On a Theorem of Coleman

E. V. Flynn
Mathematical Institute, University of Oxford, Oxford OX1 3LB, England

A simplified method of descent via isogeny is given for Jacobians of curves of genus 2. This method is then used to give applications of a theorem of Coleman for computing all the rational points on certain curves of genus 2.

0 Introduction

The following classical result of Chabauty [3] is a curiosity of the literature in that there has been a 50 year period during which applications have been virtually impossible.

Proposition 0.1. *Let $\mathcal{C}$ be a curve of genus g defined over a number field K, whose Jacobian has Mordell-Weil rank $\leqslant g-1$. Then $\mathcal{C}$ has only finitely many K-rational points.*

This result is now superceded by Falting's work. However it has been shown by Coleman [4] that Chabauty's method can be used in many situations to give good bounds for the number of points on a curve. In particular, there are two potential genus 2 applications [4], [8].

Proposition 0.2. *Let $\mathcal{C}$ be a curve of genus 2 defined over $\mathbb{Q}$, and $p \geqslant 5$ be a prime of good reduction. If the Jacobian of $\mathcal{C}$ has rank at most 1 and $\widetilde{\mathcal{C}}$ is the reduction of $\mathcal{C}$ mod p then $\#\mathcal{C}(\mathbb{Q}) \leqslant \#\widetilde{\mathcal{C}}(\mathbb{F}_p) + 2$.*

Proposition 0.3. *Let $\mathcal{C}$ be a curve of genus 2 defined over $\mathbb{Q}$ with 4 rational branch points and good reduction at 3, whose Jacobian has rank at most 1. Then $\#\mathcal{C}(\mathbb{Q}) \leqslant 6$.*

If the the rational branch points of the curve in Proposition 0.3 are mapped to $(0,0), (1,0), (-1,0), (1/\lambda, 0)$, then there is the following situation for which Coleman's method is guaranteed to determine $\mathcal{C}(\mathbb{Q})$ completely.

Proposition 0.4. *Let $\mathcal{C}$ be the curve of genus 2:*

$$\mathcal{C} : Y^2 = X(X^2-1)(X-1/\lambda)(X^2+aX+b)$$

with $\lambda, a, b \in \mathbb{Z}$. *Suppose* $3^{2r} \| \lambda$ *, for some* $r > 0$*, and* 3 *does not divide* $b(1-a+b)(1+a+b)$*, and that the Jacobian of* $\mathcal{C}$ *has rank at most* 1*. Then* $\mathcal{C}(\mathbb{Q})$ *contains precisely the points* $(0,0), (1,0), (-1,0), (1/\lambda, 0)$ *and the 2 rational points at infinity.*

In principle these methods should, in many situations, determine $\mathcal{C}(\mathbb{Q})$ completely. The main impediment to applying such methods has been the lack of workable techniques for finding the rank of the Jacobian of a curve (apart from elliptic curves, for which Proposition 0.1 is uninteresting). This has recently changed, and a number of techniques have become available during the last 3 years ([2],[6],[7],[11]) which can find ranks of Jacobians. The method of complete 2-descent ([7],[8]) has been used to find the following application, in which the bound of Proposition 0.2 is attained.

Example 0.5. *Let* $\mathcal{C}$ *be the curve* $Y^2 = X(X-1)(X-2)(X-5)(X-6)$ *defined over* $\mathbb{Q}$*. Then the Jacobian of* $\mathcal{C}$ *has rank 1, and* $\#\mathcal{C}(\mathbb{Q}) = \#\mathcal{C}(\mathbb{F}_7) + 2 = 10$.

This remains the only non-trivial example in the literature for which Coleman's bound has been used to determine $\mathcal{C}(\mathbb{Q})$ completely (see also [10]). It seems unlikely that Proposition 0.2 in its current form will typically resolve $\mathcal{C}(\mathbb{Q})$ completely, since the given bound may not be attained. For example, the bound is not attained for the other rank 1 examples in the literature [6], and a brief search by the author of other curves of similar appearance to that in Example 0.5 has not yet found any further examples for which the bound is attained.

Proposition 0.4 seems potentially a more promising source of applications, since the bound is guaranteed to be attained whenever the Jacobian of any curve of the given form has rank at most 1, and Coleman has issued a general request for an explicit example. The main purpose here is to satisfy this request, by finding examples of curves of the given form whose Jacobian has rank 1.

