Research in Number Theory

RESEARCH

Explicit two-cover descent for genus 2 curves

Daniel Rayor Hast

*Correspondence:
drhast@bu.edu
Department of Mathematics and Statistics, Boston University, 111 Cummington Mall, Boston, MA 02215, USA

Abstract

Given a genus 2 curve C with a rational Weierstrass point defined over a number field, we construct a family of genus 5 curves that realize descent by maximal unramified abelian two-covers of C, and describe explicit models of the isogeny classes of their Jacobians as restrictions of scalars of elliptic curves. All the constructions of this paper are accompanied by explicit formulas and implemented in Magma and/or SageMath. We apply these algorithms in combination with elliptic Chabauty to a dataset of 7692 genus 2 quintic curves over $\mathbb{Q}$ of Mordell–Weil rank 2 or 3 whose sets of rational points have not previously been provably computed. We analyze how often this method succeeds in computing the set of rational points and what obstacles lead it to fail in some cases.

Keywords: Rational points on curves, Chabauty's method, Étale descent

Mathematics Subject Classification: 11G30, 14G05, 11Y50

1 Introduction

Let C be a nice (smooth, projective, geometrically integral) curve over a number field k. A central problem in arithmetic geometry is to determine the set of rational points $C(k)$. When C is of genus at least two, by Faltings' theorem, $C(k)$ is a finite set [13,14]; however, no general algorithm for provably computing $C(k)$ is currently known. (See [30] for an overview.)

One common strategy for computing $C(k)$ is *descent*, which involves finding a family of curves D_δ (with δ ranging over some computable finite set) together with maps $\varphi_\delta : D_\delta \to C$ with the property that $C(k) \subseteq \bigcup_\delta \varphi_\delta(D_\delta(k))$. In many cases, one can construct such families so that the covering curves D_δ are amenable to other techniques for determining the set of rational points that might not apply directly to C.

In this paper, we make explicit a particular descent construction for curves of genus two with a rational Weierstrass point. All the constructions involved are implemented in Magma [4] and/or SageMath [32]; source code is available online at [22]. We then apply these algorithms to all 7692 genus 2 curves over $\mathbb{Q}$ with a rational Weierstrass point and Mordell–Weil rank 2 or 3 in the database of genus 2 genus computed by Booker, Sijsling, Sutherland, Voight, and Yasaki [3] (available at [25]) and analyze the results.

The general strategy is inspired by prior work of Bruin, Flynn, Stoll, and Wetherell computing rational points on curves using explicit descent constructions; see, for example, [6,8,16,17]. The constructions of this paper are closely related to those of Bruin and Stoll [9] for two-cover descent on arbitrary hyperelliptic curves $C\colon y^2 = f(x)$; we construct genus 5 quotients of their two-covering curves along with explicit formulas (as a restriction of scalars of an elliptic curve) for a model of the isogeny class of the Jacobian of these quotients. The elliptic curves constructed in this way are isomorphic to those arising from degree four factors of f as discussed in [9, Sect. 8].

From now on, suppose C is of genus 2 and has a k-rational Weierstrass point. Then C has an affine model given by an equation $y^2 = f(x)$, where f has degree exactly 6, is squarefree, and has a rational root α. Thus, elements of $C(k)$ correspond to solutions in k to the equation $y^2 = f(x)$, with the possible addition of two rational points at infinity that are excluded from the affine model. (More precisely, C has two points at infinity, and these points are rational if and only if the leading coefficient of f is a square in k.)

Let $J = \mathrm{Jac}(C)$ be the Jacobian variety of C. This is an abelian surface whose points correspond to degree zero divisors on C modulo linear equivalence. Embed C in J by the Abel–Jacobi map $P \mapsto (P) - ((\alpha, 0))$ associated to the given Weierstrass point $(\alpha, 0)$. Since the chosen base point is a Weierstrass point, multiplication by -1 on J induces the hyperelliptic involution $i\colon C \to C$.

A natural 16-covering of C is given by pullback along $[2]\colon J \to J$, where $[2]$ is multiplication by 2 in J: Let $W = [2]^{-1}(C)$. Then $[2]\colon W \to C$ is a degree 16 étale covering, so by the Riemann–Hurwitz formula [20, Ch. IV, Cor. 2.4], the curve W has genus 17. In order to compute $C(k)$ via descent using this covering, we would need to do the following:

1. compute a finite set of twists $\varphi_\delta\colon W_\delta \to C$ such that $C(k) \subseteq \bigcup_\delta \varphi_\delta(W_\delta(k))$; and
2. compute $W_\delta(k)$ for each twist W_δ.

To make the computations more tractable, it is useful to work instead with a suitable quotient of W. Since multiplication by -1 on J induces the hyperelliptic involution on C, we can lift the hyperelliptic involution to an involution on W. Let Z be the quotient of W by this involution. The map $W \to Z$ is ramified exactly at the 2-torsion points of J, of which there are 16, so Z has genus 5 by the Riemann–Hurwitz formula. (Another model for this curve can be constructed using the methods of [6, Sect. 3.1]; we choose this approach to emphasize the connection with Kummer surfaces.)

The purpose of this paper is to give explicit, computationally tractable formulas for Z and its Jacobian (and their twists), along with the associated maps realizing the correspondence with C; to apply these constructions in combination with the elliptic Chabauty method to the aforementioned large dataset of curves; and to determine what the obstructions are in the cases where it does not succeed. The key ingredient is to embed (twists of) Z in (twists of) the desingularized Kummer surface of J. Our primary references for the requisite explicit descriptions of Kummer surfaces and their twists are [10,15].

In Sect. 2, we provide the necessary background on desingularized twisted Kummer surfaces, construct the canonical embedding of Z and its twists as hyperplane sections of these surfaces, and describe the primes of bad reduction. In Sect. 3, we prove an explicit formula for the twisted duplication map and describe its ramification divisor. In Sect. 4, we construct a map to a genus one curve through which the twisted duplication map factors, which supplies the necessary data to apply the elliptic Chabauty method [7]; we also use this to give an explicit model for the Jacobian of Z up to isogeny. In Sect. 5, we report on the results of applying this method to the aforementioned dataset of 7692 curves; the method succeeds for 1045 of these curves, and we analyze the obstacles encountered for the remaining curves. Finally, in Sect. 6, we analyze the method and results in detail for several examples.

2 Genus 5 curves in twisted Kummer surfaces

Let k be a field not of characteristic 2. Let $C\colon y^2 = f(x)$ be a genus 2 curve over k with $\deg(f) = 6$ such that C has a k-rational Weierstrass point $(\alpha, 0)$. (Although such a curve does have a quintic model over k, we work with sextic models in order to use the explicit description of desingularized twisted Kummer surfaces outlined below.) Let $i\colon C \to \mathbf{P}^1$ be the canonical map. Let $f_0, f_1, \ldots, f_6 \in k$ and $\gamma_1, \gamma_2, \ldots, \gamma_6 \in k$ such that

$$f(x) = \sum_{i=0}^{6} f_i x^i = (x-\alpha)(\gamma_1 + \gamma_2 x + \cdots + \gamma_6 x^5).$$

Let J be the Jacobian variety of C. Let $L = k[X]/\langle f(X)\rangle$, and let $\delta = \sum_{i=0}^{5} d_i X^i \in L^*$ be arbitrary. When k is a global or local field, Flynn, Testa, and van Luijk [15, Sect. 7] construct a twist $\pi_\delta\colon A_\delta \to J$ of the multiplication-by-2 map $[2]\colon J \to J$, depending up to isomorphism only on the class of δ in $L^*/L^{*2}k^*$, whose class in $H^1(k, J[2])$ maps to δ under the Cassels map $\mu\colon J(k)/2J(k) \to L^*/L^{*2}k^*$. They also show that every two-covering of J that has a k-rational point arises in this way [15, Prop. 2.15], and so if $\Delta \subseteq L^*$ is any subset whose image in $L^*/L^{*2}k^*$ contains the image of the Cassels map μ, we have

$$J(k) = \bigcup_{\delta\in\Delta} \pi_\delta(A_\delta(k)).$$

Each surface A_δ is equipped with a natural involution $\iota_\delta\colon A_\delta \to A_\delta$ lifting $[-1]\colon J \to J$. The (twisted) Kummer surfaces $\mathcal{K}_\delta = A_\delta/\langle\iota_\delta\rangle$ have 16 simple nodes. For computational purposes, it turns out to be more convenient to work with their minimal desingularizations $\mathcal{Y}_\delta$. Let $p_\delta\colon A_\delta \dashrightarrow \mathcal{Y}_\delta$ be the rational quotient map. Let $W_\delta = \pi_\delta^{-1}(C)$, where we embed C in J by the Abel–Jacobi map $P \mapsto (P) - ((\alpha, 0))$. By the Riemann–Hurwitz formula, W_δ has genus 17. Let

$$Z_\delta = p_\delta(W_\delta),$$

and let

$$\bar{\pi}_\delta\colon Z_\delta \to \mathbf{P}^1$$

be the map defined by sending a general point $Q \in Z_\delta$ to $i(\pi_\delta(\tilde{Q}))$, where $\tilde{Q} \in A_\delta$ is such that $p_\delta(\tilde{Q}) = Q$. (Since C is embedded in J via an Abel–Jacobi map whose base point is a Weierstrass point, the hyperelliptic involution on C lifts to ι_δ on A_δ, so this is well-defined.)

