ON THE INFINITUDE OF ELLIPTIC CURVES OVER A NUMBER FIELD WITH PRESCRIBED SMALL RANK

DAVID ZYWINA

Abstract. For any number field K and integer $0 \leq r \leq 4$, we prove that there are infinitely many elliptic curves over K of rank r. Our elliptic curves are obtained by specializing well-chosen nonisotrivial elliptic curves over the function field $K(T)$ at elements of K. We use a result of Kai, which generalizes work of Green, Tao and Ziegler to number fields, to choose our specializations so that we have control over the bad primes and can perform a 2-descent to obtain an optimal upper bound on the rank.

1. Introduction

Let K be a 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 $E(K)$.

There are two natural questions concerning the distribution of ranks. What integers occur as the rank of an elliptic curve over K? What integers occur as the rank of infinitely many elliptic curves over K? Our main theorem addresses these questions for small ranks. Let $\overline{K}$ be an algebraic closure of K.

Theorem 1.1. *For any number field K and integer $0 \leq r \leq 4$, there are infinitely many elliptic curves E over K, up to isomorphism over $\overline{K}$, of rank r.*

This theorem covers all cases of number fields K and integers r for which it known that there are infinite many elliptic curve over K of rank r, cf. §1.1 for earlier results.

We state the following immediate consequence to emphasize that even the existence of an elliptic curve of a given rank is a nontrivial result when working over a general number field.

Corollary 1.2. *For any number field K and integer $0 \leq r \leq 4$, there is an elliptic curve E over K of rank r.*

There is a natural method for constructing many elliptic curves of large rank. From Elkies [Elk07, II], there is a nonisotrivial elliptic curve E over the function field $\mathbb{Q}(T)$ so that the finitely generated group $E(\mathbb{Q}(T))$ has rank 18. A theorem of Silverman [Sil83] then implies that for all but finitely many $t \in K$, specializing a fixed Weierstrass model of E at t produces an elliptic curve E_t over K of rank *at least* 18. Unfortunately, it is unclear how to compute the rank of E_t for infinitely many $t \in K$. For each $0 \leq r \leq 4$, our theorem is proved by using a specific nonisotrivial elliptic curve $E/\mathbb{Q}(T)$ of rank r and showing that there are infinitely many $t \in K$ for which E_t/K has rank r.

Concerning what ranks actually occur over a fixed number field, it is not even clear if they are uniformly bounded, cf. [PPVW19, §3] for a brief history on the problem. In [PPVW19], a heuristic is given for uniformly bounded ranks which predicts that there are infinitely many

2020 *Mathematics Subject Classification.* Primary 11G05; Secondary 14J27.

elliptic curves over $\mathbb{Q}$ of rank r for each $0 \leq r \leq 20$ and that there are only finitely many elliptic curves over $\mathbb{Q}$ of rank greater than 21.

1.1. **Earlier results.** The $r = 0$ case of Theorem 1.1 was proved by Mazur and Rubin, cf. [MR10, Theorem 1.11]. The $r = 1$ case of Theorem 1.1 was until recently known only for a few number fields K; for example, see [Sat87, Théorème 3.1] or [BS14] for $K = \mathbb{Q}$.

Other special cases of Theorem 1.1 are very recent. With $K = \mathbb{Q}$, the $r = 2$ case of Theorem 1.1 was proved in [Zyw25b]. The full $r = 1$ case was proved in [Zyw25c] and also independently by Koymans and Pagano [KP25] who built off their ideas in [KP24]. In [Sav25], it is shown that there are infinitely many elliptic curves over $\mathbb{Q}(i)$ of rank 2 however they all have j-invariant 1728.

The basic strategy in the author's recent rank papers [Zyw25a, Zyw25b, Zyw25c] is to consider a well-chosen nonisotrivial E over a function field $K(T)$ that has rank r and to prove that the specialization E_t over K also has rank r for infinitely many $t \in K$. In [KP25], rank 1 elliptic curves over K are constructed by considering quadratic twists of a "generic" elliptic over K with full 2-torsion.

1.2. **Overview.** We give some motivation for our proof in the optional section §2. In §3, we recall what we need on Selmer groups and compute some local conditions. In §4, we state an axiomatic version of our theorem which is proved in §5. Finally in §6, we use five explicit elliptic curves $E/K(T)$ to prove Theorem 1.1 for each $0 \leq r \leq 4$ by applying our axiomatic version.

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 $v_\mathfrak{p}(K^\times) = \mathbb{Z}$.

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 finite, we let $\mathcal{O}_v$ be the valuation subring of K_v. Note that 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. Ideas and motivation

We now describe some strategy and motivation for our proof; this will not be used later and can be safely skipped. Let K be a number field. We will identify $K(T)$ with the function field of $\mathbb{P}^1_K = \operatorname{Spec} K[T] \cup \{\infty\}$.

Consider a nonisotrivial elliptic curve E over $K(T)$ defined by a Weierstrass of the form

$$y^2 = x^3 + ax^2 + bx$$

with $a, b \in K[T]$ and is minimal over $K[T]$. The point $(0,0) \in E(K(T))$ has order 2. There is a degree 2 isogeny $\phi\colon E \to E'$ whose kernel is generated by $(0,0)$, where E' is the elliptic curve over $K(T)$ defined by

$$y^2 = x^3 + a'x^2 + b'x$$

with $a' := -2a$ and $b' := a^2 - 4b$. We assume that the groups $E(K(T))$ and $E'(K(T))$ are known.

Let $\pi\colon \mathscr{E} \to \mathbb{P}^1_K$ be the smooth minimal elliptic surface corresponding to $E/K(T)$. Let $\mathcal{B}$ be the (finite) set of points in $\mathbb{P}^1(K)$ over which the fiber of π is singular. After replacing T

by another generator of the function field of $\mathbb{P}^1_K$ over K and changing the Weierstrass model, we may assume that $\mathcal{B}$ is a subset of $\mathcal{O}_K \subseteq K \cup \{\infty\} = \mathbb{P}^1(K)$.

Let $\Delta \in K[T]$ be the discriminant of our Weierstrass model. Note that $\mathcal{B}$ is the set of roots of Δ in K. For each $t \in K - \mathcal{B}$, specializing our model at t gives an elliptic curve E_t over K defined by the equation $y^2 = x^3 + a(t)x^2 + b(t)x$. We also have an elliptic curve E'_t over K defined by $y^2 = x^3 + a'(t)x^2 + b'(t)x$. Using that the fiber of π over ∞ is smooth, one can show that here is a finite set S of nonzero prime ideals of $\mathcal{O}_K$ such that for each $t \in K - \mathcal{B}$, E_t has good reduction at a nonzero prime ideal $\mathfrak{p} \notin S$ of $\mathcal{O}_K$ if and only if $\Delta(t)$ has positive $\mathfrak{p}$-adic valuation.

The abelian group $E(K(T))$ is finitely generated and we denote its rank by r. From Silverman [Sil83], specialization defines an injective homomorphism $E(K(T)) \to E_t(K)$ for all but finitely many $t \in K - \mathcal{B}$. In particular, we have

$$\operatorname{rank} E_t(K) \geq r$$

for all but finitely many $t \in K - \mathcal{B}$. The challenge is to prove the existence of $t \in K - \mathcal{B}$ for which $E(K)$ has rank *exactly* r. A *minimalist conjecture* loosely predicts that the density of $t \in K - \mathcal{B}$ for which E_t has rank r will have positive density (the heuristic being that a typical curve over K in the family should have the smallest possible rank that is compatible with the parity conjecture).

The main approach to computing upper bounds of ranks is via Selmer groups. In our case, we will perform descent by 2-isogeny, cf. §3.1 for details. Take any $t \in K - \mathcal{B}$. There is an isogeny $\phi_t \colon E_t \to E'_t$ of degree 2 whose kernel is generated by $(0,0)$. Using group cohomology, we will obtain a group homomorphism

$$\delta_{E'_t} \colon E'_t(K) \to K^\times/(K^\times)^2$$

with kernel $\phi_t(E(K))$ that satisfies $\delta_{E'_t}((x,y)) = x \cdot (K^\times)^2$ for $(x,y) \in E'_t(K) - \{0, (0,0)\}$ and $\delta_{E'_t}((0,0)) = a'(t) \cdot (K^\times)^2$. Similarly for each place v of K, we have a homomorphism $\delta_{E'_t,v} \colon E'_t(K_v) \to K_v^\times/(K_v^\times)^2$.

We can define the ϕ_t-*Selmer group* $\operatorname{Sel}_{\phi_t}(E_t/K)$ to be the subgroup of $K^\times/(K^\times)^2$ consisting of those cosets whose image in $K_v^\times/(K_v^\times)^2$ lies in the image of $\delta_{E'_t,v}$ for all places v of K. The group $\operatorname{Sel}_{\phi_t}(E_t/K)$ is finite and $\delta_{E'_t}$ induces an injective homomorphism

$$E'_t(K)/\phi_t(E_t(K)) \hookrightarrow \operatorname{Sel}_{\phi_t}(E_t/K).$$

Similarly, we have a group homomorphism $\delta_{E_t} \colon E_t(K) \to K^\times/(K^\times)^2$ that induces an injective homomorphism

$$E_t(K)/\hat{\phi}_t(E'_t(K)) \hookrightarrow \operatorname{Sel}_{\hat{\phi}_t}(E'_t/K),$$

where $\hat{\phi}_t \colon E'_t \to E_t$ is the dual isogeny of ϕ_t. Viewing our groups as vector spaces over $\mathbb{F}_2$, we have

$$\operatorname{rank} E_t(K) = \dim_{\mathbb{F}_2} \delta_{E_t}(E_t(K)) + \dim_{\mathbb{F}_2} \delta_{E'_t}(E'_t(K)) - 2.$$

cf. Lemma 3.1, which gives the upper bound

$$\operatorname{rank} E_t(K) \leq \dim_{\mathbb{F}_2} \operatorname{Sel}_{\hat{\phi}_t}(E'_t/K) + \dim_{\mathbb{F}_2} \operatorname{Sel}_{\phi_t}(E_t/K) - 2.$$

The Selmer groups $\operatorname{Sel}_{\hat{\phi}_t}(E'_t/K)$ and $\operatorname{Sel}_{\phi_t}(E_t/K)$ are in principle computable and hence we have a computable upper bound for the rank of E_t. Unfortunately, the computation of

Selmer groups requires knowledge of the primes of bad reduction of E_t which is difficult to control if we are varying over infinitely many t.

To control the primes of bad reduction, we will make the additional assumption that $\mathcal{B}$ is also the the set of points in $\mathbb{P}^1(\overline{K})$ over which the fiber of π is singular. Equivalently, Δ factors into linear polynomials in $K[T]$.

Let $\mathcal{O}_{K,S}$ be the ring of S-integers in K and let S_∞ be the set of archimedean places of K. For each $v \in S$, fix a nonempty open subset U_v of K_v^2. For each place $v \in S_\infty$, fix a nonempty open subset U_v of K_v. We will make use of a result of Kai [Kai25, Proposition 13.2] which implies that there are nonzero $m, n \in \mathcal{O}_{K,S}$ such that the following hold:

- $m - en$ with $e \in \mathcal{B}$ generate distinct prime ideals of $\mathcal{O}_{K,S}$,
- (m, n) lies in U_v for all $v \in S$,
- m/n lies in U_v for all $v \in S_\infty$.

Kai's theorem is a generalization of work of Green, Tao and Ziegler to number fields. After possibly increasing S first and taking $t := m/n \in K$ with m and n as above, E_t has bad reduction at a nonzero prime ideal $\mathfrak{p} \notin S$ of $\mathcal{O}_K$ if and only if $\mathfrak{p}\mathcal{O}_{K,S} = (m - en)\mathcal{O}_{K,S}$ for some $e \in \mathcal{B}$. The type of reduction that E_t has a prime ideal $\mathfrak{p} \in S$ can be imposed by making suitable choice of $U_\mathfrak{p}$. By shrinking the sets U_v, we may assume that $\operatorname{rank} E_t(K) \geq r$ always holds when $t := m/n$.

The goal is to possible extend the finite set S and choose sets $\{U_v\}_{v \in S \cup S_\infty}$ appropriately so that, with m and n as above and $t := m/n$, the local conditions imposed guarantee that the homomorphisms

$$E(K(T)) \to E_t(K) \xrightarrow{\delta_{E_t}} \mathrm{Sel}_{\hat{\phi}_t}(E'_t/K) \tag{2.1}$$

and

$$E'(K(T)) \to E'_t(K) \xrightarrow{\delta_{E'_t}} \mathrm{Sel}_{\phi_t}(E_t/K) \tag{2.2}$$

are both surjective. If (2.1) and (2.2) were surjective, then we would know the image of δ_{E_t} and $\delta_{E'_t}$ from which we could deduce the upper bound $\operatorname{rank} E_t(K) \leq r$ and thus prove that $\operatorname{rank} E_t(K) = r$.

We still might have the inequality $\operatorname{rank} E_t(K) \leq r$ even if one of the homomorphisms (2.1) or (2.2) is not surjective; in this case one can show that $Ш(E_t/K)[2] \neq 0$ or $Ш(E'_t/K)[2] \neq 0$. In §4, we give additional conditions on E to ensure this surjectivity and hence avoid 2-torsion in our Tate–Shafarevich groups; many of the conditions are constraints on the singular fibers of $\mathscr{E} \to \mathbb{P}^1_K$.

