

*Pacific  
Journal of  
Mathematics*

**RANK GROWTH OF ELLIPTIC CURVES IN  
 $S_4$ - AND  $A_4$ -QUARTIC EXTENSIONS OF THE RATIONALS**

DANIEL KELIHER

# RANK GROWTH OF ELLIPTIC CURVES IN $S_4$ - AND $A_4$ -QUARTIC EXTENSIONS OF THE RATIONALS

DANIEL KELIHER

We investigate the rank growth of elliptic curves from  $\mathbb{Q}$  to  $S_4$ - and  $A_4$ -quartic extensions  $K/\mathbb{Q}$ . In particular, we are interested in the quantity  $\text{rk}(E/K) - \text{rk}(E/\mathbb{Q})$  for fixed  $E$  and varying  $K$ . When  $\text{rk}(E/\mathbb{Q}) \leq 1$ , with  $E$  subject to some other conditions, we prove there are infinitely many  $S_4$ -quartic extensions  $K/\mathbb{Q}$  over which  $E$  does not gain rank, i.e., such that  $\text{rk}(E/K) - \text{rk}(E/\mathbb{Q}) = 0$ . To do so, we show how to control the 2-Selmer rank of  $E$  in certain quadratic extensions, which in turn contributes to controlling the rank in families of  $S_4$ - and  $A_4$ -quartic extensions of  $\mathbb{Q}$ .

## 1. Introduction

**1A. Rank growth.** For a number field  $L$  and an elliptic curve  $E$  defined over  $L$ , let  $E(L)$  be the group of  $L$ -rational points of  $E$ . The Mordell–Weil theorem says  $E(L)$  is a finitely generated abelian group. The rank of  $E(L)$ , denoted  $\text{rk}(E/L)$ , has been the subject of much study. Of particular interest here is the behavior of the rank upon base change, i.e., for an extension of number fields  $K/L$ , what is  $\text{rk}(E/K) - \text{rk}(E/L)$ ? We call this difference the *rank growth* of  $E$  in  $K/L$ .

Suppose  $L = \mathbb{Q}$  and  $K/\mathbb{Q}$  denotes a quadratic extension. Given an elliptic curve  $E/\mathbb{Q}$ , a conjecture of Goldfeld predicts that 50% of quadratic twists,  $E^K$ , of  $E$  have analytic rank zero and 50% have analytic rank one. See [Section 3B](#) for a definition and discussion of quadratic twists. Recent work of Smith [[2017](#); [2023a](#); [2023b](#)] studies the distribution of  $\ell^\infty$ -Selmer groups and proves a version of Goldfeld’s conjecture for  $2^\infty$ -Selmer coranks.

We are interested in studying rank growth in higher degree and nonabelian extensions. In this setting, ranks of quadratic twists,  $E^K$ , measure the rank growth of  $E$  from  $\mathbb{Q}$  to  $K$ , which will be essential for rank growth in some larger degree extensions. Previously, and in higher degrees, David, Fearnley, and Kisilevsky [[David et al. 2007](#)] have given conjectures for how frequently the rank of an elliptic curve grows in cyclic prime degree extensions. Lemke Oliver and Thorne [[2021](#)] gave asymptotic lower bounds for the number of  $S_d$ -extensions for which an elliptic

MSC2020: 11G05.

Keywords: rank growth, elliptic curve, Selmer group, arithmetic statistics.

curve  $E$  gains rank. Further, Shnidman and Weiss [2023] study rank growth of elliptic curves from a number field  $L$  up to an extension  $L(\sqrt[2n]{d})$ .

**1B. Results for  $S_4$ - and  $A_4$ -quartic extensions.** We investigate the rank growth of elliptic curves in  $S_4$ - and  $A_4$ -quartic extensions of the rationals. In what follows, unless stated otherwise, we will always assume  $E$  is an elliptic curve defined over  $\mathbb{Q}$ . Further,  $K/\mathbb{Q}$  will always be an  $S_4$ - or  $A_4$ -quartic extension. That is, one for which the normal closure of  $K$  over  $\mathbb{Q}$  is an  $S_4$ - or  $A_4$ -Galois extension. For an elliptic curve  $E/\mathbb{Q}$  with discriminant  $\Delta_E$ , we'll consider  $\text{rk}(E/K) - \text{rk}(E/\mathbb{Q})$  for many such  $K$ . It will often be convenient to use the rank of a Selmer group of an elliptic curve  $E/K$  (here we only need the 2-Selmer group) in place of the rank,  $\text{rk}(E/K)$ . See Definition 3.1 for the definition of the 2-Selmer group,  $\text{Sel}_2(E/K)$ , of an elliptic curve  $E/K$  and Section 3A for a discussion of their utility in our context.

In particular, for an elliptic curve  $E$  with Selmer rank zero over the rationals, subject to some mild constraints, we prove there are infinitely many  $S_4$ - or  $A_4$ -quartic extensions over which  $E$  does not gain rank. Further, we give a lower bound on the number of such extensions with bounded discriminant with some fixed cubic resolvent field.

**Theorem 1.1.** *Let  $E$  be an elliptic curve over  $\mathbb{Q}$  such that  $\text{Gal}(\mathbb{Q}(E[2])/\mathbb{Q}) \simeq S_3$ , and  $\text{Sel}_2(E/\mathbb{Q}) = 0$ . Let  $K_3$  be an  $S_3$ -cubic (resp.,  $C_3$ -cubic) extension of  $\mathbb{Q}$  such that  $\tilde{K}_3$  and  $\mathbb{Q}(E[2])$  are linearly disjoint. Suppose also that there is a place  $v_0$  of  $K_3$ , unramified in  $\tilde{K}_3$ , such that either  $v_0$  is real and  $\Delta_E < 0$ , or  $v_0 \nmid 2\infty$ ,  $E$  has multiplicative reduction at  $v_0$  and  $\text{ord}_{v_0}(\Delta_E)$  is odd. Then there are infinitely many  $S_4$ -quartic (resp.,  $A_4$ -quartic) extensions  $K$  over  $\mathbb{Q}$  with cubic resolvent  $K_3$  such that*

- if  $\dim_{\mathbb{F}_2} \text{Sel}_2(E/K_3) \equiv 0 \pmod{2}$ , then  $\text{rk}(E/K) = 0$ ;
- if  $\dim_{\mathbb{F}_2} \text{Sel}_2(E/K_3) \equiv 1 \pmod{2}$ , and also assuming the parity condition  $\dim_{\mathbb{F}_2} \text{Sel}_2(E/K_3) \equiv \text{rk}(E/K_3) \pmod{2}$ , then  $\text{rk}(E/K) = 1$ .

To prove the theorem above, we utilize two tools. First, we reduce the problem of studying rank growth in our quartic extensions,  $K/\mathbb{Q}$ , to one of studying rank growth in certain quadratic subextensions of the Galois closure of  $K$ , and thus to studying the rank of certain quadratic twists. Second, we use and further develop some Selmer group machinery of Mazur and Rubin. Indeed, in [Mazur and Rubin 2010], they show that under suitable assumptions, an elliptic curve has infinitely many twists of a prescribed Selmer rank. In subsequent work, Klagsbrun, Mazur, and Rubin [Klagsbrun et al. 2014] study the distribution of 2-Selmer ranks of quadratic twists of an elliptic curve. The quadratic twists we study here, see Definition 1.2 below, are thin in the full family of quadratic twists, so we require a different approach. Nonetheless, we use similar ideas to show one can reduce the 2-Selmer

ranks of the appropriate quadratic twists either to one or zero. Translating from the language of Selmer groups to ranks yields [Theorem 1.1](#).

To emphasize the extra properties imposed on the quadratic twists we consider here, we make the following definition.

**Definition 1.2** (square norm twists). Let  $E$  be an elliptic curve defined over a number field  $L$ , and let  $F/L$  be a quadratic extension. We call a quadratic twist  $E^F$  over  $L$  a *square norm twist* if  $F = L(\sqrt{\alpha})$  where  $\alpha \in L^\times / (L^\times)^2$  and  $N_{L/\mathbb{Q}}(\alpha)$  is a square.

Such twists will be key to keeping track of an associated  $S_4$ -quartic extension when working over a suitable cubic field (see [Lemma 2.2](#)).

Likewise, to streamline the discussion and highlight the properties required of the cubic resolvents of our  $S_4$ - or  $A_4$ -quartic extensions, which are  $S_3$ - or  $C_3$ -cubic extensions of the rationals, respectively, always denoted  $K_3$ , we make the next definition.

**Definition 1.3** (admissible cubic resolvent). Let  $K_3$  be a cubic extension of the rationals and fix an elliptic curve  $E/\mathbb{Q}$  with discriminant  $\Delta_E$ . Suppose  $E(K_3)[2] = 0$ ,  $\tilde{K}_3$  (the Galois closure of  $K_3$  over  $\mathbb{Q}$ ) and  $\mathbb{Q}(E[2])$  are linearly disjoint, and there is a place  $v_0$  of  $K_3$ , unramified in  $\tilde{K}_3$ , such that either  $v_0$  is real and  $(\Delta_E)_{v_0} < 0$  or  $v_0 \nmid 2\infty$ ,  $E$  has multiplicative reduction at  $v_0$  and  $\text{ord}_{v_0}(\Delta_E)$  is odd. For such an extension,

- if  $K_3$  is an  $S_3$ -cubic extensions, we call  $K_3$  an *admissible  $S_3$ -cubic resolvent* for  $E$ ;
- if  $K_3$  is a  $C_3$ -cubic extension, we call  $K_3$  an *admissible  $C_3$ -cubic resolvent* for  $E$ .

In the event we do not need to specify one of the two Galois group cases above, we will call a  $K_3$  as in one of the two cases above an *admissible cubic resolvent* for some  $E$ .

The restrictions placed on  $K_3$  to make it admissible for some elliptic curve are not overly burdensome. The conditions on the distinguished place should be compared to the assumptions of [[Mazur and Rubin 2010](#), Theorem 1.6].

[Theorem 1.1](#) is a consequence of the following result.

**Theorem 1.4.** *Let  $E$  be an elliptic curve over  $\mathbb{Q}$  such that  $\text{Gal}(\mathbb{Q}(E[2])/\mathbb{Q}) \simeq S_3$ , and  $\text{Sel}_2(E/\mathbb{Q}) = 0$ , and let  $K_3$  be an admissible cubic resolvent for  $E$ . Then there are infinitely many square norm twists,  $E^F/K_3$ , such that*

- if  $\dim_{\mathbb{F}_2} \text{Sel}_2(E/K_3) \equiv 0 \pmod{2}$ , then  $\dim_{\mathbb{F}_2} \text{Sel}_2(E^F/K_3) = 0$ ;
- if  $\dim_{\mathbb{F}_2} \text{Sel}_2(E/K_3) \equiv 1 \pmod{2}$ , then  $\dim_{\mathbb{F}_2} \text{Sel}_2(E^F/K_3) = 1$ .

**Remark 1.5.** In [Theorems 1.1](#) and [1.4](#), and in what follows, when we say “infinitely many” we mean the number of such things with the norm of their discriminant

bounded above by  $X$  is  $\gg X^{1/2}/\log X^\alpha$  for some  $\alpha > 0$ . Further,  $\alpha$  depends on  $E$  and the two-torsion field  $K_3(E[2])$ . The sizes of these lower bounds, particularly the values of  $\alpha$  depending on  $K_3$  and  $E$ , are elucidated in [Proposition 4.1](#).

