Rational points on Jacobians of hyperelliptic curves

Jan Steffen Müller
Institut für Mathematik, Carl von Ossietzky Universität Oldenburg, 26111 Oldenburg, Germany
e-mail: jan.steffen.mueller@uni-oldenburg.de

Abstract. We describe how to prove the Mordell-Weil theorem for Jacobians of hyperelliptic curves over $\mathbb{Q}$ and how to compute the rank and generators for the Mordell-Weil group.

Keywords. hyperelliptic curves, Jacobians, rational points, descent, heights

1. The Mordell-Weil theorem

If $C/\mathbb{Q}$ is a hyperelliptic curve, then the rational points on its Jacobian J form a finitely generated abelian group $J(\mathbb{Q})$ by the Mordell-Weil theorem. In this section, we outline its proof, as well as introducing some general notions about hyperelliptic curves and their Jacobians.

1.1. Abelian varieties

Let k be a field. The Jacobian is an example of an abelian variety over k; i.e. a projective variety over k that carries a group structure, such that the group structure and the variety structure are compatible. More generally, we define:

Definition 1.1. An *algebraic group* G over k is a variety G/k such that $G(k')$ is a group for all field extensions $k \subset k'$ and such that the group operation $G \times G \to G$ and the inversion $G \to G$ are regular functions.

In fancier language, an algebraic group over k is a group object in the category of varieties over k.

Example 1.2. The additive group $\mathbb{G}_a$ over k is the affine line over k, the group law being addition. Similarly, the multiplicative group $\mathbb{G}_m$ over k is the affine line over k with the origin removed, the group law given by multiplication.

Definition 1.3. An *abelian variety* A over k is a projective algebraic group over k.

Note that the additive and the multiplicative group are not abelian varieties.

Example 1.4. An abelian variety of dimension 1 is an elliptic curve.

Example 1.5. An abelian variety A of dimension g over $\mathbb{C}$ is isomorphic to a complex torus $\mathbb{C}^g/\Lambda$, where $\Lambda \cong \mathbb{Z}^{2g}$ is a lattice. Every one-dimensional complex torus is an abelian variety, but in higher dimension this is no longer the case, see [37, §5.2]. The theory of abelian varieties over $\mathbb{C}$ is a classical area of mathematics that was particularly popular in the 19th century. In contrast, the algebraic theory of abelian varieties was essentially initiated by Weil in the 1940s.

Remark 1.6. The group law on an abelian variety is always commutative, see [37, Lemma A.7.1.3].

For further details on abelian varieties see [37, §A.7] or [49].

1.2. Mordell-Weil

The fundamental result in the arithmetic of abelian varieties is the following:

Theorem 1.7. *(Mordell, Weil) Let k be a global field and let A/k be an abelian variety. Then the group $A(k)$ is finitely generated. In other words, we have*

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

where the rank *r is a nonnegative integer and the* torsion subgroup *$A(k)_{\mathrm{tors}} \subset A(k)$ is finite.*

Here a global field is a number field or a finite extension of $\mathbb{F}_q(T)$ for some prime power q. Theorem 1.7 was first proved by Mordell [51] for elliptic curves over the rationals. Weil [84] generalized it to abelian varieties over number fields. Lang and Néron [44] have proved a further generalization, see also [45, Theorem 6.1].

The theorem can be proved by combining the following steps:

(i) Show that $A(k)/2A(k)$ can be embedded into a finite group $\mathrm{Sel}_2(A/k)$, the 2-*Selmer group* of A/k.
(ii) Construct a quadratic form $\hat{h} : A(k) \to \mathbb{R}$, the *canonical height*, such that for all $B \in \mathbb{R}$ the set $\{P \in A(k) : \hat{h}(P) \leq B\}$ is finite.
(iii) Show that (i) and (ii) imply the theorem.

We first prove (iii).

Lemma 1.8. *Suppose that (i) and (ii) hold for A. Let $P_1, \ldots, P_s \in A(k)$ be a set of representatives for $A(k)/2A(k)$, let $c = \max\{\hat{h}(P_i) : i \in \{1, \ldots, s\}\}$ and let T denote the set $\{P \in A(k) : \hat{h}(P) \leq c\}$. Then T is a finite set and $A(k)$ is generated by T.*

Proof. The finiteness of T follows from (ii). Furthermore, (ii) implies that $\hat{h}$ is nonnegative and vanishes precisely on torsion points. Now suppose that T does not generate $A(k)$; then there is an element $Q_1 \in A(k) \setminus \langle T \rangle$ of minimal canonical height. We can write

$$Q_1 = P_i + 2Q_2$$

for some $i \in \{1, \ldots, s\}$ and $Q_2 \in A(k)$. But

$$4\hat{h}(Q_2) = \hat{h}(Q_1 - P_i) \leq 2\hat{h}(Q_1) + 2\hat{h}(P_i) < 4\hat{h}(Q_1),$$

since $\hat{h}$ satisfies the parallelogram law and since $\hat{h}(P_i) \leq c < \hat{h}(Q_1)$. By minimality of $\hat{h}(Q_1)$, we have $Q_2 \in \langle T \rangle$, but this implies $Q_1 \in \langle T \rangle$. Contradiction! □

Remark 1.9. The proof of Lemma 1.8 is an example of what's usually called "infinite descent". The term originates with Fermat and was coined by him to describe his method of proving that there are no positive integers x,y,z such that $x^4+y^4=z^2$.

Remark 1.10. If we can find representatives for $A(k)/2A(k)$, then Lemma 1.8 gives an effective method for computing a set of generators for $A(k)$, provided we have a way of listing all points whose canonical height is bounded by a given real number.

We now discuss how to

- *prove* (i) and (ii) and
- *compute* r and generators of $A(k)$.

For simplicity, we restrict to the following situation: The field k is the field $\mathbb{Q}$ of rational numbers and the abelian variety A is the Jacobian of a hyperelliptic curve $C/\mathbb{Q}$. The proof of Theorem 1.7 turns out to be constructive in the following sense: It provides us with a method to compute these objects which often works in practice; however, this method is not currently effective.

1.3. Hyperelliptic curves

Let k be a field of characteristic not 2 with fixed separable closure k^{sep}, let g be a positive integer. Every hyperelliptic curve C of genus g over k has an equation

$$Y^2 = F(X,Z) \tag{1}$$

in the weighted projective plane over k with weights $1, g+1, 1$ assigned to the variables X,Y and Z, respectively, where $F\in k[X,Z]$ is a binary form of degree $2g+2$ with nonvanishing discriminant. We set

$$f(x) = F(X,1)\in k[x];$$

then f is separable and either has degree $d=2g+1$ or $d=2g+2$. In the first situation, there is a unique point $\infty=(1:0:0)\in C$ at infinity (i.e. having vanishing Z-coordinate), whereas in the second situation there are two points $\infty_{\pm s}=(1:\pm s:0)\in C$ at infinity, s^2 being the leading coefficient of f. It follows that if d is odd, then we always have $\infty\in C(k)$ – in particular the set of k-rational points on C is nonempty. In contrast, the points $\infty_{\pm s}$ are defined over k if and only if $s\in k$ and $C(k)$ may be empty if d is even.

We will often describe a hyperelliptic curve given by an equation (1) in terms of the affine piece $y^2=f(x)$. Note that C is covered by the affine pieces $y^2=f(x)$ and $v^2=F(1,u)$.

We denote the hyperelliptic involution, sending a point $(X:Y:Z)\in C$ to the point $(X:-Y:Z)$ by w. There are precisely $2g+2$ fixed points of w in $C(k^{\mathrm{sep}})$, the *Weierstrass points* of C. These consist of the points $(r,0)$, where r is a root of f, plus (if d is odd) the point ∞. In geometric terms, the Weierstrass points are precisely the ramification points of the $2-1$ covering $C\to\mathbb{P}^1$ sending $(X:Y:Z)$ to $(X:Z)$.

1.4. Divisors

We briefly review the facts about divisors on C that we shall need. Recall that a *divisor* D on C is a finite formal sum $D=\sum_{P\in C(k^{\mathrm{sep}})} n_P\cdot P$ of points in $C(k^{\mathrm{sep}})$. The set of divisors forms a group Div_C under pointwise addition. We call the set $\mathrm{supp}(D)=\{P\in C(k^{\mathrm{sep}}) : n_P\neq 0\}$ the *support* of D; D is said to be *effective* if $n_P \geq 0$ for all $P \in C$. The *degree* of D is defined as $\deg(D) = \sum_{P \in C(k^{\mathrm{sep}})} n_P$. It is clear that the degree map $\deg : \mathrm{Div}_C \to \mathbb{Z}$ is a group homomorphism, and we let Div_C^0 denote its kernel.

The absolute Galois group $G_k = \mathrm{Gal}(k^{\mathrm{sep}}/k)$ acts on $C(k^{\mathrm{sep}})$ in the obvious way. If $\sigma \in G_k$, and $D = \sum_P n_P \cdot P \in \mathrm{Div}_C$, then σ acts on D via $D^\sigma = \sum_{P \in C} n_P \cdot P^\sigma$. We say D is *rational over k* if D is invariant under the action of G_k and we write $\mathrm{Div}_C(k)$ for the subgroup of k-rational divisors (and $\mathrm{Div}_C^0(k)$ for $\mathrm{Div}_C^0 \cap \mathrm{Div}_C(k)$).

Remark 1.11. Note that $D = \sum n_P \cdot P \in \mathrm{Div}_C(k)$ does not imply that all $P \in C(k)$. For instance, if d is even, then the divisor $(\infty_s) + (\infty_{-s})$ is always k-rational, even if $s \notin k$.

The divisor of a rational function $\varphi \in k^{\mathrm{sep}}(C)^\times$ is defined as

$$\mathrm{div}(\varphi) = \sum_{P \in C} \mathrm{ord}_P(\varphi) \cdot P,$$

where ord_P is the normalized discrete valuation on the local ring of C at P, extended to $k^{\mathrm{sep}}(C)^\times$. Such divisors are called *principal*; their degree is always 0. We say that two divisors $D_1, D_2 \in \mathrm{Div}_C$ are *linearly equivalent* and write $D_1 \sim D_2$ if $D_1 - D_2$ is principal. In fact $\mathrm{div} : k^{\mathrm{sep}}(C)^\times \to \mathrm{Div}_C^0$ is a Galois equivariant group homomorphism, so that G_k acts on the quotient $\mathrm{Pic}_C = \mathrm{Div}_C / \sim$, called the *Picard group* or *divisor class group* of C. In particular, we will be interested in the group $\mathrm{Pic}_C^0(k) = \left(\mathrm{Pic}_C^0\right)^{G_k}$ of k-rational divisor classes of degree 0.

Example 1.12. If C is an elliptic curves, then $C(k) \cong \mathrm{Pic}_C^0(k)$.

1.5. The Jacobian

For $g > 1$, there is no algebraic group law on C, but we can still work with Pic_C^0.

Theorem 1.13. *(Weil) There is an abelian variety $J = \mathrm{Jac}(C)$ over k of dimension g such that we have $J(k') = \mathrm{Pic}_C^0(k')$ for every extension field $k \subset k' \subset k^{\mathrm{sep}}$. We call J the* Jacobian *of C.*

Weil [85] constructed the Jacobian by first applying the Riemann-Roch theorem to construct a birational group law (i.e. a group law that is defined on the complement of a proper Zariski-closed subset) on the gth symmetric power

$$\mathrm{Sym}^g(C) = C^g / \mathfrak{S}_g$$

of C, where $\mathfrak{S}_g$ is the symmetric group on $\{1, \dots, g\}$, and then constructing a projective variety J over k birational to $\mathrm{Sym}^g(C)$ such that the birational group law gives J the structure of an abelian variety. See [37, §A.8] for an exposition of a similar, but simpler construction due to Chow. Note that Theorem 1.13 and the proofs just mentioned hold more generally for a smooth projective geometrically irreducible curve. For more information about Jacobians see [37, §A.8] and [50].

By Theorem 1.13 we can embed C into J as follows: Fix a divisor class $c \in \mathrm{Pic}_C$ of degree 1 and define

$$\iota_c : C \hookrightarrow J, \quad P \mapsto [P] - c.$$

If $c \in \mathrm{Pic}_C(k)$, then ι_c is also defined over k and we have $\iota_c(C(k)) \subset J(k)$. Hence information on the group $J(k)$ can be used to obtain information about $C(k)$. If there is a rational point $P_0 \in C(k)$, we can choose $c = [P_0]$ to get an embedding defined over k.

Example 1.14. Recall that if f has odd degree, then $C(k)$ always contains the point ∞ at infinity. In this situation, we set

$$\iota : C \hookrightarrow J, \quad P \mapsto [P - \infty].$$

What about the even degree case? By [60, §3], there is always a k-rational divisor class of degree 1 if g is even and k is a finite field, a local field (e.g. $\mathbb{R}, \mathbb{C}$ or a finite extension of the p-adics) or a global field. Fortunately, these are precisely the fields we will be interested in. In all of these cases (including odd degree), we can represent every k-rational divisor class by a rational divisor. We shall mostly ignore the slightly irritating case of odd genus and even degree.

Theorem 1.13 implies in particular that J can be embedded into projective space.

Example 1.15. If C has genus 1, then J is an elliptic curve over k (cf. Example 1.4). In particular, J can be embedded into $\mathbb{P}^2$. In fact, C and J are isomorphic over any field $k \subset k' \subset k^{\mathrm{sep}}$ such that $C(k') \neq \emptyset$.

Example 1.16. Suppose that $g = 2$. An explicit embedding of J into $\mathbb{P}^8$, valid for $\deg(f) = 5$, was constructed by Grant [33]. An explicit embedding of the Jacobian of a general curve of genus 2 over k into $\mathbb{P}^{15}$ was constructed by Flynn [28], see also [11]. Here the Jacobian is cut out by the vanishing of 72 quadratic forms.

Example 1.16 suggests that it is usually not a good idea to work explicitly with a model of the Jacobian in projective space. In general, J can be embedded into $\mathbb{P}^{4^g-1}$ as an intersection of quadrics by a result of Mumford [56] ($\mathbb{P}^{3^g-1}$ suffices if f has odd degree). Instead, we use that elements of $J(k)$ can be represented using divisors on C.

