Selmer groups and Mordell–Weil groups of elliptic curves over towers of function fields

Jordan S. Ellenberg

Abstract

Silverman has discussed the problem of bounding the Mordell–Weil ranks of elliptic curves over towers of function fields (J. Algebraic Geom. **9** (2000), 301–308; J. reine. angew. Math. **577** (2004), 153–169). We first prove generalizations of the theorems of Silverman by a different method, allowing non-abelian Galois groups and removing the dependence on Tate's conjectures. We then prove some theorems about the growth of Mordell–Weil ranks in towers of function fields whose Galois groups are p-adic Lie groups; a natural question is whether the Mordell–Weil rank is bounded in such a tower. We give some Galois-theoretic criteria which guarantee that certain curves $\mathcal{E}/\mathbb{Q}(t)$ have finite Mordell–Weil rank over $\mathbb{C}(t^{p^{-\infty}})$, and show that these criteria are met for elliptic K3 surfaces whose associated Galois representations have sufficiently large image.

1. Introduction

Let k be a field of characteristic prime to 6, C/k a smooth (but not necessarily proper) curve, and $\mathcal{E} \to C$ a non-isotrivial elliptic surface. Write k^{s} for the separable closure of k. The rank of $\mathcal{E}$ over $k^{\mathrm{s}}(C)$ is bounded by the geometric expression

$$\mathrm{rank}_{\mathbb{Z}}\, \mathcal{E}(k^{\mathrm{s}}(C)) \leqslant f(\mathcal{E}) := |N(\mathcal{E})| - 2\chi(C) \tag{1}$$

where $N(\mathcal{E})$ is the conductor of $\mathcal{E}$, a divisor on C (see [Shi92]). We emphasize that $N(\mathcal{E})$ records only the places of bad reduction of $\mathcal{E}$ over C, not over a compactification of C.

If $C' \to C$ is an étale cover of curves over k, one can try to bound the Mordell–Weil rank $\mathrm{rank}_{\mathbb{Z}}\, \mathcal{E}(k(C'))$ in terms of invariants of $\mathcal{E}/C$ and of the cover C'/C. Denoting by $\mathcal{E}'$ the pullback of $\mathcal{E} \to C$ by $C' \to C$, we have the elementary bound

$$\mathrm{rank}_{\mathbb{Z}}\, \mathcal{E}(k(C')) \leqslant \mathrm{rank}_{\mathbb{Z}}\, \mathcal{E}(k^{\mathrm{s}}(C')) = \mathrm{rank}_{\mathbb{Z}}\, \mathcal{E}'(k^{\mathrm{s}}(C')) \leqslant f(\mathcal{E}') = [C' : C]f(\mathcal{E}).$$

However, one can typically do much better by using the fact that $\mathcal{E}'$ is not an arbitrary elliptic surface over C', but one descending to a surface over C. In [Sil00] and [Sil04], Silverman proved upper bounds on $\mathrm{rank}_{\mathbb{Z}}\, \mathcal{E}(k(C'))$ in the case where $C = \mathbb{G}_m$ and $C' \to C$ is multiplication by n, or in the case where C is proper and $C' \to C$ is abelian, and under the hypotheses that k is a number field and Tate's conjecture holds for the elliptic surface $\mathcal{E} \times_C C'$. In the first part of this paper, we generalize Silverman's theorems to the case of arbitrary étale covers and arbitrary base field of characteristic prime to 6, and remove the dependence on Tate's conjecture.

If K is a finite group carrying an action of $\mathrm{Gal}(k^{\mathrm{s}}/k)$, we define a real number $\epsilon(K, \Sigma)$ in Definition 2.6. This definition depends only on K and on the finite group Σ, which is the image of $\mathrm{Gal}(k^{\mathrm{s}}/k)$ in $\mathrm{Aut}(K)$.

This journal is © Foundation Compositio Mathematica 2006.

THEOREM (Theorem 2.8). *Let k be a field of characteristic prime to 6, and C_0/k a smooth (but not necessarily proper) curve. Let $f : C \to C_0$ be a map of curves such that $C_{k^s} \to (C_0)_{k^s}$ is an étale Galois cover, with group K, and let $\mathcal{E}/C_0$ be a non-isotrivial elliptic curve over C_0. Then*

$$\mathrm{rank}_{\mathbb{Z}} \, \mathcal{E}(k(C)) \leqslant \epsilon(K, \Sigma)(|N(\mathcal{E})| - 2\chi(C_0))$$

where $N(\mathcal{E})$ is the conductor of $\mathcal{E}/C_0$ and $\chi(C_0)$ is the Euler characteristic of C_0.

When the action of $\mathrm{Gal}(k^s/k)$ on K is trivial (e.g. if k is separably closed), one has $\epsilon(K, \Sigma) = |K|$ and we do no better than (1). In the cases treated by Silverman, $\epsilon(K, \Sigma)$ agrees with his upper bound. There are two main ideas. The first is to rephrase the problem in terms of a Selmer group $\mathcal{S}(C, \mathcal{E}[p^\infty])$, a discrete p-primary $\mathrm{Gal}(k^s/k)$-module containing $\mathcal{E}(k^s(C)) \otimes_{\mathbb{Z}} \mathbb{Q}_p/\mathbb{Z}_p$. The Selmer group, being a Galois-cohomological object, is easier to manipulate than the Mordell–Weil groups themselves. Then the inclusion of Mordell–Weil groups into Selmer groups allows us to derive the desired upper bounds on Mordell–Weil ranks from theorems on Selmer groups. The second idea is the observation that theorems of this kind can be derived from (1) using the representation theory of finite groups; no arithmetic input is needed and the dependence on Tate's conjecture is avoided.

Theorem 2.8 and the results of Silverman show that, as C' varies through some natural families of covers of C, the Mordell–Weil rank of $\mathcal{E}$ over $k(C')$ grows much more slowly than does $[C' : C]$. A natural question is thus: is the rank in fact unbounded in such a family? Stiller [Sti87], Shioda [Shi86], and Fastenberg [Fas97] have given examples of elliptic curves over $\mathbb{C}(t)$ which have finite rank over $\bigcup_{r \in \mathbb{Z}} \mathbb{C}(t^{1/r})$, and Ulmer [Ulm05] gives examples of elliptic curves over $k(t)$ with finite rank over $\bigcup_{n \in \mathbb{Z}_{\geqslant 0}} k(t^{1/p^n})$ for certain finite fields k and primes p. On the other hand, Ulmer exhibits in [Ulm02] an elliptic curve over $\mathbb{F}_p(t)$ whose rank over $\mathbb{F}_p(t^{1/r})$ is unbounded as r grows. In [Sil04], Silverman asks the following question.

Question 1. Let

$$\cdots \to C_n \to \cdots \to C_2 \to C_1 \to C_0 = C \tag{2}$$

be a tower of curves over k such that $k^s(C_n)/k^s(C)$ is an étale Galois extension for each n. Write $k(C_\infty)$ for the direct limit of the fields $k(C_n)$. Under what circumstances is $\mathcal{E}(k(C_\infty))$ finitely generated? What about $\mathcal{E}(k^s(C_\infty))$?

The second part of the present paper is devoted to the above question in the case where the Galois group of the tower is a pro-p p-adic Lie group K. In this case, the Selmer group of $\mathcal{E}/C_\infty$ can be thought of as a module for the Iwasawa algebra of K. Using this point of view, we prove that the rank of $\mathcal{E}(k^s(C_n))$ is bounded as n grows in the case where $K \cong \mathbb{Z}_p$ and the image of $\mathrm{Gal}(k^s/k)$ on the Selmer group $\mathcal{S}(C_0, \mathcal{E}[p^\infty])$ is large enough.

THEOREM (Theorem 4.4). *Let k be a field of characteristic prime to 6, let $\cdots \to C_2 \to C_1 \to C_0$ be a tower of curves with Galois group $K \cong \mathbb{Z}_p$, and let $\mathcal{E}/k(C_0)$ be an elliptic curve. Let p be a prime not equal to $\mathrm{char}\, k$ and greater than $|N(\mathcal{E})| - 2\chi(C_0)$. Let k_∞ be an extension of k such that $\mathrm{Gal}(k^s/k_\infty)$ acts trivially on K.*

Suppose that, for every extension ℓ/k_∞ which is an abelian pro-p extension of a finite extension of k_∞, no divisible subgroup of $\mathcal{S}(C_0, \mathcal{E}[p^\infty])$ is fixed by $\mathrm{Gal}(k^s/\ell)$. Then $\mathrm{rank}_{\mathbb{Z}} \, \mathcal{E}(k^s(C_n))$ is bounded independently of n.

The conditions above appear to be fairly mild; in the final section of the paper we show that the generic minimal elliptic K3 surface satisfies the conditions of Theorem 4.4. It follows from a Hilbert irreducibility argument that there are infinitely many elliptic K3 surfaces $E/\mathbb{Q}(t)$ and primes p such that $E(\bar{\mathbb{Q}}(t^{1/p^\infty}))$ has finite rank.

The generalization of Theorem 4.4 to p-adic Galois groups other than $\mathbb{Z}_p$ seems to involve interesting questions about Galois representations with coefficients in Iwasawa algebras: see, for instance, Remarks 3.5 and 4.3.

2. Selmer groups of elliptic curves over finite extensions of function fields

The main idea of this section is the following: if C is a curve and $K \subset \mathrm{Aut}(C_{k^s})$ is a finite subgroup, then $M = \mathcal{E}(k^s(C)) \otimes_{\mathbb{Z}} \mathbb{C}$ is a complex representation of the group $K \rtimes \mathrm{Gal}(k^s/k)$, and indeed of a finite quotient $K \rtimes \Sigma$ of this group. Then $\mathcal{E}(k(C))$ is closely related to M^Σ; moreover, the structure of M as a K-module is strongly constrained by (1). We can then use purely group-theoretic facts about the irreducible characters of $K \rtimes \Sigma$ to bound the dimension of M^Σ, and thereby the rank of $\mathcal{E}$ over $k(C)$. The key group-theoretic quantity $\epsilon(K, \Sigma)$ is defined in Definition 2.6; we give elementary upper and lower bounds for $\epsilon(K, \Sigma)$ in Proposition 2.11, but there is certainly room for a more precise understanding of this combinatorial invariant.

