# A LOWER BOUND FOR THE CANONICAL HEIGHT ON ABELIAN VARIETIES OVER ABELIAN EXTENSIONS

MATTHEW H. BAKER AND JOSEPH H. SILVERMAN

ABSTRACT. Let $A$ be an abelian variety defined over a number field $K$ and let $\hat{h}$ be the canonical height function on $A(\bar{K})$ attached to a symmetric ample line bundle $\mathcal{L}$. We prove that there exists a constant $C = C(A, K, \mathcal{L}) > 0$ such that $\hat{h}(P) \geq C$ for all nontorsion points $P \in A(K^{\mathrm{ab}})$, where $K^{\mathrm{ab}}$ is the maximal abelian extension of $K$.

## Introduction

The purpose of this paper is to provide a proof of the following result.

**Theorem 0.1.** *Let $A/K$ be an abelian variety defined over a number field $K$. Let $\mathcal{L}$ be a symmetric ample line bundle on $A/K$, and let $\hat{h} : A(\bar{K}) \to \mathbb{R}$ be the associated canonical height function. Then there exists a constant $C = C(A, K, \mathcal{L}) > 0$ such that*

$$\hat{h}(P) \geq C \quad \text{for all nontorsion points } P \in A(K^{\mathrm{ab}}).$$

Together with Remark 5.4, Theorem 0.1 establishes both parts of Conjecture 1.10 in [3].

In the case of elliptic curves, Theorem 0.1 was proven by the first author [3] for CM elliptic curves and by the second author [27] for non-CM elliptic curves. The present paper is thus a combination and extension of these two earlier works to abelian varieties of arbitrary dimension. The two papers [3] and [27] were themselves motivated by work of Amoroso-Dvornicich and Amoroso-Zannier ([1], [2]) providing absolute lower bounds for the height of nontorsion points in the multiplicative group over abelian extensions of a given number field $K$. For more history and background information on the elliptic curve and multiplicative group analogues of Theorem 0.1, we refer the reader to sections 1 and 2 of [27].

Theorem 0.1 fits into the general context of providing lower bounds for the heights of nontorsion points on abelian varieties. An open problem in this context is the generalized Lehmer conjecture (Conjecture 1.4 of [4]):

| Lower bound for $\hat{h}(P)$ | Restrictions | Reference |
|---|---|---|
| $cD^{-\kappa}$ | none | Masser (1984) [13] |
| $cD^{-\frac{1}{g}}\left(\frac{\log\log(3D)}{\log(3D)}\right)^{\kappa}$ | CM, $g = g_0(P)$ | David-Hindry (2000) [4] |
| $c$ | $P \in A(K^{\mathrm{ab}})$ $K$ totally real | Zhang (1998) [32] |
| $c$ | $P \in A(K^{\mathrm{ab}})$ $g = 1$ | Baker, Silverman (2003) [3],[27] |

TABLE 1. History of lower bounds for $\hat{h}$ in $A(\bar{K})$

**Conjecture 0.2.** *Suppose $A$ is an abelian variety over a number field $K$, and that $\mathcal{L}$ is a symmetric ample line bundle on $A$. Then there exists a positive constant $c = c(A, K, \mathcal{L})$ such that*
$$\hat{h}(P) \geq cD^{-1/g_0(P)}$$
*for all non-torsion points $P \in A(\bar{K})$, where $D = [K(P) : K]$ and $g_0(P)$ denotes the dimension of the smallest algebraic subgroup of $A$ containing $P$.*

Table 1 gives an abbreviated history of lower bounds for $\hat{h}(P)$, where $A$ is an abelian variety of dimension $g$ over a number field $K$, $\mathcal{L}$ is a symmetric ample line bundle on $A$, $P \in A(\bar{K})$ is a nontorsion point, and $D = [K(P) : K]$. In the table, $c$ denotes a positive constant that depends on $A/K$ and on $\mathcal{L}$, but not on $P$, and $\kappa$ denotes a positive constant depending only on the dimension of $A$.

In light of the results of [1] and [2] for the multiplicative group, one might also ask if Theorem 0.1 admits a generalization to arbitrary semiabelian varieties. We do not address this question here.

## 1. Notation

We set the following notation and normalizations, which will be used throughout this paper.

$K$    a number field.

$K^{\mathrm{ab}}$    the maximal abelian extension of $K$.

$\mathcal{O}_K$    the ring of integers of $K$.

$q_{\mathfrak{p}}$    the absolute norm $\mathrm{N}_{K/\mathbb{Q}}(\mathfrak{p})$ of the ideal $\mathfrak{p}$.

$M_K$    the set of places of $K$.

$n_v$    the normalized local degree $[K_v : \mathbb{Q}_v]/[K : \mathbb{Q}]$, for $v \in M_K$.

$|\cdot|_v$    the unique absolute value on $K$ in the equivalence class of $v \in M_K$ that extends the standard absolute value on the completion $\mathbb{Q}_v$.

$h$    The absolute logarithmic Weil height $h : \mathbb{P}^n(\bar{\mathbb{Q}}) \to \mathbb{R}$ defined for $[x_0, \ldots, x_n] \in \mathbb{P}^n(K)$ by

$$h\big([x_0, \ldots, x_n]\big) = \sum_{v \in M_K} n_v \log\max\{|x_0|_v, \ldots, |x_n|_v\}.$$

The height $h(P)$ is well-defined, independent of the choice of a particular number field $K$ over which the point $P = [x_0, \ldots, x_n]$ is defined. See [10, 12, 25] for this and other basic properties of height functions.

*Remark* 1.1. Let $\mathfrak{p}$ be a prime ideal of $K$ corresponding to a place $v \in M_K$. Then the largest value less than 1 of the normalized absolute value attached to $v$ is

$$\max_{\alpha \in \mathfrak{p}} |\alpha|_v = q_{\mathfrak{p}}^{-1/[K_v : \mathbb{Q}_v]}.$$

We set the following additional notation.

$A/K$     an abelian variety of dimension $g$ defined over $K$.

$\mathrm{End}(A)$     the endomorphism ring of $A$ over $\bar{K}$.

$\mathcal{L}$     an ample symmetric line bundle on $A/K$.

$\hat{h}$     the canonical height $\hat{h} : A(\bar{K}) \to [0, \infty)$ associated to $\mathcal{L}$. If we need to make the dependence on $A$ and/or $\mathcal{L}$ explicit, we will write $\hat{h}_{\mathcal{L}}$ or $\hat{h}_{A, \mathcal{L}}$.

$\mathcal{S}$     a finite set of places of $K$ that includes at least all archimedean places and all places of bad reduction of $A$. From time to time we may expand the set $\mathcal{S}$, but it will depend only on $A/K$, and not on particular points of $A$ or the extensions over which they are defined.

## 2. A reduction step

Theorem 0.1 deals with arbitrary abelian varieties and ample line bundles. We begin with a reduction step to a simpler situation.

**Proposition 2.1** (Reduction Step).   (a) *If Theorem 0.1 is true for geometrically simple abelian varieties and very ample symmetric line bundles, then it is true for all abelian varieties and all ample symmetric line bundles.*

(b) *If Theorem 0.1 is true for $A/K'$ for some finite extension $K'/K$, then it is true for $A/K$. In particular, if $A$ has complex multiplication, it suffices to prove Theorem 0.1 under the assumption that $\mathrm{End}_K(A) = \mathrm{End}_{\bar{K}}(A)$ and $\mathrm{End}_K(A) \otimes \mathbb{Q} \subset K$.*

*Proof.* (a) Let $A/K$ be an arbitrary abelian variety and $\mathcal{L}$ an ample symmetric line bundle on $A/K$.

Over an algebraically closed field, Poincaré's complete reducibility theorem [16, Section 19] says that every abelian variety decomposes, up to isogeny, into a product of simple abelian varieties. We may thus find a finite extension $K'$ and geometrically simple abelian varieties $A_1, \ldots, A_r$ defined over $K'$ so that there are isogenies

$$\phi : A_1 \times \cdots \times A_r \longrightarrow A \quad \text{and} \quad \psi : A \longrightarrow A_1 \times \cdots \times A_r$$

defined over $K'$ with the property that $\phi \circ \psi = [m]$ is multiplication-by-$m$ on $A$ for some integer $m \geq 1$.

The line bundle $\phi^* \mathcal{L}$ is ample on the product $A_1 \times \cdots \times A_r$, since $\phi$ is a finite morphism [8, Exercise III.5.7(d)]. We fix an integer $n \geq 1$ so that $\phi^* \mathcal{L}^{\otimes n}$

is very ample on the product, and we let $\mathcal{L}'_i = \phi^* \mathcal{L}^{\otimes n}\big|_{A_i}$ be the restriction to the $i^{\text{th}}$ factor. Then $\mathcal{L}'_i$ is a very ample line bundle on $A_i$.

