Annali della
Scuola Normale Superiore di Pisa
Classe di Scienze

E. Bombieri
U. Zannier

Heights of algebraic points on subvarieties of abelian varieties

Annali della Scuola Normale Superiore di Pisa, Classe di Scienze 4e série, tome 23, nº 4 (1996), p. 779-792
<http://www.numdam.org/item?id=ASNSP_1996_4_23_4_779_0>

Heights of Algebraic Points on Subvarieties of Abelian Varieties

E. BOMBIERI - U. ZANNIER

1. – Introduction and results

Let $G = \mathbf{G}_m^n$ be the standard n-dimensional torus over $\mathbf{Z}$ and let

$$\widehat{h}(\mathbf{x}) = h(x_1) + h(x_2) + \cdots + h(x_n)$$

be the height on $G(\overline{\mathbf{Q}})$ given by the sum of the absolute logarithmic Weil heights of the coordinates of $\mathbf{x}$. This height vanishes if and only if $\mathbf{x}$ is a torsion point. Since $G(\overline{\mathbf{Q}})$ is a divisible group and since $\widehat{h}(\mathbf{x}^{1/l}) = (1/l) \cdot \widehat{h}(\mathbf{x})$, we also see that on any subtorus H of G of positive dimension there are infinitely many nontorsion points of arbitrarily small height. The same of course holds if instead of subtori we consider torsion cosets of H, namely translates of H by torsion points of G.

As a consequence of his deep studies [Zh1, 2] of positive line bundles on arithmetic varieties, Shouwu Zhang proved the remarkable result that this phenomenon is characteristic of subgroups. In fact he proved that if X is a closed subvariety of G, then the Zariski closure of the set of all points of X of sufficiently small height is a finite union of torsion cosets of subtori of G.

A self-contained elementary proof of Zhang's theorem, building on previous work of W.M. Schmidt [Sch1] dealing with some special cases, was given shortly afterwards in [BZ]. These papers also considered a uniform version of Zhang's theorem, which may be stated as follows:

Let X° be the complement in X of the union of all translates of nontrivial subtori of G contained in X (a set shown to be Zariski open in X). Then there is a positive constant $\gamma = \gamma(n, d)$, depending only on the degree d of X and the dimension n of G, such that the set of algebraic points of X° of $\widehat{h}$-height at most γ is finite, of cardinality bounded only in terms of n and d.

A consequence of this result is that the set of algebraic points in X° is discrete in $G(\overline{\mathbf{Q}})$, with respect to the translation invariant semi-distance $d(P, Q) = \widehat{h}(PQ^{-1})$ induced by $\widehat{h}$, in the following strong sense:

Pervenuto alla Redazione il 1 aprile 1996 e in forma definitiva il 19 giugno 1996.

There exist a positive number $\gamma = \gamma(n, d)$ and an integer $N(n, d)$ such that, for each $Q \in G(\overline{\mathbf{Q}})$, the set of algebraic points $P \in X^{\circ}(\overline{\mathbf{Q}})$ satisfying $d(P, Q) \leq \gamma$ is finite, of cardinality at most $N(n, d)$.

This result has been made completely explicit by W.M. Schmidt in [Sch2].

Many results valid for linear tori admit counterparts, of a far deeper nature, in the case of abelian and semi-abelian varieties. Indeed, the corresponding result for curves in an abelian variety is a conjecture of Bogomolov, pre-dating Zhang's theorems for $\mathbf{G}_m^n$ (see L. Szpiro's paper [Sz, p. 240]). This can be formulated as follows. Let A be an abelian variety defined over a number field K and let $\langle\, ,\, \rangle$ be the Néron-Tate bilinear form on $A(\overline{K})$ associated to a symmetric ample divisor on A. Then

$$d(P, Q) = |P - Q| = \sqrt{\langle P - Q, P - Q\rangle}$$

determines a translation invariant semi-distance on $A(\overline{K})$, with $d(P, Q) = 0$ if and only if $P - Q$ is a torsion point of A. Now let C be a closed curve in A, defined over K, not a translate of an elliptic curve. Then the conjecture states that the set $C(\overline{K})$ of algebraic points of C is discrete with respect to the semi-distance $d(\, ,\,)$ on $A(\overline{K})$.

More generally, one may conjecture that if X is a closed subvariety of an abelian variety the same conclusion holds provided we replace X with the Zariski open subset X° obtained by removing from X all subvarieties which are translates of abelian subvarieties (of positive dimension) of A.

The purpose of the present paper is to give a proof of this conjecture (in a more precise form) for abelian varieties of special type. Namely, we assume that either

(A1) *A has complex multiplication*

or

(A2) *there exists an infinite set $\Sigma = \Sigma(A)$ of prime numbers such that, for $p \in \Sigma$ and some positive integer r, the isogeny $[p^r]$ on the reduction $A/\mathfrak{p}$ of A modulo some prime ideal $\mathfrak{p} \mid p$ in K coincides with some power of the Frobenius map on $A/\mathfrak{p}$.*

Property (A2) means that there are infinitely many supersingular primes for A in the sense that the separable kernel of $[p^r]$ on $A/\mathfrak{p}$ is a point. By a theorem of Elkies [El], (A2) holds whenever A is a power of an elliptic curve defined over $\mathbf{Q}$. Although this shows that property (A2) is nonvacuous, it is unlikely to be satisfied by a general abelian variety.

Special cases of the Bogomolov Conjecture are already present in the literature. For a curve C embedded in its Jacobian $J(C)$, this was proved by Burnol [Bu] assuming the strong condition that C has good reduction everywhere and $J(C)$ has complex multiplication.

In another paper, Zhang [Zh3] has considered the generalized Bogomolov Conjecture in the form:

Let $X \subset A$ be a subvariety, not a translate of an abelian subvariety by a torsion point. Then the set $X_\varepsilon = \{x \in X(\overline{\mathbf{Q}}) : \widehat{h}(x) < \varepsilon\}$ is not Zariski-dense in X for some positive ε.

