D. W. MASSER

Small values of the quadratic part of the Néron-Tate height on an abelian variety

Compositio Mathematica, tome 53, nº 2 (1984), p. 153-170

<http://www.numdam.org/item?id=CM_1984__53_2_153_0>

Compositio Mathematica 53 (1984) 153–170.

SMALL VALUES OF THE QUADRATIC PART OF THE NÉRON-TATE HEIGHT ON AN ABELIAN VARIETY

D.W. Masser

1. Introduction

Let A be an abelian variety of dimension $g \geqslant 1$ defined over the field $\overline{\mathbb{Q}}$ of algebraic numbers and embedded in projective space $\mathbb{P}_N$ of dimension $N \geqslant 1$. Then A is in fact defined over some smallest algebraic number field K, and for any subfield F of $\mathbb{C}$ containing K the set of points $A(F)$ of A defined over F is an additive group. We may construct absolute Weil height functions $H(P)$, $h(P)$ on $A(\overline{\mathbb{Q}})$ in the usual way as follows. First of all, if P is a point of $\mathbb{P}_N$ defined over $\overline{\mathbb{Q}}$, we can assume that P has projective coordinates $\xi_0, \dots, \xi_N$ lying in some algebraic number field F, and we put

$$H_F(P) = \prod_v \max(|\xi_0|_v, \dots, |\xi_N|_v),$$

where v runs over all valuations of F. To avoid the customary ramification indices we shall assume that these are normalized in such a way that each non-archimedean valuation extends the underlying p-adic valuation on $\mathbb{Q}$ and we have the product formula

$$\prod_v |\xi|_v = 1$$

for any non-zero ξ in F.

Next, if D is the degree of F the expression

$$H(P) = (H_F(P))^{1/D}$$

is independent of the choice of F, and we write

$$h(P) = \log H(P).$$

These are the standard absolute height functions on the set of points of $\mathbb{P}_N$ defined over $\overline{\mathbb{Q}}$, and by specialization they give the required height functions on the subset $A(\overline{\mathbb{Q}})$ (here, as always, we identify A with $A(\mathbb{C})$, and we regard both as subsets of $\mathbb{P}_N$).

Now we have the fundamental Néron-Tate decomposition

$$h(P)=q(P)+l(P)+c(P),$$

where $q(P)$ is a quadratic form on $A(\overline{\mathbb{Q}})$, $l(P)$ is a linear form on $A(\overline{\mathbb{Q}})$, and $c(P)$ is a function bounded on $A(\overline{\mathbb{Q}})$ (see for example Theorem 3 of [4]). Moreover it is well-known that $q(P)$ is positive definite on the quotient of $A(\overline{\mathbb{Q}})$ by the group of torsion points of A (a simple proof is to use Lemma 7 below to deduce that $h(nP)$ is bounded independently of the integer n as soon as $q(P)=0$).

Hence if P is a non-torsion point of $A(\overline{\mathbb{Q}})$, we have $q(P)>0$. One of the aims of the present paper is to give a refinement of this assertion in terms of the degree $d(P)$ of P. This is simply the degree over $\mathbb{Q}$ of the field generated over K by the ratios of the projective coordinates of P. It is not too difficult to see that there exist positive functions $\psi(D)$ and $\omega(D)$, depending only on A and the integer $D\geqslant 1$, such that if P is a point of $A(\overline{\mathbb{Q}})$ with $d(P)\leqslant D$ and $q(P)<(\psi(D))^{-1}$, then P is a torsion point of order at most $\omega(D)$ (and so necessarily $q(P)=0$ as well). Such inequalities have applications to questions of linear independence on A, as explained in [7]. As an example, let $P_1,\dots,P_m$ be points of $A(F)$ for a field F containing K, with $[F:\mathbb{Q}]\leqslant D$ and $q(P_i)\leqslant Q$ $(1\leqslant i\leqslant m)$ for some integer $D\geqslant 1$ and some real $Q\geqslant(\psi(D))^{-1}$. Then the arguments of [7] (Sections 2 and 5) show that $P_1,\dots,P_m$ are linearly dependent over $\mathbb{Q}$ if and only if $t_1P_1+\cdots+t_mP_m=0$ for rational integers $t_1,\dots,t_m$ with

$$0<\max(|t_1|,\dots,|t_m|)\leqslant\omega(D)\big(m^2\psi(D)Q\big)^{(m-1)/2}.$$

Now the simple counting method of [7] (p. 217) allows us to take $\psi(D)$ and $\omega(D)$ not exceeding c^{D^2} for some positive constant c depending only on A. With more care, and the use of the Box Principle as in [10], these can both be improved to c^D; it is also interesting that an argument of Stuhler using reduction theory appears to yield the slightly weaker estimate $(cD)^{cD}$ for $\omega(D)$. However, we do not give the details of these elementary methods, as the results proved in the present paper are rather stronger. They are summarized in the following theorem.

THEOREM: *There are positive constants κ and λ, depending only on the dimension g of A, and a positive constant C depending only on A, with the following properties. Suppose for some integer $D\geqslant 1$ that P is a point of $A(\overline{\mathbb{Q}})$ with $d(P)\leqslant D$ and $q(P)<C^{-1}D^{-\kappa}$. Then P is a torsion point of order at most CD^{λ}.*

In particular it follows that

$$(d(P))^{\kappa}q(P) \geqslant C^{-1}$$

for all non-torsion P in $A(\overline{\mathbf{Q}})$.

We have taken some trouble to calculate the best value of κ that our method will give, and we find that any κ with

$$\kappa > 2g + 6 + 2g^{-1}$$

is permissible. Thus, in accordance with the main result of Anderson and the author in [1] on elliptic curves, we may take any $\kappa > 10$ for $g = 1$; and we may further take any $\kappa > 11$ for $g = 2$. Some improvements are possible in special cases; for example, the methods of [1] easily extend to permit any value $\kappa > 3$ (independently of g) if A has many complex multiplications.

