ON THE 2-SELMER GROUP OF JACOBIANS OF HYPERELLIPTIC CURVES.

DANIEL BARRERA SALAZAR, ARIEL PACETTI, AND GONZALO TORNARÍA

ABSTRACT. Let $\mathcal{C}$ be a hyperelliptic curve $y^2 = p(x)$ defined over a number field K with $p(x)$ integral of odd degree. The purpose of the present article is to prove lower and upper bounds for the 2-Selmer group of the Jacobian of $\mathcal{C}$ in terms of the class group of the K-algebra $K[x]/(p(x))$. Our main result is a formula relating these two quantities under some mild hypothesis. We provide some examples that prove that our lower and upper bounds are as sharp as possible.

As a first application, we study the rank distribution of the 2-Selmer group in families of quadratic twists. Under some extra hypothesis we prove that among prime quadratic twists, a positive proportion has fixed 2-Selmer group. As a second application, we study the family of octic twists of the genus 2 curve $y^2 = x^5 + x$.

1. INTRODUCTION

Let K be a number field and $\mathcal{C}$ be a hyperelliptic curve over K given by

$$\mathcal{C} : y^2 = p(x) = x^d + a_{d-1}x^{d-1} + a_{d-2}x^{d-2} + \cdots + a_1x + a_0, \tag{1.1}$$

where d is odd and the coefficients are integral (we do not assume $p(x)$ irreducible). Without loss of generality, we will assume that a_{d-1} is divisible by all prime ideals over 2 of K . Let J denote the Jacobian of $\mathcal{C}$ and g its genus. By Mordell's theorem, we know that the abelian group $J(K)$ is finitely generated. It is an important problem to determine its rank, namely the rank of its free part.

The standard algorithm to compute the rank of $J(K)$ is the so called "descent" method. The idea behind the 2-descent method is that the short exact sequence

$$\begin{tikzcd} 1 \arrow[r] & J[2] \arrow[r] & J(\overline{K}) \arrow[r, "\times 2"] & J(\overline{K}) \arrow[r] & 1, \end{tikzcd}$$

where $J[2]$ denotes the 2-torsion points on $J(\overline{K})$, induces a short exact sequence in cohomology $J(K)/2J(K) \hookrightarrow H^1(\mathrm{Gal}_K, J[2])$ (here Gal_K denotes the absolute Galois group $\mathrm{Gal}(\overline{\mathbb{Q}}/K)$). The so called *2-Selmer group*, denoted by $\mathrm{Sel}_2(J)$ (whose definition is recalled in Definition 2.2), is a subgroup of the cohomology group $H^1(\mathrm{Gal}_K, J[2])$. It is a finite dimensional $\mathbb{F}_2$-vector space whose understanding provides deep information of the rank of $J(K)$ (its dimension equals the rank of $J(K)$ plus the dimension of the elements of order 2 in the Tate-Shafarevich group).

The pioneer work of Brumer and Kramer ([BK77, Proposition 7.1]) gives an upper bound for the order of the 2-Selmer group of an elliptic curve

$$y^2 = f(x) = x^3 + ax + b,$$

2010 *Mathematics Subject Classification.* Primary: 11G05, Secondary: 11G40.

Key words and phrases. 2-Selmer group, quadratic twists.

DBS was supported by the MathAMSUD 2020018, FONDECYT 11201025 and PAI 77180007.

AP was partially supported by FonCyT BID-PICT 2018-02073 and by the Portuguese Foundation for Science and Technology (FCT) within project UIDB/04106/2020 (CIDMA).

GT was partially supported by CSIC–I+D 2020/651.

in terms of the 2-rank of the class group of $\mathbb{Q}[x]/(f(x))$ when $f(x)$ is irreducible (see also [Sch96]). One is led to expect that a similar phenomena should hold in general, namely the order of $\mathrm{Sel}_2(J)$ should be related to a ray class group of the K-algebra $K[x]/(p(x))$. In [Li19] Chao Li gave not only an upper bound, but also a lower bound of the 2-Selmer group of a rational elliptic curve in terms of the class group of $K[x]/(p(x))$ (under some hypothesis). Li's result was generalized to general number fields under less restricted hypothesis in [BSPT21]. Moreover, in [BSPT21] we provided a general framework which could be applied to more general situations, like the case of hyperelliptic curves $\mathcal{C}$. In the present article we pursuit this goal, obtaining a similar result. More precisely in this work:

(1) We obtain general bounds for $\dim_{\mathbb{F}_2}(\mathrm{Sel}_2(J))$.
(2) We obtain applications related to quadratic twists of hyperelliptic curves and certain families of hyperelliptic curves.

1.1. **Bounding the 2-Selmer group.** Attached to the curve $\mathcal{C}$ with equation $\mathcal{C} : y^2 = p(x)$ we consider the étale K-algebra $A_K = K[x]/(p(x))$. Our main result gives a lower and upper bound for $\mathrm{Sel}_2(J)$ in terms of a 2-class group similar to the one obtained in [BSPT21]. We denote by $\mathrm{Cl}(A_K)$ the class group of A_K as defined in §5 and we consider a group $\mathrm{Cl}_*(A_K, \mathcal{C})$ between the classical class group $\mathrm{Cl}(A_K)$ and the narrow class group (see definition 5.6). Our main result is the following.

Theorem 5.15. *Let K be a number field and $\mathcal{C}/K$ be a hyperelliptic curve. Suppose that hypotheses 5.2 hold. Then*

$$\dim_{\mathbb{F}_2} \mathrm{Cl}_*(A_K, \mathcal{C})[2] - \sum_{v \mid 2} \big(r_v - 1 - \dim_{\mathbb{F}_2}(\mathbb{V}_v)\big) \\ \leq \quad \dim_{\mathbb{F}_2} \mathrm{Sel}_2(J) \quad \leq \quad \dim_{\mathbb{F}_2} \mathrm{Cl}_*(A_K, \mathcal{C})[2] + g\,[K : \mathbb{Q}]\,.$$

The lower bound includes local correction terms (possibly zero) at places over 2 defined as follows. For $v \mid 2$ let K_v be the completion of K at v and k its residue field. Over K_v the polynomial $p(x)$ factors as $p(x) = p_{v,1}(x) \cdots p_{v,r_v}(x)$ so that $K_{v,i} = K_v[x]/p_{v,i}(x)$ is a field extension of K_v. We denote k_i the residue field of $K_{v,i}$ and let $\overline{T}_i$ be the image of x in k_i. The space $\mathbb{V}_v$ is defined as follows:

$$\mathbb{V}_v = \langle \mathrm{Tr}_{k_i/k}(\overline{T}_i) \ : \ i = 1, ..., r_v \rangle \subset k.$$

Under our assumption on a_{d-1} we have $\dim_{\mathbb{F}_2} \mathbb{V}_v \leq r_v - 1$ (see Lemma 3.7) so the last terms at the left hand side are all non-negative.

The best lower bound occurs when $\mathbb{V}_v$ has dimension equal to $r_v - 1$ for all $v \mid 2$, in which case the difference between the upper and the lower bound equals $g\,[K : \mathbb{Q}]$, exactly as in the case of elliptic curves studied in [BSPT21, Theorem 2.16]. For example, if $p(x)$ is irreducible over K_v then $r_v = 1$ and $\mathbb{V}_v = \{0\}$. Assuming the parity conjecture we can then deduce from our bounds the precise 2-Selmer rank when $g\,[K : \mathbb{Q}] = 1$, and also when $g\,[K : \mathbb{Q}] = 2$ and the root number has the right parity.

To our knowledge, the only previous general result to bound the 2-Selmer group of a hyperelliptic curve is due to Stoll. In [Sto01] Stoll developed a very nice algorithm to compute the 2-Selmer group of an hyperelliptic curve, and as a Corollary of his results ([Sto01, Lemma 4.10]), he obtained an upper bound for the 2-Selmer group similar to the one obtained by Brumer and Kramer (see also [Sch95]). A similar upper bound was obtained in [DLRW20] in the particular situation where $p(x)$ is the minimal polynomial of $\zeta_p + \zeta_p^{-1}$ (where ζ_p denotes a p-th root of unity) under the assumption that $(p-1)/2$ is a prime number. Note that our result improves theirs in the sense that we get the same upper bound when $p \equiv 3 \pmod 4$

(although we do not need to impose the condition $(p-1)/2$ to be a prime number), but we also get a lower bound.

The proof of our main result has two key ingredients. We start considering the long exact sequence in cohomology

$$1 \longrightarrow J(K)/2J(K) \longrightarrow \mathrm{H}^1(\mathrm{Gal}_K, J[2]) \longrightarrow \mathrm{H}^1(\mathrm{Gal}_K, J)[2]. \tag{1.2}$$

By a result of Cassels, the cohomology group $\mathrm{H}^1(\mathrm{Gal}_K, J[2])$ is isomorphic to $(A_K^\times/(A_K^\times)^2)_\square$. To get the upper bound, we need to assure that any cocycle in $\mathrm{H}^1(\mathrm{Gal}_{K_v}, J[2])$ coming from $J(K_v)$ is unramified at any odd place of A_K. Under Cassels isomorphism, this is equivalent to proving that the image of any point P in $J(K_v)$, a priori in $(A_{K_v}^\times/(A_{K_v}^\times)^2)_\square$, actually belongs to the class of integral elements $(A_{\mathcal{O}}^\times/(A_{\mathcal{O}}^\times)^2)_\square$ (a purely local computation, see Theorem 3.4). The hypotheses imposed are the ones needed for this statement to be true.

A second key ingredient is needed to get the lower bound: we need to construct points on $J(K_v)$. Luckily enough (by dimension reasons) this last hard problem only needs to be done at primes dividing 2. The spaces $\mathbb{V}_v$ appearing in Theorem 5.15 play a crucial role in this construction.

1.2. **Applications.** The present article contains two different applications of our main result. The first one concerns the study of quadratic twists of hyperelliptic curves. If $a \in K^\times$, then the quadratic twist of our hyperelliptic curve $\mathcal{C}$ by a is the curve

$$\mathcal{C}(a) : ay^2 = p(x).$$

If the polynomial $p(x)$ is irreducible, and the number a is divisible only by prime ideals which are inert or ramified in A_K/K, then the curve $\mathcal{C}(a)$ also satisfies the hypothesis of our main theorem as proved in Lemma 6.2. In particular, the rank of the 2-Selmer group of $\mathcal{C}(a)$ also satisfies the same bounds as $\mathcal{C}$ does. This allows us to prove:

Theorem 6.3. *Let $\mathcal{C}$ be an hyperelliptic curve satisfying hypotheses 5.2 over a number field K with odd narrow class number. Suppose that $p(x)$ is irreducible, and suppose furthermore that there is a principal prime ideal of K which is inert in A_K/K. Then among all quadratic twists by principal prime ideals, there exists a subset of positive density $\mathscr{S}$ such that the abelian varieties* $\mathrm{Jac}(\mathcal{C}(a))$ *have the same* 2*-Selmer group for all $a \in \mathscr{S}$.*

To our knowledge this is the first general result regarding 2-Selmer group distributions in quadratic twists of hyperelliptic curves.

A second application comes from a particular family of hyperelliptic curves considered in [Jęd21]. Let a be a non-zero integer, and consider the genus 2 hyperelliptic curve over $K = \mathbb{Q}$

$$\mathcal{C}(a) : y^2 = x^5 + ax.$$

Note that in this case, the polynomial on the right hand side is reducible. The surface $\mathrm{Jac}(\mathcal{C}(a))$ has some very interesting properties. For example, it has complex multiplication by $\mathbb{Z}[\zeta_8]$ (over the extension $\mathbb{Q}(\zeta_8)$), but it is also isogenous to the product of two elliptic curves over the field $\mathbb{Q}(\sqrt[4]{a})$ (see Corollary 6.6). In particular, they are all octic twists of the curve $\mathcal{C}(1)$.

What can be said of the rank of the surface $\mathrm{Jac}(\mathcal{C}(a))$? The point $(0,0)$ has order 2, giving a point in its 2-Selmer group. It follows from Lemma 6.8 that if a is square-free and $a \equiv 1 \pmod 4$, then $\mathcal{C}(a)$ satisfies the hypothesis of Theorem 5.15

at all primes except at the primes p dividing a. Still, one can provide an upper bound of the form

$$\dim_{\mathbb{F}_2} \operatorname{Sel}_2(\operatorname{Jac}(\mathcal{C}(a)) \leq \dim_{\mathbb{F}_2} \operatorname{Cl}_*(A_{\mathbb{Q}}, \mathcal{C}(a))[2] + 2 + \#\{p \, : \, p \mid a\}.$$

To give a complete description of the 2-Selmer rank of $\operatorname{Jac}(\mathcal{C}(a))$, we need to understand the class group of $\mathbb{Q}(\sqrt[4]{a})$. Although one expects that such a class group should be well understood, we could not find any reference in this direction.

Theorem 6.12. *If p is an odd prime, $p \equiv 3 \pmod 8$ then $\operatorname{Cl}(\mathbb{Q}[\sqrt{-1}, \sqrt[4]{p}])$ has odd cardinality.*

Then the class group $\operatorname{Cl}_*(A_{\mathbb{Q}}, \mathcal{C}(a))[2]$ is trivial, providing the bound, for p a prime congruent to 3 modulo 8,

$$1 \leq \dim_{\mathbb{F}_2} \operatorname{Sel}_2(\operatorname{Jac}(\mathcal{C}(-p)) \leq 3,$$

where the lower bound 1 comes from the existence of a 2-torsion point. Since the family does not have other 2-torsion points under our assumption (a prime) and the Tate-Shafarevich group of $\operatorname{Jac}(\mathcal{C}(-p))$ has order a square (by a result of Poonen-Stoll), the rank of $\operatorname{Jac}(\mathcal{C}(-p))$ belongs to the set $\{0, 1, 2\}$.

In Theorem 6.9 we prove that the root number of $\operatorname{Jac}(\mathcal{C}(-p))$ is -1 (assuming p prime and $p \equiv 3 \pmod 8$) so the parity conjecture implies that the rank of $\operatorname{Jac}(\mathcal{C}(-p))$ is always 1.

The article is organized as follows: Section 2 contains the basic definitions as well as some preliminary results used throughout this work. Section 3 contains the main local results needed to understand the 2-Selmer group of hyperelliptic curves defined over non-archimedean fields, including the definition of the (†) hypothesis (it is also part of hypotheses 5.2). Section 4 contains the needed results for archimedean places. Section 5 is devoted to prove Theorem 5.15. Section 6 contains the two main applications stated before, namely the study of quadratic twists and the particular family

$$\mathcal{C}(a) : y^2 = x^5 + ax.$$

At last, Section 7 contains different examples showing that both our upper and our lower bounds are attained.

Acknowledgments. We would like to thank Professor John Cremona for some fruitful discussions regarding the splitting of the surface considered in Section 6.2. We also would like to thank Davide Lombardo for explaining how to use his algorithm ([Lom19]) used to deduce such a splitting. Special thanks go to Alvaro Lozano-Robledo, who draw our attention that our previous result could be generalized to the case of hyperelliptic curves.

