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>
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 $N$, $\phi$ for Euler's $\phi$-function, and $C_d(N) = \phi(N)/(\lfloor 12d!2^{d-1}v(N)+1 \rfloor)$. In §5 (Corollaries 4 and 5) we show that for every $\varepsilon > 0$ there is a positive constant $C_{k,d,\varepsilon}$ so that

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

(1.1)

The constant depends only on $\varepsilon$, $d$, 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 $d$, $(A, \theta)$ is of type $(M_{n_1}(K_1) \times \cdots \times M_{n_m}(K_m), \Psi)$ (see §2 for definitions) where $K_1, \ldots, K_m$ are CM-fields and $\sum_{i=1}^m n_i[K_i:Q] = 2d$, $C$ is a polarization of $A$ compatible with the embedding $\theta$ of $M_{n_1}(K_1) \times \cdots \times M_{n_m}(K_m)$ into $\text{End}(A) \otimes \mathbb{Q}$, and $t$ is a point of $A$ of order $N$. Let $k_0$ and $k_t$ be the fields of moduli of $(A, C, \theta)$ and $(A, C, \theta, t)$ respectively, let $\mu$ be the number of roots of unity in $K_1 \times \cdots \times K_m$, and let $r_b(N) = \# \{m \in (\mathbb{Z}/N\mathbb{Z})^*: m \equiv 1(\text{mod } N) \}$ where $b = [\bar{K}:Q]/2$ and $\bar{K}$ is the compositum of the reflex fields of the $K_i$'s. In §4 (Theorems 1 and 2) we show:

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

(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 \( \varepsilon \), \([k:Q]\), 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:

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

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

2. Definitions

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

\[
2d = \sum_{i=1}^{m} n_i [K_i:Q]. \quad (2.1)
\]

Let \( Z = M_{n_1}(K_1) \times \cdots \times M_{n_m}(K_m) \), \( W = K_1^{n_1} \times \cdots \times K_m^{n_m} \), \( K = K_1 \times \cdots \times K_m \), and \( W \otimes Q R \). Then \( W \) is a left \( Z \)-module. Suppose \( \Psi \) is a faithful complex representation of \( Z \) of dimension \( d \), \( Z \) is a \( Z \)-lattice
in $W, U: W \times W \to \mathbb{Q}$ is an alternating form, and $v_1, \ldots, v_s$ are elements of $W$. Also, suppose $A$ is an abelian variety over $\mathbb{C}$ of dimension $d$, $\theta$ is an embedding of $\mathbb{Z}$ in $\text{End}(A) \otimes \mathbb{Q}$, $C$ is a polarization on $A$, and $t_1, \ldots, t_s$ are points of $A$ of finite order. Let $\varrho$ be the involution of $\text{End}(A) \otimes \mathbb{Q}$ determined by $C$, and write $\bar{a}$ for the complex conjugate of $a \in K$.

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

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

$$
\begin{array}{c}
0 \to \mathcal{I} \to W_\mathbb{R} \to W_\mathbb{R}/\mathcal{I} \to 0 \\
\downarrow \quad \downarrow u \quad \downarrow \\
0 \to D \to \mathbb{C}^d \xrightarrow{\xi} A \to 0
\end{array}
$$

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

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

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

**Definition 3.** $(A, \theta)$ is of type $(\mathbb{Z}, \Psi)$ if (a) and (b) of Definition 2 hold for some $u$ and $\xi$. We also say $(A, \theta)$ is of CM-type if $(A, \theta)$ is of type $(\mathbb{Z}, \Psi)$ for some $(\mathbb{Z}, \Psi)$ as above (for some positive integers $m$ and $n_1, \ldots, n_m$).

