Explicit bounds on torsion of CM abelian varieties over p-adic fields with values in Lubin-Tate extensions

Yoshiyasu Ozeki*

September 11, 2023

Abstract

Let K and k be p-adic fields. Let L be the composite field of K and a certain Lubin-Tate extension over k (including the case where $L = K(\mu_{p^\infty})$). In this paper, we show that there exists an explicitly described constant C, depending only on K, k and an integer $g \geq 1$, which satisfies the following property: If $A_{/K}$ is a g-dimensional CM abelian variety, then the order of the p-torsion subgroup of $A(L)$ is bounded by C. We also give a similar bound in the case where $L = K(\sqrt[p^\infty]{K})$. Applying our results, we study bounds of orders of torsion subgroups of some CM abelian varieties over number fields with values in full cyclotomic fields.

1 Introduction

Let p be a prime number and K a p-adic field (= a finite extension of $\mathbb{Q}_p$). It is a theorem of Mattuck [Mat] that, for a g-dimensional abelian variety A over K and a finite extension L/K, the Mordell-Weil group $A(L)$ is isomorphic to the direct sum of $\mathbb{Z}_p^{\oplus g\cdot[L:\mathbb{Q}_p]}$ and a finite group. Our interest is to study various information about the torsion subgroup $A(L)_{\rm tor}$ of $A(L)$. For this, Clark and Xarles [CX] gave an explicit upper bound of the order of $A(L)_{\rm tor}$ of $A(L)$ in terms of p, g and some numerical invariants of L if A has anisotropic reduction. This includes the case where A has potential good reduction and in this case the existence of a bound can be found in some literatures (cf. [Si2], [Si3]). We consider the case where L/K is *of infinite degree*. There are some situations in which the torsion part $A(L)_{\rm tor}$ is finite. Suppose that A has potential good reduction. It is a theorem of Imai [Im] that $A(K(\mu_{p^\infty}))_{\rm tor}$ is finite. Here, $K(\mu_{p^\infty})$ is the extension field of K obtained by adjoining all p-power roots of unity. Moreover, Kubo and Taguchi showed in [KT] that $A(K(\sqrt[p^\infty]{K}))_{\rm tor}$ is also finite where $K(\sqrt[p^\infty]{K})$ is the extension field of K obtained by adjoining all p-power roots of all elements of K. The author showed in [Oz2] that there exists a "uniform" and "theoretical" bound of the order of $A(K(\sqrt[p^\infty]{K}))_{\rm tor}$ under the assumption that A has complex multiplication. (Here we say that A has complex multiplication if there exists a ring homomorphism $F \to \mathbb{Q} \otimes_{\mathbb{Z}} {\rm End}_{\overline{K}} A$ for some algebraic number field F of degree $2g$.)

The main purpose of this paper is to give explicit upper bounds of the orders of $A(K(\mu_{p^\infty}))_{\rm tor}$ and $A(K(\sqrt[p^\infty]{K}))_{\rm tor}$ for abelian varieties A/K with complex multiplication. For this, we should note that to give an upper bound of the order of the prime-to-p part of $A(K(\mu_{p^\infty}))_{\rm tor}$ is not so difficult. In fact, the reduction map gives an injection from the prime-to-p part of the group which we want to study into certain rational points of the reduction $\bar{A}$ of A (if A has good reduction), and the order of the target is bounded by the Weil bound. Hence the essential obstruction for our purpose appears in a study of the p-part $A(K(\mu_{p^\infty}))[p^\infty]$ of $A(K(\mu_{p^\infty}))_{\rm tor}$.

