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

Yoshiyasu Ozeki*

September 6, 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 $A(K)_{\mathrm{tors}}$ of $A(K)$ is finite. The following question for $A(K)_{\mathrm{tors}}$ is quite natural and have been studied for a long time:

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

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 $\sharp A(K)_{\mathrm{tors}} < B(d)$. 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 $A(K)_{\mathrm{tors}}$ 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 $A(L)_{\mathrm{tors}}$ 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 $A(L)_{\mathrm{tors}}$ is finite. Imai [Im] showed that $A(L)_{\mathrm{tors}}$ is finite if A has potential good reduction and $L = K(\mu_{p^\infty})$, where μ_{p^∞} 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 $L = Kk_\pi$, where k is a p-adic field and k_π is the Lubin-Tate extension of k associated with a certain uniformizer π of k. The result [KT] of Kubo and Taguchi is also interesting. They showed that the torsion subgroup of $A(K(\sqrt[p^\infty]{K}))$ is finite, where A is an abelian variety over K with potential good reduction and $K(\sqrt[p^\infty]{K})$ is the extension field

*Department of Mathematics and Physics, Faculty of Science, Kanagawa University, 2946 Tsuchiya, Hiratsuka-shi, Kanagawa 259–1293, JAPAN
e-mail: ozeki@kanagawa-u.ac.jp
This work is supported by JSPS KAKENHI Grant Number JP19K03433.

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 $A(K(\sqrt[p^\infty]{K}))_{\mathrm{tors}}$ 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*

$$\sharp A\left(K(\sqrt[p^\infty]{K})\right)_{\mathrm{tors}} < C(K,g).$$

The theorem above gives a global result: For any integer $d>0$, we denote by $\mathbb{Q}_{\leq d}$ the composite of all number fields of degree $\leq d$. If we fix an embedding $\overline{\mathbb{Q}} \hookrightarrow \overline{\mathbb{Q}}_p$, then $\mathbb{Q}_{\leq d}$ 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 $\mathbb{Q}_{\leq d,p}$ the extension field of $\mathbb{Q}_{\leq d}$ obtained by adjoining all p-power roots of all elements of $\mathbb{Q}_{\leq d}$, 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 $\mathbb{Q}_{\leq d}$ with complex multiplication, then we have*

$$\sharp A(\mathbb{Q}_{\leq d,p})_{\mathrm{tors}} < C(d,g,p).$$

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 $\mathbb{F}_F$ 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 Γ_F the set of $\mathbb{Q}_p$-algebra embeddings of F into $\overline{\mathbb{Q}}_p$. We put $d_F=[F:\mathbb{Q}_p]$. 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 χ of G_K, we often regard χ as a character of $\mathrm{Gal}(K^{\mathrm{ab}}/K)$. We denote by Art_K the local Artin map $K^\times \to \mathrm{Gal}(K^{\mathrm{ab}}/K)$ with arithmetic normalization. We set $\chi_K := \chi\circ \mathrm{Art}_K$. We denote by $\widehat{K}^\times$ the profinite completion of $K^\times$. Note that the local Artin map induces a topological isomorphism $\mathrm{Art}_K\colon \widehat{K}^\times \xrightarrow{\sim} \mathrm{Gal}(K^{\mathrm{ab}}/K)$.

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

$$\begin{aligned}&\mathrm{Min}\left\{\sum_{i=1}^n v_p(\chi_i(\sigma)-1)\mid \sigma\in G_{Kk_\pi}\right\}\\ \leq\ &\mathrm{Min}\left\{\sum_{i=1}^n v_p(\chi_{i,K}\circ \mathrm{Nr}_{Kk/K}(\omega)-1)\mid \omega\in \mathrm{Nr}_{Kk/k}^{-1}(\pi^{f_{Kk/k}\mathbb{Z}})\right\}.\end{aligned}$$

Proof. We have a topological isomorphism $\mathrm{Art}_k^{-1}\colon \mathrm{Gal}(k^{\mathrm{ab}}/k)\xrightarrow{\sim}\widehat{k}^\times$ and $\mathrm{Art}_k^{-1}(\mathrm{Gal}(k^{\mathrm{ab}}/k^{\mathrm{ur}}))=\mathcal{O}_k^\times$. We denote by M the maximal unramified extension of k contained in Kk. Since the group

