ACTA ARITHMETICA
XCVIII.3 (2001)

Implementing 2-descent for Jacobians of hyperelliptic curves

by

Michael Stoll (Düsseldorf)

1. Introduction. Given a hyperelliptic curve C over $\mathbb{Q}$, it is often necessary or at least interesting to determine as many of its arithmetical invariants as possible. One of the most basic and important invariants is the Mordell–Weil rank of its Jacobian J, i.e., the free abelian rank of the group of rational points $J(\mathbb{Q})$. There is no algorithm known so far that provably determines this rank in all cases, but it is possible, at least in theory, to bound it from above by computing the size of a suitable Selmer group. Depending on the size of the generators, it is also more or less practical to find lower bounds by looking for independent rational points on the Jacobian. With some luck, both bounds coincide, and the rank is determined. In general, the difference between the actual rank and the upper bound obtained from a Selmer group is controlled by the rather mysterious Shafarevich–Tate group $Ш(\mathbb{Q}, J)$.

One usually looks at the 2-Selmer group $\mathrm{Sel}^{(2)}(\mathbb{Q}, J)$, since the multiplication-by-2 map is always available as a $\mathbb{Q}$-defined isogeny and has fairly low degree. Furthermore, its kernel is easily described explicitly in the case of hyperelliptic curves. As usual, we have the following exact sequence:

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

Thus one obtains the formula

$$\text{(1.1)}\quad \operatorname{rank} J(\mathbb{Q}) + \dim_{\mathbb{F}_2} J(\mathbb{Q})[2] + \dim_{\mathbb{F}_2} Ш(\mathbb{Q}, J)[2] = \dim_{\mathbb{F}_2} \mathrm{Sel}^{(2)}(\mathbb{Q}, J)$$

and hence

$$\operatorname{rank} J(\mathbb{Q}) \le \dim_{\mathbb{F}_2} \mathrm{Sel}^{(2)}(\mathbb{Q}, J) - \dim_{\mathbb{F}_2} J(\mathbb{Q})[2].$$

2000 *Mathematics Subject Classification*: 11G10, 11G30, 11Y99, 14H25, 14H40, 14H45, 14Q05.

The author thanks the Deutsche Forschungsgemeinschaft for supporting the present work by a research grant.

This work forms part of the author's Habilitation in Düsseldorf.

The general procedure for the determination of a Selmer group calls for studying suitable principal homogeneous spaces for J. This is feasible for elliptic curves (see for example Cremona [5]), but becomes unwieldy in genus 2 and higher. For some examples, see Gordon and Grant [7]. If one is willing to do computations in number fields of moderate degree, there is a method available that completely avoids homogeneous spaces. It turns out that this method is feasible for general curves of genus 2 over $\mathbb{Q}$ and even for hyperelliptic curves of still higher genus, as long as the coefficients in the defining equation are not too large.

The basic algorithm in the genus 2 case is described in Cassels' article [3]. Another description, together with a specific example, can be found in [6]. See also Cassels and Flynn [4]. Schaefer [15, 16] puts it into a more general and more conceptual framework. We will follow his approach here. The theory underlying the most general case treated here ($y^2 = f(x)$ with f non-monic of even degree) is explained by Poonen and Schaefer [13], who consider, more generally, equations of the form $y^p = f(x)$ with $\deg f$ divisible by p.

The problem of determining the parity of $\dim_{\mathbb{F}_2} Ш(\mathbb{Q}, J)[2]$ is studied by Poonen and Stoll [14]. Unlike the case of elliptic curves, the dimension can be odd. In this case, the bound on the rank can be improved.

The paper is organised as follows. We first introduce some notation that is used throughout the paper. Then we discuss what basic algorithms for arithmetic in number fields and in p-adic fields we need to build our 2-descent procedure on. In Section 4, we present the algorithm in the somewhat simpler case when the curve has a rational Weierstraß point. Section 5 discusses the modifications that are necessary in the general case. In this case, we have to assume that the genus is even. In both variants of the algorithm, it is necessary to do certain local computations. These are described in Section 6. The last section describes a method for determining the parity of $\dim Ш(\mathbb{Q}, J)[2]$.

Acknowledgments. I thank Bjorn Poonen and in particular Ed Schaefer for the useful comments they made on earlier versions of this paper. Colin Stahlke provided me with a list of genus 2 curves, one of which figures as a nice example at the end of Section 5.

2. Notation.

Let $f \in \mathbb{Q}[x]$ be some square-free polynomial and consider the hyperelliptic curve given by the affine equation

$$y^2 = f(x). \tag{2.1}$$

We let C be its non-singular projective model, and we denote by J the Jacobian of C.

If p is some fixed prime, we let $\mathcal{J}$ denote the Néron model of J over $\mathbb{Z}_p$ (see [2], especially Chapter 9). The kernel of reduction in $J(\mathbb{Q}_p)$ is denoted by $J^1(\mathbb{Q}_p)$. The larger subgroup of points in $J(\mathbb{Q}_p)$ mapping into the identity component $\mathcal{J}^0_{\mathbb{F}_p}$ is denoted by $J^0(\mathbb{Q}_p)$. We let $\Phi_p = \mathcal{J}_{\mathbb{F}_p}/\mathcal{J}^0_{\mathbb{F}_p}$ denote the component group; it is a finite étale group scheme over $\mathbb{F}_p$. We then have the following well known exact sequences:

$$0 \to J^0(\mathbb{Q}_p) \to J(\mathbb{Q}_p) \to \Phi_p(\mathbb{F}_p) \to 0 \tag{2.2}$$

and

$$0 \to J^1(\mathbb{Q}_p) \to J^0(\mathbb{Q}_p) \to \mathcal{J}^0(\mathbb{F}_p) \to 0. \tag{2.3}$$

The first sequence is exact at the right by [1, §2]. There are corresponding exact sequences with $\mathbb{Q}_p$ and $\mathbb{F}_p$ replaced by $\mathbb{Q}_p^{\mathrm{nr}}$ and $\overline{\mathbb{F}}_p$, respectively.

For any field extension K of $\mathbb{Q}$, let $L_K = K[T]/(f(T))$ denote the algebra defined by f; then $L_K = K[\theta]$, where θ is the image of T, and L_K is a product of finite field extensions of K,

$$L_K = L_{K,1} \times \ldots \times L_{K,m_K}.$$

The fields $L_{K,j}$ correspond to the irreducible factors of f in $K[x]$. We will drop the subscript $\mathbb{Q}$ (i.e., $L = L_{\mathbb{Q}}$, $m = m_{\mathbb{Q}}$ etc.) and use the subscript v instead of $\mathbb{Q}_v$ for a place v of $\mathbb{Q}$. This convention will be in force throughout the paper and applies to everything that has a field as a subscript.

Let $\mathcal{O}_K$, $I(K)$ and $\mathrm{Cl}(K)$ denote the ring of integers, the ideal group and the ideal class group of a number field K, respectively. Then we define

$$\begin{aligned} \mathcal{O}_{L_K} &= \mathcal{O}_{L_{K,1}} \times \ldots \times \mathcal{O}_{L_{K,m_K}}, \\ I(L_K) &= I(L_{K,1}) \times \ldots \times I(L_{K,m_K}), \\ \mathrm{Cl}(L_K) &= \mathrm{Cl}(L_{K,1}) \times \ldots \times \mathrm{Cl}(L_{K,m_K}). \end{aligned}$$

We have the norm map $L_K \to K$; we will call it, and various other maps it induces by functoriality, N_K. For a prime p, let $I_p(L)$ be the subgroup of $I(L)$ consisting of ideals with support above p. For a finite set S of places of $\mathbb{Q}$, let

$$I_S(L) = \prod_{p \in S \setminus \{\infty\}} I_p(L) \subset I(L).$$

The unit group of a ring R is denoted by $R^\times$.

We will write $\mathcal{O}^\times$, $K^\times$, $L^\times$, I and the like multiplicatively, but Cl additively. We will use 0 consistently to denote the trivial group.

If M is a group on which the absolute Galois group $\mathrm{Gal}(K)$ of a field K acts, we let $M(K)$ denote the subgroup of invariant or K-rational elements. We use $H^j(K, M)$ as an abbreviation for the Galois cohomology group $H^j(\mathrm{Gal}(K), M)$. When M is an algebraic group over K, $H^j(K, M)$ stands for $H^j(K, M(\overline{K}))$.

If M is an abelian group and m is an integer, $M[m]$ denotes the m-torsion subgroup of M, i.e., the elements of M killed by m.

Nearly everything in this paper has a structure of an $\mathbb{F}_2$-vector space, and all dimensions are $\mathbb{F}_2$-dimensions.

Recall the definitions of the Shafarevich–Tate and Selmer groups. The *Shafarevich–Tate group* $\text{Ш}(\mathbb{Q}, J)$ is defined as

$$\text{Ш}(\mathbb{Q}, J) = \ker\Big(H^1(\mathbb{Q}, J) \xrightarrow{\prod_v \operatorname{res}_v} \prod_v H^1(\mathbb{Q}_v, J)\Big),$$

where v runs through all places of $\mathbb{Q}$. The 2-*Selmer group* $\operatorname{Sel}^{(2)}(\mathbb{Q}, J)$ is defined to be the inverse image of $\text{Ш}(\mathbb{Q}, J)[2]$ under the canonical map $H^1(\mathbb{Q}, J[2]) \to H^1(\mathbb{Q}, J)[2]$.

We will describe large parts of the procedure informally, but occasionally we will present detailed algorithms performing some specific tasks. The pseudo-code we use should be sufficiently self-explanatory. The only thing to notice is that the scope of conditional or iterative constructs is indicated by the indentation level.

3. Prerequisites. In this section, we will describe what kind of algorithms we assume to be available as a basis for our implementation of the 2-descent procedure.

An essential part of this procedure deals with number fields. Let K be a number field with ring of integers $\mathcal{O}$, ideal group I and ideal class group Cl. There is the well known exact sequence

$$0 \to \mathcal{O}^\times \to K^\times \to I \to \mathrm{Cl} \to 0.$$

We need this exact sequence to be *effective.* This means that we need suitable representations for elements of K, for ideals and for ideal classes, and we must be able to do the following:

- Determine the unit group $\mathcal{O}^\times$.
- Given an element of $K^\times$, find the principal ideal it generates.
- Determine the class group Cl.
- Given an ideal, find its image in Cl.
- Given a principal ideal, find a generator.
- Given an element of Cl, find an ideal mapping to it.

In short, we want to be able to compute images and preimages under all of the maps in the sequence.

There are several packages available that can do these computations, for example PARI [20], KANT [18] and also MAGMA [19], which contains KANT's number field machinery.

The first implementation of the 2-descent procedure described here that was able to deal with general curves of genus 2 over $\mathbb{Q}$ was done by the author in Common Lisp. It made use of the PARI libraries (version 1.39.x). There is now another implementation in MAGMA, again by the author, as part of a package dealing with hyperelliptic curves. We will use this second implementation as a reference when we are discussing implementation details. In its present form, this program can compute the size of the 2-Selmer group for general curves of genus 2 and curves with f of odd degree of moderate genus.

The main feature of the 2-descent procedure as described by Schaefer [16] and Poonen and Schaefer [13] is that it replaces the group $H^1(K, J[2])$, which is difficult to deal with directly, by a more tractable group like $L_K^\times/(L_K^\times)^2$.

This means that we will have to find the splitting of the étale algebra L into number fields, and similarly we must find the splitting of L_p into p-adic fields. This essentially amounts to factoring the polynomial f in $\mathbb{Q}[x]$ or $\mathbb{Q}_p[x]$, which is easily possible with all the computer algebra packages mentioned above.

We will also have to deal with groups of the form

$$L_p^\times/(L_p^\times)^2 = \prod_{j=1}^{m_p} L_{p,j}^\times/(L_{p,j}^\times)^2$$

and the canonical maps from $L^\times/(L^\times)^2$ onto them. This is fairly straightforward when p is odd or $p = \infty$. The case $p = 2$ is somewhat more complicated, but does not present any essential difficulties.

In the following sections, we will tacitly assume that we can perform the computations described here.

4. The odd degree case. In this section, we assume that the polynomial f defining the curve has odd degree. By a suitable scaling of x and y, we may assume f to be *monic* and to have *integral coefficients.* The genus g of C is $\frac{1}{2}(\deg f - 1)$. Note that any hyperelliptic curve with a rational Weierstraß point has an equation with f of odd degree.

The basic references for this case are Schaefer's papers [15] and [16].

There is one point at infinity on the projective closure of the affine curve given by equation (2.1); it is covered by one point on the normalisation, which we call ∞. This point is in $C(\mathbb{Q})$.

For a field extension K of $\mathbb{Q}$, let

$$H_K = \ker(N_K : L_K^\times/(L_K^\times)^2 \to K^\times/(K^\times)^2).$$

This fairly concrete group will replace the rather abstract group $H^1(K, J[2])$.

Let $\mathrm{Div}^0_\perp(C)$ denote the group of degree zero divisors on C with support disjoint from the support of the principal divisor $\mathrm{div}(y)$. Then for every K

we get a homomorphism

$$F_K : \mathrm{Div}^0_\perp(C)(K) \to L_K^\times, \qquad \sum_P n_P P \mapsto \prod_P (x(P) - \theta)^{n_P},$$

which induces a homomorphism

$$\delta_K : J(K) \to H_K$$

with kernel $2J(K)$. The induced map $J(K)/2J(K) \to H_K$ will also be denoted by δ_K.

