J. S. Müller, B. Reitsma *Res. Number Theory (2023)9:23*
https://doi.org/10.1007/s40993-023-00429-x

Research in Number Theory

RESEARCH

Computing torsion subgroups of Jacobians of hyperelliptic curves of genus 3

J. Steffen Müller* and Berno Reitsma

*Correspondence:
steffen.muller@rug.nl
Bernoulli Institute, University of Groningen, Nijenborgh 9, 9747 AG Groningen, The Netherlands

Abstract

We introduce an algorithm to compute the structure of the rational torsion subgroup of the Jacobian of a hyperelliptic curve of genus 3 over the rationals. We apply a `Magma` implementation of our algorithm to a database of curves with low discriminant due to Sutherland as well as a list of curves with small coefficients. In the process, we find several torsion structures not previously described in the literature. The algorithm is a generalisation of an algorithm for genus 2 due to Stoll, which we extend to abelian varieties satisfying certain conditions. The idea is to compute p-adic torsion lifts of points over finite fields using the Kummer variety and to check whether they are rational using heights. Both have been made explicit for Jacobians of hyperelliptic curves of genus 3 by Stoll. This article is partially based on the second-named author's Master thesis.

Keywords: Torsion points, Hyperelliptic curves, Abelian varieties, Jacobians, Curves of genus three

1 Introduction

For an abelian variety $A/\mathbb{Q}$, the torsion subgroup $A(\mathbb{Q})_{\text{tors}}$ of the group $A(\mathbb{Q})$ of $\mathbb{Q}$-rational points on A is finite. If $A = E$ is an elliptic curve, it is easy to compute $E(\mathbb{Q})_{\text{tors}}$, and for Jacobians of genus 2 curves, there is a p-adic algorithm due to Stoll (see [27, Sect. 11]). In the present paper, we give a theoretical extension of Stoll's algorithm to arbitrary abelian varieties $A/\mathbb{Q}$. We then make this extension practical for Jacobians of hyperelliptic curves of genus 3. The latter heavily uses explicit arithmetic on the Kummer variety of such a Jacobian, also due to Stoll [30].

Our main motivation comes from a database of hyperelliptic curves of genus 3 due to Andrew Sutherland [32]. Similar to databases of elliptic curves and curves of genus 2 in the `LMFDB` [34], it would be useful to compute the most important arithmetic invariants of these curves, including the structure of the subgroup of rational torsion points on its Jacobian. Sutherland asked for an algorithm to accomplish this in 2017. We have used our algorithm to compute the torsion subgroups of all curves in the database, see Sect. 5.2.

In this computation we found several torsion structures that were not previously known in the literature. Recall that for elliptic curves over $\mathbb{Q}$, Mazur's Theorem gives a complete list of all torsion subgroups up to isomorphism. For dimension $d > 1$, it is not even known whether there is a uniform bound on the size of all rational torsion subgroups of abelian

© The Author(s) 2023. This article is licensed under a Creative Commons Attribution 4.0 International License, which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons licence, and indicate if changes were made. The images or other third party material in this article are included in the article's Creative Commons licence, unless indicated otherwise in a credit line to the material. If material is not included in the article's Creative Commons licence and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder. To view a copy of this licence, visit http://creativecommons.org/licenses/by/4.0/.

varieties over $\mathbb{Q}$ of dimension d. A lot of work has gone into constructing Jacobians of genus 2 curves with large torsion orders (see for instance [13] and the references therein). Some constructions of rational torsion points of large order on Jacobians of hyperelliptic genus 3 curves can be found in [12,17,23] and in [8,18], where families of Jacobians with large rational torsion are constructed that contain hyperelliptic genus 3 examples. A list of orders of rational torsion points for such curves known in the literature can be found in [23, Table 3.2]. However, much less is known than for genus 2. Therefore it is interesting to investigate which abelian groups actually occur. Inspired by a search by Howe for $g = 2$ [13], we ran through a list of certain hyperelliptic genus 3 curves with small coefficients, and we found many new torsion structures in this way, see Sect. 5.3.2. We obtain the following list of all torsion structures that are currently known to occur.

Theorem 1.1 *Every abelian group of order ≤ 44 is isomorphic to the group of rational torsion points on a geometrically simple Jacobian of a hyperelliptic curve over $\mathbb{Q}$ of genus 3, with the possible exception of the groups with invariant factors* [3, 3, 3], [3, 9], [2, 4, 4], [6, 6]. *In addition, the abelian groups with the following invariant factors are isomorphic to the group of rational torsion points on a geometrically simple Jacobian of a hyperelliptic curve over $\mathbb{Q}$ of genus 3:*

[46], [2, 2, 2, 6], [2, 2, 12], [2, 24], [4, 12], [48], [49], [50], [51], [2, 26], [52], [3, 18], [54], [2, 2, 14], [2, 28], [56], [58], [2, 30], [63], [2, 2, 2, 2, 2, 2], [2, 2, 2, 2, 4], [2, 2, 2, 8], [2, 4, 8], [2, 32], [64], [65], [70], [6, 12], [72], [2, 2, 2, 10], [2, 2, 20], [2, 42], [2, 44], [91], [2, 2, 28], [2, 52], [2, 2, 2, 2, 10],

All torsion structures in Theorem 1.1 came up in our search or in Sutherland's database, except for the groups $(\mathbb{Z}/2\mathbb{Z})^5$, $(\mathbb{Z}/2\mathbb{Z})^6$, $(\mathbb{Z}/2\mathbb{Z})^4 \times \mathbb{Z}/4\mathbb{Z}$ and $(\mathbb{Z}/2\mathbb{Z})^3 \times \mathbb{Z}/6\mathbb{Z}$, which we constructed. We do not claim that the groups listed as exceptions in Theorem 1.1 do not occur; we simply did not find such examples in our computations or the literature. Using our computations we found examples for all torsion structures that appeared in the literature prior to our work; in particular, we found new examples for the largest known prime group order 43 and the largest known point order 91, both exhibited by Nicholls [23]. The group $(\mathbb{Z}/2\mathbb{Z})^4 \times \mathbb{Z}/10\mathbb{Z}$ is the largest group of rational torsion points on a geometrically simple Jacobian of a hyperelliptic genus 3 curve found so far; no such group of size > 91 was previously known.

Remark 1.2 We focused on geometrically simple examples. More generally, we have found, for every abelian group A of order < 45 except for the groups with invariant factors [3, 3, 3] and [3, 9], a Jacobian of a hyperelliptic curve over $\mathbb{Q}$ of genus 3 with group of rational torsion points isomorphic to A. We expect that many additional structures can be found by systematically gluing abelian varieties of lower dimension, for instance using the methods of [15].

There are other possible applications of our algorithm: The order of the rational torsion subgroup appears in the strong version of the conjecture of Birch and Swinnerton-Dyer, and we therefore need an algorithm to compute this quantity to gather empirical evidence for the conjecture. Finally, if J is the Jacobian of a smooth projective curve $X/\mathbb{Q}$ with $\mathrm{rk} J(\mathbb{Q}) = 0$, and we have an Abel–Jacobi embedding $j\colon X \to J$ defined over $\mathbb{Q}$, then

we can compute the set $X(\mathbb{Q})$ by finding $J(\mathbb{Q}) = J(\mathbb{Q})_{\mathrm{tors}}$ and checking which points $P \in J(\mathbb{Q})_{\mathrm{tors}}$ have a rational preimage under j.

1.1 Upper bounds using reduction

Let $A/\mathbb{Q}$ be an abelian variety. An upper bound on the order of $A(\mathbb{Q})_{\mathrm{tors}}$ can be computed easily as follows: For a prime p of good reduction for A and an integer m (which we require to be odd if $p = 2$), the restriction of the reduction map

$$\rho_p \colon A(\mathbb{Q}_p) \to \tilde{A}(\mathbb{F}_p)$$

to $A(\mathbb{Q}_p)[m]$ is injective, where $\tilde{A}/\mathbb{F}_p$ is the reduction of A modulo p (see [14, Theorem C.1.4]). We choose a set S containing a few small odd primes of good reduction and compute $\#\tilde{A}(\mathbb{F}_p)$ for all $p \in S$; then

$$\#A(\mathbb{Q})_{\mathrm{tors}} \mid \gcd_{p \in S} \#\tilde{A}(\mathbb{F}_p)\,.$$

We can obtain more information from the structure of $\tilde{A}(\mathbb{F}_p)$ rather than only its order.

Example 1.3 Consider the Jacobian J of

$$X \colon y^2 = x^8 + 2x^7 + 3x^6 + 4x^5 + 9x^4 + 8x^3 + 7x^2 + 2x + 1 =: f(x)\,.$$

The primes of bad reduction for X are 2, 3 and 13177. We find $\#\tilde{J}(\mathbb{F}_5) = 180$, $\#\tilde{J}(\mathbb{F}_7) = 666$, so that $\#J(\mathbb{Q})_{\mathrm{tors}} \mid 18$. A closer inspection shows

$$\tilde{J}(\mathbb{F}_5) \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/60\mathbb{Z}\,; \quad \tilde{J}(\mathbb{F}_7) \cong \mathbb{Z}/666\mathbb{Z}\,.$$

We conclude that $J(\mathbb{Q})_{\mathrm{tors}}$ is isomorphic to a subgroup of $\mathbb{Z}/6\mathbb{Z}$. We will see in Example 4.9 that $\#J(\mathbb{Q})[2] = 2$. To find $\#J(\mathbb{Q})_{\mathrm{tors}}$, it remains to check whether there is a rational point of order 3. Searching among small rational points on X, we find that $[(0, -1) - \infty_1]$ has this property, where ∞_1 is the point with coordinates $(0, 1)$ on the model

$$w^2 = 1 + 2z + 3z^2 + 4z^3 + 9z^4 + 8z^5 + 7z^6 + 2z^7 + z^8\,.$$

Most of the time, the upper bound that we get from considering the structure of $\tilde{A}(\mathbb{F}_p)$ for a reasonable number of primes p of good reduction is actually equal to the correct order. For instance, in the database [32], we found this to be the case for more than 97% of all Jacobians, where we used all good primes below 1000. For the remaining ones, the quotient is a small power of 2 in the vast majority of cases. See Sect. 5.2 for more details.

Example 1.3 has the convenient property that X has a rational point, which allows us to add points in $J(\mathbb{Q})$. The computer algebra system `Magma` [1] contains an algorithm to compute the group law in $J(k)$ for the Jacobian of a hyperelliptic curve of odd genus over a field k if a k-rational point on the curve is known; alternatively, one may use Sutherland's (more efficient) balanced divisor approach [33].

Now consider the following example, brought to our attention by Andrew Sutherland.

Example 1.4 Let $X/\mathbb{Q}$ be the hyperelliptic curve defined by

$$y^2 = 5x^8 - 14x^7 + 33x^6 - 36x^5 + 30x^4 + 2x^3 - 16x^2 + 20x - 7.$$

with Jacobian $J/\mathbb{Q}$. There seems to be a point of order 13 in $\tilde{J}(\mathbb{F}_p)$ for all good primes p. Is there a global point of order 13? The curve X does not seem to have any rational points, so

arithmetic in $J(\mathbb{Q})$ is not implemented. In any case, there are no obvious nontrivial points in $J(\mathbb{Q})$. We will show in Example 5.2 that $J(\mathbb{Q})_{\text{tors}} \cong \mathbb{Z}/13\mathbb{Z}$.

Our method for computing $J(\mathbb{Q})_{\text{tors}}$ follows an approach due to Stoll for dimension 2 [27, Sect. 11], and works as follows: We lift points of order m coprime to p to $A(\mathbb{Q}_p)[m]$ and then check whether the lift is rational. To do so, one potential approach is to represent points in $A(\mathbb{Q}_p)$ using a projective embedding of A. This, however, is much too complicated in practice, since in general one would have to work in $\mathbb{P}^{4^g-1}$ and no explicit projective embedding is known for $g > 2$. Instead, we follow Stoll in using the Kummer variety of A. This is practical for Jacobians of hyperelliptic curves of genus 3, since the required explicit theory of the Kummer variety and of heights was developed by Stoll in [30].

1.2 Outline

We gather preliminaries on Kummer varieties and heights on abelian varieties in Sect. 2. In Sect. 3 we generalise Stoll's algorithm for the computation of $J(\mathbb{Q})_{\text{tors}}$ when J is the Jacobian of a genus 2 curve to abelian varieties $A/\mathbb{Q}$ that satisfy Assumption 3.1. Then we show that this assumption is satisfied for Jacobians of hyperelliptic curves of genus 3 in Sect. 4. Finally, we discuss our computations in Sect. 5.

2 Kummer varieties and heights

If A/k is an abelian variety of dimension $g > 0$ over a field k, then the *Kummer variety* K/k of A is defined as $K := A/\langle -1\rangle$. The quotient map is $2:1$ except at points of order 2 in A, where it is injective. The images of these points are the singular points of K. By [2, Theorem 4.8.1], K can be embedded into $\mathbb{P}^{2^g-1}$. We fix a rational map

$$\kappa : A \to \mathbb{P}^{2^g-1} \tag{2.1}$$

such that the image $\kappa(A)$ is a birational model for K.

