ON 2-SELMER GROUPS AND QUADRATIC TWISTS OF ELLIPTIC CURVES

DANIEL BARRERA SALAZAR, ARIEL PACETTI, AND GONZALO TORNARÍA

To the memory of John Tate

Abstract. Let K be a number field and E/K be an elliptic curve with no 2-torsion points. In the present article we give lower and upper bounds for the 2-Selmer rank of E in terms of the 2-torsion of a narrow class group of a certain cubic extension of K attached to E. As an application, we prove (under mild hypotheses) that a positive proportion of prime conductor quadratic twists of E have the same 2-Selmer group.

Introduction

Given an elliptic curve E over a number field K, the Mordell-Weil theorem implies that its set of K-rational points is a finitely generated abelian group. In particular, it has a torsion part and a free one. From a computational point of view finding the torsion part is the "easy" task (and is implemented in most number theory computational systems, such as PARI/GP [PAR19], SageMath [Sag19] or Magma [BCP97]). The computation of the free part is more subtle, and involves the *descent* method (see for example section VIII.3 of [Sil09]), and is still an open question whether the proposed algorithms to compute ranks of elliptic curves end or not (depending on the finiteness of the Tate-Shafarevich group).

The most effective way to compute the rank is to apply 2-descent, which involves computing the 2-Selmer group (see Definition 2.2). Since computing the 2-Selmer group involves hard computations, a natural question is whether one can give a bound for it. Let E be an elliptic curve of the form

$$E : y^2 = F(x)$$

with $F(x) \in \mathcal{O}_K[x]$ a monic irreducible cubic polynomial and let $A_K = K[x]/F(x)$ be the cubic extension of K given by $F(x)$. In [BK77] the authors give, for $K = \mathbb{Q}$, an upper bound for semistable elliptic curves in terms of the class group of $A_{\mathbb{Q}}$ (which can be efficiently computed), and is the first article to show a relation between the 2-Selmer group and a class group. Recently, in [Li19] the author used similar ideas to provide a lower bound for the 2-Selmer group of a rational elliptic curve under some restrictive hypotheses; namely has odd and square-free discriminant.

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

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

DBS was supported by the FONDECYT PAI 77180007.

AP was partially supported by PIP 2014-2016 11220130100073 and Proyecto Consolidar 2018-2021 33620180100781CB.

GT was partially supported by ANII–FCE 2017–136609.

The purpose of the present article is to extend the ideas of Brumer-Kramer and Li to give both lower and upper bounds for the 2-Selmer groups of elliptic curves over number fields with more relaxed hypotheses. Denote by $\mathrm{Cl}_*(A_K, E)$ the narrow class group given in Definition 2.8. One of our main results is the following:

Theorem 2.16. *Let K be a number field and let E/K be an elliptic curve satisfying hypotheses 2.1. Then*

$$\dim_{\mathbb{F}_2} \mathrm{Cl}_*(A_K, E)[2] \leq \dim_{\mathbb{F}_2} \mathrm{Se}l_2(E) \leq \dim_{\mathbb{F}_2} \mathrm{Cl}_*(A_K, E)[2] + [K : \mathbb{Q}].$$

In particular, if $K = \mathbb{Q}$, the order of the Selmer group is determined by the 2-torsion of $\mathrm{Cl}_*(A_K, E)$ and the root number of E.

The advantage of our results is twofold: on the one hand, we can get a lower and upper bound which we expect to be sharp for general number fields (we show this is the case in some examples).

On the other hand, our relaxed hypotheses allow us to consider families of quadratic twists of elliptic curves: let for example $E/\mathbb{Q}$ be a rational elliptic curve satisfying hypotheses 2.1, and let p be a prime congruent to 1 modulo 4 which is inert or totally ramified in A_K. Then the quadratic twist E_p of E by a character of conductor p also satisfies hypotheses 2.1, hence our rank bound also applies to its 2-Selmer group. Studying the root number change from E to E_p allows us to deduce that for a positive proportion of them, the rank of their 2-Selmer group is constant. In particular, all such twists have precisely the same 2-Selmer group (see Theorems 3.3 and 3.7). Such interesting phenomena has implication in distributions of ranks of elliptic curves under quadratic twists and the order of the Tate-Shafarevich group $Ш(E_p)[2]$. For example, let $d_2(E)$ denote the 2-Selmer rank of E and define

$$N_r(E, X) = |\{\text{quadratic } L/\mathbb{Q} \ : \ d_2(E^L) = r \text{ and } |\delta(L/\mathbb{Q})| < X\}|,$$

where E^L denotes the quadratic twist of E corresponding to L and $\delta(L/\mathbb{Q})$ is the discriminant of the extension $L/\mathbb{Q}$. A direct application of our result proves the following Corollary.

Corollary 3.4. *Let $E/\mathbb{Q}$ be an elliptic curve satisfying hypotheses 2.1, and suppose furthermore that either $\Delta(E) < 0$ or $\mathrm{Cl}_+(A_\mathbb{Q}) = \mathrm{Cl}(A_\mathbb{Q})$. Let $r \geq 0$, and suppose that E has a quadratic twist by a prime inert in $A_\mathbb{Q}$ whose 2-Selmer group has rank r. Then $N_r(E, X) \gg X/\log(X)^{1-\alpha}$, where*

$$\alpha = \begin{cases} 1/3 & \text{if } A_\mathbb{Q}/\mathbb{Q} \text{ is Galois,} \\ 1/6 & \text{otherwise.} \end{cases}$$

When $\Delta(E) > 0$ a similar result holds replacing α by $\alpha/2$. Such results are important to understand the so called Goldfeld's conjecture. In [MR10] the authors study the problem of the variation of the 2-Selmer group in quadratic twists families, and they obtain a little stronger result for any base field K (see Theorem 1.4), although their techniques are slightly different from ours. In [KL19] the authors obtain similar results as ours over $\mathbb{Q}$ (see the proofs of [KL19, Lemma 5.9 and Lemma 5.10] and [KL19, Theorem 1.12]).

An immediate application of the result is the following: suppose that $E/\mathbb{Q}$ is an elliptic curve with trivial 2-Selmer group, and let $K/\mathbb{Q}$ be the (infinite) polyquadratic extension obtained by composing all quadratic extensions in the hypothesis of Theorems 3.3 and 3.7. Then $E(K)$ is finitely generated (see Corollary 3.6).

The article is organized as follows: Section 1 contains the local computations of the Kummer map and its image, which are needed to bound the 2-Selmer group. Section 2 contains the main result (Theorem 2.16). Our main contributions are: we can work with polynomials $F(x)$ which do not generate the whole ring of integers of A_K (a key fact for allowing quadratic twists), and also we explain in detail how to handle the case of "positive discriminants", i.e. the real places of K where the discriminant of $F(x)$ is positive. In order to treat this case we work with a "narrow class group" instead of a classical one. Section 3 contains the application of the main results to families of quadratic twists. We stated two results (Theorems 3.3 and 3.7) for elliptic curves over $\mathbb{Q}$ (which historically received a lot of attention) but they have a similar version over general number fields. At last, Section 4 includes many examples of elliptic curves over number fields; the purpose of the examples is to show that the bounds obtained in this article are sharp for different number fields. At the same time we show that the lower bound and the upper bound do not hold when twisting by primes not satisfying hypotheses 2.1.

Acknowledgments. The present article grew as a research project in the BIRS-CMO workshop "Number Theory in the Americas" held in Oaxaca. We would like to thank the organizers for providing such a fruitful environment. Part of this project was done in a visit of the second author to the Centro de Matemática of Universidad de la República, we want to thank the institution for its hospitality. We thank Myungjun Yu for reporting a mistake in an earlier verision of Lemma 2.5. Last but not least, we want to thank the referee for many suggestions that improved the exposition and quality of the present article.

1. Kummer map

Let us recall some general statements on the 2-Selmer group on elliptic curves (we refer to Section 2 of [BK77]). Let K be a field of characteristic different from 2, let $\bar{K}$ be a Galois closure of K and let $G_K = \mathrm{Gal}(\bar{K}/K)$. Let E/K be an elliptic curve of the form

$$E : y^2 = F(x)$$

for some monic cubic square-free polynomial $F(x) \in K[x]$. The following exact sequence of G_K-modules

$$0 \longrightarrow E(\bar{K})[2] \longrightarrow E(\bar{K}) \xrightarrow{\times 2} E(\bar{K}) \longrightarrow 0$$

gives rise to a long exact sequence in cohomology. In particular, it induces an injective morphism called the Kummer map

$$\delta_K : E(K)/2E(K) \hookrightarrow H^1(G_K, E(\bar{K})[2]).$$

Let A_K be the K-algebra $K[T]/(F(T))$. Then $H^1(G_K, E(\bar{K})[2])$ is isomorphic to the subgroup of elements in $A_K^\times/(A_K^\times)^2$ whose norm is a square in K (see

[Cas66, p. 240]); let us denote by $(A_K^\times/(A_K^\times)^2)_\square$ such set. In particular, we get an injective map

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

Explicitly, let $P \in E(K)$ and let $x(P)$ denote its first coordinate. Then,

$$\delta_K(P) = x(P) - T,$$

whenever $x(P) - T$ is invertible in A_K (see [BK77, p. 716-717]). Note that the algebra A_K and the map δ_K do not depend on the choice of model for E. Moreover, we denote by $\delta_K(E)$ the image of the Kummer map and remark that it is a hard problem to describe it.

1.1. **The case K a complete archimedean field.** Let Δ denote the discriminant of $F(x)$ and K be a complete archimedean field. Then clearly

$$A_K \simeq \begin{cases} \mathbb{R}\times\mathbb{C} & \text{if } K=\mathbb{R} \text{ and } \Delta<0,\\ \mathbb{R}\times\mathbb{R}\times\mathbb{R} & \text{if } K=\mathbb{R} \text{ and } \Delta>0,\\ \mathbb{C}\times\mathbb{C}\times\mathbb{C} & \text{if } K=\mathbb{C}. \end{cases}$$

In the second case, let $\theta_1 < \theta_2 < \theta_3$ denote the roots of $F(x)$, and take the isomorphism sending T to $(\theta_1, \theta_2, \theta_3)$.