Lemma 4.1. *The assignments $K \mapsto J(K)/2J(K)$, $K \mapsto H_K$ and $K \mapsto H^1(K, J[2])$ are functors from the category of field extensions of $\mathbb{Q}$ into the category of $\mathbb{F}_2$-vector spaces. There is a natural isomorphism $\iota_K : H_K \xrightarrow{\cong} H^1(K, J[2])$. The maps δ_K give a natural injection $J(K)/2J(K) \hookrightarrow H_K$, and $\iota_K \circ \delta_K$ equals the coboundary morphism $J(K)/2J(K) \to H^1(K, J[2])$.*

Proof. This is proved in [16]. ∎

This gives us the following characterisation of the Selmer group. Recall that $H = H_{\mathbb{Q}}$ according to our convention.

Proposition 4.2. *The 2-Selmer group of J over $\mathbb{Q}$ can be identified as follows*:

$$\mathrm{Sel}^{(2)}(\mathbb{Q}, J) = \{\xi \in H \mid \mathrm{res}_v(\xi) \in \delta_v(J(\mathbb{Q}_v)) \text{ for all } v\}.$$

Here, res_v *denotes the canonical "restriction" map $H \to H_v$, induced by functoriality from the inclusion $\mathbb{Q} \hookrightarrow \mathbb{Q}_v$.*

In order to make this practical, we have to reduce the set of places that have to be considered to a finite set. This requires some preparations. The reader who is only interested in the resulting algorithm can safely proceed to Corollary 4.7.

We will need some additional information on the 2-torsion subgroup of J and on the maps δ_K. Recall that all dimensions in this paper are $\mathbb{F}_2$-dimensions.

Lemma 4.3. *Let K be a field extension of $\mathbb{Q}$.*

(1) *For a point $P \in C(K)$ not in the support of* $\mathrm{div}(y)$, $\delta_K(P - \infty) = x(P) - \theta \bmod (L_K^\times)^2$.

(2) *Let $f = f_1 \ldots f_{m_K}$ be the factorisation of f over K into monic irreducible factors. Then with every factor f_j, we can associate an element $P_j \in J(K)[2]$ such that*:

(i) *The P_j generate $J(K)[2]$ and satisfy $\sum_{j=1}^{m_K} P_j = 0$.*

(ii) *Let h_j be the polynomial with $f = f_j h_j$. Then*

$$\delta_K(P_j) = (-1)^{\deg f_j} f_j(\theta) + (-1)^{\deg h_j} h_j(\theta) \bmod (L_K^\times)^2.$$

(3) $\dim J(K)[2] = m_K - 1$.

Proof. See [16]. P_j is the divisor class of $\sum_{f_j(\alpha)=0}(\alpha, 0) - (\deg f_j)\infty$. ∎

Let $\mathbb{Q}_p^{\mathrm{nr}}$ be the maximal unramified extension of $\mathbb{Q}_p$. Denote the Frobenius automorphism of $\mathbb{Q}_p^{\mathrm{nr}}/\mathbb{Q}_p$ by Fr_p. In order to avoid double subscripts, we set $H_p^{\mathrm{nr}} = H_{\mathbb{Q}_p^{\mathrm{nr}}}$. By functoriality, we have an action of $\mathrm{Gal}(\mathbb{Q}_p^{\mathrm{nr}}/\mathbb{Q}_p)$ on H_p^{nr}. If p is odd, we can identify the invariants $H_p^{\mathrm{nr}}(\mathbb{Q}_p) = (H_p^{\mathrm{nr}})^{\mathrm{Fr}_p}$ with

$$I_p = \ker(N : I_p(L)/I_p(L)^2 \to I_p(\mathbb{Q})/I_p(\mathbb{Q})^2).$$

We denote by val_p the map $H_p \to I_p$ induced by the valuations of the fields $L_{p,j}$. For odd p, it corresponds to the map $H_p \to (H_p^{\mathrm{nr}})^{\mathrm{Fr}_p}$ induced by the inclusion of $\mathbb{Q}_p$ in $\mathbb{Q}_p^{\mathrm{nr}}$. This map val_p is surjective for all p. By taking all the primes together, we get a map

$$\mathrm{val} = \prod_p \mathrm{val}_p \,\mathrm{res}_p : H \to I(L)/I(L)^2.$$

This map val is induced by the usual map $L^\times \to I(L)$ associating with an element the principal ideal it generates.

We will need to know the dimensions of the various groups for local fields.

Lemma 4.4. *Let K be a p-adic local field, and let $d_K = [K : \mathbb{Q}_2]$ if $p = 2$ and $d_K = 0$ if p is odd. Then*

(1) $\dim J(K)/2J(K) = \dim J(K)[2] + d_K g = m_K - 1 + d_K g$.

(2) $\dim H_K = 2 \dim J(K)/2J(K) = 2(m_K - 1 + d_K g)$.

(3) $\dim I_K = m_K - 1$.

Proof. (1) See [16, Prop. 2.4] or [11, Lemma I.3.3].

(2) For a p-adic local field M, we have $\dim M^\times/(M^\times)^2 = 2 + d_M$. Hence $\dim L_K^\times/(L_K^\times)^2 = 2m_K + d_{L_K}$. Since $\deg f$ is odd, the norm map $N_K : L_K^\times/(L_K^\times)^2 \to K^\times/(K^\times)^2$ is surjective, and so

$$\dim H_K = 2m_K + d_{L_K} - 2 - d_K = 2(m_K - 1 + d_K g).$$

Alternatively, this follows from Tate local duality and the identification $H_K \cong H^1(K, J[2])$ (see [11, Thm. I.3.2]).

(3) Easy. ∎

With these preparations, we can determine the image of δ_v for almost all places v of $\mathbb{Q}$. Before we do this, let us first state a general result on the image of $J(\mathbb{Q}_p)$ in I_p, when p is odd. Recall the notation Φ_p for the group of connected components of the special fibre of $\mathcal{J}$, the Néron model of J over $\mathbb{Z}_p$.

Lemma 4.5. *If p is odd, then the image of $J(\mathbb{Q}_p)$ in I_p under* $\mathrm{val}_p\,\delta_p$ *is isomorphic to the image of $\Phi_p(\mathbb{F}_p)$ in $\Phi_p/2\Phi_p$.*

Proof. We refer back to the exact sequences (2.2) and (2.3) and the corresponding sequences over $\mathbb{Q}_p^{\mathrm{nr}}$. Since $\mathcal{J}^0$ is a connected algebraic group and since $\overline{\mathbb{F}}_p$ is algebraically closed, the multiplication-by-2 map from $\mathcal{J}^0(\overline{\mathbb{F}}_p)$ to itself is onto. Since p is odd and J^1 is a formal group, multiplication-by-2 is an automorphism of $J^1(\mathbb{Q}_p^{\mathrm{nr}})$. Together, these two facts imply that $J(\mathbb{Q}_p^{\mathrm{nr}})/2J(\mathbb{Q}_p^{\mathrm{nr}}) \cong \Phi_p/2\Phi_p$.

Similarly, we get an exact sequence

$$\mathcal{J}^0(\mathbb{F}_p)/2\mathcal{J}^0(\mathbb{F}_p) \to J(\mathbb{Q}_p)/2J(\mathbb{Q}_p) \to \Phi_p(\mathbb{F}_p)/2\Phi_p(\mathbb{F}_p) \to 0.$$

Under the map from $J(\mathbb{Q}_p)/2J(\mathbb{Q}_p)$ to $J(\mathbb{Q}_p^{\mathrm{nr}})/2J(\mathbb{Q}_p^{\mathrm{nr}})$, the first term in this sequence vanishes. Hence the image of $J(\mathbb{Q}_p)$ in $J(\mathbb{Q}_p^{\mathrm{nr}})/2J(\mathbb{Q}_p^{\mathrm{nr}})$ is isomorphic to the image of $\Phi_p(\mathbb{F}_p)$ in $\Phi_p/2\Phi_p$.

Because of naturality, the following diagram commutes:

$$\begin{tikzcd}
J(\mathbb{Q}_p)/2J(\mathbb{Q}_p) \arrow[r, "\delta_p"] \arrow[d] & H_p \arrow[d, "\mathrm{val}_p"] \\
J(\mathbb{Q}_p^{\mathrm{nr}})/2J(\mathbb{Q}_p^{\mathrm{nr}}) \arrow[r, "\delta_p^{\mathrm{nr}}"] & H_p^{\mathrm{nr}} \supset I_p
\end{tikzcd}$$

Since the lower horizontal map is an injection, the claim follows. ∎

Remark. Let $c_p = \#J(\mathbb{Q}_p)/J^0(\mathbb{Q}_p)$. These so-called *Tamagawa numbers* show up in the Birch and Swinnerton-Dyer conjecture that relates the leading term of the L-series of J at $s = 1$ to invariants of J. The lemma implies that $\#G_p$ divides c_p when p is odd, where $G_p = \mathrm{val}_p\,\delta_p(J(\mathbb{Q}_p))$. Our algorithm computes G_p for all p where it is non-trivial and therefore gives us also some partial information on the numbers c_p.

The following is an immediate consequence.

Proposition 4.6. *If p is an odd prime such that p^2 does not divide the discriminant of f, then*

$$0 \to J(\mathbb{Q}_p)/2J(\mathbb{Q}_p) \xrightarrow{\delta_p} H_p \xrightarrow{\mathrm{val}_p} I_p \to 0$$

is an exact sequence.

Proof. We already know that δ_p is injective and that val_p is onto.

If p does not divide the discriminant of f, then the Jacobian has good reduction at p. This means that $J(\mathbb{Q}_p) = J^0(\mathbb{Q}_p)$, and so $\Phi_p(\mathbb{F}_p) = 0$.

If p does divide $\mathrm{disc}(f)$, but p^2 does not, then the model of the curve is regular, and its special fibre has only one component. This again implies that Φ_p is trivial (cf. [1]).

Lemma 4.5 shows that in both cases $\mathrm{val}_p\,\delta_p = 0$. Since by Lemma 4.4, $\dim H_p = \dim J(\mathbb{Q}_p)/2J(\mathbb{Q}_p) + \dim I_p$ for odd p, this implies exactness at H_p. ∎

Corollary 4.7. *Let* $S = \{\infty, 2\} \cup \{p \mid p^2$ *divides* $\operatorname{disc}(f)\}$. *Then*

$$\begin{aligned}\mathrm{Sel}^{(2)}(\mathbb{Q}, J) = \{\xi \in H \mid \operatorname{val}(\xi) \in I_S(L)/I_S(L)^2,& \\ \operatorname{res}_v(\xi) \in \delta_v(J(\mathbb{Q}_v)) \textit{ for all } v \in S\}.&\end{aligned}$$

This suggests the following strategy:

(1) Find the set S.

(2) For each $v \in S$, determine $J_v = \delta_v(J(\mathbb{Q}_v)) \subset H_v$.

(3) Determine a suitable finite subgroup $\widetilde{H}$ of $L^\times/(L^\times)^2$ that contains the Selmer group and find a basis of $\widetilde{H}$.

(4) Compute $\mathrm{Sel}^{(2)}(\mathbb{Q}, J)$ as the inverse image of $\prod_{v \in S} J_v$ under

$$\prod_{v \in S} \operatorname{res}_v : \widetilde{H} \to \prod_{v \in S} H_v.$$

We will consider each of the steps in turn.

Step (1). We must compute the discriminant of f and factor it. Since we have to factor f anyway in order to find the splitting of L into fields, we may do that first and then find the bad primes from the product formula for $\operatorname{disc}(f)$ in terms of the discriminants and resultants of the factors. In practice, f will often be irreducible, and this simplification cannot be used. Another possible simplification is that we only need primes that occur at least twice in the factorisation. This means that we can split off "small" primes first. If d is the remaining factor, we check if d is a square. If it is not, it will suffice to find all prime factors of d below $\sqrt[3]{d}$, and if it is, we only have to factor $\sqrt{d}$. I do not know if one can get a measurable speedup this way. The current implementation simply factors the discriminant.

Step (2). The reason for doing this step before step (3) is that the knowledge of the J_v allows us to find a smaller bounding group $\widetilde{H}$ in the third step. For example, if it turns out that $J_p = \ker(\operatorname{val}_p)$ for some odd $p \in S$, then we can drop p from S altogether.

Hence we can subdivide this step.

(2.1) For all $p \in S \setminus \{\infty\}$, compute $J_p = \delta_p(J(\mathbb{Q}_p))$ and its image $G_p = \operatorname{val}_p(J_p)$ in I_p.

(2.2) Remove from S all odd p with $G_p = 0$.

(2.3) Compute J_∞.

We require p to be odd in step (2.2), because for $p = 2$, $G_p = 0$ does not imply that $J_p = \ker(\operatorname{val}_p)$. This comes from the fact that $\dim H_2$ is larger than $\dim J_2 + \dim I_2$ (compare Lemma 4.4).

Step (2.1). This step will be dealt with in detail in Section 6.

Step (2.3). The determination of J_∞ is fairly easy with the following result.