$\mathrm{Art}_k^{-1}(\mathrm{Gal}(k^{\mathrm{ab}}/M))$ contains $\mathcal{O}_k^\times$ and is a subgroup of $\widehat{k}^\times = \pi^{\widehat{\mathbb{Z}}} \times \mathcal{O}_k^\times$ of index $[M : k]$, we see $\mathrm{Art}_k^{-1}(\mathrm{Gal}(k^{\mathrm{ab}}/M)) = \pi^{[M:k]\widehat{\mathbb{Z}}} \times \mathcal{O}_k^\times$. On the other hand, we have $\mathrm{Art}_k^{-1}(\mathrm{Gal}(k^{\mathrm{ab}}/k_\pi)) = \pi^{\widehat{\mathbb{Z}}}$. Thus we obtain $\mathrm{Art}_k^{-1}(\mathrm{Gal}(k^{\mathrm{ab}}/Mk_\pi)) = \pi^{[M:k]\widehat{\mathbb{Z}}}$. Now we denote by $\mathrm{Res}_{Kk/k}$ the natural restriction map $\mathrm{Gal}((Kk)^{\mathrm{ab}}/Kk) \to \mathrm{Gal}(k^{\mathrm{ab}}/k)$. It is not difficult to check that $\mathrm{Res}_{Kk/k}^{-1}(\mathrm{Gal}(k^{\mathrm{ab}}/Mk_\pi)) = \mathrm{Gal}((Kk)^{\mathrm{ab}}/Kk_\pi)$. Thus it follows that the group $\mathrm{Art}_{Kk}^{-1}(\mathrm{Gal}((Kk)^{\mathrm{ab}}/Kk_\pi))$ coincides with $\mathrm{Nr}_{Kk/k}^{-1}(\pi^{[M:k]\widehat{\mathbb{Z}}})$. Therefore, if we take any $\omega \in \mathrm{Nr}_{Kk/k}^{-1}(\pi^{[M:k]\mathbb{Z}})$, we have

$$\begin{aligned}
&\mathrm{Min}\left\{\sum_{i=1}^n v_p(\chi_i(\sigma)-1) \mid \sigma \in G_{Kk_\pi}\right\}\\
=\ &\mathrm{Min}\left\{\sum_{i=1}^n v_p(\chi_i(\sigma)-1) \mid \sigma \in \mathrm{Gal}((Kk)^{\mathrm{ab}}/Kk_\pi)\right\}\\
=\ &\mathrm{Min}\left\{\sum_{i=1}^n v_p(\chi_{i,K}\circ \mathrm{Nr}_{Kk/K}\circ \mathrm{Art}_{Kk}^{-1}(\sigma)-1) \mid \sigma \in \mathrm{Gal}((Kk)^{\mathrm{ab}}/Kk_\pi)\right\}\\
\leq\ &\sum_{i=1}^n v_p(\chi_{i,K}\circ \mathrm{Nr}_{Kk/K}(\omega)-1).
\end{aligned}$$

□

We recall an observation of Conrad. We denote by $\underline{K}^\times$ the Weil restriction $\mathrm{Res}_{K/\mathbb{Q}_p}(\mathbb{G}_m)$ and let $D_{\mathrm{cris}}^K(\cdot) := (B_{\mathrm{cris}} \otimes_{\mathbb{Q}_p} \cdot)^{G_K}$.

Proposition 4 ([Co, Proposition B.4]). *Let K and F be p-adic fields. Let $\chi\colon G_K \to F^\times$ 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 χ,*
(1) χ is crystalline[1] if and only if there exists a (necessarily unique) $\mathbb{Q}_p$-homomorphism $\chi_{\mathrm{alg}}\colon \underline{K}^\times \to \underline{F}^\times$ such that χ_K and χ_{alg} (on $\mathbb{Q}_p$-points) coincides on $\mathcal{O}_K^\times$ $(\subset K^\times = \underline{K}^\times(\mathbb{Q}_p))$.
(2) Let K_0 be the maximal unramified subextension of $K/\mathbb{Q}_p$. Assume that χ is crystalline and let χ_{alg} be as in (1). (Note that χ^{-1} is also crystalline.) Then, the filtered φ-module $D_{\mathrm{cris}}^K(F(\chi^{-1})) = (B_{\mathrm{cris}} \otimes_{\mathbb{Q}_p} F(\chi^{-1}))^{G_K}$ over K is free of rank 1 over $K_0 \otimes_{\mathbb{Q}_p} F$ and its k_0-linear endomorphism φ^{f_K} is given by the action of the product $\chi_K(\pi_K)\cdot\chi_{\mathrm{alg}}^{-1}(\pi_K) \in F^\times$. Here, π_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 $\chi\colon G_K \to K^\times$ be a crystalline character. Let $\chi_{\mathrm{LT}}\colon I_K \to K^\times$ 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 χ_{LT} is characterlized by $\chi_{\mathrm{LT}}\circ \mathrm{Art}_K(x) = x^{-1}$ for any $x \in \mathcal{O}_K^\times$. (We remark that χ_{LT} is the restriction to I_K of the p-adic cyclotomic character if $K = \mathbb{Q}_p$.) Then, we have