We have been less careful in our estimates for λ; when A is a simple abelian variety our Theorem is valid for any λ satisfying

$$\lambda > g + 4 + g^{-1};$$

and this result then allows us to take any

$$\lambda > 6g \tag{1}$$

in the Theorem when A is not necessarily simple. But for $g = 1$ it is already known from class field theory (or [6]) and the work [11] of Serre that $\lambda > \frac{1}{2}$ suffices if we are not interested in calculating constants effectively (but see [12]); and Paula Cohen has recently obtained a completely effective estimate with any $\lambda > 1$. Either result leads immediately to an improvement on (1) for arbitrary A, with $6g$ replaced by $13g/4$.

However, it should be at once pointed out that the best possible values of κ and λ are probably much smaller, and they are liable to depend on the factorization of A into simple varieties as well as on the ring of endomorphisms of A. As the Corollary below suggests, these questions are related to difficult unsolved problems of Kummer theory on abelian varieties, and there seems little point in putting forward precise conjectures at the moment. Let us just note in passing that it seems likely that if A is simple then the Theorem holds for any $\kappa > g^{-1}$; and for elliptic curves with complex multiplication a slightly sharper form of this has recently been proved by Laurent [5].

In the following Corollary we fix any constants κ, λ satisfying the conditions of the above Theorem.

COROLLARY: *Let Q be a point of $A(\overline{\mathbb{Q}})$. Then there exists a positive constant c, depending only on Q and A, with the following property*:
(i) If Q is non-torsion and P is any point on $A(\overline{\mathbb{Q}})$ with $TP = Q$ for some integer $T \geqslant 1$, then $d(P) \geqslant cT^{2/\kappa}$.
(ii) If Q is torsion and P is any point on $A(\overline{\mathbb{Q}})$ with $TP = Q$ for some minimal integer $T \geqslant 1$, then $d(P) \geqslant cT^{1/\lambda}$.

From the point of generalized Kummer theory, these lower bounds are rather weak. Nevertheless they seem to be the only results of their kind at present, and, moreover, the constants appearing are all in principle effectively computable. It should be pointed out, however, that recent work of Bogomolov [16] implies an ineffective sharpening of (ii) in a special case. Namely, if T is a power of a fixed prime l, then we can take $\lambda = 1$ provided c is now allowed to depend on l.

The proofs of these results are arranged in this paper as follows. First, in Section 2 we collect a number of results from [8] about general group varieties, and we deduce a zero estimate for the special group variety $\mathbb{C} \times A$ appropriate to our problem. After some preliminaries in Section 3 we prove in Section 4 our Theorem for a simple abelian variety. Finally in Section 5 we prove the Theorem in general and we also deduce the Corollary.

2. Zero estimates

Let G be an arbitrary quasi-projective commutative group variety of dimension $n \geqslant 1$ embedded in some projective space X. For $m \geqslant 1$ let $\gamma_1, \dots, \gamma_m$ be elements of G, and for integers $s_1, \dots, s_m$ write $\sigma = (s_1, \dots, s_m)$ for the corresponding element of $\mathbb{Z}^m$ and

$$\Psi(\sigma) = s_1\gamma_1 + \cdots + s_m\gamma_m$$

for the corresponding linear combination in G. Write also

$$|\sigma| = \max(|s_1|, \dots, |s_m|),$$

and for a real number $S \geqslant 0$ let $\mathbb{Z}^m(S)$ denote the set of σ with $0 \leqslant s_1, \dots, s_m \leqslant S$.

We say that a subset W of G is defined in G by homogeneous polynomials $P_1, \dots, P_k$ if the set of common zeroes of these polynomials in X meets G precisely in W.

LEMMA 1: *There is a constant $c > 0$, depending only on G, with the following property. Suppose for some integer $D \geqslant 1$ and some real $\theta \geqslant n/m$ there exists a homogeneous polynomial of degree at most D vanishing on*

$\Psi(\mathbb{Z}^m(n(cD)^\theta))$ but not all of G. Then there are integers k, r with

$$1 \leqslant k \leqslant m, \quad 1 \leqslant r \leqslant n, \quad k + r\theta^{-1} > m,$$

together with a subgroup Z of $\mathbb{Z}^m$ of rank at least k and an algebraic subgroup H of G of dimension at most $n - r$, such that $\Psi(Z) \subseteq H$. Furthermore, Z contains elements $\sigma_1, \dots, \sigma_k$, linearly independent over $\mathbb{Z}$, with

$$|\sigma_j| \leqslant (cD)^{r/(m+1-j)} \qquad (1 \leqslant j \leqslant k),$$

and H is contained in an algebraic subset S of G, of dimension at most $n - r$, that is defined in G by homogeneous polynomials of degrees at most cD.

Proof: This is Theorem I (Chapter I) of [8], which generalizes the earlier work of [15]. In fact c depends only on the degrees of the equations defining the Zariski closure of G in X and the degrees of the equations defining its addition laws.

Lemma 2: *There is a constant $c > 0$, depending only on G, with the following property. Suppose for some integer $D \geqslant 1$ that S is an algebraic subset of G, defined in G by homogeneous polynomials of degrees at most D. If H is an algebraic subgroup of G contained in S, there exists an algebraic subgroup H' of G, itself defined in G by homogeneous polynomials of degrees at most cD, such that*

$$H \subseteq H' \subseteq S.$$

Proof: This is the Proposition (Chapter 1) of [8]. Here in fact c depends only on the degrees of the equations defining the addition laws on G.