He proves that conclusion if $X - X$ generates A and the homomorphism of Néron-Severi groups $NS(A) \otimes \mathbf{R} \longrightarrow NS(X) \otimes \mathbf{R}$ is not injective. Although these conditions are quite restrictive, for example, the second condition is not satisfied if $\dim(A) \geq 3$ and X is a smooth hyperplane section of A), they provide examples of the validity of the Bogomolov Conjecture not covered by the results of this paper.

Let A be an abelian variety of dimension n, defined over a number field K. We fix a very ample symmetric line sheaf $\mathcal{L}$ on A, a projective embedding $j : A \longrightarrow \mathbf{P}^m$ determined by a choice of basis of sections of $\mathcal{L}$, and a complex torus $T := \mathbf{C}^n/\Lambda$, isomorphic to A as a complex manifold. Note that there is little additional generality to be gained by considering ample symmetric line bundles on A, because by a well-known theorem of Lefschetz if $\mathcal{L}$ is ample then $\mathcal{L}^{\otimes 3}$ is always very ample.

We denote by $\widehat{h}$ the Néron-Tate height associated to $\mathcal{L}$.

Given A, $\mathcal{L}$ as above satisfying the additional assumption (A1) or (A2), by *original data* we mean: The embedding $j : A \longrightarrow \mathbf{P}^m$, the field of definition K of A, the field of complex multiplication in case (A1) and the set Σ in case (A2). In principle, our estimates can be made explicit in terms of such data. We have

THEOREM 1. *Let A, $\mathcal{L}$ be as before and suppose that A satisfies* (A1) *or* (A2). *Suppose X is a closed geometrically irreducible subvariety of A of degree at most d in the embedding j and let X^{o} be the complement in X of the union of all subvarieties of X which are translates of nontrivial abelian subvarieties of A. Then:*

(a) *X^{o} is Zariski open in X. Moreover the number and degree of the irreducible components of $X \setminus X^{\mathrm{o}}$ are bounded, the bound depending on d and the original data but not otherwise on X.*

(b) *The set of algebraic points in X^{o} is discrete with respect to the semi-distance $d(P, Q)$.*

(c) *More precisely, there exist positive numbers γ and N, depending on d and the original data but not otherwise on X, with the following property: For every $Q \in A(\overline{\mathbf{Q}})$ the set*

$$\{P : P \in X^{\mathrm{o}}(\overline{\mathbf{Q}}),\ d(P, Q) \leq \gamma\}$$

is a finite set of cardinality at most N.

Part (a) is a special case of a result by Abramovich [Abr] on semi-abelian varieties. We shall give here a self-contained independent proof.

Following the pattern in [BZ], we shall deduce Theorem 1 from Theorem 2 below.

Let B be an abelian subvariety of A. We say that a coset $x + B$ is maximal in X if $x + B \subset x + B' \subset X$ (where B' is another abelian subvariety) implies

$B' = B$. A *torsion coset* of B is a translate $x + B$ by a torsion point of A. We have

THEOREM 2. *Let A, $\mathcal{L}$ be as before and suppose that A satisfies* (A1) *or* (A2). *Let X be a closed subvariety of A and let X^* to be the complement in X of all torsion cosets $x + B \subset X$, for all x and B* (*including the trivial abelian variety*). *Then:*

(a) *The number of maximal torsion cosets $x + B \subset X$ is finite.*

(b) *There exists a positive number $\gamma_1 = \gamma_1(X, A, \mathcal{L})$ such that every point $Q \in X^*(\overline{\mathbf{Q}})$ has height $\widehat{h}(Q) \geq \gamma_1$.*

It may be useful to compare the relative strengths of Theorem 1 and Theorem 2. Theorem 1 is a uniform statement with respect to X, which applies to the subset X^{o} obtained by removing from X all cosets of abelian subvarieties of positive dimension. Theorem 2 instead applies to the subset X^* obtained by removing from X all torsion cosets, including all torsion points of A. Clearly $X^{\mathrm{o}} \subset X^* \cup \{X^{\mathrm{o}} \cap \{\text{torsion points of } A\}\}$ and $X^{\mathrm{o}} \cap \{\text{torsion points of } A\}$ is a finite set. Hence Theorem 2 is stronger than Theorem 1 in the sense that it applies to a larger subset of X, and weaker than Theorem 1 because the conclusion is not uniform in X. The passage from the non-uniform statement of Theorem 2 to the uniform statement of Theorem 1 is achieved by embedding X in a universal subvariety of a power of A (in our case, a determinantal variety) and applying Theorem 2 to this universal situation in order to obtain uniformity. We believe that this procedure can be of wide applicability in other interesting situations.

Added in proof: In the meantime (June 1996) S. Zhang has kindly sent us a preprint in which he obtains a complete solution of Bogomolov's conjecture as a consequence of an equidistribution result about points of small height. A paper by L. Szpiro, E. Ullmo and S. Zhang on this topic will appear in Inventiones Math. Also Y. Bilu (September 1996) has sent to us a preprint with a simple proof of a toric analogue of this equidistribution theorem.

In the present form these new equidistribution methods, which make use of weak convergence of measures, lead to ineffective constants. With this proviso, it follows that our Theorem 1 is valid for all abelian varieties.

We begin by proving some simple results needed for the proof of Theorem 2, following the same path as in [BZ]. The crucial Lemma 4 parallels the key Lemma 1 in [BZ], but we have found it necessary to use either (A1) or (A2) above. Also, compared to [BZ], Lemma 3 leads to Theorem 2 more directly.

