There are genus one curves of every index over every infinite, finitely generated field

Pete L. Clark and Allan Lacy

Abstract. Every nontrivial abelian variety over a Hilbertian field in which the weak Mordell-Weil theorem holds admits infinitely many torsors with period any \( n > 1 \) which is not divisible by the characteristic. The corresponding statement with “period” replaced by “index” is plausible but much more challenging. We show that for every infinite, finitely generated field \( K \), there is an elliptic curve \( E_K \) which admits infinitely many torsors with index any \( n > 1 \).

Contents

1. Introduction 1
1.1. Review of the Period-Index Problem 1
1.2. Constructing WC-Classes With Prescribed Period 3
1.3. Constructing WC-Classes With Prescribed Index 4
2. Linear Independence in Torsion Groups 5
3. The Proof of Theorem 1.6 6
3.1. The Proof 6
3.2. A Generalization 8
4. The Proof of the Main Theorem: Outline 8
5. The Proof of Theorem 4.1 9
5.1. Mordell-Weil Groups of Abelian Varieties Over Local Fields 9
5.2. A Local-Global Isomorphism in WC-Groups 12
5.3. Proof of Theorem 4.1 13
6. The Proof of Theorem 4.2 14
6.1. Controlling the torsion 14
6.2. Controlling the rank 15
6.3. Controlling III 16
6.4. Proof of Theorem 4.2 16
7. The Proof of Theorem 4.3 17
7.1. Some preliminaries 17
7.2. Proof of Theorem 4.3 20
References 20

1. Introduction

1.1. Review of the Period-Index Problem.

© Pete L. Clark and Allan Lacy, 2013.
Let \( K \) be a field, with a choice of separable closure \( K^{\text{sep}} \) and algebraic closure \( \overline{K} \). Let \( g_K = \text{Aut}(K^{\text{sep}}/K) = \text{Aut}(\overline{K}/K) \) be the absolute Galois group of \( K \).

By a variety \( X/K \), we will mean a finite type integral scheme over \( \text{Spec} \, K \) such that \( K \) is algebraically closed in \( K(X) \). (Thus if \( K \) is not perfect, \( X/K \) need not be a variety.) A field extension \( L/K \) is a splitting extension for \( X \) if \( X(L) \neq \emptyset \). For a regular geometrically integral variety \( X/K \), we define the index \( I(X) \) as the least positive degree of a \( K \)-rational zero-cycle on \( X \). Equivalently, it is the gcd of all degrees of finite splitting extensions. Clearly we have \( I(X/L) \mid I(X) \) for every extension \( L/K \).

Let \( M \) be a commutative \( g_K \)-module. For \( i \in \mathbb{N} \) we have the Galois cohomology groups \( H^i(K, M) = H^i(g_K, M) \). For \( i \geq 1 \), \( H^i(K, M) \) is a torsion commutative group. For \( i \geq 1 \) and \( \eta \in H^i(K, M) \), the period \( P(\eta) \) as the order of \( \eta \) in \( H^i(K, M) \).

Let \( L/K \) be any field extension. There is a field embedding \( \iota : \overline{K} \to \overline{L} \). Any automorphism \( \sigma \in \text{Aut}(\overline{L}/K) \) fixes \( K \) pointwise so restricts to an automorphism of \( \overline{K} \). This gives continuous group homomorphism \( g_L \to g_K \) and thus for all \( i \geq 1 \) a restriction map

\[
\text{Res}_L : H^i(K, M) \to H^i(L, M).
\]

It can be shown that \( \text{Res}_L \) is independent of the choice of \( \iota \) (CITE). We put

\[
H^i(L/K, M) = \text{Ker} \, \text{Res} : H^i(K, M) \to H^i(L, M).
\]

If \( \eta \in H^i(L/K, M) \), we say \( L \) is a splitting field for \( \eta \). Every \( \eta \in H^i(K, M) \) has a finite Galois splitting extension \( L/K \). We define the index \( I(\eta) \) to be the greatest common divisor of all degrees \( [L : K] \) for \( L/K \) a finite splitting field of \( \eta \). For all \( \eta \in H^i(K, M) \) with \( i \geq 1 \) we have \( P(\eta) \mid I(\eta) \) and \( I(\eta) \) divides some power of \( P(\eta) \) [WCII, Prop. 11]. The period-index problem in Galois cohomology is to explore the relations between the period and index.

The following standard result reduces us to the case of prime power period.

**Lemma 1.1.** (Primary Decomposition) Let \( i, r \geq 1 \), and let \( \eta_1, \ldots, \eta_r \in H^i(K, M) \) be such that \( P(\eta_1), \ldots, P(\eta_r) \) are pairwise coprime. Let \( \eta = \eta_1 + \ldots + \eta_r \). Then

\[
(1) \quad P(\eta) = \prod_{j=1}^r P(\eta_j)
\]

and

\[
(2) \quad I(\eta) = \prod_{j=1}^r I(\eta_j).
\]

**Proof.** Easy group theory gives (1). For (2) see e.g. [WCII, Prop. 11d]].

Here we are interested in the case \( M = A(K^{\text{sep}}) \) for an abelian variety \( A/K \). Then \( H^1(K, A) \) is naturally isomorphic to the Weil-Châtelet group of \( A/K \), whose elements are torsors under \( A_K \). When \( A = E \) is an elliptic curve, classes in \( H^1(K, E) \) correspond to genus one curves \( C_K \) together with an identification \( \text{Pic}^0 C \cong E \).
1.2. Constructing WC-Classes With Prescribed Period.

Fix a field $K$ and consider the problem of characterizing all possible periods and indices of elements in $\text{H}^1(K, A)$, either for a fixed abelian variety $A/K$ or as $A$ varies in a class of abelian varieties defined over $K$. The point is that it is much easier to understand this problem for the period than for the index. Indeed, in the earliest days of Galois cohomology Shafarevich established the following result.

**Theorem 1.2.** (Shafarevich [III57]) Let $K$ be a number field and $A/K$ a nontrivial abelian variety. For each $n > 1$, there are infinitely many classes $\eta \in \text{H}^1(K, A)$ with $P(\eta) = n$.

We wish to indicate a vast proving ground for the period-index problem in WC-groups by establishing a generalization of Theorem 1.2. In order to do so we first define some suitable classes of fields.

A field $K$ is **MW** if for every abelian variety $A/K$, the group $A(K)$ is finitely generated. For $n \in \mathbb{Z}^+$, a field $K$ is **n-WMW** if for every abelian variety $A/K$, the group $A(K)/nA(K)$ is finite. (The nomenclature may be new, but the study of such fields in the Galois cohomology of abelian varieties goes back to [LT58, §5].) Finally, $K$ is **WMW** if it is $n$-WMW for all $n \in \mathbb{Z}^+$.

**Remark 1.3.**

a) $\mathbb{F}_p$ is an MW field: for any variety $V/\mathbb{F}_p$, $V(\mathbb{F}_p)$ is finite.
b) $\mathbb{Q}$ is an MW field: the Mordell-Weil Theorem.
c) An algebraically closed field $K$ is WMW: for any abelian variety $A/K$, $A(K)$ is a divisible commutative group, so $A(K)/nA(K) = 0$ for all $n \in \mathbb{Z}^+$.
d) $\mathbb{R}$ is a WMW field: by Lie theory, for any $g$-dimensional abelian variety $A/\mathbb{R}$, $A(\mathbb{R})$ is a (split) extension of the finite commutative group $\pi_0(A(\mathbb{R}))$ by the connected component of the identity, which is isomorphic to $(\mathbb{R}/\mathbb{Z})^g$ and thus divisible.
e) $\mathbb{Q}_p$ is a WMW field: by $p$-adic Lie theory, for any $g$-dimensional abelian variety $A/\mathbb{Q}_p$, $A(\mathbb{Q}_p)$ is a (split) extension of a finite commutative group by the group $\mathbb{Z}_p^g$.

This will be shown in detail in §5.1

f) For any prime number $p$, the Laurent series field $K = \mathbb{F}_p((t))$ is $n$-WMW for all $n$ prime to $p$. However $K$ is not $p$-WMW: see §5.1 for stronger results.

**Proposition 1.4.** Let $L/K$ be a finitely generated field extension.

a) If $K$ is an MW field, so is $L$.
b) If $K$ is a WMW field, so is $L$.

**Proof.** Let $\{t_1, \ldots, t_n\}$ be a transcendence basis for $L/K$, and put $K' = K(t_1, \ldots, t_n)$, so $K'/K$ is finitely generated regular and $L/K'$ is finite. Thus we may deal separately with the two cases $L/K$ finitely generated regular and $L/K$ finite.

Step 1: Suppose $L/K$ is finitely generated regular, and let $A/L$ be an abelian variety. By the Lang-Néron Theorem [LN59], [Co06, §7] there is an abelian variety $B/K$ and an injective homomorphism $\tau: B(K) \hookrightarrow A(L)$ such that $A(L)/\tau(B(K))$ is finitely generated. Thus if $K$ is MW (resp. WMW), so is $L$.

