DETERMINING THE RATIONAL POINTS ON A CURVE OF GENUS 2 AND MORDELL-WEIL RANK 1

MICHAEL STOLL

ABSTRACT. We explain how one can efficiently determine the (finite) set of rational points on a curve of genus 2 over $\mathbb{Q}$ with Jacobian variety J, given a point $P \in J(\mathbb{Q})$ generating a subgroup of finite index in $J(\mathbb{Q})$.

1 Introduction

Let C be a ("nice": smooth, projective and geometrically irreducible) algebraic curve of genus 2 over $\mathbb{Q}$. Concretely, C can be specified by a polynomial $f \in \mathbb{Z}[x]$, squarefree and of degree 5 or 6; then C is the smooth projective model of the affine plane curve given by

$$y^2 = f(x) .$$

We denote the Jacobian variety of C by J.

By Faltings's Theorem [Fal83, Fal84], whose statement was first conjectured by Mordell [Mor22], we know that the set $C(\mathbb{Q})$ of $\mathbb{Q}$-rational points on any nice algebraic curve C over $\mathbb{Q}$ of genus at lest 2 is finite. (More generally, the corresponding result holds for curves over any algebraic number field.) However, all known proofs (see [BG06, Chapter 11] and [LV20] for two alternative proofs) of this theorem are *infeffective:* they do not give us an algorithm (not even a terribly inefficient one) that would determine this finite set in any concrete case. (It should be noted that there is a general algorithm that would compute the set of rational points on a curve of higher genus, whose termination is conditional on the Hodge, Tate and Fontaine-Mazur conjectures; see [AL24]. However, this algorithm is so complex that it is unlikely to finish for any concrete example before the end of the universe.)

So it is an interesting problem to determine this set $C(\mathbb{Q})$ explicitly and in reasonable time. The setting of curves of genus 2 over $\mathbb{Q}$ is the simplest possible case; it is therefore natural to consider it.

The purpose of this note is to explain how $C(\mathbb{Q})$ can be computed if we know a point $P \in J(\mathbb{Q})$ such that P generates a subgroup of finite index in $J(\mathbb{Q})$. It is known (due to Weil [Wei29]) that $J(\mathbb{Q})$ is a finitely generated abelian group; the assumption above then implies that its rank is at most 1. In particular, the rank of $J(\mathbb{Q})$ is strictly less than the genus of the curve. In this setting, Chabauty [Cha41] gave a proof of Mordell's Conjecture some forty years before Faltings proved it in general. Coleman [Col85] showed how Chabauty's approach can be used to obtain quite good explicit *bounds* on the *number* of rational points. This approach can also be used to *find* the set of rational

Date: September 29, 2025.

2020 *Mathematics Subject Classification.* 11G30, 11D41, 14G05, 11Y50, 11-04; 11G10, 14G25, 14H25, 14H40, 14Q05.

Key words and phrases. Rational points, genus 2, Mordell-Weil group, local solvability.

points. This was first done in [FPS97]; further expositions can be found in [MP12, Sto06], and another concrete application, e.g., in [Sto08].

We note that a rational point $P \in J(\mathbb{Q}) \setminus \{0\}$ can be specified by its *Mumford representation*; this is a pair of polynomials $a, b \in \mathbb{Q}[x]$, with a monic of degree at most 2, such that P is in the linear equivalence class of $D - D_\infty$, where D is cut out by $a(x) = 0$, $y = b(x)$ (when $\deg(a) < 2$, one has to modify this slightly to include points at infinity) and D_∞ is the polar divisor of x.

Our main result in this note is the following.

Theorem 1.1. *There is an algorithm that*

(1) *takes as input a polynomial $f \in \mathbb{Z}[x]$ as above and (the Mumford representation of) a point $P \in J(\mathbb{Q})$;*
(2) *terminates assuming that Conjectures 5.1 and 5.2 hold for C;*
(3) *upon termination returns a subset of $C(\mathbb{Q})$ that is all of $C(\mathbb{Q})$ when $(J(\mathbb{Q}) : \langle P \rangle) < \infty$.*

This algorithm has been implemented in the Magma computer algebra system [BCP97]; it is included in the package files shipped with Magma as of version 2.29. In practice, it terminates within a few seconds on most inputs of reasonable size.

Here is a rough outline of the algorithm. We assume that $(J(\mathbb{Q}) : \langle P \rangle) < \infty$.

1. Check whether C has points everywhere locally (i.e., over all completions of $\mathbb{Q}$). If not, then $C(\mathbb{Q}) = \emptyset$; Stop.
2. Determine the torsion subgroup $J(\mathbb{Q})_{\mathrm{tors}}$ of $J(\mathbb{Q})$.
3. If P is of finite order, then $J(\mathbb{Q})$ is torsion. We can determine $C(\mathbb{Q})$ via its image in $J(\mathbb{Q})$ under $Q \mapsto [Q - \iota(Q)]$ ($\iota\colon (x, y) \mapsto (x, -y)$ is the hyperelliptic involution); Stop.
4. Check whether C has rational divisors of odd degree. If not, then $C(\mathbb{Q}) = \emptyset$; Stop.
5. Use a rational divisor of odd degree to embed C into J and run a "Mordell-Weil sieve + Chabauty" computation. This will terminate in practice (and in theory subject to Conjectures 5.1 and 5.2) and in this case return $C(\mathbb{Q})$.

Before we go into details regarding the steps of the above algorithms, we give in Section 2 a short summary of how we can obtain generators of a finite-index subgroup of the Mordell-Weil group $J(\mathbb{Q})$. This is essential in order to obtain the necessary input, namely, to show that the rank r is at most 1 and that we have a point P that generates a subgroup of rank r.

The computation in Step 1 is essentially standard. Section 3 discusses an efficient implementation for hyperelliptic curves.

An algorithm for Step 2 is described in [Sto99, § 11] and is available in Magma as `TorsionSubgroup(J)`.

Step 3 has been available in Magma for a while as `Chabauty0(J)`.

Step 4 is new. See Section 4 below for a description.

The basic algorithm for Step 5 is described in [BS10]. What is new here is a complete treatment of the case when the Jacobian splits. See Section 5 for details.

2 Computing the Mordell-Weil group

Let C be a nice curve of genus $g \geq 2$ over a number field K, with Jacobian variety J. By the (Mordell-)Weil Theorem [Wei29], the group $J(K)$ of K-rational points on J is a finitely generated abelian group; it therefore has a finite torsion subgroup $J(K)_{\text{tors}}$, and the quotient $J(K)/J(K)_{\text{tors}}$ is a free abelian group of some rank $r \in \mathbb{Z}_{\geq 0}$, which is the *rank* of $J(K)$.

It is then an interesting problem and also an important step in the solution of various other problems related to the arithmetic of C to determine $J(K)_{\text{tors}}$, the rank r, and explicit points $P_1, \ldots, P_r \in J(K)$ whose images are free generators of the quotient $J(K)/J(K)_{\text{tors}}$.

The usual approach is as follows.

1. Search for points in $J(K)$ and check for relations between them. This will give a lower bound on r.
2. Compute a Selmer group (and use perhaps further methods) to obtain an upper bound on r.
3. If both bounds agree, r is determined, and we know points that generate a subgroup of finite index. If the bounds do not agree, go back and try to improve one or both of the bounds.
4. Saturate the known finite-index subgroup to obtain generators of the full group.

For any $n \geq 2$, there is the n-*Selmer group* $\operatorname{Sel}_n(J/K)$ of J over K. It is a finite $\mathbb{Z}/n\mathbb{Z}$-module sitting in an exact sequence

$$0 \longrightarrow J(K)/nJ(K) \longrightarrow \operatorname{Sel}_n(J/K) \longrightarrow Ш(J/K)[n] \longrightarrow 0\,,$$

where $Ш(J/K)$ is the Tate-Shafarevich group of J over K. When $n = p$ is a prime, then $\operatorname{Sel}_p(J/K)$ is a finite-dimensional $\mathbb{F}_p$-vector space, and we have

$$\dim_{\mathbb{F}_p} \operatorname{Sel}_p(J/K) = r + \dim_{\mathbb{F}_p} J(K)[p] + \dim_{\mathbb{F}_p} Ш(J/K)[p]\,,$$

so (assuming we can determine $J(K)[p]$) we obtain a bound on r from it. At least in principle, Selmer groups are computable. In practice, we can usually compute the 2-Selmer group of the Jacobian of a *hyperelliptic* curve $C \colon y^2 = f(x)$, when the number fields generated by the roots of f over K are not "too large". (The main bottleneck is the computation of the class groups of these number fields. In practice, one frequently works assuming GRH to speed up this part of the computation.) See [Cas83, CF96] for the case of genus 2 and [PS97, Sch98, BPS16] for a more general setting. The algorithm for the computation of 2-Selmer groups of hyperelliptic Jacobians is described in detail in [Sto01] (and implemented in Magma).