**Remark 1.6.** In the case that one obtains infinitely many  $A_4$ -quartic extensions for which the Mordell or 2-Selmer rank has some prescribed behavior, the “infinitely many” given by the two theorems above differs from the predicted number of  $A_4$ -quartic extensions only by some factors of  $\log X$ . In particular, Malle’s conjecture [\[2004\]](#) predicts that the number of  $A_4$ -quartic extensions of a number field  $L$  with absolute value of the norm of the relative discriminant bounded by  $X$  is asymptotic to  $c_L X^{1/2} \log X^{b_L}$  for constants  $b_L$  and  $c_L$  depending on  $L$ .

The number of  $S_4$ -quartic extensions of  $L$  with absolute value of the norm of the relative discriminant bounded by  $X$  is asymptotic to  $d_L X$  for a constant  $d_L$  depending on  $L$  [\[Bhargava et al. 2015\]](#). In this case the “infinitely many” given by the two theorems above differs from  $S_4$ -quartic asymptotic by both a logarithmic factor and a factor of  $X^{1/2}$ .

**1C. Layout.** In [Section 2](#) we outline the connection between rank growth in  $S_4$  and  $A_4$ -quartic extensions with rank growth in certain quadratic extensions. In [Section 3](#), we recall some facts about Selmer groups and record some related results of Mazur and Rubin [\[Mazur and Rubin 2010\]](#) on quadratic twists. In [Sections 4](#) and [5](#), we interface the tools of [Section 3](#) with the notion of square norm twists to show we can decrease the 2-Selmer rank of an elliptic curve with a suitable square norm twist and can indeed find many such twists. Finally, in [Section 6](#), we prove the main theorems stated above.

## 2. Rank growth in $S_4$ -quartics

**2A. Preliminaries.** For an extension of number fields  $L/\mathbb{Q}$ , we write  $\tilde{L}$  for the Galois closure of  $L$  in some choice of algebraic closure  $\tilde{\mathbb{Q}}$ .

Consider an  $S_4$ - or  $A_4$ -extension  $K/\mathbb{Q}$  with Galois closure  $\tilde{K}$ . We are principally concerned with the change (or lack of change) in rank in the group of  $K$ -rational points vs. the group of  $\mathbb{Q}$ -rational points of  $E$ . We will show this rank change is governed by the rank growth in a quadratic extension of fields between  $\mathbb{Q}$  and  $\tilde{K}$ .  $K_3$  will always denote a cubic resolvent for our quartic extension(s). Of particular interest will be fixing an admissible cubic resolvent  $K_3$  and considering many quartic  $S_4$ - or  $A_4$ -extensions  $K$  with cubic resolvent  $K_3$ .

**2B.  $S_4$ - and  $A_4$ -quartic extensions.** Before we turn to the question of rank growth, we record a few facts about  $S_4$ - and  $A_4$ -quartic extensions with cubic resolvent field  $K_3$ .

**Lemma 2.1.** *Let  $K_3/\mathbb{Q}$  be a cubic extension and  $F$  be a quadratic extension of  $K_3$ . There is always an embedding  $\text{Gal}(\tilde{F}/\mathbb{Q}) \hookrightarrow S_2 \wr S_3$ .*

Quadratic extensions of  $S_3$ -cubics generically have Galois group  $S_2 \wr S_3$  over  $\mathbb{Q}$ . We are interested in the case where the Galois group is instead  $S_4 < S_2 \wr S_3$ . Likewise for  $C_3$ -cubics, we wish to consider the case where quadratic extensions of  $K_3$  have Galois group  $A_4$ .

**Lemma 2.2.** *Fix an  $S_3$ - or  $C_3$ -cubic extension  $K_3/\mathbb{Q}$ , and let  $F$  denote a quadratic extension of the form  $K_3(\sqrt{\alpha})$ , where  $\alpha \in K_3$  and  $N_{K_3/\mathbb{Q}}(\alpha)$  is a square.*

- *If  $K_3/\mathbb{Q}$  is an  $S_3$ -cubic, then  $\text{Gal}(\tilde{F}/\mathbb{Q}) \simeq S_4$ . Further, there is a one-to-one correspondence between such quadratic extensions  $F/K_3$  and  $S_4$ -quartic extensions of  $\mathbb{Q}$  with cubic resolvent  $K_3$ .*
- *If  $K_3/\mathbb{Q}$  is a  $C_3$ -cubic, then  $\text{Gal}(\tilde{F}/\mathbb{Q}) \simeq A_4$ . Further, there is a three-to-one correspondence between such quadratic extensions  $F/K_3$  and  $A_4$ -quartic extensions of  $\mathbb{Q}$  with cubic resolvent  $K_3$ .*

This correspondence is described in detail in, for example, Section 2 of [Cohen and Thorne 2016].

**Remark 2.3.** Fix a cubic field,  $K_3$ . For each  $L = K_3(\sqrt{\alpha})$  where  $\alpha \in K_3^\times / (K_3^\times)^2$  and  $N_{K_3/\mathbb{Q}}(\alpha)$  is a square, there is an  $S_4$ - or  $A_4$ -quartic extension  $K/\mathbb{Q}$  with cubic resolvent  $K_3$ . Use Lemma 2.2 and observe that  $\tilde{L} = \tilde{K}$ . For our purposes, we will fix  $K_3$  and range over quadratic extensions of  $K_3$  as in Lemma 2.2 to range over  $S_4$ -quartic extensions of  $\mathbb{Q}$  with cubic resolvent  $K_3$ . We will then consider a fixed elliptic curve  $E$  over these extensions, and consider various differences in rank.

**2C. Measuring rank growth in  $S_4$ - and  $A_4$ -quartic extensions.** Our aim now is to show that measuring rank growth of an elliptic curve  $E$  from  $\mathbb{Q}$  to  $S_4$ - or  $A_4$ -quartic extensions  $K/\mathbb{Q}$  with cubic resolvent  $K_3/\mathbb{Q}$  is a matter of measuring the rank growth of  $E$  from  $K_3$  to a quadratic extension  $F/K_3$ , namely the quadratic extension of Lemma 2.2.

**Lemma 2.4.** *Let  $E$  be an elliptic curve defined over  $\mathbb{Q}$ ,  $K$  be an  $S_4$ - or  $A_4$ -quartic extension of  $\mathbb{Q}$  with cubic resolvent  $K_3$ , and  $F/K_3$  be the quadratic extension of Lemma 2.2. Then*

$$(2-1) \quad \text{rk}(E/K) - \text{rk}(E/\mathbb{Q}) = \text{rk}(E/F) - \text{rk}(E/K_3).$$

The rank relation of Lemma 2.4 is a manifestation of the following more general fact [Dokchitser and Dokchitser 2010, page 572]. Suppose  $L/k$  is a Galois extension of number fields with  $G = \text{Gal}(L/k)$ , and  $E/k$  is an elliptic curve. For  $H \leq G$ ,

write  $\mathbb{1}_H$  for the trivial character on  $H$ . If there are subextensions  $K_i/k$  and  $K'_j/k$  of  $L$ , cut out by subgroups  $H_i$  and  $H'_j$  of  $G$ , such that

$$(2-2) \quad \bigoplus_i \text{Ind}_{H_i}^G \mathbb{1}_{H_i} \simeq \bigoplus_j \text{Ind}_{H'_j}^G \mathbb{1}_{H'_j}$$

as complex representations of  $G$ , then

$$(2-3) \quad \sum_i \text{rk}(E/K_i) = \sum_j \text{rk}(E/K'_j).$$

The see this relation on the ranks, let  $\chi_L$  be the character of the representation of the complex representation of the Mordell–Weil group,  $E(L) \otimes \mathbb{C}$ , and note that

$$(2-4) \quad \text{rk}(E/K_i) = \langle \text{Ind}_{H_i}^G \mathbb{1}_{H_i}, \chi_L \rangle.$$

The same statement can be made for the rank of  $E$  over each  $K'_j$  as well. Using (2-4) together with (2-2) yields (2-3).

*Proof of Lemma 2.4.* Consider the following subgroups of  $G = \text{Gal}(\tilde{K}/\mathbb{Q}) \simeq S_4$  which fix the subfields  $K$ ,  $K_3$ , and  $F$  of  $\tilde{K}$ . Let  $H_K \simeq S_3$  be the subgroup fixing  $K$ ,  $H_{K_3} \simeq D_8$  be the subgroup fixing  $K_3$ , and  $H_F \simeq V_4$ , the Klein four group, be the subgroup fixing  $F$ . Then one can verify

$$(2-5) \quad \text{Ind}_{H_K}^G \mathbb{1}_{H_K} \oplus \text{Ind}_{H_{K_3}}^G \mathbb{1}_{H_{K_3}} \simeq \mathbb{1} \oplus \text{Ind}_{H_F}^G \mathbb{1}_{H_F}.$$

The lemma now follows from (2-3). Note that relations like that of (2-5) are an example of those provided in [Bartel and Dokchitser 2015]. □

### 3. The 2-Selmer groups and quadratic twists

In the previous section, we established that the rank growth from  $\mathbb{Q}$  to  $K$  is the same as the rank growth from  $K_3$  to a quadratic extension of  $K_3$  determined by  $K$ . So we may restrict ourselves to the study of rank growth in quadratic extensions. This is governed by the theory of quadratic twists.

**3A. The 2-Selmer group.** We now recall the definition of the 2-Selmer group for an elliptic curve  $E$  over a number field  $L$ . The multiplication-by-2 map on  $E$  gives rise to a short exact sequence of Galois modules:

$$0 \rightarrow E[2] \rightarrow E(\bar{\mathbb{Q}}) \xrightarrow{\times 2} E(\bar{\mathbb{Q}}) \rightarrow 0.$$

This in turn yields a long exact sequence of Galois cohomology groups, which, after quotienting appropriately, gives rise to the diagram

$$\begin{array}{ccccccc} 0 & \longrightarrow & E(L)/2E(L) & \longrightarrow & H^1(L, E[2]) & \longrightarrow & H^1(L, E)[2] \longrightarrow 0 \\ & & \downarrow & & \downarrow & & \downarrow \\ 0 & \longrightarrow & \prod_v E(L_v)/2E(L_v) & \longrightarrow & \prod_v H^1(L_v, E[2]) & \longrightarrow & \prod_v H^1(L_v, E)[2] \longrightarrow 0 \end{array}$$

Now, define subgroups  $H_f^1(L_v, E[2])$  of each local cohomology  $H^1(L_v, E[2])$  as

$$H_f^1(L_v, E[2]) := \text{Image}(E(L_v)/2E(K_v) \rightarrow H^1(L_v, E[2])).$$

**Definition 3.1.** The 2-Selmer group of  $E/L$ , denoted  $\text{Sel}_2(E/L)$ , is the  $\mathbb{F}_2$ -vector space defined by the exactness of the sequence

$$0 \rightarrow \text{Sel}_2(E/L) \rightarrow H^1(L, E[2]) \rightarrow \bigoplus_v H^1(L_v, E[2])/H_f^1(L_v, E[2]).$$

We may think of the elements of the 2-Selmer group as being the classes in  $H^1(L, E[2])$  which, for every place  $v$  of  $L$ , land in the image of  $E(L_v)/2E(L_v)$ ; that is, elements of  $H^1(L, E[2])$  which everywhere locally satisfy the local conditions determined by  $H_f^1(L_v, E[2])$ .