We observe that the condition on a, b, λ of Proposition 0.4 implies that the quadratic factor: $X^2 + aX + b$ does not split over $\mathbb{Q}$, and so the technique of Gordon and Grant in [7] is not applicable. In principle, the complete 2-descent outlined in [2],[11] could be adapted, but this would require work over the number field $\mathbb{Q}(\sqrt{a^2 - 4b})$. All of the worked examples in both [7] and [11] are such that $\mathcal{C}(\mathbb{Q})$ contains all of its hyperelliptic branch points. By far the most natural technique to apply is descent via isogeny, as described in [6], which can be attempted on curves of the form: $Y^2 = q_1(X)q_2(X)q_3(X)$,

where each $q_i(X)$ is a quadratic defined over $\mathbb{Q}$. This technique has the drawback (shared with [7]) that computer algebra packages are required to compute the large equations describing the homogeneous spaces, making the rank computations difficult to verify, and somewhat inaccessible to those not prepared to follow through the algebra. Our second purpose here will be to present a simplified pen-and-paper method of descent via isogeny in genus 2, which does not require anything in the way of computer algebra packages (since the homogeneous spaces need not be computed explicitly), and which is easier for the reader to verify, once the rank computation has been completed. It is hoped that this will facilitate not only applications of Coleman's result, but will also make the computation of ranks more accessible to a wider group of participants.

1 A Simplified Descent via Isogeny

In this section, we shall summarise the technique of descent via isogeny given in [6], and then describe an improvement which removes the need for symbolic algebra packages. For a general curve $\mathcal{C} : Y^2 = \mathsf{F}_6X^6 + \ldots + \mathsf{F}_0$, of genus 2 ($\mathsf{F}_i \in K$ of characteristic $\neq 2, 3, 5$, discriminant of $\mathcal{C} \neq 0$), we let $\mathrm{Pic}^0(\mathcal{C})$ denote the Picard group of $\mathcal{C}$; that is, the group of divisors of $\mathcal{C}$ of degree 0 modulo linear equivalence. It is convenient (following [2],[5]) to represent any element of $\mathrm{Pic}^0(\mathcal{C})$ by an unordered pair of points $\{(x_1, y_1), (x_2, y_2)\}$ on $\mathcal{C}$, where we also allow ∞^+, ∞^- to appear in the unordered pair when $\mathsf{F}_6 \neq 0$, or ∞ to appear when $\mathsf{F}_6 = 0$. Such an unordered pair is a shorthand notation for the divisor class containing $(x_1, y_1) + (x_2, y_2) - \infty^+ - \infty^-$ for the case when $\mathsf{F}_6 \neq 0$, and $(x_1, y_1) + (x_2, y_2) - 2\infty$ when $\mathsf{F}_6 = 0$. This representation is unique except that we must identify all pairs of the form $\{(x, y), (x, -y)\}$ to give the canonical equivalence class, which we denote by $\mathcal{O}$. As a group, the Jacobian $\mathcal{J} = \mathcal{J}(\mathcal{C})$ may be identified with $\mathrm{Pic}^0(\mathcal{C})$. The Mordell-Weil group $\mathcal{J}(K)$ of divisors defined over K corresponds to those pairs for which (x_1, y_1) and (x_2, y_2) are either both in $\mathcal{C}(K)$ or are quadratic over K and conjugate. The 16 points over the closure of K which are 2-torsion are: $\mathcal{O}$ together with the 15 divisors in $\mathrm{Pic}^0(\mathcal{C})$ of the form $\{(x_1, 0), (x_2, 0)\}$, where x_1, x_2 are distinct roots of the sextic $\mathsf{F}_6X^6 + \ldots + \mathsf{F}_0$. Any K-rational quadratic factor of $\mathsf{F}_6X^6 + \ldots + \mathsf{F}_0$ therefore corresponds to a rational point of order 2 in $J(K)$.

From now on, the curve $\mathcal{C}$ will be taken to have the form:

$$\mathcal{C} : Y^2 = q_1(X)q_2(X)q_3(X),$$

where each $q_i(X)$ is a quadratic defined over $\mathbb{Q}$. In this case, $\mathcal{J}(\mathbb{Q})$ contains 3 points of order 2. We recall the following isogeny on $\mathcal{J}$ described in [1].

Definition 1.1. Let $\mathcal{C}$ be the curve of genus 2 defined over $\mathbb{Q}$ as:

$$\begin{aligned}\mathcal{C} : Y^2 &= q_1(X)q_2(X)q_3(X) \\ &= (f_1X^2+g_1X+h_1)(f_2X^2+g_2X+h_2)(f_3X^2+g_3X+h_3).\end{aligned} \tag{1}$$

For any two polynomials $p(X)$, $q(X)$, let $[p,q]$ denote $p'q - pq'$. Define $\widehat{\mathcal{C}}$ by:

$$\widehat{\mathcal{C}} : \Delta Y^2 = \hat{q}_1(X)\hat{q}_2(X)\hat{q}_3(X) = [q_2,q_3][q_3,q_1][q_1,q_2],$$

where

$$\Delta = \begin{vmatrix} h_1 & g_1 & f_1 \\ h_2 & g_2 & f_2 \\ h_3 & g_3 & f_3 \end{vmatrix}.$$

Denote $b_{ij} = \text{resultant}(q_i,q_j)$, $b_i = b_{ij}b_{ik}$, $\hat{b}_{ij} = \text{resultant}(\hat{q}_i,\hat{q}_j)$, $\hat{b}_i = \hat{b}_{ij}\hat{b}_{ik}$. Let $\mathcal{J}$, $\widehat{\mathcal{J}}$ be the Jacobians of $\mathcal{C}$ and $\widehat{\mathcal{C}}$, and let α_i denote the point of order 2 in $\mathcal{J}(\mathbb{Q})$ corresponding to $q_i(X)$; similarly for $\hat{\alpha}_i$.