This is where the fact that C is hyperelliptic comes in handy, because it enables us to choose a particularly simple way of representing points on J. For simplicity, we restrict to the case of odd degree d. Suppose that $D = \sum_{i=1}^n P_i \in \mathrm{Div}_C(k)$ is an effective divisor on C. We call D *semi-reduced* if $\infty \notin \mathrm{supp}(D)$ and if $P_i \in \mathrm{supp}(D)$ implies that $w(P_i) \notin \mathrm{supp}(D)$, unless P_i is a Weierstrass point. We also call D *reduced* if D is semi-reduced and $n \leq g$. In order to compute with (semi-)reduced divisors, it is convenient to encode them using univariate polynomials as follows:

Lemma 1.17. *Let d be odd and let $D = \sum_{i=1}^n P_i \in \mathrm{Div}_C(k)$ be a semi-reduced divisor on C, where $P_i = (x_i, y_i) \in C(k^{\mathrm{sep}})$. Then there are unique polynomials $a, b \in k[x]$ such that*

(i) a is monic of degree n and factors as $a(x) = \prod_{i=1}^n (x - x_i)$;
(ii) b has degree at most $n-1$ and we have $b(x_i) = y_i$ for all i;
(iii) there is a polynomial $c \in k[x]$ such that $f = ac + b^2$.

The divisor D is uniquely determined by the pair (a, b). More precisely, the ideal generated by the pair of polynomials $(a(x), y - b(x))$ represents the divisor $\sum_{i=1}^n (P_i)$ in the affine coordinate ring of C. We call the pair (a, b) the *Mumford representation* of D.

There is an algorithm for addition of points on J due to Cantor [9] which uses the Mumford representation and relies on the first part of the following result, which can be proved using Riemann-Roch.

Lemma 1.18. *Let d be odd and let $P \in J(k)$. Then there is a unique reduced divisor $D \in \mathrm{Div}_C(k)$ such that $D - \deg(D) \cdot \infty$ represents P. Moreover, there is a semi-reduced divisor $D' \in \mathrm{Div}_C(k)$ such that $D' - \deg(D') \cdot \infty$ represents P and D' contains no Weierstrass point in its support.*

Remark 1.19. The even degree case is similar, at least when the genus is even. For odd degree one has to be more careful.

1.6. Software

Most of the algorithms described in the present article are not suitable for pen-and-paper computations. Fortunately, most of them are implemented in (at least) one of the computer algebra systems `Magma` [3], `Pari/GP` [80] or `Sage` [71]. Whereas all three of these contain extensive functionality for computing with elliptic curves, the situation is different for hyperelliptic curves of genus $g > 1$: Here `Sage` has little functionality, especially for Jacobians, while `Pari/GP` has none at all. In contrast, `Magma` contains basically all algorithms discussed in this article.

1.7. Applications

Recall that we are interested in computing the rank r of $J/\mathbb{Q}$ and generators of $J(\mathbb{Q})$, where J is the Jacobian of a hyperelliptic curve C/Q. These problems are interesting in their own right, but they also have several important applications, some of which we will now list.

By Faltings' Theorem [21], we know that there are only finitely many rational points on C when $g > 1$, but all currently known general proofs are ineffective. Fortunately, there are several methods to find all of these rational points, some of which are described elsewhere in this volume. These include the method of Chabauty-Coleman and the Mordell-Weil sieve, see Siksek's article. Both methods require generators of a subgroup of $J(\mathbb{Q})$ of finite index and, in addition, some information on the index. So at the very least we need to be able to compute the rank.

We need generators of the full Mordell-Weil group to apply an algorithm of Bugeaud-Mignotte-Siksek-Stoll-Tengely [8] for the computation all integral points on C (if $f \in \mathbb{Z}[x]$). Another application for which we do need generators for $J(\mathbb{Q})$ is the computation of the *regulator* of $J(\mathbb{Q})$ (see (8)), which appears in the statement of the full conjecture of Birch and Swinnerton-Dyer for J, c.f. [37, §F.4.1]. There is extensive numerical evidence for this conjecture for elliptic curves (see for instance [34]) and some for Jacobians of genus 2 curves [26].

2. Two-descent

Let J be the Jacobian of a hyperelliptic curve $C/\mathbb{Q}$, given by an equation (1). We may assume, without loss of generality, that $F \in \mathbb{Z}[X,Z]$. We construct the 2-Selmer group $\mathrm{Sel}_2(J/\mathbb{Q})$, whose finiteness implies that $J(\mathbb{Q})/2J(\mathbb{Q})$ is also finite; this constitutes part (i) of the proof of the Mordell-Weil theorem, also known as the weak Mordell-Weil theorem. We then discuss how to find (an upper bound on) the rank r of $J/\mathbb{Q}$. This method is known as *2-descent on J*.

2.1. High-brow construction of the 2-Selmer group

We only give a brief review of a high-brow construction of the 2-Selmer group $\mathrm{Sel}_2(J/\mathbb{Q})$, using the language of *Galois cohomology*. See [67, Appendix B.3] or [37, Appendix C.5] for a short introduction to H^0 and H^1 in Galois cohomology, sufficient for our purposes. For a more complete account see [64].

The starting point is the short exact sequence

$$0 \longrightarrow J[2] \longrightarrow J(\bar{\mathbb{Q}}) \xrightarrow{[2]} J(\bar{\mathbb{Q}}) \to 0,$$

where $[2] : J \to J$ is the duplication map. We can view the terms appearing in this exact sequence as $G_{\mathbb{Q}}$-modules (recall that $G_{\mathbb{Q}} = \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$) and apply Galois cohomology to it; this results in the long exact sequence

$$\begin{tikzcd}
0 \arrow[r] & J(\mathbb{Q})[2] \arrow[r] & J(\mathbb{Q}) \arrow[r, "{[2]}"] & J(\mathbb{Q}) \arrow[r, "\lambda"] & H^1(G_{\mathbb{Q}}, J[2]) \\
\arrow[r] & H^1(G_{\mathbb{Q}}, J) \arrow[r] & H^1(G_{\mathbb{Q}}, J),
\end{tikzcd}$$

where λ is the connecting homomorphism. From this we get the fundamental short exact sequence

$$\begin{tikzcd}
0 \arrow[r] & J(\mathbb{Q})/2J(\mathbb{Q}) \arrow[r, "\lambda"] & H^1(G_{\mathbb{Q}}, J[2]) \arrow[r] & H^1(G_{\mathbb{Q}}, J)[2] \arrow[r] & 0.
\end{tikzcd}$$

For every prime number $v = p$ (and, setting $\mathbb{Q}_\infty = \mathbb{R}$, for the place $v = \infty$), there is an analogous exact sequence

$$\begin{tikzcd}
0 \arrow[r] & J(\mathbb{Q}_v)/2J(\mathbb{Q}_v) \arrow[r, "\lambda"] & H^1(G_v, J[2]) \arrow[r] & H^1(G_v, J)[2] \arrow[r] & 0,
\end{tikzcd}$$

where $G_v = \mathrm{Gal}(\overline{\mathbb{Q}_v}/\mathbb{Q})$. Hence there is a commutative diagram

$$\begin{tikzcd}
0 \arrow[r] & J(\mathbb{Q})/2J(\mathbb{Q}) \arrow[r, "\lambda"] \arrow[d] & H^1(G, J[2]) \arrow[r] \arrow[d] & H^1(G, J)[2] \arrow[r] \arrow[d, "\mathrm{res}_v"] & 0 \\
0 \arrow[r] & J(\mathbb{Q}_v)/2J(\mathbb{Q}_v) \arrow[r, "\lambda_v"] & H^1(G_v, J[2]) \arrow[r] & H^1(G_v, J)[2] \arrow[r] & 0,
\end{tikzcd}$$

where the vertical maps are induced by the embedding $\mathbb{Q} \hookrightarrow \mathbb{Q}_v$. We define the *2-Selmer group* of $J/\mathbb{Q}$ as

$$\mathrm{Sel}_2(J/\mathbb{Q}) = \bigcap_v \ker\left(H^1(G, J[2]) \to H^1(G_v, J)[2]\right)$$

and the *Shafarevich-Tate group* of $J/\mathbb{Q}$ as

$$Ш(J/\mathbb{Q}) = \bigcap_v \ker\left(H^1(G, J) \to H^1(G_v, J)\right).$$

By the above, there is an exact sequence

$$0 \to J(\mathbb{Q})/2J(\mathbb{Q}) \to \mathrm{Sel}_2(J/\mathbb{Q}) \to Ш(J/\mathbb{Q})[2] \to 0. \tag{2}$$

According to [37, Proposition C.4.2 (b)], the 2-Selmer group is actually contained in the subgroup $H^1(G, J[2]; S)$ consisting of classes that are unramified outside S, where S is the set of places consisting of the archimedean place and the primes dividing $2 \cdot \mathrm{disc}(f)$. By [37, Proposition C.4.2 (a)], $H^1(G, J[2]; S)$ is finite, hence $\mathrm{Sel}_2(J/\mathbb{Q})$ is finite as well. In constrast, the Shafarevich-Tate group $Ш(J/\mathbb{Q})$ is a torsion group which is conjectured (but in general not proved) to be finite. If it were known to be finite for J, then we would have an algorithm for the computation of r.

2.2. *Bounding the rank*

The exactness of the sequence (2) implies that $J(\mathbb{Q})/2J(\mathbb{Q})$ is finite, because $\mathrm{Sel}_2(J/\mathbb{Q})$ is finite; it also implies the formula

$$r = \dim \mathrm{Sel}_2(J/\mathbb{Q}) - \dim Ш(J/\mathbb{Q})[2] - \dim J(\mathbb{Q})[2] \tag{3}$$

for the rank, since

$$r = \dim J(\mathbb{Q})/2J(\mathbb{Q}) + \dim J(\mathbb{Q})[2]$$

by Theorem 1.7. Here and in the following, all dimensions are dimensions as $\mathbb{F}_2$-vector spaces. By (3), we can find an upper bound on r if we can compute $\dim \mathrm{Sel}_2(J/\mathbb{Q})$ and $\dim J(\mathbb{Q})[2]$: Setting

$$r' := \dim \mathrm{Sel}_2(J/\mathbb{Q}) - \dim J(\mathbb{Q})[2],$$

we have $r' \geq r$ by (3).

The 2-torsion subgroup of $J(\mathbb{Q})$ is trivial to compute using the following result.

Lemma 2.1. *Suppose that d is odd or that both g and d are even. Let k be an extension field of $\mathbb{Q}$ and let m_k denote the number of irreducible factors of f over k. Then we have*

$$J(k)[2] \cong (\mathbb{Z}/2\mathbb{Z})^{m_k - 1}$$

if d is odd or if all irreducible factors of f have even degree and we have

$$J(k)[2] \cong (\mathbb{Z}/2\mathbb{Z})^{m_k - 2}$$

otherwise.

Proof. See the proof of [63, Proposition 3.2] and of Lemmas 6.1 and 12.9 in [60]. □

Hence we obtain an algorithm for bounding the rank r of $J(\mathbb{Q})$ from above by r', if we can compute the dimension of $\mathrm{Sel}_2(J/\mathbb{Q})$. We will discuss an algorithm for this computation in Section 2.4. Unfortunately, as of yet no one has come up with an algorithm for the computation of $\dim Ш(J/\mathbb{Q})[2]$, so that at present the above does not yield an algorithm for the computation of r.

To get a lower bound on r we can try to search for r' (or $r' - d$, if we can show $\dim Ш(J/\mathbb{Q})[2] \geq d$ somehow) independent nontorsion points in $J(\mathbb{Q})$. If successful, this both proves that $r = r'$ (resp. $r = r' - d$) and provides us with generators of a subgroup of $J(\mathbb{Q})/J(\mathbb{Q})_{\mathrm{tors}}$ of finite index.

If we assume that the 2-part of $Ш(J/\mathbb{Q})$ is finite, then work of Poonen and Stoll [61] shows that $\dim Ш(J/\mathbb{Q})[2]$ is even in the case of odd degree d and that there is an algorithm which will determine whether $\dim Ш(J/\mathbb{Q})[2]$ is even or odd in the case of even degree. See [74, §8]. Hence we can sometimes gain a little extra information that can help us deduce r from r' if we are willing to assume the finiteness of the 2-part of $Ш(J/\mathbb{Q})$.

2.3. Principal homogeneous spaces

The elements of $\mathrm{Sel}_2(J/\mathbb{Q})$ and of $\text{Ш}(J/\mathbb{Q})$ have a geometric interpretation, see [37, §C.4]

Definition 2.2. A *principal homogeneous space* of $J/\mathbb{Q}$ is a variety $V/\mathbb{Q}$ together with a simple transitive action of J on V.

In particular, a principal homogeneous space V of $J/\mathbb{Q}$ is a *twist* of $J/\mathbb{Q}$: the varieties V and J are isomorphic over $\bar{\mathbb{Q}}$, but not necessarily over $\mathbb{Q}$.

It turns out that every element of $\mathrm{Sel}_2(J/\mathbb{Q})$ and $\text{Ш}(J/\mathbb{Q})$ can be represented by a principal homogeneous space V which is everywhere locally soluble, i.e. $V(\mathbb{Q}_v) \neq \emptyset$ for all completions $\mathbb{Q}_v$ of $\mathbb{Q}$. More precisely, $\mathrm{Sel}_2(J/\mathbb{Q})$ consists of those elements of $H^1(G, J[2]; S)$ which are everywhere locally soluble as principal homogeneous spaces; this results in an algorithm for the computation of $\mathrm{Sel}_2(J/\mathbb{Q})$ which is practical for $g = 1$ (see for instance [13, §3.6]). Cremona's program `mwrank` uses this idea; it is now also included in `Sage`. Gordon and Grant have an algorithm for the computation of $\mathrm{Sel}_2(J/\mathbb{Q})$ along these lines for a Jacobian of a genus 2 curve in [32] (see also [27]), but this is usually much less efficient than the procedure we will describe in the next section. For higher genus, using principal homogeneous spaces looks quite hopeless.

The nontrivial elements of $\text{Ш}(J/\mathbb{Q})$ are represented by principal homogeneous spaces that, in addition to being everywhere locally soluble, have no $\mathbb{Q}$-rational point. So $\text{Ш}(J/\mathbb{Q})$ measures the failure of the Hasse principle for J. If we had an algorithm for deciding whether an everywhere locally soluble principal homogeneous space of J has a $\mathbb{Q}$-rational point or not, then we would have an algorithm for the computation of r, but at this point no algorithm for this decision problem is known, even for $g = 1$.

2.4. Concrete description of the 2-Selmer group

We now present a rather down-to-earth construction of the 2-Selmer group.

