This forces $p < 318$. The only prime $p < 318$ satisfying $p = 1+b_8^4$ is $p = 17$, which again yields a contradiction. ■

References

[1] L. Baumert, *Cyclic difference sets*, Lecture Notes in Mathematics, 182, Springer-Verlag, Berlin 1971.

[2] B. Berndt and R. Evans, *Sums of Gauss, Jacobi, and Jacobsthal*, J. Number Theory (to appear in 1979).

[3] — — *Sums of Gauss, Eisenstein, Jacobi, Jacobsthal, and Brewer*, Illinois J. Math. 23 (1979), pp. 374–437.

[4] T. Storer, *Cyclotomy and difference sets*, Markham, Chicago 1967.

[5] A. Whiteman, *The cyclotomic numbers of order sixteen*, Trans. Amer. Math. Soc. 86 (1957), pp. 401–413.

Received on 30. 7. 1977
and in revised form on 23. 1. 1978 (967)

ACTA ARITHMETICA
XXXVIII (1980)

Linear forms on abelian varieties over local fields

by

DANIEL BERTRAND (Palaiseau) and YUVAL FLICKER (Cambridge)

0. Introduction. Let A be a simple abelian variety of dimension d, defined over a number field F. Denote by End A the ring of endomorphisms of A. Assume that *A admits sufficiently many complex multiplications in the sense that the algebra* End $A \otimes Q$ *is isomorphic to a totally imaginary quadratic extension K of a totally real field K_1, with $[K_1:Q] = d$.* For any field C, denote by A_C the set of C-rational points on the variety A. We shall study here linear forms in algebraic points of the (normalized) exponential map on A_C, when the field C is non-archimedean.

Lower bounds for linear forms in algebraic points of exponential maps are fundamental in the theory of diophantine approximations. Such studies were initiated by Baker, who obtained lower bounds for linear forms in (ordinary) logarithms by means of a new extrapolation technique (see, e.g. [1]). Masser [8] later showed that similar techniques can be applied so as to yield lower bounds in the case of an elliptic curve with complex multiplication. This corresponds to the case of an abelian variety A as above, with dimension $d = 1$. Masser's work was generalized by Masser [9] and Lang [7] to deal with arbitrary dimension d. A variant of the method, leading to sharper bounds, was then given by Coates and Lang [5], using a theorem of Ribet [11] on the degree of the division fields attached to rational points of A, and these bounds were subsequently improved by Masser [10].

Our object here is to establish a p-adic analogue of the main Masser–Coates–Lang theorem on linear forms in algebraic points on abelian varieties of complex multiplication type. In the elliptic case, such p-adic linear forms were studied by Bertrand [3]. An essential ingredient in the study of the higher dimensional case is a many variables p-adic version of the "Schwarz lemma" principle, which has recently been established by Robba [12]. However, Robba's result applies only for sufficiently well-distributed extrapolation sets. In order to check this hypothesis in our situation, we have been led to require (see § 6) that the *rational prime p splits completely in the totally real field K_1, and all primes of K_1 which lie above p have the same splitting type in K.* We assume this from now on. It is likely that our results hold in fact without any restriction on p and it would be of interest to remove this condition. Note, however, that in the elliptic case, that is, when the dimension d is equal to 1, we have $K_1 = Q$, whence the splitting assumption on p is always satisfied, and our results imply those of [3].

1. Statements of the theorem and transcendence results. Signify by $\mathfrak{p}$ a prime ideal of F which divides p. Denote by $F_\mathfrak{p}$ the completion of F at $\mathfrak{p}$, and by $|\ |_\mathfrak{p}$ (or, when there is no risk of confusion, by $|\ |$) the valuation on $F_\mathfrak{p}$, normalized by $|p|_\mathfrak{p} = p^{-1}$, as well as the corresponding sup norm on $F_\mathfrak{p}^d$. We assume, as we may without loss of generality, that F contains the field K together with all its conjugates. We define the product of two elements $\alpha = (\alpha_i)$ and $\beta = (\beta_i)$ in F^d by $\alpha\beta = (\alpha_i \beta_i)$. The normalized $\mathfrak{p}$-adic exponential map $\tilde{f}$ (whose definition we recall in § 2) maps a subgroup $\mathscr{F}_\mathfrak{p}$ of $F_\mathfrak{p}^d$ into $A_{F_\mathfrak{p}}$. By an *algebraic point* of $\tilde{f}$ we mean an element of $\mathscr{F}_\mathfrak{p}$ whose image under $\tilde{f}$ lies in $A_{\bar{Q}}$, where $\bar{Q}$ denotes the algebraic closure of Q in $F_\mathfrak{p}$. The analytic representation of End $A \otimes Q$ endows the set of algebraic points of $\tilde{f}$ with a structure of End A-module.

Let now $u_1, \ldots, u_n$ be algebraic points of $\tilde{f}$, linearly independent over End A, and denote by $\mathbf{1}$ the vector of $F_\mathfrak{p}^d$ whose coordinates are all equal to 1. Taking a finite extension of F if necessary we may assume that each component of $\tilde{f}(u_j)$ $(1 \leqslant j \leqslant n)$ belongs to F. Suppose further that the size (see below) of the points $\tilde{f}(u_j)$ are bounded by some $U \geqslant 3$. Put

$$\varkappa_1 = 5d\big(d(n+1)+2\big), \quad \varkappa_2 = (2d-1)\varkappa_1, \quad \varkappa_3 = d(n+1)\varkappa_1.$$

Our main result, which we prove in § 3–§ 8 (under the hypotheses on the abelian variety A and the prime $\mathfrak{p}$ specified in § 0) is the following

THEOREM. *There exists a positive constant C, effectively computable in terms of A, F and n only, such that for any vectors $\beta_0, \beta_1, \ldots, \beta_n$ in F^d, not all 0, with sizes bounded by some $B \geqslant 3$, we have*

$$|\beta_0 + \beta_1 u_1 + \ldots + \beta_n u_n|_\mathfrak{p} > \exp\{-C(\log B)^{\varkappa_1} p^{\varkappa_2} (\log U)^{\varkappa_3}\}.$$

Here the *size*, size (α), of an algebraic number α, is the maximum of $\|\alpha\|$ and den α, where $\|\alpha\|$ denotes the maximum of the archimedean absolute values of the conjugates of α, and den α denotes the least natural number for which $(\alpha \operatorname{den} \alpha)$ is an algebraic integer. By the size of a vector with algebraic coordinates we mean the maximum of the sizes of its coordinates.