It has been shown in [1] that $\mathcal{J}$, $\widehat{\mathcal{J}}$ are isogenous. There exists isogenies: $\phi : \mathcal{J} \to \widehat{\mathcal{J}}$ with kernel $\{\mathcal{O},\alpha_1,\alpha_2,\alpha_3\}$ and $\hat{\phi} : \widehat{\mathcal{J}} \to \mathcal{J}$ with kernel $\{\widehat{\mathcal{O}},\hat{\alpha}_1,\hat{\alpha}_2,\hat{\alpha}_3\}$, such that $\hat{\phi}\circ\phi = [2]$, the duplication map on $\mathcal{J}$. As with elliptic curves, there is a natural injection [6] from $\widehat{\mathcal{J}}(\mathbb{Q})/\phi(\mathcal{J}(\mathbb{Q}))$ into a known finite group which provides the foundation for descent via isogeny.

Lemma 1.2. *Let $\mathcal{C},\widehat{\mathcal{C}}$ be as in Definition 1.1, and let $\mathbf{w} \in \widehat{\mathcal{J}}(\mathbb{Q})$. Then there exists a unique pair $(d_1,d_2) \in \mathbb{Q}^*/(\mathbb{Q}^*)^2 \times \mathbb{Q}^*/(\mathbb{Q}^*)^2$ such that for every $\mathbf{v} \in \phi^{-1}(\mathbf{w})$, the sets $\{\mathbf{v}\}$, $\{\mathbf{v},\mathbf{v}+\alpha_i\}$, $\{\mathbf{v},\mathbf{v}+\alpha_1,\mathbf{v}+\alpha_2,\mathbf{v}+\alpha_3\}$ are defined over $\mathbb{Q}(\sqrt{d_1},\sqrt{d_2})$, $\mathbb{Q}(\sqrt{d_i})$, $\mathbb{Q}$, respectively ($i=1,2,3$, $d_3=d_1d_2$). Let $\psi : \widehat{\mathcal{J}}(\mathbb{Q})/\phi(\mathcal{J}(\mathbb{Q})) \mapsto \mathbb{Q}^*/(\mathbb{Q}^*)^2 \times \mathbb{Q}^*/(\mathbb{Q}^*)^2 : \mathbf{w} \mapsto (d_1,d_2)$. Then ψ is a well defined injective homomorphism. Let*

$$\begin{aligned}\mathcal{S} &= \{p : p \mid 2\Delta b_1b_2b_3\hat{b}_1\hat{b}_2\hat{b}_3\} = \{p_1 \dots p_r\}, \\ \mathbb{Q}(\mathcal{S}) &= \{\pm p_1^{e_1}\dots p_r^{e_r}\} \leqslant \mathbb{Q}^*/(\mathbb{Q}^*)^2.\end{aligned}$$

Then $im\,\psi \leqslant \mathbb{Q}(\mathcal{S}) \times \mathbb{Q}(\mathcal{S})$.

The problem of finding $\widehat{\mathcal{J}}(\mathbb{Q})/\phi(\mathcal{J}(\mathbb{Q}))$ is therefore reduced to that of determining, for each member of $\mathbb{Q}(\mathcal{S}) \times \mathbb{Q}(\mathcal{S})$, whether a preimage exists

under ψ. The following from [6] will work provided that no violation of the Hasse principle occurs.

Lemma 1.3. *Let $\mathcal{C}, \widehat{\mathcal{C}}$ be as in Definition 1.1, and for any p, define $\psi_p : \mathcal{J}(\mathbb{Q}_p) \longrightarrow \mathbb{Q}_p^*/(\mathbb{Q}_p^*)^2 \times \mathbb{Q}_p^*/(\mathbb{Q}_p^*)^2$ in the same manner as ψ, but with each occurrence of $\mathbb{Q}$ replaced by $\mathbb{Q}_p$. Then the following diagram commutes:*

$$\begin{array}{ccc} \widehat{\mathcal{J}}(\mathbb{Q})/\phi(\mathcal{J}(\mathbb{Q})) & \xrightarrow{\psi} & \mathbb{Q}^*/(\mathbb{Q}^*)^2 \times \mathbb{Q}^*/(\mathbb{Q}^*)^2 \\ \downarrow{\scriptstyle i_p} & & \downarrow{\scriptstyle j_p} \\ \widehat{\mathcal{J}}(\mathbb{Q}_p)/\phi(\mathcal{J}(\mathbb{Q}_p)) & \xrightarrow{\psi_p} & \mathbb{Q}_p^*/(\mathbb{Q}_p^*)^2 \times \mathbb{Q}_p^*/(\mathbb{Q}_p^*)^2 \end{array}$$

where i_p, j_p are the identity maps. It follows that, if we let S_p^ϕ denote $j_p^{-1}\big(im(\psi_p)\big)$ and $S^\phi = \underset{p}{\cap} S_p^\phi$, with $\underset{p}{\cap}$ over all primes including ∞, then $im(\psi) \leqslant S^\phi$.