The first three lemmas are stated for arbitrary abelian varieties defined over $\mathbf{C}$. Proofs of Lemma 1 and Lemma 3 have been given by several authors. Algebraic proofs are due to M. Raynaud [Ray], M. Hindry [Hi, Lemma 9 and 10] and D. Bertrand and P. Philippon [BP]. Another proof of Lemma 3 appears in [McQ], using a previous idea of Faltings. For completeness we give here self-contained short analytical proofs, of Lemma 1 by means of considerations not unlike those in [BP] and of Lemma 3 by what appears to be a new argument.

LEMMA 1. *Let $A/\mathbf{C}$ be an abelian variety together with an embedding $j : A \longrightarrow \mathbf{P}^m$. Then the number of abelian subvarieties of A of degree at most d in this embedding is bounded in terms of d and j.*

PROOF. Let B be an abelian subvariety of A, of dimension k. By [GH, p. 171] we may calculate the degree of B as its volume divided by $k!$, namely

$$\deg(B) = \frac{1}{k!}\int_B \omega^k = \frac{1}{k!}\mathrm{vol}(B)$$

where ω is the standard Kähler form on $\mathbf{P}^m$.

Let B correspond to a complex subtorus $T^* \subset T$. Since $T \to A \subset \mathbf{P}^m$ is an embedding of compact complex manifolds, the pull-back of the k-dimensional volume on $\mathbf{P}^m$ exceeds a positive multiple c^{-1} of the k-volume on T induced by the euclidean metric. So, if $\deg(B) \le d$, we have

$$\mathrm{vol}(T^*) \le ck!d\,.$$

Since T^* is a complex subtorus of T, its inverse image in $\mathbf{C}^n$ consists of the Λ translates of a k-dimensional complex vector space V, whose intersection with Λ is a $2k$-dimensional sublattice Λ^* with basis $\lambda_1, \dots, \lambda_{2k}$, say. Let F be the fundamental domain for V/Λ^* given by

$$F := \left\{\sum t_i\lambda_i : 0 \le t_i < 1\right\}.$$

Then the euclidean volume of T^* is the k-dimensional volume of F as a subset of $\mathbf{C}^n = \mathbf{R}^{2n}$. If $e_1, \dots, e_{2n}$ denotes the standard basis for $\mathbf{C}^n = \mathbf{R}^{2n}$ then, putting

$$\lambda_1 \wedge \cdots \wedge \lambda_{2k} := \sum_{|S|=2k} a_S \wedge_{i\in S} e_i\,,$$

we have by the Cauchy-Binet formula

$$\mathrm{vol}(F) = \sqrt{\sum a_S^2}\,.$$

In particular $|a_S| \le ck!d$. Let $\beta_1 \dots, \beta_{2n}$ be some basis of Λ. Then $\wedge_{i\in S}\beta_i$ is a basis of $\wedge^{2k}\mathbf{R}^{2n}$. It follows that the coordinates of $\lambda_1 \wedge \cdots \wedge \lambda_{2k}$ in the basis $\wedge_{i\in S}\beta_i$ are bounded, whence they have finitely many possibilities, since they are integers. In particular the vector $\lambda_1 \wedge \cdots \wedge \lambda_{2k}$ has finitely many possibilities. Hence the spaces V and T^* also have finitely many possibilities, as wanted. □

LEMMA 2. *Let X be a closed irreducible subvariety of $A/\mathbf{C}$ of degree at most d in the embedding $j : A \subset \mathbf{P}^m$. Let B be an abelian subvariety of A and let $x + B$ be a coset of B contained in X. We say that the coset $x + B$ is maximal for X if $x + B \subset x + B' \subset X$ (where B' is another abelian subvariety of A) implies $B' = B$.*

Then only finitely many abelian subvarieties B can occur in a maximal coset for X, and their number is bounded in terms of d and of the embedding j.

PROOF. We construct inductively irreducible varieties $X_1 = X \supset X_2 \supset \dots$ such that $x + B \subset X_i$, as follows. We start with $X_1 = X$. Having performed the first i steps, we let $X_{i+1} = X_i$ if for all $g \in B$ we have $\dim(X_i) = \dim(X_i \cap (g + X_i))$; note that in this case $g + X_i = X_i$ for every $g \in B$. Otherwise, we pick $g^* \in B$ such that $\dim(X_i) > \dim(X_i \cap (g^* + X_i))$ and define X_{i+1} as any irreducible component of the intersection $X_i \cap (g^* + X_i)$ containing $x + B$. Clearly this inductive procedure stabilizes after at most n steps, and we set $Y = X_n$. Note that $\deg(Y)$ is bounded in terms of d and n, as one sees using the general Bézout theorem in [Fu, Proposition at p. 10].

By construction, $x \in Y \subset X$, $g + Y = Y$ for $g \in B$ and the degree of Y is bounded in terms of d and n.

Next, we construct inductively varieties $Y_1 = Y \supset Y_2 \supset \dots$ as follows. Let us choose a point $y \in Y_i$ and put $W = Y_i \cap (x - y + Y_i)$. Again, we have $x \in W$ and $g + W = W$ for every $g \in B$. If $W_1, \dots, W_s$ are the irreducible components of W then a translation by $g \in B$ permutes them. Hence B acts on $\cup W_j$ as a permutation group, whence a subgroup of finite index of B must act trivially on $\cup W_j$. Since B is an abelian variety, it is *a fortiori* a divisible group and any subgroup of finite index of B is B itself. Thus $g + W_j = W_j$ for every j and $g \in B$, while $x \in W_j$ for at least one j. If there is a choice $y^* \in Y_i$ such that one of the components W_j containing x so constructed has dimension strictly smaller than $\dim(Y)$, we set $Y_{i+1} = W_j$; otherwise we set $Y_{i+1} = Y_i$. Again, this procedure stabilizes after at most n steps and setting $Z = Y_n$ we obtain a variety such that $x \in Z \subset X$, $g + Z = Z$ for every $g \in B$ and also $(x - z) + Z = Z$ for every $z \in Z$. As before, the general Bézout theorem shows that the degree of Z is bounded in terms of d and n.

