

ELLIPTIC CURVES AND FINITELY GENERATED GALOIS GROUPS

BO-HAE IM AND MICHAEL LARSEN

ABSTRACT. Let K be an extension of $\mathbb{Q}$ and A/K an elliptic curve. If $\text{Gal}(\bar{K}/K)$ is finitely generated, then A is of infinite rank over K . In particular, this implies the $g = 1$ case of the Junker-Koenigsmann conjecture.

This “anti-Mordellic” result follows from a new “Mordellic” theorem, which asserts that if K_0 is finitely generated over $\mathbb{Q}$, the points of an abelian variety A_0/K_0 over the compositum of all bounded-degree Galois extensions of K_0 form a virtually free abelian group. This, in turn, follows from a second Mordellic result, which asserts that the group of A_0 over the extension of K_0 defined by the torsion of $A_0(\bar{K}_0)$ is free modulo torsion.

1. INTRODUCTION

This paper proves the following theorem:

Theorem 1.1. Let A_0 be an elliptic curve over a finitely generated field K_0 of characteristic zero. Let $\sigma_1, \dots, \sigma_n$ be elements of the Galois group $G_{K_0} := \text{Gal}(\bar{K}_0/K_0)$. The rank of A_0 over the invariant field $\bar{K}_0^{\langle \sigma_1, \dots, \sigma_n \rangle}$ is infinite.

More generally, let A_0 be any non-trivial abelian variety over a finitely generated field K_0 of characteristic zero. Let $\sigma_1, \dots, \sigma_n$ be random elements of G_{K_0} , chosen independently and uniformly with respect to Haar measure. In 1974, Gerhard Frey and Moshe Jarden [FJ] proved that, with probability 1, the rank of A_0 over $\bar{K}_0^{\langle \sigma_1, \dots, \sigma_n \rangle}$ is infinite. In 2003, one of us [L1] asked whether this is, in fact, true for all choices of σ_i .

Conjecture 1.2. If A_0 is a non-trivial abelian variety over a finitely generated extension K_0 of $\mathbb{Q}$ and $\sigma_1, \dots, \sigma_n \in \text{Gal}(\bar{K}_0/K_0)$, then

$$\dim_{\mathbb{Q}} A_0(\bar{K}_0^{\langle \sigma_1, \dots, \sigma_n \rangle}) \otimes \mathbb{Q} = \infty.$$

If K is any field of characteristic zero such that G_K is (topologically) finitely generated and A is any non-trivial abelian variety over K , then

Bo-Hae Im was supported by the Basic Science Research Program through the National Research Foundation of Korea (NRF) grant funded by the Korean government (MSIT) (NRF-2023R1A2C1002385). Michael Larsen was partially supported by DMS-2401098 and the Simons Foundation.

there exists a finitely generated subfield K_0 of K and an abelian variety A_0/K_0 such that $A \cong A_0 \times_{\text{Spec } K_0} \text{Spec } K$. Moreover, choosing a finite set $\{\tau_1, \dots, \tau_n\}$ of generators of $\text{Gal}(\bar{K}/K)$, and restricting each τ_i to an automorphism σ_i of $\bar{K}_0$, Conjecture 1.2 would imply the vector space $A_0(\bar{K}_0^{(\sigma_1, \dots, \sigma_n)}) \otimes \mathbb{Q}$ is infinite-dimensional, so the same would be true for $A(K) \otimes \mathbb{Q}$, which contains a subspace isomorphic to $A_0(\bar{K}_0^{(\sigma_1, \dots, \sigma_n)}) \otimes \mathbb{Q}$. Conversely, if every non-trivial abelian variety over a characteristic zero field with finitely generated Galois group has infinite rank, applying this in the case of $K = \bar{K}_0^{(\sigma_1, \dots, \sigma_n)}$ would give Conjecture 1.2. So Conjecture 1.2 has this equivalent formulation:

Conjecture 1.3. If A is a non-trivial abelian variety over a field K of characteristic zero and G_K is finitely generated, then A has infinite rank over K .

Over the last twenty years, several variants of these conjectures have been considered in the literature, sometimes for all possible K and sometimes just for subfields of $\bar{\mathbb{Q}}$, sometimes but not always assuming $K_0 = \mathbb{Q}$, and sometimes but not always assuming A is an elliptic curve. A variety of different basic approaches have been tried (there is, of course, some overlap in methods). The difficulty in every case is locating points on $A_0(\bar{K}_0)$ over which one has enough control to guarantee invariance under all the σ_i . For a more detailed survey of previous work on this problem than is provided in the following brief summary, the reader could consult [IL3].

For the case that A_0/K_0 is an elliptic curve over $\mathbb{Q}$, one can exploit modularity and take advantage of Heegner points. This has been done in various cases [BI, Ha, I2] and most recently, by Bo-Hae Im and Seokhyun Choi, for all $(\sigma_1, \dots, \sigma_n)$ and all elliptic curves over $\mathbb{Q}$ [CI]. In a somewhat different arithmetic direction, Tim and Vladimir Dokchitser gave [DD] a proof for all elliptic curves over number fields which are not totally imaginary, conditional on the Birch-Swinnerton-Dyer conjecture.

A second approach to Conjecture 1.2 uses Diophantine geometry, the basic idea being to find rational curves on quotients of A_0^n in order to use their points over K_0 to construct points of $A_0(\bar{K}_0)$. Hilbert irreducibility plays a role in proving that the points so constructed span an infinite-dimensional space. The papers [I1, ILR, L1] all use this method. A fairly general result in this direction [IL1] is that in every dimension, Conjecture 1.3 holds for topologically cyclic fields K .

A third approach is via field arithmetic. The original paper [FJ] falls into this category. A 2010 conjecture of Markus Junker and Jochen Koenigsmann [JK] asserts that every characteristic zero field K with finitely generated Galois group is *ample*, meaning that every pointed non-singular curve over K has infinitely many K -points (see [BF] for a discussion of ample fields). Arno Fehm and Sebastian Petersen prove [FP] that if K is ample, then every non-trivial abelian variety over K has infinite rank.

A fourth approach comes from additive combinatorics. In [IL2], we use Ramsey-theoretic ideas to prove Conjecture 1.2 whenever A_0 is an elliptic curve containing an affine open of the form

$$(1.1) \quad v^2 = (u + c_0)(u + c_1)(u + c_2)(u + c_3),$$

or more briefly, $v^2 = f(u)$, where f is always understood in this paper to be a monic polynomial of degree 4 which splits completely into linear factors. This paper follows the method of [IL2] but eliminates this additional hypothesis, thereby proving the one-dimensional case of Conjecture 1.3.

As an immediate corollary of Theorem 1.1, we obtain the genus 1 case of the Junker-Koenigsmann conjecture, since every pointed non-singular curve of genus 1 over K is a cofinite subset of an elliptic curve over K .