$$\chi = \prod_{\sigma\in\Gamma_K} \sigma^{-1}\circ \chi_{\mathrm{LT}}^{h_\sigma}$$

on the inertia I_K for some (unique) integer h_σ. Equivalently, the character χ_{alg} (appeared in Proposition 4) on $\mathbb{Q}_p$-points is given by

$$\chi_{\mathrm{alg}}(x) = \prod_{\sigma\in\Gamma_K} (\sigma^{-1}x)^{-h_\sigma}$$

for $x \in K^\times$. We say that $\mathbf{h} = (h_\sigma)_{\sigma\in\Gamma_K}$ is the *Hodge-Tate type of* χ. Note that $\{h_\sigma \mid \sigma \in \Gamma_K\}$ as a set is the set of Hodge-Tate weights of $K(\chi)$, that is, $C \otimes_{\mathbb{Q}_p} K(\chi) \simeq \oplus_{\sigma\in\Gamma_K} C(h_\sigma)$ where C is the completion of $\overline{\mathbb{Q}}_p$.

[1] This means that the $\mathbb{Q}_p$-representation $F(\chi)$ of G_K is crystalline.

For any set of integers $\mathbf{h} = (h_\sigma)_{\sigma\in\Gamma_K}$ indexed by Γ_K, we define a continuous character $\psi_{\mathbf{h}}\colon \mathcal{O}_K^\times \to \mathcal{O}_K^\times$ by

$$\psi_{\mathbf{h}}(x) = \prod_{\sigma\in\Gamma_K} (\sigma^{-1}x)^{-h_\sigma}. \tag{2.1}$$

Lemma 5. *For $1 \le i \le r$, let $\mathbf{h}_i = (h_{i,\sigma})_{\sigma\in\Gamma_K}$ 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 ω of $\ker \mathrm{Nr}_{K/\mathbb{Q}_p}$ such that $\psi_{\mathbf{h}_1}(\omega), \dots, \psi_{\mathbf{h}_r}(\omega)$ are of infinite orders.

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

$$\ker \mathrm{Nr}'_{K/\mathbb{Q}_p} \not\subset \bigcup_{i=1}^{r} \ker \psi'_{\mathbf{h}_i}. \tag{2.2}$$

(In fact, any non-trivial element of $\mathrm{Im}\ \psi'_{\mathbf{h}_i}$ is of infinite order since $\mathrm{Im}\ \psi'_{\mathbf{h}_i}$ is a subgroup of a torsion free group $1+p^2\mathcal{O}_K$.) Since $N'_{K/\mathbb{Q}_p}(1+p^2\mathcal{O}_K)$ is an open subgroup of $\mathbb{Z}_p^\times$, we see that the dimension[2] of $\ker N'_{K/\mathbb{Q}_p}$ is $d_K - 1$. We claim that $\dim \ker \psi_{\mathbf{h}_i} < d_K - 1$. By the assumption (a), we see that $\mathrm{Im}\ \psi'_{\mathbf{h}_i}$ contains an open subgroup H of $\mathbb{Z}_p^\times$. Thus we have $\dim \ker \psi'_{\mathbf{h}_i} = d_K - \dim \mathrm{Im}\ \psi'_{\mathbf{h}_i} \le d_K - 1$. If we assume $\dim \ker \psi'_{\mathbf{h}_i} = d_K - 1$, then $\dim \mathrm{Im}\ \psi'_{\mathbf{h}_i} = 1$ and thus H is a finite index subgroup of $\mathrm{Im}\ \psi'_{\mathbf{h}_i}$. It follows that there exists an open subgroup U of $\mathcal{O}_K^\times$ such that $\psi_{\mathbf{h}_i}$ restricted to U has values in $\mathbb{Z}_p^\times$. By [Oz, 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 $\dim \ker \psi'_{\mathbf{h}_i} < d_K - 1$.