The next lemma is a technical estimate for primary ideal components. For $n \geqslant 1$ let $\mathfrak{R} = \mathbb{C}[X_0, \dots, X_n]$ be a polynomial ring in $n + 1$ variables. Recall that a non-zero proper homogeneous ideal $\mathfrak{J}$ of $\mathfrak{R}$ has rank r satisfying $1 \leqslant r \leqslant n + 1$; the dimension of its associated variety in $\mathbb{P}_n$ is then $n - r$. It is convenient here to define the rank of the zero ideal as 0. Also, if $1 \leqslant r \leqslant n$, we denote the degree of $\mathfrak{J}$ by deg $\mathfrak{J}$; this is a positive integer. In addition, for $1 \leqslant t \leqslant k$ and integers $D_1 \geqslant 1, \dots, D_k \geqslant 1$ we write $M_t(D_1, \dots, D_k)$ for the maximum of the products of $D_1, \dots, D_k$ taken t at a time. If $t = 0$ we interpret this expression as 1.

Lemma 3: *For $0 \leqslant r \leqslant n$ and an integer $D \geqslant 1$ let $\mathfrak{J}_0$ be an ideal of $\mathfrak{R}$ of rank r generated by homogeneous polynomials of degrees at most D. For $k \geqslant 1$ and integers $D_1 \geqslant D, \dots, D_k \geqslant D$ let $P_1, \dots, P_k$ be homogeneous poly-*

nomials of degrees at most $D_1, \ldots, D_k$ respectively. Suppose that $\mathfrak{J} = (\mathfrak{J}_0, P_1, \ldots, P_k)$ is a non-zero proper ideal of $\mathfrak{R}$ and that for some s with $r \leqslant s \leqslant n$ it has at least one isolated primary component of rank s. Then as $\mathfrak{Q}$ runs over all such isolated primary components of $\mathfrak{J}$ of rank s, we have

$$\sum \deg \mathfrak{Q} \leqslant D^{s-t} M_t(D_1, \ldots, D_k),$$

where $t = \min(s - r, k)$.

Proof. This is Theorem II (Chapter 2) of [8].

Now we shall consider the special group variety $G = \mathbb{C} \times A$, where A is a simple abelian variety of dimension $g \geqslant 1$ embedded in $\mathbb{P}_N$ for some $N \geqslant 1$. If the additive group variety $\mathbb{C}$ is embedded in $\mathbb{P}_1$ in the usual way, the Segre map provides an embedding of G in $\mathbb{P}_{2N+1}$. Let $\pi_{\mathbb{C}}$, π_A denote the projections from $\mathbb{C} \times A$ to the factors $\mathbb{C}$, A respectively.

Lemma 4: *There is a constant* $c > 0$, *depending only on* A, *with the following property. For an integer* $D \geqslant 1$ *let* H *be a proper algebraic subgroup of* $\mathbb{C} \times A$, *defined in* $\mathbb{C} \times A$ *by homogeneous polynomials of degrees at most* D, *such that* $\pi_{\mathbb{C}}(H) \neq 0$. *Then* $\pi_A(H)$ *is a finite group of order at most* cD^g.

Proof: Since there are no surjective homomorphisms from $\mathbb{C}$ to A or from A to $\mathbb{C}$, Kolchin's Theorem [3] (p. 1152) shows that the algebraic groups $\pi_{\mathbb{C}}(H)$, $\pi_A(H)$ satisfy either $\pi_{\mathbb{C}}(H) \neq \mathbb{C}$ or $\pi_A(H) \neq A$. As $\pi_{\mathbb{C}}(H) \neq 0$ by hypothesis and $\mathbb{C}$ has no non-zero proper algebraic subgroups, we must have $\pi_{\mathbb{C}}(H) = \mathbb{C}$. Hence $B = \pi_A(H) \neq A$. Because A is simple, this means that B is a finite group. Now as b runs over all elements of B the disjoint algebraic sets $H_b = H \cap \pi_A^{-1}(b)$ exactly cover H and they are cosets of the group H_0 corresponding to $b = 0$. If $\pi_{\mathbb{C}}(H_0) = 0$ it would follow that $\pi_{\mathbb{C}}(H)$ is finite, which is not so; therefore $\pi_{\mathbb{C}}(H_0) = \mathbb{C}$. We deduce easily that $H = \mathbb{C} \times B$.

Hence for each b in B the Zariski closure $\mathbb{P}_1 \times b$ of H_b in $\mathbb{P}_{2N+1}$ is an irreducible component of the Zariski closure $\mathbb{P}_1 \times B$ of H in $\mathbb{P}_{2N+1}$. Now we can find an integer $c_0 \geqslant 1$ depending only on A, and homogeneous polynomials $Q_1, \ldots, Q_l$, of degrees at most c_0, whose set of common zeroes in $\mathbb{P}_{2N+1}$ is $\mathbb{P}_1 \times A$. Thus the ideal $\mathfrak{J}_0 = (Q_1, \ldots, Q_l)$ has rank $r = 2N - g$. Also by hypothesis we can find homogeneous polynomials $P_1, \ldots, P_k$, of degrees at most D, whose set of common zeroes in $\mathbb{P}_{2N+1}$ meets $\mathbb{C} \times A$ exactly in $H = \mathbb{C} \times B$. It follows easily that for each b in B the ideal $\mathfrak{J} = (\mathfrak{J}_0, P_1, \ldots, P_k)$ has an isolated prime component of rank $s = 2N$ corresponding to $\mathbb{P}_1 \times b$ (it may well have other isolated components, but if so, they correspond to subvarieties of $\infty \times A$, where ∞ is the point of $\mathbb{P}_1$ not in $\mathbb{C}$).

Finally Lemma 3 with $n = 2N + 1$ shows that the total number of isolated prime components of $\mathfrak{J}$ of rank $2N$ is at most

$$c_0^{2N-t}\left(\max(c_0, D)\right)^t \leqslant c_0^{2N}D^t,$$

where $t = \min(g, k)$. Hence we get the required estimate for the cardinality of B, with $c = c_0^{2N}$.

