university of groningen

faculty of science and engineering

Computing the torsion subgroup of Jacobian surfaces over number fields

Master Project Mathematics

October 2023

Student: M. Posthumus

First supervisor: Prof. dr. J.S. Müller

Second supervisor: Prof. dr. J. Top

Abstract

We describe and prove the correctness of an algorithm that theoretically computes the K-rational torsion subgroup of an abelian variety defined over a number field K. We make this concrete for Jacobians of genus 2 curves over number fields and implement this in `Magma`. The algorithm is largely based on work by Michael Stoll. Using this algorithm we look into various applications, such as finding unknown torsion structures and finding isogenies between abelian varieties.

Contents

Notation

Let us first introduce some notation. Let K be a number field and define:

- $d := [K : \mathbb{Q}]$,
- $\mathcal{O}_K$ ring of integers of K,
- $\mathfrak{p}$ a prime ideal of $\mathcal{O}_K$ lying above some prime number p,
- $e(\mathfrak{p})$ and $f(\mathfrak{p})$ the ramification index and residue field degree of $\mathfrak{p}$ over p,
- $v_\mathfrak{p} \colon K \to \mathbb{Z} \cup \{\infty\}$ the discrete valuation induced by $\mathfrak{p}$,
- $K_\mathfrak{p}$ the completion of K with respect to $v_\mathfrak{p}$,
- $\mathcal{O}_\mathfrak{p}$ the valuation ring of $K_\mathfrak{p}$,
- $\mathfrak{m}_\mathfrak{p}$ the maximal ideal of $\mathcal{O}_\mathfrak{p}$,
- If k is a field, $\bar{k}$ denotes an algebraic closure of k.

1 Introduction

If K is a number field and A/K is an abelian variety, the K-rational torsion subgroup $A(K)_{\text{tors}}$ is finite by the Mordell-Weil theorem. In case A is an elliptic curve, it is known how to compute the torsion subgroup [Cre97]. Moreover, for $K = \mathbb{Q}$ and A the Jacobian of a genus 2 curve, [Sto98] gives an algorithm to compute the torsion subgroup. A theoretical extension of this algorithm to arbitrary $A/\mathbb{Q}$ is due to [MR23]. In addition, [vB23] gives an algorithm that computes the torsion subgroup of Jacobians of non-hyperelliptic curves of genus 3. However, there is not yet a practical algorithm that computes the torsion subgroup of A/K where K is any number field. This thesis presents such an algorithm in a theoretical setting and implements it in practice for Jacobians of genus 2 curves over number fields. Our algorithm extends the algorithm by [Sto98] which uses a p-adic approach to determine the rational torsion subgroup. If J denotes the Jacobian of a genus 2 curve over $\mathbb{Q}$, [Sto98] reduces J modulo some prime number to obtain points over a finite field. Moreover, [Sto98] derives a bound on the height of torsion points using the height difference between the canonical and the naive height. In order to determine which of the points of J over the finite field lift to $\mathbb{Q}$-rational torsion points, the Kummer variety $\mathcal{K} := J/\{\pm 1\}$ is used together with the theory of heights and the LLL algorithm. The main issue when generalizing this to number fields is that the height of a point P does not relate easily to the absolute values of the coordinates of the point P considered on the Kummer variety. Since the height on projective space over $\mathbb{Q}$ is simply the maximum of the absolute values of the coordinates, we can directly bound the individual coordinate sizes when a height bound is given. In contrast, for the height on projective space over number fields this is not immediately clear. We combine the results of [Tur13] and [FF00] to obtain such a relation. This allows us to generalize Stoll's algorithm since the required theory on heights described in [Sto98] also applies to number fields. The `Magma` [BCP97] code for the implementation of the algorithm for Jacobians of genus 2 curves over number fields can be found on `https://github.com/MaxPosthumus/MasterProject/blob/main/`.

Using the algorithm we compute for different number fields K, the K-rational torsion subgroups of Jacobians of various genus 2 curves defined over K. For elliptic curves over $\mathbb{Q}$, Mazur's theorem [MG78] asserts that all rational torsion subgroups must be isomorphic to one of 15 distinct groups. For elliptic curves over number fields of small degree analogues of Mazur's theorem have been proven, see for example [Sut12]. Additionally, [Mer96] proved the *uniform boundedness conjecture* for elliptic curves over number fields. For a number field K and E/K an elliptic curve, this bounds $|E(K)_{\text{tors}}|$ in terms of the degree of K. However, for abelian varieties of dimension $g \geq 2$, the uniform boundedness conjecture remains a conjecture. Intermediate steps have been made by for instance [CX08]. Hence, it is interesting to determine what torsion structures occur for the Jacobians of genus 2 curves over number fields. Furthermore, the Birch and Swinnerton-Dyer conjecture for abelian varieties over a number field K contains also the order of the K-rational torsion subgroup (see e.g., [Jor05, Conjecture 3.15]).

Section 2 introduces the necessary definitions and theorems. Section 3 describes and proves the correctness of the algorithm. Section 4 concretizes the algorithm for Jacobians of genus 2 curves over number fields. In Section 5 we apply the algorithm to the Jacobians of the 66158 genus 2 curves of the L-functions and Modular Forms Database (`LMFDB`) [LMF23] over various number fields and consider a few applications of the algorithm. Lastly, we make some concluding remarks in Section 6.

2 Preliminaries

This section introduces the necessary preliminaries regarding algebraic geometry and algebraic number theory. We will mainly follow [HS00]. Subsections 2.1, 2.2 and 2.3 provide us with the tools to briefly discuss the idea of the algorithm in Subsection 2.4 after which Subsections 2.5 and 2.6 complete the required preliminaries.

2.1 Hyperelliptic curves and abelian varieties

This section introduces hyperelliptic curves and their Jacobian with corresponding Kummer varieties. Unless stated otherwise, k will denote any field.

2.1.1 Hyperelliptic curves

In this paragraph we will heavily rely on [Sto14].

Definition 2.1. Let $g \in \mathbb{Z}_{\geq 0}$. The *weighted projective plane* $\mathbb{P}^2_g = \mathbb{P}^2_{(1,g+1,1)}$ is the geometric object consisting of the set of all 3-tuples

$$(\xi, \eta, \zeta) \in \mathbb{A}^3(k) \backslash \{0,0,0\}$$

modulo the equivalence relation given by

$$(\xi, \eta, \zeta) \sim (\xi', \eta', \zeta')$$

if there is some $\lambda \in \bar{k}^\times$ such that $(\xi', \eta', \zeta') = (\lambda\xi, \lambda^{g+1}\eta, \lambda\zeta)$. We denote the corresponding equivalence class by $(\xi : \eta : \zeta)$.

Definition 2.2. Let k be a perfect field with $\mathrm{char}(k) \neq 2$ and let $g \in \mathbb{Z}_{\geq 2}$. A *hyperelliptic curve of genus* g over k is the subvariety C of $\mathbb{P}^2_g$ defined by the equation $y^2 = F(x,z)$ where

$$F(x,z) = f_{2g+2}x^{2g+2} + f_{2g+1}x^{2g+1}z + \cdots + f_1 x z^{2g+1} + f_0 z^{2g+2} \in k[x,z] \tag{2.1}$$

is homogeneous of degree $2g+2$ and squarefree.

For the remainder of this paragraph we will assume that C is a hyperelliptic curve as in Definition 2.2 and that k is a perfect field to work with simpler definitions. Note that C is guaranteed to be smooth. If we also allowed fields of characteristic 2, the equation of a hyperelliptic curve takes on a more general form. However, if the characteristic is not equal to 2 this can be transformed into the form as in Definition 2.2.

Remark 2.3. Every genus 2 curve is a hyperelliptic curve of genus 2. See for example [Ber10, Proposition 12.4].

The set of *k-rational points* of C is given by

$$C(k) = \{(\xi : \eta : \zeta) \in \mathbb{P}_g^2(k) \mid \eta^2 = F(\xi, \zeta)\}.$$

We define the affine variety C^{aff} as the intersection of C with the affine patch of $\mathbb{P}_g^2$ defined by $z = 1$, i.e., C^{aff} is defined by the equation $y^2 = F(x, 1) =: f(x)$. In order to reconstruct $F(x, z)$ from $f(x)$ we need $\deg(f) \in \{2g + 1, 2g + 2\}$. But this always holds, since if $f_{2g+2} = f_{2g+1} = 0$ we would be able to write $F(x, z) = z^2 H(x, z)$ for some $H(x, z) \in k[x, z]$ contradicting that F is squarefree.
The *points at infinity* of C are the points obtained by setting $z = 0$ and $x = 1$ in (2.1), i.e., solutions to the equation $y^2 = f_{2g+2}$. If $f_{2g+2} = 0$ there will be exactly one such point, namely $(1 : 0 : 0)$. Otherwise, $(1 : \sqrt{f_{2g+2}} : 0)$ and $(1 : -\sqrt{f_{2g+2}} : 0)$ are the two points at infinity. Depending on whether k contains $\sqrt{f_{2g+2}}$ these may be k-rational points.

Definition 2.4. The map

$$\iota \colon C \to C, \quad (\zeta : \eta : \xi) \mapsto (\zeta : -\eta : \xi)$$

is called the *hyperelliptic involution* of C.
Furthermore, the points that are fixed by ι, that is, points $P \in C$ such that $\iota(P) = P$, are called *Weierstrass points*.

Definition 2.5. The *coordinate ring* of C over k is the quotient ring $k[C] := k[x, y, z]/\langle y^2 - F(x, z)\rangle$ with induced grading from $k[x, y, z]$.

Definition 2.6. The *function field* of C over k, denoted by $k(C)$, is the subfield of the field of fractions of $k[C]$ defined as

$$k(C) := \{\varphi_1/\varphi_2 : \varphi_1, \varphi_2 \in k[C] \text{ are homogeneous of the same degree}\}.$$

Let $\bar{k}$ be an algebraic closure of k and recall that we assume that k is perfect, so $\bar{k}$ is a separable extension of k.

Definition 2.7. Let $\mathrm{Gal}(k)$ denote the absolute Galois group of k, that is, the group of all automorphisms of $\bar{k}$ that fix k. Then we can define an action of $\mathrm{Gal}(k)$ on the points of $C(\bar{k})$ as follows:

$$\begin{aligned} \mathrm{Gal}(k) \times C(\bar{k}) &\to C(\bar{k}) \\ (\sigma, (\zeta : \eta : \xi)) &\mapsto (\sigma(\zeta) : \sigma(\eta) : \sigma(\xi)). \end{aligned}$$

For $\varphi \in k[x, y, z]$, $P \in \mathbb{P}_g^2$ and $\sigma \in \mathrm{Gal}(k)$ we have $\varphi(\sigma(P)) = \sigma(\varphi(P))$. Hence, points of $C(\bar{k})$ are indeed mapped to $C(\bar{k})$ since C is defined over k.

Definition 2.8. The *divisor group* of C, written as Div_C, is the free abelian group generated by the $\bar{k}$-points of C. A divisor $D \in \mathrm{Div}_C$ is of the form

$$D = \sum_{P \in C(\bar{k})} n_P P,$$

where $n_P \in \mathbb{Z}$ for all $P \in C(\bar{k})$ and $n_P = 0$ for all but finitely many points P.
The *degree of* D is the sum of the integers n_P, that is, $\deg(D) := \sum_{P \in C(\bar{k})} n_P$. The set of divisors of degree zero is denoted by Div_C^0. This is in fact a subgroup of Div_C since the degree of divisors is a homomorphism of groups.

The Galois action in Definition 2.7 induces an action on Div_C which we will use in the following definition.

Definition 2.9. A divisor $D \in \mathrm{Div}_C$ is *k-rational* if it is fixed by the action of $\mathrm{Gal}(k)$.

Definition 2.10. For $P \in C(\bar{k})$, the *local ring of C at P* is defined as

$$\bar{k}[C]_P := \{\varphi_1/\varphi_2 \in \bar{k}(C) : \varphi_2(P) \neq 0\}.$$

Definition 2.11. The *valuation* on $\bar{k}[C]_P$ is given by

$$\begin{aligned} v_P : \bar{k}[C]_P &\to \mathbb{Z}_{\geq 0} \cup \{\infty\} \\ \varphi &\mapsto \begin{cases} 0 & \text{if } P \text{ is not a root of } \varphi, \\ m & \text{if } P \text{ is a root of } \varphi \text{ of multiplicity } m, \\ \infty & \text{if } \varphi = 0. \end{cases} \end{aligned}$$

This can be extended to $\bar{k}(C)$ by defining $v_P(\varphi_1/\varphi_2) := v_P(\varphi_1) - v_P(\varphi_2)$.

The valuation in Definition 2.11 makes $\bar{k}[C]_P$ a *discrete valuation ring* (DVR).

Definition 2.12. For $\phi \in \bar{k}(C)^\times$, define the *divisor of* ϕ as

$$\mathrm{div}(\phi) = \sum_{P \in C(\bar{k})} v_P(\phi) P.$$

A divisor $D \in \mathrm{Div}_C$ is called *principal* if $D = \mathrm{div}(\phi)$ for some function $\phi \in \bar{k}(C)^\times$. Write Princ_C for the set of principal divisors. Now consider the map

$$\begin{aligned} \bar{k}(C)^\times &\to \mathrm{Div}_C, \\ \phi &\mapsto \mathrm{div}(\phi). \end{aligned}$$

This is a group homomorphism since v_P is a valuation which implies that for $\phi_1, \phi_2 \in \bar{k}(C)^\times$ we have $v_P(\phi_1\phi_2) = v_P(\phi_1) + v_P(\phi_2)$. Hence its image, i.e., the set of principal divisors, is a subgroup of Div_C.

Definition 2.13. Define the *Picard group* of C as

$$\mathrm{Pic}_C = \mathrm{Div}_C/\mathrm{Princ}_C.$$

Consider the class of the divisor D in Pic_C, which we will denote by $[D]$. Then by definition of Pic_C we can write every element D' in $[D]$ as $D' = D + \mathrm{div}(\phi)$ for some $\phi \in \bar{k}(C)^\times$. For $\phi \in \bar{k}(C)^\times$ and $\sigma \in \mathrm{Gal}(k)$ we have $\mathrm{div}(\sigma(\phi)) = \sigma(\mathrm{div}(\phi))$, which implies that

$$\sigma(D + \mathrm{div}(\phi)) = \sigma(D) + \sigma(\mathrm{div}(\phi)) = \sigma(D) + \mathrm{div}(\sigma(\phi))$$

and thus leads us to the group action

$$\begin{aligned} \mathrm{Pic}_C \times \mathrm{Gal}(k) &\to \mathrm{Pic}_C \\ ([D], \sigma) &\mapsto [\sigma(D)]. \end{aligned}$$

We write $\mathrm{Pic}_C(k)$ for the subgroup of Pic_C fixed by this action; its elements are again called k-rational. For each class in Pic_C we can compute its degree as the degree of any of the representatives since the degree of elements in Princ_C is zero. Similarly as for the divisor group, we define Pic_C^0 to be the subgroup of Pic_C consisting of divisors of degree zero.

2.1.2 Jacobian

Definition 2.14. An *algebraic group* defined over k is a variety A defined over k, a point $e \in A(k)$ and morphisms $+\colon A \times A \to A$ and $-\colon A \to A$ such that $+$ satisfies the axioms of a group law with identity element e and inverses are given by $-$. For more details see [HS00, §A.1.4].

Since morphisms are rational maps and A is defined over k, the set $A(k)$ of k-rational points inherits a group structure.

Definition 2.15. An *abelian variety* is a projective variety that is also an algebraic group.

Example 2.16. An elliptic curve is an abelian variety of dimension 1.

Two important results regarding abelian varieties are presented in the following theorem:

Theorem 2.17. *Let A be an abelian variety.*

(1) A is a commutative algebraic group.

(2) A is smooth.

Proof.

(1) See [HS00, Lemma A.7.1.3].

(2) See [HS00, §A.7.1].

□

We will write $A(k)_{\mathrm{tors}}$ for the k-rational torsion subgroup of A and $A[m]$ for the m-torsion subgroup of A if $m \in \mathbb{Z}$.

Theorem 2.18. *(Mordell-Weil) Let K be a number field and A an abelian variety defined over K. Then $A(K)$ is finitely generated.*

Proof. See [Mor22] and [Wei29]. □

Consequently, we have

$$A(K) \cong A(K)_{\text{tors}} \times \mathbb{Z}^r,$$

where $r \in \mathbb{Z}_{\geq 0}$ is called the *rank* of A and $A(K)_{\text{tors}}$ is finite.

Theorem 2.19. *Given a hyperelliptic curve C/k of genus g, there exists an abelian variety over k with dimension g such that for each $k \subset L \subset \bar{k}$ we have $J(L) \cong \text{Pic}^0_C(L)$.*

Proof. See [HS00, §A.8]. □

The extension L is guaranteed to be a perfect field so $\text{Pic}^0_C(L)$ is well-defined.

Definition 2.20. The abelian variety J is called the *Jacobian variety* (or just *Jacobian*) of the curve C.

Given a point $P_0 \in C(k)$, there is a morphism of algebraic varieties

$$i = i_{P_0} \colon C \to J, \quad P \mapsto [P - P_0]$$

which is injective if $g > 0$ and maps $C(k)$ to $J(k)$. For details see [HS00, §A.8.1].

Remark 2.21. Let C be a hyperelliptic curve over some number field K and denote its Jacobian by J. Assume $P_0 \in C(K)$ and define i_{P_0} as above. If $\text{rank}(J(K)) = 0$, Theorem 2.18 implies that $J(K) \cong J(K)_{\text{tors}}$ so we can use $J(K)_{\text{tors}}$ to compute $C(K)$.

2.1.3 Kummer variety

Definition 2.22. Let A be an abelian variety. The *Kummer variety* is defined as $\mathcal{K} := A/\{-1\}$.

Example 2.23. If $A = E$ is an elliptic curve given by a Weierstrass equation $y^2 = x^3 + ax + b$, the Kummer variety $\mathcal{K}$ is equal to $\mathbb{P}^1$ and is obtained by only considering the x-coordinate of each point $P \in E$. After doing so we can no longer differentiate between P and $-P$.

Theorem 2.24. *Let $\mathcal{K}$ be the Kummer variety of an abelian variety of dimension g. Then $\mathcal{K}$ is an algebraic variety and can be embedded in $\mathbb{P}^{2^g-1}$.*

Proof. See [BL04, Theorem 4.8.1]. □

Once we fix an embedding of $\mathcal{K}$ into $\mathbb{P}^{2^g-1}$, denote the quotient map by

$$\kappa\colon A \to \mathcal{K} \subseteq \mathbb{P}^{2^g-1}. \tag{2.2}$$

We will always assume that κ maps $0 \in A$ to $(0 : 0 : \cdots : 1)$, the *origin of the Kummer*. For $P \in A$, $\kappa(P)$ and $\kappa(-P)$ coincide. Hence, κ is $2:1$ except for points of order 1 or 2 where it is injective. Consequently, the group structure from A is lost in $\mathcal{K}$. However, we can still define multiplication by n for each $n \in \mathbb{Z}$. Firstly, for the abelian variety A and $P \in A$ we already have multiplication by n. In particular, if $n > 0$ define

$$[n](P) = \underbrace{P + P + \cdots + P}_{n \text{ times}}.$$

If $n < 0$, define $[n](P) = [-n](-P)$ and set $[0](P)$ equal to the identity element of A. Now note that $[-1] \circ [n] = [n] \circ [-1]$ because the group law is commutative. Consequently, we can define multiplication by n on the Kummer, denoted by $[[n]]$, such that the following diagram commutes:

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

Assume that we have an algorithm to present $\mathcal{K}$ as a variety in $\mathbb{P}^{2^g-1}$. Then for $Q \in \mathcal{K}$ we will need an algorithm to compute $[[n]](Q)$. For $P \in A$, let $\kappa(P) = (x_1 : x_2 : \cdots : x_{2^g})$ denote the image of P on the Kummer. We start by doubling points on $\mathcal{K}$, that is, computing $[[2]]\kappa(P) = \kappa([2]P)$ for $P \in A$. However, if n is odd we need some way to add distinct points as well. To that end, we want to use the group structure of A to add points on the Kummer. However, consider $\kappa(P_1), \kappa(P_2) \in \mathcal{K}$ and suppose we want to determine $\kappa(P_1+P_2)$ when P_1, P_2 are not known. We know that $\kappa^{-1}(P_1) \in \{P_1, -P_1\}$ and similarly for P_2. Hence, using addition on A we can compute the set $\{\kappa(P_1+P_2), \kappa(P_1-P_2)\}$. However, we do not know which of the elements in the set represents $\kappa(P_1+P_2)$. Consequently, addition on the Kummer is not well-defined, but we can use something called *pseudo addition* which requires more information. More specifically, given $\kappa(P_1), \kappa(P_2), \kappa(P_1-P_2)$ pseudo addition computes $\kappa(P_1+P_2)$. Together with the map $[[2]]$ this leads to an algorithm to compute $[[n]](Q)$ for $Q \in \mathcal{K}$ as described in [MR23, Algorithm 2.1].

2.2 Valuations and absolute values

Definition 2.25. A *valuation* on a field k is a function $v\colon k \to \mathbb{R} \cup \{\infty\}$ such that for all $x, y \in k$

(1) $v(xy) = v(x) + v(y)$,

(2) $v(x+y) \geq \min\{v(x), v(y)\}$,

(3) $v(0) = \infty$.

Moreover, one can show that for $x, y \in k$ with $v(x) \neq v(y)$, one has $v(x+y) = \min\{v(x), v(y)\}$. Call v *discrete* if $v(k^\times) = \delta\mathbb{Z}$ for some $\delta \in \mathbb{R}$.

Definition 2.26. An *absolute value* on a field k is a function $|\cdot|\colon k \to \mathbb{R}_{\geq 0}$ such that for all $x, y \in k$

(1) $|x| = 0 \iff x = 0$,

(2) $|xy| = |x||y|$,

(3) $|x + y| \leq |x| + |y|$

If in addition $|\cdot|$ satisfies $|x+y| \leq \max\{|x|, |y|\}$, call $|\cdot|$ *non-archimedean*. Otherwise, call $|\cdot|$ *archimedean*.

We can use a valuation to define an absolute value in the following way.

Example 2.27. Given $0 < \alpha < 1$ and a valuation v on k we can define a non-archimedean absolute value

$$|\cdot|\colon k \to \mathbb{R}_{\geq 0}, \quad x \mapsto \begin{cases} 0 & \text{if } x = 0, \\ \alpha^{v(x)} & \text{else.} \end{cases}$$

In case $k = \mathbb{Q}$ we can define a valuation as follows. For a prime p and $x \in \mathbb{Z}\backslash\{0\}$, define the *p-adic valuation* as $v_p(x) = \max\{n \geq 0 : p^n \mid x\}$ and set $v_p(0) = \infty$. Moreover, we can extend v_p to $\mathbb{Q}$ by defining $v_p(\frac{a}{b}) := v_p(a) - v_p(b)$ for $\frac{a}{b} \in \mathbb{Q}$ with $a, b \in \mathbb{Z}$. By setting $\alpha = 1/p$ in Example 2.27, we obtain the p-adic absolute value on $\mathbb{Q}$:

$$|\cdot|_p\colon \mathbb{Q} \to \mathbb{R}_{\geq 0}, \quad q \mapsto p^{-v_p(q)}.$$

Now let K be a number field with integers $\mathcal{O}_K$. Note that $\mathcal{O}_K$ is Dedekind and that in Dedekind domains every nonzero prime ideal is invertible which leads to unique prime ideal factorization. Let $\beta \in \mathcal{O}_K\backslash\{0\}$. Then we can write $\beta\mathcal{O}_K = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_s^{e_s}$ for prime ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_s$ of $\mathcal{O}_K$. Define a discrete valuation

$$v_\mathfrak{p}\colon \mathcal{O}_K \to \mathbb{Z}_{\geq 0} \cup \{\infty\}, \quad \beta \mapsto \sup\{n \geq 0 : x \in \mathfrak{p}^n\}.$$

We can extend this to K by using that every element in K can be written as $\frac{a}{b}$ for $a, b \in \mathcal{O}_K$ and setting $v_\mathfrak{p}(\frac{a}{b}) = v_\mathfrak{p}(a) - v_\mathfrak{p}(b)$. For $m \in \mathbb{N}$ we have $v_\mathfrak{p}(\beta) = m \iff \beta \in \mathfrak{p}^m\backslash\mathfrak{p}^{m+1}$.