Now we fix an isomorphism $\iota\colon 1 + p^2\mathcal{O}_K \simeq \mathbb{Z}_p^{\oplus d_K}$ of topological groups. We define vector subspaces N and P_i of $\mathbb{Q}_p^{\oplus d_K}$ by $N := \iota(\ker \mathrm{Nr}'_{K/\mathbb{Q}_p}) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$ and $P_i := \iota(\ker \psi'_{\mathbf{h}_i}) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$. We know that $\dim_{\mathbb{Q}_p} N = d_K - 1$ and $\dim_{\mathbb{Q}_p} P_i < d_K - 1$. Assume that (2.2) does not hold, that is, $\ker \mathrm{Nr}'_{K/\mathbb{Q}_p} \subset \bigcup_{i=1}^r \ker \psi'_{\mathbf{h}_i}$. Then we have $N \subset \bigcup_{i=1}^r P_i$. This implies $N = \bigcup_{i=1}^r (N \cap P_i)$. By the lemma below, we find that $N = N \cap P_i \subset P_i$ 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 $W_1, \dots, W_r$ 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 $W_1 \not\subset \bigcup_{i=2}^{r+1} W_i$ and $W_{r+1} \not\subset \bigcup_{i=1}^{r} W_i$ holds. Then there exist elements $\mathbf{x}_1 \in W_1 \smallsetminus \bigcup_{i=2}^{r+1} W_i$ and $\mathbf{x}_{r+1} \in W_{r+1} \smallsetminus \bigcup_{i=1}^{r} W_i$. It is not difficult to check that we have $\lambda\mathbf{x}_1 + \mathbf{x}_{r+1} \notin W_1 \bigcup W_{r+1}$ for any $\lambda \in F^\times$. Hence there exists an integer $2 \le j_n \le r$ for each integer $n > 0$ such that $n\mathbf{x}_1 + \mathbf{x}_{r+1} \in W_{j_n}$. Take any integers $0 < \ell < k$ so that $j_\ell = j_k (=: j)$. Then $(k-\ell)\mathbf{x}_1 = (k\mathbf{x}_1 + \mathbf{x}_{r+1}) - (\ell\mathbf{x}_1 + \mathbf{x}_{r+1}) \in W_j$. Since F is of characteristic zero, we have $\mathbf{x}_1 \in W_j$ but this contradicts the fact that $\mathbf{x}_1 \notin \bigcup_{i=2}^{r+1} W_i$. Therefore, either $W_1 \subset \bigcup_{i=2}^{r+1} W_i$ or $W_{r+1} \subset \bigcup_{i=1}^{r} W_i$ 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*

$$\det(T - \varphi^{f_K} \mid D^K_{\mathrm{cris}}(H^i_{\text{ét}}(X_{\overline{K}}, \mathbb{Q}_p)) = \det(T - \mathrm{Frob}_K^{-1} \mid H^i_{\text{ét}}(X_{\overline{K}}, \mathbb{Q}_\ell))$$

for any prime $\ell \neq p$. Here, Frob_K *stands for the arithmetic Frobenius of K.*

[2] If a profinite group G has an open subgroup U which is isomorphic to $\mathbb{Z}_p^{\oplus d}$, then d does not depend on the choice of U and we say that d is the *dimension of* G. For example, $\dim \mathbb{Z}_p^{\oplus d} = d$. 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 $D^K_{\mathrm{cris}}(H^i_{\mathrm{\acute{e}t}}(X_{\overline{K}}, \mathbb{Q}_p)) \simeq K_0 \otimes_{W(\mathbb{F}_{q_K})} H^i_{\mathrm{cris}}(Y/W(\mathbb{F}_{q_K}))$ of φ-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 $K_0 \otimes_{W(\mathbb{F}_{q_K})} H^i_{\mathrm{cris}}(Y/W(\mathbb{F}_{q_K}))$ for the (f_K-iterate) Frobenius action coincides with $\det(T - \mathrm{Frob}_K^{-1} \mid H^i_{\mathrm{\acute{e}t}}(X_{\overline{K}}, \mathbb{Q}_\ell))$ for any prime $\ell \neq p$. Thus the result follows. □