It turns out that the easiest way to bound the size of Mordell–Weil groups is by means of corresponding Selmer groups; this is the approach we take below. We begin by introducing the notation that we will use throughout the paper.

Let C/k^s be a curve (smooth and absolutely irreducible) over a separably closed field of characteristic prime to 6, and let $f : \mathcal{E} \to C$ be a non-isotrivial family of curves whose generic fiber is an elliptic curve. (From now on we refer to such an $\mathcal{E}$ simply as a 'non-isotrivial elliptic curve over C'.) In particular, we assume f admits a section. Let U be the maximal open dense subscheme of C over which $\mathcal{E}$ is smooth. Let X be the closure of C (that is, the unique nonsingular curve having C as open dense subscheme). Let P be the set $X(k^s) \backslash C(k^s)$ and let Q be the set $C(k^s) \backslash U(k^s)$. Write g for the genus of X; so $\chi(C) = 2 - 2g - |P|$. Finally, let M be the set of points in $C(k^s)$ where $\mathcal{E}$ has multiplicative reduction. Then the conductor $N(\mathcal{E})$ is a divisor on C whose degree is $2|Q| - |M|$.

We now fix a prime p not equal to $\mathrm{char}\, k$. There is a natural descent map

$$\delta_p : \mathcal{E}(k^s(C)) \otimes_{\mathbb{Z}} \mathbb{Q}_p/\mathbb{Z}_p \hookrightarrow H^1(\pi_1^{\text{ét}}(U), \mathcal{E}[p^\infty]).$$

We can replace the étale fundamental group above with a tame fundamental group, as the following proposition demonstrates.

PROPOSITION 2.1. *The descent map δ_p factors through a map*

$$\mathcal{E}(k^s(C)) \otimes_{\mathbb{Z}} \mathbb{Q}_p/\mathbb{Z}_p \hookrightarrow H^1(\pi_1^{\text{tame}}(U), \mathcal{E}[p^\infty]).$$

Proof. Let x be a point in $\mathcal{E}(k^s(C))$ and let y be a point of $\mathcal{E}(k(C)^s)$ with $p^\alpha y = x$. We need to show that for every place v of $k^s(C)$, the extension of the local field $k^s(C)_v$ generated by y is tamely ramified. Since $\mathrm{char}\, k > 3$, we know that $\mathcal{E}$ acquires semistable reduction over a tamely ramified extension of $k^s(C)_v$; we therefore assume that $\mathcal{E}$ has semistable reduction. If $\mathcal{E}$ has good reduction at v, the extension of $k^s(C)_v$ generated by y is unramified. If $\mathcal{E}$ has multiplicative reduction at v, the theory of the Tate curve implies that the extension generated by y is that obtained by adjoining a pth root of an element of the local field $k^s(C)_v$; such an extension is again tamely ramified, since $p \neq \mathrm{char}\, k$. $\qquad\square$

We now define the Selmer group whose study makes up the rest of this paper.

DEFINITION 2.2. Let $j : \eta \hookrightarrow C$ be the inclusion of the generic point into C, and let A be a discrete p-primary torsion sheaf on the étale site of η (alternately, a module for the absolute Galois group of η). Then take $\mathcal{F}_A = j_* A$, and define $\mathcal{S}(C, A)$ to be $H^1(C, \mathcal{F}_A)$.

When there is no danger of confusion, we write $\mathcal{F}$ for the sheaf $\mathcal{F}_{\mathcal{E}[p^\infty]}$.

1217

Remark 2.3. The fact that k^{s} is only separably closed, not algebraically closed, presents no problems, since we may base change to the algebraic closure without affecting cohomology: compare [Mil80, 2.4.(c)].

We now explain briefly how this definition conforms with the more classical definition. Let π be the tame fundamental group $\pi_1^{\mathrm{tame}}(U)$. For each place v of $k^{\mathrm{s}}(C)$, let $k^{\mathrm{s}}(C)_v$ be the completion of $k^{\mathrm{s}}(C)$ at v; write π_v for the local tame fundamental group $\mathrm{Gal}((k^{\mathrm{s}}(C)_v)^{\mathrm{tame}}/k^{\mathrm{s}}(C)_v)$. This group is isomorphic to $\hat{\mathbb{Z}}$ if $\mathrm{char}\, k = 0$ and to $\prod_{\ell \neq q} \mathbb{Z}_\ell$ if $\mathrm{char}\, k = q$. There is a long exact sequence (see, e.g., [Mil80, III.1.25])

$$0 \to \mathcal{S}(C, A) \to H^1(U, \mathcal{F}_A) \to \bigoplus_{v \in Q} H^2_v(C, \mathcal{F}_A) \to H^2(C, \mathcal{F}_A). \tag{3}$$

Now $H^2_v(C, \mathcal{F}_A) = H^1(\pi_v, A)$ by excision, and $H^1(U, \mathcal{F}_A) = H^1(\pi, A)$ (see [Mil80, V.2.17]). So we can alternatively describe the Selmer group as

$$\mathcal{S}(C, A) = \ker(H^1(\pi, A) \to \bigoplus_{v \in Q} H^1(\pi_v, A)). \tag{4}$$

When $A = \mathcal{E}[p^\infty]$, we have a local descent map

$$\delta_{p;v} : \mathcal{E}(k^{\mathrm{s}}(C)_v) \otimes_{\mathbb{Z}} \mathbb{Q}_p/\mathbb{Z}_p \to H^1(\pi_v, \mathcal{E}[p^\infty]).$$

Note that we have $\mathcal{E}(k^{\mathrm{s}}(C)_v) \otimes_{\mathbb{Z}} \mathbb{Q}_p/\mathbb{Z}_p = 0$, since $p \neq \mathrm{char}\, k$. So (4) agrees with the classical definition of the Selmer group $\mathcal{S}(C, \mathcal{E}[p^\infty])$. We denote the group $\bigoplus_{v \in Q} H^1(\pi_v, \mathcal{E}[p^\infty])$ by $\mathcal{L}(C, \mathcal{E}[p^\infty])$. Note that the summand $H^1(\pi_v, \mathcal{E}[p^\infty])$ is trivial unless $\mathcal{E}$ has multiplicative reduction at v, in which case $H^1(\pi_v, \mathcal{E}[p^\infty])$ is a cofree $\mathbb{Z}_p$-module of corank 1 by the theory of the Tate curve.

The global descent map δ_p gives an injection

$$\mathcal{E}(k^{\mathrm{s}}(C)) \otimes_{\mathbb{Z}} \mathbb{Q}_p/\mathbb{Z}_p \hookrightarrow \mathcal{S}(C, \mathcal{E}[p^\infty])$$

whence an inequality

$$\mathrm{rank}_{\mathbb{Z}}\, \mathcal{E}(k^{\mathrm{s}}(C)) \leqslant \mathrm{corank}_{\mathbb{Z}_p}\, \mathcal{S}(C, \mathcal{E}[p^\infty])$$

which is the source of all bounds on Mordell–Weil groups in this paper. In a slight abuse of notation, when C and $\mathcal{E}$ are defined over a field k which is not separably closed, we take $\mathcal{S}(C, \mathcal{E}[p^\infty])$ to mean $\mathcal{S}(C \times_k k^{\mathrm{s}}, \mathcal{E}[p^\infty])$.

Remark 2.4. It will often be useful to know that the action of π on the torsion points of $\mathcal{E}$ has large image. To be more precise: the image of π in $\mathrm{Aut}(\mathcal{E}[p^\infty]) \cong \mathrm{GL}_2(\mathbb{Z}_p)$ contains a finite-index subgroup of $\mathrm{SL}_2(\mathbb{Z}_p)$, since the j-invariant map from C to $X(1)$ is dominant, and thus exhibits C as a finite cover of the j-line. In particular, $\mathcal{E}[p^\infty]^\pi$ is a finite group.

PROPOSITION 2.5. *Let $C, \mathcal{E}, p$ be as above. Then:*

- *$H^1(\pi, \mathcal{E}[p^\infty])$ is a cofree $\mathbb{Z}_p$-module of corank $|N(\mathcal{E})| - 2\chi(C) + |M|$;*
- *$\mathcal{S}(C, \mathcal{E}[p^\infty])$ is a $\mathbb{Z}_p$-module of corank $|N(\mathcal{E})| - 2\chi(C)$.*

Proof. Write $\mathcal{F}$ for $\mathcal{F}_{\mathcal{E}[p^\infty]}$. By [Mil80, V.2.17], we have $H^1(\pi, \mathcal{E}[p^\infty]) = H^1(U, \mathcal{F})$. Note that $H^0(U, \mathcal{F}) = \mathcal{E}[p^\infty]^\pi$; this group is finite by Remark 2.4. It then follows from [Mil80, V.2.18] that $H^1(\pi, \mathcal{E}[p^\infty])$ has $\mathbb{Z}_p$-corank

$$4g - 4 + 2|P| + 2|Q| = |N(\mathcal{E})| - 2\chi(C) + |M|.$$

Now $H^2(\pi, \mathcal{E}[p]) = 0$ (again by [Mil80, V.2.17]) so $H^1(\pi, \mathcal{E}[p^\infty])$ is divisible, which implies it is cofree.