Thus Z_δ fits into a commutative diagram

$$\begin{tikzcd}
& W_\delta \arrow[dl, "p_\delta"'] \arrow[dr, "\pi_\delta"] & & & & A_\delta \arrow[dl, dashed, "p_\delta"'] \arrow[dr, "\pi_\delta"] & \\
Z_\delta \arrow[dr, "\bar{\pi}_\delta"'] & & C \arrow[dl, "i"] & & \mathcal{Y}_\delta \arrow[dr, "\bar{\pi}_\delta"'] & & J \arrow[dl] \\
& \mathbf{P}^1 & & & & \mathcal{K} &
\end{tikzcd} \qquad (2.1)$$

where each curve in the left diagram embeds into the corresponding surface in the right diagram, and $\mathcal{K} = J/[-1]$ is the Kummer surface of J.

We reproduce here the model of $\mathcal{Y}_\delta$ constructed in [15, Sect. 4] as the complete intersection of three quadrics in $\mathbf{P}^5 = \mathbf{P}(L)$ (recall that $L = k[X]/\langle f(X)\rangle$), which we have implemented in both SageMath and Magma.

Definition 2.1 Write $f(X) = \sum_{i=0}^{6} f_i X^i$ and $\delta = \sum_{i=0}^{5} d_i X^i \in L$. Let

$$R = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & -f_0 f_6^{-1} \\ 1 & 0 & 0 & 0 & 0 & -f_1 f_6^{-1} \\ 0 & 1 & 0 & 0 & 0 & -f_2 f_6^{-1} \\ 0 & 0 & 1 & 0 & 0 & -f_3 f_6^{-1} \\ 0 & 0 & 0 & 1 & 0 & -f_4 f_6^{-1} \\ 0 & 0 & 0 & 0 & 1 & -f_5 f_6^{-1} \end{pmatrix} \quad \text{and} \quad T = \begin{pmatrix} f_1 & f_2 & f_3 & f_4 & f_5 & f_6 \\ f_2 & f_3 & f_4 & f_5 & f_6 & 0 \\ f_3 & f_4 & f_5 & f_6 & 0 & 0 \\ f_4 & f_5 & f_6 & 0 & 0 & 0 \\ f_5 & f_6 & 0 & 0 & 0 & 0 \\ f_6 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}.$$

Let $g_1, \ldots, g_6$ be the basis of L defined by

$$\begin{aligned} g_1 &= f_1 + f_2 X + f_3 X^2 + f_4 X^3 + f_5 X^4 + f_6 X^5, \\ g_2 &= f_2 + f_3 X + f_4 X^2 + f_5 X^3 + f_6 X^4, \\ g_3 &= f_3 + f_4 X + f_5 X^2 + f_6 X^3, \\ g_4 &= f_4 + f_5 X + f_6 X^2, \\ g_5 &= f_5 + f_6 X, \\ g_6 &= f_6, \end{aligned}$$

and let $v_1, \ldots, v_6$ be the dual basis of $\hat{L}$. For $j \geq 0$, let $Q_j^{(\delta)}$ be the quadratic form corresponding to the symmetric matrix $\sum_{i=0}^{5} f_6 d_i R^{i+j} T$ in the basis $v_1, \ldots, v_6$. Let $\mathcal{Y}_\delta \subset \mathbf{P}(L)$ be defined by

$$Q_0^{(\delta)} = Q_1^{(\delta)} = Q_2^{(\delta)} = 0.$$

Flynn, Testa, and van Luijk show that $\mathcal{Y}_\delta$ is indeed the minimal desingularization of $\mathcal{K}_\delta$ [15, Sect. 7].

Theorem 2.2 *Let* $\mathrm{ev}_\alpha : L \to k$ *be the homomorphism defined by* $\mathrm{ev}_\alpha(\xi) = \xi(\alpha)$. *The curve* Z_δ *is the intersection of* $\mathcal{Y}_\delta$ *with the hyperplane* $\mathbf{P}(\ker(\mathrm{ev}_\alpha)) \subset \mathbf{P}(L)$, *which is given in coordinates by*

$$\gamma_1 v_1 + \gamma_2 v_2 + \gamma_3 v_3 + \gamma_4 v_4 + \gamma_5 v_5 + \gamma_6 v_6 = 0,$$

where as above, $\gamma_1, \ldots, \gamma_6$ *are the coefficients of* $f(x)/(x - \alpha)$.

Proof Note that ev_α is well-defined since $f(\alpha) = 0$. The first step is to understand how the base $\mathbf{P}^1$ embeds into $\mathcal{K}$. Recall that a *trope* of a quartic surface $\mathcal{K} \subset \mathbf{P}^3$ is a tangent plane that intersects the surface at a conic (with multiplicity two). A Kummer surface has exactly 16 tropes, which are the projective duals of the 16 nodes [10, Sect. 3.7] [23, Sects. 8–9].

The description of six of the tropes of the Kummer surface given in [10, Sect. 7.6] shows that the image of $\mathbf{P}^1$ in $\mathcal{K}$ corresponding to the Abel–Jacobi map with base point $(\alpha, 0)$ is contained in the trope T_α with equation $\alpha^2\kappa_1 - \alpha\kappa_2 + \kappa_3 = 0$, where $\kappa_1, \kappa_2, \kappa_3, \kappa_4$ are the coordinates of the usual embedding of $\mathcal{K}$ as a quartic surface in $\mathbf{P}^3$ (as described in [10, Sect. 3.1], using the letters ξ_i instead of κ_i). (Strictly speaking, T_α intersects $\mathcal{K}$ in *twice* the conic corresponding to the base $\mathbf{P}^1$; we also denote this conic by T_α.)

Instead of constructing Z_δ as the quotient of a genus 17 curve embedded in J, we compute Z_δ using maps between the twisted Kummer surfaces. The preimage of T_α under the map $\bar{\pi}_\delta \colon \mathcal{Y}_\delta \to \mathcal{K}$ also contains some exceptional divisors, which we wish to omit when constructing Z_δ, so we instead consider the condition for a *general* element of $\mathcal{Y}_\delta$ to map to T_α via the map $\bar{\pi}_\delta$.

Let $P \in \mathcal{Y}_\delta$ be an arbitrary point not contained in the locus of indeterminacy of the rational map $p_\delta \colon A_\delta \dashrightarrow \mathcal{Y}_\delta$. Let $\xi \in L$ be an arbitrary lift of P from $\mathbf{P}(L)$ to L. We will show that $\bar{\pi}_\delta(P) \in T_\alpha$ if and only if $\xi(\alpha) = 0$.

We first treat the untwisted case $\delta = 1$. Let $D = ((x_1, y_1)) + ((x_2, y_2)) - K_C$ such that $p_1([D]) = [\pm D] = P$. As explained in the paragraph preceding [15, Prop. 4.11], the x-coordinates of the points R_1 and R_2 such that $2D \sim R_1 + R_2 - K_C$ are the roots of the quadratic polynomial $H(X)$ corresponding to ξ^2. (This does not depend on the choice of lift $\xi \in L$ since choosing a different lift multiplies H by an element of k^*, which does not change the roots.) The condition that $\pm 2D$ is contained in T_α is exactly that one of the x-coordinates of R_1 and R_2 is α, i.e., that α is a root of H, or equivalently, that $\xi^2(\alpha) = 0$, which is the case if and only if $\xi(\alpha) = 0$.

Now we handle the twisted case. Let $D = ((x_1, y_1)) + ((x_2, y_2)) - K_C$ such that $p_\delta([D]) = P$. Let k^s be a separable closure of k, let $L^s = L \otimes_k k^s$, and let $\varepsilon \in L^s$ such that $\varepsilon^2 = \delta$. Then $\delta\xi^2 = (\varepsilon\xi)^2$, so $\varepsilon\xi \in \mathcal{Y}_1$. Let $D' \in J$ such that the image of D' in $\mathcal{Y}_1$ is $\varepsilon\xi$. By [15, Sect. 7], we have $\bar{\pi}_\delta = [2] \circ g$, where g is defined by multiplication by ε in L. So

$$\bar{\pi}_\delta(\xi) = \bar{\pi}_\delta(g^{-1}(\varepsilon\xi)) = [2](\varepsilon\xi),$$

and lifting to the Jacobian, the divisor class corresponding to $\bar{\pi}_\delta(\xi)$ is equal to $[2D']$, i.e., $\pi_\delta([D]) = [2D']$. As in the previous paragraph, the roots r_1, r_2 of the quadratic polynomial H such that $\delta\xi^2 \equiv H \pmod{f}$ are the x-coordinates of points $R_1, R_2 \in C$ such that $(R_1) + (R_2) - K_C \sim 2D'$. Thus, $\bar{\pi}_\delta(P) \in T_\alpha$ if and only if α is a root of H, which is equivalent to $\delta(\alpha)\xi^2(\alpha) = 0$. Since $\delta \in L^*$, we have $\delta(\alpha) \neq 0$, so this is equivalent to $\xi(\alpha) = 0$.