Let us state our main results. For a p-adic field k and a uniformizer π of k, we denote by k_π/k the Lubin-Tate extension associated with π (that is, k_π is the extension field of k obtained

*Faculty of Science, Kanagawa University, 3-27-1 Rokkakubashi, Kanagawa-ku, Yokohama-shi, Kanagawa 221-8686, JAPAN
e-mail: ozeki@kanagawa-u.ac.jp

by adjoining all π-power torsion points of the Lubin-Tate formal group associated with π). For example, we have $k_\pi = \mathbb{Q}_p(\mu_{p^\infty})$ if $k = \mathbb{Q}_p$ and $\pi = p$. We set $d_L := [L : \mathbb{Q}_p]$ for any p-adic field L. For any integer $n > 0$, we set

$$\Phi(n) := \mathrm{Max}\{m \in \mathbb{Z} \mid \varphi(m) \text{ divides } 2n\},$$
$$H(n) := \gcd\{\sharp \mathrm{GSp}_{2n}(\mathbb{Z}/N\mathbb{Z}) \mid N \geq 3\}.$$

Here, φ is the Euler's totient function. There are some upper bounds related with $H(n)$ and $\Phi(n)$ (see Section 5). It is a theorem of Silverberg [Si1] that we have $H(n) < 2(9n)^{2n}$ for any $n > 0$. It follows from elementary arguments that we have $\Phi(n) < 6n\sqrt[3]{n}$ for $n > 1$. Furthermore, a lower bound (5.3) of φ proved by Rosser and Schoenfeld [RS] gives $\Phi(n) < 4n \log\log n$ for $n > 3^{3^9}$.

Theorem 1.1 (= a special case of Theorem 3.1)**.** *Let $g > 0$ be a positive integer. Let k be a p-adic field with residue cardinality q_k and π a uniformizer of k. Assume the following conditions.*

(i) *$q_k^{-1}\mathrm{Nr}_{k/\mathbb{Q}_p}(\pi)$ is a root of unity[1]; we denote by $0 < \mu < p$ the minimum integer so that $(q_k^{-1}\mathrm{Nr}_{k/\mathbb{Q}_p}(\pi))^\mu = 1$, and*

(ii) *d_k is prime to $(2g)!$.*

Then, for any g-dimensional abelian variety A over a p-adic field K with complex multiplication, we have

$$A(Kk_\pi)[p^\infty] \subset A[p^C]$$

where

$$C := 2g^2 \cdot (2g)! \cdot \Phi(g)H(g) \cdot \mu \cdot d_{Kk} + 12g^2 - 18g + 10.$$

In particular, we have

$$\sharp A(Kk_\pi)[p^\infty] \leq p^{2gC}.$$

As an immediate consequence of the theorem above, we obtain a result for cyclotomic extensions; see Corollary 3.7. Furthermore, the method of our proof of Theorem 1.1 can be applied to the filed $K(\sqrt[p^\infty]{K})$ discussed in Kubo and Taguchi, which gives a refinement of the main theorem of [Oz2].

Theorem 1.2. *Let $g > 0$ be a positive integer. For any g-dimensional abelian variety A over a p-adic field K with complex multiplication, we have*

$$A(K(\sqrt[p^\infty]{K}))[p^\infty] \subset A[p^C]$$

where

$$C := 2g^2 \cdot (2g)! \cdot p^{1+v_p(2)} \cdot (\Phi(g)H(g))^2 \cdot p^{v_p(d_K)} d_K + 12g^2 - 18g + 10.$$

(Here, v_p is the p-adic valuation normalized by $v_p(p) = 1$.) In particular, we have

$$\sharp A(K(\sqrt[p^\infty]{K}))[p^\infty] \leq p^{2gC}.$$

We can consider some further topics. For example, we do not know what will happen if we remove the CM assumption from above theorems. Our proofs in this paper deeply depend on the theory of locally algebraic representations, which can be adapted only for abelian representations. This is the main reason why we can not remove the CM assumption form our arguments. To overcome this obstruction, it seems to be helpful for us to study the case of (not necessary CM) elliptic curves. We will study this case as a future work. We are also interested in giving the list of the groups that appears as $A(Kk_\pi)[p^\infty]$ or $A(K(\sqrt[p^\infty]{K}))[p^\infty]$. However, this should be quite difficult; the author does not know such classification results even for $A(K)[p^\infty]$.

