

COMPOSITIO MATHEMATICA

ALICE SILVERBERG

Torsion points on abelian varieties of *CM*-type

Compositio Mathematica, tome 68, n° 3 (1988), p. 241-249

http://www.numdam.org/item?id=CM_1988__68_3_241_0

© Foundation Compositio Mathematica, 1988, tous droits réservés.

L'accès aux archives de la revue « Compositio Mathematica » (<http://www.compositio.nl/>) implique l'accord avec les conditions générales d'utilisation (<http://www.numdam.org/conditions>). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

NUMDAM

Article numérisé dans le cadre du programme
Numérisation de documents anciens mathématiques

<http://www.numdam.org/>

Torsion points on abelian varieties of CM-type

ALICE SILVERBERG*

Department of Mathematics, The Ohio State University, 231 W. 18 Avenue, Columbus, OH 43210, USA

Received 14 May 1987; accepted 19 November 1987

1. Introduction

Given an abelian variety A of dimension d of CM-type defined over a number field k , and a point t of A of order N , let D be the number of conjugates of t over k . Write $v(N)$ for the number of prime divisors of N , ϕ for Euler's ϕ -function, and $C_d(N) = \phi(N)/((12)^d d! 2^{(d-1)v(N)+1})$. In §5 (Corollaries 4 and 5) we show that for every $\varepsilon > 0$ there is a positive constant $C_{k,d,\varepsilon}$ so that

$$D \geq C_d(N)[k:\mathbf{Q}]^{-1} \geq C_{k,d,\varepsilon} N^{1-\varepsilon}. \quad (1.1)$$

The constant depends only on ε , d , and k , not on the abelian variety A , and can be made explicit. Thus, for a given number field k and dimension d , there are only finitely many possibilities for $A(k)_{\text{torsion}}$, where A is an abelian variety of CM-type and dimension d defined over k .

More specifically, suppose A is an abelian variety of dimension d , (A, θ) is of type $(M_{n_1}(K_1) \times \cdots \times M_{n_m}(K_m), \Psi)$ (see §2 for definitions) where K_1, \dots, K_m are CM-fields and $\sum_{i=1}^m n_i [K_i:\mathbf{Q}] = 2d$, C is a polarization of A compatible with the embedding θ of $M_{n_1}(K_1) \times \cdots \times M_{n_m}(K_m)$ into $\text{End}(A) \otimes \mathbf{Q}$, and t is a point of A of order N . Let k_0 and k_t be the fields of moduli of (A, C, θ) and (A, C, θ, t) respectively, let μ be the number of roots of unity in $K_1 \times \cdots \times K_m$, and let $r_b(N) = \#\{m \in (\mathbf{Z}/N\mathbf{Z})^\times : m \equiv 1 \pmod{N}\}$ where $b = [\tilde{K}:\mathbf{Q}]/2$ and \tilde{K} is the compositum of the reflex fields of the K_i 's. In §4 (Theorems 1 and 2) we show:

$$[k_t:k_0] \geq \phi(N)/r_b(N)\mu \geq \phi(N)/(2^{(d-1)v(N)+1} 6^d). \quad (1.2)$$

We will show that (1.2) implies (1.1).

* NSF Postdoctoral Fellow.

For comparison, results of Masser, Bertrand, and Serre give lower bounds for the degree of a torsion point which hold for all abelian varieties, but have constants which *depend on the abelian variety*. For example, transcendence theory leads to the result:

THEOREM (Bertrand [1]). *If A is a simple abelian variety of dimension d defined over a number field k , and t is a point of A of degree D over k and order N , then for every $\varepsilon > 0$ there is a positive constant $C_{A,k,\varepsilon}$ so that $D \geq C_{A,k,\varepsilon} N^{1/(d+2+\varepsilon)}$.*

Here, the constant $C_{A,k,\varepsilon}$ is effectively computable in terms of ε , $[k:\mathbf{Q}]$, and the height of the equations defining A . (See also [3]).