Represent ξ in the basis $g_1, \dots, g_6$ as $\xi = \sum_{i=1}^{6} v_i(\xi) g_i$. Then

$$\xi(\alpha) = \sum_{i=1}^{6} g_i(\alpha) v_i(\xi),$$

so in the basis $v_1, \dots, v_6$, the condition $\xi(\alpha) = 0$ becomes

$$g_1(\alpha)v_1 + g_2(\alpha)v_2 + g_3(\alpha)v_3 + g_4(\alpha)v_4 + g_5(\alpha)v_5 + g_6(\alpha)v_6 = 0.$$

It follows immediately from the definitions of $g_1, \dots, g_6$ that

$$f(x) = (x - \alpha)(g_1(\alpha) + g_2(\alpha)x + g_3(\alpha)x^2 + g_4(\alpha)x^3 + g_5(\alpha)x^4 + g_6(\alpha)x^5),$$

i.e., $\gamma_i = g_i(\alpha)$ for each $i \in \{1, \dots, 6\}$, so Z_δ is in fact the hyperplane section of $\mathcal{Y}_\delta$ whose coefficients in the basis $v_1, \dots, v_6$ are the coefficients of the polynomial $f(x)/(x - \alpha)$. □

Proposition 2.3 *The curve Z_δ is smooth, has genus 5, and is canonically embedded in* $\mathbf{P}(\ker(\mathrm{ev}_\alpha)) \cong \mathbf{P}^4$.

Proof Let $q_\delta\colon A_\delta \to \mathcal{K}_\delta$ be the quotient map. The ramification divisor of q_δ is $\pi_\delta^{-1}(0)$. At each point $P \in \pi_\delta^{-1}(0)$, since q_δ has degree 2, the point $q_\delta(P)$ is either nonsingular or a simple node. The map $\mathcal{Y}_\delta \to \mathcal{K}_\delta$ is given by blowing up at $q_\delta(\pi_\delta^{-1}(0))$, which desingularizes any simple nodes, so Z_δ (being the proper transform of $q_\delta(W_\delta)$) is smooth.

By Theorem 2.2, the curve Z_δ is a complete intersection of three quadrics in $\mathbf{P}^4$, so Z_δ is a canonical curve of genus 5 (cf. [20, Ch. IV, Ex. 5.5.3]). □

Proposition 2.4 *Suppose that k is a local field with residue field $\mathbb{F}_q$, and that C/k has good reduction. If q is odd, then Z_δ also has good reduction.*

Proof Write $q = p^n$, where p is an odd prime. By [19, Exposé X, Cor. 3.9], specialization to $\mathbb{F}_q$ induces an isomorphism between the prime-to-p parts of the étale fundamental groups of C and the special fiber $\bar{C}/\mathbb{F}_q$. Thus W_δ, being a degree 16 étale cover of C, also has good reduction. Euler characteristic (and hence also arithmetic genus) are locally constant in proper flat families [28, Sect. 5, Cor. 1], so Proposition 2.3 implies that the special fiber $\bar{Z}_\delta/\mathbb{F}_q$ has arithmetic genus 5, hence geometric genus at most 5. Since p is odd, the quotient map $\bar{W}_\delta \to \bar{Z}_\delta$ is tamely ramified, so the Riemann–Hurwitz formula implies that $\bar{Z}_\delta$ has geometric genus exactly 5 and thus is smooth over $\mathbb{F}_q$. □

3 The twisted duplication map

In this section, we give explicit formulas for the map $\bar{\pi}_\delta\colon Z_\delta \to \mathbf{P}^1$ induced by the twisted duplication map. We also give an explicit description of the ramification divisor of this map.

Theorem 3.1 *For all $P \in Z_\delta$, we have*

$$\bar{\pi}_\delta(P) = \left(-(f_5 + f_6\alpha)Q_3^{(\delta)}(P) - f_6 Q_4^{(\delta)}(P) : f_6 Q_3^{(\delta)}(P)\right) \in \mathbf{P}^1.$$

Proof As in [15, Sect. 4], let $C_0^{(\delta)}, \ldots, C_5^{(\delta)} \in \mathrm{Sym}^2(\hat{L})$ be quadratic forms such that $C_j^{(\delta)}(z) = p_j(\delta z^2)$ for $z \in L$, where p_j gives the coefficient of X^j. We have

$$f_6 \cdot \left(C_0^{(\delta)}\ C_1^{(\delta)}\ \ldots\ C_5^{(\delta)}\right) = \left(Q_0^{(\delta)}\ Q_1^{(\delta)}\ \ldots\ Q_5^{(\delta)}\right) \cdot T,$$

where T is the matrix defined in Definition 2.1, so that in particular

$$\begin{aligned} f_6 C_1^{(\delta)} &= f_2 Q_0^{(\delta)} + f_3 Q_1^{(\delta)} + f_4 Q_2^{(\delta)} + f_5 Q_3^{(\delta)} + f_6 Q_4^{(\delta)}, \\ f_6 C_2^{(\delta)} &= f_3 Q_0^{(\delta)} + f_4 Q_1^{(\delta)} + f_5 Q_2^{(\delta)} + f_6 Q_3^{(\delta)}. \end{aligned}$$

Thus, taking into account that $Q_j^{(\delta)}$ vanishes on $\mathcal{Y}_\delta$ for $j \in \{0, 1, 2\}$, we have

$$(-(f_5 + f_6\alpha)Q_3^{(\delta)}(P) - f_6 Q_4^{(\delta)}(P) : f_6 Q_3^{(\delta)}(P)) = (-C_1^{(\delta)}(P) - \alpha C_2^{(\delta)}(P) : C_2^{(\delta)}(P)).$$

Moreover, $C_3^{(\delta)} = C_4^{(\delta)} = C_5^{(\delta)} = 0$ on $\mathcal{Y}_\delta$.

Let $\xi \in L$ be a lift of $P \in Z_\delta \subset \mathbf{P}(L)$. By construction of $\mathcal{Y}_\delta$, we have

$$\delta\xi^2 \equiv C_2^{(\delta)}(\xi)X^2 + C_1^{(\delta)}(\xi)X + C_0^{(\delta)}(\xi) \pmod{f}.$$

As explained in the proof of Theorem 2.2, the roots of this quadratic polynomial are the x-coordinates of points of the divisor in J corresponding to $\bar{\pi}_\delta(P)$. Moreover, since $P \in Z_\delta$, one of these roots is α. Thus, in the affine patch where the second coordinate of $\mathbf{P}^1$ is nonzero, writing $\bar{\pi}_\delta(P) = (r : 1)$, we have

$$C_2^{(\delta)}(\xi)X^2 + C_1^{(\delta)}(\xi)X + C_0^{(\delta)}(\xi) = c(X - \alpha)(X - r)$$

for some nonzero $c \in k^s$. Comparing coefficients, we obtain $C_2^{(\delta)}(\xi) = c$ and $C_1^{(\delta)}(\xi) = -c(\alpha + r)$, so

$$r = \frac{-C_1^{(\delta)}(\xi) - \alpha C_2^{(\delta)}(\xi)}{C_2^{(\delta)}(\xi)}.$$

This gives the desired formula for $\bar{\pi}_\delta(P)$. Finally, we have $\bar{\pi}_\delta(P) = (1 : 0)$ if and only if $C_2^{(\delta)}(\xi) = 0$, completing the proof. □

Theorem 3.2 *Let $\Omega \subset k^s$ be the set of roots of f. The branch locus of $\bar{\pi}_\delta \colon Z_\delta \to \mathbf{P}^1$ is $\Omega \setminus \{\alpha\}$. For each $\omega \in \Omega \setminus \{\alpha\}$, we have*

$$\bar{\pi}_\delta^{-1}(\omega) = Z_\delta \cap \mathbf{P}(\ker(\mathrm{ev}_\omega)) \subset \mathbf{P}(L),$$

which consists of 8 geometric points, each of ramification index 2.