The idea of our proof of Theorem 1.1 is as follows. Let L_0 be a finite Galois extension of K_0 such that the 2-torsion points of A_0 and at least one additional point are defined over L_0 . Over L_0 , there exists an affine open subset of A_0 of the form (1.1). As above, let $K = \bar{K}_0^{\langle \sigma_1, \dots, \sigma_n \rangle}$, and let $L = KL_0$. In §4, we use a Ramsey-theoretic argument to prove that there exists a finite set

$$\Sigma := \{a_i t + b_i \mid i = 1, 2, \dots, n\}$$

of non-constant linear functions in t , with $a_i, b_i \in L_0$, such that for all but finitely many $t_0 \in L_0$, there exists $u_0 \in \Sigma(t_0)$ such that $\pm \sqrt{f(u_0)} \in L$. Choose a square root v_0 , so $P := (u_0, v_0) \in A_0(L)$. Applying trace, we obtain

$$(1.2) \quad Q := \text{Tr}_{L/K} P \in A_0(K).$$

We would like to show that the set of points constructed in this way generates a group of infinite rank. Each point $P = (u_0, v_0)$ is defined over some quadratic extension of L_0 , so each point Q in (1.2) is defined over an extension of K_0 of bounded degree which is contained in K .

In §2, we use known results about the image of the representation of G_{K_0} on the adelic Tate module of A_0 to prove that if $(K_0)_{\text{tor}}$ denotes the extension of K_0 generated by all coordinates of points in $A_0(\bar{K}_0)_{\text{tor}}$, then the torsion-free part of $A_0((K_0)_{\text{tor}})$ is free. The Kummer theory of A_0 over $(K_0)_{\text{tor}}$ is simple to understand, and in §3, we use it to prove that the group of points of A_0 over any extension of K_0 generated by algebraic elements of bounded degree is the direct sum of a finite torsion group and a free group (which is usually of infinite rank). If $A_0(K) \otimes \mathbb{Q}$ were finite-dimensional, this would imply that the points Q constructed in (1.2) all lie in a finitely generated abelian group.

We remark that merely showing there exists some finite extension L/K for which we can construct an infinite subset of $A_0(L)$ is very easy. Finding such an extension and such a subset for which one can prove that the traces generate an infinite rank group is much more difficult. What is good about the combinatorial construction mentioned above is that the points it

produces behave in some sense as if they were of positive density, and this offers hope of proving the claim of infinite rank.

To implement this idea, in §5, we first use Chebotarev density to show that for any finite sequence $Q_1, Q_2, Q_3, \dots, Q_N$ of points of the form (1.2), there exists a specialization of A_0 to an elliptic curve $E/\mathbb{F}_p$ such that the subgroup of $E(\mathbb{F}_p)$ generated by the Q_i in the sequence is of arbitrarily large index in $E(\mathbb{F}_p)$. We then show that the proportion of elements of $E(\mathbb{F}_p)$ which can be represented by reducing points from (1.2) is bounded away from 0. Together these two facts imply that the group generated by points from (1.2) cannot be generated by any finite set, which finishes the proof.

2. KUMMER THEORY OF ABELIAN VARIETIES

In this section, we recall some facts about Galois representations associated to abelian varieties over finitely generated fields and use them to control the extent to which non-divisible points on an abelian variety over such a field may become divisible when the coordinates of torsion of the abelian variety are adjoined to that field. Most of what we do here is contained in the unpublished preprint [L2], but the argument is clarified by using more recent results. We remark that our results are close in spirit to those of Kenneth Ribet [Ri].

To avoid unnecessary subscripts, in this section and the next, we write K for K_0 , thus dropping the assumption that K has finitely generated absolute Galois group and assuming instead that it is finitely generated over $\mathbb{Q}$. We denote by A an abelian variety of dimension g over K (so A will be denoted A_0 in §5). For every rational prime ℓ and positive integer n , we denote by $A[\ell^n] \cong (\mathbb{Z}/\ell^n\mathbb{Z})^{2g}$ the kernel of multiplication by ℓ^n on $A(\bar{K})$, regarded as a module over G_K . We write $T_\ell \cong \mathbb{Z}_\ell^{2g}$ for the ℓ -adic Tate module of A , again regarded as a module over G_K . We denote by ρ_{ℓ^n} (respectively ρ_{ℓ^∞}) the homomorphism $G_K \rightarrow \text{Aut } A[\ell^n]$ (respectively $G_K \rightarrow \text{Aut } T_\ell$), by G_{ℓ^n} (resp. G_{ℓ^∞}) the image of the corresponding ρ and by K_{ℓ^n} (resp. K_{ℓ^∞}) the subfield of $\bar{K}$ associated to $\ker \rho_{\ell^n}$ (resp. $\ker \rho_{\ell^\infty}$). If S is a set of primes, we write K_S for the compositum of K_{ℓ^∞} , as ℓ ranges over S . By K_{tor} , we mean the field generated over K by all K_{ℓ^∞} , which can also be written K_S where S is the set of all primes.

We recall that a theorem of Fedor Bogomolov [Bo] states that if K is a number field, for all ℓ , the group C_{ℓ^∞} of homotheties in $\rho_{\ell^\infty}(G_K)$ is of finite index in $\mathbb{Z}_\ell^\times$. Jean-Pierre Serre observed that the result holds more generally for finitely generated K (see [S1, 2.2.5]) and that the index is bounded uniformly in ℓ :

Theorem 2.1. *If K is finitely generated over $\mathbb{Q}$, there exists c such that $[\mathbb{Z}_\ell^\times : C_{\ell^\infty}] \leq c$ for all ℓ .*

(See [S2, §2]) for a proof in the number field case and, e.g., [JJ, Lemma 3.4] for an explanation of how the general case follows from the number field case.)

By passing from K to a finite extension, we may assume that the fields K_{ℓ^∞} are *independent* in the sense that the Galois group of the compositum of the K_{ℓ^∞} over K is the product of the groups G_{ℓ^∞} . In the number field case, this is due to Serre [S3, Theorem 1], and in the general case to Anna Cadoret [Ca, Theorem 2.1].

Lemma 2.2. Let $C = \langle t \rangle$ be a cyclic group of order ℓ^n . If t acts on $M \cong (\mathbb{Z}/\ell^m\mathbb{Z})^r$ by a scalar $\gamma \not\equiv 1 \pmod{\ell^k}$ then for all $i \geq 0$, $H^i(C, M)$ is annihilated by ℓ^{k-1} .

Proof. Without loss of generality we may assume $r = 1$. For $i = 0$, the cohomology is the kernel of $1 - t$ acting on $\mathbb{Z}/\ell^m\mathbb{Z}$ this is cyclic and is killed by $1 - \gamma$ and by ℓ^m and therefore by ℓ^{k-1} . Therefore, the order of $H^0(C, M)$ divides ℓ^{k-1} , and it follows immediately that the order of the Tate cohomology group $\hat{H}^0(C, M)$ divides ℓ^{k-1} . As the Herbrand quotient of finite modules is 1, the same follows for $\hat{H}^1(C, M)$. By the periodicity of Tate cohomology for cyclic groups, it is true for all $\hat{H}^i(C, M)$, and it follows that ℓ^{k-1} annihilates all Tate cohomology and therefore also ordinary cohomology for $i \geq 1$. $\square$

Proposition 2.3. If $\ell > c + 1$, then any point $P \in A(K)$ which is divisible by ℓ in $A(K_{\ell^\infty})$ is divisible by ℓ in $A(K)$.

Proof. Let C_{ℓ^n} denote the image of C_{ℓ^∞} in G_{ℓ^n} . As C_{ℓ^∞} is of index $< \ell - 1$ in $\mathbb{Z}_\ell^\times$, it follows that C_{ℓ^n} is of index $< \ell - 1$ in $(\mathbb{Z}/\ell^n\mathbb{Z})^\times$. Therefore, any generator of C_{ℓ^n} acts on $A[\ell]$ by a scalar which is not 1. By Lemma 2.2, $H^i(C_{\ell^n}, A[\ell]) = 0$ for all $i \geq 0$.