Let $P \in A(\bar{K})$ and write $\psi(P) = (P_1, \dots, P_r)$. Then standard transformation properties of canonical heights (see [12, Chapters 4–5] or [10, Sections B.3–B.5]) allow us to compute

$$
\begin{aligned}
\hat{h}_{A,\mathcal{L}}(P) &= \frac{1}{m^2} \hat{h}_{A,\mathcal{L}}([m]P) \\
&= \frac{1}{m^2 n} \hat{h}_{A,\mathcal{L}^{\otimes n}}([m]P) \\
&= \frac{1}{m^2 n} \hat{h}_{A_1 \times \cdots \times A_r, \phi^* \mathcal{L}^{\otimes n}}(\psi(P)) \\
&= \frac{1}{m^2 n} \left( \hat{h}_{A_1, \mathcal{L}'_1}(P_1) + \hat{h}_{A_2, \mathcal{L}'_2}(P_2) + \cdots + \hat{h}_{A_r, \mathcal{L}'_r}(P_r) \right).
\end{aligned}
$$

By assumption, Theorem 0.1 is true for each abelian variety $A_i/K'$ and line bundle $\mathcal{L}'_i$, say

$$
\hat{h}_{A_i, \mathcal{L}'_i}(P) \geq C_i > 0 \qquad \text{for all nontorsion } P \in A_i(K'^{\mathrm{ab}}).
$$

Since $K^{\mathrm{ab}} \subset K'^{\mathrm{ab}}$ and since

$$
P \in A_{\mathrm{tors}} \iff P_i \in (A_i)_{\mathrm{tors}} \text{ for all } 1 \leq i \leq r,
$$

we conclude that if $P \in A(K^{\mathrm{ab}})$ is a nontorsion point, then

$$
\hat{h}_{A,\mathcal{L}}(P) \geq \frac{1}{m^2 n} \min_{1 \leq i \leq r} C_i.
$$

This completes the proof of reduction step (a).

(b) It is clear that Theorem 0.1 for $K'$ implies Theorem 0.1 for $K$, since $K^{\mathrm{ab}} \subset K'^{\mathrm{ab}}$. The second part of (b) follows, since there is always a finite extension $K'/K$ satisfying $\mathrm{End}_{K'}(A) = \mathrm{End}_{\bar{K}}(A)$ and $\mathrm{End}_{K'}(A) \otimes \mathbb{Q} \subset K'$. $\qquad \square$

In view of Proposition 2.1(a), we will assume henceforth that the abelian variety $A/K$ is geometrically simple and that the line bundle $\mathcal{L}$ on $A/K$ is very ample. We fix an embedding

$$
\psi : A \longrightarrow \mathbb{P}^n_K
$$

with $\psi^*(\mathcal{O}(1)) \cong \mathcal{L}$. We fix a proper model $\mathcal{A}/\mathcal{O}_K$ for $A/K$ by letting $\mathcal{A}$ be the Zariski closure of $\psi(A)$ in $\mathbb{P}^n_{\mathcal{O}_K}$. In particular, the embedding $\psi$ extends to a closed immersion

$$
\mathcal{A} \longrightarrow \mathbb{P}^n_{\mathcal{O}_K}.
$$

Adding a finite number of primes to the set $\mathcal{S}$, we may assume that $\mathcal{A}$ is a group scheme over $\mathrm{Spec}\, \mathcal{O}_{K,\mathcal{S}}$ with generic fiber $A/K$. In particular, the group law on $\mathcal{A}$ commutes with reduction modulo $\mathfrak{p}$ for $\mathfrak{p} \notin \mathcal{S}$. More precisely, if $P, Q, R \in A(K')$ for some finite extension $K'/K$, and if $\mathfrak{P} \in \mathrm{Spec}\, \mathcal{O}_{K'}$ is a prime of $K'$ that does not lie above a prime in $\mathcal{S}$, then

$$
P \equiv Q \pmod{\mathfrak{P}} \iff P + R \equiv Q + R \pmod{\mathfrak{P}}.
$$

### 3. An elementary local-global height inequality

For each place $v \in M_K$, we define a logarithmic $v$-adic distance function on $\mathbb{P}^n(K)$ by the formula

$$\delta_v(x, y) = -\log\left(\frac{\left(\max_{i,j} |x_i y_j - x_j y_i|_v\right)}{\left(\max_k |x_k|_v\right)\left(\max_k |y_k|_v\right)}\right).$$

Note that $\delta_v(x, y)$ does not depend on the choice of projective coordinates for $x$ and $y$. The intuition is that

$$\delta_v(x, y) = -\log |v\text{-adic distance from } x \text{ to } y|,$$

so $\delta_v(x, y)$ becomes large as $x$ and $y$ become $v$-adically close to one another. We set $\delta_v(x, x) = \infty$ by convention.

**Lemma 3.1.** *Let $K$ be a number field and let $T \subset M_K$ be any set of places of $K$. Then for all* distinct *points $x, y \in \mathbb{P}^n(K)$,*

$$h(x) + h(y) \geq \sum_{v \in T} n_v \delta_v(x, y) - \log 2.$$

*Proof.* For each $v \in M_K$, let $\epsilon_v = 1$ if $v$ is archimedean, and $\epsilon_v = 0$ otherwise. The triangle inequality gives

$$\max_{i,j} |x_i y_j - x_j y_i|_v \leq \max_{i,j} 2^{\epsilon_v} \max\{|x_i y_j|_v, |x_j y_i|_v\}$$
$$= 2^{\epsilon_v} \max_i\{|x_i|_v\} \max_j\{|y_j|_v\}.$$

Hence

(3.2)        $\delta_v(x, y) \geq -\epsilon_v \log 2$ for all $x, y \in \mathbb{P}^n(K)$ and all $v \in M_K$.

We are given that $x \neq y$, so there exist indices $\alpha, \beta$ so that

$$x_\alpha y_\beta \neq x_\beta y_\alpha.$$

We apply the product formula and the inequality (3.2) to compute

$$h(x) + h(y) = \sum_{v \in M_K} n_v \left(\log \max_k |x_k|_v + \log \max_k |y_k|_v\right)$$
$$= \sum_{v \in M_K} n_v \left(\max_{i,j} \log |x_i y_j - x_j y_i|_v + \delta_v(x, y)\right)$$
$$\geq \sum_{v \in M_K} n_v \left(\log |x_\alpha y_\beta - x_\beta y_\alpha|_v + \delta_v(x, y)\right)$$
$$= \sum_{v \in M_K} n_v \delta_v(x, y) \qquad \text{(by the product formula)}$$
$$\geq \sum_{v \in T} n_v \delta_v(x, y) - \sum_{v \notin T} n_v \epsilon_v \log 2 \qquad \text{(from (3.2))}$$

$$\geq \sum_{v \in T} n_v \delta_v(x, y) - (\log 2) \sum_{v \in M_K^\infty} n_v \qquad \text{(from def of } \epsilon_v)$$

$$\geq \sum_{v \in T} n_v \delta_v(x, y) - \log 2.$$

$\square$

*Remark* 3.3. It is possible to put Lemma 3.1 into a more general context, albeit with an inexplicit constant, using functorial properties of Weil height functions associated to subschemes. We briefly sketch the idea; see [26] for the general theory. Let $H$ be a hyperplane in $\mathbb{P}^n$, and for each $i \neq j$, let $D_{ij} \in \text{Div}(\mathbb{P}^n \times \mathbb{P}^n)$ be the divisor of type $(1, 1)$ defined by $x_i y_j = x_j y_i$. Then

$$D_{ij} \sim \pi_1^* H + \pi_2^* H, \quad \text{so} \quad h_{D_{ij}} = h_H \circ \pi_1 + h_H \circ \pi_2 + O(1).$$

The diagonal $\Delta \subset \mathbb{P}^n \times \mathbb{P}^n$ is the intersection $\Delta = \cap D_{ij}$, hence [26, Theorem 4.1(b)] says that

$$h_\Delta \leq \min_{i \neq j} h_{D_{ij}} + O(1) = h_H \circ \pi_1 + h_H \circ \pi_2 + O(1).$$

Finally we use the fact that $h_\Delta$ is defined as a sum of local heights

$$h_\Delta = \sum_v \lambda_{\Delta, v},$$

and the local heights are uniformly bounded below away from the support of $\Delta$. Thus for any set of places $T$,

$$h_\Delta \geq \sum_{v \in T} n_v \lambda_{\Delta, v} + O(1).$$

Combining these inequalities and using the fact that $\lambda_{\Delta, v} = \delta_v + O(1)$ yields

$$h(x) + h(y) \geq \sum_{v \in T} n_v \delta_v(x, y) + O(1) \quad \text{for all } (x, y) \in (\mathbb{P}^n \times \mathbb{P}^n)(\bar{K}) \smallsetminus \Delta,$$

which is Lemma 3.1 with an inexplicit constant.

We will apply Lemma 3.1 to our abelian variety as follows.