Lemma 1.1. *For complete archimedean fields, the following holds:*

(i) *If $K = \mathbb{R}$ and $\Delta < 0$, $\delta_{\mathbb{R}}(E) = \{(1, 1)\}$,*
(ii) *If $K = \mathbb{R}$ and $\Delta > 0$, $\delta_{\mathbb{R}}(E) = \langle(1, -1, -1)\rangle$,*
(iii) *If $K = \mathbb{C}$, $\delta_{\mathbb{C}}(E) = \{(1, 1, 1)\}$.*

Proof. In cases (i) and (iii) $E(K)/2E(K)$ is trivial. In case (ii) $E(K)/2E(K)$ has order 2, and a point P with $\theta_1 < x(P) < \theta_2 < \theta_3$ maps to $(1, -1, -1)$ up to squares (see also [BK77, Proposition 3.7]). □

Remark 1.2. When $K = \mathbb{R}$ and $\Delta > 0$, A_K has three real places, and one of them is distinguished, as it is the unique one satisfying that the composition of $\delta_{\mathbb{R}}$ with its projection is trivial. Lemma 1.1 states that when the roots of $F(T)$ are ordered, such place corresponds to the first one, but for a general elliptic curve $E/\mathbb{R}$, we can always talk of such distinguished place.

1.2. **The case K is a finite extension of $\mathbb{Q}_p$.** For the rest of this section we assume that K is a finite extension of $\mathbb{Q}_p$. Let $\mathcal{O}$ denote its ring of integers, $\mathfrak{p}$ its maximal ideal, π a generator of $\mathfrak{p}$ and $k = \mathcal{O}/\mathfrak{p}$ its residue field.

Lemma 1.3. *The order of $\delta_K(E)$ equals $[\mathcal{O} : 2\mathcal{O}] \cdot \big|E(K)[2]\big|$.*

Proof. See Lemma 3.1 of [BK77]. □

Let $A_{\mathcal{O}}$ be the ring of integers of A_K.

Remark 1.4. Since A_K is isomorphic to a product of local fields, $A_{\mathcal{O}}$ is isomorphic to the product of the ring of integers of such fields. Furthermore, since $[A_K : K] = 3$, the norm map $\mathcal{N} : A_{\mathcal{O}}^\times/(A_{\mathcal{O}}^\times)^2 \to \mathcal{O}^\times/(\mathcal{O}^\times)^2$ is surjective (it is the identity on the class of elements of $\mathcal{O}^\times$).

Denote $(A_{\mathcal{O}}^\times/(A_{\mathcal{O}}^\times)^2)_\square$ the subgroup of elements in $A_{\mathcal{O}}^\times/(A_{\mathcal{O}}^\times)^2$ with square norm. There is a natural inclusion $(A_{\mathcal{O}}^\times/(A_{\mathcal{O}}^\times)^2)_\square \subset (A_K^\times/(A_K^\times)^2)_\square$.

Lemma 1.5. *The order of* $(A_{\mathcal{O}}^\times/(A_{\mathcal{O}}^\times)^2)_\square$ *equals* $[\mathcal{O}:2\mathcal{O}]^2 \cdot |E(K)[2]|$.

Proof. The K-algebra A_K is isomorphic to a product of fields $L_1 \times \cdots \times L_t$, where $1 \le t \le 3$. Let R_i be the ring of integers of L_i, so that $A_{\mathcal{O}} \simeq R_1 \times \cdots \times R_t$. By [O'M00, Proposition 63:9] we have $[\mathcal{O}^\times : (\mathcal{O}^\times)^2] = 2\,[\mathcal{O}:2\mathcal{O}]$ and $[R_i^\times : (R_i^\times)^2] = 2\,[R_i : 2R_i]$.

Since A_K has dimension 3 over K, we have $\prod [R_i : 2R_i] = [\mathcal{O}:2\mathcal{O}]^3$. It follows that $[A_{\mathcal{O}}^\times : (A_{\mathcal{O}}^\times)^2] = 2^t\,[\mathcal{O}:2\mathcal{O}]^3$. 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 $[A_{\mathcal{O}}^\times : (A_{\mathcal{O}}^\times)^2]\,/\,[\mathcal{O}^\times : (\mathcal{O}^\times)^2] = 2^{t-1}\,[\mathcal{O}:2\mathcal{O}]^2$.

The result follows by noting that $2^{t-1} = |E(K)[2]|$. □

Definition 1.6. We say that $E : y^2 = F(x)$ satisfies (†) if $F(x) \in \mathcal{O}[x]$ is a monic cubic square-free polynomial and any of the following conditions holds:

- (†.i) A_K is a field extension of K, or
- (†.ii) $A_{\mathcal{O}} = \mathcal{O}[T]/(F(T))$, or
- (†.iii) $\mathrm{char}(k) > 2$ and $[E(K) : E_0(K)]$ is odd, where $E_0(K)$ is the subgroup of the points of $E(K)$ whose reduction is non-singular, or
- (†.iv) $\mathrm{char}(k) = 2$, $K/\mathbb{Q}_2$ is unramified, and E has good reduction.

Remark 1.7. When $\mathrm{char}(k) > 2$ condition (†.*i*) or condition (†.*ii*) imply (†.*iii*). To see it let $I_K \subset \mathrm{Gal}(\overline{K}/K)$ be the inertia subgroup and consider the following three possibilities $E[2](\overline{K})^{I_K} = \{0\}$ or $E[2](\overline{K})^{I_K} \cong \mathbb{Z}/2\mathbb{Z}$ or $E[2](\overline{K})^{I_K} \cong (\mathbb{Z}/2\mathbb{Z})^2$. If $E[2](\overline{K})^{I_K} = \{0\}$ then $[E(K) : E_0(K)]$ is odd by [GP12, Lemma 4]. Observe that if (†.*i*) is true then $E[2](\overline{K})^{I_K} \cong \mathbb{Z}/2\mathbb{Z}$ is not possible. If $E[2](\overline{K})^{I_K} \cong \mathbb{Z}/2\mathbb{Z}$ and (†.*ii*) holds $v_{\mathfrak{p}}(\mathrm{disc}(F(x))) = 1$ hence $[E(K) : E_0(K)] = 1$ by Tate's algorithm ([Tat75]). Finally if $E[2](\overline{K})^{I_K} \cong (\mathbb{Z}/2\mathbb{Z})^2$ then hypothesis (†.*i*) or (†.*ii*) implies that E has good reduction hence (†.*iii*) is clearly true.

Theorem 1.8. *If E satisfies* (†) *then* $\delta_K(E) \subset (A_{\mathcal{O}}^\times/(A_{\mathcal{O}}^\times)^2)_\square$.

Proof. A similar result (for particular cases) is given in Corollary 3.3, Proposition 3.4, Lemma 3.5, Proposition 3.6, and Lemma 4.2 of [BK77], and in Lemma 2.12 of [Li19].

Suppose first that E satisfies (†.i), i.e. A_K is a cubic field extension of K (either unramified or totally ramified). Let $\mathfrak{P}$ denote the maximal ideal of $A_{\mathcal{O}}$. Let $P = (x, y) \in E(K)$. The equality $y^2 = F(x)$ implies that $2v_{\mathfrak{P}}(y) = 3v_{\mathfrak{P}}(x - T)$, hence $v_{\mathfrak{P}}(x - T) = 2n$ is even. If $\tilde{\pi}$ denotes a local uniformizer in $A_{\mathcal{O}}$ then $\tilde{\pi}^{-2n}(x - T) \in A_{\mathcal{O}}^\times$ so that $\delta_K(P) \in (A_{\mathcal{O}}^\times/(A_{\mathcal{O}}^\times)^2)_\square$.

Suppose now that E satisfies (†.ii). If A_K is a field the result is already proven, hence we can restrict to the cases $A_K \simeq K \times K \times K$ or $A_K \simeq K \times L$, for L/K a quadratic extension. In the case $A_K \simeq K \times K \times K$, $F(x) = (x - c_1)(x - c_2)(x - c_3)$ with $c_i \in \mathcal{O}$, and hypothesis (†.ii) implies $v_{\mathfrak{p}}(c_i - c_j) = 0$ for $i \ne j$. Let $P = (x, y) \in E(K)$. If $v_{\mathfrak{p}}(x) < 0$ then $v_{\mathfrak{p}}(x - c_i) = v_{\mathfrak{p}}(x)$, hence $2v_{\mathfrak{p}}(y) = 3v_{\mathfrak{p}}(x)$ and so $v_{\mathfrak{p}}(x - c_i)$ is even for all i. Otherwise $v_{\mathfrak{p}}(x) \ge 0$ and $v_{\mathfrak{p}}(x - c_i) \ge 0$ for all i. Since $v_{\mathfrak{p}}(c_i - c_j) = 0$ for $i \ne j$, at least two terms in the right hand side of the equality

$$2v_{\mathfrak{p}}(y) = v_{\mathfrak{p}}(x - c_1) + v_{\mathfrak{p}}(x - c_2) + v_{\mathfrak{p}}(x - c_3),$$

are 0, hence the third term must also be even. In either case $\delta_K(P) = (\pi^{-v_\mathfrak{p}(x-c_1)}(x-c_1), \pi^{-v_\mathfrak{p}(x-c_2)}(x-c_2), \pi^{-v_\mathfrak{p}(x-c_3)}(x-c_3)) \in (A_\mathcal{O}^\times/(A_\mathcal{O}^\times)^2)_\square$.