We first set some notation. For simplicity, we restrict to the case of odd degree d, since the even degree case involves some additional complications, but we will sometimes remark on how the results have to be adjusted so that they hold in the case of even degree and even genus. Since $\deg(f)$ is odd, we may also assume without loss of generality that f is monic. For an extension field k of $\mathbb{Q}$ let A_k denote the étale algebra

$$A_k = k[x]/\langle f(x) \rangle \cong A_{k,1} \otimes \ldots \otimes A_{k,m_k},$$

where $A_{k,i}$ is the field $k[x]/\langle f_{k,i}(x) \rangle$ and $f = \prod_{i=1}^{m_k} f_{k,i}$ is the factorisation of f into irreducible factors over k. We let T denote the image of x in A_k, so that

$$A_k = k[T].$$

Example 2.3. If f is irreducible over k, then A_k is a field extension of k of degree $d = \deg(f)$.

Example 2.4. If f factors completely into linear polynomials $x - e_1, \ldots, x - e_d$ over k, then A_k is isomorphic to $\mathbb{Q}^d$. An explicit isomorphism is given by

$$A_k \to \mathbb{Q}^d, \quad T \mapsto (e_1, \ldots, e_d).$$

Suppose that $D = \sum_P n_P(P) \in \mathrm{Div}_C^0(k)$ is a divisor whose support does not contain a Weierstrass point. Following Schaefer [62] (who generalized earlier constructions due to Brumer and Kramer [7] for $g = 1$ and Cassels [10] for $g = 2$), we define the value of the "$x - T$-map" at D by

$$(x-T)(D) = \prod_P (x(P) - T)^{n_P} \in A_k^\times.$$

Note that we have

$$(x-T)(D_1 + D_2) = (x-T)(D_1) \cdot (x-T)(D_2)$$

for all $D_1, D_2 \in \mathrm{Div}_C^0(k)$ that have no Weierstrass points in their support.

Lemma 2.5. *Let $P \in J(k)$. Then there is a divisor $D \in \mathrm{Div}_C^0(k)$ representing P whose support does not contain a Weierstrass point.*

Proof. With a view toward computation, Schaefer [62, Lemma 2.2] gives an explicit and constructive proof of this fact, but for the proof of this result, it actually suffices to appeal to the moving lemma [37, Lemma A.2.2.5]. □

We denote the set of squares in $A_k^\times$ by

$$A_k^\square = \{\xi^2 : \xi \in A^\times\}.$$

Lemma 2.6. *The map $x - T$ induces a group homomorphism $\lambda_k : J(k) \to A_k^\times / A_k^\square$.*

Proof. By Lemma 2.5, it suffices to show that $(x-T)(D)$ is a square whenever $D \in \mathrm{Div}_C^0(k)$ is a principal divisor whose support does not contain a Weierstrass point. This follows using Weil reciprocity [62, Lemma 2.1] or from a straightforward calculation [76]. □

If we want to compute $\lambda_k(P)$ for a point $P \in J(k)$, then we can use the proof of [62, Lemma 2.2] to find a divisor of degree 0 representing P whose support does not contain a Weierstrass point. Alternatively, we can find a representative $D - \deg(D) \cdot \infty$, where D is semi-reduced by Lemma 1.18. Because λ_k is a group homomorphism, we may assume that D is irreducible over k; let (a, b) denote its Mumford representation. If a does not divide f, then we have

$$\lambda_k(P) = (-1)^{\deg(D)} a(T) \bmod A^\square,$$

and if f factors as $f = a \cdot \ell$, then we have

$$\lambda_k(P) = (-1)^{\deg(D)} a(T) + (-1)^{d - \deg(D)} \ell(T) \bmod A^\square,$$

see [76].

Proposition 2.7. *The kernel of λ_k is $2J(k)$.*

Proof. As the codomain of λ_k has exponent 2, its kernel must contain $2J(k)$. To show that it is not any bigger, one can use the Mumford representation [76]. For genus 1 or genus 2, it is possible to work explicitly with the geometric group law on J, see [10]. □

Remark 2.8. This result does not always hold for even degree and even genus. In this case, $2J(k)$ either has index 1 or 2 in the kernel of λ_k, but it is not hard to distinguish between these cases. See [60, Theorem 11.2] and [74, §5].

By Proposition 2.7, λ_k embeds $J(k)/2J(k)$ into $A_k/A_k^{\square}$. Hence, for $k = \mathbb{Q}$, we can study $J(\mathbb{Q})/2J(\mathbb{Q})$ through its image under $\lambda_{\mathbb{Q}}$. First we will exhibit a subgroup of $A_k/A_k^{\square}$ which contains the image of $J(k)/2J(k)$.

We can define a norm map from A_k to k as follows: Since A_k is a finite-dimensional commutative k-algebra, the map $m_a : A_k \to A_k$ given by $x \mapsto a \cdot x$ is k-linear for an $a \in A_k$ and we define the norm $N_{A_k/k}(a) = \det(m_a)$. Then $N_{A_k/k} : A_k^{\times} \to k^{\times}$ is obviously a group homomorphism. We set

$$H_k := \ker\left(N_{A_k/k} : A^{\times}/A^{\square} \to k^{\times}/k^{\square}\right),$$

where $k^{\square}$ is the set of squares in $k^{\times}$. This group will play an important part in our construction of $\mathrm{Sel}_2(J/\mathbb{Q})$.

Example 2.9. If A_k is a field, then $N_{A_k/k}$ is the usual norm associated to the field extension A_k/k .

Example 2.10. If $A_k \cong k^d$, then we have $N_{A_k/k}(\xi_1,\ldots,\xi_d) = \xi_1 \cdots \xi_d \bmod k^{\square}$. Hence $H_k \cong (k/k^{\square})^{d-1}$.

More generally, if $s(T) \in A_k$ for some $s \in k[x]$, then $N_{A_k/k}(s(T) \bmod A_k^{\square})$ is equal to the resultant $\mathrm{Res}(s,f)$ of s and f, see [76].

Lemma 2.11. *The image of λ_k is contained in H_k.*

Proof. We can represent P by a divisor $D - \deg(D) \cdot \infty$, where D is semi-reduced and has support disjoint from the set of Weierstrass points. By linearity, we may assume that D is irreducible over k; let (a,b) denote its Mumford representation. Then one computes

$$N_{A_k/k}(\lambda_k(P)) = N_{A_k/k}((-1)^{\deg(D)}a(T)) = \mathrm{Res}(a,b)^2.$$

See [76]. □

Example 2.12. Suppose that $f = \prod_{i=1}^{d}(x - e_i)$ factors completely over k and let $P \in J(k)$ be represented by $D = (x_p, y_p) - \infty$, where $(x_P, y_P) \in C(k)$. Then we have

$$\lambda_k(P) = (x_p - e_1, \ldots, x_p - e_d) \bmod A_k^{\square},$$

if $y_P \neq 0$. If $y_P = 0$, then $x_P = e_i$ for some i and we get

$$\lambda_k(P) = (l_1, \ldots, l_d) \bmod A_k^{\square},$$

where $l_j = e_i - e_j$ for $j \neq i$ and l_i is determined by the condition that the product $l_1 \cdots l_d$ must be a square.

Remark 2.13. An analogue of Lemma 2.11 also holds when the degree and the genus are even, but in this situation we have to adjust the definition of H_k. See [74, §5].

To ease notation, we will drop all $\mathbb{Q}$'s in subscripts, denoting $H_{\mathbb{Q}}$ by H and so on. We will also use v as a shorthand for $\mathbb{Q}_v$ in subscripts, denoting $H_{\mathbb{Q}_v}$ by H_v etc.

Letting ρ_v denote the natural map $H \to H_v$ induced by the injection $\mathbb{Q} \hookrightarrow \mathbb{Q}_v$, we get a commutative diagram

$$\begin{tikzcd}
J(\mathbb{Q}) \arrow[r, "\lambda"] \arrow[d] & H \arrow[d, "\rho_v"] \\
J(\mathbb{Q}_v) \arrow[r, "\lambda_v"] & H_v
\end{tikzcd}$$

for every place v of $\mathbb{Q}$. By the commutativity, we see that if $\xi \in H$ can be written as $\lambda(P)$ for some $P \in J(\mathbb{Q})$, then $\rho_v(\xi)$ is also in the image of λ_v. Hence the image of λ is contained in

$$\{\xi \in H : \rho_v(\xi) \in \operatorname{im}(\lambda_v) \text{ for all } v\}.$$

Theorem 2.14. *The 2-Selmer group satisfies*

$$\operatorname{Sel}_2(J/\mathbb{Q}) \cong \{\xi \in H : \rho_v(\xi) \in \operatorname{im}(\lambda_v) \textit{ for all } v\}. \tag{4}$$

Proof. This result follows from Theorems 1.1 and 1.2 of [62]. □

Remark 2.15. If d and g are even, then one defines the "fake" 2-Selmer group $\operatorname{Sel}_2^{\text{fake}}(J/\mathbb{Q})$ of $J/\mathbb{Q}$ using a similar commutative diagram. Then either $\operatorname{Sel}_2^{\text{fake}}(J/\mathbb{Q}) \cong \operatorname{Sel}_2(J/\mathbb{Q})$ or $\dim \operatorname{Sel}_2^{\text{fake}}(J/\mathbb{Q}) = \operatorname{Sel}_2(J/\mathbb{Q}) + 1$, see [60, Theorem 9.4].

Theorem 2.14 does not guarantee that the 2-Selmer group is finite. However, it turns out that there is a finite subgroup of H which already contains an isomorphic copy of $\operatorname{Sel}_2(J/\mathbb{Q})$. Note that in the cohomological setting, one proves finiteness of $\operatorname{Sel}_2(J/\mathbb{Q})$ by showing that it is contained in the finite group $H^1(G, J[2]; S)$ consisting of classes that are unramified outside S, where

$$S = \{\infty, 2\} \cup \{p : p \mid \operatorname{disc}(f)\};$$

see the discussion following (2). In our more concrete setting we define H_S as the subgroup of H consisting of elements ξ that have a representative $(\xi_1, \ldots, \xi_m)$ such that for all i, ξ_i is a $\mathfrak{p}$-adic unit for all primes $\mathfrak{p}$ of A_i not above S. Equivalently, an element $\xi \in H$ lies in H_S if and only if every representative $(\xi_1, \ldots, \xi_m)$ of ξ satisfies the following: For all i, $A_i(\sqrt{\xi_i})/A_i$ is ramified only at primes above S.

Proposition 2.16. *We have*

$$\operatorname{Sel}_2(J/\mathbb{Q}) \cong \{\xi \in H_S : \rho_v(\xi) \in \operatorname{im}(\lambda_v) \textit{ for all } v \in S\}.$$

Proof. The first step is to show that if p is an odd prime not dividing $\operatorname{disc}(f)$, then the image of λ_p in H_p lies in the subgroup H_p^0 consisting of those elements which can be represented by a tuple consisting solely of units. Therefore λ maps $\operatorname{Sel}_2(J/\mathbb{Q})$ into H_S. The proof is finished by showing that $\lambda_p(J(\mathbb{Q}_p)) = H_p^0$ for every odd prime $p \notin S$. See [74, Theorem 5.8]. □

Corollary 2.17. *The 2-Selmer group* $\operatorname{Sel}_2(J/\mathbb{Q})$ *is finite.*

By Proposition 2.7, the map $\lambda = \lambda_{\mathbb{Q}}$ induces an injection $J(\mathbb{Q})/2J(\mathbb{Q}) \hookrightarrow \operatorname{Sel}_2(J/\mathbb{Q})$. Hence we find:

Corollary 2.18. *The group* $J(\mathbb{Q})/2J(\mathbb{Q})$ *is finite.*

Remark 2.19. In fact we can shrink the set S by restricting to the set

$$S' = \{\infty, 2\} \cup \{p : \mathrm{ord}_p(\mathrm{disc}(f))) > 1\};$$

then we have

$$\mathrm{Sel}_2(J/\mathbb{Q}) \cong \{\xi \in H_{S'} : \rho_v(\xi) \in \mathrm{im}(\lambda_v) \text{ for all } v \in S'\}$$

by [74, Proposition 4.6]. For the proof, Stoll relates the image of $J(\mathbb{Q}_p)$ under λ_p to the image of $\Phi(\mathbb{F}_p)$ in $\Phi/2\Phi$ for an odd prime p, where Φ is the component group of the Néron model of J over $\mathbb{Z}_p$. But Φ is trivial if $\mathrm{ord}_p(\mathrm{disc}(f)) \leq 1$.

2.5. *Computing the 2-Selmer group*

We keep the assumption that f is odd and monic. In this case we obtain the following algorithm for the computation of $\mathrm{Sel}_2(J/\mathbb{Q})$:

1. Compute the set S'.
2. Compute generators for the group $H_{S'}$.
3. For every $v \in S'$, compute $\lambda_v(J(\mathbb{Q}_v)) \subset H_v$.
4. For every $v \in S'$, compute $\ker(\rho_v : H_{S'} \to H_v)$.
5. Compute $\mathrm{Sel}_2(J/\mathbb{Q}) \cong \bigcap_{v \in S'} \rho_v^{-1}(\lambda_v(J(\mathbb{Q}_v)))$.

The first step is easy: Since we have to factor f anyway to find A, we can use the discriminants of and resultants between the various factors to obtain a factorisation of $\mathrm{disc}(f)$.

If f factors completely over $\mathbb{Q}$, then the second step is particularly simple. In this case, suppose that $S' = \{\infty, p_1, \dots, p_m\}$. By Example 2.10, we have

$$H \cong (\mathbb{Q}^\times/\mathbb{Q}^\square)^{d-1} = (\mathbb{Q}^\times/\mathbb{Q}^\square)^{2g},$$

and hence

$$H_{S'} \cong \mathbb{Q}(S')^{d-1},$$

where $\mathbb{Q}(S') = \langle -1, p_1, \dots, p_m \rangle \subset \mathbb{Q}^\times/\mathbb{Q}^\square$.

For step 3 we use the following result:

Lemma 2.20. *Let m_v be the number of irreducible factors of f over $\mathbb{Q}_v$. Then we have*

$$\dim \lambda_v(J(\mathbb{Q}_v)) = m_v - 1 + \begin{cases} g, & \text{if } v = 2 \\ 0, & \text{if } v \notin \{2, \infty\} \\ -g, & \text{if } v = \infty \end{cases}.$$

Proof. See [74, Lemma 4.4, Lemma 4.8], recalling that $\dim J(\mathbb{Q}_v)[2] = m_v$ by Lemma 2.1. □

So we know a priori the size of $\mathrm{im}\,\lambda_v$. Our strategy is to pick points $P \in J(\mathbb{Q}_v)$ until the set of images $\lambda_v(P)$ generates an $\mathbb{F}_2$-vector space having the correct dimension. We can compute $\lambda_v(P)$ using resultants or, if P is the image of a $\mathbb{Q}_v$-rational point on C under the embedding $\iota : C \hookrightarrow J$, using Example 2.12. In practice, we usually start by looking for $\mathbb{Q}$-rational points on J; this is often sufficient to generate $\lambda_v(J(\mathbb{Q}_v))$. In this case we get some simplifications, see Example 2.6 below.