**Proposition 3.4.** *There is a constant $B = B(K, A, \mathcal{L})$ so that for all finite extensions $L/K$ and all pairs of distinct points $P, Q \in A(L)$, the following two inequalities are valid.*

(a) *Let $T \subset M_K$ be any set of places of $K$. Then*

$$\hat{h}(P) + \hat{h}(Q) \geq \sum_{v \in T} n_v \delta_v(P, Q) - B.$$

(b) *Let $\mathfrak{P}_1, \ldots, \mathfrak{P}_r$ be primes of $\mathcal{O}_L$ lying over primes of $\mathcal{O}_K$ that are not in the set of excluded primes $\mathcal{S}$. Assume further that*

$$P \equiv Q \pmod{\mathfrak{P}_i} \qquad \text{for all } 1 \leq i \leq r.$$

*Then*

$$\hat{h}(P) + \hat{h}(Q) \geq \frac{1}{[L:\mathbb{Q}]} \sum_{1 \leq i \leq r} \log \mathrm{N}_{L/\mathbb{Q}} \, \mathfrak{P}_i - B.$$

*Proof.* Recall that we have fixed an embedding $\psi : A \to \mathbb{P}^n$ corresponding to the line bundle $\mathcal{L}$. We apply Lemma 3.1 to the points $\psi(P)$ and $\psi(Q)$ in $\mathbb{P}^n(L)$ and to the set of places $v \in T$. This yields

$$(3.5) \qquad h(\psi(P)) + h(\psi(Q)) \geq \sum_{v \in T} n_v \delta_v \big( \psi(P), \psi(Q) \big) - \log 2.$$

For all points $R \in A(\bar{K})$, functorial properties of height functions give

$$h_{\mathbb{P}^n, \mathcal{O}(1)}(\psi(R)) = h_{A, \psi^* \mathcal{O}(1)}(R) + O(1)$$
$$(3.6) \qquad\qquad\qquad = h_{A, \mathcal{L}}(R) + O(1) = \hat{h}_{A, \mathcal{L}}(R) + O(1).$$

Combining (3.5) and (3.6) gives part (a) of the proposition.

Let $\{v_1, \dots, v_r\}$ be the places of $L$ corresponding to the set of primes $\{\mathfrak{P}_1, \dots, \mathfrak{P}_r\}$. The congruence $P \equiv Q \pmod{\mathfrak{P}_i}$ implies that $\psi(P) \equiv \psi(Q) \pmod{\mathfrak{P}_i}$ (remember that the map $\psi$ has good reduction at all primes not in $\mathcal{S}$). Hence from Remark 1.1 we see that

$$\delta_{v_i} \big( \psi(P), \psi(Q) \big) \geq \frac{1}{[L_{\mathfrak{P}_i} : \mathbb{Q}_{\mathfrak{P}_i}]} \log \mathrm{N}_{L/\mathbb{Q}} \, \mathfrak{P}_i.$$

Substituting this into (a) gives

$$\hat{h}(P) + \hat{h}(Q) \geq \sum_{1 \leq i \leq r} \frac{n_{v_i}}{[L_{\mathfrak{P}_i} : \mathbb{Q}_{\mathfrak{P}_i}]} \log \mathrm{N}_{L/\mathbb{Q}} \, \mathfrak{P}_i - B$$
$$= \frac{1}{[L:\mathbb{Q}]} \sum_{1 \leq i \leq r} \log \mathrm{N}_{L/\mathbb{Q}} \, \mathfrak{P}_i - B.$$

$\square$

## 4. A mod $\mathfrak{p}$ annihilating polynomial

The proof of Theorem 0.1 is by induction on the amount of ramification in a given finite abelian extension of $K$. The key to handling the unramified case is to note that there is an element of the group ring $\mathbb{Z}[G_{\bar{K}/K}]$ that simultaneously annihilates $A(K^{\mathrm{ab}})$ modulo every prime of $K^{\mathrm{ab}}$ lying above $\mathfrak{p}$, an idea already exploited in [27] for the case of elliptic curves. In this section we describe the analogous fact for abelian varieties.

**Theorem 4.1.** *Let $K/\mathbb{Q}$ be a number field, let $\mathfrak{p}$ be a prime of $K$, and let $q = \mathrm{N}_{K/\mathbb{Q}}(\mathfrak{p})$. Let $A/K$ be an abelian variety of dimension g with good reduction at $\mathfrak{p}$, and let*

$$\Phi_{\mathfrak{p}}(X) = \det \big( X - \mathrm{Frob}_{\mathfrak{p}} \mid T_\ell(A) \big) \in \mathbb{Z}[X]$$

be the characteristic polynomial of Frobenius at $\mathfrak{p}$. (Here $\ell$ is any prime number different from the residue characteristic of $\mathfrak{p}$, and $T_\ell(A)$ is the $\ell$-adic Tate module of $A$.)

Fix a prime $\bar{\mathfrak{p}}$ of $\bar{K}$ lying over $\mathfrak{p}$ and let $\sigma \in (\bar{\mathfrak{p}}, \bar{K}/K) \subset G_{\bar{K}/K}$ be in the associated Frobenius conjugacy class.

(a) Write $\Phi_{\mathfrak{p}}(X)$ as

$$\Phi_{\mathfrak{p}}(X) = \sum_{i=0}^{2g} a_i X^i = \prod_{j=1}^{2g} (X - \alpha_j).$$

Then the roots of $\Phi_{\mathfrak{p}}$ satisfy $|\alpha_j| = q^{1/2}$ and the coefficients of $\Phi_{\mathfrak{p}}$ satisfy $|a_i| \leq (4q)^g$.

(b) For all $P \in A(\bar{K})$,

$$\Phi_{\mathfrak{p}}(\sigma)P \equiv O \pmod{\bar{\mathfrak{p}}}.$$

(This congruence is taking place on a model $\mathcal{A}$ for $A$ whose special fiber $\tilde{A}$ is smooth.)

(c) If $P \in A(\bar{K})$ satisfies $\Phi_{\mathfrak{p}}(\sigma)P = O$, then $P$ is a torsion point.

*Proof.* (a) The equality $|\alpha_j| = q^{1/2}$ is the Riemann hypothesis for $A(\mathbb{F}_{\mathfrak{p}})$, which was proven originally by Weil, see [16, IV.21, Theorem 4]. The coefficient $a_j$ is the $j^{\text{th}}$ symmetric polynomial of the roots of $\Phi_{\mathfrak{p}}$, so

$$|a_j| \leq \binom{2g}{j} \max |\alpha_i|^j \leq 4^g q^{j/2} \leq (4q)^g.$$

(b) When reduced modulo $\bar{\mathfrak{p}}$, the element $\sigma \in G_{\bar{K}/K}$ acts as the $q$-power Frobenius map $f_q \in \text{End}(\tilde{A})$. Further, the map $\Phi_{\mathfrak{p}}(f_q)$ annihilates $T_\ell(\tilde{A})$, since $\Phi_{\mathfrak{p}}$ is the characteristic polynomial of $f_q$ acting on $T_\ell(\tilde{A})$ and the Cayley-Hamilton theorem tells us that a linear transformation satisfies its own characteristic equation.

We have the general fact that if $B$ is an abelian variety over a field $k$, then the map

$$(4.2) \qquad\qquad \text{End}(B) \longrightarrow \text{End}(T_\ell(B))$$

is injective; see [16, IV.19, Theorem 3] for the stronger result that $\text{End}(B) \otimes \mathbb{Z}_\ell \hookrightarrow \text{End}(T_\ell(B))$. We can prove the injectivity of (4.2) directly by noting that if $\phi \in \text{End}(B)$ induces the zero map on $T_\ell(B)$, then $\phi(B[\ell^n]) = 0$ for all $n \geq 1$. Hence $\phi$ factors through the isogeny $[\ell^n]$, say $\phi = \psi_n \circ [\ell^n]$. This implies that $\deg(\phi) = \deg(\psi_n)\deg([\ell])^n$. Since this holds for all $n \geq 1$, and since $\deg(\phi)$ and $\deg(\psi_n)$ are integers and $\deg([\ell]) > 1$, it follows that $\deg(\phi) = 0$, and hence that $\phi = 0$.

Thus the fact that $\Phi_{\mathfrak{p}}(f_q)$ annihilates $T_\ell(\tilde{A})$ implies that $\Phi_{\mathfrak{p}}(f_q) = 0$ as an element of $\text{End}(\tilde{A})$. In other words,

$$\Phi_{\mathfrak{p}}(f_q)Q = O \qquad \text{for all } Q \in \tilde{A}(\bar{\mathbb{F}}_{\mathfrak{p}}).$$

Finally, using the fact that the reduction map commutes with the group law on $A$, we see that for any $P \in A(\bar{K})$,

$$\Phi_{\mathfrak{p}}(\sigma)P \equiv \Phi_{\mathfrak{p}}(f_q)P \pmod{\bar{\mathfrak{p}}} \equiv O \pmod{\bar{\mathfrak{p}}}.$$

(c) Let $P \in A(\bar{K})$ satisfy $\Phi_{\mathfrak{p}}(\sigma)P = O$. Fix a finite Galois extension $L/K$ with $P \in E(L)$, say of degree $m = [L{:}K]$. Then $\sigma^m = 1$ in $G_{L/K}$, so in particular, $\sigma^m P = P$. Let

$$r = \mathrm{Resultant}(\Phi_{\mathfrak{p}}(X), X^m - 1) \in \mathbb{Z}.$$

The complex roots of $X^m - 1$ have absolute value 1 and from (a), the complex roots of $\Phi_{\mathfrak{p}}(X)$ have absolute value $q^{1/2}$, so the two polynomials have no complex roots in common. It follows that $r \neq 0$.