In the case $A_K \simeq K \times L$ for a quadratic extension L/K (either unramified or ramified), $F(x) = (x-c)(x-\gamma)(x-\gamma')$, with $c \in \mathcal{O}$ and $\gamma \in \mathcal{O}_L$. Let $v_\mathfrak{p}$ denote the valuation of L which extends that of K. Hypothesis (†.ii) implies $v_\mathfrak{p}(c-\gamma) = 0$ and $v_\mathfrak{p}(x-\gamma) \in \{0, \frac{1}{2}\}$ if $x \in \mathcal{O}$. Let $P = (x,y) \in E(K)$, then

$$2v_\mathfrak{p}(y) = v_\mathfrak{p}(x-c) + 2v_\mathfrak{p}(x-\gamma).$$

When $v_\mathfrak{p}(x) < 0$ this implies $v_\mathfrak{p}(x-c) = v_\mathfrak{p}(x-\gamma) = v_\mathfrak{p}(x)$ is even. When $v_\mathfrak{p}(x) \geq 0$ then $v_\mathfrak{p}(x-c) \geq 0$ and $v_\mathfrak{p}(x-\gamma) \geq 0$, and at least one must be 0 since $v_\mathfrak{p}(c-\gamma) = 0$. It follows that $v_\mathfrak{p}(x-\gamma) \in \mathbb{Z} \cap \{0, \frac{1}{2}\}$. Hence $v_\mathfrak{p}(x-\gamma) = 0$ and $v_\mathfrak{p}(x-c)$ is also even. In either case we have $v_\mathfrak{p}(x-c)$ and $v_\mathfrak{p}(x-\gamma)$ are both even, hence $\delta_K(P) = (\pi^{-v_\mathfrak{p}(x-c)}(x-c), \pi^{-v_\mathfrak{p}(x-\gamma)}(x-\gamma)) \in (A_\mathcal{O}^\times/(A_\mathcal{O}^\times)^2)_\square$.

When E satisfies (†.iii) the result is given in [BK77, Corollary 3.3]. Finally, suppose E satisfies (†.iv). When E has supersingular reduction, then the assumption $K/\mathbb{Q}_2$ unramified implies that A_K is a cubic ramified extension of K [BK77, Proposition 3.4], in which case E satisfies (†.i) so the result is already proved. When E has ordinary reduction, the result is proved under the assumption $K/\mathbb{Q}_2$ unramified in [BK77, Proposition 3.6]. □

It is not true that Theorem 1.8 holds in full generality. Here are some examples where the hypotheses (†) are not satisfied and the statement of Theorem 1.8 does not hold.

Example 1. Let

$$E : y^2 = x(x+3p)(x+1-p)$$

be the elliptic curve over $\mathbb{Q}_p$, with Kodaira type I_2 if $p \neq 2,3$, type I_4 if $p = 3$ and type III if $p = 2$, and let $P = (p, 2p) \in E(\mathbb{Q}_p)$. Here $A_{\mathbb{Q}_p} \simeq \mathbb{Q}_p \times \mathbb{Q}_p \times \mathbb{Q}_p$, but two roots are congruent (hence (†.ii) is not satisfied); $\delta_{\mathbb{Q}_p}(P) = (p, 4p, 1) \notin (A_{\mathbb{Z}_p}^\times/(A_{\mathbb{Z}_p}^\times)^2)_\square$.

Example 2. Let $r \in \mathbb{Z}$ with $\left(\frac{r}{p}\right) = -1$ if $p \neq 2$, $r \equiv 1 \pmod 8$ if $p = 2$ and let

$$E : y^2 = x(x^2 - rp^2 - r^2p^4)$$

be the elliptic curve over $\mathbb{Q}_p$, with Kodaira type I_0^* if $p \neq 2$ and type I_2^* if $p = 2$. Let $P = (-rp^2, rp^2) \in E(\mathbb{Q}_p)$. Here $A_{\mathbb{Q}_p} \simeq \mathbb{Q}_p \times \mathbb{Q}_p(\gamma)$ with $\gamma = p\sqrt{r + r^2p^2}$, the latter a quadratic unramified extension (whose ring of integers is not generated by γ, so (†.ii) is not satisfied); $\delta_{\mathbb{Q}_p}(P) = (-rp^2, -rp^2 - \gamma) \notin (A_{\mathbb{Z}_p}^\times/(A_{\mathbb{Z}_p}^\times)^2)_\square$.

Example 3. Let

$$E : y^2 = x(x^2 - p - p^2),$$

with Kodaira type III and let $P = (-p, p) \in E(\mathbb{Q}_p)$. Here $A_{\mathbb{Q}_p} \simeq \mathbb{Q}_p \times \mathbb{Q}_p(\gamma)$ via $T \to (0, \gamma)$ with $\gamma = \sqrt{p + p^2}$ generating a quadratic ramified extension. Since the image satisfies that both coordinates are congruent modulo p, (†.ii) is not satisfied; $\delta_{\mathbb{Q}_p}(P) = (-p, -p-\gamma) \notin (A_{\mathbb{Z}_p}^\times/(A_{\mathbb{Z}_p}^\times)^2)_\square$

Corollary 1.9. *Suppose that E satisfies* (†) *and* $\mathrm{char}(k) > 2$. *Then* $\delta_K(E) = (A_\mathcal{O}^\times/(A_\mathcal{O}^\times)^2)_\square$.

Proof. By Theorem 1.8 we know that $\delta_K(E) \subset (A_{\mathcal{O}}^\times/(A_{\mathcal{O}}^\times)^2)_\square$, and by Lemmas 1.3 and 1.5 both sets have the same cardinality. $\square$

1.2.1. *The case K is a finite extension of $\mathbb{Q}_2$.* Consider the set

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

Note that $(A_{\mathcal{O}}^\times)^2 \subset U_4$.

Lemma 1.10. *Suppose $p = 2$. Then:*

1. *For $\alpha \in \mathcal{O}$ we have*
$$1 + 4\alpha = \square \iff \operatorname{Tr}_{k/\mathbb{F}_2} \alpha = 0$$
2. *Let L/K be a finite extension with odd ramification index. For all $\alpha \in \mathcal{O}_L$ we have*
$$1 + 4\alpha = \square \iff \mathcal{N}_{L/K}(1 + 4\alpha) = \square$$
3. *Let L/K be a finite extension with even ramification index. For all $\alpha \in \mathcal{O}_L$ we have $\mathcal{N}_{L/K}(1 + 4\alpha) = \square$.*
4. *The group $\{u \in \mathcal{O}^\times \ : \ u \equiv \square \pmod 4\}$ contains $(\mathcal{O}^\times)^2$ with index 2.*
5. *The index of $(A_{\mathcal{O}}^\times)^2$ in U_4 is given by*
$$\#(U_4/(A_{\mathcal{O}}^\times)^2) = \begin{cases} 1 & \text{if } A_K \text{ is a field,} \\ 2 & \text{if } A_K \simeq K \times L, \text{ with } L \text{ a field,} \\ 4 & \text{if } A_K \simeq K \times K \times K. \end{cases}$$

Proof. Note first that if $1 + 4\alpha$ is a square, say $1 + 4\alpha = \beta^2$, then $\beta \equiv 1 \pmod 2$. Indeed, $v_{\mathfrak{p}}(\beta - 1) < v_{\mathfrak{p}}(2)$ would imply $v_{\mathfrak{p}}(\beta + 1) = v_{\mathfrak{p}}(\beta - 1) < v_{\mathfrak{p}}(2)$, but then $v_{\mathfrak{p}}(4\alpha) = v_{\mathfrak{p}}(\beta - 1) + v_{\mathfrak{p}}(\beta + 1) < v_{\mathfrak{p}}(4)$ contradicting $\alpha \in \mathcal{O}$.

Furthermore, recall that units in a local field which are congruent to 1 modulo $4\mathfrak{p}$ are squares (see for example [O'M00, Theorem 63:1]), hence $1+4\alpha$ is a square in $\mathcal{O}_L$ if and only if there exists $v \in \mathcal{O}_L$ such that $\alpha \equiv v + v^2 \pmod{\mathfrak{p}}$ (so $(1 + 4\alpha) = (1 + 2v)^2$ up to squares).

Consider the map $\phi : \mathcal{O}/\mathfrak{p} \to \mathcal{O}/\mathfrak{p}$ given by $\phi(v) = v^2 + v$; it is a group homomorphism with kernel $\{0, 1\}$, hence its image has index 2. Furthermore, the composite map $\operatorname{Tr}_{k/\mathbb{F}_2} \circ \phi : \mathcal{O}/\mathfrak{p} \to \mathbb{F}_2$ is the trivial map. Since the trace map is surjective, we conclude that the image of ϕ equals the kernel of the trace map, which proves the first statement.

To prove statements (2) and (3), let L/K be a finite extension of local fields with ramification index e_L, ring of integers $\mathcal{O}_L$, maximal ideal $\mathfrak{p}_L$ and residue field k_L. Clearly $\mathcal{N}_{L/K}(1 + 4\alpha) \equiv 1 + 4 \operatorname{Tr}_{L/K}(\alpha) \pmod{4\mathfrak{p}}$, hence the results follow from a comparison between the trace map on L/K and the one on their residue fields. Recall that if $x \in \mathcal{O}_L$, $\operatorname{Tr}_{L/K}(x) \equiv e_L \operatorname{Tr}_{k_L/k}(\bar{x}) \pmod{\mathfrak{p}}$ (see [CF69] Lemma 1, page 20), so the result follows.

To prove (4) note that $u \equiv \square \pmod 4$ if and only if $K(\sqrt{u})/K$ is a quadratic unramified extension, and there are exactly two such extensions (the split extension and the unramified field extension).

The last statement follows easily from the previous ones. For example when A_K is a field apply (4) to A_K to obtain $\{u \in A_{\mathcal{O}}^\times \ : \ u \equiv \square \pmod 4\}/(A_{\mathcal{O}}^\times)^2$ has exactly two elements and statement (2) implies that only the trivial one has square norm. The other two cases follow from a similar computation using (3) and (4).

□

Theorem 1.11. *Let $K/\mathbb{Q}_2$ be a finite extension and let E/K be an elliptic curve satisfying (†). Then $\delta_K(E) \subset (A_{\mathcal{O}}^\times/(A_{\mathcal{O}}^\times)^2)_\square$ with index $2^{[K:\mathbb{Q}_2]}$. Furthermore, $U_4 \subset \delta_K(E)$.*

Proof. The first claim follows from Theorem 1.8 and Lemmas 1.3 and 1.5. For the second statement, suppose first that E satisfies (†.i), so that A_K is a field. Then the result follows since $U_4/(A_{\mathcal{O}}^\times)^2$ is trivial by Lemma 1.10.

