Descent on elliptic surfaces and arithmetic bounds for the Mordell-Weil rank

Jean Gillibert Aaron Levin

June 2021

Abstract

We introduce the use of p-descent techniques for elliptic surfaces over a perfect field of characteristic not 2 or 3. Under mild hypotheses, we obtain an upper bound for the rank of a non-constant elliptic surface. When $p = 2$, this bound is an arithmetic refinement of a well-known geometric bound for the rank deduced from Igusa's inequality. This answers a question raised by Ulmer. We give some applications to rank bounds for elliptic surfaces over the rational numbers.

1 Introduction

The aim of this paper is to introduce the use of classical p-descent techniques for elliptic curves over function fields of one variable, and to use these techniques to derive general bounds for the Mordell-Weil rank which are sensitive to the field of constants of the function field. Let k be a field of characteristic not 2 or 3 and let S be a smooth projective geometrically integral curve over k. Let E be a (nonconstant) elliptic curve over the function field $k(S)$. Using cohomological arguments (see §1.2), one obtains the following well-known upper bound for the rank:

$$\mathrm{rk}_{\mathbb{Z}}\, E(k(S)) \leq 4g(S) - 4 + \deg(\mathfrak{f}_E), \tag{1}$$

where $g(S)$ is the genus of S and $\deg(\mathfrak{f}_E)$ is the degree of the conductor of E, viewed as a divisor on S (in fact, (1) also holds in characteristics 2 and 3). Following [Sil04], we call (1) the *geometric rank bound*. This bound is geometric in the sense that the right-hand side does not depend on the field k, and in particular the inequality (1) holds with k replaced by its algebraic closure. In positive characteristic, there are examples with conductor of arbitrarily large degree for which the inequality (1) is sharp (see [Shi86], [Ulm02]).

When k is a number field, Ulmer [Ulm04, Section 9] has raised the question of the existence of *arithmetic bounds* improving (1), that is, refinements of the inequality (1) which depend on the arithmetic of the field k. Ulmer noted that work of Silverman [Sil00, Sil04] on ranks of elliptic curves over abelian towers provided some evidence for the existence of such a bound. Under mild hypotheses, we give a positive answer to Ulmer's question, providing a bound for the rank which is equivalent to (1) when k is algebraically closed (see §1.2), and which in general yields an improvement depending on the arithmetic of the field k. The precise statement is given in Theorem 1.1: for each suitable prime p, we obtain a bound which depends crucially on the number of k-rational p-torsion points in the Jacobian of a certain curve associated to the p-torsion subgroup of E. Two examples (1.10, 1.11), and one application (Theorem 1.13), are given when $k = \mathbb{Q}$.

When $k = \mathbb{F}_q$ is a finite field, Brumer [Bru92] used Weil's "explicit formula" to prove an arithmetic bound for the rank of E depending on q:

$$\mathrm{rk}_{\mathbb{Z}}\, E(k(S)) \leq \frac{4g(S) - 4 + \deg(\mathfrak{f}_E)}{2\log_q \deg(\mathfrak{f}_E)} + c\frac{\deg(\mathfrak{f}_E)}{(\log_q \deg(\mathfrak{f}_E))^2}, \tag{2}$$

where c is an explicit constant depending only on $g(S)$ and q. Although there are examples with conductor of arbitrarily large degree for which the main term in the inequality (2) is sharp (see [Ulm02]), our bounds will frequently also provide an improvement to (2). Silverman [Sil04, Conjecture 4] has stated a conjectural analogue of Brumer's inequality over number fields, and Theorem 1.1 provides a possible approach towards Silverman's conjecture (Remark 1.16).

It is quite surprising that, although p-descent techniques have been extensively used in order to bound the rank of elliptic curves over number fields, we have not been able to track a similar use of these techniques in the function field setting, apart from a few exceptions (see Remark 1.4).

Instead, a more common approach takes advantage of the rich theory that can be developed in this setting by relating the geometry of surfaces and the Mordell-Weil group of an elliptic curve over a function field, enriched with the lattice structure on the torsion-free part induced by the Néron-Tate height pairing. The detailed analysis of these Mordell-Weil lattices was developed simultaneously by Elkies and Shioda in the late 80's, and quickly became a powerful and central tool in the study of elliptic curves over function fields.

Despite the success of this approach, we believe that p-descent techniques can shed new light on classical results in the function field setting, and provide new ideas to tackle open questions. Additionally, these techniques may be advantageous for studying "arithmetic" problems, where one desires finer information over a non-algebraically closed field. For instance, in recent work we give applications of our general p-descent result to the construction of number fields with "large" ideal class groups [GL19], and in a forthcoming paper, we give applications to the study of integral points on elliptic curves over function fields.

1.1 p-descent: the generic case

Let k be a perfect field of characteristic not 2 or 3. In the applications we have in mind, k may be a number field, or a finite field, or the algebraic closure of such fields.

Let S be a smooth projective geometrically integral curve over k, and let $k(S)$ be the function field of S. By abuse of notation, we identify closed points of the scheme S and discrete valuations of $k(S)/k$. If v is such a valuation, we denote by k_v the residue field of v, which is a finite extension of k. The scheme S being a Dedekind scheme, if we start with an elliptic curve over $k(S)$ we may consider its Néron model over S. In the present paper, the word *Néron model* refers to Néron's group scheme model, which is the smooth locus of Néron's minimal regular model (see [BLR90, §1.5] or [Liu02, §10.2]).

Throughout this paper, we consider the following setting:

1. E is an elliptic curve over $k(S)$.
2. $\mathcal{E} \to S$ is the Néron model of E over S.
3. $\Sigma \subset S$ is the set of places of bad reduction of $\mathcal{E}$.
4. $p \neq \mathrm{char}(k)$ is a prime number.
5. $\mathcal{E}[p] \to S$ is the group scheme of p-torsion points of $\mathcal{E}$. The map $\mathcal{E}[p] \to S$ is étale, and its restriction to $S \setminus \Sigma$ is finite of degree p^2.

The étaleness of $\mathcal{E}[p] \to S$ stated above follows from the fact that the prime p is invertible on S (assumption 4); see [BLR90, §7.3, Lemma 2, (b)] for a proof. Since S is smooth and the composition of smooth morphisms is smooth, one deduces that $\mathcal{E}[p] \setminus \{0\}$ is smooth over k.

If $v \in \Sigma$ is a place of bad reduction of $\mathcal{E}$, we denote by $\mathcal{E}_v := \mathcal{E} \times_S k_v$ the special fiber of $\mathcal{E}$ at v, by $\mathcal{E}_v^0$ the connected component of the identity in $\mathcal{E}_v$, and by Φ_v the component group of $\mathcal{E}_v$. By definition, we have an exact sequence for the étale topology on k_v

$$0 \longrightarrow \mathcal{E}_v^0 \longrightarrow \mathcal{E}_v \longrightarrow \Phi_v \longrightarrow 0, \tag{3}$$

and Φ_v is a finite étale group scheme over k_v. The *Tamagawa number* of $\mathcal{E}$ at v is by definition the order of $\Phi_v(k_v)$, and we denote it by c_v. Finally, we denote by Φ the skyscraper sheaf over S whose fiber at v is Φ_v, and by $\mathcal{E}^{p\Phi}$ the inverse image of $p\Phi$ by the natural map $\mathcal{E} \to \Phi$.

The scheme $\mathcal{E}[p] \setminus \{0\}$ (where $\{0\}$ denotes the image of the unit section of $\mathcal{E} \to S$) is a smooth scheme of dimension one over k, with a degree $p^2 - 1$ quasi-finite map to S. The deficiency of finiteness of this map can be understood as follows: above a place v of multiplicative reduction at which Φ_v has no p-torsion, the fiber of $\mathcal{E}[p] \to S$ has p points instead of p^2. Above a place v of additive reduction at which Φ_v has no p-torsion, the fiber of $\mathcal{E}[p] \to S$ has only one point. As a result, the scheme $\mathcal{E}[p]$ is not projective over k.

We shall denote by C the smooth compactification of $\mathcal{E}[p] \setminus \{0\}$, endowed with its canonical finite map $C \to S$ of degree $p^2 - 1$. By construction, C is a smooth projective curve over k, and the inclusion $\mathcal{E}[p] \setminus \{0\} \hookrightarrow C$ is an isomorphism above the open subset of good reduction of E.

By elementary Galois theory, the following conditions are equivalent:

(i) C is a geometrically integral k-curve;

(ii) $(E[p] \otimes_k \overline{k}) \setminus \{0\}$ is the spectrum of a field;

(iii) the action of $\mathrm{Gal}(\overline{k(S)}/\overline{k}(S))$ on $E[p] \setminus \{0\}$ is transitive.

In the sequel, we shall assume that these conditions hold. This implies that E is non-constant, but does not prevent it from being isotrivial. On the other hand, if E is not isotrivial, then it was proved by Igusa [Igu59] that, for all but finitely many p, the image of the Galois representation $\mathrm{Gal}(\overline{k(S)}/\overline{k}(S)) \to \mathrm{GL}_2(\mathbb{F}_p)$ attached to $E[p]$ is $\mathrm{SL}_2(\mathbb{F}_p)$, which implies condition (iii).

We are ready to state the main result of this paper, which provides an arithmetic upper bound on the rank of elliptic curves over function fields. The proof, which is given in §2.1, relies on p-descent techniques, analogous to the number field case.

Theorem 1.1. *Assume that the action of* $\mathrm{Gal}(\overline{k(S)}/\overline{k}(S))$ *on* $E[p] \setminus \{0\}$ *is transitive, and let* C *be the smooth compactification of* $\mathcal{E}[p] \setminus \{0\}$. *Then:*

1) If $p \geq 3$, *there is an injective morphism*

$$\mathcal{E}^{p\Phi}(S)/p\mathcal{E}(S) \longrightarrow \ker\left(N_{C/C^+} : \mathrm{Pic}(C)[p] \to \mathrm{Pic}(C^+)[p]\right), \tag{4}$$

where C^+ *is the quotient of* C *by the involution* $P \mapsto -P$, *and* N_{C/C^+} *denotes the norm map. It follows that*

$$\mathrm{rk}_{\mathbb{Z}}\, E(k(S)) \leq \dim_{\mathbb{F}_p} \mathrm{Pic}(C)[p] - \dim_{\mathbb{F}_p} \mathrm{Pic}(C^+)[p] + \#\{v \in \Sigma, p \mid c_v\}. \tag{5}$$

where c_v *denotes the Tamagawa number of* $\mathcal{E}$ *at* v.