Step 2: Suppose $L/K$ is finite. For an abelian variety $A/L$, let $B/K$ be the abelian variety obtained by Weil restriction. Then $A(L) = B(K)$, hence $A(L)/nA(L) \cong B(K)/nA(K)$ for all $n \in \mathbb{Z}^+$. Thus if $K$ is MW (resp. WMW), so is $L$. 

\qed
Combining Remark 1.3 and Proposition 1.4 yields:

**Corollary 1.5.**

a) (Néron) Every finitely generated field is an MW field.

b) Every field which is finitely generated over an algebraically closed field, \( \mathbb{R} \) or \( \mathbb{Q}_p \), is a WMW-field.

We also need the notion of a **Hilbertian field**. We refer to the text [FJ] both for the definition (p. 219) and for the proofs of the following basic results:

- The field \( \mathbb{Q} \) is Hilbertian (Hilbert’s Irreducibility Theorem) [FJ, Thm. 13.4.2].
- If \( K \) is Hilbertian and \( L/K \) is finite, then \( L \) is Hilbertian [FJ, Prop. 12.3.3].
- For any field \( K \), the rational function field \( K(t) \) is Hilbertian [FJ, Thm. 13.4.2].

Thus every infinite, finitely generated field (or “IFG field”) is Hilbertian.

We can now state the following generalization of Shafarevich’s theorem.

**Theorem 1.6.** Let \( K \) be Hilbertian, and let \( A_{/K} \) be a nontrivial abelian variety.

a) If \( n > 1 \) is an integer indivisible by \( \text{char} \ K \) and such that \( A(K)/nA(K) \) is finite, then there are infinitely many classes \( \eta \in H^1(K, A) \) of period \( n \).

b) Thus if \( K \) is WMW, there are infinitely many classes \( \eta \in H^1(K, A) \) with any given period \( n > 1 \).

We will prove Theorem 1.6 in §3.

**Remark 1.7.** A field \( K \) is **PAC** (pseudo-algebraically closed) if every geometrically integral variety \( V_{/K} \) has a \( K \)-rational point. Thus all WC-groups over a PAC field are trivial. Any algebraically closed field is PAC and WMW (but not Hilbertian): thus the hypothesis “\( K \) is Hilbertian” cannot be omitted from Theorem 1.6. On the other hand, there are fields which are both Hilbertian and PAC: it follows from Theorem 1.6 that for every nontrivial abelian variety \( A \) over such a field and all \( n \geq 2 \), \( A(K)/nA(K) \) is infinite. In particular the hypothesis “\( K \) is WMW” cannot be omitted from Theorem 1.6.

1.3. Constructing WC-Classes With Prescribed Index.

It is much harder to construct classes in \( H^1(K, A) \) with prescribed index. This problem was first studied in [LT58], and they proved the following result.

**Theorem 1.8.** (Lang-Tate) Let \( n \in \mathbb{Z}^+ \), and let \( K \) be a field with an infinite number of abelian extensions of exponent \( n \). Let \( A_{/K} \) be an abelian variety such that \( A(K)/nA(K) \) is finite and \( A(K) \) contains at least one element of order \( n \). Then \( H^1(K, A) \) contains an infinite number of elements of period \( n \) and, in fact, an infinite number such that the corresponding homogeneous spaces have index \( n \) as well as period \( n \).

It is interesting to compare this result to Theorem 1.6: we have the same hypothesis on weak Mordell-Weil groups, and the hypothesis on abelian extensions holds over every Hilbertian field. On the other hand, the hypothesis on the existence of a point \( P \in A(K) \) of order \( n \) is prohibitively strong: by Merel’s Theorem, for each number field \( K \), there are only finitely many \( n \in \mathbb{Z}^+ \) for which an elliptic curve \( E_{/K} \) can have order \( n \). (Similarly, we expect that for any infinite, finitely generated field \( K \) and \( d \in \mathbb{Z}^+ \), torsion is uniformly bounded on \( d \)-dimensional abelian varieties \( A_{/K} \).)
Lang and Tate asked whether for every positive integer $n$ there is some elliptic curve $E = \mathbb{Q}$ and class $\eta \in H^1(\mathbb{Q}, E)$ with index $n$. This question remained wide open for years until W. Stein showed that for every number field $K$ and every positive integer $n$ which is not divisible by 8, there is an elliptic curve $E = K$ and a class $\eta \in H^1(K, E)$ with index $n$. In [Cl05] the first author showed that for any number field $K$ and every $n \in \mathbb{Z}^+$ there is an elliptic curve $E = K$ and a class $\eta \in H^1(K, E)$ with $I(\eta) = P(\eta) = n$.

Thus the answer to the question of Lang and Tate is affirmative, but it took almost 50 years to get there. Since then there has been some dramatic progress: recently, building on prior work of his own, work of the first author and joint work with the first author, S. Sharif established a magnificent result which we view as a “complete solution of the period-index problem for elliptic curves over number fields”.

**Theorem 1.9.** (Sharif [Sh12]) Let $E = K$ be an elliptic curve over a number field, and let $P, I \in \mathbb{Z}^+$ be such that $P | I | P^2$. Then there is a class $\eta \in H^1(K, E)$ with $P(\eta) = P$ and $I(\eta) = I$.

We find it plausible that the analogue of Sharif’s result should hold for every elliptic curve over every Hilbertian, WMW field $K$. However, this looks very difficult. Consider the case of global fields of positive characteristic: i.e., finite field extensions of $\mathbb{F}_p(t)$. In this case the methods of [Sh12] work to establish the analogue of Theorem 1.9 as long as we require $\gcd(P, p) = 1$. The case of $p$-power period in characteristic $p$ leads to additional technicalities involving an explicit form of the period-index obstruction map in flat cohomology. (The first author and S. Sharif have been working on this problem for several years: at present we can handle the ordinary case but not the supersingular case.) Thus it seems to be of interest to retreat to the construction of genus one curves with prescribed period over various fields, but where we get to choose the Jacobian elliptic curve to our advantage.

We can now state the main result of this paper.

**Main Theorem.** Let $K$ be any infinite, finitely generated field. There is an elliptic curve $E = K$ such that for all $n > 1$, there are infinitely many classes $\eta \in H^1(K, E)$ with $I(\eta) = P(\eta) = n$.

**Remark 1.10.** In the statement of the Main Theorem, it is easy to replace the elliptic curve $E = K$ with a $g$-dimensional abelian variety $A = K$ for any fixed $g \geq 1$: for any torsor $C$ under $E$ with $P(C) = I(C) = n, C \times E^{g-1}$ is a torsor under $E^g$ with $P(C) = I(C) = n$. It would of course be more interesting to treat torsors and abelian varieties which are not products in this way.

**Remark 1.11.** The hypothesis that $K$ is infinite is necessary: by a classic result of Lang [La56] $H^1(\mathbb{F}_q, A) = 0$ for every abelian variety $A$ over a finite field $\mathbb{F}_q$.

2. Linear Independence in Torsion Groups

At several points in the coming proofs, we will find ourselves in the following situation: we have an integer $n > 1$, a commutative group $A$, a subset $S \subseteq A$ such that every element of $S$ has order $n$, and a homomorphism of groups $R : A \to B$. Under what circumstances does $R(S)$ contain infinitely many elements of order $n$?
It suffices for $R$ to be injective, but in our applications this hypothesis is too strong. On the other hand, if $\ker R$ is too large then we may have $S \subset \ker R$. So it is natural to assume $S$ is infinite and $\ker S$ is finite. In this case $R$ has finite fibers and thus $R(S)$ is infinite. However, it still need not be the case that $R(S)$ has infinitely many elements of order $n$.

**Example 2.1.** Let $p$ be a prime and $I$ an infinite set. Put $A = \bigoplus_{i \in I} \mathbb{Z}/p\mathbb{Z} \oplus \mathbb{Z}/p^2\mathbb{Z}$, $K = \mathbb{Z}/p\mathbb{Z}^2$, $B = A/K$, and $R : A \to B$ be the quotient map. Then $S = \{1 + x \mid x \in \bigoplus_{i \in I} \mathbb{Z}/p\mathbb{Z}\}$ has cardinality $\#I$ and consists of elements of order $p^2$, but $R(S) \subset B = B[p]$ consists of elements of order dividing $p$.

Thus we see that some stronger group-theoretic hypothesis must be imposed, which serves to motivate the definitions of the next paragraph.