On the other hand, since $x + B$ is maximal for X it is also maximal for Z, therefore the set $\{g : g \in A,\ g + Z = Z\}$ is a finite union of translates $g_i + B$ (indeed, this set is *a priori* a finite union of translates of an abelian subvariety containing B). Clearly, this set contains $x - Z \supset B$. It follows that $B \subset x - Z \subset \cup(g_i + B)$, whence $B = x - Z$, because Z is irreducible and has the same dimension as B. Thus the degree of B is bounded and Lemma 1 completes the proof. $\square$

We identify the abelian variety A with the complex torus $\mathbf{C}^n/L$ where L is a lattice of rank $2n$. An endomorphism b of A is then represented by multiplication by a matrix $\Phi \in \mathrm{GL}_n(\mathbf{C})$ such that $\Phi L \subset L$ and, after a linear change of coordinates, the matrix Φ can be put in diagonal form with eigenvalues λ_i, $i = 1, \dots, n$. The λ_i satisfy the characteristic equation of b.

LEMMA 3. *If $X \subset A$ and b is an endomorphism, we denote by bX the set $\{bx : x \in X\}$.*

Suppose b is represented by multiplication in $\mathbf{C}^n$ by a matrix B with no eigenvalue equal to a root of unity or zero, and suppose that X is a closed irreducible subvariety of A such that $bX \subset X$. Then X is a translate of an abelian subvariety of A by a torsion point.

REMARK. The condition that no eigenvalue of b is a root of unity is necessary for the validity of Lemma 3, otherwise A may have an abelian subvariety B on which b is the identity, and any subvariety $X \subset B$ would have $bX \subset X$.

PROOF. Let $T = \mathbf{C}^n/L$ be the complex torus associated to A. We begin by proving that the union of the torsion points of $b^m - 1$, as m varies, contain a subset of the torsion points of A, dense in T for the euclidean topology. The subring $\mathbf{Z}[b]$ of $\mathrm{End}(A)$ is integral over $\mathbf{Z}$ and is isomorphic to $\mathbf{Z}^a$ as a $\mathbf{Z}$-module, for some a. It then follows from the pigeon-hole principle that, given an integer q, two powers b^r, b^{r+m} must be congruent modulo $q\mathbf{Z}[b]$. Now the determinant of b is by assumption a non-zero integer d, divisible by b in $\mathbf{Z}[b]$ (as constant term in an equation for b), and we get $d^r(b^m - 1) \equiv 0 \pmod{q\mathbf{Z}[b]}$. Thus if q is coprime with d we deduce that $b^m \equiv 1 \pmod{q\mathbf{Z}[b]}$ and in particular the kernel of $b^m - 1$ contains the kernel of multiplication by q, which corresponds to the lattice $(1/q)L$ in the complex representation. Such lattice has diameter tending to 0 as q grows, proving what we want.

The preimage of X in T under the embedding $T \to A$ is an analytic subvariety W, say of complex dimension r. We have $bW \subset W$.

We may assume that we have coordinates in $\mathbf{C}^n$ such that b is induced by the linear map

$$\Phi(z_1, \dots, z_n) = (\lambda_1 z_1, \dots, \lambda_n z_n)$$

with $\lambda_i \in \overline{\mathbf{Q}}$.

In a cubic open neighborhood U of a smooth point of W we may renumber coordinates and suppose that $W' := W \cap U$ is given by a system of equations

$$z_{r+i} \equiv f_i(z_1, \dots, z_r) \pmod{L}, \qquad i = 1, \dots, n-r$$

for certain analytic functions f_i. Let π be the projection on the first r coordinates and let V be an open set contained in $\pi(U)$. Removing from V the set of zeros of any derivative $\partial f_i/\partial z_j$ which does not vanish identically on V, we are left with an open set. Hence, shrinking V and U if necessary, we may assume that if $\partial f_i/\partial z_j$ vanishes somewhere on V, then it vanishes identically.

In view of the above claim, and replacing b with a suitable positive power b^m if needed, we have a point $\mathbf{z}^* := (\mathbf{x}^*, \mathbf{y}^*) \in U$, where $\mathbf{x}^* = \pi(\mathbf{z}^*) \in V$, such that the class of $\mathbf{z}^*$ in A is fixed by b, or in other words $\Phi\mathbf{z}^* \equiv \mathbf{z}^* \pmod{L}$.

Let $\boldsymbol{\theta} \in \mathbf{C}^r$ be so small that $\mathbf{x}^* + \boldsymbol{\theta} \in V$. Then $P(\boldsymbol{\theta}) := (\mathbf{x}^* + \boldsymbol{\theta}, \mathbf{f}(\mathbf{x}^* + \boldsymbol{\theta}))$ belongs to $W + L$, hence $\Phi P(\boldsymbol{\theta}) \in W + L$ and we can write

$$\Phi P(\boldsymbol{\theta}) = \Phi\mathbf{z}^* + \Phi(\boldsymbol{\theta}, \mathbf{f}(\mathbf{x}^* + \boldsymbol{\theta}) - \mathbf{y}^*) = \mathbf{z}^* + \Phi(\boldsymbol{\theta}, \mathbf{f}(\mathbf{x}^* + \boldsymbol{\theta}) - \mathbf{y}^*) + \mathbf{l}^*,$$

for some $\mathbf{l}^* \in L$.

Now, let U' be any fixed small, open subset of U, with projection $V' \subset V$. Then it is clear that we can actually choose $\mathbf{z}^*$ such that $\mathbf{x}^* \in V'$ and $(\mathbf{x}^*, \mathbf{f}(\mathbf{x}^*))$, $\mathbf{z}^*$ lie in U', so that $\mathbf{f}(\mathbf{x}^*)$ is very near to $\mathbf{y}^*$. It follows that

$$\mathbf{z}^* + \Phi(\boldsymbol{\theta}, \mathbf{f}(\mathbf{x}^* + \boldsymbol{\theta}) - \mathbf{y}^*) \in U$$

for small $\boldsymbol{\theta}$, whence

$$\lambda_{r+i} f_i(\mathbf{x}^* + \boldsymbol{\theta}) = f_i(\mathbf{x}^* + (\lambda_1\theta_1, \dots, \lambda_r\theta_r)) + c_i \tag{1}$$

for $i = 1, \dots, r$ and all small $\boldsymbol{\theta}$. Here $c_i \in \mathbf{C}$ are independent of $\boldsymbol{\theta}$.