The resultant of two polynomals in $\mathbb{Z}[X]$ is an element of the ideal that they generate [11, Chapter IV, Section 8], so we can find polynomials $u(X), v(X) \in \mathbb{Z}[X]$ satisfying

$$u(X)\Phi_{\mathfrak{p}}(X) + v(X)(X^m - 1) = r.$$

Substituting $X = \sigma$ gives the identity

$$u(\sigma)\Phi_{\mathfrak{p}}(\sigma) + v(\sigma)(\sigma^m - 1) = r$$

in the group ring $\mathbb{Z}[G_{\bar{K}/K}]$. Hence

$$rP = u(\sigma)\big(\Phi_{\mathfrak{p}}(\sigma)P\big) + v(\sigma)\big((\sigma^m - 1)P\big) = O,$$

so $P$ is a point of finite order.                                              □

## 5. Selection of a "good" prime

In order to prove our main result (Theorem 0.1), we will show that there is a prime $\mathfrak{p}$ of $K$ and positive constants $C_1, C_2, C_3$, depending only on $A/K$ and $\mathcal{L}$, such that

$$\hat{h}_{A,\mathcal{L}}(P) \geq C_1 \frac{\log N_{K/\mathbb{Q}} \, \mathfrak{p} - C_2}{(N_{K/\mathbb{Q}} \, \mathfrak{p})^{C_3}} > 0 \qquad \text{for all nontorsion } P \in A(K^{\mathrm{ab}}).$$

The next proposition will help us choose such a prime $\mathfrak{p}$. We assume from now on that the abelian variety $A$ is $\bar{K}$-simple and that $\mathcal{L}$ is very ample. By Proposition 2.1, these assumptions are harmless.

**Proposition 5.1.** *There exist infinitely many primes $\mathfrak{p}$ of $K$ satisfying the following conditions:*

1. *$\mathfrak{p}$ is unramified of degree one, so that in particular $N_{\mathbb{Q}}^K \mathfrak{p}$ is a prime number $p$.*
2. *Reduction modulo $\mathfrak{p}$ commutes with the embedding $\psi : A \hookrightarrow \mathbb{P}^n$ coming from the very ample symmetric line buncle $\mathcal{L}$.*
3. *The abelian variety $A$ has good reduction at $\mathfrak{p}$, so that in particular, reduction modulo $\mathfrak{p}$ commutes with the group law on $A$.*
4. *$p > \exp([K : \mathbb{Q}](B + 1))$, where $B$ is the constant appearing in Proposition 3.4.*

5. *One of the following holds:*
   (a) *Either $A(K^{\mathrm{ab}})$ has no points of order $p$, or*
   (b) *$A$ has complex multiplication and ordinary reduction at $\mathfrak{p}$.*

*Proof.* It is clear that conditions (2), (3), and (4) exclude only finitely many primes. If $A$ does not have complex multiplication, then the same is true for condition (5a) by a theorem of Zarhin (Theorem 5.3 below). On the other hand, if $A$ does have complex multiplication, then it is well-known that $A$ has ordinary reduction at all sufficiently large primes which split completely in some fixed finite extension of $K$ (see Theorem 5.2 below). Since there are infinitely many rational primes which split completely in any given number field, this shows that we can find (infinitely many) primes satisfying all five conditions. $\qquad\square$

**Theorem 5.2.** *Let $A$ be a $g$-dimensional abelian variety over the number field $K$, and suppose that $L := (\mathrm{End}\,A) \otimes \mathbb{Q}$ is a field of degree $2g$ over $\mathbb{Q}$. Let $\mathfrak{p}$ be a degree-1 prime of $K$ and let $p$ be the rational prime under $\mathfrak{p}$. Suppose that*

1. *$A$ has good reduction at $\mathfrak{p}$;*
2. *Every endomorphism of $A$ has good reduction at $\mathfrak{p}$;*
3. *$\mathrm{End}_K(A) = \mathrm{End}_{\bar{K}}(A)$; and*
4. *$p$ is unramified in $L$.*

*Then $A$ has ordinary reduction at $\mathfrak{p}$.*

*Proof.* Since the property of being ordinary is preserved by isogenies and products, we may assume without loss of generality that $A$ is simple and that $A$ is *principal*, i.e., that $\mathrm{End}(A)$ is the maximal order in $(\mathrm{End}\,A) \otimes \mathbb{Q}$. It then follows from [24, Chapter III, Theorem 2] and our hypotheses that the reduction $\tilde{A}$ of $A$ modulo $\mathfrak{p}$ is also simple, and that the natural reduction map gives an *isomorphism*

$$\mathrm{End}(A) \otimes \mathbb{Q} \xrightarrow{\sim} \mathrm{End}(\tilde{A}) \otimes \mathbb{Q}.$$

In particular, since $L := \mathrm{End}(A) \otimes \mathbb{Q}$ is a CM field of degree $2g$, we conclude that $\mathrm{End}(\tilde{A}) \otimes \mathbb{Q} = L$ is a CM field of degree $2g$ as well.

Let $\pi \in L$ be the Frobenius morphism of $\tilde{A}$ over $\mathbb{F}_p$; then $\pi$ is in fact an element of the ring of integers $\mathcal{O}_L$ of $L$. Let $\bar{\pi}$ be the complex conjugate of $\pi$. A consideration of degrees and the fact that $L$ is a CM field shows that $\pi\bar{\pi} = p$. Since $[L : \mathbb{Q}] = 2g$, it follows from [29, Theorem 2, page 140] that $L = \mathbb{Q}(\pi)$ and that $\Phi$, the characteristic polynomial of $\pi$ acting on $T_\ell(\tilde{A})$ for some prime $\ell \neq p$, has no multiple roots. Since every conjugate of $\pi$ satisfies the polynomial $\Phi$ as an endomorphism of $\tilde{A}$, it follows that

$$\Phi(X) = \prod_{i=1}^{2g}(X - \pi_i),$$

where $\pi_1, \dots, \pi_{2g}$ are the conjugates of $\pi$.

Since $p$ is unramified in $\mathcal{O}_L$, it follows from the relation $p = \pi\pi'$ that for any prime ideal $\mathfrak{q}$ of $\mathcal{O}_L$ lying over $p$ and for each $i$, exactly one of $\pi_i$ and $\bar{\pi}_i$

is divisible by $\mathfrak{q}$. This implies that $\tilde{A}$ is ordinary (see [30, proof of Proposition 7.1]).  $\square$

**Theorem 5.3.** *Let $A/K$ be a geometrically simple abelian variety that does not have complex multiplication (over $\bar{K}$). Then $A(K^{\mathrm{ab}})_{\mathrm{tors}}$ is finite. In particular,*

$$A(K^{\mathrm{ab}})[p] = 0 \quad \text{for all but finitely many primes } p.$$

*Proof.* This is proven by Zarhin in [31], using methods developed by Faltings [5] in his proof of Tate's isogeny conjecture. See also [18, 19, 20, 21].  $\square$

*Remark* 5.4. In the statament of Theorem 5.3, one can replace the hypothesis that $A/K$ is a geometrically simple abelian variety without complex multiplication over $\bar{K}$ by the hypothesis that $A/K$ is an abelian variety having no abelian subvariety with complex multiplication over $K$ (see [18]).

For the remainder of this paper, we fix a prime $\mathfrak{p}$ of $K$ satisfying the conditions described in Proposition 5.1, and we let $p = \mathrm{N}_{K/\mathbb{Q}}\,\mathfrak{p}$.

## 6. Proof of the main theorem in the unramified case

Let $A/K$ be an abelian variety and $\mathcal{L}$ a line bundle on $A/K$. As we have already mentioned, we may assume that $A$ is geometrically simple and $\mathcal{L}$ is very ample. Recall that we have fixed a prime $\mathfrak{p}$ of $K$ satisfying the conditions in Proposition 5.1, and that $p$ is the residue characteristic of $\mathfrak{p}$.