2. Preliminaries

Let K be a number field or a local field of characteristic 0, and let $\mathcal{O}$ be its ring of integers. By $\mathfrak{p} \subset \mathcal{O}$ we denote a maximal ideal (the unique one when K is local). Let $\mathcal{C}$ be the hyperelliptic curve over the field K given by the equation

$$\mathcal{C} : y^2 = p(x),$$

where $p(x) \in \mathcal{O}[x]$ is a *monic* polynomial of odd degree $d \geq 3$ and (without loss of generality) non-zero discriminant $\Delta(p)$. Furthermore, if K is a number field (or a local field of residual characteristic 2), we also assume that the coefficient of x^{d-1} is even, i.e. is divisible by all maximal primes of residual characteristic 2 (which always occurs after an integral translation). The hypothesis that $p(x)$ has non-zero discriminant implies that the curve $\mathcal{C}$ is a non-singular curve of genus

$$g = \operatorname{genus}(\mathcal{C}) = \frac{d-1}{2}. \tag{2.1}$$

Let J denote its Jacobian. Let us clarify a subtlety (for readers who never studied this problem before) on what we mean by a rational point on J. Let $\overline{K}$ denote an algebraic closure of K and $\mathrm{Gal}_K := \mathrm{Gal}(\overline{K}/K)$ its Galois group. There is a natural action of Gal_K on the group of divisors $\mathrm{Div}(\mathcal{C}_{/\overline{K}})$, on $\mathrm{Princ}(\mathcal{C}_{/\overline{K}})$ (the principal divisors) and on $\mathrm{Pic}(\mathcal{C}_{/\overline{K}})$ (the quotient of the two previous ones). The group $\mathrm{Pic}(\mathcal{C}) := \mathrm{Div}(\mathcal{C}_{/\overline{K}})^{\mathrm{Gal}_K} / \mathrm{Princ}(\mathcal{C}_{/\overline{K}})^{\mathrm{Gal}_K} \hookrightarrow \mathrm{Pic}(\mathcal{C}_{/\overline{K}})^{\mathrm{Gal}_K}$. Although the curve $\mathcal{C}$ is singular at the infinity point $(0:1:0)$, the hypothesis on the polynomial $p(x)$ having odd degree implies that the desingularization of $\mathcal{C}$ at $(0:1:0)$ has a unique rational point that we denote by ∞. In particular, we have a rational map $\mathcal{C} \to J$ defined over K given by $P \to P - \infty$. Hence $\mathrm{Pic}(\mathcal{C}) = \mathrm{Pic}(\mathcal{C}_{/\overline{K}})^{\mathrm{Gal}_K}$ (see for example [PS97, Proposition 3.1]) so the two possible definitions of a rational point on J coincide.

Decompose $p(x)$ into its irreducible factors

$$p(x) = p_1(x) \cdots p_r(x),$$

where $p_i(x) \in \mathcal{O}[x]$ are all distinct (due to our assumption $\Delta(p) \neq 0$). For $i \in \{1, ...r\}$, let $d_i = \deg(p_i(x))$. Then the K-algebra $A_K = K[x]/(p(x))$ is étale, i.e., it decomposes as a product of fields

$$A_K \simeq K[x]/(p_1(x)) \times \cdots \times K[x]/(p_r(x)), \tag{2.2}$$

where each $K_i := K[x]/(p_i(x))$ is a finite field extension of K. By T we will denote the class of the variable x in A_K and by $(T_1, \ldots, T_r)$ its image under the isomorphism (2.2). Let $A_{\mathcal{O}}$ be the ring of integers of A_K, which is isomorphic to the product $\mathcal{O}_1 \times \cdots \times \mathcal{O}_r$ where $\mathcal{O}_i$ is the ring of integers of K_i.

Let $\mathcal{N} : A_K \to K$ denote the usual norm map (i.e. $\mathcal{N}(x)$ equals the determinant of the K-linear map given by multiplication by x), which gives a well defined map $\mathcal{N} : A_K^\times/(A_K^\times)^2 \to K^\times/(K^\times)^2$. Let $(A_K^\times/(A_K^\times)^2)_\square$ denote its kernel.

Theorem 2.1. *The group* $\mathrm{H}^1(\mathrm{Gal}_K, J[2])$ *is isomorphic to* $(A_K^\times/(A_K^\times)^2)_\square$.

Proof. See [Sch95, Theorem 1.1], which generalizes [Cas66, p. 240]. □

The exact sequence (1.2), with $m = 2$, then gives an injective morphism

$$\delta_K : J(K)/2J(K) \hookrightarrow (A_K^\times/(A_K^\times)^2)_\square.$$

One can give an explicit description of such a map for points on J which are not of order 2. Recall that $J(K)$ consists of degree zero divisors of $\mathcal{C}$ defined over K, hence it is spanned by divisors of the form

$$D = \sum_\sigma (\sigma(P) - \infty), \tag{2.3}$$

where $P \in \mathcal{C}(\overline{K})$ and the sum is over the different conjugates of P. By [Sto01, Lemma 4.1], if $y(P) \neq 0$ then we have

$$\delta_K(D) = \prod_\sigma (\sigma(x(P)) - T), \tag{2.4}$$

where $x(P)$ denotes the x-coordinate of the point P. When K is a number field, for each place v we have a similar injective morphism

$$\delta_v : J(K_v)/2J(K_v) \hookrightarrow (A_{K_v}^\times/(A_{K_v}^\times)^2)_\square$$

which can be explicitly described as done in (2.4).

Definition 2.2. The 2-Selmer group of J consists of the cohomology classes in $H^1(\mathrm{Gal}_K, J[2])$ whose restriction to Gal_{K_v} lies in the image of δ_v for all places v.

Under the isomorphism of Theorem 2.1, the 2-Selmer group of J corresponds to

$$\mathrm{Sel}_2(J) = \{[\alpha] \in (A_K^\times/(A_K^\times)^2)_\square :\ \mathrm{loc}_v([\alpha]) \in \mathrm{Im}(\delta_{K_v}) \text{ for each place } v \text{ of } K\},$$

where $\mathrm{loc}_v : (A_K^\times/(A_K^\times)^2)_\square \to (A_{K_v}^\times/(A_{K_v}^\times)^2)_\square$ is the natural map. This description of the 2-Selmer group coincides with the one given in [Sto01, Proposition 4.2] for $K = \mathbb{Q}$.

3. Some local non-Archimedean computations

The main reference for the first part of this section is the article [Sto01]. Let $p \geq 2$ be a prime number and let K be a finite extension of $\mathbb{Q}_p$, with ring of integers $\mathcal{O}$. Let $v : \overline{K}^\times \to \mathbb{Q}$ be the valuation normalized so that $v(K^\times) = \mathbb{Z}$. Set $d_2 = [K : \mathbb{Q}_2]$ if $p = 2$, and $d_2 = 0$ otherwise, so in any case $[\mathcal{O} : 2\mathcal{O}] = 2^{d_2}$. Recall the factorization

$$p(x) = p_1(x) \cdots p_r(x),$$

of $p(x)$ into irreducible polynomials.

Lemma 3.1. *Under the previous hypothesis and notations*

(1) $\dim_{\mathbb{F}_2} J(K)/2J(K) = r - 1 + d_2 \cdot g = \dim_{\mathbb{F}_2} J(K)[2] + d_2 \cdot g$.
(2) $\dim_{\mathbb{F}_2}(A_K^\times/(A_K^\times)^2)_\square = 2\dim_{\mathbb{F}_2} J(K)/2J(K)$.
(3) $\dim_{\mathbb{F}_2}(A_\mathcal{O}^\times/(A_\mathcal{O}^\times)^2)_\square = \dim_{\mathbb{F}_2} J(K)/2J(K) + d_2 \cdot g$.

Proof. The first two statements follow from [Sto01, Lemma 4.4]. The proof of the last statement follows the lines of the proof of [BSPT21, Lemma 1.5]. The decomposition $A_\mathcal{O} \simeq \mathcal{O}_1 \times \cdots \times \mathcal{O}_r$ implies that

$$[A_\mathcal{O}^\times : (A_\mathcal{O}^\times)^2] = \prod_{i=1}^r [\mathcal{O}_i^\times : (\mathcal{O}_i^\times)^2] = 2^r \prod_{i=1}^r [\mathcal{O}_i : 2\mathcal{O}_i] = 2^r [\mathcal{O} : 2\mathcal{O}]^d.$$

Since $\mathcal{N} : A_\mathcal{O}^\times/(A_\mathcal{O}^\times)^2 \to \mathcal{O}^\times/(\mathcal{O}^\times)^2$ is surjective, its kernel $(A_\mathcal{O}^\times/(A_\mathcal{O}^\times)^2)_\square$ has order $[A_\mathcal{O}^\times : (A_\mathcal{O}^\times)^2]/[\mathcal{O}^\times : (\mathcal{O}^\times)^2] = 2^{r-1}\,[\mathcal{O} : 2\mathcal{O}]^{d-1} = 2^{r-1}2^{d_2 \cdot 2g}$. The result then follows from the first statement. □

Recall that J has a Néron model $\mathcal{J}$ over $\mathcal{O}$, which provides a reduction map on $J(K)$. Following the standard notation, let $J^0(K)$ denote the set of points mapping into the identity component of $\mathcal{J}_k$ (where k denotes the residual field of K). Then there is an exact sequence

$$\begin{tikzcd} 1 \arrow[r] & J^0(K) \arrow[r] & J(K) \arrow[r] & \mathcal{J}_k \,/\, \mathcal{J}_k^0 \arrow[r] & 1. \end{tikzcd}$$

3.1. The condition (†).

Definition 3.2. The polynomial $p(x)$ satisfies condition (†) if either one of the following two conditions holds:

(†.i) The ring $\mathcal{O}[x]/(p(x))$ is isomorphic to the product $\prod_{i=1}^r \mathcal{O}[x]/(p_i(x))$.
(†.ii) The residual characteristic of K is odd and the order of the component group $[J(K) : J^0(K)]$ is odd.

Remark 3.3. Since the polynomials $p_1(x), \ldots, p_r(x)$ are prime to each other, there exists an injective map

$$\pi : \mathcal{O}[x]/(p(x)) \to \prod_{i=1}^r \mathcal{O}[x]/(p_i(x)). \tag{3.1}$$

The Chinese Remainder Theorem (CRT) states that if $\mathcal{O}[x]$ were a principal ideal domain, then the map π would be an isomorphism. Over the ring $\mathcal{O}[x]$ this might not be true, for example if $\mathcal{O} = \mathbb{Z}_2$ and $p(x) = x(x+2)$, the image of the map π consists of pairs of elements (a, b) in $\mathbb{Z}_2 \times \mathbb{Z}_2$ such that $a \equiv b \pmod 2$.

Let $\overline{\mathcal{O}}$ denote the ring of integers of an algebraic closure of K and let $\mathfrak{p}$ denote its maximal ideal. The hypothesis (†.i) (surjectivity of π) is equivalent to impose the condition that if α is a root of a polynomial $p_i(x)$ and β is a root of other polynomial $p_j(x)$, then $\mathfrak{p} \nmid \alpha - \beta$. Indeed, if $p(x)$ and $q(x)$ are two monic polynomials in $\mathcal{O}[x]$ without common roots, then

$$\mathcal{O}[x]/(p(x)q(x)) \simeq \mathcal{O}[x]/(p(x)) \times \mathcal{O}[x]/(q(x))$$

if and only if there exist polynomials $a, b \in \mathcal{O}[x]$ such that $1 = ap + bq$ (the usual CRT hypothesis). The proof that the condition is sufficient mimics the proof of the CRT. To prove the other implication, suppose that π is an isomorphism. Then the element $(1, 0)$ lies in its image so there exists $f \in \mathcal{O}[x]$ such that $\pi(f) = (1, 0)$. In particular $q \mid f$, so $f = bq$ for some $b \in \mathcal{O}[x]$ (here we use the fact that $q(x)$ is monic). Similarly, there exists $a \in \mathcal{O}[x]$ such that $\pi(ap) = (0, 1)$. But then $\pi(ap + bq) = \pi(1)$, so

$$1 = ap + bq + cpq.$$

A standard argument using resultants proves that $1 = ap+bq$ if and only if $\mathfrak{p} \nmid \alpha-\beta$ for any root α of p and any root β of q.

Here are two easy instances where the condition (†.i) is satisfied:

- The polynomial $p(x)$ is irreducible.
- $A_{\mathcal{O}}$ (the ring of integers of A_K) equals $\mathcal{O}[x]/(p(x))$.

These two cases correspond to the first two hypothesis of [BSPT21] (Definition 1.6) while studying the case of elliptic curves. Our assumption (†.i) is less restrictive (improving the results of loc. cit.).

Theorem 3.4. *If the polynomial $p(x)$ satisfies (†) then* $\operatorname{Im}(\delta_K) \subset (A_{\mathcal{O}}^\times/(A_{\mathcal{O}}^\times)^2)_\square$.

Before giving the proof, let us state a particular (and easy to prove) instance of the result.

Lemma 3.5. *Let $P = (a, b) \in \mathcal{C}(\overline{K})$ and suppose that $v(a) < 0$. Consider the divisor $D = \sum_\sigma (\sigma(p) - \infty) \in J(K)$ where the sum is over the different conjugates of P. Then $\delta_K(D) \in (A_{\mathcal{O}}^\times/(A_{\mathcal{O}}^\times)^2)_\square$. Moreover, if $p > 2$ then $\delta_K(D) = 1$.*

Proof. Suppose first that $P = (a, b) \in \mathcal{C}(K)$ and $v(a) < 0$. Equation (1.1), with the assumption that $p(x)$ has integral coefficients, implies that $b \neq 0$ and $2\,v(b) = d\,v(a)$. Since $b \in K^\times$ we have $v(b) \in \mathbb{Z}$ and so in particular $v(a)$ is even. Since $T_i \in \mathcal{O}_i$ for all $i = 1, \dots, r$, it follows that $v(a-T_i) = v(a)$ is even as well, hence, up to a square in $K_i^\times$, it can be taken to be a unit. Thus $\delta_K(P - \infty) = (a - T) \in (A_{\mathcal{O}}^\times/(A_{\mathcal{O}}^\times)^2)_\square$ as claimed.

In general, let $L = K(a, b)$ with ramification index e. The same argument as above, now using $v(b) \in \frac{1}{e}\mathbb{Z}$, shows that $e\,v(\sigma(a) - T_i)$ is even. Since $e \mid [L : K]$ it follows that $\prod_\sigma(\sigma(a) - T_i) \in K_i^\times$ has even valuation and the argument goes through to show

$$\delta_K(D) = \prod_\sigma (\sigma(a) - T) \in (A_{\mathcal{O}}^\times/(A_{\mathcal{O}}^\times)^2)_\square.$$

To prove the second claim, note that since $v(b) < v(a) < 0$ the divisor D lies in $J^0(K)$, the kernel of the reduction map. But $J^0(K)$ has a formal group structure, hence it is a pro-p-group and so $\delta_K(D) = 1$ if $p \neq 2$ (as it is an element of order at most 2). □

Proof of Theorem 3.4. Start supposing that (†.i) holds. The proof is similar to that due to Michael Stoll given in [BG13, Proposition 8.5]. Let us just recall the main ingredients: let $D = \sum_{i=1}^{m} P_i - m \cdot \infty$ be a degree zero divisor, which satisfies the following hypothesis (which can always be assumed):

- The value $x(P_i)$ is not a root of $p(x)$ (see [Sch95, Lemma 2.2]).
- The degree of D^+ (equal to m) is at most $\frac{d-1}{2}$ (by Riemann-Roch's theorem).
- The values $\{x(P_i)\}$ are all distinct.
- Each point P_i has integral coordinates (otherwise the result follows from Lemma 3.5).

To ease the notation, let $P_i = (a_i, b_i)$. Then

$$\delta_K(D) = \prod_{i=1}^{m} (a_i - T) = (-1)^m q(T),$$

where $q(x) = (x - a_1) \cdots (x - a_m) \in \mathcal{O}[x]$. There exists a unique $R(x) \in K[x]$ of degree $\leq m-1$ with $R(a_i) = b_i$. Observe that $R(x)^2 - p(x)$ vanishes at $\{a_1, \ldots, a_m\}$ so it is divisible by $q(x)$. Consider the following two cases:

Case 1: $R(x)$ has integral coefficients. Let $I_D \subset A_{\mathcal{O}}$ be the $\mathcal{O}[T]$-ideal generated by $(q(T), R(T))$.

Claim: $I_D^2 = (q(T))$ as $\mathcal{O}[T]$-ideals.

Indeed, since $p(T) = 0$, $q(T) \mid R(T)^2$. From this observation it is clear that $I_D^2 \subset (q(T))$. Then the proof of the claim follows from the fact that both ideals have the same norm (as proved in loc. cit.).