Lemma 4.8. (1) *The dimension of* $J(\mathbb{R})/2J(\mathbb{R})$ *is* $m_\infty - 1 - g$.

(2) J_∞ *is generated by the* $\delta_\infty(P - \infty)$ *for* $P \in C(\mathbb{R})$.

(3) *The value of* $\delta_\infty(P - \infty)$ *only depends on the connected component of* $C(\mathbb{R})$ *containing* P.

Proof. (1) See [16, Prop. 2.5].

(2) This follows from Lemma 6.1 and $J(\mathbb{C})/2J(\mathbb{C}) = 0$.

(3) The map δ_∞ is continuous, and $L_\infty^\times/(L_\infty^\times)^2$ is discrete. ■

In practice, we have to find the real roots of f and order them to find the connected components of $C(\mathbb{R})$. The map from $C(\mathbb{R})$ to $L_\infty^\times/(L_\infty^\times)^2$ is then given on a point (x, y) by the collection of signs of $x - \alpha$ for all the real roots α.

Step (3). We let $G = \prod_{p \in S\setminus\{\infty\}} G_p \subset I(L)/I(L)^2$. Recall that G_p denotes the image of J_p in I_p; it was determined in step (2.1). Obviously, the group

$$\{\xi \in H \mid \mathrm{val}(\xi) \in G\}$$

contains the Selmer group. Since it turns out that we do not have to restrict to the kernel of the norm map at this point (see the discussion at the end of this section), we replace the group above by the larger group

$$\widetilde{H} = \{\xi \in L^\times/(L^\times)^2 \mid \mathrm{val}(\xi) \in G\}.$$

A basis of $\widetilde{H}$ is computed in two steps.

(3.1) Find a basis of $V = \ker(\mathrm{val} : L^\times/(L^\times)^2 \to I(L)/I(L)^2)$.

(3.2) Enlarge this basis to get a basis of $\widetilde{H} = \mathrm{val}^{-1}(G)$.

Step (3.1)

Lemma 4.9. *Let* $V = \ker(\mathrm{val} : L^\times/(L^\times)^2 \to I(L)/I(L)^2)$. *There is an exact sequence*

$$0 \to \mathcal{O}_L^\times/(\mathcal{O}_L^\times)^2 \to V \to \mathrm{Cl}(L)[2] \to 0.$$

Proof. Consider

$$\begin{tikzcd}
 & L^\times \arrow[r, "2"] \arrow[d] & L^\times \arrow[r] \arrow[d] & L^\times/(L^\times)^2 \arrow[r] \arrow[d, "\mathrm{val}"] & 0 \\
0 \arrow[r] & I(L) \arrow[r, "2"] & I(L) \arrow[r] & I(L)/I(L)^2 \arrow[r] & 0
\end{tikzcd}$$

and apply the snake lemma. ■

To get a basis of V, we first take a basis of $\mathcal{O}_L^\times/(\mathcal{O}_L^\times)^2$, which is obtained from a set of fundamental units and a suitable power of some primitive root of unity for each of the fields L_j. Then we have to take a basis of $\mathrm{Cl}(L)[2]$ and lift it back to $L^\times/(L^\times)^2$. This is done as follows. We take some representative ideal $\mathfrak{a} \in I(L)$ of a basis element in $\mathrm{Cl}(L)[2]$. Then $\mathfrak{a}^2 = \alpha\mathcal{O}_L$ is principal, and we can use the generator α as the lifting. The union of the two sets thus obtained is a basis of V.

Step (3.2). To extend the basis of V in order to get a basis of $\widetilde{H}$, we have to lift a basis of

$$G \cap \mathrm{val}(L^\times/(L^\times)^2) = \ker(G \to \mathrm{Cl}(L)/2\mathrm{Cl}(L))$$

back under val to $L^\times/(L^\times)^2$. We can do this as follows.

(3.2.1) Put the results of step (2.1) together to produce a basis of G.

(3.2.2) Compute the image of this basis in $\mathrm{Cl}(L)/2\mathrm{Cl}(L)$ and find a basis of the kernel W of the map $G \to \mathrm{Cl}(L)/2\mathrm{Cl}(L)$.

(3.2.3) For each element $\mathfrak{a}I(L)^2$ of this basis of W, find some ideal $\mathfrak{b} \in I(L)$ such that $\mathfrak{a}\mathfrak{b}^2$ is principal, and take a generator of $\mathfrak{a}\mathfrak{b}^2$ as an element of the basis of $\widetilde{H}$.

The image of $\mathfrak{a}$ in $\mathrm{Cl}(L)$ is needed in step (3.2.3) to find $\mathfrak{b}$.

Once we know the class groups, we can give an upper bound for the Selmer group dimension without having to find generators for principal ideals and without having to compute the fundamental units of the number fields involved. (Both of these tasks tend to require much more computational effort than the determination of the class group alone for fields of medium complexity.) We only need to find the ideal class an ideal belongs to and to know the unit rank of the number fields, which is determined by the signature.

Lemma 4.10. *We have the following bound on the Selmer group dimension*:

$$\dim \mathrm{Sel}^{(2)}(\mathbb{Q}, J) \le m_\infty + \dim \mathrm{Cl}(L)[2] + \dim\ker(G \to \mathrm{Cl}(L)/2\mathrm{Cl}(L)) - 1.$$

Proof. The sum of the numbers of real and pairs of conjugate complex embeddings of all the number fields L_j equals m_∞. By Lemma 4.9, we have

$$\dim V = \dim \mathcal{O}_L^\times/(\mathcal{O}_L^\times)^2 + \dim \mathrm{Cl}(L)[2] = m_\infty + \dim \mathrm{Cl}(L)[2].$$

By the definition of $\widetilde{H}$, we see that the bound given is just one less than its dimension. Since G_p lies in the kernel of the norm map to $I_p(\mathbb{Q})/I_p(\mathbb{Q})^2$, the norm map on $L^\times/(L^\times)^2$ maps $\widetilde{H}$ into $\langle -1\rangle \subset \mathbb{Q}^\times/(\mathbb{Q}^\times)^2$. Since $-1 \in \widetilde{H}$ and $N(-1) = -1$, this implies that

$$\dim\ker(N : \widetilde{H} \to \mathbb{Q}^\times/(\mathbb{Q}^\times)^2) = \dim \widetilde{H} - 1.$$

But the Selmer group is contained in the kernel of N on $\widetilde{H}$, whence the claim. ■

Note that for the computation of $\ker(G \to \mathrm{Cl}(L)/2\mathrm{Cl}(L))$, we only need to find the images of various prime ideals in the ideal class group, whereas in order to find an actual basis of $\widetilde{H}$, we must find the units, and we must determine generators for principal ideals. We can of course bound $\dim\ker(G \to \mathrm{Cl}(L)/2\mathrm{Cl}(L))$ by $\dim G$, if we even want to avoid the computation of images in the class group.

Suppose that we already have got a lower bound l on the Mordell–Weil rank. We might have found a number of independent points on J, for example. If at this point, we see that $\dim\widetilde{H} = l + \dim J(\mathbb{Q})[2] + 1$, the computation can be stopped, since $\ker(N|_{\widetilde{H}})$ must be the Selmer group, and the rank must be l.

Step (4). This is simply linear algebra over $\mathbb{F}_2$. If only a bound for the Mordell–Weil rank is needed, it is sufficient to compute the dimension of $\mathrm{Sel}^{(2)}(\mathbb{Q}, J)$ instead of a basis. Let $J_S = \bigoplus_{v\in S} J_v$, and denote by res_S the map from $L^\times/(L^\times)^2$ into $\bigoplus_{v\in S} L_v^\times/(L_v^\times)^2$. Then

$$\dim \mathrm{Sel}^{(2)}(\mathbb{Q}, J) = \dim\widetilde{H} + \dim J_S - \dim(\mathrm{res}_S(\widetilde{H}) + J_S).$$

At some point in the calculation, we have to restrict to the kernel of $N : L^\times/(L^\times)^2 \to \mathbb{Q}^\times/(\mathbb{Q}^\times)^2$. This could be done between steps (3) and (4), but it turns out to be unnecessary, since step (4) does take care of it automatically. To see this, note that an element $a \in \mathbb{Q}^\times$ is a square if and only if $v_p(a)$ is even for all primes p and a is positive. This implies that an element α of $L^\times/(L^\times)^2$ with $\mathrm{val}(\alpha) \in I_S(L)/I_S(L)^2$ that maps into J_p for all $p \in S$ automatically has trivial norm in $\mathbb{Q}^\times/(\mathbb{Q}^\times)^2$, since the norm of its representative is a square at all $p \in S$ and has even valuation outside S.

If we want to use a number field other than $\mathbb{Q}$ as the base field, we will need an extra step to find the kernel of the norm on $\widetilde{H}$, unless the S-class group of the base field has odd order.

5. The even degree case. In this section, we assume f to have even degree $\deg f = 2n$. By a suitable scaling of the variables, we can again assume f to have *integral coefficients* or even to have the form $f(x) = cf_1(x)$ with a non-zero integer c and a *monic* polynomial f_1 with *integral coefficients*. This form is often convenient for practical purposes, since some computer algebra systems require a monic polynomial with integral coefficients to define a number field, and some statements become simpler when θ is known to be integral in $L = \mathbb{Q}[x]/(f(x)) = \mathbb{Q}[x]/(f_1(x))$. Hence we will assume f to have this form.

The curve C has two points at infinity (i.e., points that cover the point at infinity on the projective closure of the affine curve $y^2 = f(x)$); they are $\mathbb{Q}$-rational if and only if c is a square; otherwise they are defined over $\mathbb{Q}(\sqrt{c})$

and conjugate. We let $\mathfrak{m} \in \mathrm{Div}(C)(\mathbb{Q})$ denote their sum. The genus g of C is $n-1$.

Remark. A general curve of genus 2 over $\mathbb{Q}$ can be defined by an equation $y^2 = f(x)$ with f of degree 5 or 6 and square-free (see [4, §1.1]).

The approach is similar to that used for the odd degree case, but there are some additional complications. The theoretical background can be found in Poonen and Schaefer [13]. The first contribution (for genus 2) goes back to Cassels [3].

The first complication is that the definition of H_K has to be adjusted as follows. For a field extension K of $\mathbb{Q}$, let

$$H_K = \ker(N_K : L_K^\times/(L_K^\times)^2 K^\times \to K^\times/(K^\times)^2).$$

Note that the norm map is well defined here since $K^\times$ is in the kernel.

As before, there is a homomorphism

$$F_K : \mathrm{Div}^0_\perp(C)(K) \to L_K^\times, \qquad \sum_P n_P P \mapsto \prod_P (x(P) - \theta)^{n_P}.$$

We will say that the field K *satisfies condition* (†) if every element of $J(K)$ is represented by a K-rational divisor. In this case, F_K induces a homomorphism

$$\delta_K : J(K) \to H_K.$$

Condition (†) is satisfied when K is a local or number field and C has a K-rational point or the genus is even (compare [13, Prop. 3.3 and 3.4]; note that the period divides 2).

If the genus is odd, condition (†) is not always satisfied. But even when there is a rational point on C, there are other problems. For example, it is no longer true in general that for an odd prime p not dividing $\mathrm{disc}(f)$, the local image J_p equals the kernel of $\mathrm{val}_p : H_p \to I_p$. Therefore, we will suppose that $g > 0$ is *even* (and consider $g = 2$ in particular). This means that the degree of f satisfies $\deg f \equiv 2 \bmod 4$.

A major difference compared to the odd degree situation is that the kernel of δ_K can be larger than $2J(K)$.

Let us say that K *satisfies condition* (‡) if either f has a factor of odd degree in $K[x]$, or f_1 factors as $f_1 = h\overline{h}$ over a quadratic extension K' of K, with $\overline{h}$ the $\mathrm{Gal}(K'/K)$-conjugate of h. The latter condition is equivalent to L_K containing a quadratic extension of K, i.e., there is a field M of degree 2 over K with $K \subset M \subset L_K$, where $K \hookrightarrow L_K$ is the canonical embedding $K \hookrightarrow K[T] \twoheadrightarrow L_K$.

Lemma 5.1. *Assume that K satisfies condition* (†). *Then the kernel of δ_K is $2J(K)$ if K satisfies condition* (‡), *or if there is no K-rational divisor class of degree* 1 *on C. Otherwise*, $2J(K)$ *has index* 2 *in the kernel of δ_K.*

Proof. See [13, Thm. 11.2]. ∎

We note a few cases where condition (‡) is always satisfied.

Lemma 5.2. *Condition* (‡) *is satisfied in each of the following situations*:

(1) $K = \mathbb{R}$.

(2) *K is a p-adic field, and the irreducible factors of f in $K[x]$ all define unramified extensions of K.*

(3) *$K = \mathbb{Q}_p^{\mathrm{nr}}$ for an odd prime p.*

Proof. We can assume that f has no irreducible factors of odd degree in $K[x]$. Suppose that the compositum M of the fields $L_{K,j}$ defined by the irreducible factors of f is a cyclic extension of K. Then each $L_{K,j}$ is a subfield of even degree of M and must therefore contain the unique subfield of degree two of M. Hence L_K contains this quadratic extension of K. This proves (1) and (2). For part (3), note that there is a unique quadratic extension of $\mathbb{Q}_p^{\mathrm{nr}}$, and this extension is contained in every extension of even degree of $\mathbb{Q}_p^{\mathrm{nr}}$. ∎

For genus $g = 2$, i.e. $\deg f = 6$, the second alternative in condition (‡) can be tested as follows. Note that another form of this condition is that the six zeros of f in $\overline{K}$ allow a $\mathrm{Gal}(\overline{K}/K)$-stable partition into two three-sets.

