Journal de Théorie des Nombres
de Bordeaux 00 (XXXX), 000–000

Supplement to: 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 élḿents 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 associé 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 Shafarevich-Tate 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

This document is intended as a supplement to the article *Non-trivial Ш in the Jacobian of an infinite family of curves of genus 2*, which is under consideration by J. Théor. Nombres Bordeaux. It gives further details of the descent computations.

Let $\mathcal{C} : y^2 = F(x)$, where $F(x)$ is a polynomial of degree 5 or 6, denote a hyperelliptic 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

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

$S^{(2)}(\mathcal{J}/\mathbb{Q})$ can be determined by means of descent methods. The method of complete 2-descent [9] 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 [4], [6] 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 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. [1] contains an example of a pair of curves of genus 2, $\mathcal{C}$ and $\mathcal{D}$, over $\mathbb{Q}$ with 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 $Ш(\mathrm{Jac}(\mathcal{C})(\mathbb{Q}))[2]$. We will 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 [1] is only for a specific numerical example (there is also a family of examples in [1] using instead the Brauer-Manin obstruction on a related degree 4 del Pezzo surface, as is also the case in [2],[8]).

2. Descent methods

First, we give outline the method of complete 2-descent [3],[7],[9],[10]. We let $\mathcal{C} : y^2 = F(x)$ denote a hyperelliptic 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

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

given by

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

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 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

$$\begin{array}{ccc} \mathcal{J}(\mathbb{Q})/2\mathcal{J}(\mathbb{Q}) & \stackrel{\mu'}{\rightarrow} & M \\ \downarrow i_p & & \downarrow j_p \\ \mathcal{J}(\mathbb{Q}_p)/2\mathcal{J}(\mathbb{Q}_p) & \stackrel{\mu'_p}{\rightarrow} & M_p \end{array} \tag{2.3}$$

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 out 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 [3]

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

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 $\mathcal{J}(\mathbb{Q})/2\mathcal{J}(\mathbb{Q})$ – and thus $\mathrm{rank}(\mathcal{J}(\mathbb{Q}))$ – has been completely determined. Otherwise, we are either missing some generators for $\mathcal{J}(\mathbb{Q})/2\mathcal{J}(\mathbb{Q})$ or there are non-trivial members of $Ш(\mathcal{J}/\mathbb{Q})[2]$.

Next, we describe the method of descent via isogeny [3],[4],[6]. We let $\mathcal{C}: y^2 = F(x)$ denote a hyperelliptic 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 $\mathcal{C}$ 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 so-called Richelot isogenies, the kernel is exactly the group consisting of the 4 rational points of order 2 on the corresponding Jacobian. The exact sequence

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

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 $\mathcal{J}(\mathbb{Q})/\hat{\varphi}(\mathcal{J}(\mathbb{Q}))$ which can be done in a way similar to complete 2-descent: Letting $b_{ij} = \mathrm{resultant}(G_i, G_j)$, $b_i = b_{ij}b_{jk}$, and similarly, $\hat{b}_{ij} = \mathrm{resultant}(L_i, L_j)$ and $\hat{b}_i = \hat{b}_{ij}\hat{b}_{jk}$ for $i, j, k =$

$1,2,3$, we define $\mathcal{S}$ as the finite set of rational primes consisting of the prime 2 and the primes dividing $\Delta b_1 b_2 b_3 \hat{b}_1 \hat{b}_2 \hat{b}_3$. We can write $\mathcal{S} = \{p_1, \ldots, p_r\}$ and we define $\mathbb{Q}(\mathcal{S}) = \{\pm p_1^{e_1} \cdots p_r^{e_r} \,|\, e_1, \ldots, e_r = 0, 1\}$. 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, $\mathrm{im}\mu^{\varphi}$ 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

$$\begin{array}{ccc} \widehat{\mathcal{J}}(\mathbb{Q})/\varphi(\mathcal{J})(\mathbb{Q}) & \stackrel{\mu^{\varphi}}{\to} & \mathbb{Q}(\mathcal{S})^{\times 2} \\ \downarrow i_p & & \downarrow j_p \\ \widehat{\mathcal{J}}(\mathbb{Q}_p)/\varphi(\mathcal{J}(\mathbb{Q}_p) & \stackrel{\mu_p^{\varphi}}{\to} & (\mathbb{Q}_p^*/(\mathbb{Q}_p^*)^2)^{\times 2} \end{array} \tag{2.6}$$

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. 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 [5],[3]

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

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

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

which, by the commutativity of (2.6), contain $\mathrm{im}\mu^{\varphi}$ and $\mathrm{im}\mu^{\hat{\varphi}}$, 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 2 easier steps, involving only computations over $\mathbb{Q}$ instead of some larger number field.

3. The explicit family of curves

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

[1] We note that in (2.8) it is sufficient to intersect over the set of primes p satisfying $p|2\Delta b_1 b_2 b_3 \hat{b}_1 \hat{b}_2 \hat{b}_3$ or $p = \infty$.

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

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

4. The torsion subgroups

Let q be a prime congruent to 5 modulo 8. We let $\mathcal{C}$, $\widehat{\mathcal{C}}$, $\mathcal{J}$ and $\widehat{\mathcal{J}}$ be as in the previous section. We compute the torsion subgroups of $\mathcal{J}(\mathbb{Q})$ and $\widehat{\mathcal{J}}(\mathbb{Q})$, respectively:

Lemma 4.1. *Let $q \equiv 5 \pmod 8$. Then $\mathcal{J}(\mathbb{Q})_{tors} \cong \mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$ and $\widehat{\mathcal{J}}(\mathbb{Q})_{tors} \cong \mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$. More precisely,*

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

and

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

Proof. We have

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

and

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

so $\#\mathcal{J}(\mathbb{Q})_{\mathrm{tors}} \geq 4$ and $\#\widehat{\mathcal{J}}(\mathbb{Q})_{\mathrm{tors}} \geq 4$.

The only primes dividing $2\cdot\mathrm{disc}(F)$ are $2,3,q$. Hence, for $p \notin \{2,3,q\}$ we have

$$\sim: \quad \mathcal{J}(\mathbb{Q})_{\mathrm{tors}} \hookrightarrow \widetilde{\mathcal{J}}(\mathbb{F}_p)$$

and

$$\sim: \quad \widehat{\mathcal{J}}(\mathbb{Q})_{\mathrm{tors}} \hookrightarrow \widetilde{\widehat{\mathcal{J}}}(\mathbb{F}_p)$$

by [3]. We will apply these injective mappings in order to obtain bounds on the size of $\mathcal{J}(\mathbb{Q})_{\mathrm{tors}}$ and $\widehat{\mathcal{J}}(\mathbb{Q})_{\mathrm{tors}}$. In this connection we will make use of the fact [3] that

$$\#\widetilde{\mathcal{J}}(\mathbb{F}_p) = \frac{1}{2}\cdot\#\widetilde{\mathcal{C}}(\mathbb{F}_{p^2}) + \frac{1}{2}\cdot(\#\widetilde{\mathcal{C}}(\mathbb{F}_p))^2 - p \tag{4.1}$$

for any $p \nmid 2\cdot\mathrm{disc}(F)$ (a similar equation holds for $\widetilde{\mathcal{C}}$, of course).

First, we observe that, for a given $p \notin \{2,3,q\}$, $\#\widetilde{\mathcal{C}}(\mathbb{F}_p)$ is constant on the set consisting of those q that are squares in $\mathbb{F}_p$ and constant on the set consisting of those q that are non-squares in $\mathbb{F}_p$. Similarly, it is seen that $\#\widetilde{\widehat{\mathcal{C}}}(\mathbb{F}_p)$ only depends on whether q is a square or non-square in $\mathbb{F}_p$. Furthermore, the size of $\#\widetilde{\mathcal{C}}(\mathbb{F}_{p^2})$ (and $\#\widetilde{\widehat{\mathcal{C}}}(\mathbb{F}_{p^2})$) does not depend on the value of q at all, since q is always a square in $\mathbb{F}_{p^2}$.

Hence, in view of (4.1), we only need to consider two values of q – a square and a non-square in $\mathbb{F}_p$. In the following we only consider the curve

$\widetilde{\mathcal{C}}$, since the computations for the curve $\widetilde{\widetilde{\mathcal{C}}}$ are completely similar – in fact, the exact same values are obtained.

First, we let $p = 11$. 5 is a square in $\mathbb{F}_{11}$ and 13 is a non-square in $\mathbb{F}_{11}$. A finite computation gives that for $q = 5$ $\#\widetilde{\mathcal{C}}(\mathbb{F}_{11}) = 12$ and $\#\widetilde{\mathcal{C}}(\mathbb{F}_{11^2}) = 142$. Hence, $\widetilde{\mathcal{J}}(\mathbb{F}_{11}) = 132$ by (4.1). Another finite computation gives that for $q = 13$ $\#\widetilde{\mathcal{C}}(\mathbb{F}_{11}) = 12$ and $\#\widetilde{\mathcal{C}}(\mathbb{F}_{11^2}) = 142$. Hence, $\widetilde{\mathcal{J}}(\mathbb{F}_{11}) = 132$ by (4.1).

Next, we put $p = 17$. 5 is a non-square in $\mathbb{F}_{17}$ and 13 is a square in $\mathbb{F}_{17}$. Arguing in the exact same way as in the case of $p = 11$ we get that for $q = 5$ $\#\widetilde{\mathcal{C}}(\mathbb{F}_{17}) = 18$ and $\#\widetilde{\mathcal{C}}(\mathbb{F}_{17^2}) = 318$, and so $\widetilde{\mathcal{J}}(\mathbb{F}_{17}) = 304$. For $q = 13$ we also get $\#\widetilde{\mathcal{C}}(\mathbb{F}_{17}) = 18$ and $\#\widetilde{\mathcal{C}}(\mathbb{F}_{17^2}) = 318$, and so $\#\widetilde{\mathcal{J}}(\mathbb{F}_{17}) = 304$.

Hence, we have proven that for every $q \equiv 5 \pmod 8$

$$\widetilde{\mathcal{J}}(\mathbb{F}_{11}) = 132 \quad \text{and} \quad \widetilde{\mathcal{J}}(\mathbb{F}_{17}) = 304.$$

Since $\gcd(132, 304) = 4$ the map $\sim$ enables us to conclude that $\#\mathcal{J}(\mathbb{Q})_{\text{tors}} \leq 4$, and so $\#\mathcal{J}(\mathbb{Q})_{\text{tors}} = 4$. □

5. The descent via isogeny

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. Using the notation from the 2 we find that $\Delta b_1 b_2 b_3 \hat{b_1} \hat{b_2} \hat{b_3} = -2^{14} \cdot 3^{17} \cdot q^{23}$, 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

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

The generators of the torsion subgroups map as follows:

$$\begin{aligned}
\mathfrak{A}_1 &:= \{(\sqrt{2},0),(\sqrt{2},0)\} \overset{\mu^{\hat\varphi}}{\mapsto} [2,2],\\
\mathfrak{A}_2 &:= \{(0,0),(-1,0)\} \overset{\mu^{\hat\varphi}}{\mapsto} [2,1],\\
\widehat{\mathfrak{A}}_1 &:= \{(1-\sqrt{2},0),(1+\sqrt{2},0)\} \overset{\mu^{\varphi}}{\mapsto} [-1,1],\\
\widehat{\mathfrak{A}}_2 &:= \{(0,0),\infty\} \overset{\mu^{\varphi}}{\mapsto} [-1,2].
\end{aligned}$$

(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,

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

5.1. The case $p=\infty$. A set of representatives for $\mathbb{R}^*/(\mathbb{R}^*)^2$ is given by $\{\pm 1\}$, so

$$(\mathbb{R}^*/(\mathbb{R}^*)^2)^{\times 2} = \{\pm 1\}^{\times 2} = \langle [-1,1],[1,-1]\rangle$$

and

$$\ker j_\infty = \mathbb{Q}(\mathcal{S})^{\times 2} \cap ((\mathbb{R}^*)^2/(\mathbb{Q}^*)^2)^{\times 2} = \langle [2,1],[1,2],[3,1],[1,3],[q,1],[1,q]\rangle.$$

We have

$$\mathfrak{A}_1 \overset{\mu^{\hat\varphi}}{\mapsto} [2,2] \overset{j_\infty}{\mapsto} [1,1], \quad \mathfrak{A}_2 \overset{\mu^{\hat\varphi}}{\mapsto} [2,1] \overset{j_\infty}{\mapsto} [1,1]$$

and

$$\widehat{\mathfrak{A}}_1 \overset{\mu^{\varphi}}{\mapsto} [-1,1] \overset{j_\infty}{\mapsto} [-1,1], \quad \widehat{\mathfrak{A}}_2 \overset{\mu^{\varphi}}{\mapsto} [-1,2] \overset{j_\infty}{\mapsto} [-1,1].$$

Since $\#\widehat{\mathcal{J}}(\mathbb{R})/\varphi(\mathcal{J}(\mathbb{R}))\cdot \#\mathcal{J}(\mathbb{R})/\hat\varphi(\widehat{\mathcal{J}}(\mathbb{R})) = 2^2$ by (2.7), we are missing 1 generator.

We find $\mathfrak{B} := \{(2,\beta),(0,0)\} \in \mathcal{J}(\mathbb{R})$, where $\beta\in\mathbb{R}^*$ and $\beta^2 = 2^2\cdot 3\cdot 5\cdot q$. We see that

$$\begin{aligned}
\mathfrak{B} \overset{\mu^{\hat\varphi}_\infty}{\mapsto} &[G_1(2)G_1(0), G_2(2)G_2(0)]\\
&= [G_1(2)G_1(0), G_2(2)G_1(0)G_3(0)]\\
&= [2q\cdot(-2q), 6\cdot(-2q)]\\
&= [-1,-1] \in (\mathbb{R}^*/(\mathbb{R}^*)^2)^{\times 2},
\end{aligned}$$

where $G_1(x) = q(x^2-2)$, $G_2(x) = x^2+x$ and $G_3(x) = x^2+1$. Hence, $\mathcal{J}(\mathbb{R})/\hat\varphi(\widehat{\mathcal{J}}(\mathbb{R})) = \langle\mathfrak{B}\rangle$ and $\widehat{\mathcal{J}}(\mathbb{R})/\varphi(\mathcal{J}(\mathbb{R})) = \langle\widehat{\mathfrak{A}}_1\rangle$. The commutativity of (2.6) implies

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

and

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

5.2. The case p=3. Using $\{\pm 1, \pm 3\}$ as a set of representatives for $\mathbb{Q}_3^*/(\mathbb{Q}_3^*)^2$ we find $(\mathbb{Q}_3^*/(\mathbb{Q}_3^*)^2)^{\times 2} = \langle [-1,1],[1,-1],[3,1],[1,3]\rangle$. We determine the elements of $\mathbb{Q}(\mathcal{S})$ that are squares in $\mathbb{Q}_3^*$. We can immediately discard the members $\pm 3, \pm 3q, \pm 6, \pm 6q$. So we only need to consider $\pm 1, \pm 2, \pm q, \pm 2q$. Since $q \equiv 13 \pmod{24}$, we have $q \equiv 1 \pmod 3$. Therefore, $(\frac{q}{3}) = (\frac{1}{3}) = 1$. Furthermore, $(\frac{-1}{3}) = -1$ and $(\frac{2}{3}) = -1$. We conclude that $\mathbb{Q}(\mathcal{S}) \cap (\mathbb{Q}_3^*)^2 = \{1, -2, q, -2q\}$, and so

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

We have

$$\mathfrak{A}_1 \overset{\mu^{\hat\varphi}}{\mapsto} [2,2] \overset{j_3}{\mapsto} [-1,-1], \quad \mathfrak{A}_2 \overset{\mu^{\hat\varphi}}{\mapsto} [2,1] \overset{j_3}{\mapsto} [-1,1]$$

and

$$\widehat{\mathfrak{A}}_1 \overset{\mu^{\varphi}}{\mapsto} [-1,1] \overset{j_3}{\mapsto} [-1,1], \quad \widehat{\mathfrak{A}}_2 \overset{\mu^{\varphi}}{\mapsto} [-1,2] \overset{j_3}{\mapsto} [-1,-1],$$

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 $\mathfrak{A}_2$ 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 $\mathcal{J}(\mathbb{Q}_3)/\hat\varphi(\mathcal{J}(\mathbb{Q}_3)) = \langle \mathfrak{A}_1, \mathfrak{A}_2\rangle$ 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

$$\mathrm{im}\mu^{\hat\varphi} \le \langle \ker j_3, H\rangle = \langle [-2,1],[1,-2],[q,1],[1,q],[2,2],[2,1]\rangle \tag{5.1}$$

and

$$\mathrm{im}\mu^{\varphi} \le \langle \ker j_3, \widehat{H}\rangle = \langle [-2,1],[1,-2],[q,1],[1,q],[-1,1],[-1,2]\rangle. \tag{5.2}$$

5.3. The case $p = q$. Since $q \equiv 13 \pmod{24}$, we have $q \equiv -3 \pmod 8$. Hence, $(\frac{2}{q}) = -1$, and so a set of representatives for $\mathbb{Q}_q^*/(\mathbb{Q}_q^*)^2$ is given by $\{1, 2, q, 2q\}$, i.e. $(\mathbb{Q}_q^*/(\mathbb{Q}_q^*)^2)^{\times 2} = \langle [2,1],[1,2],[q,1],[1,q]\rangle$.