Since κ identifies inverses on A, the group structure is lost, but scalar multiplication $[n]\colon A \to A$ descends, since it commutes with inversion. In fact, there is a rational map $[[n]]\colon K \to K$ such that

$$\begin{array}{ccc} A & \xrightarrow{[n]} & A \\ \downarrow{\scriptstyle\kappa} & & \downarrow{\scriptstyle\kappa} \\ K & \xrightarrow{[[n]]} & K \end{array}$$

commutes. Furthermore, there is a rational map $B\colon \mathrm{Sym}^2(K) \to \mathrm{Sym}^2(K)$ which, for $Q_1, Q_2 \in A$, sends the unordered pair $\{\kappa(Q_1), \kappa(Q_2)\}$ to the unordered pair $\{\kappa(Q_1 + Q_2), \kappa(Q_1 - Q_2)\}$. We suppose that algorithms for the following tasks are available:

- `Double`: Given $\kappa(Q)$ for $Q \in A(k)$, return $[[2]](\kappa(Q)) = \kappa(2Q)$.
- `PseudoAdd`: Given $\kappa(Q_1), \kappa(Q_2), \kappa(Q_1 - Q_2)$ for $Q_1, Q_2 \in A(k)$, return $\kappa(Q_1 + Q_2)$.

This leads to the following double-and-add algorithm to compute $[[n]](R)$ for $n \in \mathbb{Z} \setminus \{0\}$ and $R \in K$.

Algorithm 2.1 **Multiplication-by-n on the Kummer**
Input: $R \in K(k)$, $n \in \mathbb{Z}$
Output: $[[n]](R)$

(1) Set $\boldsymbol{x} := \kappa(0)$, $\boldsymbol{y} := R$, $\boldsymbol{z} := R$ and $m := |n|$.

(2) While $m \neq 0$, repeat the following steps.

  (a) If m is odd, then set $\boldsymbol{x} := \texttt{PseudoAdd}(\boldsymbol{x}, \boldsymbol{z}, \boldsymbol{y})$. Else, set $\boldsymbol{y} := \texttt{PseudoAdd}(\boldsymbol{y}, \boldsymbol{z}, \boldsymbol{x})$.
  (b) Set $\boldsymbol{z} := \texttt{Double}(\boldsymbol{z})$.
  (c) Set $m := \lfloor \frac{m}{2} \rfloor$.

(3) Return $\boldsymbol{x} := [[m]](R)$.

Algorithm 2.1 is a generalisation of the Montgomery ladder for elliptic curves; the genus 2 case is discussed in [11].

Now suppose that $k = \mathbb{Q}$. Then we can use the map κ to define heights on $A(\mathbb{Q})$ as follows. The *naive height* $h\colon A(\mathbb{Q}) \to \mathbb{R}_{\geq 0}$ is the function $h := \log(H \circ \kappa)$, where $H\colon \mathbb{P}^{2^g-1}(\mathbb{Q}) \to \mathbb{R}_{\geq 0}$ is the usual height given by mapping $P = (x_1 : \ldots : x_{2^g})$ to $\max(|x_1|, \ldots, |x_{2^g}|)$, where $x_1, \ldots, x_{2^g}$ are coprime integers. The map h is quadratic up to a bounded function, hence the *canonical height* is well-defined:

$$\hat{h}(Q) := \lim_{n\to\infty} \frac{h(nQ)}{n^2}$$

Theorem 2.2 (Néron-Tate) [14, Theorem B.5.1] *The following properties are satisfied.*

(1) $\hat{h}(nQ) = n^2\hat{h}(Q)$ *for all* $n \in \mathbb{Z}$ *and* $Q \in A(\mathbb{Q})$.
(2) *For* $Q \in A(\mathbb{Q})$, *we have* $\hat{h}(Q) = 0$ *if and only if* $Q \in A(\mathbb{Q})_{\text{tors}}$.
(3) *The set* $\{Q \in A(\mathbb{Q}) : \hat{h}(Q) \leq B\}$ *is finite for every constant* $B \geq 0$.
(4) *The height difference* $|\hat{h} - h|$ *is bounded.*

By Theorem 2.2(2), torsion points have small naive height. More precisely, suppose that $\beta \in \mathbb{R}_{\geq 0}$ satisfies

$$|\hat{h}(Q) - h(Q)| < \beta$$

for all $Q \in A(\mathbb{Q})$. We call β a *height difference bound*.

Corollary 2.3 *Let* $Q \in A(\mathbb{Q})_{\text{tors}}$. *Then* $H(Q) < e^{\beta}$.

To compute an explicit bound β, the standard approach is to decompose the difference between the naive height and the canonical height into local components, see for instance [11, Theorem 4]. As we shall see, β will help us decide whether a p-adic torsion point is $\mathbb{Q}$-rational or not.

3 An algorithm for finding torsion subgroups of abelian varieties

Let $A/\mathbb{Q}$ denote an abelian variety with Kummer variety $K/\mathbb{Q}$ and a fixed map κ as in (2.1). In this section we discuss an algorithm which computes the group $A(\mathbb{Q})_{\text{tors}}$ as an abstract abelian group, provided Assumption 3.1 below is satisfied. Our algorithm is based on an algorithm for Jacobians of genus 2 curves due to Stoll [27, Sect. 11].

Assumption 3.1 *We have algorithms for the following:*

(1) *the map* $\kappa : A \to K \subset \mathbb{P}^{2^g-1}$ *and equations for its image;*
(2) *deciding whether a given point* $R \in K(\mathbb{Q})$ *lifts to* $A(\mathbb{Q})$ *under* κ*;*
(3) *the maps* $[[2]]$ *and* B*;*
(4) *a height difference bound* β*;*

(5) *arithmetic in the group $\tilde{A}(\mathbb{F}_p)$ for primes of good reduction p and enumeration of its elements.*

The algorithm in [27, Sect. 11] crucially relies on the fact that Assumption 3.1 is satisfied for Jacobians of curves of genus 2, see Sect. 3.4. We will show in Sect. 4 that it is also satisfied for Jacobians of hyperelliptic curves of genus 3.

Remark 3.2 We can replace (5) by the assumption that we also have (1), (2) and (3) for the reduction $\tilde{K}/\mathbb{F}_p$ if p is a prime of good reduction. This is the case, for instance, for Jacobians of hyperelliptic curves of genus ≤ 3 (for $g = 3$, we need $p > 2$). We can then enumerate $\tilde{K}(\mathbb{F}_p)$ and check which elements lift to $\tilde{A}(\mathbb{F}_p)$ to compute the latter. Moreover, arithmetic in $\tilde{A}(\mathbb{F}_p)$ can be reduced to arithmetic in $\tilde{K}(\mathbb{F}_p)$, for which we can use (3). In practice, we prefer to compute (in) $\tilde{A}(\mathbb{F}_p)$ directly.

The strategy can be summarised as follows. One first uses reduction modulo p for a number of good primes p to obtain an integer $d > 0$ such that $\#A(\mathbb{Q})_{\text{tors}} \mid d$. For each prime $q \mid d$, we find the q-Sylow subgroup of $A(\mathbb{Q})_{\text{tors}}$; to this end, we first choose a suitable good prime $p \neq q$. For each $\tilde{Q} \in \tilde{A}(\mathbb{F}_p)$ of q-power order m, we can compute the unique lift[1] $\tilde{\kappa}(\tilde{Q})$ in $\kappa(A(\mathbb{Q}_p)[m])$ to any desired precision p^N. Using β, we choose N and construct a lattice L with the following property: If there is a point $R \in \kappa(A(\mathbb{Q}_p)[m]) \cap K(\mathbb{Q})$ that reduces to our approximation of $\tilde{\kappa}(\tilde{Q})$ modulo p^N, then the shortest nontrivial vector in L must be this point R. We can decide whether such a point exists by applying the LLL algorithm. If it does, then it remains to check whether it lifts to $A(\mathbb{Q})[m]$. See Algorithm 3.4 for odd q. This is then used in Algorithm 3.14, which computes the q-part of $A(\mathbb{Q})_{\text{tors}}$ for odd q. The case $q = 2$ is discussed in Sect. 3.2.1. Finally, Algorithm 3.15 computes $A(\mathbb{Q})_{\text{tors}}$, provided Assumption 3.1 is satisfied.

Remark 3.3 We stress that we do not assume that we can explicitly compute in $A(\mathbb{Q})$; nor do we assume that we can explicitly write down points in $A(\mathbb{Q})$. If the latter is possible and if we can compute the preimages under κ in (2), then we can also find $A(\mathbb{Q})_{\text{tors}}$ as a set, see Remark 3.16 below.

3.1 Checking whether reduced points lift

The most challenging part of the algorithm is to check whether a reduced torsion point lifts to a rational torsion point or not. More specifically, given a prime p of good reduction and a point $\tilde{Q} \in \tilde{A}(\mathbb{F}_p)$ of order m coprime to p, there exists a unique lift $Q \in A(\mathbb{Q}_p)[m]$ such that Q reduces to $\tilde{Q}$. This algorithm decides whether $Q \in A(\mathbb{Q}) \subset A(\mathbb{Q}_p)$. Below, we will apply the LLL-algorithm with standard parameter $\delta = \frac{3}{4}$ (see [19]).

Algorithm 3.4 **Lifting Torsion Points**

Input: An abelian variety $A/\mathbb{Q}$ such that Assumption 3.1 is satisfied and a point $\tilde{Q} \in A(\mathbb{F}_p)$ of order $m > 2$ coprime to p.

Output: TRUE if there is a point $Q \in A(\mathbb{Q})_{\text{tors}} \subset A(\mathbb{Q}_p)_{\text{tors}}$ that reduces to $\tilde{Q}$, else FALSE.

(1) Compute a height difference bound β for A.

[1] We hope that no confusion arises from using the word "lift" both for Hensel lifts as well as lifts of points from K to A.

(2) Choose $M = 1 + am$ such that $p \nmid a$.
(3) Let $\tilde{R}_0$ be $\tilde{\kappa}(\tilde{Q})$, considered on an affine patch in $\mathbb{A}^{2g}(\mathbb{Z}/p\mathbb{Z})$ and normalised such that the first nonzero coordinate is equal to 1. Set $r := 1$, $n := 0$.
(4) Let $N > 1$ such that $p^N > 2^{(2g+g)}e^{2\beta}$. While $r < N$, repeat the following steps:

  (a) Set $r := \min\{2r, N\}$.
  (b) Let $\tilde{R}'_n$ be any lift of $\tilde{R}_n$ to $\mathbb{A}^{2g}(\mathbb{Z}/p^r\mathbb{Z})$.
  (c) Set $\tilde{R}_{n+1} := \frac{1}{M-1}(M\tilde{R}'_n - [[M]](\tilde{R}'_n))$, where $M\tilde{R}'_n$ is obtained by multiplying the coordinates of $\tilde{R}'_n$ by M.
  (d) Set $n := n + 1$.

(5) Now, consider $\tilde{R}_n =: (\tilde{r}_1 : \ldots : \tilde{r}_{2g})$ in $K(\mathbb{Z}/p^N\mathbb{Z})$. Let $(r_1, \ldots, r_{2g}) \in \mathbb{Z}^{2g}$ reduce to $(\tilde{r}_1, \ldots, \tilde{r}_{2g})$ modulo p^N such that $0 \le r_i < p^N$ for all i. Let L be the lattice generated by $(r_1, \ldots, r_{2g})$ and by $(p^N e_1, \ldots, p^N e_{2g})$, where $(e_1, \ldots, e_{2g})$ is the standard basis of $\mathbb{Z}^{2g}$. Let w be the first basis vector of an LLL-reduced basis of L and let $R = \mathbb{P}w$ be the corresponding point in $\mathbb{P}^{2g-1}(\mathbb{Q})$.
(6) If $R \notin K(\mathbb{Q})$ or $H(R) > e^{\beta}$, return FALSE.
(7) If $[[m]](R) \neq \kappa(0)$, return FALSE.
(8) If $\kappa^{-1}(R) \subset A(\mathbb{Q})$, return TRUE. Else return FALSE.

We prove the correctness of the algorithm in Sect. 3.1.3. For Jacobians of curves of genus 2, this is sketched in Stoll [27, Sect. 11].

Theorem 3.5 *Algorithm 3.4 terminates and returns TRUE if and only if there is a point $Q \in A(\mathbb{Q})_{\text{tors}} \subset A(\mathbb{Q}_p)_{\text{tors}}$ that reduces to $\tilde{Q}$.*

We first need some preliminary results.

3.1.1 The lifting procedure

We start by showing that Step (4) of Algorithm 3.4 lifts to the m-torsion point that we want to approximate. We say that a point on K is *m-torsion* if the map $[[m]]$ sends it to $\kappa(0) \in K$. Equivalently, a point on K is m-torsion if and only if there is a point in $A[m]$ that maps to it under κ.

Proposition 3.6 *After Step (4)* of Algorithm 3.4, $\tilde{R}_n$ is the unique m-torsion point in $K(\mathbb{Z}/p^N\mathbb{Z})$ that reduces to $\kappa(\tilde{Q})$.