Clearly $\mathcal{O}[T] \subseteq \operatorname{End}(I_D) \subseteq \operatorname{End}(I_D^2) \subseteq \prod \mathcal{O}[T_i]$, where the last inequality follows from the claim. Then (†.i) implies they are all equalities, so $\operatorname{End}(I_D) = \mathcal{O}[T]$ (i.e. I_D is a proper ideal). As explained in [BG13], the ring $\mathcal{O}[T]$ is generated by a single element over $\mathcal{O}$, hence it is Gorenstein of dimension one. In particular, an $\mathcal{O}[T]$-ideal is principal if and only if it is proper, so I_D is indeed a principal $\mathcal{O}[T]$-ideal. It follows that $q(T)$ is a square up to a unit, thus $\delta_K(D) \in (A_{\mathcal{O}}^\times/(A_{\mathcal{O}}^\times)^2)_\square$. Note that when $m = 1$, $R(x)$ does have integral coefficients, so we have proven the statement (in both cases) for $m \leq 1$.

Case 2: $R(x)$ is not integral. Then $p(x) - R(x)^2$ is not integral, but it has at most $2m - 2$ integral roots. Since $a_1, \ldots, a_m$ are integral roots, there are other integral roots $\alpha_1, \ldots, \alpha_t$ (with $t \leq m - 2$). Let $\beta_i = R(\alpha_i)$. Then the divisor of $y - R(x)$ on $\mathcal{C}$ equals

$$D + D' + D''$$

where $D' = \sum_{i=1}^{t} [(\alpha_i, \beta_i) - \infty]$ and D'' is a sum of non-integral points. From Lemma 3.5 we know that $\delta_K(D'') \in (A_{\mathcal{O}}^\times/(A_{\mathcal{O}}^\times)^2)_\square$, hence $\delta_K(D) \in (A_{\mathcal{O}}^\times/(A_{\mathcal{O}}^\times)^2)_\square$ is equivalent to $\delta_K(D') \in (A_{\mathcal{O}}^\times/(A_{\mathcal{O}}^\times)^2)_\square$. Since the positive part of D' has degree at most $m - 2$ the claim follows by an inductive argument on m.

Suppose at last that (†.ii) holds. By [Sto01, Lemma 4.5], the valuation of the image of $J(K)$ under δ is isomorphic to the 2-group of connected components, which is trivial by hypothesis. □

Corollary 3.6. *Suppose that* $p(x)$ *satisfies* (†). *Then* $\operatorname{Im}(\delta_K) \subset (A_{\mathcal{O}}^\times/(A_{\mathcal{O}}^\times)^2)_\square$ *with index* $2^{d_2 \cdot g}$.

Proof. By Lemma 3.1, if $p \neq 2$ then both sets have the same cardinality, while when $p = 2$, the index equals $2^{d_2 \cdot g}$ as claimed. □

3.2. **The case $p = 2$.** Suppose for the rest of the section that K is a finite extension of $\mathbb{Q}_2$. The problem at even characteristic is that the image of the map δ_K is not the whole group $(A_{\mathcal{O}}^\times/(A_{\mathcal{O}}^\times)^2)_\square$ (as stated in Corollary 3.6), so we need to give a "lower bound" for the group $\operatorname{Im}(\delta_K)$. Ideally, the lower bound would be related to unramified extensions of A_K (justifying the class group formula in our main theorem), but this is not always the case.

As before, let $(T_1, \dots, T_r)$ denote the image of T under the isomorphism $A_K \simeq K_1 \times \cdots \times K_r$. Let k_i denote the residue field of K_i for each $i = 1, \dots, r$, and let k denote the residue field of K. Let $\overline{T_i}$ denote the image of T_i under the reduction map $\mathcal{O}_i \to k_i$. Let e_i denote the ramification degree of the extension K_i/K. Note that at least one of the e_i must be odd, since $d = \sum_{i=1}^r e_i[k_i : k]$ is odd.

Recall our assumption that the coefficient of x^{d-1} in $p(x)$ is "even" (i.e. divisible by any local uniformizer at places dividing 2).

Lemma 3.7. *Keeping the previous notation,*

$$\sum_{i=1}^{r} e_i \operatorname{Tr}_{k_i/k}(\overline{T}_i) = 0.$$

Proof. The coefficient of x^{d-1} in $p(x)$ equals the trace $\operatorname{Tr}_{A_K/K}(T)$ (an element of $\mathcal{O}_K$) which under the isomorphism $A_K \simeq K_1 \times \cdots \times K_r$ equals $\sum_{i=1}^r \operatorname{Tr}_{K_i/K}(T_i)$. The assumption on the coefficient of x^{d-1} implies that $\operatorname{Tr}_{A_K/K}(T)$ is congruent to zero modulo the maximal ideal $\mathfrak{p}$ of $\mathcal{O}_K$. Thus, the result follows from the well known equality

$$\operatorname{Tr}_{K_i/K}(T_i) \equiv e_i \operatorname{Tr}_{k_i/k}(\overline{T}_i) \pmod{\mathfrak{p}}.$$

□

Let $\mathbb{V}$ denote the $\mathbb{F}_2$-vector space

$$\mathbb{V} = \langle \operatorname{Tr}_{k_i/k}(\overline{T}_i) \;:\; i = 1, ..., r\rangle \subset k. \tag{3.2}$$

Lemma 3.7 implies that $\dim_{\mathbb{F}_2} \mathbb{V} \le r - 1$.

Definition 3.8. We say that $p(x)$ satisfies $(*)$ if $\dim_{\mathbb{F}_2} \mathbb{V} = r - 1$.

Theorem 3.9. *If $p(x)$ satisfies $(*)$ then it satisfies* (†.i).

Proof. Suppose that (†.i) does not hold, so by Remark 3.3 there exist a root (over $\overline{\mathcal{O}}$) α say of $p_1(x)$ and β of $p_2(x)$ such that $\mathfrak{p} \mid \alpha - \beta$. Let $\mathfrak{l} = k_1 \cap k_2$, so $\overline{T_1}$ and $\overline{T_2}$ are the same as elements of $\mathfrak{l}$ and satisfy the relation

$$[k_1 : \mathfrak{l}] \operatorname{Tr}_{k_2/k}(\overline{T_2}) = [k_2 : \mathfrak{l}] \operatorname{Tr}_{k_1/k}(\overline{T_1}).$$

In particular, the values $\{\operatorname{Tr}_{k_1/k}(\overline{T_1}), \dots, \operatorname{Tr}_{k_r/k}(\overline{T_r})\}$ in the $\mathbb{F}_2$-vector space k satisfy the following two relations:

- $e_1 \operatorname{Tr}_{k_1/k}(\overline{T_1}) + \cdots + e_r \operatorname{Tr}_{k_r/k}(\overline{T_r}) = 0$,
- $[k_2 : k] \operatorname{Tr}_{k_1/k}(\overline{T_1}) + [k_1 : k] \operatorname{Tr}_{k_2/k}(\overline{T_2}) = 0$.

But they also span an $r - 1$-dimensional subspace, so both equations must generate a 1-dimensional relations space. Then either $[k_1 : k] \equiv [k_2 : k] \equiv 0 \pmod 2$ (in which case $\operatorname{Tr}_{k_1:k}(\overline{T_1}) \equiv \operatorname{Tr}_{k_2:k}(\overline{T_2}) \equiv 0$, contradicting $(*)$) or $e_i \equiv 0 \pmod 2$ for all $i = 3, \dots, r$ and the vectors $([k_2 : k], [k_1 : k])$ and (e_1, e_2) are linearly dependent in $\mathbb{F}_2^2$. The hypothesis d odd implies that $\sum_{i=1}^r e_i[k_i : k]$ is odd, hence $e_1[k_1 : k] + e_2[k_2 : k]$ is also odd, so the determinant

$$\det \begin{pmatrix} e_1 & e_2 \\ [k_2 : k] & [k_1 : k] \end{pmatrix} \equiv 1 \pmod 2,$$

contradicting the fact that $([k_2 : k], [k_1 : k])$ and (e_1, e_2) are linearly dependent.

□

Corollary 3.10. *If $p(x)$ satisfies $(*)$ then* $\operatorname{Im}(\delta_K) \subset (A_{\mathcal{O}}^\times/(A_{\mathcal{O}}^\times)^2)_\square$.

Proof. Follows from the last theorem and Theorem 3.4. □

Remark 3.11. The condition $(*)$ is not equivalent to (†.i) as the following example shows. Let $K = \mathbb{Q}_8 = \mathbb{Q}_2[t]/(t^3 - t - 1)$, be the unramified cubic extension of $\mathbb{Q}_2$. Consider the hyperelliptic curve

$$\mathcal{C} : y^2 = x(x-1)(x-t)(x-t^2)(x-(1+t+t^2)).$$

Since all roots belong to K and are not congruent modulo its maximal ideal, the curve $\mathcal{C}$ satisfies (†.i). However, condition $(*)$ cannot be satisfied, since $\dim_{\mathbb{F}_2}(k) = 3 < 5 - 1$.

Consider the following subgroup of $A_{\mathcal{O}}^\times$ (corresponding to quadratic extensions unramified at places dividing 2).

Definition 3.12. Let U_4 denote the subgroup of $A_{\mathcal{O}}^\times$ defined by

$$U_4 = \{u \in A_{\mathcal{O}}^\times \;:\; u \equiv \square \pmod{4A_{\mathcal{O}}} \text{ and } \mathcal{N}(u) = \square\}.$$

Note that $(A_{\mathcal{O}}^\times)^2 \subset U_4$ and furthermore each class in $U_4/(A_{\mathcal{O}}^\times)^2$ has a representative of the form $1 + 4\beta$ for some $\beta \in A_{\mathcal{O}}$. Define the set

$$\mathcal{S} := \left\{ (s_1, \ldots, s_r) \in \mathbb{F}_2^r \;:\; \sum_{i=1}^{r} e_i s_i = 0 \right\}. \tag{3.3}$$

Note that some e_i must be odd, hence the subspace $\mathcal{S}$ has dimension $r - 1$.

Lemma 3.13. *The map $\phi : U_4/(A_{\mathcal{O}}^\times)^2 \to \mathcal{S}$ induced by the map*

$$1 + 4\beta \mapsto (\operatorname{Tr}_{k_1/\mathbb{F}_2}(\overline{\beta}_1), \ldots, \operatorname{Tr}_{k_r/\mathbb{F}_2}(\overline{\beta}_r))$$

for $\beta \in A_{\mathcal{O}}$, is a group isomorphism. In particular $\dim_{\mathbb{F}_2} U_4/(A_{\mathcal{O}}^\times)^2 = r - 1$.

Proof. Consider the equality

$$(1 + 4\alpha)(1 + 4\beta) = 1 + 4(\alpha + \beta) + 16\alpha\beta = (1 + 4(\alpha + \beta))(1 + 16z),$$

where $z = \frac{\alpha\beta}{1+4(\alpha+\beta)} \in A_{\mathcal{O}}$. By [BSPT21, Lemma 1.10], $1 + 16z \in (A_{\mathcal{O}}^\times)^2$ so $(1 + 4\alpha)(1 + 4\beta) \equiv 1 + 4(\alpha + \beta) \pmod{(A_{\mathcal{O}}^\times)^2}$. This implies that the map is a morphism.

The facts that the map is well defined on equivalence classes and that it is injective follow from Lemma 1.10 (1) of [BSPT21]. At last, note that by Lemma 1.10 (5) (and its natural generalization) of [BSPT21] both sets $U_4/(A_{\mathcal{O}}^\times)^2$ and $\mathcal{S}$ have the same cardinality 2^{r-1} hence the statement. □

Let W be the subgroup of U_4 given by

$$W = \{u = (1 - 4T_1 w^2, \ldots, 1 - 4T_r w^2) : w \in \mathcal{O} \text{ and } \mathcal{N}(u) = \square\}(A_{\mathcal{O}}^\times)^2 \subset U_4. \tag{3.4}$$

Theorem 3.14. *With the previous notations, $W \subset \operatorname{Im}(\delta_K)$ and the dimension $\dim_{\mathbb{F}_2} W/(A_{\mathcal{O}}^\times)^2 = \dim_{\mathbb{F}_2} \mathbb{V}$. Moreover, the index of W in U_4 equals*

$$[U_4 : W] = 2^{r-1-\dim_{\mathbb{F}_2} \mathbb{V}}.$$

Proof. To prove the first statement, we need to construct points in $J(K)$ hitting each element of W. Actually, the points we construct lie on $\mathcal{C}(K)$. The expansion around the infinity point of the curve $\mathcal{C}$ in terms of the local uniformizer $z = \frac{y}{x^{\frac{d+1}{2}}}$ is given by

$$\begin{cases} x(z) = z^{-2} + zO_1(z), \\ y(z) = z^{-d} + z^{-d+3}O_2(z), \end{cases}$$

where $O_1(z), O_2(z) \in \mathcal{O}[[z]]$. If $w \in \mathcal{O}$, $2w$ lies in the maximal ideal, and since $O_1(z), O_2(z) \in \mathcal{O}[[z]]$, we get a well defined point $P = (x(2w), y(2w)) \in \mathcal{C}(\mathcal{O})$ (i.e. the series converges). Then we have

$$\delta_K(P - \infty) = [((2w)^{-2} + 2wO_1(2w) - T_1, \cdots, (2w)^{-2} + 2wO_1(2w) - T_r)].$$

Multiplying by $(2w)^2$ (a square), we get

$$\left[\left((1 - 4T_1w^2)\left(1 + \frac{8w^3O_1(2w)}{1 - 4T_1w^2}\right), \cdots, (1 - 4T_rw^2)\left(1 + \frac{8w^3O_1(2w)}{1 - 4T_rw^2}\right)\right)\right].$$

Note that the second factors are squares (by [O'M00, Theorem 63:1]), so

$$\delta_K(P - \infty) = [(1 - 4T_1w^2, \cdots, 1 - 4T_rw^2)].$$

Varying w over the elements of $\mathcal{O}$ proves the first statement.

To compute the dimension, we look at the image of W under ϕ. Indeed, given $w \in \mathcal{O}$ we have

$$\phi((1 - 4T_1w^2, \cdots, 1 - 4T_rw^2)) = (\mathrm{Tr}_{k_1/\mathbb{F}_2}(\overline{T_1}\overline{w}^2), \ldots, \mathrm{Tr}_{k_r/\mathbb{F}_2}(\overline{T_r}\overline{w}^2)).$$

Note that over a perfect field of characteristic two, squaring is a bijection, so it is enough to determine for which elements $s = (s_1, \ldots, s_r) \in \mathcal{S}$, there exists $v \in k$ such that $\mathrm{Tr}_{k_i/\mathbb{F}_2}(\overline{T_i}v) = s_i$ for all $1 \le i \le r$. Let $\sigma_i = \mathrm{Tr}_{k_i/k}(\overline{T}_i) \in k$, so by the property of traces in towers

$$\phi(W) = \{(\mathrm{Tr}_{k/\mathbb{F}_2}(\sigma_1 v), \ldots, \mathrm{Tr}_{k/\mathbb{F}_2}(\sigma_r v)) \mid v \in k\}.$$

Recall that the bilinear mapping $k \times k \to \mathbb{F}_2$ given by $(x, y) \mapsto \mathrm{Tr}_{k/\mathbb{F}_2}(xy)$ is perfect. By definition, the set $\{\sigma_1, \ldots, \sigma_r\} \subset k$ generates an $\mathbb{F}_2$-vector space of dimension $\dim_{\mathbb{F}_2} \mathbb{V}$ in k, then the same holds for the set of linear functions $(\mathrm{Tr}_{k/\mathbb{F}_2}(\sigma_1 v), \ldots, \mathrm{Tr}_{k/\mathbb{F}_2}(\sigma_r v))$, hence $\dim_{\mathbb{F}_2} W/(A_{\mathcal{O}}^\times)^2 = \dim_{\mathbb{F}_2} \phi(W) = \dim_{\mathbb{F}_2} \mathbb{V}$. □

Remark 3.15. When $p(x)$ satisfies $(*)$, the last statement proves that $U_4 = W$, hence $U_4/(A_{\mathcal{O}}^\times)^2$ is contained in the image of the elements of $\mathcal{C}(K)$ under δ_K.

4. Archimedean places

Let K be an archimedean place, namely $K = \mathbb{R}$ or $K = \mathbb{C}$. If $K = \mathbb{C}$, then $A_K = A_{\mathbb{C}} \simeq \mathbb{C}^d$, and the map $\delta_K : J(\mathbb{C})/2J(\mathbb{C}) \to (A_{\mathbb{C}}^\times/(A_{\mathbb{C}}^\times)^2)_\square = \{1\}$ is the trivial map.