We can now give our special zero estimate as a consequence of these lemmas. There exists a Riemann lattice $\mathscr{L}$ in $\mathbb{C}^g$, together with associated theta functions $\theta_0(z),\dots,\theta_N(z)$ having no common zeroes in $\mathbb{C}^g$, such that by sending the point z of $\mathbb{C}^g$ to the point $\Theta(z)$ of $\mathbb{P}_N$ with projective coordinates $\theta_0(z),\dots,\theta_N(z)$, we obtain an analytic isomorphism between the quotient $\mathbb{C}^g/\mathscr{L}$ and our simple abelian variety A. Let $\theta_0'(z)$ be any linear combination of $\theta_0(z),\dots,\theta_N(z)$, not vanishing at $z = 0$, and assume that the quotients $f_i(z) = \theta_i(z)/\theta_0'(z)$ $(1 \leqslant i \leqslant g)$ are algebraically independent.

Proposition: *There is a constant $C > 0$, depending on A but not on the functions $f_1(z),\dots,f_g(z)$, with the following property. For an integer $D \geqslant 1$ let v be a point of $\mathbb{C}^g$ such that $f_1(z),\dots,f_g(z)$ are analytic at sv for all integers s with $0 \leqslant s \leqslant CD^{g+1}$, and let P be a non-zero polynomial of total degree at most D such that*

$$P\left(s, f_1(sv),\dots,f_g(sv)\right) = 0$$

for all integers s with $0 \leqslant s \leqslant CD^{g+1}$. Then there is an integer s_0 with $1 \leqslant s_0 \leqslant CD^{2g+1}$ such that $s_0 v$ lies in $\mathscr{L}$.

Proof: We use constants c_1, ... depending only on A. We apply Lemma 1 with $G = \mathbb{C} \times A$, so $n = g + 1$, and $m = 1$, with γ_1 as the point of G defined by

$$\pi_{\mathbb{C}}(\gamma_1) = 1, \quad \pi_A(\gamma_1) = \Theta(v).$$

We take $\theta = n/m = g + 1$. On writing $f_1(z),\dots,f_g(z)$ as quotients of linear forms in $\theta_0(z),\dots,\theta_N(z)$, we see without difficulty that if C is sufficiently large our polynomial P gives rise to a homogeneous polynomial satisfying the conditions of Lemma 1; this does not vanish on all of G because $f_1(z),\dots,f_g(z)$ are algebraically independent. The resulting integers k, r necessarily satisfy $k = 1$ and $1 \leqslant r \leqslant g + 1$, so we obtain an integer s_1, with $0 < |s_1| \leqslant c_1 D^{g+1}$, such that the group Γ generated by $s_1\gamma_1$ lies in a proper algebraic subgroup H of G. Furthermore H lies in an algebraic subset S of G, of dimension at most g, that is defined in G by homogeneous polynomials of degrees at most $c_2 D$. Hence by Lemma 2 we can find an algebraic subgroup H' of G, itself defined in G by homogeneous polynomials of degrees at most $c_3 D$, with $H \subseteq H' \subseteq S$. So

H' is a proper algebraic subgroup, and $\pi_{\mathbb{C}}(H') \neq 0$ because this projection contains $\pi_{\mathbb{C}}(H) \supseteq \pi_{\mathbb{C}}(\Gamma) = s_1\mathbb{Z}$. Thus by Lemma 4 we conclude that $\pi_A(H')$ is a finite group of order t not exceeding $c_4 D^g$. Hence $t\pi_A(H') = 0$, and since $s_1\gamma_1$ lies in $\Gamma \subseteq H \subseteq H'$ this gives

$$0 = t\pi_A(s_1\gamma_1) = ts_1\Theta(v).$$

We may evidently suppose $s_1 > 0$; and now the Proposition follows with $s_0 = ts_1$.

We need one more preliminary result about zeroes of polynomials. We shall actually be working with the group variety $(\mathbb{C} \times A)^t$ for a large integer t, but it would not have been so straightforward to analyse the algebraic subgroups of this group. However, the following simple lemma on Cartesian products will suffice for our purposes. For $n \geqslant 1$, $t \geqslant 1$ and a subset S of $\mathbb{C}^n$ denote by S^t the t-fold Cartesian product of S in $\mathbb{C}^{nt}$.

LEMMA 5: *Let S be a subset of $\mathbb{C}^n$, and for some integer $D \geqslant 1$ suppose there is a non-zero polynomial of total degree at most D that vanishes on S^t. Then there is a non-zero polynomial of total degree at most D that vanishes on S.*

PROOF: This is a straightforward induction on t, and we omit the details. If S is a finite set, then, with the notation of [14], this result says that $\omega_1(S) \leqslant \omega_1(S^t)$, and in fact it is just as easy to see that we always have equality here.

3. Preliminaries

For $n \geqslant 1$ let P be a non-zero polynomial in variables $x_1, \ldots, x_n$ with algebraic coefficients. Regarding these coefficients as projective coordinates in some space of large dimension, we may define as in Section 1 the projective absolute height $H(P)$ of P. If $P = 0$ we define $H(P) = 0$. We note that if $P_1, \ldots, P_k$ are such polynomials whose product $P_1 \ldots P_k$ has total degree at most $D \geqslant 1$, then

$$H(P_1 \ldots P_k) \geqslant e^{-nD} H(P_1) \ldots H(P_k); \tag{2}$$

this follows in the usual way from Gelfond's well-known inequality in [2] (p. 135) and its conjugates, together with the corresponding non-archimedean equalities.

The classical height $H(\alpha)$ of an algebraic number α is then just the height of the polynomial $x_1 - \alpha$. If P as above has total degree at most $D \geqslant 1$ and its coefficients are in fact rational integers of absolute values at most $U \geqslant 1$, then we have

$$H(\beta) \leqslant U(D+1)^n (H(\alpha_1)\dots H(\alpha_n))^D \tag{3}$$

for any algebraic numbers $\alpha_1, \dots, \alpha_n$ and $\beta = P(\alpha_1, \dots, \alpha_n)$. See for example Lemma 1 (p. 26) of [1].