There are two (not mutually exclusive) ways in which Step 3 above can fail: there may be nontrivial p-torsion in $Ш(J/K)$; then the upper bound will not be tight, or we missed some generators in our search, because they are too large, so the lower bound is not tight. We now assume that $p = 2$. We can determine what the parity of the $\mathbb{F}_2$-dimension of $Ш(J/K)[2]$ should be [PS99]; this will be correct assuming that the 2-primary part of $Ш(J/K)$ is finite. Note that it is generally conjectured that $Ш(J/K)$ is finite. If the parity is odd, then we can subtract 1 from the upper bound. Then if the upper bound is not tight, the difference with the lower bound must be at least 2, so this can give an indication whether it is worth while trying to improve the upper bound. There are various ways in which this can be attempted. One is to consider other abelian varieties A that are isogenous over K (by an isogeny of 2-power degree) to J; then A and J have the same rank, but it is possible that the upper bound for the rank of A that we obtain from its 2-Selmer group is smaller than that obtained for J. The Magma implementation (for genus 2 Jacobians over $\mathbb{Q}$) looks at all 2-power isogenous Jacobians, products of elliptic curves and Weil restrictions of elliptic curves over quadratic number fields for this purpose. Another possibility is to try to *visualize* nontrivial elements of $Ш(J/K)[2]$ in another abelian variety that shares some part of the 2-torsion Galois module with J; see [CM00, BF06]. In our implementation we work with quadratic twists of J. Finally, one can try to compute the Cassels-Tate pairing [Cas62, Tat63] on the 2-Selmer group, for which there is a recent algorithm by Fisher and Yan [FY23] (this algorithm is not yet part of the Magma distribution and so is not currently used in our implementation).

To search for rational points on the (genus 2) Jacobian (over $\mathbb{Q}$), one can use the `j-points` program written by the author of this note, which is included in Magma. It uses a quadratic sieve to find rational points on the associated Kummer surface that lift to the Jacobian. This approach has cubic complexity in the bound for the multiplicative height of the points we want to find; it is therefore not of much use when we want to find points of larger height. Instead, we can construct the 2-covering spaces associated to the elements of the Selmer group that are not yet hit by the points we found and search for rational points on them. The advantage of this approach is that the points have smaller height on the covering spaces, but these spaces are geometrically more complicated than the Kummer surface.

For the saturation step we first find a bound on the index of the subgroup G we have found in $J(\mathbb{Q})$. We then check for each prime p below this bound whether G is already p-saturated, i.e., whether the natural map $G/pG \to J(\mathbb{Q})/pJ(\mathbb{Q})$ is an isomorphism. This can be achieved by considering the image of G in $J(\mathbb{F}_\ell)$ for various primes ℓ such that p divides $\#J(\mathbb{F}_\ell)$. Even when G is not p-saturated, this will give strong restrictions on the elements of G that might be divisible by p in $J(\mathbb{Q})$; we can then check enough of these elements individually. Note that the input to the algorithm in Theorem 1.1 need not be saturated. However, in the course of running the algorithm, we will need to saturate the known subgroup at certain primes, and so we need a procedure that does the p-saturation for a given prime p.

A function that uses the approach described here to try to determine generators of the Mordell-Weil group $J(\mathbb{Q})$ when J is the Jacobian variety of a curve of genus 2 over $\mathbb{Q}$ is available as `MordellWeilGroupGenus2` (or also as part of the more general `MordellWeilGroup` function) in Magma.

3 Testing for local points

In this section we assume that C is a hyperelliptic curve of genus g over a number field K with affine model of the form $y^2 = f(x)$, where f is a squarefree polynomial with coefficients in K and $\deg f \in \{2g+1, 2g+2\}$. We assume that $g \geq 2$ in the following.

We do not claim that this section contains any original results; the material is certainly well-known to the experts. We use the shorthand “ELS” for “everywhere locally soluble”, i.e., the statement that $C(K_v) \neq \emptyset$ for all places v of K.

The algorithm has two parts:

(1) Determine a set S of places of K such that $C(K_v) \neq \emptyset$ for all $v \notin S$ can be shown without computation at individual places, with S as small as possible.

(2) For each $v \in S$, decide whether $C(K_v) = \emptyset$ or not.

We note that when $\deg(f) = 2g + 1$ is odd, then there is a K-rational point at infinity, and so in particular, the curve is ELS. So we will assume that $\deg(f) = 2g + 2$.

We begin with the first part. Recall the following two well-known facts.

Lemma 3.1 (Lower Weil bound). *If C is a nice curve of genus g over a finite field $\mathbb{F}_q$, then*

$$\#C(\mathbb{F}_q) \geq q - 2g\sqrt{q} + 1 .$$

Lemma 3.2 (Hensel lifting). *If C is a nice curve over a p-adic field K with residue class field k and there is a smooth k-rational point P on the reduction of C, then $C(K)$ contains points reducing to P.*

By scaling the variables x and y, we can always assume that our hyperelliptic curve is given by a polynomial f with coefficients in the ring of integers $\mathcal{O}$ of the number field K. We denote the completions of $\mathcal{O}$ and of K at the place corresponding to a prime ideal $\mathfrak{p}$ of $\mathcal{O}$ by $\mathcal{O}_\mathfrak{p}$ and $K_\mathfrak{p}$, respectively. We write $F(x, z) = z^{2g+2} f(x/z)$ for the homogenization of f as an even degree binary form. Then a smooth projective model of C is given by the weighted homogeneous equation

$$Y^2 = F(X, Z)$$

where X and Z have degree 1 and Y has degree $g + 1$; this model sits in a weighted projective plane.

Proposition 3.3. *Let $\mathfrak{p}$ be a prime ideal of $\mathcal{O}$ of odd residue characteristic, write $k = \mathcal{O}/\mathfrak{p}$, and set $q = \#k$. Assume that $q > 4g^2 - 2$. Let $f \in \mathcal{O}[x]$ be squarefree (as an element of $K[x]$) of degree $2g + 2$; then $C\colon y^2 = f(x)$ defines a hyperelliptic curve of genus $g \geq 1$ over K. Write $\bar{f} \in k[x]$ for the reduction mod $\mathfrak{p}$ of f.*

If $\bar{f}$ is not of the form $ch(x)^2$ with a polynomial $h \in k[x]$ and a non-square $c \in k^\times$ (so in particular, $\bar{f} \neq 0$), then $C(K_\mathfrak{p}) \neq \emptyset$.

Proof. Let $\bar{F}$ be the reduction mod $\mathfrak{p}$ of the homogenized version F of f. By assumption, $\bar{F} \neq 0$, so we can write $\bar{F} = H^2 U$ with nonzero binary forms $H, U \in k[X, Z]$ and U squarefree. We first consider the case that U is not constant. Then the curve over k given by $Y^2 = U(X, Z)$ is a nice curve of genus $\deg(U)/2 - 1$. By Lemma 3.1, this curve has at least $q - (\deg(U) - 2)\sqrt{q} + 1$ points. At most $2\deg(H) = 2g + 2 - \deg(U)$ of these points satisfy $H = 0$ (there are at most $\deg(H)$ images $(X : Z)$ on $\mathbb{P}^1$ and each corresponds to at most two points), so there are at least

$$q - (\deg(U) - 2)\sqrt{q} + 1 - (2g + 2 - \deg(U)) > 0$$

smooth k-points on the (usually singular) curve $Y^2 = H(X, Z)^2 U(X, Z)$. By Lemma 3.2, this gives us a point in $C(K_\mathfrak{p})$. (The inequality above follows from $\deg(U) - 2 \leq 2g < (q - 2g + 1)/(\sqrt{q} - 1)$.)

If $U = c$ is constant and $c \in k^\times$ is a square, then every choice of $(X : Z) \in \mathbb{P}^1(k)$ gives rise to k-points on $Y^2 = cH(X, Z)^2$, and there are at least $2(q+1-\deg(H)) = 2(q-g) > 0$ such points that are smooth, so that we can conclude as before. So the only remaining case is that $U = c$ is a constant non-square. In this case, $\bar{f} = cH(x, 1)^2$, which is not true by assumption. □

So we can restrict to

(i) infinite places,
(ii) “small” odd finite places (i.e., such that $q < 4g^2 - 2$),
(iii) even finite places,
(iv) odd finite places such that $\bar{f} = 0$, and
(v) odd finite places such that $\bar{f}$ is a non-square constant times a nonzero square.

We discuss these sets of places in the following subsections.

A function that performs the check for local points over all completions on hyperelliptic curves over $\mathbb{Q}$ is available as `IsLocallySolvable` in Magma.

3.1 Infinite places

The infinite places are easy to deal with: we always have points at complex places, and for a real embedding $\sigma\colon K \to \mathbb{R}$, we have $C(K_\sigma) = \emptyset$ if and only if f^σ has no real roots and the constant term of f^σ is negative (here $f^\sigma \in \mathbb{R}[x]$ denotes the polynomial obtained by applying σ to the coefficients of f).

3.2 Small odd finite places

For the small odd finite places, we use the following procedure (which works for any odd finite place, but can be inefficient when q is large). The case of even residue characteristic is more involved; see below.

