Bounds on torsion of CM abelian varieties over a $p$-adic field with values in a field of $p$-power roots

Yoshiyasu Ozeki

September 8, 2022

Abstract

Let $p$ be a prime number and $M$ the extension field of a $p$-adic field $K$ obtained by adjoining all $p$-power roots of all elements of $K$. In this paper, we show that there exists a constant $C$, depending only on $K$ and an integer $g > 0$, which satisfies the following property: If $A/K$ is a $g$-dimensional CM abelian variety, then the order of the torsion subgroup of $A(M)$ is bounded by $C$.

1 Introduction

Let $p$ be a prime number. Let $K$ be a number field (= a finite extension of $\mathbb{Q}$) or a $p$-adic field (= a finite extension of $\mathbb{Q}_p$). Let $A$ be an abelian variety defined over $K$ of dimension $g$. It follows from the Mordell-Weil theorem and the main theorem of [Mat] that the torsion subgroup $A(K)_{\text{tors}}$ of $A(K)$ is finite. The following question for $A(K)_{\text{tors}}$ is quite natural and have been studied for a long time:

Question. What can be said about the size of the order of $A(K)_{\text{tors}}$?

If $K$ is a number field of degree $d$ and $A$ is an elliptic curve (i.e., $g = 1$), it is really surprising that there exists a constant $B(d)$, depending only on the degree $d$, such that $\sharp A(K)_{\text{tors}} < B(d)$. The explicit formula of such a constant $B(d)$ is given by Merel, Oesterlé and Parent (cf. [Me], [Pa]). The amazing point here is that the constant $B(d)$ is uniform in the sense that it depends not on the number field $K$ but on the degree $d = [K : \mathbb{Q}]$. Such uniform boundedness results are not known for abelian varieties of dimension greater than one. Next we consider the case where $K$ is a $p$-adic field. As remarked by Cassels, the "uniform boundedness theorem" for $p$-adic base fields would be false (cf. Lemma 17.1 and p.264 of [Ca]). For abelian varieties $A$ over $K$ with anisotropic reduction, Clark and Xarles [CX] give an upper bound of the order of $A(K)_{\text{tors}}$ in terms of $g, p$ and some numerical invariants of $K$. This includes the case in which $A$ has potentially good reduction, and in this case the existence of a bound can be found in some literatures (cf. [Si2], [Si3]).

We are interested in the order of $A(L)_{\text{tors}}$ for certain algebraic extensions $L$ of $K$ of infinite degree. Now we suppose that $K$ is a $p$-adic field. There are not so many known $L$ so that $A(L)_{\text{tors}}$ is infinite. Imai [Im] showed that $A(L)_{\text{tors}}$ is finite if $A$ has potential good reduction and $L = K(\mu_{p^{\infty}})$, where $\mu_{p^{\infty}}$ is the set of $p$-power root of unity. The author [Oz] showed that Imai’s finiteness result holds even if we replace $L = K(\mu_{p^{\infty}})$ with $L = K k_{\pi}$, where $k$ is a $p$-adic field and $k_{\pi}$ is the Lubin-Tate extension of $k$ associated with a certain uniformizer $\pi$ of $k$. The result [KT] of Kubo and Taguchi is also interesting. They showed that the torsion subgroup of $A(K(\sqrt{K}))$ is finite, where $A$ is an abelian variety over $K$ with potential good reduction and $K$ is the extension field $K(\sqrt{K})$. This is quite surprising.
of $K$ obtained by adjoining all $p$-power roots of all elements of $K$. Our main theorem is motivated by the result of Kubo and Taguchi. The goal of this paper is to show that, under the assumption that $A$ has complex multiplication, the order of $A(K(\sqrt[p]{R}))_{\text{tors}}$ is "uniformly" bounded.

**Theorem 1.** There exists a constant $C(K,g)$, depending only on a $p$-adic field $K$ and an integer $g > 0$, which satisfies the following property: If $A$ is a $g$-dimensional abelian variety over $K$ with complex multiplication, then we have

$$\sharp A(K(\sqrt[p]{R}))_{\text{tors}} < C(K,g).$$

The theorem above gives a global result: For any integer $d > 0$, we denote by $Q_{\leq d}$ the composite of all number fields of degree $\leq d$. If we fix an embedding $\mathbb{Q} \hookrightarrow \mathbb{Q}_p$, then $Q_{\leq d}$ is embedded into the composite field of all $p$-adic fields of degree $\leq d$, which is a finite extension of $\mathbb{Q}_p$. If we denote by $Q_{\leq dp}$ the extension field of $Q_{\leq d}$ obtained by adjoining all $p$-power roots of all elements of $Q_{\leq d}$, then the following is an immediate consequence of our main theorem.

**Corollary 2.** There exists a constant $C(d,g,p)$, depending only on positive integers $d,g$ and a prime number $p$, which satisfies the following property: If $A$ is a $g$-dimensional abelian variety over $Q_{\leq d}$ with complex multiplication, then we have

$$\sharp A(Q_{\leq dp})_{\text{tors}} < C(d,g,p).$$

**Notation:** Throughout this paper, a $p$-adic field means a finite extension of $\mathbb{Q}_p$ in a fixed algebraic closure $\overline{\mathbb{Q}}_p$ of $\mathbb{Q}_p$. If $F$ is an algebraic extension of $\mathbb{Q}_p$, we denote by $\mathcal{O}_F$ and $\mathcal{F}_F$ the ring of integers of $F$ and the residue field of $F$, respectively. We denote by $G_F$ the absolute Galois group of $F$ and also denote by $\Gamma_F$ the set of $\mathbb{Q}_p$-algebra embeddings of $F$ into $\mathbb{Q}_p$. We set $d_F = [F : \mathbb{Q}_p]$. For an algebraic extension $F'/F$, we denote by $e_{F'/F}$ and $f_{F'/F}$ the ramification index of $F'/F$ and the extension degree of the residue field extension of $F'/F$, respectively. We set $e_F := e_{F/\mathbb{Q}_p}$ and $f_F := f_{F/\mathbb{Q}_p}$, and also set $q_F := p^{f_F}$. If $F$ is a $p$-adic field, we denote by $F^{ab}$ and $F^{ur}$ the maximal abelian extension of $F$ and the maximal unramified extension of $F$, respectively.