2) If $p = 2$, there is an injective morphism

$$\mathcal{E}^{2\Phi}(S)/2\mathcal{E}(S) \longrightarrow \ker\left(N_{C/S} : \mathrm{Pic}(C)[2] \to \mathrm{Pic}(S)[2]\right). \tag{6}$$

It follows that

$$\begin{aligned}\mathrm{rk}_{\mathbb{Z}}\, E(k(S)) \leq & \dim_{\mathbb{F}_2} \mathrm{Pic}(C)[2] - \dim_{\mathbb{F}_2} \mathrm{Pic}(S)[2] + \#\{v \in \Sigma, 2 \mid c_v\} \\ & + \#\{v \in \Sigma, \textit{the red. type of } \mathcal{E} \textit{ at } v \textit{ is } \mathrm{I}_{2n}^* \textit{ for some } n \geq 0\}.\end{aligned} \tag{7}$$

A few comments on the statement of Theorem 1.1:

1. The group $\mathcal{E}^{p\Phi}(S)$ is the group of sections of $\mathcal{E}$ which, in each fiber, reduce to a component which is a multiple of p in the group of components. The quotient $\mathcal{E}^{p\Phi}(S)/p\mathcal{E}(S)$ measures the difference between sections which are locally multiples of p and those which are globally multiples of p (where locally should be understood in the sense of étale topology). The injective morphism (4) is, roughly speaking, a coboundary map for the Kummer exact sequence induced by multiplication by p on $\mathcal{E}$.

2. Let J_C be the Jacobian of C. Then $\mathrm{Pic}(C)[p]$ is a subgroup of $J_C(k)[p]$, the group of k-rational p-torsion points on J_C (equality holds, for example, if $C(k) \neq \emptyset$). Thus, $\mathrm{Pic}(C)[p]$ is a quantity which depends on the arithmetic of C over k.

3. Observe that the norm map $N_{C/C^+} : \mathrm{Pic}(C)[p] \to \mathrm{Pic}(C^+)[p]$ is surjective when $p \geq 3$, because the degree of $C \to C^+$ is 2, which is coprime to p. It follows that the quantity $\dim_{\mathbb{F}_p} \mathrm{Pic}(C)[p] - \dim_{\mathbb{F}_p} \mathrm{Pic}(C^+)[p]$ cannot decrease when enlarging the field k. The same remark applies when $p = 2$, in which case $C \to S$ has degree 3, and hence the norm map $N_{C/S} : \mathrm{Pic}(C)[2] \to \mathrm{Pic}(S)[2]$ is surjective.

4. In the bound (5), the terms $\dim_{\mathbb{F}_p} \mathrm{Pic}(C)[p] - \dim_{\mathbb{F}_p} \mathrm{Pic}(C^+)[p]$ and $\#\{v \in \Sigma, p \mid c_v\}$ are both of arithmetic nature. As we have seen, the first one depends on the size of the k-rational p-torsion subgroups of the Jacobians of the curves C and C^+. The second one is the number of closed points of S at which $\mathcal{E}$ has bad reduction and Tamagawa number divisible by p. In fact, it follows from Lemma 2.1 that

   $$\#\{v \in \Sigma, p \mid c_v\} = \dim_{\mathbb{F}_p} H^0(S, \Phi[p]).$$

   When enlarging k, this number can increase for two reasons: firstly, a closed point which is not k-rational can split as the sum of several points over a larger field, which has the effect of enlarging the set Σ; secondly, a component of order p in the group Φ_v which is not k_v-rational can become rational over a larger field. The same remark applies, *mutatis mutandis*, for $p = 2$.

5. In the case when $p = 2$, the bound (7) is a geometric analogue of the classical bound of Brumer and Kramer [BK77, Proposition 7.1] for the rank of an elliptic curve over $\mathbb{Q}$ (which does not have a rational point of order 2) in terms of the 2-torsion of the class group of a cubic field and bad reduction data.

6. A comment on the terminology: when we say that E has a fiber of type I_{2n}^* at v, we mean it over k_v, and not just over $\overline{k}$. More precisely, this means that the Kodaira type of $\mathcal{E}_v$ over $\overline{k}$ is I_{2n}^*, and that the four components of $\mathcal{E}_v$ are rational over k_v, in other terms $\Phi_v(k_v) \simeq (\mathbb{Z}/2\mathbb{Z})^2$. In general, the reduction type at v can be described by the data of the reduction type over $\overline{k}$ together with the action of the absolute Galois group of k_v on Φ_v. See [Liu02, §10.2].

7. In practice, given a Weierstrass equation $y^2 = x^3 + Ax + B$ for E, with $A, B \in k(S)$, one can obtain explicit defining equations for C and C^+ over S. More precisely, if $p = 2$ then $C \to S$ is the degree 3 cover defined by the equation $x^3 + Ax + B = 0$. If $p \geq 3$, then $C^+ \to S$ is the degree $(p^2 - 1)/2$ cover defined by the vanishing of the p-division polynomial ψ_p of E, and the curve C is the double cover of C^+ defined by $y^2 = x^3 + Ax + B$, with $\psi_p(x) = 0$.

8. In specific examples, computing the bound (5) requires an efficient algorithm for computing the p-torsion in the Jacobian of a curve. Over finite fields, polynomial-time algorithms exist (see [Cou09]). Over number fields the situation is more complicated, but by reduction modulo a good prime $\neq p$ one obtains an upper bound on the p-torsion.

Remark 1.2. When $p \geq 5$, one can improve (4) as follows: we have an injective morphism

$$\mathcal{E}^{p\Phi}(S)/p\mathcal{E}(S) \longrightarrow \bigcap_{C \to C'} \ker\left(N_{C/C'} : \mathrm{Pic}(C)[p] \to \mathrm{Pic}(C')[p]\right)$$

where $C \to C'$ runs through all proper subcovers of $C \to S$. See Remark 2.8 for the details.

Remark 1.3. It is possible to generalize the statement above by replacing $E[p]$ by a group $G \subset E$ of order $p > 2$ satisfying conditions similar to (i)–(iii). By considering the isogeny $\lambda : E \to F$ with kernel G, one can prove an analogous result in which $\mathcal{E}^{p\Phi}(S)/p\mathcal{E}(S)$ is replaced by $\mathcal{F}^{\lambda\Phi}(S)/\lambda\mathcal{E}(S)$, with obvious notation. Note that $p = 2$ is excluded here, because we need the sum of all elements of $G(\overline{k(S)})$ to be zero in order to make Lemma 2.5 work.

Remark 1.4. The proof of Theorem 1.1 relies on the computation of a geometric analogue of the p-Selmer group, under the assumption that $\mathrm{Gal}(\overline{k(S)}/\overline{k}(S))$ acts transitively on $E[p] \setminus \{0\}$.

There are a few occurrences in the literature of geometric analogues of Selmer groups. Let us cite in particular [CTSSD98], whose Section 4 contains definitions and various properties of these groups; as we note in Remark 2.6, the étale cohomology groups that we compute are closely related to them. We also refer the reader to [Ell06], which is more focused on p^∞-Selmer groups and fundamental groups.

Remark 1.5. When the full p-torsion of E is defined over $k(S)$, one can prove with the same techniques that there exists an injective morphism

$$\mathcal{E}^{p\Phi}(S)/p\mathcal{E}(S) \to H^1(S, \mu_p)^2,$$

where

$$H^1(S, \mu_p) \simeq (k^\times/(k^\times)^p) \oplus \mathrm{Pic}(S)[p].$$

In this case, if k is a number field, then $k^\times/(k^\times)^p$ is infinite, and so the natural generalization of Theorem 1.1 is not relevant (bounding a finite number by $+\infty$). This provides examples in which the geometric analogue of the Selmer group is infinite.

On the other hand, if k is algebraically closed, then $k^\times/(k^\times)^p = \{1\}$, and we obtain the upper bound

$$\dim_{\mathbb{F}_p} \mathcal{E}^{p\Phi}(S)/p\mathcal{E}(S) \leq 4g(S),$$

where $g(S)$ denotes the genus of S. The rationality of the full p-torsion puts strong constraints on the reduction type of $\mathcal{E}$, and in particular, $p \mid c_v$ for each place v of bad reduction. It follows that, in this case, the natural analogues of the inequalities (5) and (7) are both equivalent, whatever the value of p is, to

$$\mathrm{rk}_{\mathbb{Z}}\, E(k(S)) \leq 4g(S) - 2 + \deg(\mathfrak{f}_E),$$

a bound which is weaker than the geometric rank bound (1).

1.2 Refinements of the geometric rank bound

Let us assume that k is algebraically closed. In this case, there are well-known bounds for the rank of elliptic curves over $k(S)$ in terms of the conductor of the curve and the genus of S. For a nice overview of this topic, we refer the reader to [Shi92].

Let $\overline{\mathcal{E}}$ denote the minimal regular model of E over S, which is also a smooth compactification of the k-surface $\mathcal{E}$, and let $\mathrm{NS}(\overline{\mathcal{E}}) := \mathrm{Pic}(\overline{\mathcal{E}})/\mathrm{Pic}^0(\overline{\mathcal{E}})$ be the Néron-Severi group of $\overline{\mathcal{E}}$, which is a free $\mathbb{Z}$-module of finite rank. We let

$$\rho := \mathrm{rk}_{\mathbb{Z}}\,\mathrm{NS}(\overline{\mathcal{E}}),$$

the so-called Picard number of $\overline{\mathcal{E}}$. Igusa's inequality asserts that

$$\rho \leq b_2,$$

where b_2 is the second Betti number of the surface $\overline{\mathcal{E}}$. If the characteristic of k is not zero, b_2 is computed using ℓ-adic cohomology, with $\ell \neq \mathrm{char}(k)$.

Let $\mathfrak{f}_E := \sum_{v\in\Sigma} f_v \cdot v$ be the conductor of $\mathcal{E}$, which is a divisor on S. It is well-known [Sil94, Chap. IV, Theorem 10.2] that $f_v = 1$ if the reduction type of $\mathcal{E}$ at v is multiplicative and $f_v = 2$ if the reduction is additive; the wild part of the conductor is zero since $\mathrm{char}(k) \neq 2, 3$.