Example 2.28. Let $K = \mathbb{Q}(i)$ with $\mathcal{O}_K = \mathbb{Z}[i]$. In K we have

$$5 = \underbrace{(1+2i)}_{=:\mathfrak{p}_1}\underbrace{(1-2i)}_{=:\mathfrak{p}_2}.$$

Then $v_{\mathfrak{p}_i}|_\mathbb{Q} = v_5$ for $i \in \{1, 2\}$ but $v_{\mathfrak{p}_1}(1-2i) = 0$ and $v_{\mathfrak{p}_1} = (1+2i) = 1$.

We define the (*normalized*) non-archimedean absolute value on K with respect to $\mathfrak{p}$ by setting $\alpha = 1/N(\mathfrak{p})$ in Example 2.27, which leads to

$$|\cdot|_{\mathfrak{p}} : K \to \mathbb{R}_{\geq 0}, \quad x \mapsto N(\mathfrak{p})^{-v_{\mathfrak{p}}(x)}.$$

For a discussion on normalization of absolute values see [Mil08, §7].

For K we can actually describe how the absolute values on K arise. Call absolute values $|\cdot|_1, |\cdot|_2$ equivalent if there exist $c > 0$ such that $|\cdot|_1 = |\cdot|_2^c$.

Theorem 2.29. *(Ostrowski) Every nontrivial absolute value on K is equivalent to exactly one of the following:*

(1) A non-archimedean absolute value coming from a valuation corresponding to a unique prime ideal in $\mathcal{O}_K$ as described above.

(2) An archimedean absolute value coming from a real or complex embedding of K.

Proof. See [HS00, Proposition B.1.3]. □

We call the set of absolute values in (1) the *finite places* of K and the set of the absolute values in (2) the *infinite places* of K.

Given an absolute value $|\cdot|$ on a field k, we can complete k with respect to $|\cdot|$. In case $k = \mathbb{Q}$, completing with respect to the p-adic absolute value yields $\mathbb{Q}_p$, *the field of p-adic numbers*. In case of a number field K, denote the completion of K with respect to $|\cdot|_{\mathfrak{p}}$ by $K_{\mathfrak{p}}$. Let p be the unique prime number in $\mathfrak{p}$. Then by [Wri14, Corollary 38.2], $[K_{\mathfrak{p}} : \mathbb{Q}_p] < \infty$.

Definition 2.30. Let $K_{\mathfrak{p}}$ be the completion of a number field K with respect to $|\cdot|_{\mathfrak{p}}$. Then define the *valuation ring* of $K_{\mathfrak{p}}$, denoted by $\mathcal{O}_{\mathfrak{p}}$, as

$$\mathcal{O}_{\mathfrak{p}} := \{x \in K_{\mathfrak{p}} : |x|_{\mathfrak{p}} \leq 1\}$$

with unique maximal ideal given by

$$\mathfrak{m}_p = \{x \in K_{\mathfrak{p}} : |x|_{\mathfrak{p}} < 1\}.$$

Moreover, define the *residue field* of $\mathcal{O}_{\mathfrak{p}}$, denoted by $k_{\mathfrak{p}}$, as $k_{\mathfrak{p}} := \mathcal{O}_{\mathfrak{p}}/\mathfrak{m}_{\mathfrak{p}}$.

Elements of $\mathcal{O}_{\mathfrak{p}}$ can be uniquely expressed as a sequence $(x_n)_{n\geq 1}$ with $x_n \in \mathcal{O}_K$ such that $x_{n+1} = x_n \bmod \mathfrak{p}^n$ for all $n \geq 1$.

Remark 2.31. Let $x \in \mathcal{O}_{\mathfrak{p}}$. Now consider $x \bmod \mathfrak{p}^m$ for some $m \geq 1$. This will give a truncation y of x with $y \in \mathcal{O}_K$ such that $y \equiv x \bmod p^m$.

An important isomorphism is given by the following theorem:

Theorem 2.32. *Let $n \geq 1$. Then $\mathcal{O}_K/\mathfrak{p}^n \cong \mathcal{O}_\mathfrak{p}/\mathfrak{m}_\mathfrak{p}^n$. The isomorphism is given by the map*

$$\begin{aligned} \mathcal{O}_K/\mathfrak{p}^n &\to \mathcal{O}_\mathfrak{p}/\mathfrak{m}_\mathfrak{p}^n \\ x + \mathfrak{p}^n &\mapsto x + \mathfrak{m}_\mathfrak{p}^n. \end{aligned}$$

Proof. See [Wri14, Theorem 29.1]. □

The choice of prime ideal affects the structure of $\mathcal{O}_K/\mathfrak{p}$ and $K_\mathfrak{p}$. It is useful to state some general results regarding residue fields and completions of K. Firstly, for a prime ideal I of $\mathcal{O}_K$, we have that $\mathcal{O}_K/I$ is a field. Now define the map

$$\varphi\colon \mathbb{Z}/p\mathbb{Z} \to \mathcal{O}_K/\mathfrak{p}, \quad a + p \mapsto a + \mathfrak{p}.$$

Note that φ is a well-defined field homomorphism since $\mathbb{Z} \subset \mathcal{O}_K$ and $\mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$. Consequently, $\mathcal{O}_K/\mathfrak{p}$ is an extension of $\mathbb{Z}/p\mathbb{Z}$ which is finite since $\mathcal{O}_K$ is a finitely generated $\mathbb{Z}$-module. In particular, $\mathcal{O}_K/\mathfrak{p} \cong \mathbb{F}_{p^{f(\mathfrak{p})}}$ where $f(\mathfrak{p})$ denotes the residue class degree of $\mathfrak{p}$. Secondly, let us study the completion $K_\mathfrak{p}$ more closely.

Lemma 2.33. *Let $\mathfrak{p}$ be a prime ideal lying above the prime p. Then*

$$[K_\mathfrak{p} : \mathbb{Q}_p] = e(\mathfrak{p})f(\mathfrak{p}),$$

where $e(\mathfrak{p})$ and $f(\mathfrak{p})$ denote the ramification index and residue class degree respectively of $\mathfrak{p}$ over p.

Proof. See [Wri14, Theorem 38.2]. □

In order to work with $\mathbb{Q}_p$, we will select $\mathfrak{p}$ such that $K_\mathfrak{p} \cong \mathbb{Q}_p$. In fact, we will work in practice with split primes $\mathfrak{p}$ such that $e(\mathfrak{p}) = f(\mathfrak{p}) = 1$.
If $\mathfrak{p}$ is such that $e(\mathfrak{p}) = f(\mathfrak{p}) = 1$, we have

(i) $\mathcal{O}_K/\mathfrak{p} \cong \mathbb{Z}/p\mathbb{Z}$.

(ii) $K_\mathfrak{p} \cong \mathbb{Q}_p$.

We can generalize (i) as follows.

Lemma 2.34. *Let $n \geq 1$ and assume $e(\mathfrak{p}) = f(\mathfrak{p}) = 1$. Then $\mathcal{O}_K/\mathfrak{p}^n \cong \mathbb{Z}/p^n\mathbb{Z}$.*

Proof. Let π be uniformizer of $\mathfrak{m}_\mathfrak{p}$. Then we have $p = \pi^m \cdot u$ for some $m \in \mathbb{Z}$ and unit u. Now note that $e(\mathfrak{p}) = v_\mathfrak{p}(p) = v_\mathfrak{p}(\pi^m \cdot u) = m \implies m = 1$. Using that $K_\mathfrak{p} \cong \mathbb{Q}_p$, which implies that $\mathcal{O}_\mathfrak{p} \cong \mathbb{Z}_p$, this leads us to the following chain of isomorphisms:

$$\mathcal{O}_K/\mathfrak{p}^n \cong \mathcal{O}_\mathfrak{p}/\mathfrak{m}_\mathfrak{p}^n \cong \mathbb{Z}_p/\pi^n\mathbb{Z}_p \cong \mathbb{Z}_p/p^n\mathbb{Z}_p \cong \mathbb{Z}/p^n\mathbb{Z}.$$

□

2.3 Reduction

From now on, K denotes a number field with integers $\mathcal{O}_K$ and $[K:\mathbb{Q}] = d$. Let v be a finite place of K and note that v corresponds to a non-archimedean absolute value $|\cdot|_\mathfrak{p}\colon K \to \mathbb{R}$ as described in Subsection 2.2. In addition, let p be the unique prime number in $\mathfrak{p}$.
Using the natural reduction map $\bar{}\colon \mathcal{O}_\mathfrak{p} \to \mathcal{O}_\mathfrak{p}/\mathfrak{m}_\mathfrak{p}$ we can define the map

$$\begin{aligned} \bar{}\colon \mathcal{O}_\mathfrak{p}[x,z] &\to (\mathcal{O}_\mathfrak{p}/m_\mathfrak{p})[x,z] \\ \sum a_{i,j}x^i z^j &\mapsto \sum \bar{a}_{i,j}x^i z^j, \quad \bar{a_i} = a_i \bmod \mathfrak{m}_\mathfrak{p}. \end{aligned}$$

Let $C/K_\mathfrak{p}$ be a hyperelliptic curve of genus g defined by $y^2 = F(x,z)$ and assume (possibly after scaling) that $F(x,1) \in \mathcal{O}_\mathfrak{p}[x]$. Write $\tilde{C}$ for the curve over $\mathcal{O}_\mathfrak{p}/\mathfrak{m}_\mathfrak{p}$ defined by $y^2 = \bar{F}(x,z)$. This is not necessarily a hyperelliptic curve. For any $P = (\xi : \eta : \zeta) \in \mathbb{P}^2_g(K_\mathfrak{p})$, after dividing by some $\lambda \in K_\mathfrak{p}$, we can choose a representative (ξ', η', ζ') of P such that $\max\{|\xi'|_\mathfrak{p}, |\eta'|_\mathfrak{p}, |\zeta'|_\mathfrak{p}\} = 1$. We must keep in mind that we are working in weighted projective space, so if $|\eta|_\mathfrak{p}$ is the largest amongst the absolute values of the coordinates divide by η^{g+1} and otherwise divide by ξ or ζ depending on which absolute value is largest. Hence, every point in $\mathbb{P}^2_g$ has some representative with all coordinates in $\mathcal{O}_\mathfrak{p}$ and at least one coordinate not in $\mathfrak{m}_\mathfrak{p}$. This leads us to reduction on weighted projective space:

$$\tilde{}\colon \mathbb{P}^2_g(K_\mathfrak{p}) \to \mathbb{P}^2_g(\mathcal{O}_\mathfrak{p}/\mathfrak{m}_\mathfrak{p}), \quad (\xi : \eta : \zeta) \mapsto (\bar{\xi} : \bar{\eta} : \bar{\zeta}).$$

Let $P = (\xi : \eta : \zeta) \in C(K_\mathfrak{p})$. Using the above map we reduce P to obtain $\tilde{P} \in \mathbb{P}^2_g(\mathcal{O}_\mathfrak{p}/\mathfrak{m}_\mathfrak{p})$ and in fact $\tilde{P} \in \tilde{C}(\mathcal{O}_\mathfrak{p}/\mathfrak{m}_\mathfrak{p})$. This gives rise to the reduction map

$$\rho_\mathfrak{p}\colon C(K_\mathfrak{p}) \to \tilde{C}(\mathcal{O}_\mathfrak{p}/\mathfrak{m}_\mathfrak{p}), \quad (\xi : \eta : \zeta) \mapsto (\bar{\xi} : \bar{\eta} : \bar{\zeta}).$$

Remark 2.35. Similarly as above we can define a reduction map

$$\mathbb{P}^N(K_\mathfrak{p}) \to \mathbb{P}^N(\mathcal{O}_\mathfrak{p}/\mathfrak{m}_\mathfrak{p}) \text{ for all } N \geq 1.$$

Let A be an abelian variety over $K_\mathfrak{p}$. Since A is a projective variety, it can be embeddded in projective space $\mathbb{P}^N(K_\mathfrak{p})$ for some $N \geq 1$. Consequently, we can also define a reduction map

$$\rho_\mathfrak{p}\colon A(K_\mathfrak{p}) \to \tilde{A}(\mathcal{O}_\mathfrak{p}/\mathfrak{m}_\mathfrak{p}).$$

Definition 2.36. Let $C/K_\mathfrak{p}$ be a hyperelliptic curve defined by $y^2 = F(x,z)$ and assume that $F(x,1) \in \mathcal{O}_\mathfrak{p}[x]$. Then C has *good reduction* if $\bar{F}$ is squarefree and $p \neq 2$. Otherwise, C has *bad reduction*. For C/K we say C has good reduction at $\mathfrak{p}$ if $C/K_\mathfrak{p}$ has good reduction and otherwise C has bad reduction at $\mathfrak{p}$.
For a definition of good reduction for general smooth projective varieties see [HS00, §A.9]. In particular, if A/K is the Jacobian variety of C/K then A/K has good reduction if C has good reduction but the converse does not always hold [HS00, §A.9.4].

Remark 2.37. If A has good reduction at $\mathfrak{p}$, the reduction map $\rho_\mathfrak{p} : A(K_\mathfrak{p}) \to \tilde{A}(\mathcal{O}_\mathfrak{p}/\mathfrak{m}_\mathfrak{p})$ is a group homomorphism.

Theorem 2.38. *Let A/K be an abelian variety and let v be a finite place of K at which A has good reduction. Without loss of generality assume that v corresponds to a non-archimedean absolute value $|\cdot|_\mathfrak{p}$ with $\mathfrak{p}$ lying above the prime p. Then for any $m \geq 1$ for which $p \nmid m$, the restriction of the reduction map*

$$\rho_\mathfrak{p} \colon A(K_\mathfrak{p}) \to \tilde{A}(\mathcal{O}_\mathfrak{p}/\mathfrak{m}_\mathfrak{p})$$

to $A(K_\mathfrak{p})[m]$ is injective. In other words, the only torsion in

$$\ker(\rho_\mathfrak{p} : A(K_\mathfrak{p}) \to \tilde{A}(\mathcal{O}_\mathfrak{p}/\mathfrak{m}_\mathfrak{p}))$$

is torsion divisible by p.

Proof. See [HS00, Theorem C.1.4 & Theorem C.2.6]. □

Hence the reduction map is also injective on the m-torsion of $A(K)$ since $K \subset K_\mathfrak{p}$. Denote the kernel of the reduction map $\rho_\mathfrak{p}$ restricted to $A(K_\mathfrak{p})_{\text{tors}}$ by H. Then H actually contains only p power torsion. To see this, let x be an element of H and let $\text{ord}(x) = m$ for $m = p^n q$ with $\gcd(p, q) = 1$. Then $\text{ord}(x^{p^n}) = \text{ord}(x)/\gcd(\text{ord}(x), p^n) = p^n q/p^n = q$. If $q > 1$, this would imply that H contains a nontrival q-torsion element with $p \nmid q$ which contradicts Theorem 2.38. Consequently the reduction map is injective if there is no p-power torsion in the kernel of the reduction map. The following lemma provides a condition on the reduction map being injecive.

Lemma 2.39. *Let $\mathfrak{p}$ be a prime ideal at which A has good reduction and denote the ramification index of $\mathfrak{p}$ by $e(\mathfrak{p})$. In addition, assume that the unique prime p in $\mathfrak{p}$ satisfies $e(\mathfrak{p}) < p - 1$. Then the restriction of reduction map $\rho_\mathfrak{p} : A(K_\mathfrak{p}) \to \tilde{A}(\mathcal{O}_\mathfrak{p}/\mathfrak{m}_\mathfrak{p})$ to $A(K)_{tors}$ is injective.*

Proof. See [Kat80, Appendix]. □

Consequently, if $e(\mathfrak{p}) < p - 1$ we have that $\#A(K)_{\text{tors}} \mid \#\tilde{A}(\mathcal{O}_\mathfrak{p}/\mathfrak{m}_\mathfrak{p})$ since the reduction map is a group homomorphism. We can use this to derive an upper bound on $\#A(K)_{\text{tors}}$ as follows. Select a set of prime ideals S such that each $\mathfrak{p} \in S$ satisfies $e(\mathfrak{p}) < p - 1$, where p is the unique prime lying below $\mathfrak{p}$. Then computing $\#\tilde{A}(\mathcal{O}_p/\mathfrak{m}_p)$ for all $\mathfrak{p} \in S$ leads to

$$\#A(K)_{\text{tors}} \mid \gcd_{\mathfrak{p} \in S} \#\tilde{A}(\mathcal{O}_\mathfrak{p}/\mathfrak{m}_\mathfrak{p}). \tag{2.3}$$

Example 2.40. Let $\mathfrak{p}$ and $\mathfrak{q}$ be prime ideals of $\mathcal{O}_K$ satisfying the conditions in Lemma 2.39. Suppose that $\#\tilde{A}(\mathcal{O}_p/\mathfrak{m}_\mathfrak{p})$ and $\#\tilde{A}(\mathcal{O}_\mathfrak{q}/\mathfrak{m}_\mathfrak{q})$ are coprime. Then we can conclude that $A(K)_{\text{tors}}$ is trivial.

Remark 2.41. Besides computing the gcd as in (2.3) we can sometimes infer a better bound by using the groups structure of $\tilde{A}(\mathcal{O}_\mathfrak{p}/\mathfrak{m}_\mathfrak{p})$ as well (see Example 4.13).

We know now when the reduction map is injective, but we want the reduction map to be surjective as well. Given a point $\tilde{P} \in \tilde{A}(\mathcal{O}_\mathfrak{p}/\mathfrak{m}_\mathfrak{p})$ we want to know if there exists some $P \in A(K_\mathfrak{p})$ such that P reduces to $\tilde{P}$. The following lemma helps us in that regard.

Lemma 2.42. *(Hensel) Let $f_1, \ldots, f_r \in \mathcal{O}_\mathfrak{p}[x_1, \ldots, x_d]$ with $r \leq d$ and $a \in \mathcal{O}_\mathfrak{p}^d$ such that*

$$f_i(a) \equiv 0 \bmod \mathfrak{m}_\mathfrak{p} \text{ for } 1 \leq i \leq d \quad \text{and} \quad \operatorname{rank}\left(\tfrac{\partial f_i}{\partial x_j}(a) \bmod \mathfrak{m}_\mathfrak{p}\right)_{\substack{1 \leq i \leq r \\ 1 \leq j \leq d}} = r.$$

Then there exists a unique $b \in \mathcal{O}_\mathfrak{p}^d$ satisfying

$$f_i(b) = 0 \text{ for } 1 \leq i \leq d \quad \text{and} \quad b \equiv a \bmod \mathfrak{m}_\mathfrak{p}.$$

Proof. See for example [Con20, Theorem 3.3]. □

We can use Lemma 2.42 to prove that the reduction map $\rho_\mathfrak{p} : A(K_\mathfrak{p}) \to \tilde{A}(\mathcal{O}_\mathfrak{p}/\mathfrak{m}_\mathfrak{p})$ is surjective. Following [HS00, Exercise C.9], let $\tilde{P} \in \tilde{A}(\mathcal{O}_\mathfrak{p}/\mathfrak{m}_\mathfrak{p})$ and assume that $\tilde{P}$ is nonsingular. Since we can embed A in projective space $\mathbb{P}^N(K_\mathfrak{p})$ for some $N \geq 1$, we can find a set of generators $f_1, \ldots, f_r \in \mathcal{O}_\mathfrak{p}[x_1, \ldots, x_{N+1}]$ of A. Reducing these generators modulo $\mathfrak{m}_\mathfrak{p}$ yields generators for $\tilde{A}$. Using that $\tilde{P}$ is nonsingular we can verify that both conditions of Lemma 2.42 are satisfied. Hence, there exists $P \in A(K_\mathfrak{p})$ that reduces modulo $\mathfrak{m}_\mathfrak{p}$ to $\tilde{P}$. Consequently, the reduction map is surjective onto the smooth points of $\tilde{A}(\mathcal{O}_\mathfrak{p}/\mathfrak{m}_\mathfrak{p})$ which implies that if A has good reduction at $\mathfrak{p}$, the reduction map $\rho_\mathfrak{p}\colon A(K_\mathfrak{p}) \to \tilde{A}(\mathcal{O}_\mathfrak{p}/\mathfrak{m}_\mathfrak{p})$ is surjective. Moreover, in case A has good reduction at $\mathfrak{p}$, we already concluded that $\rho_\mathfrak{p}$ is injective on m-torsion for m coprime to p. In fact, following [Sto98, §11], each $\tilde{P} \in A(\mathcal{O}_\mathfrak{p}/\mathfrak{m}_\mathfrak{p})[m]$ has a unique lift $P \in A(K_\mathfrak{p})[m]$ if m is coprime to p and A has good reduction at $\mathfrak{p}$.

2.4 The set-up

Now that we have described some of the preliminaries we can make more precise how the algorithm is set up. In Subsection 2.3 we saw that every $\tilde{P} \in A(\mathcal{O}_\mathfrak{p}/\mathfrak{m}_\mathfrak{p})[m]$ has a unique lift $P \in A(K_\mathfrak{p})[m]$ for a prime of good reduction $\mathfrak{p}$ lying above a prime p such that $p \nmid m$. This prompts the question of how to determine whether $P \in A(K)_{\text{tors}} \subset A(K_\mathfrak{p})_{\text{tors}}$. Firstly, by Theorem 2.32 we can work with $\mathcal{O}_K/\mathfrak{p}$ instead of $\mathcal{O}_\mathfrak{p}/\mathfrak{m}_\mathfrak{p}$. Similarly to κ in (2.2), define $\tilde{\kappa} : \tilde{A}(\mathcal{O}_K/\mathfrak{p}) \to \mathcal{K}(\mathcal{O}_K/\mathfrak{p})$ and define $\tilde{R} := \tilde{\kappa}(\tilde{P})$. Then for any $N \geq 1$, we can use Hensel lifting on the Kummer variety to obtain a point $\tilde{R}_N \in \mathcal{K}(\mathcal{O}_K/\mathfrak{p}^N)$ that reduces to $\tilde{R}$ and thereby approximates $\kappa(P)$ (see also Remark 2.31). Next we construct a lattice that contains all lifts of $\tilde{R}_N$ to $A(K_\mathfrak{p})$ and use the theory of heights in Subsection 2.6 to determine what precision is necessary to conclude whether $\tilde{P}$ lifts to a point in $A(K)_{\text{tors}}$.

2.5 Lattices

In this subsection we will outline the main ideas used in the Lenstra–Lenstra–Lovász (LLL) lattice basis reduction algorithm. Furthermore, we describe $\mathcal{O}_K$-lattices and how they can be related to the usual notion of a lattice. We will use $||\cdot||$ to denote the Euclidean norm on $\mathbb{R}^n$.

Definition 2.43. Let $b_1, \dots, b_k \in \mathbb{R}^n$ be $\mathbb{R}$-linear independent. Then

$$\Lambda = \bigoplus_{i=1}^{k} \mathbb{Z} b_i \subset \mathbb{R}^n$$

is a $(\mathbb{Z})$-*lattice* of rank k and $b_1, \dots, b_k$ is a *basis* of Λ.

Definition 2.44. Let $\Lambda \subset \mathbb{R}^n$ be a lattice of rank k. For $1 \leq i \leq k$, the *i-th successive minimum* of Λ is

$$M_i(\Lambda) := \min \left\{ \lambda > 0 : \begin{array}{r} \text{there exist } \mathbb{R}\text{-linearly independent } x_1, \dots, x_i \in \Lambda \\ \text{such that } ||x_j||^2 \leq \lambda \text{ for } 1 \leq j \leq i. \end{array} \right\}.$$

Additionally, the *minimal distance*, denoted by $\mu(\Lambda)$, is defined by $\mu(\Lambda) := \min_{x \in \Lambda \setminus \{0\}} \{||x||\}$.

Remark 2.45. The quantities defined in Definition 2.44 are related in the following way:

$$M_1(\Lambda) = \mu(\Lambda)^2 \quad \text{and} \quad M_1(\Lambda) \leq M_2(\Lambda) \leq \cdots \leq M_k(\Lambda).$$

Given a basis $b_1, \dots, b_k$ of a lattice Λ we can find an orthogonal basis $b_1^*, \dots, b_k^*$ via Gram-Schmidt orthogonalisation:

$$b_1^* := b_1, \quad \mu_{i,j} := \frac{\langle b_i, b_j^* \rangle}{||b_j^*||^2} \quad \text{and} \quad b_j^* := b_j - \sum_{j=1}^{i-1} \mu_{i,j} b_j^*.$$

where $\langle \cdot, \cdot \rangle$ denotes the usual inner product on $\mathbb{R}^n$.

Given a lattice Λ, we want to find a "useful" basis, i.e., a basis that satisfies certain properties and that can be computed relatively easily. For example, if we can relate its basis vectors to the successive minima, we can say something about the length of the vectors in Λ. Additionally, it is often convenient if the basis vectors are orthogonal or "nearly orthogonal", see for example [Gal12, Example 16.3.3]. To address the first issue, we ideally want to find a basis $b_1, \dots, b_k$ of Λ such that $||b_i|| = M_i(\Lambda)$ for $1 \leq i \leq k$. However, as mentioned in [NS04, §2.2], if $k \geq 5$ such a basis may not exist. Instead, LLL finds a basis with the norm of the i-th basis vector close to $M_i(\Lambda)$. Moreover, this basis is "nearly orthogonal".