In order to prove Proposition 3.6, we first show that Step (c) approximates Q by an m-torsion lift to the required p-adic precision p^N. By [3, III, Sect. 8, Corollary 2] and [20], the group $A(\mathbb{Q}_p)$ is a p-adic abelian Lie group whose topology is the local product topology: a neighborhood of a point $Q \in A(\mathbb{Q}_p)$ is a neighborhood U of Q contained in an affine space, and for any $d \ge 1$, the p-adic topology on $\mathbb{A}^d(\mathbb{Q}_p) = \mathbb{Q}_p^d$ is induced by the maximum norm $\|\cdot\|_p$.

Lemma 3.7 *Let $Q \in A(\mathbb{Q}_p)$ be a torsion point of order m, not divisible by p. Let $n \ge 1$, let $\phi\colon A \to \mathbb{A}^n$ be a rational map defined over $\mathbb{Q}_p$ that is differentiable as a map $A(\mathbb{Q}_p) \to \mathbb{A}^n(\mathbb{Q}_p)$ and a p-adic immersion near Q, and let $a \in \mathbb{Z}$. If $U \subset A(\mathbb{Q}_p)$ is a neighborhood of Q, then for any $Q' \in U$, we have*

$$\phi([1 + am]Q') - \phi(Q) = (1 + am)(\phi(Q') - \phi(Q)) + O(\|\phi(Q') - \phi(Q)\|_p^2). \tag{3.1}$$

Proof For the proof, we set $M := 1 + am$, so that $[M](Q) = Q$. Near Q, the map ϕ is an immersion, so there is a well-defined map $[[M]]$ that makes the diagram

$$\begin{array}{ccc} A(\mathbb{Q}_p) & \xrightarrow{[M]} & A(\mathbb{Q}_p) \\ \downarrow{\scriptstyle\phi} & & \downarrow{\scriptstyle\phi} \\ \phi(A(\mathbb{Q}_p)) & \xrightarrow{[[M]]} & \phi(A(\mathbb{Q}_p)) \end{array} \tag{3.2}$$

commute on a neighborhood of Q. Since ϕ is a rational map to $\mathbb{A}^n$, we have that $\phi(A(\mathbb{Q}_p))$ consists of the $\mathbb{Q}_p$-rational points on an affine variety over $\mathbb{Q}_p$. Hence the differential of $[[M]]\colon \phi(A)(\mathbb{Q}_p) \to \phi(A)(\mathbb{Q}_p)$ at $\phi(Q)$ is the best linear approximation of $[[M]]$ around $\phi(Q)$. In other words, it consists of the linear terms of the Taylor expansion of $[[M]]$ around $\phi(Q)$. By [3, Chap. III, Sect. 2.2] the differential of the multiplication-by-M-map $[M]$ is scalar multiplication on the tangent space, and a computation using (3.2) shows that the same holds for the differential of $[[M]]$.

Now let Q' be close to Q, so that $\phi(Q')$ is close to $\phi(Q)$. By the above, we find

$$\begin{aligned}[[1+am]](\phi(Q')) - [[1+am]](\phi(Q)) &= (1+am)(\phi(Q') - \phi(Q)) \\ &\quad + O(\|\phi(Q') - \phi(Q)\|_p^2).\end{aligned}$$

Using (3.2), we have $[[1+am]](\phi(Q)) = \phi([1+am](Q)) = \phi(Q)$. Therefore (3.1) follows. □

We now apply Lemma 3.7 to a map $\phi\colon A \to \mathbb{A}^{2g}$ that factors through $\kappa\colon A \to K$.

Proof of Proposition 3.6 Since κ is differentiable outside $A[2]$, composing with a map that projects onto an affine patch results in a differentiable map that is a local immersion outside $A[2]$. Let ϕ denote the map κ composed with the projection onto a suitable affine patch. Then ϕ satisfies the conditions of Lemma 3.7 and we obtain

$$[[M]](\tilde{R}'_n) - \tilde{R}_{n+1} = M(\tilde{R}'_n - \tilde{R}_{n+1}) + O(\|\tilde{R}_{n+1} - \tilde{R}'_n\|_p^2).$$

By construction, we have $\|\tilde{R}_{n+1} - \tilde{R}'_n\|_p^2 = p^{-r}$ in Step (4) of Algorithm 3.4, and therefore

$$\tilde{R}_{n+1} = \frac{1}{M-1}(M\tilde{R}'_n - [[M]](\tilde{R}'_n)) + O(p^r)$$

is the m-torsion point in $K(\mathbb{Z}/p^r\mathbb{Z})$ that reduces to $\kappa(\tilde{Q})$. □

Remark 3.8 Intuitively, one can view ϕ as a map that gives local affine coordinates of Q with the property that we can find a best linear approximation of the multiplication-by-$(1+am)$-map. For the approximation in Step (c), one may use a different projection onto $\mathbb{A}^{2g}$ in every iteration of Step (4). This may be necessary if, for example, the first coordinate of R is divisible by p^r, but is not divisible by p^{2r} for some $r \geq 1$.

Remark 3.9 In [27, Sect. 11], it is assumed that p divides M. Here, we generalise this by allowing $M \not\equiv 1 \mod p$. One way to use this additional flexibility in practice is to choose M to be a power of 2, because doubling on K is often faster than applying the map B. See Sect. 3.3.

3.1.2 Determining a suitable p-adic precision

We now show that we can find a p-adic precision such that the corresponding rational approximation $\tilde{R}_n \in K(\mathbb{Z}/p^N\mathbb{Z})$ either leads to a rational lift $R = \kappa(Q)$ such that $Q \in A(\mathbb{Q})$, or no such rational lift exists.

Proposition 3.10 *Let $N \in \mathbb{Z}$ be such that $p^N > 2^{(g+2^g)}e^{2\beta}$. Let $\tilde{R}_n$, $(r_1, \ldots, r_{2^g})$, L, w and R be as computed in Step (5)* of Algorithm 3.4. Then we have:

(a) If $H(R) \leq e^\beta$, then R is the unique point in $\mathbb{P}^{2^g-1}(\mathbb{Q})$ that satisfies $H(R) \leq e^\beta$ and reduces to $\tilde{R}_n$.
(b) If $H(R) > e^\beta$, then no point on $\mathbb{P}^{2^g-1}(\mathbb{Q})$ of height $\leq e^\beta$ reduces to $\tilde{R}_n$.

To lift points, we use the following result, whose proof is immediate.

Lemma 3.11 *Let $n, d \in \mathbb{Z}_{\geq 1}$ and let $\tilde{R} \in \mathbb{P}^d(\mathbb{Z}/p^n\mathbb{Z})$. Let*

$$v := (r_0, \ldots, r_d) \in \mathbb{Z}^{d+1} \setminus \{0\}$$

be primitive, i.e. $\gcd(r_0, \ldots, r_d) = 1$, *such that $R := \mathbb{P}v := (r_0 : \ldots : r_d) \in \mathbb{P}^d(\mathbb{Q})$ lifts $\tilde{R}$. Then the lattice L generated by $\{v\} \cup \{e_i p^n : 0 \leq i \leq d\}$ contains all vectors w such that the corresponding point $\mathbb{P}w \in \mathbb{P}^d(\mathbb{Q})$ reduces modulo p^n to $\tilde{R}$. Moreover, let*

$$u := a_0 v + p^n a_1 e_1 + \cdots p^n a_{d+1} e_{d+1} \in L,$$

where $a_0, \ldots, a_{d+1} \in \mathbb{Z}$. If $p \nmid a_0$, then $\mathbb{P}u \in \mathbb{P}^d(\mathbb{Q})$ reduces modulo p^n to $\tilde{R} \in \mathbb{P}^d(\mathbb{Z}/p^n\mathbb{Z})$.

Moreover, we need the following uniqueness result.

Lemma 3.12 *Let $B \geq 1$ be a real number and let $d \in \mathbb{Z}$ be positive. Let $u, u' \in \mathbb{Z}^{d+1} \setminus \{0\}$ such that*

(a) $\|u\|_\infty, \|u'\|_\infty \leq B$
(b) *there is an integer $D > 2B^2$ such that all 2×2 minors of the matrix $\begin{pmatrix} u \\ u' \end{pmatrix} \in \mathbb{Z}^{2\times(d+1)}$ are divisible by D.*

Then the points $\mathbb{P}u$ and $\mathbb{P}u'$ in $\mathbb{P}^d(\mathbb{Q})$ represented by u and u', respectively, are equal.

Proof By (a), the 2×2 minors have absolute value bounded by $2B^2$. Hence they all vanish by (b). Therefore $u = \lambda u'$ for some nonzero $\lambda \in \mathbb{Q}$. □

We apply Lemma 3.12 to the lattice L from Step (5) of Algorithm 3.4. We thank an anonymous referee for suggesting the structure of the following proof.

Proof of Proposition 3.10 By Lemma 3.11, the lattice L in Step (5) contains all integer representatives of the points in $\mathbb{P}^{2^g-1}(\mathbb{Q})$ that reduce to $\tilde{R}_n \in \mathbb{P}^{2^g-1}(\mathbb{Z}/p^N\mathbb{Z})$ as obtained after Step (4) of Algorithm 3.4. Moreover, any vector that corresponds to a lift of $\tilde{R}_n$ is of the form $u = a_0 v + p^N a_1 e_1 + \cdots p^N a_{2^g} e_{2^g}$ with $p \nmid a_0$. For such a vector u, we have

$$H(\mathbb{P}u) \leq \|u\|_\infty, \quad \text{with equality if and only if } u \text{ is primitive.} \tag{3.3}$$

Let $w \in \mathbb{Z}^{2^g}$ be the first vector of an LLL-reduced basis of L as in Step (5) of Algorithm 3.4. We distinguish cases as follows. First suppose that $\|w\|_\infty > 2^{(2^g-1)/2}\sqrt{2^g}e^\beta$. In this case, we claim that there is no nonzero vector $u \in L$ such that $\|u\|_\infty \leq e^\beta$. Indeed, our choice $\delta = 3/4$ of parameter in the LLL-algorithm implies that the first basis vector of an LLL-reduced basis has euclidean length at most $2^{(2^g-1)/2}$ times the euclidean length of the shortest nonzero vector (see [19]). In particular, there is no point in $\mathbb{P}^{2^g-1}(\mathbb{Q})$ of height $\leq e^\beta$ that reduces to $\tilde{R}_n$ by Lemma 3.11 and by (3.3).

Now suppose that $\|w\|_\infty \leq 2^{(2^g-1)/2}\sqrt{2^g}e^\beta$. By construction, all pairs of nonzero vectors in L satisfy condition (b) of Lemma 3.12 with $D = p^N > 2e^{2\beta}$. Since $2\cdot(2^{(2^g-1)/2}\sqrt{2^g}e^\beta)^2 = 2^{2^g}(2^g)e^{2\beta} < p^N$, we can apply Lemma 3.12 with $d = 2^g - 1$ and $B = 2^{(2^g-1)/2}\sqrt{2^g}e^\beta$. This implies that for any vector $w' \in L$ satisfying $\|w'\|_\infty \leq B$, we have $\mathbb{P}w' = \mathbb{P}w = R$. Hence, by Lemma 3.11 and by (3.3), if there is a point in $\mathbb{P}^{2^g-1}(\mathbb{Q})$ that reduces to $\tilde{R}_n$ and has height $\leq e^\beta$, then it must be R. □

3.1.3 The conclusions of the lift-checking algorithm

Proof of Theorem 3.5 It is clear that the algorithm terminates. To prove Theorem 3.5, it suffices to prove the correctness of Steps (6)–(8) of Algorithm 3.4, which we do now. Since a torsion point $P \in A(\mathbb{Q})$ satisfies $H(P) = H(\kappa(P)) \leq e^\beta$, Proposition 3.6 and Proposition 3.10 imply that if there is a point $Q \in A(\mathbb{Q})[m]$ that reduces to $\tilde{Q}$, then the point $R \in K(\mathbb{Q})$ from Step (4) of Algorithm 3.4 satisfies $R = \kappa(Q)$. Clearly we then have $[[m]](R) = \kappa(0)$ and $\kappa^{-1}(R) = \{\pm Q\} \subset A(\mathbb{Q})$, so that the algorithm returns TRUE.

Conversely, suppose that the algorithm returns TRUE. Then, using Propositions 3.6 and 3.10 again, R is the unique m-torsion point in $K(\mathbb{Q})$ that reduces to $\tilde{\kappa}(\tilde{Q})$. Thus the points in $\kappa^{-1}(R)$ are $\mathbb{Q}$-rational points of order m, so one of these two points is a point in $A(\mathbb{Q})[m] \subset A(\mathbb{Q})_{\text{tors}}$ that reduces to $\tilde{Q}$. □

Remark 3.13 In practice, we can often terminate the algorithm long before the required precision in Step (4) is reached, as follows: Let $\tilde{R}_r$ be as in Step (4), for some $r < N$. From $\tilde{R}_r$, determine R using Step (5) and check if the conditions of Step (6)–(8) are satisfied. If they are, then we have found a point $Q \in A(\mathbb{Q})[m]$ that reduces to $\tilde{Q}$. However, if no such point is found, then it is not guaranteed that no other candidate exists.