Further, the 2-Selmer group fits into a short exact sequence

$$0 \rightarrow E(L)/2E(L) \rightarrow \text{Sel}_2(E/L) \rightarrow \text{III}(E/L)[2] \rightarrow 0,$$

where  $\text{III}(E/L)[2]$  are the elements of the Shafarevich–Tate group of  $E/L$  with order dividing 2. We have

$$(3-1) \quad \dim_{\mathbb{F}_2} \text{Sel}_2(E/L) = (\text{rk}(E/L) + \dim_{\mathbb{F}_2} E(L)[2]) + \dim_{\mathbb{F}_2} \text{III}(E/L)[2]$$

and further that  $\text{rk}(E/L) \leq \dim_{\mathbb{F}_2} \text{Sel}_2(E/L)$ . It is by this relation that we'll access the ranks of the various elliptic curves and twists discussed later in the paper.

**3B. Quadratic twists.** Suppose our elliptic curve  $E/L$  is given in short Weierstrass form:

$$E : y^2 = x^3 + Ax + B$$

with  $A, B \in L$ . A quadratic twist,  $E^F/L$ , of  $E/L$  is an elliptic curve of the form

$$(3-2) \quad E^F : \delta y^2 = x^3 + Ax + B,$$

where  $\delta \in L^\times/(L^\times)^2$  and  $F = L(\sqrt{\delta})$ . With a change of variables, one can put (3-2) in short Weierstrass form:

$$E^F : y^3 = x^3 + a\delta^2x + b\delta^3.$$

An elliptic curve  $E/L$  and a quadratic twist  $E^F/L$  are not, in general, isomorphic as elliptic curves over  $L$  but *are* isomorphic as elliptic curves over  $F$ . In particular, quadratic twists will be the main tool for measuring growth in quadratic extensions as we have

$$\text{rk}(E^F/L) = \text{rk}(E/F) - \text{rk}(E/L).$$



**3C. The 2-Selmer of quadratic twists.** Mazur and Rubin [2010] gave results in which understanding the behavior of an elliptic curve  $E/L$  and its 2-Selmer group,  $\text{Sel}_2(E/L)$ , locally at only a few places of  $L$  is sufficient to, under some mild conditions, understand the relation between  $\dim_{\mathbb{F}_2} \text{Sel}_2(E/L)$  and  $\dim_{\mathbb{F}_2} \text{Sel}_2(E^F/L)$  for some quadratic twists,  $E^F$ , of  $E$ .

One defines the 2-Selmer group of a twist  $E^F/L$  following the definition laid out in Section 3A, just with  $E^F$  in place of  $E$ . It is important to note that  $E^F[2]$  and  $E[2]$  are isomorphic as Galois modules, so we may view both Selmer groups inside  $H^1(L, E[2])$ .

Lemma 2.4 shows that understanding the rank growth in quadratic extensions will be sufficient for understanding rank growth in the quartic extensions of interest. In the remainder of this section we will record some results from [Mazur and Rubin 2010] on how local information about  $E$  relates the 2-Selmer rank of  $E$  to the 2-Selmer rank of quadratic twists of  $E$ .

**Lemma 3.2** [Mazur and Rubin 2010, Lemma 2.2]. *With the notation as above:*

- If  $v \nmid 2\infty$ , then  $\dim_{\mathbb{F}_2} H_f^1(L_v, E[2]) = \dim_{\mathbb{F}_2} E(L_v)[2]$ .
- If  $v \nmid 2\infty$  and  $E$  has good reduction at  $v$ , then

$$H_f^1(L_v, E[2]) \cong E[2]/(\text{Frob}_v - 1)E[2].$$

**Definition 3.3.** Suppose  $T$  is a finite set of places of  $L$ . Let  $\text{loc}_T$  be the sum of the localization maps for each place of  $T$ ,

$$\text{loc}_T : H^1(L, E[2]) \rightarrow \bigoplus_{v \in T} H^1(L_v, E[2]).$$

Also set

$$V_T = \text{loc}_T(\text{Sel}_2(E/L)) \subset \bigoplus_{v \in T} H_f^1(L_v, E[2]).$$

We finish the section by recalling two results from [Mazur and Rubin 2010] that we'll later use to control the rank of the 2-Selmer groups in the quadratic extension of Lemma 2.4.

**Lemma 3.4** [Mazur and Rubin 2010, Proposition 3.3]. *Let  $E/L$  be an elliptic curve, and let  $F/L$  be a quadratic extension in which the following places of  $L$  split:*

- all primes where  $E$  has additive reduction;
- all places  $v$  where  $E$  has multiplicative reduction such that  $\text{ord}_v(\Delta_E)$  is even;
- all primes above 2;
- all real places  $v$  with  $(\Delta_E)_v > 0$ .

Further, suppose that all  $v$  where  $E$  has multiplicative reduction and  $\text{ord}_v(\Delta_E)$  is odd are unramified in  $F/L$ .

Let  $T$  be the set of finite primes  $\mathfrak{p}$  of  $L$  such that  $F/L$  is ramified at  $\mathfrak{p}$  and  $E(L_{\mathfrak{p}})[2] \neq 0$ . Then,

$$(3-3) \quad \dim_{\mathbb{F}_2} \text{Sel}_2(E^F/L) = \dim_{\mathbb{F}_2} \text{Sel}_2(E/L) - \dim_{\mathbb{F}_2}(V_T) + d$$

for some  $d$  such that

$$0 \leq d \leq \dim_{\mathbb{F}_2} \left( \bigoplus_{\mathfrak{p} \in T} H_f^1(L_{\mathfrak{p}}, E[2])/V_T \right)$$

and

$$d \equiv \dim_{\mathbb{F}_2} \left( \bigoplus_{\mathfrak{p} \in T} H_f^1(L_{\mathfrak{p}}, E[2])/V_T \right) \pmod{2}.$$

An immediate consequence of the above is the following lemma.

**Lemma 3.5** [Mazur and Rubin 2010, Corollary 3.4]. *For an elliptic curve  $E/L$  and for  $F/L$  and  $T$  as defined in Lemma 3.4, we have:*

(1) *If  $\dim_{\mathbb{F}_2} \left( \bigoplus_{\mathfrak{p} \in T} H_f^1(L_{\mathfrak{p}}, E[2])/V_T \right) \leq 1$ , then*

$$\dim_{\mathbb{F}_2} \text{Sel}_2(E^F/L) = \dim_{\mathbb{F}_2} \text{Sel}_2(E/L) - 2 \dim_{\mathbb{F}_2} V_T + \sum_{\mathfrak{p} \in T} \dim_{\mathbb{F}_2} H_f^1(L_{\mathfrak{p}}, E[2]).$$

(2) *If  $T$  is empty, then  $\dim_{\mathbb{F}_2} \text{Sel}_2(E^F/L) = \dim_{\mathbb{F}_2} \text{Sel}_2(E/L)$ .*

We will use Lemma 3.5, setting  $L$  to be some admissible cubic resolvent, say  $K_3$ , to understand the 2-Selmer rank of some square norm twists by controlling  $\dim_{\mathbb{F}_2} \text{loc}_T(\text{Sel}_2(E/K_3))$  and  $\dim_{\mathbb{F}_2} H_f^1((K_3)_{\mathfrak{p}}, E[2])$  for each  $\mathfrak{p} \in T$ .

#### 4. Twisting by square norm extensions

We will consider elliptic curves  $E/\mathbb{Q}$  together with some  $K_3$  which will always be assumed to be an *admissible cubic resolvent* for  $E$  as in Definition 1.3. Recall that among other conditions, we require  $E(K_3)[2] = 0$  and  $K_3$  to  $\mathbb{Q}(E[2])$  be linearly disjoint.

We are concerned with quadratic twists  $E^F$  over  $K_3$  where we impose conditions on  $F$ . In Section 1 we introduced Definition 1.2 defining *square norm twists* to keep track of conditions on the twists. Recall that for an elliptic curve defined over a number field  $L$ ,  $E/L$ , these are quadratic twists  $E^F/L$  of  $E/L$  where  $F = L(\sqrt{\alpha})$ ,  $\alpha \in L^\times/(L^\times)^2$ , and  $N_{L/\mathbb{Q}}(\alpha)$  is a square.

We will be interested in the application of the definition above where  $L = K_3$ , which, as above, will be the cubic resolvent for some quartic  $S_4$ -extensions of  $\mathbb{Q}$ .

Further, define  $N_r^\square(E, X)$  as follows to count quadratic extensions  $F/K_3$  with bounded conductor,  $\mathfrak{f}(F/K_3)$ , that give square norm twists  $E^F$  of  $E$  with 2-Selmer group of dimension  $r$ :

$$N_r^\square(E, X) = \#\{F = K_3(\sqrt{\alpha}) \mid \alpha \in K_3^\times / (K_3^\times)^2, N_{K_3/\mathbb{Q}}(\alpha) \text{ a square,} \\ \dim_{\mathbb{F}_2} \text{Sel}_2(E^F/K_3) = r, N_{K_3/\mathbb{Q}}\mathfrak{f}(F/K_3) < X\}.$$

With that in mind, we prove the following.

**Proposition 4.1.** *Fix an  $S_3$ - or  $C_3$ -cubic field  $K_3/\mathbb{Q}$ , an elliptic curve  $E/\mathbb{Q}$ , and a nonnegative even integer  $r$ . Suppose there exists a square norm twist,  $E^L/K_3$ , of  $E/K_3$ , with  $\dim_{\mathbb{F}_2} \text{Sel}(E^L/K_3) = r$ . Then we have:*

- If  $\text{Gal}(K_3/\mathbb{Q}) \simeq S_3$  and  $\text{Gal}(K_3(E[2])/K_3) \simeq S_3$ , then

$$N_r^\square(E, X) \gg X^{1/2} / \log(X)^{5/6}.$$

- If  $\text{Gal}(K_3/\mathbb{Q}) \simeq S_3$  and  $\text{Gal}(K_3(E[2])/K_3) \simeq C_3$ , then

$$N_r^\square(E, X) \gg X^{1/2} / \log(X)^{2/3}.$$

- If  $\text{Gal}(K_3/\mathbb{Q}) \simeq C_3$  and  $\text{Gal}(K_3(E[2])/K_3) \simeq S_3$ , then

$$N_r^\square(E, X) \gg X^{1/2} / \log(X)^{8/9}.$$

- If  $\text{Gal}(K_3/\mathbb{Q}) \simeq C_3$  and  $\text{Gal}(K_3(E[2])/K_3) \simeq C_3$ , then

$$N_r^\square(E, X) \gg X^{1/2} / \log(X)^{7/9}.$$

**Remark 4.2.** In [Section 5](#), we will prove the existence of the quadratic extension  $L/K_3$  from the hypotheses of [Proposition 4.1](#). With this, we will use the relationship between the rank growth from  $\mathbb{Q}$  to  $K$  and the rank growth  $K_3$  to a quadratic extensions  $F/K_3$  to prove [Theorem 1.1](#).