Definition 2.46. A basis $b_1, \dots, b_k$ of a lattice is *LLL-reduced* if

(1) $|\mu_{i,j}| \leq 1/2$ for $1 \leq j < i \leq k$.

(2) $||b_i^* + \mu_{i,i-1} b_{i-1}^*||^2 \geq \delta ||b_{i-1}^*||^2$, where $1/4 < \delta < 1$.

Mostly $\delta = \frac{3}{4}$ is used.

Theorem 2.47. *Let $b_1, \ldots, b_k$ be LLL-reduced as in Definition 2.46 with $\delta = 3/4$. Then*

$$||b_1|| \leq 2^{\frac{n-1}{2}} \mu(\Lambda).$$

Proof. See [Gal12, Lemma 17.2.12] □

We can use the LLL-algorithm (see e.g., [Gal12, Algorithm 25]) to compute an LLL-reduced basis for a given lattice Λ.

When working with number fields we can define lattices as well.

Definition 2.48. An *$\mathcal{O}_K$-lattice* M is a finitely generated, torsion free module over $\mathcal{O}_K$. In fact, M is free if $\mathcal{O}_K$ is a principal ideal domain (PID).

Lemma 2.49. *Let M be an $\mathcal{O}_K$-lattice. Then there exists $a_1, \ldots, a_n \in M$ and nonzero fractional ideals $\mathfrak{a}_1, \ldots, \mathfrak{a}_n$ of $\mathcal{O}_K$ such that*

$$M = \bigoplus_{i=1}^{n} \mathfrak{a}_i a_i.$$

Proof. See [Coh00, Corollary 1.2.25] □

The representation $(a_i, \mathfrak{a}_i)$ as in Lemma 2.49 is called a *pseudo-basis* of M. We cannot use the LLL algorithm directly for $\mathcal{O}_K$-lattices. Instead, we want to represent $\mathcal{O}_K$ as a $\mathbb{Z}$-lattice as in Definition 2.43. To that end, fix an integral basis of K, that is,

$$\mathcal{O}_K = \mathbb{Z}\omega_1 \oplus \mathbb{Z}\omega_2 \oplus \cdots \oplus \mathbb{Z}\omega_d, \text{ for } \omega_1, \ldots, \omega_d \in \mathcal{O}_K.$$

This defines a group isomorphism

$$\begin{aligned} &\delta_{\mathbb{Z}} : \mathcal{O}_K \to \mathbb{Z}^d \\ &\sum_{i=1}^{d} a_i \omega_i \mapsto (a_1, \ldots, a_d). \end{aligned} \tag{2.4}$$

Defining $\Delta_{\mathbb{Z}} := \mathbb{Z}^d$ we see that $\mathcal{O}_K$ is isomorphic to the $\mathbb{Z}$-lattice $\Delta_{\mathbb{Z}}$.
On the other hand, we can define the *Minkowski embedding* as

$$\begin{aligned} \delta_{\mathbb{R}} \colon \mathcal{O}_K &\to \mathbb{R}^d \\ \alpha &\mapsto \Big(\sigma_1(\alpha), \ldots, \sigma_{r_1}(\alpha), \\ &\qquad \sqrt{2}\mathrm{Re}(\sigma_{r_1+1}(\alpha)), \sqrt{2}\mathrm{Im}(\sigma_{r_1+1}(\alpha)), \ldots, \sqrt{2}\mathrm{Im}(\sigma_{r_1+r_2}(\alpha))\Big) \end{aligned} \tag{2.5}$$

One can show that $\delta_{\mathbb{R}}$ injects into $\mathbb{R}^d$ and that $\delta_{\mathbb{R}}(\mathcal{O}_K)$ is a full lattice in $\mathbb{R}^d$, see for example [Mol99, Theorem 3.10]. Moreover, if we denote the lattice $\delta_{\mathbb{R}}(\mathcal{O}_K)$ by $\Delta_{\mathbb{R}}$, then $\delta_{\mathbb{R}}\colon \mathcal{O}_K \to \Delta_{\mathbb{R}}$ is a group isomorphism. This induces a third group isomorphism

$$\psi\colon \Delta_{\mathbb{Z}} \to \Delta_{\mathbb{R}}, \quad x \mapsto \delta_{\mathbb{R}} \circ \delta_{\mathbb{Z}}^{-1}(x) = A \cdot x, \tag{2.6}$$

where $A = (\delta_{\mathbb{R}}(\omega_1), \ldots, \delta_{\mathbb{R}}(\omega_d))$.

Now let $M = \oplus_{i=1}^{n} \mathfrak{a}_i a_i$ be an $\mathcal{O}_K$-lattice as in Lemma 2.49 and assume that $\mathfrak{a}_1, \ldots, \mathfrak{a}_n$ are nonzero integral ideals. Since every ideal is a free $\mathbb{Z}$-module of rank d, there exist $\beta_1^{(i)}, \ldots, \beta_d^{(i)} \in \mathfrak{a}_i$ such that $\mathfrak{a}_i = \oplus_{j=1}^{d} . \mathbb{Z}\beta_j^{(i)}$ for all $1 \leq i \leq n$. Hence, we can write $M = \oplus_{i,j} \mathbb{Z}\beta_j^{(i)} a_i$. Relabeling the basis vectors leads to

$$M = \oplus_{i=1}^{nd} \mathbb{Z} b_i \text{ for } b_i \in \mathcal{O}_K^m \text{ and some } 1 \leq m \leq n.$$

Using the maps in (2.4) and (2.5) we can embed the b_i's to $\mathbb{R}^{md}$ in two different ways. Hence, we have two ways to consider an $\mathcal{O}_K$-lattice as a $\mathbb{Z}$-lattice. To circumvent precision problems when determining the image of $\delta_{\mathbb{R}}$, we follow [FF00, §4] and use $\delta_{\mathbb{Z}}$ to construct a $\mathbb{Z}$-lattice. Nevertheless, we will use $\delta_{\mathbb{R}}$ to determine bounds on the coefficients of the elements of the $\mathbb{Z}$-lattice in §3.2.2.

Let $\mathfrak{a}$ be an integral ideal such that $\mathfrak{a} = \oplus_{i=1}^{d} \mathbb{Z} a_i$ and note that $\delta_{\mathbb{Z}}(\mathfrak{a})$ is a sublattice of $\mathbb{Z}^d$. Writing

$$\begin{pmatrix} a_1 & \cdots & a_d \end{pmatrix} = \begin{pmatrix} \omega_1 & \cdots & \omega_d \end{pmatrix} \cdot B, \text{ for } B \in \mathbb{Z}^{d \times d} \tag{2.7}$$

we see that the columns $B_1, \ldots, B_d$ of B form a basis of the $\mathbb{Z}$-lattice $\delta_{\mathbb{Z}}(\mathfrak{a})$.
We will not present the construction for general $\mathcal{O}_K$-lattices but instead assume that M is an $\mathcal{O}_K$-lattice such that

$$M = \mathcal{O}_K \begin{pmatrix} a_{11} \\ \vdots \\ a_{1k} \end{pmatrix} \oplus \cdots \oplus \mathcal{O}_K \begin{pmatrix} a_{n1} \\ \vdots \\ a_{nk} \end{pmatrix}, \tag{2.8}$$

with $a_{ij} \in \mathcal{O}_K$ for $1 \leq i \leq n$ and $1 \leq j \leq k$.
Note that $a_{ij}\mathcal{O}_K$ is an integral ideal for all $1 \leq i \leq n$ and $1 \leq j \leq k$. For each $a_{ij}\mathcal{O}_K$ let $B_{ij} \in \mathbb{Z}^{d \times d}$ denote the matrix in (2.7) and write $B_{ij}^{(m)}$ for the m-th column of B_{ij}. Then define

$$L := \begin{pmatrix} B_{11}^{(1)} \\ B_{12}^{(1)} \\ \vdots \\ B_{1k}^{(1)} \end{pmatrix} \oplus \cdots \oplus \mathbb{Z} \begin{pmatrix} B_{11}^{(d)} \\ B_{12}^{(d)} \\ \vdots \\ B_{1k}^{(d)} \end{pmatrix} \oplus \cdots \oplus \mathbb{Z} \begin{pmatrix} B_{n1}^{(1)} \\ B_{n2}^{(1)} \\ \vdots \\ B_{nk}^{(1)} \end{pmatrix} \oplus \cdots \oplus \mathbb{Z} \begin{pmatrix} B_{n1}^{(d)} \\ B_{n2}^{(d)} \\ \vdots \\ B_{nk}^{(d)} \end{pmatrix} \subset \mathbb{Z}^{nd}. \tag{2.9}$$

Since these matrices may not be very clear, it is useful to consider a small example.

Example 2.50. Assume $d = 2$ and consider

$$M = \mathcal{O}_K \begin{pmatrix} a \\ b \end{pmatrix} \oplus \mathcal{O}_K \begin{pmatrix} c \\ e \end{pmatrix} \text{ for } a, b, c, e \in \mathcal{O}_K.$$

Using the integral basis we can write:

$$\begin{aligned} a\omega_1 &= a_{11}\omega_1 + a_{12}\omega_2, & a\omega_2 &= a_{21}\omega_1 + a_{22}\omega_2, \\ b\omega_1 &= b_{11}\omega_1 + b_{12}\omega_2, & b\omega_2 &= b_{21}\omega_1 + b_{22}\omega_2, \\ c\omega_1 &= c_{11}\omega_1 + c_{12}\omega_2, & c\omega_2 &= c_{21}\omega_1 + c_{22}\omega_2, \\ e\omega_2 &= e_{11}\omega_1 + e_{12}\omega_2, & e\omega_2 &= e_{21}\omega_1 + e_{22}\omega_2, \end{aligned}$$

for some $a_{ij}, b_{ij}, c_{ij}, e_{ij} \in \mathbb{Z}$ for $1 \leq i, j \leq 2$.
We can already write down the matrices B_a, B_b, B_c, B_e but for illustration purposes note that

$$a\mathcal{O}_K = a(\mathbb{Z}\omega_1 \oplus \mathbb{Z}\omega_2) = \mathbb{Z}a\omega_1 \oplus \mathbb{Z}a\omega_2 = \mathbb{Z}(a_{11}\omega_{11} + a_{12}\omega_2) \oplus \mathbb{Z}(a_{21}\omega_1 + a_{22}\omega_2).$$

Hence,

$$\begin{pmatrix} a_{11}\omega_1 + a_{12}\omega_2 & a_{21}\omega_1 + a_{22}\omega_2 \end{pmatrix} = \begin{pmatrix} \omega_1 & \omega_2 \end{pmatrix} \begin{pmatrix} a_{11} & a_{21} \\ a_{12} & a_{22} \end{pmatrix} =: \begin{pmatrix} \omega_1 & \omega_2 \end{pmatrix} B_a.$$

The other matrices B_b, B_c, B_e can be defined in exactly the same way. Hence

$$L = \mathbb{Z} \begin{pmatrix} a_{11} \\ a_{12} \\ b_{11} \\ b_{12} \end{pmatrix} \oplus \mathbb{Z} \begin{pmatrix} a_{21} \\ a_{22} \\ b_{21} \\ b_{22} \end{pmatrix} \oplus \mathbb{Z} \begin{pmatrix} c_{11} \\ c_{12} \\ e_{11} \\ e_{12} \end{pmatrix} \oplus \mathbb{Z} \begin{pmatrix} c_{21} \\ c_{22} \\ e_{21} \\ e_{22} \end{pmatrix}.$$

Lemma 2.51. *Let M be an $\mathcal{O}_K$-lattice as in* (2.8) *and L its corresponding $\mathbb{Z}$-lattice as in* (2.9)*. Then M and L are isomorphic as $\mathbb{Z}$-modules.*

Proof. Since in the general case it is rather cumbersome to write down the isomorphism, we will only prove the lemma for M and L as defined in Example 2.50 but the general proof is analogous. To that end, let $\alpha, \beta \in \mathcal{O}_K$ such that $\alpha = \alpha_1\omega_1 + \alpha_2\omega_2$ and $\beta = \beta_1\omega_1 + \beta_2\omega_2$ and consider the map

$$\begin{aligned} \varphi\colon M &\to L \\ \alpha \begin{pmatrix} a \\ b \end{pmatrix} + \beta \begin{pmatrix} c \\ d \end{pmatrix} &\mapsto \alpha_1 \begin{pmatrix} a_{11} \\ a_{12} \\ b_{11} \\ b_{12} \end{pmatrix} + \alpha_2 \begin{pmatrix} a_{21} \\ a_{22} \\ b_{21} \\ b_{22} \end{pmatrix} + \beta_1 \begin{pmatrix} c_{11} \\ c_{12} \\ d_{11} \\ d_{12} \end{pmatrix} + \beta_2 \begin{pmatrix} c_{21} \\ c_{22} \\ d_{21} \\ d_{22} \end{pmatrix}. \end{aligned}$$

Firstly note that φ is well-defined. Moreover, we have

$$\begin{aligned}\varphi\Big(\alpha\begin{pmatrix}a\\b\end{pmatrix}+\beta\begin{pmatrix}a\\b\end{pmatrix}\Big)&=\varphi\Big((\alpha+\beta)\begin{pmatrix}a\\b\end{pmatrix}\Big)\\&=(\alpha_1+\beta_1)\begin{pmatrix}a_{11}\\a_{12}\\b_{11}\\b_{12}\end{pmatrix}+(\alpha_2+\beta_2)\begin{pmatrix}a_{21}\\a_{22}\\b_{21}\\b_{22}\end{pmatrix}\\&=\varphi\Big(\alpha\begin{pmatrix}a\\b\end{pmatrix}\Big)+\varphi\Big(\beta\begin{pmatrix}a\\b\end{pmatrix}\Big).\end{aligned}$$

Furthermore, for $k\in\mathbb{Z}$ we have

$$\begin{aligned}\varphi\Big(k\alpha\begin{pmatrix}a\\b\end{pmatrix}\Big)&=k\alpha_1\begin{pmatrix}a_{11}\\a_{12}\\b_{11}\\b_{12}\end{pmatrix}+k\alpha_2\begin{pmatrix}a_{21}\\a_{22}\\b_{21}\\b_{22}\end{pmatrix}\\&=k\varphi\Big(\alpha\begin{pmatrix}a\\b\end{pmatrix}\Big).\end{aligned}$$

Note that φ is surjective by construction. Lastly, φ must be injective since the $B_{ij}^{(m)}$'s form a basis of the $\mathbb{Z}$-lattice $\delta_{\mathbb{Z}}(a_{ij}\mathcal{O}_K)$. □

We will always use M to refer to an $\mathcal{O}_K$-lattice and L for its corresponding $\mathbb{Z}$-lattice as in (2.9).

Remark 2.52. By Lemma 2.51, vectors in M and L are in one-to-one correspondence. We can make this explicit as follows. Assume $M\subset\mathcal{O}_K^{N+1}$ for some $N\in\mathbb{Z}_{\geq 0}$ and consider $\gamma=(\gamma_0,\dots,\gamma_N)\in M\subset\mathcal{O}_K^{N+1}$. Then for $0\leq i\leq N$ we can write

$$\gamma_i=\begin{pmatrix}\gamma_{i1}&\cdots&\gamma_{id}\end{pmatrix}^T\begin{pmatrix}\omega_1&\cdots&\omega_d\end{pmatrix}\text{ and }\mathbf{y}_i:=\begin{pmatrix}\gamma_{i1}&\cdots&\gamma_{id}\end{pmatrix}\in\mathbb{Z}^d.$$

Now consider the map

$$\begin{aligned}\phi\colon M&\to L\\\gamma&\mapsto\begin{pmatrix}\mathbf{y}_0^T\\\vdots\\\mathbf{y}_N^T.\end{pmatrix}.\end{aligned}$$

and note that elements of M are indeed mapped to L. We will use this map in §3.2.2. Specifically, for arbitrary $x\in M$ we will always denote $\phi(x)$ by x_L.

2.6 Heights

In this subsection we describe the necessary theory on heights. For v a place of K, let K_v denote the completion of K with respect to v. If v is an infinite place then either $K_v = \mathbb{R}$ or $K_v = \mathbb{C}$. On the other hand, if v is a finite place of K it corresponds to an absolute value $|\cdot|_{\mathfrak{p}}$ for $\mathfrak{p} \subset \mathcal{O}_K$ a prime ideal and we have $K_v = K_{\mathfrak{p}}$. In addition, let $\mathbb{Q}_v$ denote the completion of $\mathbb{Q}$ with respect to v restricted to $\mathbb{Q}$. In case v is an infinite place we have $\mathbb{Q}_v = \mathbb{R}$ and if v is a finite place we have $\mathbb{Q}_v = \mathbb{Q}_p$ for p the unique prime number in the ideal $\mathfrak{p}$ corresponding to v. Lastly, let A/K be an abelian variety of dimension g with corresponding Kummer variety $\mathcal{K}$ and fix an embedding κ of $\mathcal{K}$ into $\mathbb{P}^{2^g-1}$.

2.6.1 Height definition

Definition 2.53. Let $N \in \mathbb{Z}_{\geq 1}$ and $P = (x_0 : \cdots : x_N) \in \mathbb{P}^N(K)$. Then the *height* of P is defined by

$$H_K(P) := \prod_v \max\{||x_0||_v, \ldots, ||x_N||_v\},$$

where v runs through the places of K and $||\cdot||_v$ is the normalised absolute value $||x||_v = |x|_v^{n_v}$ where $n_v = [K_v : \mathbb{Q}_v]$.

In fact,

$$\begin{aligned} K_v = \mathbb{R} &\implies ||x||_v = |x|_{\mathbb{R}}, \\ K_v = \mathbb{C} &\implies ||x||_v = |x|_{\mathbb{C}}^2, \\ K_v = K_{\mathfrak{p}} &\implies ||x||_v = N(\mathfrak{p})^{-v_{\mathfrak{p}}(x)}. \end{aligned}$$

Definition 2.54. Let $P \in \mathbb{P}^N(K)$. Then $(x_0, \ldots, x_N) \in K^{N+1}$ is called a *representative of* P if $P = (x_0 : \cdots : x_N)$. Moreover, $(x_0, \ldots, x_N)$ is called an *integral representative of* P if additionally $(x_0, \ldots, x_N) \in \mathcal{O}_K^{N+1}$. By scaling we can always find an integral representative of P.

Definition 2.55. If r_1 is the number of real embeddings of K let

$$\sigma_i \colon K \to \begin{cases} \mathbb{R}, & 1 \leq i \leq r_1, \\ \mathbb{C}, & r_1 + 1 \leq i \leq d, \end{cases}$$

denote the field embeddings of K, where we sorted them to satisfy $\sigma_{r_1+i} = \overline{\sigma_{r_1+r_2+i}}$.

Lemma 2.56. *(Product formula) Let $\alpha \in K^\times$ and $\mathcal{P}_K = \{\mathfrak{p} \subset \mathcal{O}_K \text{ prime}\}$. Then*

$$\prod_{i=1}^{d} |\sigma_i(\alpha)| \prod_{\mathfrak{p} \in \mathcal{P}_K} N(\mathfrak{p})^{-v_{\mathfrak{p}}(\alpha)} = 1$$

Proof.

$$|N(\alpha)| = N(\alpha\mathcal{O}_K) = \prod_{\mathfrak{p}\in\mathcal{P}_K} N(\mathfrak{p})^{v_\mathfrak{p}(\alpha)} \text{ and } |N(\alpha)| = |\prod_{i=1}^{d} \sigma_i(\alpha)|.$$

□

Using Lemma 2.56 we conclude that for $x \in K^\times$

$$\prod_v ||x||_v = 1.$$

Consequently the height of P is independent of the choice of representative for P.

Example 2.57. In case $K = \mathbb{Q}$, the height definition simplifies. Scale $P = (x_0, \ldots, x_N) \in \mathbb{P}^N(\mathbb{Q})$ such that $x_i \in \mathbb{Z}$ for all $1 \leq i \leq N$ and $\gcd(x_0, \ldots, x_N) = 1$. Recall the definition of the p-adic valuation on $\mathbb{Q}$ from Subsection 2.2. Then $|x_i|_p \leq 1$ for all $1 \leq i \leq N$ and $|x_i| = 1$ for at least one i. This implies all nonarchimedean absolute values $|\cdot|_p$ do not contribute to the product in $H_\mathbb{Q}(P)$. Hence, we are left with

$$H_\mathbb{Q}(P) = \max\{|x_0|, \ldots, |x_N|\}.$$

Define the logarithmic height h_K by $h_K(P) := \log H_K(P)$. Now we can define a height function on the K-rational points of abelian varieties using that abelian varieties can be embedded in $\mathbb{P}^N$ for some $N \in \mathbb{Z}_{\geq 1}$.

Definition 2.58. Recall that A/K denotes an abelian variety defined over K. Let $P \in A(K)$. The *naive height* of P with respect to κ is the map $H_{K,\kappa}\colon A(K) \to \mathbb{R}_{\geq 0}$ defined by $H_{K,\kappa}(P) := H_K(\kappa(P))$. In addition, define the *naive logarithmic height* $h_{K,\kappa}$ by $h_{K,\kappa}(P) := \log(H_{K,\kappa}(P))$.

In what follows we will drop the subscript κ from $H_{K,\kappa}$ and $h_{K,\kappa}$ since with the exception of §2.6.2 we work only with heights of points on abelian varieties. Next to the naive height we define the *canonical height* which is well-defined by [HS00, Corollary B.3.4].

Definition 2.59. The *canonical height* $\hat{h}$ on A associated with h_K is defined by

$$\hat{h}(P) = \lim_{n\to\infty} h_K([n]P)/n^2.$$

Important properties of the canonical height are given in the following theorem:

Theorem 2.60. *(Néron-Tate)*

(1) $\hat{h}([n]P) = n^2\hat{h}(P)$ *for all* $n \in \mathbb{Z}$ *and* $P \in A(\bar{K})$.

(2) For $P \in A(\bar{K})$, *we have* $\hat{h}(P) = 0 \iff P \in A(\bar{K})_{tors}$.

(3) The set $\{P \in A(K) \colon \hat{h}(P) \leq B\}$ *is finite for every constant* $B \geq 0$.

(4) The height difference $|\hat{h}(P) - h_K(P)|$ *is bounded for all* $P \in A(\bar{K})$.

Proof. For (1) and (4) see [HS00, Theorem B.5.1], for (2) see [HS00, Proposition B.5.3] and (3) follows from [HS00, Corollary B.5.4.1]. □

It follows that if we are able to derive an actual bound for the height difference, we immediately bound the height of a torsion point since the canonical height of torsion points is zero by (2) of Theorem 2.60.

Corollary 2.61. *Assume that* $|\hat{h}(P) - h_K(P)| \leq \beta$ *for all* $P \in A(K)$ *for some* $\beta \in \mathbb{R}_{\geq 0}$. *Then for all* $P \in A(K)_{tors}$ *we have* $h_K(P) \leq \beta$.

2.6.2 Heights and norms

As explained in Subsection 2.4, given a point $\tilde{P} \in \tilde{A}(\mathcal{O}_K/\mathfrak{p})$ the idea of the algorithm is to construct a lattice that contains all possible lifts of $\tilde{P}$ to $A(K_\mathfrak{p})$. In order to use the lattice to find torsion points, we need some relation between the height bound on torsion points and the length of the lattice vectors. In particular, given a height bound, we want to derive an upper bound on the length of the first vector of an LLL-reduced basis of the lattice (see Subsection 2.5). This is trivial for $\mathbb{Q}$ but not clear for K. One key ingredient is provided by [Tur13], who proves the existence of a representative of a point such that the size of the representative is bounded in some way. We will outline this approach here.

Firstly, let us take a closer look at the definition of the height function. To that end, define the functions $H_\infty \colon K^{N+1} \to \mathbb{R}$ and $H_f \colon K^{N+1} \to \mathbb{R}$ by

$$H_\infty(x_0, \ldots, x_N) = \prod_{v|\infty} \max\{||x_0||_v, \ldots, ||x_N||_v\},$$
$$H_f(x_0, \ldots, x_N) = \prod_{\mathfrak{p}} \max\{|x_0|_\mathfrak{p}, \ldots, |x_N|_\mathfrak{p}\}.$$

Then by definition of H_K, for any point $P = (x_0 : \cdots : x_N) \in \mathbb{P}^N(K)$ we have:

$$H_K(P) = H_\infty(x_0, \ldots, x_N) H_f(x_0, \ldots, x_N).$$

Call H_∞ and H_f the *infinite* and *finite* height respectively.