Taking the cohomology sequence of the short exact sequence of G_{ℓ^n} -modules

$$0 \rightarrow A[\ell] \rightarrow A(K_{\ell^n}) \rightarrow \ell A(K_{\ell^n}) \rightarrow 0,$$

we conclude that every element of $A(K)$ which is divisible by ℓ in $A(K_{\ell^n})$ is divisible by ℓ in $A(K)$. Since this is true for all n , the proposition follows.

Proposition 2.4. Suppose the fields K_{p^∞} , as p ranges over the rational primes, are independent. If $\ell > c + 1$ then every element of $A(K)$ which is divisible by ℓ in $A(K_{\text{tor}})$ is divisible by ℓ in $A(K)$.

Proof. By Proposition 2.3, it suffices to prove that if $\ell \notin \{\ell_1, \dots, \ell_n\}$ and $P \in A(K)$ is divisible by ℓ in $A(K_{\{\ell, \ell_1, \dots, \ell_n\}})$, then P is divisible by ℓ in $A(K_{\ell^\infty})$. Fix P and choose $Q \in A(K_{\{\ell, \ell_1, \dots, \ell_m\}})$ such that $\ell Q = P$. As $Q \notin A(K_{\ell^\infty})$, we can pick $\tau \in \prod_{i=1}^n G_{\ell_i^\infty}$ so that $\tau(Q) \neq Q$. Let $T = \tau(Q) - Q \in A[\ell] \setminus \{0\}$ and $S = \sigma(Q) - Q \in A[\ell]$. Let $\sigma \in C_{\ell^\infty}$ reduce to a non-trivial scalar in G_ℓ , so $\sigma(T) \neq T$. As σ and τ commute,

$$(Q + S) + \sigma(T) = \sigma(Q + T) = \sigma\tau(Q) = \tau\sigma(Q) = \tau(Q + S) = (Q + T) + S,$$

contradicting the fact that $\sigma(T) \neq T$. $\square$

Proposition 2.5. Suppose the fields K_{p^∞} , as p ranges over rational primes, are independent. Then for any ℓ there exists k such that any $P \in A(K)$ which is not divisible by ℓ in $A(K) + A(\bar{K})_{\text{tor}}$ is not divisible by ℓ^k in $A(K_{\text{tor}})$.

Proof. This is essentially a repetition of the proofs of Propositions 2.3 and 2.4, working modulo a suitable power of ℓ . However, we need to be slightly more careful because an extension of two groups killed by ℓ^{m-1} need not be killed by ℓ^{m-1} but only by $\ell^{2(m-1)}$; also, C_{2^n} need not be cyclic.

For odd ℓ , we choose m so that $c < \ell^{m-1}(\ell - 1)$, so that for $n \geq 2m$, a generator $t \in C_{\ell^n}$ acts on $A[\ell^{2m}]$ by some scalar $a \not\equiv 1 \pmod{\ell^m}$. If $\ell = 2$, by abuse of notation, we replace C_{2^n} for all n by a cyclic subgroup of index ≤ 2 and choose m large enough that for all $n \geq 2m$, so any generator t of C_{2^n} acts on $A[2^{2m}]$ by some scalar $\gamma \not\equiv 1 \pmod{2^m}$. By Lemma 2.2, $H^i(C_{\ell^n}, A[\ell^{2m}])$ is annihilated by ℓ^{m-1} .

We first suppose that P is divisible by ℓ^{2m} in $A(K_{\ell^n})$ for some $n \geq 2m$. By the inflation-restriction sequence

$$0 \rightarrow H^1(G_{\ell^n}/C_{\ell^n}, A[\ell^{2m}])^{C_{\ell^n}} \rightarrow H^1(G_{\ell^n}, A[\ell^{2m}]) \rightarrow H^1(C_{\ell^n}, A[\ell^{2m}])^{G_{\ell^n}/C_{\ell^n}},$$

so $H^1(G_{\ell^n}, A[\ell^{2m}])$ is annihilated by ℓ^{2m-2} . By the cohomology sequence of

$$0 \rightarrow A[\ell^{2m}] \rightarrow A(K_{\ell^n}) \rightarrow \ell^{2m} A(K_{\ell^{2m}}) \rightarrow 0,$$

every element $P \in A(K)$ which is divisible by ℓ^{2m} in $A(K_{\ell^n})$ has the property that $\ell^{2m-2}P$ is divisible by ℓ^{2m} in $A(K)$. This means that P is divisible by ℓ in $A(K) + A(\bar{K})_{\text{tor}}$, contrary to assumption.

Therefore, setting $k = 3m$, P cannot be divisible by ℓ^k in $A(K_{\ell^\infty})$. Suppose, nevertheless, there exists $Q \in A(K_{\text{tor}})$ such that $\ell^k Q = P$. As P is not divisible by ℓ^{2m} in $A(K_{\ell^\infty})$, there exists $\tau \in \prod_{i=1}^n G_{\ell_i^\infty}$ such that $T := \tau(Q) - Q$ is not killed by ℓ^m . It follows that there exists $\sigma \in C_{\ell^\infty} \subset G_{\ell^\infty}$ such that $\sigma(T) \neq T$. The proof now finishes as before. $\square$

Lemma 2.6. Let V be a vector space over $\mathbb{Q}$, $\Lambda \subset V$ a subgroup and $V_1 \subset V_2 \subset V_3 \subset \dots$ a chain of finite-dimensional subspaces with union V . If $\Lambda \cap V_i$ is free abelian for all i , then Λ is free abelian.

Proof. Let $\Lambda_0 = 0$ and $\Lambda_n = \Lambda \cap V_n$ for $n > 0$. Then Λ_{n+1}/Λ_n is finitely generated and torsion-free and therefore free. It therefore lifts to a free subgroup M_{n+1} of Λ_{n+1} . It follows that $\Lambda = \bigoplus_{n \geq 0} M_{n+1}$ is free. $\square$

Theorem 2.7. Let K be a finitely generated extension of $\mathbb{Q}$ and A/K an abelian variety of dimension $g \geq 1$. Then $A(K)$ is the direct sum of its torsion subgroup $A(K)_{\text{tor}} \cong (\mathbb{Q}/\mathbb{Z})^{2g}$ and a free abelian group.

Proof. Without loss of generality, we may assume the K_{ℓ^∞} are independent. Let $K \subset K_1 \subset K_2 \subset \dots$ be a chain of finite extensions of K in K_{tor} such that for each i , the $(K_i)_{\ell^\infty}$ are independent and $\bigcup_i K_i = K_{\text{tor}}$. Let

$V = A(K_{\text{tor}}) \otimes \mathbb{Q}$, $V_i = A(K_i) \otimes \mathbb{Q}$, and $\Lambda = A(K_{\text{tor}}) \otimes 1$. Thus $\Lambda \cap V_i$ is the set of $P \otimes 1$, where $P \in A(K_{\text{tor}})$ and some positive integer multiple kP satisfies $kP \otimes 1 \in A(K_i) \otimes 1$. By Propositions 2.3 and 2.5, for each i , k can be taken to divide some fixed positive integer N_i depending on i . By Néron's generalization [Ln, Chapter 6, Theorem 1] of the Mordell-Weil theorem, $A(K_i)$ is finitely generated, so $A(K_i) \otimes 1$ is free abelian, and the same is therefore true of $\Lambda \cap V_i \subset A(K_i) \otimes 1/N_i$. The theorem follows from Lemma 2.6. $\square$

$\square$

3. SILVERMAN'S LEMMA AND THE MORDELL-WEIL-NÉRON THEOREM

Silverman proves [Si, Lemma] that if K is a number field, d is a positive integer, and A is an elliptic curve over K then there is an upper bound on the order of $A(K')_{\text{tor}}$ as K' ranges over extensions of K of degree $\leq d$. In [IL2, Proposition 6], this is extended to higher dimensional abelian varieties A and arbitrary finitely generated fields K .