Lemma 5.3. *Write $f_1(x) = \prod_{j=1}^{6}(x - \alpha_j)$, and let*

$$h(f_1) = \prod_{\sigma}(x - (\alpha_{\sigma(1)}\alpha_{\sigma(2)}\alpha_{\sigma(3)} + \alpha_{\sigma(4)}\alpha_{\sigma(5)}\alpha_{\sigma(6)})),$$

where the product is over left coset representatives $\sigma \in S_6$ modulo the stabiliser of the partition $\{\{1,2,3\},\{4,5,6\}\}$. Then $h(f_1)$ has degree 10.

(1) *For $a \in K$, the second alternative in condition* (‡) *holds for f if and only if it holds for $f(x+a)$.*

(2) *If $h(f_1)$ has a simple root in K, then K satisfies the second alternative in condition* (‡).

(3) *If $h(f_1)$ has no root in K, then K does not satisfy the second alternative in condition* (‡).

(4) *There are at most* 45 *values of $a \in K$ such that $h(f_1(x+a))$ is not square-free.*

Proof. (1) Obvious.

(2) Assume $\alpha_1\alpha_2\alpha_3 + \alpha_4\alpha_5\alpha_6$ is in K and distinct from the other zeros of $h(f_1)$. Then $\mathrm{Gal}(\overline{K}/K)$ must stabilise $\{\{\alpha_1,\alpha_2,\alpha_3\},\{\alpha_4,\alpha_5,\alpha_6\}\}$.

(3) If $\mathrm{Gal}(\overline{K}/K)$ stabilises $\{\{\alpha_1,\alpha_2,\alpha_3\},\{\alpha_4,\alpha_5,\alpha_6\}\}$ (say), then $\alpha_1\alpha_2\alpha_3 + \alpha_4\alpha_5\alpha_6$ must be in K.

(4) We show that for each pair of roots of $h(f_1)$, there is at most one value of $a \in K$ such that the two corresponding roots of $h(f_1(x+a))$ coincide. Since there are 45 pairs of roots, the claim follows.

Since S_6 acts transitively on pairs of partitions of $\{1,2,3,4,5,6\}$ into two three-sets, we may assume that the two roots are $\alpha_1\alpha_2\alpha_3+\alpha_4\alpha_5\alpha_6$ and $\alpha_1\alpha_2\alpha_4+\alpha_3\alpha_5\alpha_6$. Let

$$\begin{aligned} T = \{a \in K \mid (\alpha_1 - a)(\alpha_2 - a)(\alpha_3 - a) + (\alpha_4 - a)(\alpha_5 - a)(\alpha_6 - a) \\ = (\alpha_1 - a)(\alpha_2 - a)(\alpha_4 - a) + (\alpha_3 - a)(\alpha_5 - a)(\alpha_6 - a)\}\end{aligned}$$

and suppose that a and b are two distinct elements of T. This gives

$$(\alpha_1 - a)(\alpha_2 - a)(\alpha_3 - \alpha_4) = (\alpha_5 - a)(\alpha_6 - a)(\alpha_3 - \alpha_4)$$

and similarly with b instead of a. Since $\alpha_3 \neq \alpha_4$, we get

$$\begin{aligned} \alpha_1\alpha_2 - a(\alpha_1+\alpha_2) &= \alpha_5\alpha_6 - a(\alpha_5+\alpha_6), \\ \alpha_1\alpha_2 - b(\alpha_1+\alpha_2) &= \alpha_5\alpha_6 - b(\alpha_5+\alpha_6) \end{aligned}$$

and then $\alpha_1\alpha_2 = \alpha_5\alpha_6$ and $\alpha_1+\alpha_2 = \alpha_5+\alpha_6$, whence $\{\alpha_1,\alpha_2\} = \{\alpha_5,\alpha_6\}$, contradicting the fact that f_1 has no multiple roots. ■

To determine whether $\mathbb{Q}$ and all relevant $\mathbb{Q}_p$'s satisfy condition (‡) or not, we can therefore proceed as follows:

(0.1) If f_1 has a factor of odd degree over $\mathbb{Q}$, then condition (‡) is satisfied for $\mathbb{Q}$ and all its completions.

(0.2) Otherwise, let $a = 0$ and compute $h = h(f_1(x))$.

(0.3) If h has a simple rational root, then again condition (‡) is satisfied for $\mathbb{Q}$ and all its completions.

(0.4) If h is not square-free, replace a by $a+1$ and set $h = h(f_1(x+a))$. Go back to step (0.3).

(0.5) Now we have a square-free resolvent h without rational roots. Then $\mathbb{Q}$ does not satisfy condition (‡). To determine whether $\mathbb{Q}_p$ satisfies condition (‡), we first factor f_1 over $\mathbb{Q}_p$. If there is a factor of odd degree, then condition (‡) is satisfied. Otherwise, condition (‡) is satisfied if and only if h has a root in $\mathbb{Q}_p$.

There are essentially two methods for computing the resolvent $h(f_1)$. The first method is to determine the roots α_j to sufficient accuracy (in $\mathbb{C}$ or perhaps in $\overline{\mathbb{Q}}_p$) and from them the coefficients of $h(f_1)$, using the fact that they must be integers. The second method is to find explicit expressions for the coefficients of $h(f_1)$ in terms of the coefficients of f_1 and use them to compute $h(f_1)$.

Our implementation uses the second approach. We also remark that the resolvent can be simplified when f_1 factors into polynomials of degrees 2 and 4 or 2, 2 and 2.

For even genus $g > 2$, the best method to check the second alternative in condition (‡) probably is to find the quadratic subextensions of the fields L_j directly and see if there is one contained in all of them.

The relationship between δ_K, H_K and the coboundary map from Galois cohomology is less direct than in the odd degree case, but still sufficient to get the information we want.

LEMMA 5.4. *The assignments $K \mapsto J(K)/2J(K)$, $K \mapsto H^1(K, J[2])$, $K \mapsto H_K$ and $K \mapsto Q_K = H^1(K, \mu_2(L_{\overline{K}})/\mu_2(\overline{K}))$ are functors from the category of field extensions of $\mathbb{Q}$ into the category of $\mathbb{F}_2$-vector spaces. There are natural homomorphisms $\iota_K : H^1(K, J[2]) \to Q_K$ and $q_K : H_K \to Q_K$. The maps δ_K give a natural homomorphism $J(K)/2J(K) \to H_K$, which, when followed by q_K, equals the coboundary morphism $J(K)/2J(K) \to H^1(K, J[2])$, followed by ι_K. In other words, the following diagram is commutative*:

$$\begin{tikzcd}
J(K)/2J(K) \arrow[r, "\delta_K"] \arrow[d] & H_K \arrow[d, "q_K"] \\
H^1(K, J[2]) \arrow[r, "\iota_K"] & Q_K
\end{tikzcd}$$

Proof. See [13, Thm. 9.4]. ■

PROPOSITION 5.5. *The dimension of the 2-Selmer group of J over $\mathbb{Q}$ can be determined as follows. Let*

$$\mathrm{Sel}^{(2)}_{\mathrm{fake}}(\mathbb{Q}, J) = \{\xi \in H \mid \mathrm{res}_v(\xi) \in \delta_v(J(\mathbb{Q}_v)) \text{ for all } v\}.$$

Here again, res_v *denotes the canonical map $H \to H_v$, induced by functoriality from the inclusion $\mathbb{Q} \hookrightarrow \mathbb{Q}_v$. Then*

$$\dim \mathrm{Sel}^{(2)}(\mathbb{Q}, J) = \begin{cases} \dim \mathrm{Sel}^{(2)}_{\mathrm{fake}}(\mathbb{Q}, J) & \text{if } \mathbb{Q} \text{ satisfies } (\ddagger), \\ \dim \mathrm{Sel}^{(2)}_{\mathrm{fake}}(\mathbb{Q}, J) + 1 & \text{otherwise.} \end{cases}$$

Proof. See [13, Thm. 13.2]. ■

The computation of $\mathrm{Sel}^{(2)}_{\mathrm{fake}}(\mathbb{Q}, J)$ proceeds essentially in the same way as for the odd degree case. Note, however, that we have to deal with the additional complication that the fake Selmer group sits in the quotient of $L^\times/(L^\times)^2$ by $\mathbb{Q}^\times/(\mathbb{Q}^\times)^2$. We will deal with this difficulty later. Let us first state the results parallel to those in the odd degree case.

LEMMA 5.6. *Let K be a field extension of $\mathbb{Q}$.*

(1) *Suppose that the points $\infty_\pm$ at infinity on C are K-rational. Then for a point $P \in C(K)$ not in the support of* $\mathrm{div}(y)$, *we have $\delta_K(P - \infty_\pm) = x(P) - \theta \pmod{(L_K^\times)^2 K^\times}$.*

(2) *With every monic polynomial $h \in K[x]$ of even degree such that h divides f_1, we can associate an element $P_h \in J(K)[2]$ such that*:

(i) *The P_h generate $J(K)[2]$ and satisfy $\sum_j P_{h_j} = 0$, if $\prod_j h_j = f_1$.*

(ii) *Let $\widetilde{h}$ be the polynomial with $f = h\widetilde{h}$. Then $\delta_K(P_h) = h(\theta) - \widetilde{h}(\theta) \pmod{(L_K^\times)^2 K^\times}$.*

(3) $\dim J(K)[2] = m_K - 1$ *if all irreducible factors of f over K have even degree*, *and* $\dim J(K)[2] = m_K - 2$ *otherwise.*

Proof. See [13]. P_h is the divisor class of $\sum_{h(\alpha)=0}(\alpha, 0) - \frac{1}{2}(\deg h)\mathfrak{m}$. ■

We adjust the definition of I_p in the following way:

$$I_p = \ker(N : I_p(L)/I_p(L)^2 I_p(\mathbb{Q}) \to I_p(\mathbb{Q})/I_p(\mathbb{Q})^2).$$

There is again the valuation map $\mathrm{val}_p : H_p \to I_p$, or more generally,

$$\mathrm{val}_p : L^\times/(L^\times)^2 \to L^\times/(L^\times)^2\mathbb{Q}^\times \to L_p^\times/(L_p^\times)^2\mathbb{Q}_p^\times \to I_p(L)/I_p(L)^2 I_p(\mathbb{Q}).$$

These maps val_p, taken together, give us a map

$$\mathrm{val} : H \subset L^\times/(L^\times)^2\mathbb{Q}^\times \to I(L)/I(L)^2 I(\mathbb{Q}).$$

We will also need to use the canonical map $\widetilde{\mathrm{val}} : L^\times/(L^\times)^2 \to I(L)/I(L)^2$. If p is odd, we can again identify I_p with the Fr_p-invariants in $H_p^{\mathrm{nr}} = H_{\mathbb{Q}_p^{\mathrm{nr}}}$, and the map val_p corresponds in this way to the map $H_p \to H_p^{\mathrm{nr}}$ induced from the inclusion $\mathbb{Q}_p \hookrightarrow \mathbb{Q}_p^{\mathrm{nr}}$.

The determination of the dimensions of the various local groups is less straightforward than in the odd degree case.

For an arbitrary field extension K of $\mathbb{Q}$, we let $t_K = 0$ if all the factors of f in $K[x]$ have even degree, and $t_K = 1$ otherwise. We let $u_K = 0$ if there is a quadratic extension of K contained in L_K, and $u_K = 1$ otherwise. If K is a p-adic field, we let $r_K = 0$ if all the ramification indices of the field extensions $L_{K,j}/K$ are even, and $r_K = 1$ otherwise. Similarly, we let $s_K = 0$ if all the residue class degrees of the field extensions $L_{K,j}/K$ are even, and $s_K = 1$ otherwise. Finally, we let $d_K = [K : \mathbb{Q}_2]$ if $p = 2$ and $d_K = 0$ if p is odd.

Lemma 5.7. *Let K be a p-adic local field. Then*

(1) $\dim J(K)/2J(K) = \dim J(K)[2] + d_K g = m_K - 1 - t_K + d_K g$.

(2) $\dim I_K = m_K - r_K - s_K$.

(3) $\dim H_K = 2 \dim I_K$ *if p is odd.*

(4) *If p is odd and $r_K = 1$, then* $\mathrm{val}_p : H_p \to I_p$ *is onto.*

Proof. (1) The first equality is shown in the same way as in Lemma 4.4. The second equality was proved in Lemma 5.6.

(2) The group $I(L_K)/I(L_K)^2$ has dimension m_K. The image of $I(K)/I(K)^2$ in it is trivial if and only if $r_K = 0$. The norm map from $I(L_K)/I(L_K)^2$ to $I(K)/I(K)^2$ is the zero map if $s_K = 0$ and has a kernel of codimension one otherwise.