Let $n \geq 2$, let $H$ be a commutative group, and let $S = \{\eta_i\} \subset H[n]$. For $r \in \mathbb{Z}^+$, we say $S$ is $r$-LI over $\mathbb{Z}/n\mathbb{Z}$ if for every $r$-element subset $\{\eta_1, \ldots, \eta_r\}$ is linearly independent over $\mathbb{Z}/n\mathbb{Z}$: if for $a_1, \ldots, a_r \in \mathbb{Z}$ we have $a_1\eta_1 + \ldots + a_r\eta_r = 0$, then $a_1 \equiv \ldots \equiv a_r \equiv 0 \pmod{n}$. Equivalently, the subgroup generated by $\eta_1, \ldots, \eta_r$ has cardinality $r^n$. We say $S$ is LI over $\mathbb{Z}/n\mathbb{Z}$ if it is $r$-LI over $\mathbb{Z}/n\mathbb{Z}$ for all $r \in \mathbb{Z}^+$.

In particular, $S$ is 1-LI over $\mathbb{Z}/n\mathbb{Z}$ iff every element of $S$ has order $n$, and $S$ is 2-LI over $\mathbb{Z}/n\mathbb{Z}$ iff for any distinct elements $\eta_i \neq \eta_j \in S$, $\langle \eta_i \rangle \cap \langle \eta_j \rangle = \{0\}$.

**Lemma 2.2.** Let $n \in \mathbb{Z}^+$, let $R : H_K \to H_L$ be a homomorphism of commutative groups, and let $S \subset H_K[n]$ be a subset.

a) If $\ker R = 0$, then $\#R(S) = \#R$, and for each $r \in \mathbb{Z}^+$, $S$ is $r$-LI over $\mathbb{Z}/n\mathbb{Z}$ if and only if $R(S)$ is $r$-LI over $\mathbb{Z}/n\mathbb{Z}$.

b) Suppose $\ker R$ is finite and $S$ is infinite and 2-LI over $\mathbb{Z}/n\mathbb{Z}$. Then there is a subset $S' \subset S$ such that $R(S')$ is an infinite 1-LI over $\mathbb{Z}/n\mathbb{Z}$ subset of $H_L$.

**Proof.** Primary decomposition (1.1) reduces us to the case $n = \ell^a$ a prime power.

a) If $\ker R = 0$, then $R$ is an injection of $n$-torsion groups. Thus $R : S \to R(S)$ is a bijection and all linear independence relations are preserved.

b) Let $N = \# \ker R$. Let $\eta_1, \ldots, \eta_{N+1}$ be any $N + 1$ elements of $S$. We claim that for at least one $i$, $1 \leq i \leq N + 1$, $R(\eta_i)$ has order $n$: if not, then for all $i$ we have $0 = \ell^{a-1}R(\eta_i) = R(\ell^{a-1}\eta_i)$, so $\ell^{a-1}\eta_i \in \ker R$ for all $i$. By the Pigeonhole Principle we must have $\ell^{a-1}\eta_i - \ell^{a-1}\eta_j = 0$ for some $i \neq j$, contradicting the hypothesis that $S$ is 2-LI over $\mathbb{Z}/n\mathbb{Z}$. This constructs an infinite $S' \subset S$ such that for all $\eta \in S$, $R(\eta)$ has order $n$. Since $\ker R$ is finite, all the fibers of $R$ are finite, and thus $R(S')$ is infinite.

\[\square\]

3. **The Proof of Theorem 1.6**

3.1. **The Proof.**

Step 0: Let $n > 1$ be indivisible by the characteristic of $K$, and let $A/K$ be an
abelian variety of dimension \( g \geq 1 \) such that \( A(K)/nA(K) \) is finite. We write \( A[n] \) for both the group scheme – which is finite étale – and the associated \( g_K \)-module \( A[n](K^{sep}) \), which has underlying commutative group \( (\mathbb{Z}/n\mathbb{Z})^{2g} \). Recall the Kummer sequence in (étale = Galois) cohomology

\[
0 \to A(K)/nA(K) \to H^1(K,A[n]) \to H^1(K,A)[n] \to 0.
\]

We claim that the \( n \)-torsion group \( H^1(K,A[n]) \) has an infinite LI over \( \mathbb{Z}/n\mathbb{Z} \) subset \( S \). (For our application it would be sufficient for \( S \) to be 2-LI over \( \mathbb{Z}/n\mathbb{Z} \). But the more general result is no harder to prove.) Applying Lemma 2.2b) with \( H_K = H^1(K,A[n]) \), \( H_L = H^1(K,A)[n] \) and \( R \) the natural map between them, we get an infinite subset \( S' \subset S \) whose image in \( H^1(K,A)[n] \) is 1-LI over \( \mathbb{Z}/n\mathbb{Z} \). In other words, \( H^1(K,A) \) has infinitely many elements of order \( n \), which is what we want to show. The remainder of the argument establishes the claim.

Step 1: Let \( L = K(A[n](K^{sep})) \) – in other words, the fixed field of the kernel of the \( g_K \)-action on \( A[n] \) – let \( g_{L/K} = \text{Gal}(L/K) \), and consider the associated extended inflation-restriction sequence \[CG\]

\[
0 \to H^1(g_{L/K},A[n](L)) \to H^1(K,A[n]) \xrightarrow{\Phi} H^1(L,A[n])^{g_{L/K}} \xrightarrow{\partial} H^2(g_{L/K},A[n](L)).
\]

Since \( H^1(g_{L/K},A[n](L)) \) is finite for all \( i \), the kernel and cokernel of \( \Phi \) are finite. We will construct an infinite LI over \( \mathbb{Z}/n\mathbb{Z} \) subset of \( S' = \Phi(H^1(K,A[n])) \). For each \( \eta_i \in S' \), choose \( \eta_i \in \Phi^{-1}(\eta_i) \). Then \( S = \{ \eta_i \}_{i \in S'} \) is an infinite LI over \( \mathbb{Z}/n\mathbb{Z} \) subset of \( H^1(K,A[n]) \).

Step 2: We have \( H^1(L,A[n]) = \text{Hom}(g_L,A[n](L)) \), so the surjective elements \( \eta \in H^1(L,A[n]) \) – i.e., such that \( \eta(g_L) = A[n](L) \) – parameterize Galois extensions \( M/L \) with \( \text{Gal}(M/L) \cong A[n](L) \cong (\mathbb{Z}/n\mathbb{Z})^{2g} \) together with an isomorphism \( \text{Gal}(M/L) \cong A[n](L) \). The natural action of \( g_{L/K} \) on this set of order \( n \) elements in \( H^1(L,A[n]) \) consists of precomposing \( \chi : g_L \to A[n](L) \) with the automorphism \( \sigma^* \) of \( g_L \) obtained by restricting conjugation by \( \sigma \in g_K \) to the normal subgroup \( g_L \). (Because \( A[n](L) \) is commutative, the map \( \sigma^* \) depends only on the coset of \( \sigma \) modulo \( g_L \).) A class \( \eta \in H^1(L,A[n]) \) is fixed by \( g_{L/K} \) if and only if the extension \( (L^{sep})^\ker \eta / K \) is Galois. So we’ve shown that the surjective elements of \( H^1(L,A[n])^{g_{L/K}} \) correspond to liftings of the Galois extension \( L/K \) to Galois extensions \( M/K \). For \( \eta_i' \in H^1(L,A[n])^{g_{L/K}} \), the class \( \partial \eta_i' \in H^2(g_{L/K},A[n](L)) \) is the class of the extension

\[
1 \to \text{Gal}(M/L) \to \text{Gal}(M/K) \to g_{L/K} \to 1,
\]

so by exactness of (3), we find that \( \eta_i' \in \Phi(H^1(K,A[n])) \) if and only if the above extensions splits. In summary, the surjective elements of \( \Phi(H^1(K,A[n])) \) parameterize split extensions of \( g_{L/K} \) by \( A[n](L) \).

Step 3: It was shown by Ikeda [Ik60] that over a Hilbertian field, every split embedding problem with abelian kernel \( A \) has a proper solution: this means precisely that there is at least one surjective (hence order \( n \)) element of \( \Phi(H^1(K,A[n])) \). The proof of Ikeda’s Theorem (see [FJ, §16.4] for a nice modern treatment) goes by specializing a regular \( A \)-Galois cover of \( L(t) \). Over a Hilbertian field, a regular Galois covering not only has an irreducible specialization but has an infinite linearly disjoint set of irreducible specializations, so we get an infinite set \( \{ M_i/L \} \) of \( A[n](L) \)-Galois extensions of \( L \) such that \( M_i/K \) is Galois and \( \text{Gal}(M_i/K) \cong A[n](L) \times g_{L/K} \) (see [FJ, Lemma 16.4.2], which gives a slightly weaker statement; the stronger version...
needed here follows immediately by an inductive argument). The linear disjoint-
ness of the extensions $M_i/L$ means that the Galois group of the compositum is the
direct product of the Galois groups, and this implies that the set of classes $\eta'_i$ is LI
over $\mathbb{Z}/n\mathbb{Z}$ in $H^1(L, A[n])^{\text{et}}/\mathbb{F}_n$, completing the proof.

