow[r, "\mu'"] \arrow[d, "i_p"] & M \arrow[d, "j_p"] \\ \mathcal{J}(\mathbb{Q}_p)/2\mathcal{J}(\mathbb{Q}_p) \arrow[r, "\mu'_p"] & M_p \end{tikzcd}$$

where μ'_p and M_p are the local equivalents of μ' and M and the maps i_p and j_p are induced by the natural injection $\mathbb{Q} \hookrightarrow \mathbb{Q}_p$. The method now works as follows: we start with a finite set of elements of $\mathcal{J}(\mathbb{Q})$ which we suspect generate (or form part of a generating set of) $\mathcal{J}(\mathbb{Q})/2\mathcal{J}(\mathbb{Q})$. We then search for a set of generators for $\mathcal{J}(\mathbb{Q}_p)/2\mathcal{J}(\mathbb{Q}_p)$. According to [4] (p.73):

(2.4)
$$\#\mathcal{J}(\mathbb{Q}_p)/2\mathcal{J}(\mathbb{Q}_p) = \#\mathcal{J}(\mathbb{Q}_p)[2]/|2|_p^2,$$

which tells us when a complete set of generators has been found. Now, we can compute $j_p^{-1}(\mathrm{im}\mu'_p)$ which, by the commutativity of (2.3), contains $\mathrm{im}\mu'$. Repeating this process for every $p \in \mathcal{S}$ we can compute

$$\bigcap_{p\in\mathcal{S}} j_p^{-1}(\mathrm{im}\mu'_p) \cong S^{(2)}(\mathcal{J}/\mathbb{Q}).$$

which contains $\mathrm{im}\mu'$. If $\bigcap_{p\in\mathcal{S}} j_p^{-1}(\mathrm{im}\mu'_p) = \mathrm{im}\mu'$, then $\mathcal{J}(\mathbb{Q})/2\mathcal{J}(\mathbb{Q})$ has been completely determined, and thus $r = \mathrm{rank}(\mathcal{J}(\mathbb{Q}))$, using the fact that $\mathcal{J}(\mathbb{Q})/2\mathcal{J}(\mathbb{Q}) \cong (\mathbb{Z}/2\mathbb{Z})^r \times \mathcal{J}(\mathbb{Q})[2]$, given that $\mathcal{J}(\mathbb{Q})[2]$ is easy to compute. Otherwise, we are either missing some generators for $\mathcal{J}(\mathbb{Q})/2\mathcal{J}(\mathbb{Q})$ or there are non-trivial members of $\text{Ш}(\mathcal{J}/\mathbb{Q})[2]$.

Next, we describe the method of descent via Richelot isogeny [4],[5],[7]. We let $\mathcal{C} : y^2 = F(x)$ denote a curve of genus 2 defined over $\mathbb{Q}$ and we assume that $F(x) = G_1(x)G_2(x)G_3(x)$, where each $G_i(x) = g_{i2}x^2 + g_{i1}x + g_{i0} \in \mathbb{Q}[x]$, $i = 1, 2, 3$, has degree 2. We let $\mathcal{J}$ denote the Jacobian of $\mathcal{C}$. We define

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

where $L_k(x) := G'_{k+1}(x)G_{k+2}(x) - G_{k+1}(x)G'_{k+2}(x)$, $k = 1, 2, 3$ (here the indices should be interpreted modulo 3) and $\Delta := \det(g_{ij})$. Letting $\widehat{\mathcal{J}}$ denote the Jacobian of $\widehat{\mathcal{C}}$ it can be shown that $\mathcal{J}$ is isogenous to $\widehat{\mathcal{J}}$ over $\mathbb{Q}$. More precisely, there exist isogenies defined over $\mathbb{Q}$, $\varphi : \mathcal{J} \to \widehat{\mathcal{J}}$ and $\hat{\varphi} : \widehat{\mathcal{J}} \to \mathcal{J}$, such that $\hat{\varphi} \circ \varphi = [2]$. For each of these Richelot isogenies, the kernel is exactly the group consisting of the identity and the three rational points of order 2 corresponding to the above quadratic factors (G_1, G_2, G_3 or L_1, L_2, L_3). The exact sequence

(2.5)
$$0 \to \ker\hat{\varphi} \to \widehat{\mathcal{J}}(\mathbb{Q})/\varphi(\mathcal{J}(\mathbb{Q})) \xrightarrow{\hat{\varphi}} \mathcal{J}(\mathbb{Q})/2\mathcal{J}(\mathbb{Q}) \to \mathcal{J}(\mathbb{Q})/\hat{\varphi}(\widehat{\mathcal{J}}(\mathbb{Q})) \to 0$$

now reduces the problem of determining $\mathcal{J}(\mathbb{Q})/2\mathcal{J}(\mathbb{Q})$ and the rank of $\mathcal{J}(\mathbb{Q})$ to finding generators for $\widehat{\mathcal{J}}(\mathbb{Q})/\varphi(\mathcal{J}(\mathbb{Q}))$ and $\mathcal{J}(\mathbb{Q})/\hat{\varphi}(\widehat{\mathcal{J}}(\mathbb{Q}))$ which can be performed in a way similar to complete 2-descent: letting $b_{ij} = \text{resultant}(G_i, G_j)$, and similarly, $\hat{b}_{ij} = \text{resultant}(L_i, L_j)$, we define $\mathcal{S}$ as the finite set of rational primes consisting of the prime 2 and the primes dividing $\Delta b_{12}b_{23}b_{31}\hat{b}_{12}\hat{b}_{23}\hat{b}_{31}$. We can write $\mathcal{S} = \{p_1, \dots, p_r\}$ and define $\mathbb{Q}(\mathcal{S}) = \{\pm p_1^{e_1} \cdots p_r^{e_r} \mid e_1, \dots, e_r = 0, 1\}$. There exists an injective homomorphism

$$\mu^{\varphi} : \widehat{\mathcal{J}}(\mathbb{Q})/\varphi(\mathcal{J}(\mathbb{Q})) \to (\mathbb{Q}^*/(\mathbb{Q}^*)^2)^{\times 2}$$

given by

$$\{(x_1, y_1), (x_2, y_2)\} \mapsto [L_1(x_1)L_1(x_2), L_2(x_1)L_2(x_2)].$$

In fact, $\text{im}\mu^{\varphi}$ sits inside the finite group $\mathbb{Q}(\mathcal{S})^{\times 2}$ and for any rational finite or infinite prime p we have a commutative diagram

$$\begin{tikzcd}
\widehat{\mathcal{J}}(\mathbb{Q})/\varphi(\mathcal{J}(\mathbb{Q})) \arrow[r, "\mu^{\varphi}"] \arrow[d, "i_p"] & \mathbb{Q}(\mathcal{S})^{\times 2} \arrow[d, "j_p"] \\
\widehat{\mathcal{J}}(\mathbb{Q}_p)/\varphi(\mathcal{J}(\mathbb{Q}_p)) \arrow[r, "\mu_p^{\varphi}"] & (\mathbb{Q}_p^*/(\mathbb{Q}_p^*)^2)^{\times 2}
\end{tikzcd} \tag{2.6}$$