The rest of this section will be devoted to proving [Proposition 4.1](#). Before proceeding, we first need to enumerate ideals in  $K_3$  that allow us to get quadratic extensions for square norm twists. We will then show for each such ideal, there is a square norm twist of  $E$  corresponding to that ideal.

**Lemma 4.3.** *Suppose  $E/\mathbb{Q}$  is an elliptic curve where  $K_3$  is an admissible  $S_3$ -cubic resolvent for  $E$  and  $\text{Gal}(K_3(E[2])/K_3)$  is  $C_3$  or  $S_3$ . Let  $S$  be the set of the elements of order 3 in  $\text{Gal}(K_3(E[2])/K_3)$ , and  $N$  be a ray class field of  $K_3$ . Then the number of ideals  $\mathfrak{b}$  of  $K_3$  such that*

- $N\mathfrak{b} < X$  and  $[\mathfrak{b}, N/K_3] = 1$ , and
- for every prime ideal  $\mathfrak{p}$  dividing  $\mathfrak{b}$ ,  $N\mathfrak{p}$  is a square and  $\text{Frob}_{\mathfrak{p}}(K_3(E[2])/K_3) \subset S$

is asymptotic to

$$(C + o(1)) \frac{X^{1/2}}{\log(X)^{1-(1/2)(|S|/|K_3(E[2]):K_3|)}}$$

as  $X \rightarrow \infty$ , where  $C$  is some positive constant,  $[-, N/K_3]$  is the global Artin symbol and  $N$  is the ideal norm.

*Proof.* An unramified, noninert rational prime  $p$  can split as a product of primes in two ways in the ring of integers,  $\mathcal{O}_{K_3}$ , of the cubic field  $K_3$ . Either  $p\mathcal{O}_{K_3} = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3$  where each factor has degree one, or  $p\mathcal{O}_{K_3} = \mathfrak{p}_1\mathfrak{p}_2$  where one factor has degree one and one factor has degree two. Primes of degree two only appear as factors in the latter splitting type.

First we will count rational primes  $p$  such that  $p\mathcal{O}_{K_3} = \mathfrak{p}\mathfrak{q}$  where the residue degrees of the prime factors are  $f(\mathfrak{p}|p) = 1$  and  $f(\mathfrak{q}|p) = 2$ . For each such  $p < X$  we get one prime  $\mathfrak{q}$  of  $K_3$  of square norm such that  $N\mathfrak{q} < X^2$ . Let  $\mathcal{S}_{(1,2)}$  be the set of such rational primes, i.e.,

$$(4-1) \quad \mathcal{S}_{(1,2)} := \{p \in \mathbb{N} \text{ prime} \mid p\mathcal{O}_{K_3} = \mathfrak{p}\mathfrak{q}, f(\mathfrak{p}|p) = 1, f(\mathfrak{q}|p) = 2\}$$

Also set

$$\mathcal{P}_{(1)} := \{\mathfrak{p} \subset \mathcal{O}_{K_3} \text{ prime ideal} \mid (\mathfrak{p} \cap \mathbb{Z})\mathcal{O}_{K_3} = \mathfrak{p}\mathfrak{q}, f(\mathfrak{p}|\mathfrak{p} \cap \mathbb{Z}) = 1, f(\mathfrak{q}|\mathfrak{p} \cap \mathbb{Z}) = 2\}$$

and

$$(4-2) \quad \mathcal{Q}_{(2)} := \{\mathfrak{q} \subset \mathcal{O}_{K_3} \text{ prime ideal} \mid f(\mathfrak{q}|\mathfrak{q} \cap \mathbb{Z}) = 2\}.$$

Likewise, define

- $\mathcal{S}_{(1,2)}(X) := \{p \in \mathcal{S}_{(1,2)} \mid p < X\}$ ;
- $\mathcal{P}_{(1)}(X) := \{\mathfrak{p} \in \mathcal{P}_{(1)} \mid N\mathfrak{p} < X\}$ ;
- $\mathcal{Q}_{(2)}(X) := \{\mathfrak{q} \in \mathcal{Q}_{(2)} \mid N\mathfrak{q} < X\}$ .

With this notation, the discussion above amounts to

$$(4-3) \quad \#\mathcal{S}_{(1,2)}(X) = \#\mathcal{P}_{(1)}(X) = \#\mathcal{Q}_{(2)}(X^2).$$

A rational prime  $p$  belongs to  $\mathcal{S}_{(1,2)}$  if and only if  $\text{Frob}_p(\tilde{K}_3/\mathbb{Q})$  acts on the three cosets of  $\text{Gal}(\tilde{K}_3/\mathbb{Q})/\text{Gal}(\tilde{K}_3/K_3)$  like a transposition. Via the Chebotarev density theorem, this happens with probability  $\#\{\text{transpositions in } S_3\}/\#S_3 = \frac{1}{2}$ . That is, the density of  $\mathcal{S}_{(1,2)}$  in the set of all rational primes is  $\frac{1}{2}$ .

We can conclude the Dirichlet density,  $\delta_{\text{dir}}$ , of the set of primes  $\mathfrak{p}$  in  $K_3$  corresponding to each  $p \in \mathcal{S}_{(1,2)}$  is also  $\frac{1}{2}$ , i.e.,

$$(4-4) \quad \delta_{\text{dir}}(\{\mathfrak{p} \mid f(\mathfrak{p}|\mathfrak{p} \cap \mathbb{Z}) = 1, (\mathfrak{p} \cap \mathbb{Z})\mathcal{O}_{K_3} = \mathfrak{p}\mathfrak{q}, f(\mathfrak{q}|\mathfrak{p} \cap \mathbb{Z}) = 2\}) = \delta_{\text{dir}}(\mathcal{P}_{(1)}) = \frac{1}{2}.$$

Now define some notation. Set  $M = K_3(E[2])$  and recall that  $S$  is the set of all elements of order 3 in  $\text{Gal}(M/K_3)$  and note that  $S$  is a union of conjugacy classes when  $\text{Gal}(M/K_3) = C_3$  and is a conjugacy class when  $\text{Gal}(M/K_3) = S_3$ . Now, set

- $\mathcal{P} = \{\mathfrak{p} \in \mathcal{P}_{(1)} \mid \mathfrak{p} \text{ unramified in } NM/K_3, \text{Frob}_{\mathfrak{p}}(M/K_3) \subset S\}$ ;
- $\mathcal{Q} = \{\mathfrak{q} \in \mathcal{Q}_{(2)} \mid \mathfrak{p} \text{ unramified in } NM/K_3, \text{Frob}_{\mathfrak{q}}(M/K_3) \subset S\}$ ;
- $\mathcal{N} = \{\mathfrak{a} \mid \text{squarefree product of ideals from } \mathcal{P}\}$ ;
- $\mathcal{N}_1 = \{\mathfrak{a} \mid \text{squarefree product of ideals from } \mathcal{P}, [\mathfrak{a}, N/K_3] = 1\}$ ;
- $\mathcal{R}_1 = \{\mathfrak{b} \mid \text{squarefree product of ideals from } \mathcal{Q}, [\mathfrak{b}, N/K_3] = 1\}$ .

Our goal is now to access the number of ideals in  $\mathcal{N}_1(X)$  via the Dirichlet series  $\sum_{\mathfrak{a} \in \mathcal{N}_1} N\mathfrak{a}^{-1}$  and a Tauberian theorem of Wintner. Indeed, we'll see knowing  $\mathcal{N}_1(X)$  suffices to understand  $\mathcal{R}_1(X^2)$ .

To that end, for an irreducible character  $\chi : \text{Gal}(N/K_3) \rightarrow \mathbb{C}^\times$  where we will write  $\chi(\mathfrak{a})$  for  $\chi([\mathfrak{a}, N/K_3])$ , set

$$(4-5) \quad f_\chi(s) := \sum_{\mathfrak{a} \in \mathcal{N}} \chi(\mathfrak{a})N\mathfrak{a}^{-s} = \prod_{\mathfrak{p} \in \mathcal{P}} (1 + \chi(\mathfrak{p})N\mathfrak{p}^{-s}).$$

Note that  $\mathfrak{p} \in \mathcal{P}$  can't be above a rational prime  $p$  which splits completely in  $\tilde{K}_3$ ; if it split completely in  $\tilde{K}_3$ , then it splits completely in  $K_3$ , too. Thus,  $\text{Frob}_{\mathfrak{p}}(\tilde{K}_3/K_3)$  isn't trivial.

Let  $\tau$  be the nontrivial element of  $\text{Gal}(\tilde{K}_3/K_3)$  and set

$$(4-6) \quad S' = \{\tau\} \times S \subset \text{Gal}(\tilde{K}_3M/K_3) = \text{Gal}(\tilde{K}_3/K_3) \times \text{Gal}(M/K_3)$$

and

$$\delta(S, \chi) = \begin{cases} 0 & \text{if } \chi \text{ nontrivial,} \\ \frac{1}{2} \frac{|S|}{[M : K_3]} & \text{if } \chi \text{ trivial,} \end{cases}$$

noting that, in the  $\chi$  trivial case,

$$\frac{1}{2} \frac{|S|}{[M : K_3]} = \#S' / \#\text{Gal}(\tilde{K}_3M/K_3).$$

We write  $g_1(s) \sim g_2(s)$  for two complex functions  $g_1, g_2$  on the half plane  $\Re s > 1$  if  $g_1(s) - g_2(s)$  extends to a holomorphic function on the half plane  $\Re s \geq 1$ . Now, starting from the logarithm of (4-5) and using the Chebotarev density theorem,

$$\log f_\chi(s) \sim \sum_{\mathfrak{p} \in \mathcal{P}} \chi(\mathfrak{p})N\mathfrak{p}^{-s} \sim \delta(S, \chi) \sum_{\mathfrak{p} \text{ prime}} \chi(\mathfrak{p})N\mathfrak{p}^{-s} \sim \delta(S, \chi) \log \frac{1}{s-1}.$$

Using character orthogonality, observe

$$(4-7) \quad \begin{aligned} \frac{1}{[N : K_3]} \sum_{\chi} f_{\chi}(s) &= \frac{1}{[N : K_3]} \sum_{\mathfrak{a} \in \mathcal{N}} N \mathfrak{a}^{-s} \sum_{\chi} \chi(\mathfrak{a}) \\ &= \sum_{\mathfrak{a} \in \mathcal{N}_1} N \mathfrak{a}^{-s} = (s-1)^{-(1/2)(|S|/[M:K_3])} h(s), \end{aligned}$$

where the first two sums range over irreducible characters  $\chi$  of  $\text{Gal}(N/K_3)$ , and where  $h(s)$  is a nonzero, holomorphic function for  $\Re s \geq 1$ .