3.2. A Generalization.

In the setup of Theorem 1.6, the hypothesis that $n$ is not divisible by char $K$ was
used to ensure that $A[n]$ is an etale group scheme. In fact we need only that $A[n]$ admits an etale subgroup scheme $H$ of exponent $n$; equivalently, $A(K^\text{sep})$ contains a point of order $n$. For instance this condition holds if $A$ is ordinary and $K$ is perfect. Running the argument with $H$ in place of $A[n]$ gives the following result.

**Theorem 3.1.** Let $A/K$ be a nontrivial abelian variety over a Hilbertian field. Let $n > 1$ be such that $A(K)/nA(K)$ is finite. If char $K | n$, suppose $A(K^\text{sep})$ contains a point of order $n$. Then in $H^1(K, A)$ there are infinitely many classes of period $n$.

4. The Proof of the Main Theorem: Outline

The proof of the Main Theorem is a three step argument. We go by induction on the transcendence degree, and in fact two out of the three steps go into establishing the base cases. Here is the first step.

**Theorem 4.1.** Let $K$ be a global field, and let $E/K$ be an elliptic curve with $E(K) = \mathbb{N}(K, E) = 0$. Then for all $n \geq 1$, there is a $g$-dimensional abelian variety $A$ such that $A(K^\text{sep})$ contains points of order $n$ for all $n > 1$. Thus Theorem 3.1 shows that every Hilbertian WMW field admits abelian varieties whose WC-groups contain infinitely many elements of every period $n > 1$.

The second step of the proof is to verify that for every prime global field $K$ there is an elliptic curve satisfying the hypotheses of Theorem 4.1. In the case of $K = \mathbb{Q}$ we may take the same elliptic curve used in [Cl05]: namely Cremona’s 1813B1 curve

$$E : y^2 + y = x^3 - 49x - 86.$$
THERE ARE GENUS ONE CURVES OF EVERY INDEX OVER EVERY INFINITE, FINITELY GENERATED FIELD

That \( E(\mathbb{Q}) = \text{III}(\mathbb{Q}, E) = 0 \) is a deep theorem of Kolyvagin [Ko89, Thm. H].

We also need such a curve \( E/F_p(t) \) for every prime \( p \). We will show:

**Theorem 4.2.** For every prime number \( p \), the elliptic curve 
\[
E : y^2 + txy + t^3y = x^3 + t^2x^2 + t^4x + t^5
\]
defined over \( F_p(t) \) has \( E(F_p(t)) = 0 \) and \( \text{III}(F_p(t), E) = 0 \).

The proof of Theorem 4.2 takes advantage of some deep work on the Birch-Swinnerton Dyer conjecture in the function field case. It is given in § 3.4.

Here is the inductive step.

**Theorem 4.3.** Let \( n > 1 \), \( K \) a WMW field, \( A_{/K} \) an abelian variety, and \( L/K \) be a finitely generated separable field extension. Let \( S \subseteq H^1(K, A)[n] \) be an infinite \( 2\text{-LI} \) over \( \mathbb{Z}/n\mathbb{Z} \) subset. Then there is an infinite subset \( S' \subseteq S \) such that \( \text{Res}_L S' \subseteq H^1(L, A)[n] \) is infinite and consists of elements of order \( n \). Moreover, if each element of \( S \) has index \( n \), then each element of \( \text{Res}_L S' \) has index \( n \).

We will prove Theorem 4.3 in § 3.5.

We now explain how to put Theorems 4.1, 4.2 and 4.3 together to prove the Main Theorem. Let \( L \) be an infinite, finitely generated field. Let \( k_0 \) be its prime subfield: either \( \mathbb{Q} \) or \( \mathbb{F}_p \). Since \( k_0 \) is perfect, \( L/k_0 \) is separable.

Case 1: Suppose \( k_0 = \mathbb{Q} \). Then we take the elliptic curve \( E/\mathbb{Q} \) of (4), with \( E(\mathbb{Q}) = \text{III}(\mathbb{Q}, E) = 0 \). By Theorem 4.1, for each \( n > 1 \) there is an infinite LI over \( \mathbb{Z}/n\mathbb{Z} \) subset \( S \subseteq H^1(K, E) \) such that every element of \( S \) has index \( n \). We apply Theorem 4.3 with \( K = \mathbb{Q} \) and \( A = E \) to get the desired result.

Case 2: Suppose \( k_0 = \mathbb{F}_p \). Since \( k_0 \) is perfect, the finitely generated extension \( L/k_0 \) admits a separating transcendence basis \( t, t^2, \ldots, t_d \). We take the elliptic curve \( E/F_p(t) \) of Theorem 4.2. The rest of the argument proceeds as in Case 1.

5. The Proof of Theorem 4.1


By a local field we mean a field \( K \) which is complete and nondiscrete with respect to an ultrametric norm \( | \cdot | \), and with finite residue field \( k \). A local field of characteristic 0 is (canonically) a finite extension of \( \mathbb{Q}_p \), and a locally compact field of positive characteristic is (noncanonically) isomorphic to \( k((t)) \).

If \( K \) is a local field and \( G_{/K} \) is an algebraic group, then the set \( G \) of \( K \)-rational points of a K-analytic Lie group in the sense of [LALG, LG, Ch. IV]. Since \( G \) is quasi-projective, \( G \) is homeomorphic to a subspace of \( \mathbb{P}^N(K) \) for some \( K \) and is thus second countable. When \( G = A \) is an abelian variety, \( G \) is commutative and compact. In this case, we can use \( K \)-adic Lie theory to analyze the structure of the Mordell-Weil group and – crucially for us in what follows – the weak Mordell-Weil groups \( A(K)/nA(K) \).
This was done somewhat breezily in [Cl05]: we asserted (6) below, and our justification was “by $p$-adic Lie theory”. Here we need also the positive characteristic case, which although certainly known to some experts, to the best of our knowledge do not appear in the literature. This time around we give a careful treatment of both the $p$-adic and Laurent series field cases here, with an eye towards providing a suitable reference for future work.

**Lemma 5.1.** Let $H$ be a commutative, torsionfree pro-$p$-group, endowed with its profinite topology. Then, as a topological group, $H \cong \prod_{i \in I} \mathbb{Z}_p$ for some index set $I$. If $H$ is second countable, then $I$ is countable.

**Proof.** The Pontrjagin dual $H^\vee$ of $H$ is a commutative $p$-primary torsion group. Since $H[p] = 0$, $H^\vee/H[p] = 0$, so $H$ is divisible. It is a classical result that a divisible commutative group is a direct sum of copies of $\mathbb{Q}$ and $\mathbb{Q}_p/\mathbb{Z}_p$ for various primes $p$ [Sc, 5.2.12], and the number of summands of each isomorphism type is invariant of the chosen decomposition. (Or: an injective module over a commutative Noetherian ring $R$ is a direct sum of copies of injective envelopes of modules of the form $R/p$ as $p$ ranges over prime ideals of $R$. [Ma, Thms. 18.4 and 18.5]: applying this with $R = \mathbb{Z}(p)$ recovers this classical result.) Thus for some index set $I$,

$$H^\vee \cong \bigoplus_{i \in I} \mathbb{Q}_p/\mathbb{Z}_p,$$

and taking Pontrjagin duals gives

$$H \cong \prod_{i \in I} \mathbb{Z}_p.$$

An uncountable product of second countable Hausdorff spaces, each with more than a single point, is not second countable [Wi, Thm. 16.2c]), so if $H$ is second countable, $I$ is countable.

**Theorem 5.2.** Let $K$ be a local field, with valuation ring $R$, maximal ideal $m$ and residue field $\mathbb{F}_q = \mathbb{F}_{p^d}$. If $\text{char} \ K = 0$, let $d = [K : \mathbb{Q}_p]$. Let $G$ be a compact commutative second countable $K$-analytic Lie group, of dimension $g \geq 1$.

a) If $\text{char} \ K = 0$, then $G[\text{tors}]$ is finite and we have a topological group isomorphism

$$G \cong \mathbb{Z}_p^d \oplus G[\text{tors}].$$

b) If $\text{char} \ K = p$, then $G[\text{tors}]$ is finite if and only if $G[p]$ is finite. When these equivalent conditions hold – e.g. when $G = A(K)$ for a semi-abelian variety $A/K$ – then we have a group isomorphism

$$G \cong \left( \prod_{i=1}^{\infty} \mathbb{Z}_p \right) \oplus G[\text{tors}].$$

**Proof.** Step 0: By [LALG, LG IV.9], $G$ has a filtration by open subgroups

$$G = G^{-1} \supset G^0 \supset G^1 \supset \ldots \supset G^n \supset \ldots$$

such that:

(i) Each $G^i$ is obtained by evaluating a $g$-dimensional formal group law on $(m^i)^g$;

(ii) $\bigcap_{i \geq 1} G^i = \{0\}$;

(iii) For all $i \geq 1$, $G^i/G^{i+1} \cong (k, +)$ is finite of exponent $p$; and
THERE ARE GENUS ONE CURVES OF EVERY INDEX OVER EVERY INFINITE, FINITELY GENERATED FIELD

(iv) $G^1[\text{tors}] = G^1[p^\infty]$ [LALG, LG 4.25, Thm. 3].