## 2 Proof

### 2.1 Some technical tools

We denote by $v_p$ the $p$-adic valuation on a fixed algebraic closure $\overline{\mathbb{Q}}_p$ of $\mathbb{Q}_p$ normalized by $v_p(p) = 1$. Let $K$ be a $p$-adic field. For any continuous character $\chi$ of $G_K$, we often regard $\chi$ as a character of $\text{Gal}(K^{ab}/K)$. We denote by $\text{Art}_K$ the local Artin map $K^\times \to \text{Gal}(K^{ab}/K)$ with arithmetic normalization. We set $\chi_K := \chi \circ \text{Art}_K$. We denote by $\hat{K}^\times$ the profinite completion of $K^\times$. Note that the local Artin map induces a topological isomorphism $\text{Art}_K: \hat{K}^\times \cong \text{Gal}(K^{ab}/K)$.

**Proposition 3.** Let $K$ and $k$ be $p$-adic fields. We denote by $k_\pi$ the Lubin-Tate extension of $k$ associated with a uniformizer $\pi$ of $k$. (If $k = \mathbb{Q}_p$ and $\pi = p$, then we have $k_\pi = \mathbb{Q}_p(\mu_{p^\infty})$.) Let $\chi_1, \ldots, \chi_n: G_K \to \overline{\mathbb{Q}}_p^\times$ be continuous characters. Then we have

$$\\begin{align*}
\min \left\{ \sum_{i=1}^n v_p(\chi_i(\sigma) - 1) \mid \sigma \in G_{K^\pi} \right\} \\
\leq \min \left\{ \sum_{i=1}^n v_p(\chi_i \circ \text{Nr}_{K^\pi/K}(\omega) - 1) \mid \omega \in \text{Nr}_{K^\pi/k}(\pi^{f_{K^\pi}/k} \mathbb{Z}) \right\}.
\end{align*}$$

**Proof.** We have a topological isomorphism $\text{Art}_k^{-1}: \text{Gal}(k^{ab}/k) \cong \hat{k}^\times$ and $\text{Art}_k^{-1}(\text{Gal}(k^{ab}/k^{ur})) = \mathcal{O}_k^\times$. We denote by $M$ the maximal unramified extension of $k$ contained in $Kk$. Since the group
Art^{-1}(\text{Gal}(k^{ab}/M)) \text{ contains } \Omega_k^\flat \text{ and is a subgroup of } \hat{k}^\times = \pi^\flat \times \Omega_k^\flat \text{ of index } [M : k], \text{ we see Art}_{k}^{-1}(\text{Gal}(k^{ab}/M)) = \pi^{[M:k] \hat{\mathbb{Z}}} \times \Omega_k^\flat. \text{ On the other hand, we have Art}_{k}^{-1}(\text{Gal}(k^{ab}/k)) = \pi^\flat. \text{ Thus we obtain Art}_{k}^{-1}(\text{Gal}(k^{ab}/M_{k})) = \pi^{[M:k] \hat{\mathbb{Z}}}. \text{ Now we denote by } \text{Res}_{K/k} \text{ the natural restriction map } \text{Gal}((K/k)^{ab}/K) \to \text{Gal}(k^{ab}/k). \text{ It is not difficult to check that } \text{Res}_{K/k}^{-1}(\text{Gal}(k^{ab}/M_{k})) = \text{Gal}((K/k)^{ab}/K_{k}). \text{ Thus it follows that the group Art}_{k}^{-1}(\text{Gal}((K/k)^{ab}/K_{k})) \text{ coincides with } \text{Nr}_{K/k}^{-1}(\pi^{[M:k] \hat{\mathbb{Z}}}). \text{ Therefore, if we take any } \omega \in \text{Nr}_{K/k}^{-1}(\pi^{[M:k] \hat{\mathbb{Z}}})), \text{ we have }

\begin{align*}
\text{Min} \left\{ \sum_{i=1}^{n} v_{p}(\chi_{i}(\sigma)) - 1 \mid \sigma \in G_{K_{k}} \right\} \\
= \text{Min} \left\{ \sum_{i=1}^{n} v_{p}(\chi_{i}(\sigma)) - 1 \mid \sigma \in \text{Gal}((K/k)^{ab}/K_{k}) \right\} \\
= \text{Min} \left\{ \sum_{i=1}^{n} v_{p}(\chi_{i,K} \circ \text{Nr}_{K/k} \circ \text{Art}_{k}^{-1}(\sigma) - 1) \mid \sigma \in \text{Gal}((K/k)^{ab}/K_{k}) \right\} \\
\leq \sum_{i=1}^{n} v_{p}(\chi_{i,K} \circ \text{Nr}_{K/k}(\omega) - 1).
\end{align*}

\[ \square \]

We recall an observation of Conrad. We denote by \( K^\times \) the Weil restriction \( \text{Res}_{K/\mathbb{Q}_{p}}(\mathbb{G}_{m}) \) and let \( D_{\text{cris}}^{K}(\cdot) := (B_{\text{cris}} \otimes_{\mathbb{Q}_{p}})^{G^{\times}}. \)

**Proposition 4 [CLO Proposition B.4].** Let \( K \) and \( F \) be p-adic fields. Let \( \chi: G_{K} \to F^{\times} \) be a continuous character. We denote by \( F(\chi) \) the \( \mathbb{Q}_{p} \)-representation of \( G_{K} \) underlying a 1-dimensional \( F \)-vector space endowed with an \( F \)-linear action by \( G_{K} \) via \( \chi \).

1. \( \chi \) is crystalline if and only if there exists a (necessarily unique) \( \mathbb{Q}_{p} \)-homomorphism \( \chi_{\text{alg}}: K^\times \to F^{\times} \) such that \( \chi_{K} \text{ and } \chi_{\text{alg}} \) (on \( \mathbb{Q}_{p} \)-points) coincides on \( \Omega_{K} \subset K^{\times} = K^\times(\mathbb{Q}_{p}) \).