where i_p and j_p are natural maps on the quotient induced by the inclusion map $\mathbb{Q} \hookrightarrow \mathbb{Q}_p$ and μ_p^{φ} is the local equivalent of μ^{φ}. Reversing the roles of $\mathcal{J}$ and $\widehat{\mathcal{J}}$ we obtain an injective homomorphism $\mu^{\hat{\varphi}} : \mathcal{J}(\mathbb{Q})/\hat{\varphi}(\widehat{\mathcal{J}}(\mathbb{Q})) \to (\mathbb{Q}^*/(\mathbb{Q}^*)^2)^{\times 2}$ and a diagram similar to (2.6). Using the fact [4],[6]

$$\#\widehat{\mathcal{J}}(\mathbb{Q}_p)/\varphi(\mathcal{J}(\mathbb{Q}_p)) \cdot \#\mathcal{J}(\mathbb{Q}_p)/\hat{\varphi}(\widehat{\mathcal{J}}(\mathbb{Q}_p)) = (4/|2|_p)^2 \tag{2.7}$$

to tell us when complete sets of generators for $\widehat{\mathcal{J}}(\mathbb{Q})/\varphi(\mathcal{J}(\mathbb{Q}))$ and $\mathcal{J}(\mathbb{Q})/\hat{\varphi}(\widehat{\mathcal{J}}(\mathbb{Q}))$ have been found, we now proceed similarly to the method of complete 2-descent and compute

$$\bigcap_p j_p^{-1}(\text{im}\mu_p^{\varphi}) \cong S^{(\varphi)}(\mathcal{J}/\mathbb{Q}) \quad \text{and} \quad \bigcap_p j_p^{-1}(\text{im}\mu_p^{\hat{\varphi}}) \cong S^{(\hat{\varphi})}(\widehat{\mathcal{J}}/\mathbb{Q}) \tag{2.8}$$

which, by the commutativity of (2.6), contain $\text{im}\mu^{\varphi}$ and $\text{im}\mu^{\hat{\varphi}}$, respectively.[1]

The main advantage of descent via isogeny is that of breaking the process of determining $\mathcal{J}(\mathbb{Q})/2\mathcal{J}(\mathbb{Q})$ into two easier steps, involving only computations over $\mathbb{Q}$ instead of some larger number field.

3. Family of Jacobians with non-trivial Ш

We consider the infinite family of curves of genus 2 given by

$$\mathcal{C} : \quad y^2 = F(x) = q(x^2 - 2)(x^2 + x)(x^2 + 1), \tag{3.1}$$

where q is a prime congruent to 13 modulo 24. Unless something else is explicitly stated we will always assume that q is of this form. We denote the Jacobian of $\mathcal{C}$ by $\mathcal{J}$. The curve whose Jacobian is isogenous to $\mathcal{J}$ is given

[1] We note that in (2.8) it is sufficient to intersect over the set of primes p satisfying $p | 2\Delta b_{12}b_{23}b_{31}\hat{b}_{12}\hat{b}_{23}\hat{b}_{31}$ or $p = \infty$.

by $y^2 = -3q(-x^2+2x+1)(-6qx)(qx^2+4qx+2q)$ which is birationally equivalent to

$$\widehat{\mathcal{C}}: \quad y^2 = (-x^2+2x+1)\cdot 2qx \cdot (x^2+4x+2). \tag{3.2}$$

The primes not dividing $2\cdot \mathrm{disc}(F)$ are the primes p satisfying $p \notin \{2,3,q\}$. Using the fact that the reduction map is injective on the rational torsion subgroup for $p = 11, 17$, in particular, we obtain

Lemma 3.1. *Let q be a prime congruent to 5 modulo 8. The torsion subgroups, $\mathcal{J}(\mathbb{Q})_{tors}$ and $\widehat{\mathcal{J}}(\mathbb{Q})_{tors}$, of $\mathcal{J}(\mathbb{Q})$ and $\widehat{\mathcal{J}}(\mathbb{Q})$ are given by*

$$\mathcal{J}(\mathbb{Q})_{tors} = \langle\{(\sqrt{2},0),(-\sqrt{2},0)\},\{(0,0),(-1,0)\}\rangle$$

and

$$\widehat{\mathcal{J}}(\mathbb{Q})_{tors} = \langle\{(1-\sqrt{2},0),(1+\sqrt{2},0)\},\{(0,0),\infty\}\rangle.$$

The curve $\mathcal{C}$ in (3.1) is seen to be in the form suitable for descent via isogeny and so we perform a descent via isogeny on its Jacobian (we have placed further details on the descent at [1]). Using the notation from the previous section we find that $2\Delta b_{12}b_{23}b_{31}\hat{b}_{12}\hat{b}_{23}\hat{b}_{31} = -2^8\cdot 3^5\cdot q^9$, so $\mathcal{S} = \{2,3,q\}$. Furthermore, we have injective homomorphisms

$$\mu^{\varphi}: \quad \widehat{\mathcal{J}}(\mathbb{Q})/\varphi(\mathcal{J}(\mathbb{Q})) \to (\mathbb{Q}^*/(\mathbb{Q}^*)^2)^{\times 2}$$

given by

$$\{(x_1,y_1),(x_2,y_2)\} \mapsto \left[\prod_{i=1}^{2}(-x_i^2+2x_i+1), \prod_{i=1}^{2} 2qx_i\right]$$

and

$$\mu^{\hat{\varphi}}: \quad \mathcal{J}(\mathbb{Q})/\hat{\varphi}(\widehat{\mathcal{J}}(\mathbb{Q})) \to (\mathbb{Q}^*/(\mathbb{Q}^*)^2)^{\times 2}$$

given by

$$\{(x_1,y_1),(x_2,y_2)\} \mapsto \left[\prod_{i=1}^{2} q(x_i^2-2), \prod_{i=1}^{2}(x_i^2+x_i)\right].$$

These satisfy

$$\mathrm{im}\mu^{\varphi}, \mathrm{im}\mu^{\hat{\varphi}} \le \mathbb{Q}(\mathcal{S})^{\times 2} = \langle[-1,1],[1,-1],[2,1],[1,2],[3,1],[1,3],[q,1],[1,q]\rangle.$$

The generators of the torsion subgroups map as follows:

$$\mathfrak{A}_1 := \{(\sqrt{2},0),(\sqrt{2},0)\} \overset{\mu^{\hat{\varphi}}}{\mapsto} [2,2],$$

$$\mathfrak{A}_2 := \{(0,0),(-1,0)\} \overset{\mu^{\hat{\varphi}}}{\mapsto} [2,1],$$

$$\widehat{\mathfrak{A}}_1 := \{(1-\sqrt{2},0),(1+\sqrt{2},0)\} \overset{\mu^{\varphi}}{\mapsto} [-1,1],$$

$$\widehat{\mathfrak{A}}_2 := \{(0,0),\infty\} \overset{\mu^{\varphi}}{\mapsto} [-1,2].$$