Step 1: We show that $G[\text{tors}]$ is finite if and only if $G[p]$ is finite. (They need not hold in characteristic $p$; take $G = G_a = (R,+).$) Clearly $G[\text{tors}]$ finite implies $G[p]$ finite. Conversely, if $G[p]$ is finite, then it follows from (iv) and (ii) that $G^n$ is torsionfree for all sufficiently large $n$, and then (iii) implies that $G[\text{tors}]$ is finite.

Step 2: From now on we assume that $G[\text{tors}]$ is finite. In particular then $G[\text{tors}]$ has finite exponent, and then [Ba36, Thm. 8:5] implies that there is a torsionfree subgroup $H$ of $G$ such that

$$G = H \oplus G[\text{tors}]$$

Thus (at least as an abstract group), $H$ is isomorphic to the torsionfree profinite commutative group $G/G[\text{tors}]$. Since $G$ has a finite index pro-$p$-subgroup (namely $G^n$ for sufficiently large $n$), it follows that $H$ is pro-$p$, so by Lemma 5.1,

$$H \cong G/G[\text{tors}] \cong \prod_{i \in I} \mathbb{Z}_p$$

for some index set $I$, and since $G/G[\text{tors}]$ is second countable, $I$ is countable. Thus

$$G \cong \left( \bigoplus_{i \in I} \mathbb{Z}_p \right) \oplus G[\text{tors}]$$

Step 3: Suppose char $K = 0$. Then $K$-adic Lie groups $G$ and $H$ have isomorphic open subgroups if and only if their Lie algebras are isomorphic [LALG, LG 5.34 Cor. 1]. So every $g$-dimensional compact, commutative $K$-adic Lie has an open subgroup isomorphic to $R^g \cong \mathbb{Z}_p^{dg}$. This applies to our $G$ and gives in particular that $G$ is topologically finitely generated, so all finite index subgroups of $G$ are open. Thus $H \cong \prod_{i \in I} \mathbb{Z}_p$ and $\mathbb{Z}_p^{dg}$ are both open subgroups of $G$; it follows easily that $H \cong \mathbb{Z}_p^{dg}$. This completes the proof of part a).

Step 4: If char $K = p > 0$, then in the formal group $G_1$, we have $[p] \in R[[X_1^{p^a}, \ldots, X_g^{p^a}]]^g$ [LALG, LG 4.21 Cor. and LG 4.29 Exc. 7]. (A different proof using invariant differentials is given in the $g = 1$ case – which is the case of our Main Theorem – in [AECI, Cor. 4.4]. It is straightforward to adapt this argument to the general case using the corresponding properties of invariant differentials on abelian varieties.) Consider $pG_1$ as a subset of the profinite space $G_1 = (tF_q[[t]])^g$. It is compact, hence closed. Moreover, it lies in $(tF_q[[t^p]])^g$, so it is not open. We deduce that $G_1/pG_1$ is infinite. Since $G_1$ and $H$ are finite index subgroups of $G$, it follows that $H/pH$ is infinite, and thus $I$ is infinite. Since $I$ is countable, $G \cong \prod_{i=1}^\infty \mathbb{Z}_p \oplus G[\text{tors}]$. 

We immediately deduce the following result.

**Corollary 5.3.** We retain the notation of Theorem 5.2.

a) If $A(K)$ contains a point of order $n$, then so does $A(K)/nA(K)$.

b) For all $a \geq 1$, $A(K)/p^aA(K)$ contains a point of order $p^a$.

c) If char $K > 0$, then for all $a \geq 1$, $A(K)/p^aA(K)$ contains an infinite subset which is LI over $\mathbb{Z}/p^a\mathbb{Z}$.

The following key technical result records a global consequence of this local analysis.
Lemma 5.4. Let $K$ be a global field, and let $A/K$ be an abelian variety of dimension $g \geq 1$. Let $n > 1$ be an integer.

a) If $\text{char } K \nmid n$, then there is a positive density set $\mathcal{P}$ of finite places of $K$ such that for all $v \in \mathcal{P}$, $H^1(K_v, A)$ has an element of $n$.

b) If $\text{char } K = p$ is a prime and $n = p^\alpha$ for $\alpha \geq 1$, then for every place $v$ of $K$, $H^1(K_v, A)$ has infinitely many elements of order $n$.

Proof. Step 1: For any finite place $v$ of $K$, the discrete torsion group $H^1(K_v, A)$ is Pontrjagin dual to the compact profinite group $A(K_v)$: this celebrated Local Duality Theorem is due to Tate [Ta57, Proposition 1] when $\text{char } K = 0$ and to Milne [Mi70] when $\text{char } K > 0$. It follows that for $n \geq 1$, the groups $H^1(K_v, A)[n]$ and $A(K_v)/nA(K_v)$ are Pontrjagin dual.

Step 2: Suppose $\text{char } K \nmid n$. Then, as already recalled, $A[n]$ is a finite etale group scheme, so there is a finite Galois extension $L/K$ such that $A(L)[n] \cong (\mathbb{Z}/n\mathbb{Z})^{2g}$. By the Cebotarev Density Theorem, the set of finite places $v$ which split completely in $L$ has positive density (which one can explicitly bound below in terms of $n$ and $g$, if needed). For each such $v$, there is a $K$-algebra embedding $L \hookrightarrow K_v$ and thus $A(K_v)[n] \cong (\mathbb{Z}/n\mathbb{Z})^{2g}$. By Corollary 5.3, $A(K_v)/nA(K_v)$ has a point of order $n$ (in fact $2g$ points which are LI over $\mathbb{Z}/n\mathbb{Z}$), so by Local Duality so does $H^1(K_v, A)$. This establishes part a).

Step 3: Suppose $\text{char } K = p$ and $n = p^\alpha$ for $\alpha \geq 1$. In this case $A[p^\alpha]$ is never etale and need not admit an etale subgroup scheme of exponent $p^\alpha$: c.f. Remark 6.3, so the argument of Step 2 breaks down. Fortunately it is not needed Combining Corollary 5.3 with Local Duality yields the (stronger!) result in this case.

5.2. A Local-Global Isomorphism in WC-Groups.

Let $K$ be a global field, $A/K$ an abelian variety, and $p$ be a prime number. Put

$$T_p \text{Sel } A = \lim_{\alpha} \text{Ker } \left( H^1(K, A[p^\alpha]) \to \bigoplus_{v \in \Sigma_K} H^1(K_v, A[p^\alpha]) \right).$$

We need the following result of González-Avilés-Tan, a generalization of work of Cassels-Tate. In what follows, $A^\lor$ denotes the dual abelian variety of the abelian variety $A$, $G^\lor$ denotes the pro-$p$-completion of the commutative group $G$, and $G^\lor$ denotes the Pontrjagin dual of the commutative group $G$.

Theorem 5.5. For $A/K$ an abelian variety over a global field, and $p$ any prime number – the case $p = \text{char } K$ is allowed – we have an exact sequence

$$0 \to T_p \text{Sel } A^\lor \to \prod_{v \in \Sigma_K} (A^\lor(K_v))^\lor \to (H^1(K, A)[p^\infty])^* \to (\text{III}(K, A)[p^\infty])^* \to 0. \quad (8)$$

Using Tate-Milne Local Duality to identify $H^1(K_v, A)$ and $A^\lor(K_v)$ as Pontrjagin duals, the map $\alpha$ is the Pontrjagin dual of the natural map

$$H^1(K, A)[p^\infty] \to \bigoplus_{v \in \Sigma_K} H^1(K_v, A)[p^\infty].$$

Proof. This is the main result of [GAT07].
Corollary 5.6. Let $A/K$ be an abelian variety defined over a global field. If $A^\vee(K) = \Sha(K, A) = 0$, then the local restriction maps induce an isomorphism of groups

$$H^1(K, A) \simeq \bigoplus_{v \in \Sigma_K} H^1(K_v, A).$$

Proof. Since WC-groups are torsion, it is enough to restrict to $p$-primary components for all primes $p$. Since $A^\vee(K) = 0$, $T_p \Sel A^\vee = 0$, and then (8) gives an isomorphism

$$\prod_{v \in \Sigma_K} (A^\vee(K_v))^\wedge \simeq H^1(K, A)[p^n].$$

Taking Pontrjagin duals and applying Tate-Milne Local Duality, we get

$$H^1(K, A)[p^n] \xrightarrow{\sim} \bigoplus_{v \in \Sigma_K} H^1(K_v, A)[p^n].$$

Lemma 5.7. Let $E/K$ be an elliptic curve over a global field, and let $\eta \in H^1(K, E)$ be locally trivial at all places of $\Sigma_K$ except (possibly) one. Then $P(\eta) = I(\eta)$.