Next, we determine the set $\mathbb{Q}(\mathcal{S}) \cap (\mathbb{Q}_q^*)^2$. The members $\pm q, \pm 2q, \pm 3q, \pm 6q$ of $\mathbb{Q}(\mathcal{S})$ can immediately be discarded. So we only need to consider $\pm 1, \pm 2, \pm 3, \pm 6$. Since $q \equiv 13 \pmod{24}$, we have $q \equiv 1 \pmod 4$. Therefore, $(\frac{-1}{q}) = 1$, $(\frac{2}{q}) = -1$ and

$$\left(\frac{3}{q}\right) = \left(\frac{q}{3}\right) \cdot (-1)^{\frac{1}{2}(3-1)\cdot\frac{1}{2}(q-1)} = \left(\frac{1}{3}\right) \cdot (-1)^{\frac{1}{2}(q-1)} = 1.$$

We conclude that $\mathbb{Q}(\mathcal{S}) \cap (\mathbb{Q}_q^*)^2 = \{\pm 1, \pm 3\}$. Hence,

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

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 $\mu_q^{\hat\varphi}$. We claim that the following holds:

Lemma 5.1. *Let $\mathcal{C}$ and $\mathcal{J}$ be as in Section 3. For every $q \equiv 13 \pmod{24}$ there exists $(x, y) \in \mathcal{C}(\mathbb{Q}_q)$ 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 $\mu_q^{\hat{\varphi}}$.

In order to prove the lemma it is only necessary to prove that there exists $x \in \mathbb{Z}$ such that

- $x^2 - 2 =$ non-trivial quadratic residue mod q.[2]
- $x^2 + x =$ non-trivial quadratic non-residue mod q.
- $x^2 + 1 = q\cdot$(non-trivial quadratic non-residue mod q).

For if we have found an $x \in \mathbb{Z}$ satisfying these 3 conditions we have that

$$(-2)(x^2-2) = \text{non-trivial quadratic non-residue mod } q \tag{5.3}$$

and

$$(-2q)(x^2+x) = q \cdot (\text{non-trivial quadratic residue mod } q), \tag{5.4}$$

since -2 is a quadratic non-residue mod q. Furthermore,

$$\begin{aligned} q(x^2-2)(x^2+x)(x^2+1) &= q \cdot (\text{non-trivial quadratic residue mod } q) \\ &\quad \cdot (\text{non-trivial quadratic non-residue mod } q) \\ &\quad \cdot q \cdot (\text{non-trivial quadratic non-residue mod } q) \\ &= \text{non-trivial quadratic residue mod } q, \end{aligned}$$

so there exists $y \in \mathbb{Q}_q$ such that $y^2 = q(x^2-2)(x^2+x)(x^2+1)$. Hence, $(x,y) \in \mathcal{C}(\mathbb{Q}_q)$. Using (5.3) and (5.4) and the fact that 2 is a quadratic non-residue mod q we conclude that

$$\begin{aligned} \mu_q^{\hat{\varphi}}(\{(0,0),(x,y)\}) &= [(-2q)q(x^2-2),(-2q)(x^2+x)] \\ &= [-2(x^2-2),(-2q)(x^2+x)] \\ &= [\text{non-trivial quadratic non-residue mod } q, \\ &\qquad q \cdot (\text{non-trivial quadratic residue mod } q)] \\ &= [2,q] \in (\mathbb{Q}_q^*/(\mathbb{Q}_q^*)^2)^{\times 2}. \end{aligned}$$

Hence, we have proven that Lemma 5.1 is a consequence of the following lemma:

Lemma 5.2. *For every $q \equiv 13 \pmod{24}$ there exists $x \in \mathbb{Z}$ such that*
(A) $x^2 - 2 =$ non-trivial quadratic residue mod q.
(B) $x^2 + x =$ non-trivial quadratic non-residue mod q.
(C) $x^2 + 1 = q\cdot$(non-trivial quadratic non-residue mod q).

[2] By "non-trivial residue mod q" we just mean a residue $\not\equiv 0 \pmod{q}$.

Proof. Since $q \equiv 1 \pmod 4$, we have $\left(\frac{-1}{q}\right) = 1$ so there exists $x \in \mathbb{Z}$ such that $x^2 \equiv -1 \pmod q$, i.e.

$$x^2 + 1 \equiv 0 \pmod q. \tag{5.5}$$

Using (5.5) we see that

$$x^2 - 2 = (x^2 + 1) - 3 \equiv -3 \pmod q.$$

Since $(\frac{-3}{q}) = 1$ we conclude that x satisfies (A).

Using (5.5) we get that

$$\begin{aligned}(x^2 + x)((-x)^2 + (-x)) &= x^2(x^2 - 1) \\ &= x^2((x^2 + 1) - 2) \\ &\equiv x^2(-2) \pmod q,\end{aligned}$$

and so (using the fact that $(\frac{-2}{q}) = -1$, c.f. the beginning of this subsection)

$$\left(\frac{(x^2 + x)((-x)^2 + (-x))}{q}\right) = \left(\frac{x^2(-2)}{q}\right) = \left(\frac{x}{q}\right)^2 \cdot \left(\frac{-2}{q}\right) = -1,$$

i.e., exactly one of $x^2+x, (-x)^2+(-x)$ is a quadratic residue mod q. Letting r denote that of the two values $x, -x$ which added to its square gives a quadratic non-residue mod q, we see that r satisfies (B). Furthermore, r satisfies (5.5) and (A), since changing the sign of x does not change the value of $x^2 + 1$ or $x^2 - 2$. Hence, we have found $r \in \mathbb{Z}$ such that

- $r^2 - 2 =$ non-trivial quadratic residue mod q.
- $r^2 + r =$ non-trivial quadratic non-residue mod q.
- $r^2 + 1 = qv$ for some $v \in \mathbb{Z}$.

If v were a non-trivial quadratic non-residue mod q, then we would also have proven (C).

Next, we modify the value of r in such a way that the new value of r still satisfies (A) and (B) and, in addition to this, (C). We do this by using the fact that all representatives of the equivalence class of r mod q satisfy (A) and (B).

Let a denote an arbitrary non-trivial quadratic non-residue mod q. Define

$$k := (a - v)(2r)^{-1},$$

where $(2r)^{-1}$ denotes the multiplicative inverse of $2r$ mod q (this exists as $2r \not\equiv 0 \pmod q$). Next, put

$$s := r + kq.$$

We note that $s \equiv r \pmod{q}$, and so s satisfies (A) and (B). In addition to this, we have

$$\begin{aligned} s^2+1 &= (r+kq)^2+1 \\ &= k^2q^2+2rkq+(r^2+1) \\ &= k^2q^2+2rkq+qv \\ &= q(k^2q+2rk+v) \end{aligned}$$

and $k^2q+2rk+v \equiv v+2rk = v+(a-v) = a \pmod{q}$. Hence,

$$s^2+1 = q \cdot (\text{non-trivial quadratic non-residue mod } q),$$

and so s satisfies (C).

Thus we have found $s \in \mathbb{Z}$ satisfying (A), (B) and (C). □

Letting $\mathfrak{D} := \{(0,0),(x,y)\}$ we have by Lemma 5.1 that $\mathcal{J}(\mathbb{Q}_q)/\hat{\varphi}(\widehat{\mathcal{J}}(\mathbb{Q}_q)) = \langle \mathfrak{A}_1, \mathfrak{A}_2, \mathfrak{D}\rangle$ 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

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

5.4. The case $p = 2$. A set of representatives for $\mathbb{Q}_2^*/(\mathbb{Q}_2^*)^2$ is given by $\{\pm1,\pm2,\pm3,\pm6\}$, and so $(\mathbb{Q}_2^*/(\mathbb{Q}_2^*)^2)^{\times 2} = \{\pm1,\pm2,\pm3,\pm6\}^{\times 2}$. Since $q \equiv 13 \pmod{24}$, we have $-3q \equiv 1 \pmod 8$, and so $\mathbb{Q}(\mathcal{S}) \cap (\mathbb{Q}_2^*)^2 = \{1,-3q\}$. Hence,

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

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 $\mathfrak{E}_1 := \{(5,\eta_1),(0,0)\} \in \mathcal{J}(\mathbb{Q}_2)$, 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 $\mathfrak{E}_1 \mapsto [2,-3] \in (\mathbb{Q}_2^*/(\mathbb{Q}_2^*)^2)^{\times 2}$ by $\mu_2^{\hat{\varphi}}$. Next, we find $\mathfrak{E}_2 := \{(\frac{1}{4},\eta_2),(0,0)\} \in \mathcal{J}(\mathbb{Q}_2)$, 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 $-5 \cdot 17 \cdot 31 \cdot 1 \equiv 1 \pmod 8$, since $q \equiv 5 \pmod 8$. We have $\mathfrak{E}_2 \mapsto [-2,-2] \in (\mathbb{Q}_2^*/(\mathbb{Q}_2^*)^2)^{\times 2}$ by $\mu_2^{\hat{\varphi}}$.

Hence, $\mathcal{J}(\mathbb{Q}_2)/\hat{\varphi}(\widehat{\mathcal{J}}(\mathbb{Q}_2)) = \langle \mathfrak{A}_1, \mathfrak{A}_2, \mathfrak{E}_1, \mathfrak{E}_2\rangle$ and $\widehat{\mathcal{J}}(\mathbb{Q}_2)/\varphi(\mathcal{J}(\mathbb{Q}_2)) = \langle \widehat{\mathfrak{A}}_2, \widehat{\mathfrak{A}}_2\rangle$. (2.6) tells us that

(5.6)

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

and

$$\mathrm{im}\mu^{\varphi} \leq \langle \ker j_2, \widehat{H}\rangle = \langle [-3q,1],[1,-3q],[-1,1],[-1,2]. \tag{5.7}$$

5.5. The rank bound. Using (5.1) and (5.6) we get $\mathrm{im}\mu^{\hat{\varphi}} \leq \langle [-2,-2],[1,q],[2,2],[2,1]\rangle$. Taking the information at ∞ and q into account does not improve this bound on $\mathrm{im}\mu^{\hat{\varphi}}$. Thus, $H \leq \mathrm{im}\mu^{\hat{\varphi}} \leq \langle H,[-2,-2],[1,q]\rangle$, and so $\#\mathcal{J}(\mathbb{Q})/\hat{\varphi}(\widehat{\mathcal{J}}(\mathbb{Q})) \in \{4,8,16\}$. Similarly, from (5.2) and (5.7) we get $\mathrm{im}\mu^{\varphi} \leq \widehat{H}$, and so $\mathrm{im}\mu^{\varphi} = H$, i.e. $\#\widehat{\mathcal{J}}(\mathbb{Q})/\varphi(\mathcal{J}(\mathbb{Q})) = 4$. 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 proven the following lemma:

Lemma 5.3. *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*

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

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.

A search for generators for $\mathcal{J}(\mathbb{Q})$ of infinite order does not yield any results, and so we suspect that $\mathrm{rank}(\mathcal{J}(\mathbb{Q}))$ is actually 0. In the next section we prove that this is in fact the case by performing a complete 2-descent on $\mathcal{J}(\mathbb{Q})$.

6. The complete 2-descent

Again, we consider the family of curves of genus 2 given by

$$y^2 = q(x^2-2)(x^2+x)(x^2+1), \tag{6.1}$$

where q is a prime congruent to 13 modulo 24. We observe that the polynomial $q(x^2-2)(x^2+x)(x^2+1)$ has a root in $\mathbb{Q}$, and so we can write the equation of the curve 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 (6.1) is seen to be birationally equivalent to the family of curves given by

$$y^2 = W(x) = (x-2q)(x^2-2q^2)(x^2+2^2q^2), \quad q \equiv 13 \pmod{24}. \tag{6.2}$$

By a slight abuse of notation we denote this curve by $\mathcal{C}$ and its Jacobian by $\mathcal{J}$. By Lemma 4.1 $\mathcal{J}(\mathbb{Q})_{tors} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, 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 Section 2 –

(6.3)

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

for fixed positive integers a and b satisfying $a^2+b^2=q$, $2|a$ and $2\nmid b$.[3] The generators for the torsion subgroup map as follows:[4]

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

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 $\overline{H}=\mathrm{im}\mu'$.

Finally, we note that by [3] we have

(6.4)

$$\begin{aligned}\mathcal{J}(\overline{\mathbb{Q}})[2]=\{&\mathfrak{O},\{(2q,0),\infty\},\{(q\sqrt{2},0),(-q\sqrt{2},0)\},\{(2qi,0),(-2qi,0)\},\\&\{(q\sqrt{2},0),\infty\},\{(-q\sqrt{2},0),\infty\},\{(2qi,0),\infty\},\{(-2qi,0),\infty\},\\&\{(2q,0),(q\sqrt{2},0)\},\{(2q,0),(-q\sqrt{2},0)\},\{(2q,0),(2qi,0)\},\\&\{(2q,0),(-2qi,0)\},\{(q\sqrt{2},0),(2qi,0)\},\{(q\sqrt{2},0),(-2qi,0)\},\\&\{(-q\sqrt{2},0),(2qi,0)\},\{(-q\sqrt{2}),(-2qi,0)\}\}.\end{aligned}$$

6.1. The case $p=\infty$. We have

$$\begin{aligned}M_\infty&=\mathbb{Q}_\infty^*/(\mathbb{Q}_\infty^*)^2\times\mathbb{Q}_\infty(\sqrt{2})^*/(\mathbb{Q}_\infty(\sqrt{2})^*)^2\times\mathbb{Q}_\infty(i)^*/(\mathbb{Q}_\infty(i)^*)^2\\&\cong\mathbb{R}^*/(\mathbb{R}^*)^2\times(\mathbb{R}^*/(\mathbb{R}^*)^2)^{\times 2}\times\mathbb{C}^*/(\mathbb{C}^*)^2,\end{aligned}$$

[3] The existence of $a,b\in\mathbb{Z}$ such that $a^2+b^2=q$ is a consequence of the fact that the prime q is congruent to 1 modulo 4. We may assume that $a,b\in\mathbb{Z}^+$ since changing one or both signs of a and b does not change the value of a^2+b^2. Furthermore, we see that exactly one of a,b is divisible by 2. For $q\equiv 1\pmod 4$ implies $a^2+b^2\equiv 1\pmod 4$, and so ($a^2\equiv 0\pmod 4$ and $b^2\equiv 1\pmod 4$) or ($a^2\equiv 1\pmod 4$ and $b^2\equiv 0\pmod 4$), i.e. the parities of a and b are distinct. We may assume that $2|a$ and $2\nmid b$ since interchanging a and b does not affect the value of q nor does it collide with our first assumption.

[4] We note that we may use the fact that the product of the 3 components of the map μ' is a square (by the defining equation of $\mathcal{C}$) to compute μ' at those $\{(x_1,y_1),(x_2,y_2)\}$ for which one of the components is zero.

since we have 2 embeddings of $\mathbb{Q}(\sqrt{2})^*$ into $\mathbb{R}^*$. These are given by

$$x+y\sqrt{2}\mapsto x+y\sqrt{2} \quad \text{and} \quad x+y\sqrt{2}\mapsto x-y\sqrt{2},$$

respectively. Sets of representatives for $\mathbb{R}^*/(\mathbb{R}^*)^2$ and $\mathbb{C}^*/(\mathbb{C}^*)^2$ are given by $\{\pm 1\}$ and $\{1\}$, respectively. Hence,

$$M_\infty \cong \{\pm 1\}\times\{\pm 1\}^{\times 2}\times\{1\} = \langle [-1,[1,1],1],[1,[-1,1],1],[1,[1,-1],1]\rangle.$$

We also have

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

and so $j_\infty\circ\mu'(\overline{\mathfrak{A}}_1)=[1,[1,1],1]$ and $j_\infty\circ\mu'(\overline{\mathfrak{A}}_2)=[1,[1,1],1]$. From (6.4) we immediately see that

$$\mathcal{J}(\mathbb{R})[2] = \{\mathfrak{O},\{(2q,0),\infty\},\{(q\sqrt{2},0),(-q\sqrt{2},0)\},\{(2qi,0),(-2qi,0)\},$$
$$\{(q\sqrt{2},0),\infty\},\{(-q\sqrt{2},0),\infty\},\{(2q,0),(q\sqrt{2},0)\},\{(2q,0),(-q\sqrt{2},0)\}\},$$

and so $\#\mathcal{J}(\mathbb{R})[2]=8$. (2.4) now implies that $\#\mathcal{J}(\mathbb{R})/2\mathcal{J}(\mathbb{R})=2$, so we are missing 1 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

$$\mathrm{im}\mu' \le \langle \ker j_\infty, \overline{H}, [-1,\sqrt{2},1]\rangle. \tag{6.5}$$

6.2. The case $p=3$. We have

$$M_3 = \mathbb{Q}_3^*/(\mathbb{Q}_3^*)^2\times\mathbb{Q}_3(\sqrt{2})^*/(\mathbb{Q}_3(\sqrt{2})^*)^2\times\mathbb{Q}_3(i)^*/(\mathbb{Q}_3(i)^*)^2.$$

Lemma 6.1. *A set of representatives for $\mathbb{Q}_3^*/(\mathbb{Q}_3^*)^2$ is given by $\{\pm1,\pm3\}$, a set of representatives for $\mathbb{Q}_3(\sqrt{2})^*/(\mathbb{Q}_3(\sqrt{2})^*)^2$ is given by $\{1,1+\sqrt{2},3,3(1+\sqrt{2})\}$ and a set of representatives for $\mathbb{Q}_3(i)^*/(\mathbb{Q}_3(i)^*)^2$ is given by $\{1,1+i,3,3(1+i)\}$.*

The first claim of the theorem is clear. The proofs of the second and third claims are similar as they both rely on the fact that 3 is prime in $\mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}(i)$, respectively. Therefore, we will restrict ourselves to proving the second claim.