The main result of this section is the following result, which can be regarded as a simultaneous generalization of this extension of Silverman's result and Néron's extension of the Mordell-Weil theorem to finitely generated fields of characteristic zero. For any field K and any positive integer d , let $K(d)$ denote the subfield of $\bar{K}$ over K generated by all K' , $K \subset K' \subset \bar{K}$, with $[K' : K] \leq d$.

Theorem 3.1. If K is finitely generated over $\mathbb{Q}$, d is a positive integer, and A is an abelian variety over K , then $A(K(d))$ is virtually free.

This is equivalent to saying that $A(K(d))_{\text{tor}}$ is finite and $A(K(d))/A(K(d))_{\text{tor}}$ is free abelian. We begin with the first part, for which we use the following two group-theoretic propositions:

Proposition 3.2. For all integers k there exists an integer M such that no elementary abelian group of rank M is isomorphic to a quotient G/H of any closed subgroup G of $\text{GL}_k(\mathbb{Z}_\ell)$, for any ℓ , by any open normal subgroup H of G .

Proof. For any (topological) group G , we denote by $d(G)$ the minimum number of (topological) generators of G . If H is an (open) normal subgroup of G , then the union of any generating set of H and any set of representatives for a generating set of G/H necessarily generates G , so $d(G) \leq d(H) + d(G/H)$. Moreover, $d(G) \geq d(G/H)$, since the image of a generating set under a surjective homomorphism is always generating.

Let $U \subset \text{GL}_k(\mathbb{Z}_\ell)$ denote the matrices congruent to 1 (mod ℓ) if ℓ is odd and the matrices congruent to 1 (mod 4) if $\ell = 2$. By [DDMS, Theorem 5.2], U is a powerful pro- ℓ group, and $d(U) = k^2$. By [DDMS, Theorem 3.8], $d(H \cap U) \leq k^2$. If ℓ is odd, $H/H \cap U$ is isomorphic to a subgroup of $\text{GL}_k(\mathbb{F}_\ell)$.

By [LS, Theorem 16.4.15], for all finite groups $\bar{G}$, $d(\bar{G}) \leq 1 + \max_p d(\bar{G}_p)$, where $\bar{G}_p$ is a Sylow p -subgroup. Every ℓ -Sylow subgroup $\bar{G}_\ell$ of a subgroup $\bar{G}$ of $\mathrm{GL}_k(\mathbb{F}_\ell)$ is contained in an ℓ -Sylow of $\mathrm{GL}_k(\mathbb{F}_\ell)$ and therefore satisfies $d(\bar{G}_\ell) \leq \frac{k(k-1)}{2}$. Every p -Sylow subgroup of $\bar{G} \subset \mathrm{GL}_k(\mathbb{F}_\ell)$ for $p \neq \ell$ embeds in $\mathrm{GL}_k(\mathbb{C})$. By Jordan's theorem, it has a diagonal normal subgroup of bounded index, and any finite diagonal subgroup of $\mathrm{GL}_k(\mathbb{C})$ can be generated by k elements, so $d(\bar{G}_p)$ is bounded in terms of k . Defining $\bar{G} := G/(U \cap G)$, which is a subgroup of $\mathrm{GL}_k(\mathbb{F}_\ell)$ if ℓ is odd or a subgroup of $\mathrm{GL}_k(\mathbb{F}_2)$ if $\ell = 2$, we conclude that $d(G)$ is bounded above by a quantity depending only on k . Therefore, any continuous homomorphism from G to an elementary abelian group has image of bounded rank. $\square$

Proposition 3.3. Let h and k be fixed positive integers. There exists N such that if there exists a prime p , a closed subgroup G of $\mathrm{GL}_k(\mathbb{Z}_p)$, a finite sequence $H_1, \dots, H_n$ of groups of order $\leq h$, and a continuous surjective homomorphism from G to a subquotient H of $H_1 \times \dots \times H_n$, then $|H| \leq N$.

Proof. The hypothesis on H gives an upper bound on the largest prime factor which can divide $|H|$, from which one deduces that as $|H| \rightarrow \infty$, the order of the largest Sylow subgroup of H likewise diverges. By a theorem of Burnside [Bu], this implies that the largest abelian subgroup of the largest Sylow subgroup likewise goes to infinity in order, and since the exponent of H is bounded, the same is true of the rank of the largest elementary abelian subgroup of H . Since the inverse image of an elementary abelian subgroup of H in G is again a closed subgroup of $\mathrm{GL}_k(\mathbb{Z}_p)$, the proposition follows from Proposition 3.2. $\square$

Proposition 3.4. If A/K is an abelian variety over a finitely generated extension of $\mathbb{Q}$ and d is a positive integer, then $A(K(d))_{\mathrm{tor}}$ is finite.

Proof. Let $K_1, K_2, \dots$ be an ordering of the sequence of subfields of $\bar{K}$ which are extensions of K of degree d . For each such K_i , the action of G_K permutes the set of embeddings of K_i in $\bar{K}$ as extensions of K , and this gives a permutation representation of degree $\leq d$, so there exists a homomorphism $\sigma_i: G_K \rightarrow \mathrm{S}_d$ whose kernel is contained in G_{K_i} . As $G_{K(d)}$ is the intersection of all open subgroups of G_K of index $\leq d$, we can identify it with the kernel of the homomorphism $G_K \rightarrow \prod_i \mathrm{S}_d$ given by $(\sigma_1, \sigma_2, \dots)$.

Suppose that there are infinitely many elements of $A(\bar{K})_{\mathrm{tor}}$ fixed by $G_{K(d)}$. Then there are infinitely many such elements of prime power order. Each such element is in fact fixed by a finite intersection of subgroups of the form $\ker \sigma_i$ for permutation representations σ_i of bounded degree. The fixed field of such an intersection has a Galois group which is a product of groups H_i of bounded order, so the Galois group of the intersection of the fixed field with K_{ℓ^∞} is a subquotient of such a product of H_i . Since it is also a quotient of G_{ℓ^∞} , by Proposition 3.3, it is of bounded degree over K . By [IL2, Proposition 6], this gives an upper bound for degree of ℓ -power torsion

in $A(K(d))$ for each ℓ , and that, in turn, gives an upper bound for all torsion in $A(K(d))$. $\square$

If W is any subspace of $A(\bar{K}) \otimes \mathbb{Q}$, we define $A(K)_W$ to be the intersection of W with $A(K) \otimes 1$.

Proposition 3.5. If K is any finitely generated field, $W = A(K) \otimes \mathbb{Q}$, and d is a positive integer, then $A(K_{\text{tor}}(d))_W$ is finitely generated.