(3) Since p is odd, there is an exact sequence

$$0 \to k^\times/(k^\times)^2 \to K^\times/(K^\times)^2 \to I(K)/I(K)^2 \to 0,$$

where k is the residue field of K. There is a similar sequence for L_K and ℓ_K, where ℓ_K denotes the product of the residue fields of the $L_{K,j}$. Then we have snake lemma diagrams

$$\begin{tikzcd}
0 \arrow[r] & \mathrm{Ker}_1 \arrow[r] \arrow[d] & \mathrm{Ker}_2 \arrow[r] \arrow[d] & \mathrm{Ker}_3 \arrow[r] \arrow[d] & {} \\
0 \arrow[r] & k^\times/(k^\times)^2 \arrow[r] \arrow[d] & K^\times/(K^\times)^2 \arrow[r] \arrow[d] & I(K)/I(K)^2 \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & \ell_K^\times/(\ell_K^\times)^2 \arrow[r] \arrow[d] & L_K^\times/(L_K^\times)^2 \arrow[r] \arrow[d] & I(L_K)/I(L_K)^2 \arrow[r] \arrow[d] & 0 \\
{} \arrow[r] & \ell_K^\times/(\ell_K^\times)^2 k^\times \arrow[r] & L_K^\times/(L_K^\times)^2 K^\times \arrow[r] & I(L_K)/I(L_K)^2 I(K) \arrow[r] & 0
\end{tikzcd}$$

and

$$\begin{tikzcd}
\mathrm{Cok}_4 \arrow[r] \arrow[d, equal] & \mathrm{Ker}_4 \arrow[r] \arrow[d] & H_K \arrow[r] \arrow[d] & I_K \arrow[r] \arrow[d] & {} \\
\mathrm{Cok}_4 \arrow[r] & \ell_K^\times/(\ell_K^\times)^2 k^\times \arrow[r] \arrow[d, "N"] & L_K^\times/(L_K^\times)^2 K^\times \arrow[r] \arrow[d, "N"] & I(L_K)/I(L_K)^2 I(K) \arrow[r] \arrow[d, "N"] & 0 \\
0 \arrow[r] & k^\times/(k^\times)^2 \arrow[r] \arrow[d] & K^\times/(K^\times)^2 \arrow[r] \arrow[d] & I(K)/I(K)^2 \arrow[r] \arrow[d] & 0 \\
{} \arrow[r] & \mathrm{Cok}_1 \arrow[r] & \mathrm{Cok}_2 \arrow[r] & \mathrm{Cok}_3 \arrow[r] & 0
\end{tikzcd}$$

We have denoted by Ker_j and Cok_j ($j = 1, 2, 3$) the obvious kernels and cokernels. Cok_4 is the cokernel of the map $\mathrm{Ker}_2 \to \mathrm{Ker}_3$, and Ker_4 is the kernel of the leftmost norm map in the second diagram.

From elementary considerations, we find

$$\dim \mathrm{Ker}_1 = \dim \mathrm{Cok}_3 = 1 - s_K \quad \text{and} \quad \dim \mathrm{Ker}_3 = \dim \mathrm{Cok}_1 = 1 - r_K.$$

Also, by local class field theory

$$\dim \mathrm{Ker}_2 = \dim \mathrm{Cok}_2 = 1 - u_K.$$

Hence

$$\begin{aligned}
\dim \mathrm{Cok}_4 &= \dim \mathrm{Ker}_2 - \dim \mathrm{Ker}_1 - \dim \mathrm{Ker}_3 \\
&= \dim \mathrm{Cok}_2 - \dim \mathrm{Cok}_1 - \dim \mathrm{Cok}_3 .
\end{aligned}$$

This implies $\dim H_K = \dim I_K + \dim \mathrm{Ker}_4$, and from the diagrams, it is easily read off that $\dim \mathrm{Ker}_4 = m_K - r_K - s_K = \dim I_K$.

(4) This follows from the second diagram above, noting that $\mathrm{Cok}_1 = 0$ when $r_K = 1$. ∎

Following our convention, we denote r_K, s_K, t_K and u_K by r_p, s_p, t_p and u_p, respectively, when $K = \mathbb{Q}_p$.

LEMMA 5.8. *The following combinations of the values of* r_p, s_p, t_p *and* u_p *are possible when* p *is odd. We use* $J/2J$ *to abbreviate* $J(\mathbb{Q}_p)/2J(\mathbb{Q}_p)$. *The fifth column indicates whether* $\mathbb{Q}_p$ *satisfies condition* (‡), *the last column indicates whether the map* $\mathrm{val}_p : H_p \to I_p$ *is onto or not.*

r_p	s_p	t_p	u_p	(‡)	$\dim J/2J$	$\dim J_p$	$\dim H_p$	$\dim I_p$	$H_p \twoheadrightarrow I_p$?
1	1	1	1	y	$m_p - 2$	$m_p - 2$	$2m_p - 4$	$m_p - 2$	y
1	1	0	1	n	$m_p - 1$	$m_p - 2$	$2m_p - 4$	$m_p - 2$	y
1	0	0	0	y	$m_p - 1$	$m_p - 1$	$2m_p - 2$	$m_p - 1$	y
0	1	0	1	n	$m_p - 1$	$m_p - 2$	$2m_p - 2$	$m_p - 1$	n
0	1	0	0	y	$m_p - 1$	$m_p - 1$	$2m_p - 2$	$m_p - 1$	y

Proof. By Lichtenbaum [10], there is a $\mathbb{Q}_p$-rational divisor class of degree $g - 1$. Since g is even, and since there are $\mathbb{Q}_p$-rational divisors of degree 2, there is a $\mathbb{Q}_p$-rational divisor class of degree one. By Lemma 5.1, this means that $\dim J(\mathbb{Q}_p)/2J(\mathbb{Q}_p)$ and $\dim J_p$ are equal if and only if $\mathbb{Q}_p$ satisfies condition (‡), otherwise they differ by one. On the other hand, (‡) is equivalent to $t_p = 1$ or $u_p = 0$. Together with the fact that $\dim J(\mathbb{Q}_p)/2J(\mathbb{Q}_p) = m_p - 1 - t_p$ (see part (1) of the preceding lemma), this explains columns 5, 6 and 7 of the table. Columns 8 and 9 are explained by the preceding lemma. From its proof, we can deduce that val_p is onto precisely when $1 + u_p = r_p + s_p$. This explains the last column. Note also that $r_p = 0$ or $s_p = 0$ implies $t_p = 0$, that $s_p = 0$ implies $u_p = 0$ and that $r_p = s_p = 0$ is impossible, since the degree of f is not divisible by four. Furthermore, $r_p = s_p = 1$ implies $u_p = 1$. This shows that all possible combinations of the first four entries are given in the table. ∎

With these preparations, we can again determine the image of δ_v for almost all places v of $\mathbb{Q}$. Recall that Φ_p denotes the group of components of the special fibre of the Néron model $\mathcal{J}$ of J over $\mathbb{Z}_p$.

LEMMA 5.9. *If* p *is odd, then the image of* $J(\mathbb{Q}_p)$ *in* I_p *under* $\mathrm{val}_p\,\delta_p$ *is isomorphic to the image of* $\Phi_p(\mathbb{F}_p)$ *in* $\Phi_p/2\Phi_p$.

Proof. By Lemma 5.2(3), the map δ_p^{nr} from $J(\mathbb{Q}_p^{\mathrm{nr}})/2J(\mathbb{Q}_p^{\mathrm{nr}})$ to H_p^{nr} is injective. Since I_p is again contained in H_p^{nr}, we can conclude in the same way as we did for Lemma 4.5. ∎

PROPOSITION 5.10. *If* p *is an odd prime not dividing the discriminant of* f, *then*

$$0 \to J(\mathbb{Q}_p)/2J(\mathbb{Q}_p) \xrightarrow{\delta_p} H_p \xrightarrow{\mathrm{val}_p} I_p \to 0$$

is an exact sequence. If we only assume that p^2 *does not divide* $\operatorname{disc}(f)$, *then we still have the exact sequence*

$$J(\mathbb{Q}_p)/2J(\mathbb{Q}_p) \xrightarrow{\delta_p} H_p \xrightarrow{\mathrm{val}_p} I_p \to 0.$$

Proof. If p does not divide the discriminant, we have $r_p = 1$ and $s_p = t_p$. By Lemma 5.8, val_p is surjective and $\mathbb{Q}_p$ satisfies condition (‡). This implies that δ_p is injective. It remains to show exactness at H_p. Since the dimensions match, it suffices to show that $\mathrm{val}_p \delta_p = 0$. This follows from Lemma 5.9, since $\Phi_p = 0$.

If p does divide $\operatorname{disc}(f)$, but p^2 does not, then we again have $\Phi_p = 0$, implying $\mathrm{val}_p \delta_p = 0$. Furthermore, one of the fields $L_{p,j}$ has ramification index 2 and residue class degree 1, whereas the remaining fields (there is at least one) are unramified. Hence $r_p = s_p = 1$, and Lemma 5.8 shows that val_p is onto and that $\dim H_p = \dim J_p + \dim I_p$. Together with $\mathrm{val}_p \delta_p = 0$, this implies exactness at H_p. ■

Corollary 5.11. *Let* $S = \{\infty, 2\} \cup \{p \mid p^2$ *divides* $\operatorname{disc}(f)\}$. *Then*

$$\begin{aligned}\mathrm{Sel}^{(2)}_{\mathrm{fake}}(\mathbb{Q}, J) = \{\xi \in H \mid \mathrm{val}(\xi) \in I_S(L)/I_S(L)^2 I_S(\mathbb{Q}),\\ \mathrm{res}_v(\xi) \in \delta_v(J(\mathbb{Q}_v)) \textit{ for all } v \in S\}.\end{aligned}$$

Now it is time to consider the question of how to represent the fake Selmer group, or more generally, a finite subgroup of $L^\times/(L^\times)^2\mathbb{Q}^\times$. Consider the following diagram:

(5.1)
$$\begin{tikzcd}
0 \arrow[r] & \mathrm{Ker} \arrow[r] \arrow[d, equal] & \mathrm{Sel}_2 \arrow[r] \arrow[d] & \mathrm{Sel}_1 \arrow[r] \arrow[d] & \mathrm{Sel}^{(2)}_{\mathrm{fake}}(\mathbb{Q}, J) \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & \mathrm{Ker} \arrow[r] & \mathbb{Q}^\times/(\mathbb{Q}^\times)^2 \arrow[r] & L^\times/(L^\times)^2 \arrow[r] & L^\times/(L^\times)^2\mathbb{Q}^\times \arrow[r] & 0
\end{tikzcd}$$

We define Ker to make the bottom row exact. A good way to represent $\mathrm{Sel}^{(2)}_{\mathrm{fake}}(\mathbb{Q}, J)$ is to find finite subgroups Sel_1 and Sel_2 of $L^\times/(L^\times)^2$ and $\mathbb{Q}^\times/(\mathbb{Q}^\times)^2$, respectively, that make the top row exact. Note that $\mathrm{Ker} = 0$ if there is no quadratic extension of $\mathbb{Q}$ contained in L, and $\mathrm{Ker} = \langle d \rangle$ is one-dimensional if $\mathbb{Q}(\sqrt{d})$ is contained in L. The group Sel_2 will be simplest to deal with when it is the span of -1 and some primes. The following proposition gives an indication of how we can proceed.

Proposition 5.12. *Let* G_p *be the image of* $J(\mathbb{Q}_p)$ *in* I_p, *and recall that* $r_p = 0$ *if and only if all the fields* $L_{p,j}$ *have even ramification index. Let* Sel_2 *be the span in* $\mathbb{Q}^\times/(\mathbb{Q}^\times)^2$ *of* $\{-1\} \cup S'$, *where*

$$S' = \{p \mid r_p = 0 \textit{ or } G_p \neq 0\}.$$

Define

$$\widetilde{H} = \{\xi \in L^\times/(L^\times)^2 \mid \widetilde{\mathrm{val}}(\xi) \in I_{S'}(L)/I_{S'}(L)^2 \textit{ and } \mathrm{val}_p(\xi) \in G_p \textit{ for all } p \in S'\},$$

where $\widetilde{\mathrm{val}}$ *is the canonical map from* $L^\times/(L^\times)^2$ *to* $I(L)/I(L)^2$*. Then* $\widetilde{H}$ *is finite. Let* $S = S' \cup \{\infty, 2\}$ *and set*

$$\mathrm{Sel}_1 = \{\xi \in \widetilde{H} \mid \mathrm{res}_v(\xi) \in J_v \textit{ for all } v \in S\}.$$

Then with these definitions of Sel_1 *and* Sel_2*, the top row in the diagram* (5.1) *is exact.*

Proof. It is clear that $\widetilde{H}$ is finite (compare the odd degree case).