Steps 4 and 5 are simply linear algebra over $\mathbb{F}_2$, and we will not discuss them further.

Remark 2.21. If g and d are both even, then a method analogous to the one outlined above will give us the fake 2-Selmer group.

Remark 2.22. If f does not factor completely, then we have to use (and hence compute) information about the number fields A_i, such as the class groups and generators of the unit groups. We also need to find generators of principal ideals. See [74, §4]. This is possible for number fields of moderate degree, but becomes infeasible when these degrees are too large.

Remark 2.23. If f is defined over a number field k, then the 2-Selmer group can be defined and computed in an analogous manner.

More details on the 2-descent algorithm for Jacobians of hyperelliptic curves can be found in Stoll's paper [74]. It is implemented in `Magma`.

2.6. *Example*

Consider

$$f(x) = x(x-2)(x+2)(x+3)(x+7)$$

and the curve C of genus 2 defined by

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

In this case we have

$$A = A_{\mathbb{Q}} = \mathbb{Q}[T]/\langle f(T)\rangle \cong \mathbb{Q}^5,$$

a possible isomorphism given by

$$T \mapsto (0,2,-2,-3,-7).$$

The discriminant of f factors as $2^{12}\cdot 3^6 \cdot 5^4 \cdot 7^2$, so we take $S' = S = \{2,3,5,7,\infty\}$. Then we have

$$\mathbb{Q}(S) = \langle -1,2,3,5,7\rangle \subset \mathbb{Q}^\times/\mathbb{Q}^\square$$

and

$$H_S = \{(\xi_1,\dots,\xi_5) \;:\; \xi_1,\dots,\xi_5 \in \mathbb{Q}(S),\;\; \xi_1\cdots\xi_5 \in \mathbb{Q}^\square\} \cong \mathbb{Q}(S)^4.$$

Because the Weierstrass points are $\mathbb{Q}$-rational, we have

$$J(k)[2] \cong (\mathbb{Z}/2\mathbb{Z})^4$$

for all fields k extending $\mathbb{Q}$ by Lemma 2.1. In addition to the Weierstrass points, a quick search reveals some further points

$$(-1,\pm 6),(-4,\pm 12),(3,\pm 30),(-6,\pm 24),(-7,\pm 210) \in C(\mathbb{Q}).$$

We let G denote the subgroup of $J(\mathbb{Q})$ generated by $J(\mathbb{Q})[2]$ and the points $Q_1 = [(-1,6)-\infty]$ and $Q_2 = [(-4,12)-\infty]$. Its image $\lambda(G) \subset H$ is generated by the following elements, computed using Example 2.12:

$$\begin{aligned}
\lambda((0,0)-\infty) &= (-21,-2,2,3)\\
\lambda((2,0)-\infty) &= (2,10,1,5)\\
\lambda((-2,0)-\infty) &= (-2,-1,10,1)\\
\lambda((-3,0)-\infty) &= (-3,-5,-1,-15)\\
\lambda((-1,6)-\infty) &= (-1,-3,1,2)\\
\lambda((-4,12)-\infty) &= (-1,-6,-2,-1)
\end{aligned}$$

As $\lambda(G)$ can be shown to have rank 6 using elementary linear algebra over $\mathbb{F}_2$, we find

$$\dim \mathrm{Sel}_2(J/\mathbb{Q}) \geq 6. \tag{5}$$

We will show that $\mathrm{Sel}_2(J/\mathbb{Q}) \cong G$, so that we actually have equality in (5).

Next we compute $\lambda_3(J(\mathbb{Q}_3))$, which is four-dimensional according to Lemma 2.20. We find that the following elements of H_3 are independent, hence they generate $\operatorname{im}\lambda_3$:

$$\begin{aligned}
\lambda_3((0,0)-\infty) &= (3,1,-1,3)\\
\lambda_3((2,0)-\infty) &= (-1,1,1,-1)\\
\lambda_3((-2,0)-\infty) &= (1,-1,1,1)\\
\lambda_3((-1,6)-\infty) &= (-1,-3,1,-1).
\end{aligned}$$

Here we use the classes of $1,-1,3,-3$ as generators of $\mathbb{Q}_3^\times/\mathbb{Q}_3^\square$. Note that we only need points in G to generate $\operatorname{im}\lambda_3$; thus there is a surjection from $\lambda(G)$ onto $\operatorname{im}\lambda_3$ and every element in the image of $\mathrm{Sel}_2(J/\mathbb{Q})$ under λ must be of the form $\xi\cdot\eta$, where $\xi\in\lambda(G)$ and $\eta\in\ker\rho_3$.

We leave the task of completing the computation of $\ker\rho_v$ and $\operatorname{im}\lambda_v$ for $v\in S$ to the reader. These computations reveal $\lambda_v(J(\mathbb{Q}_v)) = \lambda_v(G)$ for all $v\in S$, so that

$$\mathrm{Sel}_2(J/\mathbb{Q}) = \bigcap_{v\in S}\rho_v^{-1}(\lambda_v(J(\mathbb{Q}_v))) = \bigcap_{v\in S}\langle\ker\rho_v,\lambda(G)\rangle.$$

Using linear algebra over $\mathbb{F}_2$, we can show

$$\bigcap_{v\in S}\langle\ker\rho_v,\lambda(G)\rangle = \lambda(G),$$

which suffices to prove $\mathrm{Sel}_2(J/\mathbb{Q})\cong\lambda(G)$ and implies $\dim\mathrm{Sel}_2(J/\mathbb{Q}) = 6$. It follows that

$$r = 6-4 = 2.$$

Actually we know a little more: The subgroup $\langle Q_1,Q_2\rangle$ of $J(\mathbb{Q})/J(\mathbb{Q})_{\mathrm{tors}}$ generated by Q_1 and Q_2 is *saturated* at 2, meaning that the index of $\langle Q_1,Q_2\rangle$ in $J(\mathbb{Q})/J(\mathbb{Q})_{\mathrm{tors}}$ is not divisible by 2.

2.7. *Other methods for bounding the rank*

There are several alternative methods available for the computation of the rank, but most of them are not as well-developed as 2-descent. The results summarized in Section 2.1 hold in a much more general context (with some slight modifications), see [37, Appendix C.4]: We can replace J by an arbitrary abelian variety A defined over a number field and we can replace the multiplication-by-2 map $[2] : J \to J$ by any rational isogeny $\varphi : A \to B$, where B is another abelian variety. For instance, when $C/\mathbb{Q}$ is an elliptic curve with rational 2-torsion, the map $[2]$ factors as $[2] = \hat{\varphi} \circ \varphi$, where $\varphi : C \to C'$ is a rational isogeny and $\hat{\varphi}$ is the dual isogeny of φ. In this case it is often possible to bound the rank by computing $\dim \mathrm{Sel}_{\varphi}(J/\mathbb{Q})$, cf. [13, §3.6]. Alternatively, we can use N-descent (cf. [14,15,16]), or descent by rational N-isogeny for some $N > 2$, see for instance [48].

For algorithms to bound the rank when $g = 2$ which rely on isogenies other than $[2]$ see [24] and [58].

If we are willing to assume the validity of the conjecture of Birch and Swinnerton-Dyer (cf. [79]), then there is an actual algorithm for the computation of r (and of generators for $J(\mathbb{Q})$). Such an algorithm was first described by Manin [46]; it is outlined in [37, §F.4.1]. The paper [31] contains further details and the description of an implementation. The conjecture of Birch and Swinnerton-Dyer asserts that r is equal to $\mathrm{ord}_{s=1} L_J(s)$, where L_J is the complex L-function associated to J, see [37, §F.4.1]. This function can often be computed in practice. The conjecture is known to hold, for instance, when J is an elliptic curve and $\mathrm{ord}_{s=1} L_J(s) \leq 1$ due to work of Gross-Zagier [35] and Kolyvagin [43] (then we also know that $\text{Ш}(J/\mathbb{Q})$ is finite), but beyond this we don't know much at all.

At present it is not even known that L_J, which a priori is only defined for $\Re(s) > 3/2$, can be analytically continued to all of $\mathbb{C}$. If J is *modular* in the sense that it is a quotient of the Jacobian $J_1(N)$ of the modular curve $X_1(N)$ for some N, then analytic continuation is known. For such Jacobians, there is a different method for bounding the rank from above: We can associate a p-adic L-function $L_{J,p}$ to J for suitable primes p; there is then a p-adic version of the conjecture of Birch and Swinnerton-Dyer, stating that (at least when p is a prime of good and ordinary reduction) the rank r is equal to the order of vanishing of the p-adic L-function at the critical value $s = 1$, see [47,1]. The great advantage of the p-adic approach is that one direction of the conjecture has been proved by Kato [42]: We know that $r \leq \mathrm{ord}_{s=1} L_{J,p}$, giving us an honest algorithm for bounding r from above and this bound can be better than the upper bound computed using 2-descent (or even possible to compute when 2-descent is not feasible). See [70] for a discussion of the case of elliptic curves and extensive numerical experiments.

3. The torsion subgroup

In this section, we discuss the computation of the torsion subgroup. To this end, we use the technique of reduction.

Suppose that p is an odd prime number and that C is a hyperelliptic curve of genus g over $k = \mathbb{Q}_p$, given by a model

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

in the projective plane over $\mathbb{Q}_p$ with weights $1, g+1, 1$ assigned to the variables X,Y,Z, respectively. We assume, without loss of generality, that F has coefficients in $\mathbb{Z}_p$.

We can then reduce the curve C modulo p as follows: Let $\tilde{F}(X,Z) \in \mathbb{F}_p[X,Z]$ denote the binary form of homogeneous degree $2g+2$ obtained by reducing the coefficients of F modulo p. We call the curve $\tilde{C}$ defined by

$$Y^2 = \tilde{F}(X,Z)$$

the *reduction* of C modulo p. Then $\tilde{C}$ need not be hyperelliptic; it might be singular and, in addition, reducible or non-reduced. We say that C has *good reduction* if $\tilde{C}$ is a hyperelliptic curve. As $\operatorname{disc}(\tilde{F}) = \operatorname{disc}(F) \bmod p$, the curve C has good reduction if and only if $\operatorname{disc}(F) \in \mathbb{Z}_p^\times$.

Suppose now that C has good reduction and let $\tilde{J}$ denote the Jacobian of $\tilde{C}$. We can define a reduction map $\mathrm{red} : C(\mathbb{Q}_p) \to \tilde{C}(\mathbb{F}_p)$ as follows: For $P \in C(\mathbb{Q}_p)$ choose a set of coordinates $(X,Y,Z) \in \mathbb{Z}_p^3$ such that at least one of the entries is a unit. Then we define

$$\mathrm{red}(P) := (X \bmod p : Y \bmod p : Z \bmod p) \in \tilde{C}(\mathbb{F}_p).$$

We extend this to a group homomorphism $\mathrm{red} : \mathrm{Div}_C(\mathbb{Q}_p) \to \mathrm{Div}_{\tilde{C}}(\mathbb{F}_p)$ by linearity. It turns out that the reduction morphism respects the degree and sends a principal divisor to a principal divisor, so that it induces a group homomorphism

$$\mathrm{red} : J(\mathbb{Q}_p) \to \tilde{J}(\mathbb{F}_p). \tag{6}$$

Remark 3.1. There is also a more intrinsic notion of good reduction for the Jacobian itself (see [65]) in terms of the special fiber of the Néron model of J, but we shall not need it. If C has good reduction, then so does J, but the converse is not always true.

Let $J(\mathbb{Q}_p)_1$ denote the kernel of the reduction morphism (6). Then we have an exact sequence

$$\begin{tikzcd} 0 \arrow[r] & J(\mathbb{Q}_p)_1 \arrow[r] & J(\mathbb{Q}_p) \arrow[r, "\mathrm{red}"] & \tilde{J}(\mathbb{F}_p) \arrow[r] & 0, \end{tikzcd}$$

so $J(\mathbb{Q}_p)_1$ has finite index in $J(\mathbb{Q}_p)$. Here we are using that C has good reduction; otherwise the definition (6) of the reduction morphism still makes sense, but it need not be surjective any longer. We have the following precise description of the group structure of the kernel of reduction:

Proposition 3.2. *There is a group isomorphism $J(\mathbb{Q}_p)_1 \cong \mathbb{Z}_p^g$. In particular, the kernel of reduction is torsion-free.*

Proof. The usual proof establishes a relation between $J(\mathbb{Q}_p)_1$ and a formal group over $\mathbb{Z}_p$. For elliptic curves, such a proof can be found in Silverman's book [67]. The case of genus 2 is treated in [11, §7.4], but the argument is easily generalized to arbitrary genus. □

Propisition 3.2 immediately implies:

Corollary 3.3. *The reduction morphism* (6) *is injective on torsion.*

Now suppose that $C : Y^2 = F(X,Z)$ is a hyperelliptic curve of genus g defined over $\mathbb{Q}$ and suppose without loss of generality that $F \in \mathbb{Z}[X,Z]$. We say that a prime p is a *prime of good reduction for C* or that C *has good reduction at* p if $C \otimes \mathbb{Q}_p$ has good reduction. Otherwise we call p a *prime of bad reduction for C* and we say that C *has bad reduction at* p. We see that C has good reduction at p if and only if $p \nmid 2\operatorname{disc}(F)$.

The torsion subgroup $J(\mathbb{Q})_{\mathrm{tors}}$ obviously injects into $J(\mathbb{Q}_p)_{\mathrm{tors}}$, so using Corollary 3.3 we conclude:

Corollary 3.4. *The reduction morphism $J(\mathbb{Q})_{\mathrm{tors}} \to \tilde{J}(\mathbb{F}_p)$ is injective. In particular, $J(\mathbb{Q})_{\mathrm{tors}}$ is finite and is isomorphic to a subgroup of $\tilde{J}(\mathbb{F}_p)$.*

This gives us a method for computing the torsion subgroup of $J(\mathbb{Q})$, or at least narrowing down the number of possibilities: List all primes $p_1,\dots,p_n$ of good reduction up to some bound B and compute $\tilde{J}(\mathbb{F}_{p_i})$ for $i=1,\dots,n$ (or at least the order of the group). If $J(\mathbb{Q})$ is trivial, then this can often be detected at this stage:

Example 3.5. Let $f(x)=x^7+x^3+1$. Then the discriminant of f factors as $5\cdot 41\cdot 4051$, so $p=3$ and $p=7$ are primes of good reduction for the hyperelliptic genus 3 curve C given by $y^2=f(x)$. We compute $\tilde{J}(\mathbb{F}_3)\cong\mathbb{Z}/36\mathbb{Z}$ and $\tilde{J}(\mathbb{F}_7)\cong\mathbb{Z}/229\mathbb{Z}$. Therefore $J(\mathbb{Q})_{\mathrm{tors}}$ is trivial by Corollary 3.4.