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 [Si1, 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 semi-stable 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 $\mathrm{End}_K(A) \otimes_{\mathbb{Z}} \mathbb{Q}$ is a CM field of degree $2g$. Then we have*

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

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

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

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

$$H/H^{\chi_p(\sigma)-1} \twoheadrightarrow H/\overline{(G,G)} = \mathrm{Gal}(M_{\mathrm{ab}}/K(\mu_{p^\infty})) \quad \text{for any } \sigma \in G. \tag{2.4}$$

Let ν 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 $\mathrm{Gal}(M_{\mathrm{ab}}/K(\mu_{p^\infty}))$ is of exponent ν, that is, $\sigma \in G_{K(\mu_{p^\infty})}$ implies

$\sigma^\nu \in G_{M_{\rm ab}}$. Hence it follows from (2.3) that, for any point $P \in T$ such that its image $\bar{P}$ in T/p^nT is fixed by G_M, we have

$$\det(\rho(\sigma)^\nu - E)\iota(P) \in p^n\mathbb{Z}_p^{\oplus 2g} \quad \text{for any } \sigma \in G_{K(\mu_{p^\infty})}. \tag{2.5}$$

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

$$v_p(\det(\rho(\sigma_0)^\nu - E)) \leq C_0(K,g)$$

for some $\sigma_0 \in G_{K(\mu_{p^\infty})}$.

Admitting this claim, we can finish the proof of Proposition 8 immediately: It follows from Claim 1 and (2.5) that $(T/p^nT)^{G_M} \subset p^{n-C_0(K,g)}T/p^nT$ for $n > C_0(K,g)$. Setting $C(K,g)_p := p^{C_0(K,g)2g}$, we obtain $\sharp A(M)[p^n] = \sharp(T/p^nT)^{G_M} \leq \sharp(T/p^{C_0(K,g)}T) = C(K,g)_p$, which shows $\sharp A(M)[p^\infty] \leq C(K,g)_p$, On the other hand, we remark that Kubo and Taguchi showed in [KT, Lemma 2.3] that the residue field $\mathbb{F}_M$ of M is finite. The reduction map indues an injection from the prime-to-p part of $A(M)$ into $\overline{A}(\mathbb{F}_M)$ where $\overline{A}$ is the reduction of A. If we denote by q the order of $\mathbb{F}_M$, it follows from the Weil bound that $\sharp\overline{A}(\mathbb{F}_M) \leq (1+\sqrt{q})^{2g}$. Therefore, setting $C(K,g) := C(K,g)_p \cdot (1+\sqrt{q})^{2g}$, we conclude that $\sharp A(M)_{\rm tors} \leq C(K,g)$. 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 Hölder factor of $V \otimes_{\mathbb{Q}_p} \overline{\mathbb{Q}}_p$ is of dimension one. Let $\psi_1, \dots, \psi_{2g} \colon G_K \to \overline{\mathbb{Q}}_p^\times$ be the characters associated with the Jordan Hölder factors of $V \otimes_{\mathbb{Q}_p} \overline{\mathbb{Q}}_p$. Since K contains all p-adic fields of degree $\leq 2g$, we know that each ψ_i has values in $K^\times$ (in fact, for any $\sigma \in G_K$, we know that $\psi_1(\sigma), \dots, \psi_{2g}(\sigma)$ are the roots of the polynomial $\det(T - \sigma \mid V) \in \mathbb{Q}_p[T]$ of degree $2g$). In the rest of the proof, we regard ψ_i as a character $G_K \to K^\times$ of G_K with values in $K^\times$. We remark that each ψ_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 $\sigma \in G_{K(\mu_{p^\infty})}$. Hence it follows from Lemma 3 that we have

$$\begin{aligned} &\mathrm{Min}\left\{v_p(\det(\rho(\sigma)^\nu - E) \mid \sigma \in G_{K(\mu_{p^\infty})}\right\} \\ &\leq \mathrm{Min}\left\{\sum_{i=1}^{2g} v_p(\psi_{i,K}^\nu(p\omega)^{-1} - 1) \mid \omega \in \ker \mathrm{Nr}_{K/\mathbb{Q}_p}\right\}. \end{aligned} \tag{2.6}$$