2. Let \( K_{0} \) be the maximal unramified subextension of \( K/\mathbb{Q}_{p} \). Assume that \( \chi \) is crystalline and let \( \chi_{\text{alg}} \) be as in (1). (Note that \( \chi^{-1} \) is also crystalline.) Then, the filtered \( \varphi \)-module \( D_{\text{cris}}^{K}(F(\chi^{-1})) = (B_{\text{cris}} \otimes_{\mathbb{Q}_{p}} F(\chi^{-1}))^{G^{\times}} \) over \( K \) is free of rank 1 over \( K_{0} \otimes_{\mathbb{Q}_{p}} F \) and its \( k_{0} \)-linear endomorphism \( \varphi^{K} \) is given by the action of the product \( \chi_{K}(\pi_{K}) : \chi_{\text{alg}}^{-1}(\pi_{K}) \in F^{\times} \). Here, \( \pi_{K} \) is any uniformizer of \( K \).

We define some notations for later use. Assume that \( K \) is a Galois extension of \( \mathbb{Q}_{p} \). Let \( \chi: G_{K} \to K^{\times} \) be a crystalline character. Let \( \chi_{\text{LT}}: I_{K} \to K^{\times} \) be the restriction to the inertia \( I_{K} \) of the Lubin-Tate character associated with any choice of uniformizer of \( K \) (it depends on the choice of a uniformizer of \( K \), but its restriction to the inertia subgroup does not). By definition, the character \( \chi_{\text{LT}} \) is characterized by \( \chi_{\text{LT}} \circ \text{Art}_{K}(x) = x^{-1} \) for any \( x \in \mathbb{O}_{K}^{\times} \). (We remark that \( \chi_{\text{LT}} \) is the restriction to \( I_{K} \) of the p-adic cyclotomic character if \( K = \mathbb{Q}_{p} \).) Then, we have

\[ \chi = \prod_{\sigma \in \Gamma_{K}} \sigma^{-1} \circ \chi_{\text{LT}}^{h_{\sigma}} \]

on the inertia \( I_{K} \) for some (unique) integer \( h_{\sigma} \). Equivalently, the character \( \chi_{\text{alg}} \) (appeared in Proposition 3 on \( \mathbb{Q}_{p} \)-points) is given by

\[ \chi_{\text{alg}}(x) = \prod_{\sigma \in \Gamma_{K}} (\sigma^{-1} x)^{-h_{\sigma}} \]

for \( x \in K^{\times} \). We say that \( h = (h_{\sigma})_{\sigma \in \Gamma_{K}} \) is the Hodge-Tate type of \( \chi \). Note that \( \{ h_{\sigma} \mid \sigma \in \Gamma_{K} \} \) as a set is the set of Hodge-Tate weights of \( K(\chi) \), that is, \( C \otimes_{\mathbb{Q}_{p}} K(\chi) \simeq \otimes_{\sigma \in \Gamma_{K}} C(h_{\sigma}) \) where \( C \) is the completion of \( \mathbb{Q}_{p}^{\circ} \).

\[ ^{1} \text{This means that the } \mathbb{Q}_{p} \text{-representation } F(\chi) \text{ of } G_{K} \text{ is crystalline.} \]
For any set of integers $h = (h_\sigma)_{\sigma \in \Gamma_K}$ indexed by $\Gamma_K$, we define a continuous character $\psi_h: \mathcal{O}_K^\times \rightarrow \mathcal{O}_K^\times$ by

$$
\psi_h(x) = \prod_{\sigma \in \Gamma_K} (\sigma^{-1} x)^{-h_\sigma}.
$$

(2.1)

**Lemma 5.** For $1 \leq i \leq r$, let $h_i = (h_{i, \sigma})_{\sigma \in \Gamma_K}$ be a set of integers. For each $i$, assume that

(a) $\sum_{\sigma \in \Gamma_K} h_{i, \sigma}$ is not zero, and

(b) $h_{i, \sigma} \neq h_{i, \tau}$ for some $\sigma, \tau \in \Gamma_K$.

Then, there exists an element $\omega$ of $\ker N_{R/K}/Q_p$ such that $\psi_{h_i}(\omega), \ldots, \psi_{h_r}(\omega)$ are of infinite orders.

**Proof.** For any character $\chi$ on $\mathcal{O}_K^\times$, we denote by $\chi'$ the restriction of $\chi$ to $1 + p^2 \mathcal{O}_K$. To show the lemma, it suffices to show

$$
\ker N_{R/K}/Q_p \nsubseteq \bigcup_{i=1}^r \ker \psi_{h_i}'.
$$

(2.2)

(In fact, any non-trivial element of $\text{Im} \, \psi_{h_i}'$ is of infinite order since $\text{Im} \, \psi_{h_i}'$ is a subgroup of a torsion free group $1 + p^2 \mathcal{O}_K$.) Since $N_{R/K}/Q_p (1 + p^2 \mathcal{O}_K)$ is an open subgroup of $\mathbb{Z}_p^r$, we see that the dimension$^2$ of $\ker N_{R/K}/Q_p$ is $d_K - 1$. We claim that $\dim \ker \psi_{h_i} < d_K - 1$. By the assumption (a), we see that $\text{Im} \, \psi_{h_i}'$ contains an open subgroup $H$ of $\mathbb{Z}_p^{r'}$. Thus we have $\dim \ker \psi_{h_i}' = d_K - \dim \text{Im} \, \psi_{h_i}' \leq d_K - 1$. If we assume $\dim \ker \psi_{h_i}' = d_K - 1$, then $\dim \ker \psi_{h_i}' = 1$ and thus $H$ is a finite index subgroup of $\text{Im} \, \psi_{h_i}'$. It follows that there exists an open subgroup $U$ of $\mathcal{O}_K^\times$ such that $\psi_{h_i}'$ restricted to $U$ has values in $\mathbb{Z}_p$. By [O2, Lemma 2.4], we obtain that $h_{i, \sigma} = h_{i, \tau}$ for any $\sigma, \tau \in \Gamma_K$ but this contradicts the assumption (b) in the statement of the lemma. Thus we conclude that $\dim \ker \psi_{h_i} < d_K - 1$.

Now we fix an isomorphism $\iota: 1 + p^2 \mathcal{O}_K \simeq \mathbb{Z}_p^{d_K}$ of topological groups. We define vector subspaces $N$ and $P_i$ of $\mathbb{Z}_p^{d_K}$ by $N := i(\ker N_{R/K}/Q_p) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$ and $P_i := i(\ker \psi_{h_i}') \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$. We know that $\dim_{\mathbb{Q}_p} N = d_K - 1$ and $\dim_{\mathbb{Q}_p} P_i < d_K - 1$. Assume that $\mathbb{Z}_p$ does not hold, that is, $\ker N_{R/K}/Q_p \nsubseteq \bigcup_{i=1}^r \ker \psi_{h_i}'$. Then we have $N \nsubseteq \bigcup_{i=1}^r P_i$. This implies $N = \bigcup_{i=1}^r (N \cap P_i)$. By the lemma below, we find that $N = N \cap P_i \subseteq P_i$ for some $i$ but this contradicts the fact that $\dim_{\mathbb{Q}_p} N > \dim_{\mathbb{Q}_p} P_i$.