In general, however, this process will leave us with a finite list of abstract finite abelian groups that $J(\mathbb{Q})_{\mathrm{tors}}$ could be isomorphic to. We then have to find elements of $J(\mathbb{Q})_{\mathrm{tors}}$ to decide on the correct group.

Example 3.6. Consider the curve C of genus 2 defined by

$$y^2=f(x)=x(x-2)(x+2)(x+3)(x+7),$$

In Section 2.6 we saw that 11 and 13 are primes of good reduction. We find $\tilde{J}(\mathbb{F}_{11})\cong(\mathbb{Z}/2\mathbb{Z})^3\times\mathbb{Z}/22\mathbb{Z}$ and $\tilde{J}(\mathbb{F}_{13})\cong(\mathbb{Z}/2\mathbb{Z})^3\times\mathbb{Z}/30\mathbb{Z}$. Therefore $J(\mathbb{Q})_{\mathrm{tors}}$ is isomorphic to a subgroup of $(\mathbb{Z}/2\mathbb{Z})^4$. But the 2-torsion subgroup $J(\mathbb{Q})[2]$ is already isomorphic to $(\mathbb{Z}/2\mathbb{Z})^4$ because of Lemma 2.1; thus we conclude $J(\mathbb{Q})_{\mathrm{tors}}\cong(\mathbb{Z}/2\mathbb{Z})^4$.

Remark 3.7. The method described in this section can also be used for hyperelliptic curves defined over a number field k: See [37, Proposition C.2.5, Theorem C.2.6] for a generalization of Proposition 3.2 and Corollary 3.3 to this more general situation: The kernel of reduction (over the completion of k at a prime $\mathfrak{p}$ dividing the prime number p) is isomorphic to a formal group and has no prime-to-p torsion. Therefore combining information at primes of different residue characteristic will often suffice to compute $J(k)_{\mathrm{tors}}$.

Note that this approach does not yield an actual algorithm for the computation of $J(\mathbb{Q})_{\mathrm{tors}}$, but it does work very well in practice. In particular, it does not require a factorisation of $\mathrm{disc}(F)$. See [11, §8.2] for more complicated examples and further discussion. Also note that in the examples above, we did not actually need to know the group structure of $\tilde{J}(\mathbb{F}_p)$; the number of points was already sufficient to find $J(\mathbb{Q})_{\mathrm{tors}}$. For $g=2$, this number can be computed as

$$\#\tilde{J}(\mathbb{F}_p)=\frac{1}{2}\left(\#\tilde{C}(\mathbb{F}_{p^2})+\#\tilde{C}(\mathbb{F}_p)^2\right)-p;$$

for other genera, a similar expression can be obtained from the characteristic polynomial of the Frobenius morphism on $\tilde{C}$. However, it usually suffices to consider only a few small primes of good reduction, so naive techniques will usually suffice to compute $\tilde{J}(\mathbb{F}_p)$ as an abelian group.

If C is an elliptic curve, then we can also use the theorem of Nagell-Lutz, which says that if $P=(x,y)\in C(\mathbb{Q})$ is a torsion point, then x and y are integers and either $y=0$ or $y^2\mid\mathrm{disc}(f)$, leading to an obvious algorithm. In practice this is usually slower than the approach discussed above and, moreover, requires the factorisation of $\mathrm{disc}(f)$; this computation might not be feasible when the coefficients of f are large. No analogue of Nagell-Lutz is known in higher genus.

In the genus 2 situation, Stoll has turned the reduction-based approach presented above into an algorithm using the theory of heights on J, discussed in Section 4. See [73, §11].

For elliptic curves over number fields (including $\mathbb{Q}$), the computation of the torsion subgroup is implemented in `Magma`, `Pari/GP`, and `Sage`. A complete implementation for curves of genus 2 over $\mathbb{Q}$ exists in `Magma`, but even for higher genus hyperelliptic curves defined over number fields, the computations are often rather easy.

4. Heights and saturation

We now construct the canonical height $\hat{h}$ on $J(\mathbb{Q})$ needed for the proof of Theorem 1.7 and show how it can be used to compute generators of the Mordell-Weil group $J(\mathbb{Q})$.

4.1. Heights on projective space

In general, height functions are supposed to measure the arithmetic complexity of a geometric object defined over a global field. We first define a height function on projective space $\mathbb{P}^N(\mathbb{Q})$ by

$$h((X_0 : \ldots : X_N)) := \log \max\{|X_i| : i \in \{0, \ldots, N\}\},$$

where $X_0, \ldots, X_N$ are integers satisfying $\gcd(X_0, \ldots, X_N) = 1$. So the height of a point $P \in \mathbb{P}^N(\mathbb{Q})$ tells us how much "space" is needed to write down coordinates of P.

Remark 4.1. Defining a height function h on $\mathbb{P}^N(k)$ for some number field k is also possible, but a little more cumbersome. See [37, §B.2].

4.2. The Kummer variety

We let C denote a hyperelliptic curve of genus g over a field k of characteristic $\neq 2$, given by an equation $Y^2 = F(X,Z)$ as in (1). We do not assume that $d = \deg(f)$ is odd.

In order to define a height function on a projective variety V, one typically pulls back the height just defined along a suitable morphism from V to some projective space. In our situation we could, of course, simply make use of an embedding $J \hookrightarrow \mathbb{P}^{4^g-1}$, but we already remarked in Section 1.5 that it is rather unpleasant (or, when $g \geq 3$, outright infeasible) to use such an embedding for explicit computations. Instead we try to cut down the embedding degree by first looking for a suitable quotient of J that can be embedded into projective space.

By [2, §4.8] the quotient of J by the map taking a point to its inverse is a projective variety.

Definition 4.2. The quotient $\mathscr{K} = J/\{\pm 1\}$ is called the *Kummer variety* of J.

Lemma 4.3. *The Kummer variety can be embedded into $\mathbb{P}^{2^g-1}$ over k and its image is generated by relations of degree at most 4.*

Proof. For the first assertion, see [56]. The second assertion has certainly been well-known for a long time, but the first published seems to appear in [54]. □

For the following, we fix a morphism $\kappa : J \to \mathbb{P}^{2^g-1}$ over k such that κ factors through the canonical surjection $J \to \mathscr{K}$. The image $\kappa(J)$ is then a model for $\mathscr{K}$ in $\mathbb{P}^{2^g-1}$, and we identify $\mathscr{K}$ with $\kappa(J)$. Moreover, we add the normalization condition

$$\kappa(O) = (0 : \ldots : 0 : 1),$$

where $O \in J(k)$ is the zero element.

Example 4.4. If C is an elliptic curve, then $\mathscr{K} = \mathbb{P}^1$, and we can take κ to be the map sending an affine point $(x,y) \in E$ to x and the point $\infty \in C(k)$ at infinity to $(0 : 1)$.

Example 4.5. Suppose that $g = 2$. Then the *Kummer surface* $\mathscr{K}$ is a classical object, much studied in algebraic geometry. It can be embedded as a singular quartic hypersurface into $\mathbb{P}^3$; see Hudson's book [41] for an account of the classical theory. The Kummer surface has 16 double points (the maximal number possible for a quartic surface in $\mathbb{P}^3$ without singular curves), coming from the elements of $J[2]$. If we resolve these singularities, we get a K3-surface. Explicit formulas for the map κ and a defining equation were found by Flynn, see [23] and [11, Chapter 3]. See [19] for an analogue in characteristic 2 and [52] for formulas that work in arbitrary characteristic. A different embedding was found by Gaudry [29] for characteristic $\neq 2$ and by Gaudry-Lubicz [30] in characteristic 2. That embedding has a significant disadvantage for our purposes, though: in general it is not defined over k.

Example 4.6. If $g = 3$, then the Kummer variety can be embedded into $\mathbb{P}^7$ as an intersection of a quadric and 34 quartics. An explicit map κ was constructed in this situation by Stubbs [78] who also found 27 defining relations. A complete list of defining equations was later given in [54]. Using a different approach, Stoll [77] found different formulas for κ and its image in $\mathbb{P}^7$.

4.3. Naive and canonical height

Now suppose that the ground field k is $\mathbb{Q}$. We use the Kummer variety to define a height function on $J(\mathbb{Q})$.

Definition 4.7. The *naive height* $h : J(\mathbb{Q}) \to \mathbb{R}_{\geq 0}$ is defined by $h(P) := h(\kappa(P))$.

The naive height has the following properties:

Proposition 4.8. *(i) For every $B \in \mathbb{R}$ there are only finitely many points $P \in J(\mathbb{Q})$ such that $h(P) \leq B$.*
(ii) The function $P \mapsto h(2P) - 4h(P)$ is bounded on $J(\mathbb{Q})$.

Proof. Property (i) is immediate from the definition. See [37, Corollary B.3.4] for a proof of a much more general version of (ii). □

Property (i) of Proposition 4.8 states that h is quadratic up to a bounded function. In 1958, Néron raised the question whether there is a quadratic form on $J(\mathbb{Q})$ with bounded difference from h at the ICM in Edinburgh. Here an $\mathbb{R}$-valued *quadratic form* on $J(\mathbb{Q})$ is a function $q : J(\mathbb{Q}) \to \mathbb{R}$ such that $(P, Q) \mapsto q(P + Q) - q(P) - q(Q)$ is bilinear on $J(\mathbb{Q}) \times J(\mathbb{Q})$ and such that $q(-P) = q(P)$ for all $P \in J(\mathbb{Q})$. Néron [57] and Tate both found constructions for such a quadratic form, the canonical height. Tate's method is much shorter and easier, but Néron's approach is more suitable for explicit computations.

Definition 4.9. (Tate) The canonical height of a point $P \in J(\mathbb{Q})$ is defined by

$$\hat{h}(P) := \lim_{n\to\infty} 4^{-n} h(2^n P).$$

Note that the limit is well-defined because h is quadratic up to a bounded function. We'll come back to (a variant of) Néron's construction later on.

Theorem 4.10. *(Néron, Tate) The canonical height has the following properties:*

(i) The difference $\hat{h} - h$ is bounded.
(ii) $\hat{h}$ is a quadratic form on $J(\mathbb{Q})$.
(iii) For every $B \in \mathbb{R}$ there are only finitely many points $P \in J(\mathbb{Q})$ such that $\hat{h}(P) \leq B$.
(iv) $\hat{h}(P) \geq 0$, with equality if and only if P is torsion.

Moreover, $\hat{h}$ is the unique function $J(\mathbb{Q}) \to \mathbb{R}$ satisfying (i) and $h(2P) = 4h(P)$ for all $P \in J(\mathbb{Q})$.

Proof. The first property follows from

$$\begin{aligned}\hat{h}(P) &= \lim_{n\to\infty} 4^{-n} h(2^n P)\\ &= h(P) + \sum_{n=0}^{\infty} 4^{-(n+1)} \big(h(2^{n+1}P) - 4h(2^n P)\big).\end{aligned}$$

To show (ii), one proves that the parallelogram law

$$\hat{h}(P+Q) + \hat{h}(P-Q) = 2\hat{h}(P) + 2\hat{h}(Q)$$

holds for all $P, Q \in J(\mathbb{Q})$ by first showing that it holds for h up to a constant and then applying the limit defining $\hat{h}$, cf. [37, Theorem B.5.1]. The fact that a function satisfying the parallelogram law is a quadratic form is a standard exercise that is solved in Lemma B.5.2 of [37].

Property (iii) follows at once from the corresponding statement for h (Proposition 4.8). The nonnegativity of $\hat{h}$ is immediate as well, since h is nonnegative. But if a point $P \in J(\mathbb{Q})$ has vanishing canonical height, then the set $\{\hat{h}(nP) : n \in \mathbb{Z}\}$ is finite. By (iii), the set of multiples of P must then be finite, so P has finite order. Conversely, if $nP = O$ for some $n \geq 1$, then the quadraticity of $\hat{h}$ implies

$$\hat{h}(P) = \frac{1}{n^2}\hat{h}(O) = 0.$$

For the uniqueness statement, suppose that $h' : J(\mathbb{Q}) \to \mathbb{R}$ is a function such that there is a constant c with $h(P) - h'(P) \leq c$ for all $P \in J(\mathbb{Q})$. If h' also satisfies $h'(2P) = 4h'(P)$ for all $P \in J(\mathbb{Q})$, then

$$\left| h'(P) - \frac{h(2^n P)}{4^n} \right| \leq \frac{c}{4^n}$$

for all $n \geq 0$, so that $h'(P) = \lim_{n\to\infty} 4^{-n} h(2^n P) = \hat{h}(P)$. □

Remark 4.11. Theorem 4.10 finishes our proof of Theorem 1.7, as $\hat{h}$ has precisely the desired properties.

By parts (iii) and (v) of Theorem 4.10, the canonical height induces a positive definite quadratic form on $J(\mathbb{Q})/J(\mathbb{Q})_{\text{tors}}$. In fact more is true:

Proposition 4.12. *The canonical height can be extended $\mathbb{R}$-linearly to a positive definite quadratic form on $J(\mathbb{Q}) \otimes \mathbb{R}$.*

Proof. The extension to a quadratic form on $J(\mathbb{Q}) \otimes \mathbb{R}$ is immediate, but the positive definiteness is not quite as easy as it may sound. One can deduce it from Minkowski's theorem on lattice points in symmetric domains, see [37, Proposition B.5.3]. □

Remark 4.13. If C is defined over a number field k, then we can define the canonical height on $J(k)$ exactly as in Definition 4.9, using the naive height $h = h \circ \kappa$ (see 4.1). All results of the present section continue to hold in this more general setting.

4.4. Saturation

Now we return to the problem of computing generators of $J(\mathbb{Q})$. We assume that we already know the torsion subgroup and the rank.