The technique used in [6] maybe summarised as follows. One first computes the known members of $im(\psi)$. For the remaining $(d_1, d_2) \in \mathbb{Q}^*/(\mathbb{Q}^*)^2 \times \mathbb{Q}^*/(\mathbb{Q}^*)^2$, one constructs a homogeneous space $\mathcal{J}_{d_1,d_2}$ with the property that $\mathcal{J}_{d_1,d_2}(\mathbb{Q}) \neq \emptyset \iff (d_1, d_2) \in im(\psi)$. In each case, one then hopes to find a p such that $\mathcal{J}_{d_1,d_2}(\mathbb{Q}_p) = \emptyset$, giving that (d_1, d_2) is not in S_p^ϕ and hence not in $im(\psi)$. This will resolve $im(\psi)$, and hence $\widehat{\mathcal{J}}(\mathbb{Q})/\phi(\mathcal{J}(\mathbb{Q}))$, provided that $S^\phi = im(\psi)$. This process is repeated with respect to the dual objects: $\hat{\phi}, \hat{\psi}$, to determine $\mathcal{J}(\mathbb{Q})/\hat{\phi}(\widehat{\mathcal{J}}(\mathbb{Q}))$. These may then be combined to give $\mathcal{J}(\mathbb{Q})/2\mathcal{J}(\mathbb{Q})$, and hence the rank of $\mathcal{J}(\mathbb{Q})$.

The main barrier which makes this technique (as with [7]) inaccessible to a wider audience is the algebra involved in the construction of the homogeneous spaces $\mathcal{J}_{d_1,d_2}$. The construction is described in [6], where $\mathcal{J}_{d_1,d_2}$ is obtained by twisting an explicit model of the Jacobian variety, giving a variety described by 72 quadratic forms in $\mathbf{P}^{15}$. This means that anyone who wishes to verify such a rank computation must first check the construction of $\mathcal{J}_{d_1,d_2}$, and then (in many cases) check that there are no points on $\mathcal{J}_{d_1,d_2}(\mathbb{Q}_p)$, by running through all possibilities modulo some power of p (this last step may be speeded by Henselian lifts). We bypass this by working in a similar spirit to [11], which simplifies the complete 2-descent in [2],[7], by computing each $\mathcal{J}(\mathbb{Q}_p)/2\mathcal{J}(\mathbb{Q}_p)$ completely. This idea can be adapted to the situation of descent via isogeny. We first recall from [9] the following properties of abelian varieties.

Lemma 1.4. *For any boolean group G, let $\|G\|$ represent the number of generators of G. Let A be an abelian variety of dimension g defined over $\mathbb{Q}_p$, and let $[2]_p$ be the multiplication by 2 map on $A(\mathbb{Q}_p)$. Then, when*

$p \neq 2, \infty$, we have $\|A(\mathbb{Q}_p)/2A(\mathbb{Q}_p)\| = \|ker[2]_p\|$. When $p = 2$, we have $\|A(\mathbb{Q}_2)/2A(\mathbb{Q}_2)\| = \|ker[2]_2\|+g$. For $p = \infty$, we have $\|A(\mathbb{R})/2A(\mathbb{R})\| \leqslant g$.

The following technical lemma gives a clear way to check, for any p, that $\widehat{\mathcal{J}}(\mathbb{Q}_p)/\phi(\mathcal{J}(\mathbb{Q}_p))$ and $\mathcal{J}(\mathbb{Q}_p)/\hat{\phi}(\widehat{\mathcal{J}}(\mathbb{Q}_p))$ have been determined completely.

Lemma 1.5. *Let $\mathcal{C} : Y^2 = q_1(X)q_2(X)q_3(X)$ be a curve of genus 2, where each $q_i(X)$ is a quadratic defined over $\mathbb{Q}$. Let $\widehat{\mathcal{C}}$, $\mathcal{J}$, $\widehat{\mathcal{J}}$, ϕ and $\hat{\phi}$ be as in Definition 1.1. Then, for any p,*

$$\|\widehat{\mathcal{J}}(\mathbb{Q}_p)/\phi(\mathcal{J}(\mathbb{Q}_p))\| + \|\mathcal{J}(\mathbb{Q}_p)/\hat{\phi}(\widehat{\mathcal{J}}(\mathbb{Q}_p))\| = 4 + \epsilon_p,$$

where $\epsilon_2 = 2$, $\epsilon_\infty = -2$, and $\epsilon_p = 0$ for all $p \neq 2, \infty$.