Let $\mathcal{N}$ be the *conductor* of the elliptic surface $\pi\colon \mathscr{E} \to \mathbb{P}^1_K$, i.e., the divisor of $\mathbb{P}^1_K$ supported on the closed points of $\mathbb{P}^1_K$ over which the fiber of π is singular and each such point has multiplicity 1 if the fiber is multiplicative and multiplicity 2 if the fiber is additive. There is a simple upper bound

$$r = \operatorname{rank} E(K(T)) \leq \operatorname{rank} E(\overline{K}(T)) \leq \deg \mathcal{N} - 4,$$

cf. [Shi92, Corollary 2]. In §4, we will impose conditions that imply that $\operatorname{rank} E(K(T)) = \deg \mathcal{N} - 4$. Having "maximal rank" will make the proof easier and in particular make it easier to find $t = m/n$ for which (2.1) and (2.2) are surjective. This is strong constraint on E and it implies that the surface $\mathscr{E}$ has geometric genus 0, cf. [Shi92, equation (1.13′)]. For the explicit $E/K(T)$ we will consider, $\mathscr{E}$ will be a rational elliptic surface with a 2-torsion point and hence $r \leq 4$ by [OS91, Corollary 2.1].

In our proof of Theorem 1.1, we will use an explicit elliptic curve $E/K(T)$ for each $0 \leq r \leq 4$. For example when $r = 4$, we will make use of the elliptic curve E over $K(T)$ defined by the Weierstrass equation

$$y^2 = x^3 - 70(T^2 - 25^2) \cdot x^2 + 2^4 7^2 (T^2 - 11^2)(T^2 - 25^2) \cdot x$$

whose discriminant is

$$\Delta = 2^{14} 3^2 7^6 (T - 11)^2 (T + 11)^2 (T - 25)^3 (T + 25)^3 (T - 39)(T + 39).$$

The set of points of $\mathbb{P}^1_K$ over which the corresponding elliptic surface $\mathscr{E} \to \mathbb{P}^1_K$ is singular is $\mathcal{B} := \{\pm 11, \pm 25, \pm 39\}$. The conductor of E is $\mathcal{N} = (-11) + (11) + (-39) + (39) + 2 \cdot (-25) + 2 \cdot (25)$ and hence $\operatorname{rank} E(K(T)) \leq \deg \mathcal{N} - 4 = 4$. In fact, $E(K(T))$ has rank 4. Moreover, $E(K(T))$ is isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}^4$ and is generated by the 2-torsion point $(0, 0)$ and the following independent points:

$$\begin{aligned}
&(14(T - 11)(T + 11), 1176(T - 11)(T + 11)),\\
&(2(T - 11)(T - 25), 12(3T + 65)(T - 11)(T - 25)),\\
&(14(T - 25)(T + 25), 2352(T - 25)(T + 25)),\\
&(8(T + 11)(T + 25), -48(T + 11)(T + 25)(T - 45)).
\end{aligned}$$

Our proof will show that the elliptic curve E_t over K has rank 4 for infinitely many $t \in K - \mathcal{B}$.

3. Background on descent

We recall some background on descent by a 2-isogeny. See [Sil09, §X.4], and in particular [Sil09, §X.4 Example 4.8], for the basics.

3.1. **2-descent.** Fix a field K of characteristic 0 and let $\overline{K}$ be a fixed algebraic closure.

Let E be an elliptic curve over K with a fixed K-rational point P_0 of order 2. There is a degree 2 isogeny $\phi\colon E \to E'$ whose kernel is generated by P_0. Let $\hat{\phi}\colon E' \to E$ be the dual isogeny of ϕ. We can choose a Weierstrass model for E of the form

$$y^2 = x^3 + ax^2 + bx \tag{3.1}$$

with $a, b \in K$ and $P_0 = (0, 0)$. We may take E' to be the elliptic curve over K defined by the Weierstrass equation $y^2 = x^3 + a'x^2 + b'x$, where $a' := -2a$ and $b' := a^2 - 4b$, and take $\phi\colon E \to E'$ to be

$$\phi(x, y) = (y^2/x^2, y(b - x^2)/x^2).$$

The kernel of $\hat{\phi}$ is generated by the 2-torsion point $(0, 0)$ of E'.

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

$$0 \to \ker \phi \to E(K) \xrightarrow{\phi} E'(K) \xrightarrow{\delta_{E'}} H^1(\mathrm{Gal}_K, \ker \phi).$$

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

$$H^1(\mathrm{Gal}_K, \ker \phi) \xrightarrow{\sim} H^1(\mathrm{Gal}_K, \{\pm 1\}) \xrightarrow{\sim} K^\times/(K^\times)^2. \tag{3.2}$$

Using the isomorphism (3.2), we may view $\delta_{E'}$ as a homomorphism

$$\delta_{E'}\colon E'(K) \to K^\times/(K^\times)^2$$

whose kernel is $\phi(E(K))$. In particular, we can identify $E'(K)/\phi(E(K))$ with a subgroup of $K^\times/(K^\times)^2$. For any point $(x, y) \in E'(K) - \{0, (0, 0)\}$, we have

$$\delta_{E'}((x, y)) = x \cdot (K^\times)^2.$$

We also have $\delta_{E'}(0) = 1$ and $\delta_{E'}((0, 0)) = b' \cdot (K^\times)^2$.

In the same manner, we obtain a homomorphism $\delta_E\colon E(K) \to K^\times/(K^\times)^2$ with kernel $\hat{\phi}(E'(K))$ that satisfies $\delta_E((x, y)) = x \cdot (K^\times)^2$ for $(x, y) \in E(K) - \{0, (0, 0)\}$ and $\delta_E((0, 0)) = b \cdot (K^\times)^2$. We now show that the images of δ_E and $\delta_{E'}$ determine the rank of E.

Lemma 3.1. *If $E(K)$ is a finitely generated abelian group of rank r, then*

$$r = \dim_{\mathbb{F}_2} \delta_E(E(K)) + \dim_{\mathbb{F}_2} \delta_{E'}(E'(K)) - 2.$$

Proof. Since $E(K)$ is a finitely generated abelian group of rank r, the group $E(K)/2E(K)$ is finite and we have $\dim_{\mathbb{F}_2} E(K)/2E(K) = r + \dim_{\mathbb{F}_2} E(K)[2]$. There is an exact sequence

$$0 \to \frac{\langle(0, 0)\rangle}{\phi(E(K)[2])} \to \frac{E'(K)}{\phi(E(K))} \xrightarrow{\hat{\phi}} \frac{E(K)}{2E(K)} \to \frac{E(K)}{\hat{\phi}(E'(K))} \to 0. \tag{3.3}$$

We have $\dim_{\mathbb{F}_2} \langle(0, 0)\rangle/\phi(E(K)[2]) = 1 - (\dim_{\mathbb{F}_2} E(K)[2] - 1) = 2 - \dim_{\mathbb{F}_2} E(K)[2]$ and hence from (3.3) we find that $\dim_{\mathbb{F}_2} E(K)/2E(K)$ is equal to

$$\dim_{\mathbb{F}_2} E(K)/\hat{\phi}(E'(K)) + \dim_{\mathbb{F}_2} E'(K)/\phi(E(K)) - (2 - \dim_{\mathbb{F}_2} E(K)[2]).$$

The lemma follows by combining our two expressions for $\dim_{\mathbb{F}_2} E(K)/2E(K)$ and using the isomorphisms $\delta_E(E(K)) \cong E(K)/\hat{\phi}(E'(K))$ and $\delta_{E'}(E'(K)) \cong E'(K)/\phi(E(K))$. ☐

3.2. **Number field case.** Now assume further that K is a number field. Take any place v of K. Applying the construction of §3.1 with E base changed to K_v we obtain a homomorphism

$$\delta_{E',v}\colon E'(K_v) \to K_v^\times/(K_v^\times)^2$$

with kernel $\phi(E(K_v))$. We can identify the ϕ-Selmer group of E/K, which we denote by $\mathrm{Sel}_\phi(E/K)$, 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 $\mathrm{Im}(\delta_{E',v})$ for all places v of K. The image of $\delta_{E'}$ lies in $\mathrm{Sel}_\phi(E/K)$ and hence we have an injective homomorphism

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

Similar, we have an injective homomorphism $E(K)/\hat{\phi}(E'(K)) \hookrightarrow \mathrm{Sel}_{\hat{\phi}}(E'/K)$. These Selmer groups are finite and are in principle computable. Using Lemma 3.1, these Selmer groups give an upper bound on the rank of E. The following lemma links their cardinalities.

Lemma 3.2.

(i) *We have*

$$|\mathrm{Sel}_\phi(E/K)|/|\mathrm{Sel}_{\hat{\phi}}(E'/K)| = \prod_v \tfrac{1}{2}|\mathrm{Im}(\delta_{E',v})|,$$

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*

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

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

Proof. This was shown in [Zyw25c, Lemma 2.1]. Part (i) was a consequence of a result of Cassels [Cas65] and part (ii) was deduced from [DD15]. □

3.3. **Some local computations.** Let R be a complete discrete valuation ring and let K be its fraction field. Let $\mathfrak{m}$ be the maximal ideal of R and let $k = R/\mathfrak{m}$ be the residue field. Assume that k does not have characteristic 2.

Now fix an elliptic curve E over K as in §3.1. With notation as in §3.1, we have an elliptic curve E' over K and a homomorphism

$$\delta_{E'}\colon E'(K) \to K^\times/(K^\times)^2.$$

We can identify $R^\times/(R^\times)^2$ with a subgroup of $K^\times/(K^\times)^2$. Using the discrete valuation ring R, we can apply Tate's algorithm [Sil94, Algorithm 9.4] to the curves E and E' to obtain Kodaira symbols.

Lemma 3.3. *Suppose that E and E' have Kodaira symbol I_{2n} and I_n, respectively, for some $n \geq 0$.*

(i) *If E has split multiplicative reduction or n is odd, then $\operatorname{Im}(\delta_{E'}) = 1$.*
(ii) *If E and E' have good reduction, i.e., $n = 0$, then $\operatorname{Im}(\delta_{E'}) \subseteq R^\times/(R^\times)^2$.*

Proof. Let $v\colon K \to \mathbb{Z} \cup \{+\infty\}$ be the discrete valuation normalized so that $v(K^\times) = \mathbb{Z}$. Choose an element $\pi \in R$ for which $v(\pi) = 1$. Since R is a complete discrete valuation ring and k has characteristic not equal to 2, we find that an element of $R^\times$ is a square if and only if its image in k is a square.

We may choose a model (3.1) for E/K with coefficients in R that is a minimal Weierstrass model over R. The curve E'/K is given by the model $y^2 = x^3 - 2ax + (a^2 - 4b)x$. By our assumptions on the Kodaira symbols, we have $n = v(b)$ and $a^2 - 4b \in R^\times$. In particular, $(a^2 - 4b)\cdot(K^\times)^2$ lies in $R^\times/(R^\times)^2 \subseteq K^\times/(K^\times)^2$.

Suppose that $n \geq 1$. We have $v(a) = 0$ since otherwise $v(a^2 - 4b) > 0$. Observe that $a^2 - 4b$ is a square in $K^\times$ since $a^2 - 4b$ lies in $R^\times$ and $a^2 - 4b \equiv a^2 \pmod{\mathfrak{m}}$. Therefore, $(a^2 - 4b)\cdot(K^\times)^2 = 1$ when $n \geq 1$.

Now take any $\alpha \in \operatorname{Im}(\delta_{E'}) - \{1, (a^2-4b)\cdot(K^\times)^2\}$. We have $\alpha = d\cdot(K^\times)^2$ for some $d \in K^\times$ that satisfies $v(d) \in \{0,1\}$. Therefore, $\alpha = \delta_{E'}((x,y))$ for some $(x,y) \in E'(K)$ where $x = dz^2$ with $z \in K^\times$. We have $y^2 = x^3 - 2ax^2 + (a^2-4b)x$ and hence

$$w^2 = dz^4 - 2az^2 + (a^2-4b)/d \tag{3.4}$$

for some $w \in K$. Since d is not a square in K we deduce that d is not square modulo $\mathfrak{m}$ when $v(d) = 0$.

Suppose that $v(z) < 0$. We have $v(dz^4) = 4v(z) + v(d) \leq 4v(z) + 1$. Therefore, $v(dz^4) < 2v(z) \leq v(-2az^2)$ and $v(dz^4) < -1 \leq v((a^2-4b)/d)$. From (3.4) and these valuations, we deduce that $2v(w) = v(w^2)$ is equal to $v(dz^4) = 4v(z)+v(d)$. This gives a contradiction when $v(d)$ is odd, so we have $v(d) = 0$ and $v(w) = 2v(z)$. With $e := -v(z)$, we have $z = \pi^{-e}z_0$ and $w = \pi^{-2e}w_0$ with $w_0, z_0 \in R^\times$. Multiplying both sides of (3.4) by π^{4e} and reducing modulo $\mathfrak{m}$, we deduce that $w_0^2 \equiv dz_0^4 \pmod{\mathfrak{m}}$. Thus d is a square modulo $\mathfrak{m}$ which is a contradiction.

Suppose that $v(z) \geq 0$ and $v(d) = 1$. From (3.4) we deduce that $2v(w) = v(w^2)$ equals $v((a^2 - 4b)/d) = -v(d) = -1$ which gives a contradiction.