Lemma 6: *For an integer $D \geqslant 1$ suppose F is an algebraic number field of degree at most D, and let m, n be positive integers with $\delta n \geqslant (1+\delta)Dm$ for some $\delta > 0$. For $H \geqslant 1$ let $L_1, \dots, L_m$ be linear forms with coefficients in F and projective absolute heights at most H. Then there exist rational integers $x_1, \dots, x_n$ with*

$$0 < \max(|x_1|, \dots, |x_n|) \leqslant (nH)^\delta$$

such that

$$L_i(x_1, \dots, x_n) = 0 \qquad (1 \leqslant i \leqslant m).$$

Proof: See the Proposition (p. 32) of [1].

Let now A be an abelian variety as in the introduction, and let $h(P)$, $q(P)$, $c(P)$ be the associated functions defined on $A(\overline{\mathbb{Q}})$.

Lemma 7: *Let c be any constant such that $|c(P)| \leqslant c$ for all P in $A(\overline{\mathbb{Q}})$. Then we have*

$$(h(P))^{1/2} \leqslant (q(P))^{1/2} + c^{1/2}$$

for all P in $A(\overline{\mathbb{Q}})$.

Proof: Let P be an arbitrary point on $A(\overline{\mathbb{Q}})$. Then for any integers r, s with $s \neq 0$ we can find Q on $A(\overline{\mathbb{Q}})$ such that $sQ = rP$. Now

$$0 \leqslant h(Q) = q(Q) + l(Q) + c(Q)$$

$$= (r/s)^2 q(P) + (r/s) l(P) + c(Q) \leqslant f(r/s),$$

where $f(x)$ denotes the quadratic polynomial $x^2 q(P) + x l(P) + c$. Hence f is non-negative on $\mathbb{Q}$, so non-negative on $\mathbb{R}$, so we must have $(l(P))^2 \leqslant 4cq(P)$. Thus we get

$$h(P) = q(P) + l(P) + c(P) \leqslant q(P) + 2(cq(P))^{1/2} + c,$$

and the lemma follows on taking the square root. We note that the opposite inequality

$$(h(P))^{1/2} \geqslant (q(P))^{1/2} - (1+\sqrt{2})c^{1/2}$$

is almost as easy to prove.

Next, for the abelian variety A as above, we recall the period lattice $\mathscr{L}$ and the theta functions $\theta_0(z), \ldots, \theta_N(z)$ of Section 2.

LEMMA 8: *There exists a constant $c > 0$, depending only on $\mathscr{L}$, with the following property. For any real $B \geqslant 1$ and any element u of $\mathbb{C}^g$ we can find an integer b with $1 \leqslant b \leqslant B$ such that*

$$|bu - \omega| \leqslant cB^{-1/(2g)}$$

for some period ω of $\mathscr{L}$.

PROOF: This is a straightforward application of the Box Principle; compare Lemma 5 (p. 28) of [1].

LEMMA 9: *There is a constant $c > 0$, depending only on the functions $\theta_0(z), \ldots, \theta_N(z)$, such that*

$$c^{-1-|z|^2} \leqslant \max_{0 \leqslant i \leqslant N} |\theta_i(z)| \leqslant c^{1+|z|^2}$$

for any z in $\mathbb{C}^g$.

PROOF: This follows easily from the functional equations for $\theta_0(z), \ldots, \theta_N(z)$ together with the fact that these have no common zeroes; compare the proof of Lemma 3 (p. 27) of [1].

Finally we record a well-known Schwarz Lemma in several complex variables. For $t \geqslant 1$ let $F(z_1, \ldots, z_t)$ be an entire function and for real $R \geqslant 0$ let $M(F, R)$ be its maximum modulus for $|z_1| = \cdots = |z_t| = R$. Recall the notation $\mathbb{Z}^t(R)$ of Section 2.

LEMMA 10: *For $R \geqslant 0$ let $F(z_1, \ldots, z_t)$ be an entire function vanishing on $\mathbb{Z}^t(R)$. Then for any $S \geqslant R$ we have*

$$M(F, S) \leqslant 2^{-R/t} M(F, 5S).$$

PROOF: See Proposition 7.2.1 (p. 122) of [14]; however, it should be noted that there is a factor $1/n$ missing in the displayed formula, because of an incorrect application on p. 127 of the Landau trick of replacing f by f^k.

4. The auxiliary function

Here we shall prove our Theorem when the abelian variety is simple. We fix arbitrary numbers κ, λ with

$$\kappa > 2g + 6 + 2g^{-1}, \lambda > g + 4 + g^{-1}. \tag{4}$$

It will suffice to show that if D is sufficiently large and P is a point on $A(\overline{\mathbb{Q}})$ with

$$d(P) \leqslant D, \quad q(P) \leqslant D^{-\kappa}, \tag{5}$$

then P is necessarily a torsion point of order at most D^{λ}. This we proceed to do by constructing a suitable auxiliary function.