The theorem implies, in particular, that the above points $\mathbf{1}, u_1, \ldots, u_n$ are linearly independent over F^d, and in fact over $\bar{Q}^d$, as can easily be seen by extending the number field F if necessary. More especially, for any j $(1 \leqslant j \leqslant d)$, a set of j th components of algebraic points linearly independent over End A, together with 1, is in fact linearly independent over $\bar{Q}$. Thus, we obtain:

COROLLARY 1. *Every coordinate of a non-zero algebraic point of $\tilde{f}$ is transcendental.*

[For general abelian varieties, it is known only (as in the complex case) that at least one of the coordinates of such a point is transcendental (see [2], Prop. 2).]

It will be noted that, unlike in the works mentioned above over the complex domain, we have computed the explicit dependence of our estimate on U (and p). This enables us (see § 2) to give an intrinsic geometric formulation of the theorem, and further applications concerning the greatest prime divisor of the denominator of a point on a CM-type curve; see also Bertrand [3] and Masser [9].

It can be checked that the arguments used in the course of the demonstration of the theorem apply also in the complex case, and they furnish an improvement on the result of Coates and Lang [5], who assumed that $\beta_0 = 0$ and at least one of $\beta_1, \ldots, \beta_n$ has no zero components. The latter condition was also assumed by Masser [10], though in this paper he obtained a stronger dependence on B. The corresponding sharpening in the p-adic case has recently been established by Flicker [6], who showed that, in the above estimate, the constant $\varkappa_1$ can then be chosen arbitrarily close to 1, independently of d and n.

2. Geometric corollaries. For the reader's convenience, we first recall some basic facts concerning the $\mathfrak{p}$-adic abelian functions, referring to [4] for a more complete exposition. The $\mathfrak{p}$-adic exponential map on $A_{F_\mathfrak{p}}$ is a local diffeomorphism defined on a subgroup $\mathscr{F}_\mathfrak{p}$ of the tangent space at the origin e of $A_{F_\mathfrak{p}}$, which we identify with $F_\mathfrak{p}^d$. We choose a coordinate system $z_1, \ldots, z_d$ on $F_\mathfrak{p}^d$ such that the analytic representation of End $A \otimes Q$ acts on $F_\mathfrak{p}^d$ in the following way (see [13], II):

$$\gamma z = (\gamma^{(1)} z_1, \ldots, \gamma^{(d)} z_d) \quad (\gamma \text{ in } K = \operatorname{End} A \otimes Q),$$

where $\gamma \to \gamma^{(i)}$ are certain extensions to K of the different embeddings of K_1 in $F_\mathfrak{p}$.

Let $\tilde{x} = (x_1, \ldots, x_{d'})$ be a set of affine coordinates on an open subset A_0 of A containing e, such that $\tilde{x}(e) = 0$. By definition, the normalized $\mathfrak{p}$-adic abelian functions $f_1, \ldots, f_{d'}$ are the components of the $\mathfrak{p}$-adic exponential map in the coordinate systems described above. We put $\tilde{f} = (f_1, \ldots, f_{d'})$. The normalization of $F_\mathfrak{p}^d$ implies that the ring $F[\tilde{f}]$ is mapped into itself by the partial derivations $\partial/\partial z_j$ $(1 \leqslant j \leqslant d)$. It follows from this property (see [4], Prop. 3) that, after performing a suitable homothety on the coordinates, the derivatives of all orders of the f_i's at 0 are $\mathfrak{p}$-adic integers. Choosing a set $\tilde{x}$ such that $f_1, \ldots, f_{d'}$ are integral over $F[f_1, \ldots, f_d]$, we further have that the map $f = (f_1, \ldots, f_d)$ is an isometry on $\mathscr{F}_\mathfrak{p}$, where

$$\mathscr{F}_\mathfrak{p} = \{z \in F_\mathfrak{p}^d,\ |z| < p^{-1/(p-1)}\}.$$

In order to state the geometric corollaries announced in § 1, we now introduce two functions on the set of F-rational points P of A_0: the $\mathfrak{p}$-adic distance between e and P:

$$d_\mathfrak{p}(e, P) = \max_{1 \leq i \leq d'} |x_i(P)|$$

and the (absolute) height of P:

$$h(P) = \prod_v \max\left(1, |x_1(P)|_v, \ldots, |x_{d'}(P)|_v\right)^{\delta_v/\delta}$$

where the product is taken over all places v of F, δ_v denotes the local degree of F at v, and δ the degree of F over Q.

The height function has a canonical extension to the group A_Q which will also be denoted by h. In order to simplify some computations in the course of the proof of the theorem, we further choose a system of affine coordinates $\bar{x}$ such that the function h satisfies the Néron–Tate theorem in the following form:

LEMMA 1. *The function* $P \mapsto \log h(P)$ *on* A_Q *is equal to the sum of a positive definite quadratic form and a bounded function.*

Proof. See, e.g., [7], § 7; the absence of linear terms in $\log h(P)$ is due to the choice of $\bar{x}$. The uniformity of the bounded function on the set A_Q has been proved by Lang.

In the proof of the theorem we shall also use the following related multiplication formula.

LEMMA 2. *For any* γ *in* End A *with* $\|\gamma\| \leqslant h$ *there are polynomials* $\Phi_{i\gamma}$ *and* $\Psi_{i\gamma}$ *with degrees* $\ll h^2$, *and with coefficients in* F *whose sizes are at most* $\exp(c_0 h^2)$, *such that*

$$f_i(\gamma z) = \Phi_{i\gamma}(\bar{f}(z))/\Psi_{i\gamma}(f(z)) \quad (1 \leqslant i \leqslant d').$$

These polynomials can be chosen so that $\Psi_{i\gamma}(f(u)) \neq 0$ $(1 \leqslant i \leqslant d')$ *for* $u = u_1, \ldots, u_n$.