Thus suppose that $K = \mathbb{R}$. Let $2t$ denote the number of complex roots of $p(x)$ and $2s + 1$ the number of real ones (so $d = 2s + 1 + 2t$). Then

$$A_{\mathbb{R}} \simeq \mathbb{R}^{2s+1} \times \mathbb{C}^t\,. \tag{4.1}$$

Order the real roots in the form $\tilde{v} < v_1 < v_1' < v_2 < v_2' \ldots < v_s < v_s'$ (as in Figure 1) and let $w_1, \overline{w_1}, \ldots, w_t, \overline{w_t}$ denote the complex ones. Let $P \in J(\mathbb{R})$ be a real point. Then

$$\delta_{\mathbb{R}}(P - \infty) = (x(P) - \tilde{v}, x(P) - v_1, x(P) - v_1', \ldots, x(P) - v_s', x(P) - w_1, \ldots, x(P) - w_t).$$

Lemma 4.1. *We have* $\mathrm{Im}(\delta_{\mathbb{R}}) \subset \{\pm 1\}^{2s+1} \times \{1\}^t$ *and moreover*

$$\mathrm{Im}(\delta_{\mathbb{R}}) = \{(1, \epsilon_1, \epsilon_1, \ldots, \epsilon_s, \epsilon_s, 1, \ldots, 1) \in \{\pm 1\}^{2s+1} \times \{1\}^t \mid \epsilon_i \in \{\pm 1\}, i = 1, \ldots, s\}.$$

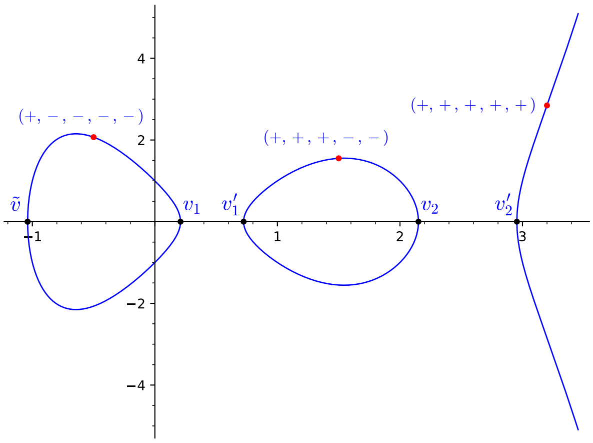

Figure 1. Points of $\mathcal{C}(\mathbb{R})$

Proof. The fact that $\operatorname{Im}(\delta_{\mathbb{R}}) \subset \{\pm 1\}^{2s+1} \times \{1\}^t$ is clear from (4.1). A point between $\tilde{v}$ and v_1 has image $(1, -1, \ldots, -1) \times (1)^t$ as shows Figure 1. In general, a real point between v_i' and v_{i+1} maps into a vector with $2i+1$ plus signs, and $2s+1-(2i+1)$ minus ones (and trivial at the complex places). This proves the containment

$$\operatorname{Im}(\delta_{\mathbb{R}}) \supset \{(1, \epsilon_1, \epsilon_1, \ldots, \epsilon_s, \epsilon_s, 1, \ldots, 1) \in \{\pm 1\}^{2s+1} \times \{1\}^t \mid \epsilon_i \in \{\pm 1\}, i = 1, \ldots, s\}.$$

The opposite inclusion is clear for real points $P \in \mathcal{C}(\mathbb{R})$. If $P \in \mathcal{C}(\mathbb{C}) - \mathcal{C}(\mathbb{R})$ then

$$\delta_{\mathbb{R}}(P - \infty)\delta_{\mathbb{R}}(\overline{P} - \infty) = (|x(P) - \tilde{v}|^2, |x(P) - v_1|^2, \ldots, |x(P) - v_s'|^2) \times (1)^t,$$

a vector whose components are all positive (and hence trivial in the quotient). □

5. 2-Selmer groups and Class groups

In this section K denotes a number field and $\mathcal{C}$ an hyperelliptic curve defined over K. Keeping the previous notation, if $p(x)$ factors like

$$p(x) = p_1(x) \cdots p_r(x),$$

then the K-algebra A_K is isomorphic to $K_1 \times \cdots \times K_r$, where K_i is the number field $K[x]/(p_i(x))$. We will denote by $\operatorname{Cl}(A_K)$ the finite abelian group

$$\operatorname{Cl}(A_K) := \operatorname{Cl}(K_1) \times \cdots \operatorname{Cl}(K_r),$$

where $\operatorname{Cl}(K_i)$ is the class group of the number field K_i. A similar notation will be used for the set of ideals, fractional ideals, principal ideals and the ring of integers of A_K. If $\alpha \in A_K$ corresponds to $\alpha = (\alpha_1, \ldots, \alpha_r)$ under the isomorphism (2.2), we denote by $A_K(\sqrt{\alpha})$ the K-algebra $K_1(\sqrt{\alpha_1}) \times \cdots \times K_r(\sqrt{\alpha_r})$, and we call the extension $A_K(\sqrt{\alpha})/A_K$ unramified if each extension in the previous product is unramified.

For v a real place of K we follow the notations of §4, i.e. we denote by $\tilde{v}, v_1, v_1', \ldots, v_{s_v}, v_{s_v}'$ the real roots of $p(x)$ in K_v, where $s_v \in \mathbb{Z}_{\geq 0}$ depends on v.

Remark 5.1. A real root v of the polynomial $p_i(x)$ determines an embedding of K_i into $\mathbb{R}$. Abusing notation, we will use the same symbol to denote either a real root of $p_i(x)$ or the embedding it determines.

From now on we assume the following hypotheses:

Hypotheses 5.2. The hyperelliptic curve $\mathcal{C}$ and the field K satisfy the following conditions:

(1) The degree of $p(x)$ is odd.
(2) The narrow class group of K is odd.
(3) For all finite places v of K, $\mathcal{C}/K_v$ satisfies (†).

Remark 5.3. The first two conditions together with (†.i) are very easy to verify with most computational programs (like [PAR19]).

The hypothesis (†) implies that for all finite places v of K the image of the connecting morphism δ_{K_v} belongs to the subgroup $(A_{\mathcal{O}_v}^{\times}/(A_{\mathcal{O}_v}^{\times})^2)_{\square} \subset (A_{K_v}^{\times}/(A_{K_v}^{\times})^2)_{\square}$.

Definition 5.4. Let $C_*(\mathcal{C}) \subset A_K^{\times}/(A_K^{\times})^2$ be the subgroup made of elements $[\alpha]$ satisfying the following properties:

- $A_K(\sqrt{\alpha})$ is unramified at all finite places of A_K,
- if v is a real place of K then $A_K(\sqrt{\alpha})$ is unramified at $\tilde{v}$ (equivalently $\tilde{v}(\alpha) > 0$),
- if v is a real place of K then $A_K(\sqrt{\alpha})$ ramifies at v_i if and only if it ramifies at v_i' for each $i = 1, \ldots, s_v$.

The group $C_*(\mathcal{C})$ plays a crucial role in our bounds, as it is deeply connected to the 2-class group of A_K. Let $\operatorname{Frac}(A_K)$ denote the group of fractional ideals of A_K. Consider the following subgroup of the group of principal ideals:

$$P_*(\mathcal{C}) = \{(\alpha) \in \operatorname{Frac}(A_K) : v_i(\alpha)\, v_i'(\alpha) > 0, \text{for each real place } v,\ \ i = 1, ..., s_v\}.$$

Remark 5.5. If $A_K = K_1 \times \ldots \times K_r$, the places v_i and v_i' need not be places of the same field K_j. A priori the condition $v_i(\alpha)v_i'(\alpha) > 0$ might imply a relation between embeddings of different fields.

Definition 5.6. Let $\operatorname{Cl}_*(A_K, \mathcal{C})$ be the class group attached to $P_*(\mathcal{C})$, i.e.

$$\operatorname{Cl}_*(A_K, \mathcal{C}) = \operatorname{Frac}(A_K)/P_*(\mathcal{C})$$

Proposition 5.7. *The group $C_*(\mathcal{C})$ is isomorphic to the torsion 2-subgroup of $\operatorname{Cl}_*(A_K, \mathcal{C})$, i.e. $C_*(\mathcal{C}) \simeq \operatorname{Cl}_*(A_K, \mathcal{C})[2]$.*

Proof. The proof mimics the one given in [BSPT21, Proposition 2.10]. If $\alpha \in C_*(\mathcal{C})$ (say $\alpha = (\alpha_1, \ldots, \alpha_r)$) then the extension $F = A_K(\sqrt{\alpha})$ (i.e., $K_1(\sqrt{\alpha_1}) \times \cdots \times K_r(\sqrt{\alpha_r})$) is an extension of A_K that is abelian and unramified at all finite places (meaning that each L_i/K_i is abelian and unramified at all finite places). Furthermore, the extension F/A_K is unramified at the Archimedean place $\tilde{v}$ above v, and satisfies that it ramifies at a place v_i if and only if it ramifies at the place v_i'. Let $L = L_1 \times \cdots \times L_r$ denote the maximal abelian extension of A_K which is unramified at all finite places and satisfies the same property at the Archimedean places. Clearly $F \subset L$ and $C_*(\mathcal{C}) \simeq \operatorname{Hom}(\operatorname{Gal}(L/A_K), \mu_2)$ (the extension F corresponds to the morphism whose kernel equals $\operatorname{Gal}(L/F)$). The Artin reciprocity map $\operatorname{Frac}(A_K) \to \operatorname{Gal}(L/A_K)$ has kernel $P_*(\mathcal{C})$, so $\operatorname{Cl}_*(A_K, \mathcal{C}) \simeq \operatorname{Gal}(L/A_K)$ and $C_*(\mathcal{C}) \simeq \operatorname{Cl}_*(A_K, \mathcal{C})[2]$. □

The hypotheses 5.2 are needed to bound the Selmer group $\operatorname{Sel}_2(J)$ in terms of $\operatorname{Cl}_*(A_K, \mathcal{C})[2]$. For that purpose, we need to introduce two subgroups of $A_K^{\times}/(A_K^{\times})^2$. If v is a finite place of K dividing 2, we denote by $U_{4,v} \subset A_{\mathcal{O}_v}^{\times}$ the subgroup introduced in definition 3.12 and by $W_v \subset U_{4,v}$ the subgroup defined in (3.4).

Definition 5.8. Let $C_W(\mathcal{C}) \subset A_K^{\times}/(A_K^{\times})^2$ be the subgroup of the classes $[\alpha] \in A_K^{\times}/(A_K^{\times})^2$ satisfying the following properties:

- for each place v of K over 2 the class $[\alpha]$ belong to the image of W_v in $A_{K_v}^{\times}/(A_{K_v}^{\times})^2$,
- $A_K(\sqrt{\alpha})$ is unramified at all finite places of A_K,
- if v is a real place of K then $A_K(\sqrt{\alpha})$ is unramified at $\tilde{v}$,
- if v is a real place of K then $A_K(\sqrt{\alpha})$ ramifies at v_i if and only if it ramifies at v_i' for each $i = 1, \dots, s_v$.

Proposition 5.9. *If hypotheses 5.2 are satisfied then* $C_W(\mathcal{C}) \subset \mathrm{Sel}_2(J)$.

Proof. Let $\alpha \in A_K^{\times}$ such that $[\alpha] \in C_W(\mathcal{C})$. We need to verify $\mathrm{loc}_v([\alpha]) \in \mathrm{Im}(\delta_v)$ for each place v of K, where $\mathrm{loc}_v : (A_K^{\times}/(A_K^{\times})^2)_\square \to (A_{K_v}^{\times}/(A_{K_v}^{\times})^2)_\square$ is the natural map. At Archimedean places, the result follows from Lemma 4.1. If v corresponds to a prime not dividing 2, then the condition $A_K(\sqrt{\alpha})/A_K$ unramified implies that α (up to squares) is a unit in $A_{\mathcal{O}_v}$, so the result follows from Corollary 3.6. The result for places dividing 2 follows from Theorem 3.14. □

To obtain an upper bound we use the following auxiliary group.

Definition 5.10. Let $\tilde{C}(\mathcal{C}) \subset A_K^{\times}/(A_K^{\times})^2$ be the subgroup of the $[\alpha] \in A_K^{\times}/(A_K^{\times})^2$ such that

- For each finite place w of A_K the w-adic valuation of α is even.
- $\mathcal{N}(\alpha)$ is a square in K.
- if v is a real place of K then $A_K(\sqrt{\alpha})$ is unramified at $\tilde{v}$ (i.e. $\tilde{v}(\alpha) > 0$),
- if v is a real place of K then $A_K(\sqrt{\alpha})$ ramifies at v_i if and only if it ramifies at v_i' for each $i = 1, \dots, s_v$.

Proposition 5.11. *If hypotheses 5.2 are satisfied, then* $\mathrm{Sel}_2(J) \subset \tilde{C}(\mathcal{C})$.

Proof. The condition at the Archimedean places is clear (by Lemma 4.1). The result for finite primes follows from Theorem 3.4. □

Note that $C_W(\mathcal{C}) \subset C_*(\mathcal{C}) \subset \tilde{C}(\mathcal{C})$, so it is enough to bound the indexes $[\tilde{C}(\mathcal{C}) : C_*(\mathcal{C})]$ and $[C_*(\mathcal{C}) : C_W(\mathcal{C})]$ in order to get explicit bounds for $\mathrm{Sel}_2(J)$ in terms of the 2-class group $\mathrm{Cl}_*(A_K, \mathcal{C})[2]$.

Theorem 5.12. *Following the previous notations,*

- $[\tilde{C}(\mathcal{C}) : C_*(\mathcal{C})] \le 2^{g[K:\mathbb{Q}]}$.
- $[C_*(\mathcal{C}) : C_W(\mathcal{C})] \le 2^{\sum_{v \mid 2}(r_v - 1 - \dim_{\mathbb{F}_2}(\mathbb{V}_v))}$.

Proof. The second claim is clear, since by definition, $C_W(\mathcal{C})$ consists of the elements of $C_*(\mathcal{C})$ that locally at places v dividing 2 lie in W_v, hence the index is bounded by the product of the local indexes which were computed in Theorem 3.14.