Combining the cyclotomic case of Theorem 1.1 and Ribet's arguments in [KL], we can obtain a result on a bound of the order of the torsion subgroup of some CM abelian variety defined over a number field with values in full cyclotomic fields. (Here, a number field is a finite extension of $\mathbb{Q}$.)

[1] This condition is equivalent to say that some finite extension of k_π contains $\mathbb{Q}_p(\mu_{p^\infty})$ (cf. [Oz1, Lemma 2.7 (2)]).

Theorem 1.3. *Let $g > 0$ be an integer. Let K be a number field of degree d and denote by h the narrow class number of K. Let $K(\mu_\infty)$ be the field obtained by adjoining to K all roots of unity. Let A be a g-dimensional abelian variety over K with complex multiplication which has good reduction everywhere. Then, we have*

$$A(K(\mu_\infty))_{\mathrm{tor}} \subset A[N]$$

where

$$N := \left(\prod_p p\right)^{2g^2\cdot(2g)!\cdot\Phi(g)H(g)\cdot dh+12g^2-18g+10}.$$

Here, p ranges over the prime numbers such that either $p \le (1+\sqrt{2}^{dh})^{2g}$ or p is ramified in K.

We should note that Chou gave in [Ch] the complete list of the groups that appears as $A(\mathbb{Q}(\mu_\infty))_{\mathrm{tor}}$ as A ranges over all elliptic curves defined over $\mathbb{Q}$. For CM elliptic curves A over a number field K, more precise observations for the order of $A(K(\mu_\infty))_{\mathrm{tor}}$ than ours are studied in [CCM].

Acknowledgments. The author would like to thank Yuichiro Taguchi for useful discussion and correspondence to the proof of our main results. The author would like to thank Manabu Yoshida for giving us various advice on an earlier draft. Thanks also are due to Takaichi Fujiwara for helpful advice on functions discussed in Section 5. This work is supported by JSPS KAKENHI Grant Number JP19K03433.

Notation : For any perfect field F, we denote by G_F the absolute Galois group of F. In this paper, a p-adic field is a finite extension of $\mathbb{Q}_p$. If F is an algebraic extension of $\mathbb{Q}_p$, we denote by $\mathcal{O}_F$ and $\mathbf{m}_F$ the ring of integers of F and its maximal ideal, respectively. We also denote by F^{ab} the maximal abelian extension of F (in a fixed algebraic closure of F). We put $d_F = [F : \mathbb{Q}_p]$ if F is a p-adic field. 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 $q_F := p^{f_F}$. Finally, we denote by Γ_F the set of $\mathbb{Q}_p$-algebra embeddings of F into a (fixed) algebraic closure $\overline{\mathbb{Q}}_p$ of $\mathbb{Q}_p$.

.

2 Evaluations of some p-adic valuations for characters

We fix an algebraic closure $\overline{\mathbb{Q}}_p$ of $\mathbb{Q}_p$. Throughout this section, we assume that all p-adic fields are subfields of $\overline{\mathbb{Q}}_p$. Denote by v_p the p-adic valuation normalized by $v_p(p) = 1$. For any continuous character ψ of G_K, we often regard ψ 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 $\psi_K := \psi \circ \mathrm{Art}_K$. We denote by $\widehat{K}^\times$ the profinite completion of $K^\times$. Note that the local Artin map induces a topological isomorphism $\mathrm{Art}_K \colon \widehat{K}^\times \xrightarrow{\sim} \mathrm{Gal}(K^{\mathrm{ab}}/K)$. For a uniformizer π_K of K , we denote by $\chi_{\pi_K} \colon G_K \to \mathcal{O}_K^\times$ the Lubin-Tate character associated with π_K. By definition, the character χ_{π_K} is characterized by $\chi_{\pi_K,K}(\pi_K) = 1$ and $\chi_{\pi_K,K}(x) = x^{-1}$ for any $x \in \mathcal{O}_K^\times$. Let π be a uniformizer of k and denote by k_π the Lubin-Tate extension of k associated with π. The field corresponding to the kernel of the Lubin-Tate character $\chi_\pi \colon G_k \to \mathcal{O}_k^\times$ is k_π, and k_π is a totally ramified abelian extension of k.