Here and in the sequel the constants $c_0, c_1, \ldots,$ as well as the constants implied by $\ll$, depend on A, F and n alone.

Proof. See [7], Lemma 7.2, and the "safe" multiplication formula (Lemma 1) of [10]. Note that this implies that the degree of the extension of F which is generated by a q-division point is $\ll q^{2d}$.

Using the Mordell–Weil theorem, we can now give an intrinsic formulation of the theorem:

COROLLARY 2. *There exists a positive constant* C', *effectively computable in terms of a basis of the Mordell–Weil group* A_F, *such that for any point* $P \neq e$ *on* A_F *we have*:

$$d_\mathfrak{p}(e, P) > \exp\left(-C' p^{\varkappa_4}(\log\log H(P))^{\varkappa_1}\right),$$

where $\varkappa_4 = \varkappa_2 + 2\delta d \varkappa_3$.

Proof. The procedure developed in [3] can easily be generalized to the higher dimensional case, noticing that, in view of the Taylor expansions of the $\mathfrak{p}$-adic abelian functions, the set $\mathscr{F}_\mathfrak{p}$ is mapped by $\bar{f}$ onto a subgroup of $A_{F_\mathfrak{p}}$ whose index $\mu_\mathfrak{p}$ is bounded by $c_1 p^{\varrho d}$. Hence, if $P_1, \ldots, P_r$ represent a set of generators of the group A_F modulo torsion, and P belongs to A_F, the point $\mu_\mathfrak{p} P$ can be expressed as a linear combination of the points $\mu_\mathfrak{p} P_1, \ldots, \mu_\mathfrak{p} P_r$, which all lie in $\bar{f}(\mathscr{F}_\mathfrak{p})$. Using the isometry property of the map $(f_1, \ldots, f_d)$ and the quadraticity of the height, we can then pull back the lower bound of the theorem on the abelian variety to conclude; (for a more detailed discussion, see [4], § 2.2).

The next corollary to the theorem concerns CM-type curves (see [9], § 5). In order to make the discussion shorter, we shall consider only plane curves Γ. We assume that there exists a non-constant rational map $\varphi: \Gamma \to A$, where A is a simple abelian variety of CM-type, and also that Γ, φ and A are defined over F. Consider an affine model $\Gamma_0 = \{\psi(x, y) = 0\}$ of Γ. For any F-rational point R on Γ_0 we denote by $H(R)$ the height of $x(R)$, and by $P(R)$ the greatest prime factor of the denominator of $x(R)$. Then the following corollary holds.

COROLLARY 3. *There exist (ineffective) positive constants* $C'' = C''(\Gamma)$ *and* $\varkappa = \varkappa(\varkappa_4)$, *such that for any* F-*rational point* R *of* Γ_0, *which is integral outside the set* Π *of primes for which the theorem holds, we have*

$$P(R) > C''(\log H(R))^{\varkappa}.$$

Proof. According to [4], § 2.3, there exists a set $\{\gamma_\mathfrak{p}; \mathfrak{p} \in \Pi\}$ of real numbers depending only on Γ and $\mathfrak{p}$, and equal to 1 for all but a finite number of primes $\mathfrak{p}$, such that, for any point R on Γ_0 we have

$$\max(1, |x(R)|_\mathfrak{p}) \leqslant \gamma_\mathfrak{p} \max\Big(1, \max_{i=1,\ldots,g}\big(d_\mathfrak{p}(e_i, \varphi(R))^{-\nu_i}\big)\Big),$$

where $e_1, \ldots, e_g$ denote the images under φ of the points at infinity on Γ, and $-\nu_i$ the order of x at $\varphi^{-1}(e_i)$. Thus, Corollary 1, applied to the abelian variety A, together with the archimedean result of [5], implies (see [9], § 5 and [4], § 3.3):

$$H(R) \leqslant C_1'' \exp\Big(C_2''(\log\log h(\varphi(R))^{\varkappa_1} \sum_p p^{\varkappa_4})\Big)$$

where the sum is over all primes p not exceeding $P(R)$ which are divisible by some $\mathfrak{p}$ in Π. Since Γ is a curve, the height functions attached to the maps x and φ on Γ are multiplicatively equivalent. Therefore:

$$H(R) \leqslant \exp\big(C_3''(\log\log H(R))^{\varkappa_1}(P(R))^{\varkappa_4+1}\big)$$

and the corollary follows.

As an illustration of the above results we consider the hyperelliptic curve $ay^2+bx^l+c = 0$, where a, b and c are rational integers, and l is an odd prime number. Such a curve is a CM-type curve, since its jacobian is a simple abelian variety of CM-type, in fact with a CM-field $K = Q(\zeta_l)$, where ζ_l denotes some non-trivial lth root of unity. The theorem applies to prime numbers p of the form:

(i) $p = \mu l+1$,

(ii) $p = \mu l-1$,

where μ runs through the rational integers. Indeed we recall that the field K is galois over Q, the primes p of the form (i) are those which split completely in K, and the primes p of the form (ii) are those that split completely in its totally real subfield $K_1 = Q(\zeta_l+\zeta_l^{-1})$. Finally, using the map described in [9], p. 564, we can further deduce that if x, y, and z are positive integers satisfying Fermat's equation $x^l+y^l = z^l$, and if z is composed of primes p of the form (i) or (ii) only, then

$$P(z) > C''(\log z)^{\varkappa}.$$

3. Proof of the theorem. We shall now proceed to prove the theorem. For any natural number n and real numbers $B, U \geqslant 3$, we put

$$h = (\log B)\left(p^{2d-1}(\log U)^d\right)^{n+1},$$

and

$$\Omega = h^{\varkappa_1}, \quad L = h^{5d-1/n},$$

where as above $\varkappa_1 = 5d\left(d(n+1)+2\right)$. Let $u_1, \ldots, u_n$ be algebraic points of $\bar{f} = (f_1, \ldots, f_{d'})$, linearly independent over End A, with size $(f_i(u_j)) \leqslant U$ $(1 \leqslant i \leqslant d', 1 \leqslant j \leqslant n)$. Assume that $\beta_0, \beta_1, \ldots, \beta_n$ are vectors in F^d, not all 0, whose sizes are bounded by B. If P belongs to A_0, we denote by $x(P)$ the set of its first d coordinates. By the choice of $x_1, \ldots, x_d$ described in § 1, $x(P)$ form a set of d independent variables.