3.2 Computing the rational torsion subgroup

Now that we can conclusively decide for good primes p whether a point in $\tilde{A}(\mathbb{F}_p)$ lifts to $A(\mathbb{Q})_{\text{tors}}$ or not, we can find the rational torsion subgroup of $A(\mathbb{Q})$. Since we do not assume that we can represent or compute with general points in $A(\mathbb{Q})$, we compute $A(\mathbb{Q})_{\text{tors}}$ as an abstract abelian group by finding its invariant factors. This is again a generalisation of the idea proposed in [27, Sect. 11] for Jacobians of curves of genus 2. For a prime q and a finite abelian group G, we let the *q-part of G* be the q-Sylow subgroup of G, as an abstract abelian group. Then the reduction map $\rho_p\colon A(\mathbb{Q}_p) \to A(\mathbb{F}_p)$ is injective on q-parts of $A(\mathbb{Q})_{\text{tors}}$ for any prime number $q \neq p$.

Algorithm 3.14 **Computing the q-part of the torsion subgroup**

Input: an abelian variety $A/\mathbb{Q}$ for which Assumption 3.1 is satisfied and a prime $q > 2$.
Output: The q-part of $A(\mathbb{Q})_{\text{tors}}$ as an abstract abelian group.

(1) Let G_0 be the q-part of $\tilde{A}(\mathbb{F}_p)$, where p is a good prime not equal to q. Set $T_0 := \{0\} \subset G_0$, $S_0 := G_0 \setminus \{0\}$, $S_0' := \{0\}$. (Throughout, G_i is a quotient of G_0, T_i is a subgroup of G_0, and S_i and S_i' are subsets of G_i.)
(2) Set $n := 0$, repeat the following steps until $S_n = \emptyset$.
    (a) Let $g \in S_n \subset G_n$ and choose a representative $\tilde{g} \in G_0$ of g.
    (b) Using Algorithm 3.4, compute the smallest $\ell > 0$ such that $q^\ell\tilde{g}$ lifts to $A(\mathbb{Q})$.

(c) Set

$$\begin{aligned} T_{n+1} &:= \langle T_n, q^\ell \cdot \tilde{g} \rangle, \\ G_{n+1} &:= G_n / \langle q^\ell \cdot g \rangle, \\ S'_{n+1} &:= \text{ image of } S'_n \cup \langle g \rangle \text{ in } G_{n+1}, \\ S_{n+1} &:= G_{n+1} \setminus S'_{n+1}. \end{aligned}$$

(d) Set $n := n + 1$.

(3) Return T_n as an abstract abelian group.

It is preferable to take a primitive element in Step (a), but this is not required. In Step (1), we typically pick a prime p such that the q-part of $\tilde{A}(\mathbb{F}_p)$ is small. If it is trivial, then there is nothing to do. In practice, we have already computed $\tilde{A}(\mathbb{F}_p)$ for all good primes below some bound, see Algorithm 3.15 below.

3.2.1 Two-power torsion

Algorithm 3.4 excludes the case $m = 2$ because the lifting procedure does not work on points of order 2, since $\kappa(A[2])$ consists of singular points. It is still possible to compute $A(\mathbb{Q})[2]$, for instance by finding the solutions $R \in K(\mathbb{Q})$ of the projective system of equations $[[2]](R) = \kappa(0)$ and checking which of these lift . Hence we can skip this case in Algorithm 3.14. We can, alternatively, determine $A(\mathbb{Q})[2^\infty]$ iteratively as follows: For $s \geq 2$, we find $A(\mathbb{Q})[2^s]$ from $A(\mathbb{Q})[2^{s-1}]$ for $s \geq 2$ by solving the system $[[2]](R) = S$ for each $S \in \kappa(A(\mathbb{Q})[2^{s-1}])$ and checking which solutions lift. We implemented this strategy for Jacobians of hyperelliptic curves of genus 3, but we found that this is quite expensive. Fortunately, in this case there is a simpler method, discussed in Sect. 4.5.

3.2.2 The algorithm

Algorithm 3.15 **Computing the Torsion Subgroup**

Input: an abelian variety $A/\mathbb{Q}$ satisfying Assumption 3.1.

Output: the invariant factors of $A(\mathbb{Q})_{\text{tors}}$.

(1) Compute a height difference bound β.
(2) Compute a multiplicative upper bound t for the size of the torsion subgroup by computing the structure of $\tilde{A}(\mathbb{F}_p)$ for a reasonable number of good odd primes p.
(3) For each prime factor q of t, compute the q-part of $A(\mathbb{Q})_{\text{tors}}$ using Algorithm 3.14 and Sect. 3.2.1.
(4) Deduce the invariant factors of $A(\mathbb{Q})_{\text{tors}}$ from the invariant factors of its q-parts.

Remark 3.16 If we can describe points in $A(\mathbb{Q})$ explicitly and if we have an algorithm to compute $\kappa^{-1}(R)$ for given $R \in K(\mathbb{Q})$, then we can also return $\kappa^{-1}(R)$ in Step (8) of Algorithm 3.4. In this case, we can also compute (generators for) the q-part in Algorithm 3.14, rather than only its structure as an abstract abelian group. Hence we can amend Algorithm 3.15 to find generators for $A(\mathbb{Q})_{\text{tors}}$.

3.3 Avoiding the use of sum-and-difference-laws

In practice, one of the most expensive tasks in Algorithm 3.15 is the computation of $[[n]](R)$ for points $R \in K$ and potentially large $n \in \mathbb{Z}$. Namely, in Algorithm 3.4, we apply $[[M]]$ in Step (c) and we apply $[[m]]$ in Step (7). Recall from Algorithm 2.1 that the multiplication-by-n-map $[[n]]\colon K \to K$ requires formulas for the doubling map $[[2]]\colon K \to K$ and for the map $B\colon \mathrm{Sym}^2(K) \to \mathrm{Sym}^2(K)$ such that

$$B(\{\kappa(Q_1), \kappa(Q_2)\}) = \{\kappa(Q_1 + Q_2), \kappa(Q_1 - Q_2)\}$$

for $Q_1, Q_2 \in A$. For Jacobians of hyperelliptic curves of genus ≤ 3, the formulas for the map B are much more complicated than those for the map $[[2]]$. Hence, we prefer to apply the map $[[n]]$ only for small n of the form $n = \pm 2^s$ since then the doubling formulas suffice. In addition, we might be in a situation where the doubling map $[[2]]$ is available explicitly, but the map B is not. Then it turns out that it is often still possible to compute $A(\mathbb{Q})_{\mathrm{tors}}$, as we now explain.

Recall that by construction, m is a power of a prime $q \geq 2$. In most cases, m will be small. We require M to satisfy $M \equiv 1 \bmod m$ and $M \not\equiv 1 \bmod p$, so we can use $M = 1 - m$ if we want to keep M small. If m is odd, it is clear that we can instead find a suitable M of the form $M = \pm 2^s$, and Step (c) of Algorithm 3.4 can be performed using only the map $[[2]]$. This does not work when m is even. However, recall that we can use the strategy discussed in Sect. 3.2.1 to compute the 2-part of $A(\mathbb{Q})_{\mathrm{tors}}$ without Step (c) of Algorithm 3.4.

Besides Step (c), arithmetic on K is also used in Step (7) of Algorithm 3.4. Here, we check whether a point $R \in K(\mathbb{Q})$ satisfies $[[m]](R) = \kappa(0)$. If arithmetic in $A(\mathbb{Q})$ is implemented, for instance when A is the Jacobian of a hyperelliptic curve of even genus or odd degree, then we can avoid Step (7) by first computing $\kappa^{-1}(R) \cap A(\mathbb{Q})$. If this set is non-empty, say containing a point Q, then we can check directly whether $mQ = 0 \in A(\mathbb{Q})$. If no algorithm for arithmetic in $A(\mathbb{Q})$ is available, then we can only avoid the use of the map B in Step (7) for specific values of m. For instance, suppose that all prime powers m dividing t in Algorithm 3.15 are at most 60. Then we can avoid the use of B if and only if all these m satisfy $m \in \{2^u : u \in \mathbb{Z}_{\geq 1}\} \cup \{3, 9, 5, 7, 17, 31\}$, and if t is not divisible by both 7 and 9. See [25, Sect. 4.7] for details.

3.4 Computing torsion subgroups for Jacobians of genus 2 curves

Suppose that $A = J$ is the Jacobian of a curve $X/\mathbb{Q}$ of genus 2 and let K denote its Kummer surface. We may assume that X is given by an equation $y^2 = f(x)$, where $f \in \mathbb{Q}[x]$ is squarefree and has degree 5 or 6. If $\deg(f) = 5$, then we can represent points on J using the (affine) Mumford representation. More generally, points in $J(\mathbb{Q})$ correspond bijectively to triples (A, B, C) of binary forms over $\mathbb{Q}$ of homogeneous degrees 2, 3 and 4, respectively, such that the degree 6 homogenisation F of f satisfies $F = B^2 - AC$ (see [4]). One can use this representation to compute in the group $J(\mathbb{Q})$ via a generalisation of Cantor's algorithm [6]. In fact, Cantor's algorithm has been extended to any curve of genus 2 over any field.

Assumption 3.1 is satisfied for J:

- A morphism $\kappa\colon J \to \mathbb{P}^3$ such that $\kappa(J)$ is a model for K was given by Flynn [9], see also [7, Chap. 3]. In this case the Kummer surface is a quartic hypersurface.
- A point in $K(\mathbb{Q})$ lifts to $J(\mathbb{Q})$ if and only if the expressions in Equations (5.1, 5.2) of [29] are squares in $\mathbb{Q}$.

- The map $[[2]]$ is given by quartic polynomials and $B\colon \mathrm{Sym}^2(K) \to \mathrm{Sym}^2(K)$ is given by biquadratic forms; explicit formulas can be found in [7, Sect. 3].
- There is an explicit theory of heights which allows us to compute a height difference bound β; see [10,11,21,27].

Hence Algorithm 3.15 can be used to compute $\#J(\mathbb{Q})_{\mathrm{tors}}$. In fact, one can compute (in) $\tilde{J}(\mathbb{F}_p)$ for primes p of good reduction using the (generalised) Mumford representation, which is faster than the approach in Remark 3.2. Moreover, we can compute $J(\mathbb{Q})[2]$ easily using the prime factorisation of f in $\mathbb{Q}[x]$, see [28, Lemma 4.3, Lemma 5.6].

Using the generalised Mumford representation, we can actually compute generators of $J(\mathbb{Q})_{\mathrm{tors}}$. As mentioned above, this is essentially already discussed in [27, Sect. 11] and an implementation is available in `Magma`.

4 Computing torsion subgroups of Jacobians of genus 3 hyperelliptic curves

Section 3 gives a complete algorithm to compute the torsion subgroup for an abelian variety that satisfies Assumption 3.1. In this section, we show that Assumption 3.1 is satisfied when $A = J$ is the Jacobian of a hyperelliptic curve of genus 3. Hence we obtain an algorithm to compute $J(\mathbb{Q})_{\mathrm{tors}}$, which we have implemented in `Magma` and which is available at https://github.com/bernoreitsma/g3hyptorsion. This answers a question raised by Andrew Sutherland at the 2017 Banff Workshop "Arithmetic Aspects of Explicit Moduli Problems".

Throughout this section, we fix a field k such that $\mathrm{char}(k) \neq 2$ and a hyperelliptic curve X/k of genus 3 given by an equation

$$X\colon y^2 = f(x),$$

where $f \in k[x]$ is squarefree of degree 7 or 8. Let $\iota\colon X \to X$ be the hyperelliptic involution and let J/k be the Jacobian of X. We will represent (most) points on J using the following notion:

Definition 4.1 A divisor D on X is *in general position* if it is effective and if there is no point $P \in X$ such that $D \geq (P) + \iota(P)$.

In the literature, the explicit theory of hyperelliptic curves is usually first developed for the case where the polynomial f has odd degree. More generally, if $X(k)$ contains a Weierstrass point, then we may apply a transformation to get an odd degree equation over k. In this case, every point on the Jacobian can be represented uniquely by a divisor of the form $D - d(\infty)$, where $d \leq 3$ and D is in in general position. This leads to the unique Mumford representation (a, b) of a point $Q \in J(k)$, where $a \in k[x]$ is monic of degree d and vanishes precisely in the x-coordinates of the points in $\mathrm{supp}(D)$, and $b \in k[x]$ determines the y-coordinates. The Mumford representation can be used to perform arithmetic in $J(k)$ using Cantor's algorithm [6]. Based on this, an explicit theory of the Kummer variety was found for the degree 7 case in [22,31].

For our application, we do not assume that X contains a k-rational Weierstrass point (or, in fact, any k-rational point). Instead, we rely on an explicit theory of the Kummer variety in the general case developed and implemented by Stoll (see [26,30]). We summarise his results here and describe a few modest additions of ours.

4.1 Representing points on the Jacobian

In order to find an explicit map $\kappa : J \to \mathbb{P}^7$ such that $\kappa(J)$ is a model of K, we need an explicit description of points on J without the assumption $\deg(f) = 7$. We will now show that we can represent points Q on J using divisors of degree 4, but we cannot expect uniqueness anymore.

We follow the discussion in [30]. The idea is to use the canonical isomorphism between $\mathrm{Pic}^0(X)$ and $\mathrm{Pic}^4(X)$ given by adding the canonical class. Let the divisor D_∞ on X be equal to $2(\infty)$ if $\deg(f) = 7$ and to $(\infty_1) + (\infty_2)$ otherwise, where ∞_1 and ∞_2 are the two points at infinity on X. Then $2D_\infty$ is a canonical divisor of X.