If p is a prime outside S', then $G_p = 0$. This implies that $\mathrm{Sel}^{(2)}_{\mathrm{fake}}(\mathbb{Q}, J)$ is contained in

$$H' = \{\xi \in L^\times/(L^\times)^2\mathbb{Q}^\times \mid \mathrm{val}(\xi) \in I_{S'}(L)/I_{S'}(L)^2 I_{S'}(\mathbb{Q}), \mathrm{val}_p(\xi) \in G_p \text{ for all } p \in S'\}.$$

If p is odd and $r_p = 1$, then by Lemma 5.8, we have $\dim H_p = \dim J_p + \dim I_p$. Furthermore, $\mathrm{val}_p : H_p \to I_p$ is onto. Therefore, if $G_p = 0$, then $J_p = \ker \mathrm{val}_p$. Hence

$$\mathrm{Sel}^{(2)}_{\mathrm{fake}}(\mathbb{Q}, J) = \{\xi \in H' \mid \mathrm{res}_v(\xi) \in J_v \text{ for all } v \in S\}.$$

Since $\mathbb{Q}$ has trivial class group, $\widetilde{H}$ surjects onto H', and by definition, Sel_1 is the inverse image of $\mathrm{Sel}^{(2)}_{\mathrm{fake}}(\mathbb{Q}, J)$ in $\widetilde{H}$. The kernel of $\widetilde{H} \twoheadrightarrow H'$ is the intersection of $\widetilde{H}$ with the image of $\mathbb{Q}^\times/(\mathbb{Q}^\times)^2$ in $L^\times/(L^\times)^2$, which is the same as the image of the kernel of the composition $\mathbb{Q}^\times/(\mathbb{Q}^\times)^2 \to L^\times/(L^\times)^2 \to I_{S'}(L)/I_{S'}(L)^2$. This kernel is easily seen to equal Sel_2. ■

Remark. It is possible to remove from S those odd primes p that have $G_p = 0$ (and $r_p = 0$) and are such that L_p contains a quadratic extension of $\mathbb{Q}_p$. The reason is that one can show that in this case, we again have $J_p = \ker \mathrm{val}_p$, compare Lemma 5.8. Note also that by Proposition 5.10, any odd prime $p \in S'$ must satisfy $p^2 \mid \mathrm{disc}(f)$.

We get the following outline of the algorithm.

(0) Perform steps (0.1) through (0.5) in order to determine whether $\mathbb{Q}$ satisfies condition (‡) or not. If it does not, we also prepare the necessary data for deciding whether $\mathbb{Q}_v$ satisfies condition (‡) or not, for any given v.

(1) Let $S' = \{2\} \cup \{p \mid p^2 \text{ divides } \mathrm{disc}(f)\}$ and set $S = S' \cup \{\infty\}$.

(2) For all $v \in S$, compute the local images $J_v = \delta_v(J(\mathbb{Q}_v)) \subset H_v$ and (for $v \neq \infty$) $G_v = \mathrm{val}_v(J_v) \subset I_v$.

(3) Remove from S' all primes p that have $G_p = 0$ and $r_p = 1$. Remove from S all odd primes p that have $G_p = 0$ and ($r_p = 1$ or $u_p = 0$).

(4) Find a basis of $\widetilde{H}$ as defined in Proposition 5.12.

(5) Find Sel_1 as the inverse image of $\prod_{v\in S} J_v$ under $\prod_{v\in S}\mathrm{res}_v : \widetilde{H} \to \prod_{v\in S} H_v$. Let $\mathrm{Sel}_2 \subset \mathbb{Q}^\times/(\mathbb{Q}^\times)^2$ be the span of $\{-1\}\cup S'$. Let $\mathrm{Sel}_3 \subset \mathrm{Sel}_2$ be the trivial group if L does not contain a quadratic extension of $\mathbb{Q}$, and let Sel_3 be generated by d if $L \supset \mathbb{Q}(\sqrt{d})$. Then there is an exact sequence

$$0 \to \mathrm{Sel}_3 \to \mathrm{Sel}_2 \to \mathrm{Sel}_1 \to \mathrm{Sel}^{(2)}_{\mathrm{fake}}(\mathbb{Q}, J) \to 0.$$

In particular,

$$\dim \mathrm{Sel}^{(2)}_{\mathrm{fake}}(\mathbb{Q}, J) = \dim \mathrm{Sel}_1 - \dim \mathrm{Sel}_2 + \dim \mathrm{Sel}_3\,.$$

If we let $t = 0$ if all irreducible factors of f in $\mathbb{Q}[x]$ have even degree and $t = 1$ otherwise, and $u = 0$ if there is a quadratic extension of $\mathbb{Q}$ contained in L, $u = 1$ otherwise, then we finally get the formula

$$(5.2)\quad \operatorname{rank} J(\mathbb{Q}) + \dim Ш(\mathbb{Q}, J)[2] = \dim \mathrm{Sel}_1 - \#S' - m + 1 + t(1-u).$$

Note that condition (‡) is equivalent to $(1-t)u = 0$, that $\dim J(\mathbb{Q})[2] = m - 1 - t$, that $\dim \mathrm{Sel}_2 = \#S' + 1$, and that $\dim \mathrm{Sel}_3 = 1 - u$.

As in the odd degree case, we get a bound on the rank from the knowledge of $\dim \widetilde{H}$ only, which can be found as in the odd degree case; see also below.

Lemma 5.13. *We have the following inequality*:

$$\operatorname{rank} J(\mathbb{Q}) + \dim Ш(\mathbb{Q}, J)[2] \le \dim \widetilde{H} - \#S' - m + 1 - tu.$$

Proof. Trivially, $\mathrm{Sel}_1 \subset \widetilde{H}$. When $t = 1$, then we can find elements in $\widetilde{H}$ with norm -1. (Construct an element of L by taking it to be -1 in a field L_j of odd degree and 1 in every other field L_j. This element has norm -1 and gives rise to an element of $\widetilde{H}$.) Hence $\dim \mathrm{Sel}_1 \le \dim \widetilde{H} - t$, and the claim follows from equation (5.2). ∎

We discuss some of the main steps in more detail.

Step (2). The method is the same as in the odd degree case. We know the dimension of $J(\mathbb{Q}_v)/2J(\mathbb{Q}_v)$, and we can decide whether δ_v has nontrivial kernel on $J(\mathbb{Q}_v)/2J(\mathbb{Q}_v)$ by checking whether $\mathbb{Q}_v$ satisfies condition (‡) or not. Hence we know the dimension of J_v. For details, see Section 6.

In the case $v = \infty$, we have the following analogue of Lemma 4.8.

Lemma 5.14. (1) $\dim J(\mathbb{R})/2J(\mathbb{R}) = \dim J_\infty = \dim J(\mathbb{R})[2] - g$.

(2) *J_∞ is generated by the $\delta_\infty(P + Q - \mathfrak{m})$ with $P, Q \in C(\mathbb{R})$, and $\delta_\infty(P + Q - \mathfrak{m})$ only depends on the connected components of $C(\mathbb{R})$ containing P and Q.*

Proof. The proof is straightforward. ∎

From this, the procedure is very similar to that in the odd degree case. We only have to be careful to take the sign of the leading coefficient of f into account when we determine the connected components of $C(\mathbb{R})$.

Step (4). A basis of $\widetilde{H}$ is constructed in the same way as in the odd degree case. Instead of the group G_p (for $p \in S'$), we have to use its preimage $\widetilde{G}_p$ in $I_p(L)/I_p(L)^2$ when extending the basis of $\ker(\mathrm{val} : L^\times/(L^\times)^2 \to I(L)/I(L)^2)$ to a basis of $\widetilde{H}$, but apart from this small difference, everything proceeds in exactly the same fashion as before.

We note that $\dim \widetilde{H} = m_\infty + \dim \mathrm{Cl}(L)[2] + \dim \ker(\widetilde{G} \to \mathrm{Cl}(L)/2\mathrm{Cl}(L))$, where $\widetilde{G} = \prod_{p \in S'} \widetilde{G}_p$. We remark that we could remove all p with $r_p = 0$ and $G_p = 0$ from S' in this formula, since in this case $\widetilde{G}_p = G_p = 0$.

As an example, consider the curve given by the equation

$$y^2 = x^6 - 56x^5 + 176x^4 + 74x^3 - 81x^2 - 282x + 169.$$

This curve is one in a list of genus 2 curves with small coefficients and many rational points constructed by Colin Stahlke. The divisor classes of degree zero containing divisors supported in small rational points on the curve generate a subgroup of $J(\mathbb{Q})$ of rank 12. The discriminant is a power of 2 times the product of the two primes 27605791 and 12261635838401, so 2 is the only really bad prime. After computing the local image at $p = 2$, one sees that G_2 is trivial. Since the class group of the number field L defined by the right hand side is $(\mathbb{Z}/2\mathbb{Z})^8$ and there is no quadratic subfield, Lemma 5.13 tells us that the rank is bounded by

$$(5 + 8) - 1 - 1 + 1 - 0 = 12.$$

(We have $m = 1$, $m_\infty = 5$, $t = 0$ and $S = \{2\}$; note that 2 is ramified in L, so $r_2 = 0$.) Hence the rank *is* 12.

6. Local images.

6. Local images. In this section, we will discuss how we can find the local image J_p of $J(\mathbb{Q}_p)/2J(\mathbb{Q}_p)$ in H_p. We assume that we know $\dim J_p$ beforehand. The basic procedure is to construct points in $J(\mathbb{Q}_p)$ and to compute their image in H_p until these images generate a subspace of the right dimension.

Let K be an arbitrary field extension of $\mathbb{Q}$. We extend the definition of δ_K to all K-rational divisors on C. Essentially, we put

$$\delta_K\Big(\sum_P n_P \cdot P\Big) = \prod_P (x(P) - \theta)^{n_P} \bmod (L_K^\times)^2 \text{ or } (L_K^\times)^2 K^\times.$$

This is defined for divisors $\mathcal{D} \in \mathrm{Div}(C)(K)$ with support not containing points at infinity or points with zero y-coordinate. In [16] and [13], it is shown that δ_K is trivial on principal divisors. We therefore can extend its definition to all K-rational divisors if we move a divisor in its linear equivalence class when necessary. Explicitly, we get the following.

For divisors $\mathcal{D}$ supported at the point(s) at infinity, we simply have $\delta_K(\mathcal{D}) = 1$. If $\mathcal{D}$ is a prime divisor that is the sum of points $(\alpha, 0)$, where α runs through the zeros of a monic irreducible factor $h(x) \in K[x]$ of $f(x)$, we get

$$\delta_K(\mathcal{D}) = \begin{cases} (-1)^{\deg h}(h(\theta) - \widetilde{h}(\theta)) \bmod (L_K^\times)^2 & \text{if } \deg f \text{ is odd,} \\ h(\theta) - \widetilde{h}(\theta) \bmod (L_K^\times)^2 K^\times & \text{if } \deg f \text{ is even,} \end{cases}$$

where $f(x) = h(x)\widetilde{h}(x)$ in each case (compare Lemmas 4.3 and 5.6).

The following two lemmas provide us with the tools for constructing elements in J_p.

LEMMA 6.1. *Suppose that the degree of f is odd. Then the image of δ_K in H_K is generated by the images under δ_K of all prime divisors in* $\mathrm{Div}(C)(K)$ *of degree at most g.*

Proof. Let $\mathcal{D}$ be a K-rational divisor class of degree zero on C. Consider the divisor classes $\mathcal{D} + n \cdot \infty$ for $n = 0, 1, \ldots$ By Riemann–Roch, there is some $0 \le n \le g$ such that there is a unique effective divisor (of degree n) in $\mathcal{D} + n \cdot \infty$. Because this divisor is unique, it must be K-rational, and we can write it as a sum of prime divisors $\mathcal{P}_j$ over K of degree at most g. Hence,

$$\delta_K(\mathcal{D}) = \delta_K\Big(\sum_j \mathcal{P}_j - n \cdot \infty\Big) = \prod_j \delta_K(\mathcal{P}_j).$$

(Note that $\delta_K(\infty) = 1$.) ■

The even degree case is a little bit more involved. We let δ'_K be the following map.

$$\delta'_K : \mathrm{Div}(C)(K) \to H_K \times \mathbb{F}_2, \qquad \mathcal{D} \mapsto (\delta_K(\mathcal{D}), \deg \mathcal{D} \bmod 2).$$

LEMMA 6.2. *Suppose that the degree of f is even and that the genus is even. Let J'_p be the subspace of $H_K \times \mathbb{F}_2$ generated by the images under δ'_K of all prime divisors of degree at most g. Then $J_p = \{\xi \in H_K \mid (\xi, 0) \in J'_p\}$.*

Proof. Recall that $\mathfrak{m}$ is the divisor given by the sum of the two points at infinity on C. Again from Riemann–Roch, every point $P \in J(K)$ is represented by a K-rational divisor of the form $\mathcal{D} - n \cdot \mathfrak{m}$, where $\mathcal{D}$ is effective of degree $2n$, and $2n \le g$. (This uses the fact that g is even.) We can write $\mathcal{D}$ as a sum of prime divisors of degrees at most g. Therefore, $\delta'_K(\mathcal{D} - n \cdot \mathfrak{m}) = (\delta_K(\mathcal{D}), 0) \in J'_p$. The converse is obvious. ■

Now we specialise to the case that $K = \mathbb{Q}_p$. We need some means to cut down the work for the determination of J_p to a finite amount of computation.

Lemma 6.3. *Let $\{\alpha_j\}$ denote the zeros of f in $\overline{\mathbb{Q}}_p$, and let K be a finite extension of $\mathbb{Q}_p$ with p-adic absolute value $|\cdot|$, which we extend to $\overline{\mathbb{Q}}_p$. Let $x, x' \in K$.*

(1) If $|x - x'| < |4| \cdot |x - \alpha_j|$ for all j, then $f(x')$ is a square in K if and only if $f(x)$ is a square in K. When this is the case, let $P = (x, y)$ and $P' = (x', y')$ be points in $C(K)$. Then $\delta_K(P) = \delta_K(P')$.