Note that we have

$$\begin{aligned} \psi_{i,K}(p\omega)^{-1} &= \psi_{i,K}(\pi_K^{-e_K} \cdot \pi_K^{e_K} p^{-1}) \cdot \psi_{i,K}(\omega)^{-1} \\ &= \psi_{i,K}(\pi_K)^{-e_K}\psi_{i,\mathrm{alg}}(\pi_K^{e_K}p^{-1}) \cdot \psi_{i,K}(\omega)^{-1} \\ &= \alpha_i^{-e_K} \cdot \psi_{i,\mathrm{alg}}(p)^{-1} \cdot \psi_{i,K}(\omega)^{-1} \end{aligned} \tag{2.7}$$

for $\omega \in \ker \mathrm{Nr}_{K/\mathbb{Q}_p}$ where $\alpha_i := \psi_{i,K}(\pi_K)\psi_{i,\mathrm{alg}}(\pi_K)^{-1}$.

Lemma 9. *Let the notation be as above. Let $A^\vee$ be the dual abelian variety of A, and let $\overline{A}$ and $\overline{A^\vee}$ be the reductions of A and $A^\vee$, respectively.*
(1) *α_i is a root of the characteristic polynomial of the geometric Frobenius endomorphism of $\overline{A}_{/\mathbb{F}_K}$.*
(2) *$\alpha_i^{-1}q_K$ is a root of the characteristic polynomial of the geometric Frobenius endomorphism of $\overline{A^\vee}_{/\mathbb{F}_K}$.*

Proof. Since $K(\psi_i^{-1})$ is a subquotient of $V_p(A)^\vee \otimes_{\mathbb{Q}_p} K$, it follows from Proposition 4 that α_i is a root of the characteristic polynomial $f(T) := \det(T - \varphi^{f_K} \mid D^K_{\mathrm{cris}}(V_p(A)^\vee))$ of the K_0-linear endomorphism φ^{f_K}, the f_K-th iterate of the Frobenius φ, on the K_0-vector space $D^K_{\mathrm{cris}}(V_p(A)^\vee)$. We find that

$$\begin{aligned} f(T) &= \det(T - \varphi^{f_K} \mid D^K_{\mathrm{cris}}(H^1_{\text{ét}}(A_{\overline{K}}, \mathbb{Q}_p)) \\ &= \det(T - \mathrm{Frob}_K^{-1} \mid H^1_{\text{ét}}(A_{\overline{K}}, \mathbb{Q}_\ell) = \det(T - \mathrm{Frob}_K \mid V_\ell(\overline{A})) \end{aligned}$$

for any prime $\ell \neq p$ where Frob_K 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 $\overline{A}_{/\mathbb{F}_K}$. This shows (1). On the other hand, it follows from Proposition 4 again that α_i^{-1} is a root of $\det(T - \varphi^{f_K} \mid D^K_{\mathrm{cris}}(V_p(A)))$. Since $V_p(A)(-1) \simeq V_p(A^\vee)^\vee$, we see that $\alpha_i^{-1} q_K$ is a root of $f^\vee(T) := \det(T - \varphi^{f_K} \mid D^K_{\mathrm{cris}}(V_p(A^\vee)^\vee))$. Now the same argument of the proof of (1) with replacing A by $A^\vee$ gives a proof of (2). □

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

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

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

Consider the case $\mathbf{h}_i = (0)_{\sigma \in \Gamma_K}$. If this is the case, ψ_i is unramified. This implies that $\psi_{i,\mathrm{alg}}$ on ($\mathbb{Q}_p$-points) is trivial. Take any $\omega \in \ker \mathrm{Nr}_{K/\mathbb{Q}_p}$ and consider the p-adic value $v_p(\psi^\nu_{i,K}(p\omega)^{-1} - 1)$. By (2.7), we have

$$\psi^\nu_{i,K}(p\omega)^{-1} = \alpha_i^{-\nu e_K}. \tag{2.8}$$

We remark that the right hand side is independent of the choice of $\omega \in \ker \mathrm{Nr}_{K/\mathbb{Q}_p}$ and α_i must be a p-adic unit (since so is the left hand side). Next consider the case $\mathbf{h}_i = (1)_{\sigma \in \Gamma_K}$. If this is the case, we have $\psi_i = \chi_p$ on I_K, that is, $\psi_{i,\mathrm{alg}}$ (on $\mathbb{Q}_p$-points) is $\mathrm{Nr}^{-1}_{K/\mathbb{Q}_p}$. Take any $\omega \in \ker \mathrm{Nr}_{K/\mathbb{Q}_p}$ and consider the p-adic value $v_p(\psi^\nu_{i,K}(p\omega)^{-1} - 1)$. By (2.7), we have

$$\psi^\nu_{i,K}(p\omega)^{-1} = (\alpha_i^{-e_K} \cdot \mathrm{Nr}_{K/\mathbb{Q}_p}(p))^\nu = (\alpha_i^{-1} q_K)^{\nu e_K}. \tag{2.9}$$

