

# RANK ONE ELLIPTIC CURVES AND RANK STABILITY

DAVID ZYWINA

**ABSTRACT.** For any quadratic extension  $L/K$  of number fields, we prove that there are infinitely many elliptic curves  $E$  over  $K$  so that the abelian groups  $E(K)$  and  $E(L)$  both have rank 1. In particular, there are infinitely many elliptic curves of rank 1 over any number field. This result generalizes theorems of Koymans–Pagano and Alpöge–Bhargava–Ho–Shnidman which were used to independently show that Hilbert’s tenth problem over the ring of integers of any number field has a negative answer. Our approach differs since we are obtaining our elliptic curves by specializing a nonisotrivial rank 1 family of elliptic curves and we compute all the ranks involved.

## 1. INTRODUCTION

Let  $K$  be any number field. For an elliptic curve  $E$  defined over  $K$ , the abelian group  $E(K)$  consisting of the  $K$ -rational points of  $E$  is finitely generated. The **rank** of  $E$  is the rank of the abelian group  $E(K)$ .

A *minimalist conjecture* loosely predicts that if we order elliptic curves over  $K$  by their height, the density of those curves with rank 0 and the density of those curves with rank 1 should both be  $1/2$  (the idea being that a typical curve over  $K$  should have the smallest possibly rank that is compatible with the parity conjecture). In their work on Hilbert’s tenth problem, Mazur and Rubin proved that there are elliptic curves over  $K$  of rank 0, cf. [MR10, Theorem 1.11]. Our first result guarantees the existence of elliptic curves over  $K$  of rank 1.

**Theorem 1.1.** *For any number field  $K$ , there are infinitely many elliptic curves  $E$  over  $K$ , up to isomorphism, of rank 1.*

Theorem 1.1 was already known for  $K = \mathbb{Q}$ , for example see [Sat87, Théorème 3.1] or [BS14], but these methods do not readily extend to a general number field. One also knew that Theorem 1.1 held under various conjectures; for example [MR10, Corollary 1.12] implies the theorem assuming the finiteness of the 2-part of the Tate–Shafarevich group for elliptic curves over number fields. Our proof builds off of the ideas introduced in [Zyw25a] and [Zyw25b]; in the second paper we proved that there are infinitely many elliptic curves over  $\mathbb{Q}$  of rank 2. An independent proof of Theorem 1.1 has been given by Koymans and Pagano [KP25] which extends their earlier techniques from [KP24]; they show that a “generic” elliptic curve over  $K$  with full 2-torsion has infinitely many quadratic twists of rank 1.

Our main result is the stronger rank stability theorem.

**Theorem 1.2.** *For any quadratic extension  $L/K$  of number fields, there are infinitely many elliptic curves  $E$  over  $K$ , up to isomorphism, for which  $\text{rank } E(K) = \text{rank } E(L) = 1$ .*

---

2020 *Mathematics Subject Classification.* Primary 11G18; Secondary 14J27.

The interest in Theorem 1.2 is that it generalizes the following two recent results which both imply that Hilbert's tenth problem for the ring of integers of a number field has a negative answer.

**Theorem 1.3** (Koymans–Pagano [KP24, Theorem 2.4]). *Let  $K$  be a number field with at least 32 real places and define  $L := K(i)$ . Then there are infinitely many elliptic curves  $E$  over  $K$  such that  $\text{rank } E(K) = \text{rank } E(L) > 0$ .*

**Theorem 1.4** (Alpöge–Bhargava–Ho–Shnidman [ABHS25, Theorem 1.1]). *For any quadratic extension  $L/K$  of number fields, there are infinitely many abelian varieties  $A$  over  $K$  such that  $\text{rank } A(K) = \text{rank } A(L) > 0$ .*

The theorems from [KP24] and [ABHS25] are both stated in terms of the existence of such an abelian variety but it is clear from their proofs that they can produce infinitely many. Note that the existence is all that is needed for their application to Hilbert's tenth problem.

**1.1. Our curves.** Our approach to proving Theorem 1.1 is to consider the elliptic curve  $\mathcal{E}$  over the function field  $\mathbb{Q}(T)$  defined by the Weierstrass equation

$$y^2 = x^3 + 4T(T+1)x^2 + 2T(T+1)^2(T-1)x.$$

The discriminant of this Weierstrass model is  $2^9 T^3 (T+1)^7 (T-1)^2$ . The group  $\mathcal{E}(\mathbb{Q}(T))$  contains a 2-torsion point  $(0, 0)$  and a point  $P := (-2T(T+1), 2T(T+1)^2)$  of infinite order.

Consider any number field  $K$ . For each  $t \in K - \{0, 1, -1\}$ , the specialization of  $\mathcal{E}$  at  $t$  is the elliptic curve  $\mathcal{E}_t$  over  $K$  defined by the equation  $y^2 = x^3 + 4t(t+1)x^2 + 2t(t+1)^2(t-1)x$  with a point  $P_t := (-2t(t+1), 2t(t+1)^2) \in \mathcal{E}_t(K)$ . From Silverman [Sil83] we know that the point  $P_t$  will have infinite order for all but finitely many choice of  $t$ . For such  $t$ , we have  $\text{rank } \mathcal{E}_t(K) \geq 1$ . The challenge is to find examples for which equality holds.

Our strategy is to try and choose  $t \in K - \{0, 1, -1\}$  such that an explicit 2-descent will produce the desired upper bound  $\text{rank } \mathcal{E}_t(K) \leq 1$ . To perform a 2-descent we will need to fully understand the bad primes of  $\mathcal{E}_t$ . Taking  $t = a/b$  with  $a, b \in K$  such that  $ab(a+b)(a-b) \neq 0$  and scaling the coordinates of the Weierstrass model appropriately, we find that  $\mathcal{E}_t/K$  can be given by the Weierstrass equation

$$(1.1) \quad y^2 = x^3 + 4a(a+b)x^2 + 2a(a+b)^2(a-b)x$$

which has discriminant  $\Delta = 2^9 a^3 (a+b)^7 (a-b)^2$ .

**1.2. Technical result.** For a finite set  $S$  of nonzero prime ideals of  $\mathcal{O}_K$ , we will denote by  $\mathcal{O}_{K,S}$  the ring of  $S$ -integers in  $K$ . The main task of this paper is to prove the following.

**Theorem 1.5.** *Let  $K$  be a number field and fix a  $D \in K$  that is not a square. There is a finite set  $S$  of nonzero prime ideals of  $\mathcal{O}_K$  and a nonempty open subset  $U_{\mathfrak{p}}$  of  $K_{\mathfrak{p}}^2$  for each  $\mathfrak{p} \in S$  such that if  $a$  and  $b$  are elements of  $\mathcal{O}_{K,S}$  that satisfy the following conditions:*

- $a$ ,  $a+b$  and  $a-b$  generate distinct nonzero prime ideals of  $\mathcal{O}_{K,S}$ ,
- $(a, b)$  lies in  $U_{\mathfrak{p}}$  for all  $\mathfrak{p} \in S$ ,
- $0 < a < b$  in  $K_v$  for all real places  $v$  of  $K$ ,

*then the elliptic curve over  $K$  defined by (1.1) has rank 1 and its quadratic twist by  $D$  has rank 0.*

The key idea of Theorem 1.5 is that the sets  $U_{\mathfrak{p}}$  are forcing very specific local conditions when performing the relevant 2-descents. The sets  $S$  and  $U_{\mathfrak{p}}$  in our proof will be a little complicated but the general philosophy is that we are reverse engineering a successful 2-descent.

In order to find  $a$  and  $b$  satisfying the conditions of Theorem 1.5, we will use a result of Kai [Kai25, Proposition 13.2] which generalizes work of Green, Tao and Ziegler to number fields. With this result of Kai, we will see that Theorems 1.1 and 1.2 are easy consequences of Theorem 1.5. The work of Kai also shows up in the proofs of Theorem 1.3 and 1.4. Since we are interested in primes in a 3-term arithmetic progression  $a - b, a, a + b$ , it seems likely that one could also use classical analytic number theory as in [ABHS25, §3] to prove the existence of  $a$  and  $b$ .

**1.3. Notation.** Let  $K$  be a number field and let  $\mathcal{O}_K$  be its ring of integers. For each nonzero prime ideal  $\mathfrak{p}$  of  $\mathcal{O}_K$ , let  $v_{\mathfrak{p}}$  be the discrete valuation on  $K$  normalized so that  $v_{\mathfrak{p}}(K^{\times}) = \mathbb{Z}$ . Let  $|\cdot|_{\mathfrak{p}}$  be the absolute value on  $K$  for which  $|a|_{\mathfrak{p}} = |\mathcal{O}_K/\mathfrak{p}|^{-v_{\mathfrak{p}}(a)}$ . Let  $K_{\mathfrak{p}}$  be the  $\mathfrak{p}$ -adic completion of  $K$  and let  $\mathcal{O}_{\mathfrak{p}}$  be its valuation ring.

For a finite set  $S$  of nonzero prime ideals of  $\mathcal{O}_K$ , let  $\mathcal{O}_{K,S}$  be the ring of  $S$ -integers, i.e., the ring of  $a \in K$  for which  $v_{\mathfrak{p}}(a) \geq 0$  for all nonzero prime ideals  $\mathfrak{p} \notin S$  of  $\mathcal{O}_K$ .

For a place  $v$  of  $K$ , we denote by  $K_v$  the completion of  $K$  at  $v$ . When  $v$  is a finite place of  $K$ , we will frequently switch between  $v$  and the corresponding prime ideal  $\mathfrak{p}$  of  $\mathcal{O}_K$ .

## 2. 2-DESCENT BACKGROUND

Fix a number field  $K$ . In this section we recall the Selmer group associated to a degree 2 isogeny of an elliptic curve over  $K$ . We also compute the local relations that will be needed for our Selmer group calculations.

**2.1. 2-descent background.** We first recall some background on descent via a 2-isogeny. See [Sil09, §X.4], and in particular [Sil09, §X.4 Example 4.8], for details.

Let  $E$  be an elliptic curve over a number field  $K$  given by a Weierstrass equation  $y^2 = x^3 + \alpha x^2 + \beta x$  with  $\alpha, \beta \in K$ . Let  $E'/K$  be the elliptic curve defined by  $y^2 = x^3 + \alpha' x^2 + \beta' x$ , where  $\alpha' := -2\alpha$  and  $\beta' := \alpha^2 - 4\beta$ . There is a degree 2 isogeny  $\phi: E \rightarrow E'$  given by  $\phi(x, y) = (y^2/x^2, y(\beta - x^2)/x^2)$ . Let  $\hat{\phi}: E' \rightarrow E$  be the dual isogeny of  $\phi$ . The kernel of  $\phi$  and the kernel of  $\hat{\phi}$  are generated by the 2-torsion point  $(0, 0)$  of  $E$  and  $E'$ , respectively.

Set  $\text{Gal}_K := \text{Gal}(\bar{K}/K)$ . Starting with the short exact sequence  $0 \rightarrow \ker \phi \rightarrow E \xrightarrow{\phi} E' \rightarrow 0$  and taking Galois cohomology yields an exact sequence

$$0 \rightarrow \ker \phi \rightarrow E(K) \xrightarrow{\phi} E'(K) \xrightarrow{\delta} H^1(\text{Gal}_K, \ker \phi).$$

Since  $\ker \phi$  and  $\{\pm 1\}$  are isomorphic  $\text{Gal}_K$ -modules, we have a natural isomorphism

$$(2.1) \quad H^1(\text{Gal}_K, \ker \phi) \xrightarrow{\sim} H^1(\text{Gal}_K, \{\pm 1\}) \xrightarrow{\sim} K^{\times}/(K^{\times})^2.$$

Using the isomorphism (2.1), we may view  $\delta$  as a homomorphism

$$\delta: E'(K) \rightarrow K^{\times}/(K^{\times})^2$$

whose kernel is  $\phi(E(K))$ . For any point  $(x, y) \in E'(K) - \{0, (0, 0)\}$ , we have  $\delta((x, y)) = x \cdot (K^{\times})^2$ . We also have  $\delta(0) = 1$  and  $\delta((0, 0)) = \beta' \cdot (K^{\times})^2$ .

For each place  $v$  of  $K$ , a similar construction defines a homomorphism

$$\delta_v: E'(K_v) \rightarrow K_v^\times / (K_v^\times)^2$$

with kernel  $\phi(E(K_v))$ . We can identify the  $\phi$ -Selmer group of  $E/K$ , which we denote by  $\text{Sel}_\phi(E/K)$ , with the subgroup of  $K^\times / (K^\times)^2$  consisting of those square classes whose image in  $K_v^\times / (K_v^\times)^2$  lies in  $\text{Im}(\delta_v)$  for all places  $v$  of  $K$ . The image of  $\delta$  lies in  $\text{Sel}_\phi(E/K)$  and hence we have an injective homomorphism

$$E'(K)/\phi(E(K)) \hookrightarrow \text{Sel}_\phi(E/K).$$

Similar, we have an injective homomorphism  $E(K)/\hat{\phi}(E'(K)) \hookrightarrow \text{Sel}_{\hat{\phi}}(E'/K)$ . These groups will help us understand the rank of  $E$  via the exact sequence

$$(2.2) \quad 0 \rightarrow \frac{\langle (0,0) \rangle}{\phi(E(K)[2])} \rightarrow \frac{E'(K)}{\phi(E(K))} \xrightarrow{\hat{\phi}} \frac{E(K)}{2E(K)} \rightarrow \frac{E(K)}{\hat{\phi}(E'(K))} \rightarrow 0.$$

The following lemma links the cardinalities of  $\text{Sel}_\phi(E/K)$  and  $\text{Sel}_{\hat{\phi}}(E'/K)$ .

**Lemma 2.1.**

- (i) We have  $|\text{Sel}_\phi(E/K)|/|\text{Sel}_{\hat{\phi}}(E'/K)| = \prod_v \frac{1}{2} |\text{Im}(\delta_v)|$ , where the product is over the places  $v$  of  $K$ .
- (ii) Let  $\mathfrak{p}$  be a nonzero prime ideal of  $\mathcal{O}_K$  that does not divide 2. Then

$$\frac{1}{2} |\text{Im}(\delta_{\mathfrak{p}})| = c_{\mathfrak{p}}(E')/c_{\mathfrak{p}}(E),$$

where  $c_{\mathfrak{p}}(E)$  and  $c_{\mathfrak{p}}(E')$  are the Tamagawa numbers of  $E$  and  $E'$ , respectively, at  $\mathfrak{p}$ .