For any integer $t \geqslant 1$ and any real number $\epsilon > 0$ we define exponents

$$\phi = g^{-1} + t^{-1}g^{-1} + 2\epsilon, \quad \theta_0 = 1 + g^{-1} + t^{-1}g^{-1} + 3\epsilon$$

$$\theta = 1 + g^{-1} + t^{-1}(1 + g^{-1}) + (2g + 3)\epsilon.$$

Then we have the inequalities

$$(g+1)t\phi > t\theta_0 + 1 \tag{6}$$

$$\theta > (g+1)\phi \tag{7}$$

$$\theta_0 > 1 + \phi. \tag{8}$$

We put

$$L = [D^{\phi}], \quad S_0 = D^{\theta_0}, \quad D = D^{\theta}.$$

Further we define the exponent

$$\psi = g + 2 + t^{-1}(2g + 2) + (4g^2 + 6g + 1)\epsilon;$$

then

$$\psi > 2g\theta - g, \tag{9}$$

and we take

$$B = D^{\psi}.$$

Finally we put

$$\xi = 2g + 6 + 2g^{-1} + t^{-1}(4g + 6 + 2g^{-1}) + (8g^2 + 16g + 9)\epsilon,$$

so that

$$\xi > 2\theta + 2\psi. \tag{10}$$

As $t \to \infty$ and $\epsilon \to 0$ we see that $\xi \to 2g + 6 + 2g^{-1}$ and $(2g+1)\phi + \psi \to g + 4 + g^{-1}$; hence by (4) we may fix t and ϵ such that

$$\xi < \kappa, \quad (2g+1)\phi + \psi < \lambda. \tag{11}$$

We then have from (5)

$$q(P) \leqslant D^{-\xi}.$$

Henceforth all constants $c_1, \ldots$ will be positive and they will depend only on A (and the fixed numbers t, ϵ). Also we shall suppose D is sufficiently large in terms of these quantities. We start by choosing any u in $\mathbb{C}^g$ such that $P = \Theta(u)$. Then we use an idea of Stewart [13] which is necessary to counteract the analytic growth of the theta functions. Namely, by Lemma 8 there exists an integer b with $1 \leqslant b \leqslant B$ and a period ω of $\mathscr{L}$ such that the vector

$$v = bu - \omega$$

satisfies

$$|v| \leqslant c_1 B^{-1/(2g)}. \tag{12}$$

We now observe that for any integer s with $0 \leqslant s \leqslant S$ we have

$$q(sbP) = s^2 b^2 q(P) \leqslant S^2 B^2 D^{-\xi},$$

which by (10) does not exceed c_2. Hence from Lemma 7 we deduce the inequality

$$H(sbP) \leqslant c_3 \tag{13}$$

for all integers s with $0 \leqslant s \leqslant S$.

LEMMA 11: *There exist integers $k_0, \ldots, k_N$ of absolute values at most c_4 such that the function*

$$\theta_0'(z) = k_0\theta_0(z) + \cdots + k_N\theta_N(z)$$

satisfies

$$\theta_0'(sv) \neq 0$$

for all integers s with $0 \leqslant s \leqslant S$.

Proof: Suppose k is a positive integer such that

$$\theta_0(sv) + k\theta_1(sv) + \cdots + k^N\theta_N(sv) = 0$$

for some integer s with $0 \leqslant s \leqslant S$. We can find a non-zero complex number w such that the polynomial

$$S(x) = w\big(\theta_0(sv) + x\theta_1(sv) + \cdots + x^N\theta_N(sv)\big)$$

has algebraic coefficients, and then its absolute height $H(S)$ is simply the Weil height $H(sbP)$ of the point sbP on $A(\overline{\mathbb{Q}})$. But $S(k) = 0$, so $S(x)$ has a factor $L(x) = x - k$. Writing $S(x) = L(x)T(x)$, we have by (2)

$$H(sbP) = H(S) \geqslant \mathrm{e}^{-N}H(L)H(T) \geqslant \mathrm{e}^{-N}H(L) = \mathrm{e}^{-N}k.$$

Thus by (13) we deduce that $k \leqslant c_3\mathrm{e}^N$. The lemma follows on taking k_1 as the least positive integer exceeding $c_3\mathrm{e}^N$, and $k_i = k_1^i$ $(0 \leqslant i \leqslant N)$.

Next, the quotients

$$f_i(z) = \theta_i(z)/\theta_0'(z) \qquad (0 \leqslant i \leqslant N)$$

generate the field of all abelian functions with respect to $\mathscr{L}$, and without loss of generality we may suppose that $f_1(z),\ldots,f_g(z)$ are algebraically independent over $\mathbb{C}$. By the preceding lemma these are analytic at $z = sv$ for all integers s with $0 \leqslant s \leqslant S$. Furthermore it follows easily from (13) and the standard estimates (3) that

$$H(f_i(sv)) \leqslant c_5 \qquad (0 \leqslant i \leqslant N, \quad 0 \leqslant s \leqslant S). \tag{14}$$

It is now usual to construct an auxiliary function whose coefficients involve a basis of the field we are working over. However, it seems that this would introduce estimates of order c^D. We are able to improve upon this by restricting the coefficients to $\mathbb{Z}$ and using a large number of variables, by analogy with an idea of Philippon [9].

Lemma 12: *There exists a non-zero polynomial P_0 of total degree at most L, whose coefficients are rational integers of absolute values at most D^{c_6L}, such that the function $f(z_1,\ldots,z_t) = P_0(z_1,\ldots,z_t, f_1(z_1v),\ldots,f_g(z_1v),\ldots, f_1(z_tv),\ldots,f_g(z_tv))$ vanishes on $\mathbb{Z}^t(S_0)$.*

Proof: We have here

$$m \leqslant (S_0+1)^t \leqslant c_7S_0^t$$

conditions and

$$n \geqslant c_8 L^{(g+1)t}$$

unknowns, corresponding to m linear forms in n variables with coefficients in the field F generated over K by the ratios of the projective coordinates of P. From (6) we deduce $n \geqslant 2Dm$, and since F has degree at most D, the basic inequality of Lemma 6 holds with $\delta = 1$. Thus it remains to calculate an upper bound H for the heights of the linear forms involved. Let $(s_1,\ldots,s_t)$ be an element of $\mathbb{Z}^t(S_0)$. Then from (14) and (3) we find without difficulty that the height of the corresponding linear form is at most $c_9^L(s_1+1)^L\ldots(s_t+1)^L$. We deduce that $H \leqslant c_9^L(2S_0)^{tL} \leqslant D^{c_{10}L}$, and now the present lemma follows at once from the estimates of Lemma 6.