The Grothendieck-Ogg-Shafarevich formula [Ray95] states that

$$b_2 - \rho = 4g(S) - 4 - \mathrm{rk}_{\mathbb{Z}}\,E(k(S)) + \deg(\mathfrak{f}_E), \tag{8}$$

where $\deg(\mathfrak{f}_E) = \sum_{v\in\Sigma} f_v$ is the degree of the divisor $\mathfrak{f}_E$. Therefore, Igusa's inequality is equivalent to the geometric bound:

$$\mathrm{rk}_{\mathbb{Z}}\,E(k(S)) \leq 4g(S) - 4 + \deg(\mathfrak{f}_E).$$

In §2.2, we prove the following.

Theorem 1.6. *Assume that $E(\overline{k}(S))[2] = 0$, and let C be the smooth compactification of $\mathcal{E}[2]\setminus\{0\}$. Then*

$$\begin{aligned} 4g(S) - 4 + \deg(\mathfrak{f}_E) = 2g(C) - 2g(S) + \#\{v \in \overline{\Sigma}, 2 \mid c_v\} \\ + \#\{v \in \overline{\Sigma}, \text{the red. type of } \mathcal{E} \text{ at } v \text{ is } \mathrm{I}^*_{2n} \text{ for some } n \geq 0\}. \end{aligned} \tag{9}$$

It follows that the bound (7) *is a refinement of the geometric rank bound* (1).

Thus, as mentioned in the introduction, we obtain a positive answer to Ulmer's question from the survey [Ulm04, §9]. This refinement allows one to improve on known bounds even in characteristic zero (see Example 1.10 and Theorem 1.13).

As a matter of fact, another refinement occurs via 3-descent, provided the field k does not contain cube roots of unity.

Theorem 1.7. *Assume that the prime 3 satisfies (i)–(iii). Let C be the smooth compactification of $\mathcal{E}[3]\setminus\{0\}$, and let C^+ be the quotient of C by the involution $P \mapsto -P$. Then*

$$4g(S) - 4 + \deg(\mathfrak{f}_E) = g(C) - g(C^+) + \#\{v \in \overline{\Sigma}, 3 \mid c_v\}. \tag{10}$$

It follows that, for $p = 3$, the bound (5) *is a refinement of the geometric rank bound* (1) *provided the field k does not contain cube roots of unity.*

Remark 1.8. In fact, Theorem 1.1 provides a family of upper bounds on the rank of E over $k(S)$, one for each prime $p \neq \mathrm{char}(k)$ satisfying assumptions (i)–(iii). While over $\overline{k}$, the bound for $p = 2$ is equivalent to the geometric rank bound (1), the same phenomenon does not hold for $p = 3$, as Theorem 1.7 shows: the difference between the rank bound coming from 3-descent and the geometric rank bound is equal to $g(C) - g(C^+)$ over $\overline{k}$. In fact, the genus of C increases with p, and so for large p the bound (5) will be weaker than the bound (1) over $\overline{k}$ (also note that when $p \geq 5$ our p-descent bound may be improved as in Remark 2.8). However, over nonalgebraically closed fields k, it may still be the case that (5) provides an improved bound, depending on the size of the rational p-torsion subgroup of the Jacobian of C (see Remark 1.16).

Remark 1.9. When k is an algebraically closed field of positive characteristic, the bound (1) can be improved under the assumption that the formal Brauer group of $\mathcal{E}$ has finite height h, in which case it was proved by Artin and Mazur [AM77] that $b_2 - \rho \geq 2h$. This result, which relies on computations in crystalline cohomology, is called the Igusa-Artin-Mazur inequality. As with Igusa's inequality, this is a result of geometric nature.

We end this section by discussing the case when k has characteristic zero, and in particular, the case when k is a number field. When k is an algebraically closed field of characteristic zero, the bound (1) can be improved as follows: Lefschetz's inequality states that $\rho \leq h^{1,1}$, and hence it follows from Hodge theory that $b_2 - \rho \geq 2p_g$, where p_g is the geometric genus of the surface $\mathcal{E}$. By Grothendieck-Ogg-Shafarevich (8), we conclude that

$$\mathrm{rk}_{\mathbb{Z}}\, E(k(S)) \leq 4g(S) - 4 + \deg(\mathfrak{f}_E) - 2p_g. \tag{11}$$

In contrast to the bound (1) in positive characteristic, Lefschetz's bound (11) is not known to be sharp when the right-hand side is large, even over the field of complex numbers. In fact, we do not even know whether or not there exist non-constant elliptic curves over $\mathbb{C}(t)$ with arbitrarily large rank (the current record, due to Shioda [Shi92], is a curve of rank 68 over $\mathbb{C}(t)$).

As the next example shows, when working over $\mathbb{Q}(t)$, the inequality (7) allows one in practice to improve on the bound (11), provided one is able to compute the rational 2-torsion in the Jacobian of a certain trigonal curve.

Example 1.10. Let $q \geq 5$ be a prime number, and let $a \in \mathbb{Z}$ be an odd integer. Let E be the elliptic curve over $\mathbb{Q}(t)$ defined by the equation

$$y^2 = x^3 + t^q + a.$$

Since the polynomial $t^q + a$ is square-free, it follows from Tate's algorithm [Tat75] that E has additive reduction of type II at roots of $t^q + a$, and additive reduction of type II or II* at infinity (because $q \equiv 1$ or $5 \pmod 6$). The degree of the conductor of E is $2(q+1)$. One also computes that the geometric genus is $p_g = \left\lfloor \frac{q-1}{6} \right\rfloor$. Hence, according to (11), we have the bound

$$\mathrm{rk}_{\mathbb{Z}}\, E(\overline{\mathbb{Q}}(t)) \leq 2q - 2 - 2\left\lfloor \frac{q-1}{6} \right\rfloor.$$

Let us now compute the bound (7) from Theorem 1.1. The Tamagawa numbers of E are all equal to 1, hence

$$\mathrm{rk}_{\mathbb{Z}}\, E(\mathbb{Q}(t)) \leq \dim_{\mathbb{F}_2} \mathrm{Pic}(C)[2],$$

where C is the curve defined by the equation $x^3 = t^q + a$. According to [Jed16, Theorem 2.6], the Jacobian of C has no rational 2-torsion, the integer a being odd. Therefore, (7) yields

$$\mathrm{rk}_{\mathbb{Z}}\, E(\mathbb{Q}(t)) = 0.$$

On the other hand, the bound (7) over $\overline{\mathbb{Q}}$ is equivalent to the geometric rank bound:

$$\mathrm{rk}_{\mathbb{Z}}\, E(\overline{\mathbb{Q}}(t)) \leq 2q - 2.$$

Example 1.11. Let $\beta \in \mathbb{Q}^\times$ and let E be the elliptic curve over $\mathbb{Q}(t)$ defined by

$$y^2 = x^3 + tx^2 + t^2(t^2 + \beta).$$

The singular fibers of this curve are listed below (we assume that $\beta \neq 2^2 \cdot 3^{-6}$ so that $27(t^2+\beta)+4t$ is not a square over $\overline{\mathbb{Q}}$):

	$t^2 + \beta = 0$	$27(t^2 + \beta) + 4t = 0$	$t = 0$	$t = \infty$
fiber type	I_1	I_1	IV	IV
order of Φ_v	1	1	3	3

Its conductor is

$$\mathfrak{f}_E = \{t^2 + \beta = 0\} + \{27(t^2 + \beta) + 4t = 0\} + 2 \cdot (\{0\} + \{\infty\})$$

which has degree 8. Moreover, $\mathcal{E}$ is a rational elliptic surface, hence has geometric genus $p_g = 0$, and so the bounds (1) and (11) agree and yield:

$$\mathrm{rk}_{\mathbb{Z}}\, E(\overline{\mathbb{Q}}(t)) \leq \deg(\mathfrak{f}_E) - 4 = 4.$$

In fact, this bound is sharp and the exact value of the rank over $\overline{\mathbb{Q}}(t)$ is 4. More generally, the structure of the Mordell-Weil lattice and related information for $\mathcal{E}$ can be found in entry No. 11 in the table of Oguiso and Shioda [OS91], who classified Mordell-Weil lattices of rational elliptic surfaces over algebraically closed fields.

On the other hand, let C be the curve defined by the equation $x^3 + tx^2 + t^2(t^2 + \beta) = 0$. The Tamagawa numbers being odd, none of the bad fibers contributes to the arithmetic bound (7), and hence we have

$$\mathrm{rk}_{\mathbb{Z}}\, E(\mathbb{Q}(t)) \leq \dim_{\mathbb{F}_2} \mathrm{Pic}(C)[2].$$

By substituting $X = x/t$ and $Y = 2t + X^3 + X^2$, we find that C is a hyperelliptic curve of genus 2, with equation

$$Y^2 = X^4(X + 1)^2 - 4\beta.$$

Let s be the number of irreducible factors of $X^4(X + 1)^2 - 4\beta$ over $\mathbb{Q}$; then

$$\dim_{\mathbb{F}_2} \mathrm{Pic}(C)[2] \leq \dim_{\mathbb{F}_2} J_C(\mathbb{Q})[2] = \begin{cases} s - 1 & \text{if all factors of } X^4(X + 1)^2 - 4\beta \text{ have even degree} \\ s - 2 & \text{otherwise} \end{cases}$$

We compute some examples in the following table:

β	$2^2 5^4 3^{-12}$	$2^2 3^4 7^{-6}$	1	9	$-3^4 5^4 2^{-8}$	2
factorization type of $X^4(X + 1)^2 - 4\beta$	$[1, 1, 2, 2]$	$[1, 1, 1, 3]$	$[1, 2, 3]$	$[3, 3]$	[2,4]	[6]
rank bound over $\mathbb{Q}(t)$	2	2	1	0	1	0

In fact, it can be shown that these examples exhaust all of the possible factorization types for $\beta \in \mathbb{Q}^\times \setminus \{2^2 \cdot 3^{-6}\}$, and it's not hard to parametrize each possibility. For instance, the first four factorization types can occur only when β is a perfect square, and the factorization type $[1,1,2,2]$ occurs precisely when $\beta = \frac{(\alpha^3+\alpha)^4(\alpha-1)^2}{4(\alpha^3+1)^6}$ for some $\alpha \in \mathbb{Q}$.