(2) If $|x - \alpha_i| < |4| \cdot |x - \alpha_j|$ for some i and all $j \neq i$, and $P = (x, y)$ is a point in $C(K)$, then $\alpha_i \in K$, and $\delta_K(P) = \delta_K((\alpha_i, 0))$.

(3) If $|x| > |4|^{-1}$ and $P = (x, y)$ is a point in $C(K)$, then $\delta_K(P) = 1$.

Proof. For elements $x, x' \in R^\times$, where R is some ring, we write $x \sim_R x'$ if $x/x' \in (R^\times)^2$. We claim that for elements $x, y, z \in K$, we have

$$|x - y| < |4| \cdot |x - z| \;\Rightarrow\; x - z \sim_K y - z.$$

For the proof, we write $y - z = (x - z)(1 + w)$ with $|w| < |4|$. Hence $1 + w$ is a square, and the claim follows.

(1) The condition implies that $x' - \alpha_j \sim_{K(\alpha_j)} x - \alpha_j$ for all j. By Galois theory, this means $x' - \theta \sim_{L_K} x - \theta$. This already proves the second claim. Taking norms, we see that $f(x') \sim_K f(x)$. This proves the first claim.

(2) If $x = \alpha_i$, there is nothing to prove. Hence we assume that $x \neq \alpha_i$. The condition implies first that $\alpha_i \in K$ by Krasner's Lemma (see [17, II, Ex. 2.1]), and then that $x - \alpha_j \sim_{K(\alpha_j)} \alpha_i - \alpha_j$ for all $j \neq i$. Setting $h(x) = f(x)/(x - \alpha_i) = c \prod_{j \neq i}(x - \alpha_j)$, we also have

$$y^2 = f(x) = (x - \alpha_i)h(x) \sim_{K(\alpha_i)} (x - \alpha_i)h(\alpha_i).$$

This implies that $x - \alpha_j \sim_{K(\alpha_j)} (\alpha_i - \alpha_j) + h(\alpha_j)$ for *all* j and hence

$$\delta_K(P) \equiv x - \theta \equiv (\alpha_i - \theta) + h(\theta) \equiv \delta_K((\alpha_i, 0)) \bmod (L_K^\times)^2 \text{ or } (L_K^\times)^2 K^\times.$$

(3) The condition implies that $y^2 = f(x) \sim_K cx^n$, where c is the leading coefficient of f and n is its degree. When n is odd and $c = 1$, this means that x is a square. Since all the α_j are integral, the condition then also implies that $x - \theta$ is a square in L_K, whence $\delta_K(P) = 1$.

When n is even, we have in any case $x - \theta \sim_{L_K} x$, and hence $\delta_K(P) \equiv x \equiv 1 \bmod (L_K^\times)^2 K^\times$, since $x \in K^\times$. ∎

Let K be some finite extension of $\mathbb{Q}_p$. Then the following diagram obviously commutes:

$$\begin{tikzcd}
\mathrm{Div}(C)(K) \arrow[r, "\mathrm{Tr}_{K/\mathbb{Q}_p}"] \arrow[d, "\delta_K"] & \mathrm{Div}(C)(\mathbb{Q}_p) \arrow[d, "\delta_p"] \\
H_K \arrow[r, "N_{K/\mathbb{Q}_p}"] & H_p
\end{tikzcd}$$

The upper horizontal map is the trace map, the lower horizontal map is induced from the norm map $K \to \mathbb{Q}_p$. In more down-to-earth terms, this means the following. Suppose we have a prime divisor $\mathcal{P} \in \operatorname{Div}(C)(\mathbb{Q}_p)$ of degree d. Then there is a field extension K of $\mathbb{Q}_p$ of degree d and a point $P = (x, y) \in C(K)$ such that $\mathcal{P} = \operatorname{Tr}_{K/\mathbb{Q}_p}(P)$. Let h be the characteristic polynomial of x. Then the diagram tells us that $\delta_p(\mathcal{P}) \equiv (-1)^{\deg h} h(\theta)$.

By Lemmas 6.1 and 6.2, we have to take all extensions K of $\mathbb{Q}_p$ of degree at most g, and for each of them, we must find the image of $C(K)$ under $\delta_p \operatorname{Tr}_{K/\mathbb{Q}_p}$. In practice, we will stop as soon as the span of the values has attained the right dimension. In order to save work, we will look at the extensions of low degree first, in the hope that it will not be necessary to look at high degree extensions at all. The following algorithm finds this image for a given K, when p is odd. Let $v : K^\times \twoheadrightarrow \mathbb{Z}$ be the normalised valuation, let $\mathcal{O}$ be the integers of K, let π be a uniformiser, and let $k = \mathcal{O}/\pi\mathcal{O}$ be the residue field.

```
Input:    $f \in \mathcal{O}[x]$, $T \subset H_p$
Output:    $T \cup \delta_p \operatorname{Tr}_{K/\mathbb{Q}_p}(C(K))$

delta($f$, $T$, $K$) :
  $T$ := $T \cup \{\delta_p \operatorname{Tr}_{K/\mathbb{Q}_p}((\alpha, 0)) \mid \alpha \in K$ with $f(\alpha) = 0\}$;
  return delta_rec($f$, 0, 1, $T$).

delta_rec($f$, $\xi_0$, $a$, $T$) :
  for $\xi \in k$:
    fx := $f(\xi)$    $(\in k)$;
    if fx = 0 then
      fx1 := $f'(\xi)$    $(\in k)$;
      if fx1 = 0 then
        $\xi_1$ := lift($\xi$, $\mathcal{O}$);
        if $v(f(\xi_1)) \geq 2$ then
          $T$ := delta_rec($\frac{1}{\pi^2} f(\xi_1 + \pi x)$, $\xi_0 + a\xi_1$, $a\pi$, $T$);
    else // fx $\neq 0$
      if fx $\in (k^\times)^2$ then
        $\xi_1$ := lift($\xi$, $\mathcal{O}$);
        $T$ := $T \cup \{(-1)^d$charpol$(\xi_0 + a\xi_1)(\theta) \bmod (L_p^\times)^2$ or $(L_p^\times)^2 \mathbb{Q}_p^\times\}$;
  return $T$.
```

Why does this algorithm work? We claim that delta_rec(f_n, ξ_n, π^n, T), where $f_n = \pi^{-2n} f(\xi_n + \pi^n x) \in \mathcal{O}[x]$, adjoins to T all images $\delta_p \operatorname{Tr}_{K/\mathbb{Q}_p}(P)$ with $P = (x, y) \in C(K)$ such that $v(x - \xi_n) \geq n$, except possibly those that are also images of $(\alpha, 0)$ for some zero $\alpha \in K$ of f. To see this, we first consider the `else` branch. Here, $f_n(\xi)$ is non-zero in k. If $f_n(\xi)$ is a non-square in k, then there is no point in $C(K)$ with x-coordinate satisfying the condition. If $f_n(\xi)$ is a square in k, then all x satisfying the condition give rise to points in $C(K)$. It is easily verified that for any two such x, x', we have $v(x-x') > v(x-\alpha)$ for all zeros α of f, hence by Lemma 6.3, δ gives the same value on all of them. We find it for some representative x and adjoin it to T.

If, on the other hand, $f_n(\xi)$ vanishes in k, we look at the derivative, $f_n'(\xi)$. If this does not vanish in k, then there is some zero α of f such that every x such that $(x-\xi_n)/\pi^n \equiv \xi$ is nearer to α than to every other zero of f. By Lemma 6.3 again, this implies that δ gives the same value on all those x, and this value is the same as that it takes on $(\alpha, 0)$. Since we have computed this value right at the beginning of the algorithm, we need not include it at this point. If $f_n'(\xi)$ does vanish in k, then it is easily seen that $f_n(\xi_1) \bmod \pi^2$ is independent of the representative $\xi_1 \in \mathcal{O}$ of $\xi \in k$ chosen. When $f_n(\xi_1)$ is not divisible by π^2, then there is no point in $C(K)$ with x-coordinate satisfying the condition. Otherwise, we can rescale f_n and set $f_{n+1}(x) = \pi^{-2} f_n(\xi_1 + \pi x) \in \mathcal{O}[x]$ and call `delta_rec` recursively. Since f is square-free, this cannot go on indefinitely, and the algorithm terminates.

The case $p = 2$ is somewhat more involved, since we cannot decide whether a unit is a square or not by just looking at its image in the residue field. This means that we have to modify the `else` branch of `delta_rec` accordingly. Essentially, we have to look at all lifts $\widetilde{\xi} \in \mathcal{O}/4\pi\mathcal{O}$ of ξ and check if $f(\widetilde{\xi})$ is a square in $\mathcal{O}/4\pi\mathcal{O}$ or not. The details are left to the reader. There is also the additional complication that points with non-integral x-coordinate can have non-trivial image under δ. This problem can be overcome by scaling the variable of f in such a way that $|\alpha| \le |4|$ for all zeros α of f with respect to the 2-adic absolute value; then the proof of Lemma 6.3 shows that points with non-integral x-coordinate have trivial image under δ. Another possibility is to look at `delta_rec_1`($x^{2g+2} f(1/x)$, 0, π, T), where `delta_rec_1` is like `delta_rec`, except that it takes the characteristic polynomial of the reciprocal of $\xi_0 + a\xi_1$.

In practice, we compute the image of δ_p or δ_p' on prime divisors supported on $y = 0$ at the very beginning and leave out the corresponding first step in the algorithm above. When p is odd and there is no 4-torsion in $J(\mathbb{Q}_p)$, then this image will be all we need. Otherwise, we find the points on C defined over extensions of $\mathbb{Q}_p$ of increasing degree, keeping track of the subspace of H_p or H_p' generated so far, until this subspace has reached the right dimension.

When the field K is Galois over $\mathbb{Q}_p$, or more generally, when it has non-trivial automorphisms, then we can save some time by considering only one representative of each $\mathrm{Aut}(K/\mathbb{Q}_p)$-orbit in K.

One problem has still to be dealt with, and this is that we have to find all extensions of a given degree $d \leq g$ of $\mathbb{Q}_p$. It is easy to find all tamely ramified extensions (see for example Lang [9, §§II.4, 5] or Neukirch [12, §II.7]). It is possible to find all the totally ramified extensions by classifying Eisenstein polynomials (see Krasner [8]). Below, we list the fields in the cases $p = d = 2$ and $p = d = 3$. This is sufficient for the 2-descent procedure when the genus is at most 3. Note that even for genus 2, it can be necessary to know the ramified extensions of $\mathbb{Q}_3$ of degree 3, when one wants to determine the parity of $\dim Ш(\mathbb{Q}, J)[2]$; see the next section.

The first result is straightforward, since every extension of degree 2 is obtained by adjoining a suitable square root.

Lemma 6.4. *There are six ramified extensions of* $\mathbb{Q}_2$ *of degree* 2. *They are generated by roots of the following Eisenstein polynomials*:

$$x^2 + 2x + 2, \quad x^2 + 2x - 2, \quad x^2 - 2, \quad x^2 + 2, \quad x^2 - 6, \quad x^2 + 6.$$

The case $d = p = 3$ requires more work, but is still fairly easily dealt with. We leave the proof as an exercise for the interested reader.

Lemma 6.5. *There are nine ramified extensions of* $\mathbb{Q}_3$ *of degree* 3. *They are generated by roots of the following Eisenstein polynomials*:

$$x^3 - 3, \quad x^3 + 6, \quad x^3 - 12, \quad x^3 + 3x - 3, \quad x^3 - 3x - 3,$$
$$x^3 - 3x^2 - 3, \quad x^3 + 3x^2 - 3, \quad x^3 + 3x^2 + 6, \quad x^3 + 3x^2 - 12.$$

If we do not want to find all these fields explicitly, for example when the genus is fairly large and we would have to construct all wildly ramified extensions of some $\mathbb{Q}_p$ with $p \geq 5$, we can use the following alternative approach. Either systematically or randomly, we choose a monic polynomial $h \in \mathbb{Q}_p[x]$ of degree $d \leq g$. This polynomial specifies an effective $\mathbb{Q}_p$-rational divisor of degree d on $\mathbb{P}^1$. We then check whether this divisor is the image of an effective $\mathbb{Q}_p$-rational divisor of degree d on C under the canonical map $C \to \mathbb{P}^1$. This is the case if the resultant with respect to the variable x of the polynomials $h(x)$ and $y^2 - f(x)$ has no irreducible factors in $\mathbb{Q}_p[y]$ that are polynomials in y^2. In this case, the image of $(-1)^d h(\theta)$ in H_p belongs to J_p (in the odd degree case; a similar statement holds in the even degree case). Lemma 6.3 shows that we can take $h \in \mathbb{Z}_p[x]$ when p is odd, and it gives bounds on the denominators of the coefficients when $p = 2$. From the same lemma, we can also deduce an estimate for the precision we need in the coefficients of h. The current implementation uses this approach and selects the polynomials randomly. This has the disadvantage, however, that it is possible that a generator of $J(\mathbb{Q}_p)/2J(\mathbb{Q}_p)$ has to be found in a p-adically tiny set, and it can take quite a long time to hit this set by chance. We therefore plan to implement the systematic approach described in the main part of this section.