Proposition 4.2 *For every $Q \in J \setminus \{0\}$, exactly one of the following holds*

(a) $Q = [D_Q - 2D_\infty]$ *for a divisor D_Q of degree 4 in general position;*
(b) $Q = [D_Q - D_\infty]$ *for a divisor D_Q of degree 2 in general position.*

In case (b), the divisor D_Q is uniquely determined by Q.

Proof The proof is sketched in [30, Sect. 2]. Suppose that $Q \in J \setminus \{0\}$ is represented by $E_Q \in \mathrm{Div}^0(X)$. By Riemann–Roch, the Riemann–Roch space $L(E_Q + 2D_\infty)$ has dimension at least 2; let φ be a nontrivial element. Then $D'_Q := E_Q + 2D_\infty + \mathrm{div}(\varphi)$ is effective of degree 4 and we have $Q = [D'_Q - 2D_\infty]$. If D'_Q is in general position, then we set $D_Q := D'_Q$; otherwise $D'_Q = D_Q + (P) + (\iota(P))$ for some $P \in X$ and D_Q is effective of degree 2 and in general position, since $Q \neq 0$.

For D_Q of degree 2 in general position, the Riemann–Roch space $L(D_Q + D_\infty)$ has dimension 2, generated by 1 and x. Hence all elements of the corresponding linear system, containing all divisors linearly equivalent to $D_Q + D_\infty$, are of the form $D_Q + (P) + (\iota(P))$ for some $P \in X$. This shows that the two cases (a) and (b) are mutually exclusive and also proves the uniqueness of D_Q in case (b). □

From now on, we say that Q is of *degree* 4 in case (a) and of *degree* 2 in case (b). The point $0 \in J$ is defined to have degree 0.

We first consider the case where $Q \in J$ has degree 4. Then the divisor D_Q in Proposition 4.2(a) is not unique by [30, Lemma 2.1]. As in Sect. 3.4, D_Q yields a generalised Mumford representation as follows. Let F be the degree 8 homogenisation of f. There is a model $y^2 = F(x, z)$ of X in the weighted projective plane over k with weight 1 associated to x and z and weight $4 = g + 1$ associated to y. By [30, p. 4], divisors $D \in \mathrm{Div}^4(X)$ in general position correspond bijectively to triples of binary forms $A, B, C \in k[x, z]$ of degree 4 such that

$$B^2 - F = AC\,. \tag{4.1}$$

The image of a point $P = (x_0 : y_0 : z_0)$ in the support of D under the hyperelliptic covering $\pi : X \to \mathbb{P}^1$ corresponds to a root of A with the correct multiplicity, and we have $y_0 = B(\pi(P))$. Note that this Mumford representation of D_Q is unique up to adding multiples of A to B.

Remark 4.3 If $X(k)$ is non-empty, then we can find an equation $y^2 = f(x)$ for X such that we either have $\deg(f) = 7$ or we have $\deg(f) = 8$ and the leading coefficient of f is a square. We have already discussed the former case. In the latter case, we can arbitrarily fix one of the two points $\infty_1, \infty_2 \in X(k)$ at infinity, say ∞_1. If $Q \in J(k)$ has degree 4,

then requiring that $\infty_1 \in \mathrm{supp}(D_Q)$ fixes D_Q uniquely. By the above, we can represent Q using a triple (A, B, C) representing D_Q. Moreover, we can use this representation for arithmetic in $J(k)$ using a generalisation of Cantor's Algorithm. This is implemented in `Magma`. In practice, it is better to use Sutherland's balanced divisor approach [33], which is more efficient. It also requires the existence of a k-rational point.

If the leading coefficient of f is not a square in k, then it is not clear how to represent degree 4 points consistently (and hence uniquely). In this case, `Magma` does not represent such points and arithmetic in $J(k)$ has not been implemented.

4.2 The Kummer variety

In [30, Lemma 2.1], Stoll shows that there is a subgroup Γ of $\mathrm{SO}(Q)$, where Q is the ternary quadratic form $y^2 - xz$, with the following property: Two triples (A, B, C) and (A', B', C') represent divisors in general position of degree 4 with the same image on J if and only if they are equivalent under the action of Γ. Moreover, they represent inverse points if and only if they are equivalent under the action of $-\Gamma$. Stoll then uses this observation to construct the Kummer variety K of J explicitly as follows. There is a canonical theta divisor Θ on J such that the support of Θ consists of 0 and the points on J of degree 2 in the sense of Proposition 4.2. A basis for the Riemann-Roch space $\mathcal{L}(2\Theta)$ defines a rational map $\kappa : J \to \mathbb{P}^7$ such that $\kappa(J)$ is a model for the Kummer variety K of J. By the above, the complement of the image of Θ in Pic^4 under the canonical isomorphism can be described by the affine variety V defined by (4.1), quotiented out by the action of Γ. Stoll finds a basis $\xi_1, \ldots, \xi_8$ of $\mathcal{L}(2\Theta)$ from $\pm\Gamma$-invariants in $k[V]$. Let $\kappa : J \to \mathbb{P}^7$ be the map defined by $\xi_1, \ldots, \xi_8$. Then κ is invariant under multiplication by -1 on J. Hence its image $K := \kappa(J)$ describes a birational model of the Kummer variety by [30, Theorem 2.5].

According to [22, Proposition 3.1], K can be defined by quartic relations. To find such relations, Stoll notes that $\xi_1, \ldots, \xi_7$ are of degree 2 in the coefficients of A, B and C, whereas ξ_8 is quadratic in $\xi_1, \ldots, \xi_7$, leading to a quadratic relation, and hence 36 quartic ones, satisfied by the ξ_i. By [30, Theorem 2.5], one needs an additional 34 quartic relations; such relations are constructed before [30, Lemma 2.2].

To describe the map κ on points $Q \in J(k)$ of degree 2 (which lie on Θ), Stoll approximates the divisor $D_Q + D_\infty$, where D_Q is as in Proposition 4.2(b) (see the discussion following [30, Theorem 2.5]). Write $D_Q = (P_1) + (P_2)$, where $P_i = (x_i : y_i : z_i) \in X$, and

$$A(x, z) = (z_1 x - x_1 z)(z_2 x - x_2 z) =: a_0 x^2 + a_1 xz + a_2 z^2 \in k[x, z].$$

Then we have

$$\kappa(Q) = (0 : a_0^2 : a_0 a_1 : a_0 a_2 : a_1^2 - a_0 a_2 : a_1 a_2 : a_2^2 : \xi_8).$$

If $z_1 = z_2 = 1$ and $x_1 \neq x_2$, then $a_0 = 1$ and $\xi_8 = \frac{2y_1 y_2 - G(x_1, x_2)}{(x_1 - x_2)^2}$, where

$$G(x_1, x_2) = 2 \sum_{j=0}^{4} f_{2j} (x_1 x_2)^j + (x_1 + x_2) \sum_{j=0}^{3} f_{2j+1} (x_1 x_2)^j$$

and $F(x, z) = f_0 z^8 + f_1 xz^7 + \ldots + f_8 x^8$. In this case, ξ_8 satisfies

$$((x_1 - x_2)^2 \xi_8 + G(x_1, x_2))^2 - 4 f(x_1) f(x_2) = 0. \tag{4.2}$$

We now give $\kappa(Q)$ explicitly for the remaining special cases. More details can be found in [25, Sect. 5.4]. If $z_1 = z_2 = 1$ and $x_1 = x_2$, then we can find ξ_8 by writing (4.2) as

$$s_2 \xi_8^2 + s_1 \xi_8 + s_0 = 0. \tag{4.3}$$

Then $s_2 = 0$ and $s_1 = -2G(x_1, x_1) = -4f(x_1)$. If $s_1 \neq 0$, then $Q \neq 0$, and it follows that

$$\kappa(Q) = \left(0 : 1 : -2x_1 : x_1^2 : 3x_1^2 : -2x_1^3 : x_1^4 : \frac{-s_0}{s_1}\right). \tag{4.4}$$

If $z_1 = 1$ and $P_2 = (1 : w : 0)$ for some $w \in \bar{k}$ such that $w^2 = f_8$, then we can use an approximation to find

$$\kappa(Q) = (0 : 0 : 0 : 0 : 1 : -x_1 : x_1^2 : 2y_1 w - 2f_8 x_1^4 - f_7 x_1^3). \tag{4.5}$$

If $P_1 = P_2 = (1 : w : 0)$, then we can use (4.3) to find

$$\kappa(Q) = (0 : 0 : 0 : 0 : 0 : 0 : 4f_8 : 4f_6 f_8 - f_7^2). \tag{4.6}$$

Finally, we have

$$\kappa(0) = (0 : 0 : 0 : 0 : 0 : 0 : 0 : 1).$$

Remark 4.4 If $s_2 = 0$, then we can also express ξ_8 in terms of the coefficients of the polynomials A, B, C:

$$\begin{aligned}\xi_8 = &-a_0^3 c_6 - a_0^2 a_2 c_4 + 2a_0^2 b_2 b_4 - 2a_0 a_1 b_1 b_4 - a_0 a_2^2 c_2 + 2a_0 a_2 b_1 b_3 \\ &+2a_1^2 b_0 b_4 - 2a_1 a_2 b_0 b_3 - a_2^3 c_0 + 2a_2^2 b_0 b_2\end{aligned}$$

where $B(x, z) = b_0 z^4 + b_1 x z^3 + b_2 x^2 z^2 + b_3 x^3 z + b_4 x^4$ and $C(x, z) = c_0 z^6 + \ldots + c_6 x^6$.

4.2.1 Traces of the group law

Recall that Assumption 3.1 requires, in particular, algorithms for

- the map $[[2]]\colon K \to K$ such that $\kappa(2Q) = [[2]](\kappa(Q))$ for all $Q \in J$;
- the map $B\colon \mathrm{Sym}^2(K) \to \mathrm{Sym}^2(K)$ such that for all $Q_1, Q_2 \in J$ we have

$$B(\{\kappa(Q_1), \kappa(Q_2)\}) = \{\kappa(Q_1 + Q_2), \kappa(Q_1 - Q_2)\}.$$

Similar to the genus 2 case [7, Sect. 3], there are homogeneous quartic polynomials

$$\delta_1, \ldots, \delta_8 \in \mathbb{Z}[f_0, \ldots, f_8][x_1, \ldots, x_8]$$

such that $[[2]](R) = (\delta_1(R) : \ldots : \delta_8(R))$ for all $R \in K$, normalised to map $(0, \ldots, 0, 1)$ to itself. The polynomials can be constructed using representation theory; see [30, Theorem 7.3]. The map B is constructed using representation theory in [30, Lemma 8.1].

4.3 Checking whether rational points lift to rational points

This section gives a procedure that decides whether the preimage under κ of a point

$$R = (\xi_1 : \ldots : \xi_8) \in K(k)$$

is in $J(k)$ or not. Let $Q \in J$ such that $\kappa(Q) = R$. Then Q is of degree 4 if and only if $\xi_1 \neq 0$. Also, we have $Q = 0$ if and only if $R = (0 : 0 : 0 : 0 : 0 : 0 : 0 : 1)$.

The case where $Q \in J$ has degree 4 is treated in [30, Sect. 4]. Briefly, the idea is that when h is a nonzero odd function on J/k, then h^2 induces a function j on K/k, and $R \in K(k)$ can only have rational preimages if $j(R)$ is a square in k. Conversely, if $j(R)$ is a nonzero square in k, then R has rational preimages. Stoll constructs suitable functions j as 3×3-minors of a 4×4 matrix $M = M(\xi_1, \ldots, \xi_7)$ (see [30, (2.7)]). The preimage of R consists of rational points if and only if all values $j(R)$ are squares in k.

Suppose that $Q \in J$ has degree 2. In this case [30, Sect. 4] suggests to simply consider the map κ explicitly. The uniqueness of the divisor $D_Q = (P_1)+(P_2)$ such that $Q = [D_Q - D_\infty]$ implies that $Q \in J(k)$ if and only if D_Q is defined over k. By Sect. 4.2, we have $\xi_1 = 0$. We now distinguish cases, using the explicit expression for R given in Sect. 4.2.

First suppose that $\xi_2 = 0$. Since $Q \neq O$, we are either in case (4.5) or in case (4.6). If $\xi_5 = 0$, then it is the latter. Note that $\xi_7 \neq 0$, since otherwise we would have $R = (0:0:0:0:0:0:0:1)$. Therefore $P_1 = P_2 = \infty_{1/2}$, and the preimage of R is rational if and only if X has rational points at infinity.

If $\xi_2 = 0$, but $\xi_5 \neq 0$, then R is as in Eq. (4.5). Hence without loss of generality $P_1 = (x_1, y_1)$ and $P_2 = \infty_{1/2}$. We have $\kappa^{-1}(R) \subset J(k)$ if and only if $\infty_{1/2}$ and (x_1, y_1) are rational. The latter holds if and only if $f(-\xi_6) = y_1^2$ is a square in k.