Lemma 2.62.

$$H_K(P) = H_\infty(x_0, \ldots, x_N)/N(\mathfrak{a}),$$

where $\mathfrak{a}$ *is the fractional ideal of* $\mathcal{O}_K$ *generated by* $x_0, \ldots, x_N$.

Proof. (This is also proved in [Sil07, Theorem 3.7].) We have

$$\begin{aligned}\prod_{\mathfrak{p}} \max\{|x_0|_{\mathfrak{p}}, \ldots, |x_N|_{\mathfrak{p}}\} &= \prod_{\mathfrak{p}} \max\{N(\mathfrak{p})^{-v_{\mathfrak{p}}(x_0)}, \ldots, N(\mathfrak{p})^{-v_{\mathfrak{p}}(x_N)}\} \\ &= 1/\prod_{\mathfrak{p}} \min\{N(\mathfrak{p})^{v_{\mathfrak{p}}(x_0)}, \ldots, N(\mathfrak{p})^{v_{\mathfrak{p}}(x_N)}\} \\ &= 1/\prod_{\mathfrak{p}} N(\mathfrak{p})^{\min\{v_{\mathfrak{p}}(x_0),\ldots,v_{\mathfrak{p}}(x_N)\}} \\ &= 1/N(\mathfrak{a}),\end{aligned}$$

where we used that

$$\begin{aligned}N(\mathfrak{a}) &= N(x_0\mathcal{O}_K + \cdots + x_N\mathcal{O}_K) \\ &= N(\gcd(x_0\mathcal{O}_K, \ldots, x_N\mathcal{O}_K)) \\ &= N(\gcd(\prod_{\mathfrak{p}} \mathfrak{p}^{v_{\mathfrak{p}}(x_0)}, \ldots, \prod_{\mathfrak{p}} \mathfrak{p}^{v_{\mathfrak{p}}(x_N)}) \\ &= N(\mathfrak{p})^{\min\{v_{\mathfrak{p}}(x_0),\ldots,v_{\mathfrak{p}}(x_0)\}}.\end{aligned}$$

□

Similarly to §2.6.1, let $h_\infty = \log H_\infty$ and $h_f = \log H_f$ denote the logarithmic infinite and finite height respectively. Hence, for $x = (x_0, \ldots, x_N)$ such that $P = (x_0 : \cdots : x_N)$, we have:

$$h_K(P) = h_\infty(x) + h_f(x).$$

The values of h_∞ and h_f vary depending on which representative for P we choose. Selecting a representative such that h_f is maximal leads to a minimal value of h_∞. This is useful since h_∞ can be related to the size of x. Before explaining what we mean exactly by the size of x, let us consider how to maximize h_f. Specifically, we want to find an integral representative such that h_f is maximal. Given the class group of K, select from each of its classes an integral ideal that has minimal norm amongst the integral ideals in its class. Denote the collection of these ideals by B and note that $|B| = |\mathrm{CL}(K)|$. Moreover, define $N_K := \max_{\mathfrak{b}\in B} N(\mathfrak{b})$.

Lemma 2.63. *Every $P \in \mathbb{P}^N(K)$ has an integral representative $x = (x_0, \ldots, x_N) \in \mathcal{O}_K^{N+1}$ such that $I(x) \in B$, where $I(x)$ is the content ideal of x, that is, $I(x) = \langle x_0, \ldots, x_N\rangle$.*

Proof. Firstly, $x \neq (0, 0, \ldots, 0)$ so $I(x) \neq \{0\}$. Assume for a contradiction that $I(x) \notin B$. Let J denote the integral ideal in B with $[J] = [I(x)]$. Then we have $aJ = bI(x)$ for some $a, b \in \mathcal{O}_K$. Hence, multiplying $I(x)$ by $a^{-1}b$ yields J. Multiplying all coordinates of x by $a^{-1}b$ still leads to a representative of P. Moreover, since J is an integral ideal we must have that $a^{-1}bx_i \in \mathcal{O}_K$ for $0 \leq i \leq N$. □

Selecting x as in Lemma 2.63 makes sure that the norm of its content ideal is minimal or equivalently that h_f is maximal. Although the choice of x is not unique, the ideal $I(x)$ is since there is only one element in B corresponding to $I(x)$. Now define the ideal of P to be $I(P) := I(x)$ for x as in the Lemma 2.63. Having dealt with the finite height, we will now introduce a notion of size for vectors in the lattice in order to relate this to the infinite height. Recall the field embeddings from Definition 2.55 and let r_1 and r_2 denote the number of real embeddings and pairs of complex embeddings respectively.

Definition 2.64. For $\alpha \in K$, define the T_2-*norm* of α by

$$T_2(\alpha) := \sum_{i=1}^{d} |\sigma_i(\alpha)|^2 = \sum_{i=1}^{r_1+r_2} c_i |\sigma_i(\alpha)|^2, \quad \text{where } c_i := \begin{cases} 1 & i \leq r_1, \\ 2 & \text{otherwise.} \end{cases}$$

We will use the definition of the c_i's in Definition 2.64 throughout this paragraph.

Lemma 2.65. *Let $\alpha, \beta \in K$. Then*

$$T_2(\alpha\beta) \leq T_2(\alpha)T_2(\beta).$$

Proof.

$$T_2(\alpha\beta) = \sum_{i=1}^{n} |\sigma_i(\alpha\beta)|^2 = \sum_{i=1}^{n} |\sigma_i(\alpha)|^2 |\sigma_i(\beta)|^2 \leq (\sum_{i=1}^{n} |\sigma_i(\alpha)|^2)(\sum_{i=1}^{n} |\sigma_i(\beta)|^2) = T_2(\alpha)T_2(\beta).$$

□

Lemma 2.66. *Let $\beta \in \mathcal{O}_K$. Then*

$$|N(\beta)|^{2/d} \leq \frac{1}{d} T_2(\beta).$$

Proof. See [FF00, Lemma 4] □

The T_2-norm is not a norm because it does not satisfy subadditivity, but we can use it to define a proper norm.

Definition 2.67. For $\alpha \in K$, define

$$||\alpha|| := \sqrt{T_2(\alpha)}.$$

Lemma 2.68. *Let $||\cdot||$ be as in Definition 2.67. Then $||\cdot||$ is a norm.*

Proof. We will only prove subadditivity since the other properties are trivial. Let $\alpha, \beta \in K$. Then we have

$$\begin{aligned}||\alpha+\beta|| &= \sqrt{T_2(\alpha+\beta)} = \sqrt{\sum_{i=1}^{d} |\sigma_i(\alpha+\beta)|^2} = \sqrt{\sum_{i=1}^{d} |\sigma_i(\alpha)+\sigma_i(\beta)|^2} \\ &\leq \sqrt{\sum_{i=1}^{d} (|\sigma_i(\alpha)|+|\sigma_i(\beta)|)^2} \leq \sum_{i=1}^{d} \sqrt{(|\sigma_i(\alpha)|+|\sigma_i(\beta)|)^2} \\ &= \sum_{i=1}^{d} |\sigma_i(\alpha)|+|\sigma_i(\beta)| = ||\alpha|| + ||\beta||,\end{aligned}$$

where we used the subadditivity of the square root in the second inequality. □

We can extend these definitions in the following way. Firstly, for $x, y \in K$ define

$$T_2(x,y) = \sum_{i=1}^{d} \sigma_i(x)\overline{\sigma}_i(y).$$

In addition, for $x, y \in K^N$ define $T_2(x,y) = \sum_{i=1}^{N} T_2(x_i, y_i)$. Lastly, for $x \in K^N$ define

$$||x|| := \sqrt{T_2(x,x)}. \tag{2.10}$$

Writing out its definition yields the following for $x \in K^N$:

$$T_2(x,x) = \sum_{i=1}^{N} T_2(x_i,x_i) = \sum_{i=1}^{N}\sum_{j=1}^{d} \sigma_j(x_i)\overline{\sigma}_j(x_i) = \sum_{i=1}^{N}\sum_{j=1}^{d} |\sigma_j(x_i)|^2 = \sum_{i=1}^{N} T_2(x_i).$$

For $\lambda \in \mathbb{Z}$ we have

$$||\lambda x|| = \sqrt{T_2(\lambda x, \lambda x)} = \sqrt{\sum_{i=1}^{N} T_2(\lambda x_i)} = \sqrt{|\lambda| \sum_{i=1}^{N} T_2(x_i)} \leq \sqrt{|\lambda|} \sum_{i=1}^{N} \sqrt{T_2(x_i)}.$$

Hence, contrary to the one-dimensional case, this is not a proper norm if $N > 1$.

We can relate the infinite height and $||\cdot||$ as in (2.10) in the following way. Let $r := r_1 + r_2$ and define

$$L\colon K^\times \to \mathbb{R}^r, \quad \alpha \mapsto (c_i \log|\sigma_i(\alpha)|)_{1\leq i\leq r}.$$

One can show that this is a group homomorphism from $K^\times$ to $(\mathbb{R}^r, +)$ with $\ker L|_{\mathcal{O}_K} = \mathrm{TU}(\mathcal{O}_K)$, the torsion units of $\mathcal{O}_K$ (see e.g., [Mol99, Lemma 3.4]). We can extend this to

$(K^\times)^N$ as follows:

$$\begin{aligned} L\colon (K^\times)^N &\to \mathbb{R}^{N\times r} \\ (x_1,\dots,x_N) &\mapsto \begin{pmatrix} L_{11}(x) & \cdots & L_{1r}(x) \\ \vdots & \ddots & \vdots \\ L_{N1(x)} & \cdots & L_{Nr}(x) \end{pmatrix}, \end{aligned}$$

where

$$L_{ij}(x) = c_j \log|\sigma_j(x_i)|.$$

In addition, define

$$\hat{L}\colon (K^\times)^N \to \mathbb{R}^r, \quad x \mapsto \Big(\max_i L_{i1}(x),\dots,\max_i L_{ir}(x)\Big).$$

and denote $\hat{L}_j(x) = \max_i L_{ij}(x)$. We can relate $\hat{L}$ to the logarithmic infinite height as follows:

$$\sum_j \hat{L}_j(x) = \sum_{j=1}^r c_j \max_i \log|\sigma_j(x_i)| = h_\infty(x). \tag{2.11}$$

Let $z_1,\dots,z_r$ be coordinates on $\mathbb{R}^r$ and define $\Pi(w)$ to be the hyperplane $\sum_j z_j = w$ in $\mathbb{R}^r$. For $x \in (K^\times)^N$ with $h_\infty = w$, (2.11) implies that $\hat{L}(x) \in \Pi(w)$.
Define the function

$$\mu\colon \mathbb{R}^r \to \mathbb{R}, \quad (z_1,\dots,z_r) \mapsto (N+1)\sum_j c_j(\exp(z_j))^{2/c_j}.$$

Lemma 2.69. *[Tur13, Proposition 3.5] The function μ defined above is convex and satisfies*

$$\mu \circ \hat{L}(x) \geq ||x||^2.$$

Proof. Let $x \in K^{N+1}$. The inequality follows from:

$$\begin{aligned} ||x||^2 = T_2(x,x) = \sum_{i=1}^{N+1} T_2(x_i) = \sum_{i=1}^{N+1}\sum_{j=1}^r c_j|\sigma_j(x_i)|^2 = \sum_{i=1}^{N+1}\sum_{j=1}^r c_j \exp(L_{ij}(x))^{2/c_j} \\ \leq (N+1)\sum_{j=1}^r c_j\Big(\exp(\hat{L}_j(x))\Big)^{2/c_j}. \end{aligned}$$

Differentiating μ we see that its Hessian matrix is positive definite which implies that μ is convex. □

The representative $x \in \mathcal{O}_K^{N+1}$ such that $I(P) = I(x)$ is unique up to multiplication by elements of $\mathcal{O}_K^\times$. Hence, it is interesting to see what the effect of units is on the map $\hat{L}$. By Dirichlet's unit theorem (see e.g., [Ste12, Theorem 5.13]) we know that

$$\mathcal{O}_K^\times = \mu_{\mathcal{O}_K} \times \langle \eta_1 \rangle \times \langle \eta_2 \rangle \times \cdots \times \langle \eta_{r-1} \rangle,$$

where $\mu_{\mathcal{O}_K}$ is the group of roots of unity in $\mathcal{O}_K$ and $\eta_1, \eta_2, \ldots, \eta_{r-1}$ are fundamental units.

For $\beta \in \mathcal{O}_K^\times$ we have:

$$1 = |N(\beta)| = \prod_{i=1}^{d} |\sigma_i(\beta)| = \prod_{i=1}^{r} |\sigma_i(\beta)|^{c_i} \implies \sum_{i=1}^{r} \log c_i |\sigma_i(\beta)| = 0.$$

Hence, $L(\mathcal{O}^\times) \subset \Pi(0)$. Consequently, $L(\mathcal{O}^\times)$ is a lattice of full rank in $\Pi(0)$ which we will denote by Λ. Moreover, $\{L(\eta_1), \ldots, L(\eta_{r-1})\}$ forms a basis of this lattice. For a different set of fundamental units we will get a different basis. Using the definition of $\hat{L}$, we can easily verify that for $t_k \in \mathbb{Z}_{\geq 1}$ we have

$$\hat{L}\Big(\prod_k \eta_k^{t_k} x\Big) = \hat{L}(x) + L\Big(\prod_k \eta_k^{t_k}\Big).$$

This means that multiplying x by a product of fundamental units shifts the image under $\hat{L}$ by the image of L of this product. This leads us to the following action:

$$\begin{aligned} \Lambda \times \Pi(w) &\to \Pi(w) \\ (g, y) &\mapsto g + y. \end{aligned}$$

Let $C(w)$ be a fundamental domain for the action of Λ on $\Pi(w)$. For $x \in (K^\times)^n$ with $h_\infty(x) = w$, we have $\hat{L}(x) \in \Pi(w)$ by (2.11). Hence, there exists some $g \in \Lambda$ such that $g + \hat{L}(x) \in C(w)$. This is equivalent to the existence of some unit $\beta \in \mathcal{O}^\times$ such that $\hat{L}(\beta x) \in C(w)$. Consequently, keeping in mind that the domain of $\hat{L}(x)$ is $(K^\times)^{N+1}$, we deduce:

Lemma 2.70. *Let $P \in \mathbb{P}^N(K)$ with no zero coordinates. Then there exists a representative $x \in \mathcal{O}_K^{N+1}$ for P satisfying*

$$h_\infty(x) = h_K(P) + \log(N(I(P))),$$

and

$$\hat{L}(x) \in C(h_\infty(x)) \subset \Pi(h_\infty(x)),$$

where $C(h_\infty(x))$ is any fundamental domain for the action of Λ on $\Pi(h_\infty(x))$.

Lemma 2.71. *There exists a fundamental domain $C(w)$ such that for $x \in C(w)$ we have:*

$$\mu(x) \leq (N+1)\exp(2w/d)c_K,$$

where

$$c_K = \begin{cases} \sum_j c_j \prod_k \exp(|\log|\sigma_j(\eta_k)||) & \text{if } r > 1, \\ 2 & \text{if } r_1 = 0, r_2 = 1, \\ 1 & \text{if } K = \mathbb{Q}. \end{cases}$$

Proof. We choose $C(w)$ in such a way that it is a polytope (for details see [Tur13, Proposition 3.7]). We already saw that μ is convex, which implies that μ attains its maximum on $C(w)$ on one of the vertices of $C(w)$. Evaluating μ at these points yields the result. □

Theorem 2.72. *([Tur13, Theorem 3.8]) Let $P \in \mathbb{P}^N(K)$ with no zero coordinates. Then there exists a representative $x \in \mathcal{O}_K^{N+1}$ for P satisfying*

$$||x||^2 \leq (N+1)\exp\Big(\frac{2(h_K(P) + \log(N(I(P))))}{d}\Big)c_K.$$

Proof. From Lemma 2.70 it follows that we can choose a representative $x \in \mathcal{O}_K^{N+1}$ such that $\hat{L}(x) \in C(h_K(P) + \log(N(I(P))))$. The result now follows from the bounds in Lemma 2.69 and Lemma 2.71. □

For Theorem 2.72 we assume that $P \in \mathbb{P}^K$ has no zero coordinates. However, one can show that Theorem 2.72 holds for general points in $\mathbb{P}^N(K)$ using that if one of the coordinates of P is zero, we can consider a point $P' \in \mathbb{P}^{N-1}(K)$ with $H_K(P) = H_K(P')$. For more details see [Tur13, Lemma 3.9]. This allows us to extend Theorem 2.72 to the following:

Theorem 2.73. *Let $\beta > 0$. Then every $P \in \mathbb{P}^N(K)$ such that $h_K(P) \leq \beta$ has a representative such that*

$$||x||^2 \leq B_L$$

where

$$B_L = (N+1)\exp\Big(\frac{2(\beta + \log(N_K))}{d}\Big)c_K.$$

Proof. See [Tur13, Theorem 3.10]. □

It is important to remember that the set of fundamental units that we choose will affect B_L. In particular, the value of c_K might not be the smallest possible but is likely to be reasonable as noted in [Tur13, §3.8].

3 An algorithm to compute the torsion subgroup of abelian varieties over number fields

In this section we will outline an algorithm that, if assumption 3.1 below is satisfied, can compute the rational torsion subgroup of abelian varieties over number fields. Let A/K be an abelian variety of dimension g defined over a number field K with integers $\mathcal{O}_K$ and $[K:\mathbb{Q}] = d$. Moreover, fix an integral basis of K, that is,

$$\mathcal{O}_K = \mathbb{Z}\omega_1 \oplus \mathbb{Z}\omega_2 \oplus \cdots \oplus \mathbb{Z}\omega_d, \text{ for } \omega_1, \ldots, \omega_d \in \mathcal{O}_K.$$

Additionally, let $\mathcal{K}$ be the Kummer variety of A with κ as in (2.2).
The algorithm builds upon the algorithms presented in [Sto98, §11] and [MR23, Algorithm 3.15] which compute the $\mathbb{Q}$-rational torsion subgroup of Jacobians of hyperelliptic curves defined over $\mathbb{Q}$ of genus 2 and 3 respectively. Specifically, the algorithm essentially generalizes the algorithm in [MR23] to abelian varieties over number fields. The main difference is the construction of the lattice that contains all K-rational torsion points. In case $K = \mathbb{Q}$, the points in $\mathcal{K}(\mathbb{Q})$ can be represented as vectors in a $\mathbb{Z}$-lattice straightforwardly. The height on $\mathbb{Q}$-rational points of A is defined by first mapping the points of A to $\mathcal{K} \subset \mathbb{P}^{2^g-1}$ and subsequently using the usual height on projective space over $\mathbb{Q}$ as given in Example 2.57. This definition of height naturally relates to the length of vectors in a $\mathbb{Z}$-lattice. If K is a general number field we can similarly construct a lattice that contains all K-rational torsion points, although we have to be careful how to represent points of $\mathcal{K}(K)$ as vectors in a $\mathbb{Z}$-lattice. The main issue however is that it is not immediately clear how the height of points on A relates to the length of vectors in this $\mathbb{Z}$-lattice. Using the results of [Tur13, §3] and [FF00], this thesis provides a way to do this.

Assumption 3.1. *We have algorithms for the following:*

(1) The map $\kappa : A \to \mathcal{K} \subset \mathbb{P}^{2^g-1}$ and equations for its image (see Theorem 2.24 and (2.2)).

(2) Deciding whether a given point $R \in \mathcal{K}(K)$ lifts to $A(K)$ under κ.

(3) The map [[2]] and pseudo addition as described in §2.1.3.

(4) A height difference bound β as in Theorem 2.60.

(5) Arithmetic in the group $\tilde{A}(\mathcal{O}_K/\mathfrak{p})$ for prime ideals $\mathfrak{p}$ of $\mathcal{O}_K$ of good reduction, and enumeration of its elements.

We will introduce the different ingredients of the algorithm one by one before giving the complete algorithm.

3.1 Lifting torsion points

The crucial step in computing the K-rational torsion subgroup is deciding whether a point in the reduction modulo $\mathfrak{p}$ of A lifts to a K-rational torsion point. The following algorithm provides a way to do this. Firstly, recall the definition of B_L from Theorem 2.73. Additionally, c_1 and c_2 in Algorithm 3.1 will be defined in the next section in Lemma 3.12. Lastly, for $\mathfrak{p}$ a prime at which A has good reduction define $\tilde{\kappa}$ as $\tilde{\kappa} : \tilde{A}(\mathcal{O}_K/\mathfrak{p}) \to \mathcal{K}(\mathcal{O}_K/\mathfrak{p})$.

Algorithm 3.1:
Input: An abelian variety A/K of dimension g defined over a number field K of degree d with integers $\mathcal{O}_K$, a prime ideal $\mathfrak{p} \subset \mathcal{O}_K$ at which A has good redution lying above p such that $e(\mathfrak{p}) = f(\mathfrak{p}) = 1$ and a point $\tilde{Q} \in \tilde{A}(\mathcal{O}_K/\mathfrak{p})$ of order $m > 2$ with $\gcd(p, m) = 1$.
Output: TRUE if there is a point $Q \in A(K)_{\text{tors}} \subset A(K_p)$ that reduces to $\tilde{Q}$, else FALSE.

---

1. Compute a height bound β such that $H_K(Q) < e^\beta$ for any $Q \in A(K)_{\text{tors}}$.

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 $\mathbb{A}^{2^g}(\mathcal{O}_K/\mathfrak{p})$ and normalised such that the first nonzero coordinate is equal to 1. Set $r := 1, n := 0$.

4. Let $N > 1$ such that $p^N > \left(2^g d(2^{(2^g d-1)/2}\sqrt{2^g d}\sqrt{B_L \cdot c_2})^2 c_1\right)^d (4/d)^{d/2}$. 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 $\mathbb{A}^{2^g}(\mathcal{O}_K/\mathfrak{p}^r)$.

   (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 $\tilde{R}_n =: (\tilde{r}_1 : \cdots : \tilde{r}_{2^g})$ in $\mathcal{K}(\mathcal{O}_K/\mathfrak{p}^N)$. Let $(r_1, \ldots, r_{2^g}) \in \mathbb{Z}^{2^g}$ reduce to $(\tilde{r}_1, \ldots, \tilde{r}_{2^g})$ modulo $\mathfrak{p}^N$. Let M be the $\mathcal{O}_K$-lattice generated by $(r_1, \ldots, r_{2^g})$ and $\mathfrak{p}^N e_1, \ldots, \mathfrak{p}^N e^{2^g}$, where e_i are the standard basis vectors in $\mathcal{O}_K^{2^g}$. Fix an integral basis of $\mathcal{O}_K$ and let L denote the corresponding $\mathbb{Z}$-lattice as described in Subsection 3.2. Moreover, 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 $\mathbb{P}^{2^g-1}(K)$.

6. If $R \notin \mathcal{K}(K)$ or $H(R) > e^\beta$, return FALSE.

7. If $[[m]](R) \neq \kappa(0)$, return FALSE.

8. If $\kappa^{-1}(R) \subset A(K)$, return TRUE. Else return FALSE.

Theorem 3.2. *Algorithm 3.1 terminates and returns TRUE if and only if there is a point $Q \in A(K)_{tors}$ that reduces to $\tilde{Q}$.*

Remark 3.3. If we know how to represent points in $A(K)$ explicitly and can determine $\kappa^{-1}(Q)$ for any $Q \in \mathcal{K}(K)$, we can actually return $\kappa^{-1}(R)$ in step $\boxed{8}$ of Algorithm 3.1 instead of only TRUE or FALSE.

Remark 3.4. Note that $\mathcal{O}_K/\mathfrak{p}^N$ is not a field if $N > 1$. However, for all $P \in \mathbb{P}^{2g-1}(K)$ we can consider an integral representative s of P and reduce the coefficients of s by $\mathfrak{p}^N$ to obtain an element in $\mathbb{P}^{2g-1}(\mathcal{O}_K/\mathfrak{p}^n)$. Hence, $\tilde{R}_n$ in step $\boxed{5}$ of Algorithm 3.1 is well-defined.

Remark 3.5. We need (1) of Assumption 3.1 throughout Algorithm 3.1, (3) in step $\boxed{4}$, (4) in step $\boxed{1}$ and (2) in step $\boxed{8}$.

It is clear that the algorithm terminates, but in order to show correctness we will prove a series of lemmas in the next subsection.

3.2 Correctness of the algorithm

Call $Q \in \mathcal{K}$ an *m-torsion point* if and only if there is some $P \in A[m]$ such that $\kappa(P) = Q$.