Proof. General properties of group homomorphisms applied to the sequence: $\mathcal{J}(\mathbb{Q}_p) \xrightarrow{\phi} \widehat{\mathcal{J}}(\mathbb{Q}_p) \xrightarrow{\hat{\phi}} \mathcal{J}(\mathbb{Q}_p)$, with $[2]_p = \hat{\phi} \circ \phi$, immediately gives that:

$$\|\widehat{\mathcal{J}}(\mathbb{Q}_p)/\phi(\mathcal{J}(\mathbb{Q}_p))\| + \|\mathcal{J}(\mathbb{Q}_p)/\hat{\phi}(\widehat{\mathcal{J}}(\mathbb{Q}_p))\| = \|ker\phi\| + \|ker\hat{\phi}\| + \omega_p,$$

where $\omega_p = \|\mathcal{J}(\mathbb{Q}_p)/2\mathcal{J}(\mathbb{Q}_p))\| - \|ker[2]_p\|$. For $p \neq \infty$, Lemma 1.4, with $A = \mathcal{J}$, $g = 2$ immediately gives that $\omega_p = \epsilon_p$.

For the remaining case, $p = \infty$, the injection on $\mathcal{J}(\mathbb{R})/2\mathcal{J}(\mathbb{R})$ described in Section 5 of [2], gives that $\|\mathcal{J}(\mathbb{R})/2\mathcal{J}(\mathbb{R})\|$ is 0 if none of the $q_i(X)$ split over $\mathbb{R}$, and is otherwise equal to $(\#q_i(X)$ which split over $\mathbb{R}) - 1$. By comparison, from the fact that each 2-torsion member of $\mathcal{J}(\mathbb{R})$ corresponds to a quadratic defined over $\mathbb{R}$ which divides $q_1(X)q_2(X)q_3(X)$, we obtain: $\|ker[2]_\infty\| = \|\{$ 2-torsion members of $\mathcal{J}(\mathbb{R})\}\| = 2$, if none of the $q_i(X)$ split over $\mathbb{R}$, and is otherwise $(\#q_i(X)$ which split over $\mathbb{R}) + 1$. In all cases, $\omega_\infty = -2 = \epsilon_\infty$, as required. □

The simplified method of descent via isogeny may therefore be summarised as follows. As before, one first computes the known members of $im(\psi)$. For any given p, one then searches for divisors $\{(x_1, y_1), (x_2, y_2)\}$ in $\widehat{\mathcal{J}}(\mathbb{Q}_p)/\phi(\mathcal{J}(\mathbb{Q}_p))$ and $\mathcal{J}(\mathbb{Q}_p)/\hat{\phi}(\widehat{\mathcal{J}}(\mathbb{Q}_p))$ until a complete set of $4 + \epsilon_p$ independent divisors have been found (independence being verified by use of the injections ψ_p and $\hat{\psi}_p$), so that both S_p^ϕ and $S_p^{\hat{\phi}}$ are completely determined. This process is repeated for different primes until it is established (one hopes) that $S^\phi = im(\psi)$ and $S^{\hat{\phi}} = im(\hat{\psi})$. Each step of the above involves only minor computations, such as checking the independence of sets of members of $\mathbb{Q}_p^*/(\mathbb{Q}_p^*)^2 \times \mathbb{Q}_p^*/(\mathbb{Q}_p^*)^2$.

2 Worked Examples

We give two examples which illustrate the method described in Section **1**, and which give applications of Coleman's result, Proposition 0.4.

Example 2.1. *The Jacobian of the curve:*

$$Y^2 = X(X^2-1)(X+\frac{1}{9})(X^2-4X-1)$$

has rank 1 over $\mathbb{Q}$*. Hence, by Proposition 0.4, there are no* $\mathbb{Q}$*-rational points on the curve apart from the points* $(0,0),(1,0),(-1,0),(-1/9,0)$ *and the 2 rational points at infinity.*

Proof. By the map $(X,Y) \mapsto ((1-X)/X, 3Y/X^3)$, the above curve is birationally equivalent to:

$$\mathcal{C} : Y^2 = X(X+2)(X+10)(X^2+6X+4)$$

where $q_1(X) = X$, $q_2(X) = (X+2)(X+10)$, $q_3(X) = X^2+6X+4$, $\Delta = -16$, $\hat{q}_1(X) = -6X^2-32X-72$, $\hat{q}_2(X) = X^2-4$ and $\hat{q}_3(X) = -X^2+20$, so that:

$$\widehat{\mathcal{C}} : (-16)Y^2 = (-6X^2-32X-72)(X^2-4)(-X^2+20).$$

The set of bad primes is $\mathcal{S} = \{2,5,11\}$, so that $\mathrm{im}(\psi)$ and $\mathrm{im}(\hat{\psi})$ are both subgroups of $\langle (-1,1),(2,1),(5,1),(11,1),(1,-1),(1,2),(1,5),(1,11)\rangle$. Taking images under ψ and $\hat{\psi}$:

$$\langle \hat{\alpha}_1 \rangle \xrightarrow{\psi} \langle (5,5) \rangle$$

$$\langle \alpha_1, \alpha_2, \{\infty,(-1,3)\}, \{(-2,0),(-1,3)\} \rangle \xrightarrow{\hat{\psi}} \langle (5,5),(5,-55),(-1,1),(2,2) \rangle.$$