The exact sequence (3) shows that the map $H^1(\pi, \mathcal{E}[p^\infty]) \to \mathcal{L}(C, \mathcal{E}[p^\infty])$ has cokernel a subgroup of $H^2(C, \mathcal{F})$. If C is affine, this cohomology group vanishes; if C is projective, $H^2(C, \mathcal{F})$ is dual to $H^0(C, \mathcal{F})$, which is finite as already noted.

We conclude that

$$\operatorname{corank}_{\mathbb{Z}_p} \mathcal{S}(C, \mathcal{E}[p^\infty]) = (N(\mathcal{E}) - 2\chi(C) + |M|) - \operatorname{corank}_{\mathbb{Z}_p} \mathcal{L}(C, \mathcal{E}[p^\infty])$$

which yields the desired result. $\qquad\square$

We are now ready to state our first bound on Selmer groups. First, we need a group-theoretic definition.

DEFINITION 2.6. Let K be a finite group, and Σ a subgroup of $\operatorname{Aut}(K)$. Let G be the semidirect product $K \rtimes \Sigma$. Let V_G be the real vector space spanned by the irreducible complex-valued characters of G, and V_K the real vector space spanned by the irreducible complex-valued characters of K; we say a vector v in V_G (respectively, V_K) is *nonnegative* if its inner product with each irreducible representation of G (respectively, K) is nonnegative. Let $[G/\Sigma] \in V_G$ be the coset character of G attached to Σ, and let $[K/1] \in V_K$ be the regular character of K. Finally, let $\epsilon(K, \Sigma)$ be the maximum of the inner product $\langle v, [G/\Sigma] \rangle$ over all $v \in V_G$ such that:

- v is nonnegative;
- $[K/1] - r(v)$ is nonnegative, where $r : V_G \to V_K$ is the restriction map.

Remark 2.7. The region of V_G demarcated by the two conditions above is a compact polytope, so $\epsilon(K, \Sigma)$ is well defined.

The first main theorem of this paper is the following.

THEOREM 2.8. *Let k be a field of characteristic prime to 6, and C_0/k a smooth (but not necessarily proper) curve. Let $f : C \to C_0$ be a map of curves such that $C_{k^s} \to (C_0)_{k^s}$ is an étale Galois cover, with group K, let Σ be the image of $\operatorname{Gal}(k^s/k)$ in $\operatorname{Aut}(K)$, and let $\mathcal{E}/C_0$ be a non-isotrivial elliptic curve over C_0. Then*

$$\operatorname{rank}_{\mathbb{Z}} \mathcal{E}(k(C)) \leqslant \epsilon(K, \Sigma)(|N(\mathcal{E})| - 2\chi(C_0))$$

where $N(\mathcal{E})$ is the conductor of $\mathcal{E}/C_0$ and $\chi(C_0)$ is the Euler characteristic of C_0.

Proof. Define X, U, P, Q, M, π, g as in the first part of this section; we denote the corresponding objects attached to C_0, by adding a subscript 0, so that, for example, M_0 is the set of places of C_0 where $\mathcal{E}$ has multiplicative reduction. Let p be a prime not equal to $\operatorname{char} k$.

LEMMA 2.9. *Let $\mathcal{S}(C, \mathcal{E}[p^\infty])$ be the Selmer group defined above. Then*

$$\operatorname{Hom}(\mathcal{S}(C, \mathcal{E}[p^\infty]), \mathbb{Q}_p/\mathbb{Z}_p) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$$

is a free $\mathbb{Q}_p[K]$-module of rank $|N(\mathcal{E})| - 2\chi(C_0)$.

Proof. If A is a discrete cofinitely generated $\mathbb{Z}_p[K]$-module, we denote by $W(A)$ the finitely generated $\mathbb{Q}_p[K]$-module $\operatorname{Hom}(A, \mathbb{Q}_p/\mathbb{Z}_p) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$.

First of all, $\mathcal{L}(C, \mathcal{E}[p^\infty])$ is a direct sum of $|K|$ copies of $\mathcal{L}(C_0, \mathcal{E}[p^\infty])$, permuted faithfully by K. So $W(\mathcal{L}(C, \mathcal{E}[p^\infty]))$ is a free $\mathbb{Q}_p[K]$-module of rank $|M_0|$. As in the proof of Proposition 2.5, the finiteness of $H^2(\mathcal{C}, \mathcal{F})$ shows that

$$[W(H^1(\pi, \mathcal{E}[p^\infty]))] = [W(S, \mathcal{E}[p^\infty])] + [W(\mathcal{L}(C, \mathcal{E}[p^\infty]))]$$

in the Grothendieck group of the category of $\mathbb{Q}_p[K]$-modules. By Shapiro's lemma,

$$H^1(\pi, \mathcal{E}[p^\infty]) = H^1(\pi_0, \mathcal{E}[p^\infty] \otimes_{\mathbb{Z}} \mathbb{Z}[K])$$

and, as in [Mil80, Remark V.2.19], there is an identity

$$[H^1(\pi_0, A)] - [H^0(\pi_0, A)] = (2g_0 - 2 + |P_0| + |Q_0|)[A] \tag{5}$$

for any π_0-module A. Since the construction there is functorial, (5) is an identity in the Grothendieck group of discrete cofinitely generated $\mathbb{Z}_p[K]$-modules when $A = \mathcal{E}[p^\infty] \otimes_{\mathbb{Z}} \mathbb{Z}[K]$. Since $H^0(\pi_0, \mathcal{E}[p^\infty])$ is a cotorsion $\mathbb{Z}_p$-module, it is killed by the functor W; we conclude that

$$[W(H^1(\pi, \mathcal{E}[p^\infty]))] = (4g_0 - 4 + 2|P_0| + 2|Q_0|)[\mathbb{Q}_p[K]]$$

from which the desired result follows. $\qquad\square$

Now let ℓ be the smallest extension of k over which the automorphisms in K are defined; then Σ can be identified with $\mathrm{Gal}(\ell/k)$. Define

$$W = W(\mathcal{E}(\ell(C)) \otimes_{\mathbb{Z}} \mathbb{Q}_p/\mathbb{Z}_p).$$

Then W is a representation of $K \rtimes \Sigma$ over $\mathbb{Q}_p$, and $\dim W = \mathrm{rank}_{\mathbb{Z}} \mathcal{E}(\ell(C))$. Moreover, we know by Lemma 2.9 that W, considered as $\mathbb{Q}_p[K]$-module, is a quotient of $\mathbb{Q}_p[K]^{|N(\mathcal{E})| - 2\chi(C_0)}$.

It follows by the definition of $\epsilon(K, \Sigma)$ that

$$\mathrm{rank}_{\mathbb{Z}} \mathcal{E}(k(C)) = \dim_{\mathbb{Q}_p} W^\Sigma \leqslant \epsilon(K, \Sigma)(|N(\mathcal{E})| - 2\chi(C_0))$$

which was to be proved. $\qquad\square$

Remark 2.10. The methods used to prove Theorem 2.8 should be applicable to abelian varieties of arbitrary dimension. Pacheco has carried this out in a recent preprint [Pac06]; we thank him for communicating this to us. See [Pac05] for an extension of Silverman's results to abelian varieties of higher dimension.

We now turn to the problem of computing, or at least bounding, the value of $\epsilon(K, \Sigma)$ in terms of more readily computable invariants.

PROPOSITION 2.11. *Let K/Σ be the set of orbits of Σ on K, and let $\mathrm{Irr}(K)/\Sigma$ be the set of orbits of Σ on irreducible characters of K. Then*

$$|K/\Sigma| \leqslant \epsilon(K, \Sigma) \leqslant \sum_{\chi \in \mathrm{Irr}(K)/\Sigma} \chi(1)^2.$$

In particular, if K is abelian,

$$\epsilon(K, \Sigma) = |K/\Sigma|.$$

Proof. The lower bound on $\epsilon(K, \Sigma)$ is obtained merely by taking $V = [G/\Sigma]$. Then $r(V)$ is the regular character of K, while $\langle V, [G/\Sigma] \rangle$ is $|K/\Sigma|$, yielding

$$|K/\Sigma| \leqslant \epsilon(K, \Sigma)$$

as desired.

We now address the upper bound. Let W be an irreducible representation of $G = K \rtimes \Sigma$ with character ψ; then there is a unique orbit $\mathcal{O}$ of $\mathrm{Irr}(K)$ under Σ such that

$$\psi = \sum_{\chi \in \mathcal{O}} \langle \psi | K, \chi \rangle \chi.$$

Note that $\langle \psi | K, \chi \rangle$ does not depend on the choice of $\chi \in \mathcal{O}$. Choose such a χ, and write W_χ for the χ-isotypical part of W.

Choose a projection $\pi : W \to W_\chi$ compatible with the action of K. Then we have a map of complex vector spaces $\Pi : W \to (W_\chi)^{|\Sigma|}$ defined by

$$\Pi(w) = \bigoplus_{\sigma \in \Sigma} \pi(w^\sigma).$$

1220

The kernel of Π is preserved by all of G; since W is irreducible, the map Π must be an injection. Now $\Pi(W^\Sigma)$ is contained in the diagonal of $(W_\chi)^{|\Sigma|}$; we conclude that

$$\dim W^\Sigma \leqslant \dim W_\chi = \langle \psi | K, \chi \rangle \chi(1).$$

Now let V be an arbitrary representation of G satisfying the two constraints in the definition of $\epsilon(K, \Sigma)$. By the above argument, each irreducible constituent W of V satisfies

$$\dim W^\Sigma \leqslant \langle \psi_W | K, \chi \rangle \chi(1)$$

whenever χ is an irreducible character of K with $\langle \psi_W | K, \chi \rangle$ nonzero. On the other hand, the fact that $[K/1] - r(V)$ is nonnegative implies that

$$\sum_W \langle \psi_W | K, \chi \rangle \leqslant \chi(1).$$

For each orbit $\mathcal{O}$ of $\mathrm{Irr}(K)/\Sigma$, let $V(\mathcal{O})$ be the sum of all irreducible constituents W of V such that $\langle \psi_W | K, \chi \rangle > 0$ for some (whence every) $\chi \in \mathcal{O}$. Then the above inequalities show

$$\dim V(\mathcal{O})^\Sigma \leqslant \sum_{W \subset V(\mathcal{O})} \dim W^\Sigma \leqslant \chi(1)^2.$$

Summing over all orbits $\mathcal{O}$ yields the desired upper bound on $\epsilon(K, \Sigma)$.