Proof Observe that $\pi_\delta \colon W_\delta \to C$ is étale, the branch locus of $i \colon C \to \mathbf{P}^1$ is Ω, and the branch locus of $p_\delta \colon W_\delta \to Z_\delta$ is $\bar{\pi}_\delta^{-1}(\alpha)$, with all ramification indices in the preimage of the branch locus equal to 2. Thus, commutativity of diagram (2.1) implies that the branch locus of $\bar{\pi}_\delta$ is $\Omega \setminus \{\alpha\}$, and for each $\omega \in \Omega \setminus \{\alpha\}$, the preimage $\bar{\pi}_\delta^{-1}(\omega)$ consists of 8 geometric points of ramification index 2.

The remaining claim that $\bar{\pi}_\delta^{-1}(\omega)$ is the hyperplane section of Z_δ given by intersection with $\mathbf{P}(\ker(\mathrm{ev}_\omega))$ follows from the description of $\bar{\pi}_\delta$ given in the proofs of Theorems 2.2 and 3.1: For $\xi \in L$ lifting a point $P \in Z_\delta$, we have $\bar{\pi}_\delta(P) = (\omega : 1)$ if and only if the quadratic polynomial defining $\delta\xi^2$ has roots α and ω, which is equivalent to the condition $\xi(\alpha) = \xi(\omega) = 0$, i.e., P is in the kernel of both the evaluation maps ev_α (which defines Z_δ as a hyperplane section of $\mathcal{Y}_\delta$) and ev_ω, as was to be shown. □

4 Maps to genus one curves

We now construct a map to a genus one curve through which the twisted duplication map factors, and prove that this map induces an isogeny from the Jacobian of Z_δ to the restriction of scalars of the Jacobian of this genus one curve. These genus one curves are geometrically Prym varieties [2, Ch. 12] associated to double coverings of C. This is a substantial motivation for the constructions of this paper, since a restriction of scalars of an elliptic curve is much more computationally accessible than a general Jacobian variety of the same dimension.

Theorem 4.1 *Let $K = k(\omega)$, where $\omega \in k^s$ is a root of f and $\omega \neq \alpha$. Write $f(x) = (x-\alpha)(x-\omega)h(x)$, let $H(x, z)$ be the homogenization of $h(x)$ with respect to z, and let $\beta_1, \beta_2, \beta_3, \beta_4 \in k^s$ be the roots of h. Let $Y_{\alpha,\omega} = \mathrm{ev}_{\beta_1} \cdot \mathrm{ev}_{\beta_2} \cdot \mathrm{ev}_{\beta_3} \cdot \mathrm{ev}_{\beta_4}$, where $\mathrm{ev}_{\beta_j} = \sum_{i=1}^6 g_i(\beta_j)v_i$ is given by evaluation at β_j. (Note that $Y_{\alpha,\omega}$ is a quartic form over K.)*

Define a curve $D_{\delta,\omega} \subset \mathbf{P}(1, 2, 1)$ in weighted projective space by the equation

$$Y_{\alpha,\omega}(\delta)y^2 = h(\alpha)H(x, z).$$

Define a map $\varphi\colon Z_\delta \to \mathbf{P}(1,2,1)$ *over* K *by*

$$\varphi(P) = \left(-(f_5 + f_6\alpha)Q_3^{(\delta)}(P) - f_6 Q_4^{(\delta)}(P) : f_6^3 Y_{\alpha,\omega}(P) : f_6 Q_3^{(\delta)}(P)\right).$$

Then the image of φ *is* $D_{\delta,\omega}$, *and the following diagram commutes:*

$$\begin{tikzcd}
Z_\delta \arrow[r, "\varphi"] \arrow[dr, "\bar{\pi}_\delta"'] & D_{\delta,\omega} \arrow[d, "x"] \\
& \mathbf{P}^1
\end{tikzcd}$$

Proof Since ev_{β_j} is a ring homomorphism for each j, the quartic form $Y_{\alpha,\omega}$ is multiplicative with respect to L, i.e., $Y_{\alpha,\omega}(\xi\eta) = Y_{\alpha,\omega}(\xi)Y_{\alpha,\omega}(\eta)$ for all $\xi, \eta \in L$. As proved in Theorem 3.1, for all $\xi \in L^s$ lifting a point $P \in Z_\delta(k^s)$, we have

$$f_6\delta\xi^2 = (X - \alpha)\left(f_6 Q_3^{(\delta)}(\xi)X + (f_5 + f_6\alpha)Q_3^{(\delta)}(\xi) + f_6 Q_4^{(\delta)}(\xi)\right).$$

Putting these together, we obtain

$$\begin{aligned}
Y_{\alpha,\omega}(\delta)(f_6^3 Y_{\alpha,\omega}(\xi))^2 &= f_6^6 Y_{\alpha,\omega}(\delta\xi^2) = f_6^2 Y_{\alpha,\omega}(f_6\delta\xi^2) \\
&= f_6 \prod_{j=1}^{4}(\beta_j - \alpha) \cdot f_6 \prod_{j=1}^{4}\left(f_6 Q_3^{(\delta)}(\xi)\beta_j + (f_5 + f_6\alpha)Q_3^{(\delta)}(\xi) + f_6 Q_4^{(\delta)}(\xi)\right) \\
&= h(\alpha)H(-(f_5 + f_6\alpha)Q_3^{(\delta)}(\xi) - f_6 Q_4^{(\delta)}(\xi), f_6 Q_3^{(\delta)}(\xi)).
\end{aligned}$$

Thus $\varphi(Z_\delta) \subseteq D_{\delta,\omega}$. Since φ is non-constant and $D_{\delta,\omega}$ is an irreducible curve, $\varphi(Z_\delta) = D_{\delta,\omega}$. Commutativity of the diagram is immediate from the formulas. □

Remark 4.2 Theorem 3.2 gives another perspective on Theorem 4.1 in terms of divisors: Denote $\varphi = (\varphi_x : \varphi_y : \varphi_z)$. By Theorem 3.2, for each root β of h,

$$\bar{\pi}_\delta^*((\beta) - (\infty)) = \mathrm{div}(\mathrm{ev}_\beta^2 / \varphi_z).$$

Consider the rational functions $R = \varphi_x/\varphi_z$ and $S = \varphi_y/\varphi_z^2$. Then

$$\mathrm{div}(h \circ R) = \bar{\pi}_\delta^*(\mathrm{div}(h)) = \bar{\pi}_\delta^*((\beta_1) + (\beta_2) + (\beta_3) + (\beta_4) - 4(\infty)) = \mathrm{div}(S^2).$$

So S^2 is a scalar multiple of $h \circ R$; comparing their values at any point outside the divisor of zeroes and poles yields Theorem 4.1. (This is how the author initially discovered the formulas.)

Remark 4.3 If $D_{\delta,\omega}(K)$ is empty, then so is $Z_\delta(K)$. If $D_{\delta,\omega}(K)$ is nonempty, then $D_{\delta,\omega}$ is isomorphic to an elliptic curve $E_\delta = \mathrm{Jac}(D_{\delta,\omega})$ over K. In the latter case, if $k = \mathbb{Q}$, then Theorem 4.1 provides exactly the requisite data to compute $Z_\delta(\mathbb{Q})$ using the elliptic Chabauty method, provided that we can compute generators for the Mordell–Weil group $E_\delta(K)$ and that the rank of $E_\delta(K)$ is less than $[K : \mathbb{Q}]$.

One can find an upper bound on the rank of $E_\delta(K)$ by computing the 2-Selmer group (and this is the method we use in the examples of the next section). This requires computing the class group of $K[x]/\langle\eta_\delta(x)\rangle$, where we write $E_\delta\colon y^2 = \eta_\delta(x)$. This is often computationally expensive unless we assume Bach's bound [1] on the norm of prime ideals needed to generate the class group, which is conditional on the generalized Riemann hypothesis (GRH). However, since varying δ only changes $D_{\delta,\omega}$ by a quadratic twist, the elliptic curves E_δ also only differ by a quadratic twist, so the quotient algebra $K[x]/\langle\eta_\delta(x)\rangle$ does not depend on δ. Thus, the expensive class group computation need only be carried out once for the whole twist family, rather than for each twist individually.

We now relate the above genus one curves to the Jacobian of Z_δ.

Theorem 4.4 *Let $g(x) = f(x)/(x-\alpha)$, let $B = k[w]/\langle g(w)\rangle$, let $K_1, \ldots, K_r$ be fields over k such that $B \cong K_1 \times \cdots \times K_r$, and let ω_i be the image of w in K_i for each i. Let $D_\delta = \coprod_{i=1}^r D_{\delta,\omega_i}$ be the curve from Theorem 4.1 considered as a curve over B, let $\varphi\colon Z_\delta \to D_\delta$ be the corresponding morphism over B, and let $E_\delta = \mathrm{Jac}(D_\delta) = \coprod_{i=1}^r \mathrm{Jac}(D_{\delta,\omega_i})$. Then the induced k-morphism of abelian varieties*

$$\mathrm{Jac}(Z_\delta) \to \mathrm{Res}_k^B(E_\delta) \cong \prod_{i=1}^r \mathrm{Res}_k^{K_i}(\mathrm{Jac}(D_{\delta,\omega_i}))$$

is an isogeny.