Proposition 2.1. *Let $\psi_1, \dots, \psi_n \colon G_K \to M^\times$ be continuous characters. Then we have*

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

Proof. This is Proposition 3 of [Oz2] but we include a proof here for the sake of completeness. Let M be the maximal unramified extension of k contained in Kk. The group $\mathrm{Art}_k^{-1}(\mathrm{Gal}(k^{\mathrm{ab}}/M))$ contains $\mathrm{Art}_k^{-1}(\mathrm{Gal}(k^{\mathrm{ab}}/k^{\mathrm{ur}})) = \mathcal{O}_k^\times$. Furthermore, $\mathrm{Art}_k^{-1}(\mathrm{Gal}(k^{\mathrm{ab}}/M))$ is a subgroup of $\widehat{k}^\times = \pi^{\widehat{\mathbb{Z}}} \times \mathcal{O}_k^\times$ of index $[M:k] = f_{Kk/k}$. Thus it holds that $\mathrm{Art}_k^{-1}(\mathrm{Gal}(k^{\mathrm{ab}}/M)) = \pi^{f_{Kk/k}\widehat{\mathbb{Z}}} \times \mathcal{O}_k^\times$. Since we have $\mathrm{Art}_k^{-1}(\mathrm{Gal}(k^{\mathrm{ab}}/k_\pi)) = \pi^{\widehat{\mathbb{Z}}}$, we obtain $\mathrm{Art}_k^{-1}(\mathrm{Gal}(k^{\mathrm{ab}}/Mk_\pi)) = \pi^{f_{Kk/k}\widehat{\mathbb{Z}}}$. If we denote by $\mathrm{Res}_{Kk/k}$ the natural restriction map from $\mathrm{Gal}((Kk)^{\mathrm{ab}}/Kk)$ to $\mathrm{Gal}(k^{\mathrm{ab}}/k)$, it is not difficult to check $\mathrm{Res}^{-1}_{Kk/k}(\mathrm{Gal}(k^{\mathrm{ab}}/Mk_\pi)) = \mathrm{Gal}((Kk)^{\mathrm{ab}}/Kk_\pi)$. Thus we find $\mathrm{Art}^{-1}_{Kk}(\mathrm{Gal}((Kk)^{\mathrm{ab}}/Kk_\pi)) = \mathrm{Nr}^{-1}_{Kk/k}(\pi^{f_{Kk/k}\widehat{\mathbb{Z}}})$. Now the lemma follows from

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

□

We recall an observation of Conrad. We denote by K_0 the maximal unramified extension of $\mathbb{Q}_p$ contained in K and set $D^K_{\mathrm{cris}}(*) := (B_{\mathrm{cris}} \otimes_{\mathbb{Q}_p} *)^{G_K}$. We denote by $\underline{K}^\times$ the Weil restriction $\mathrm{Res}_{K/\mathbb{Q}_p}(\mathbb{G}_m)$.

Proposition 2.2. *Let $\psi \colon G_K \to M^\times$ be a continuous character.*
(1) $M(\psi)$ is crystalline if and only if there exists a (necessarily unique) $\mathbb{Q}_p$-homomorphism $\psi_{\mathrm{alg}} \colon \underline{K}^\times \to \underline{M}^\times$ such that ψ_K and ψ_{alg} (on $\mathbb{Q}_p$-points) coincides on $\mathcal{O}_K^\times (\subset \underline{K}^\times(\mathbb{Q}_p))$.
(2) Assume that $M(\psi)$ is crystalline and let ψ_{alg} be as in (1). (Note that $M(\psi^{-1})$ is also crystalline.) Then, the filtered φ-module $D^K_{\mathrm{cris}}(M(\psi^{-1})) = (B_{\mathrm{cris}} \otimes_{\mathbb{Q}_p} M(\psi^{-1}))^{G_K}$ over K is free of rank 1 over $K_0 \otimes_{\mathbb{Q}_p} M$ and its K_0-linear endomorphism φ^{f_K} is given by the action of the product $\psi_K(\pi_K)\cdot\psi^{-1}_{\mathrm{alg}}(\pi_K) \in M^\times$. Here, π_K is any uniformizer of K.