- (iii) If  $v$  is a real place of  $K$  and  $\beta < 0$  in  $K_v$ , then  $\text{Im}(\delta_v) = 1$ .

*Proof.* For each place  $v$  of  $K$ , let  $\phi_v: E(K_v) \rightarrow E'(K_v)$  be the homomorphism obtained from the isogeny  $\phi$ . Define  $T(E/E') := \prod_v |\text{coker}(\phi_v)|/|\text{ker}(\phi_v)|$ , where the product is over the places  $v$  of  $K$ . From [Cas65, Lemma 3.1 and equation (3.6)], we find that all but finitely many terms of the product  $T(E/E')$  are 1 and hence  $T(E/E')$  is well-defined. Note that our product is the inverse of Cassels' but our notation is compatible by equation (1.23) of [Cas65]. By Theorem 1.1 of [Cas65], we have

$$T(E/E') = \frac{|\text{Sel}_\phi(E/K)|}{|\text{Sel}_{\hat{\phi}}(E'/K)|} \cdot \frac{|\text{ker}(\hat{\phi})(K)|}{|\text{ker}(\phi)(K)|} = \frac{|\text{Sel}_\phi(E/K)|}{|\text{Sel}_{\hat{\phi}}(E'/K)|}.$$

From our two expressions for  $T(E/E')$ , we find that  $|\text{Sel}_\phi(E/K)|/|\text{Sel}_{\hat{\phi}}(E'/K)| = \prod_v \tau_v$ , where  $\tau_v := |\text{coker}(\phi_v)|/|\text{ker}(\phi_v)|$ . We have  $\tau_v = \frac{1}{2} |\text{Im}(\delta_v)|$  since  $\text{ker}(\phi_v) = \langle (0,0) \rangle$  and  $\text{Im}(\delta_v) \cong E'(K_v)/\phi(E(K_v))$ . This completes the proof of (i).

Fix a nonzero prime ideal  $\mathfrak{p} \nmid 2$  of  $\mathcal{O}_K$ . For a nonsingular Weierstrass model  $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$  over  $K$ , we have a corresponding invariant differential  $dx/(2y + a_1x + a_3)$  on the elliptic curve defined by this model. Let  $\omega$  be an invariant differential on  $E$  arising from a Weierstrass model of  $E$  that is minimal at  $\mathfrak{p}$ . Let  $\omega'$  be an invariant differential on  $E'$  arising from a Weierstrass model of  $E'$  that is minimal at  $\mathfrak{p}$ . There is a unique  $\alpha \in K^\times$  such that  $\phi^*\omega' = \alpha\omega$ . By [DD15, Lemma 4.2], we have

$$\frac{1}{2} |\text{Im}(\delta_{\mathfrak{p}})| = \frac{|\text{coker}(\phi_{\mathfrak{p}})|}{|\text{ker}(\phi_{\mathfrak{p}})|} = |\alpha|_{\mathfrak{p}}^{-1} \frac{c_{\mathfrak{p}}(E')}{c_{\mathfrak{p}}(E)}.$$

Since  $\mathfrak{p} \nmid 2 = \deg \phi$ , [DD15, Lemma 4.3] implies that  $|\alpha|_{\mathfrak{p}}^{-1} = 1$  which proves (ii).

Finally fix a real place  $v$  of  $K$  for which  $\beta < 0$ . We have  $\tau_v = 1/2$  by [DD15, Proposition 7.6]. Therefore,  $|\text{Im}(\delta_v)| = 2\tau_v = 1$  and (iii) follows.  $\square$

**2.2. Our curves and local conditions.** Fix  $a, b \in K$  such that  $ab(a+b)(a-b) \neq 0$ . Take any  $d \in K^\times$  and let  $E_d$  be the elliptic curve over  $K$  defined by the Weierstrass equation

$$(2.3) \quad y^2 = x^3 + 4a(a+b)dx^2 + 2a(a+b)^2(a-b)d^2x;$$

its discriminant is  $\Delta_d := 2^9 a^3(a+b)^7(a-b)^2 \cdot d^6 \neq 0$ . From §2.1, there is a degree 2 isogeny  $\phi_d: E_d \rightarrow E'_d$  with  $\phi_d((0,0)) = 0$ , where  $E'_d$  is the elliptic curve over  $K$  defined by the Weierstrass equation

$$(2.4) \quad y^2 = x^3 - 8a(a+b)dx^2 + 8a(a+b)^3d^2x.$$

The discriminant of the Weierstrass model (2.4) is  $\Delta'_d := 2^{15} a^3(a+b)^8(a-b) \cdot d^6$ . As in §2.1, we have a homomorphism

$$\delta_{d,v}: E'_d(K_v) \rightarrow K_v^\times / (K_v^\times)^2$$

with kernel  $\phi(E_d(K_v))$  for every place  $v$  of  $K$ .

We now describe the image of  $\delta_{d,v}$  in various cases that will arise in our proof of the main theorems. For each nonzero prime ideal  $\mathfrak{p}$  of  $\mathcal{O}_K$ , we have an inclusion  $\mathcal{O}_\mathfrak{p}^\times / (\mathcal{O}_\mathfrak{p}^\times)^2 \hookrightarrow K_\mathfrak{p}^\times / (K_\mathfrak{p}^\times)^2$ .

**Lemma 2.2.** *Let  $\mathfrak{p}$  be a prime ideal of  $\mathcal{O}_K$  with  $v_\mathfrak{p}(2) = v_\mathfrak{p}(d) = 0$ . Define*

$$m := (v_\mathfrak{p}(a), v_\mathfrak{p}(a+b), v_\mathfrak{p}(a-b)).$$

- (i) *If  $m = (0, 0, 0)$ , then  $\text{Im}(\delta_{d,\mathfrak{p}}) = \mathcal{O}_\mathfrak{p}^\times / (\mathcal{O}_\mathfrak{p}^\times)^2$  and hence  $|\text{Im}(\delta_{d,\mathfrak{p}})| = 2$ .*
- (ii) *If  $m = (0, 0, 1)$ , then  $|\text{Im}(\delta_{d,\mathfrak{p}})| = 1$ .*
- (iii) *If  $m = (1, 0, 0)$ , then  $|\text{Im}(\delta_{d,\mathfrak{p}})| = 2$  and  $\text{Im}(\delta_{d,\mathfrak{p}}) \neq \mathcal{O}_\mathfrak{p}^\times / (\mathcal{O}_\mathfrak{p}^\times)^2$ .*
- (iv) *If  $m = (0, 1, 0)$  and  $d$  is a square in  $K_\mathfrak{p}$ , then  $|\text{Im}(\delta_{d,\mathfrak{p}})| = 2$ .*
- (v) *If  $m = (0, 1, 0)$  and  $d$  is not a square in  $K_\mathfrak{p}$ , then  $|\text{Im}(\delta_{d,\mathfrak{p}})| = 4$ .*
- (vi) *If  $m = (-1, 1, -1)$  and  $-2a(a+b)d$  is a square in  $K_\mathfrak{p}$ , then  $|\text{Im}(\delta_{d,\mathfrak{p}})| = 4$ .*
- (vii) *If  $m = (-1, 1, -1)$  and  $-2a(a+b)d$  is not a square in  $K_\mathfrak{p}$ , then  $|\text{Im}(\delta_{d,\mathfrak{p}})| = 2$ .*
- (viii) *If  $m = (0, 2, 0)$  and  $-2a(a+b)d$  is a square in  $K_\mathfrak{p}$ , then  $|\text{Im}(\delta_{d,\mathfrak{p}})| = 4$ .*
- (ix) *If  $m = (0, 2, 0)$  and  $-2a(a+b)d$  is not a square in  $K_\mathfrak{p}$ , then  $|\text{Im}(\delta_{d,\mathfrak{p}})| = 2$ .*

*Proof.* By Lemma 2.1(ii), we have  $|\text{Im}(\delta_{d,\mathfrak{p}})| = 2c_\mathfrak{p}(E'_d)/c_\mathfrak{p}(E_d)$ . We now compute these Tamagawa numbers by using Tate's algorithm, cf. [Sil94, Algorithm 9.4]. The applications of Tate's algorithm below are straightforward; in each case, we give a specific Weierstrass model that is minimal at  $\mathfrak{p}$  for which the algorithm can be applied directly as in [Sil94, Algorithm 9.4] without having to change the model.

First consider the case  $m = (0, 0, 0)$ . Since  $E_d$  and  $E'_d$  have good reduction at  $\mathfrak{p}$ , we have  $|\text{Im}(\delta_{d,\mathfrak{p}})| = 2c_\mathfrak{p}(E'_d)/c_\mathfrak{p}(E_d) = 2 \cdot 1/1 = 2$ . We have  $\delta_{d,\mathfrak{p}}((0,0)) = 2a(a+b) \cdot (K_\mathfrak{p}^\times)^2$  and  $2a(a+b) \in \mathcal{O}_\mathfrak{p}^\times$ . Now take any point  $(x, y) \in E'_d(K_\mathfrak{p}) - \{0, (0,0)\}$ . Since  $\delta_{d,\mathfrak{p}}((x, y)) = x \cdot (K_\mathfrak{p}^\times)^2$ , to complete the proof of (i) it suffices to show that  $v_\mathfrak{p}(x)$  is even. Since  $v_\mathfrak{p}(2) = v_\mathfrak{p}(a) = v_\mathfrak{p}(a+b) = 0$ , from (2.4) we find that  $2v_\mathfrak{p}(y) = v_\mathfrak{p}(y^2) = v_\mathfrak{p}(x)$  if  $v_\mathfrak{p}(x) > 0$  and  $2v_\mathfrak{p}(y) = v_\mathfrak{p}(y^2) = 3v_\mathfrak{p}(x)$  if  $v_\mathfrak{p}(x) < 0$ . Therefore,  $v_\mathfrak{p}(x)$  must be even.

Consider the case  $m = (0, 0, 1)$ . We have  $v_\mathfrak{p}(\Delta_d) = 2$  and  $v_\mathfrak{p}(\Delta'_d) = 1$ . Applying Tate's algorithm with (2.3) we find that  $E_d$  has Kodaira symbol  $I_2$  at  $\mathfrak{p}$  and hence  $c_\mathfrak{p}(E_d) = 2$ .

Replacing  $x$  by  $x + 4a(a+b)d$  in the model (2.4), we obtain another Weierstrass model

$$y^2 = x^3 + 4a(a+b)dx^2 - 8a(a+b)^2(a-b)d^2x - 32a^2(a+b)^3(a-b)d^3$$

for  $E'_d$ . Applying Tate's algorithm to this model, we find that  $E'_d$  has Kodaira symbol  $I_1$  at  $\mathfrak{p}$  and hence  $c_{\mathfrak{p}}(E'_d) = 1$ . Therefore,  $|\text{Im}(\delta_{d,\mathfrak{p}})| = 2 \cdot 1/2 = 1$ .

Consider the case  $m = (1, 0, 0)$ . Note that  $a$  is a uniformizer of  $K_{\mathfrak{p}}$ . Applying Tate's algorithm with (2.3) and (2.4), we find that  $E_d$  and  $E'_d$  both have Kodaira symbol III at  $\mathfrak{p}$  and hence  $c_{\mathfrak{p}}(E_d) = c_{\mathfrak{p}}(E'_d) = 2$ . Therefore,  $|\text{Im}(\delta_{d,\mathfrak{p}})| = 2 \cdot 2/2 = 2$ . We have  $\text{Im}(\delta_{d,\mathfrak{p}}) \neq \mathcal{O}_{\mathfrak{p}}^{\times}/(\mathcal{O}_{\mathfrak{p}}^{\times})^2$  since  $\delta_{d,\mathfrak{p}}((0,0)) = 2a(a+b) \cdot (K_{\mathfrak{p}}^{\times})^2$  and  $v_{\mathfrak{p}}(2a(a+b)) = 1$ .

Consider the case  $m = (0, 1, 0)$ . Note that  $a+b$  is a uniformizer of  $K_{\mathfrak{p}}$ . Replacing  $x$  by  $x - 2a(a+b)d$  in the model (2.3), we obtain another Weierstrass model

$$(2.5) \quad y^2 = x^3 - 2a(a+b)dx^2 - 2a(a+b)^3d^2x + 4a^2(a+b)^4d^3$$

for  $E_d$ . Applying Tate's algorithm to this model and using  $v_{\mathfrak{p}}(\Delta_d) = 7$ , we find that  $E_d$  has Kodaira symbol  $I_1^*$  at  $\mathfrak{p}$  with  $c_{\mathfrak{p}}(E_d) = 4$  if  $d$  is a square in  $K_{\mathfrak{p}}$  and  $c_{\mathfrak{p}}(E_d) = 2$  otherwise. Applying Tate's algorithm with (2.4) and using  $v_{\mathfrak{p}}(\Delta'_d) = 8$ , we find that  $E'_d$  has Kodaira symbol  $I_2^*$  at  $\mathfrak{p}$  with  $c_{\mathfrak{p}}(E'_d) = 4$ . Therefore,  $|\text{Im}(\delta_{d,\mathfrak{p}})|$  is equal to  $2 \cdot 4/4 = 2$  if  $d$  is a square in  $K_{\mathfrak{p}}$  and is equal to  $2 \cdot 4/2 = 4$  otherwise.

Consider the case where  $m = (-1, 1, -1)$ . Applying Tate's algorithm to the model (2.5) for  $E_d$ , and using  $v_{\mathfrak{p}}(\Delta) = 2$ ,  $v_{\mathfrak{p}}(2a(a+b)) = 0$  and  $v_{\mathfrak{p}}(2a(a+b)^3) = v_{\mathfrak{p}}(4a^2(a+b)^4) = 2$ , we find that  $E_d$  has Kodaira symbol  $I_2$  at  $\mathfrak{p}$  and hence  $c_{\mathfrak{p}}(E_d) = 2$ . Using that  $v_{\mathfrak{p}}(\Delta'_d) = 4$ ,  $v_{\mathfrak{p}}(8a(a+b)) = 0$  and  $v_{\mathfrak{p}}(8a(a+b)^3) = 2$ , Tate's algorithm applied to (2.4) shows that  $E'_d$  has Kodaira symbol  $I_4$  at  $\mathfrak{p}$  and has split multiplication at  $\mathfrak{p}$  if and only if  $-2a(a+b)d$  is a square in  $K_{\mathfrak{p}}$ . Therefore,  $c_{\mathfrak{p}}(E'_d) = 4$  if  $-2a(a+b)d$  is a square in  $K_{\mathfrak{p}}$  and  $c_{\mathfrak{p}}(E'_d) = 2$  otherwise. Therefore,  $|\text{Im}(\delta_{d,\mathfrak{p}})|$  is equal to  $2 \cdot 4/2 = 4$  if  $-2a(a+b)d$  is a square in  $K_{\mathfrak{p}}$  and is equal to  $2 \cdot 2/2 = 2$  otherwise.