Lemma 3.6. *After step $\boxed{4}$ of Algorithm 3.1, $\tilde{R}_n$ is the unique m-torsion point in $\mathcal{K}(\mathcal{O}_K/\mathfrak{p}^N)$ that reduces to $\tilde{\kappa}(\tilde{Q})$.*

Proof. This follows from $K_{\mathfrak{p}} \cong \mathbb{Q}_p$ and [MR23, Proposition 3.6]. □

3.2.1 Lattice construction

We want to construct a lattice that contains all integral points that reduce to $\tilde{R}_n$ as in step $\boxed{5}$ of Algorithm 3.1. A first step is to determine how the points that reduce to $\tilde{R}_n$ relate to the vector $(r_1, \ldots, r_{2^g}) \in \mathbb{Z}^{2^g}$ as in step $\boxed{5}$ of Algorithm 3.1. Instead of using $\tilde{R}_n$ directly, we will use a point $\tilde{P} \in \mathbb{P}^N(\mathcal{O}_K/\mathfrak{p}^n)$ for some $N, n \in \mathbb{Z}_{\geq 1}$ and assume that $\tilde{P}$ modulo $\mathfrak{p}$ is nonzero. This is purely to ease notation and one can think of $\tilde{P}$ as being $\tilde{R}_n$.

Definition 3.7. Let $\tilde{P} \in \mathbb{P}^N(\mathcal{O}_K/\mathfrak{p}^n)$. Call $(x_0, \ldots, x_N) \in \mathcal{O}_K^{N+1}$ an *integral representative of* $\tilde{P}$ if $(x_0, \ldots, x_N)$ reduces to $\tilde{P}$ modulo $\mathfrak{p}^n$. Note that we already defined integral representatives for points in $\mathbb{P}^N(K)$ in Definition 2.54.

For a given $\tilde{P} \in \mathbb{P}^N(\mathcal{O}_K/\mathfrak{p}^n)$ we want to find all points $P \in \mathbb{P}^N(K)$ that reduce to $\tilde{P}$. Every such point has an integral representative, so it suffices to find all integral representatives of $\tilde{P}$. Since $\mathcal{O}_K$ is Dedekind we have $\mathfrak{p}^n = (\pi_1, \pi_2)$ for some $\pi_1, \pi_2 \in \mathcal{O}_K$ [Mol99, Exercise 1.46]. Then we can find the integral representatives in the following way.

Lemma 3.8. *Let $\tilde{P} \in \mathbb{P}^N(\mathcal{O}_K/\mathfrak{p}^n)$ such that $\tilde{P}$ modulo $\mathfrak{p}$ is nonzero and let s be an integral representative for $\tilde{P}$. Then every integral representative of $\tilde{P}$ is given by $cs + \pi_1 y + \pi_2 z$ for some $c \in \mathcal{O}_K$ satisfying $c \notin \mathfrak{p}$ and some $y, z \in \mathcal{O}_K^{N+1}$.*

Proof. Let x be any integral representative of $\tilde{P}$. Without loss of generality we have:

$$s = \alpha x + y\pi_1 + z\pi_2,$$

for some $\alpha \in K^\times$ and $y, z \in \mathcal{O}_K^{N+1}$.
Write $s = (s_0, \ldots, s_N)$ and $x = (x_0, \ldots, x_N)$. We will use the valuation induced by $\mathfrak{p}$. We need $v_\mathfrak{p}(s_i) = 0$ for some $0 \leq i \leq N$, otherwise each coordinate of s would be in $\mathfrak{p}$ and s would reduce to the zero vector modulo $\mathfrak{p}$. However, by construction, reducing $\tilde{P}$ modulo $\mathfrak{p}$ is nonzero. Let us now distinguish two cases:

(1) $v_\mathfrak{p}(\alpha) > 0$. Then we get:

$$v_\mathfrak{p}(s_i) \geq \min\{v_\mathfrak{p}(\alpha x_i), v_\mathfrak{p}(y_i\pi), v_\mathfrak{p}(z_i\pi)\} > 0 \text{ for all } i \in \{0, \ldots, N\} \lightning,$$

where we used that $x_i, y_i, z_i \in \mathcal{O}_K \subset \mathcal{O}_\mathfrak{p}$ and $\pi_1, \pi_2 \in \mathfrak{p}^n \subset \mathfrak{p}$.

(2) $v_\mathfrak{p}(\alpha) < 0$. Then we can write:

$$x = \alpha^{-1}s - \alpha^{-1}y\pi_1 - \alpha^{-1}z\pi_2.$$

Hence,

$$v_\mathfrak{p}(x_i) \geq \min\{v_\mathfrak{p}(\alpha^{-1}s_i), v_\mathfrak{p}(\alpha^{-1}y_i\pi_1), v_\mathfrak{p}(\alpha^{-1}z_i\pi_2)\} > 0 \text{ for all } i \in \{0, \ldots, N\} \lightning,$$

where we used that $v_\mathfrak{p}(\alpha^{-1}) = -v_\mathfrak{p}(\alpha)$ and the same reasoning as in (1).

Consequently, we must have that $v_\mathfrak{p}(\alpha) = 0$, which means that $\alpha \in \mathcal{O}_p^\times$. This allows us to write:

$$\beta s - \beta y\pi_1 - \beta z\pi_2 = x,$$

where $\alpha^{-1} =: \beta \in \mathcal{O}_\mathfrak{p}$.
Reducing modulo $\mathfrak{m}_\mathfrak{p}$ and noting that $\pi_1, \pi_2 \in \mathfrak{m}_\mathfrak{p}$, we get:

$$\beta s_i \equiv x_i \bmod \mathfrak{m}_\mathfrak{p} \text{ for all } i \in \{0, \ldots, N\}.$$

Using the isomorphism of Theorem 2.32 and that $s_i, x_i \in \mathcal{O}_K$, we have:

$$\gamma s_i \equiv x_i \bmod \mathfrak{p} \text{ for all } i \in \{0, \ldots, N\},$$

for some $\gamma \in \mathcal{O}_K/\mathfrak{p}$. We can lift this to $\mathcal{O}_K/\mathfrak{p}^n$ to get:

$$\gamma s + w_1\pi_1 + w_2\pi_2 = x,$$

for some $w_1, w_2 \in \mathcal{O}_K^{N+1}$. □

Starting with an integral representative of $\tilde{P}$, Lemma 3.8 provides a way to find all integral representatives. We will use this to construct the lattice.

Proposition 3.9. *Let $n, N \in \mathbb{Z}_{\geq 1}$ and let $\tilde{P} \in \mathbb{P}^N(\mathcal{O}_K/\mathfrak{p}^n)$ such that $\tilde{P}$ modulo $\mathfrak{p}$ is nonzero. Let*

$$v := (r_0, \ldots, r_N) \in \mathcal{O}_K^{N+1} \backslash \{0\}$$

be such that $R := \mathbb{P}v := (r_0 : \cdots : r_N) \in \mathbb{P}^N(K)$ lifts $\tilde{P}$.
Let M be the $\mathcal{O}_K$-lattice defined by:

$$M := \mathcal{O}_K v \oplus \mathfrak{p}^n e_1 \oplus \mathfrak{p}^n e_2 \oplus \cdots \oplus \mathfrak{p}^n e_{N+1}.$$

Then M contains all vectors w such that the corresponding point $\mathbb{P}w \in \mathbb{P}^N(K)$ reduces modulo $\mathfrak{p}^n$ to $\tilde{P}$. Let

$$u := a_0 v + (\pi_1 a_{11} + \pi_2 a_{12})e_1 + (\pi_1 a_{21} + \pi_2 a_{22})e_2 + \cdots + (\pi_1 a_{N+1,1} + \pi_2 a_{N+1,2})e_{N+1},$$

with $a_0, a_{ij} \in \mathcal{O}_K$ for $1 \leq j \leq 2$ and $1 \leq i \leq N+1$.
If $a_0 \notin \mathfrak{p}$, then $\mathbb{P}u \in \mathbb{P}^N(K)$ reduces modulo $\mathfrak{p}^n$ to $\tilde{P} \in \mathbb{P}^N(\mathcal{O}_K/\mathfrak{p}^n)$.

Proof. We claim that we can obtain all vectors corresponding to points reducing modulo $\mathfrak{p}^n$ to $\tilde{P}$ by considering $v_0 := v$, and following a combination of either of the following steps iteratively:

(i) Setting $v_{j+1} := \alpha_0 v_j$ for $\alpha_0 \in \mathcal{O}_K \backslash \mathfrak{p}$

(ii) Setting $v_{j+1} := v_j + (\pi_1 \alpha_1 + \pi_2 \alpha_2)e_i$ for $1 \leq i \leq N+1$ and $\alpha_1, \alpha_2 \in \mathcal{O}_K$.

Let us justify (i) and (ii). Firstly, we need $a_0 \notin \mathfrak{p}$ as explained in the proof of Lemma 3.8. Secondly, Lemma 3.8 shows that we can start with any integral representative of $\tilde{P}$ and subsequently find all points reducing to $\tilde{P}$ using the construction in (i) and (ii). In particular, starting with v suffices. Moreover, the vectors produced by following (i) and (ii) are clearly in M. □

Using that $\mathfrak{p}^n = \pi_1 \mathcal{O}_K + \pi_2 \mathcal{O}_K$ we see that M is in the form as in (2.8). Hence, we can use the correspondence between $\mathcal{O}_K$-lattices and $\mathbb{Z}$-lattices as described by (2.9) to find a $\mathbb{Z}$-lattice L that is isomorphic to M as $\mathbb{Z}$-modules. Since we will use L extensively, we will make its construction explicit. To that end, we can express the result of multiplying π_1, π_2 by elements of $\mathcal{O}_K$ in terms of the integral basis, that is,

$$\pi_i \omega_j = a_{ij}^{(1)} \omega_1 + a_{ij}^{(2)} \omega_2 + \cdots + a_{ij}^{(d)} \omega_k \text{ for } i \in \{1, 2\} \text{ and } 1 \leq j \leq d \text{ and some } a_{ij}\text{'s} \in \mathbb{Z}.$$

Now define:

$$c_{ij} = (a_{ij}^{(1)}, a_{ij}^{(2)}, \ldots, a_{ij}^{(d)}) \text{ for } i \in \{1, 2\} \text{ and } 1 \leq j \leq d.$$

Then using these c_{ij}'s, we can define:

$$c_{ij}^{(m)} = (\underbrace{0,0,\ldots,0}_{m\cdot d \text{ times}}, c_{ij}, \underbrace{0,0,\ldots,0}_{(N-1)\cdot d - m\cdot d \text{ times}}) \text{ for } 0 \leq m \leq N-1.$$

Additionally, define

$$\begin{aligned}
b_0 &= (r_0, \underbrace{0,0,\ldots,0}_{d-1 \text{ times}}, r_1, \underbrace{0,0,\ldots,0}_{d-1 \text{ times}}, \ldots\ldots, r_N, \underbrace{0,0,\ldots,0}_{d-1 \text{ times}}) \\
b_1 &= (0, r_0, \underbrace{0,\ldots,0,0}_{d-2 \text{ times}}, 0, r_1, \underbrace{0,0,\ldots\ldots,0}_{d-2 \text{ times}}, 0, r_N, \underbrace{0,0,\ldots,0}_{d-2 \text{ times}}) \\
&\vdots \\
b_{d-1} &= (\underbrace{0,0,\ldots,0}_{d-1 \text{ times}}, r_0, \underbrace{0,0,\ldots,0}_{d-1 \text{ times}}, r_1, \ldots\ldots, \underbrace{0,,0\ldots,0}_{d-1 \text{ times}}, r_N)
\end{aligned}$$

Finally, we can define the $\mathbb{Z}$-lattice as follows:

$$L := \oplus_{i=0}^{d-1} \mathbb{Z} b_i \oplus_{i,j,m} \mathbb{Z} c_{ij}^{(m)}. \tag{3.1}$$

Then using Lemma 3.9 and the correspondence between vectors in M and L, we see that the lattice L contains all vectors u such that its corresponding vectors w in M satisfy that $\mathbb{P}w \in \mathbb{P}^d(K)$ reduces to $\tilde{P}$ modulo $\mathfrak{p}^n$.

Remark 3.10. In case $\mathfrak{p}^n$ is principal, we can use only 1 generator instead of 2. This reduces the amount of vectors needed to define the lattice L. In practice, this leads to slightly faster computations.

Example 3.11. Let us now illustrate this in a small example, assume $d = 2, N = 1$ and $\mathfrak{p}^n = (\pi)$. Consider $P = (x_0 : x_1) \in \mathbb{P}^1(K)$ with $x_0, x_1 \in \mathcal{O}_K$ reducing to $\tilde{P}$ modulo $\mathfrak{p}^n$. We know that $\mathbb{P}v = (r_0 : r_1)$ with v as in Proposition 3.9 also reduces to $\tilde{P}$ modulo $\mathfrak{p}^n$. Using Lemma 3.8, this implies:

$$\begin{aligned}
x_0 &= \alpha r_0 + \pi y, \\
x_1 &= \alpha r_1 + \pi z,
\end{aligned}$$

for $\alpha, y, z \in \mathcal{O}_K$.
Using the integral basis, we can write $\alpha = \alpha_1\omega_1 + \alpha_2\omega_2$, $y = y_1\omega_1 + y_2\omega_2$ and $z = z_1\omega_1 + z_2\omega_2$ for some $\alpha_1, \alpha_2, y_1, y_2, z_1, z_2 \in \mathbb{Z}$. Consequently, we get:

$$\begin{aligned}
\alpha r_0 + \pi y &= (\alpha_1\omega_1 + \alpha_2\omega_2)r_0 + \pi(y_1\omega_1 + y_2\omega_2) = \alpha_1 r_0\omega_1 + \alpha_2\omega_2 v_1 + y_1\pi\omega_1 + y_2\pi\omega_2, \\
\alpha r_1 + \pi z &= (\alpha_1\omega_1 + \alpha_2\omega_2)r_1 + \pi(z_1\omega_1 + z_2\omega_2) = \alpha_1 r_1\omega_1 + \alpha_2\omega_2 r_1 + z_1\pi\omega_1 + z_2\pi\omega_2.
\end{aligned}$$

Note that

$$\begin{aligned}(\alpha_1 r_0\omega_1, \alpha_1 r_1\omega_1) &= \alpha_1 b_0 \in L,\\ (\alpha_2 r_0\omega_2, \alpha_2 r_1\omega_2) &= \alpha_2 b_1 \in L,\\ (y_1\pi\omega_1, z_1\pi\omega_1) &= y_1 c_{11}^{(0)} + z_1 c_{11}^{(1)} \in L.\\ (y_2\pi\omega_1, z_2\pi\omega_1) &= y_2 c_{12}^{(0)} + z_2 c_{12}^{(1)} \in L.\end{aligned}$$

Hence, the vector corresponding to P is indeed contained in the lattice L.

3.2.2 p-adic precision

Now that we have shown that the lattice in (3.1) includes all points reducing to $\tilde{R}_n$ (as in Algorithm 3.1), we have to justify the p-adic precision used in the algorithm. We have to select the p-adic precision such that we can be certain that a point in $A(K_\mathfrak{p})$ actually lifts to $A(K)$. In what follows we will use many of the functions introduced in §2.6.2. Recall Definitions 2.64 and 2.67 and that for $x = (x_0, \ldots, x_N) \in \mathcal{O}_K^{N+1}$ we have

$$||x|| = \sqrt{T_2(x,x)} \text{ with } T_2(x,x) = \sum_{i=0}^{N} T_2(x_i).$$

Additionally, define

$$||x||_\infty := \max_i \sqrt{T_2(x_i)}. \tag{3.2}$$

Recall that for $\beta \in \mathcal{O}_K$,

$$||\beta|| = \sqrt{T_2(\beta)}$$

defines a norm on the 1-dimensional K-vector space K.
Theorem 2.73 asserts that every $P \in \mathbb{P}^N(K)$ such that $H_K(P) \leq e^\beta$ has a representative $x \in \mathcal{O}_K^{N+1}$ with $||x||^2 \leq B_L$ where B_L is defined as

$$B_L = (N+1)\exp\Big(\frac{2(\beta + \log(N_K))}{d}\Big)c_K. \tag{3.3}$$

Writing $x = (x_0, \ldots, x_N) \in \mathcal{O}_K^{N+1}$, we have the following:

$$||x||^2 = T_2(x,x) = \sum_{i=0}^{N} T_2(x_i) \leq B_L \implies T_2(x_i) \leq B_L \text{ for all } i \in \{0, \ldots, N\}.$$

If x is contained in M we want to relate the norm of x to the norm of its corresponding integer vector in the lattice L. Recall the definitions of $\delta_\mathbb{Z}$ and $\delta_\mathbb{R}$ in (2.4) and (2.5) respectively. As in Subsection 2.5 define the lattices $\Delta_\mathbb{Z} := \mathbb{Z}^d$ and $\Delta_\mathbb{R} := \delta_\mathbb{R}(\mathcal{O}_K)$. We

want to define quadratic forms on $\Delta_{\mathbb{Z}}$ and $\Delta_{\mathbb{R}}$. By applying the scalar product of $\mathbb{R}^n$ to the image of $\delta_{\mathbb{Z}}$ we get the following map:

$$\begin{aligned} Q_{\Delta_{\mathbb{Z}}} \colon \mathcal{O}_K &\to \mathbb{R}_{\geq 0} \\ \alpha &\mapsto (a_1)^2 + (a_2)^2 + \cdots + (a_d)^2. \end{aligned}$$

Furthermore, we define $Q_{\mathbb{R}}(\alpha) := T_2(\alpha)$.

Lemma 3.12. *Recall the definition of ψ and the corresponding matrix A as defined in (2.6). Then there exist constants $c_1, c_2 \in \mathbb{R}$ such that for all $x, y \in \mathcal{O}_K$*

(i) $Q_{\mathbb{R}}(x) \leq c_1 Q_{\mathbb{Z}}(x)$,

(ii) $Q_{\mathbb{Z}}(y) \leq c_2 Q_{\mathbb{R}}(y)$.

Here we can take c_1 to be the largest eigenvalue of $A^T \cdot A$ and c_2 to be the inverse of the smallest eigenvalue of $A^T \cdot A$.

Proof. See [FF00, §4]. □

Remark 3.13. Note that the eigenvalues of $A^T \cdot A$ are real and positive, which means that c_1 and c_2 in Lemma 3.12 are real and positive.

Lemma 3.14. *Let $\gamma \in \mathcal{O}_K$. If $T_2(\gamma) \leq c$, then $Q_{\mathbb{Z}}(\gamma) \leq c_2 \cdot c$.*

Proof. See [FF00, Lemma 6]. □

Finally, let $P \in \mathbb{P}^N(K)$ with $H_K(P) \leq e^{\beta}$. Let $x = (x_0, \ldots, x_N) \in \mathcal{O}_K^{N+1}$ be the integral representative as in Theorem 2.73 and assume that $x \in M$. Then following Remark 2.52, x corresponds to a vector x_L in L, and writing

$$x_i = \begin{pmatrix} x_{i1} & \cdots & x_{id} \end{pmatrix}^T \begin{pmatrix} \omega_1 & \cdots & \omega_d \end{pmatrix} \text{ and } \mathbf{y}_i := \begin{pmatrix} x_{i1} & \cdots & x_{id} \end{pmatrix} \in \mathbb{Z}^d$$

for $0 \leq i \leq N$, we have

$$x_L = \begin{pmatrix} \mathbf{y}_0^T \\ \vdots \\ \mathbf{y}_N^T \end{pmatrix}.$$

Then using Lemma 3.14 we have:

$$T_2(x_i) \leq B_L \text{ for all } i \in \{0, \ldots, N) \implies Q_{\mathbb{Z}}(x_i) \leq B_L \cdot c_2 \text{ for all } i \in \{0, \ldots, N\}.$$

Hence,

$$B_L \cdot c_2 \geq Q_{\mathbb{Z}}(x_i) = \sum_{j=1}^{d} (\mathbf{y}_i)_j^2 = ||\mathbf{y}_i||_2^2,$$

which implies that

$$||\mathbf{y}_i||_\infty \leq \sqrt{B_L \cdot c_2} \text{ for all } i \in \{0, \dots, N\}. \tag{3.4}$$

To summarize, if the T_2-norm of an element $x \in M$ is bounded from above by B_L, then the corresponding vector $x_L \in L$ has coefficients bounded from above by $\sqrt{B_L \cdot c_2}$.

Before proving the main proposition, we need an intermediate result which generalizes [MR23, Lemma 3.12].

Lemma 3.15. *Let $B \geq 1$ be a real number and let $N \in \mathbb{Z}_{\geq 1}$. Let $u, u' \in \mathcal{O}_K^{N+1} \backslash \{0\}$ such that*

(a) $||u||_\infty, ||u'||_\infty \leq B$ (see (3.2) for the definition of $|| \cdot ||_\infty$),

(b) there is an ideal $D \subset \mathcal{O}_K$ with $N(D) > (4B^4/d)^{d/2}$ such that all ideals generated by 2×2 minors of the matrix $\begin{pmatrix} u \\ u' \end{pmatrix} \in \mathcal{O}_K^{2\times(N+1)}$ are divisible by D.

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

Proof. Let

$$\begin{pmatrix} u \\ u' \end{pmatrix} = \begin{pmatrix} u_0 & u_2 & \cdots & u_N \\ u'_0 & u'_2 & \cdots & u'_N \end{pmatrix} \implies m_i := \det \begin{pmatrix} u_i & u_{i+1} \\ u'_i & u'_{i+1} \end{pmatrix} = u_i u'_{i+1} - u'_i u_{i+1}.$$

Hence, using the triangle inequality for the norm $|| \cdot ||$ and Lemma 2.65, we have

$$||m_i|| \leq ||u_i||||u'_{i+1}|| + ||u'_i||||u_{i+1}|| \leq 2B^2,$$

where the last inequality follows from (a) and nonnegativity of the norm.
Now consider an arbitrary 2×2 minor and denote it by m. Moreover, denote the ideal $m\mathcal{O}_K$ by M. Then by (b) we have that $D \mid M$ so that there exists an ideal $C \subset \mathcal{O}_K$ such that $M = CD$. Taking norms on both sides leads to $N(D) \mid N(M)$. On the other hand, using that $|N_{K/\mathbb{Q}}(m)| = N(M)$, we have the following:

$$\left.\begin{array}{l} ||m|| \leq 2B^2 \implies T_2(m) \leq 4B^4 \\ |N_{K/\mathbb{Q}}(\beta)|^{2/d} \leq 1/dT_2(\beta) \text{ for all } \beta \in \mathcal{O}_K \text{ (Lemma 2.66)} \end{array}\right\} \implies N(M) \leq (4B^4/d)^{d/2}.$$

However, (b) implies that $N(D) > (4B^4/d)^{d/2}$. Consequently, $N(M) = 0$ which implies that m vanishes. Therefore, $u = \lambda u'$ for some nonzero $\lambda \in K$. □

Proposition 3.16. *Let $\tilde{R}_n, L, w, R$ be as in step $\boxed{5}$ of of Algorithm 3.1 and define $C := \sqrt{B_L \cdot c_2}$. Let $N \in \mathbb{Z}_{\geq 1}$ such that $p^N > \left(2^g d(2^{(2^g d-1)/2}\sqrt{2^g d}C)^2 c_1\right)^d (4/d)^{d/2}$. Then*

(a) If $H_K(R) \leq e^\beta$, then R is the unique point in $\mathbb{P}^{2^g-1}(K)$ of height $\leq e^\beta$ that reduces to $\tilde{R}_n$.

(b) If $H_K(R) > e^\beta$, then there are no points of height $\leq e^\beta$ that reduce to $\tilde{R}_n$.

Proof. We distinguish two cases:

(i) Suppose that $||w||_\infty > 2^{(2^g d-1)/2}\sqrt{2^g d}C$. Then if we choose $\delta = \frac{3}{4}$ in the LLL-algorithm, Theorem 2.47 asserts that w has euclidean length at most $2^{(2^g d-1)/2}$ times the euclidean length of the shortest nonzero vector. Denote the shortest vector by z. Then we have:

$$||w||_2 \leq 2^{(2^g d-1)/2}||z||_2 \implies ||w||_\infty \leq 2^{(2^g d-1)/2}||z||_2 \leq \sqrt{2^g d}2^{(2^g d-1)/2}||z||_\infty,$$

which implies that $||z||_\infty > C$.
Hence, suppose there exists a vector $y \in L$ such that $\mathbb{P}y$ has height $\leq e^\beta$. Then by Theorem 2.73 there exists a representative $x = (x_0, \ldots, x_{2^g-1}) \in \mathcal{O}_K^{2^g}$ of $\mathbb{P}y$ such that $||x||^2 \leq B_L$. Moreover, by Proposition 3.9 this x is contained in the lattice M since x has coordinates in $\mathcal{O}_K$. Consequently, x is also contained in L which we will denote by x_L. For the construction of x_L see Remark 2.52. We have $||x_L||_\infty > C$, since $||z||_\infty > C$. However, by (3.4) we have $||x_L||_\infty \leq C$. Hence, no point in $\mathbb{P}^{2^g-1}(K)$ of height $\leq e^\beta$ reduces to $\tilde{R}_n$.