Let us first dicsuss how to decide whether a set $Q_1, \dots, Q_t$ of points in $J(\mathbb{Q})$ has the property that their images in $J(\mathbb{Q})/J(\mathbb{Q})_{\text{tors}}$ are independent. By the properties of the canonical height discussed in the previous section, it suffices to check that their *regulator*

$$\operatorname{Reg}(Q_1, \dots, Q_t) := \det\left(\frac{1}{2}(\hat{h}(Q_i + Q_j) - \hat{h}(Q_i) - \hat{h}(Q_j)\right)_{1 \le i,j \le t}. \tag{7}$$

is nonzero. Alternatively (and this is usually easier), one can show independence by reduction modulo suitable small primes of good reduction. However, if $t = r$ and the points $Q_1, \dots, Q_r$ are the result of a two-descent as described in Section 2, so that the images of $Q_1, \dots, Q_r$ under the two-descent map λ are independent, then we know a priori that $Q_1, \dots, Q_r$ must be independent as well.

From now on, we shall therefore assume that we have at our disposal a set $Q_1, \dots, Q_r$ of nontorsion points whose images in $J(\mathbb{Q})/J(\mathbb{Q})_{\text{tors}}$ are independent. Then our task is to find generators of the full group $J(\mathbb{Q})/J(\mathbb{Q})_{\text{tors}}$ from its subgroup $\langle Q_1, \dots, Q_r \rangle$ of finite index. By Proposition 4.12, we can rephrase this problem in the following way: The group $J(\mathbb{Q})/J(\mathbb{Q})_{\text{tors}}$ sits as a lattice Λ in the r-dimensional Euclidean vector space $V = (J(\mathbb{Q}) \otimes \mathbb{R}, \hat{h})$ and $Q_1, \dots, Q_r$ generate a sublattice Λ' of Λ of finite index. We want to compute the *saturation* Λ of Λ'.

There are several effective approaches to this problem. The first one is due to Siksek [66] for elliptic curves; it was later adapted by Flynn and Smart [25, §8] for Jacobians of curves of genus 2. The method can be summarized as follows:

(i) Compute an upper bound N on the index n of Λ' in Λ.
(ii) Check for every prime $p \le N$ whether p divides n. If it does, enlarge Λ'.

For step (i), we need the *successive minima* of the lattice Λ, or at least positive lower bounds for them. We fix $\ell > 0$ and enumerate all points $P \in J(\mathbb{Q})$ such that $\hat{h}(P) \le \ell$. Among these points, we find independent points $R_1, \dots, R_t \in J(\mathbb{Q})$ such that

$$0 < \hat{h}(R_1) < \hat{h}(R_2) < \ldots < \hat{h}(R_t) \le \ell,$$

and such that $\hat{h}(R) > \ell$ for all non-torsion points $R \notin \langle R_1, \dots, R_t \rangle$. Then $M_i = \hat{h}(R_i)$ is the ith successive minimum of the lattice Λ for $i = 1, \dots, t$ and $M_i = \ell$ is a lower bound for the ith successive minimum for $i = t+1, \dots, r$. We define the *regulator of* $J/\mathbb{Q}$ as

$$\operatorname{Reg}(J/\mathbb{Q}) := \operatorname{Reg}(P_1, \dots, P_r), \tag{8}$$

where the images of $P_1, \dots, P_r$ generate $J(\mathbb{Q})/J(\mathbb{Q})_{\text{tors}}$. See (7) and note that this is independent of the choice of generators of $J(\mathbb{Q})/J(\mathbb{Q})_{\text{tors}}$. If the index of Λ' in Λ is n, then we have

$$\operatorname{Reg}(Q_1, \dots, Q_r) = n^2 \operatorname{Reg}(J/\mathbb{Q}).$$

By classical results from the geometry of numbers (see [59, Lemma 3.34]), we have an upper bound

$$n \le N := \sqrt{\frac{\operatorname{Reg}(Q_1, \dots, Q_r)\gamma_r^r}{M_1 \cdots M_r}},$$

where γ_r is the rth Hermite constant.

In the second stage, we check for every prime $p \mid N$, whether the lattice Λ' is already saturated at p, meaning that there is no $Q \in \Lambda \setminus \Lambda'$ such that $pQ \in \Lambda'$. Let $M = \langle Q_1, \dots, Q_r \rangle \subset J(\mathbb{Q})$. Then we try to find a set of primes q of good reduction such that $p \mid \#\tilde{J}(\mathbb{F}_q)$ and such that the kernel of the natural map

$$M/pM \to \prod_q \tilde{J}(\mathbb{F}_q)/p\tilde{J}(\mathbb{F}_q)$$

is trivial. If this is the case, then no point $Q \in J(\mathbb{Q})$ that is not already in M can satisfy $pQ \in M$, since such a point has to reduce to the identity in $\tilde{J}(\mathbb{F}_q)/p\tilde{J}(\mathbb{F}_q)$ for every prime q of good reduction. If this process is not successful, then we have to find a point $Q \notin \Lambda'$ such that $pQ \in \Lambda'$. See [25, §8] for a possible solution to this problem for $g = 2$. Having found Q, we start over with the lattice $\Lambda' := \langle Q_1, \dots, Q_r, Q \rangle$ Note, however, that in practice we usually start with a set $Q_1, \dots, Q_r$ for which we expect the index to be 1, so that this step does not often occur.

For elliptic curves, Siksek's method is implemented in `Magma`, `Pari/GP` and `Sage`.

The following alternative approach to the problem of saturation is due to Stoll [75]: Let ρ denote the *covering radius* of the lattice Λ':

$$\rho = \min\{\sqrt{\|P - \Lambda'\|_{\hat{h}}} : P \in V\}.$$

The covering radius can be computed using the *Voronoi cell* of Λ'. This is the polytope consisting of all points of V whose distance from the origin is at most the distance to any other point of Λ'. The covering radius of Λ' is then the circumradius of the Voronoi cell.

The paper [36] discusses algorithms and, in particular, the complexity of this computation, see also [20]. However, the Voronoi cell has $(r+1)!$ vertices, so its computation is inherently exponential in the rank r and becomes infeasible when r is large. Instead, Stoll proposes to split Λ' into orthogonal parts Λ'_1 and Λ'_2 of smaller rank and shows that

$$\rho^2 \leq \rho(\Lambda'_1)^2 + \rho(\Lambda'_2)^2.$$

By definition, the ball in V of radius ρ^2 around the origin contains a fundamental domain for Λ and hence a set of generators. So it suffices to compute an upper bound B for ρ^2 and to enumerate all points of canonical height bounded by B in order to find generators of Λ.

Example 4.14. Suppose that $r = 2$ and that R_1, R_2 is a Minkowski-reduced basis for Λ'. Then we have

$$\rho^2 = \frac{\hat{h}(R_1)\hat{h}(R_2)\hat{h}(R_1 \pm R_2)}{4\operatorname{Reg}(R_1, R_2)},$$

where the sign is the one that leads to a smaller value. See [75].

Note that both algorithms for saturation crucially rely on algorithms to

(a) compute $\hat{h}(P)$ for given $P \in J(\mathbb{Q})$;
(b) enumerate $\{P \in J(\mathbb{Q}) : \hat{h}(P) \leq B\}$ for given $B \in \mathbb{R}$.

From now on we assume that $g \leq 3$, so that we have explicit formulas for $\kappa : J \twoheadrightarrow \mathscr{K} \subset \mathbb{P}^{2^g-1}$ and defining equations for $\mathscr{K} \subset \mathbb{P}^{2^g-1}$. Then we can at least compute $h(P) = h(\kappa(P))$ for $P \in J(\mathbb{Q})$ and enumerate $\{P \in J(\mathbb{Q}) : h(P) \leq B'\}$ for a reasonably small bound $B' \in \mathbb{R}$. For the latter, one employs a sieving strategy to enumerate

$$\{P \in \mathscr{K}(\mathbb{Q}) : h(P) \leq B'\};$$

then one checks which of these points lift to $J(\mathbb{Q})$. Stoll has very efficient implementations for this problem for $g = 1$ (`ratpoints`, this program can actually be used to find points of bounded height on C for arbitrary g) and for $g = 2$ (`j-points`), see [72].

In the following sections, we will tackle problems (a) and (b). Note that Tate's construction of $\hat{h}$ is not suitable for the computation of $\hat{h}$, as the convergence rate is slow and the size of the coordinates grows exponentially. Instead, we will use that the difference

$$\mu := h - \hat{h}$$

is a bounded function on $J(\mathbb{Q})$ and we will decompose μ into a finite sum of local error functions μ_v.

Remark 4.15. Most of the results in the following sections continue to hold over number fields. Namely, all non-archimedean statements are still true (possibly up to a constant normalization factor), but some of the archimedean statements are currently restricted to real places.

4.5. Local error functions

In order to analyze μ, we will analyze locally how far the naive height is away from being a quadratic form. More precisely, we will decompose the function

$$P \mapsto 4h(P) - h(2P)$$

into a sum of local terms. As the naive height is defined on the Kummer variety, we need to investigate how duplication on J is reflected on $\mathscr{K}$.

The Kummer variety does not inherit the full group structure from J: If P and Q are points on J, then we cannot determine $\kappa(P+Q)$ from $\kappa(P)$ and $\kappa(Q)$ alone. However, the unordered pair $\{\kappa(P+Q), \kappa(P-Q)\}$ can be determined; hence we can find $\kappa(P+Q)$ from $\kappa(P), \kappa(Q)$ and $\kappa(P-Q)$. This observation can be used to devise a pseudo-addition algorithm on $\mathscr{K}$ which leads to an honest algorithm for addition on J if we know how to lift points from $\mathscr{K}$ to J. See [25] for such an algorithm in genus 2; a related Montgomery-ladder aproach is due to Duquesne [18]. Gaudry [29] has used his embedding of the Kummer surface (see Example 4.5) to devise a fast addition algorithm on the Jacobian, suitable for cryptographic applications.

Fortunately, we are mostly interested in duplication, which commutes with inversion and therefore does descend from J to $\mathscr{K}$.

Lemma 4.16. *There are homogeneous quartic polynomials $\delta_1, \ldots, \delta_{2^g} \in k[x_1, \ldots, x_n]$ without common nontrivial zero such that the associated map $\delta := (\delta_1, \ldots, \delta_{2^g}) : \mathbb{P}^{2^g-1} \to \mathbb{P}^{2^g-1}$ makes the following diagram commute:*

$$\begin{tikzcd} J \arrow[r, "{[2]}"] \arrow[d, "\kappa"] & J \arrow[d, "\kappa"] \\ \mathscr{K} \arrow[r, "\delta"'] & \mathscr{K}. \end{tikzcd}$$

Moreover, we have

$$\delta(0, \ldots, 0, 1) = (0, \ldots, 0, 1).$$

Explicit formulas for δ are classical for elliptic curves. For genus 2, such formulas are due to Flynn, cf. [23]. In genus 3, Stoll derives explicit formulas in [77], corresponding to his formulas for κ and confirming formulas for δ valid for the map κ constructed by Stubbs that were conjectured by the author, see [54].

To construct the local error functions μ_v, we proceed as follows: Fix polynomials $\delta_1,\dots,\delta_{2^g}$ as in Lemma 4.16 and let v be a place of $\mathbb{Q}$. For a point $P \in J(\mathbb{Q}_v)$, we define

$$\varepsilon_v(P) = -\log\max\{|\delta_j(\xi_1,\dots,\xi_{2^g})|_v : 1 \le j \le 2^g\} + 4\log\max\{|\xi_j|_v : 1 \le j \le 2^g\},$$

where $\kappa(P) = (\xi_1 : \dots : \xi_{2^g})$; the homogeneity of the quadric polynomials δ_j implies that this is independent of the choice of coordinates $(\xi_1,\dots,\xi_{2^g})$.

Lemma 4.17. *(i) The function ε_v is continuous with respect to the v-adic topology and bounded.*

(ii) We have $\varepsilon_p(P) \ge 0$ for all primes p and all $P \in J(\mathbb{Q}_p)$.

(iii) If p is a prime such that C has good reduction at p, then ε_p vanishes identically on $J(\mathbb{Q}_p)$.

(iv) We have $4h(P) - h(2P) = \sum_v \varepsilon_v(P)$ for all $P \in J(\mathbb{Q})$, where the sum is over all places of $\mathbb{Q}$.

Proof. The continuity of ε_v is immediate; hence ε_v must be bounded, as $J(\mathbb{Q}_v)$ is compact. The δ_j have integral coefficients, implying (ii). For (iii), note that reducing the equations of $\mathscr{K}$ gives the Kummer variety $\widetilde{\mathscr{K}}$ of the Jacobian $\widetilde{J}$ of the reduction $\widetilde{C}$ of C modulo p. Moreover, duplication on $\widetilde{\mathscr{K}}$ is represented by the map $\widetilde{\delta} = (\widetilde{\delta_1},\dots,\widetilde{\delta_{2^g}})$. Thus, if the second term in the definition of ε_p vanishes, then the first term must vanish as well, which proves (iii). Assertion (iv) follows immediately from the product formula for $\mathbb{Q}$. □

Since ε_v is bounded, we can define

$$\mu_v(P) = \sum_{n=0}^{\infty} 4^{-(n+1)}\varepsilon_v(2^n P). \tag{9}$$

The following properties of μ_v follow at once from the corresponding properties of ε_v listed in Lemma 4.17:

Corollary 4.18. *(i) The function μ_v is continuous with respect to the v-adic topology and bounded.*

(ii) We have $\mu_p(P) \ge 0$ for all primes p and all $P \in J(\mathbb{Q}_p)$.

(iii) If p is a prime such that C has good reduction at p, then μ_p vanishes identically on $J(\mathbb{Q}_p)$.

(iv) We have $4\mu_v(P) - \mu_v(2P) = \varepsilon_v(P)$ for all $P \in J(\mathbb{Q}_v)$.

It remains to show that the local error functions μ_v provide the promised decomposition of the difference between the naive and the canonical height.

Corollary 4.19. *If $P \in J(\mathbb{Q})$, then*

$$\hat{h}(P) = h(P) - \sum_v \mu_v(P).$$

Proof. We have

$$\begin{aligned}\hat{h}(P) &= \lim_{n\to\infty} 4^{-n} h(2^n P)\\ &= h(P) + \sum_{n=0}^{\infty} 4^{-(n+1)} \left(h(2^{n+1}P) - 4h(2^n P)\right)\\ &= h(P) - \sum_{n=0}^{\infty} 4^{-(n+1)} \sum_v \varepsilon_v(2^n P)\\ &= h(P) - \sum_v \mu_v(P).\end{aligned}$$

□

By Corollary 4.19, we get algorithms for problems (a) and (b) of Section 4.4 once we have algorithms for the following tasks, for all places v of $\mathbb{Q}$:

(A) Compute $\mu_v(P)$ for a given point $P \in J(\mathbb{Q}_v)$.
(B) Find an upper bound β_v for $\sup\{|\mu_v(P)| : P \in J(\mathbb{Q}_v)\}$.