The last image was computed by using the fact that μ^{φ} is a homomorphism on $\{(1-\sqrt{2},0),(1+\sqrt{2},0)\}+\{(0,0),\infty\}=\{(-2+\sqrt{2},0),(-2-\sqrt{2},0)\}$. Thus,

$$H := \langle [2,2],[2,1]\rangle \le \mathrm{im}\mu^{\hat{\varphi}} \text{ and } \widehat{H} := \langle [-1,1],[-1,2]\rangle \le \mathrm{im}\mu^{\varphi}.$$

At $p=\infty$ we have in (2.6)

$$\ker j_{\infty} = \langle [2,1],[1,2],[3,1],[1,3],[q,1],[1,q]\rangle,$$

so $\mathfrak{A}_1$ and $\mathfrak{A}_2$ are both mapped to $[1,1]$ by $\mu^{\hat{\varphi}}$ whereas $\widehat{\mathfrak{A}}_1$ and $\widehat{\mathfrak{A}}_2$ are both mapped to $[-1,1]$. By (2.7) $\#\widehat{\mathcal{J}}(\mathbb{R})/\varphi(\mathcal{J}(\mathbb{R}))\cdot\#\mathcal{J}(\mathbb{R})/\hat{\varphi}(\widehat{\mathcal{J}}(\mathbb{R}))=2^2$ so we are missing 1 generator. A search yields $\mathfrak{B} := \{(2,\beta),(0,0)\}\in\mathcal{J}(\mathbb{R})$, where $\beta\in\mathbb{R}^*$ and $\beta^2=2^2\cdot 3\cdot 5\cdot q$, and $\mathfrak{B}\mapsto[-1,-1]\in(\mathbb{R}^*/(\mathbb{R}^*)^2)^{\times 2}$ by $\mu_{\infty}^{\hat{\varphi}}$. Hence, $\mathcal{J}(\mathbb{R})/\hat{\varphi}(\widehat{\mathcal{J}}(\mathbb{R}))=\langle\mathfrak{B}\rangle$ and $\widehat{\mathcal{J}}(\mathbb{R})/\varphi(\mathcal{J}(\mathbb{R}))=\langle\mathfrak{A}_1\rangle$. The commutativity of (2.6) implies

$$\begin{aligned}\mathrm{im}\mu^{\hat{\varphi}} &\le \langle \ker j_{\infty}, H, [-1,-1]\rangle\\ &= \langle [2,1],[1,2],[3,1],[1,3],[q,1],[1,q],[-1,-1]\rangle\end{aligned}$$

and

$$\begin{aligned}\mathrm{im}\mu^{\varphi} &\le \langle \ker j_{\infty}, \widehat{H}\rangle\\ &= \langle [2,1],[1,2],[3,1],[1,3],[q,1],[1,q],[-1,1]\rangle.\end{aligned}$$

Next, let $p=3$. Using $\{\pm1,\pm3\}$ as a set of representatives for $\mathbb{Q}_3^*/(\mathbb{Q}_3^*)^2$ we find

$$\ker j_3 = \langle [-2,1],[1,-2],[q,1],[1,q]\rangle,$$

and so the images of $\mathfrak{A}_1$ and $\mathfrak{A}_2$ in $\mathbb{Q}_3^*/(\mathbb{Q}_3^*)^2$ are independent and the images of $\widehat{\mathfrak{A}}_1$ and $\widehat{\mathfrak{A}}_2$ in $\mathbb{Q}_3^*/(\mathbb{Q}_3^*)^2$ are independent. By (2.7) $\#\widehat{\mathcal{J}}(\mathbb{Q}_3)/\varphi(\mathcal{J}(\mathbb{Q}_3))\cdot\#\mathcal{J}(\mathbb{Q}_3)/\hat{\varphi}(\widehat{\mathcal{J}}(\mathbb{Q}_3))=2^4$, so that $\mathcal{J}(\mathbb{Q}_3)/\hat{\varphi}(\widehat{\mathcal{J}}(\mathbb{Q}_3))=\langle\mathfrak{A}_1,\mathfrak{A}_2\rangle$ and $\widehat{\mathcal{J}}(\mathbb{Q}_3)/\varphi(\mathcal{J}(\mathbb{Q}_3))=\langle\widehat{\mathfrak{A}}_1,\widehat{\mathfrak{A}}_2\rangle$. From diagram (2.6) we now get

$$\mathrm{im}\mu^{\hat{\varphi}} \le \langle \ker j_3, H\rangle = \langle [-2,1],[1,-2],[q,1],[1,q],[2,2],[2,1]\rangle \tag{3.3}$$

and

$$\mathrm{im}\mu^{\varphi} \le \langle \ker j_3, \widehat{H}\rangle = \langle [-2,1],[1,-2],[q,1],[1,q],[-1,1],[-1,2]\rangle. \tag{3.4}$$

We now let $p=q$ and observe that a set of representatives for $\mathbb{Q}_q^*/(\mathbb{Q}_q^*)^2$ is given by $\{1,2,q,2q\}$. We have

$$\ker j_q = \langle [-1,1],[1,-1],[3,1],[1,3]\rangle,$$

and so $\mathfrak{A}_1 \overset{j_q\circ\mu^{\hat{\varphi}}}{\mapsto} [2,2]$ and $\mathfrak{A}_2 \overset{j_q\circ\mu^{\hat{\varphi}}}{\mapsto} [2,1]$ while $\widehat{\mathfrak{A}}_1 \overset{j_q\circ\mu^{\varphi}}{\mapsto} [1,1]$ and $\widehat{\mathfrak{A}}_2 \overset{j_q\circ\mu^{\varphi}}{\mapsto} [1,2]$. Since $\#\widehat{\mathcal{J}}(\mathbb{Q}_q)/\varphi(\mathcal{J}(\mathbb{Q}_q))\cdot\#\mathcal{J}(\mathbb{Q}_q)/\hat{\varphi}(\widehat{\mathcal{J}}(\mathbb{Q}_q))=2^4$ according to (2.7), we are missing 1 generator. We suspect that we may choose the missing generator in $\mathcal{J}(\mathbb{Q}_q)/\hat{\varphi}(\widehat{\mathcal{J}}(\mathbb{Q}_q))$, in such a way that it is mapped to $[2,q]\in\mathbb{Q}_q^*/(\mathbb{Q}_q^*)^2$ by $\mu_q^{\hat{\varphi}}$. More precisely, by considering the explicit expression for the homomorphism $\mu_q^{\hat{\varphi}}$ it can be proved that there exists $(x,y) \in \mathcal{J}(\mathbb{Q}_q)$ such that $\mathcal{J}(\mathbb{Q}_q) \ni \{(0,0),(x,y)\} \mapsto [2,q] \in (\mathbb{Q}_q^*/(\mathbb{Q}_q^*)^2)^{\times 2}$ by $\mu_q^{\hat{\varphi}}$. Letting $\mathfrak{D} := \{(0,0),(x,y)\}$ we have $\mathcal{J}(\mathbb{Q}_q)/\hat{\varphi}(\widehat{\mathcal{J}}(\mathbb{Q}_q)) = \langle \mathfrak{A}_1, \mathfrak{A}_2, \mathfrak{D}\rangle$ and $\widehat{\mathcal{J}}(\mathbb{Q}_q)/\varphi(\mathcal{J}(\mathbb{Q}_q)) = \langle \widehat{\mathfrak{A}}_2\rangle$. The commutative diagram (2.6) tells us that