Proof Our strategy is to consider universal families of curves and abelian varieties corresponding to the above situation, observe that the properties of interest are deformation-invariant, and deform the problem to a more computationally tractable case.

Let $S = \operatorname{Spec} A$ be the space parametrizing triples $(g, \alpha, \delta) \in k[w] \times k \times k[X]$ such that g is a monic squarefree quintic polynomial with $g(\alpha) \neq 0$, the degree of δ is at most 5, and δ is invertible modulo $(X-\alpha)\cdot g(X)$. Let $P \in A[w]$ be the generic monic quintic polynomial, and let $T = \operatorname{Spec} A[w]/\langle P(w)\rangle$. Let $\mathcal{Z} \to S$ and $\mathcal{D} \to T$ be the relative curves whose fibers above a point $(g, \alpha, \delta) \in S$ are the genus 5 curve Z_δ and the genus 1 curve D_δ, respectively, that are associated to the twisting parameter δ for the hyperelliptic curve $y^2 = (x-\alpha)g(x)$. Let $\mathcal{J} \to S$ be the relative Jacobian variety of $\mathcal{Z}$, and let $\mathcal{A} = \mathrm{Res}_S^T(\mathrm{Jac}(\mathcal{D}))$, which exists as a scheme since $T \to S$ is étale.

The formulas of Theorem 4.1 define a T-morphism $\mathcal{Z} \times_S T \to \mathcal{D}$, which induces a homomorphism of abelian S-schemes $\Phi\colon \mathcal{J} \to \mathcal{A}$. By [29, Lemma 6.12], the homomorphism $\mathcal{J} \to \Phi(\mathcal{J})$ is flat. The kernel $\ker(\Phi)$ is the fiber product of Φ with the unit section $S \to \mathcal{A}$, so $\ker(\Phi)$ is a flat proper S-group scheme since flatness and properness are preserved by base change. By [12, Exposé VI$_B$, Cor. 4.3], since S is also connected, the fibers of the map $\ker(\Phi) \to S$ all have the same dimension. Moreover, if $\ker(\Phi) \to S$ has relative dimension zero, then $\ker(\Phi)$ is a finite flat S-group scheme by [18, Thm. 8.11.1]. Thus, we can compute the relative dimension of Φ on any fiber, and if Φ is an isogeny, we can also compute its degree on any fiber.

Let $g \in k[w]$ such that $s := (g, 0, 1) \in S(k)$ and g splits completely over k. Let $\omega_1, \ldots, \omega_5$ be the roots of g. By functoriality of restriction of scalars,

$$\mathcal{A}_s \cong \mathrm{Res}_k^{k^5}(\mathrm{Jac}(\mathcal{D}_s)) \cong \prod_{i=1}^5 E_i,$$

where E_i is the Jacobian of the genus 1 curve defined by $y^2 = -\omega_i^{-1} g(0) g(x)/(x-\omega_i)$. Furthermore, choose g so that the elliptic curves E_i are pairwise non-isogenous. (If no such polynomial g is defined over k, it is harmless to extend scalars to a larger field, since this preserves both dimension and degree.)

The composition of the map $\Phi_s\colon \mathcal{J}_s \to \prod_{i=1}^5 E_i$ with any of the five projection maps $\prod_{i=1}^5 E_i \to E_j$ is induced by the map φ of Theorem 4.1 (with $\omega = \omega_i$), hence is surjective. Thus, the image of Φ_s contains an elliptic curve isogenous to E_j for each j. Since the E_j are

Table 1 Outcomes of running the code on the dataset of 7692 genus 2 curves

Outcome	Count	Percent (%)
Success	1045	13.6
Apparent failure of Hasse principle	2120	27.6
Mordell–Weil rank too high	802	10.4
Unable to compute Mordell–Weil group	2271	29.5
Exceeded time or memory limits	1685	21.9
Miscellaneous error	19	0.2

pairwise non-isogenous, this implies that Φ_s is surjective. Since $\dim \mathcal{J}_s = 5$, this means Φ_s is an isogeny. □

Remark 4.5 An analytic computation using Magma's algorithms for period matrices of Riemann surfaces shows that in characteristic zero, up to numerical error, $\mathrm{Jac}(Z_\delta)$ is isogenous to $\mathrm{Res}_k^B(E_\delta)$ via a degree 32 isogeny. The above proof shows that it suffices to compute the degree for any one example, and we then apply the algorithms to the example $f(x) = \prod_{\omega=-2}^{3}(x-\omega)$. Given big period matrices P_1 and P_2 of the corresponding Riemann surfaces, the `IsIsogenousPeriodMatrices` function in Magma computes matrices $M \in M_5(\mathbb{C})$ and $N \in M_{10}(\mathbb{Z})$ such that $MP_1 = P_2N$. This defines an isogeny of degree $\det(N)$ between the corresponding complex tori; we compute $\det(N) = 32$ for this example.

5 Results

Using Magma v2.26-10 and SageMath 9.3 on Boston University's Shared Computing Cluster [5], a heterogeneous Linux-based computing cluster with approximately 21,000 cores, the above algorithms were applied to all 7692 genus 2 curves over $\mathbb{Q}$ in [3] that have at least one rational Weierstrass point and Mordell–Weil rank at least 2. Each of these curves has Mordell–Weil rank 2 or 3, so Chabauty's method [11,26] is not directly applicable. Table 1 summarizes the results.

By "apparent failure of the Hasse principle", we mean that one of the genus 5 covering curves Z_δ is locally solvable, but a point search did not find any rational points on it. Note that the counts add up to more than 7692 because multiple obstructions were found for some curves—for example, a genus 5 curve might map to two different elliptic curves, one of which has too high rank and the other for which Magma cannot compute the Mordell–Weil group.

The raw data is publicly available on GitHub [21]. The data is in the format of a JSON file for each curve, containing the results of the computation as well as the necessary data to reproduce some of the intermediate steps. (This data includes, for example, coefficients of all curves constructed, as well as coordinates of generators of any Mordell–Weil groups computed.)

The computations of Mordell–Weil groups of Jacobians, and hence the results on rational points on curves, are conditional on GRH. Additionally, since Magma's implementation of elliptic curve arithmetic over p-adic fields is not fully numerically stable, we cannot entirely rule out the possibility of an error in precision tracking that compromises the correctness of the computation; however, such errors, even if theoretically possible, are highly unlikely to occur in practice, as this would require unfortunate numerical coin-

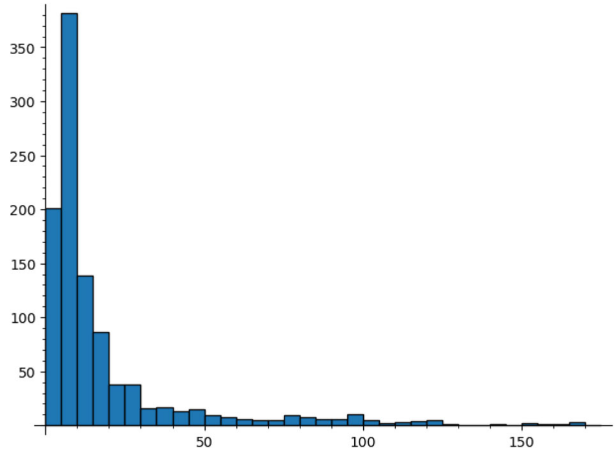

Fig. 1 Histogram of runtimes (in min) for the curves where the method succeeded in computing the set of rational points

cidences at a high degree of precision. At such time as numerically stable p-adic elliptic curve arithmetic is implemented in Magma, the computations could be re-run to rule out this possibility.

The runtime and memory requirements seem hard to predict for any given curve, so a time limit of several hours and a memory limit of 8 GB of RAM was set for each curve. Processes that exceeded these limits were terminated. For curves where the computation completed successfully, runtimes appeared to follow a long-tail distribution (Fig. 1); the median runtime was 529 s, and the mean was 1145 s. For curves where a Mordell–Weil group could not be provably computed (but without timing out) or was found to have too high rank, the distribution of runtimes was similar: median 581 s and mean 1250 s.

Interestingly, while the success rate decreased for curves with larger discriminant, the average runtimes in the cases where the method succeeded did not appear to significantly increase with the discriminant. Rather, the majority of this decrease was due to an increase in failures of the Hasse principle (see Fig. 2).

To reduce the computational resources required, the code was designed to terminate for a given curve as soon as certain obstructions to the success of the computation were detected. Hence, for example, Mordell–Weil groups were not computed when there is an apparent failure of the Hasse principle, so the runtimes for such curves are typically much shorter: a mean of 35 s, a median of 17 s, and only three such curves having a runtime over 10 min.