Suppose that $v(z) > 0$ and $v(d) = 0$. From (3.4) we deduce that $2v(w) = v(w^2)$ equals $v((a^2 - 4b)/d) = -v(d) = 0$. So $w \in R^\times$ and $w^2 \equiv (a^2 - 4b)/d \pmod{\mathfrak{m}}$. Since $(a^2 - 4b)/d$ lies in $R^\times$ and is a square modulo $\mathfrak{m}$, we deduce that $(a^2 - 4b)/d$ is a square in K. However, this is impossible since $\alpha = d \cdot (K^\times)^2$ was chosen not to be equal to $(a^2 - 4b) \cdot (K^\times)^2$.

From the above cases, we find that $v(z) = 0$ and $v(d) = 0$. Since $d \in R^\times$, we have $\alpha \in R^\times/(R^\times)^2$. This completes the proof of (ii). We may now assume that $n \geq 1$ and hence $v(a) = 0$. Multiplying (3.4) by d and completing the square gives

$$dw^2 = (dz^2 - a)^2 - 4b. \tag{3.5}$$

We have $w \in R$ and reducing gives $dw^2 \equiv (dz^2 - a)^2 \pmod{\mathfrak{m}}$. Since d is not a square modulo $\mathfrak{m}$, we must have $dz^2 - a \equiv 0 \pmod{\mathfrak{m}}$. The congruence $dz^2 \equiv a \pmod{\mathfrak{m}}$ and $v(d) = v(a) = 0$ implies that $\alpha = d \cdot (K^\times)^2 = a \cdot (K^\times)^2$.

Suppose that E has split reduction. Since $v(a) = 0$, this implies that a is a square modulo $\mathfrak{m}$ and hence a is a square in K. We have $\alpha = a \cdot (K^\times)^2 = 1$ which contradicts our choice of α.

Suppose that n is odd. Since $v(b) = n$ is odd and $v(d) = 0$, (3.5) implies that the even integers $v(dw^2)$ and $v((dz^2 - a)^2)$ agree. So there is an integer e such that $w = \pi^e w_0$ and $dz^2 - a = \pi^e u_0$ with $u_0, w_0 \in R^\times$. Dividing (3.5) by π^{2e} gives $dw_0^2 = u_0^2 - 4b/\pi^{2e}$. Since $v(b)$ is odd, this implies that $dw_0^2 \equiv u_0^2 \pmod{\mathfrak{m}}$ which contradicts that d is not a square modulo $\mathfrak{m}$.

In the setting of (i), we have now proved that $\delta_{E'}$ has trivial image. $\square$

4. General theorem

Let K be a number field. Let E be an elliptic curve defined over the function field $K(T)$ with a fixed point $P_0 \in E(K(T))$ of order 2. There is a degree 2 isogeny $\phi\colon E \to E'$ whose kernel is generated by P_0. Using the isogeny ϕ and its dual, we obtain group homomorphisms

$$\delta_E\colon E(K(T)) \to K(T)^\times/(K(T)^\times)^2 \quad \text{and} \quad \delta_{E'}\colon E'(K(T)) \to K(T)^\times/(K(T)^\times)^2$$

as in §3.1.

We will identify $K(T)$ with the function field of $\mathbb{P}^1_K = \operatorname{Spec} K[T] \cup \{\infty\}$. For a closed point P of $\mathbb{P}^1_K$, let v_P be the corresponding discrete valuation of $K(T)$. Let K_P be the completion of K with respect to v_P and let $\mathcal{O}_P$ be its valuation ring. After base extending our curves E and E' to K_P we can apply Tate's algorithm to obtain Kodaira symbols and Tamagawa numbers $c_P(E)$ and $c_P(E')$.

Let $\mathcal{B}$ be the set of closed points of $\mathbb{P}^1_K$ over which E has bad reduction. Let $\mathcal{A}$ be the set of points in $\mathcal{B}$ over which E has additive reduction. Let $\mathcal{M}$ be the set of $P \in \mathcal{B} - \mathcal{A}$ for which the the Kodaira symbol of E and E' at P is I_{2n} and I_n, respectively, for some $n \geq 1$. Let $\mathcal{M}'$ be the set of $P \in \mathcal{B} - \mathcal{A}$ for which the the Kodaira symbol of E and E' at P is I_n and I_{2n}, respectively, for some $n \geq 1$. We have a disjoint union

$$\mathcal{B} = \mathcal{A} \cup \mathcal{M} \cup \mathcal{M}'.$$

We also impose the following additional conditions on E and E':

(a) Every point in $\mathcal{B}$ has degree 1; equivalently, $\mathcal{B}$ can be viewed as a subset of $\mathbb{P}^1(K)$.
(b) The sets $\mathcal{M}$ and $\mathcal{M}'$ are nonempty.
(c) For every point $P \in \mathcal{M}$, the curve E' has split multiplicative reduction at P or its Kodaira symbol at P is I_n for some odd n.
(d) For every point $P \in \mathcal{M}'$, the curve E has split multiplicative reduction at P or its Kodaira symbol at P is I_n for some odd n.
(e) If the Kodaira symbol of E at a point $P \in \mathcal{A}$ is I_n^* for some $n \geq 0$, then $c_P(E) = c_P(E') = 4$.
(f) We have $\dim_{\mathbb{F}_2} \delta_E(E(K(T))) \geq |\mathcal{A}| + |\mathcal{M}| - 1$.
(g) We have $\dim_{\mathbb{F}_2} \delta_{E'}(E'(K(T))) \geq |\mathcal{A}| + |\mathcal{M}'| - 1$.

Define the integer

$$r := 2|\mathcal{A}| + |\mathcal{M}| + |\mathcal{M}'| - 4.$$

By the Lang–Néron theorem, we know that $E(K(T))$ is a finitely generated abelian group. By Lemma 3.1 with conditions (f) and (g), we find that $\operatorname{rank} E(K(T)) \geq r$. However, the rank of $E(K(T))$ is at most r by [Shi92, Corollary 2] and (a). Therefore,

$$r = \operatorname{rank} E(K(T)).$$

Given an explicit Weierstrass model of E, we can specialize it at all but finitely many $t \in K$ to obtain an elliptic curve E_t over K. Our main result is the following theorem which will be proved in §5.

Theorem 4.1. *With assumptions as above, there are infinitely many $t \in K$ for which $E_t(K)$ has rank r. In particular, there are infinitely many elliptic curves over K, up to isomorphism over $\overline{K}$, that have rank r.*

5. Proof of Theorem 4.1

Set $L := K(T)$. After possibly replacing T by another element that generates the field L over K, we may assume without loss of generality that

$$\mathcal{B} \subseteq \mathcal{O}_K \subseteq K \cup \{\infty\} = \mathbb{P}^1(K).$$

We can choose a Weierstrass model

$$y^2 = x^3 + ax^2 + bx \tag{5.1}$$

of E with $a, b \in \mathcal{O}_K[T]$ so that $P_0 = (0,0)$ is our fixed 2-torsion point. We may further assume that the Weierstrass model (5.1) is minimal over the PID $K[T]$. From §3.1, we may assume that E' is given by the Weierstrass model $y^2 = x^3 - 2ax^2 + (a^2 - 4b)x$. The discriminant of our models for E and E' are $\Delta = 16(a^2 - 4b)b^2$ and $\Delta' = 16(a^2 - 4b)^2 b$, respectively.

Using the minimality of this model for E, we can now explicitly describe the sets $\mathcal{B}$, $\mathcal{A}$, $\mathcal{M}$ and $\mathcal{M}'$ in terms of a and b. From condition (a) and $\mathcal{B} \subseteq \mathcal{O}_K$, we find that $\mathcal{B}$ is the set of roots in $\overline{K}$ of the polynomial Δ. The set $\mathcal{M}$ is equal to the set of roots of b that are not roots of $a^2 - 4b$. The set $\mathcal{M}'$ is equal to the set of roots of $a^2 - 4b$ that are not roots of b. The set $\mathcal{A}$ is equal to the set of common roots of $a^2 - 4b$ and b.

Note that with these Weierstrass equations, the specializations E_t and E'_t are well-defined for all $t \in K - \mathcal{B}$.

5.1. **Geometric Mordell–Weil.** We can choose points $e_0 \in \mathcal{M}$ and $e_0' \in \mathcal{M}'$ by condition (b). Let $\mathscr{F}$ be the set of squarefree polynomials $f \in K[T]$ that divide b, have even degree, and satisfy $f(e_0') = 1$. Let $\mathscr{F}'$ be the set of squarefree polynomials $f \in K[T]$ that divide $a^2 - 4b$, have even degree, and satisfy $f(e_0) = 1$. We can now describe the image of δ_E and $\delta_{E'}$.

Lemma 5.1.

(i) *We have* $\delta_E(E(K(T))) = \{f \cdot (K(T)^\times)^2 : f \in \mathscr{F}\}$.

(ii) *We have* $\delta_{E'}(E'(K(T))) = \{f \cdot (K(T)^\times)^2 : f \in \mathscr{F}'\}$.

Proof. Take any $\alpha \in \delta_E(E(K(T))$. We have $\alpha = f \cdot (K(T)^\times)^2$ for some squarefree polynomial $f \in K[T]$. Take any closed point P of $\mathbb{P}^1_K$ that is not in $\mathcal{A} \cup \mathcal{M}$. If $P \notin \mathcal{M}'$, then E and E' base extended to $K(T)_P$ both have good reduction. If $P \in \mathcal{M}'$, then condition (d) implies that E base extended to $K(T)_P$ has split multiplicative reduction or has Kodaira symbol I_n for some odd n. Lemma 3.3 thus implies that $v_P(f)$ is even for all closed points $P \notin \mathcal{A} \cup \mathcal{M}$. Since $K[T]$ is a PID and f is squarefree, we deduce that f divides b; recall the set of roots of b is $\mathcal{A} \cup \mathcal{M}$. Since $\infty \in \mathbb{P}^1(K)$ does not lie in $\mathcal{A} \cup \mathcal{M} \cup \mathcal{M}' = \mathcal{B}$, $v_\infty(f)$ being even implies that f has even degree. Therefore, $f = cf_1$ for a unique polynomial $f_1 \in \mathscr{F}$ and constant $c \in K^\times$. Lemma 3.3(i) implies that $f \cdot (K(T)_{e_0'}^\times)^2 = 1$ and hence $f(e_0') = c$ is a square in K. Therefore, $\alpha = f \cdot (K(T)^\times)^2 = f_1 \cdot (K(T)^\times)^2$ with $f_1 \in \mathscr{F}$. We have proved the inclusion

$$\delta_E(E(K(T))) \subseteq \{f \cdot (K(T)^\times)^2 : f \in \mathscr{F}\} =: G.$$

It is actually an equality since $|G| = 2^{|\mathcal{A}|+|\mathcal{M}|-1}$ and $|\delta_E(E(K(T)))| \geq 2^{|\mathcal{A}|+|\mathcal{M}|-1}$ by condition (f). This proves (i). Part (ii) is proved in the same way but making use of condition (g). ☐

We now consider specializations.

Lemma 5.2. *There is a finite set $D \subseteq K$ with $\mathcal{B} \subseteq D$ such that the inclusions*

$$\delta_{E_t}(E_t(K)) \supseteq \{f(t) \cdot (K^\times)^2 : f \in \mathscr{F}\} \quad \text{and} \quad \delta_{E_t'}(E_t'(K)) \supseteq \{f(t) \cdot (K^\times)^2 : f \in \mathscr{F}'\}$$

hold for all $t \in K - D$.

Proof. Let D be a finite subset of K containing $\mathcal{B}$ that we can extend a finitely number of times. Take any $t \in K - D$.

Take any $f \in \mathscr{F}$. We have $f(t) \neq 0$ since $t \notin \mathcal{B}$ and f divides Δ. By Lemma 5.1(i), there is a point $P \in E(K(T))$ such that $\delta_E(P) = f \cdot (K(T)^\times)^2$. If $P = 0$, then f is a square in $K(T)$ and hence $f(t) \cdot (K^\times)^2 = (K^\times)^2$ is an element of $\delta_{E_t}(E_t(K))$. Suppose that $P = (0,0)$ and hence $f \cdot (K(T)^\times)^2 = \delta_E(P) = b \cdot (K(T)^\times)^2$. Since the roots of f and b both lie in $\mathcal{B}$, we have $f(t) \cdot (K^\times)^2 = b(t) \cdot (K^\times)^2 = \delta_{E_t}((0,0))$ which proves that $f(t) \cdot (K^\times)^2 \in \delta_{E_t}(E_t(K))$. Now suppose that $P = (x, y)$ with $x, y \in K(T)$ and $x \neq 0$. We have $x = fz^2$ for some nonzero $z \in K(T)$. After increasing the finite set D, we may assume that z and y have no poles at t and that $z(t) \neq 0$. Therefore, $P_t := (x(t), y(t))$ is a point in $E_t(K)$ and $\delta_{E_t}(P_t) = x(t) \cdot (K^\times)^2 = f(t) \cdot (K^\times)^2$.

Since $\mathscr{F}$ is finite, after increasing the finite set D appropriately we will have $f(t) \cdot (K^\times)^2 \in \delta_{E_t}(E_t(K))$ for all $t \in K - D$ and all $f \in \mathscr{F}$. This proves the first inclusion of the lemma. The second inclusion is proved in the exact same way by making use of Lemma 5.1(ii). ☐

5.2. **Choice of primes.** In this section, we construct a set $S \cup \{\mathfrak{q}_1, \mathfrak{q}_2\}$ of nonzero prime ideals of $\mathcal{O}_K$ that satisfy various properties. These primes will be used to choose a specialization E_t for which we can compute the appropriate Selmer groups and prove that E_t has rank r.