Lemma 13: *For any integer s with $0 \leqslant s \leqslant S$ we have*

$$|\theta_0'(sv)| \geqslant \exp(-c_{11}D).$$

Proof: From (14) it follows that

$$|f_i(sv)| \leqslant c_5^D \qquad (0 \leqslant i \leqslant N).$$

So we get

$$\max_{0 \leqslant i \leqslant N} |\theta_i(sv)| \leqslant c_5^D |\theta_0'(sv)|.$$

On the other hand, the lower bound of Lemma 9 shows that the left-hand side of the above exceeds $\exp(-c_{12}(1+|sv|^2))$. From (12) we see that

$$|sv| \leqslant S|v| \leqslant c_1 S B^{-1/(2g)},$$

and now the inequality of the lemma follows on appealing to (9).

Lemma 14: *For all $(s_1,\ldots,s_t)$ in $\mathbb{Z}^t(S)$ we have*

$$|f(s_1,\ldots,s_t)| \leqslant \exp(-c_{13}S_0).$$

Proof: We write

$$\Theta(z_1,\ldots,z_t) = \big(\theta_0'(z_1v)\big)^L \ldots \big(\theta_0'(z_tv)\big)^L,$$

so that

$$F(z_1,\ldots,z_t) = \Theta(z_1,\ldots,z_t) f(z_1,\ldots,z_t)$$

is an entire function on $\mathbb{C}^t$. Since F vanishes on $\mathbb{Z}^t(S_0)$, Lemma 10 shows that

$$M(F, S) \leqslant 2^{-S_0/t} M(F, 5S). \tag{15}$$

Now the upper bound of Lemma 9 together with (12) gives

$$M(F, 5S) \leqslant D^{c_{14}L} \exp\left(c_{15} L S^2 B^{-1/g}\right),$$

which by (9) does not exceed c_{16}^{LD}. Substituting this into (15) and using (8), we find that for any $(s_1, \ldots, s_t)$ in $\mathbb{Z}^t(S)$ we have

$$|F(s_1, \ldots, s_t)| \leqslant \exp(-c_{17} S_0).$$

Finally from Lemma 13 we deduce

$$|\Theta(s_1, \ldots, s_t)| \geqslant \exp(-c_{18} LD),$$

which leads immediately to the desired estimate for $|f(s_1, \ldots, s_t)|$, again using (8).

LEMMA 15: *For all* $(s_1, \ldots, s_t)$ *in* $\mathbb{Z}^t(S)$ *we have*

$$f(s_1, \ldots, s_t) = 0.$$

PROOF: Let $\xi = f(s_1, \ldots, s_t)$. From (14) and (3) we find easily that $H(\xi) \leqslant D^{c_{19}L}$. Hence if $\xi \neq 0$, we have

$$|\xi| \geqslant (H(\xi))^{-D} \geqslant D^{-c_{19}LD}.$$

Once more using (8), we see that this contradicts the upper bound of Lemma 14, and so the present lemma follows.

Now the definition of $f(z_1, \ldots, z_t)$ together with Lemma 5 for $n = g + 1$ shows that there exists a non-zero polynomial P^* of total degree at most L such that

$$P^*\left(s, f_1(sv), \ldots, f_g(sv)\right) = 0$$

for all integers s with $0 \leqslant s \leqslant S$. By (7), we have enough zeroes to be able to apply the Proposition. We deduce that $s_0 v$ is in the period lattice $\mathscr{L}$ for some integer s_0 with $1 \leqslant s_0 \leqslant c_{20} L^{2g+1}$. Hence, recalling the definition of v, we see that $P = \Theta(u)$ is a torsion point whose order is at most $s_0 b \leqslant c_{21} L^{2g+1} B$. By the second inequality of (11) this does not exceed D^{λ}. Thus we have completed the proof of the Theorem when A is a simple abelian variety.

5. Proof of the Theorem

We start by noting the following simple result. Let A, A_0 be abelian varieties defined over $\overline{\mathbb{Q}}$ and embedded in (possibly different) projective spaces, let q, q_0 be the quadratic parts of the corresponding Néron-Tate heights, and let d, d_0 be the corresponding degree functions.

Lemma 16: *Suppose $\varphi : A \to A_0$ is a morphism of projective group varieties. Then there is a constant c, depending only on A, A_0 and φ, such that*

$$q_0(\varphi(P)) \leqslant cq(P), \quad d_0(\varphi(P)) \leqslant cd(P)$$

for all P in $A(\overline{\mathbb{Q}})$.

Proof: Let H, H_0 denote the absolute Weil heights on A, A_0 respectively, and let $d \geqslant 1$ be an integer such that the morphism φ can be defined at each point by homogeneous polynomials of degrees at most d. It is easy to see (cf. (3)) that there exists a constant C, depending only on A, A_0 and φ, such that $H_0(\varphi(P)) \leqslant C(H(P))^d$ for all P in $A(\overline{\mathbb{Q}})$. Then the first inequality of the lemma follows with $c = d$ by taking logarithms, replacing P by mP, and making $m \to \infty$. The second inequality is obvious.

Now let A be an arbitrary abelian variety, of dimension $g \geqslant 1$, defined over $\overline{\mathbb{Q}}$. Let κ, λ be any real numbers satisfying

$$\kappa > 2g + 6 + 2g^{-1}, \quad \lambda > 6g. \tag{16}$$

We shall prove the Theorem for A with these values of κ, λ.