Using the theory of l -adic Galois representations, Serre can show (with notation as above):

THEOREM (Serre [5]). *If A contains no abelian subvariety of CM-type, then for every $\varepsilon > 0$ there is a positive constant $C_{A,k,\varepsilon}$ so that $D \geq C_{A,k,\varepsilon} N^{2-\varepsilon}$. If A does contain an abelian subvariety of CM-type, one must replace $2 - \varepsilon$ by $1 - \varepsilon$.*

Serre's inequalities are stronger than Bertrand's, but Serre's constants are ineffective.

The proof of (1.2) essentially appears in [9] (proof of Proposition 7.3), where only a weaker result was explicitly stated, namely:

$$[k_i:k_0] \geq C_d N^s \quad \text{with } s = 2/3 - \log_3 2$$

(with an explicit positive constant C_d depending *only* on d). Also, in [9] we had $n_i = 1$ for $i = 1, \dots, m$.

2. Definitions

Suppose K_1, \dots, K_m are CM-fields, and d, n_1, \dots, n_m are positive integers so that

$$2d = \sum_{i=1}^m n_i [K_i:\mathbf{Q}]. \tag{2.1}$$

Let $Z = M_{n_1}(K_1) \times \dots \times M_{n_m}(K_m)$, $W = K_1^{n_1} \times \dots \times K_m^{n_m}$, $K = K_1 \times \dots \times K_m$, and $W_{\mathbf{R}} = W \otimes_{\mathbf{Q}} \mathbf{R}$. Then W is a left Z -module. Suppose Ψ is a faithful complex representation of Z of dimension d , \mathfrak{J} is a Z -lattice

in W , $U: W \times W \rightarrow \mathbf{Q}$ is an alternating form, and v_1, \dots, v_s are elements of W . Also, suppose A is an abelian variety over \mathbf{C} of dimension d , θ is an embedding of \mathbf{Z} in $\text{End}(A) \otimes \mathbf{Q}$, C is a polarization on A , and t_1, \dots, t_s are points of A of finite order. Let ρ be the involution of $\text{End}(A) \otimes \mathbf{Q}$ determined by C , and write \bar{a} for the complex conjugate of $a \in K$.

DEFINITION 1. C is an admissible polarization for (A, θ) if $\theta(a)^{\rho} = \theta(\bar{a})$ whenever $a \in K$.

DEFINITION 2. $(A, C, \theta, t_1, \dots, t_s)$ is of type $(Z, \Psi, \mathfrak{J}, U, v_1, \dots, v_s)$ if C is an admissible polarization for (A, θ) and there is a commutative diagram with exact rows:

$$\begin{array}{ccccccc} 0 & \longrightarrow & \mathfrak{J} & \longrightarrow & W_{\mathbf{R}} & \longrightarrow & W_{\mathbf{R}}/\mathfrak{J} \longrightarrow 0 \\ & & \downarrow & & \downarrow u & & \downarrow \\ 0 & \longrightarrow & D & \longrightarrow & \mathbf{C}^d \xrightarrow{\xi} & A & \longrightarrow 0 \end{array}$$

where D is a lattice in \mathbf{C}^d , ξ gives an isomorphism of \mathbf{C}^d/D onto A , u is an \mathbf{R} -linear isomorphism of $W_{\mathbf{R}}$ onto \mathbf{C}^d which maps W onto $\mathbf{Q}D$, $\mathfrak{J} = u^{-1}(D)$, and:

- (a) $\theta(a) \circ \xi = \xi \circ \Psi(a)$ for every $a \in Z$,
- (b) $u(ax) = \Psi(a)u(x)$ for every $a \in Z$ and $x \in W_{\mathbf{R}}$,
- (c) $U(x, y) = E(u(x), u(y))$ for every $x, y \in W$, where E is a Riemann form on \mathbf{C}^d/D , induced by the polarization C , and
- (d) $\xi(u(v_j)) = t_j$ for $j = 1, \dots, s$.