LEMMA 3. *There is a positive constant B_0, effectively computable in terms of A, F and n, such that if*

$$|\beta_0+\beta_1 u_1+\ldots+\beta_n u_n| < \exp(-\Omega)$$

for some $B \geqslant B_0$, then there exists a non-zero polynomial P with integer coefficients in F, and with degree at most L in each of its dn variables $x_{i,j}$ $(1 \leqslant i \leqslant d, 1 \leqslant j \leqslant n)$ such that:

$$P[x(\gamma P_1/q), \ldots, x(\gamma P_n/q)] = 0; \tag{1}$$

here q is a prime larger than $L^{1/2}$, γ is an element of End A *with $(\gamma, q) = 1$ and P_i/q denotes the image of u_i/q on A (under $\bar{f}$).*

We shall prove Lemma 3 in § 4–§ 8.

LEMMA 4. *Let $P_1, \ldots, P_n$ be points of A_F, linearly independent over* End A. *For every prime q, $q > c_2(\log U)^{dn}$, the galois group*

$$\mathrm{Gal}\,[F(A_q, P_1/q, \ldots, P_n/q)/F(A_q)]$$

is isomorphic to the group of translations by A_q^n, where A_q denotes the group of q-torsion points of A.

Note that the multiplication by γ in End A with $(\gamma, q) = 1$, gives an automorphism of A_q; hence the result of Lemma 5 remains valid on substituting P_i/q by $\gamma P_i/q$ $(1 \leqslant i \leqslant n)$ (see [2], Remark 6).

Proof. This is established in [11] for all "sufficiently large" primes q. The dependence of q on $\log U$ can be calculated similarly to [3], Prop. 4. The Néron–Tate theorem holds for abelian varieties as well, and the change from the elliptic to the abelian case is that now we approximate simultaneously $2nd$ real numbers by rationals, whose denominators are bounded by q.

LEMMA 5. *Let P be an element of $F[x_{i,j}; 1 \leqslant i \leqslant d; 1 \leqslant j \leqslant n]$, such that* (1) *holds for a prime $q > L^{1/2}$. Then $P \equiv 0$.*

Proof. Since $\bar{f}$ is an isomorphism of End A-modules on $\mathscr{F}_p$, and $u_1, \ldots, u_n$ are linearly independent over End A, the same is true of the points $P_1, \ldots, P_n$. In view of the relation $q > L^{1/2} > c_2(\log U)^{dn}$, (1) and Lemma 4 then imply that, for any q-torsion point Q we have

$$P\left(\ldots, x\left(\gamma(P_j/q)+Q\right), \ldots\right) = 0.$$

The complex abelian functions $f_C = (f_{1,C}, \ldots, f_{d,C})$ giving an analytic isomorphism between a complex torus and A_C, we infer that the points $\left\{\left(x_i\left(\gamma(P_j/q)+Q\right)\right)_{1 \leqslant i \leqslant d;\, 1 \leqslant j \leqslant n};\ Q \in A_q\right\}$ come within a (complex) distance $\ll 1/q$ of each point of some ball of radius c_3 centered at 0 in C^{nd} (see [5]). By Masser's theorem ([8], p. 127), it now follows that the polynomial P vanishes identically. (It would be of interest to deduce this lemma from a p-adic version of Masser's theorem.)

Finally we note that Lemma 5 contradicts the assumption of Lemma 3, and this concludes the proof of the theorem.

4. The auxiliary function. In the sequel we shall construct an auxiliary function which will turn out (under certain modifications) to be the polynomial whose existence is asserted in Lemma 3.

Let $B_0 = B_0(A, F, n)$ be a positive constant such that for all $B \geqslant B_0$ the estimates below are valid. Assume $\beta_1, \ldots, \beta_n$ are vectors in F^d, not all 0, and let β be an element of F, such that the size of each β, $\beta_1, \ldots, \beta_n$ is bounded by some B, $B \geqslant B_0$; without loss of generality we may further assume that $\beta, \beta_1, \ldots, \beta_n$ are integral. For any vector $z = (z_1, \ldots, z_d)$ we define the function e_r $(1 \leqslant r \leqslant d)$ by $e_r(z) = z_r$ (projection on the rth coordinate).

Since not all $\beta_1, \ldots, \beta_n$ are 0, we may assume that β_n is not zero, hence there is some r $(1 \leqslant r \leqslant d)$ for which $e_r(\beta_n) \neq 0$. We assume that

$$|e_r(\beta_1 u_1 + \ldots + \beta_n u_n) - \beta|_p < \exp(-\Omega); \tag{2}$$

our aim is to deduce from this assumption the existence of a polynomial satisfying the conditions of Lemma 3.

Let $\{z_j = (z_{ij};\ 1 \leqslant i \leqslant d;\ 1 \leqslant j \leqslant n)\}$ be a set of n independent d-vectors. We consider an auxiliary function of the form:

$$\Phi(z_1, \ldots, z_n) = \sum_{\lambda_0, (\lambda_{ij})} a(\lambda_0, (\lambda_{ij}))\, e_r(\beta_1 z_1 + \ldots + \beta_n z_n)^{\lambda_0} \prod_{ij} f_i(z_j)^{\lambda_{ij}},$$

where the sum is taken over all integral $(dn+1)$-tuples $(\lambda_0, (\lambda_{ij}))$, with $0 \leqslant \lambda_0 < L$ and $0 \leqslant \lambda_{ij} < L$ $(1 \leqslant i \leqslant d,\ 1 \leqslant j \leqslant n)$. The coefficients $a(\lambda_0, (\lambda_{ij}))$ are integers, shortly to be determined.