Algorithm 3.4 (Local integral points; odd)**.** Let $f \in \mathcal{O}[x]$ be squarefree (as an element of $K[x]$), and let $\mathfrak{p}$ be a prime ideal of $\mathcal{O}$ of odd residue characteristic with uniformizer $\pi \in \mathcal{O}$. Let $k = \mathcal{O}/\mathfrak{p}$ denote the residue class field; as before, $\bar{f}$ denotes the image of f in $k[x]$.

This algorithm decides whether the equation $y^2 = f(x)$ has solutions in $\mathcal{O}_\mathfrak{p}$.

```
0. Set $X \leftarrow \emptyset \subset \mathcal{O}[x]$.
1. For $\xi \in k$, do the following.
    a. If $\bar{f}(\xi)$ is a nonzero square, then return **true**.
    b. If $\bar{f}(\xi) = 0$ and $\bar{f}'(\xi) \neq 0$, then return **true**.
    c. If $\bar{f}(\xi) = \bar{f}'(\xi) = 0$, then lift $\xi$ to $a \in \mathcal{O}$;
       if $f(a)$ is divisible by $\pi^2$, then set $X \leftarrow X \cup \{\pi^{-2} f(a + \pi x)\}$.
2. For each $h \in X$, call this procedure recursively.
   If one of these calls returns **true**, then return **true**.
3. Return **false**.
```

To see that Algorithm 3.4 is correct, note that when the conditions in Steps 1a or 1b are satisfied, then there is a smooth point with x-coordinate ξ on the reduced curve over k, so by Lemma 3.2, this point lifts to $\mathcal{O}_\mathfrak{p}$-solutions. If in Step 1c the polynomial $f(a)$ is not divisible by π^2, then the $\mathfrak{p}$-adic valuation of $f(a + \pi b)$ is equal to 1 for all $b \in \mathcal{O}_\mathfrak{p}$, and so the k-point considered cannot lift. Otherwise, any lift of $(\xi, 0)$ must lead to a solution of $y^2 = \pi^{-2} f(a + \pi x)$ in $\mathcal{O}_\mathfrak{p}$.

To see that the algorithm terminates, assume the contrary. This implies that we have an infinite recursion. So there is a sequence $(a_n)_{n \geq 0}$ of elements of $\mathcal{O}$ such that for all n, the polynomial

$$f_n(x) = \pi^{-2n} f(a_0 + \pi a_1 + \pi^2 a_2 + \ldots + \pi^{n-1} a_{n-1} + \pi^n x)$$

has the property that $f_n(a_n)$ is divisible by π^2 and $f'_n(a_n)$ is divisible by π. Let $a = \sum_{n=0}^{\infty} \pi^n a_n \in \mathcal{O}_\mathfrak{p}$. Then, by taking limits, we see that $f(a) = f'(a) = 0$, which contradicts the assumption that f is squarefee.

Algorithm 3.5 (Small odd prime)**.** Let $f \in \mathcal{O}[x]$ be squarefree (as an element of $K[x]$) and of degree $2g+2$, and let $\mathfrak{p}$ be a prime ideal of $\mathcal{O}$ of odd residue characteristic. We keep the notations π, k, and $\bar{f}$ from Algorithm 3.4. Recall that F denotes the homogenization of f as a binary form of even degree.

This algorithm decides whether the smooth projective curve C associated to $y^2 = f(x)$ has points in $K_\mathfrak{p}$.

```
1. If $\deg(\bar{f}) = 2g+2$ and the leading coefficient of $\bar{f}$ is a square, then return **true**.
2. If $\deg(\bar{f}) = 2g+1$, then return **true**.
3. If $F(1,0)$ is divisible by $\pi^2$ in $\mathcal{O}_\mathfrak{p}$, then call Algorithm 3.4 on $\pi^{-2}F(1,\pi x)$.
   If the result is **true**, then return **true**.
4. Call Algorithm 3.4 on $f$.
   If the result is **true**, then return **true**.
5. Return **false**.
```

To see that Algorithm 3.5 is correct, note first that a $K_\mathfrak{p}$-point on the curve C either has x-coordinate in $\mathcal{O}_\mathfrak{p}$ or the inverse of the x-coordinate is in $\pi\mathcal{O}_\mathfrak{p}$ (this includes the case that the point is at infinity). The existence of a point with $\mathfrak{p}$-adically integral x-coordinate is decided in Step 4. The first two steps check whether there is a smooth k-rational point at infinity; if this is the case, then we can lift it to a $K_\mathfrak{p}$-rational point at infinity. Otherwise, Step 3 checks whether $K_\mathfrak{p}$-rational points can reduce to the k-point at infinity, and if so, call the previous algorithm to decide whether there really are such points. The test is analogous to Step 1c in Algorithm 3.4.

3.3 Even places

The main difference compared to odd places when considering an even place is that in characteristic 2, the y-derivative of an equation $y^2 = f(x)$ is always zero, which is related to the fact that a nonzero square in the residue class field does not necessarily lift to a square in $\mathcal{O}_\mathfrak{p}$. This means that we need to work with a more general form of the curve equation. The affine case is dealt with in the following algorithm.

Algorithm 3.6 (Local integral points; even)**.** Let $c \in \mathcal{O}$ and $f \in \mathcal{O}[x]$ be such that $4f(x) + c^2$ is squarefree as an element of $K[x]$, and let $\mathfrak{p}$ be a prime ideal of $\mathcal{O}$ of residue characteristic 2 with uniformizer $\pi \in \mathcal{O}$. Let $k = \mathcal{O}/\mathfrak{p}$ denote the residue class field; as before, $\bar{f}$ denotes the image of f in $k[x]$.

This algorithm decides whether the equation $y^2 + cy = f(x)$ has solutions in $\mathcal{O}_\mathfrak{p}$.

```
0. Set $X \leftarrow \emptyset \subset \mathcal{O} \times \mathcal{O}[x]$.
1. If $\bar{c} \neq 0$, then for $\xi \in k$, do the following.
     a. If the equation $y^2 + \bar{c}y = \bar{f}(\xi)$ has solutions in $k$, then return **true**.
   Return **false**.
2. (Now $\bar{c} = 0$.) For $\xi \in k$, do the following.
     a. If $\bar{f}'(\xi) \neq 0$, then return **true**.
     b. Let $\eta \in k$ be the square root of $\bar{f}(\xi)$. Lift $\xi, \eta$ to $a, b \in \mathcal{O}$.
        If $\pi^2$ divides $f(a) - b^2 - cb$, then set
        $X \leftarrow X \cup \{(\pi^{-1}(2b + c), \pi^{-2}(f(a + \pi x) - b^2 - cb))\}$.
  2. For each pair $(c', h) \in X$, call this procedure recursively.
     If one of these calls returns **true**, then return **true**.
  3. Return **false**.
```

To see that Algorithm 3.6 is correct, note that when $\bar{c} \neq 0$, every k-point on the curve $y^2 + \bar{c}y = \bar{f}(x)$ is smooth since the y-derivative is always $\bar{c} \neq 0$. The x-derivative is $\bar{f}'(\xi)$, so the point is also smooth when that does not vanish. In both cases, Lemma 3.2 shows that there are solutions in $\mathcal{O}_\mathfrak{p}$. When the k-points with x-coordinate ξ are not smooth and $f(a) - b^2 - cb$ is not divisible by π^2, then $b^2 + cb - f(a)$ will have $\mathfrak{p}$-adic valuation 1 for *all* lifts a, b to $\mathcal{O}_\mathfrak{p}$ of ξ, η, so no lift will give a solution. Otherwise, we can make the indicated substition; each solution in $\mathcal{O}_\mathfrak{p}$ of the original equation will give a solution to the new equation.

Termination is seen in a similar way as for Algorithm 3.4. If the algorithm generates an infinite recursion, then we obtain sequences (a_n) and (b_n) in $\mathcal{O}$ such that with $a = \sum_{n=0}^{\infty} a_n \pi^n \in \mathcal{O}_\mathfrak{p}$ and $b = \sum_{n=0}^{\infty} b_n \pi^n \in \mathcal{O}_\mathfrak{p}$, we find that $b^2 + cb = f(a)$ and $2b + c = f'(a) = 0$, which implies that $4f(x) + c^2$ is divisible by $(x - a)^2$, contradicting the assumption on f and c.

To decide if there is a $K_\mathfrak{p}$-point on the projective curve, we again separate integral and non-integral x-coordinates.

Algorithm 3.7 (Even prime). Let $f \in \mathcal{O}[x]$ be squarefree (as an element of $K[x]$) and of degree $2g + 2$, and let $\mathfrak{p}$ be a prime ideal of $\mathcal{O}$ of residue characteristic 2. We keep the notations π, k, and $\bar{f}$ from Algorithm 3.6. Recall that F denotes the homogenization of f as a binary form of even degree.

This algorithm decides whether the smooth projective curve C associated to $y^2 = f(x)$ has points in $K_\mathfrak{p}$.

```
  1. Call Algorithm 3.6 on $(0, f)$.
     If the result is **true**, then return **true**.
  2. Call Algorithm 3.6 on $(0, F(1, \pi x))$.
     If the result is **true**, then return **true**.
  3. Return **false**.
```

3.4 Odd places where f reduces to zero

To find the (odd) primes $\mathfrak{p}$ such that $\bar{f} = 0$, we need to factor the content of f, i.e., the ideal generated by all the coefficients. This will typically be fairly small, so the factorization step should not be a problem.