(ii) Now suppose that $||w||_\infty \leq 2^{(2^g d-1)/2}\sqrt{2^g d}C$. The idea is to apply Lemma 3.15. Let $u, u' \in M$. Then using Lemma 3.8 we have:

$$\begin{pmatrix} u \\ u' \end{pmatrix} = \begin{pmatrix} u_1 & u_2 & \cdots & u_{2^g} \\ u'_1 & u'_2 & \cdots & u'_{2^g} \end{pmatrix} \implies \begin{pmatrix} u_i & u_{i+1} \\ u'_i & u'_{i+1} \end{pmatrix} = \begin{pmatrix} av_i + \alpha_1 & av_{i+1} + \alpha_2 \\ bv_i + \beta_1 & bv_{i+1} + \beta_2 \end{pmatrix}$$

for some $a, b \in \mathcal{O}_K$ and $\alpha_1, \alpha_2, \beta_1, \beta_2 \in \mathfrak{p}^N$.
This implies that

$$u_i u'_{i+1} - u'_i u_{i+1} \bmod \mathfrak{p}^N \equiv av_i bv_{i+1} - bv_i av_{i+1} = 0 \implies u_i u'_{i+1} - u'_i u_{i+1} \in \mathfrak{p}^N$$

Consequently, all pairs of nonzero vectors in M satisfy the second part of condition (b) of Lemma 3.15 with $D = \mathfrak{p}^N$. Moreover, $N(D) = N(\mathfrak{p}^N) = N(\mathfrak{p})^N = (p^{f(\mathfrak{p})})^N = p^N$. Let $w' \in L$ and denote its corresponding vector in M by u'. Then by Lemma 3.12 we have:

$$\sqrt{2^g d}||w'||_\infty \geq ||w'||_2 = \sqrt{\sum_{i=1}^{2^g d}(w'_i)^2} = \sqrt{\sum_{j=1}^{2^g} Q_{\Delta_Z}(a_j)} \geq \sqrt{\sum_{j=1}^{2^g} Q_{\mathbb{R}}(a_j)/c_1},$$

where

$$\begin{aligned} a_1 &= \begin{pmatrix} w_1 & \cdots & w_d \end{pmatrix}^T \begin{pmatrix} \omega_1 & \cdots & \omega_d \end{pmatrix}, \\ a_2 &= \begin{pmatrix} w_{d+1} & \cdots & w_{2d+1} \end{pmatrix}^T \begin{pmatrix} \omega_1 & \cdots & \omega_d \end{pmatrix}, \\ &\vdots \qquad\qquad \vdots \qquad\qquad \vdots \\ a_{2^g} &= \begin{pmatrix} w_{(2^g-1)d} & \cdots & w_{2^g d} \end{pmatrix}^T \begin{pmatrix} \omega_1 & \cdots & \omega_d \end{pmatrix}. \end{aligned}$$

Hence, noting that $Q_{\mathbb{R}} = T_2$, we have

$$||w'||_\infty \leq 2^{(2^g d-1)/2}\sqrt{2^g dC} \implies T_2(a_j) \leq 2^g d(2^{(2^g d-1)/2}\sqrt{2^g dC})^2 c_1$$

for all $j \in \{1, \ldots, 2^g\}$, where we used that c_1 is real and positive by Remark 3.13. Consequently,

$$||w'||_\infty \leq 2^{(2^g d-1)/2}\sqrt{2^g dC} \implies ||u'||_\infty \leq \sqrt{2^g dc_1}(2^{(2^g d-1)/2}\sqrt{2^g dC}).$$

Since $p^N > \left(2^g d(2^{(2^g d-1)/2}\sqrt{2^g dC})^2 c_1\right)^d (4/d)^{d/2}$, we can apply Lemma 3.15 with $B = \sqrt{2^g dc_1}(2^{(2^g d-1)/2}\sqrt{2^g dC})$. In particular, this implies that for any vector $w' \in L$ satisfying $||w'||_\infty \leq 2^{(2^g d-1)/2}\sqrt{2^g dC}$, its corresponding vector in M defines the same point in projective space as the vector in M corresponding to w does. In other words, we have $\mathbb{P}w' = \mathbb{P}w = R$. Now if there is a point in $\mathbb{P}^{2^g-1}(K)$ that reduces to $\tilde{R}_n$, a representative of this point must be contained in M by Proposition 3.9 and therefore in L. Furthermore, if this point has height $\leq e^\beta$, (3.4) implies that the supremum norm of this point considered on L is bounded by $C \leq 2^{(2^g d-1)/2}\sqrt{2^g dC}$. Hence, if there is a point in $\mathbb{P}^{2^g-1}(K)$ that reduces to $\tilde{R}_n$ and has height $\leq e^\beta$ then it must be R.

□

Now we have all the ingredients to prove the correctness of Algorithm 3.1.

Proof. (Theorem 3.2) We already noted that the algorithm terminates. Let $\tilde{Q}$ be as in the algorithm. Then two things can happen:

(i) There exists a point $Q \in A(K)[m]$ such that Q reduces to $\tilde{Q}$. Since Q is a torsion point we have $H_K(Q) = H_K(\kappa(Q)) \leq e^\beta$. By Lemma 3.6, $\tilde{R}_n$ is the unique m-torsion point in $\mathcal{K}(\mathcal{O}_K/\mathfrak{p}^N)$ that reduces to $\tilde{\kappa}(\tilde{Q})$. Moreover, by Proposition 3.16, R is the unique K-rational point of height $\leq e^\beta$ that reduces to $\tilde{R}_n$. Consequently, we must have that $R = \kappa(Q)$. Clearly steps $\boxed{6}$ and $\boxed{7}$ in the algorithm do not return FALSE and since $\kappa^{-1}(R) = \{Q, -Q\} \subset A(K)$ step $\boxed{8}$ will return TRUE.

(ii) No point Q as in (i) exists. Then suppose for a contradiction that the algorithm returns TRUE. The same logic using Lemma 3.6 and Proposition 3.16 as in case (i) implies that R is the unique m-torsion point in $\mathcal{K}(K)$ that reduces to $\tilde{\kappa}(\tilde{Q})$. Therefore, $\kappa^{-1}(R)$ contains a point in $A(K)[m]$ that reduces to $\tilde{Q}$. ↯

□

3.3 Complete algorithm

In the previous subsection we presented an algorithm that determines whether reduced points lift to K-rational torsion points. We can use this to construct an algorithm that actually computes the torsion subgroup. We will use the approach as presented in [Sto98, §11].

Let G be an abelian group of finite order. Then $|G| = p_1^{n_1} p_2^{n_2} \cdots p_r^{n_r}$ for some primes $p_1, \ldots, p_r$ and $n_1, \ldots, n_r \in \mathbb{Z}_{\geq 1}$. Consequently, there exist Sylow p_i subgroups with $p_i^{n_i}$ elements which we will denote by H_{p_i} for $i \in \{1, \ldots, r\}$. There is at most one Sylow p-group for every prime p since Sylow p-groups are conjugate and G is abelian. Hence, the map

$$\begin{aligned} \prod_p H_p &\to G \\ (h_1, h_2, \ldots, h_r) &\mapsto h_1 h_2 \cdots h_r \end{aligned}$$

is an isomorphism. This allows us to write the torsion subgroup as a product of its Sylow p-groups since it is finite by Theorem 2.18. We call H_q the *q-part* of G. By Theorem 2.38 the reduction map $\rho_{\mathfrak{p}} : A(K_{\mathfrak{p}}) \to A(\mathcal{O}_K/\mathfrak{p})$ is injective on the q-parts of $A(K)_{\text{tors}}$ for $\mathfrak{p} \mid p$ such that $\gcd(q, p) = 1$. Hence, denoting the q-parts of $A(\mathcal{O}_k/\mathfrak{p})$ by H_q, the q-part of $A(K)_{\text{tors}}$ is equal to $H_q \cap A(K)$. Using this, the following algorithm from [Sto98, §11] computes the q-part of $A(K)_{\text{tors}}$.

Algorithm 3.2: [Sto98, §11]
Input: An abelian variety A/K for which Assumption 3.1 is satisfied and an odd prime q.
Output: The q-part of $A(K)_{\text{tors}}$.

1. Let G_0 be the q-part of $\tilde{A}(\mathcal{O}_K/\mathfrak{p})$ for $\mathfrak{p} \mid p$ such that A has good reduction at $\mathfrak{p}$ and $p \neq q$. Set $T_0 = \{0\} \subset G$ and $S_0 = G_0 \backslash \{0\}, S_0' = \{0\}$.
2. Set $n = 0$ and repeat the following steps until $S_n = \emptyset$.
   (a) Let $g \in S_n$ and choose a representative $\tilde{g} \in G_0$ of g.
   (b) Using Algorithm 3.1, find the smallest $m \geq 0$ such that $q^m \cdot \tilde{g} \in A(K)_{\text{tors}}$.
   (c) Set
   $$\begin{aligned} T_{n+1} &= \langle T_n, q^m \cdot \tilde{g} \rangle \\ G_{n+1} &= G_n / \langle q^m \cdot g \rangle, \\ S_{n+1}' &= \text{image of } S_n' \cup \langle g \rangle \text{ in } G_{n+1}, \\ S_{n+1} &= G_{n+1} \backslash S_{n+1}'. \end{aligned}$$
   (d) Replace n with $n + 1$.
3. Return T_n.

Remark 3.17. Using Algorithm 3.2 we can determine all m-torsion for $m \neq 2$. However, if $\tilde{Q} \in A(\mathcal{O}_K/\mathfrak{p})$ has order equal to 2, we cannot use Algorithm 3.1 to decide if $\tilde{Q}$ lifts since $\kappa(\tilde{Q})$ is a singular point which means that we cannot use Hensel's lemma. In order to determine $A(K)[2]$ we can solve for $R \in \mathcal{K}(K)$ in the system of equations $[[2]]R = \kappa(0)$ (see also [MR23, §3.2.1]). In case A is the Jacobian of a genus 2 curve we can use [Sto01, Lemma 4.3, Lemma 5.3].

Finally, we now have all the ingredients for the complete algorithm.

Algorithm 3.3:
Input: An abelian variety A/K for which Assumption 3.1 is satisfied.
Output: Elementary divisors of $A(K)_{\text{tors}}$.

1. Compute a height difference bound β.
2. For some primes $\mathfrak{p}$ where A has good reduction, compute $\#A(\mathcal{O}_K/\mathfrak{p})$ and compute the gcd of these group orders.
3. For prime divisors q of this gcd determine the q-part of $A(K)_{\text{tors}}$ using Algorithm 3.2 and Remark 3.17.
4. Finally, combining the q-parts and Remark 3.17 deduce the elementary divisors of $A(K)_{\text{tors}}$. In some cases (see Remark 3.3) we can compute the actual points in $A(K)_{\text{tors}}$.

From (2.3) it follows that $A(K)_{\text{tors}}$ has only q-parts dividing the gcd in 2 of Algorithm 3.3. Hence, Algorithm 3.3 terminates and is correct.

Remark 3.18. For 2 of Algorithm 3.3 we need (5) of Assumption 3.1.

4 Jacobians of curves of genus 2

In this section we will show that Assumption 3.1 is satisfied when A is the Jacobian of a genus 2 curve over a number field. Furthermore, we will make precise how the height difference bound is derived in that case. To that end, let J denote the Jacobian of a curve C/K of genus 2 with corresponding Kummer variety $\mathcal{K}$.

Firstly, the map κ and equations for its image are given by [CF96, §3], in which case $\mathcal{K}$ is a quartic hypersurface in $\mathbb{P}^3$. These quartic surfaces were first studied over $\mathbb{C}$ and $\mathbb{R}$ by [Kum64] in 1864, and have 16 singular points, namely $\kappa(A[2])$. Kummer surfaces were only later studied over arbitrary fields. Assumption parts (2) and (5) are also satisfied. For the former see [Sto02, §5] and for the latter see the discussion in [MR23, §3.4].

4.1 Duplication map and pseudo-addition

Explicit formulae for $[[2]]$ are known; see for example [Fly93]. In particular, we can define the *duplication map* δ such that

$$\kappa([2]P) = \delta(\kappa(P)) = (\delta_1(\kappa(P)), \delta_2(\kappa(P)), \delta_3(\kappa(P)), \delta_4(\kappa(P))),$$

where δ_i are homogeneous polynomials of degree 4.
Let $\kappa = (\kappa_1 : \kappa_2 : \kappa_3 : \kappa_4)$ and let $P, Q \in J$. Then there exist biquadratic polynomials B_{ij}

given in [CF96, Chapter 3.4] such that

$$B_{ij}(\kappa(P),\kappa(Q)) = \kappa_i(P+Q)\kappa_j(P-Q) + \kappa_i(P-Q)\kappa_j(P+Q) \text{ for } 1 \le i,j \le 4.$$

Assume that we have coordinates for either $\kappa(P+Q)$ or $\kappa(P-Q)$. We will assume that $\kappa(P+Q) = (m_1 : m_2 : m_3 : m_4)$ is known. Then, following [FS97, §4], we can compute coordinates (n_1, n_2, n_3, n_4) for $\kappa(P+Q)$ by setting

$$\begin{aligned} n_i &= 2m_j B_{ij}(\kappa(P),\kappa(Q)) - m_i B_{jj}(\kappa(P),\kappa(Q)) \\ &= 2m_j\Big(\kappa_i(P+Q)\kappa_j(P-Q) + \kappa_i(P-Q)\kappa_j(P+Q)\Big) - 2m_i\kappa_j(P+Q)\kappa_j(P-Q) \\ &= 2m_j\Big(m_i\kappa_j(P-Q) + \kappa_i(P-Q)m_j\Big) - 2m_i\kappa_j(P-Q)m_j \\ &= 2m_j^2\kappa_i(P-Q), \end{aligned}$$

where we fixed j such that $m_j \neq 0$.
The last equality contains $2m_j^2$ for every n_i so in projective space the coordinates n_i indeed will be in the equivalence class $(\kappa_1(P-Q) : \kappa_2(P-Q) : \kappa_3(P-Q) : \kappa_4(P-Q))$. Hence, we are able to perform pseudo addition, that is, given $\kappa(P), \kappa(Q)$ and $\kappa(P+Q)$, we can compute $\kappa(P-Q)$. This works exactly the same if $\kappa(P-Q)$ is known instead of $\kappa(P+Q)$.

4.2 Height bound for genus 2

In this subsection we will follow [Sto98] and outline an approach to derive a height difference bound as described in (4) of Theorem 2.60. Let C/K_v be a curve of genus 2 and let J denote its Jacobian with corresponding Kummer variety $\mathcal{K}$. Moreover, assume that C is given by $y^2 = F(x,z)$ with $F \in \mathcal{O}_v[x,z]$.

Recall the duplication map δ and its corresponding polynomials δ_i defined in Subsection 4.1. In particular, $\delta_1, \delta_2, \delta_3, \delta_4 \in \mathcal{O}_v[x_1, x_2, x_3, x_4]$ are homogeneous polynomials of degree 4 in the homogeneous coordinates x_1, x_2, x_3, x_4 [Sto98, §2]. Then the *local height constant* of C over K_v is defined as in [Sto98, §2] by

$$c_v := \min_{x=(x_1:x_2:x_3:x_4)\in\mathcal{K}(K_v)} \frac{\max\{||\delta_1(x)||_v, ||\delta_2(x)||_v, ||\delta_3(x)||_v, ||\delta_4(x)||_v\}}{(\max\{||x_1||_v, ||x_2||_v, ||x_3||_v, ||x_4||_v\})^4}. \tag{4.1}$$

The first result concerning the height difference bound is the following:

Theorem 4.1. *[FS97, Theorem 4] For all points $P \in J(K)$, we have*

$$h_K(P) \le \hat{h}(P) + \frac{1}{3}\sum_v \log c_v^{-1}$$

Let us first consider the local height constants for the finite places of K.

Lemma 4.2. *Let v be a finite place of K and c_v as defined in* (4.1)*. Then*

$$c_v \geq |(2\lambda)^4 \operatorname{disc}(F_{red})|_v,$$

where λ is the content of F and F_{red} is the primitive part of F, i.e., $F = \lambda F_{red}$.

Proof. See [Sto98, Proposition 7.1]. □

This leads us to the following theorem:

Theorem 4.3. *[Sto98, Corollary 8.1] For all points $P \in J(K)$, we have*

$$h_K(P) \leq \hat{h}(P) + \frac{4}{3}[K:\mathbb{Q}]\log 2 - 2\log N(\mathfrak{a}) + \frac{1}{3}\log|N(\operatorname{disc}(F))| + \frac{1}{3}\sum_{v|\infty}\log c_v^{-1},$$

where $\mathfrak{a}$ is the content ideal of F.

Proof. For $\beta \in \mathcal{O}_K$ we have

$$|\beta|_{\mathfrak{p}} = N(\mathfrak{p})^{-v_{\mathfrak{p}}(\beta)} \implies \prod_{v \text{ finite}} |\beta|_v = \prod_{\mathfrak{p}} N(\mathfrak{p})^{-v_{\mathfrak{p}}(\beta)} = 1/N(\beta\mathcal{O}_K) = 1/|N(\beta)|.$$

By the properties of the discriminant (see e.g., [Ste12, §4]), $\operatorname{disc}(F) = \lambda^{10}\operatorname{disc}(F_{\mathrm{red}})$. Hence, the result now follows from Lemma 4.2 and Theorem 4.1. □

All quantities on the right-hand side of Theorem 4.3 can be easily computed with the exception of the local height constants. In fact, we only need the local height constants for the infinite places of K. One way to bound these constants is as follows. Firstly, we want to find an upper bound on the numerator in the definition of c_v in (4.1). Specifically, if we can find a constant $\mu > 0$ such that

$$\max_i\{||x_i||_v\} \leq \mu \max_i\{\delta_i(x)||_v,$$

then $c_v \leq \mu$. So instead of expressing $\delta_i(x)$ in terms of the x_i's, we want to express the x_i's in terms of the δ_j's. To that end, let $f(x) := F(x,1)$ and note that we have $\deg(f) \in \{5,6\}$. For the infinite places we have that K_v is either equal to $\mathbb{R}$ or to $\mathbb{C}$ and we can write

$$f(x) = c\prod_{i=1}^{\deg(f)}(x-\alpha_i), \tag{4.2}$$

for some $c \in \mathbb{C}$ and $\alpha_i \in \mathbb{C}$ for $i \in \{1,\ldots,\deg(f)\}$.

Lemma 4.4. *Let $Q \in \mathcal{K}$ and choose $P \in \kappa^{-1}(Q) = \{Q,-Q\}$. Then the map*

$$\begin{aligned} J[2]\times\mathcal{K} &\to \mathcal{K} \\ (T,Q) &\mapsto \kappa(T+P) \end{aligned}$$

defines an action of $J[2]$ on $\mathcal{K}$.

Proof. We have $\kappa(T+P) = \kappa(-(T+P)) = \kappa(-T-P) = \kappa(T-P)$ so the map is well-defined. The group action axioms are easily verified. □

Let $Q = (x_1 : x_2 : x_3 : x_4) \in \mathcal{K}$ and $\bar{K}_v$ be an algebraic closure of K_v. Then using Lemma 4.4 we get an action of $J[2]$ on homogeneous polynomials in $\bar{K}_v[x_1, x_2, x_3, x_4]$. Define G to be the group consisting of pairs (ϵ, T) with $\epsilon = \pm 1$ and $T \in J[2]$ and multiplication given by

$$(\epsilon, T)(\epsilon', T') = (\epsilon\epsilon' e(T, T'), T + T'),$$

where $e(T, T')$ denotes the *Weil pairing* of T and T' as described in [Sto98, §3].
Similarly to $J[2]$, we can define an action of G on polynomials in $\bar{K}_v[x_1, x_2, x_3, x_4]$ (see [Sto98, §3,4]). For $y \in \bar{K}_v[x_1, x_2, x_3, x_4]$ denote the action of $g \in G$ on y by $g \cdot y$. Let $\mathrm{Sym}^2 V_{K_v}$ denote the space of homogeneous polynomials in $K_v[x_1, x_2, x_3, x_4]$ of degree 2. Then it follows from basic representation theory of finite groups (see e.g., [FH91, Chapters 1,2]) that

$$\mathrm{Sym}^2 V_k = \bigoplus_{\{S,S'\}} K_v \cdot y_{\{S,S'\}}$$

for $y_{\{S,S'\}} \in K_v[x_1, x_2, x_3, x_4]$ homogeneous polynomials of degree 2 such that

$$(\epsilon, T) \cdot y_{\{S,S'\}} = \chi_{\{S,S'\}}(\epsilon, T) y_{\{S,S'\}},$$

where $\chi_{\{S,S'\}}$ is a character on G as defined in [Sto98, §4].

Theorem 4.5. *For a partition $\{S, S'\}$ of the roots of f there exist coordinates $a_{i,\{S,S'\}}$, $b_{\{S,S'\},j}$ such that*

$$x_i^2 = \sum_{\{S,S'\}} a_{i,\{S,S'\}} y_{\{S,S'\}}(P) \text{ for } i \in \{1, \ldots, 4\},$$

and

$$y_{\{S,S'\}}^2(P) = \sum_{j=0}^{4} b_{\{S,S'\},j} \delta_j(P),$$

where $P = (x_1 : x_2 : x_3 : x_4)$ is a point on $\mathcal{K}$ and $y_{\{S,S'\}} \in K_v[x_1, x_2, x_3, x_4]$ are homogeneous polynomials of degree 2 described in [Sto98, §4].

Proof. Explicit formulas for $a_{i,\{S,S'\}}$ and $b_{j,\{S,S'\}}$ in terms of the roots of f are given in [Sto98, Formula 10.2, 10.3]. □

Hence, the x_i's are defined in terms of the δ_i's using the polynomials $y_{\{S,S\}}$. Recall that for an infinite place v the absolute value $||\cdot||_v$ reduces to the usual absolute value on $\mathbb{C}$ which we denote by $|\cdot|$. The local height constants c_v for the infinite places of K can now be estimated using the following lemma.

Lemma 4.6. *For $a_{i,\{S,S'\}}$ and $b_{\{S,S'\},j}$ as in Theorem 4.5 we have*

$$\frac{1}{c_v} \leq \max_i \Big(\sum_{\{S,S'\}} |a_{i,\{S,S'\}}| \sqrt{\sum_{j=1}^{4} |b_{\{S,S'\},j}|} \Big)^2.$$

Proof. Using Theorem 4.5 and the triangle inequality we deduce that

$$|x_i|^2 \leq \sum_{\{S,S'\}} |a_{i,\{S,S'\}}| \cdot |y_{\{S,S'\}}| \quad \text{and} \quad |y_{\{S,S'\}}|^2 \leq \sum_{j=0}^{4} |b_{\{S,S'\},j}| \cdot |\delta_j|.$$

Hence,

$$\max_i |x_i|^4 \leq \max_i \Big(\sum_{\{S,S'\}} |a_{i,\{S,S'\}}| \sqrt{\sum_{j=0}^{4} |b_{\{S,S'\},j}|} \Big)^2 \max_j |\delta_j|.$$

The result now follows from the definition of c_v in (4.1). □

Remark 4.7. We can refine this bound as follows. Assume $K_v = \mathbb{R}$ and define the function

$$\begin{aligned} \varphi : \mathbb{R}^4_{\geq 0} &\to \mathbb{R}^4_{\geq 0} \\ (d_1, d_2, d_3, d_4) &\mapsto \Big(\sqrt{\sum_{\{S,S'\}} |a_{i,i,\{S,S'\}}| \sqrt{\sum_{j=1}^{k+1} |b_{\{S,S'\},j}| d_j}} \Big)_{1 \leq i \leq 4}. \end{aligned}$$

It is proven in [MS16, Lemma 16.1] that the sequence

$$c_n := \frac{4^n}{4^n - 1} \log(||\varphi^{\circ n}(1,1,1,1)||_\infty)$$

converges to a limit $\tilde{c}$ such that $c_v \leq \tilde{c}$.