$$\mathrm{im}\mu^{\hat{\varphi}} \le \langle \ker j_q, H, [2,q]\rangle = \langle [-1,1],[1,-1],[3,1],[1,3],[2,2],[2,1],[2,q]\rangle$$

and

$$\mathrm{im}\mu^{\varphi} \le \langle \ker j_q, \widehat{H}\rangle = \langle [-1,1],[1,-1],[3,1],[1,3],[-1,2]\rangle.$$

Finally, we consider $p=2$. A set of representatives for $\mathbb{Q}_2^*/(\mathbb{Q}_2^*)^2$ is given by $\{\pm 1, \pm 2, \pm 3, \pm 6\}$ and

$$\ker j_2 = \langle [-3q,1],[1,-3q]\rangle,$$

so $j_2 \circ \mu^{\hat{\varphi}}(\mathfrak{A}_1) = [2,2]$, $j_2 \circ \mu^{\hat{\varphi}}(\mathfrak{A}_2) = [2,1]$, $j_2 \circ \mu^{\varphi}(\widehat{\mathfrak{A}}_1) = [-1,1]$ and $j_2 \circ \mu^{\varphi}(\widehat{\mathfrak{A}}_2) = [-1,2]$. Since $\#\widehat{\mathcal{J}}(\mathbb{Q}_2)/\varphi(\mathcal{J}(\mathbb{Q}_2)) \cdot \#\mathcal{J}(\mathbb{Q}_2)/\hat{\varphi}(\widehat{\mathcal{J}}(\mathbb{Q}_2)) = 2^6$ by (2.7), we are missing 2 generators. First, we find $\mathfrak{C}_1 := \{(5,\eta_1),(0,0)\} \in \mathcal{J}(\mathbb{Q}_2)$, where $\eta_1 \in \mathbb{Q}_2^*$ and $\eta_1^2 = 2^2 \cdot 3 \cdot 5 \cdot 13 \cdot 23 \cdot q$. The existence of η_1 is guaranteed by the fact that $3 \cdot 5 \cdot 13 \cdot 23 \cdot q \equiv 1 \pmod 8$, since $q \equiv 5 \pmod 8$. We have $\mathfrak{C}_1 \mapsto [2,-3] \in (\mathbb{Q}_2^*/(\mathbb{Q}_2^*)^2)^{\times 2}$ by $\mu_2^{\hat{\varphi}}$. Next, we find $\mathfrak{C}_2 := \{(\frac{1}{4},\eta_2),(0,0)\} \in \mathcal{J}(\mathbb{Q}_2)$, where $\eta_2 \in \mathbb{Q}_2^*$ and $\eta_2^2 = \frac{-5\cdot 17\cdot 31\cdot q}{(2^6)^2}$. The existence of η_2 is guaranteed by the fact that $-5 \cdot 17 \cdot 31 \cdot q \equiv 1 \pmod 8$, since $q \equiv 5 \pmod 8$. We have $\mathfrak{C}_2 \mapsto [-2,-2] \in (\mathbb{Q}_2^*/(\mathbb{Q}_2^*)^2)^{\times 2}$ by $\mu_2^{\hat{\varphi}}$. Hence, $\mathcal{J}(\mathbb{Q}_2)/\hat{\varphi}(\widehat{\mathcal{J}}(\mathbb{Q}_2)) = \langle \mathfrak{A}_1, \mathfrak{A}_2, \mathfrak{C}_1, \mathfrak{C}_2\rangle$ and $\widehat{\mathcal{J}}(\mathbb{Q}_2)/\varphi(\mathcal{J}(\mathbb{Q}_2)) = \langle \widehat{\mathfrak{A}}_2, \widehat{\mathfrak{A}}_2\rangle$. Then (2.6) tells us that

$$\begin{aligned} \mathrm{im}\mu^{\hat{\varphi}} &\le \langle \ker j_2, H, [2,-3],[-2,-2]\rangle \\ &= \langle [-3q,1],[1,-3q],[2,2],[2,1],[2,-3],[-2,-2]\rangle \end{aligned} \tag{3.5}$$

and

$$\mathrm{im}\mu^{\varphi} \le \langle \ker j_2, \widehat{H}\rangle = \langle [-3q,1],[1,-3q],[-1,1],[-1,2]\rangle. \tag{3.6}$$

Using (3.3) and (3.5) we obtain $\mathrm{im}\mu^{\hat{\varphi}} \le \langle [-2,-2],[1,q],[2,2],[2,1]\rangle$. Taking the information at ∞ and q into account does not improve this bound on $\mathrm{im}\mu^{\hat{\varphi}}$. Thus, $H \le \mathrm{im}\mu^{\hat{\varphi}} \le \langle H, [-2,-2],[1,q]\rangle$, and so $\#\mathcal{J}(\mathbb{Q})/\hat{\varphi}(\widehat{\mathcal{J}}(\mathbb{Q})) \in \{4,8,16\}$. Similarly, from (3.4) and (3.6) we get $\mathrm{im}\mu^{\varphi} \le \widehat{H}$, and so $\mathrm{im}\mu^{\varphi} = \widehat{H}$, that is $\#\widehat{\mathcal{J}}(\mathbb{Q})/\varphi(\mathcal{J}(\mathbb{Q})) = 4$. By the exact sequence (2.5) we conclude that $\#\mathcal{J}(\mathbb{Q})/2\mathcal{J}(\mathbb{Q}) \in \{4,8,16\}$, giving a rank bound on $\mathcal{J}(\mathbb{Q})$ of 2. We have thus proved the following lemma:

Lemma 3.2. *Let $\mathcal{C}$ and $\widehat{\mathcal{C}}$ be as in (3.1) and (3.2), with Jacobians $\mathcal{J}$ and $\widehat{\mathcal{J}}$ and Richelot isogenies $\varphi : \mathcal{J} \to \widehat{\mathcal{J}}$ and $\hat{\varphi} : \widehat{\mathcal{J}} \to \mathcal{J}$ such that $\hat{\varphi} \circ \varphi = [2]$. Then*

$$\mathcal{J}(\mathbb{Q})/\hat{\varphi}(\widehat{\mathcal{J}}(\mathbb{Q})) \ge \langle \{(\sqrt{2},0),(-\sqrt{2},0)\}, \{(0,0),(-1,0)\}\rangle,$$

having 4 generators at the most, and

$$\widehat{\mathcal{J}}(\mathbb{Q})/\varphi(\mathcal{J}(\mathbb{Q})) = \langle \{(1-\sqrt{2},0),(1+\sqrt{2},0)\},\{(0,0),\infty\}\rangle.$$

This bounds the ranks of $\mathcal{J}(\mathbb{Q})$ *and* $\widehat{\mathcal{J}}(\mathbb{Q})$ *by 2.*

For the first 10 choices of $q \equiv 13 \pmod{24}$, a search for generators for $\mathcal{J}(\mathbb{Q})$ of infinite order does not yield any results and so we suspect that, for such cases, $\mathrm{rank}(\mathcal{J}(\mathbb{Q}))$ is in fact 0. We prove that this is the case by performing a complete 2-descent on $\mathcal{J}(\mathbb{Q})$. We have placed further details of the 2-descent at [1]. First, we observe that since $F(x)$ in (3.1) has a root in $\mathbb{Q}$ we can write the equation of the curve $\mathcal{C}$ in the form $y^2 =$ (quintic in x over $\mathbb{Q}$). In fact, using the transformation $(x,y) \mapsto (\frac{-2q}{x}, \frac{-2qy}{x^3})$ the curve given by (3.1) is seen to be birationally equivalent to the family of curves given by

$$y^2 = W(x) = (x-2q)(x^2-2q^2)(x^2+2^2q^2), \quad q \equiv 13 \pmod{24}. \tag{3.7}$$

By a slight abuse of notation we also denote this curve by $\mathcal{C}$ and its Jacobian by $\mathcal{J}$. By Lemma 3.1 $\mathcal{J}(\mathbb{Q})_{tors} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, and so $\mathcal{J}(\mathbb{Q})_{tors} = \langle \{(2q,0),\infty\},\{(q\sqrt{2},0),(-q\sqrt{2},0)\}\rangle$. In order to prove that the rank of $\mathcal{J}(\mathbb{Q})$ equals 0 it suffices to prove that $\overline{\mathfrak{A}}_1 := \{(2q,0),\infty\}$ and $\overline{\mathfrak{A}}_2 := \{(q\sqrt{2},0),(-q\sqrt{2},0)\}$ generate $\mathcal{J}(\mathbb{Q})/2\mathcal{J}(\mathbb{Q})$. By (2.1) and (2.2) there exists an injective homomorphism

$$\mu' : \quad \mathcal{J}(\mathbb{Q})/2\mathcal{J}(\mathbb{Q}) \to \mathbb{Q}^*/(\mathbb{Q}^*)^2 \times \mathbb{Q}(\sqrt{2})^*/(\mathbb{Q}(\sqrt{2})^*)^2 \times \mathbb{Q}(i)^*/(\mathbb{Q}(i)^*)^2$$

given by

$$\{(x_1,y_1),(x_2,y_2)\} \mapsto \left[\prod_{j=1}^{2}(x_j-2q), \prod_{j=1}^{2}(x_j+q\sqrt{2}), \prod_{j=1}^{2}(x_j+2qi)\right].$$

The primes dividing $\mathrm{disc}(W)$ are $2,3,q$, and so, using the notation of the previous section,

$$\begin{aligned} \mathrm{im}\mu' &\le M \\ &= \langle\, [-1,1,1],[2,1,1],[3,1,1],[q,1,1],[1,-1,1], \\ &\qquad [1,1+\sqrt{2},1],[1,\sqrt{2},1],[1,3,1],[1,q,1],[1,1,i], \\ &\qquad [1,1,1+i],[1,1,3],[1,1,a+bi],[1,1,a-bi]\,\rangle \end{aligned} \tag{3.8}$$

for fixed positive integers a and b satisfying $a^2+b^2=q$, $2|a$ and $2\nmid b$. The generators for the torsion subgroup map as follows:

$$\overline{\mathfrak{A}}_1 \overset{\mu'}{\mapsto} [1, q\sqrt{2}(1+\sqrt{2}), (a+bi)(a-bi)(1+i)i],$$
$$\overline{\mathfrak{A}}_2 \overset{\mu'}{\mapsto} [2, 3q\sqrt{2}(1+\sqrt{2}), 3i].$$

We define

$$\overline{H} := \langle [1, q\sqrt{2}(1+\sqrt{2}), (a+bi)(a-bi)(1+i)i], [2, 3q\sqrt{2}(1+\sqrt{2}), 3i] \rangle.$$

In view of our previous remark it is sufficient to show that $\overline{H} = \mathrm{im}\mu'$.

First, consider $p = \infty$. Since there are two embeddings of $\mathbb{Q}(\sqrt{2})^*$ into $\mathbb{R}^*$ we have $M_\infty \cong \mathbb{R}^*/(\mathbb{R}^*)^2 \times (\mathbb{R}^*/(\mathbb{R}^*)^2)^{\times 2} \times \mathbb{C}^*/(\mathbb{C}^*)^2$. Furthermore,

$$\ker j_\infty = \langle [2,1,1], [3,1,1], [q,1,1], [1, \sqrt{2}(1+\sqrt{2}), 1], [1,3,1], [1,q,1], [1,1,i], [1,1,1+i], [1,1,3], [1,1,a+bi], [1,1,a-bi] \rangle,$$

and so $j_\infty \circ \mu'(\overline{\mathfrak{A}}_1) = [1,[1,1],1]$ and $j_\infty \circ \mu'(\overline{\mathfrak{A}}_2) = [1,[1,1],1]$. Since $\#\mathcal{J}(\mathbb{R})[2] = 8$, (2.4) implies that $\#\mathcal{J}(\mathbb{R})/2\mathcal{J}(\mathbb{R}) = 2$, so we are missing one generator. We find $\overline{\mathfrak{B}} := \{(0,\beta), \infty\} \in \mathcal{J}(\mathbb{R})$, where $\beta \in \mathbb{R}$ and $\beta^2 = 2^4q^5$, and $\overline{\mathfrak{B}} \mapsto [-1,[1,-1],1]$ by μ'_∞. Hence, $\mathcal{J}(\mathbb{R})/2\mathcal{J}(\mathbb{R}) = \langle \overline{\mathfrak{B}} \rangle$. The commutativity of (2.3) gives

$$\mathrm{im}\mu' \leq \langle \ker j_\infty, \overline{H}, [-1, \sqrt{2}, 1] \rangle. \tag{3.9}$$