Suppose now that E satisfies (†.ii). The case when A_K is a field is already proved. Recall that if E/K is given by

$$E : y^2 = x^3 + a_2\, x^2 + a_4\, x + a_6$$

with $a_2, a_4, a_6 \in \mathcal{O}$, using the formal group structure on E, for every $z \in \mathfrak{p}$ there is a point $P = P(z)$ with x-coordinate given by

$$x(P) = z^{-2} - a_2 + O(z^2)\,.$$

Then

$$z^2\, \delta_K(P) = z^2\, (x(P) - T) = 1 - (a_2 + T)\, z^2 + O(z^4)\,.$$

In the case $A_K \simeq K \times K \times K$, by Lemma 1.10, $U_4/(A_{\mathcal{O}}^\times)^2$ has 4 elements of the form $\{(\square,\square,\square), (\not\square,\square,\not\square), (\not\square,\not\square,\square), (\square,\not\square,\not\square)\}$. It is enough to prove that there exists $z_1, z_2, z_3 \in \mathcal{O}$ such that $\delta_K(P(2z_i))$ has i-th coordinate not a square. Let $u = 1 + 4\alpha \in \mathcal{O}$ be a unit congruent to 1 modulo 4 which is not a square. Let $\{c_1, c_2, c_3\}$ be the roots of $F(x)$. The hypothesis (†.ii) implies that $\mathfrak{p} \nmid (c_2 + c_3) = -(a_2 + c_1)$, so there exists $z_1 \in \mathcal{O}$ such that $-(a_2 + c_1)z_1^2 \equiv \alpha \pmod{\mathfrak{p}}$ (since the map $x \to x^2$ is a bijection in $\mathcal{O}/\mathfrak{p}$). Then $\delta_K(P(2z_1)) = (u, *, *)$ has its first coordinate a non-square. A similar argument applies to the other two coordinates.

In the case $A_K \simeq K \times L$ for a quadratic extension L/K, let $\{c, \gamma, \gamma'\}$ be the roots of $F(x)$, with $c \in \mathcal{O}$ and $\gamma \in \mathcal{O}_L$. If L/K is unramified, consider $z = 2u$ so the first coordinate $z^2\, \delta_K(P(z))_1 \equiv 1 + 4(\gamma + \gamma')u^2 \pmod{4\mathfrak{p}}$, and the hypothesis (†.ii) implies that $\gamma + \gamma' \notin \mathfrak{p}$, hence there exists $u \in \mathcal{O}$ such that $1 + 4(\gamma + \gamma')u^2$ is not a square. If L/K is ramified, let $\mathfrak{P}$ be the maximal ideal of $\mathcal{O}_L$ and consider $z = 2u$ so the second coordinate $z^2\delta_K(P(z))_2 \equiv 1 + 4(c + \gamma')u^2 \pmod{4\mathfrak{p}}$. The hypothesis (†.ii) implies that $c + \gamma' \notin \mathfrak{P}$ so there exists $u \in \mathcal{O}$ (we can take $u \in \mathcal{O}$ because it has the same residue field as $\mathcal{O}_L$) such that $1 + 4(c + \gamma')u^2$ is not a square.

In either case, $z^2\delta_K(P(z)) \in U_4$ is not a square in A_K, but by Lemma 1.10, we know that $U_4/(A_{\mathcal{O}}^\times)^2$ has two elements so the statement follows.

The case (†.iii) does not occur since $\mathrm{char}(k) = 2$. Finally, suppose E satisfies (†.iv). If E has supersingular reduction, then A_K is a cubic ramified extension of K [BK77, Proposition 3.4], in which case the result is already proved. If E has ordinary reduction, the result follows from [BK77, Proposition 3.6]. □

2. 2-Selmer groups and Class groups

Suppose now that K is a number field and E is an elliptic curve over K. For v a place of K, let K_v denotes its completion. From now on we assume the following hypotheses:

Hypotheses 2.1. *The elliptic curve E and the field K satisfy:*

(1) The narrow class number of K is odd.
(2) $E(K)[2] = \{0\}$.
(3) For all finite places v of K, E/K_v satisfies (†) (see Definition 1.6).

Note that the second hypothesis implies that A_K is a cubic field extension of K and we denote by $A_{\mathcal{O}}$ its ring of integers. For each place v of K, let $G_v = G_{K_v}$ and fix an immersion $G_v \hookrightarrow G_K$. To ease the notation let $\delta_v = \delta_{K_v}$ and let res_v denote the restriction map $H^1(G_K, E(\bar{K})[2]) \to H^1(G_v, E(\bar{K}_v)[2])$.

Definition 2.2. The 2-Selmer group of E consists of the cohomology classes in $H^1(G_K, E(\bar{K})[2])$ whose restriction to G_v lies in the image of δ_v for all places v of K, i.e.

$$\text{S}el_2(E) = \{c \in H^1(G_K, E(\bar{K})[2]) \ : \ \text{res}_v(c) \in \delta_v(E) \text{ for each place } v \text{ of } K\}.$$

If v is an archimedean place of K then either:

(i) $K_v \simeq \mathbb{R}$ and $A_{K_v} \simeq \mathbb{R} \times \mathbb{C}$,
(ii) $K_v \simeq \mathbb{R}$ and $A_{K_v} \simeq \mathbb{R} \times \mathbb{R} \times \mathbb{R}$,
(iii) $K_v \simeq \mathbb{C}$ and $A_{K_v} \simeq \mathbb{C} \times \mathbb{C} \times \mathbb{C}$.

We say that an archimedean place of K has type (i), (ii) or (iii) depending on the above cases. Let us introduce the following notations: if $\alpha \in A_K$, the notation $\mathcal{N}(\alpha) \gg 0$ means that for each real archimedean place v of K, $v(\mathcal{N}(\alpha)) > 0$. If v is a real place of K of type (i), let $\tilde{v}$ denote the unique real place in A_K extending v. If v is a real place of K of type (ii), let $\tilde{v}$, $\tilde{v}_2$, $\tilde{v}_3$ denote the places of A_K extending v, so that $\tilde{v}$ is the distinguished one (see Remark 1.2).

Define the following subgroups of $A_K^\times/(A_K^\times)^2$:

$$C_*(E) = \big\{ [\alpha] \in A_K^\times/(A_K^\times)^2 \ : \ A_K(\sqrt{\alpha})/A_K \text{ is unramified at all finite places of } A_K, \text{ it is unramified at } \tilde{v} \text{ for all real places } v \text{ of } K, \text{ and for each } v \text{ of type (ii) it ramifies at } \tilde{v}_2 \Leftrightarrow \text{it ramifies at } \tilde{v}_3 \big\},$$

and

$$\tilde{C}(E) = \big\{ [\alpha] \in A_K^\times/(A_K^\times)^2 \ : \ \mathcal{N}(\alpha) = \square, \ w(\alpha) \text{ is even for all finite places } w \text{ of } A_K, \ \tilde{v}(\alpha) > 0 \text{ for all real places } v \text{ of } K \big\}.$$

Remark 2.3. In the definition of $C_*(E)$ and $\tilde{C}(E)$, the dependence of E comes only from the distinguished place in A_K at real archimedean places of type (ii). In particular, if no such place exists, these subgroups depend only on A_K (and not on the particular curve whose cubic field extension of K is A_K).

Example 4. Here is a concrete example where $C_*(E)$ depends on E and not only on A_K: consider the curve

$$E : y^2 = F(x) = x^3 - 7x + 3$$

over $K = \mathbb{Q}$, so that $A_{\mathbb{Q}} = \mathbb{Q}[T]/(T^3 - 7T + 3)$. The real place v of $\mathbb{Q}$ is of type (ii) since F has three real roots $\theta_1 < \theta_2 < \theta_3$. The field $A_{\mathbb{Q}}$ has class number 1, but narrow class number 2. Indeed the narrow Hilbert class field (maximal abelian extension unramified at all finite places) of $A_{\mathbb{Q}}$ is $A_{\mathbb{Q}}(\sqrt{T^2 - 8})$; it is unramified at $\tilde{v}$ and it is ramified at $\tilde{v}_2$ and $\tilde{v}_3$ (since $\theta_1^2 - 8 > 0$, $\theta_2^2 - 8 < 0$ and $\theta_3^2 - 8 < 0$). Thus $[T^2 - 8] \in C_*(E)$ and $C_*(E)$ has order 2.

On the other hand, consider the quadratic twist of E by $\mathbb{Q}(\sqrt{-1})$,

$$E_{-1} : y^2 = -F(-x) = x^3 - 7x - 3\,.$$

This curve has the same cubic field $A_{\mathbb{Q}}$, but twisting changes the distinguished place from $\tilde{v}$ to $\tilde{v}_3$, so that $[T^2 - 8] \notin C_*(E_{-1})$ and it follows that $C_*(E_{-1})$ is trivial. In Example 7 we use this to compute the 2-Selmer rank for all the quadratic twists of this curve.

Lemma 2.4. *The set $C_*(E)$ equals the set of elements $[\alpha] \in A_K^\times/(A_K^\times)^2$ satisfying the following local conditions:*

- *For all finite places w of A_K, $w(\alpha)$ is even.*
- *For all real places v of K, $\tilde{v}(\alpha) > 0$.*
- $\mathcal{N}(\alpha) \gg 0$.
- $\alpha \equiv \square \pmod{4A_{\mathcal{O}}}$.

Proof. The only non-trivial part is the condition at places dividing 2, which is a well known result and a detailed proof is given in [CP19, Lemma 3.4]. $\square$

Lemma 2.5. *We have $C_*(E) \subset (A_K^\times/(A_K^\times)^2)_\square$.*

Proof. If $[\alpha] \in C_*(E)$, by Lemma 2.4 its norm $\mathcal{N}(\alpha)$ has even valuation at all finite places of K, it is totally positive, and a square modulo $4\mathcal{O}$. Hence $K(\sqrt{\mathcal{N}(\alpha)})/K$ is unramified at all places of K, and since the class number of K is odd, this implies that $\mathcal{N}(\alpha)$ is a square. $\square$

Proposition 2.6. *The following inclusions hold*

$$C_*(E) \subset \mathrm{Sel}_2(E) \subset \tilde{C}(E).$$

Proof. Since $C_*(E) \subset (A_K^\times/(A_K^\times)^2)_\square$, to prove that $C_*(E) \subset \mathrm{Sel}_2(E)$ it is enough to check that if $[\alpha] \in C_*(E)$ then for each place v of K, $[\alpha] \in \mathrm{Im}(\delta_v)$. The condition at the infinity places is clear by Lemma 1.1. If v is a finite place of K not dividing 2, as the quadratic extension is unramified then α is a unit in A_{K_v} (up to squares), hence by Corollary 1.9 it lies in the image of δ_v. For a place v dividing 2, by Lemma 2.4, $\alpha \equiv \square \pmod{4A_{\mathcal{O}}}$, and by Theorem 1.11 such set is contained in the image of δ_v.