We remark that the last term is independent of the choice of $\omega \in \ker \mathrm{Nr}_{K/\mathbb{Q}_p}$.

Suppose $r + 1 \leq i \leq 2g$. Let L be the unramified extension of K of degree νe_K. Denote by $f_i(T)$ the characteristic polynomial of the Frobenius endomorphism of $\overline{A}_{/\mathbb{F}_L}$ (resp. $\overline{A^\vee}_{/\mathbb{F}_L}$) if $\mathbf{h}_i = (0)_{\sigma \in \Gamma_K}$ (resp. $\mathbf{h}_i = (1)_{\sigma \in \Gamma_K}$). It follows from (2.8) (resp. (2.9)) and Lemma 9 that $\psi^\nu_{i,K}(p\omega)$ (resp. $\psi^\nu_{i,K}(p\omega)^{-1}$) is a unit root of $f_i(T)$. Since $f_i(1)$ coincides with $\sharp\overline{A}(\mathbb{F}_{q_L})$ (resp. $\sharp\overline{A^\vee}(\mathbb{F}_{q_L})$), we find $v_p(\psi^\nu_{i,K}(p\omega)^{-1} - 1) \leq v_p(f_i(1))$. It follows from the Weil bound that $f_i(1) \leq (1 + \sqrt{q_L})^{2g} \leq (1 + \sqrt{p}^{\nu d_K})^{2g}$, which gives an inequality $v_p(f_i(1)) \leq \log_p(1 + \sqrt{p}^{\nu d_K})^{2g}$. Therefore, setting $C_2(K, g) := \log_p(1 + \sqrt{p}^{\nu d_K})^{2g}$, we obtain

$$v_p(\psi^\nu_{i,K}(p\omega)^{-1} - 1) \leq C_2(K, g)$$

for $r + 1 \leq i \leq 2g$.

Suppose $1 \leq i \leq r$. We define a subset $\mathcal{R} = \mathcal{R}(K, g)$ of $\overline{\mathbb{Q}}_p$ by the set consisting of $\alpha \in \overline{\mathbb{Q}}_p$ 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 $\mathcal{R}' = \mathcal{R}'(K, g) := \{(\alpha^{-e_K} p^h)^\nu \mid \alpha \in \mathcal{R}, 0 < h < d_K\}$. Then, both $\mathcal{R}$ and $\mathcal{R}'$ are finite sets and depend only on K and g. Furthermore, Lemma 9 and the Weil Conjecture imply that each α_i is an element of $\mathcal{R}$. Thus, setting $\gamma_i := \alpha_i^{-e_K} \cdot \psi_{i,\mathrm{alg}}(p)^{-1} = \alpha_i^{-e_K} \cdot p^{\sum_{\sigma \in \Gamma_K} h_{i,\sigma}}$, we have $\gamma_i^\nu \in \mathcal{R}'$. We consider the continuous character $\psi_{\mathbf{h}_i} \colon \mathcal{O}_K^\times \to \mathcal{O}_K^\times$ defined in (2.1). The character $\psi_{i,\mathrm{alg}}$ (on $\mathbb{Q}_p$-points) restricted to $\mathcal{O}_K^\times$ coincides with $\psi_{\mathbf{h}_i}$. By Lemma 5, there exists an element $\omega = \omega(K; \mathbf{h}_1, \ldots \mathbf{h}_r)$ of $\ker \mathrm{Nr}_{K/\mathbb{Q}_p}$ such that $\psi^\nu_{\mathbf{h}_1}(\omega), \ldots, \psi^\nu_{\mathbf{h}_r}(\omega)$ are of infinite order. Since $\mathcal{R}'$ is finite, there exists an integer r such that $\psi^\nu_{\mathbf{h}_1}(\omega^r), \ldots, \psi^\nu_{\mathbf{h}_r}(\omega^r)$ are not contained in $\mathcal{R}'$. Putting $\omega_0 = \omega^r$, it holds that

- ω_0 is an element of $\ker \mathrm{Nr}_{K/\mathbb{Q}_p}$. Furthermore, ω_0 depends only on K, g and $\mathbf{h}_1, \dots, \mathbf{h}_r$, and
- $\psi^{\nu}_{\mathbf{h}_1}(\omega_0), \dots, \psi^{\nu}_{\mathbf{h}_r}(\omega_0)$ are not contained in $\mathcal{R}'$.