Consider the case  $m = (0, 2, 0)$ . Fix a uniformizer  $\pi$  of  $K_{\mathfrak{p}}$ . Dividing both sides of (2.5) by  $\pi^6$  and changing coordinates we obtain a model

$$(2.6) \quad y^2 = x^3 - 2a\left(\frac{a+b}{\pi^2}\right)dx^2 - 2a\left(\frac{a+b}{\pi^2}\right)^3\pi^2d^2x + 4a^2\left(\frac{a+b}{\pi^2}\right)^4\pi^2d^3$$

for  $E_d$ . The Weierstrass equation (2.6) has coefficients in  $\mathcal{O}_{\mathfrak{p}}$  with  $-2a\left(\frac{a+b}{\pi^2}\right)d \in \mathcal{O}_{\mathfrak{p}}^{\times}$  and its discriminant is  $2^9a^3(a+b)^7(a-b)^2d^6/\pi^{12}$  which has  $\mathfrak{p}$ -adic valuation 2. Tate's algorithm shows that  $E_d$  has Kodaira symbol  $I_2$  at  $\mathfrak{p}$  and hence  $c_{\mathfrak{p}}(E) = 2$ . Dividing both sides of (2.4) by  $\pi^6$  and changing coordinates we obtain a model

$$(2.7) \quad y^2 = x^3 - 8a\left(\frac{a+b}{\pi^2}\right)dx^2 + 8a\left(\frac{a+b}{\pi^2}\right)^3\pi^2d^2x.$$

for  $E_d$ . The Weierstrass equation (2.7) has coefficients in  $\mathcal{O}_{\mathfrak{p}}$  with  $-8a\left(\frac{a+b}{\pi^2}\right)d \in \mathcal{O}_{\mathfrak{p}}^{\times}$  and its discriminant is  $2^{15}a^3(a+b)^8(a-b)d^6/\pi^{12}$  which has  $\mathfrak{p}$ -adic valuation 4. Tate's algorithm shows that  $E_d$  has Kodaira symbol  $I_4$  at  $\mathfrak{p}$  and has split multiplicative reduction at  $\mathfrak{p}$  if and only if  $-2a(a+b)d$  is a square in  $K_{\mathfrak{p}}$ . Therefore,  $c_{\mathfrak{p}}(E') = 4$  if  $-2a(a+b)d$  is a square in  $K_{\mathfrak{p}}$  and  $c_{\mathfrak{p}}(E') = 2$  otherwise. Therefore,  $|\text{Im}(\delta_{d,\mathfrak{p}})|$  is equal to  $2 \cdot 4/2 = 4$  if  $-2a(a+b)d$  is a square in  $K_{\mathfrak{p}}$  and is equal to  $2 \cdot 2/2 = 2$  otherwise.  $\square$

The following easy lemma will be used later to ensure that the local conditions we impose can be satisfied.

**Lemma 2.3.** *Let  $\mathfrak{p} \nmid 2$  be a nonzero prime ideal of  $\mathcal{O}_K$  and fix a uniformizer  $\omega$  of  $K_{\mathfrak{p}}$ .*



- (i) *There are  $a, b \in K_{\mathfrak{p}}^{\times}$  such that  $(v_{\mathfrak{p}}(a), v_{\mathfrak{p}}(a+b), v_{\mathfrak{p}}(a-b)) = (0, 1, 0)$ .*
- (ii) *There are  $a, b \in K_{\mathfrak{p}}^{\times}$  such that  $(v_{\mathfrak{p}}(a), v_{\mathfrak{p}}(a+b), v_{\mathfrak{p}}(a-b)) = (-1, 1, -1)$ ,  $-2a(a+b)$  is a square in  $K_{\mathfrak{p}}$ , and  $(a-b)\omega$  is a square in  $K_{\mathfrak{p}}$ .*
- (iii) *There are  $a, b \in K_{\mathfrak{p}}^{\times}$  such that  $(v_{\mathfrak{p}}(a), v_{\mathfrak{p}}(a+b), v_{\mathfrak{p}}(a-b)) = (-1, 1, -1)$ ,  $-2a(a+b)$  is a square in  $K_{\mathfrak{p}}$ , and  $(a-b)\omega$  is not a square in  $K_{\mathfrak{p}}$ .*
- (iv) *There are  $a, b \in K_{\mathfrak{p}}^{\times}$  such that  $(v_{\mathfrak{p}}(a), v_{\mathfrak{p}}(a+b), v_{\mathfrak{p}}(a-b)) = (0, 2, 0)$  and  $-2a(a+b)$  is a square in  $K_{\mathfrak{p}}$ .*
- (v) *There are  $a, b \in K_{\mathfrak{p}}^{\times}$  such that  $(v_{\mathfrak{p}}(a), v_{\mathfrak{p}}(a+b), v_{\mathfrak{p}}(a-b)) = (0, 0, 1)$  and  $a$  is not a square in  $K_{\mathfrak{p}}$ .*

*Proof.* For (i), we can take  $(a, b) = (1, -1 - \omega)$ . For (ii) and (iii), we can take  $(a, b) = (\frac{1}{2}u\omega^{-1}, -\frac{1}{2}u\omega^{-1} - u^{-1}\omega)$  with  $u \in \mathcal{O}_{\mathfrak{p}}^{\times}$ ;  $(a-b)\omega$  is a square in  $K_{\mathfrak{p}}$  if and only if  $u$  is a square modulo  $\mathfrak{p}$ . For (iv), we can take  $(a, b) = (1, -1 - \frac{1}{2}\omega^2)$ . For (v), we can take  $(a, b) = (u, u + \omega)$  where  $u \in \mathcal{O}_{\mathfrak{p}}^{\times}$  is not a square modulo  $\mathfrak{p}$ .  $\square$

### 3. PROOF OF THEOREM 1.5

Define  $L := K(\sqrt{D})$ ; it is a quadratic extension of  $K$ . Let  $S_0$  be a finite set of nonzero prime ideals of  $\mathcal{O}_K$  that contains all those that divide 2, are ramified in  $L$  or satisfy  $v_{\mathfrak{p}}(D) \neq 0$ . By increasing the finite set  $S_0$  appropriately, we may assume that  $\mathcal{O}_{K, S_0}$  is a PID. For a nonzero prime ideal  $\mathfrak{p} \notin S_0$  of  $\mathcal{O}_K$ ,  $D$  is a square in  $K_{\mathfrak{p}}$  if and only if  $\mathfrak{p}$  splits in  $L$ .

Let  $\mathfrak{n}$  be the conductor of the abelian extension  $L/K$  and let  $\mathfrak{n}_0 \subseteq \mathcal{O}_K$  be the corresponding integral ideal. The prime ideals of  $\mathcal{O}_K$  that divide  $\mathfrak{n}_0$  are precisely those that are ramified in  $L$ . Let  $\text{Cl}_K^{\mathfrak{n}}$  be the ray class group for the modulus  $\mathfrak{n}$ . By class field theory, there is a unique group homomorphism

$$\psi: \text{Cl}_K^{\mathfrak{n}} \rightarrow \{\pm 1\}$$

such that for any nonzero prime ideal  $\mathfrak{p} \nmid \mathfrak{n}_0$  of  $\mathcal{O}_K$  we have  $\psi([\mathfrak{p}]) = 1$  if and only if  $\mathfrak{p}$  splits in  $L$ .

Let  $S_{\infty}$  be the set of infinite places of  $K$ .

**3.1. The curves.** Consider fixed  $a, b \in K$  for which  $ab(a+b)(a-b) \neq 0$  and hence  $a$ ,  $a+b$  and  $a-b$  are distinct and nonzero. Recall that for  $d \in K^{\times}$ , we defined an elliptic curve  $E_d$  over  $K$  by

$$(3.1) \quad y^2 = x^3 + 4a(a+b)dx^2 + 2a(a+b)^2(a-b)d^2x.$$

From §2.1, there is a degree 2 isogeny  $\phi_d: E_d \rightarrow E'_d$  with  $\phi_d((0, 0)) = 0$ , where  $E'_d$  is the elliptic curve over  $K$  defined by the Weierstrass equation

$$(3.2) \quad y^2 = x^3 - 8a(a+b)dx^2 + 8a(a+b)^3d^2x.$$

For each place  $v$  of  $K$ , we have a homomorphism

$$\delta_{d,v}: E'_d(K_v) \rightarrow K_v^{\times} / (K_v^{\times})^2$$

as in in §2.2 with kernel  $\phi_d(E_d(K_v))$ . For our proof, we will be interested in the case where  $d$  is either 1 or  $D$ . Note that  $a$  and  $b$  are implicit in the notation  $E_d$  and  $\delta_{d,v}$ .

**3.2. The set of primes  $S$ .** In this section, we construct a finite set  $S$  of nonzero prime ideals of  $\mathcal{O}_K$  and a nonempty open subset  $U_{\mathfrak{p}}$  of  $K_{\mathfrak{p}}^2$  for each  $\mathfrak{p} \in S$ . For each  $\mathfrak{p} \in S$ , we will also construct subgroups  $\Phi_{1,\mathfrak{p}}$  and  $\Phi_{D,\mathfrak{p}}$  of  $K_{\mathfrak{p}}^{\times}/(K_{\mathfrak{p}}^{\times})^2$ . The complicated choices in this section are motivated by the explicit 2-descent computations that will be done later on (see especially Lemmas 3.9 and 3.10).

For each infinite place  $v \in S_{\infty}$ , we define  $\Phi_{1,v}$  and  $\Phi_{D,v}$  to be the trivial subgroup of  $K_v^{\times}/(K_v^{\times})^2$ .

**Lemma 3.1.** *There is a finite set  $S_1$  of nonzero prime ideals of  $\mathcal{O}_K$  disjoint from  $S_0$  such that for each  $\mathfrak{p} \in S_0 \cup S_1$  we have a nonempty open subset  $U_{\mathfrak{p}}$  of  $K_{\mathfrak{p}}^2$  and subgroups  $\Phi_{1,\mathfrak{p}}$  and  $\Phi_{D,\mathfrak{p}}$  of  $K_{\mathfrak{p}}^{\times}/(K_{\mathfrak{p}}^{\times})^2$  for which the following hold:*

- (a) *If  $(a, b) \in K^2$  lies in  $U_{\mathfrak{p}}$  for a prime ideal  $\mathfrak{p} \in S_0 \cup S_1$ , then  $ab(a+b)(a-b) \neq 0$  and we have*

$$\text{Im}(\delta_{1,\mathfrak{p}}) = \Phi_{1,\mathfrak{p}} \quad \text{and} \quad \text{Im}(\delta_{D,\mathfrak{p}}) = \Phi_{D,\mathfrak{p}}.$$

*Note that  $\delta_{1,\mathfrak{p}}$  and  $\delta_{D,\mathfrak{p}}$  depend on  $(a, b)$  while the groups  $\Phi_{1,\mathfrak{p}}$  and  $\Phi_{D,\mathfrak{p}}$  do not.*

- (b) *For all  $\mathfrak{p} \in S_0 \cup S_1$  and  $(a, b) \in U_{\mathfrak{p}}$ , the integers  $v_{\mathfrak{p}}(a)$ ,  $v_{\mathfrak{p}}(a+b)$  and  $v_{\mathfrak{p}}(a-b)$  do not depend on the choice of  $(a, b)$ .*  
(c) *For  $\mathfrak{p} \in S_0$  and  $(a, b) \in U_{\mathfrak{p}}$ , we have  $v_{\mathfrak{p}}(a) = v_{\mathfrak{p}}(a+b) = v_{\mathfrak{p}}(a-b) = 0$ .*  
(d) *If  $(a, b) \in K^2$  lies in  $U_{\mathfrak{p}}$  for all  $\mathfrak{p} \in S_0$ , then  $a+b \in 1 + \mathfrak{n}_0\mathcal{O}_{\mathfrak{p}}$  for all prime ideals  $\mathfrak{p} | \mathfrak{n}_0$ .*  
(e) *If  $(a, b) \in K^2$  lies in  $U_{\mathfrak{p}}$  for all  $\mathfrak{p} \in S_1$ , then*

$$\sum_{\mathfrak{p} \in S_1, \mathfrak{p} \text{ inert in } L} v_{\mathfrak{p}}(a+b) \equiv 1 \pmod{2}.$$

- (f) *We have  $\prod_{\mathfrak{p} \in S_0 \cup S_1} |\Phi_{1,\mathfrak{p}}| = \prod_{\mathfrak{p} \in S_0 \cup S_1} |\Phi_{D,\mathfrak{p}}|$ .*  
(g) *For  $d \in \{1, D\}$ , the images of the groups*

$$\mathcal{O}_{K, S_0 \cup S_1}^{\times}, \quad \prod_{v \in S_0 \cup S_1 \cup S_{\infty}} \Phi_{d,v} \quad \text{and} \quad \prod_{v \in S_0 \cup S_{\infty}} \{1\} \times \prod_{v \in S_1} \mathcal{O}_v^{\times}$$

*in  $\prod_{v \in S_0 \cup S_1 \cup S_{\infty}} K_v^{\times}/(K_v^{\times})^2$  generate  $\prod_{v \in S_0 \cup S_1 \cup S_{\infty}} K_v^{\times}/(K_v^{\times})^2$ .*