It remains to discuss the case $\xi_2 \neq 0$, i.e. $\deg A(x,1) = 2$. Then $D_Q = (P_1) + (P_2)$, where $P_i = (x_i, y_i)$ are affine and

$$R = \left(0 : 1 : -(x_1+x_2) : x_1x_2 : x_1^2 + x_1x_2 + x_2^2 : -(x_1+x_2)x_1x_2 : (x_1x_2)^2 : \frac{2y_1y_2 - G(x_1,x_2)}{(x_1-x_2)^2}\right). \tag{4.7}$$

Lemma 4.5 *The preimage $\kappa^{-1}(R)$ consists of rational points if and only if $y_1 + y_2 \in k$ and if one of the following conditions is satisfied:*

(1) $x_1 = x_2$,
(2) $x_1 \neq x_2$ *and* $\frac{y_1-y_2}{x_1-x_2} \in k$.

Proof The divisor D_Q is k-rational if and only if P_1 and P_2 are k-rational or if $P_1, P_2 \in X(k')$ for a quadratic extension k'/k and $\sigma(P_1) = P_2$, where σ is the nontrivial element of $\mathrm{Gal}(k'/k)$. Hence a necessary condition for rationality of D_Q is that the polynomial $(y-y_1)(y-y_2)$ is defined over k. It follows from (4.7) that $y_1y_2 \in k$. Suppose from now on that $y_1 + y_2 \in k$.

If $x_1 = x_2$, then $x_1 = -\frac{1}{2}\xi_3 \in k$ and $y_1 = \frac{1}{2}(y_1+y_2) \in k$, since $Q \neq 0$ by assumption; hence D_Q is k-rational. Now assume that $x_1 \neq x_2$. Then there is a Mumford representation (A, B, C) of Q such that the polynomial $b(x) = B(x,1)$ is linear and satisfies $b(x_1) = y_1$ and $b(x_2) = y_2$, and D_Q is k-rational if and only if $b \in k[x]$. Write $b(x) = b_0 + b_1x$, then $b_1 = \frac{y_1-y_2}{x_1-x_2}$ and $b_0 = \frac{y_2x_1-y_1x_2}{x_1-x_2}$. Since

$$y_1 + y_2 = 2b_0 + b_1(x_1+x_2),$$

and since both $y_1 + y_2$ and $x_1 + x_2 = -\xi_3$ are in k, we conclude that $b \in k[x]$ if and only if $b_1 \in k$. □

From (4.7), we can compute y_1y_2 and

$$y_1^2 + y_2^2 = f(x_1) + f(x_2) = \sum_{j=0}^{8} f_j(x_1^j + x_2^j),$$

hence also $(y_1 \pm y_2)^2$. Since $(x_1 - x_2)^2$ is also computed easily from (4.7), we can use Lemma 4.5 in practice to check whether R lifts to rational points.

Remark 4.6 Stoll shows in [30, Sect. 4] how to compute a lift of R when $X(k)$ is nonempty and the lifts of R have degree 4. Using the above, we can compute the unique Mumford representation of the points lifting R in the degree 2 case.

4.4 Using arithmetic on reduced Jacobians

Recall that Step (3) of Algorithm 3.15 requires the structure of $\tilde{J}(\mathbb{F}_p)$ for primes of good reduction p, where $\tilde{J}$ is the reduction of J modulo p. Moreover, in Step (b) of Algorithm 3.14, we need to enumerate all elements of the q-parts of $\tilde{J}(\mathbb{F}_p)$, where q is prime and $p \neq q$ is a prime of good reduction, and we need to compute scalar multiples.

In Remark 3.2 we discussed how to compute $\tilde{J}(\mathbb{F}_p)$ for a prime p of good reduction using arithmetic of the Kummer variety $\tilde{K}$ and checking whether points in $\tilde{K}(\mathbb{F}_p)$ lift to $\tilde{J}(\mathbb{F}_p)$. In practice, it turns out to be more efficient to compute $\tilde{J}(\mathbb{F}_p)$ using arithmetic in $\tilde{J}(\mathbb{F}_p)$, if that is implemented.

Recall from Sect. 4.1 that there are algorithms (and implementations) for arithmetic in $\tilde{J}(\mathbb{F}_p)$ if we know a point in $\tilde{X}(\mathbb{F}_p)$, but no algorithm is known if we do not. If $\tilde{X}(\mathbb{F}_p)$ is nonempty, then we fix a point $\tilde{P} \in \tilde{X}(\mathbb{F}_p)$ and use a change of coordinates $\phi\colon \tilde{X} \to \tilde{X}'$ such that $\phi(\tilde{P})$ is a point at infinity. Let $\tilde{J}'$ be the Jacobian of $\tilde{X}'$. Then we can compute in $\tilde{J}'(\mathbb{F}_p)$, for instance in `Magma`. Moreover, we can enumerate $\tilde{J}'(\mathbb{F}_p)$ and find its structure as an abelian group. We adjust Steps (3) and (4) of Algorithm 3.15 in the following way. Here, we denote the Kummer variety of $\tilde{J}'$ by $\tilde{K}'$.

- In Step (3) and (4) of Algorithm 3.15, find suitable primes p with the extra condition that $\tilde{X}(\mathbb{F}_p)$ is not empty.
- In Algorithm 3.14, let G_0 be the q-part of $\tilde{J}'(\mathbb{F}_p)$. In Step (2), find the smallest m such that $\tilde{\kappa}(\phi_*^{-1}(q^m \cdot g))$ lifts to $J(\mathbb{Q})$, where $\phi\colon \tilde{X} \to \tilde{X}'$ is as above.

This modification still allows us to choose from infinitely many primes p, since the Hasse-Weil bound implies $\#\tilde{X}(\mathbb{F}_p) \geq 1$ for all good $p \geq 41$.

Remark 4.7 In practice, we replace $\tilde{\kappa} \circ \phi_*^{-1}$ by $\phi_{\tilde{K}}^{-1} \circ \tilde{\kappa}'$, where $\phi_{\tilde{K}}\colon \tilde{K} \to \tilde{K}'$ is the isomorphism induced by ϕ. Explicit formulas for $\phi_{\tilde{K}}$ are given in [25, Appendix B].

4.5 Computing the rational two-torsion points.

It is possible to compute $J(\mathbb{Q})[2]$ via the approach sketched in Sect. 3.2.1, but this takes quite long in practice. We now discuss a more efficient method, suggested to us by Michael Stoll.

First suppose that $\deg(f) = 7$. Let $g_1, \ldots, g_r \in k[x]$ be the monic irreducible factors of f. Then, by [28, Lemma 4.3] $J(\mathbb{Q})[2]$ is generated by the points with Mumford representation

$$(g_1, 0), \ldots, (g_{r-1}, 0)\,.$$

Now suppose that $\deg(f) = 8$. Let $\Omega \subset \overline{\mathbb{Q}}$ be the set of zeros of $f(x)$. We call an unordered partition $\{\Omega_1, \Omega_2\}$ of Ω *even* if $\#\Omega_1$ (and hence $\#\Omega_2$) is even. An even partition $\{\Omega_1, \Omega_2\}$ of Ω gives rise to a two-torsion point P_{Ω_1} $(= P_{\Omega_2})$ represented by

$$\sum_{\omega \in \Omega_1} (\omega, 0) - \frac{\#\Omega_1}{2} D_\infty \sim \sum_{\omega \in \Omega_2} (\omega, 0) - \frac{\#\Omega_2}{2} D_\infty\,, \tag{4.8}$$

and every point in $J(\overline{\mathbb{Q}})[2]$ arises in this way from a unique unordered partition. See [30, Sect. 5] and [24]. More precisely, (4.8) induces a bijection between $J[2]$ and the Galois-module of unordered even partitions of roots of f (see [24, Sect. 6]). Hence $J(\mathbb{Q})[2]$ is in bijection with the set of all unordered even partitions $\{\Omega_1, \Omega_2\}$ that are fixed by the absolute Galois group $G_{\mathbb{Q}}$ of $\mathbb{Q}$. For instance, if f is monic and Ω_1 (equivalently, Ω_2) is

fixed by $G_{\mathbb{Q}}$, then $P_{\Omega_1} \in J(\mathbb{Q})[2]$, and P_{Ω_1} has Mumford representation $(A(x,z), 0, C(x,z))$, where $A(x,z) = \prod_{\omega\in\Omega_1}(x-\omega z)$ and $C(x,z) = \prod_{\omega\in\Omega_2}(x-\omega z)$.

However, in general not every point in $J(\mathbb{Q})[2]$ arises in this way. It is also possible that $\{\Omega_1, \Omega_2\}$ is fixed by $G_{\mathbb{Q}}$, but Ω_1 and Ω_2 are not fixed individually. Then both Ω_1 and Ω_2 have size 4 and we have $\Omega_2 = \Omega_1^\sigma$, where σ is the non-trivial element of $\mathrm{Gal}(k/\mathbb{Q})$ for a quadratic number field k. This corresponds to a factorisation $f = \mathrm{lc}(f)\cdot h\cdot h^\sigma$, where $h = \prod_{\omega\in\Omega_1}(x-\omega) \in k[x] - \mathbb{Q}[x]$ and $h^\sigma = \prod_{\omega\in\Omega_2}(x-\omega)$ are coprime and $\mathrm{lc}(f)$ is the leading coefficient of f. In this case, P_{Ω_1} has no Mumford representation of the form $(A, 0, C)$ defined over $\mathbb{Q}$ (the degree-4 homogenisations of h and h^σ give such a representative over k). The factorisation $f = \mathrm{lc}(f)\cdot h\cdot h^\sigma$ implies that k is a subfield of the étale algebra $\mathbb{Q}[x]/(f)$.

We may use this to compute $J(\mathbb{Q})[2]$ as follows. Let $2t_{\mathbb{Q}}$ denote the number of monic even degree divisors of f in $\mathbb{Q}[x]$. For a quadratic extension $k/\mathbb{Q}$ with Galois group $\mathrm{Gal}(k/\mathbb{Q}) = \{1,\sigma\}$, we define

$$t_k := \frac{1}{2}\#\left\{h\in k[x] \,:\, h \text{ is monic},\ f = \mathrm{lc}(f)\cdot h\cdot h^\sigma,\ \gcd(h,h^\sigma) = 1\right\}.$$

By the discussion above, we obtain the following formula.

Lemma 4.8 *We have* $\#J(\mathbb{Q})[2] = t_{\mathbb{Q}} + \sum_k t_k$, *where* k *runs through the quadratic subfields of* $\mathbb{Q}[x]/(f)$.

Example 4.9 Recall from Example 1.3 that for the Jacobian J of

$$X\colon y^2 = x^8 + 2x^7 + 3x^6 + 4x^5 + 9x^4 + 8x^3 + 7x^2 + 2x + 1 =: f(x)$$

the group $J(\mathbb{Q})_{\mathrm{tors}}$ is isomorphic to a subgroup of $\mathbb{Z}/6\mathbb{Z}$. The polynomial $f(x)$ is irreducible over $\mathbb{Q}$, but it has the factorisation

$$\begin{aligned} f = {} & (x^4 + (1-2i)x^3 + (-1-2i)x^2 + (-1-2i)x - 1)\cdot(x^4 + (1+2i)x^3 \\ & + (-1+2i)x^2 + (-1+2i)x - 1) \end{aligned}$$

over $\mathbb{Q}(i)$, where $i^2 = -1$. This shows that $\#J(\mathbb{Q})[2] = 2$.

Remark 4.10 Lemma 4.8 holds more generally for hyperelliptic curves over $\mathbb{Q}$ of arbitrary genus and even degree. However, if g is even, then $\deg(f)$ is not divisible by 4, and hence $t_k = 0$ for all quadratic fields k. In this case all rational 2-torsion points come from even degree factors of f over $\mathbb{Q}$ and we recover [28, Lemma 5.6].

4.6 Halving a rational point on *K*

In practice, the formulas found by Stoll in [30, Lemma 8.1] for the map B as in Section 2 need a lot more space to store than the δ_i, and they also take longer to evaluate. Recall from Sect. 3.3 that we can avoid the B_{ij} altogether in many situations. If $J(\mathbb{Q})[2]$ is nontrivial (and we do not already know that $J(\mathbb{Q})[2^\infty] = J(\mathbb{Q})[2]$), then this requires computing preimages under $[[2]]$, as discussed in Sect. 3.2.1. In other words, for $\kappa(Q) = (y_1 : \ldots : y_8) \in K(\mathbb{Q})$ we need to solve a projective system

$$\delta_i(x_1,\ldots,x_n) = cy_i, \quad c\in\mathbb{Q}^\times, \quad 1\le i\le 8. \tag{4.9}$$

We have implemented this approach in `Magma`, using Gröbner bases to find all rational points on the zero-dimensional projective scheme defined by (4.9) and the defining

equations of K. This approach works in practice, but we found that most of the time, computing such preimages is significantly slower than simply using the map B.

An alternative approach for computing preimages under [[2]] is proposed by Stoll in [27, Sect. 5] for genus 2. We also generalised this to genus 3 and implemented this generalisation. However, this requires working over the splitting field of f. Even when f splits completely over $\mathbb{Q}$, we still found the approach via B to be more efficient.