The claim $\mathrm{Sel}_2(E) \subset \tilde{C}(E)$ follows from Lemma 1.1 and Theorem 1.8. $\square$

Let $\mathrm{Frac}(A_K)$ denote the group of fractional ideals of A_K, let P be the subgroup of principal ideals, and consider the subgroup

$$P_*(E) = \{(\alpha) \in P : \text{ and } \tilde{v}_2(\alpha)\,\tilde{v}_3(\alpha) > 0 \text{ for all } v \text{ of type (ii) }\}$$

Let $P_+ = \{(\alpha) \in P : \alpha \gg 0\}$. Clearly $P_+ \subset P_*(E) \subset P$ and P/P_+ is an elementary 2-group.

Lemma 2.7. *We have:*

$$P_*(E) = \{(\alpha) \in P : \ \tilde{v}(\alpha) > 0 \textit{ for all real places } v \textit{ of } K, \textit{ and } \mathcal{N}(\alpha) \gg 0 \ \}$$

Proof. The inclusion $\supset$ is trivial. For the other inclusion, let $(\alpha) \in P_*(E)$. Since the narrow class number of K is odd there are units in K with arbitrary signs for the real places, in particular there is a unit $\mu \in \mathcal{O}^\times$ such that $\tilde{v}(\mu\alpha) > 0$ for all real places of K. Moreover, this implies that $\mathcal{N}(\mu\alpha) \gg 0$. Thus $(\alpha) = (\mu\alpha)$ is in the set of the right hand side. □

Definition 2.8. Denote $\mathrm{Cl}(A_K) = \mathrm{Frac}(A_K)/P$ the class group of A_K and $\mathrm{Cl}_+(A_K) = \mathrm{Frac}(A_K)/P_+$ the narrow class group of A_K. Let

$$\mathrm{Cl}_*(A_K, E) = \mathrm{Frac}(A_K)/P_*(E)$$

denote the class group attached to $P_*(E)$.

Remark 2.9. If $\mathrm{Cl}_+(A_K) = \mathrm{Cl}(A_K)$, then $P_+ = P = P_*(E)$, and therefore $\mathrm{Cl}_*(A_K, E) = \mathrm{Cl}(A_K)$. In particular, $\mathrm{Cl}_*(A_K, E)$ is independent of the elliptic curve E.

Proposition 2.10. *The group $C_*(E)$ is isomorphic to the torsion 2-subgroup of $\mathrm{Cl}_*(A_K, E)$, i.e. $C_*(E) \simeq \mathrm{Cl}_*(A_K, E)[2]$.*

Proof. Let L be the maximal abelian extension of A_K satisfying:

- it is unramified at all finite places of A_K,
- it is unramified at $\tilde{v}$ for all real places v of K,
- for each v of type (ii), $G_{\tilde{v}_2} = G_{\tilde{v}_3}$ as subgroups of $\mathrm{Gal}(L/A_K)$.

Then L is a finite extension of A_K, and $C_*(E) \simeq \mathrm{Hom}(\mathrm{Gal}(L/A_K), \mu_2)$. The Artin reciprocity map $\mathrm{rec} : \mathrm{Frac}(A_K) \to \mathrm{Gal}(L/A_K)$ has kernel $P_*(E)$, hence $\mathrm{Cl}_*(A_K, E) \simeq \mathrm{Gal}(L/A_K)$. It follows that $C_*(E) \simeq \mathrm{Cl}_*(A_K, E)[2]$ as claimed. □

Theorem 2.11. *The index $[\tilde{C}(E) : C_*(E)] \le 2^{[K:\mathbb{Q}]}$.*

Before giving the proof, we need some auxiliary results. Let A, B and C be the set of archimedean places of K of type (i), (ii) and (iii) respectively, and let a, b, c denote their cardinalities, so $[K : \mathbb{Q}] = a + b + 2c$. Consider the *sign map*

$$\mathrm{sign} : A_K^\times \to \prod_{v \in A} \{\pm 1\} \times \prod_{v \in B} (\{\pm 1\} \times \{\pm 1\} \times \{\pm 1\}) .$$

This induces a well defined map on $A_K^\times/(A_K^\times)^2$. Let

$$\tilde{W} = \prod_{v \in A} \{1\} \times \prod_{v \in B} W$$

where $W = \{(1, 1, 1), (1, -1, -1), (-1, 1, -1), (-1, -1, 1)\}$, and let

$$\tilde{V} = \prod_{v \in A} \{1\} \times \prod_{v \in B} V \subset \tilde{W}$$

where $V = \{(1, 1, 1), (1, -1, -1)\}$. Note that $\mathrm{sign}((A_K^\times/(A_K^\times)^2)_\square) \subset \tilde{W}$ and $\mathrm{sign}(\tilde{C}(E)) \subset \tilde{V}$.

Lemma 2.12. *There is an isomorphism*

$$\mathrm{sign}((A_{\mathcal{O}}^\times/(A_{\mathcal{O}}^\times)^2)_\square) \cdot \tilde{V} \simeq \frac{\mathrm{sign}(A_{\mathcal{O}}^\times) \cdot \tilde{V}}{\mathrm{sign}(\mathcal{O}^\times)} .$$

Proof. The inclusion $\operatorname{sign}((A_{\mathcal{O}}^\times/(A_{\mathcal{O}}^\times)^2)_\square) \subset \operatorname{sign}(A_{\mathcal{O}}^\times)$ induces a morphism $\operatorname{sign}((A_{\mathcal{O}}^\times/(A_{\mathcal{O}}^\times)^2)_\square)\cdot\tilde{V} \to (\operatorname{sign}(A_{\mathcal{O}}^\times)\cdot\tilde{V})/\operatorname{sign}(\mathcal{O}^\times)$. To prove it is surjective, let $\alpha \in A_{\mathcal{O}}^\times$. Clearly $\mathcal{N}(\alpha) \in \mathcal{O}^\times$, so $\operatorname{sign}(\alpha) = \operatorname{sign}(\alpha\,\mathcal{N}(\alpha))\operatorname{sign}(\mathcal{N}(\alpha))$ is the image of $\operatorname{sign}(\alpha\,\mathcal{N}(\alpha)) \in \operatorname{sign}((A_{\mathcal{O}}^\times/(A_{\mathcal{O}}^\times)^2)_\square)$.

To prove it is injective note that $\operatorname{sign}((A_{\mathcal{O}}^\times/(A_{\mathcal{O}}^\times)^2)_\square)\cdot\tilde{V} \subset \tilde{W}$ and $\operatorname{sign}(\mathcal{O}^\times)$ satisfies that for places v in B its three coordinates are the same, hence $\operatorname{sign}(\mathcal{O}^\times)\cap\tilde{W}$ is trivial. □

Let $[\alpha] \in \tilde{C}(E)$. Since $w(\alpha)$ is even for all finite places w of A_K, there is a (unique) ideal $I \in \operatorname{Frac}(A_K)$ such that $I^2 = (\alpha)$.

Lemma 2.13. *The association $[\alpha] \mapsto [I]$ induces a well defined map ϕ : $\tilde{C}(E) \to \operatorname{Cl}(A_K)$.*

Proof. Let $\alpha \in A_K^\times$ and $I \in P$ such that $I^2 = (\alpha)$. If $\beta^2 \in (A_K^\times)^2$ then $(\alpha\beta^2) = I^2(\beta^2) = (I\beta)^2$. As $I(\beta)$ lies in the same class as I then the map ϕ is well defined. □

Proof of Theorem 2.11. Consider the short exact sequences

$$0 \longrightarrow \ker\phi \longrightarrow \tilde{C}(E) \xrightarrow{\ \phi\ } \operatorname{Cl}(A_K)$$

and

$$0 \longrightarrow P/P_*(E) \longrightarrow \operatorname{Cl}_*(A_K,E)[2] \xrightarrow{\ \psi\ } \operatorname{Cl}(A_K)$$

where ψ is the restriction of the natural projection $\operatorname{Cl}_*(A_K,E) \to \operatorname{Cl}(A_K)$. From the definition of $\tilde{C}(E)$ and Lemma 2.7 it is clear that the image of ϕ is contained in that of ψ, and using Proposition 2.10 it follows that

$$[\tilde{C}(E) : C_*(E)] = \frac{\#\tilde{C}(E)}{\#\operatorname{Cl}_*(A_K,E)[2]} \le \frac{\#\ker\phi}{\#(P/P_*(E))}. \tag{2.1}$$

If $[\alpha] \in \ker\phi$, then $(\alpha) = (\beta)^2$, so $\alpha = \beta^2\mu$, with $\mu \in A_{\mathcal{O}}^\times$. Thus

$$\ker\phi = (A_{\mathcal{O}}^\times/(A_{\mathcal{O}}^\times)^2)_\square \cap \tilde{C}(E).$$

The sign map induces an isomorphism

$$\frac{(A_{\mathcal{O}}^\times/(A_{\mathcal{O}}^\times)^2)_\square}{(A_{\mathcal{O}}^\times/(A_{\mathcal{O}}^\times)^2)_\square\cap\tilde{C}(E)} \simeq \frac{\operatorname{sign}((A_{\mathcal{O}}^\times/(A_{\mathcal{O}}^\times)^2)_\square)}{\operatorname{sign}((A_{\mathcal{O}}^\times/(A_{\mathcal{O}}^\times)^2)_\square)\cap\tilde{V}}.$$

By the second isomorphism theorem,

$$\frac{\operatorname{sign}((A_{\mathcal{O}}^\times/(A_{\mathcal{O}}^\times)^2)_\square)}{\operatorname{sign}((A_{\mathcal{O}}^\times/(A_{\mathcal{O}}^\times)^2)_\square)\cap\tilde{V}} \simeq \frac{\operatorname{sign}((A_{\mathcal{O}}^\times/(A_{\mathcal{O}}^\times)^2)_\square)\cdot\tilde{V}}{\tilde{V}},$$

hence

$$\frac{\#(A_{\mathcal{O}}^\times/(A_{\mathcal{O}}^\times)^2)_\square}{\#\ker\phi} = \frac{\#(\operatorname{sign}((A_{\mathcal{O}}^\times/(A_{\mathcal{O}}^\times)^2)_\square)\cdot\tilde{V})}{\#\tilde{V}} = \frac{\#(\operatorname{sign}(A_{\mathcal{O}}^\times)\cdot\tilde{V})}{\#\tilde{V}\,\#\operatorname{sign}(\mathcal{O}^\times)},$$

where the last equality follows from Lemma 2.12.