In a recent preprint [BST+17, Theorem 7.1], Bhargava *et al.* have given the following bounds for 2-torsion over finite fields:

Theorem 1.12. *Let C be a smooth projective curve of genus g over $\mathbb{F}_q$. Then*

$$\dim_{\mathbb{F}_2} \mathrm{Pic}(C)[2] \leq \log_2 \left(\frac{q^{g+1}-1}{q-1} \right).$$

If C admits a degree n map to $\mathbb{P}^1$ (over $\mathbb{F}_q$) then

$$\dim_{\mathbb{F}_2} \mathrm{Pic}(C)[2] \leq \left(1 - \frac{1}{n}\right) g \log_2 q + O_n(1).$$

We note that these results only improve on the trivial bound $\dim_{\mathbb{F}_2} \mathrm{Pic}(C)[2] \leq 2g(C)$ when q is very small. For example, if C is trigonal, then we should take $q \leq 7$. If C is a curve over a number field k, then we consequently obtain bounds for $\dim_{\mathbb{F}_2} \mathrm{Pic}(C)[2]$ whenever C has good reduction at a prime of small (odd) norm. Thus, when k is a number field, Theorem 1.12 leads to improvements of the inequalities (1) and (11) under suitable hypotheses. Let $\chi = 1 - g(S) + p_g$, where p_g is the geometric genus of the surface $\mathcal{E}$. Then (still assuming $\mathrm{char}(k) = 0$) we have the well-known inequalities [Shi92]

$$2\chi + 2 - 2g(S) \leq \deg(\mathfrak{f}_E) \leq 12\chi.$$

In particular, in terms of the invariant χ, the bound (11) yields another well-known inequality for the rank when $\mathrm{char}(k) = 0$:

$$\mathrm{rk}_{\mathbb{Z}}\, E(k(S)) \leq 10\chi + 2g(S) - 2. \tag{12}$$

As a sample application, under suitable good reduction hypotheses, in Section 2.3 we prove the following asymptotic improvement to (12) over the rational numbers.

Theorem 1.13. *Let E be an elliptic curve over $\mathbb{Q}(S)$ and suppose that $E(\overline{\mathbb{Q}}(S))[2] = 0$. Let C be the smooth compactification of $\mathcal{E}[2] \setminus \{0\}$.*

1) If C has good reduction at 3, then

$$\mathrm{rk}_{\mathbb{Z}}\, E(\mathbb{Q}(S)) \leq 6(\log_2 3)\chi + 3(\log_2 3)g(S) - (\log_2 3 - 1)\sum_{v \in \overline{\Sigma}} \varepsilon_v - \log_2 3 - 1, \tag{13}$$

where the ε_v are defined in Lemma 2.9.

2) If $\mathbb{Q}(S) = \mathbb{Q}(t)$ and C has good reduction at $p \in \{3,5\}$, then

$$\mathrm{rk}_{\mathbb{Z}}\, E(\mathbb{Q}(t)) \leq 4(\log_2 p)\chi + O(1). \tag{14}$$

Remark 1.14. If $E(\overline{\mathbb{Q}}(S))[2] \neq 0$, then Cox [Cox82] proved the better (geometric) bound:

$$\mathrm{rk}_{\mathbb{Z}}\, E(\overline{\mathbb{Q}}(S)) \leq 6\chi + 2g(S) - 2.$$

Remark 1.15. The numerical expansions of the coefficients of χ in Theorem 1.13 are:

$$6(\log_2 3) = 9.509775\cdots$$
$$4(\log_2 3) = 6.339850\cdots$$
$$4(\log_2 5) = 9.287712\cdots .$$

If E is an elliptic curve defined over $\mathbb{Q}(t)$, there is a strategy which allows one, in specific cases, to improve on Lefschetz's bound (11) over $\overline{\mathbb{Q}}(t)$. One picks a suitable prime p of good reduction for the surface $\mathcal{E}$, and one computes the characteristic polynomial of the Frobenius acting on the second ℓ-adic cohomology group of the reduced surface over $\overline{\mathbb{F}}_p$. The details of this approach are explained in [vL07, §6] and [Klo07, §4]. Obviously, one may replace $\mathbb{Q}$ by a number field k. Nevertheless, this technique is not "arithmetic", in the sense that the bound it provides is valid over $\overline{\mathbb{Q}}$.

The question of refining Lefschetz's bound over $\mathbb{Q}$, and more generally over number fields, has been addressed previously by various authors, see the discussion in [SS10, §13.12]. In this respect, to our knowledge, only specific elliptic surfaces (e.g., K3 surfaces) have been studied so far. So, it seems to us that Theorem 1.1 is the first general result which provides an upper bound of an "arithmetic nature" on the rank of elliptic curves over function fields.

We end with a speculative remark on using our results to prove statements towards Silverman's conjectural analogue of (2) when the base field k is a number field instead of a finite field.

Remark 1.16. Silverman [Sil04, Conjecture 4] has conjectured that if k is a number field and E is a non-isotrivial elliptic curve over $k(S)$, then

$$\mathrm{rk}_{\mathbb{Z}}\, E(k(S)) \ll \frac{\deg(\mathfrak{f}_E)}{\log\deg(\mathfrak{f}_E)}, \tag{15}$$

where the implied constant depends only on k and S (in fact, Silverman states a more precise conjecture).

To approach (15) using Theorem 1.1, one needs strong bounds on the rank of p-torsion in $\mathrm{Pic}(C)$. A possible argument for the existence of such bounds is as follows. Let p be a prime and d a positive integer. Brumer and Silverman [BS96] have raised the question of the existence of a constant $c_{p,d}$ such that for every number field $k/\mathbb{Q}$ of degree d,

$$\dim_{\mathbb{F}_p} \mathrm{Cl}(k)[p] \leq c_{p,d}\frac{\log|\operatorname{Disc} k|}{\log\log|\operatorname{Disc} k|}, \tag{16}$$

where $\mathrm{Cl}(k)$ is the ideal class group of k, and $\operatorname{Disc} k$ is the discriminant of k.

Let us fix a finite field $\mathbb{F}_q$. Curves of genus g and gonality d over $\mathbb{F}_q$ are analogous to number fields of degree d over $\mathbb{Q}$ with discriminant (roughly) q^{2g}. Thus, a function field analogue of (16) might assert the existence of a constant $c_{p,d,q}$ such that

$$\dim_{\mathbb{F}_p} \mathrm{Pic}(C)[p] \leq c_{p,d,q}\frac{g}{\log 2g}, \tag{17}$$

where C is any curve over $\mathbb{F}_q$ of positive genus g admitting a morphism of degree d to $\mathbb{P}^1$. When $p \mid d$, the example of hyperelliptic[1] (or more generally superelliptic) curves shows that (17) cannot

[1]More precisely, by considering an equation $y^2 = f(x)$ where $f \in \mathbb{Q}[x]$ splits as a product of $2g+1$ distinct linear factors, one obtains a hyperelliptic curve C over $\mathbb{Q}$ for which $\dim_{\mathbb{F}_2} \mathrm{Pic}(C)[2] = 2g$.

be extended from finite fields to number fields k. However, if $p \nmid d$, it seems possible that (17) may continue to hold when k is a number field.

Now let k be a number field and let E and C be as in Theorem 1.1 (for the prime p). We have a natural morphism $C \to S$ of degree $p^2 - 1$, which is unramified outside of the set of places of bad reduction Σ. We can bound the degree of the ramification divisor by $(p^2-2)\deg(\mathfrak{f}_E)$. Assume additionally that not more than $\frac{\deg(\mathfrak{f}_E)}{\log\deg(\mathfrak{f}_E)}$ Tamagawa numbers are divisible by p. Then assuming that (17) holds for number fields when $p \nmid d$ (note that p and p^2-1 are coprime), Theorem 1.1 immediately implies that

$$\mathrm{rk}_{\mathbb{Z}}\, E(k(S)) \ll \frac{\deg(\mathfrak{f}_E)}{\log\deg(\mathfrak{f}_E)},$$

where the implied constant depends on k, S, and also p. Thus, we would obtain Silverman's conjecture for various large families of elliptic curves (one family for each fixed prime p).

2 Proofs

2.1 Proof of Theorem 1.1

We denote by $\mathcal{E}^0$ the open subgroup of $\mathcal{E}$ whose fiber at each v is $\mathcal{E}_v^0$, and we call it (by abuse of notation) the connected component of $\mathcal{E}$.

By globalizing (3), we obtain an exact sequence for the étale topology on S

$$0 \longrightarrow \mathcal{E}^0 \longrightarrow \mathcal{E} \longrightarrow \Phi := \textstyle\bigoplus_{v\in\Sigma}(i_v)_*\Phi_v \longrightarrow 0,$$

where $i_v : \mathrm{Spec}(k_v) \to S$ denotes the canonical inclusion.

We denote by $\mathcal{E}^{p\Phi}$ the open subgroup scheme of $\mathcal{E}$ which is the inverse image of $p\Phi$ by the quotient map above, so that we have an exact sequence for the étale topology on S

$$0 \longrightarrow \mathcal{E}^{p\Phi} \longrightarrow \mathcal{E} \longrightarrow \Phi/p\Phi \longrightarrow 0.$$

Applying global sections to this sequence, we obtain an exact sequence

$$0 \longrightarrow \mathcal{E}^{p\Phi}(S) \longrightarrow \mathcal{E}(S) \longrightarrow H^0(S, \Phi/p\Phi).$$

Since the group $p\mathcal{E}(S)$ is a subgroup of $\mathcal{E}^{p\Phi}(S)$, if we mod out the first two groups by $p\mathcal{E}(S)$ we obtain another exact sequence

$$0 \longrightarrow \mathcal{E}^{p\Phi}(S)/p\mathcal{E}(S) \longrightarrow \mathcal{E}(S)/p\mathcal{E}(S) \longrightarrow H^0(S, \Phi/p\Phi). \tag{18}$$

Before we proceed with the proof of Theorem 1.1, we shall prove a few lemmas.