Lemma 6.2. *Let $c\in\mathbb{Q}_3(\sqrt{2})^*$. Then c is a square and a unit in $\mathbb{Q}_3(\sqrt{2})^*$ if and only if*

$$c\equiv 1,\sqrt{2},2,2\sqrt{2} \pmod 3.$$

Proof. Since 3 is prime in $\mathbb{Q}(\sqrt{2})$ the residue class field of $\mathbb{Q}_3(\sqrt{2})$ equals $\mathbb{F}_3(\sqrt{2})$. It is easily verified that $(\mathbb{F}_3(\sqrt{2})^*)^2=\{1,\sqrt{2},2,2\sqrt{2}\}$.

First, assume that $c\in(\mathbb{Q}_3(\sqrt{2})^*)^2$ and that $|c|_3=1$. Then

$$c=\sum_{n=0}^{\infty}c_n\cdot 3^n, \quad c_0\neq 0,\ c_n\in\mathbb{F}_3(\sqrt{2}).$$

As $c \in (\mathbb{Q}_3(\sqrt{2})^*)^2$ there exists $d \in \mathbb{Q}_3(\sqrt{2})^*$ such that $c = d^2$. Hence,

$$1 = |c|_3 = |d^2|_3 = |d|_3^2,$$

i.e. $|d|_3 = 1$. So d can be written in the form

$$d = \sum_{n=0}^{\infty} d_n \cdot 3^n, \quad d_0 \neq 0,\ d_n \in \mathbb{F}_3(\sqrt{2}).$$

Now,

$$\sum_{n=0}^{\infty} c_n \cdot 3^n = \left(\sum_{n=0}^{\infty} d_n \cdot 3^n \right)^2$$

implies

$$c_0 \equiv d_0^2 \pmod 3,$$

and so $c_0 \equiv 1, \sqrt{2}, 2, 2\sqrt{2} \pmod 3$, i.e.

$$c \equiv 1, \sqrt{2}, 2, 2\sqrt{2} \pmod 3.$$

Next, let $c \in \mathbb{Q}_3(\sqrt{2})^*$ and assume that $c \equiv 1, \sqrt{2}, 2, 2\sqrt{2} \pmod 3$. Since

$$c = \sum_{n=N}^{\infty} c_n \cdot 3^n,$$

where $N \in \mathbb{Z}$, $c_N \neq 0$ and $c_n \in \mathbb{F}_3(\sqrt{2})$ this implies $N = 0$. So, $|c|_3 = 1$ and $c_0 \in \{1, \sqrt{2}, 2, 2\sqrt{2}\}$. In particular, $c_0 \in (\mathbb{F}_3(\sqrt{2})^*)^2$. Hence, there exists $d_0 \in \mathbb{F}_3(\sqrt{2})^*$ such that $c_0 = d_0^2$.

Now, define $f(x) := x^2 - c$. As $c \in \mathbb{Z}_3(\sqrt{2})$ we have $f(x) \in \mathbb{Z}_3(\sqrt{2})[x]$.

$$\begin{aligned} |f(d_0)|_3 &= |d_0^2 - c|_3 \\ &= |d_0^2 - (c_0 + c_1 \cdot 3 + c_2 \cdot 3^2 + \ldots)|_3 \\ &= |c_1 \cdot 3 + c_2 \cdot 3^2 + \ldots|_3 \\ &= 3^{-1} \\ &< 1. \end{aligned}$$

Since $f'(x) = 2x$,

$$|f'(d_0)|_3 = |2d_0|_3 = |2|_3 |d_0|_3 = 1.$$

Hence,

$$|f(d_0)|_3 < 1 = |f'(d_0)|_3^2.$$

By Hensel's Lemma there exists a unique $d \in \mathbb{Z}_3(\sqrt{2})$ such that $f(d) = 0$, i.e. $c = d^2$. So, c is a square in $\mathbb{Q}_3(\sqrt{2})^*$. □

Lemma 6.3. *Let $w \in \mathbb{Q}_3(\sqrt{2})^*/(\mathbb{Q}_3(\sqrt{2})^*)^2$ and assume that $|w|_3 = 1$. Then*

$$w = 1 \quad \textit{or} \quad w = 1 + \sqrt{2}.$$

Proof. Let $w \in \mathbb{Q}_3(\sqrt{2})^*/(\mathbb{Q}_3(\sqrt{2})^*)^2$. Assume that $|w|_3 = 1$. If w is a square in $\mathbb{Q}_3(\sqrt{2})^*$ then $w = 1$ in $\mathbb{Q}_3(\sqrt{2})^*/(\mathbb{Q}_3(\sqrt{2})^*)^2$.

Next, we consider the case that w is a non-square in $\mathbb{Q}_3(\sqrt{2})^*$. Since w is a unit and a non-square Lemma 6.2 implies that $w \not\equiv 1, \sqrt{2}, 2, 2\sqrt{2} \pmod 3$. Hence, $w \equiv 1+\sqrt{2}, 1+2\sqrt{2}, 2+\sqrt{2}, 2+2\sqrt{2} \pmod 3$, i.e. $w \equiv 1+\sqrt{2}, 2\sqrt{2}(1+\sqrt{2}), \sqrt{2}(1+\sqrt{2}), 2(1+\sqrt{2}) \pmod 3$, and so $w = 1+\sqrt{2}$ modulo $(\mathbb{Q}_3(\sqrt{2})^*)^2$. □

Lemma 6.4. *Let $w \in \mathbb{Q}_3(\sqrt{2})^*/(\mathbb{Q}_3(\sqrt{2})^*)^2$ and define $r \in \mathbb{Z}$ by $|w|_3 = 3^r$. Then the following hold:*

- *If r is even, then $w = 1$ or $w = 1+\sqrt{2}$.*
- *If r is odd, then $w = 3$ or $w = 3(1+\sqrt{2})$.*

Proof. First, assume that r is even. Then $r/2 \in \mathbb{Z}$ and $|w|_3 = 3^r = (3^{r/2})^2$. Since $w = (3^{r/2})^2 w$ modulo $(\mathbb{Q}_3(\sqrt{2})^*)^2$ and $|(3^{r/2})^2 w|_3 = |3^r|_3 \cdot |w|_3 = 3^{-r} \cdot 3^r = 1$ we conclude that w is a unit in $\mathbb{Q}_3(\sqrt{2})$. Then Lemma 6.3 implies that $w = 1$ or $w = 1+\sqrt{2}$ modulo $(\mathbb{Q}_3(\sqrt{2})^*)^2$.

Next, assume that r is odd. Then $\frac{r-1}{2} \in \mathbb{Z}$. Since $\frac{w}{3} = (3^{(r-1)/2})^2 \frac{w}{3}$ modulo $(\mathbb{Q}_3(\sqrt{2})^*)^2$ and $|(3^{(r-1)/2})^2 \frac{w}{3}|_3 = |3^{r-2}|_3 \cdot |w|_3 = 3^{-(r-2)} \cdot 3^r = 3^2$, the first part of Lemma 6.4 implies $\frac{w}{3} = 1$ or $\frac{w}{3} = 1+\sqrt{2}$, i.e. $w = 3$ or $w = 3(1+\sqrt{2})$. □

Lemma 6.1 is an immediate consequence of Lemma 6.4.

It follows from Lemma 6.1 that

$$\begin{aligned} M_3 &= \{\pm 1, \pm 3\} \times \{1, 1+\sqrt{2}, 3, 3(1+\sqrt{2})\} \times \{1, 1+i, 3, 3(1+i)\} \\ &= \langle [-1,1,1], [3,1,1], [1,1+\sqrt{2},1], [1,3,1], [1,1,1+i], [1,1,3] \rangle. \end{aligned}$$

Lemma 6.5. *Using the notation of the commutative diagram 2.3 we have*

$$\begin{aligned} \ker j_3 &= M \cap ((\mathbb{Q}_3^*)^2/(\mathbb{Q}^*)^2 \times (\mathbb{Q}_3(\sqrt{2})^*)^2/(\mathbb{Q}(\sqrt{2})^*)^2 \times (\mathbb{Q}_3(i)^*)^2/(\mathbb{Q}(i)^*)^2) \\ &= \langle [-2,1,1], [q,1,1], [1,-1,1], [1,\sqrt{2},1], [1,q,1], [1,1,i], \\ &\qquad [1,1,a+bi], [1,1,a-bi] \rangle. \end{aligned}$$

Proof. From Section 5 we know that $1, -2, q, -2q$ are the only elements of $\langle -1, 2, 3, q \rangle \leq \mathbb{Q}^*$ that are squares in $\mathbb{Q}_3^*$.

Next, we determine which of the elements in $\langle -1, 1+\sqrt{2}, \sqrt{2}, 3, q \rangle$ that are squares in $\mathbb{Q}_3(\sqrt{2})^*$. Since all of the generators except 3 have valuation equal to 1 and $|3|_3 = 3^{-1}$, 3 is a non-square in $\mathbb{Q}_3(\sqrt{2})^*$ and we only need to consider $\langle -1, 1+\sqrt{2}, \sqrt{2}, q \rangle$. We have previously seen that $(\mathbb{F}_3(\sqrt{2})^*)^2 = \{1, \sqrt{2}, 2, 2\sqrt{2}\}$. We claim that $1+\sqrt{2} \notin (\mathbb{Q}_3(\sqrt{2})^*)^2$. For if $1+\sqrt{2} \in (\mathbb{Q}_3(\sqrt{2})^*)^2$ there would exist an $a_0 \in \mathbb{F}_3(\sqrt{2})^*$ such that $1+\sqrt{2} \equiv a_0^2 \pmod 3$, i.e. $1+\sqrt{2}$ is a square in $\mathbb{F}_3(\sqrt{2})^*$. Contradiction. On the other

hand, we claim that $-1 \in (\mathbb{Q}_3(\sqrt{2})^*)^2$. We have $-1 = 2$ in $\mathbb{F}_3(\sqrt{2})^*$, so $-1 \in (\mathbb{F}_3(\sqrt{2})^*)^2$. Define $f(x) = x^2 + 1$. Then $f'(x) = 2x$ and

$$|f(\sqrt{2})|_3 = |\sqrt{2}^2 + 1|_3 = |3|_3 = 3^{-1}$$

and

$$|f(\sqrt{2})|_3^2 = |2\sqrt{2}|_3^2 = 1.$$

Hensel's Lemma then gives the existence of a $c \in \mathbb{Q}_3(\sqrt{2})^*$ such that $f(c) = 0$. I.e. -1 is a square in $\mathbb{Q}_3(\sqrt{2})^*$. In the same way it is proved that $\sqrt{2} \in (\mathbb{Q}_3(\sqrt{2})^*)^2$. Furthermore, we note that $q \in (\mathbb{Q}_3(\sqrt{2})^*)^2$ since $q \in (\mathbb{Q}_3^*)^2$. Thus, $\langle -1, \sqrt{2}, q\rangle$ is the subgroup consisting of those elements in $\langle -1, 1+\sqrt{2}, \sqrt{2}, 3, q\rangle$ that are squares in $\mathbb{Q}_3(\sqrt{2})^*$.

Finally, we determine the subgroup of $\langle i, 1+i, 3, a+bi, a-bi\rangle$ consisting of those elements that are squares in $\mathbb{Q}_3(i)^*$. This is quite similar to the previous case. We have $(\mathbb{F}_3(i)^*)^2 = \{1, 2, i, 2i\}$. Again, we note that no element having 3 as a one of its generators can be a square in $\mathbb{Q}_3(i)^*$. Thus, we only need to consider $\langle i, 1+i, a+bi, a-bi\rangle$. By applying the methods used in the previous case it is easily seen that $1+i \notin (\mathbb{Q}_3(i)^*)^2$ and $i \in (\mathbb{Q}_3(i)^*)^2$. Also, we note that $q \in (\mathbb{Q}_3(i)^*)^2$ since $q \in (\mathbb{Q}_3^*)^2$. It only remains to be checked whether $a+bi$ and $a-bi$ are squares in $\mathbb{Q}_3(i)^*$.

We claim that $a+bi, a-bi \in (\mathbb{Q}_3(i)^*)^2$. Since we already know that $(a+bi)(a-bi) = q \in (\mathbb{Q}_3(i)^*)^2$ it is only necessary to prove that $a+bi \in (\mathbb{Q}_3(i)^*)^2$. First, we prove that exactly one of $a, b \in \mathbb{Z}^+$ is divisible by 3. Clearly, a and b cannot both be divisible by 3 since this would imply that $q = a^2 + b^2$ is divisible by 3, contradicting the fact that q is prime. On the other hand, if none of a, b are divisible by 3 this means that $a, b \equiv 1, 2 \pmod 3$ and so $q = a^2 + b^2 \equiv 2 \pmod 3$, contradicting the fact that $q \equiv 1 \pmod 3$ (as $q \equiv 13 \pmod{24}$). Thus, exactly one of a, b is divisible by 3. If $3|a$ and $3 \nmid b$ we have $a + bi = bi \in \{i, 2i\}$ in $\mathbb{F}_3(i)$. If $3 \nmid a$ and $3|b$ we have $a + bi = a \in \{1, 2\}$ in $\mathbb{F}_3(i)$. Hence, in both cases we conclude that $a + bi \in (\mathbb{F}_3(i)^*)^2$. We can now use Hensel's Lemma for showing that $a + bi \in (\mathbb{Q}_3(i)^*)^2$. Define $f(x) = x^2 - (a + bi)$. Then $f'(x) = 2x$. Since $a + bi \in (\mathbb{F}_3(i)^*)^2$ there exists $c \in \mathbb{F}_3(i)^*$ such that $a + bi \equiv c^2 \pmod 3$.

$$|f(c)|_3 = |c^2 - (a + bi)|_3 \leq 3^{-1}$$

and

$$|f'(c)|_3^2 = |2c|_3^2 = |c|_3^2 = 1$$

as $|c|_3 = 1$. Then Hensel's Lemma gives the existence of a $d \in \mathbb{Q}_3(i)$ such that $f(d) = 0$. I.e. $a + bi \in (\mathbb{Q}_3(i)^*)^2$. We conclude that $\langle i, a + bi, a - bi\rangle$ is the subgroup of $\langle i, 1 + i, 3, a + bi, a - bi\rangle$ consisting of the elements that are squares in $\mathbb{Q}_3(i)^*$. □

In view of Lemma 6.5, $j_3 \circ \mu'(\overline{\mathfrak{A}}_1) = [1, 1+\sqrt{2}, 1+i]$ 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) and (6.4), the known members of $\mathcal{J}(\mathbb{Q})/2\mathcal{J}(\mathbb{Q})$ generate $\mathcal{J}(\mathbb{Q}_3)/2\mathcal{J}(\mathbb{Q}_3)$, i.e. $\mathcal{J}(\mathbb{Q}_3)/2\mathcal{J}(\mathbb{Q}_3) = \langle \overline{\mathfrak{A}}_1, \overline{\mathfrak{A}}_2 \rangle$. From (2.3) we get that

$$\mathrm{im}\mu' \leq \langle \ker j_3, \overline{H} \rangle. \tag{6.6}$$

6.3. The case $p = q$. We have

$$M_q = \mathbb{Q}_q^*/(\mathbb{Q}_q^*)^2 \times (\mathbb{Q}(\sqrt{2}))_q^*/((\mathbb{Q}(\sqrt{2}))_q^*)^2 \times (\mathbb{Q}(i))_q^*/((\mathbb{Q}(i))_q^*)^2. \tag{6.7}$$

We wish to determine a set of representatives for each of the 3 groups in the multiple appearing on the right-hand side of (6.7). By Section 5 a set of representatives for $\mathbb{Q}_q^*/(\mathbb{Q}_q^*)^2$ is given by $\{1, 2, q, 2q\}$.

Next, we consider the group $(\mathbb{Q}(\sqrt{2}))_q^*/((\mathbb{Q}(\sqrt{2}))_q^*)^2$. First, we note that $(\mathbb{Q}(\sqrt{2}))_q$ is isomorphic to $\mathbb{Q}_q(\sqrt{2})$ as q is prime in $\mathbb{Q}(\sqrt{2})$. So instead of the group $(\mathbb{Q}(\sqrt{2}))_q^*/((\mathbb{Q}(\sqrt{2}))_q^*)^2$ we will be working with $\mathbb{Q}_q(\sqrt{2})^*/(\mathbb{Q}_q(\sqrt{2})^*)^2$.