Proof. Let $\Lambda = A(K_{\text{tor}})_W$ and $\Lambda' = A(K_{\text{tor}}(d))_W$. By Theorem 2.7, Λ is a free abelian group of finite rank. Since $\Lambda \subset \Lambda' \subset W$, it suffices to prove that Λ'/Λ is annihilated by some positive integer.

Let $\ell > n$ be a prime. We claim that Λ'/Λ has no element of order divisible by ℓ . Indeed, suppose Q belongs to $A(K_{\text{tor}}(d))$ but not to $A(K_{\text{tor}})$ and $\ell Q \in A(K_{\text{tor}})$. There exists a finite sequence of Galois extensions K_{tor}^i of K_{tor} with $\text{Gal}(K_{\text{tor}}^i/K_{\text{tor}})$ contained in the symmetric group S_d , such that Q is defined over $K_{\text{tor}}^{[1,N]} := \prod_{i=1}^N K_{\text{tor}}^i$. If $G = \text{Gal}(K_{\text{tor}}^{[1,N]}/K_{\text{tor}})$, then G embeds as a subgroup of S_d^N .

Consider the cohomology sequence of the short exact sequence of G -modules

$$(3.1) \quad 0 \rightarrow A[\ell] \rightarrow A[\ell] + \mathbb{Z}Q \xrightarrow{\ell} \ell\mathbb{Z}Q \rightarrow 0.$$

By definition, all torsion points of A are defined over K_{tor} , so G acts trivially on $A[\ell]$, so $H^1(G, A[\ell]) = \text{Hom}(G, A[\ell])$. However, ℓ is prime to the $(d!)^N$ and therefore to the order of G , so this cohomology group vanishes. By the cohomology sequence of (3.1), $\ell Q \in H^0(G, \ell\mathbb{Z}Q)$ lifts to some element of $H^0(G, A[\ell] + \mathbb{Z}Q)$, which must be a G -invariant element of $Q + A[\ell]$. Since $Q + A[\ell]$ means $A(K_{\text{tor}})$, $Q \in A(K_{\text{tor}})$, contrary to assumption.

Finally, for $\ell \leq d$, it suffices to prove that there exists m such that the order of an element of Λ'/Λ cannot be divisible by ℓ^m . We choose m such that ℓ^m does not divide $d!$. This implies that no element of S_d^N has order divisible by ℓ^m . Proceeding as before, choosing $Q \in A(K_{\text{tor}}(d))$ with $\ell^m Q \in A(K_{\text{tor}})$ and considering the sequence of G -modules

$$0 \rightarrow A[\ell^m] \rightarrow A[\ell^m] + \mathbb{Z}Q \xrightarrow{\ell^m} \ell^m\mathbb{Z}Q \rightarrow 0,$$

We claim that the image of every homomorphism $G \rightarrow A[\ell^m]$ lies in $\ell A[\ell^m]$, and this implies that $\ell^{m-1}Q$ lies in $A(K_{\text{tor}})$, contrary to assumption. $\square$

We can now prove Theorem 3.1.

Proof. As every extension of K of degree $\leq d$ is contained in an extension of K_{tor} of degree $\leq d$, by Proposition 3.5, we have that $A(K(d))_W \subset A(K_{\text{tor}}(d))_W$ is finitely generated. By Lemma 2.6, $A(K(d)) \otimes 1$ is free abelian.

The short exact sequence

$$0 \rightarrow A(K(d))_{\text{tor}} \rightarrow A(K(d)) \rightarrow A(K(d)) \otimes 1 \rightarrow 0$$

implies

$$A(K(d)) \cong A(K(d)) \otimes 1 \oplus A(K(d))_{\text{tor}}.$$

By Proposition 3.4, $A(K(d))_{\text{tor}}$ is finite, so $A(K(d))$ is virtually abelian. $\square$

4. THE HALES-JEWETT CONSTRUCTION

In this section, we recall how the Hales-Jewett Theorem [HJ] can be used to construct points on $A(L)$ when G_L is finitely generated and $A(L)$ contains all points of $A[2]$ and at least one other point P_0 . The reference for this material is [IL2] (note that Corollary 9 in that paper implicitly assumes the existence of P_0).

If S is a finite set, an S -coloring of a set X will mean a function $X \rightarrow S$. A subset $Y \subset X$ is *monochromatic* if the function is constant on Y . As G_L is finitely generated,

$$L^\times / L^{\times 2} \cong \text{Hom}(G_L, \{\pm 1\})$$

is finite. We identify the set S of colors with elements of $L^\times / L^{\times 2}$ and denote by $[l] \in S$ the class of any $l \in L^\times$. Multiplication by any element of $L^\times$ takes any monochromatic subset of $L^\times$ to another monochromatic subset.

If $A(L)$ contain $A[2]$ as well as some $P_0 \notin A[2]$, then A has an affine open set of the form $y^2 = (x - e_1)(x - e_2)(x - e_3)$ with $e_i \in L$ which contains some (x_0, y_0) , with $y_0 \neq 0$. Translating x by $-x_0$, we may assume $x_0 = 0$, so $y_0^2 = -e_1 e_2 e_3$. The functions

$$u = -\frac{1}{x}, \quad v = \frac{y}{y_0 x^2},$$

satisfy equation (1.1), where

$$c_0 := 0, \quad c_i := \frac{1}{e_i}, \quad i = 1, 2, 3.$$

Any 4-term sequence in $L^\times$ whose consecutive differences are $c_1 - c_0, c_2 - c_1$, and $c_3 - c_2$ can be expressed as $u + c_0, u + c_1, u + c_2, u + c_3$ for some value of u ; if such a sequence is monochromatic, the product of its terms is a perfect square in L , so the sequence determines a pair of points in $A(L)$. More generally, any monochromatic 4-term sequence in $L^\times$ whose consecutive differences are in ratio $c_1 - c_0 : c_2 - c_1 : c_3 - c_2$ determines a pair of points of $A(L)$.

Let $Z := \{0, 1, 2, 3\}$. For any finite sequence $b_1, b_2, \dots, b_N \in L$, and any $l \in L$, we define a function $\xi: Z^N \rightarrow L$ by

$$(4.1) \quad \xi(i_1, \dots, i_N) = l + \sum_{j=1}^N b_j c_{i_j}.$$

We assume no non-empty subsequence of $b_1, \dots, b_N$ sums to 0. We regard this sequence as fixed, so for all but finitely many values of l , the image of ξ lies in $L^\times$, and ξ therefore defines an S -coloring of Z^N .