Let S_0 be a finite set of nonzero prime ideals of $\mathcal{O}_K$ that contains all those that divide $6\prod_{\alpha,\beta\in\mathcal{B},\alpha\neq\beta}(\alpha-\beta)\in\mathcal{O}_K$ or divide the leading coefficient of Δ. By adding prime ideals to the finite set S_0, we may further assume that $\mathcal{O}_{K,S_0}$ is a PID.

Lemma 5.3. *For all $P \in \mathcal{B}$ and all but finitely many nonzero prime ideals $\mathfrak{p} \notin S_0$ of $\mathcal{O}_K$, if $t \in K$ satisfies $v_\mathfrak{p}(t-P) = 1$, then*

$$\tfrac{1}{2}|\mathrm{Im}(\delta_{E'_t,\mathfrak{p}})| = \begin{cases} 2 & \text{if } P \in \mathcal{M}, \\ \frac{1}{2} & \text{if } P \in \mathcal{M}', \\ 1 & \text{if } P \in \mathcal{A}. \end{cases}$$

Proof. Take any $P \in \mathcal{B}$. Take any nonzero prime ideal $\mathfrak{p} \notin S_0$ of $\mathcal{O}_K$ so that $v_\mathfrak{p}(t-P) = 1$. For each $e \in \mathcal{B}-\{P\}$, we have $v_\mathfrak{p}(t-e) = 0$ since otherwise $v_\mathfrak{p}(P-e) > 0$ which contradicts $\mathfrak{p} \notin S_0$. By enlarging S_0 appropriately, we will have $v_\mathfrak{p}(\Delta(t)) = v_P(\Delta)$ and $v_\mathfrak{p}(\Delta'(t)) = v_P(\Delta')$. Since $\mathfrak{p} \nmid 2$, we have

$$\tfrac{1}{2}|\,\mathrm{Im}(\delta_{E'_t,\mathfrak{p}})| = c_\mathfrak{p}(E')/c_\mathfrak{p}(E),$$

by Lemma 3.2(ii).

We can apply Tate's algorithm [Sil94, Algorithm 9.4] to E over $K(T)_P$; it produces a minimal Weierstrass model over $\mathcal{O}_P$, using the uniformizer $\pi := T-P$, that satisfies various properties before the algorithm completes. Substituting t for T, and by increasing the finite set S_0 appropriately in a way that does not depend on t, the assumption $v_\mathfrak{p}(t-P) = 1$ ensures that the model obtained is a minimal model for E_t at $\mathfrak{p}$ and that E and E_t have the same Kodaira symbol κ at P and $\mathfrak{p}$, respectively. Similarly by increasing S_0, we may also assume that E' and E'_t have the same Kodaira symbol κ' at P and $\mathfrak{p}$, respectively.

Consider the case where $\kappa \in \{\mathrm{II}, \mathrm{III}, \mathrm{IV}, \mathrm{II}^*, \mathrm{III}^*, \mathrm{IV}\}$ and hence E_t has potentially good reduction at $\mathfrak{p}$. By [DD15, Table 1], we have $c_\mathfrak{p}(E'_t)/c_\mathfrak{p}(E_t) = 1$.

Consider the case where $\kappa = \mathrm{I}_n^*$ for some $n \geq 0$. Since E and E' are 2-isogenous to each other, we find that $\kappa' = \mathrm{I}_m^*$ for some $m \geq 0$. By condition (e), we have $c_P(E) = c_P(E') = 4$. In Tate's algorithm, the conditions $c_P(E) = 4$ and $c_P(E') = 4$ are equivalent to certain polynomials with coefficients in $\mathcal{O}_P$ having distinct roots and splitting completely when reduced modulo the maximal ideal $\mathfrak{m}_P$ of $\mathcal{O}_P$. Substituting t for T we deduce that $c_\mathfrak{p}(E_t) = 4$ and $c_\mathfrak{p}(E'_t) = 4$ after possibly enlarging S_0. Therefore, $c_\mathfrak{p}(E'_t)/c_\mathfrak{p}(E_t) = 1$.

We have now verified that $\frac{1}{2}|\,\mathrm{Im}(\delta_{E'_t,\mathfrak{p}})| = 1$ when $P \in \mathcal{A}$. It remains to consider the cases where $P \in \mathcal{M} \cup \mathcal{M}'$.

Consider the case $P \in \mathcal{M}'$. We have $\kappa = \mathrm{I}_n$ and $\kappa' = \mathrm{I}_{2n}$ for some $n \geq 1$; the integer n is the $\mathfrak{p}$-adic valuation of the discriminant of a Weierstrass model of E_t that is minimal at $\mathfrak{p}$. By condition (d), E has split reduction at P or n is odd. After possibly increasing the set S_0, this implies that E_t has split reduction at $\mathfrak{p}$ or n is odd. By [DD15, Table 1], we have $c_\mathfrak{p}(E'_t)/c_\mathfrak{p}(E_t) = 1/2$.

Finally consider the case $P \in \mathcal{M}$. We have $\kappa = \mathrm{I}_{2n}$ and $\kappa' = \mathrm{I}_n$ for some $n \geq 1$; the integer n is the $\mathfrak{p}$-adic valuation of the discriminant of a Weierstrass model of E'_t that is minimal at $\mathfrak{p}$. By condition (c), E' has split reduction at P or n is odd. After possibly increasing the set S_0, this implies that E_t' has split reduction at $\mathfrak{p}$ or n is odd. By [DD15, Table 1], we have $c_{\mathfrak{p}}(E_t')/c_{\mathfrak{p}}(E_t) = 2$. $\square$

Lemma 5.4. *For all but finitely many nonzero prime ideals $\mathfrak{p} \notin S_0$ of $\mathcal{O}_K$, if $t \in K - \mathcal{B}$ satisfies $v_{\mathfrak{p}}(t) < 0$, then E_t and E_t' both have good reduction at $\mathfrak{p}$.*

Proof. Set $U := T^{-1}$. We can choose a Weierstrass model $y^2 = x^3 + cx + d$ for E, with $c, d \in \mathcal{O}_K[U]$, that is minimal over the PID $K[U]$. Let $\tilde{\Delta} \in \mathcal{O}_K[U]$ be the discriminant of this model. Since E has good reduction at $\infty \in \mathbb{P}^1(K)$, we find that $U \nmid \tilde{\Delta}$. Take any $\mathfrak{p} \notin S_0$ that does not divide $\tilde{\Delta}(0) \in \mathcal{O}_K$. Take any $t \in K - \mathcal{B}$ with $v_{\mathfrak{p}}(t) < 0$. Substituting U by $t^{-1} \in \mathfrak{p}\mathcal{O}_p$, we obtain a Weierstrass model for E_t with coefficients in $\mathcal{O}_{\mathfrak{p}}$ whose discriminant $\tilde{\Delta}(t^{-1})$ lies in $\mathcal{O}_{\mathfrak{p}}^\times$. Therefore, E_t has good reduction at $\mathfrak{p}$. The curve E_t' also has good reduction at $\mathfrak{p}$ since it is isogenous to E_t. $\square$

By increasing the finite set S_0 we shall now assume that the conclusions of Lemmas 5.3 and 5.4 hold for all nonzero prime ideals $\mathfrak{p} \notin S_0$ of $\mathcal{O}_K$.

Lemma 5.5. *There is a finite set $S \supseteq S_0$ of nonzero prime ideals of $\mathcal{O}_K$ such that for each $v \in S$ we have a nonempty open subset U_v of K_v and a subgroup $\Phi_v \subseteq K_v^\times/(K_v^\times)^2$ for which the following hold:*

(a) *For each $v \in S \cup S_\infty$ and $t \in K \cap U_v$, we have $t \notin D$ and $\operatorname{Im}(\delta_{E_t',v}) = \Phi_v$.*
(b) *The natural map*
$$\mathcal{O}_{K,S}^\times/(\mathcal{O}_{K,S}^\times)^2 \to \prod_{v \in S \cup S_\infty} (K_v^\times/(K_v^\times)^2)/\Phi_v$$
is a group isomorphism.
(c) *For each $v \in S$ dividing 2, $U_v \cap \mathcal{O}_v = \emptyset$.*

Proof. Take any place $v \in S_0 \cup S_\infty$ and choose an element $u_v \in K_v^\times$ with $u_v \notin D$. When $v|2$, we assume u_v has been chosen so that $u_v \notin \mathcal{O}_v$. With a fixed real number $\epsilon_v > 0$, define the open subset
$$U_v := \{u \in K_v : |u - u_v|_v < \epsilon_v\}$$
of K_v, where $|\cdot|_v$ is an absolute value on K_v corresponding to v. By taking $\epsilon_v > 0$ sufficiently small, we may assume that $u \notin D$ for all $u \in U_v$. We can also assume that (c) holds when $v|2$. For each $u \in U_v$, we have $\Delta(u) \neq 0$ since $u \notin D$ and hence specialization of E' at u gives an elliptic curve E_u' over K_v. For $u \in U_v$, we have a homomorphism
$$\delta_{E_u'} \colon E_u'(K_v) \to K_v^\times/(K_v^\times)^2 \tag{5.2}$$
as in §3.1; we have $\delta_{E_u'}((x,y)) = x \cdot (K_v^\times)^2$ for $(x,y) \in E_u'(K_v) - \{0, (0,0)\}$ and $\delta_{E_u'}((0,0)) = (a^2 - 4b) \cdot (K_v^\times)^2$. The key topological observation is the image of (5.2) does not depend on the choice $u \in U_v$ if we take $\epsilon_v > 0$ sufficiently small. Thus by taking $\epsilon_v > 0$ sufficiently small, we may assume that (5.2) has a common image Φ_v for all $u \in U_v$. In particular, for all $t \in K \cap U_v$ we have $\operatorname{Im}(\delta_{E_t',v}) = \Phi_v$.

By weak approximation for K, there is a finite set S_1 of nonzero prime ideals of $\mathcal{O}_K$ that is disjoint from S_0 such that the natural homomorphism
$$\psi \colon \mathcal{O}_{K,S_0 \cup S_1}^\times/(\mathcal{O}_{K,S_0 \cup S_1}^\times)^2 \to \prod_{v \in S_0 \cup S_\infty} (K_v^\times/(K_v^\times)^2)/\Phi_v$$

is surjective. Choose units $u_1, \ldots, u_m \in \mathcal{O}_{K,S_0\cup S_1}^\times$ whose image in $\mathcal{O}_{K,S_0\cup S_1}^\times/(\mathcal{O}_{K,S_0\cup S_1}^\times)^2$ gives a basis of the $\mathbb{F}_2$-vector space $\ker\psi$. The field $L := K(\sqrt{u_1}, \ldots, \sqrt{u_m})$ is an abelian extension of K with $\operatorname{Gal}(L/K) \cong (\mathbb{Z}/2\mathbb{Z})^m$. By the Chebotarev density theorem, there are nonzero prime ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_m \notin S_0 \cup S_1$ of $\mathcal{O}_K$ such that u_i is a square in $\mathcal{O}_{\mathfrak{p}_j}^\times$ if and only if $i \neq j$. Define $S_2 := \{\mathfrak{p}_1, \ldots, \mathfrak{p}_m\}$. Observe that if $u \cdot (\mathcal{O}_{K,S_0\cup S_1}^\times)^2$ is in the kernel of ψ and u is a square in $\mathcal{O}_v^\times$ for all $v \in S_2$, then $u \cdot (\mathcal{O}_{K,S_0\cup S_1}^\times)^2 = 1$.

With $S := S_0 \cup S_1 \cup S_2$, we define the natural group homomorphism

$$\varphi\colon \mathcal{O}_{K,S}^\times/(\mathcal{O}_{K,S}^\times)^2 \to \prod_{v\in S\cup S_\infty} (K_v^\times/(K_v^\times)^2)/\Phi_v,$$

where $\Phi_v := K_v^\times/(K_v^\times)^2$ if $v \in S_1$ and $\Phi_v := 1$ if $v \in S_2$.

We claim that φ is injective. Take any $\alpha \in \ker\varphi$ and choose a unit $u \in \mathcal{O}_{K,S}^\times$ that represents α. Since $\varphi(\alpha) = 1$, we find that u is a square in $K_v^\times$ for all $v \in S_2$. The ring $\mathcal{O}_{K,S_0}$, and hence also $\mathcal{O}_{K,S_0\cup S_1}$, is a PID by our choice of S_0. Thus after multiplying u by a suitable square in K, we may assume that our chosen u is an element of $\mathcal{O}_{K,S_0\cup S_1}^\times$. Since $\varphi(\alpha) = 1$, we have $u \cdot (K_v^\times)^2 \in \Phi_v$ for all $v \in S_0 \cup S_\infty$. Therefore, $u \cdot (\mathcal{O}_{K,S_0\cup S_1}^\times)^2$ is in the kernel of ψ. Since $\varphi(\alpha) = 1$, we have $u \cdot (K_v^\times)^2 \in \Phi_v = 1$ for all $v \in S_2$. Since $u \cdot (\mathcal{O}_{K,S_0\cup S_1}^\times)^2$ is in the kernel of ψ and u is a square in $\mathcal{O}_v^\times$ for all $v \in S_2$, we deduce that u is a square in $\mathcal{O}_{K,S_0\cup S_1}^\times$ and hence $\alpha = 1$. This completes the proof of the claim.