Equations (1) imply

$$(\lambda_j - \lambda_{r+i}) \cdot (\partial f_i/\partial z_j)(\mathbf{x}^*) = 0, \qquad \text{for all} \quad i,\ j,$$

and, by a previous remark, if $(\partial f_i/\partial z_j)(\mathbf{x}^*) = 0$ then $\partial f_i/\partial z_j$ vanishes identically. We conclude that either $\lambda_j = \lambda_{r+i}$ or f_i does not depend on z_j. Since f_i is analytic and λ_{r+i} is not a root of unity, comparison of Taylor expansions of (1) shows that f_i is linear in $\boldsymbol{\theta}$, as claimed.

Thus we have verified that $-\mathbf{z}^* + W$ contains an open subset of an r-dimensional complex linear space, with $\mathbf{z}^*$ a suitable torsion point on A. Since $-\mathbf{z}^* + W$ is analytic, it must in fact contain the said space and, reading everything back on X, we easily verify that X contains the translate by $\mathbf{z}^*$ of an analytic subgroup of A of dimension r. Since X is irreducible we have $X = \mathbf{x}^* + B$ for some abelian subvariety B of A. □

From now on we let A satisfy (A1) or (A2). We denote by h (respectively $\widehat{h}$) the absolute logarithmic Weil height on $\mathbf{P}^m(\overline{\mathbf{Q}})$ (respectively the Néron-Tate height induced by h on A). We also assume, as in Section I, that the divisor on A associated to the embedding $j : A \longrightarrow \mathbf{P}^m$ is even, hence $\widehat{h}$ is a positive semi-definite quadratic form on $A(\overline{\mathbf{Q}})$, vanishing precisely on the torsion points of A. As mentioned before, this determines an associate bilinear form $\langle P, Q\rangle := \frac{1}{2}[\widehat{h}(P+Q) - \widehat{h}(P) - \widehat{h}(Q)]$, an associated norm $|P| = \sqrt{\langle P, P\rangle}$ and a translation invariant semi-distance $d(P, Q) := |P - Q|$ on $A(\overline{\mathbf{Q}})$.

Lemma 4. *Let $F \in K[X_0, \dots, X_m]$ be a homogeneous polynomial and let $Q \in A(\overline{\mathbf{Q}})$ be such that $F(Q) = 0$. Let p be a prime number, sufficiently large with respect to A and F, supposed to lie in Σ in case* (A2). *Then there exists an endomorphism b of A such that*

(i) *either $F(bQ) = 0$,*

or

(ii) $\widehat{h}(Q) \geq p^{-c}$, *for a constant c depending only on A and F, but not on Q.*

Moreover, in Case (A1) *we can take b as complex multiplication by α with $(\alpha) = \mathfrak{p}_0^l$ for some prime ideal $\mathfrak{p}_0 \mid p$ in the field of complex multiplication of A and some positive integer l, depending only on A and the complex multiplication of A; all eigenvalues of b are conjugates of α. In case* (A2), *we can choose $b = p^l$ for some l depending only on A.*

Proof. We first deal with abelian varieties satisfying (A1), the proof in the other case being even simpler.

We can assume that A has complex multiplication by an order R of a subfield of K.

Let p be a prime number such that A has good reduction at all prime ideals $\mathfrak{p}$ of K above p. Then the Frobenius corresponding to $\mathfrak{p}$ is represented by multiplication by a suitable ideal (see e.g. [La, Lemma 3.1, p. 61]). A suitable power of the Frobenius (depending only on K and R) will fix K and will be such that the ideal in question becomes principal, generated by an element $\alpha \in R$. There exists an open cover $A = \cup A_\mu$ (defined, say, by $A_\mu = A \setminus \{P \in A : f_\mu(P) = 0\}$), in such a way that if $P \in A_\mu$ has coordinates $P = (x_0 : \cdots : x_m)$ we have

$$\alpha P = (y_0 : \cdots : y_m), \qquad y_i = \varphi_i(x_0 \ldots, x_N)$$

where the $\varphi_i = \varphi_{i,\mu}$ are suitable homogeneous polynomials without nontrivial common zeros on A_μ. Moreover, the fact that α reduces $(\operatorname{mod} \mathfrak{p})$ to an endomorphism of $A/\mathfrak{p}$ allows us to choose the covering A_μ and the polynomials φ_i such that the reduced polynomials $\widetilde{\varphi}_i$ have no nontrivial common zeros on the reduction $A_\mu/\mathfrak{p}$. Hence, denoting reduction $(\operatorname{mod} \mathfrak{p})$ by $\widetilde{\ }$, there exist equations

$$\widetilde{f}_\mu^M x_j^M = \sum \psi_{i,j} \widetilde{\varphi}_i \tag{2}$$

where M is a suitable positive integer and the $\psi_{i,j}$ are suitable homogeneous polynomials with coefficients in $\mathcal{O}_K/\mathfrak{p}$.

Moreover, if $Q \in A$ has algebraic coordinates, integral at some valuation v above $\mathfrak{p}$ and not all lying in the corresponding maximal ideal, then there exists μ such that $\widetilde{f}_\mu(\widetilde{Q}) \neq 0$, where now the tilde denotes reduction at v.