Note 1 : The reader accustomed to the case of abelian varieties A with complex multiplication by a CM-field of degree $2(\dim A)$ may prefer to assume throughout that $m = 1$ and $n_1 = 1$. Then $Z = W =$ a CM-field.

DEFINITION 3. (A, θ) is of type (Z, Ψ) if (a) and (b) of Definition 2 hold for some u and ξ . We also say (A, θ) is of CM-type if (A, θ) is of type (Z, Ψ) for some (Z, Ψ) as above (for some positive integers m and n_1, \dots, n_m).

Note 2: Every (A, θ) of type (Z, Ψ) has an admissible polarization C (§6 of [8]).

Note 3: Given (A, θ) of type (Z, Ψ) , points of finite order t_1, \dots, t_s , and an admissible polarization C for (A, θ) there always exist $\mathfrak{J}, U, v_1, \dots, v_s$ so that $(A, C, \theta, t_1, \dots, t_s)$ is of type $(Z, \Psi, \mathfrak{J}, U, v_1, \dots, v_s)$ (see [6]).

3. Main theorem of complex multiplication

If (A, θ) is of type (Z, Ψ) , then A is isogenous to a product $A_1^{n_1} \times \cdots \times A_m^{n_m}$ where A_1, \dots, A_m are abelian varieties. The map θ induces maps $\theta_i: K_i \hookrightarrow \text{End}(A_i) \otimes \mathbf{Q}$ so that (A_i, θ_i) is of type (K_i, Φ_i) where $\Psi|_{K_i}$ is equivalent to $n_i \Phi_i +$ (a zero representation). Let $(\tilde{K}_i, \tilde{\Phi}_i)$ be the reflex of (K_i, Φ_i) , and let \tilde{K} be the compositum of $\tilde{K}_1, \dots, \tilde{K}_m$. Define $\eta: \tilde{K}^\times \rightarrow K^\times = K_1^\times \times \cdots \times K_m^\times$ by $\eta(a) = \bigoplus_{i=1}^m (\det \tilde{\Phi}_i)(N_{\tilde{K}/\tilde{K}_i}(a))$ and extend η to a map from \tilde{K}_A^\times to $K_{1_A}^\times \times \cdots \times K_{m_A}^\times$ where M_A^\times is the group of ideles in a number field M . For $c \in \tilde{K}_A^\times$ write $N(c)$ for the absolute norm of the ideal of \tilde{K} associated to c .

THEOREM (Shimura) ([6] §4.3). *Suppose $c \in \tilde{K}_A^\times$, $\sigma \in \text{Aut}(\mathbf{C})$, and $\sigma = [c, \tilde{K}]$ on \tilde{K}_{ab} . If $(A, C, \theta, t_1, \dots, t_s)$ is of type $(Z, \Psi, \mathfrak{J}, U, v_1, \dots, v_s)$ then $(A^\sigma, C^\sigma, \theta^\sigma, t_1^\sigma, \dots, t_s^\sigma)$ is of type $(Z, \Psi, \eta(c)^{-1} \mathfrak{J}, N(c)U, \eta(c)^{-1} v_1, \dots, \eta(c)^{-1} v_s)$.*

COROLLARY 1 (Shimura). *If $Q = (A, C, \theta, t_1, \dots, t_s)$ is of type $(Z, \Psi, \mathfrak{J}, U, v_1, \dots, v_s)$ then the field of moduli of Q is the subfield of \tilde{K}_{ab} corresponding under class field theory to the subgroup $\{c \in \tilde{K}_A^\times : \exists q \in K^\times \subset Z$ with $q\bar{q}N(c) = 1, q\eta(c)\mathfrak{J} = \mathfrak{J}, (q\eta(c) - 1)v_i \in \mathfrak{J}\}$ of \tilde{K}_A^\times .*

The corollary follows directly from the theorem. The special case of full complex multiplication is stated in [7].