**Lemma 6.** Let $V$ be a vector space over a field $F$ of characteristic zero. Let $W_1, \ldots, W_r$ be vector subspaces of $V$. If $V = \bigcup_{i=1}^r W_i$, then $V = W_i$ for some $i$.

**Proof.** We show by induction on $r$. The cases $r = 1, 2$ are clear. Assume that the lemma holds for $r$ and suppose $V = \bigcup_{i=1}^{r+1} W_i$. We assume both $W_1 \nsubseteq \bigcup_{i=2}^{r+1} W_i$ and $W_{r+1} \nsubseteq \bigcup_{i=1}^{r} W_i$ holds. Then there exist elements $x_1 \in W_1 \setminus \bigcup_{i=2}^{r+1} W_i$ and $x_{r+1} \in W_{r+1} \setminus \bigcup_{i=1}^{r} W_i$. It is not difficult to check that we have $\lambda x_1 + x_{r+1} \notin \bigcup_{i=2}^{r+1} W_i$ for any $\lambda \in F^\times$. Hence there exists an integer $2 \leq j_n \leq r$ for each integer $n > 0$ such that $nx_1 + x_{r+1} \in W_{j_n}$. Take any integers $0 < \ell < k$ so that $j_n \leq j \leq j_{n+1} = j_k (= j)$. Then $(k - \ell)x_1 = (kx_1 + x_{r+1}) - ((\ell x_1 + x_{r+1}) \in W_j'$. Since $F$ is of characteristic zero, we have $x_1 \in W_j'$ but this contradicts the fact that $x_1 \notin \bigcup_{i=2}^{r+1} W_i$. Therefore, either $W_1 \subseteq \bigcup_{i=2}^{r+1} W_i$ or $W_{r+1} \subseteq \bigcup_{i=1}^{r} W_i$ holds. This shows that $V = \bigcup_{i=2}^{r+1} W_i$ or $V = \bigcup_{i=1}^{r} W_i$ and the induction hypothesis implies $V = W_i$ for some $i$.

Finally we describe the following consequence of $p$-adic Hodge theory, which is well-known for experts.

**Proposition 7.** Let $X$ be a proper smooth variety with good reduction over a $p$-adic field $K$. Then we have

$$
det(T - \varphi^{K})|_{H^r_{\text{cris}}(X_K, \mathbb{Q}_p)} = \det(T - \text{Frob}_K^{-1})|_{H^r_{\text{et}}(X_K, \mathbb{Q}_p)}
$$

for any prime $\ell \neq p$. Here, $\text{Frob}_K$ stands for the arithmetic Frobenius of $K$.

\footnote{If a profinite group $G$ has an open subgroup $U$ which is isomorphic to $\mathbb{Z}_p^{d'}$, then $d$ does not depend on the choice of $U$ and we say that $d$ is the dimension of $G$. For example, $\dim \mathbb{Z}_p^{d} = d$. Note that the dimension of $G$ is zero if and only if $G$ is finite. See [DDMS] for general theories of dimensions of $p$-adic analytic groups.}
Proof. Let $Y$ be the special fiber of a proper smooth model of $X$ over the integer ring of $K$. By the crystalline conjecture shown by Faltings [Fa] (cf. [Ni], [Tsu]), we have an isomorphism\[D_{\text{cris}}^G(H^0_{\text{dR}}(X_{\overline{\mathbb{Q}}_p}, \mathbb{Q}_p)) \simeq K_0 \otimes_{W(F_{q_p})} H^0_{\text{cris}}(Y/W(F_{q_p})) \] of $\varphi$-modules over $K_0$. It follows from Corollary 1.3 of [CLS] (cf. [KM, Theorem 1] and [Na, Remark 2.2.4 (4)]) that the characteristic polynomial of $K_0 \otimes_{W(F_{q_p})} H^0_{\text{cris}}(Y/W(F_{q_p}))$ for the ($f_K$-iterate) Frobenius action coincides with $\det(T - \text{Frob}_{K_0}^\ell | H^0_{\text{dR}}(X_{\overline{\mathbb{Q}}_p}, \mathbb{Q}_p))$ for any prime $\ell \neq p$. Thus the result follows. \hfill \Box

2.2 Proof of the main theorem

Let $A$ be a $g$-dimensional abelian variety over $K$ with complex multiplication. We denote by $L$ the field obtained by adjoining to $K$ all points of $A[12]$. It follows from [ST] Theorem 4.1] that endomorphisms of $A$ are defined over $L$. By the Raynaud’s criterion of semistable reduction [Gr, Proposition 4.7], $A$ has semistable reduction over $L$. Moreover, $A$ has good reduction over $L$ since $A$ has complex multiplication [ST, Section 2, Corollary 1]. Since the extension degree of $L$ over $K$ is at most the order of $GL_{2g}(\mathbb{Z}/12\mathbb{Z})$ and there exist only finitely many $p$-adic field of a given degree, we immediately reduces a proof of Theorem 1 to show the following

**Proposition 8.** There exists a constant $\hat{C}(K, g)$, depending only on a $p$-adic field $K$ and an integer $g > 0$, which satisfies the following property: Let $A$ be a $g$-dimensional abelian variety over $K$ with the properties that $A$ has good reduction over $K$ and $\text{End}_K(A) \otimes_{\mathbb{Z}} \mathbb{Q}$ is a CM field of degree $2g$. Then we have

\[\sharp A \left(K^{(p\sqrt{K})}\right)_{\text{tors}} < \hat{C}(K, d).\]

Proof. Since there exist only finitely many $p$-adic field of a given degree, replacing $K$ by a finite extension, we may assume the following hypothesis:

(H) $K$ is a Galois extension of $\mathbb{Q}_p$ and $K$ contains all $p$-adic fields of degree $\leq 2g$.