Since a power of the Frobenius is represented by multiplication by α we have, for $Q \in A_\mu$,

$$\varphi_i(x_0, \ldots, x_N) = \varphi(x_0, \ldots, x_N) x_i^q + \pi\, g_i(x_0, \ldots, x_N)$$

where φ and the g_i are homogeneous polynomials (depending also on μ) with $\mathfrak{p}$-integral coefficients, π is a local uniformizer in K for $\mathfrak{p}$ and q is a power of p.

Now let $F(X_0, \ldots X_m)$ be a homogeneous polynomial in $K[X_0, \ldots X_m]$ with coefficients in $\mathcal{O}_K$. We have, for $(x_0 : \cdots : x_m) \in A_\mu$,

$$F(\varphi_0, \ldots, \varphi_m) = \varphi^{\deg F} F^q(x_0, \ldots, x_m) + \pi\, G(x_0, \ldots, x_m)$$

where G has $\mathfrak{p}$-integral coefficients.

Assume that F vanishes at $Q = (\xi_0 : \cdots : \xi_m) \in A$, where the ξ_i lie in a number field $L \supset K$. We can choose homogeneous coordinates for Q such that if $v \mid \mathfrak{p}$ is a place of L above $\mathfrak{p}$ then $\max |\xi_i|_v = 1$. Also, choose μ such that $\widetilde{f}_\mu(\widetilde{Q}) \neq 0$. We have, setting $\varphi_i = \varphi_i(\xi_0, \ldots, \xi_m)$,

$$F(\varphi_0, \ldots, \varphi_m) = \pi\, G(\xi_0, \ldots, \xi_m)\,.$$

If $\zeta := F(\varphi_0, \ldots, \varphi_m) \neq 0$, we exploit the product formula $\sum_{v \in M_L} \log |\zeta|_v = 0$ as follows.

If $v \mid \mathfrak{p}$ we have, in view of the fact that G has $\mathfrak{p}$-integral coefficients,

$$\begin{aligned}\log|\zeta|_v &= \log|\pi\, G(\xi_0,\dots,\xi_m)|_v \\ &\le \log|\pi|_v + \deg(G)\max_i \log|\xi_i|_v \le \log|\pi|_v\,. \end{aligned} \tag{3}$$

For the remaining $v \nmid \mathfrak{p}$ we have

$$\begin{aligned}\log|\zeta|_v &= \log|F(\varphi_0,\dots,\varphi_m)|_v \\ &\le \deg(F)\max_i \log|\varphi_i|_v + \log|F|_v + \varepsilon_v(m+1)\log(\deg(F)+1)\end{aligned} \tag{4}$$

where $\varepsilon_v = 0$ if v is finite and $\varepsilon_v = [L_v : \mathbf{Q}_v]/[L:\mathbf{Q}]$ otherwise.

Observe now that equations (2) imply

$$\max_i \log|\varphi_i|_v = 0 \qquad \text{for} \quad v \mid \mathfrak{p}\,. \tag{5}$$

Moreover, we have

$$\sum_{v\in M_L} \max_i \log|\varphi_i|_v \le h(\varphi_0,\dots,\varphi_m) \le \widehat{h}(\alpha Q) + c_1 \le q^{c_2}\widehat{h}(Q) + c_1\,, \tag{6}$$

where c_1, c_2 are positive numbers depending only on the projective embedding j and K.

Summing the preceding inequalities (3), (4) for $\log|\zeta|_v$, using

$$\sum_{v\mid\mathfrak{p}} \log|\pi|_v \le -\frac{1}{[K:\mathbf{Q}]}\log p$$

and taking into account the product formula $\sum_v \log|\zeta|_v = 0$ and (5), (6), we infer

$$\log p \le c_3 q^{c_2}\widehat{h}(P) + c_4$$

where c_2, c_3, c_4 are positive constants depending only on the projective embedding j, K and the degree and height of F.

Hence, either $F(\alpha Q) = 0$ or $\widehat{h}(Q) \ge c_5 \cdot (\log p)p^{-c_6}$ for all primes $p \ge c_7$, for certain positive constants c_5, c_6, c_7 depending only on j, the field K and the degree and height of F.

The fact that all eigenvalues of the endomorphism b are conjugates of α is clear from the discussion in [La, Ch.1, p. 13].

As remarked at the beginning, the same argument works when A satisfies (A2) provided we use primes $p \in \Sigma$. □

Before giving the proof of Theorems 1 and 2, we remark that all abelian subvarieties $B \subset A$ are automatically defined over $\overline{\mathbf{Q}}$ (e.g. since the torsion points in B lie in $B(\overline{\mathbf{Q}})$ and are Zariski dense in B). Also, if A satisfies property (A1) or (A2), the same holds for each abelian subvariety B.

PROOF OF THEOREM 2. We prove the following claim:

There exist a finite union $T = T(X)$ of torsion cosets contained in X and a positive number $\gamma(X)$ such that if $Q \in (X \setminus T)(\overline{\mathbf{Q}})$ we have $\widehat{h}(Q) \geq \gamma$.

We argue by induction on the dimension k of X, the assertion being obvious for $k = 0$. We may clearly assume that X is irreducible. Let $F_1 = \cdots = F_r = 0$ be a system of defining equations for X. Let $Q \in X \subset A \subset \mathbf{P}^m$ be a point with algebraic coordinates. We have $F_1(Q) = \cdots = F_r(Q) = 0$. Let b be as in Lemma 4, with p sufficiently large with respect to all the F_i. If there exists j such that $F_j(bQ) \neq 0$, then Lemma 4 gives the required lower bound for $\widehat{h}(Q)$. So we may assume that $bQ \in X$. Let

$$X' := \{Q \in A : bQ \in X\}.$$

Then X' is a closed subvariety of A, of pure dimension k. We have shown that $\widehat{h}(Q)$ is bounded below except possibly for points $Q \in X \cap X' := Y$, say. If $\dim(Y) < \dim(X)$ our assertion follows by induction, since in any case $T(Y) \subset X$. If Y and X have the same dimension, then $Y = X$, so $bX \subset X$. We want to apply Lemma 3 to this situation, and for this we need to know that the eigenvalues of b are not roots of unity. This is clear in case (A2), and in case (A1) this follows from the last part of Lemma 4, because all eigenvalues are conjugates of α and b is not invertible. By applying Lemma 3, we have $X = x + B$ for a suitable abelian subvariety B and a torsion point $x \in A$. This proves the above claim and part (b) of Theorem 2 follows as a particular case.