For any dn-tuple $(m) = (m_{ij})$, of length $|m| = \sum m_{ij}$, we write $D^{(m)} = \prod_{ij} (\partial/\partial z_{ij})^{m_{ij}}$. We then have:

$$D^{(m)} \Phi(z_1, \ldots, z_n) = \sum_{\lambda_0=0}^{L-1} \sum_{(\mu)} D^{(m-\mu)} \big(e_r(\beta_1 z_1 + \ldots + \beta_n z_n)\big)^{\lambda_0} D^{(\mu)} \Psi_{\lambda_0}(z_1, \ldots, z_n),$$

where the second summation is taken over all dn-tuples (μ) which are (componentwise) $\leqslant (m)$, and where we have set:

$$\Psi_{\lambda_0}(z_1, \ldots, z_n) = \sum_{(\lambda_{ij})} a(\lambda_0, (\lambda_{ij})) \prod_{ij} f_i(z_j)^{\lambda_{ij}}.$$

We finally introduce a new variable z_0 in F_p, independent of $\{z_{ij}\}$. We put:

$$D^{(m)} \Phi(z_1, \ldots, z_n; z_0) = \sum_{\lambda_0=0}^{L-1} \sum_{(\mu)} (D^{(m-\mu)} e_r^{\lambda_0})_{z_0} D^{(\mu)} \Psi_{\lambda_0}(z_1, \ldots, z_n),$$

where $(D^{(m-\mu)} e_r^{\lambda_0})_{z_0}$ denotes the value of $D^{(m-\mu)} e_r(\beta_1 z_1 + \ldots + \beta_n z_n)^{\lambda_0}$ on the set defined by: $e_r(\beta_1 z_1 + \ldots + \beta_n z_n) = z_0$.

LEMMA 6. *There exist integers $a(\lambda_0, (\lambda_{ij}))$ in F, not all 0, with*

$$\operatorname{size}\big(a(\lambda_0, (\lambda_{ij}))\big) \leqslant \exp(c_4 L h^2 \log U),$$

such that for any γ in End A *with $\|\gamma\| \leqslant h$, and any dn-tuple (m) with $|m| < k = h^{5d}$, we have*

$$D^{(m)} \Phi(\gamma u_1, \ldots, \gamma u_n;\ \beta\gamma^{(r)}) = 0.$$

Proof. The conditions of the lemma give a system of $\leqslant h^{2d} k^{nd} = h^{2d+5nd^2}$ linear equations in $L^{1+nd} \geqslant h^{5nd^2+3d}$ unknowns $a(\lambda_0, (\lambda_{ij}))$. The coefficients are elements of F whose size can be bounded as follows. By virtue of Lemma 2, each of the numbers $f_i(\gamma u_j)$, with γ as in the lemma, has a size bounded by $\exp(c_5 h^2 \log U)$. Since the ring of p-adic abelian functions is mapped into itself by partial differentiations, Lemma 5.1 of [7] implies that each function $((\partial/\partial z_{lj})^{\mu} f_i^{\lambda})(z_j)$ is a polynomial with degree $\leqslant k+L$ in $f_1(z_j), \ldots, f_{d'}(z_j)$, whose coefficients have sizes bounded by $k!\, c_6^{k+L}$. Hence the coefficients in the system above have sizes bounded by

$$L!\,(2B)^L \exp\big(c_7 h^2 (\log U)(k+L)\big) \leqslant \exp(c_8 k h^2 \log U).$$

The lemma now follows from Siegel's lemma, noting that the Dirichlet exponent is $\leqslant h^{-1}$, and that $kh \leqslant Lh^2$.

5. The extrapolation assertion. The main step in the proof of Lemma 3 is to establish the following lemma, by means of Baker's extrapolation techniques. Let $\delta > 0$ be a number such that $\delta < 1/(5dn(n+1))$, and put $G = \delta^{-1}(n+1)d$.

LEMMA 7. *For any integer g $(0 \leqslant g \leqslant G)$, for any γ in* End A *with $\|\gamma\| \leqslant h_g = hk^{g\delta/2}$, and any dn-tuple (m) with $|m| \leqslant k_g = k/2^g$, we have*

$$D^{(m)} \Phi(\gamma u_1, \ldots, \gamma u_n;\ \beta\gamma^{(r)}) = 0.$$

Proof. We prove the lemma by induction on g. For $g = 0$ the assertion is just a property of Φ by construction. Assuming the assertion holds up to g, we shall prove it for $g+1$ in the given range.

If the assertion is false for $g+1$, let (m') be a dn-tuple with minimal length $|m'| \leqslant k_{g+1}$, for which there exists γ' in End A with $\|\gamma'\| \leqslant h_{g+1}$, and

$$\xi = D^{(m')} \Phi(\gamma' u_1, \ldots, \gamma' u_n;\ \beta\gamma'^{(r)}) \neq 0.$$

We shall derive a contradiction from the assumption $\xi \neq 0$ by comparing a lower and an upper bound for the p-adic valuation of ξ.

LEMMA 8. *Under the induction hypothesis*

$$|\xi| \geqslant \exp(-c_9 h_{g+1}^2 L \log U).$$

Proof. The proof of Lemma 13 of [10] can easily be modified to compute the dependence on U, and to yield

$$\operatorname{size}(\xi) \leqslant \exp(c_{10} h_{g+1}^2 L \log U).$$

The lemma follows at once from the product formula on the field F.

We shall now start the estimation of $|\xi|$ from above.

LEMMA 9. *The assumption* (2) *implies that*

$$|D^{(m)} \Phi(\gamma u_1, \ldots, \gamma u_n;\ \beta\gamma^{(r)}) - D^{(m)} \Phi(\gamma u_1, \ldots, \gamma u_n)| < \exp(-\Omega),$$

for any γ and (m) specified in Lemma 7.

Proof. Since the derivatives of all orders of the abelian functions at 0 are $\mathfrak{p}$-adic integers, Cauchy's inequalities imply that the above difference is bounded by

$$|\beta\gamma^{(r)}-e_r(\beta_1\gamma u_1+\ldots+\beta_n\gamma u_n)|.$$

Hence, Lemma 9 follows from (2) and the integrality of γ.