The statement on abelian K now follows immediately. □

Remark 2.12. Neither bound in Proposition 2.11 is sharp in general. For instance, if we take $G = S_4, K = A_4, \Sigma = \mathbb{Z}/2\mathbb{Z}$, the proposition yields

$$7 \leqslant \epsilon(K, \Sigma) \leqslant 11.$$

In fact, by direct examination of the irreducible characters of G one computes that $\epsilon(K, \Sigma) = 8$. It would be interesting to give tighter bounds on $\epsilon(K, \Sigma)$ that do not involve knowing the character table of G. In light of the second half of this paper, it would also be interesting to understand how $\epsilon(K, \Sigma)$ varies as $K \rtimes \Sigma$ varies among quotients of a certain fixed pro-p group.

In the case where K is abelian, Theorem 2.8 and Proposition 2.11 combine to yield the following bound on Mordell–Weil rank.

COROLLARY 2.13. *Let C/k be a smooth curve with an abelian group K of fixed-point free automorphisms. Let $\mathcal{E}$ be an elliptic curve over C. Let $|K/G_k|$ be the number of orbits of K under the action of the absolute Galois group of k. Then*

$$\mathrm{rank}\, \mathcal{E}(k(C)) \leqslant (|K/G_k|/|K|)(|\mathcal{N}(\mathcal{E})| - 2\chi(C)).$$

Corollary 2.13 implies, in particular, unconditional versions of the main theorems of [Sil00] and [Sil04]. Theorem 1 of [Sil00] is the case in which $C = \mathbb{G}_m$ and K is the abelian group μ_n. Theorem 1 of [Sil04] is the case in which C is an arbitrary proper curve, and K is an abelian group of fixed-point-free automorphisms.

We now consider more specifically the case where K is a finite p-group, with $p \neq \mathrm{char}\, k$. This case can be seen as a bridge to the next section, in which K becomes an infinite pro-p group and we consider asymptotic questions about towers of function fields.

We first observe that, in some such cases, the rank of $\mathcal{E}(k(C))$ is not only subject to an upper bound as in Theorem 2.8, but is actually zero.

PROPOSITION 2.14. *Let k be a field of characteristic prime to $6p$ and C_0/k a smooth curve. Let $C/k \to C_0/k$ be a map of curves such that $C_{k^s} \to (C_0)_{k^s}$ is an étale Galois cover, with Galois group*

a finite p-group K. Let $\mathcal{E}$ be a non-isotrivial elliptic curve over C_0, and define π, π_0, M_0 as in § 2. Let ℓ be an extension of k over which all the elements of K are defined.

Suppose that $\mathcal{E}[p^\infty]^\pi$ and $\mathcal{S}(C_0, \mathcal{E}[p^\infty])^{\mathrm{Gal}(k^s/\ell)}$ are trivial. Then $\mathrm{rank}_\mathbb{Z} \mathcal{E}(\ell(C)) = 0$.

Proof. The Hochschild–Serre spectral sequence, together with the fact that $H^0(C, \mathcal{F}) = \mathcal{E}[p^\infty]^\pi$ is trivial, yields an isomorphism

$$\mathcal{S}(C_0, \mathcal{E}[p^\infty]) \to \mathcal{S}(C, \mathcal{E}[p^\infty])^K.$$

Taking $\mathrm{Gal}(k^s/\ell)$-invariants yields

$$0 = \mathcal{S}(C_0, \mathcal{E}[p^\infty])^{\mathrm{Gal}(k^s/\ell)} = (\mathcal{S}(C, \mathcal{E}[p^\infty])^{\mathrm{Gal}(k^s/\ell)})^K.$$

Since K is a p-group, the fact that the discrete $\mathbb{Z}_p[K]$-module $\mathcal{S}(C, \mathcal{E}[p^\infty])^{\mathrm{Gal}(k^s/\ell)}$ has no K-invariants implies that it is trivial, so $(\mathcal{E}(k^s(C)) \otimes_\mathbb{Z} \mathbb{Q}_p/\mathbb{Z}_p)^{\mathrm{Gal}(k^s/\ell)}$ is also trivial. The map

$$\mathcal{E}(\ell(C)) \otimes_\mathbb{Z} \mathbb{Q}_p/\mathbb{Z}_p \to \mathcal{E}(k^s(C)) \otimes_\mathbb{Z} \mathbb{Q}_p/\mathbb{Z}_p$$

has finite kernel, so $\mathrm{rank}_\mathbb{Z} \mathcal{E}(\ell(C)) = 0$ as desired. □

3. Pro-p towers of function fields

We now turn our attention to questions of a more Iwasawa-theoretic flavor, replacing our finite étale covers of curves with profinite towers of curves.

DEFINITION 3.1. Let p be a prime different from char k. A *pro-p tower* over a smooth curve C_0/k is a tower

$$\cdots \to C_n \to \cdots \to C_1 \to C_0 \tag{6}$$

such that:

- $C_n \to C_0$ is a map of curves over k;
- $C_n/k^s \to C_0/k^s$ is a finite étale Galois cover whose Galois group, denoted by K_n, is a p-group.

  If

$$C_n \to \cdots \to C_1 \to C_0$$

is a pro-p tower, we denote by $K = \varprojlim K_n$ the Galois group of the tower, and by $K^{(n)}$ the kernel of the projection $K \to K_n$. We denote by k_∞ the minimal algebraic extension of k whose Galois group acts trivially on K.

Let $\mathcal{E}$ be a non-isotrivial elliptic curve over $k(C_0)$. Then, following Silverman [Sil04], one can ask the following questions.

- Is $\mathrm{rank}_\mathbb{Z} \mathcal{E}(k(C_n))$ bounded as n grows?
- Is $\mathrm{rank}_\mathbb{Z} \mathcal{E}(k^s(C_n))$ bounded as n grows?

For example, Fastenberg [Fas97], Shioda [Shi86], and Stiller [Sti87] give examples of elliptic curves $\mathcal{E}/\mathbb{C}(t)$ with the property that $\mathrm{rank}_\mathbb{Z} \mathcal{E}(\mathbb{C}(t^{1/r}))$ is bounded independently of r. (Indeed, their results are stronger than those we will prove, since they apply to towers of extensions whose degrees involve multiple primes.) Similarly, Ulmer [Ulm05] exhibits elliptic curves over $k(t)$, with k a finite field, such that $\mathrm{rank}_\mathbb{Z} \mathcal{E}(k(t^{1/p^n}))$ is bounded as n grows.

On the other hand, Ulmer has also, in [Ulm02], exhibited an elliptic curve over $k(t)$, where k is a finite field, such that $\mathcal{E}(k(t^{1/p^n}))$ is unbounded as n grows. In fact, in this case the rank grows as fast as Theorem 2.8 permits.

In Theorem 4.4 we will show that the answer to both questions above is yes if $K = \mathbb{Z}_p$ and a certain 'large Galois image' condition is satisfied by the action of $\mathrm{Gal}(k^s/k)$ on $\mathcal{S}(C_0, \mathcal{E}[p^\infty])$.

We begin by observing that one can use Proposition 2.14 to construct towers in which $\mathcal{E}(k(C_n))$ has rank 0 for all n.

COROLLARY 3.2. *Let k be a field of characteristic prime to $6p$. Let*

$$\cdots \to C_n \to \cdots \to C_1 \to C_0$$

be a pro-p tower with Galois group K over C_0/k. Let $\mathcal{E}$ be a non-isotrivial elliptic curve over C_0. Let π be the kernel of the natural map $\pi_0 \to K$, and let k_∞ be the minimal algebraic extension of k whose Galois group acts trivially on K.

Suppose, furthermore, that:

- *$\mathcal{E}[p^\infty]^\pi$ is trivial;*
- *the action of $\mathrm{Gal}(k^s/k_\infty)$ on $\mathcal{S}(C_0, \mathcal{E}[p^\infty])$ has trivial space of invariants.*

Then $\mathrm{rank}_{\mathbb{Z}} \mathcal{E}(k_\infty(C_n)) = 0$ for all n.

Proof. The proof is immediate from Proposition 2.14 applied to $C_n \to C_0$. □

One knows from experience with the Iwasawa theory of elliptic curves that it is often useful to describe the Selmer group of an elliptic curve over an infinite extension as a module for a certain Iwasawa algebra. Suppose we are given a tower over C_0/k, and define

$$\mathcal{S}(C_\infty, \mathcal{E}[p^\infty]) = \varinjlim_n \mathcal{S}(C_n, \mathcal{E}[p^\infty]).$$

Then $\mathcal{S}(C_\infty, \mathcal{E}[p^\infty])$ is a discrete p-primary group which carries a continuous action of K, whence an action of the Iwasawa algebra

$$\Lambda(K) := \varprojlim_H \mathbb{Z}_p[K/H]$$

where H ranges over open normal subgroups of K. In general, we write $H^i(C_\infty, \mathcal{F})$ to mean $\varinjlim H^i(C_n, \mathcal{F}|C_n)$.

We now introduce a simplifying hypothesis, which is in place for the remainder of this paper.

HYPOTHESIS 1. We hypothesize that K is a nontrivial pro-p finite dimensional p-adic Lie group with no p-torsion element.