Hence:

$$\langle (5,5) \rangle \leqslant im(\psi) \text{ and } \langle (5,5),(5,-55),(-1,1),(2,2) \rangle \leqslant im(\hat{\psi}) \qquad (2)$$

Over $\mathbb{Q}_2$, let $\gamma \in \mathbb{Z}_2$ be such that $\gamma^2 = -15$, $\gamma \equiv 1 \pmod 8$, and let $D = \{(6, 64\gamma), (2,0)\} \in \widehat{\mathcal{J}}(\mathbb{Q}_2)/\phi(\mathcal{J}(\mathbb{Q}_2)) \xrightarrow{\psi_2} (-5,5)$. Combining this with the known members of $im(\psi)$ and $im(\hat{\psi})$, we find that $(5,5),(-5,5) \in im(\psi_2)$ and $(5,5),(5,-55),(-1,1),(2,2) \in im(\hat{\psi}_2)$ give 2 linearly independent elements, and 4 linearly independent elements, respectively, in $\mathbb{Q}_2^*/(\mathbb{Q}_2^*)^2 \times \mathbb{Q}_2^*/(\mathbb{Q}_2^*)^2$. Since $\|\widehat{\mathcal{J}}(\mathbb{Q}_2)/\phi(\mathcal{J}(\mathbb{Q}_2))\| + \|\mathcal{J}(\mathbb{Q}_2)/\hat{\phi}(\widehat{\mathcal{J}}(\mathbb{Q}_2))\| = 6$, it follows that $\widehat{\mathcal{J}}(\mathbb{Q}_2)/\phi(\mathcal{J}(\mathbb{Q}_2)) = \langle \hat{\alpha}_1, D \rangle$ and $\mathcal{J}(\mathbb{Q}_2)/\hat{\phi}(\widehat{\mathcal{J}}(\mathbb{Q}_2)) = \langle \alpha_1, \alpha_2, \{\infty,(-1,3)\}, \{(-2,0),(-1,3)\} \rangle$. Further, $\mathbb{Q}(\mathcal{S}) \cap \left(\mathbb{Q}_2^*\right)^2 = \langle -55 \rangle$,

so that $\big(\mathbb{Q}(\mathcal{S}) \times \mathbb{Q}(\mathcal{S})\big) \cap ker(j_2) = \langle (-55,1),(1,-55)\rangle$. From the commutative diagram given in Lemma 1.3, we see:

$$\begin{aligned} &im(\psi) \leqslant \langle (5,5),(-5,5),(-55,1),(1,-55)\rangle. \\ &im(\hat{\psi}) \leqslant \langle (5,5),(5,-55),(-1,1),(2,2),(-55,1),(1,-55)\rangle. \end{aligned} \tag{3}$$

Over $\mathbb{Q}_5$, the two branches at infinity of $\widehat{\mathcal{C}}$, denoted ∞^+,∞^-, are rational. Let $E = \{\infty^+,(2,0)\} \in \widehat{\mathcal{J}}(\mathbb{Q}_5)/\phi(\mathcal{J}(\mathbb{Q}_5))$. It does not matter which branch at infinity we select; in either case we will have $E \xrightarrow{\psi_5} (10,10)$. Combining this with the known members of $im(\psi)$ and $im(\hat{\psi})$, we find that $(5,5),(10,10) \in im(\psi_5)$ and $(5,5),(2,2) \in im(\hat{\psi}_5)$ each give 2 linearly independent elements in $\mathbb{Q}_5^*/(\mathbb{Q}_5^*)^2 \times \mathbb{Q}_5^*/(\mathbb{Q}_5^*)^2$. Since $\|\widehat{\mathcal{J}}(\mathbb{Q}_5)/\phi(\mathcal{J}(\mathbb{Q}_5))\| + \|\mathcal{J}(\mathbb{Q}_5)/\hat{\phi}(\widehat{\mathcal{J}}(\mathbb{Q}_5))\| = 4$, it follows that $\widehat{\mathcal{J}}(\mathbb{Q}_5)/\phi(\mathcal{J}(\mathbb{Q}_5)) = \langle \hat{\alpha}_1, E\rangle$ and $\mathcal{J}(\mathbb{Q}_5)/\hat{\phi}(\widehat{\mathcal{J}}(\mathbb{Q}_5)) = \langle \alpha_1, \{(-2,0),(-1,3)\}\rangle$. Further, $\mathbb{Q}(\mathcal{S}) \cap \left(\mathbb{Q}_5^*\right)^2 = \langle -1, 11\rangle$, so that $\big(\mathbb{Q}(\mathcal{S}) \times \mathbb{Q}(\mathcal{S})\big) \cap ker(j_5) = \langle (-1,1),(11,1),(1,-1),(1,11)\rangle$. From the commutative diagram given in Lemma 1.3, we see:

$$\begin{aligned} &im(\psi) \leqslant \langle (5,5),(10,10),(-1,1),(11,1),(1,-1),(1,11)\rangle. \\ &im(\hat{\psi}) \leqslant \langle (5,5),(2,2),(-1,1),(11,1),(1,-1),(1,11)\rangle. \end{aligned} \tag{4}$$

Over $\mathbb{Q}_{11}$, let $\delta \in \mathbb{Q}_{11}$ be such that $\delta^2 = 20$ and $\delta \equiv 3 \pmod{11}$. Let $F = \{(2,0),(\delta,0)\} \in \widehat{\mathcal{J}}(\mathbb{Q}_{11})/\phi(\mathcal{J}(\mathbb{Q}_{11}))$. Then $F \xrightarrow{\psi_{11}} (1,-1)$. Combining this with the known members of $im(\psi)$ and $im(\hat{\psi})$, we find that $(1,-1) \in im(\psi_{11})$ and $(5,-55),(-1,1),(2,2) \in im(\hat{\psi}_{11})$ give 1 linearly independent element and 3 linearly independent elements, respectively, in $\mathbb{Q}_{11}^*/(\mathbb{Q}_{11}^*)^2 \times \mathbb{Q}_{11}^*/(\mathbb{Q}_{11}^*)^2$. Since $\|\widehat{\mathcal{J}}(\mathbb{Q}_{11})/\phi(\mathcal{J}(\mathbb{Q}_{11}))\| + \|\mathcal{J}(\mathbb{Q}_{11})/\hat{\phi}(\widehat{\mathcal{J}}(\mathbb{Q}_{11}))\| = 4$, it follows that $\widehat{\mathcal{J}}(\mathbb{Q}_{11})/\phi(\mathcal{J}(\mathbb{Q}_{11})) = \langle F\rangle$ and $\mathcal{J}(\mathbb{Q}_{11})/\hat{\phi}(\widehat{\mathcal{J}}(\mathbb{Q}_{11})) = \langle \alpha_2, \{\infty,(-1,3)\}, \{(-2,0),(-1,3)\}\rangle$. Further, $\mathbb{Q}(\mathcal{S}) \cap \left(\mathbb{Q}_{11}^*\right)^2 = \langle -2, 5\rangle$, so that $\big(\mathbb{Q}(\mathcal{S}) \times \mathbb{Q}(\mathcal{S})\big) \cap ker(j_{11}) = \langle (-2,1),(5,1),(1,-2),(1,5)\rangle$. From the commutative diagram given in Lemma 1.3, we see:

$$\begin{aligned} &im(\psi) \leqslant \langle (1,-1),(-2,1),(5,1),(1,-2),(1,5)\rangle. \\ &im(\hat{\psi}) \leqslant \langle (5,-55),(-1,1),(2,2),(-2,1),(5,1),(1,-2),(1,5)\rangle. \end{aligned} \tag{5}$$

Finally, over $\mathbb{R}$, we find that $(5,-55),(-1,1) \in im(\hat{\psi}_\infty)$ give 2 linearly independent elements in $\mathbb{R}^*/(\mathbb{R}^*)^2 \times \mathbb{R}^*/(\mathbb{R}^*)^2$. Since $\|\widehat{\mathcal{J}}(\mathbb{R})/\phi(\mathcal{J}(\mathbb{R}))\| + \|\mathcal{J}(\mathbb{R})/\hat{\phi}(\widehat{\mathcal{J}}(\mathbb{R}))\| = 2$, it follows that $\widehat{\mathcal{J}}(\mathbb{R})/\phi(\mathcal{J}(\mathbb{R}))$ is trivial, and $\mathcal{J}(\mathbb{R})/\hat{\phi}(\widehat{\mathcal{J}}(\mathbb{R})) = \langle \alpha_2, \{\infty,(-1,3)\}\rangle$. Further, $\mathbb{Q}(\mathcal{S}) \cap \left(\mathbb{R}^*\right)^2 = \langle 2, 5, 11\rangle$, so that $\big(\mathbb{Q}(\mathcal{S}) \times \mathbb{Q}(\mathcal{S})\big) \cap ker(j_\infty) = \langle (2,1),(5,1),(11,1),(1,2),(1,5),(1,11)\rangle$. This gives no new information about $im(\hat{\psi})$, but it does give:

$$im(\psi) \leqslant \langle (2,1),(5,1),(11,1),(1,2),(1,5),(1,11)\rangle. \tag{6}$$