We claim that φ is an isomorphism. We have

$$\prod_{v\in S\cup S_\infty} |(K_v^\times/(K_v^\times)^2)/\Phi_v| = 4^m \prod_{v\in S_0\cup S_\infty} |(K_v^\times/(K_v^\times)^2)/\Phi_v| = 2^m \cdot |\mathcal{O}_{K,S_0\cup S_1}^\times/(\mathcal{O}_{K,S_0\cup S_1}^\times)^2|,$$

where the first equality uses that $|K_v^\times/(K_v^\times)^2/\Phi_v|$ is 1 for $v \in S_1$ and 4 for $v \in S_2$, and the last equality uses that ψ is surjective with kernel of cardinality 2^m. By Dirichlet's unit theorem, the groups $\mathcal{O}_{K,S_0\cup S_1}^\times$ and $\mathcal{O}_{K,S}^\times$ are finitely generated abelian groups of rank $|S_\infty| + |S_0| + |S_1| - 1$ and $|S_\infty| + |S| - 1$, respectively. Since the torsion subgroups of these unit groups are cyclic of even order, we have

$$|\mathcal{O}_{K,S}^\times/(\mathcal{O}_{K,S}^\times)^2| = 2^{|S_\infty|+|S|} = 2^{|S_2|} \cdot 2^{|S_\infty|+|S_0|+|S_1|} = 2^m \cdot |\mathcal{O}_{K,S_0\cup S_1}^\times/(\mathcal{O}_{K,S_0\cup S_1}^\times)^2|.$$

We have now shown that the domain and codomain of φ have the same finite cardinality. The claim follows since we have already proved that φ is injective.

This proves (b) and we have also verified (a) for $v \in S_0 \cup S_\infty$.

Take any $v \in S_1$ and set $\mathfrak{p} := v$. There is an element $e \in \mathcal{M}$ by (b). Since $v \notin S_0$, there is a $t_v \in K$ with $v_\mathfrak{p}(t_v - e) = 1$ and $v_\mathfrak{p}(t_v - c) = 0$ for $c \in \mathcal{B} - \{e\}$. By Lemma 5.3, we have $|\operatorname{Im}(\delta_{E'_{t_v,v}})| = 4$ and hence $\operatorname{Im}(\delta_{E'_{t_v,v}}) = K_v^\times/(K_v^\times)^2 = \Phi_v$. Arguing as above, there is an open neighborhood U_v of t_v in K_v such that $\delta_{E'_u}\colon E'_u(K_v) \to K_v^\times/(K_v^\times)^2$ has image Φ_v for all $u \in U_v$. This gives (a) for $v \in S_1$.

Take any $v \in S_1$ and set $\mathfrak{p} := v$. There is an element $e \in \mathcal{M}'$ by (b). Since $v \notin S_0$, there is a $t_v \in K$ with $v_\mathfrak{p}(t_v - e) = 1$ and $v_\mathfrak{p}(t_v - c) = 0$ for $c \in \mathcal{B} - \{e\}$. By Lemma 5.3, we have $|\operatorname{Im}(\delta_{E'_{t_v,v}})| = 1$ and hence $\operatorname{Im}(\delta_{E'_{t_v,v}}) = 1 = \Phi_v$. Arguing as above, there is an open neighborhood U_v of t_v in K_v such that $\delta_{E'_u}\colon E'_u(K_v) \to K_v^\times/(K_v^\times)^2$ has image Φ_v for all $u \in U_v$. This gives (a) for $v \in S_2$. ☐

For the rest of the proof, we fix S, $\{U_v\}_{v\in S\cup S_\infty}$ and $\{\Phi_v\}_{v\in S\cup S_\infty}$ as in Lemma 5.5. The following lemma will be key when we later compute the ratio of cardinalities of Selmer groups.

Lemma 5.6. *We have* $\prod_{v\in S\cup S_\infty}\frac{1}{2}|\Phi_v|=1$.

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. By Dirichlet's unit theorem, the abelian group $\mathcal{O}_{K,S}^\times$ is finitely generated and has rank $r+s+|S|-1$. Since the torsion subgroup of $\mathcal{O}_{K,S}^\times$ is cyclic of even order, we deduce that

$$|\mathcal{O}_{K,S}^\times/(\mathcal{O}_{K,S}^\times)^2|=2^{(r+s+|S|-1)+1}=2^{r+s+|S|}. \tag{5.3}$$

Take any place $v|2$ of K. We have $[K_v:\mathbb{Q}_2]=e_vf_v$, where e_v and f_v are the ramification index and inertia degree, respectively, of the extension $K_v/\mathbb{Q}_2$. We have $\mathcal{O}_v^\times\cong C_v\times\mathbb{Z}_2^{e_vf_v}$, 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 $\mathcal{O}_v^\times/(\mathcal{O}_v^\times)^2\cong(\mathbb{Z}/2\mathbb{Z})^{1+e_vf_v}$. Therefore, $\frac{1}{2}|K_v^\times/(K_v^\times)^2|=2^{1+e_vf_v}$. Since $\sum_{v|2}e_vf_v=[K:\mathbb{Q}]=r+2s$, we deduce that $\prod_{v|2}\frac{1}{2}|K_v^\times/(K_v^\times)^2|=2^{r+2s}\prod_{v|2}2$. For any place $v\in S$ with $v\nmid 2$, we have $\frac{1}{2}|K_v^\times/(K_v^\times)^2|=2$. We have $\prod_{v\in S_\infty}\frac{1}{2}|K_v^\times/(K_v^\times)^2|=1/2^s$. Using these computations and that S contains all the places of K dividing 2, we find that

$$\prod_{v\in S\cup S_\infty}\tfrac{1}{2}|K_v^\times/(K_v^\times)^2|=2^{-s}\cdot 2^{r+2s}\prod_{v|2}2\cdot\prod_{v\in S,\,v\nmid 2}2=2^{r+s+|S|}. \tag{5.4}$$

Using the isomorphism from Lemma 5.5(b), we have

$$\prod_{v\in S\cup S_\infty}\tfrac{1}{2}|\Phi_v|=\prod_{v\in S\cup S_\infty}\tfrac{1}{2}|K_v^\times/(K_v^\times)^2|\cdot|\mathcal{O}_{K,S}^\times/(\mathcal{O}_{K,S}^\times)^2|^{-1}=1,$$

where the last equality uses (5.3) and (5.4). $\square$

Lemma 5.7. *There is a nonzero $\pi\in\mathcal{O}_K$ such that π is a square in $K_v^\times$ for all $v\in S\cup S_\infty$ and $\pi\mathcal{O}_K$ is a prime ideal of $\mathcal{O}_K$ that does not lie in S.*

Proof. Fix an integer $n_\mathfrak{p}\geq 1$ for each $\mathfrak{p}\in S$. Let I^S be the group of fractional ideals of K generated by nonzero prime ideals $\mathfrak{p}\notin S$ of $\mathcal{O}_K$. Let H be the subgroup of I^S consisting of $\alpha\mathcal{O}_K$ where $\alpha\in K^\times$ is positive in K_v for all real place v in S_∞ and $v_\mathfrak{p}(\alpha-1)\geq n_\mathfrak{p}$ for all $\mathfrak{p}\in S$. Define $C:=I^S/H$; it is the *ray class group* of K with modulus $\mathfrak{m}:=\prod_{\mathfrak{p}\in S}\mathfrak{p}^{n_\mathfrak{p}}\cdot\prod_{v\in S_\infty \text{ real}}v$. Let $K_\mathfrak{m}$ be the corresponding *ray class field*; it is a finite abelian extension of K and a prime ideal $\mathfrak{p}\notin S$ splits completely in $K_\mathfrak{m}$ if and only if $\mathfrak{p}\in H$. By the Chebotarev density theorem, there is a nonzero prime ideal $\mathfrak{q}\notin S$ of $\mathcal{O}_K$ that splits completely in $K_\mathfrak{m}$. We have $\mathfrak{q}\in H$ and hence $\mathfrak{q}=\pi\mathcal{O}_K$ for some $\pi\in\mathcal{O}_K$ that is positive in K_v for all real place v in S_∞ and $v_\mathfrak{p}(\pi-1)\geq n_\mathfrak{p}$ for all $\mathfrak{p}\in S$. For each $v\in S_\infty$, π is a square in K_v. For each $\mathfrak{p}\in S$, we have $\pi\in 1+\mathfrak{p}^{n_\mathfrak{p}}\mathcal{O}_\mathfrak{p}$ and hence π is a square in $K_\mathfrak{p}$ assuming that $n_\mathfrak{p}$ is large enough. So by choosing the $n_\mathfrak{p}\geq 1$ large enough, we find that π is a square in $K_v^\times$ for all $v\in S\cup S_\infty$. $\square$

For the rest of the proof, we fix $\pi\in\mathcal{O}_K$ as in Lemma 5.7 and define $\mathfrak{q}_1:=\pi\mathcal{O}_K$.

Lemma 5.8. *There is a nonzero prime ideal $\mathfrak{q}_2\notin S\cup\{\mathfrak{q}_1\}$ of $\mathcal{O}_K$ such that every element in $\mathcal{O}_{K,S\cup\{\mathfrak{q}_1\}}^\times$ is a square in $K_{\mathfrak{q}_2}$.*

Proof. The group $\mathcal{O}_{K,S\cup\{\mathfrak{q}_1\}}^\times$ is finitely generated by Dirichlet's unit theorem; fix a finite set of generators B. Define $L:=K(\{\sqrt{\alpha}:\alpha\in B\})$; it is a finite Galois extension of K. By the Chebotarev density theorem, there is a nonzero prime ideal $\mathfrak{q}_2\notin S\cup\{\mathfrak{q}_1\}$ of $\mathcal{O}_K$ that splits completely in L. The lemma follows since every element of B is a square in $K_{\mathfrak{q}_2}$. $\square$

For the rest of the proof, we fix a prime ideal $\mathfrak{q}_2$ as in Lemma 5.8.

5.3. **A choice of elliptic curve.** In this section we will consider the elliptic curve E_t over K with $t := m/n$, where m and n are chosen as in the following proposition. It is here that we make use of a result of Kai that is a number field analogue of the Green–Tao–Ziegler theorem on simultaneous prime values of degree 1 polynomials.

Proposition 5.9. *There are nonzero $m, n \in \mathcal{O}_{K,S}$ such that the following hold:*

(a) *the elements $m - en$ with $e \in \mathcal{B}$ generate distinct nonzero prime ideals of $\mathcal{O}_{K,S\cup\{\mathfrak{q}_1,\mathfrak{q}_2\}}$,*
(b) *m/n lies in U_v for all $v \in S \cup S_\infty$,*
(c) *$v_{\mathfrak{q}_1}(m - en) = 1$ for some $e \in \mathcal{M}$, $v_{\mathfrak{q}_1}(n) = 0$, and n is not a square modulo $\mathfrak{q}_1$,*
(d) *$v_{\mathfrak{q}_2}(m - en) = 1$ for some $e \in \mathcal{M}'$, $v_{\mathfrak{q}_2}(n) = 0$, and n is not a square modulo $\mathfrak{q}_2$,*
(e) *$v_{\mathfrak{p}}(m - en) = 0$ for all prime ideals $\mathfrak{p}$ of $\mathcal{O}_K$ dividing 2.*

Proof. For each $\mathfrak{p} \in S$ with $\mathfrak{p} \nmid 2$, let $\mathscr{U}_{\mathfrak{p}}$ be the set of pairs $(\alpha, \beta) \in K_{\mathfrak{p}}^2$ with $\beta \neq 0$ and $\alpha/\beta \in U_{\mathfrak{p}}$. For each $\mathfrak{p} \in S$ with $\mathfrak{p}|2$, let $\mathscr{U}_{\mathfrak{p}}$ be the set of pairs $(\alpha, \beta) \in K_{\mathfrak{p}}$ with $\beta \neq 0$, $\alpha/\beta \in U_{\mathfrak{p}}$, $v_{\mathfrak{p}}(\alpha) = 0$ and $v_{\mathfrak{p}}(\beta) > 0$. For each $\mathfrak{p} \in S$, $\mathscr{U}_{\mathfrak{p}}$ is a nonempty open subset of $K_{\mathfrak{p}}^2$ since $U_{\mathfrak{p}}$ is a nonempty open subset of $K_{\mathfrak{p}}$ (when $\mathfrak{p}|2$ we also use that $U_{\mathfrak{p}} \cap \mathcal{O}_{\mathfrak{p}} = \emptyset$ to ensure the set is nonempty).

Let $\mathscr{U}_{q_1}$ be the set of $(\alpha, \beta) \in \mathcal{O}_{\mathfrak{q}_1}^2$ for which $v_{\mathfrak{q}_1}(\beta) = 0$, β is not a square modulo $\mathfrak{q}_1$, and $v_{\mathfrak{q}_1}(\alpha - e\beta) = 1$ for some $e \in \mathcal{M}$. Let $\mathscr{U}_{q_2}$ be the set of $(\alpha, \beta) \in K_{\mathfrak{q}_2}^2$ for which $v_{\mathfrak{q}_2}(\beta) = 0$, β is not a square modulo $\mathfrak{q}_2$, and $v_{\mathfrak{q}_2}(\alpha - e\beta) = 1$ for some $e \in \mathcal{M}'$. Since $\mathcal{M} \cup \mathcal{M}' \subseteq \mathcal{O}_K$, we find that $\mathscr{U}_{\mathfrak{q}_i}$ is a nonempty open subset of $\mathcal{O}_{\mathfrak{q}_i}^2 \subseteq K_{\mathfrak{q}_i}^2$ for each $i \in \{1, 2\}$.