The residue class field of $\mathbb{Q}_q(\sqrt{2})$ equals $\mathbb{F}_q(\sqrt{2})$.

Lemma 6.6. *$\sqrt{2}$ is a non-square in $\mathbb{F}_q(\sqrt{2})^*$.*

Proof. Assume that $\sqrt{2} \in (\mathbb{F}_q(\sqrt{2})^*)^2$. Then there exist $c, d \in \mathbb{F}_q$ such that $\sqrt{2} = (c + d\sqrt{2})^2$, i.e. $\sqrt{2} = c^2 + 2d^2 + 2cd\sqrt{2}$, and so $c^2 + 2d^2 = 0$ and $2cd = 1$. From $2cd = 1$ we get $d \neq 0$. Hence,

$$c^2 + 2d^2 = 0 \Rightarrow c^2 = -2d^2 \Rightarrow \left(\frac{c}{d}\right)^2 = -2.$$

But this contradicts the fact that -2 is not a quadratic residue modulo q. □

Lemma 6.7.

$$\mathbb{F}_q(\sqrt{2})^*/(\mathbb{F}_q(\sqrt{2})^*)^2 = \{1, \sqrt{2}\}.$$

Proof. Since $\mathbb{F}_q(\sqrt{2})$ is a finite field with characteristic $\neq 2$, the map $x \mapsto x^2$ is 2-1 on $\mathbb{F}_q(\sqrt{2})^*$. Hence, $\#(\mathbb{F}_q(\sqrt{2})^*)^2 = \frac{1}{2} \cdot \#\mathbb{F}_q(\sqrt{2})^*$, and so $\mathbb{F}_q(\sqrt{2})^*/(\mathbb{F}_q(\sqrt{2})^*)^2$ consists of precisely 2 elements, and these can be represented by 1 and an arbitrarily chosen non-square in $\mathbb{F}_q(\sqrt{2})^*$. Therefore, in view of Lemma 6.6, we conclude that $\mathbb{F}_q(\sqrt{2})^*/(\mathbb{F}_q(\sqrt{2})^*)^2 = \{1, \sqrt{2}\}$. □

Since $[\mathbb{Q}_q(\sqrt{2}) : \mathbb{Q}_q] = 2$ and since q is unramified in $\mathbb{Q}(\sqrt{2})$, the ramification index equals 1. Hence, there is no non-trivial extension of the valuation group. Therefore, denoting the extension of $|\cdot|_q$ to $\mathbb{Q}_q(\sqrt{2})$ by $|\cdot|_q$ also, we conclude that $|x|_q \in \{q^s | s \in \mathbb{Z}\}$ for all $x \in \mathbb{Q}_q(\sqrt{2})$.

It is clear that $1, \sqrt{2}, q, q\sqrt{2}$ are distinct elements of $\mathbb{Q}_q(\sqrt{2})^*/(\mathbb{Q}_q(\sqrt{2}))^2$. We now prove a couple of lemmas concerning these 4 elements.

Lemma 6.8. *Let $c \in \mathbb{Q}_q(\sqrt{2})^*/(\mathbb{Q}_q(\sqrt{2})^*)^2$ and assume that $|c|_q = 1$. Then the following hold:*

- $c = 1$ *in* $\mathbb{Q}_q(\sqrt{2})^*/(\mathbb{Q}_q(\sqrt{2})^*)^2 \Leftrightarrow c \equiv$ (*square in* $\mathbb{F}_q(\sqrt{2})^*$) (mod q).
- $c = \sqrt{2}$ *in* $\mathbb{Q}_q(\sqrt{2})^*/(\mathbb{Q}_q(\sqrt{2})^*)^2 \Leftrightarrow c \equiv$ (*non-square in* $\mathbb{F}_q(\sqrt{2})^*$) (mod q).

Proof. First, assume that $c = 1$ in $\mathbb{Q}_q(\sqrt{2})^*/(\mathbb{Q}_q(\sqrt{2})^*)^2$. Then $c \in (\mathbb{Q}_q(\sqrt{2})^*)^2$, and so there exists a $d \in \mathbb{Q}_q(\sqrt{2})^*$ such that $c = d^2$. Since $|c|_q = 1$, we conclude that also $|d|_q = 1$. Therefore,

$$c = (\sum_{n=0}^{\infty} d_n q^n)^2, \quad d_0 \neq 0,\, d_n \in \mathbb{F}_q(\sqrt{2}),$$

and so $c \equiv d_0^2 \pmod{q}$, $d_0 \in \mathbb{F}_q(\sqrt{2})^*$.

Conversely, assume that c is congruent to a square in $\mathbb{F}_q(\sqrt{2})^*$ modulo q, i.e. assume that there exists $d_0 \in \mathbb{F}_q(\sqrt{2})^*$ such that

$$c \equiv d_0^2 \pmod{q}. \tag{6.8}$$

Since $|c|_q = 1$, we have

$$c = \sum_{n=0}^{\infty} c_n q^n, \quad c_0 \neq 0,\, c_n \in \mathbb{F}_q(\sqrt{2}).$$

Define $f(x) := x^2 - c \in \mathbb{Z}_q[\sqrt{2}][x]$. Then $f'(x) = 2x$ and

$$|f'(d_0)|_q^2 = |2d_0|_q^2 = |2|_q^2 \cdot |d_0|_q^2 = |d_0|_q^2 = 1.$$

Using (6.8) we see that

$$\begin{aligned} |f(d_0)|_q &= |d_0^2 - c|_q \\ &= |d_0^2 - (c_0 + c_1 q) + c_2 q^2 + \ldots|_q \\ &\leq q^{-1}. \end{aligned}$$

Hence,

$$|f(d_0)_q \leq q^{-1} < 1 = |f'(d_0)|_q^2,$$

and so Hensel's Lemma gives the existence of a $d \in \mathbb{Z}_q[\sqrt{2}]$ such that $f(d) = 0$. This implies $c = d^2$, i.e. $c = 1$ in $\mathbb{Q}_q(\sqrt{2})^*/(\mathbb{Q}_q(\sqrt{2})^*)^2$.

Next, assume that $c = \sqrt{2}$ in $\mathbb{Q}_q(\sqrt{2})^*/(\mathbb{Q}_q(\sqrt{2})^*)^2$. Then $c \neq 1$ in $\mathbb{Q}_q(\sqrt{2})^*/(\mathbb{Q}_q(\sqrt{2})^*)^2$, and so c is congruent to a non-square in $\mathbb{F}_q(\sqrt{2})^*$ modulo q, by the first statement of Lemma 6.8.

Conversely, assume that c is congruent to a non-square in $\mathbb{F}_q(\sqrt{2})^*$ modulo q. Since $\sqrt{2}$ represents the class of non-squares in $\mathbb{F}_q(\sqrt{2})^*$, this means that there exists $d_0 \in \mathbb{F}_q(\sqrt{2})^*$ such that

$$c = d_0^2\sqrt{2} \pmod{q}. \tag{6.9}$$

Now, define $f(x) := \sqrt{2}x^2 - c \in \mathbb{Z}_q[\sqrt{2}][x]$. Then $f'(x) = 2\sqrt{2}x$ and

$$|f'(d_0)|_q^2 = |2\sqrt{2}d_0|_q^2 = |2\sqrt{2}|_q^2 \cdot |d_0|_q^2 = 1.$$

Also,

$$|f(d_0)|_q = |\sqrt{2}d_0^2 - c|_q \leq q^{-1}$$

by (6.9). So, $|f(d_0)|_q \leq q^{-1} < 1 = |f'(d_0)|_q^2$. From Hensel's Lemma we then get the existence of a $d \in \mathbb{Z}_q[\sqrt{2}]$ such that $f(d) = 0$. Thus, $c = \sqrt{2}d^2$, i.e. $c = \sqrt{2}$ in $\mathbb{Q}_q(\sqrt{2})^*/(\mathbb{Q}_q(\sqrt{2})^*)^2$. □

Lemma 6.9. *Let $c \in \mathbb{Q}_q(\sqrt{2})^*/(\mathbb{Q}_q(\sqrt{2})^*)^2$ and assume that $|c|_q = q^{-1}$. Then the following hold:*

- *$c = q$ in $\mathbb{Q}_q(\sqrt{2})^*/(\mathbb{Q}_q(\sqrt{2})^*)^2 \Leftrightarrow c = q{\cdot}d$, where $d \equiv$ (square in $\mathbb{F}_q(\sqrt{2})^*$) (mod q).*
- *$c = q\sqrt{2}$ in $\mathbb{Q}_q(\sqrt{2})^*/(\mathbb{Q}_q(\sqrt{2})^*)^2 \Leftrightarrow c = q{\cdot}d$, where $d \equiv$ (non-square in $\mathbb{F}_q(\sqrt{2})^*$) (mod q).*

Proof. First, we note that

$$\left|\frac{c}{q}\right|_q = |c|_q \cdot \left|\frac{1}{q}\right|_q = 1,$$

since $|c|_q = q^{-1}$.

Now, assume that $c = q$ in $\mathbb{Q}_q(\sqrt{2})^*/(\mathbb{Q}_q(\sqrt{2})^*)^2$. Then $\frac{c}{q} = 1$ in $\mathbb{Q}_q(\sqrt{2})^*/(\mathbb{Q}_q(\sqrt{2})^*)^2$ and so $\frac{c}{q} \equiv$ (square in $\mathbb{F}_q(\sqrt{2})^*$) (mod q) by Lemma 6.8. Thus $c = q \cdot d$, where $d \equiv$ (square in $\mathbb{F}_q(\sqrt{2})^*$) (mod q).

Conversely, assume that $c = q{\cdot}d$, where $d \equiv$ (square in $\mathbb{F}_q(\sqrt{2})^*$) (mod q). Then $\frac{c}{q} \equiv$ (square in $\mathbb{F}_q(\sqrt{2})^*$) (mod q), and so Lemma 6.8 gives $\frac{c}{q} = 1$ in $\mathbb{Q}_q(\sqrt{2})^*/(\mathbb{Q}_q(\sqrt{2})^*)^2$, i.e. $c = q$ in $\mathbb{Q}_q(\sqrt{2})^*/(\mathbb{Q}_q(\sqrt{2})^*)^2$.

Next, assume that $c = q\sqrt{2}$ in $\mathbb{Q}_q(\sqrt{2})^*/(\mathbb{Q}_q(\sqrt{2})^*)^2$. Then $\frac{c}{q} = \sqrt{2}$ in $\mathbb{Q}_q(\sqrt{2})^*/(\mathbb{Q}_q(\sqrt{2})^*)^2$, and so Lemma 6.8 implies that $\frac{c}{q} \equiv$ (non-square in $\mathbb{F}_q(\sqrt{2})^*$) (mod q). Hence, $c = q \cdot d$, where $d \equiv$ (non-square in $\mathbb{F}_q(\sqrt{2})^*$) (mod q).

Conversely, assume that $c = q \cdot d$, where $d \equiv$ (non-square in $\mathbb{F}_q(\sqrt{2})^*$) (mod q). Then $\frac{c}{q} \equiv$ (non-square in $\mathbb{F}_q(\sqrt{2})^*$) (mod q), and so $\frac{c}{q} = \sqrt{2}$ in $\mathbb{Q}_q(\sqrt{2})^*/(\mathbb{Q}_q(\sqrt{2})^*)^2$ by Lemma 6.8, i.e. $c = q\sqrt{2}$ in $\mathbb{Q}_q(\sqrt{2})^*/(\mathbb{Q}_q(\sqrt{2})^*)^2$. □

Lemma 6.10. *A set of representatives for $\mathbb{Q}_q(\sqrt{2})^*/(\mathbb{Q}_q(\sqrt{2})^*)^2$ is given by $\{1, \sqrt{2}, q, q\sqrt{2}\}$.*

Proof. Let $x \in \mathbb{Q}_q(\sqrt{2})^*/(\mathbb{Q}_q(\sqrt{2}))^2$. Then, according to a previous remark, $|x|_q \in \{q^{-s} | s \in \mathbb{Z}\}$. Since we are working modulo squares we may assume that $|x|_q = 1$ or $|x|_q = q^{-1}$ (as this can always be obtained by multiplying x by a suitable square in $\mathbb{Q}_q(\sqrt{2})^*$). If $|x|_q = 1$ then Lemma 6.8 implies that $x = 1$ or $x = \sqrt{2}$ in $\mathbb{Q}_q(\sqrt{2})^*/(\mathbb{Q}_q(\sqrt{2})^*)^2$. If, on the other hand, $|x|_q = q^{-1}$, then Lemma 6.9 gives that $x = q$ or $x = q\sqrt{2}$ in $\mathbb{Q}_q(\sqrt{2})^*/(\mathbb{Q}_q(\sqrt{2})^*)^2$. □

Finally, we consider the group $(\mathbb{Q}(i))_q^*/((\mathbb{Q}(i))_q^*)^2$. -1 is a quadratic residue modulo q, and so the equation $x^2 = -1$ has 2 solutions in $\mathbb{Q}_q^*$. Since $(1+x)(1-x) = 1-x^2 = 2$ and 2 is a non-square in $\mathbb{Q}_q^*$, either $1+x$ is a square in $\mathbb{Q}_q^*$ and $1-x$ is a non-square in $\mathbb{Q}_q^*$, or $1+x$ is a non-square in $\mathbb{Q}_q^*$ and $1-x$ is a square in $\mathbb{Q}_q^*$. We let α denote that of the 2 solutions to $x^2 = -1$ that makes $1+x$ a square in $\mathbb{Q}_q^*$. The other solution is then $-\alpha$. Since $1+\alpha$ is a square in $\mathbb{Q}_q^*$, $1+\alpha$ is represented by 1 in $\mathbb{Q}_q^*/(\mathbb{Q}_q^*)^2$. Furthermore, since $1-\alpha$ is a non-square in $\mathbb{Q}_q^*$ and

$$|1+\alpha|_q \cdot |1-\alpha|_q = |2|_q = 1,$$

$1-\alpha$ is represented by 2 in $\mathbb{Q}_q^*/(\mathbb{Q}_q^*)^2$.

Because of the 2 solutions to the equation $x^2 = -1$ in $\mathbb{Q}_q$ there are 2 embeddings of $\mathbb{Q}(i)^*$ into $\mathbb{Q}_q^*$:

$$x + yi \mapsto x + y\alpha \quad \text{and} \quad x + yi \mapsto x - y\alpha.$$

Thus, $(\mathbb{Q}(i))_q^*/((\mathbb{Q}(i))_q^*)^2$ is isomorphic to $\mathbb{Q}_q^*/(\mathbb{Q}_q^*)^2 \times \mathbb{Q}_q^*/(\mathbb{Q}_q^*)^2$. A set of representatives for $\mathbb{Q}_q^*/(\mathbb{Q}_q^*)^2 \times \mathbb{Q}_q^*/(\mathbb{Q}_q^*)^2$ is given by $\{1,2,q,2q\} \times \{1,2,q,2q\}$.

Using the previous remarks and Lemma 6.10 we conclude that

$$\begin{aligned} M_q &\cong \mathbb{Q}_q^*/(\mathbb{Q}_q^*)^2 \times \mathbb{Q}_q(\sqrt{2})^*/(\mathbb{Q}_q(\sqrt{2})^*)^2 \times [\mathbb{Q}_q^*/(\mathbb{Q}_q^*)^2 \times \mathbb{Q}_q^*/(\mathbb{Q}_q^*)^2] \\ &= \{1,2,q,2q\} \times \{1,\sqrt{2},q,q\sqrt{2}\} \times [\{1,2,q,2q\} \times \{1,2,q,2q\}], \end{aligned} \tag{6.10}$$

and the map $j_q : M \to M_q$ is given by

$$[x, x_1 + y_1\sqrt{2}, x_2 + y_2 i] \mapsto [x, x_1 + y_1\sqrt{2}, [x_2 + y_2\alpha, x_2 - y_2\alpha]]. \tag{6.11}$$

Lemma 6.11. *Let j_q be the map (6.11). Then*

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

Proof. $[-1,1,1], [3,1,1], [1,-1,1], [1,3,1], [1,1,3] \in \ker j_q$, since -1 and 3 are quadratic residues modulo q. Since 2 is a quadratic non-residue modulo q, we have $[2,1,1] \notin \ker j_q$. Also, $[q,1,1], [1,q,1] \notin \ker j_q$.

Now, we claim that $[1,\sqrt{2},1] \notin \ker j_q$. For if this were not the case we would have $\sqrt{2} \in ((\mathbb{Q}(\sqrt{2}))_q^*)^2$. Since $|\sqrt{2}|_q = 1$ we would then have

$$\sqrt{2} = \left(\sum_{n=0}^{\infty} y_n q^n \right)^2, \quad y_0 \in \mathbb{F}_q(\sqrt{2})^*,\ y_n \in \mathbb{F}_q(\sqrt{2}).$$

Since $y_0 \in \mathbb{F}_q(\sqrt{2})^*$ there exist $c, d \in \mathbb{F}_q$, $c \neq 0$ or $d \neq 0$, such that $y_0 = c + d\sqrt{2}$. Substituting this for y_0 in (6.3) we get

$$\sqrt{2} \equiv (c + d\sqrt{2})^2 \pmod{q},$$

in particular,

$$0 \equiv c^2 + 2d^2 \pmod{q}. \tag{6.12}$$

If $c \neq 0$ then (6.12) can be rewritten as $-2 \equiv (\frac{d}{c})^2 \pmod{q}$ and if $d \neq 0$ (6.12) can be rewritten as $-2 \equiv (\frac{c}{d})^2 \pmod{q}$. Thus in each case we conclude that -2 is a quadratic residue modulo q, and so we have reached a contradiction.