*Proof.* Consider a nonzero prime ideal  $\mathfrak{p}$  of  $\mathcal{O}_K$  and a choice of  $a_{\mathfrak{p}}, b_{\mathfrak{p}} \in K_v$  with  $a_{\mathfrak{p}}b_{\mathfrak{p}}(a_{\mathfrak{p}} + b_{\mathfrak{p}})(a_{\mathfrak{p}} - b_{\mathfrak{p}}) \neq 0$ . For a fixed real number  $\epsilon_{\mathfrak{p}} > 0$ , we define the open subset

$$U_{\mathfrak{p}} := \{(a, b) \in K_{\mathfrak{p}}^2 : |a - a_{\mathfrak{p}}|_{\mathfrak{p}} < \epsilon_{\mathfrak{p}}, |b - b_{\mathfrak{p}}|_{\mathfrak{p}} < \epsilon_{\mathfrak{p}}\}$$

of  $K_{\mathfrak{p}}^2$ . By taking  $\epsilon_{\mathfrak{p}} > 0$  sufficiently small, we may assume that  $ab(a-b)(a+b) \neq 0$  for all  $(a, b) \in U_{\mathfrak{p}}$ . We may also take  $\epsilon_{\mathfrak{p}} > 0$  sufficiently small so that the  $\mathfrak{p}$ -adic valuations of  $a$ ,  $a+b$  and  $a-b$  do not depend on the choice of  $(a, b) \in U_{\mathfrak{p}}$ . For each  $d \in \{1, D\}$  and  $(a, b) \in U_{\mathfrak{p}}$ , we obtain an elliptic curve  $E'_{d,(a,b)}$  over  $K_{\mathfrak{p}}$  defined by the equation (3.2). Following the cohomological construction of §2.1, we obtain a homomorphism

$$(3.3) \quad E'_{d,(a,b)}(K_{\mathfrak{p}}) \rightarrow K_{\mathfrak{p}}^{\times}/(K_{\mathfrak{p}}^{\times})^2$$

that takes  $(0, 0)$  to  $2a(a+b) \cdot (K_{\mathfrak{p}}^{\times})^2$  and takes any point  $(x, y) \notin \{0, (0, 0)\}$  to  $x \cdot (K_{\mathfrak{p}}^{\times})^2$ . The key topological observation is the image of (3.3) does not depend on the choice  $(a, b)$  if we take  $\epsilon_{\mathfrak{p}} > 0$  sufficiently small. Thus by taking  $\epsilon_{\mathfrak{p}} > 0$  sufficiently small, we may assume that (3.3) has a common image  $\Phi_{d,\mathfrak{p}}$  for all  $(a, b) \in U_{\mathfrak{p}}$ . For the rest of the proof if we specify a prime ideal  $\mathfrak{p}$  and a pair  $(a_{\mathfrak{p}}, b_{\mathfrak{p}})$  with  $a_{\mathfrak{p}}b_{\mathfrak{p}}(a_{\mathfrak{p}} + b_{\mathfrak{p}})(a_{\mathfrak{p}} - b_{\mathfrak{p}}) \neq 0$ , then we will have  $U_{\mathfrak{p}}$ ,  $\Phi_{1,\mathfrak{p}}$



and  $\Phi_{D,\mathfrak{p}}$  with properties as above. Parts (a) and (b) will be immediate once we have defined the set  $S_1$  and chosen  $a_{\mathfrak{p}}, b_{\mathfrak{p}} \in K_{\mathfrak{p}}$  for all  $\mathfrak{p} \in S_0 \cup S_1$ .

For  $\mathfrak{p} \in S_0$ , we take  $a_{\mathfrak{p}} = 1$  and choose  $b_{\mathfrak{p}}$  to be a nonzero element of  $\mathfrak{n}_0 \mathfrak{p} \mathcal{O}_{\mathfrak{p}}$ ; in particular,  $v_{\mathfrak{p}}(a_{\mathfrak{p}}) = v_{\mathfrak{p}}(a_{\mathfrak{p}} + b_{\mathfrak{p}}) = v_{\mathfrak{p}}(a_{\mathfrak{p}} - b_{\mathfrak{p}}) = 0$ . Take any  $(a, b) \in K^2$  that lies in  $U_{\mathfrak{p}}$  for all  $\mathfrak{p} \in S_0$ . For each  $\mathfrak{p} \mid \mathfrak{n}_0$ , we have  $\mathfrak{p} \in S_0$  and hence  $a + b \in 1 + \mathfrak{n}_0 \mathcal{O}_{\mathfrak{p}}$ . We thus have (c) and (d).

Choose a finite set  $S_1$  of nonzero prime ideals  $\mathfrak{p} \notin S_0$  of  $\mathcal{O}_K$  that are inert in  $L = K(\sqrt{D})$  along with values  $\xi_{\mathfrak{p}} \in \{1/2, 2\}$  such that

$$(3.4) \quad \prod_{\mathfrak{p} \in S_0} |\Phi_{1,\mathfrak{p}}| / |\Phi_{D,\mathfrak{p}}| \cdot \prod_{\mathfrak{p} \in S_1} \xi_{\mathfrak{p}} = 1$$

holds and  $\xi_{\mathfrak{p}} = 2$  for some  $\mathfrak{p} \in S_1$ . Note that  $D$  is not a square in  $K_{\mathfrak{p}}$  for  $\mathfrak{p} \in S_1$  since these primes are inert in  $L$ . For  $\mathfrak{p} \in S_1$ , we will now choose a pair  $(a_{\mathfrak{p}}, b_{\mathfrak{p}}) \in K_{\mathfrak{p}}^2$  using Lemma 2.3. For each  $\mathfrak{p} \in S_1$  with  $\xi_{\mathfrak{p}} = 1/2$ , we define  $\mu_{\mathfrak{p}} := 1$  and choose  $a_{\mathfrak{p}}, b_{\mathfrak{p}} \in K_{\mathfrak{p}}^2$  with  $a_{\mathfrak{p}} b_{\mathfrak{p}} (a_{\mathfrak{p}} + b_{\mathfrak{p}})(a_{\mathfrak{p}} - b_{\mathfrak{p}}) \neq 0$  and

$$(v_{\mathfrak{p}}(a_{\mathfrak{p}}), v_{\mathfrak{p}}(a_{\mathfrak{p}} + b_{\mathfrak{p}}), v_{\mathfrak{p}}(a_{\mathfrak{p}} - b_{\mathfrak{p}})) = (0, 1, 0).$$

For each  $\mathfrak{p} \in S_1$  with  $\xi_{\mathfrak{p}} = 2$ , we choose a value  $\mu_{\mathfrak{p}} \in \{1, 2\}$ . For  $\mathfrak{p} \in S_1$  with  $\xi_{\mathfrak{p}} = 2$  and  $\mu_{\mathfrak{p}} = 1$ , we choose  $a_{\mathfrak{p}}, b_{\mathfrak{p}} \in K_{\mathfrak{p}}$  with  $a_{\mathfrak{p}} b_{\mathfrak{p}} (a_{\mathfrak{p}} + b_{\mathfrak{p}})(a_{\mathfrak{p}} - b_{\mathfrak{p}}) \neq 0$ ,

$$(v_{\mathfrak{p}}(a_{\mathfrak{p}}), v_{\mathfrak{p}}(a_{\mathfrak{p}} + b_{\mathfrak{p}}), v_{\mathfrak{p}}(a_{\mathfrak{p}} - b_{\mathfrak{p}})) = (-1, 1, -1)$$

and  $-2a_{\mathfrak{p}}(a_{\mathfrak{p}} + b_{\mathfrak{p}})$  a square in  $K_{\mathfrak{p}}$ . For  $\mathfrak{p} \in S_1$  with  $\xi_{\mathfrak{p}} = 2$  and  $\mu_{\mathfrak{p}} = 2$ , we choose  $a_{\mathfrak{p}}, b_{\mathfrak{p}} \in K_{\mathfrak{p}}$  with  $a_{\mathfrak{p}} b_{\mathfrak{p}} (a_{\mathfrak{p}} + b_{\mathfrak{p}})(a_{\mathfrak{p}} - b_{\mathfrak{p}}) \neq 0$ ,

$$(v_{\mathfrak{p}}(a_{\mathfrak{p}}), v_{\mathfrak{p}}(a_{\mathfrak{p}} + b_{\mathfrak{p}}), v_{\mathfrak{p}}(a_{\mathfrak{p}} - b_{\mathfrak{p}})) = (0, 2, 0)$$

and  $-2a_{\mathfrak{p}}(a_{\mathfrak{p}} + b_{\mathfrak{p}})$  a square in  $K_{\mathfrak{p}}$ . For each  $\mathfrak{p} \in S_1$  and any  $(a, b) \in U_{\mathfrak{p}} \cap K^2$ , we can use Lemma 2.2(iv–ix) with the above  $\mathfrak{p}$ -adic valuations and  $D \notin (K_{\mathfrak{p}}^{\times})^2$  to compute  $|\text{Im}(\delta_{1,\mathfrak{p}})| / |\text{Im}(\delta_{D,\mathfrak{p}})|$  and show that  $|\text{Im}(\delta_{1,\mathfrak{p}})| / |\text{Im}(\delta_{D,\mathfrak{p}})| = \xi_{\mathfrak{p}}$ . Therefore,  $|\Phi_{1,\mathfrak{p}}| / |\Phi_{D,\mathfrak{p}}| = \xi_{\mathfrak{p}}$  for all  $\mathfrak{p} \in S_1$ . So equation (3.4) becomes

$$\prod_{\mathfrak{p} \in S_0 \cup S_1} |\Phi_{1,\mathfrak{p}}| = \prod_{\mathfrak{p} \in S_0 \cup S_1} |\Phi_{D,\mathfrak{p}}|.$$

If  $(a, b) \in K^2$  lies in  $U_{\mathfrak{p}}$  for all  $\mathfrak{p} \in S_1$ , then

$$\sum_{\mathfrak{p} \in S_1, \mathfrak{p} \text{ inert in } L} v_{\mathfrak{p}}(a + b) = \sum_{\mathfrak{p} \in S_1} v_{\mathfrak{p}}(a_{\mathfrak{p}} + b_{\mathfrak{p}}) = \sum_{\mathfrak{p} \in S_1} \mu_{\mathfrak{p}}.$$

Since we have the freedom to choose  $\mu_{\mathfrak{p}} \in \{1, 2\}$  for  $\mathfrak{p} \in S_1$  with  $\xi_{\mathfrak{p}} = 2$ , we may assume that the  $\mu_{\mathfrak{p}}$  have been chosen so that

$$(3.5) \quad \sum_{\mathfrak{p} \in S_1, \mathfrak{p} \text{ inert in } L} v_{\mathfrak{p}}(a + b) \equiv 1 \pmod{2}$$

holds for all  $(a, b) \in K^2$  that lie in  $U_{\mathfrak{p}}$  for all  $\mathfrak{p} \in S_1$ . With our set  $S_1$ , we have now proved (e) and (f).

By weak approximation for  $K$ , there is a finite set  $S'_1$  of nonzero prime ideals of  $\mathcal{O}_K$  that is disjoint with  $S_0 \cup S_1$  such that the homomorphism

$$(3.6) \quad \mathcal{O}_{K, S_0 \cup S_1 \cup S'_1}^{\times} \rightarrow \prod_{v \in S_0 \cup S_1 \cup S_{\infty}} K_v^{\times} / (K_v^{\times})^2$$

is surjective. For each  $\mathfrak{p} \in S'_1$ , we choose  $a_{\mathfrak{p}}, b_{\mathfrak{p}} \in K_{\mathfrak{p}}$  with  $a_{\mathfrak{p}}b_{\mathfrak{p}}(a_{\mathfrak{p}} + b_{\mathfrak{p}})(a_{\mathfrak{p}} - b_{\mathfrak{p}}) \neq 0$  such that  $(v_{\mathfrak{p}}(a_{\mathfrak{p}}), v_{\mathfrak{p}}(a_{\mathfrak{p}} + b_{\mathfrak{p}}), v_{\mathfrak{p}}(a_{\mathfrak{p}} - b_{\mathfrak{p}})) = (1, 0, 0)$ . We then have  $U_{\mathfrak{p}}, \Phi_{1,\mathfrak{p}}$  and  $\Phi_{D,\mathfrak{p}}$  as above. For each  $\mathfrak{p} \in S'_1$ , Lemma 2.2(iii) implies that  $\Phi_{1,\mathfrak{p}}$  and  $\Phi_{D,\mathfrak{p}}$  are subgroups of  $K_{\mathfrak{p}}^{\times}/(K_{\mathfrak{p}}^{\times})^2$  of order 2 that are not equal to  $\mathcal{O}_{\mathfrak{p}}^{\times}/(\mathcal{O}_{\mathfrak{p}}^{\times})^2$ . So for  $d \in \{1, D\}$ , the subgroup of  $\prod_{v \in S_0 \cup S_1 \cup S'_1 \cup S_{\infty}} K_v^{\times}$  generated by the groups

$$(3.7) \quad \prod_{v \in S_0 \cup S_1 \cup S'_1 \cup S_{\infty}} \Phi_{d,v} \quad \text{and} \quad \prod_{v \in S_0 \cup S_1 \cup S_{\infty}} \{1\} \times \prod_{v \in S'_1} \mathcal{O}_v^{\times}$$

contains  $\prod_{v \in S_0 \cup S_1 \cup S_{\infty}} \{1\} \times \prod_{v \in S'_1} K_v^{\times}$ . Since the homomorphism (3.6) is surjective, we deduce that  $\prod_{v \in S_0 \cup S_1 \cup S'_1 \cup S_{\infty}} K_v^{\times}$  is generated by the image of the groups (3.7) and the image of  $\mathcal{O}_{K, S_0 \cup S_1 \cup S'_1}^{\times}$ . Therefore, (g) holds when we replace  $S_1$  by  $S_1 \cup S'_1$ . Observe that (e) and (f) remain true after replacing  $S_1$  by  $S_1 \cup S'_1$  since we have  $v_{\mathfrak{p}}(a_{\mathfrak{p}} + b_{\mathfrak{p}}) = 0$  and  $|\Phi_{1,\mathfrak{p}}| = 2 = |\Phi_{D,\mathfrak{p}}|$  for all  $\mathfrak{p} \in S'_1$ .  $\square$

For the rest of the proof, we fix  $S_1$ , the sets  $U_{\mathfrak{p}}$ , and the groups  $\Phi_{1,\mathfrak{p}}$  and  $\Phi_{D,\mathfrak{p}}$  as in Lemma 3.1.

**Lemma 3.2.** *There is a finite set  $S_2$  of nonzero prime ideals of  $\mathcal{O}_K$  that is disjoint from  $S_0 \cup S_1$  such that the following hold:*

- all the prime ideals in  $S_2$  split in  $L$ ,
- the natural homomorphism

$$(3.8) \quad \mathcal{O}_{K, S_0 \cup S_1 \cup S_2}^{\times} \rightarrow \prod_{v \in S_0 \cup S_1 \cup S_{\infty}} (K_v^{\times}/(K_v^{\times})^2)/\Phi_{d,v}$$

*is surjective for each  $d \in \{1, D\}$ ,*

- $S_2$  contains a prime ideal  $\pi_1 \mathcal{O}_K$  that splits in  $L$  such that  $\pi_1 \in \mathcal{O}_K$  is a square in  $K_v$  for all places  $v \in S_0 \cup S_1 \cup S_{\infty}$ .