Next, we let $p = 3$. Sets of representatives for $\mathbb{Q}_3(\sqrt{2})^*/(\mathbb{Q}_3(\sqrt{2})^*)^2$ and $\mathbb{Q}_3(i)^*/(\mathbb{Q}_3(i)^*)^2$ are given by $\{1, 1+\sqrt{2}, 3, 3(1+\sqrt{2})\}$ and $\{1, 1+i, 3, 3(1+i)\}$, respectively. Furthermore

$$\ker j_3 = \langle [-2,1,1], [q,1,1], [1,-1,1], [1,\sqrt{2},1], [1,q,1], [1,1,i], [1,1,a+bi], [1,1,a-bi] \rangle,$$

and so $j_3 \circ \mu'(\overline{\mathfrak{A}}_1) = [1, 1+\sqrt{2}, 1+i]$ and $j_3 \circ \mu'(\overline{\mathfrak{A}}_2) = [-1, 3(1+\sqrt{2}), 3]$. Since $\#\mathcal{J}(\mathbb{Q}_3)/2\mathcal{J}(\mathbb{Q}_3) = 2^2$ by (2.4), the known members of $\mathcal{J}(\mathbb{Q})/2\mathcal{J}(\mathbb{Q})$ generate $\mathcal{J}(\mathbb{Q}_3)/2\mathcal{J}(\mathbb{Q}_3)$, that is $\mathcal{J}(\mathbb{Q}_3)/2\mathcal{J}(\mathbb{Q}_3) = \langle \overline{\mathfrak{A}}_1, \overline{\mathfrak{A}}_2 \rangle$. From (2.3) we have that

$$\mathrm{im}\mu' \leq \langle \ker j_3, \overline{H} \rangle. \tag{3.10}$$

Now, let $p = q$. A set of representatives for $\mathbb{Q}_q(\sqrt{2})^*/(\mathbb{Q}_q(\sqrt{2})^*)^2$ is given by $\{1, \sqrt{2}, q, q\sqrt{2}\}$. We let α denote the solution to $x^2 = -1$ in $\mathbb{Q}_q^*$ that makes $1+x$ a square in $\mathbb{Q}_q^*$. Then we have 2 embeddings of $\mathbb{Q}(i)^*$ into $\mathbb{Q}_q^*$ given by $x+yi \mapsto x+y\alpha$ and $x+yi \mapsto x-y\alpha$, and so $(\mathbb{Q}(i))_q^*/((\mathbb{Q}(i))_q^*)^2$ is isomorphic to $\mathbb{Q}_q^*/(\mathbb{Q}_q^*)^2 \times \mathbb{Q}_q^*/(\mathbb{Q}_q^*)^2$. Furthermore

$$\ker j_q = \langle [-1,1,1], [3,1,1], [1,-1,1], [1,1+\sqrt{2},1], [1,3,1], [1,1,3] \rangle,$$

which implies $j_q \circ \mu'(\overline{\mathfrak{A}}_1) = [1, q\sqrt{2}, [2q, q]]$ and $j_q \circ \mu'(\overline{\mathfrak{A}}_2) = [2, q\sqrt{2}, [2,2]]$. Since $\#\mathcal{J}(\mathbb{Q}_q)/2\mathcal{J}(\mathbb{Q}_q) = 2^3$ by (2.4), we are missing one generator for $\mathcal{J}(\mathbb{Q}_q)/2\mathcal{J}(\mathbb{Q}_q)$. We find $\overline{\mathfrak{D}} := \{(2\alpha q, 0), \infty\} \in \mathcal{J}(\mathbb{Q}_q)$, where $\mu'_q(\overline{\mathfrak{D}}) = [q, q\sqrt{2}(1+\alpha\sqrt{2}), [2q,1]] = [q, q\sqrt{2}, [2q,1]]$, since $1+\alpha\sqrt{2}$ is a square in

$\mathbb{Q}_q(\sqrt{2})^*$. Hence, $\mathcal{J}(\mathbb{Q}_q)/2\mathcal{J}(\mathbb{Q}_q) = \langle \overline{\mathfrak{A}}_1, \overline{\mathfrak{A}}_2, \overline{\mathfrak{D}} \rangle$. Since there exists $t \in \{a+bi, a-bi, (a+bi)i, (a-bi)i\}$ such that $M \ni [q, q\sqrt{2}, t(1+i)] \overset{j_q}{\mapsto} \mu'_q(\overline{\mathfrak{D}})$, the commutative diagram (2.3) implies that

$$\mathrm{im}\mu' \leq \langle \ker j_q, \overline{H}, [q, q\sqrt{2}, t(1+i)] \rangle. \tag{3.11}$$

Finally, we let $p = 2$. We note that 2 is ramified in $\mathbb{Q}(\sqrt{2})$. A set of representatives for $\mathbb{Q}_2(\sqrt{2})^*/(\mathbb{Q}_2(\sqrt{2})^*)^2$ is given by $\{\pm 1, \pm\sqrt{2}, \pm(1+\sqrt{2}), \pm 3, \pm\sqrt{2}(1+\sqrt{2}), \pm 3\sqrt{2}, \pm 3(1+\sqrt{2}), \pm 3\sqrt{2}(1+\sqrt{2})\}$. Also, 2 is ramified in $\mathbb{Q}(i)$ and $\{1, 1+i, 3, i, a+bi, 3i, 3(1+i), i(1+i), 3i(1+i), (a+bi)(1+i), 3(a+bi), (a+bi)i, 3i(a+bi), 3(1+i)(a+bi), i(1+i)(a+bi), 3i(1+i)(a+bi)\}$ is a set of representatives for $\mathbb{Q}_2(i)^*/(\mathbb{Q}_2(i)^*)^2$, where a and b are the integers from (3.8). Furthermore