On the other hand,

$$\frac{P}{P_*(E)} \simeq \frac{A_K^\times}{A_{\mathcal{O}}^\times\cdot\operatorname{sign}^{-1}(\tilde{V})} \simeq \frac{\operatorname{sign}(A_K^\times)}{\operatorname{sign}(A_{\mathcal{O}}^\times)\cdot\tilde{V}}$$

via the sign map. We conclude

$$[\tilde{C}(E) : C_*(E)] \leq \frac{\#\ker\phi}{\#(P/P_*(E))} = \frac{\#\tilde{V}\,\#\operatorname{sign}(\mathcal{O}^\times)\,\#(A_\mathcal{O}^\times/(A_\mathcal{O}^\times)^2)_\square}{\#\operatorname{sign}(A_K^\times)}$$

and the theorem follows from the facts that $\#\tilde{V} = 2^b$, $\#\operatorname{sign}(\mathcal{O}^\times) = 2^{a+b}$, $\#(A_\mathcal{O}^\times/(A_\mathcal{O}^\times)^2)_\square = 2^{a+2b+2c}$ (see Lemma 2.14 below), $\#\operatorname{sign}(A_K^\times) = 2^{a+3b}$ and $a + b + 2c = [K : \mathbb{Q}]$. □

Lemma 2.14. *With the previous notation,* $\#(A_\mathcal{O}^\times/(A_\mathcal{O}^\times)^2)_\square = 2^{a+2b+2c}$.

Proof. Consider the norm map $\mathcal{N} : A_\mathcal{O}^\times/(A_\mathcal{O}^\times)^2 \to \mathcal{O}^\times/(\mathcal{O}^\times)^2$. This map is surjective since $[A_K : K] = 3$ (given $\epsilon \in \mathcal{O}^\times$, $\mathcal{N}(\epsilon) = \epsilon$ up to squares) and $(A_\mathcal{O}^\times/(A_\mathcal{O}^\times)^2)_\square$ is by definition its kernel. By Dirichlet's unit theorem we have $\#\mathcal{O}^\times/(\mathcal{O}^\times)^2 = 2^{a+b+c}$. Likewise we have $\#A_\mathcal{O}^\times/(A_\mathcal{O}^\times)^2 = 2^{2a+3b+3c}$, and the result follows. □

Remark 2.15. The inequality in Theorem 2.11 becomes an equality if the image of ψ equals that of ϕ; in that case, the inequality in (2.1) becomes an equality and the proof continues mutatis mutandis. This is the case if for example K is a totally real number field. The reason is that a totally positive number field K with odd class number satisfies that all totally positive units are squares. Then if $I \in \operatorname{Cl}_*(A_K, E)[2]$, by definition $I^2 = (\alpha)$, with $\alpha \in P_*(E)$. Clearly α has even valuation at all finite places, and satisfies the hypothesis on elements of $\tilde{C}(E)$ at the archimedean places by definition of $P_*(E)$. Note that $\mathcal{N}(\alpha)$ is a square up to a unit (it matches the norm of I^2), and it is totally positive, hence the unit must be also a square.

Combining Proposition 2.6, Proposition 2.10 and Theorem 2.11, we obtain

Theorem 2.16. *Let K be a number field and let E/K be an elliptic curve satisfying hypotheses 2.1. Then*

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

In particular, if $K = \mathbb{Q}$, the order of the Selmer group is determined by the 2-torsion of $\operatorname{Cl}_*(A_K, E)$ and the root number of E.

This is a generalization of [Li19, Theorem 2.18], noting that if $\Delta(E) < 0$ then $\operatorname{Cl}_*(A_\mathbb{Q}, E) = \operatorname{Cl}(A_\mathbb{Q})$ (in particular it does not depend on the elliptic curve E). It is a natural question whether the bound in Theorem 2.16 is sharp. We will show some examples of elliptic curves over number fields which do attain the lower and upper bound in Section 4.

3. Application to quadratic twists

For this section, $E/\mathbb{Q}$ will denote an elliptic curve satisfying hypotheses 2.1. If $d \in \mathbb{Z}$, we denote by E_d the twist of E by $\mathbb{Q}(\sqrt{d})$, namely if E is given by an equation $E : y^2 = F(x)$ then $E_d : dy^2 = F(x)$, which also equals

$$E_d : y^2 = d^3 F(x/d).$$

Note that both E and E_d have the same attached cubic field.

Lemma 3.1. *If d is a fundamental discriminant satisfying that all primes $p \mid d$ are inert or totally ramified in $A_\mathbb{Q}$ then the twisted curve E_d also satisfies hypotheses 2.1.*

Proof. By definition, we need to check the condition locally at each prime p. Clearly the condition (†.i) is invariant under twisting (since the attached cubic field is invariant). Note that all primes p dividing d belong to the case (†.i) by the hypothesis. Consider now a prime $p \nmid d$. If $E/\mathbb{Q}_p$ satisfies (†.ii) then the discriminants of $F(x)$ and $d^3F(x/d)$ differ by a unit, hence E_d also satisfies (†.ii). If $E/\mathbb{Q}_p$ satisfies (†.iii) then E_d also satisfies (†.iii), since for each $p > 2$ the parity of $[E(\mathbb{Q}_p) : E_0(\mathbb{Q}_p)]$ and $[E_d(\mathbb{Q}_p) : (E_d)_0(\mathbb{Q}_p)]$ are equal (see the proof of [KL19, Lemma 5.6]). At last, if $E/\mathbb{Q}_p$ satisfies (†.iv) then E_d also satisfies (†.iv), because for $d \equiv 1 \pmod 4$, E has good reduction at 2 if and only if E_d does. □

In particular, if d is a fundamental discriminant such that all primes $p \mid d$ are inert in $A_{\mathbb{Q}}$, we can apply Theorem 2.16 to both E and E_d. The caveat is that if $\Delta(E) > 0$ the order of the roots of $F(T)$ (hence the distinguished place) is reversed when $d < 0$ and preserved when $d > 0$, hence for $d < 0$ the class groups $\mathrm{Cl}_*(A_{\mathbb{Q}}, E)$ and $\mathrm{Cl}_*(A_{\mathbb{Q}}, E_d)$ might be different (but only if $\Delta(E) > 0$ and $\mathrm{Cl}_+(A_{\mathbb{Q}}) \neq \mathrm{Cl}(A_{\mathbb{Q}})$). This issue can be overcome if we consider pairs d_1, d_2 of discriminants satisfying the above hypothesis with $d_1/d_2 > 0$.

Remark 3.2. Let $E/\mathbb{Q}$ be an elliptic curve satisfying hypotheses 2.1, and let d_1, d_2 be fundamental discriminants satisfying that all primes $p \mid d_i$, $i = 1, 2$ are inert in $A_{\mathbb{Q}}$. Suppose also that either (a) $\Delta(E) < 0$, (b) $\mathrm{Cl}_+(A_{\mathbb{Q}}) = \mathrm{Cl}(A_{\mathbb{Q}})$, or (c) $d_1/d_2 > 0$. Then we have the following diagram

$$\begin{array}{ccccc} C_*(E_{d_1}) & \subset & \mathrm{S}el_2(E_{d_1}) & \subset & \tilde{C}(E_{d_1}) \\ \| & & & & \| \\ C_*(E_{d_2}) & \subset & \mathrm{S}el_2(E_{d_2}) & \subset & \tilde{C}(E_{d_2}) \end{array}$$

As the index $[\tilde{C}(E_{d_1}) : C_*(E_{d_1})] = 2$, then $\mathrm{S}el_2(E_{d_1}) = \mathrm{S}el_2(E_{d_2})$ if and only if both curves have the same root number. In particular we have infinitely many twists of E with the same 2-Selmer group.

We can explicitly determine for which discriminants both Selmer groups coincide, and say something on their densities if we restrict to prime discriminants. Let p be an odd prime number, and let $p^* = \left(\frac{-1}{p}\right) p$; recall that the quadratic extension of $\mathbb{Q}$ unramified outside p corresponds to $\mathbb{Q}(\sqrt{p^*})$. Let $\epsilon(E)$ denote the root number of E. Recall that if $p \nmid 2\Delta(E)$, then

$$\epsilon(E)\epsilon(E_{p^*}) = \chi_p(-N_E),$$

where N_E is the conductor of E and χ_p is the quadratic character unramified outside p.

Theorem 3.3. *Let $E/\mathbb{Q}$ be an elliptic curve satisfying hypotheses 2.1, and suppose furthermore that either $\Delta(E) < 0$ or $\mathrm{Cl}_+(A_{\mathbb{Q}}) = \mathrm{Cl}(A_{\mathbb{Q}})$. Then the set of prime numbers p inert in $A_{\mathbb{Q}}$ has density at least $1/3$ and for any such prime p which does not divide $\Delta(E)$ it holds:*

- *if $-\frac{\Delta(E)}{N_E} \equiv \square \pmod p$ then E and E_{p^*} have the same root number. In particular, both curves have the same 2-Selmer group,*

- *otherwise, E and E_{p^*} have opposite root number, and all curves E_{p^*} in this second case have the same 2-Selmer group.*

In particular, the set of all quadratic twists of E by prime discriminants has a subset of density at least $1/6$ where all curves in this set have the same 2-Selmer group.