Next, we examine $[1, 1+\sqrt{2}, 1]$. We prove that $1+\sqrt{2} \in (\mathbb{F}_q(\sqrt{2})^*)^2$ and use this for proving that $1+\sqrt{2} \in (\mathbb{Q}_q(\sqrt{2})^*)^2$. Since -1 is a quadratic residue modulo q there exists $r \in \{0, 1, \ldots, q-1\}$ such that $-1 \equiv r^2 \pmod{q}$. We have the following series of equivalent statements:

$$\begin{aligned} & 1+\sqrt{2} \in (\mathbb{F}_q(\sqrt{2})^*)^2 \\ \Leftrightarrow\ & \exists v, w \in \mathbb{F}_q : 1+\sqrt{2} = (v+w\sqrt{2})^2 \\ \Leftrightarrow\ & \exists v, w \in \mathbb{F}_q : v^2+2w^2 = 1 \wedge 2vw = 1 \\ \Leftrightarrow\ & \exists v \in \mathbb{F}_q : 2v^4 - 2v^2 + 1 = 0 \end{aligned}$$

$$\Leftrightarrow \exists v \in \mathbb{F}_q : 2A^2 - 2A + 1 = 0 \wedge A = v^2. \tag{6.13}$$

We determine the solutions of $2A^2 - 2A + 1 = 0$ in $\mathbb{F}_q$:

$$A = \frac{-(-2) \pm \sqrt{(-2)^2 - 4 \cdot 2 \cdot 1}}{2 \cdot 2} = \frac{2 \pm \sqrt{(-1) \cdot 2^2}}{4} = \frac{2 \pm 2r}{4} = \frac{1 \pm r}{2}.$$

This means that (6.13) holds if and only if the equation

$$\frac{1 \pm r}{2} = v^2$$

has a solution $v \in \mathbb{F}_q$. Since 2 is a non-square in $\mathbb{F}_q$, this is equivalent to at least one of $1+r$ and $1-r$ being a non-square in $\mathbb{F}_q$. In fact, precisely one of $1+r$ and $1-r$ is a non-square in $\mathbb{F}_q$, since

$$(1+r)(1-r) = 1 - r^2 = 2$$

and 2 is a non-square in $\mathbb{F}_q$. Hence, (6.13) holds, and so $1+\sqrt{2} \in (\mathbb{F}_q(\sqrt{2})^*)^2$.

Since $1+\sqrt{2} \in (\mathbb{F}_q(\sqrt{2})^*)^2$ there exists $s_0 \in \{0, 1, \ldots, q-1\}$ such that

$$1+\sqrt{2} \equiv s_0^2 \pmod{q}. \tag{6.14}$$

Define $f(x) := x^2 - (1+\sqrt{2}) \in \mathbb{Z}_q[\sqrt{2}][x]$. Then

$$|f(s_0)|_q = |s_0^2 - (1+\sqrt{2})|_q \leq q^{-1}$$

by (6.14). Also, $f'(x) = 2x$ and

$$|f'(s_0)|_q = |2s_0|_q = |2|_q \cdot |s_0|_q = 1.$$

Hence,

$$|f(s_0)|_q \leq q^{-1} < 1 = |f'(s_0)|_q^2,$$

and so Hensel's Lemma gives the existence of an $s \in \mathbb{Z}_q[\sqrt{2}]$ such that $f(s) = 0$. Thus $1 + \sqrt{2} = s^2$, i.e. $1 + \sqrt{2} \in (\mathbb{Q}_q(\sqrt{2})^*)^2$. This means that $[1, 1 + \sqrt{2}, 1] \in \ker j_q$.

We have

$$[1, 1, i] \overset{j_q}{\mapsto} [1, 1, [\alpha, -\alpha]] = [1, 1, [\alpha, \alpha]] = [1, 1, [2, 2]], \tag{6.15}$$

since $\alpha(1 - \alpha)^2 = 2$. As noted earlier, 2 is a quadratic non-residue modulo q, so $[1, 1, i] \notin \ker j_q$.

$$[1, 1, 1 + i] \overset{j_q}{\mapsto} [1, 1, [1 + \alpha, 1 - \alpha]] = [1, 1, [1, 2]], \tag{6.16}$$

so $[1, 1, 1 + i] \notin \ker j_q$. Next, we examine $[1, 1, a + bi]$, where a, b are as in (6.3). We have

$$[1, 1, a + bi] \overset{j_q}{\mapsto} [1, 1, [a + b\alpha, a - b\alpha]] = [1, 1, [a + b\alpha, q(a + b\alpha)]]. \tag{6.17}$$

If $a + b\alpha \notin (\mathbb{Q}_q^*)^2$ then clearly $[1, 1, a + bi] \notin \ker j_q$. If $a + b\alpha \in (\mathbb{Q}_q^*)^2$ then $q(a + b\alpha) \notin (\mathbb{Q}_q^*)^2$ as $q \notin (\mathbb{Q}_q^*)^2$, and so $[1, 1, a + bi] \notin \ker j_q$. Hence, we have proven that $[1, 1, a + bi] \notin \ker j_q$.

$$[1, 1, a - bi] \overset{j_q}{\mapsto} [1, 1, [a - b\alpha, a + b\alpha]] = [1, 1, [q(a + b\alpha), a + b\alpha]]. \tag{6.18}$$

Using the same argument as in the case of $[1, 1, a + bi]$ we conclude that $[1, 1, a - bi] \notin \ker j_q$. □

Lemma 6.11 implies that

$$\overline{\mathfrak{A}}_1 \overset{\mu'}{\mapsto} [1, q\sqrt{2}(1 + \sqrt{2}), (a + bi)(a - bi)(1 + i)i] \overset{j_q}{\mapsto} [1, q\sqrt{2}, [2q, q]]. \tag{6.19}$$

Furthermore,

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

Using (2.4) and (6.4) we see that

$$\#\mathcal{J}(\mathbb{Q}_q)/2\mathcal{J}(\mathbb{Q}_q) = \#\mathcal{J}(\mathbb{Q}_q)[2] = 2^3.$$

Hence, we are missing 1 generator of $\mathcal{J}(\mathbb{Q}_q)/2\mathcal{J}(\mathbb{Q}_q)$.

Let $\overline{\mathfrak{D}} := \{(2\alpha q, 0), \infty\} \in \mathcal{J}(\mathbb{Q}_q)$. We have

(6.20)

$$\begin{aligned}\overline{\mathfrak{D}} &\overset{\mu'_q}{\mapsto} [2\alpha q - 2q, 2\alpha q + q\sqrt{2}, [2\alpha q + 2\alpha q, (2\alpha q - 2q)((2\alpha q)^2 - 2q^2)(2\alpha q + 2\alpha q)]] \\ &= [2q(\alpha - 1), q\sqrt{2}(1 + \alpha\sqrt{2}), [\alpha q, 3\alpha(\alpha - 1)]] \\ &= [-2q(1 - \alpha), q\sqrt{2}(1 + \alpha\sqrt{2}), [\alpha q, -\alpha(1 - \alpha)]] \\ &= [2q(1 - \alpha), q\sqrt{2}(1 + \alpha\sqrt{2}), [\alpha q, \alpha(1 - \alpha)]] \\ &= [2^2 q, q\sqrt{2}(1 + \alpha\sqrt{2}), [2q, 2^2]] \\ &= [q, q\sqrt{2}(1 + \alpha\sqrt{2}), [2q, 1]].\end{aligned}$$

We want to show that $\overline{\mathfrak{D}}$ is the missing generator of $\mathcal{J}(\mathbb{Q}_q)/2\mathcal{J}(\mathbb{Q}_q)$.

Lemma 6.12. *Let α be as defined after the proof of Lemma 6.10. Then*

$$1 + \alpha\sqrt{2} \in (\mathbb{Q}_q(\sqrt{2})^*)^2.$$

Proof. First, we show that $1 + \alpha\sqrt{2} \in (\mathbb{F}_q(\sqrt{2})^*)^2$. We have the following series of equivalent statements:

$$\begin{aligned}& 1 + \alpha\sqrt{2} \in (\mathbb{F}_q(\sqrt{2})^*)^2 \\ \Leftrightarrow\ & \exists c, d \in \mathbb{F}_q : 1 + \alpha\sqrt{2} = (c + d\sqrt{2})^2 \\ \Leftrightarrow\ & \exists c, d \in \mathbb{F}_q : 1 = c^2 + 2d^2 \wedge \alpha = 2cd \qquad (6.21) \\ \Leftrightarrow\ & \exists c \in \mathbb{F}_q : 2c^4 - 2c^2 + 1 = 0 \\ \Leftrightarrow\ & \exists c \in \mathbb{F}_q : 2C^2 - 2C - 1 = 0 \wedge C = c^2.\end{aligned}$$

Since 3 is a quadratic residue mod q there exists $r \in \{0, 1, \ldots, q-1\}$ such that $3 = r^2 \pmod q$. Hence, $2C^2 - 2C - 1 = 0$ has a solution w.r.t. C in $\mathbb{F}_q$, and

$$C = \frac{-(-2) \pm \sqrt{(-2)^2 - 4 \cdot 2 \cdot (-1)}}{2 \cdot 2} = \frac{2 \pm \sqrt{2^2 \cdot 3}}{4} = \frac{1 \pm r}{2}.$$

This means that (6.21) holds if and only if $\frac{1 \pm r}{2} = c^2$ has a solution $c \in \mathbb{F}_q$. Since 2 is a non-square in $\mathbb{F}_q$, this is equivalent to at least one of $1 + r$ and $1 - r$ being a non-square in $\mathbb{F}_q$. In fact, precisely one of $1 + r$ and $1 - r$ is a non-square in $\mathbb{F}_q$, since

$$(1 + r)(1 - r) = 1 - r^2 = -2$$

and -2 is a non-square in $\mathbb{F}_q$. Hence, (6.21) holds, and so $1 + \alpha\sqrt{2} \in (\mathbb{F}_q(\sqrt{2})^*)^2$.

Since $1 + \alpha\sqrt{2} \in (\mathbb{F}_q(\sqrt{2})^*)^2$ there exists $v_0 \in \{0, 1, \ldots, q-1\}$ such that

$$1 + \alpha\sqrt{2} \equiv v_0^2 \pmod q. \qquad (6.22)$$

Define $f(x) := x^2 - (1+\alpha\sqrt{2}) \in \mathbb{Z}_q[\sqrt{2}][x]$. Then

$$|f(v_0)|_q = |v_0^2 - (1+\alpha\sqrt{2})|_q \leq q^{-1}$$

by (6.22). Also, $f'(x) = 2x$ and

$$|f'(v_0)|_q = |2v_0|_q = |2|_q \cdot |v_0|_q = 1.$$

Hence,

$$|f(v_0)|_q \leq q^{-1} < 1 = |f'(v_0)|_q^2,$$

and so Hensel's Lemma gives the existence of a $v \in \mathbb{Z}_q[\sqrt{2}]$ such that $f(v) = 0$. Thus $1+\alpha\sqrt{2} = v^2$, i.e. $1+\alpha\sqrt{2} \in (\mathbb{Q}_q(\sqrt{2})^*)^2$. □

Lemma 6.13. *Let α and $\overline{\mathfrak{D}}$ be as above and consider the notation from (2.3). Then*

$$\mathcal{J}(\mathbb{Q}_q) \ni \overline{\mathfrak{D}} = \{(2\alpha q, 0), \infty\} \overset{\mu_q'}{\mapsto} [q, q\sqrt{2}, [2q, 1]] \in M_q.$$

The images of $\overline{\mathfrak{A}}_1, \overline{\mathfrak{A}}_2$ and $\overline{\mathfrak{D}}$ are independent in M_q, and so $\overline{\mathfrak{D}}$ is the missing generator of $\mathcal{J}(\mathbb{Q}_q)/2\mathcal{J}(\mathbb{Q}_q)$.

Proof. The first statement is an immediate consequence of (6.20) and Lemma 6.12.

The independence of the images of the three elements $\overline{\mathfrak{A}}_1, \overline{\mathfrak{A}}_2$ and $\overline{\mathfrak{D}}$ in M_q is seen by comparing their first coordinates which are 1, 2 and q, respectively. □

Hence, $\mathcal{J}(\mathbb{Q}_q)/2\mathcal{J}(\mathbb{Q}_q) = \langle \overline{\mathfrak{A}}_1, \overline{\mathfrak{A}}_2, \overline{\mathfrak{D}} \rangle$.

Lemma 6.14. *Let M and a, b be as above and consider the maps j_q and μ_q' from (2.3). Furthermore, let $\overline{\mathfrak{D}}$ be as in Lemma 6.13. Then there exists $t \in \{a+bi, a-bi, (a+bi)i, (a-bi)i\}$ such that*

$$M \ni [q, q\sqrt{2}, t(1+i)] \overset{j_q}{\mapsto} \mu_q'(\overline{\mathfrak{D}}).$$

Proof. $a+b\alpha$ is represented by either $1, 2, q$ or $2q$ in $\mathbb{Q}_q^*/(\mathbb{Q}_q^*)^2$. So, according to (6.17) and (6.18), the following holds:

- If $a + b\alpha$ is represented by 1 in $\mathbb{Q}_q^*/(\mathbb{Q}_q^*)^2$, then $[1, 1, a+bi] \overset{j_q}{\mapsto} [1, 1, [1, q]]$ and $[1, 1, a-bi] \overset{j_q}{\mapsto} [1, 1, [q, 1]]$.

- If $a + b\alpha$ is represented by 2 in $\mathbb{Q}_q^*/(\mathbb{Q}_q^*)^2$, then $[1, 1, a+bi] \overset{j_q}{\mapsto} [1, 1, [2, 2q]]$ and $[1, 1, a-bi] \overset{j_q}{\mapsto} [1, 1, [2q, 2]]$.

- If $a+b\alpha$ is represented by q in $\mathbb{Q}_q^*/(\mathbb{Q}_q^*)^2$, then $[1, 1, a+bi] \overset{j_q}{\mapsto} [1, 1, [q, 1]]$ and $[1, 1, a-bi] \overset{j_q}{\mapsto} [1, 1, [1, q]]$.

- If $a+b\alpha$ is represented by $2q$ in $\mathbb{Q}_q^*/(\mathbb{Q}_q^*)^2$, then $[1,1,a+bi] \overset{j_q}{\mapsto} [1,1,[2q,2]]$ and $[1,1,a-bi] \overset{j_q}{\mapsto} [1,1,[2,2q]]$.

Going through each of the above 4 cases and using (6.15), (6.16) and Lemma 6.13 the claim of the lemma follows. □

Lemma 6.14 and (2.3) imply that

$$\mathrm{im}\mu' \leq \langle \ker j_q, \overline{H}, [q, q\sqrt{2}, t(1+i)] \rangle. \tag{6.23}$$

6.4. The case $p=2$. We have

$$M_2 = \mathbb{Q}_2^*/(\mathbb{Q}_2^*)^2 \times \mathbb{Q}_2(\sqrt{2})^*/(\mathbb{Q}_2(\sqrt{2})^*)^2 \times \mathbb{Q}_2(i)^*/(\mathbb{Q}_2(i)^*)^2. \tag{6.24}$$

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

Next, we want to determine a set of representatives for $\mathbb{Q}_2(\sqrt{2})^*/(\mathbb{Q}_2(\sqrt{2})^*)^2$. First, we examine the valuation on $\mathbb{Q}_2(\sqrt{2})$. Since 2 ramifies in $\mathbb{Q}(\sqrt{2})$, the ramification index $e(\mathbb{Q}_2(\sqrt{2})/\mathbb{Q}_2)$ equals 2. Hence, there exists a non-trivial extension of the valuation group. Let $y \in \mathbb{Q}_2(\sqrt{2})$. Denoting the extension of $|\cdot|_2$ to $\mathbb{Q}_2(\sqrt{2})$ by $|\cdot|_{\mathbb{Q}_2(\sqrt{2})}$ and writing $y = y_1 + y_2\sqrt{2}$, where $y_1, y_2 \in \mathbb{Q}_2$, we have

$$|y|_{\mathbb{Q}_2(\sqrt{2})} = |N_{\mathbb{Q}_2(\sqrt{2})/\mathbb{Q}_2}(y)|_2^{1/2} = |y_1^2 - 2y_2^2|_2^{1/2},$$

where $N_{\mathbb{Q}_2(\sqrt{2})/\mathbb{Q}_2}$ denotes the norm of the extension $\mathbb{Q}_2(\sqrt{2})/\mathbb{Q}_2$. Thus, $|y|_{\mathbb{Q}_2(\sqrt{2})}$
$\in \{2^{s/2} | s \in \mathbb{Z}\}$ for all $y \in \mathbb{Q}_2(\sqrt{2})^*$.