A *combinatorial line* in Z^N is a subset of the form $\{\vec{v}, \vec{v} + \vec{w}, \vec{v} + 2\vec{w}, \vec{v} + 3\vec{w}\}$ with $\vec{v} = (v_1, \dots, v_N) \in Z^N$, $\vec{w} = (w_1, \dots, w_N) \in \{0, 1\}^N$, and $w_i \neq 0$ for some i . (Of course, when $w_i = 1$, we must have $v_i = 0$ in order for $\{v, v + \vec{w}, v + 2\vec{w}, v + 3\vec{w}\}$ to be contained in Z^N .) Restricting ξ to the combinatorial line $\{v, v + \vec{w}, v + 2\vec{w}, v + 3\vec{w}\}$, the sequence of values of (4.1) is

$$l + r_{\vec{v}}, l + r_{\vec{v}} + s_{\vec{w}}c_1, l + r_{\vec{v}} + s_{\vec{w}}c_2, l + r_{\vec{v}} + s_{\vec{w}}c_3$$

where

$$r_{\vec{v}} = \sum_{\{j|w_j=0\}} b_j c_{v_j}, \quad s_{\vec{w}} = \sum_{\{ij|w_j=1\}} b_j \neq 0.$$

The ratios between successive terms in this sequence are, as desired, $c_1 - c_0$, $c_2 - c_1$, and $c_3 - c_2$. Indeed, if the sequence above is monochromatic, there exist a pair of points $(u, \pm v) \in A(L)$, where

$$u = \frac{l + r_{\vec{v}}}{s_{\vec{w}}}.$$

A special case of the Hales-Jewett Theorem asserts

Theorem 4.1. For all n there exists N such that for every coloring of Z^N by an n -element set, there exists a monochromatic combinatorial line.

This theorem now implies:

Theorem 4.2. There exists a finite collection of linear functions in t with coefficients in L such that for all but finitely many $t_0 \in L$, at least one of these functions, evaluated at t_0 , gives the u -coordinate of a point on $A(L)$.

5. THE CHEBOTAREV DENSITY THEOREM

In this section, we use the Chebotarev density theorem for schemes over $\mathbb{Z}$ to complete the proof of the main theorem. Throughout the section, K_0 will be a finitely generated extension of $\mathbb{Q}$, K will be K_0 -subextension of $\bar{K}_0$ with finitely generated Galois group, and A_0 will be an elliptic curve over K_0 . There exists a finite Galois extension L_0/K_0 such that $A_0[2]$ and at least one other point $P_0 \in A_0(\bar{K}_0)$ are defined over K_0 .

Throughout this section, a barred expression such as $\bar{u}_i$ can mean either an element of a finite field or the reduction (mod $\mathfrak{m}$) of an element (in this case, u_i) of a finitely generated $\mathbb{Z}$ -algebra. The distinction should not cause confusion.

Lemma 5.1. Let $\bar{f}(u) \in \mathbb{F}_p[u]$ be a polynomial which is not the square of a polynomial in $\bar{\mathbb{F}}_p[u]$. For $i = 1, 2, \dots, n$, let $\bar{a}_i \in \mathbb{F}_p^\times$ and $\bar{b}_i \in \mathbb{F}_p$. There exists $\epsilon > 0$, depending only on the degree of $\bar{f}(u)$ and on n such that the number of $\bar{u}_0 \in \mathbb{F}_p$ such that $f(\bar{a}_i \bar{u}_0 + \bar{b}_i) \in \mathbb{F}_p^{\times 2}$ for all i is greater than ϵp if p is sufficiently large.

Proof. We choose any $\epsilon < 2^{-n}$. The genus of the projective non-singular curve X with function field

$$\mathbb{F}_p(u, \sqrt{a_1 u + b_1}, \dots, \sqrt{a_n u + b_n}),$$

can be bounded, using the Riemann-Hurwitz theorem, in terms of n and $\deg(\bar{f})$. By the Riemann hypothesis for curves over finite fields, the number of $\mathbb{F}_p$ -points on X is $(1 + o(1))p$. Now X admits a cover of the projective line of degree $2^d \leq 2^n$ such that every $\bar{u}_0 \in \mathbb{F}_p$ which is not in the ramification locus of $X \rightarrow \mathbb{P}^1$ satisfies the stated condition if and only if the preimage of $\bar{u}_0$ consists of 2^d points defined over $\mathbb{F}_p$. The lemma follows. $\square$

Now we consider all elliptic curves $E/\mathbb{F}_p$ where E has an open affine curve U of the form $v^2 = \bar{f}(u)$, for a monic polynomial $\bar{f}$ of degree 4. We assume, for some positive integer m , that all the m -torsion points of E are defined over $\mathbb{F}_p$. We fix k n -term sequences $\Sigma_1, \dots, \Sigma_k$, each consisting of non-constant linear functions in u . We say ordered k -tuples $(\bar{u}_1, \dots, \bar{u}_k) \in \mathbb{F}_p^k$ and $(P_1, \dots, P_k) \in U(\mathbb{F}_p)^k$ are *compatible* if for each positive integer $j \leq k$, the u -coordinate of P_j lies in the sequence $\Sigma_j(\bar{u}_j)$.

Proposition 5.2. Given k and n as above, if m is sufficiently large and p is sufficiently large in terms of m , then if $\bar{f}(u)$ and $\Sigma_1, \dots, \Sigma_k$ are as above, there exist $(\bar{u}_1, \dots, \bar{u}_k) \in \mathbb{F}_p^k$ such that for all compatible choices $(P_1, \dots, P_k) \in U(\mathbb{F}_p)^k$, the sum of any non-empty subsequence of $P_1, \dots, P_k$ is not in $mE(\mathbb{F}_p)$.

Proof. By Lemma 5.1, the number of k -tuples $(\bar{u}_1, \dots, \bar{u}_k) \in \mathbb{F}_p^k$ such that for each j , $\Sigma_j(\bar{u}_j)$ consists entirely of elements of $\mathbb{F}_p^{\times 2}$, is at least $(\epsilon p)^k$, where $\epsilon > 0$ depends only on n . For each such k -tuple, there exist at least 2^k compatible k -tuples $(P_1, \dots, P_k) \in U(\mathbb{F}_p)^k$. In total, therefore, there are at least $(2\epsilon)^k p^k$ ways of choosing compatible k -tuples $(\bar{u}_1, \dots, \bar{u}_k)$ and $(P_1, \dots, P_k)$.

We claim there exists a bound N , depending only on n and k , such that if p is sufficiently large, for each $Q \in E(\mathbb{F}_p)$ the number of ways in which $(\bar{u}_1, \dots, \bar{u}_k)$ and $(P_1, \dots, P_k)$ can be chosen compatibly with some non-empty subsequence of the P_i adding to Q is at most Np^{k-1} . Assuming such a bound exists, the number of ways of choosing $(\bar{u}_1, \dots, \bar{u}_k)$ and $(P_1, \dots, P_k)$ compatibly with some subsequence of the P_i summing to an element of $mE(\mathbb{F}_p)$ is bounded above by

$$Np^{k-1}|mE(\mathbb{F}_p)| = (1 + o(1)) \frac{Np^k}{m^2}.$$

Assuming m is chosen such that $m^2 > N/(2\epsilon)^k$, then if p is sufficiently large, there must be some choice of $(\bar{u}_1, \dots, \bar{u}_k)$ for which for all compatible choices of $(P_1, \dots, P_k)$, no non-empty subsequence of $P_1, \dots, P_k$ sums to any element of $mE(\mathbb{F}_p)$.

To find such an N , we note that for each Q , the number of ways of choosing $(P_1, \dots, P_k) \in E(\mathbb{F}_p)^k$ such that any particular subsequence of the P_i sums to Q is $|E(\mathbb{F}_p)|^{k-1}$, which is $(1 + o(1))p^{k-1}$. For each choice of P_j , there are at most n ways of choosing $\bar{u}_j$ compatibly, since one of the n terms in the sequence Σ_j must evaluate at $\bar{u}_j$ to the $\bar{u}$ -coordinate of P_j . Therefore, any value of N greater than $(2^k - 1)n^k$ suffices. $\square$

Finally, we prove Theorem 1.1.