*Proof.* Let  $\mathfrak{m}_0$  be a nonzero ideal of  $\mathcal{O}_K$  whose prime divisors are the prime ideals  $\mathfrak{p} \in S_0 \cup S_1$ . We may assume that  $\mathfrak{m}_0$  is divisible by  $\mathfrak{n}_0$ . Let  $\mathfrak{m}$  be the modulus obtained from  $\mathfrak{m}_0$  and all the real places of  $K$ .

For each fractional ideal  $I$  of  $K$  we have  $I = \prod_{\mathfrak{p}} \mathfrak{p}^{v_{\mathfrak{p}}(I)}$ , where the product is over the nonzero prime prime ideals of  $\mathcal{O}_K$  and the  $v_{\mathfrak{p}}(I)$  are unique integers that are zero for all but finitely many  $\mathfrak{p}$ . Let  $\mathcal{I}_K^{\mathfrak{m}}$  be the group of fractional ideals  $I$  of  $K$  with  $v_{\mathfrak{p}}(I) = 0$  for all  $\mathfrak{p} | \mathfrak{m}_0$ . Define  $K^{\mathfrak{m}}$  to be the group of  $\alpha \in K^{\times}$  with  $v_{\mathfrak{p}}(\alpha) = 0$  for all  $\mathfrak{p} | \mathfrak{m}_0$ . Let  $K^{\mathfrak{m},1}$  be the subgroup of  $K^{\mathfrak{m}}$  consisting of  $\alpha \in K^{\mathfrak{m}}$  with  $v_{\mathfrak{p}}(\alpha - 1) \geq v_{\mathfrak{p}}(\mathfrak{m}_0)$  for all  $\mathfrak{p} | \mathfrak{m}_0$  and with  $\alpha$  positive in  $K_v$  for all real places  $v$  of  $K$ . Let  $\mathcal{P}_K^{\mathfrak{m}}$  be the subgroup of  $\mathcal{I}_K^{\mathfrak{m}}$  consisting of  $\alpha \mathcal{O}_K$  with  $\alpha \in K^{\mathfrak{m},1}$ . Recall that the *ray class group* of  $\mathfrak{m}$  is the (finite) group  $\text{Cl}_K^{\mathfrak{m}} := \mathcal{I}_K^{\mathfrak{m}}/\mathcal{P}_K^{\mathfrak{m}}$ . We have a natural exact sequence

$$(3.9) \quad \mathcal{O}_K^{\times} \rightarrow K^{\mathfrak{m}}/K^{\mathfrak{m},1} \xrightarrow{f} \text{Cl}_K^{\mathfrak{m}} \rightarrow \text{Cl}_K \rightarrow 1,$$

where  $\text{Cl}_K$  is the class group of  $K$ . Assuming that the powers of the prime divisors of  $\mathfrak{m}_0$  were chosen large enough, we may assume that we have a well-defined homomorphism

$$(3.10) \quad K^{\mathfrak{m}}/K^{\mathfrak{m},1} \rightarrow \prod_{\mathfrak{p} \in S_0 \cup S_1} \mathcal{O}_{\mathfrak{p}}^{\times}/(\mathcal{O}_{\mathfrak{p}}^{\times})^2 \times \prod_{v \in S_{\infty}} K_v^{\times}/(K_v^{\times})^2;$$

this map is surjective by weak approximation for  $K$ .

Let  $F$  be the corresponding *ray class field* of  $\mathfrak{m}$ ; it is a finite abelian extension of  $K$  with an isomorphism  $\text{Gal}(F/K) \xrightarrow{\sim} \text{Cl}_K^{\mathfrak{m}}$  so that  $F$  is unramified at each nonzero prime ideal  $\mathfrak{p} \nmid \mathfrak{m}_0$  of  $\mathcal{O}_K$  and  $\text{Frob}_{\mathfrak{p}} \in \text{Gal}(F/K)$  is sent to the class  $[\mathfrak{p}] \in \text{Cl}_K^{\mathfrak{m}}$ .

Let  $\psi': \text{Cl}_K^{\mathfrak{m}} \rightarrow \{\pm 1\}$  be the homomorphism obtained by composing the quotient map  $\text{Cl}_K^{\mathfrak{m}} \rightarrow \text{Cl}_K^{\mathfrak{n}}$  with  $\psi$ . We have  $L \subseteq F$  and for a nonzero prime ideal  $\mathfrak{p} \notin S_0 \cup S_1$ ,  $\mathfrak{p}$  splits in  $L$  if and only if  $\psi'([\mathfrak{p}]) = 1$ . Let  $G \subseteq \text{Cl}_K^{\mathfrak{m}}$  be the intersection of  $\ker(\psi')$  with  $f(K^{\mathfrak{m}}/K^{\mathfrak{m},1})$ . We have  $[f(K^{\mathfrak{m}}/K^{\mathfrak{m},1}) : G] \leq 2$ . By the Chebotarev density theorem, we can find a finite set  $S_2$  of nonzero prime ideals of  $\mathcal{O}_K$  that is disjoint from  $S_0 \cup S_1$  such that the set  $\{[\mathfrak{p}] : \mathfrak{p} \in S_2\} \subseteq \text{Cl}_K^{\mathfrak{m}}$  generates the group  $G$ . Note that all the prime ideals  $\mathfrak{p} \in S_2$  are principal and split in  $L$ .

By our choice of  $S_2$ , the exact sequence (3.9) and the surjectivity of (3.10), we find that the quotient homomorphism

$$(3.11) \quad \mathcal{O}_{K,S_2}^{\times} \rightarrow K^{\mathfrak{m}}/K^{\mathfrak{m},1} \rightarrow \prod_{\mathfrak{p} \in S_0 \cup S_1} \mathcal{O}_{\mathfrak{p}}^{\times}/(\mathcal{O}_{\mathfrak{p}}^{\times})^2 \times \prod_{v \in S_{\infty}} K_v^{\times}/(K_v^{\times})^2$$

has cokernel of cardinality at most 2. If (3.11) is not surjective, then since  $\mathfrak{n}_0$  has only prime divisors in  $S_0$  we find that composing (3.11) with the quotient map to  $\prod_{\mathfrak{p} \in S_0} \mathcal{O}_{\mathfrak{p}}^{\times}/(\mathcal{O}_{\mathfrak{p}}^{\times})^2 \times \prod_{v \in S_{\infty}} K_v^{\times}/(K_v^{\times})^2$  gives another homomorphism that is not surjective. Therefore, the image of (3.11) must contain  $\prod_{v \in S_0 \cup S_{\infty}} \{1\} \times \prod_{\mathfrak{p} \in S_1} \mathcal{O}_{\mathfrak{p}}^{\times}/(\mathcal{O}_{\mathfrak{p}}^{\times})^2$ . By Lemma 3.1(g), we deduce that (3.8) is surjective for each  $d \in \{1, D\}$ .

By the Chebotarev density theorem, there is a nonzero prime ideal  $\mathfrak{p} \notin S_0 \cup S_1 \cup S_2$  of  $\mathcal{O}_K$  that splits completely in  $F$  and hence  $[\mathfrak{p}] = 1$  in  $\text{Cl}_K^{\mathfrak{m}}$ . The prime  $\mathfrak{p}$  splits in  $L$  since  $L \subseteq F$ . We have  $\mathfrak{p} = \pi_1 \mathcal{O}_K$  for some  $\pi_1 \in \mathcal{O}_K$ . By the exact sequence (3.9), there is a unit  $u \in \mathcal{O}_K^{\times}$  for which  $u \cdot (K^{\mathfrak{m},1}) = \pi_1 \cdot (K^{\mathfrak{m},1})$ . After replacing  $\pi_1$  by  $u^{-1}\pi_1$ , we may assume that  $\pi_1 \in K^{\mathfrak{m},1}$  and hence  $\pi_1$  is a square in  $K_v$  for all  $v \in S_0 \cup S_1 \cup S_{\infty}$  by our choice of  $\mathfrak{m}$ . The lemma follows by adding  $\mathfrak{p} = \pi_1 \mathcal{O}_K$  to  $S_2$ .  $\square$

From now on, we fix a set  $S_2$  and a prime  $\pi_1 \in \mathcal{O}_K$  as in Lemma 3.2. Take any  $d \in \{1, D\}$ . We have a natural group homomorphism

$$\gamma_d: \mathcal{O}_{K,S_0 \cup S_1 \cup S_2}^{\times}/(\mathcal{O}_{K,S_0 \cup S_1 \cup S_2}^{\times})^2 \rightarrow \prod_{v \in S_0 \cup S_1 \cup S_{\infty}} (K_v^{\times}/(K_v^{\times})^2)/\Phi_{d,v}$$

that is surjective by our choice of  $S_2$ . Define the group  $V_d := \ker \gamma_d$ .

**Lemma 3.3.**

- (i) For each  $d \in \{1, D\}$ , we have  $|V_d| = 2^{|S_2|} \cdot \prod_{v \in S_0 \cup S_1 \cup S_{\infty}} \frac{1}{2} |\Phi_{d,v}|$ .
- (ii) We have  $|V_1| = |V_D|$ .

*Proof.* Let  $r$  be the number of real embeddings of  $K$  and let  $s$  be the number of pairs of conjugate complex embeddings of  $K$ . From the definition of  $V_d$  and the surjectivity of  $\gamma_d$ , we have

$$(3.12) \quad |V_d| = |\mathcal{O}_{K,S_0 \cup S_1 \cup S_2}^{\times}/(\mathcal{O}_{K,S_0 \cup S_1 \cup S_2}^{\times})^2| \cdot \prod_{v \in S_0 \cup S_1 \cup S_{\infty}} |\Phi_{d,v}| \cdot \prod_{v \in S_0 \cup S_1 \cup S_{\infty}} |K_v^{\times}/(K_v^{\times})^2|^{-1}.$$

Consider any place  $v|2$  of  $K$ . Let  $e_v$  and  $f_v$  be the ramification index and inertia degree, respectively, of the extension  $K_v/\mathbb{Q}_2$ . We have  $[K_v : \mathbb{Q}_2] = e_v f_v$ . We have  $\mathcal{O}_v^{\times} \cong C_v \times \mathbb{Z}_2^{e_v f_v}$ , where  $C_v$  is a finite cyclic group, cf. [Neu99, II 5.7]. The group  $C_v$  has even cardinality since it contains  $-1$  and hence  $\mathcal{O}_v^{\times}/(\mathcal{O}_v^{\times})^2 \cong (\mathbb{Z}/2\mathbb{Z})^{1+e_v f_v}$ . Therefore,  $|K_v^{\times}/(K_v^{\times})^2| = 2^{2+e_v f_v}$ . Since

$\sum_{v|2} e_v f_v = [K : \mathbb{Q}] = r + 2s$ , we deduce that  $\prod_{v|2} |K_v^\times / (K_v^\times)^2| = 2^{r+2s} \prod_{v|2} 4$ . We also have  $\prod_{v \in S_\infty} |K_v^\times / (K_v^\times)^2| = 2^r$ . For any place  $v \in S_0 \cup S_1$  with  $v \nmid 2$ , we have  $|K_v^\times / (K_v^\times)^2| = 4$ . Therefore,

$$\prod_{v \in S_0 \cup S_1 \cup S_\infty} |K_v^\times / (K_v^\times)^2| = 2^{2r+2s} 4^{|S_0|+|S_1|}.$$

Let  $t$  be the rank of the finite generated abelian group  $\mathcal{O}_{K, S_0 \cup S_1 \cup S_2}^\times$ . By Dirichlet's unit theorem, we have  $t = r + s - 1 + |S_0| + |S_1| + |S_2|$ . Since the torsion subgroup of  $\mathcal{O}_{K, S_0 \cup S_1 \cup S_2}^\times$  is a finite cyclic group of even cardinality, we find that  $\mathcal{O}_{K, S_0 \cup S_1 \cup S_2}^\times / (\mathcal{O}_{K, S_0 \cup S_1 \cup S_2}^\times)^2$  has dimension  $t + 1$  over  $\mathbb{F}_2$ . Therefore,

$$|\mathcal{O}_{K, S_0 \cup S_1 \cup S_2}^\times / (\mathcal{O}_{K, S_0 \cup S_1 \cup S_2}^\times)^2| = 2^{t+1} = 2^{r+s+|S_0|+|S_1|+|S_2|}.$$

From (3.12) and the above computations, we have

$$|V_d| = 2^{r+s+|S_0|+|S_1|+|S_2|} \cdot \prod_{v \in S_0 \cup S_1 \cup S_\infty} |\Phi_{d,v}| \cdot 2^{-2r-2s} 2^{-2|S_0|} 2^{-2|S_1|} = 2^{|S_2|} \prod_{v \in S_0 \cup S_1 \cup S_\infty} \frac{1}{2} |\Phi_{d,v}|.$$

This completes the proof of (i). Since  $\Phi_{1,v} = \Phi_{D,v} = 1$  for all  $v \in S_\infty$ , part (ii) follows from (i) and Lemma 3.1(f).  $\square$

Note that  $\pi_1 \cdot (\mathcal{O}_{K, S_0 \cup S_1 \cup S_2}^\times)^2$  lies in  $V_1$  and  $V_D$  since  $\pi_1 \mathcal{O}_K \in S_2$  and  $\pi_1$  is a square in  $K_v$  for all  $v \in S_0 \cup S_1 \cup S_\infty$ . Thus there is an integer  $n \geq 0$  such that  $|V_1| = 2^{n+1}$ . By Lemma 3.3(ii), we have  $|V_D| = 2^{n+1}$ .

We can view  $V_1$  and  $V_2$  as subgroups of  $K^\times / (K^\times)^2$ . For each nonzero prime ideal  $\mathfrak{p}$  of  $\mathcal{O}_K$ , let

$$\varphi_{\mathfrak{p}} : K^\times / (K^\times)^2 \rightarrow K_{\mathfrak{p}}^\times / (K_{\mathfrak{p}}^\times)^2$$

be the natural quotient map.