The proof of the first claim follows the same idea used in the proof of [BSPT21, Theorem 2.11]. There is a natural well defined map $\phi : \tilde{C}(\mathcal{C}) \to \mathrm{Cl}(A_K)[2]$ given as follows: if $\alpha \in A_K^{\times}$ such that $[\alpha] \in \tilde{C}(\mathcal{C})$ then the even valuation condition implies the existence of an ideal I such that $I^2 = (\alpha)$. Define $\phi([\alpha]) = [I]$; the map is well defined by [BSPT21, Lemma 2.13]. Equation (2.1) of [BSPT21] implies that

$$[\tilde{C}(\mathcal{C}) : C_*(E)] \le \frac{\# \ker \phi}{\#(P/P_*(\mathcal{C}))}.$$

For each odd value $1 \le i \le d$, let

$$\mathcal{A}_i = \{v \text{ real Archimedean places of } K\ : p(x) \text{ has } i \text{ real roots in } K_v\}.$$

Let $a_i = \#\mathcal{A}_i$ and c denote the number of complex places of K, so $[K : \mathbb{Q}] = a_1 + a_3 + a_5 + \cdots + a_d + 2c$. The sign map

$$\mathrm{sign} : A_K^{\times} \to \prod_{v \in \mathcal{A}_1} \{\pm 1\} \times \cdots \times \prod_{v \in \mathcal{A}_d} \{\pm 1\}^d,$$

induces a well defined map on $A_K^\times/(A_K^\times)^2$. Let $W_i \subset \{\pm 1\}^{a_i}$ be the subset of elements whose product equals 1 (a subgroup of index two) and let

$$\widetilde{W} = \prod_{v\in\mathcal{A}_1} W_1 \times \ldots \times \prod_{v\in\mathcal{A}_d} W_d.$$

Let V_i be the subset of W_i given by

$$V_i = \left\{ \left(1, \epsilon_1, \epsilon_1, \ldots, \epsilon_{\frac{i-1}{2}}, \epsilon_{\frac{i-1}{2}}\right) \,:\, \epsilon_j = \pm 1 \right\},$$

and

$$\widetilde{V} = \prod_{v\in\mathcal{A}_1} V_1 \times \ldots \times \prod_{v\in\mathcal{A}_d} V_d.$$

Clearly $\operatorname{sign}((A_K^\times/(A_K^\times)^2)_\square) \subset \widetilde{W}$ and $\operatorname{sign}(\tilde{C}(\mathcal{C})) \subset \widetilde{V}$. The rest of the argument given in the proof of [BSPT21, Theorem 2.11] works mutatis mutandis with this definitions, and we obtain that

$$[\tilde{C}(\mathcal{C}) : C_*(\mathcal{C})] \leq \frac{\#\widetilde{V}\,\#\operatorname{sign}(\mathcal{O}^\times)\,\#(A_\mathcal{O}^\times/(A_\mathcal{O}^\times)^2)_\square}{\#\operatorname{sign}(A_K^\times)}. \tag{5.1}$$

The values appearing in the previous formula are the following:

- $\#\widetilde{V} = 2^{a_3+2a_5+3a_7+\cdots+(\frac{d-1}{2})a_d}$,
- $\#\operatorname{sign}(\mathcal{O}^\times) = 2^{a_1+a_3+a_5+\cdots+a_d}$,
- $\#\operatorname{sign}(A_K^\times) = 2^{a_1+3a_3+5a_5+\ldots+da_d}$,
- $\#(A_\mathcal{O}^\times/(A_\mathcal{O}^\times)^2)_\square = 2^{g[K:\mathbb{Q}]}\cdot 2^{a_3+2a_5+3a_7+\cdots+(\frac{d-1}{2})a_d}$ by Lemma 5.14.

But

$$\begin{aligned}(a_3 + 2a_5 + \cdots + (\tfrac{d-1}{2})a_d) + (a_1 + a_3 + a_5 \cdots + a_d) + (a_3 + 2a_5 + \cdots + (\tfrac{d-1}{2})a_d)\\ = a_1 + 3a_3 + 5a_5 + \cdots + da_d\end{aligned}$$

so the right hand side of (5.1) equals $2^{g[K:\mathbb{Q}]}$.

□

Remark 5.13. The oddness hypothesis on the class group of K is only used in the last theorem. A general result could be obtained by consider a more general class group as done in [YY22] (for the case of elliptic curves).

Lemma 5.14. *With the previous notation,*

$$\#(A_\mathcal{O}^\times/(A_\mathcal{O}^\times)^2)_\square = 2^{g[K:\mathbb{Q}]}\cdot 2^{a_3+2a_5+3a_7+\cdots+(\frac{d-1}{2})a_d}$$

Proof. By definition, $(A_\mathcal{O}^\times/(A_\mathcal{O}^\times)^2)_\square$ is the kernel of the norm map $\mathcal{N} : A_\mathcal{O}^\times/(A_\mathcal{O}^\times)^2 \to \mathcal{O}^\times/(\mathcal{O}^\times)^2$. The map is surjective (since $[A_K : K]$ is odd, in particular, if $\epsilon \in \mathcal{O}^\times$, its norm is equal to itself up to a square). Thus

$$\#(A_\mathcal{O}^\times/(A_\mathcal{O}^\times)^2)_\square = \frac{\#A_\mathcal{O}^\times/(A_\mathcal{O}^\times)^2}{\#\mathcal{O}^\times/(\mathcal{O}^\times)^2}.$$

By Dirichlet's unit theorem we have $\#\mathcal{O}^\times/(\mathcal{O}^\times)^2 = 2^\alpha$ where α is the number of archimedean places of K, i.e., $\alpha = a_1 + a_3 + \cdots + a_d + c$. As before, write $A_K \simeq K_1 \times \cdots \times K_r$. Given an archimedean place v of K, let $r_i(v)$ and $s_i(v)$ denote the number of real and complex places of K_i above v, so $[K_i : K] = r_i(v) + 2s_i(v)$ for real v and $[K_i : K] = s_i(v)$ for complex v. We can apply Dirichlet's unit theorem to each K_i to obtain

$$\#A_\mathcal{O}^\times/(A_\mathcal{O}^\times)^2 = 2^{\sum_{v \text{ real}}\sum_{i=1}^r (r_i(v)+s_i(v)) + \sum_{v \text{ complex}}\sum_{i=1}^r s_i(v)}.$$

If v is complex we have $\sum_{i=1}^r s_i(v) = d$, so the second term in the exponent is

$$\beta = \sum_{v \text{ complex}} \sum_{i=1}^{r} s_i(v) = cd = \frac{d-1}{2}(2c) + c\,.$$

For v real we have $v \in \mathcal{A}_j$ for some j and in that case $\sum_{i=1}^r r_i(v) = j$, while $\sum_{i=1}^r s_i(v) = \frac{d-j}{2}$. Hence the first term in the exponent is

$$\begin{aligned}\gamma = \sum_{v \text{ real}} \sum_{i=1}^{r} (r_i(v) + s_i(v)) &= \sum_{j=1}^{d} \left(\frac{d+j}{2}\right) a_j \\ &= \frac{d-1}{2} \sum_{j=1}^{d} a_j + (a_1 + 2a_3 + 3a_5 + \ldots + (\tfrac{d+1}{2}) a_d)\,.\end{aligned}$$

Adding both terms, and using $g = \frac{d-1}{2}$ and $[K:\mathbb{Q}] = a_1 + a_2 + \ldots + a_d + 2c$ we obtain $\gamma + \beta - \alpha = g[K:\mathbb{Q}] + (a_3 + 2a_5 + \ldots + (\tfrac{d-1}{2})a_d)$ proving the claim. □

Combining all the previous results, we can now prove our main result.

Theorem 5.15. *Let K be a number field and $\mathcal{C}/K$ be a hyperelliptic curve. Suppose that hypotheses 5.2 hold, then*

$$\begin{aligned}\dim_{\mathbb{F}_2} \operatorname{Cl}_*(A_K, \mathcal{C})[2] - \sum_{v \mid 2} \big(r_v - 1 - \dim_{\mathbb{F}_2}(\mathbb{V}_v)\big) \quad &\leq \\ \leq \quad \dim_{\mathbb{F}_2} \operatorname{Sel}_2(J) \quad &\leq \quad \dim_{\mathbb{F}_2} \operatorname{Cl}_*(A_K, \mathcal{C})[2] + g\,[K:\mathbb{Q}]\,.\end{aligned} \tag{5.2}$$

Proof. By Proposition 5.11 we have $\operatorname{Sel}_2(J) \subset \tilde{C}(\mathcal{C})$, hence

$$\# \operatorname{Sel}_2(J) \leq \# \tilde{C}(\mathcal{C}) = [\tilde{C}(\mathcal{C}) : C_*(\mathcal{C})] \cdot \# C_*(\mathcal{C}).$$

Theorem 5.12 gives the bound $[\tilde{C}(\mathcal{C}) : C_*(\mathcal{C})] \leq 2^{g[K:\mathbb{Q}]}$ and Proposition 5.7 implies that $C_*(\mathcal{C}) \simeq \operatorname{Cl}_*(A_K, \mathcal{C})[2]$, proving the upper bound

$$\dim_{\mathbb{F}_2} \operatorname{Sel}_2(J) \leq \dim_{\mathbb{F}_2} \operatorname{Cl}_*(A_K, \mathcal{C})[2] + g\,[K:\mathbb{Q}].$$

Similarly, by Proposition 5.9 we have $C_W(\mathcal{C}) \subset \operatorname{Sel}_2(J)$, and the lower bound follows from Theorem 5.12. □

6. Applications

6.1. **Quadratic twists.** The goal of the present section is to study the rank variation of families of quadratic twists of a given hyperelliptic curve. For that purpose, let K be a number field whose narrow class number is odd, and let $p(x) \in K[x]$ be an irreducible polynomial of odd degree (we cannot remove the irreducibility hypothesis as will become clear later). Let $\mathcal{C}$ be the hyperelliptic curve with equation

$$\mathcal{C} : y^2 = p(x)$$

Definition 6.1. The *quadratic twist* of the curve $\mathcal{C}$ by $a \in K^\times$ is the curve defined by the equation

$$\mathcal{C}(a) : ay^2 = p(x). \tag{6.1}$$

A change of variables transforms 6.1 into the more well known equation

$$\mathcal{C}(a) : y^2 = a^d p(x/a).$$

Let J_a denote the Jacobian of $\mathcal{C}(a)$. Note that since $p(x)$ is irreducible, A_K is a number field.

Lemma 6.2. *Let $\mathcal{C}$ be an hyperelliptic curve over K whose defining polynomial has odd degree and is irreducible. Let $a \in K^\times$ be an element satisfying that any prime ideal $\mathfrak{p} \mid a$ is either inert or totally ramified in the field extension A_K/K. Then, if $\mathcal{C}$ satisfies hypotheses 5.2 so does $\mathcal{C}(a)$.*

Proof. The first two assumptions of Hypothesis 5.2 are clearly satisfied, so we need only to to verify the last one, namely that for all finite places v of K, $\mathcal{C}(a)/K_v$ satisfies (†). Let v be finite place of K.

- If $p(x)$ is irreducible over K_v then clearly $a^d p(x/a)$ is also irreducible, as both polynomials define the same K_v-algebra A_{K_v}, so $\mathcal{C}(a)$ also satisfies (†.*i*).
- Suppose that $p(x)$ satisfies (†.i) but it's not irreducible over K_v. The inclusion $\mathcal{O}[x]/(p(x)) \subset \prod_i \mathcal{O}[x]/(p_i(x))$ is an equality if and only if both rings have the same discriminant. Our hypothesis on a implies that $v \nmid a$, so the discriminants of $p(x)$ and $a^d p(x/a)$ differ by a unit in $\mathcal{O}_{K_v}$, and similarly for $p_i(x)$. Hence $\mathcal{C}(a)$ also satisfies (†.i) over K_v.
- Finally, suppose that $p(x)$ satisfies (†.ii) over K_v but does not satisfy (†.i). Our hypotheses on a imply that $v \nmid a$, so the extension $K(\sqrt{a})/K$ is unramified. Note that the curves $\mathcal{C}$ and $\mathcal{C}(a)$ become isomorphic over such an extension. It is a well known fact that the component group of the Jacobian of a curve does not vary over unramified extensions.

□

Theorem 6.3. *Let $\mathcal{C}$ be an hyperelliptic curve satisfying hypotheses 5.2 over a number field K of odd narrow class number. Suppose that $p(x)$ is irreducible, and suppose furthermore that there is a principal prime ideal of K which is inert in A_K/K. Then among all quadratic twists by principal prime ideals, there exists a subset of positive density $\mathscr{S}$ such that the abelian varieties* $\operatorname{Jac}(\mathcal{C}(a))$ *have the same 2-Selmer group for all $a \in \mathscr{S}$.*

Proof. Let $\mathscr{P}$ denote the set of all principal prime ideals of K (they have positive density), and let $\mathscr{S}$ be those ones which are inert or totally ramified in A_K/K. Our hypothesis implies that $\mathscr{S}$ has positive density in the set of all principal prime ideals (by Tchebotarev's density theorem). Lemma 6.2 implies that if $(a) \in \mathscr{S}$ then the twisted curve $\mathcal{C}(a)$ also satisfies hypotheses 5.2, so we can apply our main result (Theorem 5.15) to $\mathcal{C}(a)$ and deduce that for each $a \in \mathscr{S}$ the 2-Selmer group of $\mathcal{C}(a)$ satisfies

$$C_W(\mathcal{C}) \subset \operatorname{Sel}_2(\operatorname{Jac}(\mathcal{C}(a))) \subset \tilde{C}(\mathcal{C}).$$

The result follows from the fact that there are finitely many $\mathbb{F}_2$-vector spaces containing $C_W(\mathcal{C})$ and contained in $\tilde{C}(\mathcal{C})$. □

6.2. **A family of octic twists.** Let

$$\mathcal{C}(a) : y^2 = x(x^4 + a). \tag{6.2}$$

The curve $\mathcal{C}(a)$ has genus two, and it contains the non-trivial point $P = (0,0)$ of order two in $\operatorname{Jac}(\mathcal{C}(a))$. The 2-Selmer rank of the surface $\operatorname{Jac}(\mathcal{C}(a))$ was studied in [Jęd21].

There are some very interesting facts concerning the surface $\operatorname{Jac}(\mathcal{C}(a))$. Note that all such curves are "twists" of each other, in the sense that they all become isomorphic over the field $\mathbb{Q}(\sqrt[8]{a})$, via the change of variables $(x, y) \mapsto (\sqrt[8]{a^5} y, \sqrt[4]{a} x)$.

The reason for the existence of such a twist is that the curve $\mathcal{C}(a)$ has an automorphism of order 8 given explicitly by $(x, y) \mapsto (\zeta_4 x, \zeta_8, y)$, where ζ_8 denotes an eighth root of unity, and $\zeta_4 = \zeta_8^2$. This implies in particular that its Jacobian is an abelian surface with complex multiplication. It is a naturall question whether one can "find" for a fixed value of a, the appropiate Hecke character.

Remark 6.4. There is a nice implementation in Pari/GP [PAR19] of algebraic Hecke characters based on the article [MP22]. For example, if $a = -1$, then one can compute the conductor of $\mathrm{Jac}(\mathcal{C}(-1))$ in Magma, and find that it equals 2^{12}. Let E/F be a finite extension of number fields, and let χ be a continuous character of Gal_E. Recall the well known formula:

$$\mathrm{cond}\left(\mathrm{Ind}_{\mathrm{Gal}_E}^{\mathrm{Gal}_F}\chi\right) = \Delta(E/F)\cdot \mathcal{N}(\mathrm{cond}(\chi)), \tag{6.3}$$

where $\Delta(E/F)$ denotes the discriminant of the extension and $\mathcal{N}$ denotes the norm from E to F (see for example [Ser68], page 105 after Proposition 4). By class field theory there is a bijection between Galois characters and Hecke characters (respecting conductors). Then the previous formula, with $E = \mathbb{Q}(\zeta_8)$ and $F = \mathbb{Q}$, implies that if $\mathfrak{p}_2$ denotes the unique prime ideal in $\mathbb{Q}(\zeta_8)$ dividing 2, the Hecke character attached to $\mathrm{Jac}(\mathcal{C}(-1))$ over $\mathbb{Q}(\zeta_8)$ must have conductor $\mathfrak{p}_2^4 = (2)$ (since $\Delta(\mathbb{Q}(\zeta_8)/\mathbb{Q}) = 2^8$). Using Pari/GP we can compute the finite set of all algebraic Hecke characters of infinity type $(1,0),(1,0)$ and conductor dividing 2 as follows:

```
g=gcharinit(bnfinit(polcyclo(8)),2);
? g.cyc
% = [0, 0, 0, 0.E-57]
```

This shows that there are no finite order characters with this conductor, hence if one Hecke character with infinity type $(1,0),(1,0)$ exists, it must be unique. We compute a Hecke character with this infinity type with the command

```
chi=gcharalgebraic(g,[[1,0],[1,0]])[1];
```

The output matches our character χ. As a sanity check, since our Hecke character has algebraic integers coefficients, we can check whether the L-function attached to our hyperelliptic curve matches the one attached to our character χ.

```
Ls1=lfuncreate([g,chi]);
Ls2=lfungenus2(x*(x^4-1));
lfunan(Ls2,1000)==round(lfunan(Ls,1000))
```

This verifies that the first thousand coefficients of the two L-functions do match.

The surface $\mathrm{Jac}(\mathcal{C}(a))$ over $\overline{\mathbb{Q}}$ is isogenous to the product of two elliptic curves. This was verified numerically for some particular values of a (using the algorithm [Lom19]) to deduce the following result whose proof was communicated to us by John Cremona.

Proposition 6.5. *If $a = 1$ then the surface $\mathrm{Jac}(\mathcal{C}(1))$ is isogenous to the product of the elliptic curves with label* 256.d1 *and* 256.a1.