7. Odd and even Jacobians. We have now learned how to find the size of the 2-Selmer group $\mathrm{Sel}^{(2)}(\mathbb{Q}, J)$ of the Jacobian J of a hyperelliptic curve C. By the fundamental equality (see (1.1))

$$\operatorname{rank} J(\mathbb{Q}) = \dim \mathrm{Sel}^{(2)}(\mathbb{Q}, J) - \dim J(\mathbb{Q})[2] - \dim Ш(\mathbb{Q}, J)[2],$$

this provides us with a bound on the Mordell–Weil rank of $J(\mathbb{Q})$. The size of the 2-torsion subgroup $J(\mathbb{Q})[2]$ is easily determined from the degrees of the irreducible factors of f in $\mathbb{Q}[x]$ (see Lemmas 4.4 and 5.7). On the other hand, information on $Ш(\mathbb{Q}, J)$ is notoriously difficult to come by. Luckily, in some cases it is possible to obtain a little bit of information, which then allows us to lower the bound for the rank by one. This will be the subject of this section. The main reference is Poonen and Stoll [14].

The relevant result for our purposes is the following.

Theorem 7.1. *Let N be the number of places v of $\mathbb{Q}$ such that there is no $\mathbb{Q}_v$-rational divisor of degree $g-1$ on C. This can only occur for $v \in \{2, \infty\}$ or v dividing the discriminant of f, hence N is a finite number. If N is odd*, *then* $\dim Ш(\mathbb{Q}, J)[2] \geq 1$. *Furthermore*, *if* $Ш(\mathbb{Q}, J)$ *is finite*, *then N and the dimension of* $Ш(\mathbb{Q}, J)[2]$ *have the same parity.*

Proof. See [14, Thm. 5, Thm. 8, Cor. 9, Thm. 11 and Cor. 12]. ∎

The places counted by N are called *deficient* for C.

The preceding theorem shows that when N is odd, we can reduce by one the bound for the Mordell–Weil rank of $J(\mathbb{Q})$ we have found from the dimension of the 2-Selmer group. Furthermore, if $Ш(\mathbb{Q}, J)$ is finite, then the difference between the improved bound and the actual rank is even. If N is even, then we cannot improve our bound, and the difference between the bound and the actual rank is again even, if $Ш(\mathbb{Q}, J)$ is finite.

We will now derive an algorithm that decides whether a place of $\mathbb{Q}$ is deficient for C or not, where C is a hyperelliptic curve given by $y^2 = f(x)$ as usual. Let us get rid of some trivial cases first.

If the curve has a $\mathbb{Q}$-rational point, then there are $\mathbb{Q}$-rational divisors of every degree and hence no place can be deficient. This holds in particular when f has odd degree, since then there is a $\mathbb{Q}$-rational point at infinity.

Further, note that there are always $\mathbb{Q}$-rational divisors of degree 2, for example $\mathfrak{m}$. If g is odd, then $g-1$ is even, and there are always $\mathbb{Q}$-rational divisors of degree $g-1$. Hence there are no deficient places in this case.

We may therefore assume that g is even and that f has degree $2g+2$. Then to have a $\mathbb{Q}_v$-rational divisor of degree $g-1$ is equivalent to having one of any odd degree, and this in turn is equivalent to having a point on C defined over some extension of $\mathbb{Q}_v$ of odd degree. By invoking the Riemann–Roch Theorem, we can bound the degree by $g+1$. So we will need an algorithm determining whether there is some point on C defined over such an extension.

Now suppose v is infinite. Then v is deficient if and only if $C(\mathbb{R}) = \emptyset$, which means that f has no real zeros and negative leading coefficient.

We may therefore assume that $v = p$ is finite. A straightforward approach is to try each of the extensions K of $\mathbb{Q}_p$ of odd degree $\leq g+1$ and see if there is a K-rational point on C. The following algorithm checks whether there is a point in $C(K)$ with integral x-coordinate. We let π denote a prime element of K, and we let $R \subset \mathcal{O}_K$ be a set of representatives of the residue field $k = \mathcal{O}_K/\pi\mathcal{O}_K$. As usual, v denotes the normalised valuation of K.

```
haspoint($f$,$K$,$\pi$,$R$) :
  if $f(0) = 0$ then return TRUE;
  if $f(0) \in (K^\times)^2$ then return TRUE;
  w := min($v$(coeff($f$,j)), j=1..deg($f$));
  if $f(0) \notin ((\mathcal{O}_K/\pi^{\mathtt{w}}\mathcal{O}_K)^\times)^2$ then return FALSE;
  for a $\in R$:
    if haspoint($f(\pi x + \mathtt{a})$,$K$,$\pi$,$R$) then return TRUE;
  return FALSE.
```

We simply call haspoint($(\pi x)^{\deg(f)} f(1/(\pi x))$,...) to check for points with non-integral x-coordinate.

In practice, for $g = 2$, say, this makes sense to use for small primes, in particular for $p = 2$, since the algorithm given below only works for odd primes. If the prime is large, there are too many elements in the residue field to check. For $g = 2$, $p = 2$, there are three fields to check ($\mathbb{Q}_2$, the unramified extension of degree 3 and $\mathbb{Q}_2(2^{1/3})$), which is fast enough.

To obtain a reasonably fast algorithm for large primes, we make use of the following two lemmas. We consider the curve $y^2 = f(x)$ over a p-adic field K with odd p. The *Newton polygon* of f is the lower convex hull of the points $(d, v(a_d))$ with $0 \leq d \leq \deg f$ such that $a_d \neq 0$, where a_d is the coefficient of x^d in $f(x)$. It is a sequence of line segments $[(d,w),(d',w')]$ (with $d < d'$), ordered by increasing d. The *slope* of the line segment above is defined to be $-(w'-w)/(d'-d)$.

Lemma 7.2. *If $f(0) = 0$, then C has a K-rational point. Otherwise, let P be the Newton polygon of f. If P has a segment of odd length, then C has a point defined over an extension of K of odd degree. Otherwise, if one of the coefficients of f corresponding to a vertex of P is a square in K, then again C has a point defined over an extension of K of odd degree. Otherwise, every point (ξ, η) defined over an extension of K of odd degree must have $v(\xi)$ equal to the slope of some segment of P; in particular, the denominator of this slope must be odd.*

LEMMA 7.3. *Write $f = \pi^n f_0$ with $f_0 \in \mathcal{O}_K[x]$ such that $\bar{f}_0$, its reduction mod π, is non-zero. If n is even and $\bar{f}_0$ is not of the form ug^2 with $u \in k^\times \setminus (k^\times)^2$ and $g \in k[x]$, then C has a point defined over an extension of K of odd degree. Otherwise, every such point (ξ, η) must have $v(f_0(\xi)) > 0$.*

These lemmas, which are not difficult to establish, give rise to the following algorithm. `def(`f`,`K`,`π`)` determines whether the curve has a point defined over an extension of K of odd degree. `def1` looks for points with x-coordinate of positive valuation, and `def2` looks for points with x-coordinate a unit.

```
def($f$,$K$,$\pi$) :
  return def1($f$,$K$,$\pi$) or def2($f$,$K$,$\pi$)
            or def1($x^{\mathrm{deg}(f)} f(1/x)$,$K$,$\pi$).

def1($f$,$K$,$\pi$) :
  if $f(0) = 0$ then return TRUE;
  if $f(0) \in (K^\times)^2$ then return TRUE;
  P := newton_polygon($f$,$\pi$);
  for all segments [(i1,j1),(i2,j2)] of P:
    if j2 $\geq$ j1 then return FALSE;
      // further segments correspond
      // to solutions with non-positive valuation
    if i2-i1 is odd then return TRUE;
      // segment of odd length
    if coeff($f$,i2) $\in (K^\times)^2$ then return TRUE;
    s := -(j1-j2)/(i1-i2); d := denominator(s);
    if d is odd then
      for $(K', \pi') \in$ totally_ramified_extensions($K, \pi,$ d):
        if def2($f((\pi')^{\mathrm{d \cdot s}} x)$,$K'$,$\pi'$) then return TRUE;
  return FALSE.

def2($f$,$K$,$\pi$) :
  n := valuation($f$,$\pi$);
  $\bar{f}$ := $f/\pi^{\mathrm{n}}$ mod $\pi$;
  u := leading_coefficient($\bar{f}$);
  F := factorisation($\bar{f}$);
  if n is even
     and (u $\in (k^\times)^2$ or some factor in F has odd multiplicity)
  then return TRUE;
  for all factors h $\neq x$ in F:
    d := deg(h);
    if d is odd then
```

```
        ($K'$,$\pi'$) := unramified_extension($K$,$\pi$,d);
        $\alpha$ := some element of $\mathcal{O}_{K'}$ reducing to a zero of h;
        if def1($f(x+\alpha)$,$K'$,$\pi'$) then return TRUE;
    return FALSE.
```

The data (K', π, α) needed in `def2` can be easily got as follows. Lift h to a monic polynomial $H \in \mathcal{O}_K[x]$ and set $K' = K[T]/(H(T))$, $\pi' = \pi$ and $\alpha = \overline{T}$.

The ramified extensions required in `def1` are more difficult to deal with; compare the discussion at the end of the preceding section. For example, if $g = 2$, the degree is at worst three, and there are either one or three such extensions if $p \neq 3$, depending on the existence of third roots of unity in $\mathbb{Q}_p$. Since we already know that there must be a point over an extension of degree three if there is any over an extension of odd degree, we can decide in practice which of the extensions needs to be considered. If $p = 3$, the situation is more difficult—there are 9 different totally ramified extensions of degree 3 to consider (see Lemma 6.5).

A variant of this algorithm for the case $g = 2$ forms part of our implementation of the 2-descent algorithm. The program switches to the `haspoint` algorithm when in `def1` it is required to loop through all the ramified extensions of degree three where $p = 3$. This is reasonable, since the residue field is small in this case.

References

[1] S. Bosch and Q. Liu, *Rational points of the group of components of a Néron model*, Manuscripta Math. 98 (1999), 275–293.

[2] S. Bosch, W. Lütkebohmert and M. Raynaud, *Néron Models*, Ergeb. Math. Grenzgeb. (3) 21, Springer, 1990.

[3] J. W. S. Cassels, *The Mordell–Weil group of curves of genus 2*, in: Arithmetic and Geometry, M. Artin and J. Tate (eds.), Vol. I, Birkhäuser, Boston, 1983, 27–60.

[4] J. W. S. Cassels and E. V. Flynn, *Prolegomena to a Middlebrow Arithmetic of Curves of Genus 2*, Cambridge Univ. Press, Cambridge, 1996.

[5] J. Cremona, *Algorithms for Modular Elliptic Curves*, 2nd ed., Cambridge Univ. Press, Cambridge, 1997.

[6] E. V. Flynn, B. Poonen and E. F. Schaefer, *Cycles of quadratic polynomials and rational points on a genus-two curve*, Duke Math. J. 90 (1997), 435–463.

[7] D. M. Gordon and D. Grant, *Computing the Mordell–Weil rank of Jacobians of curves of genus two*, Trans. Amer. Math. Soc. 337 (1993), 807–824.

[8] M. Krasner, *Nombre des extensions d'un degré donné d'un corps $\mathfrak{p}$-adique*, in: Les tendances géométriques en algèbre et théorie des nombres, Colloques Internationaux du C.N.R.S. 143, Paris, 1966, 143–169.

[9] S. Lang, *Algebraic Number Theory*, Grad. Texts in Math. 110, Springer, 1986.

[10] S. Lichtenbaum, *Duality theorems for curves over p-adic fields*, Invent. Math. 7 (1969), 120–136.

[11] J. S. Milne, *Arithmetic Duality Theorems*, Academic Press, Boston, 1986.

[12] J. Neukirch, *Algebraische Zahlentheorie*, Springer, 1992.

[13] B. Poonen and E. F. Schaefer, *Explicit descent for Jacobians of cyclic covers of the projective line*, J. Reine Angew. Math. 488 (1997), 141–188.

[14] B. Poonen and M. Stoll, *The Cassels–Tate pairing on polarized abelian varieties*, Ann. of Math. 150 (1999), 1109–1149.

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

[16] —, *Computing a Selmer group of a Jacobian using functions on the curve*, Math. Ann. 310 (1998), 447–471.

[17] J.-P. Serre, *Local Fields*, 2nd ed., Springer, New York, 1995.

[18] KANT/KASH is described in M. Daberkow, C. Fieker, J. Klüners, M. Pohst, K. Roegner and K. Wildanger: *KANT V4*, J. Symbolic Comput. 24 (1997), 267–283.

[19] MAGMA is described in W. Bosma, J. Cannon and C. Playoust, *The Magma algebra system I: The user language*, J. Symbolic Comput. 24 (1997), 235–265. (Also see the Magma home page at http://www.maths.usyd.edu.au:8000/u/magma.)

[20] PARI homepage: http://www.parigp-home.de/

Mathematisches Institut
Heinrich-Heine-Universität
Universitätsstr. 1
D-40 225 Düsseldorf, Germany
E-mail: stoll@math.uni-duesseldorf.de

Current address:
Max-Planck-Institut für Mathematik
P.O. Box 7280
D-53072 Bonn, Germany
E-mail: stoll@mpim-bonn.mpg.de

Received on 6.3.2000
and in revised form on 25.8.2000 (3769)