Lemma 6.15. *Let $c \in \mathbb{Q}_2(\sqrt{2})^*/(\mathbb{Q}_2(\sqrt{2})^*)^2$ and assume that $|c|_{\mathbb{Q}_2(\sqrt{2})} = 1$. Then the following hold:*

- $c = 1$ *in* $\mathbb{Q}_2(\sqrt{2})^*/(\mathbb{Q}_2(\sqrt{2})^*)^2 \Leftrightarrow c \equiv 1 \pmod{\sqrt{2}^5} \vee c \equiv 1 + \sqrt{2}^2 + \sqrt{2}^3 \pmod{\sqrt{2}^5}$
- $c = -1$ *in* $\mathbb{Q}_2(\sqrt{2})^*/(\mathbb{Q}_2(\sqrt{2})^*)^2 \Leftrightarrow c \equiv 1 + \sqrt{2}^2 + \sqrt{2}^4 \pmod{\sqrt{2}^5} \vee c \equiv 1 + \sqrt{2}^3 + \sqrt{2}^4 \pmod{\sqrt{2}^5}$
- $c = 3$ *in* $\mathbb{Q}_2(\sqrt{2})^*/(\mathbb{Q}_2(\sqrt{2})^*)^2 \Leftrightarrow c \equiv 1 + \sqrt{2}^2 \pmod{\sqrt{2}^5} \vee c \equiv 1 + \sqrt{2}^3 \pmod{\sqrt{2}^5}$
- $c = -3$ *in* $\mathbb{Q}_2(\sqrt{2})^*/(\mathbb{Q}_2(\sqrt{2})^*)^2 \Leftrightarrow c \equiv 1 + \sqrt{2}^4 \pmod{\sqrt{2}^5} \vee c \equiv 1 + \sqrt{2}^2 + \sqrt{2}^3 + \sqrt{2}^4 \pmod{\sqrt{2}^5}$
- $c = 1 + \sqrt{2}$ *in* $\mathbb{Q}_2(\sqrt{2})^*/(\mathbb{Q}_2(\sqrt{2})^*)^2 \Leftrightarrow c \equiv 1 + \sqrt{2} \pmod{\sqrt{2}^5} \vee c \equiv 1 + \sqrt{2} + \sqrt{2}^2 + \sqrt{2}^4 \pmod{\sqrt{2}^5}$
- $c = -(1+\sqrt{2})$ *in* $\mathbb{Q}_2(\sqrt{2})^*/(\mathbb{Q}_2(\sqrt{2})^*)^2 \Leftrightarrow c \equiv 1 + \sqrt{2} + \sqrt{2}^2 + \sqrt{2}^3 + \sqrt{2}^4 \pmod{\sqrt{2}^5} \vee c \equiv 1 + \sqrt{2} + \sqrt{2}^3 \pmod{\sqrt{2}^5}$

- $c = 3(1+\sqrt{2})$ *in* $\mathbb{Q}_2(\sqrt{2})^*/(\mathbb{Q}_2(\sqrt{2})^*)^2 \Leftrightarrow c \equiv 1+\sqrt{2}+\sqrt{2}^2+\sqrt{2}^3 \pmod{\sqrt{2}^5} \vee c \equiv 1+\sqrt{2}+\sqrt{2}^3+\sqrt{2}^4 \pmod{\sqrt{2}^5}$
- $c = -3(1+\sqrt{2})$ *in* $\mathbb{Q}_2(\sqrt{2})^*/(\mathbb{Q}_2(\sqrt{2})^*)^2 \Leftrightarrow c \equiv 1+\sqrt{2}+\sqrt{2}^4 \pmod{\sqrt{2}^5} \vee c \equiv 1+\sqrt{2}+\sqrt{2}^2$.

Proof. Let $c \in \mathbb{Q}_2(\sqrt{2})^*/(\mathbb{Q}_2(\sqrt{2})^*)^2$ and assume that $|c|_{\mathbb{Q}_2(\sqrt{2})} = 1$. First, we note that the elements $\pm 1, \pm 3, \pm(1+\sqrt{2}), \pm 3(1+\sqrt{2})$ are distinct in $\mathbb{Q}_2(\sqrt{2})^*/(\mathbb{Q}_2(\sqrt{2})^*)^2$ and that the valuation of each of these elements equals 1.

Since $|c|_{\mathbb{Q}_2(\sqrt{2})} = 1$ and since the residue class field of $\mathbb{Q}_2(\sqrt{2})$ equals $\mathbb{F}_2$, c can be written as

$$c = 1 + \sum_{n=1}^{\infty} c_n \sqrt{2}^n, \quad c_n \in \{0,1\},$$

i.e.

$$c \equiv 1 + c_1\sqrt{2} + c_2\sqrt{2}^2 + c_3\sqrt{2}^3 + c_4\sqrt{2}^4 \pmod{\sqrt{2}^5}, \quad c_1, c_2, c_3, c_4 \in \{0,1\}.$$

Hence, there are 16 possible values of c modulo $\sqrt{2}^5$. We list these 16 values and their images under the squaring map:

(6.25)

$$\begin{aligned}
1 \pmod{\sqrt{2}^5} &\mapsto 1 \pmod{\sqrt{2}^5},\\
1+\sqrt{2} \pmod{\sqrt{2}^5} &\mapsto 1+\sqrt{2}^2+\sqrt{2}^3 \pmod{\sqrt{2}^5},\\
1+\sqrt{2}^2 \pmod{\sqrt{2}^5} &\mapsto 1 \pmod{\sqrt{2}^5},\\
1+\sqrt{2}^3 \pmod{\sqrt{2}^5} &\mapsto 1 \pmod{\sqrt{2}^5},\\
1+\sqrt{2}^4 \pmod{\sqrt{2}^5} &\mapsto 1 \pmod{\sqrt{2}^5},\\
1+\sqrt{2}+\sqrt{2}^2 \pmod{\sqrt{2}^5} &\mapsto 1+\sqrt{2}^2+\sqrt{2}^3 \pmod{\sqrt{2}^5},\\
1+\sqrt{2}+\sqrt{2}^3 \pmod{\sqrt{2}^5} &\mapsto 1+\sqrt{2}^2+\sqrt{2}^3 \pmod{\sqrt{2}^5},\\
1+\sqrt{2}+\sqrt{2}^4 \pmod{\sqrt{2}^5} &\mapsto 1+\sqrt{2}^2+\sqrt{2}^3 \pmod{\sqrt{2}^5},\\
1+\sqrt{2}^2+\sqrt{2}^3 \pmod{\sqrt{2}^5} &\mapsto 1 \pmod{\sqrt{2}^5},\\
1+\sqrt{2}^2+\sqrt{2}^4 \pmod{\sqrt{2}^5} &\mapsto 1 \pmod{\sqrt{2}^5},\\
1+\sqrt{2}^3+\sqrt{2}^4 \pmod{\sqrt{2}^5} &\mapsto 1 \pmod{\sqrt{2}^5},\\
1+\sqrt{2}+\sqrt{2}^2+\sqrt{2}^3 \pmod{\sqrt{2}^5} &\mapsto 1+\sqrt{2}^2+\sqrt{2}^3 \pmod{\sqrt{2}^5},\\
1+\sqrt{2}+\sqrt{2}^2+\sqrt{2}^4 \pmod{\sqrt{2}^5} &\mapsto 1+\sqrt{2}^2+\sqrt{2}^3 \pmod{\sqrt{2}^5},\\
1+\sqrt{2}+\sqrt{2}^3+\sqrt{2}^4 \pmod{\sqrt{2}^5} &\mapsto 1+\sqrt{2}^2+\sqrt{2}^3 \pmod{\sqrt{2}^5},\\
1+\sqrt{2}^2+\sqrt{2}^3+\sqrt{2}^4 \pmod{\sqrt{2}^5} &\mapsto 1 \pmod{\sqrt{2}^5},\\
1+\sqrt{2}+\sqrt{2}^2+\sqrt{2}^3+\sqrt{2}^4 \pmod{\sqrt{2}^5} &\mapsto 1+\sqrt{2}^2+\sqrt{2}^3 \pmod{\sqrt{2}^5}.
\end{aligned}$$

Hence, squaring modulo $\sqrt{2}^5$ is 8-1.

Taking each of the 8 elements

$$\begin{aligned}
1 &\equiv 1 \pmod{\sqrt{2}^5},\\
-1 &\equiv 1+\sqrt{2}^2+\sqrt{2}^4 \pmod{\sqrt{2}^5},\\
3 &\equiv 1+\sqrt{2}^2 \pmod{\sqrt{2}^5},\\
-3 &\equiv 1+\sqrt{2}^4 \pmod{\sqrt{2}^5},\\
1+\sqrt{2} &\equiv 1+\sqrt{2} \pmod{\sqrt{2}^5},\\
-(1+\sqrt{2}) &\equiv 1+\sqrt{2}+\sqrt{2}^2+\sqrt{2}^3+\sqrt{2}^4 \pmod{\sqrt{2}^5},\\
3(1+\sqrt{2}) &\equiv 1+\sqrt{2}+\sqrt{2}^2+\sqrt{2}^3 \pmod{\sqrt{2}^5},\\
-3(1+\sqrt{2}) &\equiv 1+\sqrt{2}+\sqrt{2}^4 \pmod{\sqrt{2}^5}
\end{aligned} \tag{6.26}$$

and their multiple by the only non-trivial square in $\mathbb{Z}_2(\sqrt{2})$ modulo $\sqrt{2}^5$, $1+\sqrt{2}^2+\sqrt{2}^3 \pmod{\sqrt{2}^5}$, we obtain the 16 elements listed in (6.25). Hence, $\{\pm 1, \pm 3,$
$\pm(1+\sqrt{2}), \pm 3(1+\sqrt{2})\}$ is a set of representatives for $\mathbb{Z}_2(\sqrt{2})^*/(\mathbb{Z}_2(\sqrt{2})^*)^2$ modulo $\sqrt{2}^5$, and the equivalence classes are given by

$$\begin{aligned}
&\{1, 1+\sqrt{2}^2+\sqrt{2}^3\},\\
&\{1+\sqrt{2}^2+\sqrt{2}^4, 1+\sqrt{2}^3+\sqrt{2}^4\},\\
&\{1+\sqrt{2}^2, 1+\sqrt{2}^3\},\\
&\{1+\sqrt{2}^4, 1+\sqrt{2}^2+\sqrt{2}^3+\sqrt{2}^4\},\\
&\{1+\sqrt{2}, 1+\sqrt{2}+\sqrt{2}^2+\sqrt{2}^4\},\\
&\{1+\sqrt{2}+\sqrt{2}^2+\sqrt{2}^3+\sqrt{2}^4, 1+\sqrt{2}+\sqrt{2}^3\},\\
&\{1+\sqrt{2}+\sqrt{2}^2+\sqrt{2}^3, 1+\sqrt{2}+\sqrt{2}^3+\sqrt{2}^4\},\\
&\{1+\sqrt{2}+\sqrt{2}^4, 1+\sqrt{2}+\sqrt{2}^2\}.
\end{aligned} \tag{6.27}$$

The arrows of the type "$\Rightarrow$" in Lemma 6.15 are immediate consequences of (6.26) and (6.27).

Next, we prove the converse. As the proofs of these 8 statements are very similar we will only prove one of the statements. Let us consider the case $c \equiv 1+\sqrt{2}^2 \pmod{\sqrt{2}^5} \vee c \equiv 1+\sqrt{2}^3 \pmod{\sqrt{2}^5}$. Define $f(x) := x^2 - \frac{c}{3} \in \mathbb{Z}_2[\sqrt{2}][x]$. Then $f'(x) = 2x$, and so

$$|f'(z)|^2_{\mathbb{Q}_2(\sqrt{2})} = |2z|^2_{\mathbb{Q}_2(\sqrt{2})} = \sqrt{2}^{-4} \cdot |z|^2_{\mathbb{Q}_2(\sqrt{2})} = \sqrt{2}^{-4} \tag{6.28}$$

for all $z \in \mathbb{Z}_2[\sqrt{2}]$.

If $c \equiv 1 + \sqrt{2}^2$, we have

$$|f(1)|_{\mathbb{Q}_2(\sqrt{2})} = |1 - \frac{c}{3}|_{\mathbb{Q}_2(\sqrt{2})} = |3 - c|_{\mathbb{Q}_2(\sqrt{2})} \leq \sqrt{2}^{-5},$$

since $3 \equiv 1 + \sqrt{2}^2 \pmod{\sqrt{2}^5}$. Using (6.28) we get that $|f(1)|_{\mathbb{Q}_2(\sqrt{2})} < |f'(1)|^2_{\mathbb{Q}_2(\sqrt{2})}$ and then Hensel's Lemma gives the existence of a $d \in \mathbb{Z}_2(\sqrt{2})$ such that $f(d) = 0$. I.e. $c = 3d^2$, and so $c = 3$ in $\mathbb{Q}_2(\sqrt{2})^*/(\mathbb{Q}_2(\sqrt{2})^*)^2$.

On the other hand, if $c \equiv 1 + \sqrt{2}^3$, we have

$$\begin{aligned} 3(1+\sqrt{2})^2 - c &\equiv 3(1 + \sqrt{2}^2 + \sqrt{2}^3) - c \pmod{\sqrt{2}^5} \\ &\equiv (1 + \sqrt{2}^3) - c \pmod{\sqrt{2}^5} \\ &\equiv 0 \pmod{\sqrt{2}^5}, \end{aligned}$$

and so

$$\begin{aligned} |f(1+\sqrt{2})|_{\mathbb{Q}_2(\sqrt{2})} &= |(1+\sqrt{2})^2 - \frac{c}{3}|_{\mathbb{Q}_2(\sqrt{2})} \\ &= |3(1+\sqrt{2})^2 - c|_{\mathbb{Q}_2(\sqrt{2})} \\ &\leq \sqrt{2}^{-5}. \end{aligned}$$

Using (6.28) we get that $|f(1+\sqrt{2})|_{\mathbb{Q}_2(\sqrt{2})} < |f'(1+\sqrt{2})|^2_{\mathbb{Q}_2(\sqrt{2})}$ and then Hensel's Lemma gives the existence of a $d \in \mathbb{Z}_2(\sqrt{2})$ such that $f(d) = 0$. I.e. $c = 3d^2$, and so $c = 3$ in $\mathbb{Q}_2(\sqrt{2})^*/(\mathbb{Q}_2(\sqrt{2})^*)^2$. □

Since the elements on the right hand side of the equivalent statements in Lemma 6.15 constitute all the possible values of c modulo $\sqrt{2}^5$, we have the following corollary:

Corollary 6.1. *Let $c \in \mathbb{Q}_2(\sqrt{2})^*/(\mathbb{Q}_2(\sqrt{2})^*)^2$ and assume that $|c|_{\mathbb{Q}_2(\sqrt{2})} = 1$. Then $c \in \{\pm 1, \pm 3, \pm(1+\sqrt{2}), \pm 3(1+\sqrt{2})\}$.*

Lemma 6.16. *A set of representatives for $\mathbb{Q}_2(\sqrt{2})^*/(\mathbb{Q}_2(\sqrt{2})^*)^2$ is given by $\{\pm 1, \pm\sqrt{2}, \pm(1+\sqrt{2}), \pm 3, \pm\sqrt{2}(1+\sqrt{2}), \pm 3\sqrt{2}, \pm 3(1+\sqrt{2}), \pm 3\sqrt{2}(1+\sqrt{2})\}$.*

Proof. Let $c \in \mathbb{Q}_2(\sqrt{2})^*/(\mathbb{Q}_2(\sqrt{2})^*)^2$. Then – according to a previous remark – $|c|_{\mathbb{Q}_2(\sqrt{2})} \in \{2^{s/2} | s \in \mathbb{Z}\}$. Since we are working modulo squares in $\mathbb{Q}_2(\sqrt{2})^*$ we may assume that $|c|_{\mathbb{Q}_2(\sqrt{2})} = 1$ or $|c|_{\mathbb{Q}_2(\sqrt{2})} = 2^{-1/2}$.

If $|c|_{\mathbb{Q}_2}(\sqrt{2}) = 1$, then Corollary 6.1 gives that $c \in \{\pm 1, \pm 3, \pm(1+\sqrt{2}), \pm 3(1+\sqrt{2})\}$.

If $|c|_{\mathbb{Q}_2}(\sqrt{2}) = 2^{-1/2}$, then define $c' := \frac{c}{\sqrt{2}}$. Then

$$|c'|_{\mathbb{Q}_2(\sqrt{2})} = |c|_{\mathbb{Q}_2(\sqrt{2})} \cdot |1/\sqrt{2}|_{\mathbb{Q}_2(\sqrt{2})} = 2^{-1/2} \cdot 2^{1/2} = 1.$$

It follows from Corollary 6.1 that $c' \in \{\pm 1, \pm 3, \pm(1+\sqrt{2}), \pm 3(1+\sqrt{2})\}$. Thus $c \in \{\pm\sqrt{2}, \pm 3\sqrt{2}, \pm\sqrt{2}(1+\sqrt{2}), \pm 3\sqrt{2}(1+\sqrt{2})\}$.