Let us introduce the function

$$f(z) = D^{(m')}\Phi(zu_1, \ldots, zu_n),$$

where $z = (z_1, \ldots, z_d)$ is the set of d independent variables.

LEMMA 10. *For any d-tuple (t) with $|t| \leqslant k_{g+1}$, and any γ in* End A *with $\|\gamma\| \leqslant h_g$, we have*

$$|D^{(t)}f(\gamma)| \leqslant \exp(-\Omega).$$

Proof. We note that for any $(t) = (t_i)$ as in the lemma, the function $D^{(t)}f(z)$ is equal to

$$\sum_{(s)} b(s, u)D^{(m'+s)}\Phi(zu_1, \ldots, zu_n),$$

where the sum is taken over all dn-tuples $(s) = (s_{ij})$ of non-negative integers s_{ij} with $\sum_j s_{ij} = t_i$, and $b(s, u)$ are polynomials in $e_i(u_j)$ with binomial coefficients. Hence $|b(s, u)| \leqslant 1$. But since

$$|m'+s| \leqslant k_{g+1}+|t| \leqslant k_g,$$

the induction hypothesis (on g) implies that

$$D^{(m'+s)}\Phi(\gamma u_1, \ldots, \gamma u_n; \beta\gamma^{(r)}) = 0$$

for all γ in the required range. The lemma now follows from Lemma 9.

6. The *p*-adic Schwarz lemma. Let C be a finite extension of $\boldsymbol{Q}_p$ which is contained in $F_{\mathfrak{p}}$. Assume that its residue class degree is f and its ramification index is e, so that the cardinality of the residue field of C is $q = p^f$, and its valuation group $|C^\times|$ is generated by $\lambda = p^{1/e}$. Let $C_1, \ldots, C_d$ be such fields with equal parameters e and f. The valuation $|\ |$ on $C_1\times\ldots\times C_d$ is defined to be the restriction of the valuation on $F_{\mathfrak{p}}^d$. Assume Γ is a set of ν elements in

$$B(0, \varrho) = \{z \text{ in } C_1\times\ldots\times C_d, |z| \leqslant \varrho\}$$

where ϱ is a positive number. We put

$$\theta = \min\{|\gamma_1-\gamma_2|, \gamma_1 \neq \gamma_2 \text{ in } \Gamma\}$$

and define the natural number φ by $\varrho/\theta = \lambda^{\varphi-1}$.

Let R be a positive number, and $f(z) = \sum_{(\mu)\geqslant(0)} a_{(\mu)}z^{(\mu)}$ be a function of d variables, analytic on $B(0, R)$, i.e. such that the expression

$$|f|_0(R) = \sup_{(\mu)}(|a_{(\mu)}|R^{|\mu|})$$

is finite. If $\varrho \leqslant R$, we have: $|f|_0(\varrho) \leqslant |f|_0(R)$. The next lemma, which improves this inequality, plays a fundamental role in the extrapolation procedure. It has recently been established by Robba, after previous work of Serre.

LEMMA 11. *If f is analytic on $B(0, R)$ and Γ is a set as above in $B(0, \varrho)$, such that*

$$0 < \varrho < R \quad \textit{and} \quad \theta < p^{-1/(p-1)},$$

then for any natural number T we have

$$|f|_0(\varrho) \leqslant \max\Big[(\varrho/R)^N|f|_0(R), (\varrho/\theta)^{N-1}\max_{\substack{|t|<T\\ \gamma \text{ in } \Gamma}}|D^{(t)}f(\gamma)|\Big],$$

where

$$N = \nu T/q^{\varphi(d-1)}.$$

Proof. See [12], Theorem 2.2 and Lemma 1.4. Note that, by the definition of φ, we have

$$q^\varphi = p^f\lambda^{ef(\varphi-1)} = p^f\left(\frac{\theta}{\varrho}\right)^{-ef},$$

hence:

$$N = c\nu T\left(\frac{\theta}{\varrho}\right)^{-\omega(d-1)}$$

where $c = p^{f(d-1)}$ depends only on C and d, and ω denotes the degree ef of C over $\boldsymbol{Q}_p$. It should be emphasised that, although the proofs are very different in nature, the complex analogue of Lemma 11 provides a similar formula, with $\omega = [C:\boldsymbol{R}] = 2$ (see [7])!

Denote by $K^{(i)}$ $(1 \leqslant i \leqslant d)$ the d conjugates of the field K under the embeddings specified in § 1, by $K_{\mathfrak{p}}^{(i)}$ the completion of $K^{(i)}$ in $F_{\mathfrak{p}}$, and put $C_i = K_{\mathfrak{p}}^{(i)}$. The hypothesis that p splits completely in the maximal totally real subfield K_1 of K, and all primes above p have the same splitting type, implies that all C_i have equal parameters e and f with either $ef = 1$ or $ef = 2$. From now on, we shall view End A as a subring of $F_{\mathfrak{p}}^d$ by means of the map: $\gamma \mapsto (\gamma^{(1)}, \ldots, \gamma^{(d)})$. We shall apply Lemma 11 to the function f defined prior to Lemma 10, and to the set Γ of γ's in End A such that $\|\gamma\| < h_g$. The cardinality ν of Γ is thus $\gg h_g^{2d}$, and we take $\varrho = 1$, since End A consists of K-integers.

Lemma 12. *With the notations of Lemma* 11, *if* $T = k$, *then*

$$h_g^2 k \gg N \gg p^{2-2d} h_g^2 k.$$

Proof. By the formula for N given above, it suffices to estimate θ^{-ef}. Let γ_1 and γ_2 be two elements of Γ, such that $\theta = |\gamma_1 - \gamma_2|$ and put $\gamma_0 = \gamma_1 - \gamma_2$. For any element γ of K, we write

$$\mathcal{N}(\gamma) = \prod_{i=1}^{d} \gamma^{(i)}.$$

In view of the CM structure of the field K, the norm of γ satisfies:

$$N_{K/Q}(\gamma) = \mathcal{N}(\gamma).\mathcal{N}(\bar{\gamma})$$

where the bar denotes complex conjugation (see [13], § II).