Lemma 2.1. *Let $v \in \Sigma$ be a place of bad reduction for $\mathcal{E}$.*

1) If $p \geq 3$, then

$$\dim_{\mathbb{F}_p} H^0(k_v, \Phi_v[p]) = \dim_{\mathbb{F}_p} H^0(k_v, \Phi_v/p\Phi_v) = \begin{cases} 1 & \text{if } p \mid c_v \\ 0 & \text{otherwise.} \end{cases}$$

2) If $p = 2$, then

$$\dim_{\mathbb{F}_2} H^0(k_v, \Phi_v[2]) = \dim_{\mathbb{F}_2} H^0(k_v, \Phi_v/2\Phi_v) = \begin{cases} 2 & \text{if reduction type } \mathrm{I}_{2n}^* \text{ for some } n \geq 0 \\ 1 & \text{if } 2 \mid c_v, \text{ other reduction type} \\ 0 & \text{otherwise.} \end{cases}$$

Proof. It follows from the explicit description of the Néron model of an elliptic curve (see [Liu02, §10.2, Remark 2.24] or [Sil94, Chap. IV, Table 4.1]) that, if $p \geq 3$, or if $p = 2$ and the reduction type of $\mathcal{E}$ at v is not I_{2n}^* for some $n \geq 0$, then the p-primary component of $\Phi_v(\overline{k_v})$ is cyclic. In this situation, it follows from basic cohomology that the following conditions are equivalent:

1. the Galois module $\Phi_v/p\Phi_v$ is either trivial, or else a non-constant Galois module over k_v;
2. $H^0(k_v, \Phi_v/p\Phi_v) = 0$;
3. $p \nmid c_v = \#\Phi_v(k_v)$.

This proves the lemma in all cases except when $p = 2$ and the reduction type is I_{2n}^* for some $n \geq 0$. In this case, Φ_v is isomorphic to the constant k_v-group scheme $(\mathbb{Z}/2\mathbb{Z})^2$, hence the result. □

Lemma 2.2. *1) If $p \geq 3$, we have*

$$\dim_{\mathbb{F}_p} \mathcal{E}^{p\Phi}(S)/p\mathcal{E}(S) \geq \mathrm{rk}_{\mathbb{Z}}\, E(k(S)) - \#\{v \in \Sigma, p \mid c_v\}.$$

2) If $p = 2$, we have

$$\begin{aligned} \dim_{\mathbb{F}_2} \mathcal{E}^{2\Phi}(S)/2\mathcal{E}(S) \geq \mathrm{rk}_{\mathbb{Z}}\, E(k(S)) &- \#\{v \in \Sigma, 2 \mid c_v\} \\ &- \#\{v \in \Sigma, \text{the red. type of } \mathcal{E} \text{ at } v \text{ is } \mathrm{I}_{2n}^* \text{ for some } n \geq 0\}. \end{aligned}$$

Proof. It follows from the exact sequence (18) that

$$\dim_{\mathbb{F}_p} \mathcal{E}^{p\Phi}(S)/p\mathcal{E}(S) \geq \dim_{\mathbb{F}_p} \mathcal{E}(S)/p\mathcal{E}(S) - \dim_{\mathbb{F}_p} H^0(S, \Phi/p\Phi).$$

By the universal property of the Néron model, $\mathcal{E}(S)/p\mathcal{E}(S) = E(k(S))/pE(k(S))$. Because $E[p]$ satisfies (i)–(iii), $E(k(S))$ has no nontrivial p-torsion, hence

$$\dim_{\mathbb{F}_p} \mathcal{E}(S)/p\mathcal{E}(S) = \mathrm{rk}_{\mathbb{Z}}\, E(k(S)).$$

On the other hand,

$$H^0(S, \Phi/p\Phi) = \bigoplus_{v \in \Sigma} H^0(k_v, \Phi_v/p\Phi_v),$$

and Lemma 2.1 allows one to compute the $\mathbb{F}_p$-dimension of each of these groups. □

Let $j : \eta = \mathrm{Spec}(k(S)) \to S$ be the inclusion of the generic point of S. Let us recall that, if H is a $k(S)$-group scheme, then by definition the Néron model of H is a smooth separated S-group scheme of finite type which represents the sheaf j_*H on the smooth site of S. Therefore, we have an exact sequence

$$0 \longrightarrow H^1(S, j_*H) \longrightarrow H^1(k(S), H) \longrightarrow H^0(S, R^1 j_* H) \longrightarrow \cdots .$$

In particular, if G is a Néron model of its generic fiber, then the restriction to the generic fiber induces an injection

$$H^1(S, G) \hookrightarrow H^1(k(S), G) \tag{19}$$

Remark 2.3. The image of (19) can be described as the set of Galois cohomology classes which are unramified everywhere. We shall not make use of this description, but it may be helpful to keep in mind.

Lemma 2.4. *1) The group scheme $\mathcal{E}[p]$ is the Néron model of $E[p]$.*

2) If G is a finite étale S-group scheme, then G is the Néron model of its generic fiber.

Proof. 1) Let us note that, p being invertible on S, the S-group scheme $\mathcal{E}[p]$ is étale, and is a closed subgroup scheme of $\mathcal{E}$. Therefore, $\mathcal{E}[p]$ is the Néron model of $E[p]$, according to [BLR90, §7.1, Corollary 6].

2) By hypothesis, G is a smooth and separated S-group scheme. Moreover, the map $G \to S$ is finite, hence proper. It follows from [BLR90, §7.1, Theorem 1] that G is the Néron model of its generic fiber. □

Let $\mathrm{Res}_{k(C)/k(S)}\,\mu_p$ denote the Weil restriction of μ_p, which, by definition, satisfies

$$(\mathrm{Res}_{k(C)/k(S)}\,\mu_p)(L) = \mu_p(L \otimes k(C))$$

for any $k(S)$-algebra L. Let T denote the generic point of C, which is also the generic non-zero p-torsion point of E. Then the Weil pairing e_p induces a morphism of finite étale $k(S)$-group schemes (equivalently of Galois modules over $k(S)$)

$$\begin{aligned} w : E[p] &\longrightarrow \mathrm{Res}_{k(C)/k(S)}\,\mu_p \\ P &\longmapsto e_p(P, T). \end{aligned}$$

According to Lemma 2.4, $\mathcal{E}[p]$ and μ_p are Néron models of their generic fibers. It follows from [BLR90, §7.6, Proposition 6] that the same holds for $\mathrm{Res}_{C/S}\,\mu_p$. We denote by

$$\underline{w} : \mathcal{E}[p] \longrightarrow \mathrm{Res}_{C/S}\,\mu_p$$

the map induced by w on these Néron models.

Lemma 2.5. *The map $\underline{w}$ induces on étale cohomology an injective map*

$$h^1\underline{w} : H^1(S, \mathcal{E}[p]) \longrightarrow H^1(S, \mathrm{Res}_{C/S}\,\mu_p) = H^1(C, \mu_p),$$

whose image is contained in the kernel of the norm map

$$N_{C/S} : H^1(C, \mu_p) \longrightarrow H^1(S, \mu_p).$$

When $p \geq 3$, the image of $h^1\underline{w}$ is contained in the kernel of the norm map

$$N_{C/C^+} : H^1(C, \mu_p) \longrightarrow H^1(C^+, \mu_p).$$

Proof. It has been proved by Djabri, Schaefer and Smart [DSS00, Prop. 7 and Prop. 8] that the map w induces on Galois cohomology an injective map

$$h^1 w : H^1(k(S), E[p]) \longrightarrow H^1(k(S), \mathrm{Res}_{k(C)/k(S)}\,\mu_p) = H^1(k(C), \mu_p).$$

Let us stress here the fact that the authors cited above work over a number field or the completion of a number field. Nevertheless, their arguments are purely Galois-theoretical and extend without any change to our function field setting.

Now, consider the following commutative diagram

$$\begin{array}{ccc} H^1(S,\mathcal{E}[p]) & \xrightarrow{h^1\underline{w}} & H^1(C,\mu_p) \\ \downarrow & & \downarrow \\ H^1(k(S),E[p]) & \xrightarrow{h^1 w} & H^1(k(C),\mu_p) \end{array}$$

in which the vertical maps are injective, according to (19). Thus, one deduces the injectivity of $h^1\underline{w}$ from that of $h^1 w$. Then, we note that the composition of the maps

$$E[p] \xrightarrow{w} \mathrm{Res}_{k(C)/k(S)}\,\mu_p \xrightarrow{N_{k(C)/k(S)}} \mu_p$$

is zero, because the sum of all non-zero elements of $E[p]$ is zero. It follows that the composition of the induced maps on the Néron models is also zero, hence the same holds for the maps induced on cohomology. Finally, when $p \geq 3$, the map $P \mapsto -P$ is a nontrivial involution of C, with quotient C^+, and the composition of the maps

$$E[p] \xrightarrow{w} \mathrm{Res}_{k(C)/k(S)}\,\mu_p \xrightarrow{N_{k(C)/k(C^+)}} \mathrm{Res}_{k(C^+)/k(S)}\,\mu_p$$

is zero, because $e_p(P,T)\cdot e_p(-P,T) = 1$. This proves the last part of the statement. □

Proof of Theorem 1.1. Let us note that the map $[p] : \mathcal{E}_v^0 \to \mathcal{E}_v^0$ is surjective for the étale topology on k_v (multiplication by p on a smooth connected group scheme in characteristic $\neq p$ is étale surjective). It follows that multiplication by p on $\mathcal{E}$ induces an exact sequence for the étale topology on S

$$0 \longrightarrow \mathcal{E}[p] \longrightarrow \mathcal{E} \xrightarrow{[p]} \mathcal{E}^{p\Phi} \longrightarrow 0.$$

Applying cohomology to this sequence, we obtain an injective map

$$\delta : \mathcal{E}^{p\Phi}(S)/p\mathcal{E}(S) \longrightarrow H^1(S,\mathcal{E}[p]).$$