Under this hypothesis, the Iwasawa algebra $\Lambda(K)$ is a left and right Noetherian local ring with no zero divisors, and $H^i(K, M)$ is a cofinitely generated $\mathbb{Z}_p$-module whenever M is a cofinitely generated $\Lambda(K)$-module (see [How02, Lemma 1.6]). There is a natural notion of the *corank* of a cofinitely generated discrete $\Lambda(K)$-module. Namely, we write

$$\mathrm{corank}_{\Lambda(K)} M = \sum_{i \geqslant 0} (-1)^i \mathrm{corank}_{\mathbb{Z}_p} H^i(K, M).$$

This definition was introduced by Howson, who also showed that it agrees with other natural definitions [How02].

PROPOSITION 3.3. *The $\Lambda(K)$-module $\mathcal{S}(C_\infty, \mathcal{E}[p^\infty])$ is cofinitely generated.*

Proof. By Nakayama's lemma [Coa99, Proposition 2.1], it suffices to show that

$$\mathcal{S}(C_\infty, \mathcal{E}[p^\infty])^K$$

is a cofinitely generated $\mathbb{Z}_p$-module. By the Hochschild–Serre spectral sequence, the cokernel of the map

$$\mathcal{S}_0(C_0, \mathcal{E}[p^\infty]) \to \mathcal{S}(C_\infty, \mathcal{E}[p^\infty])^K$$

1223

is a submodule of

$$H^2(K, \mathcal{E}[p^\infty]^\pi).$$

The lemma follows from the fact that $\mathcal{S}_0(C_0, \mathcal{E}[p^\infty])$ and $H^2(K, \mathcal{E}[p^\infty]^\pi)$ are both cofinitely generated $\mathbb{Z}_p$-modules. $\qquad \square$

PROPOSITION 3.4. *The $\Lambda(K)$-corank of $\mathcal{S}(C_\infty, \mathcal{E}[p^\infty])$ is $|N(\mathcal{E})| - 2\chi(C_0)$.*

Proof. By definition of corank,

$$\sum_{j=0}^{2} (-1)^j \operatorname{corank}_{\Lambda(K)} H^j(C_\infty, \mathcal{F}) = \sum_{i \geqslant 0} \sum_{j=0}^{2} (-1)^{i+j} \operatorname{corank}_{\mathbb{Z}_p} H^i(K, H^j(C_\infty, \mathcal{F})).$$

However, by the Hochschild–Serre spectral sequence, the last quantity is equal to

$$\sum_{k \geqslant 0} \operatorname{corank}_{\mathbb{Z}_p} (-1)^k H^k(C_0, \mathcal{F}).$$

Now $H^0(C_0, \mathcal{F})$ and $H^2(C_0, \mathcal{F})$ are both finite modules as in the proof of Proposition 2.5, so their $\mathbb{Z}_p$-corank is zero. Similarly, $H^0(C_\infty, \mathcal{F})$ and $H^2(C_\infty, \mathcal{F})$ both have finite $\mathbb{Z}_p$-corank, which implies that their $\Lambda(K)$-corank is 0. We conclude that

$$\operatorname{corank}_{\Lambda(K)} S(C_\infty, \mathcal{E}[p^\infty]) = \operatorname{corank}_{\mathbb{Z}_p} \mathcal{S}(C_0, \mathcal{E}[p^\infty])$$

and the result follows from Proposition 2.5. $\qquad \square$

Remark 3.5. The map $\mathcal{S}(C_n, \mathcal{E}[p^\infty]) \to \mathcal{S}(C_\infty, \mathcal{E}[p^\infty])^{K^{(n)}}$ has kernel $H^1(K^{(n)}, \mathcal{E}[p^\infty]^\pi)$. Suppose that $\mathcal{E}[p^\infty]^\pi$ is finite; then $H^1(K^{(n)}, \mathcal{E}[p^\infty]^\pi)$ is also finite. On the other hand, the composition

$$\mathcal{E}(k_\infty(C_n)) \otimes_{\mathbb{Z}} \mathbb{Q}_p/\mathbb{Z}_p \to \mathcal{E}(k^{\mathrm{s}}(C_n)) \otimes_{\mathbb{Z}} \mathbb{Q}_p/\mathbb{Z}_p \to \mathcal{S}(C_n, \mathcal{E}[p^\infty])$$

also has finite kernel. We conclude that the map

$$\mathcal{E}(k_\infty(C_n)) \otimes_{\mathbb{Z}} \mathbb{Q}_p/\mathbb{Z}_p \to \mathcal{S}(C_\infty, \mathcal{E}[p^\infty])^{\mathrm{Gal}(k^{\mathrm{s}}/k_\infty)}$$

has finite kernel. In particular, if $\mathcal{S}(C_\infty, \mathcal{E}[p^\infty])^{\mathrm{Gal}(k^{\mathrm{s}}/k_\infty)}$ has finite $\mathbb{Z}_p$-corank, it follows that the rank of $\mathcal{E}(k_\infty(C_n))$ is bounded independently of n. This leads us to consider the image of the Galois representation

$$\rho : \mathrm{Gal}(k^{\mathrm{s}}/k_\infty) \to \mathrm{Aut}_{\Lambda(K)}(\mathcal{S}(C_\infty, \mathcal{E}[p^\infty])).$$

For example, suppose $K = \mathbb{Z}_p^m$ and that $\mathcal{S}(C_\infty, \mathcal{E}[p^\infty])$ is a $\Lambda(K)$-module of corank R. Let F be the fraction field of $\Lambda(K) \cong \mathbb{Z}_p[[T_1, \ldots, T_m]]$. We then have a composition

$$\rho_F : \mathrm{Gal}(k^{\mathrm{s}}/k_\infty) \to \mathrm{Aut}_{\Lambda(K)}[\mathrm{Hom}(\mathcal{S}(C_\infty, \mathcal{E}[p^\infty]), \mathbb{Q}_p/\mathbb{Z}_p) \otimes_{\Lambda(K)} F] \cong \mathrm{GL}_R(F).$$

To say that $\mathcal{S}(C_\infty, \mathcal{E}[p^\infty])^{\mathrm{Gal}(k^{\mathrm{s}}/k_\infty)}$ has positive $\Lambda(K)$-corank is to say that ρ_F acts trivially on some line in F^R.

Is there some general class of $\mathbb{Z}_p^m$-towers for which ρ_F is irreducible? In the case $m = 1$, irreducibility and nontriviality of ρ_F would imply that $\mathcal{S}(C_\infty, \mathcal{E}[p^\infty])^{\mathrm{Gal}(k^{\mathrm{s}}/k_\infty)}$ was a cotorsion $\Lambda(K)$-module, which is to say a module of finite $\mathbb{Z}_p$-corank; so in that case $\mathcal{E}(k_\infty(C_n))$ would have bounded rank.

We note that ρ_F is very similar to the Galois representations defined by Ihara in [Iha86]. In each case, one starts with a cofinitely generated $\mathbb{Z}_p$-module M with actions of π_0 and $\mathrm{Gal}(k^{\mathrm{s}}/k)$; in our case the module is $\mathcal{E}[p^\infty]$, while in [Iha86] it is $\mathbb{Q}_p/\mathbb{Z}_p$. Then $H^1(\pi, M)$ is a cofinitely generated $\Lambda(K)$-module which carries an action of $\mathrm{Gal}(k^{\mathrm{s}}/k_\infty)$; one then studies the properties of the representation of $\mathrm{Gal}(k^{\mathrm{s}}/k_\infty)$ in $\mathrm{Aut}_{\Lambda(K)} H^1(\pi, M)$.

4. Mordell–Weil ranks over $\mathbb{Z}_p$-towers of function fields

In this section, we show that the general machinery set up in the section above can be used to show that the Mordell–Weil rank of $\mathcal{E}(k^s(C_n))$ is bounded as n grows, under the hypothesis that $K = \mathbb{Z}_p$ and $\mathrm{Gal}(k^s/k)$ acts with sufficiently large image on $\mathcal{S}(C_0, \mathcal{E}[p^\infty])$.

Let p be a prime, k a field with characteristic prime to $6p$, and

$$\cdots \to C_n \to \cdots \to C_1 \to C_0$$

a pro-p tower over a smooth curve C_0/k with Galois group $K = \mathbb{Z}_p$. As above, let k_∞ be the minimal algebraic extension of k over which all elements of K are defined. Let $\mathcal{E}/C_0$ be a non-isotrivial elliptic surface. For every extension ℓ/k, write $\ell(C_\infty)$ for the direct limit of the function fields $\ell(C_n)$.

In this section we will prove a theorem about the Mordell–Weil group of $\mathcal{E}$ over the field $k^s(C_\infty)$. To this end, we would like to show that the action of $\mathrm{Gal}(k^s/k)$ on $\mathcal{E}(k^s(C_\infty)) \otimes_\mathbb{Z} \mathbb{Q}_p/\mathbb{Z}_p$ factors through a small quotient. Of course, if $\mathcal{E}(k^s(C_\infty))$ is a finitely generated abelian group, then this Galois action factors through some *finite* quotient $\mathrm{Gal}(\ell/k)$. We will prove a weaker condition on ℓ, which will suffice for the applications below.

PROPOSITION 4.1. *Let $\{C_n\}$ be a tower of curves as above, and suppose that $p > |N(\mathcal{E})| - 2\chi(C_0)$. Then there exists an extension ℓ/k_∞ such that:*

- $\mathrm{Gal}(k^s/\ell)$ *acts trivially on* $\mathcal{E}(k^s(C_n)) \otimes_\mathbb{Z} \mathbb{Q}_p/\mathbb{Z}_p$ *for all n;*
- ℓ *is an abelian pro-p extension of a finite extension of k_∞.*

Proof. Since $\mathcal{S}(C_\infty, \mathcal{E}[p^\infty])$ is a cofinitely generated $\Lambda(K)$-module, the group $\mathcal{S}(C_\infty, \mathcal{E}[p^\infty])[p]^K$ is a finite-dimensional vector space over $\mathbb{F}_p$. Let ℓ_0 be a finite extension of k_∞ whose absolute Galois group G_{ℓ_0} acts trivially on $\mathcal{S}(C_\infty, \mathcal{E}[p^\infty])[p]^K$.