Additionally, if we are dealing with a real place we can do better using that the δ_j are real, while some $b_{\{S,S'\},i}$ may be complex (see [MS16, §16B]). In order to deduce the inequality in Lemma 4.6 we needed to divide by $\max_j |\delta_j|$ so it makes sense to try to find an expression that bounds $y_{\{S,S'\}}$ even further while still explicitly including $\max_j |\delta_j|$. In particular, let us show the following:

Lemma 4.8. *Let $b_i \in \mathbb{C}$ and $\delta_i \in \mathbb{R}$ for $1 \leq i \leq 4$. Then we have*

$$\begin{aligned} |b_1\delta_1 + b_2\delta_2 + b_3\delta_3 + b_4\delta_4| \leq \max_i |\delta_i| \max\{ &|b_1 + b_2 + b_3 + b_4|, |b_1 - b_2 + b_3 + b_4|, \\ &|b_1 + b_2 - b_3 + b_4|, |b_1 + b_2 + b_3 - b_4|, \\ &|b_1 - b_2 - b_3 + b_4|, |b_1 - b_2 + b_3 - b_4| \\ &|b_1 + b_2 - b_3 - b_4|, |b_1 - b_2 - b_3 - b_4|\}, \end{aligned}$$

Proof. For simplicity, we will only prove the lemma in the form

$$|b_1\delta_1 + b_2\delta_2| \leq \max_j |\delta_i| \max\{|b_1 + b_2|, |b_1 - b_2|\}.$$

The general case is analogous. Writing $b_1 = a + bi$ and $b_2 = c + di$ for $a, b, c, d \in \mathbb{R}$, we have:

$$\begin{aligned} |b_1\delta_1 + b_2\delta_2|^2 &= |(a+bi)\delta_1 + (c+di)\delta_2|^2 \\ &= (a\delta_1 + c\delta_2)^2 + (b\delta_1 + d\delta_2)^2 \\ &= \delta_1^2(a^2+b^2) + \delta_2^2(c^2+d^2) + \delta_1\delta_2(2ac+2bd). \end{aligned}$$

Now note that

$$\begin{aligned} |b_1 + b_2| > |b_1 - b_2| &\implies (a+c)^2 + (b+d)^2 > (a-c)^2 + (b-d)^2 \\ &\implies 2ac + 2bd > -2ac - 2bd \\ &\implies 2ac + 2bd > 0. \end{aligned}$$

Hence if $|b_1 + b_2| > |b_1 - b_2|$, we have

$$\begin{aligned} |b_1\delta_1 + b_2\delta_2|^2 &\leq \max_{j\in\{1,2\}} \delta_j^2(a^2+b^2+c^2+d^2+2ac+2bd) \\ &= \max_{j\in\{1,2\}} \delta_j^2 |b_1 + b_2|^2. \end{aligned}$$

On the other hand, if $|b_1 + b_2| < |b_1 - b_2|$ we have that $2ac + 2bd < 0$. Therefore

$$\begin{aligned} |b_1\delta_1 + b_2\delta_2|^2 &= \delta_1^2(a^2+b^2) + \delta_2^2(c^2+d^2) + \delta_1\delta_2(2ac+2bd) \\ &\leq \max_{j\in\{1,2\}} \delta_j^2(a^2+b^2+c^2+d^2-(2ac+2bd)) \\ &= \max_{j\in\{1,2\}} \delta_j^2 |b_1 - b_2|^2. \end{aligned}$$

□

Example 4.9. To illustrate the use of this lemma, assume for sake of simplicity that $b_1 = 1, b_2 = i, \delta_1 = 1, \delta_2 = 2$. Then using only the triangle inequality we get:

$$|b_1\delta_1 + b_2\delta_2| \leq \max_j |\delta_j|(|b_1| + |b_2|) = 2 \cdot (1+1) = 4.$$

However, using the lemma we get

$$|b_1\delta_1 + b_2\delta_2| \leq \max_j |\delta_j| \max\{|b_1 + b_2|, |b_1 - b_2|\} = 2 \cdot \sqrt{2}.$$

Hence this leads to a lower bound which in turn sharpens the bound on the height constant. On the other hand, if we are dealing with a complex place the lemma does not help. For example let $b_1 = i, b_2 = 1, \delta_1 = 1, \delta_2 = i$. Then we get the following:

$$|b_1\delta_1 + b_2\delta_2| = |i + i| = 2.$$

However,

$$\max_j |\delta_j| \cdot |b_1 + b_2| = \max_j |\delta_j| \cdot |b_1 - b_2| = \sqrt{2} < 2.$$

Although Theorem 4.3 provides a straightforward way to bound the local height constants at the finite places of K, we can alternatively use the following approach.

Lemma 4.10. *Let v be a finite place corresponding to a prime ideal $\mathfrak{p}$ lying above the prime p. Then*

(1) If J has good reduction at $\mathfrak{p}$, then $c_v = 1$,

(2) If $v_\mathfrak{p}(\mathrm{disc}(F)) = 1$ and $p \neq 2$, then $c_v = 1$.

Proof. For (1) see [FS97, Lemma 1] and for (2) see [Sto02, Proposition 5.2]. □

If we use Lemma 4.10 for the finite places of K we only have to consider the contribution of the places at which J has bad reduction and for which the valuation of $\mathrm{disc}(F)$ is not equal to 1. Using this, we can improve the bound in Theorem 4.3 as follows.

Lemma 4.11. *For all points $P \in J(K)$, we have*

$$h_K(P) \leq \hat{h}(P) + \sum_{\substack{v \text{ finite} \\ v_\mathfrak{p}(\mathrm{disc}(F))>1 \text{ or } p=2}} -\log(||\operatorname{disc}(F)||_v)/4 + \frac{1}{3}\sum_{v|\infty} \log c_v^{-1},$$

where $\mathfrak{p} \mid p$ is the prime ideal corresponding to v.

Proof. See [MS16, Theorem 11.3]. □

Remark 4.12. Let v be a finite place and assume v corresponds to the prime ideal $\mathfrak{p}$. Then we can rewrite the right-hand side of the equation in Lemma 4.11 as follows:

$$-\log(||\operatorname{disc}(F)||_v)/4 = -\log(N(\mathfrak{p})^{-v_\mathfrak{p}(\mathrm{disc}(F))})/4 = v_\mathfrak{p}(\mathrm{disc}(F))\log(N(\mathfrak{p}))/4.$$

Using Lemma 4.11 in practice requires factoring $\mathrm{disc}(F)$ which can be time-consuming. However, a sharper height bound leads to a smaller necessary p-adic precision in the algorithm. In practice, we use Lemma 4.11 to bound the local height constants for the finite places of K.

4.3 Example

In order to illustrate how the algorithm works in practice we consider the following example. We will refer to the functions defined in `https://github.com/MaxPosthumus/MasterProject/blob/main/TorsionNum.m`.

Example 4.13. Define $K := \mathbb{Q}[t]/(f)$ with $f = t^2 - 2$ and let C/K be the hyperelliptic curve defined by

$$y^2 = x^6 + 4x^4 + 2x^3 + 4x^2 + 1.$$

This is isomorphic to the curve with label $294.a.294.1$ in the `LMFDB` database (`https://www.lmfdb.org/Genus2Curve/Q/249/a/249/1`). Let J be the Jacobian of C with corresponding Kummer surface $\mathcal{K}$. We will follow Algorithm 3.3 to determine $J(K)_{\text{tors}}$. To set up this example in `Magma` we can use the following:

```
R<t> := PolynomialRing(Rationals());
K := NumberField(t^2-2);
R<x> := PolynomialRing(K);
f := x^6+4*x^4+2*x^3+4*x^2+1;
C := HyperellipticCurve(f);
J := Jacobian(C);
Kummer := KummerSurface(J);
```

(1) We first want to compute a height difference bound. To that end, we have two options:

(i) Using Theorem 4.3,

(ii) Using Lemma 4.11.

For now, disregard the local height constants at infinity. Then for (i) we compute

$$[K : \mathbb{Q}] = 2,\ \operatorname{disc}(F) = -308281344,\ \mathfrak{a} = \langle 1 \rangle,$$

where $\mathfrak{a}$ is the content of F.
This leads to a bound of the local height constants at the finite places of K of 14.88. For (ii) we find 3 finite places at which J has bad reduction and for which the valuation of $\operatorname{disc}(F)$ is not equal to 1. Using Lemma 4.11 this leads to a bound of the local height constants at the finite places of K of 9.22. As explained in Subsection 4.2 we use the bound from (ii) in practice. For the local height constants at infinity note that K has two real field embeddings given by

$$\sigma_1 : K \to \mathbb{R},\ \sqrt{2} \mapsto \sqrt{2} \quad \text{and} \quad \sigma_2 : K \to \mathbb{R},\ \sqrt{2} \mapsto -\sqrt{2}.$$

In `Magma` these are given by

```
Sigma := hom< K -> ComplexField() | Conjugates(K.1)[i]>;
```

for $i \in \{1, 2\}$. Consequently, $K_v = \mathbb{R}$ for both infinite places of K. Define $f := x^6 + 4x^4 + 2x^3 + 4x^2 + 1$ and write

$$f = c \prod_{i=1}^{6} (x - \alpha_i)$$

for some $c \in \mathbb{C}$ and $\alpha_i \in \mathbb{C}$ for $i \in \{1, \ldots, 6\}$.
Then using [Sto98, Formula 10.2, 10.3] we can express the coordinates $a_{i,\{S,S'\}}$ and $b_{\{S,S'\}.j}$ in Theorem 4.5 in terms of c and the α_i's. Subsequently, Lemma 4.6 provides a bound on c_v for v one of the infinite places. In addition, we can use Remark 4.7 and Lemma 4.8 to improve the bound since both places are real. Using `HCinfinityNum()` we compute that $\log c_v^{-1} \leq 0.94$ at both infinite places and moreover

```
HeightBound(J);
```

leads us to a height difference bound $\beta \approx 9.85$.

(2) Secondly, we want to bound $\#J(K)_{\text{tors}}$ by reducing J modulo several good primes $\mathfrak{p}$. Note that $\mathcal{O}_K = \mathbb{Z}[\sqrt{2}]$, which we can also find by

```
OK := Integers(K);
```

Let S' be a set of prime numbers, usually ranging from 3 to 200. For each $p \in S'$ we find a prime ideal $\mathfrak{p} \subset \mathcal{O}_K$ lying above p. Denote the set of all of these prime ideals satisfying $e(\mathfrak{p}) < p - 1$ for p the unique prime lying below $\mathfrak{p}$, by S. By Lemma 2.39 the reduction map $\rho_{\mathfrak{p}}$ is injective for all primes $\mathfrak{p} \in S$ at which J has good reduction. Moreover, if C has good reduction at $\mathfrak{p}$ then the same applies to J. Hence, we must find the prime ideals in S at which C has good reduction. Define F as the degree 6 homogenization of f and write $f = c^6x^6 + c^5x^5 + \cdots + c_1x + c_0$. Instead of directly using Definition 2.36, we will check whether $|\text{disc}(F)|_{\mathfrak{p}} = 1$ and $v_{\mathfrak{p}}(c_i) \geq 0$ for $1 \leq 0 \leq 6$. This allows us to remove all ideals at which C has bad reduction from S. We can sort the elements of S by their norms and select the first n elements of minimal norm. In practice we use $n = 20$. In `Magma` we find S using

```
disc := Discriminant(C);
cofs := {c : c in Eltseq(f)};
S := &cat[[e[1] : e in Decomposition(OK, p) |
    e[2] lt p-1] : p in PrimesInInterval(3, 200)];
S := [p : p in S | Valuation(disc, p) eq 0 and
    forall{c : c in cofs | Valuation(c, p) ge 0}];
Sort(~S, func<p1, p2 | Norm(p1)-Norm(p2)>);
```

In this case the prime $\mathfrak{p} := \langle 17, 11 + \sqrt{2} \rangle$ lying above 17 is the ideal of minimal norm in S. Using the isomorphism in Theorem 2.32 we can reduce $J(K)$ modulo $\mathfrak{p}$ to obtain $\tilde{J}(\mathcal{O}_K/\mathfrak{p})$. In particular,

```
p := S[1];
F, red := ResidueClassField(p);
JF := BaseChange(J, map<K -> F | a :-> red(a)>);
Invariants(JF);
```

informs us that $J(\mathcal{O}_K/\mathfrak{p}) \cong \mathbb{Z}/6\mathbb{Z}\times\mathbb{Z}/48\mathbb{Z}$ and $\#J(\mathcal{O}_K/\mathfrak{p}) = 288$. By computing this for 7 primes of minimal norm in S we obtain the following non-isomorphic potential group structures:

$$\begin{aligned}\mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/48\mathbb{Z},\\ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/12\mathbb{Z} \times \mathbb{Z}/24\mathbb{Z},\\ \mathbb{Z}/12\mathbb{Z} \times \mathbb{Z}/96\mathbb{Z},\\ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/576\mathbb{Z}.\end{aligned}$$

Only taking the orders into account we can deduce that $\#J(K)_{\text{tors}} \leq 288$. However, using the group structures as well we conclude that $\#J(K)_{\text{tors}}$ is equal to a subgroup of $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/24\mathbb{Z}$ so $\#J(K)_{\text{tors}} \leq 48$.

(3) Thirdly, we consider prime divisors q of $48 = 2^4 \cdot 3$ to determine the q-part of $J(K)_{\text{tors}}$. We can use Algorithm 3.2 to compute the q-part of $J(K)_{\text{tors}}$ for $q \in \{2, 3\}$. Let $q = 3$ and select from S a prime ideal $\mathfrak{p}$ lying above some prime p that satisfies $e(\mathfrak{p}) = f(\mathfrak{p}) = 1$ and $p \neq q$. Since K is a quadratic number field, the condition $e(\mathfrak{p}) = f(\mathfrak{p}) = 1$ is equivalent to finding split primes. In this case, simply selecting $\mathfrak{p} = \langle 17, 11 + \sqrt{2}\rangle$ as defined above suffices. For (b) in Algorithm 3.2 it is crucial that we can determine whether a point of $\tilde{J}(\mathcal{O}_K/\mathfrak{p})$ lifts to $J(K)_{\text{tors}}$. From Subsection 2.3 we know that all points of $\tilde{J}(\mathcal{O}_K/\mathfrak{p})$ lift to $J(K_\mathfrak{p})$. However, in order to determine whether a point $\tilde{Q} \in \tilde{J}(\mathcal{O}_K/\mathfrak{p})$ lifts to $J(K)_{\text{tors}}$, we need the bound on the p-adic precision as described in §3.2.2. To that end, we use `Constants()` to compute c_1 and c_2 as in Lemma 3.12 and `BL()` to compute B_L as in (3.3). We get the following numerical values:

$$c_1 = 4,\ c_2 = 0.5 \text{ and } B_L \approx 457115.65$$

Finally, we compute using `BM()` that $\left(2^g d(2^{(2^g d-1)/2}\sqrt{2^g d}\sqrt{B_L \cdot c_2})^2 c_1\right)^n (4/d)^{d/2} \approx \exp(46.17)$. Hence, noting that $p = 17$, the bound on p is given by $\lceil 46.17/\log(17)\rceil = 17$. Now we define the completion $K_\mathfrak{p}$ with precision equal to the bound on the p-adic precision as

```
Kv, map := Completion(K,I);
Kv`DefaultPrecision := 17;
```

where I denotes $\mathfrak{p}$. This means that coordinates of points in $K_\mathfrak{p}$ get truncated as in Remark 2.31. Now we can use Algorithm 3.1 to decide which points in the 3-part of $\tilde{J}(\mathcal{O}_K/\mathfrak{p})$ lift to $J(K)_{\text{tors}}$. This is done by the function `LiftTorsionPoint()`. We find that $T_3 \cong \mathbb{Z}/3\mathbb{Z}$. The 2-part of $J(K)_{\text{tors}}$ can be computed similarly, although we have to be careful with two-torsion points. In particular, using Remark 3.17 and the function `TwoTorsionSubgroup()` (which is already implemented in `MAGMA` and uses [Sto98]) we find that $T_2 \cong \mathbb{Z}/4\mathbb{Z}$.

(4) Hence, $J(K)_{\text{tors}} \cong \mathbb{Z}/12\mathbb{Z}$. In addition, we found the elements of $J(K)_{\text{tors}}$ explicitly when using Algorithm 3.2. Let $P := (1 : -1 : 0)$ and $Q := (1 : 1 : 0)$ be the two points at infinity of C. Then a generator of $J(K)_{\text{tors}}$ is given by the divisor class $[P - Q]$.

Remark 4.14. Let C/K be a hyperelliptic curve and denote its Jacobian by J. Then for any quadratic extension L of K, an alternative approach to determining $J(L)_{\text{tors}}$ exists, by using a quadratic twist C' of C. Denote the Jacobian of C' by J'. Then we can determine $J(L)_{\text{tors}}$ by computing $J(K)_{\text{tors}}$ and $J'(K)_{\text{tors}}$. For Example 4.13 this implies that we can determine $J(K)_{\text{tors}}$ by only considering Jacobians of hyperelliptic curves over $\mathbb{Q}$, since in this case $[K : \mathbb{Q}] = 2$.

5 Applications

Now that we have a working algorithm that can compute the torsion subgroup of Jacobians of genus 2 curves over number fields, it is interesting to deploy this algorithm in practice. We will do this firstly by simply computing the torsion structures for a large number of curves but we will consider some specific applications as well.

5.1 LMFDB, large torsion and unknown torsion structures

In this subsection we will investigate the torsion structures that occur for genus 2 curves over number fields.

5.1.1 LMFDB database

Our starting point is the `LMFDB` database (`https://www.lmfdb.org/Genus2Curve/Q/`) which contains 66158 genus 2 curves defined over $\mathbb{Q}$. We consider the Jacobian of each of these curves over some different number fields in order to get an idea of the distribution of the torsion structures. The fields K_1 and K_2 (see Table 1) are selected as simple examples of a real and imaginary quadratic field respectively. Additionally, as in [Tur13, §3.8], K_3 is chosen because it has a nontrivial class group. Lastly, we consider K_4 as an example of a number field that arises as the extension of another number field different from $\mathbb{Q}$ and since K_1 showed the most promising torsion orders. The results are in Table 1 where the column *Elt. div* contains the elementary divisors, the column *Order* contains the order of the torsion subgroup and the other columns contain the number of occurrences of each group structure for the different number fields.

Elt. div	Order	K_1	K_2	K_3	K_4	$\mathbb{Q}$
1	1	44138	44173	44190	44061	44190
2	2	13826	14380	14681	13866	14681
3	3	2340	2311	2295	2299	2295
2,2	4	1876	1391	1352	1884	1353
4	4	1398	1491	1402	1390	1402
5	5	731	726	725	730	725
6	6	533	580	594	579	595
7	7	97	97	97	97	97
2,2,2	8	113	44	33	123	33
2,4	8	285	243	159	286	159
8	8	242	236	201	242	201
3,3	9	9	8	8	7	8
9	9	30	30	30	38	30
10	10	119	130	131	118	131
11	11	8	8	8	8	8
2,6	12	121	85	66	126	65
12	12	63	72	59	69	59
13	13	7	7	7	7	7
14	14	11	12	12	11	12
15	15	17	17	17	17	17
2,2,2,2	16	6	0	0	6	0
2,2,4	16	22	6	3	23	3
2,8	16	49	37	31	49	31
4,4	16	10	8	3	10	3
16	16	9	3	3	9	3
17	17	1	1	1	1	1

Elt. div	Order	K_1	K_2	K_3	K_4	$\mathbb{Q}$
3,6	18	10	11	6	9	6
18	18	2	3	4	2	3
19	19	1	1	1	1	1
2,10	20	16	9	7	18	7
20	20	7	6	6	7	6
21	21	5	5	5	5	5
22	22	2	2	2	2	2
2,2,6	24	10	3	2	11	2
2,12	24	11	7	4	11	4
24	24	9	6	4	9	4
3,9	27	1	1	1	2	1
27	27	1	1	1	1	1
2,14	28	2	1	1	2	1
28	28	1	1	1	1	1
29	29	1	1	1	1	1
2,2,8	32	6	2	2	6	2
2,18	36	1	0	0	1	0
6,6	36	2	1	1	4	1
3,12	36	1	0	0	1	0
39	39	1	1	1	1	1
2,2,10	40	2	0	0	2	0
2,2,2,6	48	1	0	0	1	0
2,2,12	48	1	0	0	1	0
2,24	48	1	0	0	1	0
5,10	50	1	0	0	1	0
6,12	72	1	0	0	1	0

Table 1: Torsion structure occurrences for the Jacobians of all 66158 curves of the `LMFDB` database defined over some number fields. In particular, $K_i := \mathbb{Q}[t]/(f_i)$ with $f_1 = t^2 - 2, f_2 = t^2 + 2, f_3 = t^3 - 59t - 132, f_4 = \langle t^2 - 2, t^3 - 2\rangle$.

Firstly, note that all torsion structures of the Jacobians of the 66158 curves over $\mathbb{Q}$ are also observed when considering these curves over K_i as defined in Table 1. On the other hand, there are 8 torsion structures that do not arise when considering the curves over $\mathbb{Q}$. Comparing with [Nic18, Table 3.1] we see that the torsion orders 50 and 72 have not been observed yet for genus 2 curves over $\mathbb{Q}$. Secondly, note that the majority of curves have trivial torsion structure.

Besides the torsion structures, it is also interesting to determine how close the bound in (2.3) is to $\#J(K)_{\text{tors}}$, similarly as is done in [MR23, §5.2]. To that end, we reduce the Jacobians modulo the first 20 prime ideals of good reduction and compute the corresponding bound on the torsion order which we denote by b. In this case we only considered the number fields $\mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}(-\sqrt{2})$. The results are in Table 2 below.

$b/\#J(K_i)_{\mathrm{tors}}$	1	2	3	4	5	6	7	8	9	10	12	15	16
Count K_1	61999	3167	437	402	60	40	5	30	6	4	6	2	0
Count K_2	62079	3204	408	296	60	44	5	46	7	4	2	2	1

Table 2: Quotient of $\#J(K_i)_{\mathrm{tors}}$ by the bound b obtained by reducing the Jacobians of all 66158 curves of the `LMFDB` database defined over $K_i := \mathbb{Q}[t]/(f_i)$ with $f_1 = t^2-2, f_2 = t^2+2$ modulo the first 20 primes of good reduction.

From Table 2 we see that the bound b already yields the correct torsion structure for the majority of the Jacobians. Moreover, the prime divisors of $b/\#J(K)_{\mathrm{tors}}$ (excluding the trivial case) are all in the set $\{2, 3, 5, 7\}$.

5.1.2 Unknown torsion

The previous paragraph provided a rough idea of the frequency of different torsion structures. In the process we found two previously unknown torsion structures. However, we can also actively search for unknown torsion structures or for example, for large torsion orders. Following [How15, §4], we consider curves of the form

$$y^2 + (a_3x^3 + a_2x^2 + a_1x + a_0)y = b^2x^2 + b_1x + b_0,$$

where the a_i's and b_i's are elements of some number field.
As is mentioned in [How15, §4], all genus 2 curves with a K-rational non-Weierstrass point (see Definition 2.4) are contained in this family. Using this family we can construct curves that are not defined over $\mathbb{Q}$. We choose $K = \mathbb{Q}(\sqrt{2})$ and let the coefficients vary between $c + d\sqrt{2}$ for $0 \leq c, d \leq 1$ for the a_i's and $-1 \leq c, d \leq 1$ for the b_i's. The only torsion structure we find that was not already found in the previous section is $\mathbb{Z}/33\mathbb{Z}$ for the curve given by:

$$\begin{aligned} y^2 = 2x^6 + (2\sqrt{2}+4)x^5 + (4\sqrt{2}+7)x^4 + (6\sqrt{2}+10)x^3 + (10\sqrt{2}+13)x^2 \\ + (8\sqrt{2}+10)x + 2\sqrt{2} + 3. \end{aligned}$$

However, this structure is also observed already in [How15, Table 3.1]. Furthermore, out of the 139382 curves, 135666 had trivial torsion subgroup. For $K = \sqrt{3}$ we found no new torsion structures and 136182 curves out of 139388 curves had trivial torsion subgroup. Next to searching for unknown torsion structures, we try to find large torsion groups by two different methods:

(1) Firstly, we again consider the Jacobians of the genus 2 curves of the `LMFDB` database but now we are only interested in the Jacobians for which the torsion subgroup over $\mathbb{Q}$ has order at least 25; there are 9 such curves. Subsequently, we consider these 9 curves over various number fields from the `LMFDB` database (`https://www.lmfdb.org/NumberField/`). Denoting the class number by $|\mathrm{Cl}(K)|$, we use 1000 number fields for each $d \in \{2, 3\}$ and $|\mathrm{Cl}(K)| \in \{1, 2\}$. For $d \in \{2, 3\}$ and $|\mathrm{Cl}(K)| = 2$ we

find no new torsion orders. For $d = 2$ and $|\mathrm{Cl}(K)| = 1$ we find new torsion orders in $\{64, 108, 144\}$ with elementary divisors $2, 4, 8$ and $3, 6, 6$ and $2, 2, 6, 6$ respectively. For $d = 3$ and $|\mathrm{Cl}(K)| = 1$ we find new torsion orders in $\{54, 56\}$ with elementary divisors $3, 18$ and $2, 2, 14$ respectively.