Define $S' := S \cup \{\mathfrak{q}_1, \mathfrak{q}_2\}$. By [Kai25, Proposition 13.2] and the openness of our sets, there are nonzero $m, n \in \mathcal{O}_{K,S'}$ such that the elements $m - en$ with $e \in \mathcal{B}$ generate distinct prime ideals of $\mathcal{O}_{K,S'}$, the pair (m, n) lies in $\mathscr{U}_{\mathfrak{p}}$ for all $\mathfrak{p} \in S'$, and m/n lies in U_v for all $v \in S_\infty$. Properties (a)–(d) all hold by our definitions. For (e) note that $v_{\mathfrak{p}}(m) = 0$ and $v_{\mathfrak{p}}(n) > 0$ for all $\mathfrak{p}$ dividing 2 (this uses that S contains all the prime ideals dividing 2).

We have $m, n \in \mathcal{O}_{\mathfrak{q}_i}$ for $i \in \{1, 2\}$ since $\mathscr{U}_{\mathfrak{q}_i} \subseteq \mathcal{O}_{q_i}^2$. Since m and n are in $\mathcal{O}_{K,S'}$ we deduce that m and n lie in $\mathcal{O}_{K,S}$. □

For the rest of the section, we fix $m, n \in \mathcal{O}_{K,S}$ as in Proposition 5.9 and define

$$t := m/n \in K.$$

We have $t \notin D$ since $t \in U_v$ for any $v \in S \cup S_\infty$. Set $S' := S \cup \{\mathfrak{q}_1, \mathfrak{q}_2\}$. For each $e \in \mathcal{B}$, there is a unique nonzero prime ideal $\mathfrak{p}_e \notin S'$ of $\mathcal{O}_K$ such that

$$(m - en)\mathcal{O}_{K,S'} = \mathfrak{p}_e \mathcal{O}_{K,S'}. \tag{5.5}$$

The prime ideals $\{\mathfrak{p}_e\}_{e \in \mathcal{B}}$ are distinct and do not lie in S' by our choice of m and n.

Lemma 5.10. *For any $e, e' \in \mathcal{B}$, we have $v_{\mathfrak{p}_e}(n) = 0$ and*

$$v_{\mathfrak{p}_e}(m - e'n) = \begin{cases} 1 & \text{if } e = e', \\ 0 & \text{if } e \neq e'. \end{cases}$$

Proof. Since the prime ideals $\{\mathfrak{p}_e\}_{e \in \mathcal{B}}$ are distinct and do not lie in S', the desired expression for $v_{\mathfrak{p}_e}(m - e'n)$ follows directly from the factorizations (5.5).

With $\mathfrak{p} := \mathfrak{p}_e$, it remains to show that $v_{\mathfrak{p}}(n) = 0$. Assume to the contrary that $v_{\mathfrak{p}}(n) \neq 0$ and hence $n \in \mathfrak{p}\mathcal{O}_p$. We also have $m \in \mathfrak{p}\mathcal{O}_{\mathfrak{p}}$ since $m - en \in \mathfrak{p}\mathcal{O}_{\mathfrak{p}}$ and $e \in \mathcal{O}_K$. Therefore, $m - e'n \in \mathfrak{p}\mathcal{O}_{\mathfrak{p}}$ for all $e' \in \mathcal{B}$. This contradicts that the ideals $(m - e'n)\mathcal{O}_{K,S'}$ with $e' \in \mathcal{B}$ are distinct prime ideals. Therefore, we have $v_{\mathfrak{p}}(n) = 0$. □

We will now study the elliptic curves E_t and E'_t with our specific choice of t.

Lemma 5.11. *The curves E_t and E'_t over K have good reduction at all nonzero prime ideals $\mathfrak{p} \notin S \cup \{\mathfrak{q}_1, \mathfrak{q}_2\} \cup \{\mathfrak{p}_e : e \in \mathcal{B}\}$ of $\mathcal{O}_K$.*

Proof. Take any nonzero prime ideal $\mathfrak{p} \notin S \cup \{\mathfrak{q}_1, \mathfrak{q}_2\} \cup \{\mathfrak{p}_e : e \in \mathcal{B}\}$ of $\mathcal{O}_K$. If $v_\mathfrak{p}(t) < 0$, then E_t has good reduction at $\mathfrak{p}$ by Lemma 5.4. So we may assume that $v_\mathfrak{p}(t) \geq 0$. We have $a, b, \Delta \in \mathcal{O}_K[T]$ so setting $T = t$ in the model (5.1) gives a Weierstrass model for E_t with coefficients in $\mathcal{O}_\mathfrak{p}$ that has discriminant $\Delta(t) \in \mathcal{O}_\mathfrak{p}$.

It suffices to prove that $\Delta(t)$ lies in $\mathcal{O}_\mathfrak{p}^\times$, so assume to the contrary that $\Delta(t)$ is an element of $\mathfrak{p}\mathcal{O}_\mathfrak{p}$. Since the leading coefficient of Δ lies in $\mathcal{O}_{K,S_0}^\times$ and $\mathcal{B} \subseteq \mathcal{O}_K$ is the set of roots of Δ in $\overline{K}$, we have $t - e \in \mathfrak{p}\mathcal{O}_\mathfrak{p}$ for some $e \in \mathcal{B}$. Multiplying by $n \in \mathcal{O}_{K,S}$ this implies that $m - en \in \mathfrak{p}\mathcal{O}_\mathfrak{p}$. The factorization (5.5) implies that $\mathfrak{p} \in S \cup \{\mathfrak{q}_1, \mathfrak{q}_2\} \cup \{\mathfrak{p}_e\}$ which contradicts our choice of $\mathfrak{p}$. Therefore, $\Delta(t) \in \mathcal{O}_\mathfrak{p}^\times$ and hence E_t has good reduction at $\mathfrak{p}$. The elliptic curve E'_t also has good reduction at $\mathfrak{p}$ since it is isogenous to E_t $\square$

We have a degree 2 isogeny $\phi_t \colon E_t \to E'_t$ whose kernel is generated by $(0, 0)$. Let $\hat{\phi}_t \colon E'_t \to E_t$ be the dual isogeny of ϕ_t.

Lemma 5.12.

(i) *If $v \in S \cup S_\infty$, then $\operatorname{Im}(\delta_{E'_t,v}) = \Phi_v$.*

(ii) *If $\mathfrak{p} \notin S$ is a nonzero prime ideal of $\mathcal{O}_K$, then*

$$\tfrac{1}{2}|\operatorname{Im}(\delta_{E'_t,\mathfrak{p}})| = \begin{cases} 2 & \textit{if } \mathfrak{p} \in \{\mathfrak{q}_1\} \cup \{\mathfrak{p}_e : e \in \mathcal{M}\}, \\ \frac{1}{2} & \textit{if } \mathfrak{p} \in \{\mathfrak{q}_2\} \cup \{\mathfrak{p}_e : e \in \mathcal{M}'\}, \\ 1 & \textit{otherwise.} \end{cases}$$

(iii) *We have $|\operatorname{Sel}_{\phi_t}(E_t/K)|/|\operatorname{Sel}_{\hat{\phi}_t}(E'_t/K)| = 2^{|\mathcal{M}|-|\mathcal{M}'|}$.*

Proof. Part (i) follows from Lemma 5.5(a) and that $t = m/n$ is an element of $K \cap U_v$ for all $v \in S \cup S_\infty$. Take any nonzero prime ideal $\mathfrak{p} \notin S$ of $\mathcal{O}_K$.

Consider the case where $\mathfrak{p} = \mathfrak{p}_e$ for some $e \in \mathcal{B}$. We have $v_\mathfrak{p}(t-e) = v_\mathfrak{p}(m-en) - v_\mathfrak{p}(n) = 1$, where the last equality uses Lemma 5.10. Part (ii) for $\mathfrak{p} = \mathfrak{p}_e$ follows from Lemma 5.3.

By Propostion 5.9 and our choice of t, we have $v_{\mathfrak{q}_i}(t - e) = 1$ for some $e \in \mathcal{M}$ when $i = 1$ and some $e \in \mathcal{M}'$ when $i = 2$. Part (ii) for $\mathfrak{p} \in \{\mathfrak{q}_1, \mathfrak{q}_2\}$ follows from Lemma 5.3.

For part (ii), it remains to consider the case where $\mathfrak{p} \notin S \cup \{\mathfrak{q}_1, \mathfrak{q}_2\} \cup \{\mathfrak{p}_e : e \in \mathcal{B}\}$. The elliptic curve E'_t has good reduction at $\mathfrak{p}$ by Lemma 5.11. Therefore, $\operatorname{Im}(\delta_{E'_t,\mathfrak{p}}) = \mathcal{O}_\mathfrak{p}^\times/(\mathcal{O}_\mathfrak{p}^\times)^2$ and hence $\frac{1}{2}|\operatorname{Im}(\delta_{E'_t,\mathfrak{p}})| = 1$.

We now prove (iii). Set $\tau := |\operatorname{Sel}_{\phi_t}(E_t/K)|/|\operatorname{Sel}_{\hat{\phi}_t}(E'_t/K)|$. By Lemma 3.2(i), we have $\tau = \prod_v \frac{1}{2}|\operatorname{Im}(\delta_{E'_t,v})|$, where the product is over the places v of K. By part (i) and Lemma 5.6, we have $\tau = \prod_{\mathfrak{p} \notin S} \frac{1}{2}|\operatorname{Im}(\delta_{E'_t,\mathfrak{p}})|$, where $\mathfrak{p}$ varies over the nonzero prime ideals of $\mathcal{O}_K$ not in S. From part (ii), we find that $\tau = 2^{1+|\mathcal{M}|} \cdot (\frac{1}{2})^{1+|\mathcal{M}'|} = 2^{|\mathcal{M}|-|\mathcal{M}'|}$. $\square$

We can now compute $\operatorname{Sel}_{\phi_t}(E_t/K)$ and show that it is as small as possible given what we know about the image of $\delta_{E'_t}$.

Lemma 5.13. *We have $\operatorname{Sel}_{\phi_t}(E_t/K) = \delta_{E'_t}(E'_t(K)) = \{f(t) \cdot (K^\times)^2 : f \in \mathscr{F}'\}$.*

Proof. We have inclusions

$$\mathrm{Sel}_{\phi_t}(E_t/K) \supseteq \delta_{E'_t}(E'_t(K)) \supseteq \{f(t)\cdot (K^\times)^2 : f \in \mathscr{F}'\} \tag{5.6}$$

from the definition of the Selmer group and Lemma 5.2. Take any $\alpha \in \mathrm{Sel}_{\phi_t}(E_t/K) \subseteq K^\times/(K^\times)^2$. To prove the lemma, it suffices to show that $\alpha = f(t)\cdot (K^\times)^2$ for some $f \in \mathscr{F}'$. We have $\alpha = c\cdot (K^\times)^2$ for some $c \in K^\times$.

Take any nonzero prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$ that is not in the set

$$S'' := S \cup \{\mathfrak{q}_1\} \cup \{\mathfrak{p}_e : e \in \mathcal{A} \cup \mathcal{M}\}.$$

If $\mathfrak{p} \in \{\mathfrak{q}_2\} \cup \{\mathfrak{p}_e : e \in \mathcal{M}'\}$, then $\mathrm{Im}(\delta_{E'_t,\mathfrak{p}}) = 1$ by Lemma 5.12(ii). If $\mathfrak{p} \notin \{\mathfrak{q}_1, \mathfrak{q}_2\} \cup \{\mathfrak{p}_e : e \in \mathcal{B}\}$, then E'_t has good reduction at $\mathfrak{p}$ by Lemma 5.11 and hence $\mathrm{Im}(\delta_{E'_t,\mathfrak{p}}) = \mathcal{O}_\mathfrak{p}^\times/(\mathcal{O}_\mathfrak{p}^\times)^2$. We have $c\cdot (K_\mathfrak{p}^\times)^2 \in \mathrm{Im}(\delta_{E'_t,\mathfrak{p}})$ since $\alpha \in \mathrm{Sel}_{\phi_t}(E_t/K)$ and hence $v_\mathfrak{p}(c) \equiv 0 \pmod 2$ for all $\mathfrak{p} \notin S''$. We chose S_0 so that $\mathcal{O}_{K,S_0}$ was a PID and hence $\mathcal{O}_{K,S''}$ is also a PID. So after multiplying c by an appropriate square in $K^\times$, we may assume that $c \in \mathcal{O}_{K,S''}^\times$. By Lemma 5.10 and (5.5), we have $c = c_1 \prod_{e\in\mathcal{A}\cup\mathcal{M}} (m-en)^{g_e}$ for unique $g_e \in \mathbb{Z}$ and a unique $c_1 \in \mathcal{O}_{K,S\cup\{\mathfrak{q}_1\}}$. After multiplying c by a square in $K^\times$, we may assume that

$$c = c_1 \prod_{e\in B} (m-en) \tag{5.7}$$

for some subset $B \subseteq \mathcal{A}\cup\mathcal{M}$ and unit $c_1 \in \mathcal{O}_{K,S\cup\{\mathfrak{q}_1\}}^\times$.

We claim that $m - en \in \mathcal{O}_{K,S}$ is not a square modulo $\mathfrak{q}_2$ for all $e \in \mathcal{A}\cup\mathcal{M}$. Take any $e \in \mathcal{A}\cup\mathcal{M}$. By our choice of m and n, there is an $e' \in \mathcal{M}'$ for which $m - e'n \equiv 0 \pmod{\mathfrak{q}_2}$. We have

$$m - en = (m-e'n) + (e'-e)n \equiv (e'-e)n \pmod{\mathfrak{q}_2}.$$

By our choice of S_0 and $\mathfrak{q}_2$, $e'-e$ is a nonzero square modulo $\mathfrak{q}_2$. By our choice of n, n is not a square modulo $\mathfrak{q}_2$. Therefore, $m-en$ is not a square modulo $\mathfrak{q}_2$ as claimed.