4. Main theorems

Suppose (A, C, θ) is of type $(Z, \Psi, \mathfrak{J}, U)$, $d = \dim(A)$, and $t \in A$ is a point of order N . Let k_0 and k_t be the fields of moduli of (A, C, θ) and (A, C, θ, t) , respectively. Take $v \in W$ so that $\xi(u(v)) = t$. By Corollary 1, k_0 and k_t correspond under class field theory to the groups $S_0 = \{c \in \tilde{K}_A^\times : \exists q \in K^\times$ with $q\bar{q}N(c) = 1$ and $q\eta(c)\mathfrak{J} = \mathfrak{J}\}$ and $S_t = \{c \in \tilde{K}_A^\times : \exists q \in K^\times$ with $q\bar{q}N(c) = 1, q\eta(c)\mathfrak{J} = \mathfrak{J}$, and $(q\eta(c) - 1)v \in \mathfrak{J}\}$, respectively.

Let $\mathcal{O} = \theta^{-1}(\text{End}(A) \cap \theta(K)) = \{w \in K: w\mathfrak{J} \subset \mathfrak{J}\}$, an order in K . Let $\tilde{\mathcal{O}}$ be any order in \tilde{K} so that $\eta(\tilde{\mathcal{O}} - 0) \subset \mathcal{O} - 0$. If p is a rational prime and M is a \mathbf{Z} -module, let $M_p = M \otimes_{\mathbf{Z}} \mathbf{Z}_p$. Let $F = \tilde{K}_\infty^\times \cdot \Pi_p \tilde{\mathcal{O}}_p^\times \subset \tilde{K}_A^\times$ and let L be the field corresponding to $\tilde{K}^\times F$.

$$\text{If } c \in F \text{ then (a) } N(c) = 1 \text{ and (b) } \eta(c)\mathfrak{J} = \mathfrak{J}. \tag{4.1}$$

LEMMA 1. $k_0 \subseteq L$.

Proof. By (4.1), $F \subseteq S_0$. For $c \in \tilde{K}^\times$, letting $q = \eta(c)^{-1}$ shows $\tilde{K}^\times \subset S_i \subset S_0$. Thus $\tilde{K}^\times F \subseteq S_0$. \square

Let $\omega = \{\xi \in \mathcal{O}: \xi v \in \mathfrak{I}\}$. Then $\omega \cap \mathbf{Z} = N\mathbf{Z}$ and $\omega_p = \{\xi \in \mathcal{O}_p: \xi v \in \mathfrak{I}_p\}$. Let $E_p = \{c \in \tilde{\mathcal{O}}_p^\times: (\eta(c) - 1)_p \in \omega_p\}$ and let $E = \tilde{K}_\infty^\times \prod_p E_p \subseteq F$.

Let μ be the number of roots of unity in K . (4.2)

LEMMA 2. $[k_i: k_0] \geq [F: E]/\mu$.

Proof. By Lemma 1, $[k_i: k_0] \geq [k_i L: L] = [\tilde{K}^\times F: \tilde{K}^\times F \cap S_i]$. Also, $\tilde{K}^\times F/(\tilde{K}^\times F \cap S_i)$ is isomorphic to $F/(F \cap S_i)$, since $\tilde{K}^\times \subset S_i$. Therefore:

$$[k_i: k_0] \geq [F: F \cap S_i]. \quad (4.3)$$

By (4.1)(b), if $c \in F$ and $q \in K^\times$ then the following are equivalent: (i) $q\eta(c)\mathfrak{I} = \mathfrak{I}$, (ii) $q\mathfrak{I} = \mathfrak{I}$, (iii) $q \in \mathcal{O}^\times$. For $q \in \mathcal{O}^\times$, q is a root of unity exactly when $q\bar{q} = 1$. From (4.1)(a) we now conclude that $F \cap S_i = \{c \in F: \text{for some root of unity } q \in \mathcal{O}^\times \text{ we have } (q\eta(c) - 1)_p \in \omega_p \text{ for every prime } p\}$. Let $R = \{\text{roots of unity in } \mathcal{O}^\times\}$. The map $(F \cap S_i)/E \rightarrow R/(R \cap (1 + \omega))$ which takes c to q is an injection. Therefore $[F \cap S_i: E] \leq \#(R) \leq \mu$. By (4.3), $[k_i: k_0] \geq [F: E]/\mu$. \square