Proof. If we denote by $t = \frac{1+x}{1-x}$, then $x = \frac{t-1}{t+1}$, so we can rewrite the equation of $\mathcal{C}$ in the form

$$y^2 = \frac{(t-1)}{(t+1)}\frac{(t-1)^4+(t+1)^4}{(t+1)^4} = 2\frac{(t-1)}{(t+1)}\frac{(t^4+6t^2+1)}{(t+1)^4}.$$

Cleaning denominators, we get the equation

$$((t+1)^3y)^2 = 2(t^2-1)(t^4+6t^2+1).$$

So the map $(t,y) \to (t^2,(t+1)^3y)$ send the curve $\mathcal{C}$ into the elliptic curve on the variables (u,v) with equation

$$v^2 = 2(u-1)(u^2+6u+1),$$

which is isomorphic to the elliptic curve 256.a1. Similarly, if we make the substitution $t = \frac{1-x}{1+x}$, so $x = \frac{1-t}{1+t}$, a similar computation as before gives a map from $\mathcal{C}$ to the elliptic curve

$$((t+1)^3y)^2 = -2(t^2-1)(t^4+6t^2+1),$$

a quadratic twist by $\sqrt{-1}$ of the previous one (but they are not isogenous over $\mathbb{Q}$). This proves the result. □

Corollary 6.6. *If a is a non-zero integer, then the surface* $\mathrm{Jac}(\mathcal{C}(a))$ *is isogenous to the product of the quadratic twist of the elliptic curve* 256.a1 *by $\sqrt[4]{a}$ times the quadratic twist of the curve* 256.d1 *by $\sqrt[4]{a}$ over the field extension $\mathbb{Q}(\sqrt[4]{a})$.*

Proof. Over the field $\mathbb{Q}(\sqrt[4]{a})$, the map $(x,y) \to (\sqrt[4]{a}x, \sqrt{a}y)$ gives an isomorphism between the curve $\mathcal{C}(a)$ and the curve

$$y^2 = \sqrt[4]{a}x(x^4+1).$$

Then the same proof as before gives a rational map to the curve

$$v^2 = 2\sqrt[4]{a}(u-1)(u^2+6u+1),$$

which is 256.a1, and its quadratic twist by -1, which is 256.d1. □

The main result (Theorem 1) obtained in [Jęd21] is the following: for a non-zero integer a, let $\omega(a)$ denote the number of prime divisors of a.

Theorem 6.7. *Suppose that a is 8-th power free, that the class number of $\mathbb{Q}(\sqrt[4]{-a})$ is odd and that every prime divisor of $2a$ has a unique prime dividing it in $\mathbb{Q}(\sqrt[4]{-a})$. Then if $a < 0$, the 2-selmer rank of* $\mathrm{Jac}(\mathcal{C}(a))$ *is bounded above by $\omega(2a)+3$*

Suppose that $a < 0$. A necessary condition for the class number of $\mathbb{Q}(\sqrt[4]{a})$ to be odd is that either a is prime, or it is twice a prime. Let us restrict to the case a an odd prime number (that we denote by p to emphasize our hypothesis).

We would like to apply our main result to the curve $\mathcal{C}(-p)$ over $\mathbb{Q}$ to improve the upper bound. For that purpose we need to verify whether Hypotheses 5.2 are satisfied. Our polynomial has odd degree and we are working over the rationals, hence the first two hypothesis are satisfied.

The $\mathbb{Q}$-algebra $A_{\mathbb{Q}} = \mathbb{Q}\times\mathbb{Q}(\sqrt[4]{p})$, $\Delta(x(x^4-p)) = -2^8\cdot p^5$ and $\Delta(x^4-p) = -2^8\cdot p^3$, so $(\dagger.i)$ is satisfied at all primes but p. The problem is $(\dagger.\mathrm{ii})$ is also not satisfied at p because the Neron model has two components (see [NU73], page 156, type VII). However, not everything is lost. Our local map is an injective morphism

$$\delta_p : \mathrm{Jac}(\mathcal{C}(-p))(\mathbb{Q}_p)/2\,\mathrm{Jac}(\mathcal{C}(-p))(\mathbb{Q}_p) \hookrightarrow ((\mathbb{Q}_p \times \mathbb{Q}_p(\sqrt[4]{p}))^\times/(A_{\mathbb{Q}_p}^\times)^2)_\square.$$

Any element in the image is the class of an element of the form $(\epsilon_1 p^r, \epsilon_2\sqrt[4]{p}^r)$ for ϵ_i units and $r \in 0,1$. In particular, the image is bounded above by twice the elements which are units up to squares, hence we still can provide an upper bound in terms of the class group $\mathrm{Cl}_*(A_{\mathbb{Q}}, \mathcal{C}(-p))[2]$, namely

$$0 \le \dim_{\mathbb{F}_2}\mathrm{Sel}_2(\mathrm{Jac}(\mathcal{C}(-p))) \le \mathrm{Cl}_*(A_{\mathbb{Q}}, \mathcal{C}(-p))[2] + 2 + 1. \tag{6.4}$$

We are led to compute $\mathrm{Cl}_*(A_{\mathbb{Q}}, \mathcal{C}(-p))[2]$. Firstly we need to understand the class group of the extension $\mathbb{Q}(\sqrt[4]{p})$.

Lemma 6.8. *If a is square-free and $a \equiv 1, 2 \pmod 4$ then the ring of integer of $\mathbb{Q}(\sqrt[4]{-a})$ is $\mathbb{Z}[\sqrt[4]{-a}]$.*

Proof. See [Fun84, Theorem 1]. □

Theorem 6.9. *Let p be a prime number congruent to 3 modulo 8. Then the class group of $\mathbb{Q}(\sqrt[4]{p})$ has odd cardinality, while its narrow class group has twice its cardinality. Its element of order 2 corresponds to the quadratic extension $\mathbb{Q}(\sqrt[4]{p}, \sqrt{-1})$.*

Before proving the result, we need some auxiliary results, whose proof are based on Gauss' results on binary quadratic forms (see [Cox13], §6).

Proposition 6.10. *If p is a prime number, $p \equiv 3 \pmod 4$ then $\mathrm{Cl}(\mathbb{Q}[\sqrt{-1},\sqrt{p}])$ has odd cardinality.*

Proof. Consider the following diagram

$$\begin{tikzcd}
H \arrow[d, dash] \\
L = \mathbb{Q}(\sqrt{-1},\sqrt{p}) \arrow[d, dash] \\
F = \mathbb{Q}(\sqrt{-1})
\end{tikzcd}$$

where H is the Hilbert class field of L (a Galois extension of F). Suppose that $L(\sqrt{\alpha})$ is a subextension of H. Since $\mathrm{Gal}(H/L) \simeq \mathrm{Cl}(L)$, then $L(\sqrt{\alpha}) \subseteq \tilde{L} = H^{\mathrm{Cl}(L)^2}$.

Claim: $\tilde{L}/F$ is an abelian extension.

The proof mimics the one given in [Cox13, Theorem 6.1, page 122], replacing complex conjugation by another element of order two. Let $\sigma \in \mathrm{Gal}(H/F)$ be any element such that $\sigma(\sqrt{p}) = -\sqrt{p}$. Note that if $\mathfrak{a}$ is an element in $\mathrm{Cl}(L)$ then $\mathfrak{a} \cdot \sigma(\mathfrak{a})$ matches an ideal of F extended to $\mathcal{O}_L$. In particular, $\mathfrak{a} \cdot \sigma(\mathfrak{a})$ is a principal ideal (since the class group of F is trivial), so as elements of the class group $\mathrm{Cl}(L)$, $\mathfrak{a}^{-1} = \sigma(\mathfrak{a})$.

Consider the following exact sequence

$$1 \longrightarrow \mathrm{Gal}(H/L) \longrightarrow \mathrm{Gal}(H/F) \longrightarrow \mathrm{Gal}(L/F) \longrightarrow 1. \tag{6.5}$$

The map σ provides a splitting of it, since $\sigma^2 \in \mathrm{Gal}(H/L)$ and it induces the identity on the class group $\mathrm{Cl}(L)$ (recall that $\sigma(\mathfrak{a}) = \mathfrak{a}^{-1}$). In particular, $\mathrm{Gal}(H/F) \simeq \mathbb{Z}/2 \ltimes \mathrm{Cl}(L)$, where the action of 1 send an ideal $\mathfrak{a}$ to its inverse. Then the proof of [Cox13, Theorem 6.1, page 122] proves that $\mathrm{Cl}(L)^2 = [G,G]$, where $G = \mathrm{Gal}(H/F)$, and in particular $\mathrm{Gal}(\tilde{L}/F) \simeq G/[G,G]$ is abelian.

Since $L(\sqrt{\alpha}) \subset \tilde{L}$ and $\tilde{L}/F$ is an abelian extension, the extension $L(\sqrt{\alpha})/F$ is Galois. The group $\mathrm{Gal}(L(\sqrt{\alpha})/F)$ is isomorphic to either $\mathbb{Z}/2$, to $\mathbb{Z}/2 \times \mathbb{Z}/2$ or it is cyclic of order 4. The last case cannot occur, because $\mathbb{Z}/4$ does not fit into the exact sequence (6.5).

In the first two cases, we can assume (without loss of generality) that $\alpha \in F$, so $F(\sqrt{\alpha})$ is a quadratic extension of F unramified outside p. Since the class number of F is one, α can be chosen so that the ideal it generates is supported only at the prime p (which is inert in F because p is congruent to 3 modulo 4) and hence $\alpha \in \{i, p, ip\}$ (up to squares). But among these possibilities, the only quadratic extension which is unramified at 2 is $F(\sqrt{p}) = L$. □

Proposition 6.11. *If $p \equiv 3 \pmod 8$ then the fundamental unit of $\mathbb{Q}(\sqrt{p},\sqrt{-1})$ equals $\sqrt{i \cdot \varepsilon_p}$, where ε_p is a totally positive fundamental unit of $\mathbb{Q}(\sqrt{p})$.*

Proof. Suppose that $p \neq 3$, since this case is true by a computer check. By [Azi99, Applications 1], the units of $F = \mathbb{Q}(\sqrt{p},\sqrt{-1})$ are generated by $\{i, \kappa\}$, where $\kappa = \varepsilon_p$ or $\kappa = \sqrt{i \cdot \varepsilon_p}$ (meaning that κ is an element of F whose square equals $i \cdot \varepsilon_p$). To prove the claim, it is enough to prove that $i \cdot \varepsilon_p$ is a square in F.

The extension $\mathbb{Q}(\sqrt{p},\sqrt{-1})[\sqrt{i \cdot \varepsilon_p}]$ is at most quadratic, and is unramified at all finite odd primes (i.e. those not dividing 2). If we can prove that the extension is also unramified at even primes, then the extension must be trivial (since the class number of $\mathbb{Q}(\sqrt{p}, \sqrt{-1})$ is odd by the previous proposition).

Since $p \equiv 3 \pmod 8$, there exists an isomorphism $\Phi : \mathbb{Q}_2(\sqrt{p}) \to \mathbb{Q}_2(\sqrt{3})$. The fact that the class number of $\mathbb{Q}(\sqrt{p})$ is odd also implies that the quadratic extension $\mathbb{Q}(\sqrt{p}, \sqrt{\varepsilon_p})$ is ramified at 2 (since the fundamental unit has norm 1). Then $\mathbb{Q}_2(\sqrt{p}, \sqrt{\varepsilon_p})/\mathbb{Q}_2$ is biquadratic of conductor 2^8. There are precisely two such extensions, which match $\mathbb{Q}_2(\sqrt{3}, \sqrt{\varepsilon_3})$ and $\mathbb{Q}_2(\sqrt{3}, \sqrt{-\varepsilon_3})$, where $\varepsilon_3 = 2 - \sqrt{3}$ is a fundamental unit for $\mathbb{Q}(\sqrt{3})$ (see for example Jones-Roberts tables at `https://hobbes.la.asu.edu/courses/site/Localfields-index.html`). Then extending Φ to an isomorphism between $\mathbb{Q}_2(\sqrt{p}, \sqrt{-1})$ and $\mathbb{Q}_2(\sqrt{3}, \sqrt{-1})$ we can assume that $\Phi(\varepsilon_p) = \varepsilon_3$ up to squares (so it is enough to understand the case $p = 3$).

But actually $i \cdot (2 - \sqrt{3})$ is a square in $\mathbb{Q}(\sqrt{3}, \sqrt{-1})$ (since $\left(\frac{1+i-\sqrt{3}-\sqrt{3}i}{2}\right)^2 = i(2-\sqrt{3})$), so if $\mathbb{Q}(\sqrt{p}, \sqrt{-1})[\sqrt{i\varepsilon_p}]$ is not equal to $\mathbb{Q}(\sqrt{p}, \sqrt{-1})$, the primes dividing 2 are split (not ramified). □

Theorem 6.12. *If* $p \equiv 3 \pmod 8$ *then* $\mathrm{Cl}(\mathbb{Q}[\sqrt{-1}, \sqrt[4]{p}])$ *has odd cardinality.*

Proof. In Proposition 6.9 replace F by $\mathbb{Q}(\sqrt{-1}, \sqrt{p})$ (whose class group has odd cardinality) and L by $\mathbb{Q}(\sqrt{-1}, \sqrt[4]{p})$. Let $\sigma \in \mathrm{Gal}(L/F)$ be the non-trivial element, defined by $\sigma(i) = i$, $\sigma(\sqrt[4]{p}) = -\sqrt[4]{p}$. Since we are interested in understanding quadratic extensions, instead of working with the whole extension H/L, we can consider the subextension $H^{\mathrm{Cl}(L)^2}/L$ (whose Galois group is an elementary 2-group) and the extension $\mathrm{Gal}(H^{\mathrm{Cl}(L)^2}/F)$.

Since the class group of F is odd, $\sigma(\mathfrak{a}) \cdot \mathfrak{a}$ equals the square of an ideal of F, so $\sigma(\mathfrak{a})$ has the same class as $\mathfrak{a}^{-1}$ in $\mathrm{Cl}(L)/\mathrm{Cl}(L)^2$. Then the same argument as in the previous proposition proves that $L(\sqrt{\alpha})$ is an extension of degree at most 4 of F unramified outside $2p$ whose Galois group $\mathrm{Gal}(L(\sqrt{\alpha})/F)$ is isomorphic to either $\mathbb{Z}/2$ or to $\mathbb{Z}/2 \times \mathbb{Z}/2$ (it cannot be cyclic of order 4 for the same reason as before). Since the class group of F is odd, we can assume that (α) is only supported at the prime ideal $(\sqrt{p})$ and at an ideal dividing 2. The fact that $L(\sqrt{\alpha})/L$ is unramified at primes dividing 2 together with the fact that the quadratic extension L/F has conductor exponent 2 implies that α cannot be divisible by primes dividing 2. In particular, $\alpha \in \{u, \sqrt{p}u\}$ for u a unit of F, and since we are interested in the extension $L(\sqrt{\alpha})/L$ (and $\sqrt[4]{p} \in L$), it is enough to understand the case when α is a unit up to squares.

Let ε_p denote the fundamental unit of $\mathbb{Q}(\sqrt{p})$. Supposes that $p \neq 3$ (as in this case the class number can be computed and prove the veracity of the statement), so that the only roots of unity in F are the fourth roots of unity. By Proposition 6.11, the units of F are generated by $\{i, \kappa\}$, where $\kappa = \sqrt{i \cdot \varepsilon_p}$. Then up to squares, we can restrict to the case $\alpha \in \{i, \kappa, i\kappa\}$.

Start assuming that $p \equiv 3 \pmod{16}$. Then since $p/3$ is a fourth power in $\mathbb{Q}_2$, there is an isomorphism $\Phi : \mathbb{Q}_2(\sqrt[4]{p}) \to \mathbb{Q}_2(\sqrt[4]{3})$ and also an isomorphism between $\mathbb{Q}_2(\sqrt[4]{p}, \sqrt{-1})$ and $\mathbb{Q}_2(\sqrt[4]{3}, \sqrt{-1})$. The extension $\mathbb{Q}_2(\sqrt[4]{-1}, \sqrt[4]{3})/\mathbb{Q}_2(\sqrt{-1}, \sqrt[4]{3})$ is ramified, so $\alpha \neq i$.