We also make some observations about the number and height of points on the 4748 genus 5 curves Z_δ associated to the 1045 genus 2 curves where the method succeeded. The largest cardinality of $Z_\delta(\mathbb{Q})$ observed was 6; the full distribution is shown in Table 2.

We can also analyze the maximum $H_{\max}$ of the naive heights $H(P)$ of points $P \in Z_\delta(\mathbb{Q})$ with Z_δ associated to a genus 2 curve C as above. Among the same set of 1045 genus 2 curves, the median value of the largest coordinate was 16; the arithmetic and geometric means were approximately 739.8 and 20.2, respectively, suggesting a long-tail distribution. The statistic $H_{\max}$ appears to increase gradually with the absolute discriminant Δ of C:

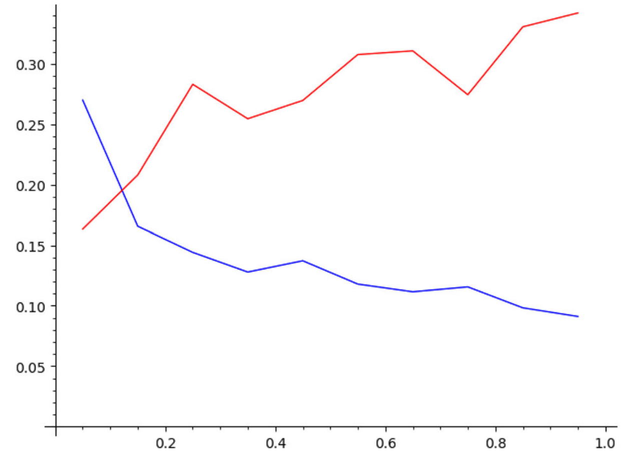

Fig. 2 Portion of curves for which the method succeeded (blue) or encountered an apparent failure of the Hasse principle (red), plotted against the discriminant of the curve (grouped into 10 bins of width 10^5)

Table 2 Distribution of cardinalities of $Z_\delta(\mathbb{Q})$

$\#Z_\delta(\mathbb{Q})$	Count	Percent (%)
0	1136	23.9
1	1602	33.7
2	1531	32.2
3	326	6.9
4	128	2.7
5	18	0.4
6	7	0.1

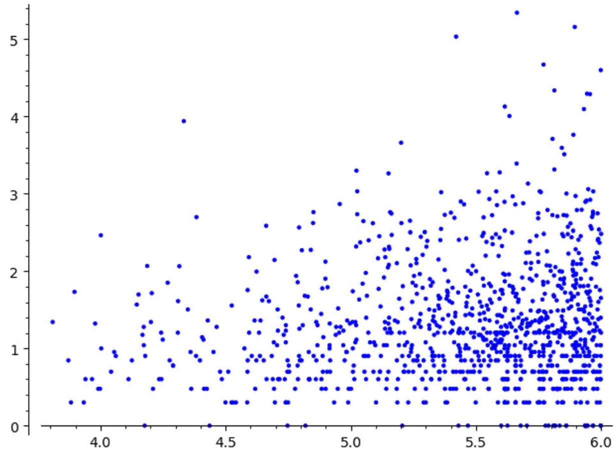

Fig. 3 Log-log plot (base 10) of the absolute discriminant Δ (x-axis) versus the maximum naive height $H_{\max}$ of points in $Z_\delta(\mathbb{Q})$ (y-axis)

a Pearson correlation test on a log-log plot yields a correlation coefficient of $r \approx 0.094$ ($p \approx 0.0023$); see Fig. 3.

Let us further note what sort of progress would be necessary to handle the remaining cases:

1. In cases where a curve Z_δ is found to be locally solvable but no rational points can be found, a method of verifying failure of the Hasse principle (such as an implementation of the Mordell–Weil sieve for such curves) would be necessary to proceed.
2. If one of the elliptic curves has rank greater than or equal to the degree of its base field, then Chabauty's method cannot be applied. In some such cases, Kim's non-abelian generalization of Chabauty's method [24] might be a promising approach.
3. If Magma is unable to provably compute the Mordell–Weil group of an elliptic curve over a number field within the allotted time, then either an unknown amount more computation time or further advances in descent algorithms for elliptic curves over number fields would be required.
4. In a small number of cases, either a local solvability test or elliptic Chabauty exceeded the time or memory limits for unclear reasons.
5. In a handful of cases, Magma threw an exception that suggests a bug in the internal codebase of Magma.

A few more computational remarks:

6. If we do not assume GRH, the bottleneck is provably computing the class group of a degree 15 number field in order to bound the 2-Selmer rank of the elliptic curves, and this rapidly becomes computationally infeasible as the discriminant grows. (We do carry out the unconditional computation in the first example of the next section.)
7. When we assume GRH, most of the time is spent either on computing the Mordell–Weil groups of the elliptic curves or on the elliptic Chabauty method.
8. We use a singular planar model of the curves to quickly test local solvability. Using Proposition 2.4, we only need to check local solvability at the primes of bad reduction of C, primes $p \leq 97$ (for which the Hasse–Weil lower bound $\#Z_\delta(\mathbb{F}_p) \geq p+1-10\sqrt{p}$ (cf. [27]) is non-positive), and the real place. For determining the existence of real points, we use the algorithm of [31, Sect. 4].

6 Examples

Let us illustrate the results of the previous sections by examining several examples of successes and failures in detail. The data for the examples in this section was generated using the batch script `paper-examples.sh` in [22]; the raw data is available at [21] in the "examples" folder.

Theorem 6.1 *Let C be the genus 2 curve with LMFDB label `6443.a.6443.1`, which has minimal weighted projective equation*

$$C\colon y^2 + z^3y = x^5z - x^4z^2 - 2x^3z^3 + x^2z^4 + xz^5.$$

The set of rational points $C(\mathbb{Q})$ is

$$\{(1:0:0), (0:0:1), (-1:0:1), (0:-1:1), (1:0:1), (-1:-1:1),$$
$$(1:-1:1), (2:2:1), (2:-3:1), (-3:6:4), (-3:-70:4)\}.$$

Proof The change of coordinates $(x:y:z) \mapsto (z:2y+z^3:x)$ yields the model

$$y^2 = x^6 + 4x^5z + 4x^4z^2 - 8x^3z^3 - 4x^2z^4 + 4xz^5,$$

Table 3 Results for genus 2 curve `6443.a.6443.1`

	δ	ELS	$D_{\delta,\omega}(K)$	$\#Z_\delta(\mathbb{Q})$
δ_1	1	yes	$\mathbb{Z}^4$	2
δ_2	X^2+X-1	yes	$\mathbb{Z}^3$	3
δ_3	$X^5+4X^4+4X^3-8X^2-5X+4$	yes	$\mathbb{Z}^3$	2
δ_4	$-X^5-4X^4-5X^3+7X^2+5X-4$	no (2)	–	0

which has a rational Weierstrass point at $(0:0:1)$. Let J be the Jacobian of C. Computing the Mordell–Weil group $J(\mathbb{Q})$ in Magma, we find it is free of rank 2, and applying the Cassels map to representatives of each element of $J(\mathbb{Q})/2J(\mathbb{Q})$, we obtain four twist parameters $\delta_1, \delta_2, \delta_3, \delta_4$, each corresponding to a genus 5 curve Z_δ as in Theorem 2.2.

We compute using Magma that Z_{δ_4} is not locally solvable at 2, so $Z_{\delta_4}(\mathbb{Q}) = \emptyset$. For each $i = 1, 2, 3$, we can find a rational point on Z_{δ_i}, so we obtain a map to an elliptic curve $Z_{\delta_i} \to E_i$ over $K = \mathbb{Q}(\omega)$ (where ω is a root of g), as in Theorem 4.1.

We then compute the Mordell–Weil group of each E_i and apply the elliptic Chabauty method to provably compute the set of K-points of each E_i whose image under the given map to $\mathbf{P}^1$ is rational. To make the computation more efficient, we first compute all four Mordell–Weil groups under the assumption of GRH (which is only used to make class group computations faster), and take note of the number field F whose class group we need to compute, along with the conditionally proven value of its class number h_F. By Remark 4.3, the number field F and the class number h_F do not depend on δ. Then we compute h_F unconditionally. The results are summarized in Table 3.

The "ELS" column indicates whether Z_δ is everywhere locally solvable, and if not, gives a prime p such that $Z_\delta(\mathbb{Q}_p) = \emptyset$. The number field whose class group is computed has defining polynomial $x^{15} - 3x^{14} + 15x^{13} - 60x^{12} + 267x^{11} - 1337x^{10} + 2375x^9 - 1676x^8 + 2625x^7 - 4167x^6 - 2687x^5 + 10176x^4 - 4556x^3 - 2616x^2 + 1238x + 406$ over $\mathbb{Q}$; this field was verified in 24,177 s to have class number 2. The other parts of the computation took 1195 s in total.