We first note that, without any assumption on the decomposition of p in K, we have:

$$h_g^{-2} \ll \theta \ll p h_g^{-1}.$$

Indeed:

$$\theta^{-d} = \max_{i=1,\dots,d} |\gamma_0^{(i)}|^{-d} \leqslant |\mathcal{N}(\gamma_0)|^{-1} \leqslant |N_{K/Q}(\gamma_0)|^{-1} \ll h_g^{2d}$$

(the second inequality follows from the integrality of γ_0, hence of $\mathcal{N}(\bar{\gamma}_0)$, while the third one is an obvious consequence of the product formula applied to the rational integer $N_{K/Q}(\gamma_0)$). On the other hand, if p^a denotes the largest power of p smaller than h_g, p^a belongs to Γ, hence $\theta \ll p h_g^{-1}$.

These inequalities can be refined under the hypothesis on p described above. We distinguish between two cases.

(i) Assume $ef = 1$. Then, each field $K^{(i)}$ is embedded in $\boldsymbol{Q}_p$. If p^b denotes the largest power of p smaller than h_g^2, there are $\ll h_g^{2d} \ll \nu$ congruence classes in $(\mathbf{Z}_p/p^b \mathbf{Z}_p)^d$, hence $\theta \ll p h_g^{-2}$.

(ii) Assume $ef = 2$. In this case, we claim that, for any element γ in K $|\gamma| = |\bar{\gamma}|$. This is trivial if γ belongs to K_1. Otherwise, $\gamma^{(i)}$ generates $K^{(i)}$ over $K_1^{(i)}$ $(i = 1, \dots, d)$. Since $K^{(i)}$ is quadratic over the completion $\boldsymbol{Q}_p$ of $K_1^{(i)}$ in F (by the assumption on p), $\bar{\gamma}^{(i)}$ is the conjugate of $\gamma^{(i)}$ over $\boldsymbol{Q}_p$, and the desired equality always holds. Hence,

$$\theta = \max_{1 \leqslant i \leqslant d} |\gamma_0^{(i)}| = \max_{1 \leqslant i \leqslant d} |\bar{\gamma}_0^{(i)}|,$$

and

$$\theta^{-2d} \leqslant |\mathcal{N}(\gamma_0)|^{-1} |\mathcal{N}(\bar{\gamma}_0)|^{-1} \leqslant |N_{K/Q}(\gamma_0)|^{-1} \ll h_g^{2d},$$

so that $\theta \gg h_g^{-1}$.

7. Proof of Lemma 7. Since, for $j = 1, \dots, n$, the point u_j belongs to the locally compact field $F_\mathfrak{p}$ and its $\mathfrak{p}$-adic valuation is $< p^{-1/(p-1)}$, there exists a constant c_{11} depending only on the ramification index of p at $\mathfrak{p}$, such that $|u_j| \leqslant R^{-1} p^{-1/(p-1)}$, where $R = p^{1/(c_{11} p)}$. Therefore, the function $f(z) = D^{(m')} \Phi(zu_1, \dots, zu_n)$ is analytic on $B(0, R)$, and the $\mathfrak{p}$-adic behaviour of the Taylor expansions of the abelian functions at 0 implies that $|f|_0(R) = 1$. Hence Lemma 11, and the computations of Lemma 12, imply that

$$|f|_0(1) \leqslant \max\left[\exp(-c_{12} p^{1-2d} h_g^2 k),\ h^{c_{13} h_g^2 k}(\exp(-\Omega))\right]$$

whence, by the definition of Ω and since $G \geqslant g$,

$$|f|_0(1) \leqslant \exp(-c_{12} p^{1-2d} h_g^2 k). \tag{3}$$

By Lemma 9, the same upper bound holds for $|\xi|$. Comparing this estimate with the lower bound provided by Lemma 8, we deduce:

$$p^{1-2d} h_g^2 k \ll L h_{g+1}^2 \log U,$$

thus

$$h^{1/(n+1)} \leqslant h^{(1/n)-5d} \ll p^{2p-1} \log U.$$

For B_0 sufficiently large, this contradicts the definition of $\boldsymbol{h}$, and Lemma 7 is established.

Remark. It can be proved that, after performing a slight modification, the set Γ of extrapolation points considered in Lemma 11 is well-distributed in the sense of [12]. Moreover, the point γ' specified in § 5 belongs to the locally compact space $C_1 \times \dots \times C_d$. Consequently, inequality (2.3.2) of [12] can be used to bound $|f(\gamma')|$, and this yields a sharper estimate for G. The application of this remark to the lower bound of the theorem is discussed in [6].

8. Proof of Lemma 3. Let q be the smallest prime $> L^{1/2}$; thus $q \neq p$, and $q \leqslant 2L^{1/2}$.

Lemma 13. *For any* γ *in* End A *with* $\|\gamma\| \leqslant c_{19} L^{1/2}$, *and any* (m) *with* $|m| \leqslant L$, *we have*

$$D^{(m)} \Phi((\gamma/q) u_1, \dots, (\gamma/q) u_n;\ \beta\gamma^{(r)}/q) = 0.$$

Proof. Let (m) be a dn-tuple with minimal length for which there exists a γ as in the lemma, such that $|m| \leqslant L$ and

$$\eta = D^{(m)} \Phi((\gamma/q) u_1, \dots, (\gamma/q) u_n;\ \beta\gamma^{(r)}/q) \neq 0.$$

Lemma 2 implies that

$$h(f_i((\gamma/q) u_j)) \leqslant \exp(c_{14} \log U) \quad (1 \leqslant i \leqslant d,\ 1 \leqslant j \leqslant n).$$

From Lemma 3 we deduce that the division field generated by $f_i((\gamma/q) u_j)$ over F has degree $\ll q^{2d}$ over $\boldsymbol{Q}$. Thus the sizes of the points $f_i((\gamma/q) u_j)$ are bounded by $\exp(c_{15} q^{2d} \log U)$. Applying Lemma 5.1 of [7] to

$D^{(m)}\Phi(z_1, \ldots, z_n)$ (as explained in the proof of Lemma 6), together with the bound $|m| \leqslant L$ we deduce:

$$\operatorname{size}(\eta) \leqslant \exp\left(c_{16}(q^{2d}+h^2)\,L\log U\right).$$

But the non-zero number η is algebraic with degree $\leqslant q^{2dn}$, hence

$$|\eta| \geqslant \exp\left(-c_{17}\,L^{d(n+1)+1}\log U\right).$$

The methods of § 7 (see estimate (3)), applied to $f(z) = D^{(m)}\Phi(zu_1, \ldots, zu_n)$ and with $g = G$, together with Lemma 9, imply that

$$|\eta| \leqslant \exp\left(-c_{18}\,p^{1-2d}\,h_G^2\,k\right).$$

Since $G\delta = d(n+1)$, these last two estimates would imply

$$h \leqslant p^{2d-1}\log U.$$

This contradiction proves the lemma.