Let $P \in A(K^{\mathrm{ab}})$ be a nontorsion point. The proof of Theorem 0.1 is by induction on $\mathrm{ord}_{\mathfrak{p}}(\mathfrak{f}_{\mathfrak{p}}(K(P)/K))$, where $\mathfrak{f}_{\mathfrak{p}}(L/K)$ denotes the local conductor of the abelian extension $L/K$ at $\mathfrak{p}$. For our purposes, we define $\mathfrak{f}_{\mathfrak{p}}(L/K)$ to be the smallest positive integer $m$ such that $L_{\mathfrak{q}} \subseteq \mathbb{Q}_p(\zeta_m)$, where $\mathfrak{q}$ is a prime of $L$ lying over $\mathfrak{p}$. It follows from local class field theory that $\mathfrak{f}_{\mathfrak{p}}(L/K)$ exists and is well-defined, and that $\mathrm{ord}_{\mathfrak{p}}(\mathfrak{f}_{\mathfrak{p}}(L/K)) \geq 1$ if and only if $L/K$ is ramified at $\mathfrak{p}$. In this section we begin the induction by proving the unramified case.

**Theorem 6.1.** *Let $L \subset K^{\mathrm{ab}}$ be unramified at $\mathfrak{p}$ and let $P \in A(L)$ be a nontorsion point. Then*

$$\hat{h}(P) \geq \frac{1}{(12p)^{2g}}.$$

*(Note that this gives a lower bound for $\hat{h}(P)$ that is independent of $L$ and $P$.)*

*Proof.* Factor the prime $\mathfrak{p}$ in $L$ as

$$\mathfrak{p}\mathcal{O}_L = \mathfrak{P}_1\mathfrak{P}_2\cdots\mathfrak{P}_r.$$

Since $\mathfrak{p}$ is unramified in $L$, the $\mathfrak{p}_i$'s are all distinct. Moreover, the fact that the extension $L/K$ is abelian implies that all of the primes $\mathfrak{P}_1,\ldots,\mathfrak{P}_r$ have the same associated Frobenius element in $G_{L/K}$, say

$$\sigma = (\mathfrak{P}_i, L/K) \in G_{L/K} \qquad \text{for all } 1 \leq i \leq r.$$

Let $\Phi_{\mathfrak{p}}(X) \in \mathbb{Z}[X]$ be the characteristic polynomial of Frobenius acting on $T_\ell(A)$. Theorem 4.1(b) tells us that

$$\Phi_{\mathfrak{p}}(\sigma)P \equiv O \pmod{\mathfrak{P}_i} \qquad \text{for all } 1 \leq i \leq r.$$

Theorem 4.1(c) and our assumption that $P$ is a nontorsion point tell us that $\Phi_{\mathfrak{p}}(\sigma)P \neq O$. Hence we can apply Proposition 3.4(b) to the *distinct* points $\Phi_{\mathfrak{p}}(\sigma)P$ and $O$. Since $\hat{h}(O) = 0$, this yields

$$\hat{h}(\Phi_{\mathfrak{p}}(\sigma)P) \geq \frac{1}{[L : \mathbb{Q}]} \sum_{i=1}^{r} \log \mathrm{N}_{L/\mathbb{Q}} \, \mathfrak{P}_i - B$$

for a constant $B$ that is independent of $L$ and $P$. The factorization $\mathfrak{p} = \mathfrak{P}_1 \cdots \mathfrak{P}_r$ implies that

$$\sum_{i=1}^{r} \log \mathrm{N}_{L/\mathbb{Q}} \, \mathfrak{P}_i = \log \mathrm{N}_{L/\mathbb{Q}} \, \mathfrak{p} = [L : K] \log \mathrm{N}_{K/\mathbb{Q}} \, \mathfrak{p},$$

so we obtain the lower bound

$$\text{(6.2)} \qquad \hat{h}(\Phi_{\mathfrak{p}}(\sigma)P) \geq \frac{\log p}{[K : \mathbb{Q}]} - B.$$

(Remember that $\mathfrak{p}$ has degree one over $\mathbb{Q}$.)

Next we write $\Phi_{\mathfrak{p}}(X) = \sum a_j X^j$ and compute

$$\hat{h}(\Phi_{\mathfrak{p}}(\sigma)P) = \hat{h}\left(\sum_{j=0}^{2g} a_j \sigma^j P\right)$$

$$\leq (2g+1) \sum_{j=0}^{2g} \hat{h}(a_j \sigma^j P) \qquad \text{parallelogram law (see Remark 6.3),}$$

$$= (2g+1) \sum_{j=0}^{2g} a_j^2 \hat{h}(\sigma^j P) \qquad \text{since } \hat{h} \text{ is a quadratic form,}$$

$$\leq (2g+1) \sum_{j=0}^{2g} (4p)^{2g} \hat{h}(\sigma^j P) \qquad \text{from Theorem 4.1(a),}$$

$$= (2g+1)^2 (4p)^{2g} \hat{h}(P) \qquad \text{since } \hat{h} \text{ is Galois invariant.}$$

Combining this with (6.2) and the trivial estimate $2g + 1 \leq 3^g$ gives

$$\hat{h}(P) \geq \frac{1}{(12p)^{2g}} \left(\frac{\log p}{[K : \mathbb{Q}]} - B\right).$$

Finally, we recall that condition (4) of Proposition 5.1 says that $p > \exp\big([K : \mathbb{Q}](B + 1)\big)$, which yields the stated lower bound $\hat{h}(P) \geq 1/(12p)^{2g}$.    $\square$

*Remark* 6.3. During the proof of Theorem 6.1 we made use of the following generalized parallelogram law. For any quadratic form $Q$, it is easy to check the formal identity

$$Q\left(\sum_{i=1}^{t} x_i\right) + \frac{1}{2}\sum_{i,j=1}^{t} Q(x_i - x_j) = t\sum_{i=1}^{t} Q(x_i).$$

Hence if $Q$ is positive semidefinite, then

$$Q\left(\sum_{i=1}^{t} x_i\right) \leq t\sum_{i=1}^{t} Q(x_i).$$

*Remark* 6.4. The proof of Theorem 6.1 actually shows that

$$\hat{h}(P) \geq \frac{1}{(2g+1)^2(4p)^{2g}}\left(\frac{\log p}{e_{\mathfrak{p}}(L/K)[K:\mathbb{Q}]} - B\right),$$

where $e_{\mathfrak{p}}(L/K)$ is the ramification index of $L/K$. This suffices to prove our main theorem for extensions whose ramification index at $\mathfrak{p}$ is bounded, but it will not handle highly ramified extensions.

## 7. A generalized Amoroso-Dvornicich lemma

In order to deal with the ramified case of Theorem 0.1, we recall the following lemma of Amoroso and Dvornicich (see [1, Lemma 2], and also [2, 3, 27]). We refer the reader to [27] for a proof of this particular formulation.

**Lemma 7.1** (Amoroso-Dvornicich [1])**.** *Let $K/\mathbb{Q}$ be a number field, let $\mathfrak{p}$ be a degree 1 prime of $K$ with residue characteristic $p$, and let $L/K$ be an abelian extension that is ramified at $\mathfrak{p}$. Let $\mathfrak{P}$ be a prime of $L$ lying over $\mathfrak{p}$, let $\mathcal{O}_{L,\mathfrak{P}}$ denote the localization of $L$ at $\mathfrak{P}$, and let $I_{L/K}$ be the inertia group at $\mathfrak{P}$. Then there exists an element $\tau \in I_{L/K}$ with $\tau \neq 1$ such that*

$$\tau(\alpha)^p \equiv \alpha^p \pmod{p\mathcal{O}_{L,\mathfrak{P}}} \qquad \text{for all } \alpha \in \mathcal{O}_{L,\mathfrak{P}}.$$

*(Note that the strength of this result is that the congruence is modulo $p$, and not merely modulo $\mathfrak{P}$.)*

*Remark* 7.2. Suppose that $L_{\mathfrak{P}} = \mathbb{Q}_p(\zeta_m)$ for some integer $m$ divisible by $p$. Then the proof of Lemma 7.1 shows that we may take $\tau$ to be any nontrivial element of $\mathrm{Gal}\big(\mathbb{Q}_p(\zeta_m)/\mathbb{Q}_p(\zeta_{m/p})\big)$, considered as a subgroup of

$$\mathrm{Gal}(\mathbb{Q}_p(\zeta_m)/\mathbb{Q}_p) = \mathrm{Gal}(L_{\mathfrak{P}}/K_{\mathfrak{p}}) \subset \mathrm{Gal}(L/K).$$

We now prove a version of the lemma of Amoroso and Dvornicich that applies to varieties and maps with a particular type of inseparable reduction.