**Lemma 3.4.** *There are distinct nonzero prime ideals  $\mathfrak{p}_1, \dots, \mathfrak{p}_n \notin S_0 \cup S_1 \cup S_2$  of  $\mathcal{O}_K$  such that  $V_1 \cap \bigcap_{i=1}^n \ker \varphi_{\mathfrak{p}_i}$  and  $V_D \cap \bigcap_{i=1}^n \ker \varphi_{\mathfrak{p}_i}$  are both equal to the group generated by  $\pi_1 \cdot (K^\times)^2$ .*

*Proof.* We shall view  $V_1$  and  $V_D$  as vector spaces over  $\mathbb{F}_2$ . Take  $m \geq 0$  maximal for which there are distinct nonzero prime ideals  $\mathfrak{p}_1, \dots, \mathfrak{p}_m \notin S_0 \cup S_1 \cup S_2$  of  $\mathcal{O}_K$  such that

- $W_1 := V_1 \cap \bigcap_{i=1}^m \ker \varphi_{\mathfrak{p}_i}$  has codimension  $m$  in  $V_1$  and contains  $\pi_1 \cdot (K^\times)^2$ ,
- $W_D := V_D \cap \bigcap_{i=1}^m \ker \varphi_{\mathfrak{p}_i}$  has codimension  $m$  in  $V_D$  and contains  $\pi_1 \cdot (K^\times)^2$ ,

This is well-defined since the case  $m = 0$  is always possible;  $V_1$  and  $V_D$  contain the square class of  $\pi_1$ . Since  $\dim_{\mathbb{F}_2} V_1 = \dim_{\mathbb{F}_2} V_D = n + 1$  and  $\pi_1 \cdot (K^\times)^2 \neq 1$ , we must have  $m \leq n$ .

Suppose that  $m < n$  and hence  $W_1$  and  $W_D$  have dimension  $n + 1 - m \geq 2$  over  $\mathbb{F}_2$ . There are units  $u, v \in \mathcal{O}_{K, S_0 \cup S_1 \cup S_2}^\times$  such that  $u \cdot (K^\times)^2$  and  $v \cdot (K^\times)^2$  lie in  $W_1$  and  $W_D$ , respectively, and both do not lie in the group generated by  $\pi_1 \cdot (K^\times)^2$ . The subgroup of  $K^\times / (K^\times)^2$  generated by  $u, v$  and  $\pi_1$  either has dimension 3 over  $\mathbb{F}_2$  or  $uv \cdot (K^\times)^2$  lies in the group  $\langle \pi_1 \cdot (K^\times)^2 \rangle$ . By the Chebotarev density theorem applied to the extension  $K(\sqrt{u}, \sqrt{v}, \sqrt{\pi_1})/K$ , we find that there is a nonzero prime ideal  $\mathfrak{p} \notin S_0 \cup S_1 \cup S_2 \cup \{\mathfrak{p}_1, \dots, \mathfrak{p}_m\}$  such that  $u$  and  $v$  are not squares in  $K_{\mathfrak{p}}$  and  $\pi_1$  is a square in  $K_{\mathfrak{p}}$ . However with  $\mathfrak{p}_{m+1} := \mathfrak{p}$ , this contradicts the maximality of  $m$ . Therefore,  $m = n$  and the lemma follows.  $\square$

For the rest of the proof, we fix prime ideals  $\mathfrak{p}_1, \dots, \mathfrak{p}_n$  as in Lemma 3.4.

**Lemma 3.5.** *There is a nonzero prime ideal  $\mathfrak{p}_0 \notin S_0 \cup S_1 \cup S_2 \cup \{\mathfrak{p}_1, \dots, \mathfrak{p}_n\}$  of  $\mathcal{O}_K$  such that every element of  $\mathcal{O}_{K, S_0 \cup S_1 \cup S_2}^\times$  is a square in  $K_{\mathfrak{p}_0}$ .*

*Proof.* Let  $u_1, \dots, u_m$  be a set of generators of the group  $\mathcal{O}_{K, S_0 \cup S_1 \cup S_2}^\times$ ; it is finitely generated by Dirichlet's unit theorem. Define  $F := K(\sqrt{u_1}, \dots, \sqrt{u_m})$ . Then any nonzero prime ideal  $\mathfrak{p} \notin S_0 \cup S_1 \cup S_2 \cup \{\mathfrak{p}_1, \dots, \mathfrak{p}_n\}$  of  $\mathcal{O}_K$  that splits completely in  $F$  will have the desired properties; the existence of such primes follows from the Chebotarev density theorem.  $\square$

For the rest of the proof, we fix a prime  $\mathfrak{p}_0$  as in Lemma 3.5. Define  $S_3 := \{\mathfrak{p}_0, \mathfrak{p}_1, \dots, \mathfrak{p}_n\}$ . Define the finite set

$$S := S_0 \cup S_1 \cup S_2 \cup S_3$$

which consists of nonzero prime ideals of  $\mathcal{O}_K$ . Fix a value  $\varepsilon \in \{\pm 1\}$ ; we will make a specific choice later.

Take any prime ideal  $\mathfrak{p} \in S_2$ . Let  $U_{\mathfrak{p}}$  be the set of pairs  $(a, b) \in K_{\mathfrak{p}}^2$  that satisfy the following conditions:

- $ab(a+b)(a-b) \neq 0$ ,
- $(v_{\mathfrak{p}}(a), v_{\mathfrak{p}}(a+b), v_{\mathfrak{p}}(a-b)) = (-1, 1, -1)$ ,
- $-2a(a+b)$  is a square in  $K_{\mathfrak{p}}$ ,
- if  $\mathfrak{p} = \pi_1 \mathcal{O}_K$ , then  $(a-b)\pi_1$  is a square in  $K_{\mathfrak{p}}$  when  $\varepsilon = 1$  and  $(a-b)\pi_1$  is not a square in  $K_{\mathfrak{p}}$  when  $\varepsilon = -1$ .

The set  $U_{\mathfrak{p}}$  is open in  $K_{\mathfrak{p}}^2$ . The set  $U_{\mathfrak{p}}$  is nonempty by Lemma 2.3 (when  $\mathfrak{p} = \pi_1 \mathcal{O}_K$ , take the uniformizer  $\omega := \pi_1$  of  $K_{\mathfrak{p}}$ ). We define  $\Phi_{1,\mathfrak{p}} = K_{\mathfrak{p}}^\times / (K_{\mathfrak{p}}^\times)^2$  and  $\Phi_{D,\mathfrak{p}} = K_{\mathfrak{p}}^\times / (K_{\mathfrak{p}}^\times)^2$ .

Take any prime ideal  $\mathfrak{p} \in S_3$ . Let  $U_{\mathfrak{p}}$  be the set of pairs  $(a, b) \in K_{\mathfrak{p}}^2$  that satisfy the following conditions:

- $ab(a+b)(a-b) \neq 0$ ,
- $(v_{\mathfrak{p}}(a), v_{\mathfrak{p}}(a+b), v_{\mathfrak{p}}(a-b)) = (0, 0, 1)$ ,
- if  $\mathfrak{p} = \mathfrak{p}_0$ , then  $a$  is not a square in  $K_{\mathfrak{p}}$ .

The set  $U_{\mathfrak{p}}$  is nonempty by Lemma 2.3. We define  $\Phi_{1,\mathfrak{p}}$  and  $\Phi_{D,\mathfrak{p}}$  to be the trivial subgroup of  $K_{\mathfrak{p}}^\times / (K_{\mathfrak{p}}^\times)^2$ . We now show that these new sets  $U_{\mathfrak{p}}$  have the same property as before.

**Lemma 3.6.** *Take any  $\mathfrak{p} \in S$  and any  $(a, b) \in K^2$  that lies in  $U_{\mathfrak{p}}$ . Then  $ab(a+b)(a-b) \neq 0$  and*

$$\text{Im}(\delta_{1,\mathfrak{p}}) = \Phi_{1,\mathfrak{p}} \quad \text{and} \quad \text{Im}(\delta_{D,\mathfrak{p}}) = \Phi_{D,\mathfrak{p}}.$$

*Note that  $\delta_{1,\mathfrak{p}}$  and  $\delta_{D,\mathfrak{p}}$  depend on  $(a, b)$  while the groups  $\Phi_{1,\mathfrak{p}}$  and  $\Phi_{D,\mathfrak{p}}$  do not.*

*Proof.* When  $\mathfrak{p} \in S_0 \cup S_1$ , this is Lemma 3.1(a).

Suppose that  $\mathfrak{p} \in S_2$  and take any  $d \in \{1, D\}$ . By our choice of  $U_{\mathfrak{p}}$ , we have  $(v_{\mathfrak{p}}(a), v_{\mathfrak{p}}(a+b), v_{\mathfrak{p}}(a-b)) = (-1, 1, -1)$  and  $-2a(a+b)$  is a square in  $K_{\mathfrak{p}}$ . Also  $-2a(a+b)D$  is a square in  $K_{\mathfrak{p}}$  since every prime in  $S_2$  splits in  $L$ . Therefore,  $|\text{Im}(\delta_{d,\mathfrak{p}})| = 4$  by Lemma 2.2(vi). Thus  $\text{Im}(\delta_{d,\mathfrak{p}}) = K_{\mathfrak{p}}^\times / (K_{\mathfrak{p}}^\times)^2 = \Phi_{d,\mathfrak{p}}$ .

Suppose that  $\mathfrak{p} \in S_3$  and take any  $d \in \{1, D\}$ . By our choice of  $U_{\mathfrak{p}}$ , we have  $(v_{\mathfrak{p}}(a), v_{\mathfrak{p}}(a+b), v_{\mathfrak{p}}(a-b)) = (0, 0, 1)$ . Therefore,  $|\text{Im}(\delta_{d,\mathfrak{p}})| = 1$  by Lemma 2.2(ii). Thus  $\text{Im}(\delta_{d,\mathfrak{p}}) = 1 = \Phi_{d,\mathfrak{p}}$ .  $\square$

**3.3. A choice of elliptic curve and a 2-descent.** With a fixed  $\varepsilon \in \{\pm 1\}$  still to be determined, we have constructed a finite set  $S$  of prime ideals and we have a nonempty open subset  $U_{\mathfrak{p}}$  of  $K_{\mathfrak{p}}^2$  for each  $\mathfrak{p} \in S$ . We also have a specific prime  $\pi_1 \in \mathcal{O}_K$  that generates a prime ideal in  $S$ .

For the rest of the proof we take any  $a, b \in \mathcal{O}_K$  for which the following hold:

- $a, a + b$  and  $a - b$  generate distinct nonzero prime ideals of  $\mathcal{O}_{K,S}$ ,
- $(a, b)$  lies in  $U_{\mathfrak{p}}$  for all  $\mathfrak{p} \in S$ ,
- $0 < a < b$  in  $K_v$  for all real places of  $K$ .

If no such  $a$  and  $b$  exist, then Theorem 1.5 trivially holds. We have  $ab(a + b)(a - b) \neq 0$ .

For  $d \in \{1, D\}$ , we have an elliptic curve  $E_d$  over  $K$  defined by (3.1) and an elliptic curve  $E'_d$  over  $K$  defined by (3.2). The curve  $E_D$  is the quadratic twist of  $E_1$  by  $D$ . To finish the proof of Theorem 1.5 we need to show that  $E_1$  has rank 1 and  $E_D$  has rank 0.

Since  $a, a + b$  and  $a - b$  generate distinct nonzero prime ideals of  $\mathcal{O}_{K,S}$ , there are distinct nonzero prime ideals  $\mathfrak{q}_1, \mathfrak{q}_2$  and  $\mathfrak{q}_3$  of  $\mathcal{O}_K$  that are not in  $S$  such that

$$(3.13) \quad a\mathcal{O}_{K,S} = \mathfrak{q}_1\mathcal{O}_{K,S}, \quad (a + b)\mathcal{O}_{K,S} = \mathfrak{q}_2\mathcal{O}_{K,S} \quad \text{and} \quad (a - b)\mathcal{O}_{K,S} = \mathfrak{q}_3\mathcal{O}_{K,S}.$$

We now work out some properties for the prime ideals  $\mathfrak{q}_2$  and  $\mathfrak{q}_3$ .

**Lemma 3.7.** *For an appropriate initial choice of  $\varepsilon \in \{\pm 1\}$ ,  $\pi_1$  is not a square in  $K_{\mathfrak{q}_3}$ .*

*Proof.* For each nonzero prime ideal  $\mathfrak{p}$  of  $\mathcal{O}_K$ , define  $e_{\mathfrak{p}} := v_{\mathfrak{p}}(a - b)$ . Since  $(a - b)\mathcal{O}_{K,S} = \mathfrak{q}_3\mathcal{O}_{K,S}$ , we have  $(a - b)\mathcal{O}_K = \mathfrak{q}_3 \prod_{\mathfrak{p} \in S} \mathfrak{p}^{e_{\mathfrak{p}}}$ . With  $\mathfrak{p} = \pi_1\mathcal{O}_K$ , we have  $(a, b) \in U_{\mathfrak{p}}$  and hence  $v_{\mathfrak{p}}((a - b)\pi_1) = -1 + 1 = 0$ . Therefore,

$$(3.14) \quad (a - b)\pi_1\mathcal{O}_K = \mathfrak{q}_3 \prod_{\mathfrak{p} \in S, \mathfrak{p} \neq (\pi_1)} \mathfrak{p}^{e_{\mathfrak{p}}} = \mathfrak{q}_3 \prod_{\mathfrak{p} \in S_1 \cup S_2 \cup S_3, \mathfrak{p} \neq (\pi_1)} \mathfrak{p}^{e_{\mathfrak{p}}},$$

where the last equality uses Lemma 3.1(c). Using second power residue symbols for the field  $K$ , cf. [Neu99, IV §8], we have

$$\left( \frac{(a - b)\pi_1}{\pi_1} \right) = \left( \frac{\pi_1}{(a - b)\pi_1} \right) = \left( \frac{\pi_1}{\mathfrak{q}_3} \right) \cdot \prod_{\mathfrak{p} \in S_1 \cup S_2 \cup S_3, \mathfrak{p} \neq (\pi_1)} \left( \frac{\pi_1}{\mathfrak{p}} \right)^{e_{\mathfrak{p}}},$$

where the first equality uses the general reciprocity law [Neu99, IV Theorem 8.3] and the second equality uses (3.14). Note that in applying the reciprocity law, we have used that  $\pi_1$  is a square in  $K_v$  for all infinite places  $v$  of  $K$  and  $\pi_1$  is a square in  $K_{\mathfrak{p}}$  for all prime ideals  $\mathfrak{p}$  of  $\mathcal{O}_K$  dividing 2. With  $\mathfrak{p} = \pi_1\mathcal{O}_K$ ,  $(a, b) \in U_{\mathfrak{p}}$  implies that  $(a - b)\pi_1 \in \mathcal{O}_{\mathfrak{p}}^{\times}$  is a square in  $K_{\mathfrak{p}}$  if and only if  $\varepsilon = 1$ . Therefore,  $\left( \frac{(a - b)\pi_1}{\pi_1} \right) = \varepsilon$  and hence

$$(3.15) \quad \left( \frac{\pi_1}{\mathfrak{q}_3} \right) = \varepsilon \prod_{\mathfrak{p} \in S_1 \cup S_2 \cup S_3, \mathfrak{p} \neq (\pi_1)} \left( \frac{\pi_1}{\mathfrak{p}} \right)^{e_{\mathfrak{p}}}.$$

If  $\mathfrak{p} \in S_2$ ,  $(a, b) \in U_{\mathfrak{p}}$  implies that  $e_{\mathfrak{p}} = -1$ . If  $\mathfrak{p} \in S_3$ ,  $(a, b) \in U_{\mathfrak{p}}$  implies that  $e_{\mathfrak{p}} = 1$ . If  $\mathfrak{p} \in S_1$ ,  $(a, b) \in U_{\mathfrak{p}}$  implies that  $e_{\mathfrak{p}}$  does not depend on the choice of  $a$  and  $b$  by Lemma 3.1(b). Therefore, the right-hand side of (3.15) does not depend on the choice of  $a$  and  $b$ . So by making a suitable initial choice of  $\varepsilon \in \{\pm 1\}$ , that does not depend on  $a$  and  $b$ , we will have  $\left( \frac{\pi_1}{\mathfrak{q}_3} \right) = -1$  and hence  $\pi_1$  is not a square in  $K_{\mathfrak{q}_3}$ .  $\square$



For the rest of the proof, we shall assume that  $\varepsilon \in \{\pm 1\}$  has been chosen so that the conclusion of Lemma 3.7 holds.