The same proof of the previous proposition implies that $\Phi(\varepsilon_p)$ equals ε_3 up to squares in $\mathbb{Q}_2(\sqrt{3}, \sqrt{-1})$. Then we proceed as follows:

- Run over all elements of $\mathcal{O}_F$ modulo 4, and keep only the elements β whose square equals $i \cdot (2 - \sqrt{3})$ modulo 4.
- For each such element β, check whether the extension $F[\sqrt{\beta}]/F$ is ramified or not.

Map	Fixed Field	Map	Fixed Field
σ_1	$\mathbb{Q}$	σ_3	$\mathbb{Q}(\sqrt{-2})$
σ_5	$\mathbb{Q}(\sqrt{-1})$	σ_7	$\mathbb{Q}(\sqrt{2})$

Table 1. Fixed fields of the maps σ_i

It turns out that the first search produces sixteen values of β, and for all of them the extension is ramified, so $\alpha \neq \kappa$. We apply the same strategy to $i \cdot \kappa$ and get no unramified extension either, so $\alpha \neq i\kappa$ deducing that there is no non-trivial extension of L as claimed.

We apply the same check when $p \equiv 11 \pmod{16}$, taking as fundamental unit $\varepsilon_{11} = 10 - 3\sqrt{11}$, obtaining no unramified extension of $\mathbb{Q}_2(\sqrt{11}, \sqrt{-1})$, finishing the proof. □

Proof of Theorem 6.9. Let $L/\mathbb{Q}(\sqrt[4]{p})$ be a quadratic unramified extension. Then the extension $L \cdot \mathbb{Q}(\sqrt[4]{p}, \sqrt{-1})/\mathbb{Q}(\sqrt[4]{p}, \sqrt{-1})$ is unramified of degree at most 2, but by the previous result there is no non-trivial such an extension, so $L = \mathbb{Q}(\sqrt[4]{p}, \sqrt{-1})$, which ramifies at both real infinite places of $\mathbb{Q}(\sqrt[4]{p})$. □

Remark 6.13. With a little more effort, one can prove a similar result for $a = -2p$, with $p \equiv 3 \pmod 8$.

Recall that our goal is to compute the value $\mathrm{Cl}_*(A_{\mathbb{Q}}, \mathcal{C}(-p))[2]$. The marked place $\tilde{v}$ attached to the infinity place of $\mathbb{Q}$ corresponds to the real root $-\sqrt[4]{p}$. Following the notation of Section 4, the extension $\mathbb{Q}(\sqrt[4]{p}, \sqrt{-1})$ ramifies at $\tilde{v}$ and at v_1', so it does not correspond to an element of $\mathrm{Cl}_*(A_{\mathbb{Q}}, \mathcal{C}(-p))$ hence $\mathrm{Cl}_*(A_{\mathbb{Q}}, \mathcal{C}(-p))[2] = 1$. Then (6.4) gives

$$0 \leq \dim_{\mathbb{F}_2} \mathrm{Sel}_2(\mathrm{Jac}(\mathcal{C}(-p))) \leq 2 + 1 = 3.$$

This already improves the upper bound of Theorem 6.7 from 5 to 3. We know that the Selmer group is non-trivial (due to the point of order two on $\mathrm{Jac}(\mathcal{C}(-p))$), so actually

$$1 \leq \dim_{\mathbb{F}_2} \mathrm{Sel}_2(\mathrm{Jac}(\mathcal{C}(-p))) \leq 3. \tag{6.6}$$

This implies that the rank of the surface belongs to the set $\{0, 1, 2\}$. If we can prove that actually the root number of our family is -1, then the parity conjecture implies that its rank is odd hence (assuming the validity of the parity conjecture) it must be one.

6.3. On the root number of $\mathrm{Jac}(\mathcal{C}(-p))$.

The main goal of the present section is to prove the following result.

Theorem 6.14. *Assuming the parity conjecture, the root number of* $\mathrm{Jac}(\mathcal{C}(-p))$ *is* -1 *for all primes* $p \equiv 3 \pmod 8$*. In particular,* $\mathrm{Jac}(\mathcal{C}(-p))$ *has rank* 1 *for all such primes.*

Proof. Let $F = \mathbb{Q}(\zeta_8)$ the field containing the eighth roots of unity. The Galois group $\mathrm{Gal}(F/\mathbb{Q})$ is isomorphic to $\mathbb{Z}/2 \times \mathbb{Z}/2$ and consists of the maps $\sigma_i : \zeta_8 \to \zeta_8^i$, for $i \in (\mathbb{Z}/8)^\times$. Note that the isomorphism between $\mathrm{Gal}(F/\mathbb{Q})$ and $(\mathbb{Z}/8)^\times$ is canonical (i.e. it does does not depend on the choice of root of unity). The fixed field of each map is given in Table 1. Over the field F the endomorphism ring of our surface $\mathrm{Jac}(\mathcal{C}(p))$ contains $\mathbb{Z}[\zeta_8]$ (of rank 4 over $\mathbb{Z}$), hence our surface has complex multiplication over $\mathbb{Q}(\zeta_8)$ (the whole endomorphism algebra equals $M_2(\mathbb{Z}[\sqrt{-2}])$ as proven in Corollary 6.6). As explained in Remark 6.4, there exists an explicit Heche character χ of infinity type $(1,0), (1,0)$ such that

$$L(\mathcal{C}(-1), s) = L(\chi, s).$$

Let θ_a denote the order eight Hecke character corresponding to the extension $L = F(\sqrt[8]{a})/F$. Then the surface $\mathrm{Jac}(\mathcal{C}(a))$ is the "twist" of $\mathrm{Jac}(\mathcal{C}(-1))$ by θ_a (since our surface contains the eighth roots of unity in its endomorphism ring, it makes sense to twist by an order 8 character). Then

$$L(\mathcal{C}(a), s) = L(\chi\theta_a, s),$$

so it is enough to compute the root number of $\chi\theta_a$ for each prime number p dividing $2a$. The problem is that the local computation at primes dividing 2 is very delicate, so we avoid this issue with the following trick: restrict to the case $a = -p$ is an odd prime number (our case of interest).

- For each residue class of p modulo 32, compute the root number of $\mathcal{C}(q)$ for a particular representative q of the congruence class via computing the rank of $\mathcal{C}(q)$ (using Magma) and assuming the parity conjecture.
- If p is another prime congruent to q modulo 32, the extension $F(\sqrt[8]{p/q})/F$ is unramified at 2, so the surfaces $\mathcal{C}(p)$ and $\mathcal{C}(q)$ differ by an octic twist whose conductor is odd (only ramified at primes dividing p and q). Compute how the root number varies under such a twist.
- Apply the previous steps to the primes $q = 3, 11, 19$ and 59 (since we assumed $a \equiv 5 \pmod 8$).

Start with the case $q = 3$. Using Magma we compute the 2-Selmer group of $\mathrm{Jac}(\mathcal{C}(-3))$ and verify that it is isomorphic to $\mathbb{Z}/2 \times \mathbb{Z}/2$. Furthermore, since our curve has a rational point, its set of deficient primes (as in [PS99, Corollary 12]) is empty, so the order of its Tate-Shafarevich group is a square, hence trivial. Since the 2-torsion of $\mathrm{Jac}(\mathcal{C}(-3))$ is $\mathbb{Z}/2$, this implies that $\mathrm{Jac}(\mathcal{C}(-3))$ has rank 1, hence (assuming the parity conjecture) the sign of the functional equation of $\mathrm{Jac}(\mathcal{C}(-3))$ is -1.

Let p be a prime congruent to 3 modulo 32. Let $a = p/3$ and let θ_a be the order 8 character of F corresponding to the extension $F(\sqrt[8]{a})/F$ (so its conductor is only divisible by primes dividing 3 and p). Let χ be the Hecke character attached to $\mathcal{C}(-3)$, so that

$$L(\mathcal{C}(-p), s) = L(\chi\theta_a, s).$$

The local root number variation at primes dividing p. The prime p factors as a product of two primes $\mathfrak{p}\mathfrak{p}'$ in F (each of them with inertial degree 2). Let $\mathcal{O}_\mathfrak{p}$ denote the completion of $\mathcal{O}_F$ at $\mathfrak{p}$. Locally at the prime $\mathfrak{p}$, θ_a has conductor $\mathfrak{p}$ and order 8, so it factors through a character

$$\theta_\mathfrak{p} : \mathcal{O}_\mathfrak{p}^\times \to \mathbb{F}_{p^2}^\times \to \mathbb{C}^\times,$$

sending a generator to an eighth root of unity. Let ψ be an additive unramified character of $F_\mathfrak{p}$ (i.e. ψ restricted to $\mathcal{O}_\mathfrak{p}$ is trivial, but its restriction to $\frac{\mathcal{O}_\mathfrak{p}}{p}$ is not). Let dx be a Haar measure on $F_\mathfrak{p}$ such that $\int_{\mathcal{O}_\mathfrak{p}} dx = 1$ (so the measure is self dual with respect to the additive character ψ). Then the local root number of χ at $\mathfrak{p}$ equals 1 (by [Del73, (3.4.3.1)], since the character is unramified at $\mathfrak{p}$), while the local root number of $\theta_a\chi$ equals

$$\varepsilon(\chi_\mathfrak{p}\theta_\mathfrak{p}, \psi, dx) = \chi_\mathfrak{p}(p) \int_{p^{-1}\mathcal{O}_\mathfrak{p}^\times} \theta_\mathfrak{p}^{-1}(x)\psi(x)dx. \tag{6.7}$$

Since $\theta_\mathfrak{p}$ has conductor exponent 1, the later equals

$$\chi_\mathfrak{p}(p)\theta_\mathfrak{p}(p) \sum_{b \in \mathbb{F}_{p^2}} \theta_\mathfrak{p}(b)\psi\left(\frac{b}{p}\right). \tag{6.8}$$

This Gauss sum has very nice properties, namely (see [BEW98, Chapter 1]):

- Its absolute value equals p.
- $\overline{\sum_{b\in\mathbb{F}_{p^2}}\theta_{\mathfrak{p}}(b)\psi\left(\frac{b}{p}\right)} = \theta_{\mathfrak{p}}(-1)\sum_{b\in\mathbb{F}_{p^2}}\overline{\theta_{\mathfrak{p}}(b)}\psi\left(\frac{a}{p}\right)$.

The same computations applies to the prime $\mathfrak{p}'$. The map σ_7 sends the ideal $\mathfrak{p}$ to $\mathfrak{p}'$ and vice-versa. In particular, it induces an isomorphism $\widetilde{\sigma_7} : \mathcal{O}_{\mathfrak{p}} \to \mathcal{O}_{\mathfrak{p}'}$. Via $\widetilde{\sigma_7}$ we define an additive character and a Haar measure on $F_{\mathfrak{p}'}$ (by composing the ones for $\mathcal{O}_{\mathfrak{p}}$ with the isomorphism σ_7). We claim that under the isomorphism $\widetilde{\sigma_7}$ the following relation holds:

$$\theta_{\mathfrak{p}'}(b) = \theta_{\mathfrak{p}}(\widetilde{\sigma_7}(b))^{-1} = \overline{\theta_{\mathfrak{p}}(\widetilde{\sigma_7}(b))}. \tag{6.9}$$

Recall that in general, if $L/F/M$ is a tower of Galois field extensions, there is an action of $\operatorname{Gal}(L/M)$ on $\operatorname{Gal}(L/F)$ (by conjugation) coming from the fact that the subgroup is normal. If furthermore, $\operatorname{Gal}(L/F)$ is abelian, then we get an action of the quotient $\operatorname{Gal}(F/M)$ on $\operatorname{Gal}(L/F)$. In our particular case, $L = \mathbb{Q}(\sqrt[8]{p/3})$, $F = \mathbb{Q}(\zeta_8)$ and $M = \mathbb{Q}$. Since L/F is abelian, there is a well defined Artin map $\operatorname{Art} : \operatorname{Frac}(F) \to \operatorname{Gal}(L/F)$ (where $\operatorname{Frac}(F)$ corresponds to the group of fractional ideals of $\mathcal{O}_F$), and the Artin map is compatible with the action of $\operatorname{Gal}(F/\mathbb{Q})$ on $\operatorname{Frac}(F)$ in the sense that for any $\sigma \in \operatorname{Gal}(F/\mathbb{Q})$,

$$\operatorname{Art}(\sigma(\mathfrak{p})) = \sigma^{-1}\operatorname{Art}(\mathfrak{p})\sigma.$$

It is easy to verify that for any ideal $\mathfrak{a}$, the Artin map satisfies

$$\operatorname{Art}(\sigma_7(\mathfrak{a})) = \operatorname{Art}(\mathfrak{a})^7. \tag{6.10}$$

Let $\alpha \in \mathcal{O}_F$ be such that:

- $\alpha \equiv 1 \pmod{\mathfrak{p}}$,
- $\alpha \equiv g \pmod{\mathfrak{p}'}$, for g a generator of $(\mathcal{O}_{\mathfrak{p}'}/\mathfrak{p}')^\times$,
- $\alpha \equiv 1 \pmod 3$.

Since θ_a only ramifies at primes dividing $3p$ (with conductor exponent 1), then

$$\theta_a((\alpha)) = \theta_{\mathfrak{p}'}(\alpha) = \theta_{\mathfrak{p}'}(g).$$

On the other hand,

$$\sigma_7\,\theta_a((\alpha)) = \theta_a(\sigma_7(\alpha)) = \theta_{\mathfrak{p}}(\widetilde{\sigma_7}(\alpha)).$$

But equation (6.10) implies that $\sigma_7\,\theta_a = \theta_a^7$, so the claim follows (because $\theta_a^{-1} = \theta_a^7$).

The p-th epsilon factor of $\chi\theta_a$ at p equals the product of the two epsilon factors at $\mathfrak{p}$ and $\mathfrak{p}'$, namely

$$\chi_{\mathfrak{p}}(p)\theta_{\mathfrak{p}}(p)\chi_{\mathfrak{p}'}(p)\theta_{\mathfrak{p}'}(p)\left(\sum_{b\in\mathbb{F}_{p^2}}\theta_{\mathfrak{p}}(b)\psi\left(\frac{b}{p}\right)\right)\left(\sum_{b\in\mathbb{F}_{p^2}}\theta_{\mathfrak{p}'}(b)\psi\left(\frac{b}{p}\right)\right).$$

Formula (6.9) together with the two properties of our Gauss sum and the fact that $\theta_{\mathfrak{p}}(-1) = -1$ (since $p \equiv 3 \pmod 8$, $v_2(p^2-1) = 3$) imply that the root number at p equals

$$-\chi_{\mathfrak{p}}(p)\chi_{\mathfrak{p}'}(p)\theta_{\mathfrak{p}}(p)\theta_{\mathfrak{p}'}(p)p^2. \tag{6.11}$$

Since the character θ_a is unramified at 2, the product formula implies that

$$1 = \theta_{\mathfrak{p}}(p)\theta_{\mathfrak{p}'}(p)\theta_{\mathfrak{q}_3}(p)\theta_{\mathfrak{q}_3'}(p),$$

where $3 = \mathfrak{q}_3\mathfrak{q}_3'$ over F.