LEMMA 4.2. *Let K be a pro-p p-adic Lie group with no p-torsion element, and let M be a cofinitely generated $\Lambda(K)$-module. Suppose that G is a subgroup of $\mathrm{Aut}_{\Lambda(K)} M$ which acts trivially on $M[p]^K$. Then G is a pro-p group.*

Proof. Let $\mathfrak{m}$ be the maximal ideal in $\Lambda(K)$; then $M[p]^K = M[\mathfrak{m}]$. So, for each g in G, the endomorphism $g - 1$ of M kills $M[\mathfrak{m}]$, so $(g - 1)$ acts nilpotently on the finite submodule $M[\mathfrak{m}^a]$ for all $a \geqslant 0$. Since $M[\mathfrak{m}^a]$ is a finite abelian p-group, the image of G on $\mathrm{Aut}(M[\mathfrak{m}^a])$ is thus also a finite p-group. Now $M = \varinjlim M[\mathfrak{m}^a]$, so G is a pro-p group. $\qquad\square$

In particular, the lemma applies to the image of G_{ℓ_0} in $\mathrm{Aut}_{\Lambda(K)}(\mathcal{S}(C_\infty, \mathcal{E}[p^\infty]))$. Let ℓ'/ℓ_0 be a pro-p extension so that $G_{\ell'}$ acts trivially on $\mathcal{S}(C_\infty, \mathcal{E}[p^\infty])$.

We now consider the action of G_{ℓ_0} on $\mathcal{E}(k^s(C_n)) \otimes_\mathbb{Z} \mathbb{Q}_p/\mathbb{Z}_p$, a cofree cofinitely generated $\mathbb{Z}_p$-module which we denote by M_n. First of all,

$$\phi : \mathcal{S}(C_n, \mathcal{E}[p^\infty]) \to \mathcal{S}(C_\infty, \mathcal{E}[p^\infty])^{K_n}$$

has kernel $H^1(K^{(n)}, H^0(C_\infty, \mathcal{F})) = H^1(K^{(n)}, \mathcal{E}[p^\infty]^\pi)$. By Remark 2.4, the image of π_0 in $\mathrm{Aut}_{\mathbb{Z}_p}(\mathcal{E}[p^\infty])$ contains a finite-index subgroup of $\mathrm{SL}_2(\mathbb{Z}_p)$, which implies that $\mathcal{E}[p^\infty]^\pi$ is a finite group. It follows that $\ker \phi$ is also finite.

Now M_n is a G_k-submodule of $\mathcal{S}(C_n, \mathcal{E}[p^\infty])$. For each $g \in G_{\ell'}$, the image $(g - 1)M_n$ of the endomorphism $g - 1$ applied to M_n vanishes in $\mathcal{S}(C_\infty, \mathcal{E}[p^\infty])$, so it lies in the finite group $\ker \phi$. Since $(g - 1)M_n$ is also a quotient of a divisible group, it is trivial. We conclude that G_{ℓ_0} acts on M_n through its pro-p quotient $\mathrm{Gal}(\ell'/\ell_0)$. Moreover, since $\mathcal{E}(k^s(C_n))$ is a finite-rank $\mathbb{Z}$-module, the action of G_{ℓ_0} on M_n in fact factors through a finite p-group quotient. Call this group G_n.

Recall that, if M is a cofinitely generated $\mathbb{Z}_p$-module, we denote by $W(M)$ the $\mathbb{Q}_p$-module $\mathrm{Hom}(M, \mathbb{Q}_p/\mathbb{Z}_p) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$. Then $W(M_n)$ is a finite-dimensional $\mathbb{Q}_p$-representation of K_n which is

1225

a quotient of $W(S(C_n, \mathcal{E}[p^\infty]))$. Write r for $|N(\mathcal{E})| - 2\chi(C_0)$. Then, by Lemma 2.9, $W(M_n)$ is a quotient of $\mathbb{Q}_p[K_n]^r$. So $W(M_n)$ is isomorphic to $\sum_{i=0}^n \mathbb{Q}_p(\zeta_{p^i})^{a_i}$, where a generator of K_n acts on the ith factor via multiplication by ζ_{p^i}, and $a_i \leqslant r$. Now, because M_n is divisible, the map $G_n \to \operatorname{Aut}_{\Lambda(K)} W(M_n)$ is injective. However, $\operatorname{Aut}_{\Lambda(K)} W(M_n)$ is just a direct sum of matrix algebras $\bigoplus_{i=0}^n M_{a_i}(\mathbb{Q}_p(\zeta_{p^i}))$. A nonabelian representation of G_n has dimension at least p, so since $p > r$, we conclude that the image of G_n inside each matrix algebra is abelian, and so G_n itself is abelian.

Now take ℓ_n to be the field fixed by the kernel of the projection $G_{\ell_0} \to G_n$. Then taking ℓ to be the compositum of all of the ℓ_n yields the desired result. $\square$

Remark 4.3. It would be interesting to extend Proposition 4.1 to towers of curves with more general Galois group. In particular, the argument above suggests the following purely group-theoretic question. Let K be a pro-p p-adic Lie group with no p-torsion, and let M be a cofinitely generated $\Lambda(K)$-module carrying an action

$$H \hookrightarrow \operatorname{Aut}_{\Lambda(K)}(M)$$

with the property that the image of H in

$$\operatorname{Aut}_{\Lambda(K)}(M^N)$$

is finite for every open normal subgroup N of K. (For example, if K is abelian the action of K on M satisfies this condition.) Is it then the case that H fits into an exact sequence

$$1 \to N \to H \to H_0 \to 1$$

where H_0 is finite and N is a uniform pro-p group? If so, what more can we say about N?

We can now show that, if the Galois action on $\mathcal{S}(C_0, \mathcal{E}[p^\infty])$ has large image, the Mordell–Weil group $\mathcal{E}(k^s(C_\infty))$ is finitely generated.

THEOREM 4.4. *Define* $p, k, \{C_n\}, \mathcal{E}$ *as in the beginning of this section, and suppose* $p > |N(\mathcal{E})| - 2\chi(C_0)$.

Suppose also that, for every extension ℓ/k_∞ *which is an abelian pro-p extension of a finite extension of* k_∞, *no divisible subgroup of* $\mathcal{S}(C_0, \mathcal{E}[p^\infty])$ *is fixed by* $\operatorname{Gal}(k^s/\ell)$.

Then $\mathcal{E}(k^s(C_\infty))$ *is finitely generated.*

Remark 4.5. For notational simplicity, we say that a cofinitely generated $\mathbb{Z}_p$-module A with action of $\operatorname{Gal}(k^s/k_\infty)$ *has property* **L** if, for every ℓ/k_∞ which is an abelian pro-p extension of a finite extension of k_∞, no divisible subgroup of A is fixed by $\operatorname{Gal}(k^s/\ell)$. It is clear that property **L** is inherited by submodules; if $F \subset A$ is a finite submodule, and A has property **L**, then so does A/F. Finally, if $0 \to A \to B \to C$ is an exact sequence and A and C have property **L**, then so does B.

Remark 4.6. Note that Theorem 4.4 bounds the Mordell–Weil rank of $\mathcal{E}$ over a tower of function fields over a separably closed field, which is not possible using Corollary 3.2. On the other hand, Theorem 4.4 never applies in the interesting case where k is a finite field; and indeed, as the example of [Ulm02] shows, it is possible for $\mathcal{E}(k(C_\infty))$ to be infinitely generated in this case.

Proof. Choose ℓ to satisfy the conditions of Proposition 4.1, and define

$$M = (\mathcal{S}(C_\infty, \mathcal{E}[p^\infty]))^{\operatorname{Gal}(k^s/\ell)}.$$

The cokernel of the map

$$\mathcal{S}(C_0, \mathcal{E}[p^\infty]) \to \mathcal{S}(C_\infty, \mathcal{E}[p^\infty])^K \tag{7}$$

is a submodule of $H^2(K, \mathcal{E}[p^\infty]^\pi)$, which is trivial since K has p-cohomological dimension 1. The group $\mathcal{E}[p^\infty]^\pi$ is finite; this follows from the fact that π is a normal subgroup of π_0 with quotient

isomorphic to $\mathbb{Z}_p$, and that the image of π_0 in $\mathrm{Aut}(\mathcal{E}[p^\infty])$ contains a finite-index subgroup of $\mathrm{SL}_2(\mathbb{Z}_p)$ as in Remark 2.4. It follows that the kernel of (7) is finite. So $\mathcal{S}(C_\infty, \mathcal{E}[p^\infty])^K$ inherits property $\mathbf{L}$ from $\mathcal{S}(C_0, \mathcal{E}[p^\infty])$, which has property $\mathbf{L}$ by hypothesis. So

$$M^K = ((\mathcal{S}(C_\infty, \mathcal{E}[p^\infty]))^K)^{\mathrm{Gal}(k^s/\ell)}$$

is a finite group. By a standard fact of Iwasawa theory, a cofinitely generated $\Lambda(K)$-module with a finite group of K-invariants is cotorsion, and in particular has finite $\mathbb{Z}_p$-corank, which we denote by N. Since

$$\mathcal{S}(C_n, \mathcal{E}[p^\infty]) \to \mathcal{S}(C_\infty, \mathcal{E}[p^\infty])$$

has finite kernel, we have $\mathrm{corank}_{\mathbb{Z}_p} \mathcal{S}(C_n, \mathcal{E}[p^\infty])^{\mathrm{Gal}(k^s/\ell)} \leqslant N$ for all n; whence also

$$\mathrm{corank}_{\mathbb{Z}_p}(\mathcal{E}(k^s(C_n)) \otimes_{\mathbb{Z}} \mathbb{Q}_p/\mathbb{Z}_p)^{\mathrm{Gal}(k^s/\ell)}$$

is at most N. By hypothesis on ℓ,

$$(\mathcal{E}(k^s(C_n)) \otimes_{\mathbb{Z}} \mathbb{Q}_p/\mathbb{Z}_p)^{\mathrm{Gal}(k^s/\ell)} = \mathcal{E}(k^s(C_n)) \otimes_{\mathbb{Z}} \mathbb{Q}_p/\mathbb{Z}_p.$$

LEMMA 4.7. *Suppose the Mordell–Weil rank of $\mathcal{E}(k^s(C_n))$ is bounded independently of n. Then $\mathcal{E}(k^s(C_\infty))$ is finitely generated.*

Proof. Without loss of generality we may suppose that the rank of $\mathcal{E}(k^s(C_n))$ is equal to the rank of $\mathcal{E}(k^s(C_0))$ for all n. (If not, just replace C_0 with a curve farther up the tower.)