Applying a Tauberian theorem of Wintner [1942] to (4-7), we obtain

$$(4-8) \quad \#\mathcal{N}_1(X) = (C + o(1)) \frac{X}{\log(X)^{1-(1/2)(|S|/[M:K_3])}}.$$

Now, if  $\mathfrak{a} \in \mathcal{N}_1$  we have, for some positive integer  $m$ ,  $\mathfrak{a} = \prod_{i=1}^m \mathfrak{p}_i$ , where  $\mathfrak{p}_i \in \mathcal{P}$ . For each rational prime  $p_i$  below  $\mathfrak{p}_i$ , we have  $\mathfrak{p}_i \mathcal{O}_{K_3} = \mathfrak{p}_i \mathfrak{q}_i$  where  $\mathfrak{q}_i \in \mathcal{Q}$ . Set  $\mathfrak{b} = \prod_{i=1}^m \mathfrak{q}_i$ .

First, we'll show  $\text{Frob}_{\mathfrak{q}_i}(M/K_3) \subset S$ . If  $E : y^2 = f(T)$ , consider the cubic extension  $L = K_3(T)/(f(T))$ , where  $f(T) \in \mathbb{Q}[x]$  is some cubic polynomial, between  $M$  and  $K_3$ . If  $\text{Gal}(M/K_3) = C_3$ , then  $M = L$ . We can look at how  $f(T)$  factors modulo  $\mathfrak{p}_i$  and  $\mathfrak{q}_i$ . The only way for  $f(T)$  to be irreducible modulo  $\mathfrak{q}_i$  (i.e., over  $\mathbb{F}_{p_i^2}$ ) is for  $f(T)$  to be irreducible modulo  $\mathfrak{p}_i$ ; this happens precisely when  $\text{Frob}_{\mathfrak{p}_i}(M/K_3) \subset S$ . If  $f(T) \pmod{\mathfrak{q}_i}$  is irreducible,  $\text{Frob}_{\mathfrak{q}_i}(M/K_3)$  has order 3. That is, demanding  $\text{Frob}_{\mathfrak{p}_i}(M/K_3) \subset S$  forces  $\text{Frob}_{\mathfrak{q}_i}(M/K_3) \subset S$ .

Second, since each  $\mathfrak{p}_i \mathfrak{q}_i$  is principle, knowing  $[\mathfrak{a}, N/K_3] = 1$  suffices to show  $[\mathfrak{b}, N/K_3] = 1$ , too. Thus,  $\mathfrak{b} \in \mathcal{R}_1$ .

Finally, since  $N\mathfrak{b} = (N\mathfrak{a})^2$ , we have established a bijection between  $\mathcal{N}_1(X)$  and  $\mathcal{R}_1(X^{1/2})$  by mapping  $\mathfrak{a} \mapsto \mathfrak{b}$ .

This and (4-8) give us

$$\#\mathcal{R}_1(X) \sim (C + o(1)) \frac{X^{1/2}}{\log(X)^{1-(1/2)(|S|/[M:K_3])}}$$

for some positive constant  $C$ , as needed. □

We now state and prove the analogue of Lemma 4.3 in the case that  $K_3$  is an admissible  $C_3$ -cubic resolvent.

**Lemma 4.4.** *Suppose  $E/\mathbb{Q}$  is an elliptic curve where  $K_3$  is an admissible  $C_3$ -cubic resolvent for  $E$  and  $\text{Gal}(K_3(E[2])/K_3)$  is  $C_3$  or  $S_3$ . Let  $S$  be the set of the elements of order 3 in  $\text{Gal}(\mathbb{Q}(E[2])/\mathbb{Q})$ , and  $N$  be an abelian extension of  $K_3$ . Then, the number of ideals  $\mathfrak{b}$  of  $K_3$  such that*

- $N\mathfrak{b} < X$ ,  $N\mathfrak{b}$  is a square, and  $[\mathfrak{b}, N/K_3] = 1$ ; and
- for every prime ideal  $\mathfrak{p}$  dividing  $\mathfrak{b}$ ,  $\text{Frob}_{\mathfrak{p}}(K_3(E[2])/K_3) \subset S$

is asymptotic to

$$(D + o(1)) \frac{X^{1/2}}{\log(X)^{1-(1/2)(|S|/[K_3(E[2]):\mathbb{Q}])}}$$

for some real, positive constant  $D$ , and where  $[-, N/K_3]$  is the global Artin symbol and  $N$  is the ideal norm.

*Proof.* Since  $K_3$  is an admissible  $C_3$ -cubic resolvent, we have that  $K_3$  and  $\mathbb{Q}(E[2])$  are linearly disjoint. Setting  $M = K_3(E[2])$ , we have  $\text{Gal}(M/\mathbb{Q}) = C_3 \times S_3$ . First, some notation. Define the following sets:

- $\mathcal{P}_{\mathbb{Q}} = \{p \in \mathbb{N} \text{ prime} \mid \text{Frob}_p(M/\mathbb{Q}) \subset \{1\} \times S, p \text{ unramified in } \tilde{N}K_3\mathbb{Q}(E[2])\}$ ;
- $\mathcal{A} = \{a \mid a \text{ a squarefree product of } p \in \mathcal{P}_{\mathbb{Q}}\}$ ;
- $\mathcal{A}_1 = \{a \in \mathcal{A} \mid [(a), \tilde{N}/\mathbb{Q}] = 1\}$  where  $[-, \tilde{N}/\mathbb{Q}]$  is the global Artin symbol.

Let  $\tilde{N}$  be the normal closure of  $N$  over  $\mathbb{Q}$ . We will use the triviality of the Artin symbol  $[-, \tilde{N}/\mathbb{Q}]$  to obtain the triviality of the Artin symbol  $[-, N/\mathbb{Q}]$  as in the statement of the lemma. Now, for a character  $\psi : \text{Gal}(\tilde{N}/\mathbb{Q}) \rightarrow \mathbb{C}^\times$ , and writing  $\psi(a)$  for  $\psi([(a), \tilde{N}/\mathbb{Q}])$ , let

$$f_\psi(s) := \sum_{a \in \mathcal{A}} \psi(a) a^{-s}.$$

For two functions  $g_1$  and  $g_2$  defined on the complex half plane  $\Re s > 1$ , write  $g_1(s) \sim g_2(s)$  to mean  $g_1(s)$  and  $g_2(s)$  differ by a function which is holomorphic on  $\Re s \geq 1$ . Taking log of the  $f_\psi(s)$ , substituting the Taylor series for  $\log(1-x)$  and truncating the Taylor series after one term, one arrives at

$$(4-9) \quad \log f_\psi(s) = \sum_{p \in \mathcal{P}_{\mathbb{Q}}} \log(1 + \psi(p)p^{-s}) \sim \sum_{p \in \mathcal{P}_{\mathbb{Q}}} \psi(p)p^{-s} \sim \delta_\psi \log \frac{1}{s-1},$$

where, using the Chebotarev density theorem,

$$\delta_\psi = \begin{cases} 0 & \text{if } \psi \text{ is nontrivial,} \\ \frac{|S|}{[M:\mathbb{Q}]} & \text{if } \psi \text{ is trivial.} \end{cases}$$

Now, using character orthogonality and summing over irreducible characters  $\psi$  of  $\text{Gal}(\tilde{N}/\mathbb{Q})$ , we have

$$(4-10) \quad \frac{1}{[\tilde{N}:\mathbb{Q}]} \sum_{\psi} f_\psi(s) = \frac{1}{[\tilde{N}:\mathbb{Q}]} \sum_{a \in \mathcal{A}} a^{-s} \sum_{\psi} \psi(a) = \sum_{a \in \mathcal{A}_1} a^{-s}.$$

But also, using (4-9), we have

$$(4-11) \quad \frac{1}{[\tilde{N}:\mathbb{Q}]} \sum_{\psi} f_\psi(s) = g(s)(s-1)^{-|S|/[M:\mathbb{Q}]},$$

where  $g(s)$  is holomorphic and nonzero on  $\Re s \geq 1$ . Thus, via (4-10) and (4-11),

$$\sum_{a \in \mathcal{A}_1} a^{-s} = g(s)(s-1)^{-|S|/[M:\mathbb{Q}]}$$

Applying a Tauberian theorem of Wintner [1942] yields

$$\#\{a \in \mathcal{A}_1 \mid a < X\} = (C + o(1)) \frac{X}{(\log X)^{1-|S|/[M:\mathbb{Q}]}}$$

for some positive, real  $C$ .

Now, suppose  $a \in \mathcal{A}_1$  and  $a = \prod_{i=1}^r p_i$ , where the  $p_i$  are distinct primes and  $p_i \in \mathcal{P}_{\mathbb{Q}}$  and each  $p_i$  splits completely in  $\mathcal{O}_{K_3}$ . Set  $\mathfrak{a} = a\mathcal{O}_{K_3}$ . Then  $\mathfrak{a}$  decomposes into prime ideals as  $\mathfrak{a} = \prod_{i=1}^r \mathfrak{p}_i \mathfrak{p}'_i \mathfrak{p}''_i$  where  $\mathfrak{p}_i$ ,  $\mathfrak{p}'_i$ , and  $\mathfrak{p}''_i$  are the three primes above  $p_i$ . For each  $\mathfrak{p}_i$  above a prime  $p_i$ , pick another prime  $\mathfrak{p}'_i$  of  $K_3$  above  $p_i$  (there are two choices), and set  $\mathfrak{b} = \prod_{i=1}^r \mathfrak{p}_i \mathfrak{p}'_i$ . Note  $N_{K_3/\mathbb{Q}} \mathfrak{b} = a^2$ .

In this way, counting  $a \in \mathcal{A}_1$  with  $a < X$  gives a way of counting ideals  $\mathfrak{b}$  in  $K_3$  such that  $N_{K_3/\mathbb{Q}} \mathfrak{b} < X^{1/2}$  such that  $N_{K_3/\mathbb{Q}} \mathfrak{b}$  is a square and, for each prime  $\mathfrak{p}$  dividing  $\mathfrak{b}$ ,  $\text{Frob}_{\mathfrak{p}}(M/K_3) \subset S$  and  $[\mathfrak{b}, N/K_3] = 1$ . The lemma follows.  $\square$

For an elliptic curve  $E$  and each of the ideals enumerated in Lemma 4.3, there is a twist of  $E$  in which the 2-Selmer rank remains the same.

**Lemma 4.5.** *Keeping the notation of Lemma 4.3, if  $\mathfrak{b}$  is an ideal of  $K_3$  such that*

- $N\mathfrak{b} < X$ ,
- if a prime ideal  $\mathfrak{p}$  divides  $\mathfrak{b}$ , then  $N\mathfrak{p}$  is a square,
- $\text{Frob}_{\mathfrak{p}}(K_3(E[2])/K_3) \subset S$ , and
- $[\mathfrak{b}, N/K_3] = 1$ ,

then there is a quadratic extension  $F/K_3$  of conductor  $\mathfrak{b}$  such that

$$\dim_{\mathbb{F}_2} \text{Sel}_2(E^F/K_3) = \dim_{\mathbb{F}_2} \text{Sel}_2(E/K_3).$$

*Proof.* This is Proposition 4.2 of [Mazur and Rubin 2010], with  $N = K_3(8\Delta_E\infty)$ , the ray class field of  $K_3$  modulo  $8\Delta_E$  and all archimedean places of  $K_3$ , applied to the relevant ideals, which are a subset of the ideals discussed in that result.  $\square$

For an elliptic curve  $E$  and each of the ideals enumerated in Lemma 4.4, there is a twist of  $E$  in which the 2-Selmer rank remains the same.