Proof. In the number field case this is [Cl05, Prop. 6], for which two proofs are given. The second proof works verbatim in the function field case. The first proof, which makes use of the period-index obstruction map, works if one uses the extension of $\Delta$ to the case char $K | n$ given in [WCIV, § 2.3].

5.3. Proof of Theorem 4.1.

Let $K$ be a global field, and let $E/K$ be an elliptic curve with $E(K) = \Sha(K, E) = 0$. Let $n > 1$; we must show that there is an LI over $\mathbb{Z}/n\mathbb{Z}$ subset of $H^1(K, A)$ consisting of classes with index $n$.

By Corollary 5.6 have an isomorphism

$$H^1(K, A) \simeq \bigoplus_{v \in \Sigma_K} H^1(K_v, A).$$

With all our preparations in hand, the proof is simple: for each of an infinite set $\mathcal{P}$ of finite places $v$ of $K$, we find a class $\eta_v \in H^1(K_v, A)$ of period $n$, realize this class as an element of the right hand side of (9) supported at $v$, and pull back via the isomorphism to get a class $\eta$ in $H^1(K, A)$. This class has period $n$, and since it is locally trivial except at $v$, by Lemma 5.7 it also has index $n$. Doing this for each $v \in \mathcal{S}$ we get a finite subset $\mathcal{S} \subset H^1(K, A)[n]$ which is LI over $\mathbb{Z}/n\mathbb{Z}$ because each class lies in a different direct summand. We implement this in several steps, corresponding to the preliminary results we have established.

Step 1: Suppose char $K \nmid n$. Then we apply Lemma 5.4a) to get our infinite set $\mathcal{P}$ of finite places of $v$ and $\eta_v \in H^1(K_v, A)$ of order $n$. This completes the proof if char $K = 0$.

Step 2: Suppose char $K = p > 0$ and $n = p^a$. Then we apply Lemma 5.4b) and
thus we may take $P = \Sigma K$.

Step 3: Finally, suppose $\text{char } K = p > 0$ and write $n = p^a m$ with $\gcd(m, p) = 1$. By Step 1, there is an infinite LI over $\mathbb{Z}/m\mathbb{Z}$ subset $S_1 \subset H^1(K, A)[m]$ such that every $\eta_1 \in S_1$ has index $m$. By Step 2, there is an infinite LI over $\mathbb{Z}/p^a\mathbb{Z}$ subset $S_2 \subset H^1(K, A)[p^a]$ such that every $\eta_2 \in S_2$ has index $p^a$. Using Lemma 6.1 we find (easily) that $S_1 + S_2$ is an infinite LI over $\mathbb{Z}/n\mathbb{Z}$ subset of $H^1(K, A)[n]$ such that every $\eta \in S$ has index $n$.

6. The Proof of Theorem 4.2

Now we will prove Theorem 4.2: for every prime number $p$, the elliptic curve

$$E_{/\mathbb{F}_p(t)} : y^2 + txy + t^4y = x^3 + t^2x^2 + t^4x + t^5$$

has trivial Mordell-Weil and Shafarevich-Tate groups.

6.1. Controlling the torsion.

We deal with the $p$-primary torsion and prime-to-$p$ torsion in $E(\mathbb{F}_p(t))$ separately.

**Lemma 6.1.** Let $k$ be a field of characteristic $p > 0$, and $E_{/k}$ an elliptic curve. If $E(k)[p^\infty] \neq 0$, then $j(E) \notin k^p$.

**Proof.** Let $P \in E(k)$ be a nontrivial $p$-torsion point. Let $E' = E/(P)$ be the quotient of $E$ by the cyclic group generated by $P$. We have a separable isogeny $\Phi : E \to E'$ with kernel $\langle P \rangle$ and of degree $p$. If $\Phi^\vee : E' \to E$ is its dual isogeny, we have a factorization of multiplication by $p$ on $E$ as

$$[p] : E \xrightarrow{\Phi} E' \xrightarrow{\Phi^\vee} E$$

Since $[p] : E \to E$ is inseparable of degree $p^2$, we must have that $\Phi^\vee$ is inseparable of degree $p$. But an elliptic curve in characteristic $p$ has a unique inseparable isogeny of degree $p$, namely the quotient by the kernel of Frobenius, so $\Phi^\vee$ must be the Frobenius map on $E'$, and thus $E \cong (E')^{(p)}$ and $j(E) = j((E')^{(p)}) = (j(E'))^p \in k^p$.

We get as an immediate consequence:

**Corollary 6.2.** Let $E_{/\mathbb{F}_p(t)}$ an elliptic curve with $j(E) \notin \mathbb{F}_p$. If $j(E) \notin \mathbb{F}_p(1^p)$, then $E(\mathbb{F}_p(t))[p^\infty] = 0$.

**Remark 6.3.** In the setting of Corollary 6.2 we have that $E$ is an ordinary elliptic curve which has no $p$-torsion over the separable closure of $\mathbb{F}_p(t)$. This is a concrete instance of a phenomenon encountered in § 3.2. In particular, it serves to clarify why assuming “$A$ is ordinary” in Theorem 1.6 would not be enough (in order for our argument to succeed, at least).

To control the prime-to-$p$ torsion we use the following standard strategy: let $E_{/K}$ be an elliptic curve over a global field, let $v$ be a finite place of $K$, and denote by $K_v$ the corresponding completion. Since $E(K) \hookrightarrow E(K_v)$, it suffices to find a place for which $E(K_v)$ contains no prime-to-$p$ torsion. For a group $G$, we denote by $G[1^p]$ its prime-to-$p$ torsion subgroup. Much as above, we let $R_v$ the valuation ring of $K_v$, $m_v$ the maximal ideal of $R_v$, and $k_v$ its residue field, of characteristic $p$. We denote by $E_{/K_v}$, the reduction of $E$ modulo $m_v$, $E_{m_v}(k_v)$ the set of nonsingular points of
Let $E(K_v)$, $E_0(K_v)$ the set of points of $E(K_v)$ with nonsingular reduction, and $E_1(K_v)$ the kernel of the reduction map $E(K_v) \rightarrow E(k_v)$. We have a short exact sequence

$$0 \rightarrow E_0(K_v) \rightarrow E(K_v) \rightarrow E(K_v)/E_0(K_v) \rightarrow 0$$

The group $E(K_v)/E_0(K_v)$ is always finite, and its order is the number of reduced geometric components of the special fiber of a minimal regular model of $E$ over $\mathbb{Q}_p$ (see e.g. [AECII, Corollary IV.9.2(d)]). We see from [AECII, Table 4.1] that $E(K_v)/E_0(K_v)$ is the trivial group whenever the special fiber is of type II or II*, and in those cases we have $\tilde{E}_\text{ns}(k_v) = k_v^+$. In this case, by [AECI, Proposition VII.2.1] we have a short exact sequence

$$0 \rightarrow E_1(K_v) \rightarrow E(K_v) \rightarrow k_v^+ \rightarrow 0$$

As recalled in § 4.2.2, $E_1(K_v)$ is obtained from a formal group law, so contains no prime-to-$p$ torsion. In particular, if $j(E) \notin (K_v)^*$, Lemma 6.1 and the above short exact sequence imply

$$E_1(K_v)[\text{tors}] = E_1(K_v)[p^\infty] \subset E(K_v)[p^\infty] = 0$$

In this case we have an injection

$$E(K_v)[\text{tors}] = E(K_v)[p^*] \hookrightarrow k_v^+$$

Since $k_v^+$ is a $p$-group, we conclude that $E(K_v)[p^*] = 0$.

We will see that for the elliptic curve in Theorem 4.2, there is always of a place of $\mathbb{P}_p(t)$ for which the special fiber of a minimal model for $E$ is of type II*.

6.2. Controlling the rank.

Let $k$ be a field, $C$ a smooth projective curve over $k$, and $K = k(C)$ the function field of $C$. Let $E/K$ be an elliptic curve. We will always assume that $E$ is nonisotrivial $- j(E) \notin k$. By Lang-Néron, this implies that $E(K)$ is finitely generated. It implies also that $\Delta(E) \notin k$, so the morphism $\Pi : S \rightarrow C$ contains singular fibers, and that the Néron-Severi group $\text{NS}(S)$ is finitely generated. The ranks of $E(K)$ and $\text{NS}(S)$ are related as follows.