Now assume that $\mathfrak{p}$ is such a prime and let $\pi \in \mathcal{O}$ be a uniformizer for $\mathfrak{p}$. Let m be the minimal $\mathfrak{p}$-adic valuation of a coefficient of f; then $m > 0$. If m is even, then we can divide f by the square π^m to get a polynomial with nonzero reduction mod $\mathfrak{p}$. Otherwise, let $f_1 = \pi^{-m} f$; then f is a square times πf_1. If $\xi \in k$ is such that $f_1(\xi) \neq 0$, then $f(a)$ will have odd $\mathfrak{p}$-adic valuation m for all $a \in \mathcal{O}$ reducing to ξ; so we do not obtain points in $C(K_\mathfrak{p})$ with such x-coordinates. Similarly, if $\deg(\bar{f}_1) = 2g + 2$, then there are no points in $C(K_\mathfrak{p})$ with non-integral x-coordinate. So we can restrict to the $\xi \in k$ such that $\bar{f}_1(\xi) = 0$ (and $\xi = \infty \in \mathbb{P}^1(k)$ when $\deg(\bar{f}_1) < 2g + 2$). Fix such a ξ and lift it to $a \in \mathcal{O}$. Then we run Algorithm 3.4 on $\pi^{-1}f_1(a + \pi x)$ (respectively, on $\pi^{-1}F_1(1, \pi x)$ when $\xi = \infty$).

3.5 Odd places where f reduces to a non-square constant times a square

We first need to find these primes. We can run Algorithm 3.5 for all primes dividing both the coefficient of x^{2g+2} (which by assumption is nonzero) and the coefficient of x^{2g+1} of f. In this way, we reduce to finding all the primes $\mathfrak{p}$ that do not divide the leading coefficient c of f and have the property that $\bar{f}$ is a constant times a square (we look at whether the constant is a square or not later).

To do this, we determine the unique monic polynomial $q \in K[x]$ of degree $g+1$ such that $\deg(r) \le g$, where $r = f - cq^2$ and c is the leading coefficient of f. The coefficients of the polynomial q can be determined recursively from the top down to the constant term; this involves divisions by 2 and by c, so $q, r \in \mathcal{O}[(2c)^{-1}, x]$. We factor the (numerator of the) fractional ideal of $\mathcal{O}$ generated by the coefficients of r; the prime ideals dividing it are the ones we are looking for: if $\bar{f} = \bar{c}\tilde{q}^2$ for some monic polynomial $\tilde{q} \in k[x]$ and $\mathfrak{p} \nmid 2c$, then necessarily $\tilde{q} = \bar{q}$ and therefore $\bar{r} = 0$.

We then check for each of the resulting prime ideals $\mathfrak{p}$ whether c reduces to a (nonzero) square mod $\mathfrak{p}$. If it does, then (recall that $\mathfrak{p}$ does not divide the leading coefficient of f) there are smooth points at infinity on the reduced curve, which via Lemma 3.2 implies that $C(K_\mathfrak{p}) \neq \emptyset$. Otherwise, the only way we can obtain a local point is that the x-coordinate reduces to a root of $\bar{q}$. So for each root $\xi \in k$ of $\bar{(}q)$, we do the following. Let $a \in \mathcal{O}$ be a lift of ξ. If π^2 does not divide $f(a + \pi x)$, then no point in $C(K_\mathfrak{p})$ can have x-coordinate reducing to ξ. Otherwise, we apply Algorithm 3.5 to $\pi^{-2}f(a + \pi x)$. If it returns **true**, we return **true**, otherwise we consider the next ξ. If no root ξ leads to success, we return **false**.

4 Rational divisors of odd degree

In this section we restrict to curves of genus 2 over $\mathbb{Q}$. We explain how one can determine whether the curve C has rational divisors of odd degree. This can be done whenever we know generators of a finite index subgroup G_0 of $J(\mathbb{Q})$. In the application that is the focus of this paper, G_0 is generated by the torsion subgroup $J(\mathbb{Q})_{\text{tors}}$ together with the point P.

Note that when C has rational points, there are also rational divisors of odd degree: every rational point gives such a divisor. So if we can show that C has no rational divisors of odd degree, then we have shown that C has no rational points.

First we saturate (see Section 2) the known subgroup G_0 at 2. This gives us a subgroup $G \subseteq J(\mathbb{Q})$ of finite odd index; in particular $G/2G \to J(\mathbb{Q})/2J(\mathbb{Q})$ is an isomorphism. Next observe that a rational divisor D of odd degree on C gives a rational point on Pic^1_C (by taking its class and subtracting a suitable multiple of the canonical class K, which has degree 2 and is defined over $\mathbb{Q}$). A rational point on Pic^1_C does not necessarily arise from a rational divisor, but if one of them does, then all of them do. This is because the difference of any two rational points on Pic^1_C is a point in $J(\mathbb{Q})$, and all rational points on J are represented by rational divisors (this is true more generally for hyperelliptic curves of even genus).

Then note that Pic^1_C is a 2-covering of J (the 2-covering map is given by $Q \mapsto 2Q - K$), so if it has rational points, then the set of their images in $J(\mathbb{Q})$ is a coset of $2J(\mathbb{Q})$. By the isomorphism above, we can determine a set of representatives of these cosets from G. We then test each representative if it is in the image of $\mathrm{Pic}^1_C(\mathbb{Q})$, and if so, whether it can be represented by a rational divisor (and in this case, we actually find such a divisor). If a rational divisor of odd degree is found, we are done. Otherwise, we have shown that no rational divisor of odd degree exists (in particular, we do not need to consider further cosets).

To check if a point in $J(\mathbb{Q})$ lifts to a rational divisor of odd degree, we use the following diagram.

$$\begin{tikzcd}
\mathrm{Pic}^1_C \arrow[r] \arrow[d] & J \arrow[d] \\
\mathcal{K}^\vee \arrow[r, "\delta"] & \mathcal{K}
\end{tikzcd}$$

Here $\mathcal{K}$ denotes the Kummer surface $J/\{\pm 1\}$ of J and $\mathcal{K}^\vee$ is the dual Kummer surface, which is the quotient of Pic^1_C by the involution induced by the hyperelliptic involution on C. The covering map $\mathrm{Pic}^1_C \to J$ descends to a twist δ of the duplication map on the Kummer surface. Everything in the second row of the diagram is completely explicit. So we can take a coset representative $Q \in J(\mathbb{Q})$, map it to $\mathcal{K}$ and then check if it lifts to a rational point on $\mathcal{K}^\vee$ under δ by solving a system of polynomial equations (whose solution set is a zero-dimensional scheme, so this is reasonably efficient). If a rational lift R to $\mathcal{K}^\vee$ is found, we then check if R comes from a rational divisor of odd degree. This can be done completely analogously to the situation for genus 3 hyperelliptic curves as described in [Sto17, § 4]. Essentially, we check if some expression is a nonzero square to see whether the point lifts to $\mathrm{Pic}^1_C(\mathbb{Q})$, and then we have to decide if the conic parameterizing the effective degree 3 divisors corresponding to the point on Pic^1_C has rational points (and find one if it does).

This functionality is available as `HasOddDegreeDivisor` in Magma.

5 Mordell-Weil-Sieve + Chabauty

The basic algorithm is described in [BS10, § 3, § 4.4]. It uses the following ingredients. First of all, we fix an embedding $\iota\colon C \to J$ defined over $\mathbb{Q}$ (which for a curve of genus 2 is given in terms of a rational point on C or an effective rational divisor of degree 3 on C).

We begin with the "Mordell-Weil sieve" part. The idea originally goes back to Scharaschkin [Sch99] and was further developed by Flynn [Fly04]; it is as follows. We pick a finite set S of primes of good reduction for C and a (smooth) positive integer N. Consider the following commutative diagram, where the vertical maps are given by reduction mod p for all $p \in S$.

$$\begin{tikzcd}
C(\mathbb{Q}) \arrow[r, "\iota"] \arrow[d] \arrow[rr, bend left, "\phi"] & J(\mathbb{Q}) \arrow[r] \arrow[d] & J(\mathbb{Q})/NJ(\mathbb{Q}) \arrow[d, "\rho"] \\
\prod_{p \in S} C(\mathbb{F}_p) \arrow[r, "\iota"] \arrow[rr, bend right, "\psi"'] & \prod_{p \in S} J(\mathbb{F}_p) \arrow[r] & \prod_{p \in S} J(\mathbb{F}_p)/NJ(\mathbb{F}_p)
\end{tikzcd}$$

We then clearly have

$$\phi\big(C(\mathbb{Q})\big) \subseteq \rho^{-1}\big(\operatorname{im}(\psi)\big) . \tag{5.1}$$

The set on the right is a set of cosets of $NJ(\mathbb{Q})$, which can be computed explicitly if we know that $J(\mathbb{Q})_{\text{tors}} + \mathbb{Z} \cdot P$ is saturated at all primes dividing N. See [BS10, § 3] for a discussion how this computation can be done efficiently (including a good choice for N). We can check the saturation condition for every prime divisor q of N and, if necessary, replace P by some point P' such that $P = qP' + T$ with some $T \in J(\mathbb{Q})_{\text{tors}}$.