Proof. This is Proposition B.4 of [Co]. □

Let $\psi \colon G_K \to M^\times$ be a crystalline character. For any $\sigma \in \Gamma_M$, let $\chi_{\sigma M} \colon I_{\sigma M} \to \sigma M^\times$ be the restriction to the inertia $I_{\sigma M}$ of the Lubin-Tate character associated with any choice of uniformizer of σM (it depends on the choice of a uniformizer of σM, but its restriction to the inertia subgroup does not). Assume that K contains the Galois Closure of $M/\mathbb{Q}_p$. Then, we have

$$\psi = \prod_{\sigma\in\Gamma_M} \sigma^{-1}\circ \chi^{h_\sigma}_{\sigma M}$$

on the inertia I_K for some integer h_σ. Equivalently, the character ψ_{alg} on $\mathbb{Q}_p$-points coincides with $\prod_{\sigma\in\Gamma_M}\sigma^{-1}\circ \mathrm{Nr}^{-h_\sigma}_{K/\sigma M}$. Note that $\{h_\sigma \mid \sigma \in \Gamma_M\}$ is the set of Hodge-Tate weights of $M(\psi)$, that is, $C \otimes_{\mathbb{Q}_p} M(\psi) \simeq \oplus_{\sigma\in\Gamma_M} C(h_\sigma)$ where C is the completion of $\overline{\mathbb{Q}}_p$.

For integers d, h and a p-adic field M, we define a constant $C(d,M,h)$ by

$$C(d,M,h) := v_p(d/d_M) + h + \frac{d_M}{2}\left(d_M + v_p(e_M) - \frac{1}{e_M} + v_p(2)(d_M-1)\right). \tag{2.1}$$

Theorem 2.3. *Let $\psi_1, \dots, \psi_n \colon G_K \to M^\times$ be crystalline characters and $h \geq 0$ an integer. Assume that M is a Galois extension of $\mathbb{Q}_p$ and K contains M. Suppose that, for each i, we have*

$$\psi_i = \prod_{\sigma \in \Gamma_M} \sigma^{-1} \circ \chi_M^{h_{i,\sigma}}$$

on the inertia I_K; thus $\{h_{i,\sigma} \mid \sigma \in \Gamma_M\}$ is the Hodge-Tate weights of $M(\psi_i)$. We assume the following conditions.

(i) *$\{h_{i,\sigma} \mid \sigma \in \Gamma_M\}$ contains at least two different integers for each i. (In particular, we have $M \neq \mathbb{Q}_p$.)*

(ii) *We have $\mathrm{Min}\,\{v_p(h_{i,\sigma} - h_{i,\tau}) \mid \sigma, \tau \in \Gamma_M\} \leq h$ for each i.*

(1) *There exists an element $\hat{\omega} \in \ker \mathrm{Nr}_{M/\mathbb{Q}_p}$ with the property that, for every $1 \leq i \leq n$, it holds that*

$$1 + v_p(2) \leq v_p(\psi_{i,K}(\hat{\omega})^{-1} - 1) \leq \delta_{(i)} + C(d_K, M, h). \tag{2.2}$$

Here,

$$\delta_{(i)} := \begin{cases} 0 & \text{if } i = 1, 2, \\ 2i - 5 & \text{if } i \geq 3. \end{cases}$$