**Proposition 7.3.** *Let $K/\mathbb{Q}$ be a number field and let $\mathfrak{p}$ be a degree 1 prime of $K$. Let $X/K \subset \mathbb{P}_K^n$ be a variety and let $\phi : X \to X$ be a finite $K$-morphism. Fix a model $\mathcal{X}/\mathcal{O}_{K,\mathfrak{p}} \subset \mathbb{P}_{\mathcal{O}_{K,\mathfrak{p}}}^n$ and let $\Phi : \mathcal{X} \to \mathcal{X}$ denote the extension of $\phi$ to $\mathcal{X}$. Make the following assumptions:*

1. *The scheme $\mathcal{X}/\mathcal{O}_{K,\mathfrak{p}}$ is embedded as a proper $\mathcal{O}_{K,\mathfrak{p}}$-subscheme of $\mathbb{P}^n_{\mathcal{O}_{K,\mathfrak{p}}}$.*
2. *The map $\Phi : \mathcal{X} \to \mathcal{X}$ is a finite $\mathcal{O}_{K,\mathfrak{p}}$-morphism.*
3. *The restriction of $\Phi$ to the special fiber, i.e., the reduction $\widetilde{\Phi} : \widetilde{\mathcal{X}} \to \widetilde{\mathcal{X}}$, of $\Phi$ modulo $\mathfrak{p}$, factors through the Frobenius map $\mathrm{Frob} : \widetilde{\mathcal{X}} \to \widetilde{\mathcal{X}}^{(p)}$.*

*Let $L/K$ be an abelian extension which is ramified at $\mathfrak{p}$, let $\mathfrak{P}|\mathfrak{p}$, and let $\tau \in I_{L/K}$ be as in Lemma 7.1. Then for all points $P \in X(L)$,*

$$(7.4) \qquad\qquad \delta_{\mathfrak{P}}\big(\phi(\tau(P)), \phi(P)\big) \geq \log p.$$

*(We recall that $\delta_{\mathfrak{P}}$ is the (logarithmic) $\mathfrak{P}$-adic distance function defined in section 3.)*

*Remark* 7.5. The crucial property of the estimate (7.4) is that the lower bound for the $\mathfrak{P}$-adic distance does not depend on the ramification degree of $\mathfrak{P}$. Since $\tau$ is in the inertia group, we know that $\tau(P) \equiv P \pmod{\mathfrak{P}}$. Hence Remark 1.1 gives the trivial lower bound

$$\delta_{\mathfrak{P}}(\tau(P), P) \geq \frac{1}{[L_{\mathfrak{P}} : \mathbb{Q}_p]} \log \mathrm{N}_{L/\mathbb{Q}} \mathfrak{P} = \frac{\log p}{e_{L/\mathbb{Q}}(\mathfrak{P})}.$$

This would not suffice for our purposes.

*Proof.* Without loss of generality, we may replace $K$ and $L$ by $K_{\mathfrak{p}}$ and $L_{\mathfrak{P}}$, respectively.

Let $\mathcal{U}/\mathcal{O}_K$ and $\mathcal{V}/\mathcal{O}_K$ be affine open subsets of $\mathcal{X}/\mathcal{O}_K$ with $\Phi(\mathcal{U}) \subset \mathcal{V}$. Choose affine coordinates (i.e., generators of the affine coordinate ring as an $\mathcal{O}_K$-algebra) $\mathbf{x} = (x_1, \ldots, x_r)$ on $\mathcal{U}$ and simlarly $\mathbf{y} = (y_1, \ldots, y_s)$ on $\mathcal{V}$. The map $\Phi : \mathcal{U} \to \mathcal{V}$ is given by polynomials

$$\Phi^* \mathbf{y} = \mathbf{A}(\mathbf{x}) = (A_1(\mathbf{x}), \ldots, A_s(\mathbf{x})) \qquad \text{with } A_1, \ldots, A_s \in \mathcal{O}_K[\mathbf{x}].$$

We are given that $\Phi$ mod $\mathfrak{p}$ factors through the Frobenius map. It follows that

$$(7.6) \qquad\qquad \Phi^* \mathbf{y} = \mathbf{B}(\mathbf{x}^p) + p\mathbf{C}(\mathbf{x}) \qquad \text{with } \mathbf{B}, \mathbf{C} \in \mathcal{O}_K[\mathbf{x}]^s,$$

where for notational convenience we write $\mathbf{x}^p = (x_1^p, \ldots, x_r^p)$. (Remember that $\mathfrak{p}$ has degree 1, so $p$ is a uniformizer for $\mathfrak{p}$.)

Let $P \in X(L) = \mathcal{X}(\mathcal{O}_L)$. Choose an open affine subsets and local coordinates as above with $P \in \mathcal{U}$ and $\Phi(P) \in \mathcal{V}$. (More formally, $P$ is really a morphism $P : \mathrm{Spec}(\mathcal{O}_L) \to \mathcal{X}$ over $\mathrm{Spec}(\mathcal{O}_K)$, and we choose $\mathcal{U}$ so that $P(\mathrm{Spec}\,\mathcal{O}_L) \subset \mathcal{U}$. Similarly for $\Phi(P)$ and $\mathcal{V}$.) We compute

$$\mathbf{y}(\Phi(\tau P)) - \mathbf{y}(\Phi(P))$$
$$= \big(\mathbf{B}(\mathbf{x}(\tau P)^p) + p\mathbf{C}(\mathbf{x}(\tau P))\big) - \big(\mathbf{B}(\mathbf{x}(P)^p) + p\mathbf{C}(\mathbf{x}(P))\big)$$
$$\text{from (7.6),}$$
$$= \big(\mathbf{B}(\mathbf{x}(P)^p + p\mathbf{a}) + p\mathbf{C}(\mathbf{x}(\tau P))\big) - \big(\mathbf{B}(\mathbf{x}(P)^p) + p\mathbf{C}(\mathbf{x}(P))\big)$$
$$\text{from Lemma 7.1, where } \mathbf{a} \in \mathcal{O}_L^r,$$
$$(7.7) \qquad \equiv 0 \pmod{p\mathcal{O}_L}.$$

The $\mathfrak{P}$-adic distance between any two points $Q_1, Q_2 \in \mathcal{V}(\mathcal{O}_L)$ is given by

(7.8) $$\delta_{\mathfrak{P}}(Q_1, Q_2) = -\log \max_{1 \le i \le s} |y_i(Q_1) - y_i(Q_2)|_{\mathfrak{P}}.$$

(Note that $\mathbf{y}$ gives affine coordinates on $\mathcal{V}$, so projective coordinates are $[1, y_1, \dots, y_s]$.) We apply this formula with $Q_1 = \Phi(\tau P)$ and $Q_2 = \Phi(P)$ to obtain the desired result:

$$\delta_{\mathfrak{P}}(\Phi(\tau P), \Phi(P)) = -\log \max_{1 \le i \le s} |y_i(\Phi(\tau P)) - y_i(\Phi(P))|_{\mathfrak{P}} \quad \text{from (7.8),}$$

$$\ge -\log |p|_{\mathfrak{p}} \quad \text{from (7.7),}$$

$$= \log p.$$

$\square$

In order to apply Proposition 7.3, we will use the following result.

**Lemma 7.9.** *If $\widetilde{A}$ is an abelian variety over a perfect field $k$ of characteristic $p > 0$, then $[p] : \widetilde{A} \to \widetilde{A}$ factors through the Frobenius map $\mathrm{Frob} : \widetilde{A} \to \widetilde{A}^{(p)}$.*

*Proof.* By the theory of isogenies and quotients, it suffices to prove that $\ker(\mathrm{Frob}) \subseteq \ker([p])$ as finite flat group schemes over $k$, i.e., that the connected group scheme $\ker(\mathrm{Frob})$ is killed by $p$. This holds for any formal commutative group scheme $G$ over $k$, as follows from the theory of the Verscheibung operator (see [6, Chapter I, Section 7.5] for details). $\square$

## 8. Proof of the main theorem in the ramified, non-CM case

We now consider the case in which the point $P \in A(K^{\mathrm{ab}})$ is defined over a field that is ramified at $\mathfrak{p}$. In this section, we assume furthermore that $A$ does not have complex multiplication. We will use the following induction hypothesis.

$$\mathrm{HYP}(e): \left( \begin{array}{l} \text{For all fields } K' \subset K^{\mathrm{ab}} \text{ whose } \mathfrak{p}\text{-ramification index satis-} \\ \text{fies } e_{\mathfrak{p}}(K'/K) \le e \text{ and all nontorsion points } P \in A(K'), \text{ the} \\ \text{height of } P \text{ satisfies } \hat{h}(P) \ge \dfrac{1}{(12p)^{2g}}. \end{array} \right)$$

We note that Theorem 6.1 shows that $\mathrm{HYP}(1)$ is true.

**Theorem 8.1.** *Suppose that $A$ does not have complex multiplication (over $\bar{K}$). Let $L$ be a finite abelian extension of $K$ and assume that $\mathrm{HYP}(e)$ is true for all $e < e_{\mathfrak{p}}(L/K)$. Then*

$$\hat{h}(P) \ge \frac{1}{(12p)^{2g}} \qquad \text{for all nontorsion } P \in A(L).$$

*Hence by induction, $\mathrm{HYP}(e)$ is true for all $e \ge 1$.*

*Proof.* As noted above, we have already shown that $\mathrm{HYP}(1)$ is true, so we may assume the $L/K$ is ramified at $\mathfrak{p}$. Let $P \in A(L)$ be a nontorsion point. If $K(P)/K$ is less ramified at $\mathfrak{p}$ than $L/K$ (i.e., if $e_{\mathfrak{p}}(K(P)/K) < e_{\mathfrak{p}}(L/K)$), then we are done by the induction hypothesis, so we may assume that

$$e_{\mathfrak{p}}(K(P)/K) = e_{\mathfrak{p}}(L/K).$$

Let $\tau \in G_{L/K}$ be chosen as in Lemma 7.1.