Now the hope is that we can use this approach to determine $C(\mathbb{Q})$. One necessary ingrendient for this is that C satisfies the following conjecture. This is a variant of Conjecture 21 in [Sto11], which a version of Poonen's Heuristic, restricted to cosets in $J(\mathbb{Q})$ (the original version assumes that $C(\mathbb{Q})$ is empty; see [Poo06]). It is also related to the Main Conjecture in [Sto07].

Conjecture 5.1. *For N sufficiently divisible and S sufficiently large depending on N, the inclusion in (5.1) is an equality, i.e.,*

$$\phi\big(C(\mathbb{Q})\big) = \rho^{-1}\big(\operatorname{im}(\psi)\big) .$$

Note that once the statement of the conjecture holds for some N and S, it will stay valid for any set S' containing S. (It may become invalid when we replace N by a multiple N': a coset modulo $NJ(\mathbb{Q})$ that contains the image of a rational point will split into a number of cosets modulo $N'J(\mathbb{Q})$ that can be in $\rho^{-1}(\operatorname{im}(\psi))$ but do not necessarily all contain images of rational points.)

We also note that we can certify that the statement of Conjecture 5.1 holds for a given N and S: for each coset in $\rho^{-1}(\operatorname{im}(\psi))$ we exhibit a rational point on C whose image under ϕ is this coset. Conjecture 5.1 ensures that we will eventually be able to do that, by successively increasing N and S until we are successful. In this case, we know that all rational points map into a given subset of $J(\mathbb{Q})/NJ(\mathbb{Q})$, but it is still possible that some of the fibers of ϕ contain more than one point.

Since we know that $C(\mathbb{Q})$ is finite and $C(\mathbb{Q})$ injects (via ι) into $J(\mathbb{Q})$, which is a finitely generated abelian group, it follows that for N sufficiently divisible, ϕ must be injective. If this holds for N, then our algorithm will have determined $C(\mathbb{Q})$. The problem we have in practice is that we need an explicit criterion that allows us to verify that ϕ is injective for a given N.

This is where the "Chabauty" part comes in. It is based on the following fact. Let p be a prime, which we assume to be of good reduction for C for simplicity. There is a pairing (see [Col85, MP12, Sto06])

$$J(\mathbb{Q}_p) \times \Omega^1_{J/\mathbb{Q}_p} \longrightarrow \mathbb{Q}_p\,, \qquad (P, \omega) \longmapsto \int_0^P \omega = \omega(\log P)\,,$$

where $\log\colon J(\mathbb{Q}_p) \to T_0 J(\mathbb{Q}_p)$ is the p-adic abelian logarithm and ω is identified with an element of the cotangent space $T_0^* J(\mathbb{Q}_p)$. Since $J(\mathbb{Q})$ has rank 1 by assumption and $\Omega^1_{J/\mathbb{Q}_p}$ is a 2-dimensional vector space over $\mathbb{Q}_p$, there must be a non-zero differential $\omega_p \in \Omega^1_{J/\mathbb{Q}_p}$ that annihilates $J(\mathbb{Q})$ under this pairing. We call such an ω_p an *annihilating differential*. There is a canonical isomorphism between the spaces of regular 1-forms on J and on C, so we can consider an annihilating differential ω_p as a regular differential on $C_{\mathbb{Q}_p}$. It then follows that for all pairs $Q, Q' \in C(\mathbb{Q})$ of rational points,

$$\int_Q^{Q'} \omega_p = 0\,.$$

When Q and Q' reduce to the same point in $C(\mathbb{F}_p)$, this integral can be computed by evaluating the formal integral of a power series representing ω_p. We can scale ω_p such that its reduction $\bar{\omega}_p$ mod p makes sense and is nonzero. By [Sto06, Prop. 6.3], the number of rational points on C that reduce to $\bar{Q} \in C(\mathbb{F}_p)$ is at most 1 plus the order of vanishing of $\bar{\omega}_p$ at $\bar{Q}$ (unless p is very small). In particular, there can be at most one rational point reducing to $\bar{Q}$ when $\bar{\omega}_p$ does not vanish at $\bar{Q}$ and $p > 2$ (by [Sto06, Lemma 6.1], we have $\delta(p, 0) = 0$ for $p > 2$). This shows that when $p > 2$ and $\bar{\omega}_p$ does not vanish at any point in $C(\mathbb{F}_p)$, then the reduction map $C(\mathbb{Q}) \to C(\mathbb{F}_p)$ is injective. This implies that the map ϕ is injective when N is a multiple of the exponent of (the image of $J(\mathbb{Q})$ in) $J(\mathbb{F}_p)$. (Note that $\bar{\omega}_p$ vanishes at the points with a certain x-coordinate $\xi \in \mathbb{F}_p$; the condition is that their y-coordinates are not in $\mathbb{F}_p$, i.e., $\bar{f}(\xi)$ is a non-square in $\mathbb{F}_p$.)

So we want to pick N in such a way that it is a multiple of the exponent of $J(\mathbb{F}_p)$ for a good prime $p > 2$ such that $\bar{\omega}_p$ does not vanish on $C(\mathbb{F}_p)$. This means that we have to find at least one such prime. The following conjecture says that we will easily find such primes unless there is a good reason why this is impossible. Such a good reason is provided by the geometry of J: if J *splits*, which means that it is isogenous over $\mathbb{Q}$ to the product of two elliptic curves E and E', then one of the elliptic curves, say E, must have rank 1 and the other one must have rank 0. The pull-back ω of a nonzero regular differential on E' then vanishes along the image of E in J (obtained via Picard functoriality from the dominant morphism $C \xrightarrow{i} J \to E \times E' \to E$) and will therefore be an annihilating differential for all (good) primes p.

Conjecture 5.2. *The set of primes p of good reduction for C such that the reduction mod p, $\bar{\omega}_p$, of a suitably scaled annihilating differential ω_p does not vanish on $C(\mathbb{F}_p)$ has positive density, unless J splits and the associated global annihilating differential ω vanishes at a rational point of C.*

This is a strengthening of Conjecture 4.2 in [BS10] in the case when C has genus 2, taking into account the heuristic computation of the density, which for hyperelliptic curves (and "rank defect" $g - r = 1$) predicts density $1/2$. The conjecture in loc. cit. makes a statement for simple, so non-split, Jacobians. If in the split case, ω does not vanish at a rational point, then it vanishes at a pair of points with x-coordinate $\xi \in \mathbb{Q}$ such that $f(\xi)$ is a non-square in $\mathbb{Q}$ (or $\xi = \infty$ and the leading coefficient of f is a non-square). There is then a set of primes of density $1/2$ such that $f(\xi)$ is a non-square mod p; for such p, $\bar{\omega}_p = \bar{\omega}$ will not vanish on $C(\mathbb{F}_p)$.

So, assuming the conjecture, we are in good shape *unless* J splits and ω vanishes at a rational point. In this case, the curve C has morphisms of some degree d (which we can assume to be minimal) to the elliptic curves E and E', with $E(\mathbb{Q})$ of rank 1 and $E'(\mathbb{Q})$ finite. If we can determine the morphism $C \to E'$ explicitly, the we can solve our problem by first determining the finitely many points in $E'(\mathbb{Q})$ and then determining the rational points on C in each fiber above one of these points.

There are fairly simple concrete criteria for when such a splitting of J exists with $d = 2$ or $d = 3$, and in this case there are formulas for the elliptic curves and the morphisms. This is implemented via the functions `Degree2Subcovers` and `Degree3Subcovers` in Magma. However, larger degrees d do occur, as the following examples show.

Examples 5.3. Here are some examples of genus 2 curves C that have maps to elliptic curves of minimal degree $d > 3$.

(4) $y^2 = 6x^5 + 28x^3 + 54x$ with $d = 4$.
(5) $y^2 = 64x^6 + 180x^3 + 125$ with $d = 5$.
(6) $y^2 = 192x^5 + 420x^4 + 504x^3 + 177x^2 + 66x + 9$ with $d = 6$.
(7) $y^2 = 4x^6 - 12x^5 + 81x^4 - 22x^3 + 181x^2 + 808x + 304$ with $d = 7$.
(8) $y^2 = x^6 - 6x^5 + 23x^4 - 32x^3 + 71x^2 + 126x + 213$ with $d = 8$.

These were found among a set of about 6 million curves in a list compiled by Drew Sutherland; they caused the previous version of the `Chabauty` procedure in Magma to get stuck.