**Lemma 3.8.** *The prime  $\mathfrak{q}_2$  is inert in  $L$ .*

*Proof.* For  $\mathfrak{p} \in S_0$ , we have  $v_{\mathfrak{p}}(a+b) = 0$  by Lemma 3.1(c). For  $\mathfrak{p} \in S_3$ ,  $(a, b) \in U_{\mathfrak{p}}$  implies that  $v_{\mathfrak{p}}(a+b) = 0$ . Since  $(a+b)\mathcal{O}_{K,S} = \mathfrak{q}_2\mathcal{O}_{K,S}$ , we have

$$(a+b)\mathcal{O}_K = \mathfrak{q}_2 \prod_{\mathfrak{p} \in S} \mathfrak{p}^{v_{\mathfrak{p}}(a+b)} = \mathfrak{q}_2 \prod_{\mathfrak{p} \in S_1 \cup S_2} \mathfrak{p}^{v_{\mathfrak{p}}(a+b)}.$$

Taking their classes in  $\text{Cl}_K^n$  and applying  $\psi$  gives

$$\psi([(a+b)\mathcal{O}_K]) = \psi([\mathfrak{q}_2]) \prod_{\mathfrak{p} \in S_1 \cup S_2} \psi([\mathfrak{p}])^{v_{\mathfrak{p}}(a+b)} = \psi([\mathfrak{q}_2]) \prod_{\mathfrak{p} \in S_1, \mathfrak{p} \text{ inert in } L} (-1)^{v_{\mathfrak{p}}(a+b)},$$

where the last equality uses that all the prime ideals in  $S_2$  split in  $L$ . Since  $(a, b) \in U_{\mathfrak{p}}$  for all  $\mathfrak{p} \in S_1$ , Lemma 3.1(e) implies that  $\psi([\mathfrak{q}_2]) = -\psi([(a+b)\mathcal{O}_K])$ .

Since  $(a, b) \in U_{\mathfrak{p}}$  for all  $\mathfrak{p} \in S_0$ , Lemma 3.1(d) implies that  $a+b \in 1 + \mathfrak{n}_0\mathcal{O}_{\mathfrak{p}}$  for all prime ideals  $\mathfrak{p}|\mathfrak{n}_0$ . By our choice of  $a$  and  $b$ ,  $a+b$  is positive in  $K_v$  for all real place  $v$  of  $K$ . Therefore, we have  $[(a+b)\mathcal{O}_K] = 1$  in  $\text{Cl}_K^n$ . So  $\psi([\mathfrak{q}_2]) = -1$  and hence  $\mathfrak{q}_2$  is inert in  $L$ .  $\square$

We now compute ratios of certain Selmer groups.

**Lemma 3.9.** *We have*

$$\frac{|\text{Sel}_{\phi_1}(E_1/K)|}{|\text{Sel}_{\hat{\phi}_1}(E'_1/K)|} = \frac{1}{2} \quad \text{and} \quad \frac{|\text{Sel}_{\phi_D}(E_D/K)|}{|\text{Sel}_{\hat{\phi}_D}(E'_D/K)|} = 1.$$

*Proof.* Take any  $d \in \{1, D\}$  and define  $\tau_d := |\text{Sel}_{\phi_d}(E_d/K)|/|\text{Sel}_{\hat{\phi}_d}(E'_d/K)|$ . By Lemma 2.1(i), we have  $\tau_d = \prod_v \frac{1}{2} |\text{Im}(\delta_{d,v})|$ , where the product is over the places  $v$  of  $K$ . We have

$$\tau_d = \prod_{v \in S \cup \{\mathfrak{q}_1, \mathfrak{q}_2, \mathfrak{q}_3\} \cup S_{\infty}} \frac{1}{2} |\text{Im}(\delta_{d,v})|$$

by Lemma 2.2(i) and (3.13).

For  $\mathfrak{p} \in S$ ,  $(a, b) \in U_{\mathfrak{p}}$  implies that  $\text{Im}(\delta_{d,\mathfrak{p}}) = \Phi_{d,\mathfrak{p}}$  by Lemma 3.6. For each complex place  $v$ , we trivially have  $\text{Im}(\delta_{d,v}) = 1 = \Phi_{d,v}$ . For each real place  $v$ , we have  $0 < a < b$  in  $K_v$  by our choice of  $a$  and  $b$  and hence  $2a(a+b)^2(a-b)d^2 < 0$  in  $K_v$ . For each real place  $v$ , Lemma 2.1(iii) implies that  $\text{Im}(\delta_{d,v}) = 1 = \Phi_{d,v}$ . For  $\mathfrak{p} \in \{\mathfrak{q}_1, \mathfrak{q}_2, \mathfrak{q}_3\}$ , we define  $\Phi_{d,\mathfrak{p}} := \text{Im}(\delta_{\mathfrak{p},d})$ .

Therefore,

$$\tau_d = \prod_{v \in S_0 \cup S_1 \cup S_{\infty}} \frac{1}{2} |\Phi_{d,v}| \cdot \prod_{\mathfrak{p} \in S_2 \cup S_3 \cup \{\mathfrak{q}_1, \mathfrak{q}_2, \mathfrak{q}_3\}} \frac{1}{2} |\Phi_{d,\mathfrak{p}}| = 2^{-|S_2|} |V_d| \prod_{\mathfrak{p} \in S_2 \cup S_3 \cup \{\mathfrak{q}_1, \mathfrak{q}_2, \mathfrak{q}_3\}} \frac{1}{2} |\Phi_{d,\mathfrak{p}}|$$

where the last equality uses Lemma 3.3. We have  $|\Phi_{d,\mathfrak{p}}| = 4$  for  $\mathfrak{p} \in S_2$  and  $|\Phi_{d,\mathfrak{p}}| = 1$  for  $\mathfrak{p} \in S_3$ . Therefore,

$$\tau_d = |V_d| 2^{-|S_3|} \prod_{\mathfrak{p} \in \{\mathfrak{q}_1, \mathfrak{q}_2, \mathfrak{q}_3\}} \frac{1}{2} |\Phi_{d,\mathfrak{p}}| = \prod_{\mathfrak{p} \in \{\mathfrak{q}_1, \mathfrak{q}_2, \mathfrak{q}_3\}} \frac{1}{2} |\text{Im}(\delta_{d,\mathfrak{p}})|,$$

where the last equality uses that  $|V_d| = 2^{n+1}$  and  $|S_3| = n+1$ . By (3.13) and Lemma 2.2(iii), we have  $\frac{1}{2} |\text{Im}(\delta_{d,\mathfrak{q}_1})| = 1$ . By (3.13) and Lemma 2.2(ii), we have  $\frac{1}{2} |\text{Im}(\delta_{d,\mathfrak{q}_3})| = 1/2$ . Therefore,  $\tau_d = |\text{Im}(\delta_{d,\mathfrak{q}_2})|/4$ .

By (3.13) and Lemma 2.2(iv), we have  $|\text{Im}(\delta_{1,q_2})| = 2$  and hence  $\tau_1 = 1/2$ . By Lemma 3.8,  $q_2$  is inert in  $L$  and hence  $D$  is not a square in  $K_{q_3}$ . By (3.13) and Lemma 2.2(v), we have  $|\text{Im}(\delta_{D,q_2})| = 4$  and hence  $\tau_D = 1$ .  $\square$

We next compute the Selmer groups associated to the isogenies  $\phi_1$  and  $\phi_D$ .

**Lemma 3.10.** *For  $d \in \{1, D\}$ , we have  $\text{Sel}_{\phi_d}(E_d/K) = \{1, 2a(a+b) \cdot (K^\times)^2\}$ .*

*Proof.* Take any  $d \in \{1, D\}$ . From the point  $(0, 0) \in E'_d(K)$ , we find that  $2a(a+b) \cdot (K^\times)^2$  is an element of  $\text{Sel}_{\phi_d}(E_d/K) \subseteq K^\times/(K^\times)^2$ . Now take any  $\alpha \in \text{Sel}_{\phi_d}(E_d/K)$ . We need to show that  $\alpha \in \{1, 2a(a+b) \cdot (K^\times)^2\}$ .

Choose an element  $c \in K^\times$  in the square class  $\alpha$ . For each  $\mathfrak{p} \in S$ ,  $c \cdot (K_\mathfrak{p}^\times)^2$  lies in  $\text{Im}(\delta_{d,\mathfrak{p}})$  since  $\alpha$  is an element of  $\text{Sel}_{\phi_d}(E_d/K)$ . For each  $\mathfrak{p} \in S$ , we have  $(a, b) \in U_\mathfrak{p}$  and hence  $c \cdot (K_\mathfrak{p}^\times)^2$  is an element of  $\Phi_{d,\mathfrak{p}}$  by Lemma 3.6.

Take any nonzero prime ideal  $\mathfrak{p} \notin S_0 \cup S_1 \cup S_2 \cup \{q_1, q_2\}$  of  $\mathcal{O}_K$ . If  $\mathfrak{p} \in S_3$ , then  $c$  is a square in  $K_\mathfrak{p}$  since  $\Phi_{d,\mathfrak{p}} = 1$ . If  $\mathfrak{p} = q_3$ , then  $c$  is a square in  $K_\mathfrak{p}$  by (3.13) and Lemma 2.2(ii). If also  $\mathfrak{p} \notin S_3 \cup \{q_3\}$ , then (3.13) implies that  $v_\mathfrak{p}(a) = v_\mathfrak{p}(a+b) = v_\mathfrak{p}(a-b) = 0$  and hence  $c \cdot (K_\mathfrak{p}^\times)^2$  is represented by an element of  $\mathcal{O}_\mathfrak{p}^\times$  by Lemma 2.2(i). Therefore, the congruence

$$v_\mathfrak{p}(c) \equiv 0 \pmod{2}$$

holds for all nonzero prime ideals  $\mathfrak{p} \notin S_0 \cup S_1 \cup \{q_1, q_2\}$  of  $\mathcal{O}_K$ . Since  $\mathcal{O}_{K,S_0}$  is a PID by our choice of  $S_0$ , we may assume that  $c \in \alpha$  was chosen so that  $v_\mathfrak{p}(c) = 0$  for all  $\mathfrak{p} \notin S_0 \cup S_1 \cup S_2 \cup \{q_1, q_2\}$ . We also have  $v_\mathfrak{p}(a) = v_\mathfrak{p}(a+b) = 0$  for all  $\mathfrak{p} \notin S_0 \cup S_1 \cup S_2 \cup \{q_1, q_2\}$  because of (3.13) and since  $(a, b) \in U_\mathfrak{p}$  for  $\mathfrak{p} \in S_3$ . Since  $v_{q_1}(a) = 1$ ,  $v_{q_2}(a) = 0$ ,  $v_{q_1}(a+b) = 0$  and  $v_{q_2}(a+b) = 1$ , we find that

$$c = ua^e(a+b)^{e'}$$

for unique integers  $e, e' \in \mathbb{Z}$  and a unique  $u \in \mathcal{O}_{K,S_0 \cup S_1 \cup S_2}^\times$ . After multiplying  $\alpha$  by an appropriate power of  $2a(a+b) \cdot (K^\times)^2 \in \text{Sel}_{\phi_d}(E_d/K)$  and using that 2 is a unit in  $\mathcal{O}_{K,S_0 \cup S_1 \cup S_2}$ , we may assume without loss of generality that  $c = ua^e$  with  $u \in \mathcal{O}_{K,S_0 \cup S_1 \cup S_2}^\times$  and  $e \in \mathbb{Z}$ . It suffices to show that  $c$  is a square in  $K^\times$ .

Consider the prime  $\mathfrak{p}_0 \in S_3$ . We know that  $c = ua^e$  is a square in  $K_{\mathfrak{p}_0}$  since  $\Phi_{d,\mathfrak{p}_0} = 1$ . Since  $u$  is a square in  $K_{\mathfrak{p}_0}$  by Lemma 3.5, we deduce that  $a^e$  is a square in  $K_{\mathfrak{p}_0}$ . However,  $(a, b) \in U_{\mathfrak{p}_0}$  implies that  $a$  is not a square in  $K_{\mathfrak{p}_0}$ . Therefore,  $e$  must be even. After replacing  $c$  by itself times a suitable square in  $K^\times$ , we may assume that  $c \in \mathcal{O}_{K,S_0 \cup S_1 \cup S_2}^\times$ .

For each complex place  $v$ , we trivially have  $\text{Im}(\delta_{d,v}) = 1 = \Phi_{d,v}$ . For each real place  $v$ , we have  $0 < a < b$  in  $K_v$  by our choice of  $a$  and  $b$  and hence  $2a(a+b)^2(a-b)d^2 < 0$  in  $K_v$ . For each real place  $v$ , Lemma 2.1(iii) then implies that  $\text{Im}(\delta_{d,v}) = 1 = \Phi_{d,v}$ . Therefore,  $c \cdot (K_v^\times)^2$  is an element of  $\Phi_{d,v}$  for all  $v \in S_0 \cup S_1 \cup S_\infty$ . In particular,  $c \cdot (\mathcal{O}_{K,S_0 \cup S_1 \cup S_2}^\times)^2$  lies in  $\ker \gamma_d := V_d$ .