Using Lemma 7.9, we now apply Proposition 7.3 to the point $P \in A(L)$ and the map $\Phi = [p]$. The proposition tells us that

$$\delta_{\mathfrak{P}}([p](\tau P), [p](P)) \geq \log p \qquad \text{for all primes } \mathfrak{P}|\mathfrak{p}.$$

Summing over all of the primes dividing $\mathfrak{p}$, we obtain a lower bound that is independent of the ramification degree of $L/K$:

$$\sum_{\mathfrak{P}|\mathfrak{p}} \frac{[L_{\mathfrak{P}} : \mathbb{Q}_p]}{[L : \mathbb{Q}]} \delta_{\mathfrak{P}}(([p](\tau P), [p](P)) \geq \frac{[K_{\mathfrak{p}} : \mathbb{Q}_p]}{[K : \mathbb{Q}]} \sum_{\mathfrak{P}|\mathfrak{p}} \frac{[L_{\mathfrak{P}} : K_{\mathfrak{p}}]}{[L : K]} \log p$$

$$(8.2) \hspace{4cm} = \frac{\log p}{[K : \mathbb{Q}]}.$$

(Remember that $\mathfrak{p}$ is a degree one prime, so $K_{\mathfrak{p}} = \mathbb{Q}_p$.)

Assume for the moment that $[p](\tau P) \neq [p](P)$. Then we can apply Proposition 3.4(a) to the *distinct* points $[p](\tau P)$ and $[p](P)$, which gives the lower bound

$$\hat{h}([p](\tau P)) + \hat{h}([p]P) \geq \sum_{\mathfrak{P}|\mathfrak{p}} \frac{[L_{\mathfrak{P}} : \mathbb{Q}_p]}{[L : \mathbb{Q}]} \delta_{\mathfrak{P}}(([p](\tau P), [p](P)) - B$$

$$\geq \frac{\log p}{[K : \mathbb{Q}]} - B \qquad \text{from (8.2),}$$

$$\geq 1 \qquad \text{from Proposition 5.1(4).}$$

Using the quadratic nature and Galois invariance of the canonical height yields

$$\hat{h}([p](\tau P)) + \hat{h}([p]P) = 2p^2 \hat{h}(P).$$

Hence $\hat{h}(P) \geq 1/2p^2$, which is considerably stronger than the desired result. This completes the proof under the assumption that $[p](\tau P) \neq [p](P)$.

Finally, let $Q = \tau P - P$, and suppose that $[p](Q) = O$. In particular, $Q \in A(L)_{\text{tors}}$. Since we are assuming that $A$ does not have complex multiplication, we may assume that our chosen prime $\mathfrak{p}$ satisfies Condition 5(a) of Proposition 5.1, i.e., that $A(K^{\text{ab}})$ contains no nontrivial points of order $p$. This implies immediately that $Q = O$, and hence that $\tau P = P$. Therefore $P$ is defined over the fixed field $L^\tau$ of $\tau$. However, $\tau$ is a nontrivial element of the inertia group at $\mathfrak{p}$, so

$$e_{\mathfrak{p}}(L^\tau/K) < e_{\mathfrak{p}}(L/K) \qquad \text{(strict inequality).}$$

Therefore $\hat{h}(P) > 1/(12p)^{2g}$ by the induction hypothesis applied to the field $L^\tau$. $\qquad \square$

*Remark* 8.3. We could just as well have proved Theorem 8.1 by induction on the local conductor $\mathfrak{f}_{\mathfrak{p}}(L/K)$ (rather than on the ramification index $e_{\mathfrak{p}}(L/K)$). In the next section, we will necessarily have to use the local conductor, in order to assume that the field $L$ contains enough roots of unity.

## 9. Completion of the proof — $L/K$ is ramified and $A$ has complex multiplication

An examination of the proof of Theorem 8.1 given in the previous section shows that we have reduced the proof of Theorem 0.1 to the case that $A$ has complex multiplication, $A$ has ordinary reduction at $\mathfrak{p}$, and the point $P \in A(L)$ satisfies

$$[p](\tau - 1)P = O.$$

We would like to conclude that $(\tau - 1)P = O$, but unfortunately this need not be true. However, we will show that it is true if we modify $P$ by a torsion point. The following well-known description of the formal group of an abelian variety at primes of ordinary reduction provides the crucial information needed to find the required torsion point.

**Theorem 9.1.** Let $K_{\mathfrak{p}}^{\mathrm{nr}}$ be the maximal unramifed extension of $K_{\mathfrak{p}}$, and let $\mathcal{O}_{\mathfrak{p}}^{\mathrm{nr}}$ be its ring of integers. Assume that $A$ has good ordinary reduction at $\mathfrak{p}$. Then the formal group $\hat{A}$ of $A$ is toroidal over $\mathcal{O}_{\mathfrak{p}}^{\mathrm{nr}}$, that is, it is isomorphic over $\mathcal{O}_{\mathfrak{p}}^{\mathrm{nr}}$ to the formal torus $\hat{\mathbb{G}}_m^g$.
  In particular, for all $n \geq 1$,

$$\hat{A}[p^n] \cong \hat{\mathbb{G}}_m^g[p^n] \cong \boldsymbol{\mu}_{p^n}^g$$

as $\mathrm{Gal}(\bar{K}_{\mathfrak{p}}/K_{\mathfrak{p}}^{\mathrm{nr}})$-modules.

*Proof.* See [3, Lemma 3.1] or [14, Lemma 4.27]. $\qquad\square$

Without loss of generality, we may assume that all of the endomorphisms of $A$ are defined over $K$, see Proposition 2.1(b). Under this assumption, it is well known (see, for example, [22, Cor. 2 of Theorem 5]) that the torsion points of $A$ generate abelian extensions of $K$. To keep the exposition as self-contained as possible, we present a proof of this fact.

**Theorem 9.2.** Let $K$ be a number field, let $A/K$ be an abelian variety with complex multiplication. Assume that $\mathrm{End}_K(A) = \mathrm{End}_{\bar{K}}(A)$. Then $K(A_{\mathrm{tors}}) \subset K^{\mathrm{ab}}$, i.e., the torsion points of $A$ generate abelian extensions of $K$.

*Proof.* Since $\mathrm{End}_K(A) = \mathrm{End}_{\bar{K}}(A)$, it follows from the theory of complex multiplication that $F = \mathrm{End}_K(A) \otimes \mathbb{Q}$ is a CM field with $[F : \mathbb{Q}] = 2d$, where $d = \dim(A)$. If $\ell$ is any prime number, then one also knows that $V_\ell(A) = T_\ell(A) \otimes \mathbb{Q}$ has rank one as a module over $F \otimes \mathbb{Q}_l$ (see [18, Lemma 2]). Let $G$ be the image of the natural map $\mathrm{Gal}(\bar{K}/K) \to \mathrm{Aut}(V_\ell(A))$. Since every endomorphism of $A$ is defined over $K$, we get an injection

$$G \hookrightarrow (F \otimes \mathbb{Q}_l)^*,$$

which implies that $G$ is abelian. Since $\ell$ is an arbitrary prime, the action of $\mathrm{Gal}(\bar{K}/K)$ on $A_{\mathrm{tors}}$ is therefore abelian. $\qquad\square$

We now prepare to state and prove a result (Theorem 9.3) which, together with Theorem 8.1, will complete the proof of our main theorem. The proof of Theorem 9.3 will use the following induction hypothesis.

$$\text{HYP}(f): \quad \begin{pmatrix} \text{For all fields } K' \subset K^{\text{ab}} \text{ whose local conductor satisfies} \\ \text{ord}_{\mathfrak{p}}(\mathfrak{f}_{\mathfrak{p}}(K'/K)) \leq f \text{ and all nontorsion points } P \in A(K'), \\ \text{the height of } P \text{ satisfies } \hat{h}(P) \geq \dfrac{1}{(12p)^{2g}}. \end{pmatrix}$$

As before, we note that Theorem 6.1 shows that $\text{HYP}(0)$ is true.

**Theorem 9.3.** *Suppose that $A$ has complex multiplication (over $\bar{K}$). Let $L \subset K^{\text{ab}}$ be ramified at $\mathfrak{p}$ and assume that $\text{HYP}(f)$ is true for all $f < \text{ord}_{\mathfrak{p}}(\mathfrak{f}_{\mathfrak{p}}(L/K))$. Then*

$$\hat{h}(P) \geq \frac{1}{(12p)^{2g}} \qquad \text{for all nontorsion } P \in A(L).$$

*Hence by induction, $\text{HYP}(f)$ is true for all $f \geq 0$.*

*Proof.* Let $m$ be the local conductor $\mathfrak{f}_{\mathfrak{p}}(L/K)$ of $L/K$ at $\mathfrak{p}$. Recall that by definition we have $L_{\mathfrak{P}} \subseteq \mathbb{Q}_p(\zeta_m)$, and $m$ is the smallest positive integer with this property.