(2) *Let $\hat{\omega}$ be as in (1). For any $x \in K^\times$, there exists an integer $0 \leq s(x) \leq n$ with the property that, for every $1 \leq i \leq n$, it holds that*

$$v_p(\psi_{i,K}(x\hat{\omega}^{p^{s(x)}})^{-1} - 1) \leq n + \delta_{(i)} + C(d_K, M, h). \tag{2.3}$$

Proof. Take an element $x \in \mathcal{O}_M$ such that $\mathcal{O}_M = \mathbb{Z}_p[x]$. We set $p' := p$ or $p' := 4$ if $p \neq 2$ or $p = 2$, respectively, and put $x' = p'x$. Set $m_{r,\sigma}^{\tau} := d_{K/M}(h_{r,\tau\sigma} - h_{r,\sigma})$ for $1 \leq r \leq n$ and $\sigma, \tau \in \Gamma_M$. We also set

$$y_{r,\ell}^{\tau} := \sum_{\sigma \in \Gamma_M} m_{r,\sigma}^{\tau} (\sigma^{-1} x')^{\ell - 1}$$

for $1 \leq \ell \leq d_M$. (Note that $y_{r,1}^{\tau} = 0$.) Set

$$\omega_\ell := \exp((x')^{\ell-1}) \quad \text{and} \quad \omega_\ell^{\tau} := \frac{\tau\omega_\ell}{\omega_\ell}$$

for any $1 \leq \ell \leq d_M$ and $\tau \in \Gamma_M$. It holds $\omega_\ell^{\tau} \in \ker \mathrm{Nr}_{M/\mathbb{Q}_p}$ by construction.

Lemma 2.4. *We have $\exp(y_{r,\ell}^{\tau}) = \psi_{r,K}(\omega_\ell^{\tau})^{-1}$.*

Proof. We see

$$\psi_{r,K}(\omega_\ell)^{-1} = \prod_{\sigma \in \Gamma_M} \sigma^{-1} \circ \mathrm{Nr}_{K/M}(\omega_\ell)^{h_{r,\sigma}} = \left(\prod_{\sigma \in \Gamma_M} \sigma^{-1} \omega_\ell^{h_{r,\sigma}} \right)^{d_{K/M}}.$$

We also have $\psi_{r,K}(\tau\omega_\ell)^{-1} = \left(\prod_{\sigma \in \Gamma_M} \sigma^{-1} \tau \omega_\ell^{h_{r,\sigma}}\right)^{d_{K/M}} = \left(\prod_{\sigma \in \Gamma_M} \sigma^{-1} \omega_\ell^{h_{r,\tau\sigma}}\right)^{d_{K/M}}$. Thus we have

$$\psi_{r,K}(\omega_\ell^{\tau})^{-1} = \left(\prod_{\sigma \in \Gamma_M} \sigma^{-1} \omega_\ell^{h_{r,\tau\sigma} - h_{r,\sigma}} \right)^{d_{K/M}} = \prod_{\sigma \in \Gamma_M} \sigma^{-1} \omega_\ell^{m_{r,\sigma}^{\tau}}.$$

On the other hand, we have

$$\exp(y_{r,\ell}^{\tau}) = \exp\left(\sum_{\sigma \in \Gamma_M} m_{r,\sigma}^{\tau} (\sigma^{-1} x')^{\ell-1} \right) = \prod_{\sigma \in \Gamma_M} \exp((\sigma^{-1} x')^{\ell-1})^{m_{r,\sigma}^{\tau}} = \prod_{\sigma \in \Gamma_M} \sigma^{-1} \omega_\ell^{m_{r,\sigma}^{\tau}}.$$

Thus we obtain the lemma. □

We furthermore need the following evaluation.