It suffices to show that there exists an integer M such that $M\mathcal{E}(k^s(C_n)) \in \mathcal{E}(k^s(C_0))$ for all n. Now an element P of $\mathcal{E}(k^s(C_n))$ gives rise to a class ζ in $H^1(K_n, \mathcal{E}(k^s(C_n))^{\mathrm{tors}})$ by the rule

$$\zeta(k) = P^k - P.$$

Since K_n is a p-group, we know that ζ lies in $H^1(K_n, \mathcal{E}(k^s(C_n))[p^\infty]) = H^1(K_n, \mathcal{E}[p^\infty]^{\pi_n})$. Let m be the order of the finite group $\mathcal{E}[p^\infty]^\pi$. Then m annihilates $H^1(K_n, \mathcal{E}(k^s(C_n))^{\mathrm{tors}})$. This means, in turn, that mP differs by a torsion element from an element of $\mathcal{E}(k^s(C_0))$. We are now finished as long as we can show that the torsion subgroup of $\mathcal{E}(k^s(C_\infty))$ is finite. We have already shown that the p-primary torsion is finite. Let q be a prime other than p and suppose that $\mathcal{E}(k^s(C_\infty))[q^\infty]$ is infinite. However, the image of K in the automorphism group of $\mathcal{E}(k^s(C_\infty))[q^\infty]$ must have finite image, since $q \neq p$; so this implies $\mathcal{E}(k^s(C_n))[q^\infty]$ is infinite for some n, which is impossible by the Mordell–Weil theorem. Taking $M = m|\mathcal{E}(k^s(C_\infty))^{\mathrm{tors}}|$, we are done. $\square$

The lemma yields the statement of the theorem. $\square$

5. Example: elliptic K3 surfaces

In this section we use Theorem 4.4 to show that there are many examples of elliptic curves over rational function fields $k(t)$ which have finite Mordell–Weil rank over $k^s(t^{p^{-\infty}})$.

We begin with some remarks on the relationship between Selmer groups of elliptic curves over function fields and the étale H^2 of the corresponding elliptic surfaces.

Let k be a field of characteristic prime to $6p$, let C/k^s be a smooth curve, and let $f : \mathcal{E} \to C$ be a non-isotrivial elliptic surface (i.e. a fibration whose generic fiber is an elliptic curve.)

Let $j : \eta \to C$ be the inclusion of the generic point, and write $\tilde{\mathcal{F}}$ for the sheaf $R^1 f_*(\mathbb{Q}_p/\mathbb{Z}_p)$ on C, so that $\mathcal{F} = j_* j^* \tilde{\mathcal{F}}$. Then the map

$$H^1(C, \tilde{\mathcal{F}}) \to H^1(C, \mathcal{F}) = \mathcal{S}(C, \mathcal{E}[p^\infty])$$

is surjective, since the kernel of $\tilde{\mathcal{F}} \to \mathcal{F}$ has zero-dimensional support.

The Leray spectral sequence yields an exact sequence

$$0 \to H^1(C, \mathbb{Q}_p/\mathbb{Z}_p) \to H^1(\mathcal{E}, \mathbb{Q}_p/\mathbb{Z}_p) \to H^0(C, \tilde{\mathcal{F}}) \to H^2(C, \mathbb{Q}_p/\mathbb{Z}_p) \to H^2(\mathcal{E}, \mathbb{Q}_p/\mathbb{Z}_p). \quad (8)$$

The image of the last map in $H^2(\mathcal{E}, \mathbb{Q}_p/\mathbb{Z}_p)$ is generated by the class of a fiber F of f in $\mathcal{E}$, which vanishes unless C is projective. Let M be the quotient of $H^2(\mathcal{E}, \mathbb{Q}_p/\mathbb{Z}_p)$ by the class of F. Then the Leray spectral sequence in degree 2 yields

$$0 \to H^1(C, \tilde{\mathcal{F}}) \to M \to H^0(C, R^2 f_*(\mathbb{Q}_p/\mathbb{Z}_p)) \to H^2(C, \tilde{\mathcal{F}}).$$

The group $H^2(C, \tilde{\mathcal{F}})$ is finite, so we find that

$$\mathrm{corank}_{\mathbb{Z}_p} H^1(C, \tilde{\mathcal{F}}) = \mathrm{corank}_{\mathbb{Z}_p} M - \mathrm{corank}_{\mathbb{Z}_p} H^0(C, R^2 f_*(\mathbb{Q}_p/\mathbb{Z}_p)).$$

The generic stalk of $R^2 f_*(\mathbb{Q}_p/\mathbb{Z}_p)$ has corank 1; the stalk of a fiber v of f with m_v irreducible components has corank m_v. So the corank of $H^0(C, R^2 f_*(\mathbb{Q}_p/\mathbb{Z}_p))$ is $1 + \sum_v (m_v - 1)$; we will use this fact later.

The composition

$$M \to H^0(C, R^2 f_*(\mathbb{Q}_p/\mathbb{Z}_p)) \to H^0(C, j_* j^* R^2 f_*(\mathbb{Q}_p/\mathbb{Z}_p)) = \mathbb{Q}_p/\mathbb{Z}_p$$

is the degree map; that is, the class of a one-dimensional subscheme of $\mathcal{E}$ is sent to its degree as a divisor on the elliptic curve $\mathcal{E}_{\overline{k(C)}}$. Denote by $G(\mathcal{E})$ the quotient of the space of degree-0 classes in $H^2(\mathcal{E}, \mathbb{Q}_p/\mathbb{Z}_p)$ by the class of F. Then $H^1(C, \tilde{\mathcal{F}})$ is a submodule of $G(\mathcal{E})$.

We can now prove the existence of many examples of elliptic surfaces meeting the conditions of Theorem 4.4.

We restrict our attention to elliptic K3 surfaces. From now on we restrict our attention to the case where k is a subfield of $\mathbb{C}$. For the basic facts used here, see [MO93, §3.2]. Suppose that $f : S \to \mathbb{P}^1$ is a minimal elliptic K3 surface over k; by minimal we mean there are no exceptional curves contained in the fibers of f. Let $\Sigma : \mathbb{P}^1 \to S$ be the zero section and F a fiber of f. Then the class $3F + \Sigma$ is a polarization of S of degree 4. The cohomology group $H^2(S(\mathbb{C}), \mathbb{Z})$ is isomorphic to $\mathbb{Z}^{22}$, and is endowed with a natural quadratic form Q by the intersection pairing. Let Γ' be the group of automorphisms of $H^2(S(\mathbb{C}), \mathbb{Z})$ which preserve Q and stabilize the classes F, Σ, and let Γ be a finite-index subgroup of Γ'.

Write $\bar{S}$ for $S \times_k \bar{k}$. For each $\alpha > 0$, denote by Γ_α the image of Γ in $\mathrm{Aut}(H^2(\bar{S}, \mathbb{Z}/p^\alpha \mathbb{Z}))$, and write Γ_p for the inverse limit of the Γ_α; so Γ_p is a closed subgroup of $\mathrm{Aut}(H^2(\bar{S}, \mathbb{Z}_p))$.

THEOREM 5.1. *Let $f : S \to \mathbb{P}^1$ be a minimal elliptic K3 surface over a field $k \subset \mathbb{C}$. Choose g in $k(t)$ and let p be a prime greater than $20 + 4 \deg(g)$. Let $E/k(t)$ be the generic fiber of f. Suppose that:*

- *the image of $\mathrm{Gal}(\bar{k}/k)$ in $\mathrm{Aut}(H^2(\bar{S}, \mathbb{Z}_p))$ contains Γ_p;*
- *the fiber S_t of f at t is an elliptic curve without complex multiplication whenever $t \in \mathbb{P}^1(\bar{k})$ is a zero or pole of g.*

Then the Mordell–Weil rank of E over $\bar{k}(g^{1/p^n})$ is bounded as $n \to \infty$.

Proof. Let $k_\infty = k(\zeta_{p^\infty})$. Then the image of $\mathrm{Gal}(\bar{k}/k_\infty)$ in $\mathrm{Aut}(H^2(\bar{S}, \mathbb{Z}_p))$ still contains a finite-index subgroup of Γ_p, since the determinant map sends Γ_p to a finite group.