**Lemma 4.6.** *Keeping the notation of Lemma 4.4, if  $\mathfrak{b}$  is an ideal of  $K_3$  such that*

- $N\mathfrak{b} < X$ ,
- if a prime ideal  $\mathfrak{p}$  divides  $\mathfrak{b}$ , then  $N\mathfrak{p}$  is a square,
- $\text{Frob}_{\mathfrak{p}}(K_3(E[2])/K_3) \subset S$ , and
- $[\mathfrak{b}, N/K_3] = 1$ ,



then there is a quadratic extension  $F/K_3$  of conductor  $\mathfrak{b}$  such that

$$\dim_{\mathbb{F}_2} \text{Sel}_2(E^F/K_3) = \dim_{\mathbb{F}_2} \text{Sel}_2(E/K_3).$$

*Proof.* The proof is the same as that of [Lemma 4.5](#).  $\square$

We are now ready to prove the main result of the section. We follow exactly the strategy of the proof of [\[Mazur and Rubin 2010, Theorem 1.4\]](#) with the additional step of keeping track of the square norm condition of the involved quadratic twists.

*Proof of [Proposition 4.1](#).* As in [Lemmas 4.3](#) and [4.4](#), let  $S$  be the set of order-3 elements in  $\text{Gal}(K_3(E[2])/K_3)$ . Then if  $\text{Gal}(K_3(E[2])/K_3) \simeq S_3$ ,

$$\frac{|S|}{[K_3(E[2]) : K_3]} = \frac{1}{3},$$

and if  $\text{Gal}(K_3(E[2])/K_3) \simeq \mathbb{Z}/3\mathbb{Z}$ ,

$$\frac{|S|}{[K_3(E[2]) : K_3]} = \frac{2}{3}.$$

We'll consider the case that  $K_3$  is an admissible  $S_3$ -cubic resolvent; there are two subcases to consider:

(1) Suppose  $\dim_{\mathbb{F}_2} \text{Sel}_2(E/K_3) = r$ . By [Lemmas 4.3](#) and [4.5](#), the number of square norm twists  $E^F/K_3$  such that  $\dim_{\mathbb{F}_2} \text{Sel}_2(E^F/K_3) = r$  is

$$\gg \frac{X^{1/2}}{\log X^{1-(1/2)(|S|/[K_3(E[2]):K_3])}}.$$

(2) Suppose  $\dim_{\mathbb{F}_2} \text{Sel}_2(E/K_3) \neq r$ . We have assumed there is a square norm twist  $E^L/K_3$  such that  $\dim_{\mathbb{F}_2} \text{Sel}_2(E^L/K_3) = r$ . Note that a square norm twist of a square norm twist results in the square norm twist. That is, a square norm twist  $(E^L)^{F'}$  of  $E^L$  is itself a square norm twist  $E^F$  of  $E$ . Now the result follows from [Case \(1\)](#) applied to  $E^L$ .

If instead  $K_3$  is an admissible  $C_3$ -cubic resolvent for  $E$ , the proof is the same as above, but with [Lemmas 4.4](#) and [4.6](#) in place of [Lemmas 4.3](#) and [4.5](#), respectively.  $\square$

## 5. Decreasing the 2-Selmer rank

Our strategy will be to use [Lemma 3.5\(2\)](#) to understand the 2-Selmer rank of square norm twists. We'll then use [Proposition 4.1](#) to show there are many square norm twist with prescribed 2-Selmer rank assuming we *have already* a square norm twist of that prescribed 2-Selmer rank. We'll show a square norm twist with that prescribed 2-Selmer rank *must exist* by showing we can take square norm twists that reduce the 2-Selmer rank by two; this is the content of [Proposition 5.1](#).

**Proposition 5.1** below can be viewed as analogous to Proposition 5.1(iii) of [Mazur and Rubin 2010]. Except, instead of decreasing the 2-Selmer rank by 1 via a quadratic twist obtained by controlling one local condition, we decrease the 2-Selmer rank by 2 via a square norm twist obtained by controlling two local conditions. Those two local conditions are obtained from two primes in the cubic resolvent above the same rational prime.

**Proposition 5.1.** *Let  $E$  be an elliptic curve defined over  $\mathbb{Q}$  and let  $K_3$  be an admissible cubic resolvent for  $E$ . Suppose further that*

$$\dim_{\mathbb{F}_2} \text{Sel}_2(E/\mathbb{Q}) = 0 \quad \text{and} \quad \dim_{\mathbb{F}_2} \text{Sel}_2(E/K_3) \geq 2.$$

*Then there exists a square norm twist  $E^F/K_3$  such that*

$$\dim_{\mathbb{F}_2} \text{Sel}_2(E^F/K_3) = \dim_{\mathbb{F}_2} \text{Sel}_2(E/K_3) - 2.$$

*Proof.* Let  $\Delta_E$  be the discriminant of (a minimal model of)  $E$ . For the admissible cubic resolvent,  $K_3$ , of  $E$ , set  $M = K_3(E[2])$ . Note that  $M/K_3$  is a Galois  $S_3$ -extension, since  $K_3$  is as in Definition 1.3, and  $K_3(\sqrt{\Delta_E})/K_3$  is an intermediate quadratic extension. Let  $v_0$  be the distinguished place of  $K_3$  guaranteed by Definition 1.3.

Let  $\Sigma$  be a finite set that contains the following places of  $K_3$ : all infinite places of  $K_3$ , places of bad reduction for  $E$ , and all primes above 2. Now set  $\mathfrak{d} = \prod_{v \in \Sigma \setminus \{v_0\}} v$ . Let  $K_3(8\mathfrak{d})$  be the ray class field of  $K_3$  with modulus  $8\mathfrak{d}$  and let  $K_3[8\mathfrak{d}]$  be the maximal extension between  $K_3(8\mathfrak{d})$  and  $K_3$  whose degree is a power of 2.

Let  $\tilde{K}_3$  be the Galois closure of  $K_3$  over  $\mathbb{Q}$  and  $\mathfrak{D} = \prod_{V|v, v|\mathfrak{d}} V$  be the product of places of  $\tilde{K}_3$  above the places of  $K_3$  dividing  $\mathfrak{d}$ . Let  $L$  be the maximal extension<sup>1</sup> of  $\tilde{K}_3$  between  $\tilde{K}_3$  and the ray class field of  $\tilde{K}_3$  with modulus  $8\mathfrak{D}$ . Note  $L \supseteq K_3[8\mathfrak{d}]$ ,  $[L : K_3]$  is a power of 2, and  $L$  is Galois over  $\mathbb{Q}$ .

By assumption,  $\tilde{K}_3$  and  $\mathbb{Q}(E[2])$  are linearly disjoint over  $\mathbb{Q}$ .  $K_3[8\mathfrak{d}]$  and  $M$  are linearly disjoint as extensions of  $K_3$  since  $v_0$  is ramified in  $K_3(\sqrt{\Delta_E})$  but not in  $K_3[8\mathfrak{d}]$ . By the conditions on  $v_0$  of Definition 1.3,  $v_0$  does not ramify from  $K_3$  to  $\tilde{K}_3$ , and hence is unramified in  $L$ . So likewise, the same consideration of  $K_3(\sqrt{\Delta_E})$  shows  $M$  and  $L$  are linearly disjoint over  $K_3$ .

Let  $\sigma$  be an element of the absolute Galois group of  $K_3$  such that  $\sigma|_M$  is a transposition in  $\text{Gal}(M/K_3) \simeq \text{Aut}(E[2])$  and  $\sigma|_L = 1$ . The former condition implies  $E[2]/(\sigma - 1)E[2] \simeq \mathbb{F}_2$ . The latter condition implies  $\sigma|_{K_3[8\mathfrak{d}]} = 1$ .

For the rest of the proof, fix a nonzero map  $\phi : \text{Sel}_2(E/K_3) \rightarrow E[2]/(\sigma - 1)E[2]$ . By [Mazur and Rubin 2010, Lemma 3.5], there is an element  $\gamma \in G_{K_3}$  for which  $\gamma = \sigma$  when restricted to  $MK_3[8\mathfrak{d}]$  and  $c(\gamma) = \phi(c)$  for all  $c \in \text{Sel}_2(E/K_3)$ .

Let  $N$  be a Galois extension of  $\mathbb{Q}$  containing  $M$  and  $L$  for which the restriction of  $\text{Sel}_2(E/K_3)$  to  $N$  is zero. For instance, take  $N$  to be the Galois closure (over  $\mathbb{Q}$ )

<sup>1</sup>Note that if  $K_3$  is  $C_3$ -cubic, then  $L = K_3[8\mathfrak{d}]$  since  $\tilde{K}_3 = K_3$ .

of the compositum of  $M$ ,  $L$ , and the fixed field of the kernel of the restriction to  $\text{Hom}(G_M, E[2])$  of every  $c \in \text{Sel}_2(E/K_3)$ .

Let  $\mathcal{P}_\gamma$  be the set of primes  $\mathfrak{p}$  of  $K_3$  for which  $\mathfrak{p} \notin \Sigma$  and  $\text{Frob}_\mathfrak{p}(N/K_3) = \gamma|_N$ . By the Chebotarev density theorem, the natural density of  $\mathcal{P}_\gamma$  among the primes of  $K_3$  is positive, i.e.,

$$\delta_\gamma := \lim_{X \rightarrow \infty} \frac{\#\{\text{primes } \mathfrak{p} \text{ of } K_3 \mid \text{Frob}_\mathfrak{p}(N/K_3) = \gamma|_N, \mathfrak{p} \notin \Sigma, N\mathfrak{p} < X\}}{\#\{\text{primes } \mathfrak{p} \text{ of } K_3 \mid N\mathfrak{p} < X\}} > 0.$$

Now, let  $\mathcal{P}_{\text{sp}}$  be the set of primes of  $K_3$  with inertia degree one over  $\mathbb{Q}$ , that is, the primes  $\mathfrak{p}$  for which the rational prime ideal  $\mathfrak{p} \cap \mathbb{Z}$  splits completely in  $K_3$ . Recall that  $\mathcal{P}_{\text{sp}}$  has natural density one among the primes of  $K_3$ . In particular, this means we can pick a prime  $\mathfrak{p}_1 \in \mathcal{P}_\gamma \cap \mathcal{P}_{\text{sp}}$ . If we could not, then  $\mathcal{P}_\gamma$  (which has positive density) would be contained in the complement of  $\mathcal{P}_{\text{sp}}$  (which has density zero). Let  $p$  be the rational prime below  $\mathfrak{p}_1$ , and let  $\mathfrak{p}_2$  and  $\mathfrak{p}_3$  be the other two primes of  $K_3$  above  $p$ , in other words,  $p\mathcal{O}_{K_3} = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3$ .

Our goal is now to construct a suitable square norm twist from two of  $\mathfrak{p}_1, \mathfrak{p}_2, \mathfrak{p}_3$ . We can understand the 2-Selmer group of this twist using Lemma 3.5(1), which requires us to compute both  $H_f^1((K_3)_{\mathfrak{p}_1}, E[2])$  and  $\text{loc}_{\mathfrak{p}_1} \text{Sel}_2(E/K_3)$ .