According to Lemma 2.5, the target group can be embedded in the kernel of the norm map

$$N_{C/S} : H^1(C,\mu_p) \longrightarrow H^1(S,\mu_p).$$

Let us determine the size of this kernel. The prime p being invertible in k, multiplication by p on $\mathbf{G}_\mathrm{m}$ is surjective for the étale topology on k-schemes. Moreover, S and C being geometrically integral projective curves over k, we have $\mathbf{G}_\mathrm{m}(S) = \mathbf{G}_\mathrm{m}(C) = k^\times$. Therefore, Kummer theory over S and C yields a commutative diagram with exact rows

$$\begin{array}{ccccccccc} 0 & \longrightarrow & k^\times/(k^\times)^p & \longrightarrow & H^1(C,\mu_p) & \xrightarrow{\kappa} & \mathrm{Pic}(C)[p] & \longrightarrow & 0 \\ & & \| & & \downarrow{\scriptstyle N_{C/S}} & & \downarrow{\scriptstyle N_{C/S}} & & \\ 0 & \longrightarrow & k^\times/(k^\times)^p & \longrightarrow & H^1(S,\mu_p) & \longrightarrow & \mathrm{Pic}(S)[p] & \longrightarrow & 0 \end{array}$$

where the vertical maps are the norm maps. We deduce, by the snake lemma, that the two norm maps $N_{C/S}$ above have the same kernel. In other words, if we compose the natural map $\kappa : H^1(C,\mu_p) \to \mathrm{Pic}(C)[p]$ with $h^1\underline{w}\circ\delta$, we obtain an injective group morphism

$$\mathcal{E}^{p\Phi}(S)/p\mathcal{E}(S) \longrightarrow \ker\big(N_{C/S} : \mathrm{Pic}(C)[p] \to \mathrm{Pic}(S)[p]\big)$$

which proves (6) when $p = 2$. When $p \geq 3$, the last statement of Lemma 2.5 allows us to prove (4) with a similar argument. When $p = 2$, $C \to S$ has degree 3, hence $N_{C/S}$ is surjective on 2-torsion, from which we deduce that

$$\dim_{\mathbb{F}_2} \ker\left(N_{C/S} : \mathrm{Pic}(C)[2] \to \mathrm{Pic}(S)[2]\right) = \dim_{\mathbb{F}_2} \mathrm{Pic}(C)[2] - \dim_{\mathbb{F}_2} \mathrm{Pic}(S)[2].$$

Similarly, when $p \geq 3$ the map $C \to C^+$ has degree 2 and we have

$$\dim_{\mathbb{F}_p} \ker\left(N_{C/C^+} : \mathrm{Pic}(C)[p] \to \mathrm{Pic}(C^+)[p]\right) = \dim_{\mathbb{F}_p} \mathrm{Pic}(C)[p] - \dim_{\mathbb{F}_p} \mathrm{Pic}(C^+)[p]$$

The statements (7) and (5) follow by combining this with Lemma 2.2. □

Remark 2.6. In [CTSSD98, §4.2], the authors define a geometric Selmer group, denoted $\mathfrak{S}(\mathcal{E}, p)$, which, according to Prop. 4.2.2 of *loc. cit.*, fits into an exact sequence

$$0 \longrightarrow H^1(S, \mathcal{E}[p]) \longrightarrow \mathfrak{S}(\mathcal{E}, p) \longrightarrow H^0(S, \Phi/p\Phi).$$

Our proof of Theorem 1.1 relies on a) bounding the size of $H^1(S, \mathcal{E}[p])$ in terms of the curves S and C, and b) computing the exact size of $H^0(S, \Phi/p\Phi)$. This yields an upper bound on the size of the geometric Selmer group.

Remark 2.7. It is important to require that C and S are both geometrically integral and projective. The fact that $\mathbf{G}_{\mathrm{m}}(S) = \mathbf{G}_{\mathrm{m}}(C)$ is a crucial argument in the proof, which implies that the units do not contribute to the kernel of the norm. Recall from Remark 1.5 that, when the full p-torsion is defined over $k(S)$, it may happen that the geometric analogue of the Selmer group is infinite.

Remark 2.8. In the framework of p-descent over a number field, it was proved by Dokchitser [Dok00, Cor. 6.5.2], under the same assumption (the Galois action on $E[p]$ is transitive), that the image of $h^1\underline{w}$ is contained in the kernel of the norm $N_{k(C)/K}$ for any proper subfield $K \subset k(C)$. So one can improve the statement of Theorem 1.1, 1) as follows: if $p \geq 3$, we have an injective morphism

$$\mathcal{E}^{p\Phi}(S)/p\mathcal{E}(S) \longrightarrow \bigcap_{C \to C'} \ker\left(N_{C/C'} : \mathrm{Pic}(C)[p] \to \mathrm{Pic}(C')[p]\right)$$

where $C \to C'$ runs through all proper subcovers of $C \to S$. In fact, for $p = 3$ this is not an improvement since every proper subcover of $C \to S$ factors through $C \to C^+$ (see the proof of Theorem 1.7).

2.2 Proof of Theorem 1.6

Let us recall that, if $f : X \to Y$ is a finite flat, tamely ramified map of smooth k-curves, then the ramification divisor of f is given by $\sum_x (e_x - 1) \cdot x$, where x runs through closed points of X, and e_x denotes the ramification index of f at x. All finite maps we shall consider here are tamely ramified.

By assumption, $\mathrm{char}(k) \neq 2, 3$ and $\mathcal{E}$ does not have a nontrivial 2-torsion section over S. In order to prove (9), we may assume that k is algebraically closed, which we do until further notice.

Let C be the smooth compactification of $\mathcal{E}[2] \setminus \{0\}$. We note that $C \to S$ is tamely ramified, because the Galois closure of its generic fiber has Galois group $\mathbb{Z}/3\mathbb{Z}$ or $\mathfrak{S}_3$, whose order is coprime to the characteristic of k.

We shall first compute the degree of the ramification divisor of $C \to S$.

Lemma 2.9. *Let $R \subset C$ be the ramification divisor of the natural cubic map $C \to S$. Then the degree of R is given by the formula*

$$\deg(R) = \deg(\mathfrak{f}_E) - \sum_{v \in \Sigma} \varepsilon_v,$$

where

$$\varepsilon_v = \begin{cases} 2 & \text{if reduction type } \mathrm{I}_{2n}^* \text{ for some } n \geq 0 \\ 1 & \text{if } 2 \mid c_v, \text{ other reduction type} \\ 0 & \text{otherwise.} \end{cases}$$

Remark 2.10. Note that $\sum_{v \in \Sigma} \varepsilon_v = \dim_{\mathbb{F}_2} H^0(S, \Phi[2])$.

Proof. By construction, $\mathcal{E}[2] \setminus \{0\}$ is an open subscheme of C. In fact, we claim that

$$C \setminus R = \mathcal{E}[2] \setminus \{0\}. \tag{20}$$

Let us prove the two inclusions: the right hand side is a subscheme of the left hand side, because $\mathcal{E}[2] \setminus \{0\} \to S$ is étale (the assumption that $\mathrm{char}(k) \neq 2$ is important here). The other inclusion follows from the universal property of the Néron model: $C \setminus R \to S$ is a smooth separated scheme over S, hence the inclusion of the generic fiber $E[2] \setminus \{0\} \hookrightarrow E$ can be extended to a map $C \setminus R \to \mathcal{E}$, which takes values in $\mathcal{E}[2] \setminus \{0\}$.

If $v \in \Sigma$ is a place of bad reduction, we denote by R_v the fiber of R above v. The map $C \to S$ being finite flat of degree 3, it follows from (20) that

$$\deg(R_v) = \begin{cases} 0 & \text{if } \#\mathcal{E}_v[2] = 4 \\ 1 & \text{if } \#\mathcal{E}_v[2] = 2 \\ 2 & \text{if } \#\mathcal{E}_v[2] = 1, \end{cases} \tag{21}$$

where $\#\mathcal{E}_v[2]$ denotes the number of k-points of $\mathcal{E}_v[2]$, or equivalently, the rank of $\mathcal{E}_v[2]$ as a finite k-group scheme (remember that k is algebraically closed here).

On the other hand, the map $[2] : \mathcal{E}_v^0 \to \mathcal{E}_v^0$ being surjective for the étale topology, we deduce from (3) a short exact sequence of étale sheaves

$$0 \longrightarrow \mathcal{E}_v^0[2] \longrightarrow \mathcal{E}_v[2] \longrightarrow \Phi_v[2] \longrightarrow 0.$$

It follows from the explicit description of the bad fibers of the Néron model of an elliptic curve [Sil94, Chap. IV, Table 4.1] that

$$\#\mathcal{E}_v[2] = \begin{cases} 4 & \text{if reduction type } \mathrm{I}_{2n}^* \text{ for some } n \geq 0 \\ 4 & \text{if reduction type } \mathrm{I}_{2n} \text{ for some } n \geq 0 \\ 2 & \text{if reduction type } \mathrm{I}_{2n+1} \text{ for some } n \geq 0 \\ 2 & \text{if reduction type III, III}^* \text{ or } \mathrm{I}_{2n+1}^* \text{ for some } n \geq 0 \\ 1 & \text{if reduction type II, II}^*, \text{ IV or IV}^*. \end{cases}$$

For example, in the case of reduction I_{2n}^*, the group Φ_v is isomorphic to $(\mathbb{Z}/2\mathbb{Z})^2$, hence $\mathcal{E}_v[2]$ has four points. In the case of multiplicative reduction I_{2n+1}, we have $\Phi_v \simeq \mathbb{Z}/(2n+1)$ and $\mathcal{E}_v^0 \simeq \mathbf{G}_{\mathrm{m}}$, hence $\mathcal{E}_v[2] = \mathcal{E}_v^0[2] = \mu_2$, which has two points.

Using (21) one checks that, in each case listed above,

$$\deg(R_v) = f_v - \varepsilon_v,$$

where f_v is the exponent of the conductor at v. The result follows immediately by summing up over all $v \in \Sigma$. □

Proof of Theorem 1.6. Applying the Riemann-Hurwitz formula to the cubic map $C \to S$, we find that

$$2g(C) - 2 = 3(2g(S) - 2) + \deg(R),$$

where $R \subset C$ is the ramification divisor of $C \to S$. Equivalently,

$$2g(C) - 2g(S) = 4g(S) - 4 + \deg(R).$$

Replacing $\deg(R)$ by its value computed in Lemma 2.9 yields

$$2g(C) - 2g(S) + \sum_{v \in \Sigma} \varepsilon_v = 4g(S) - 4 + \deg(\mathfrak{f}_E).$$

But, by definition of ε_v, we have

$$\sum_{v \in \Sigma} \varepsilon_v = \#\{v \in \Sigma, 2 \mid c_v\} + \#\{v \in \Sigma, \text{the red. type of } \mathcal{E} \text{ at } v \text{ is } \mathrm{I}_{2n}^* \text{ for some } n \geq 0\}$$

which proves (9).

Let us now prove the last statement of Theorem 1.6. Keeping for the moment the assumption that k is algebraically closed, we have

$$\dim_{\mathbb{F}_2} \mathrm{Pic}(C)[2] = 2g(C)$$

and similarly for S. Therefore, the relation (9) means that (7) is equivalent to the geometric rank bound. Dropping now the assumption that k is algebraically closed, it follows that the bound (7) is a refinement of the geometric rank bound. □

2.3 Proof of Theorem 1.13

We keep the notation of the previous section.