Regarding the second problem and its relation to (b) above, note that

$$-\beta_\infty \le h(P) - \hat{h}(P) \le \sum_v \beta_v =: \beta$$

for all points $P \in J(\mathbb{Q})$ (we can take $\beta_v = 0$ for all but finitely many v by Corollary 4.18 (iii)). Therefore we can solve (b) by enumerating the set

$$\{P \in J(\mathbb{Q}) : h(P) \le B + \beta\}.$$

4.6. Computing canonical heights

We first discuss how to tackle problem (B) for a prime p of bad reduction, still assuming $g \le 3$. In this case we have the following result

Theorem 4.20. *Suppose that $g \le 3$ and let $U = \{P \in J(\mathbb{Q}_p) : \mu_p(P) = 0\}$. Then U is a subgroup of $J(\mathbb{Q}_p)$ of finite index and both μ_p and ε_p factor through the quotient $J(\mathbb{Q}_p)/U$.*

Proof. See [68] for $g = 1$, [75] for $g = 2$ and [77] for $g = 3$. The index is finite, because U contains the kernel of reduction $J(\mathbb{Q}_p)_1$. □

For elliptic curves, the subgroup U is equal to the subgroup of points in $J(\mathbb{Q}_p)$ which reduce to the connected component of the identity of the Néron model of J over $\mathbb{Z}_p$. The quotient $J(\mathbb{Q}_p)/U$ is then isomorphic to the group of rational points of the component group of the Néron model and this group can be computed easily using Tate's algorithm [69, §IV.8]. There are explicit formulas for μ_p, depending on the reduction type of C, see [68] and [17]. Another method for the computation of μ_p can be found in [81].

If $g > 1$, then in general the relation between U and the Néron model is more complicated; there are examples of points mapping into the connected component which have $\mu_p \ne 0$, see [55]. Nevertheless, Theoren 4.20 is still useful to compute μ_p and is also used for some of the bounds on μ_p discussed in Section 4.7.

In the genus 2 situation, the following algorithm for the computation of $\hat{h}(P)$ is due to Flynn and Smart [25]: Find a multiple NP such that $\mu_p(NP) = 0$ for all p and compute

$$\hat{h}(P) = \frac{1}{N^2}\left(h(NP) + \mu_\infty(NP)\right).$$

It turns out that we can find N without any integer factorisation. The drawback is that we need to compute NP as a point over $\mathbb{Q}$; but the number of coordinates of NP grows exponentially in N, making this algorithm infeasible when N is large.

Stoll remedies this in [75] by making substantial use of Theorem 4.20. Let $m = \min\{n \geq 1 : \varepsilon_p(nP) = 0\}$ and write m as $m = 2^u s$, where s is odd. Moreover, let t be the order of 2 in $(\mathbb{Z}/s\mathbb{Z})^\times$. Then we have $\varepsilon_p(2^{n+t}P) = \varepsilon_p(2^n P)$ for $n \geq u$ and hence

$$\mu_p(P) = \sum_{n=0}^{\infty} \frac{\varepsilon_p(2^n P)}{4^{n+1}} = \sum_{n=0}^{u-1} \frac{\varepsilon_p(2^n P)}{4^{n+1}} + \frac{4^{-u-1}}{1-4^{-t}} \sum_{n=0}^{t-1} \frac{\varepsilon_p(2^{u+n}P)}{4^n}. \tag{10}$$

If we want to compute $\mu_p(P)$ using (10), we need to find nP for $n \leq m$ and $\varepsilon_p(2^n P)$ for $n \leq r+t-1$ (at most). All computations can be done over $\mathbb{Q}_p$. We do have to factor $\operatorname{disc}(f)$, but this is necessary for 2-descent anyway, see Section 2.5. Compare [83] for a similar, but slightly different algorithm. We can use essentially the same approach outlined above for $g = 3$, but we have to be a little more careful here, because $\mu_p(P) = 0$ and $\varepsilon_p(P) = 0$ are not necessarily equivalent, see [77].

In [55], we introduce the following algorithm for the computation of $\mu_p(P)$, where $g = 2$ and $P \in J(\mathbb{Q}_p)$:

- Set $B = \operatorname{ord}_p(2^4 \operatorname{disc}(f))$ (then $\geq \varepsilon_p(P)/\log p$).
- Set $M = 2\max\left\{16, \left\lfloor(\operatorname{ord}_p(2^8) + B)/3\right\rfloor\right\}$.
- Set $m = \lfloor \log(BM^2/3)/\log(4) \rfloor$.
- Compute
$$\mu_0 = 4^{-m-1} \operatorname{ord}_p(\delta^{\circ(m+1)}(\xi)), \text{ where}$$
$\xi = (\xi_1, \ldots, \xi_4) \in \mathbb{Z}_p^4$ represents $\kappa(P) \in \mathscr{K}(\mathbb{Q}_p)$ and at least one ξ_i is a p-adic unit.
- Return $\mu_1 \cdot \log p$, where μ_1 is the unique fraction with denominator at most M in the interval $[\mu_0, \mu_0 + 1/M^2]$.

The fraction in the final step can be computed easily, for instance, using continued fractions. To show that the algorithm works, we prove that M is an upper bound for the denominator of the rational number $\mu_p(P)/\log p$ and that this number must be in the interval $[\mu_0, \mu_0 + 1/M^2]$.

It remains to discuss the computation of μ_∞. Assuming that we have a bound for $|\varepsilon_\infty|$, we can compute $\mu_\infty(P)$ for $P \in J(\mathbb{R})$ from its definition to any desired accuracy using floating-point arithmetic. Such a bound is due to Stoll for genus 2 and genus 3, see Section 4.7. For $g = 1$, there are better algorithms for the computation of μ_∞:

(i) Tate has an elegant series approach, see [68] for an exposition and refinement.
(ii) One can compute μ_∞ by relating it to theta-functions or sigma-functions on $E(\mathbb{C}) \cong \mathbb{C}/\Lambda$, where Λ is a lattice, and using the arithmetic-geometric mean, see [12, Algorithm 7.5.7].
(iii) The arithmetic-geometric mean can also be applied directly, and this leads to the fastest known algorithm (with quadratic convergence rate). This is due to Bost-Mestre [4], see [5, §6.1] for an exposition.

Approaches (ii) and (iii) can be generalized to $g = 2$, but it seems rather difficult to obtain fast algorithms in this way.

4.7. Bounding the difference between the canonical and the naive height

Now we turn our attention to problem (A). Let p be a prime number.

Lemma 4.21. *Let $g \in \{1,2,3\}$. Then we have*

$$\varepsilon_p(P) \le -\log|2^{2g}\operatorname{disc}(f))|_p$$

for every $P \in J(\mathbb{Q}_p)$.

Proof. For $g = 1$, this follows from the results of [17]. The statement is due to Stoll for genus 2 [73] and genus 3 [77]. His proofs use mainly representation-theoretic methods. □

Some improvements of the bound given in Lemma 4.21 are presented in [73, §7]. If we are willing to invest enough time, then we can also search for an *optimal* bound for ε_p on $\mathscr{K}(\mathbb{Q}_p)$.

Note that if γ_p is an upper bound for ε_p, then $\gamma_p/3$ is an upper bound for μ_p by the definition (9) of μ_p.

Corollary 4.22. *If $g \le 3$, then we have*

$$\mu_p(P) \le -\frac{\log|2^{2g}\operatorname{disc}(f))|_p}{3}$$

for every $P \in J(\mathbb{Q}_p)$.

We generally expect that for a "large" prime dividing $\operatorname{disc}(f))$, its multiplicity is rather small, usually equal to 1. Hence the following lemma is extremely helpful in practice.

Lemma 4.23. *Suppose that $g \le 3$ and p is an odd prime such that $\operatorname{ord}_p(\operatorname{disc}(f)) = 1$. Then μ_p is identically zero.*

Proof. See [17] for $g = 1$ and Stoll's papers [73] and [77] for $g = 2$ and $g = 3$, respectively. □

For the saturation algorithms introduced in Section 4.4 to work in practice, it is crucial to have good bounds for the height difference $\hat{h} - h$. This special importance is due to the fact that the bound shows up *exponentially* in the enumeration step, since both h and $\hat{h}$ are logarithmic heights.

If $g = 1$ and p is a prime number, then it is not difficult to find optimal bounds β_p. To compute β_p, we only need the reduction type of C and the Tamagawa number at p and both can be computed easily using Tate's algorithm, see [17].

In forthcoming work [55], we use Theorem 4.20 to show how to find optimal bounds for the most common reduction types when $g = 2$. We also show that we can take

$$\beta_p = -\frac{\log|2^8\operatorname{disc}(f))|_p}{4}. \tag{11}$$

The proof uses reduction to the case of semistable reduction, where we determine explicit formulas for μ_p and hence bounds for μ_p using the theory of Néron models and Zhang's admissible pairing [86].

Besides bounding μ_p for primes p, we also need to bound μ_∞. Bounds for μ_∞ for elliptic curves are discussed, for instance, in [17]. Recent work on this problem for $g = 1$ is due to Uchida [82] and Bruin [6]. For $g \in \{2,3\}$, an upper bound for $|\varepsilon_\infty|$ can be obtained using the methods of [73, §7]; this uses representation theory as in the proof of Lemma 4.21 and the usual archimedean triangle inequality. As for primes p, this gives us an upper bound for $|\mu_\infty|$. It is possible to significantly improve on this bound by bounding not just $|\varepsilon_\infty(P)|$, but also $|\varepsilon_\infty(2^nP)|$ for $n \ge 1$, see [55] ($g = 2$) and [77] ($g = 3$). Another way of improving the bound on $|\varepsilon_\infty|$ for $g = 2$ can be found in [83].

4.8. *Example*

Let us compute generators for the Mordell-Weil group of our running example $C : y^2 = f(x)$, where $f = x(x-2)(x+2)(x+3)(x+7)$. We showed in Section 2.6 that the Mordell-Weil rank of $J(\mathbb{Q})$ is 2 and that the points $Q_1 = [(-1,6) - \infty]$ and $Q_2 = [(-4,12) - \infty]$ generate a subgroup of $J(\mathbb{Q})/J(\mathbb{Q})_{\mathrm{tors}}$ of odd finite index. Then we determined the torsion subgroup of $J(\mathbb{Q})$ in Example 3.6: We showed that

$$J(\mathbb{Q})_{\mathrm{tors}} = J(\mathbb{Q})[2] \cong (\mathbb{Z}/2\mathbb{Z})^4$$

and the points represented by $P_i - \infty$ generate $J(\mathbb{Q})_{\mathrm{tors}}$ for any quadruple $P_1, \dots, P_4$ of distinct Weierstrass points.

It remains to saturate the finite index subgroup of $J(\mathbb{Q})/J(\mathbb{Q})_{\mathrm{tors}}$ generated by Q_1 and Q_2. For this purpose, we use `Magma`. We apply the second approach outlined in Section 4.4. First we set up the Euclidean vector space $V = (J(\mathbb{Q}) \otimes \mathbb{R}, \hat{h})$. Our goal is to saturate the lattice Λ' generated by Q_1 and Q_2 inside V. Using `Magma`, we find that Q_1 and Q_2 form a Minkowski-reduced basis of Λ', so by Example 4.14 we have

$$\rho^2 = \frac{\hat{h}(Q_1)\hat{h}(Q_2)\hat{h}(Q_1 \pm Q_2)}{4\,\mathrm{Reg}(Q_1, Q_2)}.$$

Taking $Q_1 - Q_2$ in the numerator, we get $\rho^2 = 0.314025376$. Then we compute an upper bound β for the difference $|h(P) - \hat{h}(P)|$. The methods of [75] (implemented in `Magma`) give $\beta = 9.991786718$, while the improvements presented in [55] allow us to cut this down to $\beta = 8.177347056$. However, the latter computation depends on a result from [55] which we have not yet proved rigorously.

Hence we need to search for all points in $J(\mathbb{Q})$ of naive height bounded by $\rho^2 + \beta$. Once again, we employ `Magma` for this task. Using the larger value of β, we find that there are 558 such points; the (conjectural) smaller value leaves us with 426 points. The first search took about 200 seconds, while the second took less than 0.1 seconds, showing that indeed small improvements in β (less than 20%) can lead to major savings when searching for points. In any case, we find that the classes of these points in V are already contained in Λ', so that $\Lambda = \Lambda'$. This proves that the images of Q_1 and Q_2 generate $J(\mathbb{Q})/J(\mathbb{Q})_{\mathrm{tors}}$, finishing our quest for generators of $J(\mathbb{Q})$.

4.9. *Higher genus*

What if $g > 3$? As remarked before, the methods presented above are currently not feasible – in this situation we cannot even compute the naive height, as no explicit formulas for κ are known. It is, however, still possible to compute the canonical height of a given point $P \in J(\mathbb{Q})$ by applying a completely different algorithm which relies on arithmetic intersection theory. Namely, we can use a theorem of Faltings [22] and Hriljac [40], stating that $\hat{h}(P)$ can be decomposed into a finite sum

$$\hat{h}(P) = \sum_v \langle D, E \rangle_v, \tag{12}$$

where $D, E \in \mathrm{Div}^0_C(\mathbb{Q})$ are divisors representing P and $\langle D, E \rangle_v$ is the *local Néron symbol* at a place v. For a prime number p, the local Néron symbol $\langle D, E \rangle_p$ is the intersection multiplicity between certain extensions of D and E to a regular model $\mathscr{C}$ of C over $\mathrm{Spec}(\mathbb{Z}_p)$. For instance, if C has good reduction at p, then we can simply take the model defined by the equation of C over $\mathrm{Spec}(\mathbb{Z}_p)$ and $\langle D, E \rangle_p$ is the intersection multiplicities between the Zariski closures of D and E in $\mathscr{C}$. For primes of bad reduction, the local Néron symbol also has a contribution coming from vertical divisors on $\mathscr{C}$ and the main stumbling block is the computation of a regular model $\mathscr{C}$ – but an algorithm for this computation is contained in `Magma`. The local Néron symbol itself can be computed using resultants [39] or Gröbner bases [53].

The archimedean local Néron symbol $\langle D,E\rangle_\infty$ is defined in terms of Green's functions on the Riemann surface associated to C. For practical purposes, it can be expressed and computed as a quotient of certain theta functions on $\mathbb{C}^g$ with respect to the Jacobian $J/\mathbb{C}$ and this is used in both [39] and [53]. `Magma` contains an implementation of this algorithm. Using this implementation, we can compute canonical heights for $g \leq 10$; higher genera are currently not feasible because the computation of theta-functions becomes rather inefficient. The implementation can also handle hyperelliptic curves defined over (small degree) number fields.