In the rest of the proof, we set $M := K^{(p\sqrt{K})}$. Let $A$ be a $g$-dimensional abelian variety over $K$ with the properties that $A$ has good reduction over $K$ and $F := \text{End}_K(A) \otimes_{\mathbb{Z}} \mathbb{Q}$ is a CM field of degree $2g$. Let $T = T_p(A) := \varprojlim \ A[p^n]$ be the $p$-adic Tate module of $A$ and $V = V_p(A) := T_p(A) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$. Then $V$ is a free $F_p$-module of rank one and the representation $\rho: G_K \rightarrow GL_{\mathbb{Q}_p}(V)$ defined by the $G_K$-action on $H^1(T, V)$ has values in $GL_{F_p}(V) = F_p^\times$. In particular, $\rho$ is an abelian representation. The representation $V$ is a $H$-Tate representation with $H$-Tate weights $0$ (multiplicity $g$) and $1$ (multiplicity $g$). Moreover, $V$ is crystalline since $A$ has good reduction over $K$. Fix an isomorphism $\iota: T \rightarrow \mathbb{Z}_p^{\oplus 2g}$ of $\mathbb{Z}_p$-modules. We have an isomorphism $i: GL_{\mathbb{Z}_p}(T) \simeq GL_{2g}(\mathbb{Z}_p)$ relative to $\iota$. We abuse notation by writing $\rho$ for the composite map $G_K \rightarrow GL_{\mathbb{Z}_p}(T) \simeq GL_{2g}(\mathbb{Z}_p)$ of $\rho$ and $i$. Now let $P \in T$ and denote by $\overline{P}$ the image of $P$ in $T/p^nT$. By definition, we have $i(\sigma P) = \rho(\sigma) i(P)$ for $\sigma \in G_K$. Suppose that $P \in (T/p^nT)^{G_M}$. This implies $\sigma P = P \in p^nT$ for any $\sigma \in G_M$. This is equivalent to say that $(\rho(\sigma) - E) i(P) \in p^n\mathbb{Z}_p^{\oplus 2g}$, and this in particular implies $\det(\rho(\sigma) - E) i(P) \in p^n\mathbb{Z}_p^{\oplus 2g}$ for any $\sigma \in G_M$. If we denote by $M_{ab}$ the maximal abelian extension of $K$ contained in $M$, it holds that $\rho(G_M) = \rho(G_{M_{ab}})$ since $\rho(G_K)$ is abelian. Thus we have

\[\det(\rho(\sigma) - E) i(P) \in p^n\mathbb{Z}_p^{\oplus 2g} \quad \text{for any } \sigma \in G_{M_{ab}}. \] (2.3)

On the other hand, we set $G := \text{Gal}(M/K)$ and $H := \text{Gal}(M/K(\mu_{p\infty}))$. Let $\chi_p: G_K \rightarrow \mathbb{Z}_p^\times$ be the $p$-adic cyclotomic character. Since we have $\sigma\tau\sigma^{-1} = \tau x_{\varphi}(\sigma)$ for any $\sigma \in G$ and $\tau \in H$, we see $(G, G) \supset (G, H) \supset H^N(\varphi)^{-1}$. Hence we have a natural surjection

\[H/H^N(\varphi)^{-1} \twoheadrightarrow H/(G, G) = \text{Gal}(M_{ab}/K(\mu_{p\infty})) \quad \text{for any } \sigma \in G. \] (2.4)

Let $\nu$ be the smallest $p$-power integer with the properties that $\nu > 1$ and $\chi_p(G_K) \supset 1 + \nu\mathbb{Z}_p$. Then (2.4) gives the fact that $\text{Gal}(M_{ab}/K(\mu_{p\infty}))$ is of exponent $\nu$, that is, $\sigma \in G_{K(\mu_{p\infty})}$ implies

\[\sigma^\nu = 1 \quad \text{in } M_{ab}. \] (2.5)

Then (2.5) gives the fact that $\text{Gal}(M_{ab}/K(\mu_{p\infty}))$ is of exponent $\nu$, that is, $\sigma \in G_{K(\mu_{p\infty})}$ implies

\[\sigma^\nu = 1 \quad \text{in } M_{ab}. \] (2.6)

Therefore, we have

\[\sharp A \left(K^{(p\sqrt{K})}\right)_{\text{tors}} < \hat{C}(K, d). \] (2.7)
\( \sigma^\nu \in G_{\text{M}_0} \). Hence it follows from (2.3) that, for any point \( P \in T \) such that its image \( \tilde{P} \) in \( T/p^nT \) is fixed by \( G_M \), we have

\[
\det(\rho(\sigma)^\nu - E)(P) \in p^n\mathbb{Z}_p^{2g} \quad \text{for any } \sigma \in G_{K(\mu_p)}.
\]  

(2.5)

**Claim 1.** There exists a constant \( C_0(K,g) \), depending only on \( K \) and \( g \) such that

\[
v_p(\det(\rho(\sigma)^\nu - E)) \leq C_0(K,g)
\]

for some \( \sigma_0 \in G_{K(\mu_p)} \).

Admitting this claim, we can finish the proof of Proposition 8 immediately: It follows from Claim 1 and (2.5) that \((\cdot)^\nu \) from the prime-to-\( p \) part of \( \psi^T/p\psi^T \) for some \( \sigma \in \text{Gal}(\mathbb{Q}_p) \), which shows \( \psi^T \). On the other hand, we remark that Kubo and Taguchi showed in [KT] that the residue field \( F_M \) of \( M \) is finite. The reduction map induces an injection from the prime-to-\( p \)- part of \( A(M) \) into \( \overline{T}(F_M) \) where \( \overline{T} \) is the reduction of \( A \). If we denote by \( q \) the order of \( \overline{T} \), it follows from the Weil bound that \( \overline{T}(F_M) \leq (1 + \sqrt{q})^{2g} \). Therefore, setting \( C(K,g) := C(K,g)_p \cdot (1 + \sqrt{q})^{2g} \), we conclude that \( \psi^T \) is fixed by \( G_K \) and \( \sqrt{q} \). We remark that this finishes the proof of the proposition.