$$\text{Let } b = [\tilde{K}: \mathbf{Q}]/2. \quad (4.4)$$

If $r \in \mathbf{Q}$ then $\eta(r) = r^b$. Let $R_b(N) = \{m \in (\mathbf{Z}/N\mathbf{Z})^\times: m^b \equiv 1 \pmod{N}\}$ and let $r_b(N) = \#R_b(N)$.

THEOREM 1. $[k_i: k_0] \geq \phi(N)/r_b(N)\mu$.

Proof. If p is a rational prime then $N\mathcal{O}_p \subseteq \omega_p \subseteq \mathcal{O}_p$. We can then define a homomorphism $(\mathbf{Z}/N\mathbf{Z})^\times \rightarrow \prod_p \tilde{\mathcal{O}}_p^\times/E_p = F/E$. The kernel is $R_b(N)$, since $\omega \cap \mathbf{Z} = N\mathbf{Z}$. Thus $[F: E] \geq \phi(N)/r_b(N)$, and the theorem follows from Lemma 2. \square

LEMMA 3. Suppose M is a CM-field, $[M: \mathbf{Q}] = 2r$, and m is the number of roots of unity in M . Then $m \leq 6^r$.

Proof. Since M is a CM-field, $\phi(m) \leq [M: \mathbf{Q}] = 2r$. But $\phi(n) \geq 2 \log_6 n$ for all n , so $m \leq 6^r$. \square

From Lemma 3 and (2.1) we can conclude:

$$\mu \leq 6^d. \tag{4.5}$$

We have $\mu = 6^d$ if $K = \mathbf{Q}(\sqrt{-3})^d$.

$$\text{Let } A_{b,\mu}(N) = \phi(N)/r_b(N)\mu. \tag{4.6}$$

Note 4: If $d = 1$ then $A_{b,\mu}(N) = \phi(N)/\mu \geq \phi(N)/6 \geq N/\log \log(N)$.

$$\text{Let } D_d(N) = \phi(N)/(2^{(d-1)v(N)}6^d).$$

$$\text{Let } B_d(N) = \begin{cases} D_d(N) & \text{if } 8 \nmid N \\ D_d(N)/2 & \text{if } 8 \mid N. \end{cases} \tag{4.7}$$

LEMMA 4. $A_{b,\mu}(N) \geq B_d(N)$.

Proof. Writing (m, n) for the greatest common divisor of m and n , we have $r_b(p^t) = (b, \phi(p^t))$ if p is an odd prime, $r_b(2^t) = (b, 2)(b, 2^{t-2})$ if $t \geq 2$, and $r_b(2) = 1$. Thus $r_b(N) \leq b^{v(N)}$ if $8 \nmid N$, and $r_b(N) \leq 2b^{v(N)}$ if $8 \mid N$. Lemma 4 follows from (4.5) and the inequality:

$$b \leq 2^{d-1} \quad ((1.9.1) \text{ of [6]}). \tag{4.8}$$

□

From Theorem 1 and Lemma 5 we have:

THEOREM 2. $[k_i : k_0] \geq B_d(N)$.

LEMMA 5. For $N \geq 3$ we have $B_d(N) \geq C'_d N^{1-dC/\log \log(N)}$, with explicit positive constants C'_d and C .

Proof. Apply the estimates:

$$\phi(n) \geq n/\log \log(n), \text{ and} \tag{4.9}$$

$$v(n) \ll \log(n)/\log \log(n) \tag{4.10}$$

(see [4] for the explicit constants). □

If N is a power of a prime p , we can use the definition of $B_d(N)$ to obtain:

$$B_d(p^r) \geq p^r/(2(12)^d). \tag{4.11}$$

5. Applications to degrees of torsion points

If A is an abelian variety defined over a number field k , and $t \in A(\bar{k})$, we let $D_k = [k(t) : k]$.