Hence, for any $c \in \mathbb{Q}_2(\sqrt{2})^*/(\mathbb{Q}_2(\sqrt{2})^*)^2$ we have $c \in \{\pm 1, \pm\sqrt{2}, \pm(1+\sqrt{2}), \pm 3, \pm\sqrt{2}(1+\sqrt{2}), \pm 3\sqrt{2}, \pm 3(1+\sqrt{2}), \pm 3\sqrt{2}(1+\sqrt{2})\}$. Since all the elements of this set are distinct in $\mathbb{Q}_2(\sqrt{2})^*/(\mathbb{Q}_2(\sqrt{2})^*)^2$ we conclude that $\{\pm 1, \pm\sqrt{2}, \pm(1+\sqrt{2}), \pm 3, \pm\sqrt{2}(1+\sqrt{2}), \pm 3\sqrt{2}, \pm 3(1+\sqrt{2}), \pm 3\sqrt{2}(1+\sqrt{2})\}$ is a set of representatives for $\mathbb{Q}_2(\sqrt{2})^*/(\mathbb{Q}_2(\sqrt{2})^*)^2$. □

Next, we determine a set of representatives for $\mathbb{Q}_2(i)^*/(\mathbb{Q}_2(i)^*)^2$. First, we examine the valuation on $\mathbb{Q}_2(i)$. Since 2 ramifies in $\mathbb{Q}(i)$, the ramification index $e(\mathbb{Q}_2(i)/\mathbb{Q}_2)$ equals 2. Hence, there exists a non-trivial extension of the valuation group. Let $y \in \mathbb{Q}_2(i)$. Denoting the extension of $|\cdot|_2$ to $\mathbb{Q}_2(i)$ by $|\cdot|_{\mathbb{Q}_2(i)}$ and writing $y = y_1 + y_2 i$, where $y_1, y_2 \in \mathbb{Q}_2$, we have

$$|y|_{\mathbb{Q}_2(i)} = |N_{\mathbb{Q}_2(i)/\mathbb{Q}_2}(y)|_2^{1/2} = |y_1^2 + y_2^2|_2^{1/2},$$

where $N_{\mathbb{Q}_2(i)/\mathbb{Q}_2}$ denotes the norm of the extension $\mathbb{Q}_2(i)/\mathbb{Q}_2$. Thus, $|y|_{\mathbb{Q}_2(\sqrt{2})} \in \{2^{s/2} | s \in \mathbb{Z}\}$ for all $y \in \mathbb{Q}_2(\sqrt{2})^*$.

Lemma 6.17. *Let $c \in \mathbb{Q}_2(i)^*/(\mathbb{Q}_2(i)^*)^2$ and assume that $|c|_{\mathbb{Q}_2(i)} = 1$. Then the following hold:*

- $c = 1$ *in* $\mathbb{Q}_2(i)^*/(\mathbb{Q}_2(i)^*)^2 \Leftrightarrow c \equiv 1 \pmod{(1+i)^5} \vee c \equiv 1 + (1+i)^2 + (1+i)^3 + (1+i)^4 \pmod{(1+i)^5}$
- $c = 3$ *in* $\mathbb{Q}_2(i)^*/(\mathbb{Q}_2(i)^*)^2 \Leftrightarrow c \equiv 1 + (1+i)^2 + (1+i)^3 \pmod{(1+i)^5} \vee c \equiv 1 + (1+i)^4 \pmod{(1+i)^5}$
- $c = i$ *in* $\mathbb{Q}_2(i)^*/(\mathbb{Q}_2(i)^*)^2 \Leftrightarrow c \equiv 1 + (1+i) + (1+i)^2 + (1+i)^3 + (1+i)^4 \pmod{(1+i)^5} \vee c \equiv 1 + (1+i) + (1+i)^3 + (1+i)^4 \pmod{(1+i)^5}$
- $c = 2 + 3i$ *in* $\mathbb{Q}_2(i)^*/(\mathbb{Q}_2(i)^*)^2 \Leftrightarrow c \equiv 1 + (1+i) + (1+i)^2 \pmod{(1+i)^5} \vee c \equiv 1 + (1+i) \pmod{(1+i)^5}$
- $c = 3i$ *in* $\mathbb{Q}_2(i)^*/(\mathbb{Q}_2(i)^*)^2 \Leftrightarrow c \equiv 1 + (1+i) + (1+i)^3 \pmod{(1+i)^5} \vee c \equiv 1 + (1+i) + (1+i)^2 + (1+i)^3 \pmod{(1+i)^5}$
- $c = 3(2+3i)$ *in* $\mathbb{Q}_2(i)^*/(\mathbb{Q}_2(i)^*)^2 \Leftrightarrow c \equiv 1 + (1+i) + (1+i)^4 \pmod{(1+i)^5} \vee c \equiv 1 + (1+i) + (1+i)^2 + (1+i)^4 \pmod{(1+i)^5}$
- $c = (2+3i)i$ *in* $\mathbb{Q}_2(i)^*/(\mathbb{Q}_2(i)^*)^2 \Leftrightarrow c \equiv 1 + (1+i)^2 + (1+i)^4 \pmod{(1+i)^5} \vee c \equiv 1 + (1+i)^3 \pmod{(1+i)^5}$
- $c = 3(2+3i)i$ *in* $\mathbb{Q}_2(i)^*/(\mathbb{Q}_2(i)^*)^2 \Leftrightarrow c \equiv 1 + (1+i)^3 + (1+i)^4 \pmod{(1+i)^5} \vee c \equiv 1 + (1+i)^2 \pmod{(1+i)^5}$.

Proof. Similar to the proof of Lemma 6.15. □

Lemma 6.18. *Let a and b be as in (6.3).*

If $(a \equiv 2 \pmod 8$ and $b \equiv 1, 3 \pmod 8)$ or $(a \equiv 6 \pmod 8$ and $b \equiv 5, 7 \pmod 8)$, then $a + bi = 2 + 3i$ in $\mathbb{Q}_2(i)^*/(\mathbb{Q}_2(i)^*)^2$.

If $(a \equiv 2 \pmod 8$ and $b \equiv 5, 7 \pmod 8)$ or $(a \equiv 6 \pmod 8$ and $b \equiv 1, 3 \pmod 8)$, then $a + bi = 3(2 + 3i)$ in $\mathbb{Q}_2(i)^*/(\mathbb{Q}_2(i)^*)^2$.

Proof. From an earlier assumption we have that $2|a$ and $2 \nmid b$. In addition to this, we note that $4 \nmid a$. For if $4|a$ we would have $a^2 \equiv 0 \pmod 8$, and so $q = a^2 + b^2 \equiv 1 \pmod 8$, contradicting the fact that $q \equiv 5 \pmod 8$. Hence, the statement of the lemma includes all possible values of a and b.

First, let $a \equiv 2 \pmod 8$ and $b \equiv 1, 3 \pmod 8$. Since $8 = i(1+i)^6$ this implies $a \equiv 2 \pmod{(1+i)^5}$ and $b \equiv 1, 3 \pmod{(1+i)^5}$.

$$\begin{aligned} a + bi &\equiv \begin{cases} 2 + i \pmod{(1+i)^5}, & \text{if } b \equiv 1 \pmod{(1+i)^5}, \\ 2 + 3i \pmod{(1+i)^5}, & \text{if } b \equiv 3 \pmod{(1+i)^5}, \end{cases} \\ &\equiv \begin{cases} 1 + (1+i) \pmod{(1+i)^5}, & \text{if } b \equiv 1 \pmod{(1+i)^5}, \\ 1 + (1+i) + (1+i)^2 \pmod{(1+i)^5}, & \text{if } b \equiv 3 \pmod{(1+i)^5}, \end{cases} \end{aligned}$$

and so – by Lemma 6.17 – $a + bi = 2 + 3i$ in $\mathbb{Q}_2(i)^*/(\mathbb{Q}_2(i)^*)^2$.

Next, let $a \equiv 6 \pmod 8$ and $b \equiv 5, 7 \pmod 8$. Then $a \equiv 6 \pmod{(1+i)^5}$ and $b \equiv 5, 7 \pmod{(1+i)^5}$. Using the fact that $(1+i)^5 = -4 - 4i$ we get

$$\begin{aligned} a + bi &\equiv \begin{cases} 6 + 5i \pmod{(1+i)^5}, & \text{if } b \equiv 1 \pmod{(1+i)^5}, \\ 6 + 7i \pmod{(1+i)^5}, & \text{if } b \equiv 3 \pmod{(1+i)^5}, \end{cases} \\ &\equiv \begin{cases} 2 + i \pmod{(1+i)^5}, & \text{if } b \equiv 1 \pmod{(1+i)^5}, \\ 2 + 3i \pmod{(1+i)^5}, & \text{if } b \equiv 3 \pmod{(1+i)^5}, \end{cases} \\ &\equiv \begin{cases} 1 + (1+i) \pmod{(1+i)^5}, & \text{if } b \equiv 1 \pmod{(1+i)^5}, \\ 1 + (1+i) + (1+i)^2 \pmod{(1+i)^5}, & \text{if } b \equiv 3 \pmod{(1+i)^5}. \end{cases} \end{aligned}$$

Again, Lemma 6.17 gives that $a + bi = 2 + 3i$ in $\mathbb{Q}_2(i)^*/(\mathbb{Q}_2(i)^*)^2$.

Now, let $a \equiv 2 \pmod 8$ and $b \equiv 5, 7 \pmod 8$. Then $a \equiv 2 \pmod{(1+i)^5}$ and $b \equiv 5, 7 \pmod{(1+i)^5}$. We have

$$\begin{aligned} a + bi &\equiv \begin{cases} 2 + 5i \pmod{(1+i)^5}, & \text{if } b \equiv 5 \pmod{(1+i)^5}, \\ 2 + 7i \pmod{(1+i)^5}, & \text{if } b \equiv 7 \pmod{(1+i)^5}, \end{cases} \\ &\equiv \begin{cases} -2 + i \pmod{(1+i)^5}, & \text{if } b \equiv 5 \pmod{(1+i)^5}, \\ -2 + 3i \pmod{(1+i)^5}, & \text{if } b \equiv 7 \pmod{(1+i)^5}, \end{cases} \\ &\equiv \begin{cases} 1 + (1+i) + (1+i)^4 \pmod{(1+i)^5}, & \text{if } b \equiv 5 \pmod{(1+i)^5}, \\ 1 + (1+i) + (1+i)^2 + (1+i)^4 \pmod{(1+i)^5}, & \text{if } b \equiv 7 \pmod{(1+i)^5}, \end{cases} \end{aligned}$$

and by Lemma 6.17 we conclude that $a + bi = 3(2 + 3i)$ in $\mathbb{Q}_2(i)^*/(\mathbb{Q}_2(i)^*)^2$.

Finally, let $a \equiv 6 \pmod 8$ and $b \equiv 1, 3 \pmod 8$. Then $a \equiv 6 \pmod{(1+i)^5}$ and $b \equiv 1, 3 \pmod{(1+i)^5}$, and so

$$\begin{aligned} a + bi &\equiv \begin{cases} 6 + i \pmod{(1+i)^5}, & \text{if } b \equiv 1 \pmod{(1+i)^5}, \\ 6 + 3i \pmod{(1+i)^5}, & \text{if } b \equiv 3 \pmod{(1+i)^5}, \end{cases} \\ &\equiv \begin{cases} -2 + i \pmod{(1+i)^5}, & \text{if } b \equiv 1 \pmod{(1+i)^5}, \\ -2 + 3i \pmod{(1+i)^5}, & \text{if } b \equiv 3 \pmod{(1+i)^5}, \end{cases} \\ &\equiv \begin{cases} 1 + (1+i) + (1+i)^4 \pmod{(1+i)^5}, & \text{if } b \equiv 1 \pmod{(1+i)^5}, \\ 1 + (1+i) + (1+i)^2 + (1+i)^4 \pmod{(1+i)^5}, & \text{if } b \equiv 3 \pmod{(1+i)^5}. \end{cases} \end{aligned}$$

By Lemma 6.17 $a+bi = 3(2+3i)$ in $\mathbb{Q}_2(i)^*/(\mathbb{Q}_2(i)^*)^2$. □

Lemma 6.19. *Let a and b be as in (6.3). Then $\{1, 3, i, a+bi, 3i, 3(a+bi), (a+bi)i, 3(a+bi)i\}$ is a set of representatives for the subgroup of $\mathbb{Q}_2(i)^*/(\mathbb{Q}_2(i)^*)^2$ consisting of those elements having valuation equal to 1.*

Proof. According to Lemma 6.17 $3, i, 2+3i$ generates a set of representatives for the subgroup of $\mathbb{Q}_2(i)^*/(\mathbb{Q}_2(i)^*)^2$ consisting of those elements having valuation equal to 1. By Lemma 6.18 $\langle 3, i, 2+3i\rangle = \langle 3, i, a+bi\rangle$. □

Lemma 6.20. *Let a and b be as in (6.3). A set of representatives for $\mathbb{Q}_2(i)^*/(\mathbb{Q}_2(i)^*)^2$ is given by $\{1, 1+i, 3, i, a+bi, 3i, 3(1+i), i(1+i), 3i(1+i), (a+bi)(1+i), 3(a+bi), (a+bi)i, 3i(a+bi), 3(1+i)(a+bi), i(1+i)(a+bi), 3i(1+i)(a+bi)\}$.*

Proof. Let $c \in \mathbb{Q}_2(i)^*/(\mathbb{Q}_2(i)^*)^2$. Then $|c|_{\mathbb{Q}_2(i)} \in \{2^{s/2} | s \in \mathbb{Z}\}$. Since we are working modulo squares in $\mathbb{Q}_2(i)^*$ we may assume that $|c|_{\mathbb{Q}_2(i)} = 1$ or $|c|_{\mathbb{Q}_2(i)} = 2^{-1/2}$.

If $|c|_{\mathbb{Q}_2(i)} = 1$, then Lemma 6.19 gives that c is represented by an element in $\{1, 3, i, a+bi, 3i, 3(a+bi), (a+bi)i, 3(a+bi)i\}$.

If $|c|_{\mathbb{Q}_2(i)} = 2^{-1/2}$, then define $c' := \frac{c}{1+i}$. Then

$$|c'|_{\mathbb{Q}_2(i)} = |c|_{\mathbb{Q}_2(i)} \cdot |1+i|^{-1}_{\mathbb{Q}_2(i)} = 2^{-1/2} \cdot (2^{-1/2})^{-1} = 1,$$

and so c' is represented by an element in $\{1, 3, i, a+bi, 3i, 3(a+bi), (a+bi)i, 3(a+bi)i\}$ by Lemma 6.19, i.e. c is represented by an element in $\{1+i, 3(1+i), i(1+i), 3i(1+i), (a+bi)(1+i), 3(a+bi)(1+i), i(1+i)(a+bi), 3i(1+i)(a+bi)\}$. □

Lemma 6.21. *Let j_2 be the map from commutative diagram (2.3. Then*

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

Proof. According to Section 5 the only elements of $\langle -1, 2, 3, q\rangle$ which are squares in $\mathbb{Q}_2^*$ are 1 and $-3q$.

Next, we determine the squares in $\mathbb{Q}_2(\sqrt{2})^*$ of the subgroup $\langle -1, 1+\sqrt{2}, \sqrt{2},$
$3, q\rangle \leq \mathbb{Q}(\sqrt{2})^*$. First, we note that the only possible squares must be contained in $\langle -1, 1+\sqrt{2}, 3, q\rangle$, since $|\sqrt{2}|_{\mathbb{Q}_2(\sqrt{2})} = 2^{-1/2}$ and the valuation is 1 for each of the elements $-1, 1+\sqrt{2}, 3, q$. From Lemma 6.15 we already know that $-1, \pm 3, \pm(1+\sqrt{2}), \pm 3(1+\sqrt{2})$ are non-squares. Since $-3q \in (\mathbb{Q}_2^*)^2$, we have $-3q \in (\mathbb{Q}_2(\sqrt{2})^*)^2$. This has the following consequences:

$$-3q \in (\mathbb{Q}_2(\sqrt{2})^*)^2 \wedge -3 \notin (\mathbb{Q}_2(\sqrt{2})^*)^2 \Rightarrow q \notin (\mathbb{Q}_2(\sqrt{2})^*)^2,$$

$$-3q \in (\mathbb{Q}_2(\sqrt{2})^*)^2 \wedge 3 \notin (\mathbb{Q}_2(\sqrt{2})^*)^2 \Rightarrow -q \notin (\mathbb{Q}_2(\sqrt{2})^*)^2,$$

$$-3q \in (\mathbb{Q}_2(\sqrt{2})^*)^2 \wedge -3(1+\sqrt{2}) \notin (\mathbb{Q}_2(\sqrt{2})^*)^2 \Rightarrow q(1+\sqrt{2}) \notin (\mathbb{Q}_2(\sqrt{2})^*)^2,$$

$$-3q \in (\mathbb{Q}_2(\sqrt{2})^*)^2 \wedge 3(1+\sqrt{2}) \notin (\mathbb{Q}_2(\sqrt{2})^*)^2 \Rightarrow -(1+\sqrt{2})q \notin (\mathbb{Q}_2(\sqrt{2})^*)^2,$$

$$-3q \in (\mathbb{Q}_2(\sqrt{2})^*)^2 \wedge -(1+\sqrt{2}) \notin (\mathbb{Q}_2(\sqrt{2})^*)^2 \Rightarrow 3q(1+\sqrt{2}) \notin (\mathbb{Q}_2(\sqrt{2})^*)^2,$$

$$-3q \in (\mathbb{Q}_2(\sqrt{2})^*)^2 \wedge (1+\sqrt{2}) \notin (\mathbb{Q}_2(\sqrt{2})^*)^2 \Rightarrow -3q(1+\sqrt{2}) \notin (\mathbb{Q}_2(\sqrt{2})^*)^2.$$

Hence, we have proven that the only elements of $\langle -1, 1+\sqrt{2}, \sqrt{2}, 3, q\rangle$ that are squares in $\mathbb{Q}_2(\sqrt{2})^*$ are 1 and $-3q$.