**Note 2:** Every $(A, \theta)$ of type $(\mathbb{Z}, \Psi)$ has an admissible polarization $C$ (§6 of [8]).

**Note 3:** Given $(A, \theta)$ of type $(\mathbb{Z}, \Psi)$, points of finite order $t_1, \ldots, t_s$, and an admissible polarization $C$ for $(A, \theta)$ there always exist $\mathcal{I}, U, v_1, \ldots, v_s$ so that $(A, C, \theta, t_1, \ldots, t_s)$ is of type $(\mathbb{Z}, \Psi, \mathcal{I}, U, v_1, \ldots, v_s)$ (see [6]).
3. Main theorem of complex multiplication

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

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

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

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

4. Main theorems

Suppose \((A, C, \theta)\) is of type \((\mathbb{Z}, \Psi, \mathfrak{Z}, U)\), \(d = \dim(A)\), and \(t \in A\) is a point of order \(N\). Let \(k_0\) and \(k_t\) be the fields of moduli of \((A, C, \theta)\) and \((A, C, \theta, t)\), 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 \(S_0 = \{c \in \tilde{K}_\Lambda^\times : \exists q \in K^\times \subset \mathbb{Z}\text{ with } q\bar{q}N(c) = 1\}\) and \(S_t = \{c \in \tilde{K}_\Lambda^\times : \exists q \in K^\times \text{ with } q\bar{q}N(c) = 1, q\eta(c)\mathfrak{Z} = \mathfrak{Z}, (q\eta(c) - 1)v_i \in \mathfrak{Z}\}\), respectively.

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

If \(c \in F\) then (a) \(N(c) = 1\) and (b) \(\eta(c)\mathfrak{Z} = \mathfrak{Z}\). (4.1)
Let $p$ be the number of roots of unity in $K$. By (4.1)(b), if $c \in F$ and $q \in \overline{K}$ then the following are equivalent: (i) $q(c) = 1$, (ii) $q = 1$, (iii) $q \in \mathcal{O}$. From (4.1)(a) we now conclude that $F \cap S_1 = \{c \in F : \text{for some root of unity } q \in \mathcal{O} \text{ we have } (qq(c) - 1)p \in \mathfrak{p} \}$ for every prime $\mathfrak{p}$. Let $R = \{c \in \overline{\mathcal{O}} : (\eta(c) - 1)_p \in \mathcal{O} \}$ and let $E = \overline{K} \cap \Pi_p E_p \subseteq F$.

Let $\mu$ be the number of roots of unity in $K$. (4.2)

\textbf{Lemma 1.} $[k_i : k_0] \geq [F : E]/\mu$.

Proof. By Lemma 1, $[k_i : k_0] \geq [k_i : L] = [\overline{K} \cap \mathcal{O} : \mathcal{O} \cap S_1]$. Also, $\overline{K} \cap \mathcal{O}$ is isomorphic to $F/(F \cap S_1)$, since $\overline{K} \cap \mathcal{O} \subseteq S_1$. Therefore:

$$[k_i : k_0] \geq [F : F \cap S_1].$$

(4.3)

By (4.1)(b), if $c \in F$ and $q \in \overline{K}$ then the following are equivalent: (i) $q\eta(c) \mathfrak{O} = \mathfrak{O}$, (ii) $q \mathfrak{O} = \mathfrak{O}$, (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 $F \cap S_1 = \{c \in F : \text{for some root of unity } q \in \mathcal{O}^\times \text{ we have } (q\eta(c) - 1)_p \in \mathcal{O} \text{ for every prime } p \}$. Let $R = \{\text{roots of unity in } \mathcal{O}^\times \}$. The map $(F \cap S_1)/E \rightarrow R/(R \cap (1 + \omega))$ which takes $c$ to $q$ is an injection. Therefore $[F \cap S_1 : E] \leq \#(R) \leq \mu$. By (4.3), $[k_i : k_0] \geq [F : E]/\mu$. \hfill \Box

$$b = [\overline{K} : \mathbb{Q}]/2.$$ (4.4)

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

\textbf{Theorem 1.} $[k_i : k_0] \geq \phi(N)/r_b(N)\mu$.