We have $c\cdot (K_{\mathfrak{q}_2}^\times)^2 \in \mathrm{Im}(\delta_{E'_t,\mathfrak{q}_2})$ since $\alpha \in \mathrm{Sel}_{\phi_t}(E_t/K)$. Therefore, c is a square in $K_{\mathfrak{q}_2}$ by Lemma 5.12(ii). We have $c_1 \in \mathcal{O}_{K,S\cup\{\mathfrak{q}_1\}}^\times$ and hence c_1 is a nonzero square modulo $\mathfrak{q}_2$ by our choice of $\mathfrak{q}_2$. By the above claim and (5.7), we find that $c \in \mathcal{O}_{\mathfrak{q}_2}^\times$ is a square modulo $\mathfrak{q}_2$ if and only if $|B|$ is even. Since c is a square in $K_{\mathfrak{q}_2}$ we deduce that $|B|$ is even. We have $n^{|B|} \in (K^\times)^2$ since $|B|$ is even and hence we may assume that c was chosen such that

$$c = c_1 \prod_{e\in B} (t-e)$$

with a subset $B \subseteq \mathcal{A}\cup\mathcal{M}$ of even cardinality and a unit $c_1 \in \mathcal{O}_{K,S\cup\{\mathfrak{q}_1\}}^\times$. Since $|B|$ is even, there is a unique $f \in \mathscr{F}'$ such that $f = c_2\prod_{e\in B}(T-e)$ with a constant $c_2 \in \mathcal{O}_{K,S_0}^\times$. Using the inclusions (5.6), there is no harm in multiplying α by $f(t)\cdot (K^\times)^2$.

So without loss of generality, we may assume that $\alpha = c\cdot (K^\times)^2$ with $c \in \mathcal{O}_{K,S\cup\{\mathfrak{q}_1\}}^\times$. It suffices to show that $\alpha = 1$. Since π is a prime in $\mathcal{O}_K$ that generates $\mathfrak{q}_1$, we may assume that c was chosen so that $c = u\pi^g$ with $u \in \mathcal{O}_{K,S}^\times$ and $g \in \{0,1\}$. Take any $v \in S \cup S_\infty$. We have $c\cdot (K_v^\times)^2 \in \mathrm{Im}(\delta_{E'_t,v})$ since $\alpha \in \mathrm{Sel}_{\phi_t}(E_t/K)$. Since $t = m/n$ lies in U_v by our choice of m and n, Lemma 5.5 implies that $c\cdot (K_v^\times)^2 \in \mathrm{Im}(\delta_{E'_t,v}) = \Phi_v$. The prime π was chosen so that it is a square in K_v and hence $u\cdot (K_v^\times)^2 \in \Phi_v$. Since $u \in \mathcal{O}_{K,S}^\times$ satisfies $u\cdot (K_v^\times)^2 \in \Phi_v$ for all $v \in S\cup S_\infty$, we deduce that u is a square in $\mathcal{O}_{K,S}^\times$ by the isomorphism of Lemma 5.5(b). Therefore, $\alpha = \pi^g\cdot (K^\times)^2$ for some $g \in \{0,1\}$.

Fix an $e' \in \mathcal{M}'$ and an $e \in \mathcal{M}$ satisfying Proposition 5.9(c).

We claim that $m - e'n$ is not a square modulo $\mathfrak{q}_1$. We have $m - en \equiv 0 \pmod{\mathfrak{q}_1}$ and hence $m - e'n = (m - en) + (e - e')n \equiv (e - e')n \pmod{\mathfrak{q}_1}$. Since $e - e'$ lies in $\mathcal{O}_{K,S_0}^\times$ it is a nonzero square modulo $\mathfrak{q}_1$. By our choice of m and n, we know that n is not a square modulo $\mathfrak{q}_1$. Therefore, $m - e'n$ is not a square modulo $\mathfrak{q}_1$ as claimed.

We have $v_{\mathfrak{p}}(m - e'n) = 0$ for all prime ideals of $\mathcal{O}_K$ dividing 2 by Proposition 5.9(e). From the above claim, we have $v_{\mathfrak{q}_1}(m - e'n) = 0$. So (5.5) implies that

$$(m - e'n)\mathcal{O}_K = \mathfrak{p}_{e'} \prod_{\mathfrak{p} \in S \cup \{\mathfrak{q}_2\},\, \mathfrak{p} \nmid 2} \mathfrak{p}^{f_{\mathfrak{p}}}$$

for unique $f_{\mathfrak{p}} \in \mathbb{Z}$. Using second power residue symbols for the field K, cf. [Neu99, VI §8], we have

$$\left(\frac{m - e'n}{\pi}\right) = \left(\frac{\pi}{m - e'n}\right) = \left(\frac{\pi}{\mathfrak{p}_{e'}}\right) \cdot \prod_{\mathfrak{p} \in S \cup \{\mathfrak{q}_2\},\, \mathfrak{p} \nmid 2} \left(\frac{\pi}{\mathfrak{p}}\right)^{f_{\mathfrak{p}}} = \left(\frac{\pi}{\mathfrak{p}_{e'}}\right),$$

where the first equality uses the general reciprocity law [Neu99, VI Theorem 8.3] and the last equality uses Lemmas 5.7 and 5.8. Note that in applying the reciprocity law, we have used Lemma 5.7 which shows that our π is a square in K_v for all places v of K that are infinite or divide 2. We have already proved that $m - e'n$ is not a square modulo $\mathfrak{q}_1 = \pi\mathcal{O}_K$ and hence $\left(\frac{\pi}{\mathfrak{p}_{e'}}\right) = -1$. Therefore, π is not a square in $K_{\mathfrak{p}_{e'}}$. We have $\operatorname{Im}(\delta_{E'_t,\mathfrak{p}_{e'}}) = 1$ by Lemma 5.12(ii) and hence $\pi \cdot (K_{\mathfrak{p}_{e'}}^\times)^2 \notin \operatorname{Im}(\delta_{E'_t,\mathfrak{p}_{e'}})$. Since $\alpha = \pi^g \cdot (K^\times)^2 \in \operatorname{Sel}_{\phi_t}(E_t/K)$ this implies that $g \neq 1$ and hence $\alpha = 1$. □

We can now compute the dimensions of the images of δ_{E_t} and $\delta_{E'_t}$ from which we will be able to determine the rank of E_t.

Lemma 5.14. *As vector spaces over $\mathbb{F}_2$, $\delta_{E_t}(E_t(K))$ and $\delta_{E'_t}(E'_t(K))$ have dimensions $|\mathcal{A}| + |\mathcal{M}| - 1$ and $|\mathcal{A}| + |\mathcal{M}'| - 1$, respectively.*

Proof. For each subset $B \subseteq \mathcal{A} \cup \mathcal{M}$ with even cardinality, let $c_B \in K^\times$ be the unique value for which $f_B := c_B \prod_{e \in B}(T - e)$ lies in $\mathscr{F}$; each $f \in \mathscr{F}$ is of the form f_B for a unique such B. By our choice of S_0, we have $c_B \in \mathcal{O}_{K,S_0}^\times$. Since $f_B(t) = c_B n^{-|B|} \prod_{e \in B}(m - en)$, Lemma 5.10 implies that $v_{\mathfrak{p}_e}(f_B(t)) = 1$ if $e \in B$ and $v_{\mathfrak{p}_e}(f_B(t)) = 0$ if $e \in (\mathcal{A} \cup \mathcal{M}) - B$. In particular, we can recover any polynomial $f \in \mathscr{F}$ from the square class $f(t) \cdot (K^\times)^2$. This proves that

$$|\{f(t) \cdot (K^\times)^2 : f \in \mathscr{F}\}| = 2^{|\mathcal{A}| + |\mathcal{M}| - 1}.$$

Similarly, we have $|\{f(t) \cdot (K^\times)^2 : f \in \mathscr{F}'\}| = 2^{|\mathcal{A}| + |\mathcal{M}'| - 1}$.

By Lemma 5.13, we have $|\operatorname{Sel}_{\phi_t}(E_t/K)| = |\delta_{E'_t}(E'_t(K))| = 2^{|\mathcal{A}| + |\mathcal{M}'| - 1}$. Therefore, $|\operatorname{Sel}_{\hat{\phi}_t}(E'_t/K)| = 2^{|\mathcal{A}| + |\mathcal{M}| - 1}$ by Lemma 5.12(iii). Now consider the inclusions

$$\operatorname{Sel}_{\hat{\phi}_t}(E'_t/K) \supseteq \delta_{E_t}(E_t(K)) \supseteq \{f(t) \cdot (K^\times)^2 : f \in \mathscr{F}\} \tag{5.8}$$

coming from the definition of the Selmer group and Lemma 5.2. We have $|\delta_{E_t}(E_t(K))| = 2^{|\mathcal{A}| + |\mathcal{M}| - 1}$ since we have shown that the other two groups occurring in (5.8) have this cardinality. □

By Lemma 5.14, we have $\dim_{\mathbb{F}_2} \delta_{E_t}(E_t(K)) + \dim_{\mathbb{F}_2} \delta_{E'_t}(E'_t(K)) - 2 = r$. Therefore, the elliptic curve E_t over K has rank r by Lemma 3.1.

5.4. **End of proof.** The following result was proved in §5.3.

Lemma 5.15. *For any finite set D satisfying $\mathcal{B} \subseteq D \subseteq K$, there is a $t \in K - D$ such that the elliptic curve E_t over K has rank r.* $\square$

Let R be the set of $t \in K - \mathcal{B}$ for which E_t has rank r. If R is finite, then Lemma 5.15 with $D := R \cup \mathcal{B}$ implies that there is a $t \in K - (R \cup \mathcal{B})$ for which E_t has rank r; however, this contradicts the definition of R. Therefore, the set R is infinite.

Let $J \in K(T)$ be the j-invariant of the elliptic curve E over $K(T)$; it is nonconstant since by assumption E has a fiber of multiplicative reduction. For $t \in K - \mathcal{B}$, the j-invariant $j(E_t)$ of the elliptic curve E_t is equal to $J(t) \in K$. For any $j \in K$, there are only finitely many $t \in K - \mathcal{B}$ for which $J(t) = j$ since J is nonconstant. Since R is infinite, so is the set $\{J(t) : t \in R\} = \{j(E_t) : t \in R\}$. The theorem follows since an elliptic curve over K is determined up to $\overline{K}$-isomorphism by its j-invariant.

6. Proof of Theorem 1.1

Take any number field K. For each $0 \leq r \leq 4$, we will construct an elliptic curve E over $K(T)$ that satisfies all the conditions in §4 with this particular value of r. Theorem 1.1 will then follow from Theorem 4.1.

6.1. **Rank 0 case.** Let E be the elliptic curve over $K(T)$ defined by the Weierstrass equation

$$y^2 = x^3 + 2x^2 + Tx.$$

With notation as in §4, we have an elliptic curve E' over $K(T)$ given by the model

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

The discriminants of these models of E and E' are $\Delta = -2^6T^2(T-1)$ and $\Delta' = 2^{12}T(T-1)^2$, respectively. Conditions (a) holds since Δ factors into linear terms in $K[T]$. One can check that

$$\mathcal{A} = \{\infty\}, \quad \mathcal{M} = \{0\} \quad \text{and} \quad \mathcal{M}' = \{1\}.$$

The elliptic curve E has Kodaira symbols I_1 and III^* at 1 and ∞, respectively. The elliptic curve E' has Kodaira symbols I_1 and III^* at 0 and ∞, respectively. Therefore, conditions (b)–(e) hold.

Define the point $P_0 = (0,0)$ of $E(K(T))$. Since $\delta_E(P_0) = T \cdot (K(T)^\times)^2$ we deduce that $\delta_E(E(K(T)))$ has dimension at least $|\mathcal{A}| + |\mathcal{M}| - 1$ over $\mathbb{F}_2$. This verifies condition (f).

Define the point $Q_0 = (0,0)$ of $E'(K(T))$. Since $\delta_{E'}(Q_0) = -(T-1) \cdot (K(T)^\times)^2$ we deduce that $\delta_{E'}(E'(K(T)))$ has dimension at least $|\mathcal{A}| + |\mathcal{M}'| - 1$ over $\mathbb{F}_2$. This verifies condition (g).

Define $r := 2|\mathcal{A}| + |\mathcal{M}| + |\mathcal{M}'| - 4 = 0$. By Theorem 4.1, we deduce that there are infinitely many elliptic curves over K, up to isomorphism over $\overline{K}$, of rank $r = 0$.

6.2. **Rank 1 case.** Let E be the elliptic curve over $K(T)$ defined by the Weierstrass equation

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

With notation as in §4, we have an elliptic curve E' over $K(T)$ given by the model

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

The discriminants of these models of E and E' are $\Delta = 2^4T^3(T-1)^2(T-4)$ and $\Delta' = 2^8T^3(T-1)^4(T-4)^2$, respectively. Condition (a) holds since Δ factors into linear terms in $K[T]$. One can check that

$$\mathcal{A} = \{0\}, \quad \mathcal{M} = \{\infty\} \quad \text{ and } \quad \mathcal{M}' = \{1, 4\}.$$

The elliptic curve E' has Kodaira symbol I_3 at ∞. The elliptic curve E has split multiplicative reduction at 1 and has Kodaira symbol I_1 at 4. The elliptic curves E and E' both have Kodaira symbol III at 0. Therefore, conditions (b)–(e) hold.