COROLLARY 2. *Suppose (A, θ) is defined over a number field k and is of CM-type, and $t \in A(\bar{k})$ is a point of order N . Then*

$$D_k \geq [k : \mathbf{Q}]^{-1} A_{b,\mu}(N) \geq [k : \mathbf{Q}]^{-1} B_d(N)$$

(with b and μ as in (4.2) and (4.4)).

Proof. Let C be an admissible polarization for (A, θ) which is defined over k (such a C exists by an argument analogous to that on pp. 128–9 of [2]). Then (A, C, θ, t) is defined over $k(t)$, and so $k(t)$ contains the field of moduli of (A, C, θ, t) . Thus $[k(t) : \mathbf{Q}] \geq A_{b,\mu}(N) \geq B_d(N)$. \square

COROLLARY 3. *Suppose A is a simple abelian variety of dimension d defined over a number field k , with complex multiplication by a CM-field K of degree $2d$. Suppose t is a point of order N . Then*

$$D_k \geq ([k : \mathbf{Q}][\tilde{K} : \mathbf{Q}])^{-1} A_{b,\mu}(N) \geq (2^d [k : \mathbf{Q}])^{-1} B_d(N)$$

(where \tilde{K} is the reflex field of K , $2b = [\tilde{K} : \mathbf{Q}]$, and μ is the number of roots of unity in K).

Proof. For some θ and Ψ , (A, θ) is of type (K, Ψ) . Since A is simple, (A, θ) is defined over $\tilde{K}k$ (Prop. 30, §8.5 of [8]). By Corollary 2, $[\tilde{K}k(t) : \mathbf{Q}] \geq A_{b,\mu}(N)$. Corollary 3 now follows from (4.8). \square

LEMMA 6. *Suppose (A, θ) is of type $(K_1 \times \cdots \times K_m, \Psi)$ for CM-fields K_i (not necessarily distinct). Let L be the compositum of the Galois closures of the fields K_i . If A is defined over a field k then (A, θ) is defined over kL .*

Proof. The map θ induces a representation of $K_1 \times \cdots \times K_m$ on the space of holomorphic differential forms of A . This representation can be diagonalized over kL , showing that the actions of θ and θ^σ are the same for $\sigma \in \text{Aut}(\mathbf{C}/kL)$. \square

COROLLARY 4. *Suppose A is an abelian variety defined over a number field k , (A, θ) is of CM-type for some θ , and $t \in A(\bar{k})$ is a point of order N . Then*

$$D_k \geq ([k : \mathbf{Q}][L : \mathbf{Q}])^{-1} A_{b,\mu}(N) \geq ([k : \mathbf{Q}]2^d d!)^{-1} B_d(N)$$

(with L the field generated by the Galois closures of the CM-fields in the type of (A, θ)).

Proof. If (A, θ) is of type (Z, Ψ) , let θ' be θ restricted to $K_1^{n_1} \times \cdots \times K_m^{n_m}$. By Lemma 6, (A, θ') is defined over kL . Let L_i be the Galois closure of K_i , and let $2d_i = [K_i : \mathbf{Q}]$. Since K_i is a CM-field we have $[L_i : \mathbf{Q}] \leq 2^{d_i} (d_i)!$ and $[L : \mathbf{Q}] \leq 2^d d!$ by (2.1). From Corollary 2 we know $[kL(t) : \mathbf{Q}] \geq A_{b,\mu}(N)$, and Corollary 4 follows. □

For comparison with the results of Bertrand and Serre, we state:

COROLLARY 5. *Under the assumptions of Corollary 4, for every $\varepsilon > 0$ there is a positive, effectively computable constant $C_{\varepsilon,d,k}$ so that $D_k \geq C_{\varepsilon,d,k} N^{1-\varepsilon}$.*

Proof. Follows from Lemma 5 and Corollary 4. □

Using Lemma 5 we can obtain the same results under the hypotheses of Corollaries 2 or 3. If N is a power of a prime we obtain better inequalities from (4.11).