LEMMA 14. *Lemma 3 holds if $\beta \neq 0$.*

Proof. By virtue of Lemma 6 there is some dn-tuple (λ_{ij}^0) such that $P_{(\lambda_{ij}^0)}(z_0)$ is non-zero, where

$$P_{(\lambda_{ij})}(z_0) = \sum_{\lambda_0=0}^{L-1} a\left(\lambda_0, (\lambda_{ij})\right) z_0^{\lambda_0}.$$

It is easy to see that the cardinality of the set of γ's in End A with $\|\gamma\| \leqslant c_{19}\,L^{1/2}$ and $(\gamma, q) = 1$ exceeds $L^d \geqslant L$. Consequently, there exists an element γ in this set such that:

$$P_{(\lambda_{ij}^0)}(\beta\gamma^{(r)}/q) \neq 0.$$

By virtue of Lemma 13, Lemma 3 now holds with the polynomial

$$P(x_{ij};\ 1 \leqslant i \leqslant d;\ 1 \leqslant j \leqslant n) = \sum_{(\lambda_{ij})} P_{(\lambda_{ij})}(\beta\gamma^{(r)}/q) \prod_{ij} (x_{ij})^{\lambda_{ij}},$$

the prime $q > L^{1/2}$ and the element γ chosen above.

LEMMA 15. *Lemma 3 holds if $\beta = 0$.*

Proof. Let λ_0^0 be the minimal value of λ_0 for which there exists a dn-tuple (λ_{ij}) such that $a(\lambda_0^0, (\lambda_{ij})) \neq 0$. Let $(m) = (m_{ij})$ be the dn-tuple with $m_{rn} = \lambda_0^0$ and $m_{ij} = 0$ otherwise. Then

$$D^{(m)}\Phi(z_1, \ldots, z_n; z_0) = \sum_{\lambda_0=\lambda_0^0}^{L-1} \sum_{\mu=0}^{\lambda_0^0} \frac{\lambda_0!}{(\lambda_0-(\lambda_0^0-\mu))!}\, e_r(\beta_n)^{\lambda_0^0-\mu}\, z_0^{\lambda_0-(\lambda_0^0-\mu)} \times \\ \times (\partial/\partial z_{rn})^{\mu}\, \Psi_{\lambda_0}(z_1, \ldots, z_n).$$

Hence

$$D^{(m)}\Phi(z_1, \ldots, z_n; 0) = \lambda_0^0!\, e_r(\beta_n)^{\lambda_0^0}\, \Psi_{\lambda_0^0}(z_1, \ldots, z_n).$$

By assumption $e_r(\beta_n) \neq 0$; thus we put

$$P(x_{ij};\ 1 \leqslant i \leqslant d,\ 1 \leqslant j \leqslant n) = \sum_{(\lambda_{ij})} a(\lambda_0^0, (\lambda_{ij})) \prod_{ij} (x_{ij})^{\lambda_{ij}},$$

and by virtue of Lemma 13, Lemma 4 now holds with the polynomial P, $\gamma = 1$, and the prime $q > L^{1/2}$.

Finally, we note that Lemma 14 and Lemma 15 imply Lemma 3, and the proof of the theorem is complete.

References

[1] A. Baker, *The theory of linear forms in logarithms*, Transcendence Theory: Advances and Applications, Academic Press, 1977.

[2] D. Bertrand, *Sous-groupes à un paramètre p-adique de variétés de groupe*, Invent. Math. 40 (1977), pp. 171–193.

[3] — *Approximations diophantiennes p-adiques sur les courbes elliptiques ...*, Compositio Math., to appear.

[4] — *Fonctions abéliennes p-adiques: définitions et conjectures*, Gr. Tr. Analyse ultrametrique, Paris, 1976/77.

[5] J. Coates and S. Lang, *Diophantine approximation on abelian varieties with C. M.*, Invent. Math. 34 (1976), pp. 129–133.

[6] Y. Flicker, *Linear forms on abelian varieties of CM-type.*

[7] S. Lang, *Diophantine approximations on abelian varieties with C. M.*, Advances in Math. 17 (1975), pp. 281–336.

[8] D. Masser, *Elliptic functions and transcendence*, Springer Lecture Notes 437, 1975.

[9] — *Linear forms in algebraic points of Abelian functions, III*, Proc. London Math. Soc. 33 (1976), pp. 549–564.

[10] — *Diophantine approximations and lattices with complex multiplication*, Invent. Math.

[11] K. Ribet, *Dividing rational points on abelian varieties of CM-type*, Compositio Math. 33 (1976), pp. 69–74.

[12] P. Robba, *Lemme de Schwarz p-adique à plusieurs variables*, Gr. Tr. Analyse ultrametrique, C. R. Conf. Luminy, 1976, n° J9.

[13] G. Shimura and T. Taniyama, *Complex multiplications of abelian varieties*, Publ. Math. Soc. Japan, n° 6, 1961.

CENTRE DE MATHÉMATIQUES
ÉCOLE POLYTECHNIQUE
91128 Palaiseau Cedex, France
DEPARTMENT OF PURE MATHEMATICS AND MATHEMATICAL STATISTICS
16 Mill Lane, Cambridge CB2 1SB, England

Received on 12. 1. 1978 (1023)