The same proof as before gives that $\theta_{\mathfrak{q}_3'}(b) = \overline{\theta_{\mathfrak{q}_3}(\widetilde{\sigma_7}(b))}$ for any $b \in \mathcal{O}_{\mathfrak{q}_3}$. Since $\widetilde{\sigma_7}(p) = p$, $\theta_{\mathfrak{q}_3}(p)\theta_{\mathfrak{q}_3'}(p) = 1$. Then the local root number variation at p equals

$$\varepsilon_p := -\chi_{\mathfrak{p}}(p)\chi_{\mathfrak{p}'}(p)p^2. \tag{6.12}$$

The local root number variation at primes dividing 3. The situation is similar to the previous one, but now if $\mathfrak{p}_3$ and $\mathfrak{p}_3'$ are the two primes dividing 3, then $\chi_{\mathfrak{p}_3}$ is a ramified character, while $\theta_{\mathfrak{p}_3}\chi_{\mathfrak{p}_3}$ is not. Hence the root number variation equals

$$\varepsilon_3 := -\chi_{\mathfrak{p}_3}(3)^{-1}\chi_{\mathfrak{p}_3'}(3)^{-1}3^{-2}. \tag{6.13}$$

The local root number variation at primes dividing 2. The prime 2 ramifies completely in the extension $F/\mathbb{Q}$. Let $\mathfrak{q}_2$ denote the unique prime ideal of F dividing it. Our hypothesis $p \equiv 3 \pmod{32}$ implies that $\mathbb{Q}_2(\zeta_8, \sqrt[8]{p}) \simeq \mathbb{Q}_2(\zeta_8, \sqrt[8]{3})$, so the root number at 2 is the same for both varieties.

To finish the proof, we need to verify the equality

$$\chi_{\mathfrak{p}}(p)\chi_{\mathfrak{p}'}(p)p^2\chi_{\mathfrak{p}_3}(3)^{-1}\chi_{\mathfrak{p}_3'}(3)^{-1}3^{-2} = 1.$$

The surface $\mathrm{Jac}(\mathcal{C}(-3))$ has conductor $2^{11} \cdot 3^4$ (this can be computed using Magma). Since $\delta(F/\mathbb{Q}) = 8$, formula (6.3) implies that the conductor of $\chi_{\mathfrak{q}_2}$ equals 3, so it is trivial at $a = p/3$. Then the product formula for the character χ at the element a implies that

$$1 = \chi_{\mathfrak{q}_3}(p)\chi_{\mathfrak{q}_3'}(p)\chi_{\mathfrak{p}}(p)\chi_{\mathfrak{p}'}(p)p^2/(\chi_{\mathfrak{q}_3}(3)\chi_{\mathfrak{q}_3'}(3)\chi_{\mathfrak{p}}(3)\chi_{\mathfrak{p}'}(3)3^2).$$

The equality $\chi_{\mathfrak{q}_3}(p)\chi_{\mathfrak{q}_3'}(p) = 1 = \chi_{\mathfrak{p}}(3)\chi_{\mathfrak{p}'}(3)$ (which follows from an argument similar to the one applied to θ_a) proves that the root number of $\mathrm{Jac}(\mathcal{C}(-3))$ equals that of $\mathrm{Jac}(\mathcal{C}(-p))$. Then sign of the functional equation of $\mathrm{Jac}(\mathcal{C}(-p))$ also equals -1 and hence (assuming once again the parity conjecture) its rank is odd. But it belongs to the set $\{0, 1, 2\}$, so it equals 1.

Similarly, we compute the rank of $\mathrm{Jac}(\mathcal{C}(q))$, for $q \in \{11, 19, 59\}$. In all cases its 2-Selmer group has rank 2, and their conductors equal $2^{11} \cdot q^4$. The same proof applies to these cases mutatis mutandis. □

7. Examples

The following examples have been computed using Magma [BCP97].

7.1. The genus 2 curve of conductor 277. Consider the hyperelliptic curve

$$\mathcal{C} : y^2 + (x^3 + x^2 + x + 1)y = -x^2 - x$$

with LMFDB label 277.a. This corresponds to the semistable abelian surface of smaller conductor. Its modularity was proven in [BPP+19]. Via a standard change of variables, it can we written in the form

$$\mathcal{C} : y^2 = x^6 + 2x^5 + 3x^4 + 4x^3 - x^2 - 2x + 1.$$

The polynomial $x^6 + 2x^5 + 3x^4 + 4x^3 - x^2 - 2x + 1$ has a rational root (namely $x = -1$) so a change of variables sending -1 to infinity transforms the equation into the quintic

$$\mathcal{C} : y^2 = x^5 + 10x^4 + 8x^3 + 16x^2 - 48x + 32.$$

Over $\mathbb{Q}_2$ the polynomial is irreducible (since the prime 2 is completely ramified in the degree 5 extension $A_{\mathbb{Q}} = \mathbb{Q}[x]/(x^5 + 10x^4 + 8x^3 + 16x^2 - 48x + 32)$), so (†.i) holds at the prime 2. The quotient of the polynomial discriminant by the field discriminant equals 2^{28}, so (†.i) holds for all odd primes and we are in the hypothesis of our main theorem. The set of ramified primes of $A_{\mathbb{Q}}$ over $\mathbb{Q}$ is $\{2, 277\}$. For all primes p which are inert in $A_{\mathbb{Q}}$, Lemma 6.2 implies that the quadratic twist $\mathcal{C}(p)$ also satisfies the hypothesis of Theorem 5.15. Since the narrow class group of $A_{\mathbb{Q}}$ is one, we get that for all primes inert in $A_{\mathbb{Q}}/\mathbb{Q}$,

$$0 \le \mathrm{Sel}_2(\mathrm{Jac}(\mathcal{C}(p))) \le 2.$$

The Galois group $\mathrm{Gal}(A_K/\mathbb{Q}) \simeq S_5$, so the density of inert primes equals 1/5. The first inert primes (up to 100) are $\{3, 7, 13, 29, 41, 59\}$. We computed the 2-Selmer rank of all quadratic twists by inert primes up to 100.000, and in all cases it equals 0.

7.2. **Examples with $K = \mathbb{Q}$.**

Example 1. Consider the hyperelliptic curve

$$\mathcal{C} : y^2 = x^5 + x^2 + 1.$$

The extension $L = \mathbb{Q}[x]/x^5 + x^2 + 1$ is monogenic, and the class of x generates the ring of integers, hence (†.i) is satisfied at all primes. The narrow class number of L is one, hence Theorem 5.15 implies that

$$0 \le \dim_{\mathbb{F}_2} \mathrm{Sel}_2(J) \le 2.$$

One can check (in magma) that the 2-Selmer group is actually isomorphic to $\mathbb{Z}/2 \times \mathbb{Z}/2$, so the upper bound is attained.

The prime 31 is inert in the extension $L/\mathbb{Q}$, so we are in the hypothesis of Lemma 6.2. In particular the same bound applies to the quadratic twist of $\mathcal{C}$ by 31, corresponding to the curve with equation

$$\mathcal{C}(31) : y^2 = x^5 + 31^3x^2 + 31^5.$$

It is easy to verify (in magma) that the Jacobian of such a curve has trivial 2-Selmer group. In particular, the lower bound is also attained. The twist by the prime 101 corresponds to a curve whose 2-Selmer group has rank one. In particular, all intermediate values are also obtained.

Example 2. Let us study the case of some genus 5 curves. Most of the examples were obtained via choosing a random degree 11 polynomial (with coefficients in $[-5, 5]$) and studying the hyperelliptic curves they define. Consider first the hyperelliptic curve

$$\mathcal{C} : y^2 = x^{11} - 3x^9 - 3x^8 + x^7 - x^5 - x^4 - 2x^3 + x^2 - 5x - 1.$$

Let $L/\mathbb{Q}$ denote the degree 11 extension given by the polynomial $x^{11} - 3x^9 - 3x^8 + x^7 - x^5 - x^4 - 2x^3 + x^2 - 5x - 1$. Once again, the class of x generates the ring of integers of L, so the hypothesis (†.i) is always satisfied. The narrow class group of L equals one, hence Theorem 5.15 gives the bounds $0 \le \dim_{\mathbb{F}_2} \mathrm{Sel}_2(J) \le 5$. The Jacobian of $\mathcal{C}$ has 2-Selmer group of rank 0 (as can be verified with Magma), hence the lower bound is obtained. The prime 2 is inert in the extension $L/\mathbb{Q}$, hence one can study twists of $\mathcal{C}$ by any odd prime inert in $L/\mathbb{Q}$ (such primes always exist). An interesting phenomena is that we computed all quadratic twist for such primes up to 2000, and in all cases the twisted curve has trivial 2-Selmer group.

Consider now the hyperelliptic curve with equation

$$\mathcal{C} : y^2 = x^{11} + x^4 + x^2 + x + 1,$$

and let $L/\mathbb{Q}$ denote the degree 11 extension given by the (irreducible) polynomial $x^{11} + x^4 + x^2 + x + 1$. The ring of integers is generated by the class of x, so we are in the hypothesis of Theorem 5.15. The narrow class group of L equals 1, so once again we obtain the bound $0 \le \dim_{\mathbb{F}_2} \mathrm{Sel}_2(J) \le 5$.

The Jacobian of $\mathcal{C}$ has 2-Selmer group isomorphic to $(\mathbb{Z}/2)^5$, so the upper bound is attained. The quadratic twist by $\sqrt{13}$ has 2-Selmer group of rank 3, while the quadratic twist by $\sqrt{149}$ has 2-Selmer group of rank 4. All quadratic twist up to 2000 have 2-Selmer rank in $\{3, 4, 5\}$.

Finally, consider the hyperelliptic curve

$$\mathcal{C} : y^2 = x^{11} + 4x^{10} + 4x^9 - 4x^8 - 2x^7 - 2x^6 - 3x^5 + 4x^4 - 3x^3 - 3x^2 + 2x - 3.$$

It satisfies exactly the same properties as the previous ones. The Jacobian of the curve has 2-Selmer group isomorphic to $\mathbb{Z}/2$, and its quadratic twist by $\sqrt{23}$ (an inert prime in $L/\mathbb{Q}$) has 2-Selmer group of rank 2. All quadratic twists by prime numbers up to 2000 have 2-Selmer group of rank 1 or 2.

In particular, these three examples (and some twists) correspond to genus five hyperelliptic curves whose Jacobians have 2-Selmer group isomorphic to all the possible groups predicted by our main result.

7.3. Examples with $K = \mathbb{Q}(\sqrt{5})$.

Example 3. Let $K = \mathbb{Q}(\sqrt{5})$ and consider the hyperelliptic curve

$$\mathcal{C} : y^2 = x^5 + x^4 + \sqrt{5}x^2 + x + 1.$$

Let L denote the extension A_K, a degree 10 extension over $\mathbb{Q}$. The narrow class group of L is trivial. The prime 2 is inert in $L/\mathbb{Q}$ so (†.i) is satisfied at 2. The discriminant of the degree 10 extension differs from the discriminant of $(x^5 + x^4 + \sqrt{5}x^2 + x + 1)(x^5 + x^4 - \sqrt{5}x^2 + x + 1)$ by a power of 2; in particular, (†.i) is also satisfied for all odd primes of K. We are in the hypothesis of our main result, i.e. $0 \le \dim_{\mathbb{F}_2} \mathrm{Sel}_2(J) \le 4$. The 2-Selmer group of $\mathcal{C}$ has rank 2, the quadratic twist by $\sqrt{23}$ has 2-Selmer group of rank 1, while the quadratic twist by $\sqrt{673}$ has 2-Selmer group of rank 3.

On the other hand, the hyperelliptic curve

$$\mathcal{C} : y^2 = x^5 + 7x^4 + \sqrt{5}x^2 + 3x + 1,$$

satisfies the same properties as the previous one, but has 2-Selmer group of rank 4 (so once again the bound is sharp).

References

[Azi99] Abdelmalek Azizi. Unités de certains corps de nombres imaginaires et abéliens sur **Q**. *Ann. Sci. Math. Québec*, 23(1):15–21, 1999.

[BCP97] 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).

[BEW98] Bruce C. Berndt, Ronald J. Evans, and Kenneth S. Williams. *Gauss and Jacobi sums.* Canadian Mathematical Society Series of Monographs and Advanced Texts. John Wiley & Sons, Inc., New York, 1998. A Wiley-Interscience Publication.

[BG13] Manjul Bhargava and Benedict H. Gross. The average size of the 2-Selmer group of Jacobians of hyperelliptic curves having a rational Weierstrass point. In *Automorphic representations and L-functions*, volume 22 of *Tata Inst. Fundam. Res. Stud. Math.*, pages 23–91. Tata Inst. Fund. Res., Mumbai, 2013.

[BK77] Armand Brumer and Kenneth Kramer. The rank of elliptic curves. *Duke Math. J.*, 44(4):715–743, 1977.

[BPP$^+$19] Armand Brumer, Ariel Pacetti, Cris Poor, Gonzalo Tornaría, John Voight, and David S. Yuen. On the paramodularity of typical abelian surfaces. *Algebra Number Theory*, 13(5):1145–1195, 2019.

[BSPT21] Daniel Barrera Salazar, Ariel Pacetti, and Gonzalo Tornaría. On 2-Selmer groups and quadratic twists of elliptic curves. *Math. Res. Lett.*, 28(6):1633–1660, 2021.

[Cas66] J. W. S. Cassels. Diophantine equations with special reference to elliptic curves. *J. London Math. Soc.*, 41:193–291, 1966.

[Cox13] David A. Cox. *Primes of the form x^2+ny^2*. Pure and Applied Mathematics (Hoboken). John Wiley & Sons, Inc., Hoboken, NJ, second edition, 2013. Fermat, class field theory, and complex multiplication.

[Del73] P. Deligne. Les constantes des équations fonctionnelles des fonctions L. In *Modular functions of one variable, II (Proc. Internat. Summer School, Univ. Antwerp, Antwerp, 1972)*, Lecture Notes in Math., Vol. 349, pages 501–597. Springer, Berlin, 1973.

[DLRW20] Harris B. Daniels, Álvaro Lozano-Robledo, and Erik Wallace. Bounds of the rank of the Mordell-Weil group of Jacobians of hyperelliptic curves. *J. Théor. Nombres Bordeaux*, 32(1):231–258, 2020.

[Fun84] Takeo Funakura. On integral bases of pure quartic fields. *Math. J. Okayama Univ.*, 26:27–41, 1984.

[Jęd21] Tomasz Jędrzejak. Ranks in the family of hyperelliptic Jacobians of $y^2 = x^5 + ax$. *J. Number Theory*, 223:35–52, 2021.

[Li19] Chao Li. 2-Selmer groups, 2-class groups and rational points on elliptic curves. *Trans. Amer. Math. Soc.*, 371(7):4631–4653, 2019.

[Lom19] Davide Lombardo. Computing the geometric endomorphism ring of a genus-2 Jacobian. *Math. Comp.*, 88(316):889–929, 2019.

[MP22] Pascal Molin and Aurel Page. Computing groups of hecke characters. *ANTS XV, Aug 2022, Bristol, United Kingdom*, 2022.

[NU73] Yukihiko Namikawa and Kenji Ueno. The complete classification of fibres in pencils of curves of genus two. *Manuscr. Math.*, 9:143–186, 1973.

[O'M00] O. Timothy O'Meara. *Introduction to quadratic forms.* Classics in Mathematics. Springer-Verlag, Berlin, 2000. Reprint of the 1973 edition.

[PAR19] The PARI Group, Univ. Bordeaux. *PARI/GP version 2.11.1*, 2019. available from `http://pari.math.u-bordeaux.fr/`.

[PS97] 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.

[PS99] Bjorn Poonen and Michael Stoll. The Cassels-Tate pairing on polarized abelian varieties. *Ann. of Math. (2)*, 150(3):1109–1149, 1999.

[Sch95] Edward F. Schaefer. 2-descent on the Jacobians of hyperelliptic curves. *J. Number Theory*, 51(2):219–232, 1995.

[Sch96] Edward F. Schaefer. Class groups and Selmer groups. *J. Number Theory*, 56(1):79–114, 1996.

[Ser68] Jean-Pierre Serre. *Corps locaux.* Publications de l'Université de Nancago, No. VIII. Hermann, Paris, 1968. Deuxième édition.

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

[YY22] Hwajong Yoo and Myungjun Yu. Bounds for 2-Selmer ranks in terms of seminarrow class groups. *Pacific J. Math.*, 320(1):193–222, 2022.

Universidad de Santiago de Chile, Alameda 3363, Santiago, Chile.
Email address: `danielbarreras@hotmail.com`

Center for Research and Development in Mathematics and Applications (CIDMA), Department of Mathematics, University of Aveiro, 3810-193 Aveiro, Portugal
Email address: `apacetti@ua.pt`

Universidad de la República, Montevideo, Uruguay
Email address: `tornaria@cmat.edu.uy`