(2) Secondly, we start with some of the largest torsion orders found in (1) and by extending the number fields over which the corresponding Jacobians are defined we try to enlarge the K-rational torsion group. However, this has not led to new torsion orders yet.

5.2 Igusa invariants

As we saw in §5.1.2, our algorithm works for curves that are not defined over $\mathbb{Q}$. Let C be a curve of genus 2 defined by

$$y^2 = f(x) = a_0x^6 + a_1x^5 + \cdots + a_5x + a_6.$$

We can associate to $f(x)$ the so called *Igusa invariants* $J_2, J_4, J_6, J_{10} \in \mathbb{Z}[1/2, a_0, a_2, \ldots, a_6]$. For a precise definition of J_2, J_4, J_6, J_{10} see [Mes91]. The Igusa invariants $[J_2, J_4, J_6, J_{10}]$ should be treated as elements in weighted projective space with weights equal to $2, 4, 6$ and 10 respectively. [Mes91] proved that for given Igusa invariants defined over some field k, we can define a curve over a field of degree at most 2 over k that has these invariants. So if the Igusa invariants are defined over $\mathbb{Q}$, there must be a curve with these invariants defined either over $\mathbb{Q}$ or some quadratic number field. We try to use this to find examples of curves defined over a quadratic number field that are not defined over $\mathbb{Q}$ but have Igusa invariants in $\mathbb{Q}$ using the `Magma` function `HyperellipticCurveFromIgusaInvariants()`. However, as is also noted in the `Magma` documentation, the coefficients of the corresponding curves can become huge and no straightforward way to reduce these is available. Consequently, simply running through small values of J_2, J_4, J_4, J_{10} does not yield satisfactory curves. We cannot use the algorithm for these curves due to precision issues, see also Section A. On the other hand, if we are only interested in finding curves with rational Igusa invariants that cannot be defined over $\mathbb{Q}$, we can consider some of the curves found in §5.1.2 again. We find the following curve:

$$y^2 = 2x^6 + 4\sqrt{2}x$$

defined over $K := \mathbb{Q}(\sqrt{2})$ with Igusa invariants given by

$$(-3840 : 337920 : 10485760 : -391378894848).$$

The K-rational torsion subgroup of the corresponding Jacobian is isomorphic to $\mathbb{Z}/5\mathbb{Z}$.

5.3 Isogenies

Let A/K be an abelian variety. By Faltings' finiteness theorem for abelian varieties [Fal83] the isogeny class of A is finite. As noted in [vBCCK23, §1], besides for elliptic curves over $\mathbb{Q}$, little is known regarding the isogeny classes of abelian varieties. Therefore we are interested in all isogenies of A defined over K to get an idea of what the isogeny classes look like. Let A, B be abelian varieties and $\phi\colon A \to B$ an isogeny of degree n over K. Then by [EVdGM12, Proposition 5.12] there exists an isogeny $\hat{\phi}\colon B \to A$ over K such that $\hat{\phi} \circ \phi = [n]$. Hence, for $P \in A$ we have $\hat{\phi}(\phi(P)) = n \cdot P$. This implies that $\ker \phi \subset A[n]$. Consequently, the subgroups of $A[n]$ yield candidates for $\ker \phi$ and therefore provide information regarding what isogenies of degree n can occur. Using Algorithm 3.3 we can compute $A(K)[n]$, but in general we have the following result.

Lemma 5.1. *Let A/K be an abelian variety of dimension g and $n \in \mathbb{Z}_{\geq 0}$. Then*

$$A[n] \cong (\mathbb{Z}/n\mathbb{Z})^{2g}.$$

Proof. See [HS00, Theorem A.7.2.7]. □

Let us now make more precise how finding subgroups of $A[n]$ can help in determining the isogenies. To that end, let $A^\vee$ denote the dual abelian variety of A as defined in [HS00, §A.7.3].

Definition 5.2. Let A be an abelian variety. We call A *principally polarized* if A is equipped with a principal polarization. For a definition of a principal polarization see [vBCCK23, §2.1].

For $n \in \mathbb{Z}$, let

$$\epsilon_n\colon A[n] \times A^\vee[n] \to \mu_n$$

denote the Weil pairing as in [HS00, Exercise A.7.8].
If in addition A is principally polarized, ϵ_n gives rise to a pairing $e_n\colon A[n] \times A[n]$ where e_n is also referred to as the Weil pairing.

Definition 5.3. Let $n \in \mathbb{Z}_{>0}$ and let G be a proper subgroup of $A[n]$. Then G is called *maximal isotropic* if the following holds

(1) For all $S, T \in G$ we have $e_n(S, T) = 1$.

(2) G is a maximal subgroup with respect to property (1), i.e., if H is another proper subgroup of $A[n]$ that satisfies (1) we cannot have that $G \subsetneq H$.

Definition 5.4. Let A be an abelian variety. Call A *typical* if $\mathrm{End}_{\bar{\mathbb{Q}}}(A) = \mathbb{Z}$.

Lemma 5.5. *Let A/K be a typical principally polarized abelian variety. Then every isogeny from A to another typical principally polarized abelian variety B can be decomposed into a chain of isogenies $\phi\colon A \to B$ defined over K such that its kernels are maximal isotropic subgroups of either $A[\ell]$ or $A[\ell^2]$ where ℓ is a prime number.*

Proof. See [vBCCK23, Lemma 2.2]. □

Lemma 5.6. *Let J be the Jacobian variety of a curve C/K of genus g. Then J is principally polarized.*

Proof. See [HS00, Corollary A.8.2.3(a)]. □

Hence, for Jacobians J such that $\mathrm{End}_{\bar{\mathbb{Q}}}(J) = \mathbb{Z}$ we can find all isogenies by determining the maximal isotropic subgroups of either $J[\ell]$ or $J[\ell^2]$ for ℓ a prime number.

Lemma 5.7. *Let J be the Jacobian of a curve of genus g and $n \geq 2$. Moreover, let $G \subset J[n]$ be isotropic with respect to the Weil paring e_n. Then G is maximally isotropic if and only if $\#G = n^g$.*

Proof. See [Nic18, Proposition 5.2.1]. □

Remark 5.8. Given the kernel of an isogeny, [LR23] describes how to actually find equations for the isogeny. Alternatively, see [vBCCK23] for another method to find isogenies between abelian varieties.

We want to use our algorithm to find isogenies defined over $K = \mathbb{Q}$. Consequently, we can use that an isogeny ϕ is defined over $\mathbb{Q}$ if and only if $\ker \phi$ is defined over $\mathbb{Q}$, i.e., is fixed by the action of the absolute Galois group $\mathrm{Gal}(\mathbb{Q})$.
We do one toy example. Define the number field $L := \mathbb{Q}(\sqrt{2})$ and let C be the hyperelliptic curve defined over $\mathbb{Q}$ by:

$$y^2 = x^6 + 2x^5 + 7x^4 + 8x^3 + 11x^2 + 6x + 5.$$

Let J denote the Jacobian of C. We compute that $J(L)_{\mathrm{tors}} \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$ and $J(L)[3] \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$. If $J(L)[3]$ is isotropic then it is maximally isotropic by Lemma 5.7. By Lemma 5.1 we have $J[3] \cong (\mathbb{Z}/3\mathbb{Z})^4$. Unfortunately, we cannot easily check if $J(L)[3]$ is isotropic and hence is the kernel of an isogeny $\phi\colon J \to A$ defined over $\mathbb{Q}$ for some abelian surface A, because there is no implementation of the Weil pairing over number fields in `Magma`. So we cannot yet say something about possible isogenies.

6 Summary and discussion

6.1 Summary

For an abelian variety A defined over a number field K, we described an algorithm that computes $A(K)_{\text{tors}}$ if Assumption 3.1 is satisfied. This algorithm extends the algorithm presented in [Sto98] which computes the torsion subgroup of Jacobians of genus 2 curves over $\mathbb{Q}$. In order to extend the algorithm from [Sto98] to number fields, we needed a way to relate the height of a point to the length of the point considered on a $\mathbb{Z}$-lattice. To that end, we combined [Tur13] and [FF00] to find such a relation. Furthermore, we implemented the algorithm for genus 2 curves over number fields. Using the algorithm we examined the torsion structures of genus 2 curves of the `LMFDB` database over various number fields. Besides the distribution of the torsion structures we also found Jacobians with torsion orders equal to 52 and 72. In addition, we searched for large and unknown torsion structures. In the end, we found the torsion orders $52, 56, 64, 72, 108, 144$ which were not previously observed.

6.2 Discussion

The algorithm could be changed in various ways. First of all, we only considered primes $\mathfrak{p}$ such that $e(\mathfrak{p}) = f(\mathfrak{p}) = 1$. However, we could also consider primes such that $K_{\mathfrak{p}}$ is a proper extension of $\mathbb{Q}_{\mathfrak{p}}$, although in practice this is unlikely to improve the algorithm since there are enough primes satisfying our condition already. Secondly, we could more carefully analyze what the benefit is of using the height bound as in Lemma 4.10 and Lemma 4.11 compared to Theorem 4.3. Other ways in which the algorithm can be improved are sketched in Appendix A.
Besides the algorithm we described, one could implement other approaches to find $A(K)_{\text{tors}}$. For example, [Tur13] uses point enumeration to find all points of bounded height. Alternatively, one could also try to work exclusively with $\mathcal{O}_K$-lattices. There exists no analogue of LLL for $\mathcal{O}_K$-lattices, but the results in [FF00] and [FS10] could be used instead. In any case it is interesting to see how our algorithm compares to other approaches. For example, for Jacobians of genus 2 curves defined over a quadratic number field one could compare our algorithm to the approach described in Remark 4.14.

In theory, the algorithm works for all abelian varieties but one could try to implement it in practice for Jacobians of hyperelliptic genus 3 curves over number fields, similar to [MR23]. A height bound for torsion points is already given by [Sto17].
One could use the algorithm to explore more torsion structures of genus 2 curves over number fields. For example, the torsion structures of the examples in [Kos14, §5] can be computed. As noted in the introduction, the study of torsion structures of genus 2 curves over number fields could also provide us with more insights regarding the uniform boundedness conjecture. Next to finding new torsion structures, we could also try to find points in the rational torsion subgroup with large order. Lastly, as was noted in Subsection

5.3, there is no implementation of the Weil pairing over number fields in `Magma`. However, this would actually not be very difficult to implement, especially for small values of n. The implementation would then allow one to determine some isogenies.

References

[BCP97] W. Bosma, J. Cannon, and C. Playoust. The magma algebra system i: The user language. *Journal of Symbolic Computation*, 24(3-4):235–265, 1997. 1

[Ber10] A. Bertram. Complex algebraic geometry: Smooth curves. `https://www.math.utah.edu/~bertram/6030/12Classification.pdf`, 2010. 2.3

[BL04] C. Birkenhake and H. Lange. *Complex Abelian Varieties*, volume 302 of *Grundlehren der Mathematischen Wissenschaften*. Springer-Verlag, Berlin, second edition, 2004. 2.1.3

[CF96] J.W.S. Cassels and E.V. Flynn. *Prolegomena to a middlebrow arithmetic of curves of genus 2*, volume 230 of *Londen Mathematical Society Lecture Note Series*. Cambridge University Press, Cambridge, 1996. 4, 4.1

[Coh00] H. Cohen. *Advanced topics in computational number theory*, volume 193 of *Graduate Texts in Mathematics*. Springer-Verlag, New-York, 2000. 2.5

[Con20] K. Conrad. A multivariable hensel's lemma. `https://kconrad.math.uconn.edu/blurbs/gradnumthy/multivarhensel.pdf`, 2020. 2.3

[Cre97] J. E. Cremona. *Algorithms for modular elliptic curves*. Cambridge University Press, Cambridge, second edition, 1997. 1

[CX08] P.L. Clark and X. Xarles. Local bounds for torsion points on abelian varieties. *Canadian Journal of Mathematics*, 60(3):532–555, 2008. 1

[EVdGM12] B. Edixhoven, G. Van der Geer, and B. Moonen. Abelian varieties. `https://gerard.vdgeer.net/AV.pdf`, 2012. 5.3

[Fal83] G. Faltings. Endlichkeitssätze für abelsche Varietäten über Zahlkörpern. *Inventiones mathematicae*, 73:349–366, 1983. 5.3

[FF00] C. Fieker and C. Friedrichs. On reconstruction of algebraic numbers. In *Algorithmic Number Theory: 4th International Symposium, ANTS-IV Leiden*, volume 1838 of *Lecture Notes in Computer Science*, pages 285–296. Springer, 2000. 1, 2.5, 2.6.2, 3, 3.2.2, 3.2.2, 6.1, 6.2

[FH91] W. Fulton and J. Harris. *Representation Theory*, volume 129 of *Graduate Texts in Mathematics*. Springer, 1991. 4.2

[Fly93] E.V. Flynn. The group law on the Jacobian of a curve of genus 2. *J. Reine Angew. Math.*, (439):45–69, 1993. 4.1

[FS97] E.V. Flynn and N.P. Smart. Canonical heights on the Jacobians of curves of genus 2 and the infinite descent. *Acta Arithmetica*, 79(4):333–352, 1997. 4.1, 4.1, 4.2

[FS10] C. Fieker and D. Stehlé. Short bases of lattices over number fields. In *International Algorithmic Number Theory Symposium*, pages 157–173. Springer, 2010. 6.2

[Gal12] S.D. Galbraith. *Mathematics of public key cryptography*. Cambridge University Press, 2012. 2.5, 2.5

[How15] E. W. Howe. Genus-2 Jacobians with torsion points of large order. *Bulletin of the London Mathematical Society*, 47(1):127–135, 2015. 5.1.2, A

[HS00] M. Hindry and J.H. Silverman. *Diophantine geometry*, volume 201 of *Graduate Texts in Mathematics*. Springer-Verlag, New-York, 2000. 2, 2.14, (1), (2), 2.1.2, 2.1.2, 2.2, 2.36, 2.3, 2.3, 2.6.1, 2.6.1, 5.3, 5.3, 5.3

[Jor05] A. Jorza. *The Birch and Swinnerton-Dyer Conjecture for Abelian Varieties over Number Fields*. Senior thesis. Harvard University, 2005. 1

[Kat80] N.M. Katz. Galois properties of torsion points on abelian varieties. *Inventiones mathematicae*, 62(3):481–502, 1980. 2.3

[Kos14] C. Koster. On the units of coordinate rings of algebraic curves. `https://fse.studenttheses.ub.rug.nl/12114/1/Christiaan_Koster_WM_2014.pdf`, 2014. Master thesis, University of Groningen. 6.2

[Kum64] E.E. Kummer. Über die Flächen vierten Grades mit sechzehn singulären Punkten. *Collected papers*, 2:418–432, 1864. 4

[LMF23] The LMFDB Collaboration. The L-functions and modular forms database. `https://www.lmfdb.org`, 2023. 1

[LR23] D. Lubicz and D Robert. Fast change of level and applications to isogenies. *Research in Number Theory*, 9(1):7, 2023. 5.8

[Mer96] L. Merel. Bornes pour la torsion des courbes elliptiques sur les corps de nombres. *Inventiones mathematicae*, 124(1):437–450, 1996. 1

[Mes91] J. Mestre. Construction de courbes de genre 2 à partir de leurs modules. In *Effective methods in algebraic geometry*, pages 313–334. Springer, 1991. 5.2

[MG78] B. Mazur and D. Goldfeld. Rational isogenies of prime degree. *Inventiones mathematicae*, 44:129–162, 1978. 1

[Mil08] J.S. Milne. Algebraic number theory. `https://www.jmilne.org/math/CourseNotes/ANT.pdf`, 2008. 2.2

[Mol99] R.A. Mollin. *Algebraic number theory*. CRC press, 1999. 2.5, 2.6.2, 3.2.1

[Mor22] L.J. Mordell. On the rational resolutions of the indeterminate equations of the third and fourth degree. In *Procedings of the Cambridge Philosophical Society.*, volume 21, pages 179–192, 1922. 2.1.2

[MR23] J.S. Müller and B. Reitsma. Computing torsion subgroups of Jacobians of hyperelliptic curves of genus 3. *Research in Number Theory*, 9(2):23, 2023. 1, 2.1.3, 3, 3.2, 3.2.2, 3.17, 4, 5.1.1, 6.2, A

[MS16] J.S. Müller and M. Stoll. Canonical heights on genus-2 Jacobians. *Algebra & Number Theory*, 10(10):2153–2234, 2016. 4.7, 4.2, 4.2, A

[Nic18] C. Nicholls. *Descent methods and torsion on Jacobians of higher genus curves.* PhD thesis, University of Oxford, 2018. 5.1.1, 5.3

[NS04] P.Q. Nguyen and D. Stehlé. Low-dimensional lattice basis reduction revisited. In *International Algorithmic Number Theory Symposium*, pages 338–357. Springer, 2004. 2.5

[Sil07] J.H. Silverman. *The arithmetic of dynamical systems*, volume 241 of *Graduate Texts in Mathematics*. Springer Science & Business Media, 2007. 2.6.2

[Ste12] P. Stevenhagen. Number rings. `https://websites.math.leidenuniv.nl/algebra/ant.pdf`, 2012. Lecture notes, Leiden University. 2.6.2, 4.2

[Sto98] M. Stoll. On the height constant for curves of genus two. *Acta Arithmetica*, 90(2):183–201, 1998. 1, 2.3, 3, 3.3, 3.2, 4.2, 4.2, 4.3, 4.2, 4.5, 4.2, (1), (3), 6.1, A

[Sto01] M. Stoll. Implementing 2-descent for Jacobians of hyperelliptic curves. *Acta Arithmetica*, 98(3):245–277, 2001. 3.17

[Sto02] M. Stoll. On the height constant for curves of genus two ii. *Acta Arithmetica*, 90(2):183–201, 2002. 4, 4.2

[Sto14] M. Stoll. Arithmetic of hyperelliptic curves. `http://www.mathe2.uni-bayreuth.de/stoll/teaching/ArithHypKurven-SS2014/Skript-ArithHypCurves-pub-screen.pdf`, 2014. Course notes for Summer Semester 2014. 2.1.1

[Sto17] M. Stoll. An explicit theory of heights for hyperelliptic jacobians of genus three. In *Algorithmic and experimental methods in algebra, geometry, and number theory*, pages 665–715. Springer, 2017. 6.2

[Sut12] A. V. Sutherland. Torsion subgroups of elliptic curves over number fields. `https://math.mit.edu/drew/MazursTheoremSubsequentResults.pdf`, 2012. 1

[Tur13] C.L. Turner. *Lattice methods for finding rational points on varieties over number fields*. PhD thesis, University of Warwick, 2013. 1, 2.6.2, 2.69, 2.6.2, 2.72, 2.6.2, 2.6.2, 3, 5.1.1, 6.1, 6.2

[vB23] R. van Bommel. Computing torsion for plane quartics without using height bounds. *ArXiv preprint*, 2023. 1

[vBCCK23] R. van Bommel, S. Chidambaram, E. Costa, and J. Kieffer. Computing isogeny classes of typical principally polarized abelian surfaces over the rationals. *ArXiv Preprint*, 2023. 5.3, 5.2, 5.3, 5.8

[Wei29] A. Weil. L'arithmétique sur les courbes algébriques. *Acta mathematica*, 52:281–315, 1929. 2.1.2

[Wri14] D. Wright. Algebraic number theory. `https://math.okstate.edu/people/pyan/AlgebraicNumberTheory.pdf`, 2014. Course notes for Fall Semester 2014. 2.2, 2.2, 2.2

A Implementation issues

In this section we will outline some issues regarding the `Magma` code. As previously noted, the code can be found on `https://github.com/MaxPosthumus/MasterProject/blob/main/`.

- Following Remark 3.10, if $\mathfrak{p}^n$ is principal we can use just 1 generator instead of 2. Since this seems to be slightly faster in practice, we check for this in the code. Alternatively, we could first check if K is a PID but this seems to be slower. Lastly, we could also try to find generators with small coefficients with respect to the integral basis.

- In Algorithm 3.1 we lift $\kappa(\tilde{Q}) \in \mathcal{K}(\mathcal{O}_K/\mathfrak{p})$ to $\mathcal{K}(\mathcal{O}_K/p^N)$ by sequentially lifting $\kappa(\tilde{Q})$ to $\mathcal{K}(\mathcal{O}_K/p^r)$ for $r \leq N$. In the code accompanying [Sto98], the Kummer surface is constructed again for each of these lifts. While this is not a problem over $\mathbb{Q}$, this does cost a lot of time over K. Therefore, we immediately set the precision of the completion equal to the necessary precision. In Stoll's case the default precision is higher than "newprec" in the first few iterations.

- In order to define the field embeddings we will first try to use the standard precision in $\mathbb{C}$ of 30. However, it might be the case (especially for number fields of large discriminant such as $K := x^2 - x - 510$) that the field embeddings will map nonzero elements to zero. In that case the precision is raised to 150. The same issue occurred when computing bounds for the height constants at infinity using `HCinfinityNum`. This is resolved in the same way.

- Next to the field embeddings we also encountered problems when the coefficients of $F(x, z)$ are very large. For `HCinfinityNum` we need to compute the roots a_i as in (4.2), but this leads to problems if the coefficients of $F(x, z)$ become huge such as in Subsection 5.2.

- In order to get the constant B_L we need to compute the class group of K. Since this can take very long we added an optional parameter that allows one to use the Generalized Riemann Hypothesis (GRH) to speed up the computations. In the examples considered so far, we only needed this when we extended the number fields to find large torsion (see (2) in §5.1.2).

- The definition of B_L in (3.3) uses $N_K := \max_{\mathfrak{b} \in B} N(\mathfrak{b})$ for B the set of ideals that has minimal norm amongst the integral ideals in its class. However, in practice we will just find representatives for each class but not necessarily of minimal norm. The bound might be slightly increased because of this, but is nevertheless valid.

- Similarly as in [MR23], we try to use doubling when deciding on a value for $[[M]]$ as in Algorithm 3.1. This is different from what is done in Stoll's code. However, the doubling saves a bit of computation time.

- When determining a bound on $\#J(K))_{\text{tors}}$, we use the extra information on the torsion structures besides the torsion orders as also done in [MR23].

- The way the step function is computed in the code may seem different from [MS16, §16] but note that the function φ as defined in [MS16, §16.1] is homogeneous of degree 1/4, i.e., $\varphi(sx_1, \ldots, sx_4) = s^{1/4}\varphi(x_1, \ldots, x_4)$. Now in the code the following is computed (only the first two terms are presented here):

$$\begin{aligned}
&4 \cdot \log(||\varphi(b_0)||_\infty) + 4^2 \cdot \log\Big(||\varphi\Big(\frac{\varphi(b_0)}{||\varphi(b_0)||_\infty}\Big)||_\infty\Big) \\
&= 4 \cdot \log(||b_1||_\infty) + 4^2 \cdot \log\Big(||\varphi\Big(\frac{b_1}{||b_1||_\infty}\Big)||_\infty\Big) \\
&= 4 \cdot \log(||b_1||_\infty) + 4^2 \cdot \log\Big(||\varphi(b_1)||b_1||_\infty^{-1/4}\Big)||_\infty\Big) \\
&= 4 \cdot \log(||b_1||_\infty) + 4^2 \cdot \log\Big(||b_2||||b_1||_\infty^{-1/4}\Big)\Big) \\
&= 4 \cdot \log(||b_1||_\infty) + 4^2 \cdot \Big(\log(||b_2||) - 1/4\log(||b_1||_\infty))\Big) \\
&= 4^2 \cdot \log||b_2||_\infty,
\end{aligned}$$

  where we used that $b_{n+1} = \varphi(b_n)$ for $n \geq 0$.

- We analyzed the code with `Magma`'s profiler function in order to determine what steps take the most time and in some cases this led us to change the steps.

- Changing the number of steps used in `HCinfinityNum()` does not significantly change the computation time. Therefore, the standard 10 steps is fine.

- There is no large database of Jacobians of genus 2 curves over number fields for which the K-rational torsion structure is known. Consequently, we cannot verify the correctness of the algorithm this way. However, we can still do sanity checks. Firstly, we can try to find curves for which we know already what the torsion structure looks like and compare this with the results from our algorithm. For example, [How15, Theorem 3.1] is useful in that regard. Secondly, we can compute the torsion orders of a set of Jacobians of genus 2 curves over $\mathbb{Q}$. Then if we consider these Jacobians over some number field, the torsion orders should be at least as large as for the Jacobians over $\mathbb{Q}$. Finally, we can do stability checks, that is, running the algorithm multiple times for the same curves to check that we get the same results each time.