Let now $x + B$ be any torsion coset contained in X. Since B is a divisible group and $\widehat{h}(x) = 0$, we see that $x+B$ contains a Zariski dense subset consisting of points with arbitrarily small height. Now the above claim shows that $x + B$ is contained in $T(X)$ and, being irreducible, in at least one of finitely many torsion cosets. This proves part (a). □

PROOF OF THEOREM 1. We prove first part (a). By Lemma 2 there are only finitely many abelian subvarieties B of A such that, for some x, $x + B$ is a maximal coset contained in X. Thus it suffices to show that, for a fixed B, the union of all cosets $x + B$ contained in X is a closed subset of X for the Zariski topology, and the number and degrees of its irreducible components are bounded only in terms of d and n. Such a union plainly equals $Z(X) := \bigcap_{g \in B}(g + X)$, say. We prove by induction on $k := \dim(X)$ that if X has q irreducible components of degrees at most d then $Z(X)$ is a closed subset of X, again such that the number and degrees of its irreducible components are bounded only in terms of d, q and n.

For $k = 0$ the assertion is obvious. Suppose there exists $g \in B$ such that $\dim(X \cap (g + X)) < k$. Setting $X_g := X \cap (g + X)$, we have $Z(X_g) = Z(X)$. By the general Bézout theorem already quoted, the number and degrees of the irreducible components of X_g are bounded only in terms of d, q and n, so induction applies to X_g. Therefore we may assume that for all $g \in B$ we have $\dim(X_g) = k$. Now we proceed by a further induction on the number s of irreducible components of X of dimension k, the assertion being true for $s = 0$

(in which case $\dim(X) \leq k-1$). Arguing as before with X_g in place of X we may assume that X_g too has s components of dimension k, for every $g \in B$. This means that translation by g leaves invariant the set of components of X of dimension k, i.e. B acts as permutation group on that set. We have already remarked in the proof of Lemma 2 that such an action must be trivial. Hence, denoting by $X_1, \dots, X_s$ the components of X of dimension k, we may assume that $g + X_i = X_i$ for all i and $g \in B$. Now write an irredundant decomposition $X = X_1 \cup \dots \cup X_s \cup Y$, where $\dim(Y) < k$. We have $Z(X) = X_1 \cup \dots \cup X_s \cup Z(Y)$. The inductive assumption applied to Y concludes the proof of (a).

Now we come to statements (b), (c). It clearly suffices to prove (c). Moreover, since (c) is invariant by translation, we may assume that Q is the origin O of A, so $d(P,Q) = \widehat{h}(P)^{\frac{1}{2}}$ and it suffices to obtain a lower bound for $\widehat{h}(P)$. We shall argue by induction on the dimension n of A.

Let X/L be an irreducible proper subvariety of $A \subset \mathbf{P}^m$, of degree at most d and dimension k, defined over $\overline{\mathbf{Q}}$. Then X can be defined by finitely many homogeneous polynomials of degree at most d (consider all cones over X with vertex a general linear subspace of $\mathbf{P}^m$ of dimension $m-k-2$). Thus there is a nonzero polynomial $f(\mathbf{x}) = f(x_0, \dots, x_m)$ of degree d vanishing on X but not on A. Let $\mathcal{L}$ be the set of monomials $\mathbf{x}^\lambda$ in $x_0, \dots, x_m$ of degree d and cardinality $L = |\mathcal{L}|$ and consider the $L \times L$ matrix

$$\chi_L := \begin{pmatrix} \mathbf{x}_1^\lambda \\ \mathbf{x}_2^\lambda \\ \dots \\ \mathbf{x}_L^\lambda \end{pmatrix}_{\lambda \in \mathcal{L}} .$$

Its determinant vanishes on X^L, because the equation $f(\mathbf{x}) = 0$ yields a linear relation among the columns of the matrix. Since $f(\mathbf{x})$ does not vanish on A, the maximum rank of the matrix as the points $\mathbf{x}_i$ run through X^L is strictly smaller the the corresponding number when the points run through A^L. Hence there is an integer r and an $r \times r$ minor M of the matrix χ_L such that $\Delta := \det(M)$ vanishes on X^r but not on A^r.

Now we apply Theorem 2 to the variety $V \subset A^r$ defined by $\Delta = 0$. Certainly A^r satisfies condition (A1) or (A2) if A does. We may use a Segre embedding induced from the embedding $A \subset \mathbf{P}^m$ to embed A^r in projective space, and then the Néron-Tate height on A^r is simply the sum of the heights on the factors. Also, note that V depends only on d and the projective embedding j, in the sense that d and m determine finitely many possibilities for Δ and hence for V. By Theorem 2, (a) we infer that the number of maximal torsion cosets $x + B \subset V$, with B an abelian subvariety of A^r, is finite and their number is bounded as a function of d and the embedding j, because V is determined by d and j.

For such a coset, B will be contained properly in A^r (since Δ does not vanish on A^r), so there exists some factor

$$A_\nu := \underbrace{O \times \dots \times O \times A \times \dots \times O}_{A \text{ is the } \nu\text{-th factor}} \tag{6}$$

not contained in B. Define B' as the abelian subvariety of A determined by the obvious projection of $A_\nu \cap B$ on A. Note that $\dim(B') < \dim(A)$. Again, B' satisfies (A1) or (A2) if A does.