Proof. Given A/K , we can find a finitely generated extension K_0 of $\mathbb{Q}$ and an elliptic curve A_0/K_0 such that $A_0 \times_{\text{Spec } K_0} \text{Spec } K \cong A$. Choose a finite Galois extension L_0/K_0 such that all the 2-torsion of A_0 is rational over L_0 . Let $L = KL_0$. Its absolute Galois group, G_L , is of finite index in G_K and therefore topologically finitely generated. There is an affine open subvariety of A_0 given by the equation (1.1).

Applying Theorem 4.2, we obtain, for some n , a sequence of n non-constant linear functions $a_i t + b_i$ in L_0 such that for all but finitely many $t_0 \in L_0$, one of these linear expressions, evaluated at t_0 , gives the u -coordinate of a point (u_i, v_i) on (1.1), defined over some quadratic extension of L_0 and contained in L . We can express $\text{Tr}_{L/K}(u_i, v_i) \in A(K)$ as a sum

$$(5.1) \quad \sum_{\sigma \in \text{Gal}(L/K)} (\sigma(u_i), v_{i,\sigma}),$$

where $v_{i,\sigma}$ is the v -coordinate of some point on (1.1) with u -coordinate $\sigma(u_i)$.

Our goal is to prove that the resulting set of points generates an infinite-dimensional subspace of $A(K) \otimes \mathbb{Q}$. We know that all such points lie in $A(L_0(2))$, so by Theorem 3.1, they generate a subgroup of a virtually free abelian group, which is then also, necessarily, virtually free. If the group they generate spans a finite-dimensional subspace of $A(K) \otimes \mathbb{Q}$, then this group is finitely generated.

Suppose, indeed, that $Q_1, \dots, Q_r$ denotes a finite sequence of elements of type (5.1) which generates the group of all such elements. We define m as in Proposition 5.2. Let M_0 denote a finite Galois extension of K_0 which contains L_0 and such that all points on $A_0(\bar{K}_0)$ of order m and all points $Q' \in A_0(\bar{K}_0)$ such that $mQ' \in \{Q_1, \dots, Q_r\}$ are defined over M_0 .

We choose an integral domain R_0 , finitely generated as a $\mathbb{Z}$ -algebra, such that the field of fractions of R_0 can be identified with K_0 . Let S_0 denote the integral closure of R_0 in M_0 , which is a finitely generated module over R_0 . Replacing R_0 and S_0 by $R_0[h^{-1}]$ and $S_0[h^{-1}]$ respectively, for a suitable non-zero $h \in R_0$, we may assume R_0 and S_0 have the following additional properties:

- (1) The Galois group $G := \text{Gal}(M_0/K_0)$ acts on S_0 .
- (2) S_0 is a free R_0 -module of rank $n := [M_0 : K_0]$.
- (3) S_0 is an étale R_0 -algebra
- (4) All $2m$ -torsion points of $A_0(\bar{K}_0)$ are defined over S_0 .

- (5) The point P_0 of $A_0(L_0)$ is defined over S_0 .
- (6) All Q' such that $mQ' \in \{Q_1, \dots, Q_r\}$ are defined over S_0 .
- (7) All roots of $f(u)$ lie in S_0 , and all differences between distinct roots are units in S_0 .
- (8) All a_i , a_i^{-1} , and b_i lie in S_0 .

Indeed, let R_0 denote any finitely generated algebra over $\mathbb{Z}$. Let S_0 denote the integral closure of R_0 in M_0 . From this construction property (1) is automatic. We successively invert various elements of R_0 in R_0 and in S_0 . Each of the properties (1)–(8) is preserved under this operation, and we achieve them one by one.

As $\mathbb{Z}$ is a universally Japanese ring [SP, 0335], it follows that S_0 is a finitely generated R_0 -module. As R_0 is Noetherian, S_0 is finitely presented, so by generic freeness [SP, 051S], we may invert some element of R_0 in R_0 and in S_0 to obtain property (2).

By definition, the points at which $\pi: \text{Spec } S_0 \rightarrow \text{Spec } R_0$ fail to be smooth forms a closed set. As S_0 is a finitely generated R_0 -algebra, by Chevalley's constructibility theorem [SP, 054J], the image of the non-smooth locus by π is constructible. Since M_0/K_0 is separable, the generic point of $\text{Spec } R_0$ is not in this image, and it follows that the image is contained in a proper closed subset of $\text{Spec } R_0$. Therefore, by inverting a suitable element of R_0 , we may assume S_0 is a smooth R_0 -algebra, which implies property (3), since π is a finite morphism.

Properties (4)–(8) require that a finite collection of elements of M_0 lie in S_0 , and this can be achieved again by inverting a non-zero element of R_0 .

Note that properties (1)–(3) imply that $\text{Spec } S_0$ is a Galois étale cover of $\text{Spec } R_0$. By [SP, 03SF], the geometric points of $\text{Spec } S_0$ lying over any geometric point of $\text{Spec } R_0$, form a single G -orbit.

Let x be a point of $\text{Spec } R_0$ with residue field $\mathbb{F}_p$, where p is prime. There is a unique $\mathbb{F}_p$ -point of $\text{Spec } R_0$ lying over x . Let $\mathfrak{m}$ be the maximal ideal of R_0 corresponding to x . Then $S_0/\mathfrak{m}S_0$ is an n -dimensional $\mathbb{F}_p$ -algebra and is a product of fields; moreover, G acts on this algebra. If one $\mathbb{F}_p$ -point of $\text{Spec } S_0/\mathfrak{m}S_0$ lies over a point with residue field $\mathbb{F}_p$, the same is true for all of them, and there are n points $x_1, \dots, x_n$ of $\text{Spec } S_0$, corresponding to maximal ideals $\mathfrak{m}_1, \dots, \mathfrak{m}_n$ of S_0 , lying over $\mathfrak{m}$.

We fix such an $\mathfrak{m}$ and let E denote the elliptic curve over $\mathbb{F}_p$ with an affine open $v^2 = \bar{f}(u)$, where $\bar{f}(u)$ denotes the (mod $\mathfrak{m}$) reduction of $f(u)$. Then all points in $E(\mathbb{F}_p)$ annihilated by $2m$ are defined over $\mathbb{F}_p$, and the reduction of each point Q_i to $E(\mathbb{F}_p)$ lies in $mE(\mathbb{F}_p)$, which has $m^{-2}|E(\mathbb{F}_p)|$ elements. For each $\mathfrak{m}_j$, we define Σ_j to be the (mod $\mathfrak{m}_j$) reduction of the sequence of $a_1u + b_1, \dots, a_ku + b_k$.

By Proposition 5.2, there exists $(u_1, \dots, u_k) \in \mathbb{F}_p^k$ such that for compatible $(P_1, \dots, P_k) \in U(\mathbb{F}_p)^k$, no non-empty sum of the P_i lies in $mE(\mathbb{F}_p)$. By the

Chinese Remainder Theorem,

$$S_0/\mathfrak{m}S_0 \cong \prod_{j=1}^n S_0/\mathfrak{m}_j \cong \mathbb{F}_p^n,$$

so there exist infinitely many $u_0 \in S_0$ whose $(\bmod \mathfrak{m}_j)$ reduction is u_j for all j . Applying Theorem 4.2, we obtain $t_0 \in S_0$ such that some $a_i t_0 + b_i$ gives the u -coordinate, $u_i \in S_0$, of a point $(u_i, v_i) \in A(L)$. Without loss of generality, we assume $i = 1$. The $\text{Gal}(L/K)$ -orbit of (u_1, v_1) consists of elements of the form $(\sigma(u_1), v_\sigma)$, where σ ranges over $\text{Gal}(L/K)$ and $v_\sigma^2 = f(\sigma(u_1))$.