Proof of Theorem 1.13. We first prove the bound (13). Let $\overline{\Sigma}$ be the set of places of bad reduction of $\mathcal{E}_{\overline{\mathbb{Q}}}$ over $S_{\overline{\mathbb{Q}}}$. From the proof of Theorem 1.6, we have

$$g(C) = 3g(S) - 2 + \frac{1}{2}\left(\deg(\mathfrak{f}_E) - \sum_{v \in \overline{\Sigma}} \varepsilon_v\right).$$

Since C has good reduction at 3, the reduction map modulo 3 is injective on 2-torsion, and Theorem 1.12 implies that

$$\begin{aligned}\dim_{\mathbb{F}_2} \mathrm{Pic}(C)[2] &\leq \log_2\left(\frac{3^{g(C)+1} - 1}{2}\right) < (g(C)+1)\log_2 3 - 1 \\ &< (\log_2 3)\left(3g(S) - 1 + \frac{1}{2}\left(\deg(\mathfrak{f}_E) - \sum_{v \in \overline{\Sigma}} \varepsilon_v\right)\right) - 1.\end{aligned}$$

For $v \in \overline{\Sigma}$, let m_v denote the number of irreducible components in the fiber above v. Then it follows easily from the definition of ε_v and a known formula for 12χ [Shi92] that

$$\deg(\mathfrak{f}_E) + \sum_{v \in \overline{\Sigma}} \varepsilon_v \leq \deg(\mathfrak{f}_E) + \sum_{v \in \overline{\Sigma}} (m_v - 1) = 12\chi,$$

and this inequality is sharp only if $\varepsilon_v = m_v - 1$ for each bad v.

Let us now consider the inequality (7), in which we neglect the negative term $-\dim_{\mathbb{F}_2} \mathrm{Pic}(S)[2]$, and observe that $\sum_{v \in \Sigma} \varepsilon_v \leq \sum_{v \in \overline{\Sigma}} \varepsilon_v$, which yields:

$$\begin{aligned}
\mathrm{rk}_{\mathbb{Z}}\, E(\mathbb{Q}(S)) &\leq \dim_{\mathbb{F}_2} \mathrm{Pic}(C)[2] + \sum_{v \in \overline{\Sigma}} \varepsilon_v \\
&\leq (\log_2 3) \left(3g(S) - 1 + \frac{1}{2} \left(\deg(\mathfrak{f}_E) - \sum_{v \in \overline{\Sigma}} \varepsilon_v \right) \right) - 1 + \sum_{v \in \overline{\Sigma}} \varepsilon_v \\
&= 3(\log_2 3) g(S) + \frac{\log_2 3}{2} \deg(\mathfrak{f}_E) + \left(1 - \frac{\log_2 3}{2} \right) \sum_{v \in \overline{\Sigma}} \varepsilon_v - \log_2 3 - 1 \\
&= 3(\log_2 3) g(S) + \frac{\log_2 3}{2} \left(\deg(\mathfrak{f}_E) + \sum_{v \in \overline{\Sigma}} \varepsilon_v \right) - (\log_2 3 - 1) \sum_{v \in \overline{\Sigma}} \varepsilon_v - \log_2 3 - 1 \\
&\leq 3(\log_2 3) g(S) + 6(\log_2 3)\chi - (\log_2 3 - 1) \sum_{v \in \overline{\Sigma}} \varepsilon_v - \log_2 3 - 1.
\end{aligned}$$

For the bound (14), suppose that C has good reduction at $p \in \{3, 5\}$. Since $S = \mathbb{P}^1$, the curve C is trigonal. It is well-known that the gonality of C can only decrease after reduction modulo a good prime, and so applying Theorem 1.12 with $n = 3$ yields

$$\dim_{\mathbb{F}_2} \mathrm{Pic}(C)[2] \leq \frac{2}{3} g(C) \log_2 p + O(1).$$

Now nearly the exact same calculation as above gives

$$\mathrm{rk}_{\mathbb{Z}}\, E(\mathbb{Q}(t)) \leq 4(\log_2 p)\chi + O(1).$$

□

2.4 Proof of Theorem 1.7

By assumption, $\mathrm{char}(k) \neq 2, 3$ and the prime 3 satisfies assumptions (i)–(iii). In order to prove (10), we may assume that k is algebraically closed, which we do until further notice.

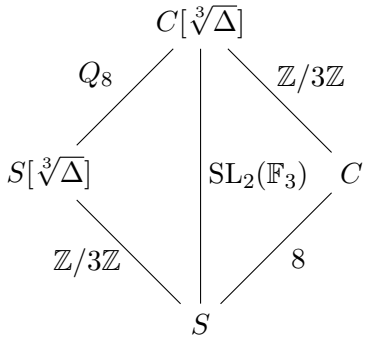
Let C be the smooth compactification of $\mathcal{E}[3] \setminus \{0\}$, and let C^+ be the quotient of C by the involution $P \mapsto -P$.

The composite morphism $\mathrm{Gal}(k(S)(E[3])/k(S)) \to \mathrm{GL}_2(\mathbb{F}_3) \xrightarrow{\det} \mathbb{F}_3^*$ is the cyclotomic character, which is trivial since k is algebraically closed. Therefore, $\mathrm{Gal}(k(S)(E[3])/k(S))$ is a subgroup of $\mathrm{SL}_2(\mathbb{F}_3)$ which, by assumption (i)–(iii), acts transitively on $\mathbb{F}_3^2 \setminus \{0\}$. It follows that $\mathrm{Gal}(k(S)(E[3])/k(S))$ is equal to $\mathrm{SL}_2(\mathbb{F}_3)$ or to its 2-Sylow subgroup the quaternionic group Q_8, which is normal in $\mathrm{SL}_2(\mathbb{F}_3)$, with quotient group cyclic of order three.

In fact, it is easy to check [Ade01, Prop. 5.4.3] that the subfield of $k(S)(E[3])$ fixed by Q_8 is $k(S)(\sqrt[3]{\Delta})$, where $\Delta \in k(S)$ is the discriminant of E. Therefore, $\mathrm{Gal}(k(S)(E[3])/k(S)) = Q_8$ if

and only if Δ is a cube in $k(S)$. If not, then $k(S)(E[3])$ is the compositum of $k(C)$ and $k(S)(\sqrt[3]{\Delta})$ over $k(S)$. Switching to geometry, if we denote by $S[\sqrt[3]{\Delta}]$ (resp. $C[\sqrt[3]{\Delta}]$) the curve with function field $k(S)(\sqrt[3]{\Delta})$ (resp. $k(S)(E[3])$), we have the following cartesian square of connected covers of curves, in which Galois covers are labelled with their corresponding Galois group.

Let us underline the fact that, in any case, $C[\sqrt[3]{\Delta}] \to S$ is tamely ramified, since it is Galois of degree 24 (resp. 8 in the quaternionic case), which is coprime to the characteristic of k. Therefore, the inertia groups of its ramified points are cyclic subgroups of $\mathrm{SL}_2(\mathbb{F}_3)$, hence have order 2, 3, 4 or 6 (resp. 2 or 4 in the quaternionic case).



Let $R \subset C$ be the ramification divisor of $C \to S$. If $v \in S$ is a closed point, we denote by C_v (resp. by R_v) the fiber of C (resp. R) at v. As previously (20), we note that

$$C \setminus R = \mathcal{E}[3] \setminus \{0\}.$$

Similarly, we denote by $R^+ \subset C^+$ the ramification divisor of $C^+ \to S$. We note that Q_8 has a unique subgroup of order two, which means that $P \mapsto -P$ is the unique automorphism of order 2 of $C[\sqrt[3]{\Delta}] \to S$. The same holds for $C \to S$ (which is not Galois in general, but over which the automorphism $P \mapsto -P$ is still defined). It then follows from the diagram above that, given a point $P \in C$ with ramification index e_P (relative to S), its image by the map $C \to C^+$ has ramification index $e_P/2$ if e_P is even, and e_P if e_P is odd.

We shall now proceed to a case-by-case description of R_v and R_v^+ depending on the reduction type of $\mathcal{E}$ at v.

1. Reduction type I_n, $3 \mid n$. In this case, $\#\mathcal{E}_v[3] = 9$ hence R_v and R_v^+ are both zero.

2. Reduction type I_n, $3 \nmid n$. In this case, $\#\mathcal{E}_v[3] = 3$ hence C_v has exactly two unramified points P_1 and P_2. Moreover, $v(\Delta) = n$, hence Δ is not a cube in $k(S)$ and, after performing the totally ramified base change $S[\sqrt[3]{\Delta}] \to S$, E has reduction type I_{3n}, in particular $C[\sqrt[3]{\Delta}] \to S[\sqrt[3]{\Delta}]$ is unramified above v (previous case). It follows that the ramified points of $C \to S$ have ramification index 3, hence $C_v = P_1 + P_2 + 3Q_1 + 3Q_2$ and $C_v^+ = P^+ + 3Q^+$. Therefore, $\deg(R_v) = 4$ and $\deg(R_v^+) = 2$.

3. Reduction type I_n^*, $3 \mid n$. In this case, $\#\mathcal{E}_v[3] = 1$ hence C_v has all its points ramified. Moreover, $v(\Delta) = 6 + n$, hence $S[\sqrt[3]{\Delta}] \to S$ is unramified above v. So without loss of generality we may assume that Δ is a cube in $k(S)$, i.e. $C \to S$ is Galois with group Q_8. On the other hand it is known that, after a quadratic ramified base change, E has reduction type I_{2n}, in which case $C \to S$ is unramified (first case). We deduce that all ramification indexes of $C \to S$ are equal to 2, i.e. $C_v = 2P_1 + 2P_2 + 2P_3 + 2P_4$, and that $C_v^+ = P_1^+ + P_2^+ + P_3^+ + P_4^+$. Therefore, $\deg(R_v) = 4$ and $\deg(R_v^+) = 0$.

4. Reduction type I_n^*, $3 \nmid n$. As in the previous case, C_v has all its points ramified. After performing a quadratic ramified base change, E has reduction type I_{2n}, and we recover the case 2. We conclude that $C_v = 2P + 6Q$ and $C_v^+ = P^+ + 3Q^+$. Therefore, $\deg(R_v) = 6$ and $\deg(R_v^+) = 2$.