First, consider the localization at  $\mathfrak{p}_1$ . Since  $\text{Frob}_{\mathfrak{p}_1} = \gamma$  when restricted to  $N$  (and  $\sigma = \gamma$  when restricted to  $MK_3[8\delta]$ ) we have both that

$$(5-1) \quad H_f^1((K_3)_{\mathfrak{p}_1}, E[2]) \simeq E[2]/(\sigma - 1)E[2] \simeq \mathbb{F}_2$$

and  $\phi(c) = c(\gamma)$  for all  $c \in \text{Sel}_2(E/K_3)$ . The localization map

$$\begin{aligned} \text{loc}_{\mathfrak{p}_1} : \text{Sel}_2(E/K_3) &\rightarrow H_f^1((K_3)_{\mathfrak{p}_1}, E[2]) \simeq E[2]/(\text{Frob}_{\mathfrak{p}_1} - 1)E[2] \\ &\simeq E[2]/(\sigma - 1)E[2] \simeq \mathbb{F}_2 \end{aligned}$$

is given by evaluation of cocycles at  $\text{Frob}_{\mathfrak{p}_1}$ , so we can identify

$$\text{loc}_{\mathfrak{p}_1}(\text{Sel}_2(E/K_3)) = \phi(\text{Sel}_2(E/K_3))$$

as subspaces of  $\mathbb{F}_2$ . Since  $\phi$  is nonzero,

$$(5-2) \quad \dim_{\mathbb{F}_2} \text{loc}_{\mathfrak{p}_1}(\text{Sel}_2(E/K_3)) = 1.$$

It remains to understand the localizations at  $\mathfrak{p}_2$  and  $\mathfrak{p}_3$ . Since  $p$  splits completely in  $K_3$ , there is an equality of local fields

$$(K_3)_{\mathfrak{p}_1} = (K_3)_{\mathfrak{p}_2} = (K_3)_{\mathfrak{p}_3} = \mathbb{Q}_p$$

and so, together with (5-1), we have

$$(5-3) \quad \begin{aligned} H_f^1((K_3)_{\mathfrak{p}_1}, E[2]) &= H_f^1((K_3)_{\mathfrak{p}_2}, E[2]) \\ &= H_f^1((K_3)_{\mathfrak{p}_3}, E[2]) = H_f^1(\mathbb{Q}_p, E[2]) \simeq \mathbb{F}_2. \end{aligned}$$

Beginning from the following commutative diagram, we will consider the localization of  $\text{Sel}_2(E/K_3)$  at primes of  $K_3$  above  $p$  and localization at  $p$ :

$$\begin{array}{ccc} H^1(K_3, E[2]) & \xrightarrow{\bigoplus_{i=1}^3 \text{loc}_{\mathfrak{p}_i}} & \bigoplus_{i=1}^3 H^1((K_3)_{\mathfrak{p}_i}, E[2]) \\ \text{cores}_{K_3/\mathbb{Q}} \downarrow & & \bigoplus_{i=1}^3 \text{cores}_{(K_3)_{\mathfrak{p}_i}/\mathbb{Q}_p} \downarrow \\ H^1(\mathbb{Q}, E[2]) & \xrightarrow{\text{loc}_{(p)}} & H^1(\mathbb{Q}_p, E[2]) \end{array}$$

where the vertical map on the left side,

$$\text{cores}_{K_3/\mathbb{Q}} : H^1(K_3, E[2]) \rightarrow H^1(\mathbb{Q}, E[2]),$$

is determined by corestriction on Galois cohomology induced by the norm map  $N_{K_3/\mathbb{Q}} : K_3 \rightarrow \mathbb{Q}$  (see [Milne 2020, Example 1.29] or [Serre 1997]). The vertical map on the right side is the sum of corestriction maps:

$$\begin{aligned} \bigoplus_{i=1}^3 \text{cores}_{(K_3)_{\mathfrak{p}_i}/\mathbb{Q}_p} : \bigoplus_{i=1}^3 H^1((K_3)_{\mathfrak{p}_i}, E[2]) &\rightarrow H^1(\mathbb{Q}_p, E[2]), \\ (c_1, c_2, c_3) &\mapsto \sum_{i=1}^3 \text{cores}_{(K_3)_{\mathfrak{p}_i}/\mathbb{Q}_p}(c_i). \end{aligned}$$

Restricting the left column to the 2-Selmer groups of  $E$  over  $K_3$  and  $\mathbb{Q}$  and to restricted cohomology on the right column, together with (5-3), we have

$$\begin{array}{ccc} \text{Sel}_2(E/K_3) & \xrightarrow{\text{cores}_{K_3/\mathbb{Q}}} & \text{Sel}_2(E/\mathbb{Q}) = 0 \\ \downarrow \bigoplus_{i=1}^3 \text{loc}_{\mathfrak{p}_i} & & \downarrow \text{loc}_p \\ \bigoplus_{i=1}^3 H_f^1((K_3)_{\mathfrak{p}_i}, E[2]) & \xrightarrow{\bigoplus_{i=1}^3 \text{cores}_{(K_3)_{\mathfrak{p}_i}/\mathbb{Q}_p}} & H_f^1(\mathbb{Q}_p, E[2]) \simeq \mathbb{F}_2 \\ \downarrow \simeq & \nearrow v_1+v_2+v_3 & \\ H_f^1(\mathbb{Q}_p, E[2])^{\oplus 3} \simeq \mathbb{F}_2^3 & & \end{array}$$

where the diagonal map  $\mathbb{F}_2^3 \rightarrow \mathbb{F}_2$  is coordinatewise addition of vectors in  $\mathbb{F}_2^3$  modulo 2. For  $c \in \text{Sel}_2(E/K_3)$  we have  $\text{loc}_p \text{cores}(c) = 0$  since  $\text{Sel}_2(E/\mathbb{Q}) = 0$ . Hence,

$$(5-4) \quad \text{loc}_{\mathfrak{p}_1}(c) + \text{loc}_{\mathfrak{p}_2}(c) + \text{loc}_{\mathfrak{p}_3}(c) = 0 \quad \text{in } \mathbb{F}_2.$$

By (5-2) there is an element  $c \in \text{Sel}_2(E/K_3)$  for which  $\text{loc}_{\mathfrak{p}_1}(c) = 1$  viewed in  $\mathbb{F}_2$ . Combining this with (5-4), there is exactly one prime  $\mathfrak{p}_i \in \{\mathfrak{p}_2, \mathfrak{p}_3\}$  for which  $\text{loc}_{\mathfrak{p}_i}(c) = 1$ ; suppose, without loss of generality, it is  $\mathfrak{p}_2$ . Whence,

$$(5-5) \quad \dim_{\mathbb{F}_2} \text{loc}_{\mathfrak{p}_2} \text{Sel}_2(E/K_3) = 1.$$

Finally, we will twist  $E/K_3$  by a quadratic extension  $F/K_3$  ramified only at  $\mathfrak{p}_1$  and  $\mathfrak{p}_2$  to get our desired result.

Let  $\mathfrak{P}$  be a prime of  $L$  above  $\mathfrak{p}_1$ . Since  $L/\mathbb{Q}$  is Galois, we have

$$\text{Frob}_{\mathfrak{P}}(L/\mathbb{Q})^{f(\mathfrak{p}_1/p)} = \text{Frob}_{\mathfrak{P}}(L/\mathbb{Q}) = \text{Frob}_{\mathfrak{P}}(L/K_3) = 1,$$

i.e.,  $p$  splits completely in  $L$ , and so  $p$  splits completely in  $K_3[8\mathfrak{d}]$ .

Since our choice of Frobenius class for  $p$  is trivial when restricted just to  $K_3[8\mathfrak{d}]$ ,  $\text{Frob}_{\mathfrak{p}_1}(K_3[8\mathfrak{d}]/K_3) = \text{Frob}_{\mathfrak{p}_2}(K_3[8\mathfrak{d}]/K_3) = 1$ , and since  $[K_3(8\mathfrak{d}) : K_3[8\mathfrak{d}]]$  is odd, there will be an odd integer, say  $h$ , such that  $(\mathfrak{p}_1\mathfrak{p}_2)^h$  is principal with generator  $\alpha$  such that  $\alpha \equiv 1 \pmod{8\mathfrak{d}}$  and  $\alpha$  positive at all real embeddings except possibly  $v_0$ .

We are now in a position to construct the quadratic extension  $F/K_3$  by which we will twist  $E$ : Define  $F = K_3(\sqrt{\alpha})$ . Only the primes  $\mathfrak{p}_1$  and  $\mathfrak{p}_2$  of  $K_3$  ramify in  $F$ . Set  $p(x) = x^2 - \alpha$  and note  $p'(1)^2 = 4$ . For any  $\mathfrak{q} \in \Sigma \setminus \{v_0\}$ , since  $\alpha \equiv 1 \pmod{8\mathfrak{d}}$ , we also have  $p(1) = 1 - \alpha \equiv 0 \pmod{4\mathfrak{q}}$ . From Hensel’s lemma (see, e.g., [Eisenbud 1995, Theorem 7.3] for an applicable statement), it follows  $p(x)$  has a root in  $(K_3)_{\mathfrak{q}}$ . So  $(K_3)_{\mathfrak{q}} \otimes F = (K_3)_{\mathfrak{q}}^2$ , that is,  $\mathfrak{q}$  splits in  $F$ . Thus all primes in  $\Sigma \setminus \{v_0\}$  split in  $F$ .

Also,  $N(\alpha) = N(\mathfrak{p}_1)N(\mathfrak{p}_2) = p^{2h}$ , so the quadratic twist  $E^F/K_3$  of  $E/K_3$  is a square norm twist.

Finally, apply Lemma 3.5(1) with  $T = \{\mathfrak{p}_1, \mathfrak{p}_2\}$ ,  $F = K_3(\sqrt{\alpha})$  as above, (5-2) and (5-5), we get

$$\begin{aligned} & \dim_{\mathbb{F}_2} \text{Sel}_2(E^F/K_3) \\ &= \dim_{\mathbb{F}_2} \text{Sel}_2(E/K_3) - 2 \dim_{\mathbb{F}_2} V_T + \sum_{\mathfrak{r} \in T} \dim_{\mathbb{F}_2} H_f^1((K_3)_{\mathfrak{r}}, E[2]) \\ &= \dim_{\mathbb{F}_2} \text{Sel}_2(E/K_3) - 2 \dim_{\mathbb{F}_2} \text{loc}_{\{\mathfrak{p}_1\}}(\text{Sel}_2(E/K_3)) - 2 \dim_{\mathbb{F}_2} \text{loc}_{\{\mathfrak{p}_2\}}(\text{Sel}_2(E/K_3)) \\ & \quad + \dim_{\mathbb{F}_2} H_f^1((K_3)_{\mathfrak{p}_1}, E[2]) + \dim_{\mathbb{F}_2} H_f^1((K_3)_{\mathfrak{p}_2}, E[2]) \\ &= \dim_{\mathbb{F}_2} \text{Sel}_2(E/K_3) - 2 \end{aligned}$$

Noting again the twist by  $F$  above is a square norm twist, we have the desired result. □

### 6. Proofs of the main theorems

We are now ready to prove Theorem 1.4. We’ll then show how it implies Theorem 1.1. Again, the “infinitely many” of both theorems is quantified by Proposition 4.1.