**Theorem 6.4** (Shioda-Tate). Let $k$ be an algebraically closed field, let $E_{/K(C)}$ be an nonisotrivial elliptic curve, and let $\Pi : S \rightarrow C$ be its associated minimal elliptic surface. Let $\Sigma$ denote the finite set of points $v \in C$ for which the fiber $\Pi^{-1}(v)$ is singular. For each $v \in \Sigma$, let $m_v$ denote the number of irreducible components of $\Pi^{-1}(v)$. We have

$$\text{rank}(\text{NS}(S)) = \text{rank}(E) + 2 + \sum_{v \in \Sigma} (m_v - 1).$$

**Proof.** See [Sh72, Cor. 1.5].

Now let $C = \mathbb{P}^1$, so $k(C) \cong k(t)$. Then $S \rightarrow \mathbb{P}^1$ admits a Weierstrass equation

$$S = \{ ([X : Y : Z], t) \in \mathbb{P}^2 \times \mathbb{P}^1 : Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3 \}$$

THERE ARE GENUS ONE CURVES OF EVERY INDEX OVER EVERY INFINITE, FINITELY GENERATED FIELD.
for some $a_i(t) \in k[t]$. We define the height of the Weierstrass elliptic surface to be the least $n \in \mathbb{N}$ such that $\deg(a_i) \leq ni$ for all $i$. The height controls the geometry of the total space $S$. If $E_{k(t)}$ has height $n = 1$, the associated minimal elliptic surface $S$ is isomorphic to $\mathbb{P}^2$ blown up at 9 points, so the rank of $\text{NS}(S)$ is 10. See [Sh90, Lemma 10.1] for a different computation of this. Therefore, the Shioda-Tate formula allows us to compute the rank of a height 1 elliptic curve $E_{k(t)}$ from the local information of the singular fibers:

**Corollary 6.5.** For a nonisotrivial elliptic curve $E_{k(t)}$ of height 1, we have

$$\text{rank } E = 8 - \sum_{v \in \Sigma} (m_v - 1)$$

where $\Sigma$ denotes the places of $k(t)$ where $E$ has bad reduction.

Our strategy is to find an elliptic curve for which the contribution from the singular fibers is exactly 8, so rank $E_{k(t)} = 0$ and a fortiori rank $E_{k(t)} = 0$. By Shioda-Tate, this occurs if there is a place $v$ of bad reduction with $m_v = 9$. So we choose the Weierstrass equation in Theorem 4.2 so as to “force” Tate’s algorithm to give us one fiber of reduction type $II^*$ (so $m_v = 9$).

### 6.3. Controlling III.

In order to compute the Shafarevich-Tate group of the elliptic curve in Theorem 1 we use some special features of elliptic curves over function fields of small height.

**Theorem 6.6.** Let $E_{k(t)}$ be an elliptic curve of height $\leq 2$. Then $E$ satisfies the Birch and Swinnerton-Dyer conjecture:

$$\frac{1}{r!} L^{(r)}(E, 1) = \frac{[\text{III}(K, E)] \cdot R \cdot \tau}{\# E(K)[\text{tors}]^{r-1}},$$

where $r = \text{rank}(E)$, $\tau$ is the product of the Tamagawa numbers, $R$ is the regulator of $E$, and $L(E, s)$ is the $L$-function of $E$.

In our application we will have rank $E = 0$, so $R = 1$. So we can compute the order of $\text{III}(k_{F_p(t)}, E)$ from its $L$-function and data from Tate’s algorithm (the Tamagawa numbers). In fact the $L$-function of the elliptic curve (5) also contributes trivially, by virtue of the following result.

**Proposition 6.7** (Grothendieck, Raynaud, Deligne). Let $E_{k(t)}$ be a nonisotrivial elliptic curve. Then the $L$-function of $E$, $L(E_{k(t)}, s)$, is a polynomial in $\mathbb{Z}[s]$ with constant coefficient 1 and degree $\deg(n) - 4$, where $n = n(E)$ is the conductor of $E$.

**Proof.** See e.g. [Ul11, Theorem. 9.3].

### 6.4. Proof of Theorem 4.2.

Now we will put together the pieces to show that the elliptic curve

$$E_{F_p(t)} : \quad y^2 + txy + t^3y = x^3 + t^2x^2 + t^4x + t^5$$
of Theorem 4.2 has \( E(\mathbb{F}_p(t)) = \text{III}(\mathbb{F}_p(t), E) = 0 \).

First, the discriminant and \( j \)-invariant of \( E \) are given by

\[
\Delta(E) = -t^{10}(83t^2 - 199t + 432), \\
j(E) = -\frac{(47)^2 t^2}{\Delta} = \frac{(47)^3 t^2}{83t^2 - 199t + 432}
\]

so we do indeed have an elliptic curve for all \( p \). For \( p \neq 47 \), \( j(E) \notin (\mathbb{F}_p(t))^p \), so by Lemma 6.1, \( E(\mathbb{F}_p(t)) \) has no \( p \)-primary torsion. We verify, using Tate’s algorithm that \( E \) has reduction of type \( \text{II}^* \) at \((t)\), so in particular it has additive reduction with trivial component group, so by the results of §6.1, we conclude that \( E(\mathbb{F}_p(t))[\text{tors}] = 0 \). For \( p = 47 \), \( j(E) = 0 \), so \( E \) is isotrivial and \( j(E) \) is a \( p \)th power

To compute the rank of \( E(\mathbb{F}_p(t)) \) we examine the other singular fibers: for \( p \neq 83 \), \( E \) has one or two more places of bad reduction, depending whether the quadratic \( 83t^2 - 199t + 432 \) factors over \( \mathbb{F}_p[t] \) into two (different) linear factors or not. For \( p = 83 \), \( E \) has bad reduction at \((t + 2)\) and at the place at infinity \((1/t)\). In any case we verify, using Tate’s algorithm, that \( E \) has reduction type \( \text{II}^* \) at \((t)\) and reduction type \( \text{II} \) and the other place(s), so Corollary 6.5 gives us

\[
\text{rank}(E) = 8 - (9 - 1) = 0.
\]

Thus \( E(\mathbb{F}_p(t)) = 0 \) for all primes \( p \).

Now we compute the order of \( \text{III}(\mathbb{F}_p(t), E) \) using formula (10): since \( E(\mathbb{F}_p(t)) = 0 \), we have \( r = 0 \) and \( R = 1 \). Fibers of type \( \text{II}^* \) and \( \text{II} \) have both Tamagawa number 1, so \( \tau = 1 \). Thus formula (10) reduces to \( L(E, 1) = |\text{III}(E)| \), so we need to compute the \( L \)-function. Luckily for us, \( E \) has trivial \( L \)-function: the conductor of \( E \) is

\[
n(E) = \begin{cases} 
3(t) + (t + 1) & , p = 2, 3 \\
2(t) + \text{(Linear}_1) + \text{(Linear}_2) \text{ or } 2(t) + \text{(Quadratic)} & , p > 3, p \neq 83 \\
2(t) + (t + 2) + (1/t) & , p = 83 
\end{cases}
\]

This completes the proof of Theorem 4.2.

**Remark 6.8.** When \( p \neq 47 \), our arguments show \( E(\mathbb{F}_p(t)) = 0 \). However the case \( p = 47 \) is really exceptional: here \( j(E) = 0 \) so \( E \) is isotrivial. Since \( 47 \equiv -1(\mod 3) \), by Deuring’s Criterion \( E \) is supersingular, so \( E(\mathbb{F}_p(t))[p] = 0 \). We still have a fiber of type \( \text{II}^* \), so \( E(\mathbb{F}_p(t))[\text{tors}] = 0 \).

7. The Proof of Theorem 4.3

7.1. Some preliminaries.

**Lemma 7.1.** Let \( L/K \) be a purely transcendental field extension.

a) Let \( V_K \) be an algebraic variety. Suppose either that \( K \) is infinite or \( V \) is complete. Then \( V(L) \neq \emptyset \iff V(K) \neq \emptyset \).

b) For every abelian variety \( A_K \), we have \( H^1(L/K, A) = 0 \).
Proof. a) Step 1: Let \( \{t_i\}_{i \in I} \) be a transcendence basis for \( L/K \). If \( P \in V(L) \), there is a finite subset \( J \subset I \) such that \( P \in V(K(\{t_i\}_{i \in J})) \). So we may assume that \( L/K \) has finite transcendence degree. Induction reduces us to the case \( L = K(t) \).

Step 2: A point \( P \in V(K(t)) \) corresponds to a rational map \( \varphi : \mathbb{P}^1 \to V \). The locus on which \( \varphi \) is not defined is a finite set of closed points of \( \mathbb{P}^1 \). If \( K \) is infinite, so is \( \mathbb{P}^1(K) \), and thus there is \( P \in \mathbb{P}^1(K) \) at which \( \varphi \) is defined, and then \( \varphi(P) \in V(K) \).

On the other hand, any rational map from a regular curve to a complete variety is a morphism, so if \( V \) is complete then e.g. \( \varphi(0) \in V(K) \).

a) Since \( \eta \in H^1(K, A) \) corresponds to a torsor \( V \) under \( A \) and thus a projective variety, this follows immediately from part a).