5. Reduction type IV or IV*. In this case, $\#\mathcal{E}_v[3] = 3$ hence C_v has exactly two unramified points P_1 and P_2. Moreover, $v(\Delta)$ is 4 or 8, hence Δ is not a cube in $k(S)$ and, after performing the totally ramified base change $S[\sqrt[3]{\Delta}] \to S$, E acquires good reduction, because

the valuation of Δ is multiplied by 3, hence is zero modulo 12. Therefore, $C[\sqrt[3]{\Delta}] \to S[\sqrt[3]{\Delta}]$ is unramified above v. We conclude that the ramification is the same as in 2.

In the remaining cases, the reduction is additive, potentially good, and C_v has all its points ramified. According to Serre-Tate [ST68, Cor. 2], the curve E acquires good reduction exactly when the field of definition of the 3-torsion points becomes unramified. Therefore, the ramification indexes of $C[\sqrt[3]{\Delta}] \to S$ are all equal to the *semistability defect* of E, which is the denominator of $v(\Delta)/12$ since $\mathrm{char}(k) \neq 2, 3$ [Kra90, Prop. 1].

6. Reduction type II or II*. In this case, $C_v = 2P + 6Q$, $\deg(R_v) = 6$ and $\deg(R_v^+) = 2$.

7. Reduction type III or III*. In this case, $C_v = 4P + 4Q$, $\deg(R_v) = 6$ and $\deg(R_v^+) = 2$.

One checks that, in each case listed above,

$$\frac{1}{2}\left(\deg(R_v) - \deg(R_v^+)\right) = f_v - \begin{cases} 1 & \text{if } 3 \mid c_v \\ 0 & \text{otherwise.} \end{cases}$$

Summing up over all $v \in \Sigma$, it follows that

$$\frac{1}{2}\left(\deg(R) - \deg(R^+)\right) = \deg(\mathfrak{f}_E) - \#\{v \in \Sigma, 3 \mid c_v\}. \tag{22}$$

The proof ends by applying the Riemann-Hurwitz formula to the covers $C \to S$ of degree 8, and $C^+ \to S$ of degree 4. Subtracting the two identities and dividing by 2, one obtains

$$g(C) - g(C^+) = 4g(S) - 4 + \frac{1}{2}\left(\deg(R) - \deg(R^+)\right),$$

and (10) follows by combining this with (22).

Let us now prove the last statement of Theorem 1.7. Keeping for the moment the assumption that k is algebraically closed, we have $\dim_{\mathbb{F}_3} \mathrm{Pic}(C)[3] = 2g(C)$, and similarly for C^+. By self-duality of the Jacobian of C, the Weil pairing induces a perfect, symplectic pairing $\mathrm{Pic}(C)[3] \times \mathrm{Pic}(C)[3] \to \mu_3$, which is Galois equivariant. Dropping now the assumption that k is algebraically closed, it follows that in particular, if k does not contain cube roots of unity, then

$$\dim_{\mathbb{F}_3} \mathrm{Pic}(C)[3] \leq g(C)$$

and similarly for C^+. Therefore, the identity (10) implies that, for $p = 3$, the bound (5) is a refinement of the geometric rank bound provided k does not contain cube roots of unity.

References

[Ade01] Clemens Adelmann, *The decomposition of primes in torsion point fields*, Lecture Notes in Mathematics, vol. 1761, Springer-Verlag, Berlin, 2001. MR 1836119

[AM77] Michael Artin and Barry Mazur, *Formal groups arising from algebraic varieties*, Ann. Sci. École Norm. Sup. (4) **10** (1977), no. 1, 87–131. MR 0457458

[BK77] Armand Brumer and Kenneth Kramer, *The rank of elliptic curves*, Duke Math. J. **44** (1977), no. 4, 715–743. MR 457453

[BLR90] Siegfried Bosch, Werner Lütkebohmert, and Michel Raynaud, *Néron models*, Ergebnisse der Mathematik und ihrer Grenzgebiete (3) [Results in Mathematics and Related Areas (3)], vol. 21, Springer-Verlag, Berlin, 1990. MR 1045822

[Bru92] Armand Brumer, *The average rank of elliptic curves. I*, Invent. Math. **109** (1992), no. 3, 445–472. MR 1176198

[BS96] Armand Brumer and Joseph H. Silverman, *The number of elliptic curves over* $\mathbf{Q}$ *with conductor* N, Manuscripta Math. **91** (1996), no. 1, 95–102. MR 1404420

[BST+17] Manjul Bhargava, Arul Shankar, Taniguchi Takashi, Frank Thorne, Jacob Tsimerman, and Yongqiang Zhao, *Bounds on 2-torsion in class groups of number fields and integral points on elliptic curves*, `arXiv:1701.02458 [math.NT]`, 2017.

[Cou09] Jean-Marc Couveignes, *Linearizing torsion classes in the Picard group of algebraic curves over finite fields*, J. Algebra **321** (2009), no. 8, 2085–2118. MR 2501511

[Cox82] David A. Cox, *Mordell-Weil groups of elliptic curves over* $\mathbf{C}(t)$ *with* $p_g = 0$ *or* 1, Duke Math. J. **49** (1982), no. 3, 677–689. MR 672502

[CTSSD98] Jean-Louis Colliot-Thélène, Alexei N. Skorobogatov, and Peter Swinnerton-Dyer, *Hasse principle for pencils of curves of genus one whose Jacobians have rational* 2*-division points*, Invent. Math. **134** (1998), no. 3, 579–650. MR 1660925

[Dok00] Tim Dokchitser, *Deformations of p-divisible groups and p-descent on elliptic curves*, Ph.D. thesis, Universiteit Utrecht, 2000.

[DSS00] Zafer Djabri, Edward F. Schaefer, and Nigel P. Smart, *Computing the p-Selmer group of an elliptic curve*, Trans. Amer. Math. Soc. **352** (2000), no. 12, 5583–5597. MR 1694286

[Ell06] Jordan S. Ellenberg, *Selmer groups and Mordell-Weil groups of elliptic curves over towers of function fields*, Compos. Math. **142** (2006), no. 5, 1215–1230. MR 2264662

[GL19] Jean Gillibert and Aaron Levin, *Elliptic surfaces over* $\mathbb{P}^1$ *and large class groups of number fields*, Int. J. Number Theory (to appear) (2019).

[Igu59] Jun-ichi Igusa, *Fibre systems of Jacobian varieties. III. Fibre systems of elliptic curves*, Amer. J. Math. **81** (1959), 453–476. MR 104669

[Jed16] Tomasz Jedrzejak, *A note on the torsion of the Jacobians of superelliptic curves* $y^q = x^p + a$, Algebra, logic and number theory, Banach Center Publ., vol. 108, Polish Acad. Sci. Inst. Math., Warsaw, 2016, pp. 143–149. MR 3559260

[Klo07] Remke Kloosterman, *Elliptic* $K3$ *surfaces with geometric Mordell-Weil rank 15*, Canad. Math. Bull. **50** (2007), no. 2, 215–226. MR 2317444

[Kra90] Alain Kraus, *Sur le défaut de semi-stabilité des courbes elliptiques à réduction additive*, Manuscripta Math. **69** (1990), no. 4, 353–385. MR 1080288

[Liu02] Qing Liu, *Algebraic geometry and arithmetic curves*, Oxford Graduate Texts in Mathematics, vol. 6, Oxford University Press, Oxford, 2002, Translated from the French by Reinie Erné, Oxford Science Publications.

[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. MR 1104782

[Ray95] Michel Raynaud, *Caractéristique d'Euler-Poincaré d'un faisceau et cohomologie des variétés abéliennes*, Séminaire Bourbaki, Vol. 9, Soc. Math. France, Paris, 1995, pp. Exp. No. 286, 129–147. MR 1608794

[Shi86] Tetsuji Shioda, *An explicit algorithm for computing the Picard number of certain algebraic surfaces*, Amer. J. Math. **108** (1986), no. 2, 415–432. MR 833362

[Shi92] ———, *Some remarks on elliptic curves over function fields*, Astérisque (1992), no. 209, 12, 99–114, Journées Arithmétiques, 1991 (Geneva). MR 1211006

[Sil94] Joseph H. Silverman, *Advanced topics in the arithmetic of elliptic curves*, Graduate Texts in Mathematics, vol. 151, Springer-Verlag, New York, 1994. MR 1312368

[Sil00] ———, *A bound for the Mordell-Weil rank of an elliptic surface after a cyclic base extension*, J. Algebraic Geom. **9** (2000), no. 2, 301–308. MR 1735774

[Sil04] ———, *The rank of elliptic surfaces in unramified abelian towers*, J. Reine Angew. Math. **577** (2004), 153–169. MR 2108217

[SS10] Matthias Schütt and Tetsuji Shioda, *Elliptic surfaces*, Algebraic geometry in East Asia—Seoul 2008, Adv. Stud. Pure Math., vol. 60, Math. Soc. Japan, Tokyo, 2010, pp. 51–160. MR 2732092

[ST68] Jean-Pierre Serre and John Tate, *Good reduction of abelian varieties*, Ann. of Math. (2) **88** (1968), 492–517. MR 236190

[Tat75] John Tate, *Algorithm for determining the type of a singular fiber in an elliptic pencil*, Modular functions of one variable, IV (Proc. Internat. Summer School, Univ. Antwerp, Antwerp, 1972), Springer, Berlin, 1975, pp. 33–52. Lecture Notes in Math., Vol. 476. MR 0393039

[Ulm02] Douglas Ulmer, *Elliptic curves with large rank over function fields*, Ann. of Math. (2) **155** (2002), no. 1, 295–315. MR 1888802

[Ulm04] ———, *Elliptic curves and analogies between number fields and function fields*, Heegner points and Rankin L-series, Math. Sci. Res. Inst. Publ., vol. 49, Cambridge Univ. Press, Cambridge, 2004, pp. 285–315. MR 2083216

[vL07] Ronald van Luijk, *An elliptic $K3$ surface associated to Heron triangles*, J. Number Theory **123** (2007), no. 1, 92–119. MR 2295433

Jean Gillibert, Institut de Mathématiques de Toulouse, CNRS UMR 5219, 118 route de Narbonne, 31062 Toulouse Cedex 9, France.

E-mail address: jean.gillibert@math.univ-toulouse.fr

Aaron Levin, Department of Mathematics, Michigan State University, 619 Red Cedar Road, East Lansing, MI 48824, USA.

E-mail address: adlevin@math.msu.edu