It suffices to show Claim 1. Since the action of \( G_K \) on \( V \) factors through an abelian quotient of \( G_K \), it follows from the Schur’s lemma that each Jordan H"older factor of \( V \otimes_{\mathbb{Q}_p} \mathbb{Q}_p \) is of dimension one. Let \( \psi_1, \ldots, \psi_{2g} : G_K \to \overline{\mathbb{Q}}_p \) be the characters associated with the Jordan H"older factors of \( V \). Since \( K \) contains all \( p \)-adic fields of degree \( \leq 2g \), we know that each \( \psi_i \) has values in \( \mathbb{K}^\times \) (in fact, for any \( \sigma \in G_K \), we know that \( \psi_i(\sigma) \) are the roots of the polynomial \( \det(T - \sigma) \in \mathbb{Q}_p[T] \) of degree \( 2g \)). In the rest of the proof, we regard \( \psi_i \) as a character \( G_K \to \mathbb{K}^\times \) of \( G_K \) with values in \( \mathbb{K}^\times \). We remark that each \( \psi_i \) is a crystalline character since \( V \) is crystalline. Furthermore, we have

\[
v_p(\det(\rho(\sigma)^\nu - E)) = v_p\left(\prod_{i=1}^{2g}(\psi_i^\nu(\sigma) - 1)\right) = \sum_{i=1}^{2g} v_p(\psi_i^\nu(\sigma) - 1)
\]

for any \( \sigma \in G_{K(\mu_p)} \). Hence it follows from Lemma 3 that we have

\[
\min\{ v_p(\det(\rho(\sigma)^\nu - E)) \mid \sigma \in G_{K(\mu_p)} \}
\]

\[
\leq \min\left\{ \sum_{i=1}^{2g} v_p(\psi_i^\nu(K)(\omega)^{-1} - 1) \mid \omega \in \ker\text{Nr}_{K/Q_p} \right\}.
\]  

(2.6)

Note that we have

\[
\psi_i(K)(\omega)^{-1} = \psi_i(K)(\pi^{-e_K} \cdot \pi^{-e_K} p^{-1}) \cdot \psi_i(K)(\omega)^{-1}
\]

\[
= \psi_i(K)(\pi^{-e_K} \cdot \psi_i(\text{alg}(\pi^{-e_K} p^{-1})) \cdot \psi_i(K)(\omega)^{-1}
\]

\[
= \alpha^{-e_K} \cdot \psi_i(\text{alg}(p))^{-1} \cdot \psi_i(K)(\omega)^{-1}
\]

(2.7)

for \( \omega \in \ker\text{Nr}_{K/Q_p} \), where \( \alpha_i := \psi_i(K)(\pi_K)\psi_i(\text{alg}(\pi_K))^{-1} \).

**Lemma 9.** Let the notation be as above. Let \( A^\nu \) be the dual abelian variety of \( A \), and let \( \overline{A} \) and \( \overline{A}^\nu \) be the reductions of \( A \) and \( A^\nu \), respectively.

(1) \( \alpha_i^\nu \) is a root of the characteristic polynomial of the geometric Frobenius endomorphism of \( \overline{A}/\mathbb{F}_K \).

(2) \( \alpha_i q^K \) is a root of the characteristic polynomial of the geometric Frobenius endomorphism of \( \overline{A}^\nu/\mathbb{F}_K \).
Proof. Since $K(\psi^{-1})$ is a subquotient of $V_p(A)^{\nu} \otimes_{Q_p} K$, it follows from Proposition 4 that $\alpha_i$ is a root of the characteristic polynomial $f(T) := \det(T - \varphi_{fK} | D_{crys}^K(V_p(A)^{\nu}))$ of the $K_0$-linear endomorphism $\varphi_{fK}$, the $f_K$-th iterate of the Frobenius $\varphi$, on the $K_0$-vector space $D_{crys}^K(V_p(A)^{\nu})$. We find that
\[
f(T) = \det(T - \varphi_{fK} | D_{crys}^K(H_{cst}(A_{fK}, Q_p))) = \det(T - \operatorname{Frob}_{K}^{-1} | H_{cst}(A_{fK}, Q_{\ell}) = \det(T - \operatorname{Frob}_{K} | V_f(A))\]
for any prime $\ell \neq p$ where $\operatorname{Frob}_fK$ stands for the arithmetic Frobenius. The second equality follows from Proposition 7. The last term above coincides with the characteristic polynomial of the geometric Frobenius endomorphism of $\overline{A}_{\ell/K}$. This shows (1). On the other hand, it follows from Proposition 4 again that $\alpha_i^{-1}$ is a root of $\det(T - \varphi_{fK} | D_{crys}^K(V_p(A)))$. Since $V_p(A)(-1) \cong V_p(A)^{\nu}$, we see that $\alpha_i^{-1}$ is a root of $f'(T) := \det(T - \varphi_{fK} | D_{crys}^K(V_p(A)^{\nu}))$. Now the same argument of the proof of (1) with replacing $A$ by $A'$ gives a proof of (2). \hfill \square

We continue the proof of Proposition 8. Let $h_i \in (h_{i,\sigma})_{\sigma \in \Gamma_K}$ be the Hodge-Tate type of $\psi_i$. Then we have $h_{i,\sigma} \in \{0, 1\}$ for any $i$ and $\sigma$. We may suppose the following:

(I) $h_i \neq (0)_{\sigma \in \Gamma_K}$, $(1)_{\sigma \in \Gamma_K}$ for $1 \leq i \leq r$, and

(II) $h_i = (0)_{\sigma \in \Gamma_K}$ or $h_i = (1)_{\sigma \in \Gamma_K}$ for $r + 1 \leq i \leq 2g$.

Consider the case $h_i = (0)_{\sigma \in \Gamma_K}$. If this is the case, $\psi_i$ is unramified. This implies that $\psi_{i, \text{alg}}$ on $(Q_p)$-points) is trivial. Take any $\omega \in \ker N_{R/K}p$ and consider the $p$-adic value $v_p(\psi_{i, K}(p\omega)^{-1})$. By (2.7), we have
\[
\psi_{i, K}(p\omega)^{-1} = \alpha_i^{-\nu e K}.
\] (2.8)

We remark that the right hand side is independent of the choice of $\omega \in \ker N_{R/K}p$ and $\alpha_i$ must be a $p$-adic unit (since so is the left hand side). Next consider the case $h_i = (1)_{\sigma \in \Gamma_K}$. If this is the case, we have $\psi_i = \chi_{p}$ on $I_K$, that is, $\psi_{i, \text{alg}}$ (on $Q_p$-points) is $N_{R/K}^{-1}$. Take any $\omega \in \ker N_{R/K}p$ and consider the $p$-adic value $v_p(\psi_{i, K}(p\omega)^{-1})$. By (2.7), we have
\[
\psi_{i, K}(p\omega)^{-1} = (\alpha_i^{-\nu e K} \cdot N_{R/K}^{-1}(p\omega))^{-\nu} = (\alpha_i^{-1})^{-\nu e K}.
\] (2.9)