4.7 Height difference bound

In [30], Stoll describes a method to compute $\beta > 0$ such that the difference between the naive and the canonical height is bounded by β. His approach generalises results for genus 2 [11,21,27]. Stoll shows in [30, Corollary 10.3] that one can take

$$\beta = \frac{1}{3}|2^6 \mathrm{disc}(f)| + \frac{1}{3}\gamma_\infty,$$

where γ_∞ is an upper bound for the local height contribution ε_∞ introduced in [30, Sect. 10]. One can find a suitable γ_∞ using the archimedean triangle inequality and representation theory of $J[2]$, see [30, Lemma 10.4]. A refined bound can be obtained by iterating this procedure [30, Lemma 10.5].

5 Examples and databases

We have implemented the algorithm of Sect. 3 for hyperelliptic curves of genus 3 using the explicit theory discussed in Sect. 4 in `Magma`. The implementation is based on Stoll's `Magma`-implementation of explicit formulas for the Kummer variety and heights available from [26]. Our code, as well as the results of the computations discussed below, can be found at https://github.com/bernoreitsma/g3hyptorsion. We used `Magma v2.6` on a 64-core 2.6 GHz AMD Opteron(TM) Processor 6276 with 256GB RAM, running `Ubuntu 18.04`.

This section provides some example computations, illustrating various aspects of the algorithm. We also used our implementation to compute all rational torsion subgroups in a database maintained by Andrew Sutherland [32]. Finally, we ran our algorithm on a large number of hyperelliptic curves of genus 3 with small coefficients. Together with a few additional constructions, these computations prove Theorem 1.1.

5.1 Example computations

Example 5.1 In Example 1.3, we showed that for the Jacobian J of the curve

$$X : y^2 = x^8 + 2x^7 + 3x^6 + 4x^5 + 9x^4 + 8x^3 + 7x^2 + 2x + 1,$$

we have $\#J(\mathbb{Q})_{\mathrm{tors}} = 3$. To find a generator using Algorithm 3.4, we pick $p = 17$ because the 3-part of $\tilde{J}(\mathbb{F}_{17})$ is isomorphic to $\mathbb{Z}/3\mathbb{Z}$. We choose a point $\tilde{Q} \in \tilde{J}(\mathbb{F}_{17})$ of order 3 and consider $\kappa(\tilde{Q}) \in \tilde{K}(\mathbb{F}_{17})$. If the lift $Q \in J(\mathbb{Q}_p)[3]$ of $\tilde{Q}$ is indeed in $J(\mathbb{Q})$, then $\kappa(Q) \in K(\mathbb{Q})$. After a few iterations of the Hensel lifting, we can check whether the coordinates define a point on $K(\mathbb{Q})$. Indeed, after computing the power series up to p^4, we arrive at a point $R \in K(\mathbb{Q})$ such that $[[3]](R) = \kappa(0)$, and we check that $\kappa^{-1}(R) \subset J(\mathbb{Q})_{\mathrm{tors}}$. We find that $J(\mathbb{Q})[3]$ is generated by the point represented by the divisor $(0 : -1 : 1) - (1 : 1 : 0)$, where the points are viewed inside the projective plane with weights 1, 4, 1.

Example 5.2 The following example was suggested by Andrew Sutherland. Let X be the hyperelliptic curve over $\mathbb{Q}$ defined by

$$y^2 = 5x^8 - 14x^7 + 33x^6 - 36x^5 + 30x^4 + 2x^3 - 16x^2 + 20x - 7.$$

The curve X has no small rational points, so this example illustrates how we can compute $J(\mathbb{Q})_{\mathrm{tors}}$ without an implementation of the group law in $J(\mathbb{Q})$. Computing the order of $\#J(\mathbb{F}_p)$ for some small primes of good reduction, we obtain that $\#J(\mathbb{Q})_{\mathrm{tors}} \mid 13$, but no rational point 13-torsion point on J is found easily.

For our algorithm, we pick the prime of good reduction $p = 3$, resulting in the curve

$$\tilde{X} : \tilde{y}^2 = 2\tilde{x}^8 + \tilde{x}^7 + 2\tilde{x}^3 + 2\tilde{x}^2 + 2\tilde{x} + 2$$

over $\mathbb{F}_3$, which is isomorphic over $\mathbb{F}_3$ to

$$\tilde{X}' : \tilde{y}^2 = \tilde{x}^8 + \tilde{x}^7 + \tilde{x}^6 + 2\tilde{x}^3 + \tilde{x}^2 + 2\,.$$

Since $\tilde{X}'$ has rational points at infinity, arithmetic in $\tilde{J}'(\mathbb{F}_3)$ is implemented, see the discussion in Sect. 4.4. As in Remark 4.7 we use the induced change of coordinates on the Kummer varieties of $\tilde{J}$ and $\tilde{J}'$ to check whether a candidate point $\kappa(\tilde{Q}) \in \tilde{J}(\mathbb{F}_3)[13]$ lifts to $J(\mathbb{Q})_{\mathrm{tors}}$. We indeed find the point

$$R = (0 : 1 : -1 : 1 : 0 : -1 : 1 : 20) \in \kappa(J[13]) \cap K(\mathbb{Q})$$

and we can show that $\kappa^{-1}(R) \subset J(\mathbb{Q})$. Therefore we have $J(\mathbb{Q})_{\mathrm{tors}} \cong \mathbb{Z}/13\mathbb{Z}$.

Since the first coordinate of R is 0, the preimages $Q \in J(\mathbb{Q})$ of R are of degree 2 and hence can be described uniquely using a divisor $D_Q - D_\infty$. A short calculation using the explicit formulas in Sect. 4.3 shows that one of the points Q has

$$D_Q = (1 + \zeta_3, 1 + \zeta_3) + (1 + \zeta_3^2, 1 + \zeta_3^2),$$

where ζ_3 is a primitive third root of unity.

Alternatively, one can search for points of bounded height on $J(\mathbb{Q})$ reducing to $\tilde{\kappa}(\tilde{Q})$ using a lattice-based approach as in [30, Sect. 11]. This also finds a rational point of order 13.

Example 5.3 According to [17, Example 3.9], the curve X defined by

$$y^2 = \frac{46656}{3125}x^7 + \frac{407097961}{39062500}x^6 + \frac{281238453}{3906250}x^5 - \frac{22959453}{312500}x^4 - \frac{2767361}{15625}x^3 + \frac{381951}{2500}x^2 + \frac{3093}{6250}x + \frac{1}{2500}$$

has a torsion point of order 41. It is easy to see that 41 is an upper bound for $\#J(\mathbb{Q})_{\mathrm{tors}}$. We run our algorithm on the curve with equation $y^2 = f(x)$, where

$$f = 583200000x^7 + 40709761x^6 + 2812384530x^5 - 2869931625x^4 - 6918402500x^3 + 5967984375x^2 + 19331250x + 15625\,.$$

The height difference bound β computed using Stoll's code satisfies $\beta \approx 97$, hence we need $N \log(p) \geq 11 \log(2) + 194$ in Step (4) of Algorithm 3.4. We pick $p = 7$; this yields the required p-adic precision $O(p^N)$ where $N = 128$, which is reached in just 7 steps in Step (4). It turns out that we need not go that far; $N = 32$ suffices to find a lift $R \in K(\mathbb{Q}) \cap \kappa(J[41])$. After showing that $R = \kappa(Q)$ for some $Q \in J(\mathbb{Q})$, we see that

Table 1 Torsion structures found in the database [32]

Inv factors	Ord	Count	Gs?	Inv factors	Ord	Count	Gs?	Inv factors	Ord	Count	Gs?
1	1	38370	Yes	17	17	5	Yes	36	36	3	Yes
2	2	17093	Yes	3, 6	18	1	Yes	37	37	1	Yes
3	3	956	Yes	18	18	30	Yes	38	38	2	Yes
2, 2	4	2483	Yes	19	19	3	Yes	2, 2, 10	40	16	Yes
4	4	2673	Yes	2, 10	20	88	Yes	2, 20	40	7	Yes
5	5	616	Yes	20	20	33	Yes	40	40	1	No
6	6	1332	Yes	21	21	2	Yes	42	42	6	Yes
7	7	701	Yes	22	22	14	Yes	2, 22	44	1	Yes
2, 2, 2	8	163	Yes	2, 2, 6	24	19	Yes	44	44	1	Yes
2, 4	8	493	Yes	2, 12	24	98	Yes	46	46	1	Yes
8	8	639	Yes	24	24	21	Yes	2, 2, 12	48	2	No
9	9	175	Yes	25	25	4	Yes	2, 24	48	7	Yes
10	10	493	Yes	26	26	9	Yes	4, 12	48	2	No
11	11	34	Yes	27	27	3	Yes	49	49	2	Yes
2, 6	12	161	Yes	2, 14	28	33	Yes	5, 10	50	1	No
12	12	403	Yes	28	28	17	Yes	52	52	2	Yes
13	13	22	Yes	30	30	6	Yes	2, 2, 14	56	1	Yes
14	14	307	Yes	2, 2, 2, 4	32	1	Yes	2, 28	56	4	Yes
15	15	5	Yes	2, 2, 8	32	21	Yes	2, 30	60	1	No
2, 2, 2, 2	16	3	Yes	2, 16	32	10	Yes	60	60	3	No
2, 2, 4	16	47	Yes	32	32	3	Yes	2, 2, 2, 8	64	1	Yes
2, 8	16	156	Yes	2, 18	36	2	Yes	2, 6, 6	72	1	No
4, 4	16	3	No	3, 12	36	1	No	2, 52	104	1	No
16	16	57	Yes	6, 6	36	2	No				

$J(\mathbb{Q})_{\text{tors}} \cong \mathbb{Z}/41\mathbb{Z}$, confirming [17, Example 3.9]. An explicit generator is represented by $(0, 125) - (\infty)$. We checked that the Jacobian is in fact geometrically simple using the results of [16, Sect. 3]; this was also done by Nicholls using [23, Proposition 2.4.2].

5.2 Sutherland's database

Using the techniques of [5], Andrew Sutherland has assembled a file with 67879 genus 3 hyperelliptic curves of small discriminant at [32]. We used our implementation to compute the rational torsion subgroups of their Jacobians. For the complete database containing the results for the 67879 curves, we refer to the file `database.txt` in https://github.com/bernoreitsma/g3hyptorsion. All torsion structures and the frequency of their appearance can be found in Table 1. Column *inv factors* contains the invariant factors, *ord* the order of the group, *count* is the number of times we found this torsion structure and *gs?* indicates whether we found at least one curve whose Jacobian has this torsion structure and is geometrically simple.

Here we summarise some of our findings.

- 38370 Jacobians ($\approx$ 56.5%) have trivial rational torsion subgroup.
- 5663 Jacobians ($\approx$ 8.3%) have a rational torsion point of odd order.
- 25679 Jacobians ($\approx$ 37.8%) have a nontrivial cyclic rational torsion subgroup, hence 3830 ($\approx$ 5.6%) have 2 or more generators.

- Of the non-cyclic torsion subgroups found, 3555 have 2 generators, 370 have 3 generators, and 5 torsion subgroups have 4 generators. The 5 curves that have four generators all have at least 3 of these generators of order 2.
- 11 Jacobians have a torsion subgroup such that there are two invariant factors that are not equal to 2.
- For 65938 ($\approx 97.1\%$) of the Jacobians, the order of the rational torsion subgroup is equal to the upper bound b obtained by reducing modulo all good primes below 1000 as in Example 1.3. For the others, we have the following, where *count* denotes the number of occurrences. Most of the Jacobians for which the quotient $b/\#J(\mathbb{Q})_{\text{tors}}$ is not 1 are geometrically split, for instance, all Jacobians for which the quotient is > 7 or equal to 6, and 182 out of the 192 Jacobians with quotient equal to 4. The three Jacobians for which the quotient is 7 are geometrically irreducible; they have upper bound 7 and $\#J(\mathbb{Q})_{\text{tors}} = 1$.

$b/\#J(\mathbb{Q})_{\text{tors}}$	2	3	4	5	6	7	8	10	16	32
count	1644	56	192	2	8	3	25	1	9	1

5.3 Large orders

5.3.1 Previous work

In [23, Table 3.2], Nicholls lists all known orders of rational torsion points on Jacobians of hyperelliptic curves of genus 3. Most of these were constructed by him in suitable families; in particular, he constructs geometrically simple Jacobians $J/\mathbb{Q}$ with a point $P \in J(\mathbb{Q})$ of order N for every $N \in \{25, \ldots, 44\}$. Moreover, he constructs such points for

$$N \in \{15, 22, 48, 49, 50, 52, 54, 56, 64, 65, 72, 91\}.$$

In particular, the Jacobians of the curves

$$y^2 = -16x^7 + 409/4x^6 - 275x^5 + 399x^4 - 334x^3 + 160x^2 - 40x + 4 \tag{5.1}$$

$$y^2 = -16x^7 + 393/4x^6 - 237x^5 + 309x^4 - 242x^3 + 116x^2 - 32x + 4 \tag{5.2}$$

have a rational point of order 43. This is the largest known prime order for a rational point on the Jacobian of a hyperelliptic curve of genus 3 (the previous record holder was the curve in Example 5.3). The largest known point order is 91, but Nicholls does not give the equation of the curve.