Remark 5.4. The two elliptic curves in the product isogenous to a split genus 2 Jacobian have isomorphic d-torsion Galois modules; such elliptic curves are said to be d-*congruent*. Conversely, from a pair of d-congruent elliptic curves (such that the isomorphism of d-torsion modules is not induced by an isomorphism of the curves), one obtains a split genus 2 Jacobian. There are split genus 2 Jacobians for which the degree d is even larger than in the examples above. See work of Fisher [Fis14, Fis15, Fis18, Fis19, Fis21] on congruent elliptic curves. Fisher [Fis21] gives two examples with $d = 17$ and conjectures (Conjecture 1.1 in *loc. cit.*) that for primes $d \geq 17$, apart from examples coming from isogenies, these are the only examples up to quadratic twist, whereas [Fis19] gives an infinite family of pairs of 13-congruent elliptic curves. Fisher's conjecture is a strong form of the Frey-Mazur Conjecture, which states that for all sufficiently large primes p, all p-congruences of elliptic curves come from isogenies. (Note that an isogeny $E \to E'$ of degree prime to p induces an isomorphism $E[p] \cong E'[p]$ of Galois modules.)

Luckily, it turns out that it is not actually necessary to find the morphism $C \to E'$ explicitly. Recall that we always assume that the rank of $J(\mathbb{Q})$ is 1.

Lemma 5.5. *Assume that there is a non-constant morphism $C \to E$ with an elliptic curve E. Let $Q \in C(\mathbb{Q})$ be such that the global annihilating differential $\omega \in \Omega^1_C(\mathbb{Q})$ vanishes at Q. Let $p > 3$ be a prime of good reduction for C. Assume that either Q is a Weierstrass point or that the reduction $\bar{Q} \in C(\mathbb{F}_p)$ is not a Weierstrass point. Then the map $C(\mathbb{Q}) \to C(\mathbb{F}_p)$ is injective.*

Proof. We already know that the fibers of $C(\mathbb{Q}) \to C(\mathbb{F}_p)$ have at most one element above points in $C(\mathbb{F}_p)$ at which $\bar{\omega}$ does not vanish. It remains to show that the fiber above the reduction $\bar{Q}$ of Q mod p consists of the single point Q. (The same argument will work for the other rational point $\iota(Q)$ on which ω vanishes, when Q is not a Weierstrass point.)

By the definition of an annihilating differential, for any point $Q' \in C(\mathbb{Q})$ such that $\bar{Q}' = \bar{Q}$ the p-adic integral

$$\int_Q^{Q'} \omega$$

vanishes. This integral can be computed by formally integrating a power series and evaluating at a suitable parameter (it is a "tiny integral").

First assume that Q is not a Weierstrass point and its reduction $\bar{Q} \in C(\mathbb{F}_p)$ is also not a Weierstrass point (i.e., the numerator of the y-coordinate of Q is not divisible by p). Then $t = x - x(Q)$ when $x(Q) \in \mathbb{Z}_p$ or $t = x^{-1} - x(Q)^{-1}$ when $x(Q)^{-1} \in \mathbb{Z}_p$ is a local parameter at Q reducing to a local parameter at $\bar{Q}$. Since ω vanishes at Q, we have (after possibly scaling ω)

$$\omega = t w(t)\, dt$$

with a power series $w(t) = 1 + a_1 t + a_2 t^2 + \ldots$ with coefficients in $\mathbb{Z}_p$, and the integral from Q to Q' (in the same p-adic residue disk) is

$$\int_Q^{Q'} \omega = \int_0^{t(Q')} (t + a_1 t^2 + ...)\, dt = \frac{1}{2} t(Q')^2 + \frac{a_1}{3} t(Q')^3 + \frac{a_2}{4} t(Q')^4 + \ldots ;$$

this has a double zero at Q and (since $p > 3$) no further zeros on the residue disk.

If Q is a Weierstrass point, then $t = y$ when $Q \neq \infty$ or $t = y/x^3$ when $Q = \infty$ is again a local parameter at Q reducing to a local parameter at $\bar{Q}$. Since ω in this case vanishes to order 2 at Q, we have (again after scaling)

$$\omega = t^2 w(t)\, dt$$

with an even power series $w(t) = 1 + a_2 t^2 + a_4 t^4 + \ldots$, and

$$\int_Q^{Q'} \omega = \int_0^{t(Q')} (t^2 + a_2 t^4 + \ldots)\, dt = \frac{1}{3} t(Q')^3 + \frac{a_2}{5} t(Q')^5 + \ldots ;$$

this has a triple zero at Q and (again since $p > 3$, note the increase by 2 of the degree) no further zeros on the residue disk. □

Note that when ω vanishes at a non-Weierstrass point Q that reduces mod p to a Weierstrass point $\bar{Q}$, then the fiber of the reduction map above $\bar{Q}$ contains (at least) the two rational points Q and $\iota(Q)$ (where ι denotes the hyperelliptic involution), so the conclusion cannot hold in this case. But in any case, we see that the reduction map will be injective for all but finitely many primes, with an explicit set of possible exceptions.

So if we seem unable to find a good odd prime p such that $\bar{\omega}_p$ does not vanish on $C(\mathbb{F}_p)$, we try to first show that J splits (and if so, determine the degree d). This can be done numerically by computing a period matrix (Magma contains functionality for analytic Jacobians of hyperelliptic curves; see [CMSV19]). The result we obtain is not rigorous, but it will be certified by the next step. This uses the following observation.

Lemma 5.6. *Let $C \to E$ be a morphism of degree d and let $\tilde{E} \subset J$ be the image of E under the induced morphism $E \to J$. Let $\mathcal{K}$ be the Kummer surface of J and denote by Y the image of $\tilde{E}$ on $\mathcal{K}$. Then $\tilde{E} \to Y$ is a double cover ramified in four points, so Y is a smooth rational curve of degree d in $\mathbb{P}^3$. Also, Y is contained in a surface of degree $\lceil d/2 \rceil$ that does not contain $\mathcal{K}$.*

Proof. Since $E \to J$ is a homomorphism of abelian varieties and $J \to \mathcal{K}$ identifies points with their negatives, the morphism $E \to J$ descends to a morphism $\mathbb{P}^1 \to \mathcal{K}$ (where $E \to \mathbb{P}^1$ is the x-coordinate map); in particular, Y is a rational curve. The degree of $\tilde{E}$ with respect to the theta divisor on J is d; this implies that the degree of Y is also d. We have that $J[2] \cap \tilde{E} = \tilde{E}[2]$, which is of size 4; as $J[2]$ is the set of ramification points of $J \to \mathcal{K}$, this shows that $\tilde{E} \to Y$ is ramified in four points (this also follows from Riemann-Hurwitz).

The morphism $\mathbb{P}^1 \to Y \subset \mathcal{K} \subset \mathbb{P}^3$ is given by a quadruple of binary forms of degree d. There is a $\binom{n+3}{3}$-dimensional space of degree n forms in four variables containing an $\binom{n-1}{3}$-dimensional subspace of multiples of the defining quartic equation of $\mathcal{K}$. So there will be a degree n form vanishing on Y that is not a multiple of the defining equation of $\mathcal{K}$ whenever

$$2n^2 + 2 = \binom{n+3}{3} - \binom{n-1}{3} > dn + 1\,,$$

where $dn + 1$ is the dimension of the space of binary forms of degree dn. This is the case for $n \geq \lceil d/2 \rceil$. □

The idea now is to find Y by interpolating points. Note that $\tilde{E}$ will contain a point of the form $P' = nP + T$ for some $n \geq 1$ and $T \in nJ(\mathbb{Q})_{\text{tors}}$, where n divides the least common multiple of d and the exponent of $J(\mathbb{Q})_{\text{tors}}$. Since $\tilde{E}$ is an abelian subvariety, it will then contain all multiples of P', so Y will contain all their images on $\mathcal{K}$.

For $n = 1$, $n = d$, $n = \operatorname{lcm}(d, \exp(J(\mathbb{Q})_{\text{tors}}))$ and in each case for all possibilities of $T \in nJ(\mathbb{Q})_{\text{tors}}$, we therefore compute enough of the multiples of $P' = nP + T$ and find all hypersurfaces of degree $m = \lceil d/2 \rceil$ that pass through these points. If there are any such hypersurfaces, we then check for whether their intersection with the Kummer surface has dimension 1 and contains a curve of degree d and genus 0 passing through exactly four points of order 2 and containing the image of P'. If this is the case for some choice of n and T as above, then we have shown that J splits and we have found the image Y of $\tilde{E}$ on the Kummer surface. We can then obtain the x-coordinate of the points on which the annihilating differential vanishes from the tangent line of Y at the origin. It remains to verify that there are rational points on C with that x-coordinate. If this is the case, then we can apply Lemma 5.5 above.

Magma's `Chabauty` function carries out the Mordell-Weil Sieve + Chabauty computation explained in this section. It includes the check for rational divisors of odd degree. More precisely, it first searches for rational points on the curve (unless a rational point on C is given as an optional argument; then that is used to embed C into J), and if it does not find one up to some height bound, then it runs `HasOddDegreeDivisor`. The search for rational points is done using `ratpoints` [Sto22]; this code is part of Magma.

6 Concluding remarks.

The functionality described here (except the part that is summarized in Section 2, which was contributed in 2019/2020) forms part of what the new (as of version 2.29) Magma function `RationalPointsGenus2` is doing. Its purpose is to try to provably determine the full set of rational points on a curve C of genus 2 over $\mathbb{Q}$. It essentially performs the following steps.