We remark that the last term is independent of the choice of $\omega \in \ker N_{R/K}p$. Suppose $r + 1 \leq i \leq 2g$. Let $L$ be the unramified extension of $K$ of degree $\nu e K$. Denote by $f_i(T)$ the characteristic polynomial of the Frobenius endomorphism of $\overline{A}_{\ell/L}$ (resp. $\overline{A}_{\ell/L}$) if $h_i = (0)_{\sigma \in \Gamma_K}$ (resp. $h_i = (1)_{\sigma \in \Gamma_K}$). It follows from (2.8) (resp. (2.9)) and Lemma 9 that $\nu_{i, K}(p\omega)$ (resp. $\nu_{i, K}(p\omega)^{-1}$) is a unit root of $f_i(T)$. Since $f_i(1)$ coincides with $z_{\overline{A}}(\overline{F}_{qL})$ (resp. $z_{\overline{A}}(\overline{F}_{qL})$), we find $v_p(\psi_{i, K}(p\omega)^{-1}) \leq v_p(f_i(1))$. It follows from the Weil bound that $f_i(1) \leq (1 + \sqrt{4}L)^{2g} \leq (1 + \sqrt{p})^{2g}$, which gives an inequality $v_p(f_i(1)) \leq \log_p(1 + \sqrt{p})^{2g}$. Therefore, setting $C_2(K, g) := \log_p(1 + \sqrt{p})^{2g}$, we obtain
\[
v_p(\psi_{i, K}(p\omega)^{-1}) \leq C_2(K, g)
\]for $r + 1 \leq i \leq 2g$.

Suppose $1 \leq i \leq r$. We define a subset $R = R(K, g)$ of $Q_p$ by the set consisting of $\alpha \in Q_p$, which is a root of a polynomial in $\mathbb{Z}[T]$ of degree at most $2g$ and also is a $q_K$-Weil integer of weight 1. We also define $R' = R'(K, g) := \{((\alpha - c_K)^{\nu} | \alpha \in R, 0 < h < d_K\}$. Then, both $R$ and $R'$ are finite sets and depend only on $K$ and $g$. Furthermore, Lemma 9 and the Weil Conjecture imply that each $\alpha_i$ is an element of $R$. Thus, setting $\gamma_i := \alpha_i - c_K \cdot \psi_{i, \text{alg}}(p)^{-1} = \alpha_i - c_K \cdot \sum_{\omega \in \Gamma_K} h_{i, \omega} \cdot \omega$, we have $\gamma_i \in R'$. We consider the continuous character $\psi_i : O_{K} \twoheadrightarrow O_{K}^{\nu}$ defined in (2.4). The character $\psi_{i, \text{alg}}$ (on $Q_p$-points) restricted to $O_{K}^{\nu}$ coincides with $\psi_{h_i}$. By Lemma 8 there exists an element $\omega = \omega(K, h_1, \ldots, h_r)$ of $\ker N_{K/K}p$ such that $\psi_{h_i}(\omega)$ are of infinite order. Since $R'$ is finite, there exists an integer $r$ such that $\psi_{h_r}(\omega)^{r}$, $\ldots$, $\psi_{h_r}(\omega)^{r}$ are not contained in $R'$. Putting $\omega_0 = \omega$, it holds that
• $\omega_0$ is an element of $\ker N_{K/Q_p}$. Furthermore, $\omega_0$ depends only on $K, g$ and $h_1, \ldots, h_r$, and
• $\psi_{h_1}(\omega_0), \ldots, \psi_{h_r}(\omega_0)$ are not contained in $R'$.

Now we define a constant $C(K, g, h_1, \ldots, h_r)$ by

$$C(K, g, h_1, \ldots, h_r) = \max \left\{ \sum_{i=1}^r v_p(\gamma_i^\prime \psi_{h_i}(\omega_0)^{-1} - 1) \mid \gamma_i^\prime \in R' \right\}.$$ 

By construction of $\omega_0$, we see that the constant above is finite and depends only on $K, g, h_1, \ldots, h_r$. We find that

$$\min \left\{ \sum_{i=1}^g v_p(\psi_{i,K}(p\omega_0)^{-1} - 1) \mid \omega \in \ker N_{K/Q_p} \right\}$$

$$\leq \sum_{i=1}^g v_p(\psi_{i,K}(p\omega_0)^{-1} - 1) = \sum_{i=1}^r v_p(\gamma_i^\prime \psi_{h_i}(\omega_0)^{-1} - 1) + \sum_{i=r+1}^{2g} v_p(\psi_{i,K}(p\omega_0)^{-1} - 1)$$

$$\leq C(K, g, h_1, \ldots, h_r) + (2g - r)C_2(K, g) \leq C_0(K, g). \quad (2.10)$$

Here,

$$C_0(K, g) := \max \{ C(K, g, h_1, \ldots, h_r) + (2g - r)C_2(K, g) \mid 0 \leq r \leq 2g, h_1, \ldots, h_r : \text{Case (I)} \}$$

(if $r = 0$, we consider the constant $C(K, g, h_1, \ldots, h_r)$ as zero). By construction, the constant $C_0(K, g)$ is finite and depends only on $K$ and $g$. By (2.3) and (2.10), we conclude that $C_0(K, g)$ defined here satisfies the desired property of Claim 4. This is the end of the proof of Proposition S.

We end this paper with the following remarks.