$$\ker j_2 = \langle [-3q, 1, 1], [1, -3q, 1], [1, 1, 3q] \rangle,$$

giving $j_2 \circ \mu'(\overline{\mathfrak{A}}_1) = [1, -3\sqrt{2}(1+\sqrt{2}), 3(1+i)i]$ and $j_2 \circ \mu'(\overline{\mathfrak{A}}_2) = [2, -\sqrt{2}(1+\sqrt{2}), 3i]$. By (2.4) $\#\mathcal{J}(\mathbb{Q}_2)/2\mathcal{J}(\mathbb{Q}_2) = 2^4$, so we are missing two generators. Since $W(5) \in (\mathbb{Q}_2^*)^2$, there exists $\varepsilon_1 \in \mathbb{Q}_2^*$ such that $\varepsilon_1^2 = W(5)$, and so $\overline{\mathfrak{E}}_1 := \{(5, \varepsilon_1), \infty\} \in \mathcal{J}(\mathbb{Q}_2)$. In fact, $\mu'_2(\overline{\mathfrak{E}}_1) = [5-2q, 5+q\sqrt{2}, 5+2qi]$, which equals $[3, -3(1+\sqrt{2}), i(a+bi)]$ if $a \equiv 2 \pmod 8, b \equiv 1, 3 \pmod 8$ or $a \equiv 6 \pmod 8, b \equiv 5, 7 \pmod 8$, and equals $[3, -3(1+\sqrt{2}), 3i(a+bi)]$ if $a \equiv 2 \pmod 8, b \equiv 5, 7 \pmod 8$ or $a \equiv 6 \pmod 8, b \equiv 1, 3 \pmod 8$. Next, we observe that $\frac{W(8)}{2^2} \in (\mathbb{Q}_2^*)^2$, and so there exists $\varepsilon_2 \in \mathbb{Q}_2^*$ such that $\varepsilon_2^2 = \frac{W(8)}{2^2}$. Therefore, $\overline{\mathfrak{E}}_2 := \{(8, 2^2\varepsilon_2)\} \in \mathcal{J}(\mathbb{Q}_2)$. In fact, $\mu'_2(\overline{\mathfrak{E}}_2) = [8-2q, 8+q\sqrt{2}, 8+2qi] = [-2, -3\sqrt{2}, 1] \in M_2$. Hence, $\mathcal{J}(\mathbb{Q}_2)/2\mathcal{J}(\mathbb{Q}_2) = \langle \overline{\mathfrak{A}}_1, \overline{\mathfrak{A}}_2, \overline{\mathfrak{E}}_1, \overline{\mathfrak{E}}_2 \rangle$ and by the commutativity of (2.3)

$$\mathrm{im}\mu' \leq \langle \ker j_2, \overline{H}, [3, -3(1+\sqrt{2}), z], [-2, 3\sqrt{2}, 1] \rangle, \tag{3.12}$$

where $z \in \{i(a+bi), 3i(a+bi)\}$.

Combining (3.9),(3.10),(3.11) and (3.12) we conclude that $\mathrm{im}\mu' \leq \overline{H}$, that is $\mathrm{im}\mu' = \overline{H}$, and so $\mathrm{rank}(\mathcal{J}(\mathbb{Q})) = 0$. The following lemma summarises the results obtained from the complete 2-descent.

Lemma 3.3. *Let $\mathcal{C}$ denote the infinite family of curves over $\mathbb{Q}$ given by (3.7) and let $\mathcal{J}$ denote its Jacobian. Then*

$$\mathcal{J}(\mathbb{Q}) = \mathcal{J}(\mathbb{Q})_{tors} = \langle \{(\sqrt{2}, 0), (-\sqrt{2}, 0)\}, \{(0,0), (-1, 0)\} \rangle.$$

Since $\mathcal{J}$ and $\widehat{\mathcal{J}}$ are isogenous over $\mathbb{Q}$, $\mathrm{rank}(\mathcal{J}(\mathbb{Q})) = \mathrm{rank}(\widehat{\mathcal{J}}(\mathbb{Q}))$. Combining the lemmas 3.2 and 3.3 we obtain the following result:

Proposition 3.1. *Let $\widehat{\mathcal{C}}$ be the curve of genus 2 over $\mathbb{Q}$ given by*

$$\widehat{\mathcal{C}}: \quad y^2 = (-x^2+2x+1)\cdot 2qx\cdot(x^2+4x+2),$$

where q is a prime congruent to 13 modulo 24, and let $\widehat{\mathcal{J}}$ denote the Jacobian of $\widehat{\mathcal{C}}$. Furthermore, let $\mathcal{J}$ denote the Jacobian that is isogenous to $\widehat{\mathcal{J}}$ and let $\hat{\varphi}$ denote the Richelot isogeny $\hat{\varphi}: \widehat{\mathcal{J}} \to \mathcal{J}$.

A descent via Richelot isogeny bounds the rank of $\widehat{\mathcal{J}}(\mathbb{Q})$ by 2 while a complete 2-descent on $\mathcal{J}$ shows that the rank of $\widehat{\mathcal{J}}(\mathbb{Q})$ is in fact 0, and so Ш$(\widehat{\mathcal{J}}/\mathbb{Q})[\hat{\varphi}]$ is non-trivial. Hence, $\widehat{\mathcal{C}}$ is an infinite family of curves of genus 2 whose Jacobian has non-trivial Tate-Shafarevich group for descent via Richelot isogeny.

Remark. The Jacobian $\mathcal{J}$ (and hence $\widehat{\mathcal{J}}$) can be shown to be simple by a method described in [4], originating from [13].

Proposition 3.1 immediately implies that Ш$(\widehat{\mathcal{J}}/\mathbb{Q})[2]$ is non-trivial. In line with the idea of [2] this fact can, of course, also be proved by performing a 2-descent on $\widehat{\mathcal{J}}$, giving a rank bound of 2 on $\widehat{\mathcal{J}}(\mathbb{Q})$.

In view of the fact that Lemma 3.1 holds for the larger family of curves with $q \equiv 5 \pmod 8$ it is natural to suspect that Proposition 3.1 might also be correct for this larger family. Letting $q \equiv 5 \pmod 8$, one does, in fact, obtain a rank bound of 2 from the descent via isogeny but the 2-descent does not yield a rank bound of 0 on $\mathcal{J}(\mathbb{Q})$, and so no non-trivial members of the Tate-Shafarevich group are demonstrated in this case.

4. Family of surfaces violating the Hasse principle

We first note that (3.1) can be transformed via $(x,y) \mapsto (1/x, y/x^3)$ to

$$\dot{\mathcal{C}}: \quad y^2 = q(1-2x^2)(1+x)(1+x^2), \tag{4.1}$$

with Jacobian $\dot{\mathcal{J}}$. Recall ([4], p.19) that the coordinates $k_1 = 1, k_2 = x_1 + x_2, k_3 = x_1x_2, k_4 = (F_0(x_1,x_2) - 2y_1y_2)/(x_1-x_2)^2$, where

$$\begin{aligned} F_0(x_1,x_2) = {} & 2f_0 + f_1(x_1+x_2) + 2f_2(x_1x_2) + f_3(x_1x_2)(x_1+x_2) \\ & +2f_4(x_1x_2)^2 + f_5(x_1x_2)^2(x_1+x_2) + 2f_6(x_1x_2)^3, \end{aligned} \tag{4.2}$$

satisfy the equation of the Kummer surface. Specialising the Kummer surface equation (see [4], p.19) to our curve $\dot{\mathcal{C}}$, and for simplicity using the affine coordinates $u_2 = k_2/k_1, u_3 = k_3/k_1, u_4 = \frac{1}{q}k_4/k_1$ gives

$$\begin{gathered} u_4^2u_2^2 - 4u_4^2u_3 - 4u_4 - 2u_4u_2 + 4u_4u_3 + 2u_4u_2u_3 \\ +8u_4u_3^2 + 4u_4u_2u_3^2 + 4u_2 + 2u_3 + 8u_2^2 - 11u_3^2 \\ +8u_2^3 + 8u_2^2u_3 - 8u_2u_3^2 - 4u_3^3 + 4u_3^4 + 5 = 0. \end{gathered} \tag{4.3}$$

Note also, that if we let $u_7 = (y_1 - y_2)/(x_1 - x_2)$ then

$$u_4 = \frac{1}{q}u_7^2 + u_2 + 2u_2^2 - 2u_2u_3 + 2u_2^3 + 1. \tag{4.4}$$

Given $u_2, u_3, u_4, u_7 \in \mathbb{Q}$, one recovers $\{x_1, x_2\}$ as the roots of $x^2 - u_2 x + u_3$, and can obtain $u_7' = (x_2 y_1 - x_1 y_2)/(x_1 - x_2)$, from which $y_i = u_7 x_i - u_7'$ can be derived.