Combining $(2),(3),(4),(5),(6)$ gives that $im\psi = S^{\phi} = \langle (5,5) \rangle$ and $im\hat{\psi} = S^{\hat{\phi}} = \langle (5,5),(5,-55),(-1,1),(2,2) \rangle$. In other words, the known points $\langle \hat{\alpha}_1 \rangle$ and $\langle \alpha_1, \alpha_2, \{\infty,(-1,3)\},\{(-2,0),(-1,3)\} \rangle$ generate $\widehat{\mathcal{J}}(\mathbb{Q})/\phi(\mathcal{J}(\mathbb{Q}))$ and $\mathcal{J}(\mathbb{Q})/\hat{\phi}(\widehat{\mathcal{J}}(\mathbb{Q}))$, respectively. It follows that $\mathcal{J}(\mathbb{Q})/2\mathcal{J}(\mathbb{Q}) = \langle \alpha_1, \alpha_2, \{\infty,(-1,3)\},\{(-2,0),(-1,3)\} \rangle$, which is the same as $\langle \alpha_1, \alpha_2, \{\infty,(-2,0)\},\{(-2,0),(-1,3)\} \rangle$. The first 3 of these generators are 2-torsion, and they generate the 2-torsion subgroup of $\mathcal{J}(\mathbb{Q})$ of size 8. The final generator $\{(-2,0),(-1,3)\}$ is easily shown to be non-torsion by a finite field reductions over $\mathbb{F}_3$. Hence, $\mathcal{J}(\mathbb{Q})$ has rank 1, as required. $\square$

The following example can also be shown in the same manner; indeed it is easier since the only bad primes are $2, 5$ and only arguments over $\mathbb{Q}_2$, $\mathbb{Q}_5$ and $\mathbb{R}$ are required.

Example 2.2. *The Jacobian of the curve:*

$$Y^2 = X(X^2-1)(X-\frac{1}{9})(X^2-18X+1)$$

has rank 1 over $\mathbb{Q}$*. Hence, by Proposition 0.4, there are no* $\mathbb{Q}$*-rational points on the curve apart from the points* $(0,0),(1,0),(-1,0),(1/9,0)$ *and the 2 rational points at infinity.*

Note, however, that this second example is special in that it has a non-simple jacobian. By the transformation $X \mapsto 1/X$, $Y \mapsto 3Y/X^3$, the curve is birationally equivalent to: $Y^2 = (X-9)(X^2-1)(X^2-18X+1)$ which in turn has a non-hyperelliptic involution, given by $x \mapsto (x-17)/(x-1)$, and $y \mapsto 64iy/(x-1)^3$, defined over $\mathbb{Q}(i)$. Therefore the jacobian is isogenous to the product of two conjugate elliptic curves, defined over $\mathbb{Q}(i)$. The equations of these are $y^2 = (x-1)(x+9)(x+(4+i)^2)$ and its conjugate, each of which has rational modular invariant. The rank of the jacobian of the curve of genus 2 in Example 2.2 over $\mathbb{Q}$ is equal to the rank of either one of these two elliptic curves over $\mathbb{Q}(i)$ (namely rank 1), which would be an alternative approach to this example.

References

1. Bost, J. B. and Mestre, J.-F.: Moyenne arithmético-géometrique et périodes des courbes de genre 1 et 2. Gaz. Math. Soc. France, **38,** 36-64 (1988).
2. Cassels, J. W. S.: The Mordell-Weil Group of Curves of Genus 2. Arithmetic and Geometry papers dedicated to I. R. Shafarevich on the occasion of his sixtieth birthday, **1.** Arithmetic, 29-60, Birkhäuser, Boston (1983).

3. Chabauty C.: Sur les points rationnels des courbes algébriques de genre supérieur à l'unité. Comptes Rendus Hebdomadaires des Séances de l'Academie des Sciences, Paris **212**, 882–885 (1941).
4. Coleman, R. F.: Effective Chabauty. Duke Math. J. **52**, 765-780 (1985).
5. Flynn, E. V.: The group law on the Jacobian of a curve of genus 2. J. Reine Angew. Math. **438**, 45-69 (1993).
6. Flynn, E. V.: Descent via isogeny on the Jacobian of a curve of genus 2. Acta Arith. **LXVI.1**, 23-43 (1994).
7. Gordon, D.M. and Grant, D.: Computing the Mordell-Weil rank of Jacobians of curves of genus 2. Transactions of the American Mathematical Society, **337**, Number 2, 807-824 (1993).
8. Grant, D.: A curve for which Coleman's Chabauty bound is sharp. Preprint, 1991.
9. Mattuck, A.: Abelian varieties over p-adic ground fields. Ann. of Math. **62**, 92-119 (1955).
10. McCallum, W.G.: The Arithmetic of Fermat Curves. Math. Ann. **294**, 503-511 (1992).
11. Schaefer, E.F.: 2-descent on the Jacobians of hyperelliptic curves. J. Number Theory. **51** 219-232 (1995).