Proof. The density of prime discriminants that are inert in $A_{\mathbb{Q}}/\mathbb{Q}$ equals

$$\text{density} = \begin{cases} \frac{2}{3} & \text{if } A_{\mathbb{Q}}/\mathbb{Q} \text{ is Galois,} \\ \frac{1}{3} & \text{otherwise.} \end{cases}$$

Recall that for an elliptic curve of the form $E : y^2 = F(x)$, $\Delta(E) = 2^4\Delta(F(x))$, hence $\Delta(A_{\mathbb{Q}})$ differ from $\Delta(E)$ by a square. In particular, since p is inert in $A_{\mathbb{Q}}$, $\chi_p(\Delta(A_{\mathbb{Q}})) = 1$, and

$$\epsilon(E)\epsilon(E_{p^*}) = \chi_p(-N_E) = \chi_p\left(-\frac{\Delta(E)}{N_E}\right).$$

This proves the claim on the root numbers. The result on the 2-Selmer group follows from Remark 3.2, noting that when $\Delta(E) < 0$ there are no real places of type (ii) so in the bounds of Theorem 2.16 are independent of E; and this is always the case when $\mathrm{Cl}_+(A_{\mathbb{Q}}) = \mathrm{Cl}(A_{\mathbb{Q}})$. $\square$

Recall the definitions given in the introduction: let $d_2(E)$ denote the 2-Selmer rank of E and define

$$N_r(E, X) = |\{\text{quadratic } L/\mathbb{Q} \ : \ d_2(E^L) = r \text{ and } |\delta(L/\mathbb{Q})| < X\}|,$$

where E^L denotes the quadratic twist of E corresponding to L and $\delta(L/\mathbb{Q})$ is the discriminant of the extension $L/\mathbb{Q}$.

Corollary 3.4. *Let $E/\mathbb{Q}$ be an elliptic curve satisfying hypotheses 2.1, and suppose furthermore that either $\Delta(E) < 0$ or $\mathrm{Cl}_+(A_{\mathbb{Q}}) = \mathrm{Cl}(A_{\mathbb{Q}})$. Let $r \geq 0$, and suppose that E has a quadratic twist by a prime inert in $A_{\mathbb{Q}}$ whose 2-Selmer group has rank r. Then $N_r(E, X) \gg X/\log(X)^{1-\alpha}$, where*

$$\alpha = \begin{cases} 1/3 & \textit{if } A_{\mathbb{Q}}/\mathbb{Q} \textit{ is Galois,} \\ 1/6 & \textit{otherwise.} \end{cases}$$

Proof. The proof is a standard application of Ikehara's tauberian theorem, as explained in [KL19], proof of Theorem 1.12. $\square$

Remark 3.5. If $-\frac{\Delta(E)}{N_E}$ is a square then all inert primes lie in the first case of Theorem 3.3 (and the proportion of twists with the same 2-Selmer group raises to $1/3$, and in the previous Corollary the constant α is doubled). This is the case for example if the elliptic curve E is semistable of odd conductor and $\Delta(E) < 0$. In such case Ogg's formula ([Sai88]) implies that for each prime of (multiplicative) bad reduction the difference between the conductor and the discriminant valuations at an odd prime p equals the number of irreducible components of the Néron model minus one; we claim that hypotheses 2.1 together with E being semistable implies that such number is always odd, hence the result. Note that the 2-division polynomial of a semistable curve always has a root on the base field, hence (†.i) cannot hold. The case (†.ii) implies that the discriminant of the polynomial has valuation 0 or 1 (recall that p is odd), hence there is a unique component. Finally, the condition (†.iii) implies that the number of components is odd.

A similar result holds for other elliptic curves where all primes of bad reduction satisfy that $[E(K) : E_0(K)]$ is odd (i.e. condition (†.iii) even for $p = 2$), since for odd primes the hypothesis implies that the number of irreducible components in the Néron model of E is odd and for $p = 2$ the result follows from the proof of [KL19, Lemma 5.9], end of part (3).

Let $\mathcal{C}_1$ be the set of prime numbers which ramify completely or are totally inert in $A_{\mathbb{Q}}$, and let $K = \mathbb{Q}\left(\sqrt{p^*} \,:\, p \in \mathcal{C}_1\right)$, an infinite polyquadratic extension.

Corollary 3.6. *In the hypotheses of Theorem 3.3, suppose that E has trivial 2-Selmer group. Then $E(K)$ is finite.*

Proof. If $P \in E(K)$ is a point of infinite order, then P belongs to a finite polyquadratic subextension $L/\mathbb{Q}$. Let $A = \operatorname{Res}_{\mathbb{Q}}^{L} E$ be the restriction of scalars, so $E(L) = A(\mathbb{Q})$. There is an isogeny

$$\phi : A \to \sum_{\chi} E_{\chi},$$

where χ runs over quadratic characters of $\operatorname{Gal}(L/\mathbb{Q})$. By Theorems 2.16 and 3.3 all curves E_χ have trivial 2-Selmer group, hence P cannot have infinite order. We deduce the corollary by noting that $E(K)_{\text{tors}}$ is finite by [Rib81]. □

Example 5. The elliptic curve E_{11a1} with LMFDB label 11.a1 has no rational 2-torsion points and is semistable. Its cubic field corresponds to the polynomial $x^3 - x^2 + x + 1$ of discriminant -44. The prime 11 is not totally ramified in $A_{\mathbb{Q}}$, hence it does not belong to $\mathcal{C}_1$. The prime 2 is totally ramified so $2 \in \mathcal{C}_1$. The set $\mathcal{C}_1 \subset \{p \,:\, \left(\frac{-44}{p}\right) = 1\} \cup \{2\}$, and over the polyquadratic extension $K = \mathbb{Q}(\sqrt{p} \,:\, p \in \mathcal{C}_1)$, the group $E(K)$ is finite.

For positive discriminants we get a similar result (with a similar corollary); see also Example 7. Let $E/\mathbb{Q}$ be an elliptic curve with $\Delta(E) > 0$, and divide the set of primes inert in $A_{\mathbb{Q}}$ into the following four different sets:

- $\mathcal{C}_{+,\square} = \{p \equiv 1 \pmod 4 \text{ such that } \frac{\Delta(E)}{N_E} \equiv \square \pmod p\}$,
- $\mathcal{C}_{+,\not\square} = \{p \equiv 1 \pmod 4 \text{ such that } \frac{\Delta(E)}{N_E} \equiv \not\square \pmod p\}$,
- $\mathcal{C}_{-,\square} = \{p \equiv 3 \pmod 4 \text{ such that } \frac{\Delta(E)}{N_E} \equiv \square \pmod p\}$,
- $\mathcal{C}_{-,\not\square} = \{p \equiv 3 \pmod 4 \text{ such that } \frac{\Delta(E)}{N_E} \equiv \not\square \pmod p\}$.

The set $\mathcal{C}_{+,\square}$ is non-empty and has density at least 1/12.

Theorem 3.7. *Let $E/\mathbb{Q}$ be an elliptic curve satisfying hypotheses 2.1, and suppose furthermore that $\Delta(E) > 0$. Then if p is a prime inert in $A_{\mathbb{Q}}$ which does not divide $\Delta(E)$, the root number of E_{p^*} equals that of E if $p \in \mathcal{C}_{+,\square} \cup \mathcal{C}_{-,\square}$, while it is the opposite one if $p \in \mathcal{C}_{+,\not\square} \cup \mathcal{C}_{-,\not\square}$. Furthermore, if p_1, p_2 are inert primes in the same set, $\mathrm{Cl}_*(A_{\mathbb{Q}}, E_{p_1^*}) = \mathrm{Cl}_*(A_{\mathbb{Q}}, E_{p_2^*})$. In particular, if p_1 and p_2 belong to the same set, the curve $E_{p_1^*}$ and the curve $E_{p_2^*}$ have the same 2-Selmer group.*

Proof. Note that primes in $\mathcal{C}_{+,\square} \cup \mathcal{C}_{+,\not\square}$ (i.e. $p \equiv 1 \pmod 4$) correspond to twists by real quadratic fields and primes in $\mathcal{C}_{-,\square} \cup \mathcal{C}_{-,\not\square}$ correspond to twists by imaginary quadratic fields.

The proof mimics the negative discriminant case. To get the root number statement, note that $\chi_p(-N_E) = \chi_p(-1)\chi_p(\Delta(E))$. Then if $p \equiv 1 \pmod 4$, the same proof applies, while if $p \equiv 3 \pmod 4$, $\chi_p(-N_E) = -\chi_p(\Delta(E))$, which explains the change of root number.

Regarding the 2-Selmer statement, if p_1 and p_2 belong to the same set, the curves $E_{p_1^*}$ and $E_{p_2^*}$ are a positive quadratic twist of each other, hence $\mathrm{Cl}_*(A_{\mathbb{Q}}, E_{p_1^*}) = \mathrm{Cl}_*(A_{\mathbb{Q}}, E_{p_2^*})$ so the bound of Theorem 2.16 and Remark 3.2 prove the statement. □

An immediate application of the previous result is that when $\Delta(E) > 0$ among the set of all quadratic twists of E there is a subset with density at least 1/12 satisfying that all curves on it have the same 2-Selmer group as E (corresponding to the primes in $\mathcal{C}_{+,\square}$). A result similar to Corollary 3.6 applies in this situation.

3.1. General fields.

The results of the previous section have a natural analogue over a general number field K. Still there are many subtleties, for example: it is not always true that given a prime ideal $\mathfrak{p}$ of K there is a quadratic extension of K which is unramified outside $\mathfrak{p}$ (and there might be more than one such extension). The way to solve it is to consider quadratic extensions $K(\sqrt{\alpha})/K$ of prime discriminant (instead of prime ideals), and twist curves by them. Although most of the results for $\mathbb{Q}$ extend mutatis mutandis for K, we give a weaker not technical version.

Theorem 3.8. *Let K be a number field and let E/K be an elliptic curve satisfying hypotheses 2.1. Then among the quadratic twists of E by quadratic extensions of prime discriminant, a positive proportion have 2-Selmer group whose rank lies in the interval* $[\mathrm{Cl}_*(A_K, E)[2], \mathrm{Cl}_*(A_K, E)[2] + [K : \mathbb{Q}]]$.