We know from the previous section that the homogeneous space corresponding to $[-2, -2]$ for $\mathrm{im}\mu^{\hat{\varphi}}$ violates the Hasse principle, as will then also be the case for $\dot{\mathcal{J}}$. A model for this homogeneous space, given by 72 equations in $\mathbb{P}^{15}$ (see [5]) would be rather unweildy, so we give here a more accessible associated surface. To say that $\{(x_1, y_1), (x_2, y_2)\} \in \dot{\mathcal{J}}(\mathbb{Q})$ maps to $[-2, -2]$ under $\mathrm{im}\mu^{\hat{\varphi}}$ is equivalent to the three additional equations: $(1 - 2x_1^2)(1 - 2x_2^2) = -2$, $(x_1 + 1)(x_2 + 1) = -2$, $(x_1^2 + 1)(x_2^2 + 1) = 1$, modulo squares. Any of these is dependent on the other two, so we need only take (for example) the second and third of these, which can be expressed as: $u_3 + u_2 + 1 = -2u_5^2$ and $u_3^2 + u_2^2 - 2u_3 + 1 = u_6^2$, for some $u_5, u_6 \in \mathbb{Q}$. What is nice here is that there is a simple resulting parametrisation of u_2, u_3, u_6 in terms of u_5 and a further parameter, as follows. We express the first equation as: $u_3 = -u_2 - 1 - 2u_5^2$ and substitute this into the second equation to give:

$$(u_2 + 2 + 2u_5^2)^2 + u_2^2 = u_6^2. \tag{4.5}$$

Using $u_2 = 0, u_6 = 2 + 2u_5^2$ as a basepoint, and letting $u_8 = (u_6 - 2 - 2u_5^2)/u_2$ (the slope from $(0, 2 + 2u_5^2)$ to (u_2, u_6)) we can express u_2, u_3 in terms of the parameters u_5, u_8, as

$$\begin{aligned} \bar{u}_2(u_5, u_8) &= \tfrac{4(u_5^2+1-u_8-u_8u_5^2)}{u_8^2-2}, \bar{u}_3(u_5, u_8) = \tfrac{4u_8-2+4u_8u_5^2-u_8^2-2u_5^2u_8^2}{u_8^2-2}, \\ \bar{u}_6(u_5, u_8) &= \tfrac{2(-u_8^2+2u_8+2u_8u_5^2-u_5^2u_8^2-2-2u_5^2}{u_8^2-2}. \end{aligned} \tag{4.6}$$

We finally obtain a model, given by a single equation in u_5, u_7, u_8 by substituting (4.4) into (4.3), to eliminate u_4, and then replacing u_2, u_3 with the parametrisations $\bar{u}_2(u_5, u_8), \bar{u}_3(u_5, u_8)$, respectively (and multiplying through by $(u_8^2 - 2)^8$). This family of affine surfaces has no affine $\mathbb{Q}$-rational point, for any $q \equiv 13 \pmod{24}$, since $[-2, -2]$ is not in the image of $\mu^{\hat{\varphi}}$. It is not immediately clear that there are affine points everywhere locally, since the local points on the homogeneous space might not correspond to affine points on our surface. However, it can easily be checked directly that there are points everywhere locally, by first checking small primes and primes of bad reduction, after which one can use Hensel's lemma, together with the Hasse-Weil bound on the genus 5 curves obtained by specialising u_8.

References

[1] A. Arnth-Jensen, E.V. Flynn, *Supplement to: Non-trivial* Ш *in the Jacobian of an infinite family of curves of genus 2.* Available at:
http://people.maths.ox.ac.uk/flynn/genus2/af/artlong.pdf

[2] N. Bruin, E.V. Flynn, *Exhibiting Sha[2] on Hyperelliptic Jacobians.* J. Number Theory **118** (2006), 266–291.

[3] N. Bruin, M. Bright, E.V. Flynn, A. Logan, *The Brauer-Manin Obstruction and Sha[2].* LMS J. Comput. Math. **10** (2007), 354–377.

[4] J. W. S. Cassels, E.V. Flynn, *Prolegomena to a Middlebrow Arithmetic of Curves of Genus 2.* LMS-LNS, Vol. 230, Cambridge University Press, Cambridge, 1996.

[5] E.V. Flynn, *Descent via isogeny in dimension 2.* Acta Arithm. **66** (1994), 23–43.

[6] E.V. Flynn, *On a Theorem of Coleman.* Manus. Math. **88** (1995), 447–456.

[7] E.V. Flynn, *The arithmetic of hyperelliptic curves.* Progress in Mathematics **143** (1996), 167–175.

[8] E.V. Flynn, J. Redmond, *Applications of covering techniques to families of curves.* J. Number Theory **101** (2003), 376–397.

[9] E.V. Flynn, B. Poonen, E. Schaefer, *Cycles of Quadratic Polynomials and Rational Points on a Genus 2 Curve.* Duke Math. J. **90** (1997), 435–463.

[10] B. Poonen, *An explicit algebraic family of genus-one curves violating the Hasse principle.* J. Théor. Nombres Bordeaux, **13** (2001), 263–274. 21st Journées Arithmétiques (Rome, 2001).

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

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

[13] M. Stoll, *Two simple 2-dimensional abelian varieties defined over $\mathbb{Q}$ with Mordell-Weil group of rank at least 19.* C. R. Acad. Sci. Paris **321**, Série I (1995), 1341–1345.

[14] M. Stoll, *Implementing 2-descent for Jacobians of hyperelliptic curves.* Acta Arith. **98** (2001), 245–277.

Anna Arnth-Jensen
Mathematical Institute, University of Oxford
24–29 St Giles', Oxford OX1 3LB
United Kingdom
E-mail: `arnth@maths.ox.ac.uk`

E. Victor Flynn
Mathematical Institute, University of Oxford
24–29 St Giles', Oxford OX1 3LB
United Kingdom
E-mail: `flynn@maths.ox.ac.uk`
URL: `http://people.maths.ox.ac.uk/flynn`