Now we define a constant $C(K, g, \mathbf{h}_1, \dots, \mathbf{h}_r)$ by

$$C(K, g, \mathbf{h}_1, \dots, \mathbf{h}_r) = \mathrm{Max}\left\{\sum_{i=1}^{r} v_p(\gamma'_i \psi^{\nu}_{\mathbf{h}_i}(\omega_0)^{-1} - 1) \mid \gamma'_i \in \mathcal{R}'\right\}.$$

By construction of ω_0, we see that the constant above is finite and depends only on $K, g, \mathbf{h}_1, \dots, \mathbf{h}_r$. We find that

$$\begin{aligned}
&\mathrm{Min}\left\{\sum_{i=1}^{2g} v_p(\psi^{\nu}_{i,K}(p\omega)^{-1} - 1) \mid \omega \in \ker \mathrm{Nr}_{K/\mathbb{Q}_p}\right\} \\
\leq &\sum_{i=1}^{2g} v_p(\psi^{\nu}_{i,K}(p\omega_0)^{-1} - 1) = \sum_{i=1}^{r} v_p(\gamma^{\nu}_i \psi^{\nu}_{\mathbf{h}_i}(\omega_0)^{-1} - 1) + \sum_{i=r+1}^{2g} v_p(\psi^{\nu}_{i,K}(p\omega_0)^{-1} - 1) \\
\leq &C(K, g, \mathbf{h}_1, \dots, \mathbf{h}_r) + (2g - r)C_2(K, g) \leq C_0(K, g). \qquad (2.10)
\end{aligned}$$

Here,

$$C_0(K, g) := \mathrm{Max}\,\{C(K, g, \mathbf{h}_1, \dots, \mathbf{h}_r) + (2g - r)C_2(K, g) \mid 0 \leq r \leq 2g,\ \mathbf{h}_1, \dots, \mathbf{h}_r : \text{Case (I)}\}$$

(if $r = 0$, we consider the constant $C(K, g, \mathbf{h}_1, \dots, \mathbf{h}_r)$ as zero). By construction, the constant $C_0(K, g)$ is finite and depends only on K and g. By (2.6) and (2.10), we conclude that $C_0(K, g)$ defined here satisfies the desired property of Claim 1. This is the end of the proof of Proposition 8. □

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 π_n a p^n-th root of π such that $\pi_{n+1}^p = \pi_n$ for any $n \geq 0$. We set $K_\infty := K(\pi_n \mid n \geq 0)$. The field K_∞ is clearly a subfield of $K(\sqrt[p^\infty]{K})$. It is well-known that K_∞ is one of key ingredients in (integral) p-adic Hodge theory since K_∞ is familiar to the theory of norm fields. We can check the equality

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

holds for any abelain 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 $A(\overline{K})_{\mathrm{tors}}$. Since K_∞ is totally ramified over K, we obtain the fact that the prime-to-p parts of $A(K)_{\mathrm{tors}}$ and $A(K_\infty)_{\mathrm{tors}}$ coincide with each other. On the other hand, we consider the following natural maps.

$$A(K)[p^n] \simeq \mathrm{Hom}_{G_K}(\mathbb{Z}/p^n\mathbb{Z}, A(\overline{K})[p^n]) \overset{\iota}{\hookrightarrow} \mathrm{Hom}_{G_{K_\infty}}(\mathbb{Z}/p^n\mathbb{Z}, A(\overline{K})[p^n]) \simeq A(K_\infty)[p^n]$$

Since A has good reduction, the injection ι above is bijective (cf. [Br, Theorem 3.4.3] for $p > 2$; [Ki], [La], [Li] 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

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

for any abelain 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 Théroie 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. Nakkajima, *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 nombress*, 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.