Define the point $P_0 = (0, 0)$ of $E(K(T))$. Since $\delta_E(P_0) = T \cdot (K(T)^\times)^2$ we deduce that $\delta_E(E(K(T)))$ has dimension at least $|\mathcal{A}| + |\mathcal{M}| - 1$ over $\mathbb{F}_2$. This verifies condition (f).

Define the points $Q_0 = (0, 0)$ and $Q_1 = (T(T-1), 2T(T-1))$ of $E'(K(T))$. Since $\delta_{E'}(Q_0) = T(T-4) \cdot (K(T)^\times)^2$ and $\delta_{E'}(Q_1) = T(T-1) \cdot (K(T)^\times)^2$ we deduce that $\delta_{E'}(E'(K(T)))$ has dimension at least $|\mathcal{A}| + |\mathcal{M}'| - 1$ over $\mathbb{F}_2$. This verifies condition (g).

Define $r := 2|\mathcal{A}| + |\mathcal{M}| + |\mathcal{M}'| - 4 = 1$. By Theorem 4.1, we deduce that there are infinitely many elliptic curves over K, up to isomorphism over $\overline{K}$, of rank $r = 1$.

6.3. **Rank 2 case.** Let E be the elliptic curve over $K(T)$ defined by the Weierstrass equation

$$y^2 = x^3 + 10(T + 16)x^2 + 9T(T + 16)x.$$

With notation as in §4, we have an elliptic curve E' over $K(T)$ given by the model

$$y^2 = x^3 - 20(T + 16)x^2 + 64(T + 16)(T + 25)x.$$

The discriminants of these models of E and E' are $\Delta = 2^{10}3^4T^2(T + 16)^3(T + 25)$ and $\Delta' = 2^{20}3^2T(T + 16)^3(T + 25)^2$, respectively. Condition (a) holds since Δ factors into linear terms in $K[T]$. One can check that

$$\mathcal{A} = \{-16, \infty\}, \quad \mathcal{M} = \{0\} \quad \text{ and } \quad \mathcal{M}' = \{-25\}.$$

The elliptic curve E' has Kodaira symbol I_1 at 0. The elliptic curve E has Kodaira symbol I_1 at -25. The elliptic curves E and E' both have Kodaira symbol III at -16. The elliptic curves E and E' both have Kodaira symbol I_0^* at ∞ and $c_\infty(E) = c_\infty(E') = 4$. Therefore, conditions (b)–(e) hold.

Define the points $P_0 = (0, 0)$ and $P_1 = (-T, 4T)$ of $E(K(T))$. Since $\delta_E(P_0) = T(T + 16) \cdot (K(T)^\times)^2$ and $\delta_E(P_1) = -T \cdot (K(T)^\times)^2$ we deduce that $\delta_E(E(K(T)))$ has dimension at least $|\mathcal{A}| + |\mathcal{M}| - 1$ over $\mathbb{F}_2$. This verifies condition (f).

Define the points $Q_0 = (0, 0)$ and $Q_1 = (4(T + 16), 48(T + 16))$ of $E'(K(T))$. Since $\delta_{E'}(Q_0) = (T + 16)(T + 25) \cdot (K(T)^\times)^2$ and $\delta_{E'}(Q_1) = (T + 16) \cdot (K(T)^\times)^2$ we deduce that $\delta_{E'}(E'(K(T)))$ has dimension at least $|\mathcal{A}| + |\mathcal{M}'| - 1$ over $\mathbb{F}_2$. This verifies condition (g).

Define $r := 2|\mathcal{A}| + |\mathcal{M}| + |\mathcal{M}'| - 4 = 2$. By Theorem 4.1, we deduce that there are infinitely many elliptic curves over K, up to isomorphism over $\overline{K}$, of rank $r = 2$.

6.4. **Rank 3 case.** Let E be the elliptic curve over $K(T)$ defined by the Weierstrass equation

$$y^2 = x^3 - (98T^2 - 9725) \cdot x^2 + 7^4(T^2 - 2^2)(T^2 - 11^2) \cdot x.$$

With notation as in §4, we have an elliptic curve E' over $K(T)$ given by the model

$$y^2 = x^3 + (196T^2 - 19450) \cdot x^2 - 2^63^25^27^2(T^2 - (\tfrac{3161}{280})^2) \cdot x.$$

The discriminants of these models of E and E' are $\Delta = -2^{10}3^25^27^{10}(T^2-2^2)^2(T^2-11^2)^2(T^2-(\frac{3161}{280})^2)$ and $\Delta' = 2^{20}3^45^47^8(T^2-2^2)(T^2-11^2)(T^2-(\frac{3161}{280})^2)^2$, respectively. Condition (a) holds since Δ factors into linear terms in $K[T]$. One can check that

$$\mathcal{A} = \emptyset, \quad \mathcal{M} = \{\pm 2, \pm 11\} \quad \text{ and } \mathcal{M}' = \{\pm \tfrac{3161}{280}, \infty\}.$$

The elliptic curve E' has Kodaira symbol I_1 at all points in $\mathcal{M}$. The elliptic curve E has Kodaira symbol I_1 at the points $\pm\frac{3161}{280}$. The elliptic curve E has split multiplicative reduction at ∞. Therefore, conditions (b)–(e) hold.

Define the following points in $E(K(T))$:

$$\begin{aligned}
P_0 &:= (0,0),\\
P_1 &:= (7^4(T-2)(T+2), 115248T(T-2)(T+2)),\\
P_2 &:= (7^2(T-2)(T+11), 4263(T-2)(T+11)).
\end{aligned}$$

By considering $\delta_E(P_i)$ with $0 \leq i \leq 2$, we find that $\delta_E(E(K(T)))$ contains the subgroup of $K(T)^\times/(K(T)^\times)^2$ generated by the set

$$\{(T-2)(T+2)(T-11)(T+11), (T-2)(T+2), (T-2)(T+11)\}.$$

In particular, $\delta_E(E(K(T)))$ has dimension at least $|\mathcal{A}| + |\mathcal{M}| - 1$ over $\mathbb{F}_2$ which verifies condition (f).

Define the points $Q_0 = (0,0)$ and

$$Q_1 = (630T + 28449/4, 8820T^2 + \tfrac{177093}{2}T - \tfrac{995715}{8})$$

of $E'(K(T))$. By considering $\delta_{E'}(Q_0)$ and $\delta_{E'}(Q_1)$, we find that $\delta_{E'}(E'(K(T)))$ contains the subgroup of $K(T)^\times/(K(T)^\times)^2$ generated by the set

$$\{-(T-\tfrac{3161}{280})(T-\tfrac{3161}{280}), 70(T+\tfrac{3161}{280})\}.$$

In particular, $\delta_{E'}(E'(K(T)))$ has dimension at least $|\mathcal{A}| + |\mathcal{M}'| - 1$ over $\mathbb{F}_2$ which verifies condition (g).

Define $r := 2|\mathcal{A}|+|\mathcal{M}|+|\mathcal{M}'|-4 = 3$. By Theorem 4.1, we deduce that there are infinitely many elliptic curves over K, up to isomorphism over $\overline{K}$, of rank $r = 3$.

6.5. **Rank 4 case.** Let E be the elliptic curve over $K(T)$ defined by the Weierstrass equation

$$y^2 = x^3 - 70(T^2-25^2)\cdot x^2 + 2^47^2(T^2-11^2)(T^2-25^2)\cdot x.$$

With notation as in §4, we have an elliptic curve E' over $K(T)$ given by the model

$$y^2 = x^3 + 140(T^2-25^2)\cdot x^2 + 2^23^27^2(T^2-25^2)(T^2-39^2)\cdot x.$$

The discriminants of these models of E and E' are $\Delta = 2^{14}3^27^6(T^2-11^2)^2(T^2-25^2)^3(T^2-39^2)$ and $\Delta' = 2^{16}3^47^6(T^2-11^2)(T^2-25^2)^3(t^2-39^2)^2$, respectively. Condition (a) holds since Δ factors into linear terms in $K[T]$. One can check that

$$\mathcal{A} = \{\pm 25\}, \quad \mathcal{M} = \{\pm 11\} \quad \text{ and } \quad \mathcal{M}' = \{\pm 39\}.$$

The elliptic curve E' has Kodaira symbol I_1 at the points in $\mathcal{M}$. The elliptic curve E has Kodaira symbol I_1 at the points in $\mathcal{M}'$. The elliptic curves E and E' both have Kodaira symbol III at the points in $\mathcal{A}$. Therefore, conditions (b)–(e) hold.

Define the following points in $E(K(T))$:

$$\begin{aligned}
P_0 &:= (0,0),\\
P_1 &:= (14(T-11)(T+11), 1176(T-11)(T+11)),\\
P_2 &:= (2(T-11)(T-25), (36T+780)(T-11)(T-25)).
\end{aligned}$$

By considering $\delta_E(P_i)$ with $0 \le i \le 2$, we find that $\delta_E(E(K(T)))$ contains the subgroup of $K(T)^\times/(K(T)^\times)^2$ generated by the set

$$\{(T-11)(T+11)(T-25)(T+25), 14(T-11)(T+11), 2(T-11)(T-25)\}.$$

In particular, $\delta_E(E(K(T)))$ has dimension at least $|\mathcal{A}| + |\mathcal{M}| - 1$ over $\mathbb{F}_2$ which verifies condition (f).

Now consider the following points in $E'(K(T))$:

$$\begin{aligned}
Q_0 &:= (0,0),\\
Q_1 &:= (2(T-25)(T-39), (64T+1760)(T-25)(T-39))\\
Q_2 &:= (-14(T-25)(T+25), 4704(T-25)(T+25)).
\end{aligned}$$

By considering $\delta_{E'}(Q_i)$ with $0 \le i \le 2$, we find that $\delta_{E'}(E'(K(T)))$ contains the subgroup of $K(T)^\times/(K(T)^\times)^2$ generated by the set

$$\{(T-25)(T+25)(T-39)(T+39), 2(T-25)(T-39), -14(T-25)(T+25)\}.$$

In particular, $\delta_{E'}(E'(K(T)))$has dimension at least $|\mathcal{A}| + |\mathcal{M}'| - 1$ over $\mathbb{F}_2$ which verifies condition (g).

Define $r := 2|\mathcal{A}|+|\mathcal{M}|+|\mathcal{M}'|-4 = 4$. By Theorem 4.1, we deduce that there are infinitely many elliptic curves over K, up to isomorphism over $\overline{K}$, of rank $r = 4$.

References

[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. ↑1.1

[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. ↑3.2

[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. ↑3.2, 5.2

[Elk07] Noam Elkies, *Three lectures on elliptic surfaces and curves of high rank* (2007). arXiv:0709.2908v1. ↑1

[Kai25] Wataru Kai, *Linear patterns of prime elements in number fields* (2025). arXiv:2306.16983. ↑2, 5.3

[KP24] Peter Koymans and Carlo Pagano, *Hilbert's tenth problem via additive combinatorics* (2024). arXiv:2412.01768. ↑1.1

[KP25] ———, *Elliptic curves of rank one over number fields* (2025). arXiv:2505.16910. ↑1.1

[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. ↑5.2, 5.3

[OS91] Keiji Oguiso and Tetsuji Shioda, *The Mordell-Weil lattice of a rational elliptic surface*, Comment. Math. Univ. St. Paul. **40** (1991), no. 1, 83–99. MR1104782 ↑2

[PPVW19] Jennifer Park, Bjorn Poonen, John Voight, and Melanie Matchett Wood, *A heuristic for boundedness of ranks of elliptic curves*, J. Eur. Math. Soc. (JEMS) **21** (2019), no. 9, 2859–2903, DOI 10.4171/JEMS/893. MR3985613 ↑1

[Sat87] Philippe Satgé, *Un analogue du calcul de Heegner*, Invent. Math. **87** (1987), no. 2, 425–439, DOI 10.1007/BF01389425 (French). ↑1.1

[Sav25] Ben Savoie, *Infinitely many elliptic curves over $\mathbb{Q}(i)$ with rank 2 and j-invariant 1728* (2025). arXiv:2506.17605. ↑1.1

[Shi92] Tetsuji Shioda, *Some remarks on elliptic curves over function fields*, Astérisque **209** (1992), 12, 99–114. Journées Arithmétiques, 1991 (Geneva). MR1211006 ↑2, 4

[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, 2

[Sil94] ———, *Advanced topics in the arithmetic of elliptic curves*, Graduate Texts in Mathematics, vol. 151, Springer-Verlag, New York, 1994. ↑3.3, 5.2

[Sil09] ———, *The arithmetic of elliptic curves*, 2nd ed., Graduate Texts in Mathematics, vol. 106, Springer, Dordrecht, 2009. ↑3

[Zyw25a] David Zywina, *An elliptic surface with infinitely many fibers for which the rank does not jump* (2025). arXiv:2502.01026. ↑1.1

[Zyw25b] ———, *There are infinitely many elliptic curves over the rationals of rank* 2 (2025). arXiv:2502.01957. ↑1.1

[Zyw25c] ———, *Rank one elliptic curves and rank stability* (2025). arXiv:2505.16960. ↑1.1, 3.2

Department of Mathematics, Cornell University, Ithaca, NY 14853, USA
Email address: `zywina@math.cornell.edu`