**Remark 10.**
1. We do not know the explicit description of the bound $C(K, g)$ in Theorem 1.
2. We do not know whether we can remove the sentence "with complex multiplication" from the statement of Theorem 1 or not.
3. Let $K$ be a $p$-adic field. Let $\pi = \pi_0$ be a uniformizer of $K$ and $\pi_n$ a $p^n$-th root of $\pi$ such that $\pi_{n+1} = \pi_n$ for any $n \geq 0$. We set $K_\infty := K(\pi_n \mid n \geq 0)$. The field $K_\infty$ is clearly a subfield of $K(\sqrt[p]{K})$. It is well-known that $K_\infty$ is one of key ingredients in (integral) $p$-adic Hodge theory since $K_\infty$ is familiar to the theory of norm fields. We can check the equality

$$A(K_\infty)_{\text{tors}} = A(K)_{\text{tors}}$$

holds for any abelian variety $A$ over $K$ with good reduction. (We do not need CM assumption here.) The proof is as follows: It follows from the criterion of Néron-Ogg-Shafarevich [ST] Theorem 1] that the inertia subgroup $I_K$ of $G_K$ acts trivially on the prime-to-$p$ part of $A(K)_{\text{tors}}$. Since $K_\infty$ is totally ramified over $K$, we obtain the fact that the prime-to-$p$ parts of $A(K)_{\text{tors}}$ and $A(K_\infty)_{\text{tors}}$ coincide with each other. On the other hand, we consider the following natural maps.

$$A(K)[p^n] \cong \text{Hom}_{G_K}(\mathbb{Z}/p^n\mathbb{Z}, A(K)[p^n]) \cong A(K_\infty)[p^n]$$

Since $A$ has good reduction, the injection $\phi_A$ above is bijective (cf. [Br] Theorem 3.4.3] for $p > 2$; [KL], [La], [L3] for $p = 2$). This implies $A(K_\infty)[p^{\infty}] = A(K)[p^{\infty}]$.

4. It follows immediately from (3), the Raynaud’s criterion of semistable reduction and the main theorem of [CX] that there exists an explicitly calculated constant $C$, depending only on $K$ and $g$, such that we have

$$\sharp A(K_\infty)_{\text{tors}} < C$$

for any abelian variety $A$ over $K$ with potential good reduction. (We do not need CM assumption here.) We leave the readers to give the explicit description of $C$ above.
References

[Br] C. Breuil, Integral p-adic Hodge theory, in Algebraic geometry 2000, Azumino (Hotaka), Adv. Stud. Pure Math., vol. 36, Math. Soc. Japan, 2002, 51–80.

[Ca] J. W. S. Cassels, Diophantine equations with special reference to elliptic curves, J. London Math. Soc., 41 (1966), 193–291.

[CLS] B. Chiarellotto and B. Le Stum, Sur la pureté de la cohomologie cristalline, C. R. Acad. Sci. Paris Sér. I Math. 8 (1998), 961–963.

[Co] B. Conrad, Lifting global representations with local properties, preprint, 2011, available at http://math.stanford.edu/~conrad/papers/locchar.pdf

[CX] P.L. Clark and X. Xarles, Local bounds for torsion points on abelian varieties, Canad. J. Math. vol. 60 (2008), 532–555.

[DDMS] J.D. Dixon, M.P.F. du Sautoy, A. Mann and D. Segal, Analytic pro-p groups, Second edition, Cambridge Studies in Advanced Mathematics, 61, Cambridge Univ. Press, Cambridge, 1999.

[Fa] G. Faltings, Crystalline cohomology and p-adic Galois-representations, Algebraic analysis, geometry, and number theory (Baltimore MD, 1988), 25–80.

[Gr] Alexander Grothendieck, Modèles de Néron et monodromie, in Groupes de monodromie en géometrie algébrique, SGA 7, Lecture Notes in Mathematics, vol. 288, 313–523 (1972).

[Im] H. Imai, A remark on the rational points of abelian varieties with values in cyclotomic $\mathbb{Z}_p$-extensions, Proc. Japan Acad. 51 (1975), 12–16.

[Ki] W. Kim, The classification of p-divisible groups over 2-adic discrete valuation rings, Math. Res. Lett. 19 (2012), no. 1, 121–141.

[KT] Y. Kubo and Y. Taguchi, A generalization of a theorem of Imai and its applications to Iwasawa theory, Math. Z. 275 (2013), 1181–1195.

[KM] N. Katz and W. Messing, Some consequences of the Riemann hypothesis for varieties over finite fields, Invent. Math. 23 (1974), 73–77.

[La] E. Lau, Relation between Dieudonné displays and crystalline Dieudonné theory, Algebra Number Theory 8 (2014), 2201–2262.

[Li] Tong Liu, The correspondence between Barsotti-Tate groups and Kisin modules when $p = 2$, Journal de Théorie des Nombres de Bordeaux, 25, no. 3 (2013), 661–676.

[Mat] A. Mattuck, Abelian varieties over p-adic ground fields, Ann. of Math. (2) 62 (1955), 92–119.

[Me] Loïc, Merel, Bornes pour la torsion des courbes elliptiques sur les corps de nombres, Invent. Math., 124 (1996), 437–449.

[Na] Y. Nakakajima, p-adic weight spectral sequences of log varieties, J. Math. Sci. Univ. Tokyo 12 (2005), 513–661.

[Ni] W. Niziol, Crystalline conjecture via K-theory, Ann. Sci. École Norm. Sup. (4) 31 (1998), 659–681.

[Oz] Y. Ozeki, Torsion of abelian varieties and Lubin-Tate extensions, J. Number Theory 207 (2020), 282–293.
[Pa] P. Parent, *Bornes effectives pour la torsion des courbes elliptiques sur les corps de nombres*, J. Reine Angew. Math., 506 (1999), 85–116.

[Se] J.-P. Serre, *Abelian l-adic representations and elliptic curves*, second ed., Advanced Book Classics, Addison-Wesley Publishing Company Advanced Book Program, Redwood City, CA, 1989, With the collaboration of Willem Kuyk and John Labute.

[Si1] A. Silverberg, *Fields of definition for homomorphisms of abelian varieties*, J. Pure Appl. Algebra 77 (1992), no. 3, 253–262.

[Si2] A. Silverberg, *Points of finite order on abelian varieties*, Contemp. Math. 133 (1992), 175–193.

[Si3] A. Silverberg, *Open questions in arithmetic algebraic geometry*, In: Arithmetic Algebraic Geometry. IAS/Park CityMath. Ser. 9, American Mathematical Society, Providence, RI, 2001, 83–142.

[ST] J.-P. Serre and J. Tate, *Good reduction of abelian varieties*, Ann. of Math. (2) 8 (1986), 492–517.

[Tsu] T. Tsuji, *p-adic étale cohomology and crystalline cohomology in the semi-stable reduction case*, Invent. Math. 137 (1999), 233–411.