Now we prove Theorem 1 by induction on $\dim(A)$, the result being trivial if $\dim(A) = 0$. Since $\dim(B') < \dim(A)$, the induction assumption applies to subvarieties $(g + X) \cap B' \subset B'$ with $g \in A$. Observe that, by the general Bézout theorem, the number and degrees of the components of $(g + X) \cap B'$ are bounded in terms of d and A and that the *original data* related to B' are determined by the data of A and by d.

Thus applying inductively Theorem 1 we obtain that there are γ' and an integer N', both depending on d and the data of A, such that if $P \in ((g + X) \cap B')(\overline{\mathbf{Q}})$, then:

(i) *either* $\widehat{h}(P) \geq \gamma'$,

or

(ii) *P belongs to some coset of positive dimension contained in* $(g + X) \cap B'$,

or

(iii) *P belongs to a finite set of at most N' elements.*

Clearly we may suppose that the same γ' and N' work for the finitely many B' involved here. Let t be their number, let $N'' = t\,N' + 1$ and take any r-tuple formed from any given N'' distinct points $P_i \in X^{\mathrm{o}}(\overline{\mathbf{Q}})$. If some such r-tuple does not lie in any of the finitely many relevant torsion cosets of B contained in V, then Theorem 2 applies and we have a positive lower bound for the height of some point P_i, depending only on d and the data for A, as wanted.

Otherwise, each r-tuple corresponds to some torsion coset of B and thus to some B', as described before. Now at least $(N'')^r/t$ distinct r-tuples will lie in a same torsion coset of B. Let A_ν be the factor as in (6) not contained in B, and let us associate to each such r-tuple the $(r-1)$-tuple obtained by projection on the $r-1$ trivial factors of A_ν. The number of $(r-1)$-tuples is $(N'')^{r-1}$, so at least $l \geq N''/t > N'$ of the r-tuples will have the same components save for the ν-th component. Therefore, subtracting from any such r-tuple a fixed one we obtain, after renumbering, that

$$P_i - P_1 \in B' \qquad \text{for} \quad i = 1, \ldots, l\,.$$

Hence $P_i - P_1 \in (-P_1 + X) \cap B'$ for all $i = 1, \ldots, l$ and (setting $g = -P_1$) we may apply one of (i), (ii) or (iii) to the points $P_i - P_1$.

Since $l > N'$, alternative (iii) cannot occur, so either $\widehat{h}(P_i - P_1) \geq \gamma'$ or $P_i - P_1$ belongs to some coset of positive dimension contained in $-P_1 + X$.

In the first case,

$$\widehat{h}(P_i) + \widehat{h}(P_1) \geq h(P_i - P_1) \geq \gamma'\,,$$

yielding the required lower bound for either $h(P_1)$ or $h(P_i)$.

In the second case, P_i lies in a coset of positive dimension contained in X, which is impossible since we assume $P_i \in X^{\circ}$.

We have shown that out of any $tN' + 1$ distinct points in $X^{\circ}(\overline{\mathbf{Q}})$ one of them has height bounded below by $\gamma'/2$. This concludes the proof. □

REFERENCES

[Abr] D. ABRAMOVICH, *Subvarieties of semi-abelian varieties*, Compositio Math. **90** (1994), 37-57.

[BP] D. BERTRAND - P. PHILIPPON, *Sous groupes de groupes algébriques commutatifs*, Illillois J. Math. **32** (1988), 263-280.

[BZ] E. BOMBIERI - U. ZANNIER, *Algebraic points on subvarieties of* $\mathbf{G}_m^n$, Internat Math. Res. Notices **7** (1995), 333-347.

[Bu] J.F. BURNOL, *Weierstrass points on arithmetic surfaces*, Inv. Math. **107** (1992), 421-432.

[El] N. ELKIES, *The existence of infinitely many supersingular primes for every elliptic curve over* **Q**, Inv. Math. **89** (1987), 561-567.

[Fu] W. FULTON, Introduction to Intersection Theory in Algebraic Geometry, Regional Conference Series in Mathematics, ISSN 0160-7642; n. 54, A.M.S., 1984.

[GH] P. GRIFFITHS - J. HARRIS, Principles of Algebraic Geometry, Wiley, 1978.

[Hi] M. HINDRY, *Autour d'une conjecture de S.Lang*, Inv. Math. **94** (1988), 575-603.

[La] S. LANG, Complex Multiplication, Springer, Verlag, 1983.

[McQ] M. MCQUILLAN, *Division points on semi-abelian varieties*, Inv. Math. **120** (1995), 143-159.

[Ray] M. RAYNAUD, *Sous variétés d'une variété abelienne et points de torsion*, In: "Arithmetic & Geometry", Coates & Helgason eds., Vol. 1, Birkhauser 1983.

[Sch1] W.M. SCHMIDT, *Heights of algebraic points lying on curves or hypersurfaces*, to appear in Proc. Amer. Math. Soc. (1995).

[Sch2] W.M. SCHMIDT, *Heights of points on subvarieties of* $\mathbf{G}_m^n$, preprint 1995.

[Sz] L. SZPIRO, *Sur les propriétés numériques du dualisant relatif d'une surface arithmétique*, The Grothendieck Festschrift Volume III, Progress in Mathematics **88**, Birkhäuser 1990.

[Zh1] S. ZHANG, *Positive line bundles on arithmetic surfaces*, Ann. of Math. **136** (1992), 569-587.

[Zh2] S. ZHANG, *Positive line bundles on arithmetic varieties*, J. Amer. Math. Soc. **8** (1995), 187-221.

[Zh3] S. ZHANG, *Small points and adelic metrics*, J. Algebraic Geom. **4** (1995), 281-300.

School of Mathematics
Institute for Advanced Study
Princeton, N.J. 08540, USA
eb@math.ias.edu

Dipartimento di
Costruzione dell'Architettura
Istituto Univ. di Architettura
Santa Croce 191
30135 Venezia, Italia
zannier@cidoc.iuav.unive.it