1. Search for small rational points.

2. If no point was found, then test whether C has points everywhere locally (see Section 3). If C fails to have points over some completion of $\mathbb{Q}$, then $C(\mathbb{Q}) = \emptyset$; Stop.
3. Search again for rational points up to a larger bound.
4. If no point was found, then compute the (fake) 2-Selmer set of C; see [BS09]. If this is empty, then $C(\mathbb{Q}) = \emptyset$; Stop.
5. Check if C admits morphisms of degree 2 or 3 to elliptic curves. If so, and one of the elliptic curves, say E, has finite group of rational points, then determine $C(\mathbb{Q})$ by finding the rational points in the fibers above the rational points of E; Stop.
6. Attempt to determine the rank r of $J(\mathbb{Q})$ (see Section 2). If not successful, then report *Failure;* Stop.
7. If $r = 0$, then determine $C(\mathbb{Q})$ by pulling back the finitely many torsion points in $J(\mathbb{Q})$ under $C \to J$, $P \mapsto [P - \iota(P)]$; Stop.
8. Now $r \geq 1$. If no rational point was found so far, then test whether C has rational divisors of odd degree (see Section 4). If this is not the case, then $C(\mathbb{Q}) = \emptyset$; Stop.
9. If $r = 1$, then run the Mordell-Weil Sieve + Chabauty computation (see Section 5). If this terminates, it will have determined $C(\mathbb{Q})$; Stop. (In the actual implementation the computation will be aborted and *Failure* is reported when certain bounds are reached.)
10. Now $r \geq 2$. If no rational point was found so far, use the rational divisor of odd degree that was found earlier to obtain an embedding $C \to J$ and run a Mordell-Weil Sieve computation as in [BS10]. If this proves that $C(\mathbb{Q}) = \emptyset$, then return $\emptyset$, otherwise report *Failure;* Stop.
11. Report *Failure;* Stop.

Assuming Conjectures 5.1 and 5.2, this algorithm will succed in determining $C(\mathbb{Q})$ whenever one of the following conditions holds.

(1) The 2-Selmer set of C is empty (this includes the case that C fails to have points over all completions of $\mathbb{Q}$).
(2) There is an elliptic subcover E of degree 2 or 3, for which it can be determined that the rank is zero.
(3) The rank r of $J(\mathbb{Q})$ can be determined and one of the following holds.
 (a) There is no rational divisor of odd degree on C.
 (b) $r \leq 1$.
 (c) $C(\mathbb{Q}) = \emptyset$.

Note that Conjecture 5.1 implies that the Mordell-Weil Sieve computation will detect that $C(\mathbb{Q}) = \emptyset$ whenever this is the case.

Drew Sutherland has constructed a database of more than 6 million curves of genus 2 over $\mathbb{Q}$ of conductor up to 2^{20} [Sut25], which extends the database [BSS+16] currently available in the LMFDB [LMFDB]. `RationalPointsGenus2` successfully determines the set of rational points on about 92% of these curves (assuming GRH for the rank computation). This high success rate is probably explained to a large part by the fact that most curves do not have rational points: heuristically, one would expect only a fraction of $\ll N^{-1/2}$ curves $y^2 = f(x)$ with integral coefficients bounded by N in absolute value to have rational points. (In the data set, 2 528 131 of 6 216 959 curves have a known rational point.) Experimentally, a fairly large proportion of genus 2 curves without rational points have an empty 2-Selmer set (see [BS09, Section 10]), so in these cases the algorithm will be successful even without attempting to determine the rank of $J(\mathbb{Q})$.

Among the curves for which the rank can be determined, we expect a large majority to have rank 0 or 1, in which cases the algorithm will also be successful.

We remark that there is currently no generally applicable (and practical) algorithm available that can determine $C(\mathbb{Q})$ when $r \geq 2$ and $C(\mathbb{Q}) \neq \emptyset$. However, there are some restricted cases when this is possible. One such case is when J has Néron-Severi rank ρ strictly larger than 1; this occurs when J has real multiplication or is split. When (for a general curve of genus g) $r < g - 1 + \rho$, then *Quadratic Chabauty* [BD18, BDM$^+$19, BD21, BBBM21, EL23] can determine $C(\mathbb{Q})$. There are also recent steps [Dog25, Dog24] in the direction of making the full second level of the Chabauty-Kim approach effective and feasible; this would lead to an algorithm that can determine $C(\mathbb{Q})$ when $r \leq g^2$.

Another observation is that every rational point on C lifts to one of finitely many 2-covering curves D_ξ of genus 17, where ξ runs through the elements of the 2-Selmer set of C. These curves D_ξ each have 15 maps to elliptic curves that are in general not defined over $\mathbb{Q}$, however; the Galois action on them corresponds to the Galois action on the points of order 2 on J, which in turn correspond to the factorizations of f into a quadric and a quartic (up to scaling). If, for each ξ, there is one such map $D_\xi \to E_\xi$, which is defined over a number field K_ξ of degree d and such that the rank of $E_\xi(K_\xi)$ is strictly less than d, then a variant of Chabauty's method, known as *Elliptic Curve Chabauty* can be used; see [Bru03]. In practice, this requires the degrees d to be reasonably small (say, $d \leq 5$ or so); otherwise, the determination of $E_\xi(K_\xi)$ is likely infeasible. This means that the Galois group of f has to be quite small. So this approach is practical only in fairly limited situations. In any case, implementing a version of this and including it in `RationalPointsGenus2` is a project for the not-too-distant future.

Acknowledgments

This work was supported by a grant from the Simons Foundation International [SFI-MPS-Infrastructure-00008651, AVS] that provided funding for a visit of the author to MIT in March 2025, during which a major part of the work described in this paper was done.

References

[AL24] Levent Alpöge and Brian Lawrence, *Conditional algorithmic Mordell*, August 21, 2024. https://arxiv.org/abs/2408.11653. ↑1

[BBBM21] Jennifer S. Balakrishnan, Amnon Besser, Francesca Bianchi, and J. Steffen Müller, *Explicit quadratic Chabauty over number fields*, Israel J. Math. **243** (2021), no. 1, 185–232, DOI 10.1007/s11856-021-2158-5. MR4299146 ↑6

[BD18] Jennifer S. Balakrishnan and Netan Dogra, *Quadratic Chabauty and rational points, I: p-adic heights*, Duke Math. J. **167** (2018), no. 11, 1981–2038, DOI 10.1215/00127094-2018-0013. With an appendix by J. Steffen Müller. MR3843370 ↑6

[BD21] ———, *Quadratic Chabauty and rational points II: Generalised height functions on Selmer varieties*, Int. Math. Res. Not. IMRN **15** (2021), 11923–12008, DOI 10.1093/imrn/rnz362. MR4294137 ↑6

[BDM$^+$19] Jennifer Balakrishnan, Netan Dogra, J. Steffen Müller, Jan Tuitman, and Jan Vonk, *Explicit Chabauty-Kim for the split Cartan modular curve of level 13*, Ann. of Math. (2) **189** (2019), no. 3, 885–944, DOI 10.4007/annals.2019.189.3.6. MR3961086 ↑6

[BG06] Enrico Bombieri and Walter Gubler, *Heights in Diophantine geometry*, New Mathematical Monographs, vol. 4, Cambridge University Press, Cambridge, 2006. MR2216774 ↑1

[BSS$^+$16] Andrew R. Booker, Jeroen Sijsling, Andrew V. Sutherland, John Voight, and Dan Yasaki, *A database of genus-2 curves over the rational numbers*, LMS J. Comput. Math. **19** (2016), 235–254, DOI 10.1112/S146115701600019X. MR3540958 ↑6

[BCP97] Wieb Bosma, John Cannon, and Catherine Playoust, *The Magma algebra system. I. The user language*, J. Symbolic Comput. **24** (1997), no. 3-4, 235–265, DOI 10.1006/jsco.1996.0125. Computational algebra and number theory (London, 1993). MR1484478 ↑1

[Bru03] Nils Bruin, *Chabauty methods using elliptic curves*, J. Reine Angew. Math. **562** (2003), 27–49, DOI 10.1515/crll.2003.076. MR2011330 ↑6

[BF06] N. Bruin and E. V. Flynn, *Exhibiting SHA[2] on hyperelliptic Jacobians*, J. Number Theory **118** (2006), no. 2, 266–291, DOI 10.1016/j.jnt.2005.10.007. MR2225283 ↑2

[BPS16] Nils Bruin, Bjorn Poonen, and Michael Stoll, *Generalized explicit descent and its application to curves of genus 3*, Forum Math. Sigma **4** (2016), Paper No. e6, 80, DOI 10.1017/fms.2016.1. MR3482281 ↑2

[BS09] Nils Bruin and Michael Stoll, *Two-cover descent on hyperelliptic curves*, Math. Comp. **78** (2009), no. 268, 2347–2370, DOI 10.1090/S0025-5718-09-02255-8. MR2521292 ↑4, 6

[BS10] ———, *The Mordell-Weil sieve: proving non-existence of rational points on curves*, LMS J. Comput. Math. **13** (2010), 272–306, DOI 10.1112/S1461157009000187. MR2685127 ↑1, 5, 5, 5, 10