For every  $\mathfrak{p} \in S_3$ ,  $\Phi_{d,\mathfrak{p}} = 1$  and hence  $c$  is a square in  $K_\mathfrak{p}$ . Since  $c \cdot (\mathcal{O}_{K,S_0 \cup S_1 \cup S_2}^\times)^2$  is in  $V_d$  and  $c \cdot (K_\mathfrak{p}^\times)^2 = (K_\mathfrak{p}^\times)^2$  for all  $\mathfrak{p} \in \{\mathfrak{p}_1, \dots, \mathfrak{p}_n\} \subseteq S_3$ , Lemma 3.4 implies that  $c \cdot (K^\times)^2$  is in the group generated by  $\pi_1 \cdot (K^\times)^2$ . After replacing  $c$  by itself times a suitable square in  $K^\times$ , we may assume that  $c = 1$  or  $c = \pi_1$ .

By Lemma 2.2(ii), we have  $\text{Im}(\delta_{d,q_3}) = 1$  and hence  $c$  is a square in  $K_{q_3}$ . By our choice of  $\varepsilon \in \{\pm 1\}$ , Lemma 3.7 implies that  $\pi_1$  is not a square in  $K_{q_3}$ . Therefore,  $c = 1$  which completes the proof.  $\square$

**Lemma 3.11.**

- (i) For  $d \in \{1, D\}$ , the group  $E'_d(K)/\phi_d(E_d(K))$  is isomorphic to  $\mathbb{Z}/2\mathbb{Z}$  and is generated by  $(0, 0)$ .
- (ii) The group  $E_D(K)/\hat{\phi}_D(E'_D(K))$  is isomorphic to  $\mathbb{Z}/2\mathbb{Z}$  and is generated by  $(0, 0)$ .
- (iii) The group  $E_1(K)/\hat{\phi}_1(E'_1(K))$  is isomorphic to  $(\mathbb{Z}/2\mathbb{Z})^2$  and is generated by  $P_0 := (0, 0)$  and  $P_1 := (-2a(a+b), 2a(a+b)^2)$ .

*Proof.* Take  $d \in \{1, D\}$ . From §2.1, there is an injective homomorphism

$$\delta_d: E'_d(K)/\phi_d(E_d(K)) \hookrightarrow \text{Sel}_{\phi_d}(E_d/K) \subseteq K^\times/(K^\times)^2$$

for which  $\delta_d((0, 0)) = 2a(a+b) \cdot (K^\times)^2$ . Part (i) is now immediate from Lemma 3.10; note that  $2a(a+b)$  is not a square in  $K^\times$  since its valuation with respect to the prime ideal  $\mathfrak{q}_1$  is 1. In particular,  $|\text{Sel}_{\phi_d}(E_d/K)| = 2$ .

By Lemma 3.9, we have  $|\text{Sel}_{\hat{\phi}_1}(E'_1/K)| = 4$  and  $|\text{Sel}_{\hat{\phi}_D}(E'_D/K)| = 2$ . From §2.1, there is an injective homomorphism

$$(3.16) \quad \delta'_d: E_d(K)/\hat{\phi}_d(E'_d(K)) \hookrightarrow \text{Sel}_{\hat{\phi}_d}(E'_d/K)$$

that satisfies  $\delta'_d((0, 0)) = 2a(a-b) \cdot (K^\times)^2$ . Note that  $2a(a-b)$  is not a square in  $K^\times$  since its valuation with respect to  $\mathfrak{q}_1$  is 1. When  $d = D$ , (3.16) is an isomorphism since  $|\text{Sel}_{\hat{\phi}_D}(E'_D/K)| = 2$ . This completes the proof of (ii).

Finally consider  $d = 1$ . Note that  $P_0$  and  $P_1$  are points in  $E_1(K)$ . By considering the valuations with respect to the prime ideals  $\mathfrak{q}_2$  and  $\mathfrak{q}_3$ , we find that  $\delta'_1(P_0) = 2a(a-b) \cdot (K^\times)^2$  and  $\delta'_1(P_1) = -2a(a+b) \cdot (K^\times)^2$  generate a subgroup of  $\text{Sel}_{\hat{\phi}_1}(E'_1/K)$  that has cardinality 4. Since  $\text{Sel}_{\hat{\phi}_1}(E'_1/K)$  has cardinality 4, we deduce that (3.16) is an isomorphism when  $d = 1$  and that the group  $E_1(K)/\hat{\phi}_1(E'_1(K))$  is generated by  $P_0$  and  $P_1$ .  $\square$

To finish the proof, we will show that  $E_1$  has rank 1 and  $E_D$  has rank 0. Take any  $d \in \{1, D\}$ . We have  $E_d(K)[2] = \{0, (0, 0)\}$  since the discriminant of  $x^2 + 4a(a+b)dx + 2a(a+b)^2(a-b)d^2$  is  $8a(a+b)^3d^2$  which is not a square in  $K$ ; it has valuation 1 with respect to the prime ideal  $\mathfrak{q}_1$ . We have  $\phi_d(E_d(K)[2]) = \phi_d(\langle(0, 0)\rangle) = 0$ . By the exact sequence (2.2) and Lemma 3.11(i), we find that the quotient map

$$E_d(K)/2E_d(K) \rightarrow E_d(K)/\hat{\phi}_d(E'_d(K))$$

is an isomorphism of groups. By Lemma 3.11(ii) and (iii), we obtain isomorphisms

$$(3.17) \quad E_1(K)/2E_1(K) \cong (\mathbb{Z}/2\mathbb{Z})^2 \quad \text{and} \quad E_D(K)/2E_D(K) \cong \mathbb{Z}/2\mathbb{Z}.$$

Since  $E_d(K)$  is a finitely generated abelian group with  $E_d(K)[2] \cong \mathbb{Z}/2\mathbb{Z}$ , we have

$$(3.18) \quad E_d(K)/2E_d(K) \cong (\mathbb{Z}/2\mathbb{Z})^{r_d+1},$$

where  $r_d$  is the rank of  $E_d(K)$ . From (3.17) and (3.18), we conclude that  $r_1 = 1$  and  $r_D = 0$ .

#### 4. PROOF OF THEOREMS 1.1 AND 1.2

We need only proof Theorem 1.2 since it clearly implies Theorem 1.1. Let  $L/K$  be any quadratic extension of number fields. Choose a  $D \in K^\times$  for which  $L = K(\sqrt{D})$ . With this  $K$  and  $D$ , we let  $S$  and  $\{U_p\}_{p \in S}$  be as in Theorem 1.5. We now apply Kai's result.

**Lemma 4.1.** *There are nonzero  $a, b \in \mathcal{O}_{K,S}$  such that  $a$ ,  $a + b$  and  $a - b$  generate distinct nonzero prime ideals of  $\mathcal{O}_{K,S}$ ,  $(a, b)$  lies in  $U_{\mathfrak{p}}$  for all  $\mathfrak{p} \in S$ , and  $0 < a < b$  in  $K_v$  for all real places  $v$  of  $K$ .*

*Proof.* For each  $\mathfrak{p} \in S$ , choose a pair  $(a_{\mathfrak{p}}, b_{\mathfrak{p}}) \in U_{\mathfrak{p}}$ . Since the sets  $U_{\mathfrak{p}}$  are open in  $K_{\mathfrak{p}}^2$  and  $S$  is finite, we can choose  $0 < \epsilon < 1/2$  such that  $\{(x, y) \in K_{\mathfrak{p}}^2 : |x - a_{\mathfrak{p}}|_{\mathfrak{p}} < \epsilon, |y - b_{\mathfrak{p}}|_{\mathfrak{p}} < \epsilon\} \subseteq U_{\mathfrak{p}}$  for all  $\mathfrak{p} \in S$ .

Using Proposition 13.2 of [Kai25] we find that there are nonzero  $a, b \in \mathcal{O}_{K,S}$  such that the following hold:

- $|a - a_{\mathfrak{p}}|_{\mathfrak{p}} < \epsilon$  and  $|b - b_{\mathfrak{p}}|_{\mathfrak{p}} < \epsilon$  for all  $\mathfrak{p} \in S$ ,
- $|a/b - 1/2|_v < \epsilon$  for all real places  $v$  of  $K$ ,
- $b > 0$  in  $K_v$  for all real places  $v$  of  $K$ ,
- $a$ ,  $a + b$  and  $a - b$  generate distinct prime ideals of  $\mathcal{O}_{K,S}$ .

From our choice of  $\epsilon$ , we have  $(a, b) \in U_{\mathfrak{p}}$  for all  $\mathfrak{p} \in S$ . Finally take any real place  $v$  of  $K_v$ . We have  $|a/b - 1/2|_v < \epsilon < 1/2$  and hence  $0 < a/b < 1$  in  $K_v$ . Since  $b > 0$  in  $K_v$ , we have  $0 < a < b$  in  $K_v$ .  $\square$

Take any  $a, b \in \mathcal{O}_{K,S}$  as in Lemma 4.1. By Theorem 1.5, the elliptic curve  $E_1$  over  $K$  defined by (1.1) has rank 1 and its quadratic twist  $E_D$  by  $D$  has rank 0. Since  $L = K(\sqrt{D})$  and  $E_D$  is the quadratic twist of  $E_1$  by  $D$ , we have

$$\text{rank } E_1(L) = \text{rank } E_1(K) + \text{rank } E_D(K);$$

this can be proved by using the action of  $\text{Gal}(L/K)$  on  $E(L) \otimes_{\mathbb{Z}} \mathbb{Q}$  and considering the eigenspaces of the nonidentity element of  $\text{Gal}(L/K)$ . Thus  $E_1(L)$  has rank  $1 + 0 = 1$ . Therefore,  $E_1$  is an elliptic curve over  $K$  for which  $E_1(K)$  and  $E_1(L)$  both have rank 1. It remains to show that there are infinitely many such elliptic curves up to isomorphism.

Let  $j \in K$  be the  $j$ -invariant of  $E_1$ . We have

$$j = 64 \frac{(5a + 3b)^3}{(a - b)^2(a + b)}.$$

For each  $\mathfrak{p} \in S$ , we let  $U'_{\mathfrak{p}}$  be the set of  $(x, y) \in U_{\mathfrak{p}}$  for which  $64(5x + 3y)^3 - j(x - y)^2(x + y) \neq 0$ . Since  $U_{\mathfrak{p}}$  is a nonempty open subset of  $K_{\mathfrak{p}}^2$  so is  $U'_{\mathfrak{p}}$ . Of course Theorem 1.5 will remain true if we replace each  $U_{\mathfrak{p}}$  by the smaller nonempty open set  $U'_{\mathfrak{p}}$ . By repeating the above argument with the smaller sets  $U'_{\mathfrak{p}}$ , we will obtain an elliptic curve  $E/K$  with  $\text{rank } E(K) = \text{rank } E(L) = 1$  whose  $j$ -invariant is not equal to  $j$ . Note that  $E_1$  and  $E$  are not isomorphic since they have different  $j$ -invariants. By repeating this process of shrinking  $U_{\mathfrak{p}}$  over and over to exclude certain  $j$ -invariants, we deduce that there are infinitely many elliptic curves  $E$  over  $K$  for which  $E(K)$  and  $E(L)$  both have rank 1.

## REFERENCES

- [ABHS25] Levent Alpöge, Manjul Bhargava, Wei Ho, and Ari Shnidman, *Rank stability in quadratic extensions and Hilbert's tenth problem for the ring of integers of a number field* (2025). arXiv:2501.18774.  $\uparrow$ 1.4, 1, 1.2
- [BS14] Manjul Bhargava and Christopher Skinner, *A positive proportion of elliptic curves over  $\mathbb{Q}$  have rank one*, J. Ramanujan Math. Soc. **29** (2014), no. 2, 221–242, DOI 10.1214/14-sts471.  $\uparrow$ 1
- [Cas65] J. W. S. Cassels, *Arithmetic on curves of genus 1. VIII. On conjectures of Birch and Swinnerton-Dyer*, J. Reine Angew. Math. **217** (1965), 180–199, DOI 10.1515/crll.1965.217.180.  $\uparrow$ 2.1

- [DD15] Tim Dokchitser and Vladimir Dokchitser, *Local invariants of isogenous elliptic curves*, Trans. Amer. Math. Soc. **367** (2015), no. 6, 4339–4358, DOI 10.1090/S0002-9947-2014-06271-5. ↑[2.1](#)
- [Kai25] Wataru Kai, *Linear patterns of prime elements in number fields* (2025). arXiv:2306.16983. ↑[1.2](#), [4](#)
- [KP24] Peter Koymans and Carlo Pagano, *Hilbert’s tenth problem via additive combinatorics* (2024). arXiv:2412.01768. ↑[1](#), [1.3](#), [1](#)
- [KP25] ———, *Elliptic curves of rank one over number fields* (2025). preprint. ↑[1](#)
- [MR10] B. Mazur and K. Rubin, *Ranks of twists of elliptic curves and Hilbert’s tenth problem*, Invent. Math. **181** (2010), no. 3, 541–575, DOI 10.1007/s00222-010-0252-0. ↑[1](#), [1](#)
- [Neu99] Jürgen Neukirch, *Algebraic number theory*, Grundlehren der mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], vol. 322, Springer-Verlag, Berlin, 1999. Translated from the 1992 German original and with a note by Norbert Schappacher; With a foreword by G. Harder. ↑[3.2](#), [3.3](#)
- [Sat87] Philippe Satgé, *Un analogue du calcul de Heegner*, Invent. Math. **87** (1987), no. 2, 425–439, DOI 10.1007/BF01389425 (French). ↑[1](#)
- [Sil83] Joseph H. Silverman, *Heights and the specialization map for families of abelian varieties*, J. Reine Angew. Math. **342** (1983), 197–211, DOI 10.1515/crll.1983.342.197. ↑[1.1](#)
- [Sil94] ———, *Advanced topics in the arithmetic of elliptic curves*, Graduate Texts in Mathematics, vol. 151, Springer-Verlag, New York, 1994. ↑[2.2](#)
- [Sil09] ———, *The arithmetic of elliptic curves*, 2nd ed., Graduate Texts in Mathematics, vol. 106, Springer, Dordrecht, 2009. ↑[2.1](#)
- [Zyw25a] David Zywina, *An elliptic surface with infinitely many fibers for which the rank does not jump* (2025). arXiv:2502.01026. ↑[1](#)
- [Zyw25b] ———, *There are infinitely many elliptic curves over the rationals of rank 2* (2025). arXiv:2502.01957. ↑[1](#)

DEPARTMENT OF MATHEMATICS, CORNELL UNIVERSITY, ITHACA, NY 14853, USA  
*Email address:* `zywina@math.cornell.edu`