Next, we apply the map $\bar{\pi}_\delta : Z_\delta \to \mathbf{P}^1$ to each point $P \in Z_\delta(\mathbb{Q})$:

$$\begin{aligned}
\bar{\pi}_1((0:0:0:0:1)) &= 0, & \bar{\pi}_{\delta_2}((22:13:8:2:2)) &= -60/59,\\
\bar{\pi}_1((-1:0:-1:0:2)) &= 1/2, & \bar{\pi}_{\delta_3}((1:0:0:0:0)) &= \infty,\\
\bar{\pi}_{\delta_2}((2:1:1:0:2)) &= 1, & \bar{\pi}_{\delta_3}((3:2:2:0:4)) &= -1.\\
\bar{\pi}_{\delta_2}((8:5:4:2:2)) &= -4/3, & &
\end{aligned}$$

(Note: we view Z_δ as embedded in $\mathbf{P}^4$ with coordinates $v_1, \ldots, v_5$. Since $\gamma_6 = f_6 \neq 0$, we can always reconstruct v_6 from this information using Theorem 2.2.) Inverting the change of coordinates on C, we see that the set of possible x-coordinates of rational points of C is

$$\{\infty, 2, 1, -3/4, -59/60, 0, -1\}.$$

The Weierstrass point lies above ∞, and there are two rational points above each of $2, 1, -3/4, 0, -1$, accounting for all 11 known points in $C(\mathbb{Q})$. The two points of C above $-59/60$ are not rational. □

Table 4 Results for genus 2 curve `141991.b.141991.1`

	δ	ELS	$D_{\delta,\omega}(K)$	$\#Z_\delta(\mathbb{Q})$
δ_1	1	yes	$\mathbb{Z}^3$	1
δ_2	X^2-1	yes	$\mathbb{Z}$	1
δ_3	$X^5+2X^4+7X^3-5X^2-8X+4$	yes	$\mathbb{Z}^3$	2
δ_4	$-X^5-X^4-8X^3+5X^2+8X-4$	yes	$\mathbb{Z}^3$	2
δ_5	$X^5+2X^4+7X^3-6X^2-8X+4$	yes	$\mathbb{Z}^3$	3
δ_6	$-5X^5-7X^4-27X^3+23X^2+28X-16$	no (2)	–	0
δ_7	$4X^5+8X^4+27X^3-23X^2-28X+16$	no (2)	–	0
δ_8	$-X^5-2X^4-8X^3+6X^2+8X-4$	no (2)	–	0

Theorem 6.2 *Let C be the genus 2 curve with LMFDB label `141991.b.141991.1`, which has minimal weighted projective equation*

$$C\colon y^2+(x^2z+xz^2+z^3)y=x^5z-2x^4z^2-2x^3z^3+x^2z^4.$$

Assuming GRH, the set of rational points $C(\mathbb{Q})$ is

$$\begin{aligned}&\{(1:0:0),(0:0:1),(-1:0:1),(0:-1:1),(-1:-1:1),(1:-1:1),\\&(1:-2:1),(2:-3:1),(2:-4:1),(-1:6:4),(1:6:9),(3:-22:4),\\&\qquad\qquad(-1:-58:4),(3:-126:4),(1:-825:9)\}.\end{aligned}$$

Proof The proof strategy is the same as in the previous example. The change of coordinates $(x:y:z)\mapsto(z:2y+x^2z+xz^2+z^3:x)$ yields the model

$$y^2=x^6+2x^5z+7x^4z^2-6x^3z^3-7x^2z^4+4xz^5,$$

which has a rational Weierstrass point at $(0:0:1)$. In this case, the Jacobian of C has Mordell–Weil group $\mathbb{Z}^3$, so there are 8 twists to consider. Of these, three have no $\mathbb{Q}_2$-points and hence no $\mathbb{Q}$-points, and the rest all have a rational point of low height and are amenable to elliptic Chabauty (with the upper bounds on Mordell–Weil ranks conditional on GRH). The results are summarized in Table 4.

The total computation time required was 894 s. The number field F whose class group computation depends on GRH has defining polynomial $x^{15}+6x^{14}+21x^{13}+88x^{12}+212x^{11}+332x^{10}+1198x^9+3248x^8+1626x^7-8560x^6-3892x^5-68524x^4-315439x^3-494742x^2-69455x+384152$ over $\mathbb{Q}$, and the class number is 2 assuming the Bach bound. Verifying this class number would remove the dependence on GRH.

We apply the map $\bar{\pi}_\delta$ to each point $P\in Z_\delta(\mathbb{Q})$:

$$\begin{aligned}\bar{\pi}_1((0:0:0:0:1))&=0, & \bar{\pi}_{\delta_4}((207:82:124:46:106))&=3361/3215,\\ \bar{\pi}_{\delta_2}((0:-1:0:-1:1))&=1/2, & \bar{\pi}_{\delta_5}((1:0:0:0:0))&=\infty,\\ \bar{\pi}_{\delta_3}((1:0:0:0:0))&=1, & \bar{\pi}_{\delta_5}((1:1:0:1:1))&=4/3,\\ \bar{\pi}_{\delta_3}((-1:2:2:4:2))&=9, & \bar{\pi}_{\delta_5}((2:1:1:0:1))&=-4.\\ \bar{\pi}_{\delta_4}((3:4:4:4:4))&=-1, & & \end{aligned}$$

Inverting the change of coordinates, the possible x-coordinates for rational points of C are

$$\{\infty,2,1,1/9,-1,3215/3361,0,3/4,-1/4\}.$$

There is the rational Weierstrass point above ∞, no rational points above 3215/3361, and two rational points above each of the others, yielding exactly the 15 known rational points. □

Now we present a few examples illustrating obstacles the method can encounter.

Example 6.3 (Probable failure of the Hasse principle) Let C be the genus 2 curve with LMFDB label `10681.a.117491.1`, which has a sextic Weierstrass model

$$C\colon y^2 = 121x^6 - 308x^5 + 276x^4 - 92x^3 + 4x.$$

We compute $J(\mathbb{Q}) \cong \mathbb{Z}^2$. One of the twist parameters we obtain by applying the Cassels map to $J(\mathbb{Q})/2J(\mathbb{Q})$ is $\delta = -X + 1$. The corresponding genus 5 curve Z_δ is locally solvable, but the `PointSearch` function in Magma finds no points on Z_δ with a bound of 10^6. (These computations took 15 s in total.) Thus, we are unable to provably compute $C(\mathbb{Q})$ unless we can prove that $Z_\delta(\mathbb{Q})$ is in fact empty.

Example 6.4 (Too high rank for elliptic Chabauty) Let C be the genus 2 curve with LMFDB label `7403.a.7403.1`, which has a sextic Weierstrass model

$$C\colon y^2 = x^6 + 4x^5 - 4x^4 - 8x^3 + 4x^2 + 4x.$$

We compute $J(\mathbb{Q}) \cong \mathbb{Z}^2$. One of the twist parameters we obtain by applying the Cassels map to $J(\mathbb{Q})/2J(\mathbb{Q})$ is $\delta = x^5 + 4x^4 - 4x^3 - 7x^2 + 3x + 4$. The corresponding genus 5 curve Z_δ has three rational points of low height, one of which is $(1 : 0 : 0 : 0 : 0)$, and using this as a base point, we obtain a map $Z_\delta \to E$ defined over the quintic field $K = \mathbb{Q}(\alpha)$ with $\alpha^5 + 4\alpha^4 - 4\alpha^3 - 8\alpha^2 + 4\alpha + 4 = 0$, where E is the elliptic curve given by

$$\begin{aligned} y^2 = x^3 &+ (2\alpha + 4)x^2 + (11\alpha^4 + 57\alpha^3 + 18\alpha^2 - 68\alpha - 34)x \\ &+ (36\alpha^4 + 179\alpha^3 + 63\alpha^2 - 211\alpha - 115). \end{aligned}$$

Magma computes that $E(K)$ is free of rank 5. Thus, we are unable to prove that the three known rational points of Z_δ are all of the rational points. These computations took 449 s in total.