Remark 5.4 We focused on geometrically simple Jacobians. In [12, Sects. 4.3–4.6], Howe, Leprevost and Poonen construct split Jacobians of hyperelliptic curves of genus 3 with large torsion orders. They find the groups with the following invariant factors:

$$[2, 30], [10, 10], [2, 8, 8], [2, 2, 2, 24], [2, 2, 2, 4, 8], [2, 2, 6, 12], [4, 4, 8], [2, 2, 2, 4, 8], [2, 2, 2, 2, 4, 8]$$

5.3.2 Searching for large orders

Howe [13] searched among genus 2 curves of the form

$$y^2 + h(x)y = g(x) \tag{5.3}$$

with $\deg(h) = 3$ and $\deg(g) = 2$ and small coefficients to find large torsion orders. Such curves are promising, because every curve of genus 2 with a rational non-Weierstrass point has a model of the form (5.3).

Similarly, we naively searched among those genus 3 curves that have a model

$$y^2 + h(x)y = g(x)$$

with $\deg(h) = 4$, $\deg(g) = 3$ and coefficients bounded in absolute value by 8. See the file `searchresults.m` at https://github.com/bernoreitsma/g3hyptorsion.

We found the following 3 pairwise non-isomorphic curves having $\#J(\mathbb{Q})_{\text{tors}} = 43$:

$$\begin{aligned}
y^2 &= x^8 + 4x^6 + 12x^5 - 4x^4 + 24x^3 + 20x^2 - 16x + 16\\
y^2 &= x^8 - 4x^7 + 10x^5 + 4x^4 - 20x^3 + x^2 + 12x + 4\\
y^2 &= x^8 - 4x^7 + 18x^5 - 16x^4 - 12x^3 + 9x^2 + 8
\end{aligned}$$

The third curve is isomorphic to the curve (5.1) found by Nicholls. We did not recover the example (5.2) and we found no larger prime order. All three Jacobians are geometrically simple.

The largest order $\#J(\mathbb{Q})_{\text{tors}}$ that we found was 160; this occurred exactly once, for the following curve, whose Jacobian is geometrically simple:

$$y^2 = 9x^8 - 48x^7 + 46x^6 + 96x^5 - 119x^4 - 72x^3 + 64x^2 + 24x\,.$$

This is the largest torsion order on a geometrically simple Jacobian of dimension 3 found so far.

The largest (finite) order of an element of $J(\mathbb{Q})$ was on the Jacobian J of the curve defined by

$$y^2 = 9x^8 - 36x^7 + 36x^6 + 18x^5 - 48x^4 + 24x^3 + x^2 - 4x + 4\,.$$

We have $J(\mathbb{Q})_{\text{tors}} \cong \mathbb{Z}/144\mathbb{Z}$. Here J is not geometrically simple. The largest (finite) order of a rational point on a geometrically simple Jacobian occurred for the curve

$$y^2 = x^8 - 2x^7 + 7x^6 - 6x^5 - x^4 + 10x^3 - 6x^2 + 1$$

whose Jacobian has $J(\mathbb{Q})_{\text{tors}} \cong \mathbb{Z}/91\mathbb{Z}$, generated by the point $[2(1,2) - D_\infty]$.

Table 2 contains all group structures found in the search which do not already appear for a geometrically simple Jacobian of a curve in Sutherland's database.

Remark 5.5 In our computations, we found all point orders in Nicholls' [23, Table 3.2]. Moreover, the following orders appeared for geometrically simple Jacobians, but were not previously described in the literature for such Jacobians:

23, 24, 46, 51, 58, 63, 70

In addition, we found every order up to 22. We also found the following new orders for split Jacobians:

60, 80, 144

The corresponding curves all have automorphism group of order greater than 2, so their Jacobians are split over $\mathbb{Q}$.

Table 2 Torsion structures found in the search

Inv factors	Ord	Gs?	Inv factors	Ord	Gs?	Inv factors	Ord	Gs?
3,3	9	Yes	2, 26	52	Yes	2, 2, 20	80	Yes
4,4	16	Yes	3,18	54	Yes	2, 40	80	No
23	23	Yes	54	54	Yes	4, 20	80	No
5, 5	25	Yes	56	56	Yes	80	80	No
29	29	Yes	58	58	Yes	2,42	84	Yes
31	31	Yes	2, 30	60	Yes	2, 44	88	Yes
2, 4, 4	32	No	60	60	No	91	91	Yes
4, 8	32	Yes	63	63	Yes	2,2, 24	96	No
35	35	Yes	2, 2, 16	64	No	2, 4, 12	96	No
3, 12	36	Yes	2, 4, 8	64	Yes	2, 48	96	No
6, 6	36	No	2, 32	64	Yes	4, 24	96	No
39	39	Yes	4, 16	64	No	2, 2, 28	104	Yes
40	40	Yes	64	64	Yes	2, 52	104	Yes
41	41	Yes	65	65	Yes	2, 60	120	No
43	43	Yes	70	70	Yes	2, 2, 2, 2, 8	128	No
2, 2, 12	48	Yes	2, 2, 18	72	No	2, 2, 2, 16	128	No
4, 12	48	Yes	2, 6, 6	72	No	2, 4, 16	128	No
48	48	Yes	2, 36	72	No	12, 12	144	No
5,10	50	No	6, 12	72	Yes	144	144	No
50	50	Yes	72	72	Yes	2, 2, 2, 2, 10	160	Yes
51	51	Yes	2, 2, 2, 10	80	Yes			

5.4 Additional examples and proof of Theorem 1.1

All torsion structures in Theorem 1.1 occurred in the computations discussed in Sects. 5.2 and 5.3.2 (see Tables 1 and 2), except for $(\mathbb{Z}/2\mathbb{Z})^5$, $(\mathbb{Z}/2\mathbb{Z})^6$, $(\mathbb{Z}/2\mathbb{Z})^4 \times \mathbb{Z}/4\mathbb{Z}$ and $(\mathbb{Z}/2\mathbb{Z})^3 \times \mathbb{Z}/6\mathbb{Z}$. It is easy to find geometrically simple Jacobians with rational torsion subgroup isomorphic to the first two using Sect. 4.5. For instance, the curves

$$X_1 \colon y^2 = x(x-1)(x-2)(x-3)(x-4)(x^2+x+1)$$

and

$$X_2 \colon y^2 = x(x-1)(x-2)(x-3)(x+1)(x+2)(x+3)$$

have geometrically simple Jacobian with rational torsion subgroup isomorphic to $(\mathbb{Z}/2\mathbb{Z})^5$ and $(\mathbb{Z}/2\mathbb{Z})^6$, respectively. In a systematic search, we also found the curves

$$X_3 \colon y^2 = x^7 - 8x^6 - 19x^5 + 235x^4 - 130x^3 - 875x^2 - 500x$$

and

$$X_4 \colon y^2 = x^7 - 15x^6 + 87x^5 - 244x^4 + 335x^3 - 191x^2 + 9x + 18$$

whose Jacobians J_3 and J_4 are geometrically simple. We have $J_3(\mathbb{Q})_{\mathrm{tors}} \cong (\mathbb{Z}/2\mathbb{Z})^4 \times \mathbb{Z}/4\mathbb{Z}$ and $J_4(\mathbb{Q})_{\mathrm{tors}} \cong (\mathbb{Z}/2\mathbb{Z})^3 \times \mathbb{Z}/6\mathbb{Z}$. This completes the proof of Theorem 1.1.

Acknowledgements

It is a pleasure to thank Andrew Sutherland for providing the motivation for this work and for helpful discussions, and Michael Stoll for answering many questions and for useful suggestions, in particular Lemma 4.8. We thank Ludwig Fürst, Timo Keller and especially Michael Stoll for many comments on preliminary versions of this article, Max Kronberg for explaining results from his thesis, and Jaap Top and Pınar Kılıçer for helpful discussions. We would also like to thank two anonymous referees for careful reports with many suggestions for improvement. We are grateful to the Artificial Intelligence Group at the Bernoulli Institute of the University of Groningen for providing access to the `Pallas`-server, which we used for our computations. The first author was supported by NWO Grant VI.Vidi.192.106.

Data availability The code described in this paper and the data generated from it can be found at https://github.com/bernoreitsma/g3hyptorsion.

Received: 8 November 2022 Accepted: 28 February 2023
Published online: 19 March 2023

References

1. Bosma, W., Cannon, J., Playoust, C.: The Magma algebra system I: the user language. J. Symb. Comput. **24**(3–4), 235–265 (1997)
2. Birkenhake, C., Lange, H.: Complex Abelian Varieties, volume 302 of Grundlehren der mathematischen Wissenschaften, 2 edn. Springer, Berlin (2004)
3. Bourbaki, N.: Lie Groups and Lie Algebras. Chapters 1–3. Elements of Mathematics (Berlin). Springer, Berlin, Translated from the French, Reprint of the 1989 English translation (1998)
4. Bruin, N., Stoll, M.: The Mordell-Weil sieve: proving non-existence of rational points on curves. LMS J. Comput. Math. **13**, 272–306 (2010)
5. 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)
6. Cantor, D.G.: Computing in the Jacobian of a hyperelliptic curve. Math. Comput. **48**(177), 95–101 (1987)
7. 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. Cambridge University Press, Cambridge (1996)
8. Flynn, E.V.: Sequences of rational torsions on abelian varieties. Invent. Math. **106**(2), 433–442 (1991)
9. Flynn, E.V.: The group law on the Jacobian of a curve of genus 2. J. Reine Angew. Math. **439**, 45–69 (1993)
10. Flynn, E.V.: An explicit theory of heights. Trans. Am. Math. Soc. **347**(8), 3003–3015 (1995)
11. Flynn, E.V., Smart, N.P.: Canonical heights on the Jacobians of curves of genus 2 and infinite descent. Acta Arith. **79**, 333–352 (1997)
12. Howe, E.W., Leprévost, F., Poonen, B.: Large torsion subgroups of split Jacobians of curves of genus two or three. Forum Math. **12**(3), 315–364 (2000)
13. Howe, E.W.: Genus-2 Jacobians with torsion points of large order. Bull. Lond. Math. Soc. **47**(1), 127–135 (2015)
14. Hindry, M., Silverman, J.H.: Diophantine Geometry, volume 201 of Graduate Texts in Mathematics. Springer, New York. An introduction (2000)
15. Hanselman, J., Schiavone, S., Sijsling, J.: Gluing curves of genus 1 and 2 along their 2-torsion. Math. Comput. **90**(331), 2333–2379 (2021)
16. Howe, E.W., Zhu, H.J.: On the existence of absolutely simple abelian varieties of a given dimension over an arbitrary field. J. Number Theory **92**(1), 139–163 (2002)
17. Kronberg, M.: Explicit construction of rational torsion divisors on Jacobians of curves. PhD thesis, Carl von Ossietzky Universität Oldenburg (2015)
18. Leprévost, F.: Sur certains sous-groupes de torsion de jacobiennes de courbes hyperelliptiques de genre $g \geq 1$. Manuscripta Math. **92**(1), 47–63 (1997)
19. Lenstra, A.K., Lenstra, H.W., Jr., Lovász, L.: Factoring polynomials with rational coefficients. Math. Ann. **261**(4), 515–534 (1982)
20. Mattuck, A.: Abelian varieties over p-adic ground fields. Ann. Math. **2**(62), 92–119 (1955)
21. Müller, J.S., Stoll, M.: Canonical heights on genus-2 Jacobians. Algebra Number Theory **10**(10), 2153–2234 (2016)
22. Müller, J.S.: Explicit Kummer varieties of hyperelliptic Jacobian threefolds. LMS J. Comput. Math. **17**(1), 496–508 (2014)
23. Nicholls, C.: Descent methods and torsion on Jacobians of higher genus curves. PhD thesis, University of Oxford (2018)
24. Poonen, B., Schaefer, E.F.: Explicit descent for Jacobians of cyclic covers of the projective line. J. Reine Angew. Math. **488**, 141–188 (1997)
25. Reitsma, B.: Computing the rational torsion subgroup of Jacobians of hyperelliptic curves. Master's thesis, Rijksuniversiteit Groningen (2020)
26. Stoll, M.: MAGMA-related directory. See http://www.mathe2.uni-bayreuth.de/stoll/magma/index.html
27. Stoll, M.: On the height constant for curves of genus two. Acta Arith. **90**, 183–201 (1999)
28. Stoll, M.: Implementing 2-descent for Jacobians of hyperelliptic curves. Acta Arith. **98**(3), 245–277 (2001)
29. Stoll, M.: On the height constant for curves of genus two II. Acta Arith. **104**(2), 165–182 (2002)
30. Stoll, M.: An explicit theory of heights for hyperelliptic Jacobians of genus three. In: Algorithmic and Experimental Methods in Algebra. Geometry, and Number Theory, pp. 665–715. Springer, Cham (2017)
31. Stubbs, A.G.J.: Hyperelliptic curves. PhD thesis, University of Liverpool (2000)
32. Sutherland, A.V.: Genus 3 hyperelliptic curves of small discriminant over $\mathbb{Q}$. See https://math.mit.edu/~drew/gce_genus3_hyperelliptic.txt
33. Sutherland, A.V.: Fast Jacobian arithmetic for hyperelliptic curves of genus 3. In: Proceedings of the Thirteenth Algorithmic Number Theory Symposium, volume 2 of Open Book Ser., pp. 425–442. Math. Sci. Publ., Berkeley, CA (2019)
34. The LMFDB Collaboration.: The L-functions and modular forms database. http://www.lmfdb.org (2022)

Publisher's Note

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