[Cas62] J. W. S. Cassels, *Arithmetic on curves of genus* 1. *IV. Proof of the Hauptvermutung*, J. Reine Angew. Math. **211** (1962), 95–112, DOI 10.1515/crll.1962.211.95. MR0163915 ↑2

[Cas83] ———, *The Mordell-Weil group of curves of genus* 2, Arithmetic and geometry, Vol. I, Progr. Math., vol. 35, Birkhäuser, Boston, MA, 1983, pp. 27–60. MR0717589 ↑2

[CF96] J. W. S. Cassels and E. V. Flynn, *Prolegomena to a middlebrow arithmetic of curves of genus* 2, London Mathematical Society Lecture Note Series, vol. 230, Cambridge University Press, Cambridge, 1996. MR1406090 ↑2

[Cha41] Claude Chabauty, *Sur les points rationnels des courbes algébriques de genre supérieur à l'unité*, Comptes Rendus Hebdomadaires des Séances de l'Académie des Sciences, Paris **212** (1941), 882–885 (French).Zbl 0025.24902 ↑1

[Col85] Robert F. Coleman, *Effective Chabauty*, Duke Math. J. **52** (1985), no. 3, 765–770, DOI 10.1215/S0012-7094-85-05240-8. MR0808103 ↑1, 5

[CMSV19] Edgar Costa, Nicolas Mascot, Jeroen Sijsling, and John Voight, *Rigorous computation of the endomorphism ring of a Jacobian*, Math. Comp. **88** (2019), no. 317, 1303–1339, DOI 10.1090/mcom/3373. MR3904148 ↑5

[CM00] John E. Cremona and Barry Mazur, *Visualizing elements in the Shafarevich-Tate group*, Experiment. Math. **9** (2000), no. 1, 13–28. MR1758797 ↑2

[Dog25] Netan Dogra, *2-descent for Bloch–Kato Selmer groups and rational points on hyperelliptic curves I*, August 13, 2025. https://arxiv.org/abs/2312.04996. ↑6

[Dog24] ———, *2-descent for Bloch–Kato Selmer groups and rational points on hyperelliptic curves II*, March 12, 2024. https://arxiv.org/abs/2403.07476. ↑6

[EL23] Bas Edixhoven and Guido Lido, *Geometric quadratic Chabauty*, J. Inst. Math. Jussieu **22** (2023), no. 1, 279–333, DOI 10.1017/S1474748021000244. MR4556934 ↑6

[Fal83] G. Faltings, *Endlichkeitssätze für abelsche Varietäten über Zahlkörpern*, Invent. Math. **73** (1983), no. 3, 349–366, DOI 10.1007/BF01388432 (German). MR0718935 ↑1

[Fal84] ———, *Erratum: "Finiteness theorems for abelian varieties over number fields"*, Invent. Math. **75** (1984), no. 2, 381, DOI 10.1007/BF01388572 (German). MR0732554 ↑1

[Fis14] Tom Fisher, *On families of 7- and 11-congruent elliptic curves*, LMS J. Comput. Math. **17** (2014), no. 1, 536–564, DOI 10.1112/S1461157014000059. MR3356045 ↑5.4

[Fis15] ———, *On families of 9-congruent elliptic curves*, Acta Arith. **171** (2015), no. 4, 371–387, DOI 10.4064/aa171-4-5. MR3430770 ↑5.4

[Fis18] ———, *Explicit moduli spaces for congruences of elliptic curves*, April 26, 2018. https://arxiv.org/abs/1804.10195. ↑5.4

[Fis19] ———, *On families of 13-congruent elliptic curves*, December 23, 2019. https://arxiv.org/abs/1912.10777. ↑5.4

[Fis21] ———, *On pairs of 17-congruent elliptic curves*, June 3, 2021. https://arxiv.org/abs/2106.02033. ↑5.4

[FY23] Tom Fisher and Jiali Yan, *Computing the Cassels-Tate pairing on the 2-Selmer group of a genus 2 Jacobian*, June 9, 2023. https://arxiv.org/abs/2306.06011. ↑2

[Fly04] E. V. Flynn, *The Hasse principle and the Brauer-Manin obstruction for curves*, Manuscripta Math. **115** (2004), no. 4, 437–466, DOI 10.1007/s00229-004-0502-9. MR2103661 ↑5

[FPS97] E. V. Flynn, Bjorn Poonen, and Edward F. Schaefer, *Cycles of quadratic polynomials and rational points on a genus-2 curve*, Duke Math. J. **90** (1997), no. 3, 435–463, DOI 10.1215/S0012-7094-97-09011-6. MR1480542 ↑1

[LV20] Brian Lawrence and Akshay Venkatesh, *Diophantine problems and* p*-adic period mappings*, Invent. Math. **221** (2020), no. 3, 893–999, DOI 10.1007/s00222-020-00966-7. MR4132959 ↑1

[LMFDB] The LMFDB Collaboration, *The L-functions and modular forms database, genus 2 curves over* $\mathbb{Q}$, 2025. https://www.lmfdb.org/Genus2Curve/Q/ [accessed 2025-09-28]. ↑6

[MP12] William McCallum and Bjorn Poonen, *The method of Chabauty and Coleman*, Explicit methods in number theory, Panor. Synthèses, vol. 36, Soc. Math. France, Paris, 2012, pp. 99–117 (English, with English and French summaries). MR3098132 ↑1, 5

[Mor22] L. J. Mordell, *On the rational solutions of the indeterminate equations of the third and fourth degrees.*, Proceedings of the Cambridge Philosophical Society **21** (1922), 179–192.JFM 48.1156.03 ↑1

[Poo06] Bjorn Poonen, *Heuristics for the Brauer-Manin obstruction for curves*, Experiment. Math. **15** (2006), no. 4, 415–420. MR2293593 ↑5

[PS97] Bjorn Poonen and Edward F. Schaefer, *Explicit descent for Jacobians of cyclic covers of the projective line*, J. Reine Angew. Math. **488** (1997), 141–188, DOI 10.1515/crll.1997.488.141. MR1465369 ↑2

[PS99] Bjorn Poonen and Michael Stoll, *The Cassels-Tate pairing on polarized abelian varieties*, Ann. of Math. (2) **150** (1999), no. 3, 1109–1149, DOI 10.2307/121064. MR1740984 ↑2

[Sch98] Edward F. Schaefer, *Computing a Selmer group of a Jacobian using functions on the curve*, Math. Ann. **310** (1998), no. 3, 447–471, DOI 10.1007/s002080050156. MR1612262 ↑2

[Sch99] Victor Scharaschkin, *Local-global problems and the Brauer-Manin obstruction*, ProQuest LLC, Ann Arbor, MI, 1999. Thesis (Ph.D.)–University of Michigan. MR2700328 ↑5

[Sto99] Michael Stoll, *On the height constant for curves of genus two*, Acta Arith. **90** (1999), no. 2, 183–201. MR1709054 ↑1

[Sto01] ———, *Implementing 2-descent for Jacobians of hyperelliptic curves*, Acta Arith. **98** (2001), no. 3, 245–277, DOI 10.4064/aa98-3-4. MR1829626 ↑2

[Sto06] ———, *Independence of rational points on twists of a given curve*, Compos. Math. **142** (2006), no. 5, 1201–1214, DOI 10.1112/S0010437X06002168. MR2264661 ↑1, 5

[Sto07] ———, *Finite descent obstructions and rational points on curves*, Algebra Number Theory **1** (2007), no. 4, 349–391, DOI 10.2140/ant.2007.1.349. MR2368954 ↑5

[Sto08] ———, *Rational 6-cycles under iteration of quadratic polynomials*, LMS J. Comput. Math. **11** (2008), 367–380, DOI 10.1112/S1461157000000644. MR2465796 ↑1

[Sto11] ———, *Rational points on curves*, J. Théor. Nombres Bordeaux **23** (2011), no. 1, 257–277 (English, with English and French summaries). MR2780629 ↑5

[Sto17] ———, *An explicit theory of heights for hyperelliptic Jacobians of genus three*, Algorithmic and experimental methods in algebra, geometry, and number theory, Springer, Cham, 2017, pp. 665–715. MR3792747 ↑4

[Sto22] ———, *Documentation for the ratpoints program*, January 8, 2022. https://arxiv.org/abs/0803.3165. ↑5

[Sut25] Andrew Sutherland, *Genus 2 curves over* $\mathbb{Q}$, 2025. https://math.mit.edu/~drew/newg2c_provisional.txt. ↑6

[Tat63] John Tate, *Duality theorems in Galois cohomology over number fields*, Proc. Internat. Congr. Mathematicians (Stockholm, 1962), Inst. Mittag-Leffler, Djursholm, 1963, pp. 288–295. MR0175892 ↑2

[Wei29] A. Weil, *L'arithmétique sur les courbes algébriques.*, Acta Mathematica **52** (1929), 281–315, DOI 10.1007/BF02592688, available at https://eudml.org/doc/192777 (French).JFM 55.0713.01 ↑1, 2

Mathematisches Institut, Universität Bayreuth, 95440 Bayreuth, Germany

Email address: Michael.Stoll@uni-bayreuth.de

URL: http://www.mathe2.uni-bayreuth.de/stoll/