Example 6.5 (Unable to compute Mordell–Weil group) Let C be the genus 2 curve with LMFDB label `7211.a.7211.1`, which has a sextic Weierstrass model

$$C\colon y^2 = x^6 - 4x^4 + 10x^3 - 8x^2 + 1.$$

We compute $J(\mathbb{Q}) \cong \mathbb{Z}^2$. One of the twist parameters we obtain by applying the Cassels map to $J(\mathbb{Q})/2J(\mathbb{Q})$ is $\delta = -4x^5 - 4x^4 + 11x^3 - 26x^2 + 3x + 4$. The corresponding genus 5 curve Z_δ has rational point $(3 : -1 : -1 : -1 : 3)$, and using this as a base point, we obtain a map $Z_\delta \to E$ defined over the quintic field $K = \mathbb{Q}(\alpha)$ with $\alpha^5 + \alpha^4 - 3\alpha^3 + 7\alpha^2 - \alpha - 1 = 0$, where E is the elliptic curve

$$\begin{aligned} y^2 = x^3 &+ (-9\alpha^4 - 13\alpha^3 + 21\alpha^2 - 54\alpha - 18)x^2 \\ &+ (73\alpha^4 + 110\alpha^3 - 163\alpha^2 + 428\alpha + 144)x \\ &+ (82336\alpha^4 + 124063\alpha^3 - 184134\alpha^2 + 483038\alpha + 162465). \end{aligned}$$

Magma can compute that the rank of $E(K)$ is at most 1; however, Magma was unable to either find any non-identity K-points on E or prove that no such points exist. Thus, we are unable to prove that the list of known rational points of Z_δ is complete. These computations took 389 s in total.

Acknowledgements
The author thanks Jennifer Balakrishnan, Raymond van Bommel, Noam Elkies, Brendan Hassett, Steffen Müller, Bjorn Poonen, Michael Stoll, Andrew Sutherland, John Voight, and several anonymous reviewers for helpful comments and conversations related to this paper.

Funding This work was supported by the Simons Collaboration on Arithmetic Geometry, Number Theory, and Computation (Simons Foundation grant #550023).

Data Availability Statement The datasets generated as part of this work are available at [21]. The code used to generate the datasets is available at [22].

Declarations

Conflict of interests

The author asserts that there are no conflicts of interest.

Received: 14 August 2022 Accepted: 1 September 2022 Published online: 13 September 2022

References

1. Bach, E.: Explicit bounds for primality testing and related problems. Math. Comput. **55**(191), 355–380 (1990). https://doi.org/10.2307/2008811
2. Birkenhake, C., Lange, H.: Complex Abelian Varieties, 2nd edn. Grundlehren der mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], vol. 302, p. 635. Springer, Berlin (2004). https://doi.org/10.1007/978-3-662-06307-1
3. Booker, A.R., Sijsling, J., Sutherland, A.V., Voight, J., Yasaki, D.: A database of genus-2 curves over the rational numbers. LMS J. Comput. Math. **19**(suppl. A), 235–254 (2016). https://doi.org/10.1112/S146115701600019X
4. Bosma, W., Cannon, J., Playoust, C.: The Magma algebra system I. The user language. J. Symbol. Comput. **24**, 235–265 (1997). (**Computational algebra and number theory (London, 1993)**)
5. Boston University Shared Computing Cluster. https://www.bu.edu/tech/support/research/computing-resources/scc/ Accessed 2022-02-18
6. Bruin, N.R.: Chabauty Methods and Covering Techniques Applied to Generalized Fermat Equations. CWI Tract, vol. 133, p. 77. Stichting Mathematisch Centrum, Centrum voor Wiskunde en Informatica, Amsterdam,: Dissertation, p. 1999. University of Leiden, Leiden (2002)
7. Bruin, N.: Chabauty methods using elliptic curves. J. Reine Angew. Math. **562**, 27–49 (2003). https://doi.org/10.1515/crll.2003.076
8. Bruin, N., Flynn, E.V.: Towers of 2-covers of hyperelliptic curves. Trans. Amer. Math. Soc. **357**(11), 4329–4347 (2005). https://doi.org/10.1090/S0002-9947-05-03954-1
9. Bruin, N., Stoll, M.: Two-cover descent on hyperelliptic curves. Math. Comp. **78**(268), 2347–2370 (2009). https://doi.org/10.1090/S0025-5718-09-02255-8
10. Cassels, J.W.S., Flynn, E.V.: Prolegomena to a Middlebrow Arithmetic of Curves of Genus 2. London Mathematical Society Lecture Note Series, vol. 230, p. 219. Cambridge University Press, Cambridge (1996). https://doi.org/10.1017/CBO9780511526084
11. Chabauty, C.: Sur les points rationnels des courbes algébriques de genre supérieur à l'unité. C. R. Acad. Sci. Paris **212**, 882–885 (1941)
12. Demazure, M., Grothendieck, A. (eds.): Schémas en Groupes. I: Propriétés Générales des Schémas en groupes. Lecture Notes in Mathematics, Vol. 151, p. 564. Springer, Berlin-New York (1970). https://doi.org/10.1007/BFb0058993. Séminaire de Géométrie Algébrique du Bois Marie 1962/64 (SGA 3)
13. Faltings, G.: Endlichkeitssätze für abelsche Varietäten über Zahlkörpern. Invent. Math. **73**(3), 349–366 (1983). https://doi.org/10.1007/BF01388432
14. Faltings, G.: Erratum: "Finiteness theorems for abelian varieties over number fields." Invent. Math. **75**(2), 381 (1984). https://doi.org/10.1007/BF01388572
15. Flynn, E.V., Testa, D., van Luijk, R.: Two-coverings of Jacobians of curves of genus 2. Proc. Lond. Math. Soc. (3) 104(2), 387–429 (2012). https://doi.org/10.1112/plms/pdr012
16. Flynn, E.V., Wetherell, J.L.: Finding rational points on bielliptic genus 2 curves. Manuscripta Math. **100**(4), 519–533 (1999). https://doi.org/10.1007/s002290050215
17. Flynn, E.V., Wetherell, J.L.: Covering collections and a challenge problem of Serre. Acta Arith **98**(2), 197–205 (2001). https://doi.org/10.4064/aa98-2-9
18. Grothendieck, A.: Éléments de géométrie algébrique. IV. Étude locale des schémas et des morphismes de schémas. III. Inst. Hautes Études Sci. Publ. Math. (28), 255 (1966). https://doi.org/10.1007/BF02684343

19. Grothendieck, A., Raynaud, M.: Revêtements étales et Groupe Fondamental (SGA 1). Documents Mathématiques (Paris), vol. 3, p. 327. Société Mathématique de France, Paris (2003). Séminaire de géométrie algébrique du Bois Marie 1960–61
20. Hartshorne, R.: Algebraic Geometry. Graduate Texts in Mathematics, No. 52, p. 496. Springer, New York-Heidelberg (1977). https://doi.org/10.1007/978-1-4757-3849-0
21. Hast, D.R.: Raw data for the paper "Explicit two-cover descent for genus 2 curves" (2022). https://github.com/HastD/twocover-results Accessed 2022-02-22
22. Hast, D.R.: Source code for the paper "Explicit two-cover descent for genus 2 curves" (2022). https://github.com/HastD/twocover-descent Accessed 2022-02-22
23. Hudson, R.W.H.T.: Kummer's Quartic Surface. Cambridge Mathematical Library, p. 222. Cambridge University Press, Cambridge (1990). With a foreword by W. Barth, Revised reprint of the 1905 original
24. Kim, M.: The unipotent Albanese map and Selmer varieties for curves. Publ. Res. Inst. Math. Sci. **45**(1), 89–133 (2009). https://doi.org/10.2977/prims/1234361156
25. LMFDB Collaboration: The L-functions and Modular Forms Database (2020). https://www.lmfdb.org Accessed 2020-09-21
26. McCallum, W., Poonen, B.: The method of Chabauty and Coleman. In: Explicit Methods in Number Theory. Panor. Synthèses, vol. 36, pp. 99–117. Soc. Math. France, Paris (2012)
27. Milne, J.S.: The Riemann hypothesis over finite fields from Weil to the present day. In: The Legacy of Bernhard Riemann After One Hundred and Fifty Years. Vol. II. Adv. Lect. Math. (ALM), vol. 35, pp. 487–565. Int. Press, Somerville, MA (2016)
28. Mumford, D.: Abelian Varieties. Tata Institute of Fundamental Research Studies in Mathematics, vol. 5, p. 263. Hindustan Book Agency, New Delhi (2008). With appendices by C. P. Ramanujam and Yuri Manin; Corrected reprint of the second (1974) edition
29. Mumford, D., Fogarty, J., Kirwan, F.: Geometric Invariant Theory, 3rd edn. Ergebnisse der Mathematik und ihrer Grenzgebiete (2) [Results in Mathematics and Related Areas (2)], vol. 34, p. 292. Springer, Berlin (1994). https://doi.org/10.1007/978-3-642-57916-5
30. Poonen, B.: Computing rational points on curves. In: Number Theory for the Millennium. III (Urbana, IL, 2000), pp. 149–172. A K Peters, Natick, MA (2002)
31. Sendra, J.R., Winkler, F.: Algorithms for rational real algebraic curves. vol. 39, pp. 211–228 (1999). Symbolic computation and related topics in artificial intelligence (Plattsburg, NY, 1998)
32. The Sage Developers: SageMath, the Sage Mathematics Software System (Version 9.3) (2021). https://www.sagemath.org

Publisher's Note

Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.