Without loss of generality, we may assume that $L$ contains a primitive $m$th root of unity, since $L(\zeta_m) \supseteq L$ is again an abelian extension of $K$ with local conductor $m$. It follows that $L_{\mathfrak{P}} = \mathbb{Q}_p(\zeta_m)$.

The assumption that $L/K$ is ramified at $\mathfrak{p}$ tells us that $p \mid m$, and indeed $\tau \in \text{Gal}(L/K)$ was chosen to generate $\text{Gal}(\mathbb{Q}_p(\zeta_m)/\mathbb{Q}_p(\zeta_{m/p}))$ (see Remark 7.2). Write

$$m = p^k m' \text{ with } k \geq 1 \text{ and } p \nmid m'.$$

Then Theorem 9.1 and the fact that the formal group has only $p$-power torsion imply that

$$(9.4) \qquad \qquad \hat{A}(L_{\mathfrak{P}}^{\text{nr}})_{\text{tors}} \cong \hat{A}[p^k] \cong \boldsymbol{\mu}_{p^k}^g$$

as $\text{Gal}(L_{\mathfrak{P}}^{\text{nr}}/K_{\mathfrak{p}}^{\text{nr}})$-modules. (We identify $\hat{A}(\overline{K}_{\mathfrak{p}})$ with the kernel of reduction in $A(\overline{K}_{\mathfrak{p}})$).

We may replace $L$ by the extension $L(\hat{A}[p^k])$. This is permissible, since from the above isomorphism, $L(\hat{A}[p^k])/L$ is unramified at $\mathfrak{p}$, and from Theorem 9.2, the extension $K(\hat{A}[p^k])$ is an abelian extension of $K$.

Now consider the point $Q = (\tau - 1)P$, which by assumption satisfies $[p](Q) = O$. The point $Q$ is in the formal group $\hat{A}(L_{\mathfrak{P}})$, since $\tau$ is in the inertia group. Hence under the identification (9.4), the point $Q$ corresponds to a $g$-tuple of $p^{\text{th}}$ roots of unity,

$$(\eta_1, \ldots, \eta_g) \in \boldsymbol{\mu}_{p^k}^g.$$

Also, by construction, the automorphism $\tau$ is a nontrivial element of the subgroup $\text{Gal}(\mathbb{Q}_p(\zeta_{p^k})/\mathbb{Q}_p(\zeta_{p^{k-1}}))$, so there is a *primitive* $p^{\text{th}}$ root of unity $\xi \in \boldsymbol{\mu}_p$ such that

$$\tau(\zeta_{p^k}) = \xi \zeta_{p^k}.$$

In other words, the map

$$(\tau - 1) : \boldsymbol{\mu}_{p^k} \longrightarrow \boldsymbol{\mu}_p, \qquad \zeta \longrightarrow \tau(\zeta)/\zeta,$$

is surjective. Again referring to the identification (9.4), this shows that the map

$$(\tau - 1) : \hat{A}(L)[p^k] \longrightarrow \hat{A}(L)[p]$$

is surjective.

The point $Q = (\tau - 1)P$ is a point of order $p$ in $\hat{A}(L)$, so this shows that we can find a point $T \in \hat{A}(L)[p^k]$ satisfying

$$Q = (\tau - 1)T.$$

It follows that $P - T$ is fixed by $\tau$, so $P - T$ is defined over the fixed field $L^\tau$ of $\tau$. Since $L^\tau$ has strictly smaller local conductor than does $L$ at $\mathfrak{p}$, the induction hypothesis says that $\hat{h}(P - T) \geq 1/(12p)^{2g}$. But $T$ is a torsion point, so

$$\hat{h}(P - T) = \hat{h}(P),$$

which completes the proof of Theorem 9.3, and with it the proof of our main theorem (Theorem 0.1). $\qquad\square$

## 10. Acknowledgements

## References

[1] F. Amoroso, R. Dvornicich, *A lower bound for the height in abelian extensions,* J. Number Theory **80** (2000), 260–272.

[2] F. Amoroso, U. Zannier, *A relative Dobrowolski lower bound over abelian extensions,* Ann. Scuola Norm. Sup. Pisa Cl. Sci. (4) **29** (2000), 711–727.

[3] M. Baker, *Lower bounds for the canonical height on elliptic curves over abelian extensions,* IMRN **29** (2003), 1571–1590.

[4] S. David, M. Hindry, *Minoration de la hauteur de Néron-Tate sur les variétés abéliennes de type C.M.,* J. Reine Angew. Math. **529** (2000), 1–74.

[5] G. Faltings, *Endlichkeitssätze für abelsche Varietäten über Zahlkörpern,* Invent. Math. **73** (1983), 349–366.

[6] J.-M. Fontaine, *Groupes p-divisibles sur les corps locaux*, Astérisque, Soc. Math. de France, (1977), 47–48.

[7] A. Fröhlich, *Formal Groups*, Lecture Notes in Math. 74, Springer Verlag, New York 1968.

[8] R. Hartshorne, *Algebraic Geometry*, Graduate Texts in Mathematics 52, Springer-Verlag, New York, 1977.

[9] M. Hazewinkel, *Formal Groups and Applications*, Academic Press Inc., New York, 1978.

[10] M. Hindry, J. Silverman, *Diophantine Geometry: An Introduction*, Graduate Texts in Mathematics 201, Springer-Verlag, New York, 2000.

[11] S. Lang, *Algebra*, Third Edition, Addison-Wesley, 1993.

[12] _____, *Fundamentals of Diophantine Geometry*, Springer-Verlag, New York, 1983.

[13] D. Masser, *Small values of the quadratic part of the Néron-Tate height on an abelian variety,* Compositio Math. **53** (1984), 153–170.

[14] B. Mazur, *Rational points on abelian varieties with values in towers of number fields,* Invent. Math. **18** (1972), 183–266.

[15] J.S. Milne, *Abelian varieties*, Arithmetic Geometry, Springer-Verlag, Berlin and New York, 1986.

[16] D. Mumford, *Abelian Varieties*, Tata Institute of Fundamental Research Studies in Mathematics, 5, Tata Institute, Bombay, 1970.

[17] N. Ratazzi, *Problème de Lehmer pour les hypersurfaces de variétés abéliennes de type C.M.,* preprint,
http://arxiv.org/abs/math.NT/0307095

[18] W.M. Ruppert, *Torsion points of abelian varieties in abelian extensions,* unpublished manuscript,
http://www.math.uiuc.edu/Algebraic-Number-Theory/0101/tpavae.dvi

[19] J.-P. Serre, *Abelian l-adic Representations and Elliptic Curves*, (revised reprint of the 1968 original), Research Notes in Mathematics, 7, A K Peters, Ltd., Wellesley, MA, 1998.

[20] _____, *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques,* Invent. Math. **15** (1972), 259–331.

[21] _____, *Oeuvres Colllected Papers*, Volume IV, 1985–1998, 136. Résumé des cours de 1985–1986 and 137. Lettre á Marie-France Vignéras du 10/2/1986, Springer-Verlag, Berlin, 2000.

[22] J.-P. Serre, J. Tate, *Good reduction of abelian varieties,* Annals of Math. **88** (1968), 492–517.

[23] I. R. Shafarevich, *Basic Algebraic Geometry I*, Second Edition, Springer-Verlag, New York, 1994.

[24] G. Shimura, *Abelian varieties with complex multiplication and modular functions*, Princeton University Press, Princeton, NJ, 1998.

[25] J.H. Silverman, *The Arithmetic of Elliptic Curves*, Graduate Texts in Mathematics 106, Springer-Verlag, New York, 1986.

[26] _____, *Arithmetic distance functions and height functions in Diophantine geometry* Math. Ann. **279** (1987), 193–216.

[27] _____, *A lower bound for the canonical height on elliptic curves over abelian extensions,* J. Number Theory **154** (2004), 353–372.

[28] L. Szpiro, E. Ullmo, S. Zhang, *Équirépartition des petis points,* Invent. Math. **127** (1997), 337–347.

[29] J. Tate, *Endomorphisms of abelian varieties over finite fields.* Invent. Math. **2** (1966), 134–144.

[30] W. Waterhouse, *Abelian varieties over finite fields,* Ann. Sci. École Norm. Sup. (4) **2** (1969), 521–560.

[31] Yu.G. Zarhin, *Endomorphisms and torsion of abelian varieties.* Duke Math. J. **54** (1987), 131–145.

[32] S. Zhang, *Equidistribution of small points on abelian varieties,* Annals of Math. **147** (1998), 159–165.

Department of Mathematics, University of Georgia, Athens, GA 30602-7403, USA

Mathematics Department, Box 1917 Brown University, Providence, RI 02912 USA
*E-mail address*: mbaker@math.uga.edu, jhs@math.brown.edu