Unfortunately, the enumeration of all points in $J(\mathbb{Q})$ with canonical height up to a given bound is much more difficult when $g > 3$. It is not at all obvious how the expression (12) can be used to relate $\hat{h}$ to a height function analogous to the naive height h, so that we can enumerate all points in $J(\mathbb{Q})$ with $h(P)$ bounded. Some progress has been achieved by Holmes [38], but a practical version of the algorithm presented there is still a long way off, mainly because the archimedean bounds are currently rather enormous.

References

[1] J. S. Balakrishnan, J. S. Müller, and W. Stein. A p-adic analogue of the conjecture of Birch and Swinnerton-Dyer for modular abelian varieties. *Preprint*, 2012.

[2] Christina Birkenhake and Herbert Lange. *Complex abelian varieties*, volume 302 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, Berlin, second edition, 2004.

[3] Wieb Bosma, John Cannon, and Catherine Playoust. The Magma algebra system. I. The user language. *J. Symbolic Comput.*, 24(3-4):235–265, 1997. Computational algebra and number theory (London, 1993).

[4] Jean-Benoît Bost and Jean-François Mestre. Calcul de la hauteur archimédienne des points d'une courbe elliptique par un algorithme quadratiquement convergent et application au calcul de la capacité de l'union de deux intervalles. unpublished manuscript, 1993.

[5] Robert Bradshaw. *Provable Computation of Motivic L-functions*. PhD thesis, University of Washington, 2013.

[6] Peter Bruin. Bornes optimales pour la différence entre la hauteur de Weil et la hauteur de Néron-Tate sur les courbes elliptiques sur $\overline{\mathbb{Q}}$. *Acta Arith.*, 160(4):385–397, 2013.

[7] Armand Brumer and Kenneth Kramer. The rank of elliptic curves. *Duke Math. J.*, 44(4):715–743, 1977.

[8] Yann Bugeaud, Maurice Mignotte, Samir Siksek, Michael Stoll, and Szabolcs Tengely. Integral points on hyperelliptic curves. *Algebra Number Theory*, 2(8):859–885, 2008.

[9] David G. Cantor. Computing in the Jacobian of a hyperelliptic curve. *Math. Comp.*, 48(177):95–101, 1987.

[10] J. W. S. Cassels. The Mordell-Weil group of curves of genus 2. In *Arithmetic and geometry, Vol. I*, volume 35 of *Progr. Math.*, pages 27–60. Birkhäuser, Boston, Mass., 1983.

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

[12] Henri Cohen. *A course in computational algebraic number theory*, volume 138 of *Graduate Texts in Mathematics*. Springer-Verlag, Berlin, 1993.

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

[14] J. E. Cremona, T. A. Fisher, C. O'Neil, D. Simon, and M. Stoll. Explicit n-descent on elliptic curves. I. Algebra. *J. Reine Angew. Math.*, 615:121–155, 2008.

[15] J. E. Cremona, T. A. Fisher, C. O'Neil, D. Simon, and M. Stoll. Explicit n-descent on elliptic curves. II. Geometry. *J. Reine Angew. Math.*, 632:63–84, 2009.

[16] J. E. Cremona, T. A. Fisher, C. O'Neil, D. Simon, and M. Stoll. Explicit n-descent on elliptic curves. III. Algorithms. *Math. Comp.*, to appear. published online July 29, 2014.

[17] J. E. Cremona, M. Prickett, and Samir Siksek. Height difference bounds for elliptic curves over number fields. *J. Number Theory*, 116(1):42–68, 2006.

[18] Sylvain Duquesne. Montgomery scalar multiplication for genus 2 curves. In *Algorithmic number theory*, volume 3076 of *Lecture Notes in Comput. Sci.*, pages 153–168. Springer, Berlin, 2004.

[19] Sylvain Duquesne. Traces of the group law on the Kummer surface of a curve of genus 2 in characteristic 2. *Math. Comput. Sci.*, 3(2):173–183, 2010.

[20] Mathieu Dutour Sikirić, Achill Schürmann, and Frank Vallentin. Complexity and algorithms for computing Voronoi cells of lattices. *Math. Comp.*, 78(267):1713–1731, 2009.

[21] G. Faltings. Endlichkeitssätze für abelsche Varietäten über Zahlkörpern. *Invent. Math.*, 73(3):349–366, 1983.

[22] Gerd Faltings. Calculus on arithmetic surfaces. *Ann. of Math. (2)*, 119(2):387–424, 1984.

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

[24] E. V. Flynn. Descent via isogeny in dimension 2. *Acta Arith.*, 66(1):23–43, 1994.

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

[26] E. Victor Flynn, Franck Leprévost, Edward F. Schaefer, William A. Stein, Michael Stoll, and Joseph L. Wetherell. Empirical evidence for the Birch and Swinnerton-Dyer conjectures for modular Jacobians of genus 2 curves. *Math. Comp.*, 70(236):1675–1697 (electronic), 2001.

[27] E. Victor Flynn, Damiano Testa, and Ronald van Luijk. Two-coverings of Jacobians of curves of genus 2. *Proc. Lond. Math. Soc. (3)*, 104(2):387–429, 2012.

[28] Eugene Victor Flynn. The Jacobian and formal group of a curve of genus 2 over an arbitrary ground field. *Math. Proc. Cambridge Philos. Soc.*, 107(3):425–441, 1990.

[29] P. Gaudry. Fast genus 2 arithmetic based on theta functions. *J. Math. Cryptol.*, 1(3):243–265, 2007.

[30] Pierrick Gaudry and David Lubicz. The arithmetic of characteristic 2 Kummer surfaces and of elliptic Kummer lines. *Finite Fields Appl.*, 15(2):246–260, 2009.

[31] Josef Gebel and Horst G. Zimmer. Computing the Mordell-Weil group of an elliptic curve over $\mathbf{Q}$. In *Elliptic curves and related topics*, volume 4 of *CRM Proc. Lecture Notes*, pages 61–83. Amer. Math. Soc., Providence, RI, 1994.

[32] Daniel M. Gordon and David Grant. Computing the Mordell-Weil rank of Jacobians of curves of genus two. *Trans. Amer. Math. Soc.*, 337(2):807–824, 1993.

[33] David Grant. Formal groups in genus two. *J. Reine Angew. Math.*, 411:96–121, 1990.

[34] Grigor Grigorov, Andrei Jorza, Stefan Patrikis, William A. Stein, and Corina Tarniţă. Computational verification of the Birch and Swinnerton-Dyer conjecture for individual elliptic curves. *Math. Comp.*, 78(268):2397–2425, 2009.

[35] Benedict H. Gross and Don B. Zagier. Heegner points and derivatives of L-series. *Invent. Math.*, 84(2):225–320, 1986.

[36] Venkatesan Guruswami, Daniele Micciancio, and Oded Regev. The complexity of the covering radius problem. *Computational Complexity*, 14(2):90–121, 2005.

[37] Marc Hindry and Joseph H. Silverman. *Diophantine geometry*, volume 201 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2000. An introduction.

[38] David Holmes. An Arakelov-theoretic approach to naive heights on hyperelliptic Jacobian. *Preprint*, 2012.

[39] David Holmes. Computing Néron-Tate heights of points on hyperelliptic Jacobians. *J. Number Theory*, 132(6):1295–1305, 2012.

[40] Paul Hriljac. Heights and Arakelov's intersection theory. *Amer. J. Math.*, 107(1):23–38, 1985.

[41] R. W. H. T. Hudson. *Kummer's Quartic Surface*. University Press, Cambridge, 1905.

[42] Kazuya Kato. p-adic Hodge theory and values of zeta functions of modular forms. *Astérisque*, (295):ix, 117–290, 2004. Cohomologies p-adiques et applications arithmétiques. III.

[43] V. A. Kolyvagin. Finiteness of $E(\mathbf{Q})$ and $\mathrm{SH}(E,\mathbf{Q})$ for a subclass of Weil curves. *Izv. Akad. Nauk SSSR Ser. Mat.*, 52(3):522–540, 670–671, 1988.

[44] S. Lang and A. Néron. Rational points of abelian varieties over function fields. *Amer. J. Math.*, 81:95–118, 1959.

[45] Serge Lang. *Fundamentals of Diophantine geometry*. Springer-Verlag, New York, 1983.

[46] Ju. I. Manin. Cyclotomic fields and modular curves. *Uspehi Mat. Nauk*, 26(6(162)):7–71, 1971.

[47] B. Mazur, J. Tate, and J. Teitelbaum. On p-adic analogues of the conjectures of Birch and Swinnerton-Dyer. *Invent. Math.*, 84(1):1–48, 1986.

[48] Robert L. Miller and Michael Stoll. Explicit isogeny descent on elliptic curves. *Math. Comp.*, 82(281):513–529, 2013.

[49] J. S. Milne. Abelian varieties. In *Arithmetic geometry (Storrs, Conn., 1984)*, pages 103–150. Springer, New York, 1986.

[50] J. S. Milne. Jacobian varieties. In *Arithmetic geometry (Storrs, Conn., 1984)*, pages 167–212. Springer, New York, 1986.

[51] Louis Mordell. On the rational solutions of the indeterminate equation of the 3rd and 4th degrees. *Proc. Camb. Phil. Soc.*, 21:179–192, 1922.

[52] Jan Steffen Müller. Explicit Kummer surface formulas for arbitrary characteristic. *LMS J. Comput. Math.*, 13:47–64, 2010.

[53] Jan Steffen Müller. Computing canonical heights using arithmetic intersection theory. *Math. Comp.*, 83(285):311–336, 2014.

[54] Jan Steffen Müller. Explicit Kummer varieties of hyperelliptic Jacobian threefolds. *LMS J. Comput. Math*, to appear.

[55] Jan Steffen Müller and Michael Stoll. Canonical heights for genus 2 Jacobians. *in preparation*.

[56] D. Mumford. On the equations defining abelian varieties. I. *Invent. Math.*, 1:287–354, 1966.

[57] A. Néron. Quasi-fonctions et hauteurs sur les variétés abéliennes. *Ann. of Math. (2)*, 82:249–331, 1965.

[58] Damiano Testa Nils Bruin, E. Victor Flynn. Descent via $(3,3)$-isogeny on jacobians of genus 2 curves. *Preprint*, 2014.

[59] M. Pohst and H. Zassenhaus. *Algorithmic algebraic number theory*, volume 30 of *Encyclopedia of Mathematics and its Applications*. Cambridge University Press, Cambridge, 1997. Revised reprint of the 1989 original.

[60] Bjorn Poonen and Edward F. Schaefer. Explicit descent for Jacobians of cyclic covers of the projective line. *J. Reine Angew. Math.*, 488:141–188, 1997.

[61] Bjorn Poonen and Michael Stoll. The Cassels-Tate pairing on polarized abelian varieties. *Ann. of Math. (2)*, 150(3):1109–1149, 1999.

[62] Edward F. Schaefer. 2-descent on the Jacobians of hyperelliptic curves. *J. Number Theory*, 51(2):219–232, 1995.

[63] Edward F. Schaefer. Computing a Selmer group of a Jacobian using functions on the curve. *Math. Ann.*, 310(3):447–471, 1998.

[64] Jean-Pierre Serre. *Galois cohomology*. Springer Monographs in Mathematics. Springer-Verlag, Berlin, english edition, 2002.

[65] Jean-Pierre Serre and John Tate. Good reduction of abelian varieties. *Ann. of Math. (2)*, 88:492–517, 1968.

[66] Samir Siksek. Infinite descent on elliptic curves. *Rocky Mountain J. Math.*, 25(4):1501–1538, 1995.

[67] Joseph H. Silverman. *The arithmetic of elliptic curves*, volume 106 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1986.

[68] Joseph H. Silverman. Computing heights on elliptic curves. *Math. Comp.*, 51(183):339–358, 1988.

[69] Joseph H. Silverman. *Advanced topics in the arithmetic of elliptic curves*, volume 151 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1994.

[70] William Stein and Christian Wuthrich. Algorithms for the arithmetic of elliptic curves using Iwasawa theory. *Math. Comp.*, 82(283):1757–1792, 2013.

[71] W. A. Stein et al. *Sage Mathematics Software (Version 6.3)*. The Sage Development Team, 2014. `http://www.sagemath.org`.

[72] Michael Stoll. Ratpoints and j-points. `http://www.mathe2.uni-bayreuth.de/stoll/programs/index.html`.

[73] Michael Stoll. On the height constant for curves of genus two. *Acta Arith.*, 90(2):183–201, 1999.

[74] Michael Stoll. Implementing 2-descent for Jacobians of hyperelliptic curves. *Acta Arith.*, 98(3):245–277, 2001.

[75] Michael Stoll. On the height constant for curves of genus two. II. *Acta Arith.*, 104(2):165–182, 2002.

[76] Michael Stoll. Arithmetic of hyperelliptic curves. Lecture notes, 2014. http://www.mathe2.uni-bayreuth.de/stoll/teaching/ArithHypKurven-SS2014/Skript-ArithHypCurves-pub-screen.pdf.

[77] Michael Stoll. An explicit theory of heights for hyperelliptic Jacobians of genus three. *Preprint*, 2014.

[78] Andy Stubbs. *Hyperelliptic curves*. PhD thesis, University of Liverpool, 2001.

[79] John Tate. On the conjectures of Birch and Swinnerton-Dyer and a geometric analog. In *Séminaire Bourbaki, Vol. 9*, pages Exp. No. 306, 415–440. Soc. Math. France, Paris, 1995.

[80] The PARI Group, Bordeaux. *PARI/GP version* `2.7.0`, 2014. available from `http://pari.math.u-bordeaux.fr/`.

[81] Heinz M. Tschöpe and Horst G. Zimmer. Computation of the Néron-Tate height on elliptic curves. *Math. Comp.*, 48(177):351–370, 1987.

[82] Yukihiro Uchida. The difference between the ordinary height and the canonical height on elliptic curves. *J. Number Theory*, 128(2):263–279, 2008.

[83] Yukihiro Uchida. Canonical local heights and multiplication formulas for the Jacobians of curves of genus 2. *Acta Arith.*, 149(2):111–130, 2011.

[84] André Weil. L`arithmétique sur les courbes algébriques. *Acta Math.*, 52:281–315, 1929.

[85] André Weil. *Variétés abéliennes et courbes algébriques*. Actualités Sci. Ind., no. 1064 = Publ. Inst. Math. Univ. Strasbourg 8 (1946). Hermann & Cie., Paris, 1948.

[86] Shouwu Zhang. Admissible pairing on a curve. *Invent. Math.*, 112(1):171–193, 1993.