Finally, we consider the subgroup $\langle i, 1+i, 3, a+bi, a-bi\rangle \leq \mathbb{Q}(i)^*$ and determine which of its elements are squares in $\mathbb{Q}_2(i)^*$. This is done by applying Lemma 6.20 and using the same kind of arguments as in the previous case. We find that the only squares are 1 and $3q$ ($3q$ is a square since $3q = i^2(-3q)$ in $\mathbb{Q}_2(i)^*$ and $-3q \in (\mathbb{Q}_2^*)^2$). □

By Lemma 6.21

$$\mathfrak{A}_1 \overset{\mu'}{\mapsto} [1, q\sqrt{2}(1+\sqrt{2}), (a+bi)(a-bi)(1+i)i] \overset{j_2}{\mapsto} [1, -3\sqrt{2}(1+\sqrt{2}), 3(1+i)i]$$

and

$$\mathfrak{A}_2 \overset{\mu'}{\mapsto} [2, 3q\sqrt{2}(1+\sqrt{2}), 3i] \overset{j_2}{\mapsto} [2, -\sqrt{2}(1+\sqrt{2}), 3i].$$

Using (2.4) and (6.4) we see that

$$\#\mathcal{J}(\mathbb{Q}_2)/2\mathcal{J}(\mathbb{Q}_2) = \#\mathcal{J}(\mathbb{Q}_2)[2] \cdot 2^2 = 2^2 \cdot 2^2 = 2^4.$$

Hence, we are missing 2 generators.

First, let $x := 5$ in the polynomial of the equation of $\mathcal{C}$. Then

$$\begin{aligned}(5-2q)(5^2-2q^2)(5^2+2^2q^2) &\equiv (5-2\cdot 5)(5^2-2\cdot 5^2)(5^2+2^2\cdot 5^2) \pmod 8\\ &\equiv 5^5 + 2^2\cdot 5^5 \pmod 8\\ &\equiv 1 \pmod 8,\end{aligned}$$

since $q \equiv 5 \pmod 8$. Hence, $(5-2q)(5^2-2q^2)(5^2+2^2q^2) \in (\mathbb{Q}_2^*)^2$, and so there exists a $\varepsilon_1 \in \mathbb{Q}_2^*$ such that $\varepsilon_1^2 = (5-2q)(5^2-2q^2)(5^2+2^2q^2)$. Consequently, $\overline{\mathfrak{E}}_1 := \{(5, \varepsilon_1), \infty\} \in \mathcal{J}(\mathbb{Q}_2)$.

Lemma 6.22. *Let a and b be as in (6.3) and let $\overline{\mathfrak{E}}_1$ be defined as above. Furthermore, let M_2 be the group (6.24) and let μ_2' be as in (2.3).*

If ($a \equiv 2 \pmod 8$ *and* $b \equiv 1, 3 \pmod 8$) *or* ($a \equiv 6 \pmod 8$ *and* $b \equiv 5, 7 \pmod 8$) *then*

$$\overline{\mathfrak{E}}_1 \overset{\mu_2'}{\mapsto} [5-2q, 5+q\sqrt{2}, 5+2qi] = [3, -3(1+\sqrt{2}), i(a+bi)] \in M_2.$$

If ($a \equiv 2 \pmod 8$ *and* $b \equiv 5, 7 \pmod 8$) *or* ($a \equiv 6 \pmod 8$ *and* $b \equiv 1, 3 \pmod 8$) *then*

$$\overline{\mathfrak{E}}_1 \overset{\mu_2'}{\mapsto} [5-2q, 5+q\sqrt{2}, 5+2qi] = [3, -3(1+\sqrt{2}), 3i(a+bi)] \in M_2.$$

Proof. Clearly, μ_2' maps $\overline{\mathfrak{E}}_1$ to $[5-2q, 5+q\sqrt{2}, 5+2qi]$. Furthermore, using the fact that $q \equiv 5 \pmod 8$ it is easily seen that $5-2q$ is represented by 3 in $\mathbb{Q}_2^*/(\mathbb{Q}_2^*)^2$.

Next, we show that $5+q\sqrt{2}$ is equal to $-3(1+\sqrt{2})$ in $\mathbb{Q}_2(\sqrt{2})^*/(\mathbb{Q}_2(\sqrt{2})^*)^2$. We have

$$5 + q\sqrt{2} \equiv 5 + 5\sqrt{2} \pmod 8,$$

since $q \equiv 5 \pmod 8$. Hence,

$$5+q\sqrt{2} \equiv 5+5\sqrt{2} \equiv 1+\sqrt{2}^4+(1+\sqrt{2}^4)\sqrt{2} \equiv 1+\sqrt{2}+\sqrt{2}^4 \pmod{\sqrt{2}^5},$$

and so $5+q\sqrt{2}$ equals $-3(1+\sqrt{2})$ in $\mathbb{Q}_2(\sqrt{2})^*/(\mathbb{Q}_2(\sqrt{2})^*)^2$ by Lemma 6.15.

Finally, we show that $5+2qi$ equals either $i(a+bi)$ or $3i(a+bi)$ in $\mathbb{Q}_2(i)^*/(\mathbb{Q}_2(i)^*)^2$. We have

$$i(a+bi)(5+2qi) \equiv \begin{cases} -25 \pmod 8, & \text{if } a \equiv 2 \pmod 8 \text{ and } b \equiv 1 \pmod 8, \\ -35-20i \pmod 8, & \text{if } a \equiv 2 \pmod 8 \text{ and } b \equiv 3 \pmod 8, \\ -85-20i \pmod 8, & \text{if } a \equiv 6 \pmod 8 \text{ and } b \equiv 5 \pmod 8, \\ -95-40i \pmod 8, & \text{if } a \equiv 6 \pmod 8 \text{ and } b \equiv 7 \pmod 8, \end{cases}$$

and so

$$i(a+bi)(5+2qi) \equiv \begin{cases} -5+4i \pmod{(1+i)^5}, & \text{if } a \equiv 2 \pmod 8 \text{ and } b \equiv 1 \pmod 8, \\ 1 \pmod{(1+i)^5}, & \text{if } a \equiv 2 \pmod 8 \text{ and } b \equiv 3 \pmod 8, \\ -5+4i \pmod{(1+i)^5}, & \text{if } a \equiv 6 \pmod 8 \text{ and } b \equiv 5 \pmod 8, \\ 1 \pmod{(1+i)^5}, & \text{if } a \equiv 6 \pmod 8 \text{ and } b \equiv 7 \pmod 8. \end{cases}$$

Since $-5+4i = 1+(1+i)^2+(1+i)^3+(1+i)^4$, we get from Lemma 6.17 that, in each of the 4 subcases, $5+2qi = i(a+bi)$ in $\mathbb{Q}_2(i)^*/(\mathbb{Q}_2(i)^*)^2$.

Similarly, we have

$$3i(a+bi)(5+2qi) \equiv \begin{cases} -135-120i \pmod 8, & \text{if } a \equiv 2 \pmod 8 \text{ and } b \equiv 5 \pmod 8, \\ -165-180i \pmod 8, & \text{if } a \equiv 2 \pmod 8 \text{ and } b \equiv 7 \pmod 8, \\ -195+60i \pmod 8, & \text{if } a \equiv 6 \pmod 8 \text{ and } b \equiv 1 \pmod 8, \\ -135 \pmod 8, & \text{if } a \equiv 6 \pmod 8 \text{ and } b \equiv 3 \pmod 8, \end{cases}$$

and so

$$3i(a+bi)(5+2qi) \equiv \begin{cases} 1 \pmod{(1+i)^5}, & \text{if } a \equiv 2 \pmod 8 \text{ and } b \equiv 5 \pmod 8, \\ -5+4i \pmod{(1+i)^5}, & \text{if } a \equiv 2 \pmod 8 \text{ and } b \equiv 7 \pmod 8, \\ 1 \pmod{(1+i)^5}, & \text{if } a \equiv 6 \pmod 8 \text{ and } b \equiv 1 \pmod 8, \\ 1 \pmod{(1+i)^5}, & \text{if } a \equiv 6 \pmod 8 \text{ and } b \equiv 3 \pmod 8. \end{cases}$$

Applying Lemma 6.17 we conclude that in each of these cases $5+2qi = i(a+bi)$ in $\mathbb{Q}_2(i)^*/(\mathbb{Q}_2(i)^*)^2$. □

Next, let $x := 8$ in the polynomial of the equation of $\mathcal{C}$. Then

$$(8-2q)(8^2-2q^2)(8^2+2^2q^2) = (2^2)^2(q^5-2^2q^4-2^4q^3+2^6q^2-2^9q+2^{11})$$

and

$$\begin{aligned} q^5 - 2^2q^4 - 2^4q^3 + 2^6q^2 - 2^9q + 2^{11} &\equiv q^5 - 2^2q^4 \pmod 8 \\ &\equiv 5^5 - 2^2 \cdot 5^4 \pmod 8 \\ &\equiv 1 \pmod 8, \end{aligned}$$

since $q \equiv 5 \pmod 8$. Hence, $q^5 - 2^2q^4 - 2^4q^3 + 2^6q^2 - 2^9q + 2^{11} \in (\mathbb{Q}_2^*)^2$, and so there exists a $\varepsilon_2 \in \mathbb{Q}_2^*$ such that $\varepsilon_2^2 = q^5 - 2^2q^4 - 2^4q^3 + 2^6q^2 - 2^9q + 2^{11}$. Therefore, $\overline{\mathfrak{E}}_2 := \{(8, 2^2\varepsilon_2), \infty\} \in \mathcal{J}(\mathbb{Q}_2)$.

Lemma 6.23. *Let $\overline{\mathfrak{E}}_2$ be defined as above. Let M_2 be the group (6.24) and let μ_2' denote the map of the diagram (2.3. Then*

$$\overline{\mathfrak{E}}_2 \overset{\mu_2'}{\mapsto} [8 - 2q, 8 + q\sqrt{2}, 8 + 2qi] = [-2, -3\sqrt{2}, 1] \in M_2.$$

Proof. Clearly, μ_2' maps $\overline{\mathfrak{E}}_2$ to $[8 - 2q, 8 + q\sqrt{2}, 8 + 2qi]$. Writing $8 - 2q = -2 \cdot (q - 4)$ and using the fact that $q - 4 \in (\mathbb{Q}_2^*)^2$, since $q \equiv 5 \pmod 8$, we see that $8 - 2q = -2$ in $\mathbb{Q}_2^*/(\mathbb{Q}_2^*)^2$.

Now, we examine $8 + q\sqrt{2}$. First, we note that $8 + q\sqrt{2} = \sqrt{2}(q + 4\sqrt{2})$. Since $q + 4\sqrt{2} \equiv 5 + 4\sqrt{2} \pmod 8$, we have

$$q + 4\sqrt{2} \equiv 5 + 4\sqrt{2} \equiv 1 + \sqrt{2}^4 + \sqrt{2}^5 \equiv 1 + \sqrt{2}^4 \pmod{\sqrt{2}^5},$$

and so, by Lemma 6.15, $q + 4\sqrt{2} = -3$ in $\mathbb{Q}_2(\sqrt{2})^*/(\mathbb{Q}_2(\sqrt{2})^*)^2$. Thus, $8 + q\sqrt{2} = -3\sqrt{2}$ in $\mathbb{Q}_2(\sqrt{2})^*/(\mathbb{Q}_2(\sqrt{2})^*)^2$.

Finally, we consider $8 + 2qi$. We note that $8 + 2qi = (1 + i)^2(q - 4i)$. Since $q - 4i \equiv 5 - 4i \pmod 8$ and $8 = i(1 + i)^6$, we have $q - 4i \equiv 5 - 4i \equiv 9 \equiv 1 \pmod{(1 + i)^5}$. □

Comparing the images of $\overline{\mathfrak{E}}_1$ and $\overline{\mathfrak{E}}_2$ given by Lemma 6.22 and Lemma 6.23, respectively, in M_2 to those of $\overline{\mathfrak{A}}_1$ and $\overline{\mathfrak{A}}_2$ we conclude that the 4 divisors are independent in $\mathcal{J}(\mathbb{Q}_2)$. Thus $\mathcal{J}(\mathbb{Q}_2) = \langle \overline{\mathfrak{A}}_1, \overline{\mathfrak{A}}_2, \overline{\mathfrak{E}}_1, \overline{\mathfrak{E}}_2 \rangle$. by the commutativity of (2.3)

$$\text{im}\mu' \leq \langle \ker j_2, \overline{H}, [3, -3(1 + \sqrt{2}), z], [-2, 3\sqrt{2}, 1] \rangle, \tag{6.29}$$

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

6.5. The rank bound. Combining (6.5),(6.6),(6.23) and (6.29) we conclude that $\text{im}\mu' \leq \overline{H}$, i.e. $\text{im}\mu' = \overline{H}$, and so, by an initial remark, $\text{rank}(\mathcal{J}(\mathbb{Q})) = 0$. The following lemma summarises the results obtained from the complete 2-descent.

Lemma 6.24. *Let $\mathcal{C}$ denote the infinite family of curves over $\mathbb{Q}$ given by (6.2) 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 5.3 and 6.24 we obtain the following result:

Proposition 6.1. *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 given example is non-trivial in the sense that the Jacobian $\mathcal{J}$ (and hence $\widehat{\mathcal{J}}$) can be shown to be simple by a method described in [3], originating from [11].

Proposition 6.1 immediately implies that $Ш(\widehat{\mathcal{J}}/\mathbb{Q})[2]$ is non-trivial. In line with the idea of [1] this fact can, of course, also be proven 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 4.1 holds for the larger family of curves with $q \equiv 5 \pmod 8$ it is natural to suspect that Proposition 6.1 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.

7. 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

$$\dot{\mathcal{C}}: \quad y^2 = q(1 - 2x^2)(1 + x)(1 + x^2), \tag{7.1}$$

with Jacobian $\dot{\mathcal{J}}$. Recall ([3], 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

$$\begin{aligned} F_0(x_1, x_2) = \; & 2f_0 + f_1(x_1 + x_2) + 2f_2(x_1x_2) + f_3(x_1x_2)(x_1 + x_2) \\ & + 2f_4(x_1x_2)^2 + f_5(x_1x_2)^2(x_1 + x_2) + 2f_6(x_1x_2)^3, \end{aligned} \tag{7.2}$$

satisfy the equation of the Kummer surface. Specialising the Kummer surface equation (see [3], 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

$$\begin{aligned} & u_4^2u_2^2 - 4u_4^2u_3 - 4u_4 - 2u_4u_2 + 4u_4u_3 + 2u_4u_2u_3 \\ & + 8u_4u_3^2 + 4u_4u_2u_3^2 + 4u_2 + 2u_3 + 8u_2^2 - 11u_3^2 \\ & + 8u_2^3 + 8u_2^2u_3 - 8u_2u_3^2 - 4u_3^3 + 4u_3^4 + 5 = 0. \end{aligned} \tag{7.3}$$

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

$$u_4 = \frac{1}{q}u_7^2 + u_2 + 2u_2^2 - 2u_2u_3 + 2u_2^3 + 1. \tag{7.4}$$

Given $u_2, u_3, u_4, u_7 \in \mathbb{Q}$, one recovers $\{x_1, x_2\}$ as the roots of $x^2 - u_2x + u_3$, and can obtain $u_7' = (x_2y_1 - x_1y_2)/(x_1 - x_2)$, from which $y_i = u_7x_i - u_7'$ 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 [4]) 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:

$$(u_2 + 2 + 2u_5^2)^2 + u_2^2 = u_6^2. \tag{7.5}$$

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

$$\begin{array}{ll} \bar{u}_2(u_5,u_8) & = \frac{4(u_5^2+1-u_8-u_8u_5^2)}{u_8^2-2}, \bar{u}_3(u_5,u_8) = \frac{4u_8-2+4u_8u_5^2-u_8^2-2u_5^2u_8^2}{u_8^2-2}, \\ \bar{u}_6(u_5,u_8) & = \frac{2(-u_8^2+2u_8+2u_8u_5^2-u_5^2u_8^2-2-2u_5^2}{u_8^2-2}. \end{array} \tag{7.6}$$

We finally obtain a model, given by a single equation in u_5, u_7, u_8 by substituting (7.4) into (7.3), 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 the Hasse-Weil bound on the genus 5 curves obtained by specialising u_8, together with Hensel's lemma.

References

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

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

[3] 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.

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

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

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

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

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

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

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

[11] 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.

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

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