*Proof of Theorem 1.4.* Let  $E$  and  $K_3$  be as in Theorem 1.4. If  $\dim_{\mathbb{F}_2} \text{Sel}_2(E/K_3) \equiv 0 \pmod{2}$ , repeated application of Proposition 5.1 gives a square norm twist  $L$  such that  $\dim_{\mathbb{F}_2} \text{Sel}_2(E^L/K_3) = 0$ . Once we have  $L$ , Proposition 4.1 provides infinitely many more square norm twists  $F$  with  $\dim_{\mathbb{F}_2} \text{Sel}_2(E^F/K_3) = 0$ .

Likewise, if  $\dim_{\mathbb{F}_2} \text{Sel}_2(E/K_3) \equiv 1 \pmod{2}$ , the argument above provides infinitely many more square norm twists  $F$  with  $\dim_{\mathbb{F}_2} \text{Sel}_2(E^F/K_3) = 1$ . □

Now we can prove Theorem 1.1 as a consequence of Theorem 1.4.

*Proof of Theorem 1.1.* Let  $E$  and  $K_3$  be as in the statement of the theorem. Theorem 1.1 is essentially an immediate consequence of Theorem 1.4 coupled with the upper bound the dimension of the 2-Selmer group provides for the rank.

As in Theorem 1.4, there are two cases. In the first case,  $\dim_{\mathbb{F}_2} \text{Sel}_2(E/K_3)$  is even. In this case, Theorem 1.4 provides infinitely many square norm twists  $E^F/K_3$  for which  $\dim_{\mathbb{F}_2} \text{Sel}_2(E^F/K_3) = 0$ .

From (3-1), we have  $\text{rk}(E/K_3) \leq \dim_{\mathbb{F}_2} \text{Sel}_2(E/K_3)$ . Thus, our infinitely many square norm twists  $E^F$  of 2-Selmer rank zero give us

$$0 = \dim_{\mathbb{F}_2} \text{Sel}_2(E^F/K_3) \geq \text{rk}(E^F/K_3) = \text{rk}(E/F) - \text{rk}(E/K_3).$$

If  $K/\mathbb{Q}$  is the  $S_4$ -quartic corresponding to quadratic extension  $F/K_3$  corresponding to each square norm twist, then having no rank growth from  $K_3$  to  $F$  means we have no rank growth from  $\mathbb{Q}$  to  $K$  for infinitely many  $K$ .

In the second case,  $\dim_{\mathbb{F}_2} \text{Sel}_2(E/K_3)$  is even. Then, in the same way as above, there are infinitely many square norm twists  $E^F$  of 2-Selmer rank one. The result follows if we assume the parity of the rank and 2-Selmer dimension are the same.  $\square$

### Acknowledgements

Much of this project was completed as part of the author's graduate work; he thanks his advisor, Robert Lemke Oliver, for all of his guidance, suggestions, and support. He also thanks George McNinch, Sun Woo Park, Ari Shnidman, David Smyth, and Jiuya Wang for fruitful conversations and helpful comments on this paper. Finally, the author also extends his thanks to an anonymous referee from PJM for multiple careful readings and comments that greatly improved the paper.

### References

- [Bartel and Dokchitser 2015] A. Bartel and T. Dokchitser, “Brauer relations in finite groups”, *J. Eur. Math. Soc. (JEMS)* **17**:10 (2015), 2473–2512. [MR](#) [Zbl](#)
- [Bhargava et al. 2015] M. Bhargava, A. Shankar, and X. Wang, “Geometry-of-numbers methods over global fields, I: Prehomogeneous vector spaces”, preprint, 2015. [arXiv 1512.03035](#)
- [Cohen and Thorne 2016] H. Cohen and F. Thorne, “Dirichlet series associated to quartic fields with given cubic resolvent”, *Res. Number Theory* **2** (2016), art. id. 29. [MR](#) [Zbl](#)
- [David et al. 2007] C. David, J. Fearnley, and H. Kisilevsky, “Vanishing of  $L$ -functions of elliptic curves over number fields”, pp. 247–259 in *Ranks of elliptic curves and random matrix theory*, edited by J. B. Conrey et al., London Math. Soc. Lecture Note Ser. **341**, Cambridge Univ. Press, 2007. [MR](#) [Zbl](#)
- [Dokchitser and Dokchitser 2010] T. Dokchitser and V. Dokchitser, “On the Birch–Swinnerton-Dyer quotients modulo squares”, *Ann. of Math. (2)* **172**:1 (2010), 567–596. [MR](#) [Zbl](#)
- [Eisenbud 1995] D. Eisenbud, *Commutative algebra: with a view toward algebraic geometry*, Graduate Texts in Mathematics **150**, Springer, 1995. [MR](#) [Zbl](#)

- [Klagsbrun et al. 2014] Z. Klagsbrun, B. Mazur, and K. Rubin, “A Markov model for Selmer ranks in families of twists”, *Compos. Math.* **150**:7 (2014), 1077–1106. [MR](#) [Zbl](#)
- [Lemke Oliver and Thorne 2021] R. J. Lemke Oliver and F. Thorne, “Rank growth of elliptic curves in non-abelian extensions”, *Int. Math. Res. Not.* **2021**:24 (2021), 18411–18441. [MR](#) [Zbl](#)
- [Malle 2004] G. Malle, “On the distribution of Galois groups, II”, *Experiment. Math.* **13**:2 (2004), 129–135. [MR](#) [Zbl](#)
- [Mazur and Rubin 2010] B. Mazur and K. Rubin, “Ranks of twists of elliptic curves and Hilbert’s tenth problem”, *Invent. Math.* **181**:3 (2010), 541–575. [MR](#) [Zbl](#)
- [Milne 2020] J. S. Milne, “Class field theory”, course notes, 2020, available at <https://www.jmilne.org/math/CourseNotes/cft.html>.
- [Serre 1997] J.-P. Serre, *Galois cohomology*, Springer, 1997. [MR](#) [Zbl](#)
- [Shnidman and Weiss 2023] A. Shnidman and A. Weiss, “Rank growth of elliptic curves over  $n$ -th root extensions”, *Trans. Amer. Math. Soc. Ser. B* **10** (2023), 482–506. [MR](#) [Zbl](#)
- [Smith 2017] A. Smith, “ $2^\infty$ -Selmer groups,  $2^\infty$ -class groups, and Goldfeld’s conjecture”, preprint, 2017. [arXiv 1702.02325](#)
- [Smith 2023a] A. Smith, “The distribution of  $\ell^\infty$ -Selmer groups in degree  $\ell$  twist families, II”, preprint, 2023. [arXiv 2207.05143](#)
- [Smith 2023b] A. Smith, “The distribution of  $\ell^\infty$ -Selmer groups in degree  $\ell$  twist families, I”, preprint, 2023. [arXiv 2207.05674](#)
- [Wintner 1942] A. Wintner, “On the prime number theorem”, *Amer. J. Math.* **64** (1942), 320–326. [MR](#) [Zbl](#)

Received May 24, 2023. Revised September 19, 2024.

DANIEL KELIHER  
CONCOURSE PROGRAM  
MASSACHUSETTS INSTITUTE OF TECHNOLOGY  
CAMBRIDGE, MA  
UNITED STATES  
[keliher@mit.edu](mailto:keliher@mit.edu)

# PACIFIC JOURNAL OF MATHEMATICS

Founded in 1951 by E. F. Beckenbach (1906–1982) and F. Wolf (1904–1989)

[msp.org/pjm](http://msp.org/pjm)

## EDITORS

Don Blasius (Managing Editor)  
Department of Mathematics  
University of California  
Los Angeles, CA 90095-1555  
[blasius@math.ucla.edu](mailto:blasius@math.ucla.edu)

Matthias Aschenbrenner  
Fakultät für Mathematik  
Universität Wien  
Vienna, Austria  
[matthias.aschenbrenner@univie.ac.at](mailto:matthias.aschenbrenner@univie.ac.at)

Robert Lipshitz  
Department of Mathematics  
University of Oregon  
Eugene, OR 97403  
[lipshitz@uoregon.edu](mailto:lipshitz@uoregon.edu)

Vyjayanthi Chari  
Department of Mathematics  
University of California  
Riverside, CA 92521-0135  
[chari@math.ucr.edu](mailto:chari@math.ucr.edu)

Kefeng Liu  
Department of Mathematics  
University of California  
Los Angeles, CA 90095-1555  
[liu@math.ucla.edu](mailto:liu@math.ucla.edu)

Ruixiang Zhang  
Department of Mathematics  
University of California  
Berkeley, CA 94720-3840  
[ruixiang@berkeley.edu](mailto:ruixiang@berkeley.edu)

Atsushi Ichino  
Department of Mathematics  
Kyoto University  
Riverside, CA 92521-0135  
[atsushi.ichino@gmail.com](mailto:atsushi.ichino@gmail.com)

Dimitri Shlyakhtenko  
Department of Mathematics  
University of California  
Los Angeles, CA 90095-1555  
[shlyakht@ipam.ucla.edu](mailto:shlyakht@ipam.ucla.edu)

## PRODUCTION

Silvio Levy, Scientific Editor, [production@msp.org](mailto:production@msp.org)

---

See inside back cover or [msp.org/pjm](http://msp.org/pjm) for submission instructions.

---

The subscription price for 2024 is US \$645/year for the electronic version, and \$875/year for print and electronic. Subscriptions, requests for back issues and changes of subscriber address should be sent to Pacific Journal of Mathematics, P.O. Box 4163, Berkeley, CA 94704-0163, U.S.A. The Pacific Journal of Mathematics is indexed by [Mathematical Reviews](#), [Zentralblatt MATH](#), [PASCAL CNRS Index](#), [Referativnyi Zhurnal](#), [Current Mathematical Publications](#) and [Web of Knowledge \(Science Citation Index\)](#).


---

The Pacific Journal of Mathematics (ISSN 1945-5844 electronic, 0030-8730 printed) at the University of California, c/o Department of Mathematics, 798 Evans Hall #3840, Berkeley, CA 94720-3840, is published twelve times a year. Periodical rate postage paid at Berkeley, CA 94704, and additional mailing offices. POSTMASTER: send address changes to Pacific Journal of Mathematics, P.O. Box 4163, Berkeley, CA 94704-0163.

---

PJM peer review and production are managed by EditFLOW® from Mathematical Sciences Publishers.

PUBLISHED BY

 **mathematical sciences publishers**  
nonprofit scientific publishing

<http://msp.org/>

© 2024 Mathematical Sciences Publishers



# PACIFIC JOURNAL OF MATHEMATICS

Volume 331    No. 2    August 2024

---

Long-time behavior of awesome homogeneous Ricci flows	187
ROBERTO ARAUJO	
Sobolev norms of $L^2$ -solutions to the nonlinear Schrödinger equation	217
ROMAN V. BESSONOV and SERGEY A. DENISOV	
Extrinsic polyharmonic maps into the sphere	259
ALI FARDOUN, STEFANO MONTALDO, CEZAR ONICIUC and ANDREA RATTO	
Balanced homogeneous harmonic maps between cones	283
BRIAN FREIDIN	
Rank growth of elliptic curves in $S_4$ - and $A_4$ -quartic extensions of the rationals	331
DANIEL KELIHER	
Obstruction complexes in grid homology	353
YAN TAO	