These points are all defined over the extension T_0 of S_0 generated by all v_σ . Reducing modulo $\mathfrak{m}_j$, we obtain a point of $E(\mathbb{F}_{p^2})$ of the form $(\sigma(\bar{u}_1), \bar{v}_\sigma)$. By the assumption concerning $(u_1, \dots, u_k)$, these points in fact all lie in $E(\mathbb{F}_p)$, and their sum does not lie in $mE(\mathbb{F}_p)$. It follows that $\text{Tr}_{L/K}(u_1, v_1)$ does not lie in the group generated by the P_i .

It therefore suffices to show that there exist arbitrarily large primes p for which $\text{Spec } S_0$ has a point whose residue field is $\mathbb{F}_p$. Any closed point $\text{Spec } F$ on the generic fiber of $\text{Spec } S_0$ extends to an $O_F(r^{-1})$ -point, where O_F is the ring of integers of the number field F , and $r \in \mathbb{Z}$ is a positive integer. Thus $\text{Spec } S_0$ contains an $\mathbb{F}_p$ -point whenever p is a sufficiently large integer which splits in F . This happens for a positive density set of rational primes by the Chebotarev density theorem, and the theorem follows. $\square$

REFERENCES

- [BF] Bary-Soroker, Lior; Fehm, Arno: Open problems in the theory of ample fields. Geometric and differential Galois theories, 1–11, Sémin. Congr., 27, Soc. Math. France, Paris, 2013.
- [Bo] Bogomolov, Fedor Aleksevich: Sur l’algébricité des représentations ℓ -adiques. *C. R. Acad. Sci. Paris Sér. A–B* **290** (1980), no. 15, A701–A703.
- [BI] Breuer, Florian; Im, Bo-Hae: Heegner points and the rank of elliptic curves over large extensions of global fields. *Canad. J. Math.* **60** (2008), no. 3, 481–490.
- [Bu] Burnside, William: On some properties of groups whose orders are powers of primes. *Proc. London Math. Soc. (2)* **13** (1913), 6–12.
- [Ca] Cadoret, Anna: An open adelic image theorem for abelian schemes, *IMRN* 2015 (2015), 10208–10242.
- [CI] Choi, Seokhyun; Im, Bo-Hae: Larsen’s conjecture for elliptic curves over $\mathbb{Q}$ with analytic rank at most 1, arXiv:2502.18761 .
- [DDMS] Dixon, J. D.; du Sautoy, M. P. F.; Mann, A.; Segal, D.: Analytic pro- p groups. Second edition. Cambridge Studies in Advanced Mathematics, 61. Cambridge University Press, Cambridge, 1999.
- [DD] Dokchitser, Tim; Dokchitser, Vladimir: A note on Larsen’s conjecture and ranks of elliptic curves. *Bull. Lond. Math. Soc.* **41** (2009), no. 6, 1002–1008.
- [FP] Fehm, Arno; Petersen, Sebastian: On the rank of abelian varieties over ample fields. *Int. J. Number Theory* **6** (2010), no. 3, 579–586.
- [FJ] Frey, Gerhard; Jarden, Moshe: Approximation theory and the rank of abelian varieties over large algebraic fields. *Proc. London Math. Soc. (3)* **28** (1974), 112–128.
- [Ha] Hadavand, A.: On Larsen’s conjecture on the ranks of elliptic curves, arXiv:2411.14097.

- [HJ] Hales, A. W.; Jewett, R. I.: Regularity and positional games. *Trans. Amer. Math. Soc.* **106** (1963), 222–229.
- [I1] Im, Bo-Hae: The rank of elliptic curves with rational 2-torsion points over large fields, *Proc. Amer. Math. Soc.* **134** (2006), 1623–1630.
- [I2] Im, Bo-Hae: Heegner points and Mordell-Weil groups of elliptic curves over large fields. *Trans. Amer. Math. Soc.* **359** (2007), no. 12, 6143–6154.
- [IL1] Im, Bo-Hae; Larsen, Michael: Abelian varieties over cyclic fields. *Amer. J. Math.* **130** (2008), no. 5, 1195–1210.
- [IL2] Im, Bo-Hae; Larsen, Michael: Some applications of the Hales-Jewett theorem to field arithmetic. *Israel J. Math.* **198** (2013), no. 1, 35–47.
- [IL3] Im, Bo-Hae; Larsen, Michael: Abelian varieties and finitely generated Galois groups. Abelian varieties and number theory, 1–12, Contemp. Math., 767, Amer. Math. Soc., RI, 2021.
- [ILR] Im, Bo-Hae; Lozano-Robledo, Álvaro: On products of quadratic twists and ranks of elliptic curves over large fields. *J. Lond. Math. Soc. (2)* **79** (2009), no. 1, 1–14.
- [JJ] Jacobson, Marcel; Jarden, Moshe: Finiteness theorems for torsion of abelian varieties over large algebraic fields. *Acta. Arith.* **98** (2001), no. 1, 15–31.
- [JK] Junker, Markus; Koenigsmann, Jochen: Schlanke Körper. *J. Symbolic Logic* **75** (2010), no. 2, 481–500.
- [Ln] Lang, Serge: Fundamentals of Diophantine geometry. Springer-Verlag, New York, 1983.
- [L1] Larsen, Michael: Rank of elliptic curves over almost separably closed fields. *Bull. London Math. Soc.* **35** (2003), no. 6, 817–820.
- [L2] Larsen, Michael: A Mordell-Weil theorem for abelian varieties over fields generated by torsion points, arXiv:math/0503378.
- [LS] Lubotzky, Alexander; Segal, Dan: Subgroup growth. Progress in Mathematics, 212. Birkhäuser Verlag, Basel, 2003.
- [Ri] Ribet, Kenneth A.: Kummer theory on extensions of abelian varieties by tori. *Duke Math. J.* **46** (1979), no. 4, 745–761.
- [S1] Serre, Jean-Pierre: Résumé des cours de 1984–1985, Annuaire du Collège de France (1985), 85–90.
- [S2] Serre, Jean-Pierre: Lettre à Ken Ribet du 7/3/1986, Collected Papers IV.
- [S3] Serre, Jean-Pierre: Un critère d’indépendance pour une famille de représentations ℓ -adiques. *Comment. Math. Helv.* **88** (2013), no. 3, 541–554.
- [Si] Silverman, Joseph H.: Integer points on curves of genus 1. *J. London Math. Soc. (2)* **28** (1983), no. 1, 1–7.
- [SP] The *Stacks Project* authors: *Stacks project*.
<https://stacks.math.columbia.edu>

DEPARTMENT OF MATHEMATICAL SCIENCES, KAIST, 291 DAEHAK-RO, YUSEONG-GU,
DAEJEON, 34141, SOUTH KOREA
Email address: `bhim@kaist.ac.kr`

DEPARTMENT OF MATHEMATICS, INDIANA UNIVERSITY, BLOOMINGTON, IN, 47405,
U.S.A.
Email address: `mjlarsen@indiana.edu`