We now rephrase Corollary 4 in the case $t \in A(k)$ to give bounds on orders of torsion points of abelian varieties of CM-type.

COROLLARY 6. *If A is an abelian variety of CM-type and dimension d defined over a number field k , and N is the order of a torsion point of $A(k)$, then*

$$\phi(N) \leq \begin{cases} [k : \mathbf{Q}](12)^d d! 2^{(d-1)v(N)+1} & \text{if } 8 \mid N \\ [k : \mathbf{Q}](12)^d d! 2^{(d-1)v(N)} & \text{if } 8 \nmid N. \end{cases}$$

As examples of applications of Corollary 6, we state two immediate consequences:

COROLLARY 7. *If E is a CM elliptic curve defined over a number field k , and N is the order of a torsion point of $E(k)$, then $\phi(N) \leq 12[k : \mathbf{Q}]$.*

COROLLARY 8. *If A is a two-dimensional abelian variety of CM-type defined over \mathbf{Q} , and N is the order of a torsion point of $A(\mathbf{Q})$, then*

- (a) $\phi(N) \leq 2^{6+v(N)} \cdot 3^2$,
- (b) $\phi(N) \leq 2^{5+v(N)} \cdot 3^2$ if $8 \nmid N$.
- (c) $v(N) \leq 6$,
- (d) $N \leq 2^3 \cdot 3 \cdot 5 \cdot 7 \cdot 13 \cdot 17 = 185\,640$,
- (e) if N is prime then $N \leq 577$,
- (f) $|A(\mathbf{Q})_{\text{torsion}}| \leq (185\,640)^4$.

Proof. Parts (c), (d), and (e) are elementary computations following from (a) and (b), while (f) follows from the fact that whenever A is an abelian variety of dimension d defined over a number field k , and M is the maximum order of a torsion point of $A(k)$, then $|A(k)_{\text{torsion}}| \leq M^{2d}$.

Note added: Using transcendence theory, Masser has recently obtained the improvement on Bertrand's theorem (see §1): $D \geq C_{A,k} N^{1/d} (\log N)^{-1}$.

I would like to thank D. Bertrand and J.-P. Serre for helpful discussions. I would also like to thank I.H.E.S. for its hospitality, and N.S.F. for a postdoctoral fellowship.

References

1. D. Bertrand: Galois orbits on abelian varieties and zero estimates. London Math. Soc. Lecture Note Series 109 (*Proc. Australian Math. Soc. Convention, 1985*), Cambridge Univ. Press (1986) pp. 21–35.
2. S. Lang: *Complex Multiplication*. Springer-Verlag (1983).
3. D. Masser: Small values of the quadratic part of the Néron–Tate height on an abelian variety. *Comp. Math.* 53 (1984) 153–170.
4. J. B. Rosser and L. Schoenfeld: Approximate formulas for some functions of prime numbers. *Ill. J. Math.* 6 (1962) 64–94.
5. J.-P. Serre: *Résumé des Cours de 1985–1986*. Collège de France (1986).
6. G. Shimura: On canonical models of arithmetic quotients of bounded symmetric domains. *Annals of Math.* 91 (1970) 144–222.
7. G. Shimura: *Introduction to the Arithmetic Theory of Automorphic Functions*. Publ. Iwanami Shoten and Princeton Univ. Press (1971).
8. G. Shimura and Y. Taniyama: *Complex Multiplication of Abelian Varieties and its Applications to Number Theory*, Publ. Math. Soc. Japan, No. 6 (1961).
9. A. Silverberg: Mordell-Weil groups of generic abelian varieties. *Inventiones Math.* 81 (1985) 71–106.