Write H for the submodule of $H^2(\bar{S}, \mathbb{Z}_p)$ generated over $\mathbb{Z}_p$ by the classes of F and Σ. Then $\mathrm{Gal}(\bar{k}/k_\infty)$ acts irreducibly on $(H^2(\bar{S}, \mathbb{Z}_p)/H) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$. Let $F^\perp$ be the submodule of $H^2(\bar{S}, \mathbb{Z}_p)$ which is orthogonal to F, and let $F\mathbb{Z}_p$ be the submodule generated over $\mathbb{Z}_p$ by F. Since $F \cdot \Sigma = 1$, the map

$$F^\perp/F\mathbb{Z}_p \to H^2(\bar{S}, \mathbb{Z}_p)/H$$

1228

is an isomorphism. On the other hand, $\mathrm{Hom}(F^\perp/F\mathbb{Z}_p, \mathbb{Q}_p/\mathbb{Z}_p)$ is precisely the subquotient $G(\mathcal{E})$ of $H^2(\bar{S}, \mathbb{Q}_p/\mathbb{Z}_p)$ that we defined above. So $\mathrm{Gal}(\bar{k}/k_\infty)$ acts irreducibly on $G(\mathcal{E})$; more precisely, no nontrivial proper divisible subgroup of $G(\mathcal{E})$ is preserved by the Galois action.

Let k' be a finite Galois extension of k_∞. Then let $A \subset G(\mathcal{E})$ be the group generated by all divisible subgroups which are fixed by some $\mathrm{Gal}(\bar{k}/\ell)$, where ℓ varies over abelian extensions of k'. Clearly A is preserved by $\mathrm{Gal}(\bar{k}/k_\infty)$, so it is either trivial or all of $G(\mathcal{E})$. However, in the latter case, there would be some abelian extension ℓ/k' such that $\mathrm{Gal}(\bar{k}/\ell)$ acted trivially on $G(\mathcal{E})$; this is not the case, since Γ_p does not have an abelian subgroup of finite index. So A is trivial. We conclude that $G(\mathcal{E})$ has property **L**, whence so does its submodule $H^1(\mathbb{P}^1, \tilde{\mathcal{F}})$.

By the corank computation above,

$$\mathrm{corank}_{\mathbb{Z}_p} H^1(\mathbb{P}^1, \tilde{\mathcal{F}}) = 21 - \left(1 + \sum_v (m_v - 1)\right) = 20 - \sum_v (m_v - 1)$$

where m_v is the number of irreducible components of the fiber of f above v. However, this corank is equal to $|N(\mathcal{E})| - 2\chi(\mathbb{P}^1)$ (see, e.g., [Shi92, Proposition 1]), which is the corank of $H^1(\mathbb{P}^1, \mathcal{F})$ by Proposition 2.5. (In fact, it follows from the irreducibility of the Galois action on $G(\mathcal{E})$ that both coranks are 20, so that all fibers of f are irreducible.) We now know that the surjection $H^1(\mathbb{P}^1, \tilde{\mathcal{F}}) \to H^1(\mathbb{P}^1, \mathcal{F})$ has finite kernel; from this we may conclude that $H^1(\mathbb{P}^1, \mathcal{F})$ also has property **L** by Remark 4.5.

Now let $Z/\bar{k}$ be the scheme of zeroes and poles of g in $\mathbb{P}^1$, and let $C/\bar{k} = \mathbb{P}^1 - Z$. We then have an exact sequence

$$0 \to H^1(\mathbb{P}^1, \mathcal{F}) \to H^1(C, \mathcal{F}) \to H^0(Z, \mathcal{F}(-1)|Z) = \bigoplus_{t \in Z(\bar{k})} H^1(S_t, \mathbb{Q}_p/\mathbb{Z}_p(-1)).$$

Since the S_t are not CM by hypothesis, we know that $H^0(Z, \mathcal{F}(-1)|Z)$ has property **L**, whence so does $H^1(C, \mathcal{F}) = \mathcal{S}(C, \mathcal{E}[p^\infty])$. Plainly, the $\mathbb{Z}_p$-corank of $\mathcal{S}(C, \mathcal{E}[p^\infty])$ is at most $20 + 4\deg(g)$. We are now in the situation of Theorem 4.4, taking C_0 to be C and C_n the étale cover of C obtained by adjoining g^{1/p^n}. The desired conclusion follows. $\qquad\square$

We recall that if k is a field and V/k a variety, a subset of $V(k)$ is called *thin* if it is contained in $f(W(k))$ for some morphism $f : W \to V$ such that $\dim W \leqslant \dim V$ and f does not admit a k-rational section. We say k is *Hilbertian* if $\mathbb{P}^1(k)$ is not a thin subset of itself. Note that number fields are Hilbertian. See [Ser92, ch. 3] for more properties of these definitions.

COROLLARY 5.2. *Suppose that k is a Hilbertian subfield of $\mathbb{C}$, and let X be $\mathbb{P}^1_k$ parametrized by the variable t. Then there are infinitely many isomorphism classes of elliptic K3 surfaces $S \to X$ such that the Mordell–Weil rank of S over $\bar{k}(t^{1/p^n})$ is bounded as $n \to \infty$.*

Proof. By [MO93, Proposition 3.27], there is an open dense subset $U \subset \mathbb{P}^{27}$ parametrizing isomorphism classes of elliptic K3 surfaces: in particular, there is a map $S \to \mathbb{P}^1_U$ of U-schemes such that, for each $u \in U$, the fiber $S_u \to \mathbb{P}^1_u$ is an elliptic K3 surface. Let Γ be the image of the monodromy map

$$\pi_1(U(\mathbb{C}), u) \to \mathrm{Aut}(H^2(S_u(\mathbb{C}), \mathbb{Z})).$$

By [MO93, Theorem 3.2.10], Γ is a finite-index subgroup of Γ'. Pick some $\alpha \gg 0$ and recall that Γ_α denotes the image of Γ in $\mathrm{Aut}(H^2(S_u(\mathbb{C}), \mathbb{Z}/p^\alpha\mathbb{Z}))$. From the surjectivity of $\pi_1(U(\mathbb{C}), u) \to \Gamma_\alpha$ and the Hilbertianness of k, one knows that there are infinitely many points $x \in U(k)$ such that the image of $\mathrm{Gal}(\bar{k}/k)$ in $\mathrm{Aut}(H^2(\bar{S}_x, \mathbb{Z}/p^\alpha\mathbb{Z}))$ contains Γ_α. For some sufficiently large α, this implies that the image of $\mathrm{Gal}(\bar{k}/k)$ in $\mathrm{Aut}(H^2(\bar{S}_x, \mathbb{Z}_p))$ contains Γ_p (see, e.g., [Ell04, Lemma 3].) We can

reparametrize the base curve so that the fibers of S over zero and infinity are smooth elliptic curves without CM. Then by Theorem 5.1, if we consider S_x as an elliptic curve $E/k(t)$, then the rank of $E(\bar{k}(t^{1/p^n}))$ is bounded as n grows. $\qquad\square$

REFERENCES

Coa99   J. Coates, *Fragments of the* GL_2 *Iwasawa theory of elliptic curves without complex multiplication*, in *Arithmetic theory of elliptic curves*, Cetraro, 1997, Lecture Notes in Mathematics, vol. 1716 (Springer, Berlin, 1999), 1–50.

Ell04   J. Ellenberg, $K3$ *surfaces over number fields with geometric Picard number one*, in *Arithmetic of higher-dimensional algebraic varieties*, Palo Alto, CA, 2002, Progress in Mathematics, vol. 226, (Birkhäuser, Boston, MA, 2004), 135–140.

Fas97   L. Fastenberg, *Mordell–Weil groups in procyclic extensions of a function field*, Duke Math. J. **89** (1997), 217–224.

How02   S. Howson, *Euler characteristics as invariants of Iwasawa modules*, Proc. London Math. Soc. (3) **85** (2002), 634–658.

Iha86   Y. Ihara, *Profinite braid groups, Galois representations and complex multiplications*, Ann. of Math. (2) **123** (1986), 43–106.

Mil80   J. Milne, *Étale cohomology* (Princeton University Press, Princeton, NJ, 1980).

MO93   J. Morgan and K. O'Grady, *Differential topology of complex surfaces*, Lecture Notes in Mathematics, vol. 1545 (Springer, Berlin, 1993).

Pac05   A. Pacheco, *On the rank of abelian varieties over function fields*, Manuscripta Math. **118** (2005), 361–381.

Pac06   A. Pacheco, *Selmer groups of abelian varieties in extensions of function fields*, Preprint (2006), arXiv:math.NT/0601580.

Ser92   J.-P. Serre, *Topics in Galois theory*, Research Notes in Mathematics, vol. 1 (Jones and Bartlett, Boston, MA, 1992).

Shi86   T. Shioda, *An explicit algorithm for computing the Picard number of certain algebraic surfaces*, Amer. J. Math. **108** (1986), 415–432.

Shi92   T. Shioda, *Some remarks on elliptic curves over function fields*, Astérisque **209** (1992) 12, 99–114.

Sil00   J. Silverman, *A bound for the Mordell–Weil rank of an elliptic surface after a cyclic base extension*, J. Algebraic Geom. **9** (2000), 301–308.

Sil04   J. Silverman, *The rank of elliptic surfaces in unramified abelian towers*, J. reine. angew. Math. **577** (2004), 153–169.

Sti87   P. Stiller, *The Picard numbers of elliptic surfaces with many symmetries*, Pacific J. Math. **128** (1987), 157–189.

Ulm02   D. Ulmer, *Elliptic curves with large rank over function fields*, Ann. of Math. (2) **155** (2002), 295–315.

Ulm05   D. Ulmer, *Jacobi sums, Fermat Jacobians, and ranks of abelian varieties over towers of function fields*, Preprint (2005), http://math.arizona.edu/~ulmer/research/R3.pdf.

Jordan S. Ellenberg   ellenber@math.wisc.edu

Department of Mathematics, University of Wisconsin, Van Vleck Hall, 480 Lincoln Drive, Madison, WI 53706, USA