Remark 7.2. a) If in the statement of Lemma 7.1a) we strengthen “complete” to “projective”, a more elementary proof can be given: let \( \varphi : V \to \mathbb{P}^N \) be a \( K \)-embedding. Since \( K(t) \) is the fraction field of the UFD \( K[t] \), if \( P \in V(L) \), we can write \( \varphi(P) = [f_0(t) : \ldots : f_N(t)] \) with \( \gcd(f_0, \ldots, f_N) = 1 \). In particular, some \( f_i(t) \) is not divisible by \( t \) and thus \( (f_0(0) : \ldots : f_N(0)) \in V(K) \).

b) Let \( K = \mathbb{F}_q \) be a finite field. Then the affine curve \( V = \mathbb{P}^1 \setminus \mathbb{P}^1(\mathbb{F}_q) \) has \( K(t) \)-rational points but no \( K \)-rational points.

Let \( K \) be a field, \( M \) a commutative \( g_K \)-module, \( i \geq 1 \), \( L/K \) a field extension, and consider the restriction map \( \text{Res}_L : H^i(K, M) \to H^i(L, M) \). For \( \eta \in H^i(K, M) \) it is natural to compare both the period and index of \( \eta \) to the period and index of \( \text{Res}_L \eta \).

Let us say that the extension \( L/K \) is index-nonreducing if \( I(\text{Res}_L \eta) = I(\eta) \) for all \( \eta \) and period-nonreducing if \( P(\text{Res}_L \eta) = P(\eta) \) for all \( \eta \). It is then easy to see:

- If \( L/K \) is index-nonreducing, it is also period-nonreducing.
- \( L/K \) is period-nonreducing if and only if \( H^i(L/K, M) = 0 \).

(Thus Lemma 7.1 may be viewed as a result on period-nonreduction.)

However an extension can be period-nonreducing but not index-nonreducing. In our context the difference is immaterial, because our inductive argument gives us classes with period equals index, but in general it would be more useful to have index-nonreduction results. So in the interest of completeness and applicability to future work we also include the following result.

Proposition 7.3. Let \( X/K \) and \( V/K \) be regular, geometrically integral varieties with \( X/K \) complete.\(^1\) Then:

a) We have \( I(V) | I(X)I(V_{/K(X)}) \).

b) If \( I(X) = 1 \) in particular if \( X(K) \neq \emptyset \), we have \( I(V_{/K(X)}) = I(V) \).

Proof. a) It suffices to show the following: for every finite splitting extensions \( M \) of \( V_{/K(X)} \), there is a \( K \)-rational zero-cycle on \( V \) of degree \( [M : K(X)]I(X) \). Let \( L \) be the algebraic closure of \( K \) in \( M \), so there is an \( L \)-variety \( \tilde{X} \) and a dominant morphism \( \pi : \tilde{X} \to X \) such that \( L(\tilde{X}) = M \). By hypothesis, there is \( P \in V(M) \), which corresponds to an \( L \)-rational map \( \varphi : \tilde{X} \to V \). There is a nonempty Zariski-open subset \( U \subset X \) such that: if \( \tilde{U} = \pi^{-1}(U) \), then \( \varphi|_{\tilde{U}} : \tilde{U} \to V \) is a morphism

\(^1\)It is enough to assume that \( X \) admits a resolution of singularities.
and \( \pi|_{\hat{U}} : \hat{U} \to U \) is a finite morphism. By [Cl07, Lemma 12], there is a \( K \)-rational zero-cycle on \( U \) of degree \( I(X) \). Then Trace_{L/K} \varphi_* \pi^* D \) is a divisor on \( V \) of degree 
\[ [M : L(X)] [L : K] \cdot I(X) = I(X)[M : L(X)][L(X) : K(X)] = [M : K(X)]I(X). \]

b) If \( I(X) = 1 \), then by part a) we have \( I(V) | I(V_{K(X)}) \). Since for any extension \( L/K \) we have \( I(V_L) | I(V) \), we conclude \( I(V_{K(X)}) = I(V) \).

\[ \square \]

**Lemma 7.4.** Let \( K \) be a WMW field, \( L/K \) be a finite separable field extension, and \( A/K \) an abelian variety. Then \( H^1(L/K, A) \) is finite.

**Proof.** Let \( M \) be the Galois closure of \( L/K \). Since \( H^1(L/K, A) \subset H^1(M/K, A) \), we may replace \( L \) with \( M \) and thus assume that \( L/K \) is finite Galois, say of degree \( n \). Because the period divides the index, we have \( H^1(L/K, A) = H^1(L/K, A)[n] \).

The short exact sequence of \( K \)-group schemes
\[
0 \to A[n] \to A \xrightarrow{n} A \to 0
\]
may be viewed as a short exact sequence of sheaves on the flat site of \( \text{Spec} \; K \), so we may take cohomology, getting the **Kummer sequence**
\[
0 \to A(K)/nA(K) \to H^1(K, A[n]) \to H^1(K, A)[n] \to 0
\]
in flat cohomology. (The finite flat group scheme \( A[n] \) is etale iff \( \text{char} \; K \nmid n \); in this case the Kummer sequence can be more simply viewed as a sequence of \( \text{étale} = \text{Galois cohomology groups. But in our application we need the general case.) There is also a Kummer associated to multiplication by } n \text{ on } A_L/\ell. Restriction from } K \text{ to } L \text{ gives a commutative ladder}
\[
\begin{array}{ccccccc}
0 & \to & A(K)/nA(K) & \longrightarrow & H^1(K, A[n]) & \longrightarrow & H^1(K, A)[n] & \longrightarrow & 0 \\
\downarrow & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \to & A(L)/nA(L) & \longrightarrow & H^1(L, A[n]) & \longrightarrow & H^1(L, A)[n] & \longrightarrow & 0 \\
\end{array}
\]
Let \( \mathcal{K} \) and \( \mathcal{C} \) be the kernel and cokernel of the restriction map \( A(K)/nA(K) \to A(L)/nA(L) \). The Snake Lemma gives an exact sequence
\[
0 \to H^1(L/K, A[n])/\mathcal{K} \to H^1(L/K, A) \to \mathcal{C},
\]
so to show that \( H^1(L/K, A) \) is finite it is sufficient to show that \( \mathcal{C} \) and \( H^1(L/K, A[n]) \) are both finite. The group \( A(L)/nA(L) \) is finite because \( K \) is WMW, hence its quotient \( \mathcal{C} \) is also finite. Finally, because \( L/K \) is Galois, by [W, Thm., § 17.7], \( H^1(L/K, A[n]) = H^1(\text{Aut}(L/K), A[n])(L) \). The right hand side of the last equation is the cohomology of a finite group with coefficients in a finite module, so it is a quotient of a finite group of cochains and thus is certainly finite.

\[ \square \]

**Remark 7.5.** Let \( p \) be a prime number, let \( K = \mathbb{F}_p((t)) \), \( L = \mathbb{F}_p((t^{1/p})) \), and let \( E_{/K} \) be a (supersingular?!?) elliptic curve. Then \( H^1(L/K, E) = H^1(K, E)[p] \) is infinite (Shatz...).
7.2. Proof of Theorem 4.3.

Let \( t_1, \ldots, t_d \) be a separating transcendence basis for \( L/K \) and put \( K' = K(t_1, \ldots, t_d) \).

By Lemma 7.1, \( H^1(K'/K, A) = 0 \), so by Lemma 2.2a), \( \text{Res}_{K'} S \subset H^1(K', A)[n] \) is infinite and 2-LI over \( \mathbb{Z}/n\mathbb{Z} \). Moreover, since \( K \) is WMW, by Proposition 1.4 so is \( K' \). Thus we may as well assume that \( K' = K \) and \( L/K \) is a finite separable.

By Lemma 7.4, \( H^1(L/K, A) \) is finite. By Lemma 2.2b), there is \( S' \subset S \) such that \( \text{Res}_L S' \subset H^1(L, A)[n] \) is infinite and 1-LI over \( \mathbb{Z}/n\mathbb{Z} \), and the latter condition means that every element of \( \text{Res}_L S' \) has period dividing \( n \).

Finally, we suppose that every element of \( S \) has index \( n \). Then on the one hand every element of \( \text{Res}_L S' \) has index dividing \( n \), whereas on the other hand every element of \( \text{Res}_L S' \) has period dividing its index, hence every element of \( \text{Res}_L S' \) has index \( n \).

References


THERE ARE GENUS ONE CURVES OF EVERY INDEX OVER EVERY INFINITE, FINITELY GENERATED FIELD


[St02] W.A. Stein, *There are genus one curves over Q of every odd index*. J. Reine Angew. Math. 547 (2002), 139-147.


DEPARTMENT OF MATHEMATICS, BOYD GRADUATE STUDIES RESEARCH CENTER, UNIVERSITY OF GEORGIA, ATHENS, GA 30602-7403, USA

E-mail address: pete@math.uga.edu
E-mail address: alacy@math.uga.edu