It is well-known that we can find $k \geqslant 1$ and simple abelian varieties $A_1, \ldots, A_k$, of dimensions $g_1 \geqslant 1, \ldots, g_k \geqslant 1$ and defined over $\overline{\mathbb{Q}}$, such that A is isogenous to $A' = A_1 \times \ldots \times A_k$. We suppose $A_1, \ldots, A_k$ embedded in suitable projective spaces so that the corresponding quadratic parts $q_1, \ldots, q_k$ of their Néron-Tate heights are well-defined. Let $\sigma : A \to A'$ be an isogeny defined over $\overline{\mathbb{Q}}$, and let $\pi_1, \ldots, \pi_k$ be the projections from A' to $A_1, \ldots, A_k$ respectively. Henceforth we use constants C, c_1, ... depending only on A, $A_1, \ldots, A_k$ and σ, as well as on the choice of κ, λ. Then by Lemma 16 applied to the map $\varphi_i : A \to A_i$ given by $\varphi_i(P) = \pi_i(\sigma(P))$ we deduce that

$$q_i(\varphi_i(P)) \leqslant c_1 q(P) \qquad (1 \leqslant i \leqslant k)$$

for all P in $A(\overline{\mathbb{Q}})$. Now let P be a point on $A(\overline{\mathbb{Q}})$ with $d(P) \leqslant D$ and $q(P) \leqslant C^{-1}D^{-\kappa}$ for some $D \geqslant 1$ and some sufficiently large constant C. By Lemma 16 the point $P_i = \varphi_i(P)$ on A_i has degree at most $D_i \leqslant c_2 D$ $(1 \leqslant i \leqslant k)$, and therefore we have

$$q_i(P_i) \leqslant c_3 C^{-1} D_i^{-\kappa} \qquad (1 \leqslant i \leqslant k).$$

As $\kappa > 2g_i + 6 + 2g_i^{-1}$ $(1 \leqslant i \leqslant k)$, we deduce from the special case of the Theorem already proved above that P_i is a torsion point on A_i of order at most T_i, where

$$T_i \leqslant c_4 D_i^{\lambda_i} \leqslant c_5 D^{\lambda_i} \qquad (1 \leqslant i \leqslant k),$$

and we choose

$$\lambda_i = g_i + 4 + g_i^{-1} + (\lambda - 6g)/k \qquad (1 \leqslant i \leqslant k).$$

Hence $\sigma(P)$ is a torsion point on A' of order at most

$$T_1 \dots T_k \leqslant c_6 D^{\lambda_1 + \cdots + \lambda_k}.$$

However, we have $\lambda_i \leqslant 6g_i + (\lambda - 6g)/k$ $(1 \leqslant i \leqslant k)$, and therefore

$$\lambda_1 + \cdots + \lambda_k \leqslant 6g + (\lambda - 6g) = \lambda.$$

So the order of $\sigma(P)$ is at most $c_6 D^{\lambda}$, and since σ has finite kernel, it follows that P itself has order at most CD^{λ}. This completes the proof of the Theorem.

We note that by using either of the sharper estimates for elliptic curves mentioned in the introduction the above argument allows $6g$ to be replaced by $13g/4$ in (16). For we can replace $g_i + 4 + g_i^{-1}$ by $13g_i/4$ if $g_i \geqslant 2$ and by 1 if $g_i = 1$ $(1 \leqslant i \leqslant k)$.

Finally we prove the Corollary. If P, Q are points on $A(\overline{\mathbb{Q}})$ with $TP = Q$ for some positive integer T, we have

$$q(P) = T^{-2} q(Q).$$

But if Q is non-torsion, so is P, whence

$$q(P) \geqslant C^{-1}(d(P))^{-\kappa},$$

which gives the first part. The second part is even easier; the order of P exceeds cT for some $c > 0$ depending only on Q; but on the other hand the order is at most $C(d(P))^{\lambda}$. This completes the proof of the Corollary.

References

[1] M. Anderson and D.W. Masser: Lower bounds for heights on elliptic curves. *Math. Zeit. 174* (1980) 23–34.

[2] A.O. Gelfond: *Transcendental and algebraic numbers*. New York: Dover (1960).

[3] E.R. Kolchin: Algebraic groups and algebraic dependence. *Amer. J. Math. 90* (1968) 1151–1164.

[4] S. Lang: Les formes bilinéaires de Néron et Tate. *Sém. Bourbaki,* 16^{e} année (1963/4), No. 274.

[5] M. LAURENT: Minoration de la hauteur de Néron-Tate, Thèse d'Etat, Université de Paris VI (1982).

[6] D.W. MASSER: Division fields of elliptic functions, *Bull. London Math. Soc. 9* (1977) 49–53.

[7] D.W. MASSER: Small values of the quadratic part of the Néron-Tate height, *Progress in Math. Vol. 12*. Boston, Basel, Stuttgart: Birkhäuser (1981) pp. 213–222.

[8] D.W. MASSER and G. WÜSTHOLZ: Fields of large transcendence degree generated by values of elliptic functions. *Invent Math. 72* (1983) 407–464.

[9] P. PHILIPPON: Indépendance algébrique de valeurs de fonctions exponentielles *p*-adiques. *J. reine angew. Math. 329* (1981) 42–51.

[10] A. SCHINZEL and H. ZASSENHAUS: A refinement of two theorems of Kronecker. *Michigan Math. J. 12* (1965) 81–85.

[11] J.-P. SERRE: Propriétés galoisiennes des points d'ordre fini des courbes elliptiques. *Invent. Math. 15* (1972) 259–331.

[12] J.-P. SERRE: Quelques applications du théorème de densité de Chebotarev. *Publ. Math. I.H.E.S. 54* (1981) 323–401.

[13] C.L. STEWART: Algebraic integers whose conjugates lie near the unit circle. *Bull. Soc. Math. France 106* (1978) 169–176.

[14] M. WALDSCHMIDT: Nombres transcendants et groupes algébriques. *Astérisque 69–70* (1979).

[15] D.W. MASSER and G. WÜSTHOLZ: Zero estimates on group varieties I. *Invent. Math. 64* (1981) 489–516.

[16] F.A. BOGOMOLOV: Sur l'algébricité des représentations *l*-adiques. *C.R. Acad. Sci. Paris 290A* (1980) 701–703.

(Oblatum 9-VIII-1982)

Department of Mathematics
University of Nottingham
University Park
Nottingham
UK