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

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

Proof. Since $M$ is a CM-field, $\phi(m) \leq [M : \mathbb{Q}] = 2r$. But $\phi(n) \geq 2 \log_6 n$ for all $n$, so $m \leq 6^r$. \hfill \Box
From Lemma 3 and (2.1) we can conclude:

$$\mu \leq 6^d.$$  \hspace{1cm} (4.5)

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

Let $A_{\mu}(N) = \phi(N)/r_b(N)\mu$.  \hspace{1cm} (4.6)

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

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

Let $B_d(N) = \begin{cases} D_d(N) & \text{if } 8 \nmid N \\ D_d(N)/2 & \text{if } 8 \mid N. \end{cases}$  \hspace{1cm} (4.7)

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

**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:

$$b \leq 2^{d-1} \quad ((1.9.1) \text{ of [6]}).$$  \hspace{1cm} (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 $B_d(N) \geq C_dN^{1-dC}/\log \log (N)$, with explicit positive constants $C_d$ and $C$.

**Proof.** Apply the estimates:

$$\phi(n) \gg n/\log \log (n), \text{ and}$$  \hspace{1cm} (4.9)

$$v(n) \ll \log (n)/\log \log (n)$$  \hspace{1cm} (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:

$$B_d(p^t) \geq p^t/(2(12)^d).$$  \hspace{1cm} (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 $(A, \theta)$ 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

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

(with $b$ and $\mu$ as in (4.2) and (4.4)).

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

**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

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

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

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

**Lemma 6.** Suppose $(A, \theta)$ 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 $(A, \theta)$ is defined over $kL$.

**Proof.** The map $\theta$ 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 $\theta$ and $\theta^\sigma$ are the same for $\sigma \in \text{Aut}(C/kL)$. □

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

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

(with $L$ the field generated by the Galois closures of the CM-fields in the type of $(A, \theta)$).
Proof. If \((A, \theta)\) is of type \((\mathbb{Z}, \Psi), \) let \(\theta'\) be \(\theta\) restricted to \(K_1^{m_1} \times \cdots \times K_m^{m_m}.\)

By Lemma 6, \((A \theta')\) is defined over \(kL.\) Let \(L_i\) be the Galois closure of \(K_i,\)
and let \(2d_i = [K_i : \mathbb{Q}].\) Since \(K_i\) is a CM-field we have \([L_i : \mathbb{Q}] \leq 2^d(d_i)!\) and \([L : \mathbb{Q}] \leq 2^d d!\) by (2.1). From Corollary 2 we know \([kL(t) : \mathbb{Q}] \geq A_{b,\theta}(N),\)
and Corollary 4 follows.

\[ \square \]

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. \[ \square \]

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
\[ \phi(N) \leq \begin{cases} [k : \mathbb{Q}] \bigl(12(2d) \times d! \times 2^{(d-1)\times(N)+1} \bigr) & \text{if } 8 \mid N, \\
 [k : \mathbb{Q}] \bigl(12(2d) \times d! \times 2^{(d-1)\times(N)} \bigr) & \text{if } 8 \not\mid N. \end{cases} \]

As examples of applications of Corollary 6, we state two immediate conse-
quences:

**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 \(\phi(N) \leq 12[k : \mathbb{Q}].\)

**Corollary 8.** If \(A\) is a two-dimensional abelian variety of CM-type defined
over \(\mathbb{Q},\) and \(N\) is the order of a torsion point of \(A(\mathbb{Q}),\) then
\begin{align*}
(a) & \quad \phi(N) \leq 2^{6+x(N)} \times 3^2, \\
(b) & \quad \phi(N) \leq 2^{5+x(N)} \times 3^2 \text{ if } 8 \not\mid N, \\
(c) & \quad \nu(N) \leq 6, \\
(d) & \quad N \leq 2^4 \times 3 \times 5 \times 7 \times 13 \times 17 = 185,640, \\
(e) & \quad \text{if } N \text{ is prime then } N \leq 577, \\
(f) & \quad |A(\mathbb{Q})_{\text{torsion}}| \leq (185,640)^4. 
\end{align*}

**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): $D \geq C_{A,\delta} N^{1/d} \left(\log N\right)^{-1}$.

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