Proof. Considering only quadratic extensions $K(\sqrt{\alpha})$ of prime discriminant which are unramified at the archimedean places of K of type (ii), we can assure that the groups $\mathrm{Cl}_*(A_K, E)$ and $\mathrm{Cl}_*(A_K, E_\alpha)$ are equal, hence the result follows from Theorem 2.16 and Remark 3.2. □

Remark 3.9. A similar application of the previous Theorem gives a result in the spirit of Corollary 3.4 for general number fields. However, even if we fix the root number, we cannot state precisely which rank in the above interval is obtained infinitely many times (except for example when $[K : \mathbb{Q}] = 2$), hence our result is not as strong as that of [MR10] (Theorem 1.4).

4. Examples

The following examples have been computed using SageMath [Sag19] and PARI/GP [PAR19]. The 2-Selmer rank, when necessary, is computed using Magma [BCP97].

4.1. Examples with $K = \mathbb{Q}$.

Example 6. Let $F(x) = x^3 - x^2 - 54x + 169$ (corresponding to the elliptic curve 106276.a1). Its rank equals 3. The discriminant of $F(x)$ equals 163^2, which also equals the discriminant of $A_{\mathbb{Q}}$, hence (†.ii) is satisfied for all primes. Furthermore, since the discriminant is a square, $A_{\mathbb{Q}}$ is a Galois extension of $\mathbb{Q}$. The class group $\mathrm{Cl}(A_{\mathbb{Q}}) = \mathrm{Cl}_+(A_{\mathbb{Q}}) \simeq \mathbb{Z}/2 \times \mathbb{Z}/2$. In particular, $\mathrm{Cl}_*(A_{\mathbb{Q}}, E_d) = \mathrm{Cl}(A_{\mathbb{Q}})$ has 2-rank 2, hence Theorems 2.16, 3.3 and 3.7 imply that the curve and all quadratic twists by primes which are inert in $A_{\mathbb{Q}}$ have 2-Selmer rank in $\{2, 3\}$.

In fact the sign of the functional equations gives the parity of the 2-Selmer rank (see [Mon96, Theorem 1.5]), hence the 2-Selmer rank of E_p is 3 for inert primes $p \equiv 1 \pmod 4$ and 2 for inert primes $p \equiv 3 \pmod 4$. For instance, E itself has 2-Selmer rank 3, while its quadratic twist by $d = -3$ has 2-Selmer rank 2. In particular, both bounds are attained.

If we consider twists by split primes (not satisfying hypotheses 2.1) we check that the twists by $d = -23$, 5, -347, 241, -331, 2341 have 2-Selmer rank 0, 1, 2, 3, 4, 5 (respectively), so neither the lower or upper bounds hold.

Example 7. Let $F(x) = x^3 - 7x + 3$ (corresponding to the elliptic curve 9032.a1, see Example 4). Its rank equals 2. The discriminant of $F(x)$ equals 1129, which also equals the discriminant of $A_{\mathbb{Q}}$, hence (†.ii) is satisfied for all primes. The class group $\mathrm{Cl}(A_{\mathbb{Q}})$ is trivial but the narrow class group $\mathrm{Cl}_+(A_{\mathbb{Q}})$ has order 2. The ray class group $\mathrm{Cl}_*(A_{\mathbb{Q}}, E)$ also has order 2. In particular, when taking quadratic twists by discriminants $d > 0$ it turns out that $\mathrm{Cl}_*(A_{\mathbb{Q}}, E_d) = \mathrm{Cl}_*(A_{\mathbb{Q}}, E)$ has 2-rank 1, hence Theorem 2.16 implies that the curve and all quadratic twists by positive prime discriminants which are inert in $A_{\mathbb{Q}}$ have 2-Selmer rank in $\{1, 2\}$, determined by the sign of the functional equation. For instance, the quadratic twists by $d = 5$ and $d = 113$ have 2-Selmer rank 1 and 2, respectively.

If we take quadratic twists by discriminants $d < 0$, the distinguished real place changes, and $\mathrm{Cl}_*(A_{\mathbb{Q}}, E_d)$ is trivial, hence all quadratic twists by negative prime discriminants which are inert in $A_{\mathbb{Q}}$ have 2-Selmer group rank in $\{0, 1\}$, determined by the sign of the functional equation. For instance, the quadratic twists by $d = -43$ and $d = -7$ have 2-Selmer rank 0 and 1, respectively.

4.2. Examples with $K = \mathbb{Q}(\sqrt{17})$.

The quadratic field K has trivial narrow class group (hence it equals the class group).

Example 8. Let $F(x) = x^3 + x + 3$ (corresponding, over $\mathbb{Q}$, to the elliptic curve 1976.a1). Its rank equals 2. The discriminant of $F(x)$ equals $-13 \cdot 19$, which also equals the discriminant of A_K, hence (†.ii) is satisfied for all primes. The narrow class group of A_K is trivial, hence $\mathrm{Cl}_*(A_K, E_d)$ is trivial. Theorem 2.16 thus implies that the curve and all quadratic twists by primes which are inert in A_K have 2-Selmer rank in $\{0, 1, 2\}$.

The curve itself, and also the quadratic twist by $d = 97 + 24\sqrt{17}$ of norm 383, have 2-Selmer rank 2, the quadratic twist by $d = -13 + 2\sqrt{17}$ of norm 101 has 2-Selmer rank 1, and the quadratic twist by $d = 45 + 8\sqrt{17}$ of norm 937 has 2-Selmer rank 0. On the other hand the quadratic twist by $d = 29 + 4\sqrt{17}$, which is *not* inert in A_K, has 2-Selmer rank 3.

4.3. **Examples with $K = \mathbf{3.1.23.1}$.** The field K corresponds to the cubic field of discriminant -23 given by $K = \mathbb{Q}(\alpha)$ with $\alpha^3 - \alpha^2 + 1$ and trivial narrow class group. Since $[K : \mathbb{Q}] = 3$, our lower and upper bound in Theorem 2.16 differ by 3 so the functional equation sign is not enough to determine the rank of the 2-Selmer group in any case.

Example 9. Let $F(x) = x^3 + x + 3$ (corresponding, over $\mathbb{Q}$, to the elliptic curve 1976.a1). The discriminant of $F(x)$ equals $-13 \cdot 19$, which also equals the discriminant of A_K, hence (†.ii) is satisfied for all primes. Its rank equals 1.

The narrow class group of A_K is trivial, hence $\mathrm{Cl}_*(A_K, E)$ is trivial. Our bound implies that the curve and all quadratic twists by primes which are inert in A_K have 2-Selmer rank in $\{0, 1, 2, 3\}$.

The curve itself and the quadratic twist by $-2\alpha^2 + \alpha - 2$ have 2-Selmer rank 1, and the quadratic twist by $-4\alpha^2 + 3\alpha + 1$ has 2-Selmer rank 0. In particular the lower bound is attained.

On the other hand, we note that all the quadratic twists by inert prime discriminants of norm up to 100 000 (there are 808 such discriminants) have 2-Selmer rank 0 or 1. This is not explained by our results.

Example 10. Let $F(x) = x^3 + x + 11$ (corresponding, over $\mathbb{Q}$, to the elliptic curve 26168.a1). The discriminant of $F(x)$ equals -3271, which also equals the discriminant of A_K, hence (†.ii) is satisfied for all primes. Its rank equals 4.

The class group $\mathrm{Cl}(A_K) = \mathrm{Cl}_+(A_K) \simeq \mathbb{Z}/2$. In particular $\mathrm{Cl}_*(A_K, E) = \mathrm{Cl}(A_K)$ has 2-rank 1. Thus our bound implies that the curve and all quadratic twists by primes which are inert in A_K have 2-Selmer rank in $\{1, 2, 3, 4\}$.

The curve itself and the quadratic twist by $-2\alpha^2 + \alpha - 2$ have 2-Selmer rank 4, and the quadratic twist by $-\alpha^2 - \alpha + 4$ has 2-Selmer rank 3. In particular the upper bound is attained.

On the other hand, we note that all the quadratic twists by inert prime discriminants of norm up to 100 000 (there are 844 such discriminants) have 2-Selmer rank 3 or 4. This is not explained by our results.

References

[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).

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

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

[CF69] John Cassels and Albrecht Frohlich. *Algebraic Number Theory.* Academis Press, 1969.

[CP19] John Cremona and Ariel Pacetti. On elliptic curves of prime power conductor over imaginary quadratic fields with class number 1. *Proc. Lond. Math. Soc. (3)*, 118(5):1245–1276, 2019.

[GP12] Benedict H. Gross and James A. Parson. On the local divisibility of Heegner points. In *Number theory, analysis and geometry*, pages 215–241. Springer, New York, 2012.

[KL19] Daniel Kriz and Chao Li. Goldfeld's conjecture and congruences between Heegner points. *Forum Math. Sigma*, 7:e15, 80, 2019.

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

[Mon96] P. Monsky. Generalizing the Birch-Stephens theorem. I. Modular curves. *Math. Z.*, 221(3):415–420, 1996.

[MR10] B. Mazur and K. Rubin. Ranks of twists of elliptic curves and Hilbert's tenth problem. *Invent. Math.*, 181(3):541–575, 2010.

[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/`.

[Rib81] Kenneth Ribet. Torsion points of abelian varieties in cyclotomic extensions. *Enseign. Math*, 27:315–319, 1981.

[Sag19] The Sage Developers. *SageMath, the Sage Mathematics Software System (Version 8.8)*, 2019. available from `https://www.sagemath.org`.

[Sai88] Takeshi Saito. Conductor, discriminant, and the Noether formula of arithmetic surfaces. *Duke Math. J.*, 57(1):151–173, 1988.

[Sil09] Joseph H. Silverman. *The arithmetic of elliptic curves*, volume 106 of *Graduate Texts in Mathematics*. Springer, Dordrecht, second edition, 2009.

[Tat75] J. Tate. Algorithm for determining the type of a singular fiber in an elliptic pencil. In *Modular functions of one variable, IV (Proc. Internat. Summer School, Univ. Antwerp, Antwerp, 1972)*, pages 33–52. Lecture Notes in Math., Vol. 476, 1975.

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

FaMAF-CIEM (CONICET), Universidad Nacional de Córdoba, Medina Allende s/n, Ciudad Universitaria, 5000 Córdoba, República Argentina.
Email address: `apacetti@famaf.unc.edu.ar`

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