Lemma 2.5. *For each $1 \le r \le n$, there exist $\tau_r \in \Gamma_M$ and an integer $2 \le \ell_r \le d_M$ such that*

$$v_p(y^{\tau_r}_{r,\ell_r}) \le C(d_K, M, h).$$

Proof. In this proof, we fix r. By the assumption (i), there exist $\tau_1, \tau_2 \in \Gamma_M$ such that $h_{r,\tau_1} \neq h_{r,\tau_2}$. We choose such τ_1 and τ_2 so that $v_p(h_{r,\tau_1} - h_{r,\tau_2}) = \mathrm{Min}\,\{v_p(h_{r,\sigma} - h_{r,\tau}) \mid \sigma, \tau \in \Gamma_M\}$. Set $\tau := \tau_2\tau_1^{-1} \in \Gamma_M$. We write $\Gamma_M = \{\tau_1, \tau_2, \dots, \tau_{d_M}\}$. Note that $m^{\tau}_{r,\tau_1} = d_{K/M}(h_{r,\tau_2} - h_{r,\tau_1})$ is not zero. We denote by $X \in M_d(\mathcal{O}_M)$ the matrix whose (i,j)-component is $(\tau_i^{-1}x')^{j-1}$. Then we have

$$\begin{pmatrix} y^{\tau}_{r,1} & \cdots & y^{\tau}_{r,d_M} \end{pmatrix} = \begin{pmatrix} m^{\tau}_{r,\tau_1} & \cdots & m^{\tau}_{r,\tau_{d_M}} \end{pmatrix} X \tag{2.4}$$

and the determinant $\det X$ of X is $\prod_{1\le i<j\le d_M}(\tau_j^{-1}x' - \tau_i^{-1}x') = (p')^{\frac{d_M(d_M-1)}{2}} \prod_{1\le i<j\le d_M}(\tau_j^{-1}x - \tau_i^{-1}x)$. We also have

$$\begin{aligned} v_p\left(\prod_{1\le i<j\le d_M}(\tau_j^{-1}x - \tau_i^{-1}x)\right) &= \sum_{1\le i<j\le d_M} v_p\left(\tau_j^{-1}x - \tau_i^{-1}x\right) \\ &= \frac{1}{2}\sum_{1\le i,j\le d_M, i\neq j} v_p\left(\tau_j^{-1}x - \tau_i^{-1}x\right) \\ &= \frac{d_M}{2} v_p(\mathcal{D}_{M/\mathbb{Q}_p}) \le \frac{d_M}{2}\left(1 + v_p(e_M) - \frac{1}{e_M}\right). \end{aligned}$$

(cf. [Se, Chapter 3, Section 6, Proposition 13]), where $\mathcal{D}_{M/\mathbb{Q}_p}$ is the differential of $M/\mathbb{Q}_p$. We find

$$v_p(\det X) \le \frac{d_M}{2}\left(d_M + v_p(e_M) - \frac{1}{e_M} + v_p(2)(d_M - 1)\right). \tag{2.5}$$

By (2.4), we have $m^{\tau}_{r,\tau_1}\det X = \sum_{\ell=1}^{d_M} y^{\tau}_{r,\ell}x_\ell$ for some $x_\ell \in \mathcal{O}_M$, which gives the fact that there exists an integer $\ell_r = \ell$ with the property that $v_p(y^{\tau}_{r,\ell}) \le v_p(m^{\tau}_{r,\tau_1}\det X)$. By (2.5), we have

$$v_p(y^{\tau}_{r,\ell}) \le v_p(d_{K/M}) + v_p(h_{r,\tau_1} - h_{r,\tau_2}) + v_p(\det X) \le C(d_K, M, h)$$

as desired. We remark that ℓ is not equal to 1 since $y^{\tau}_{r,1}$ is zero. □

Now we return to the proof of Theorem 2.3. Take τ_r and ℓ_r as in Lemma 2.5 with the additional condition that

$$v_p(y^{\tau_r}_{r,\ell_r}) = \mathrm{Min}\{v_p(y^{\tau}_{r,\ell}) \mid \tau \in \Gamma_M, 2 \le \ell \le d_M\}. \tag{2.6}$$

Here we consider an element $\hat{\omega} \in \ker \mathrm{Nr}_{M/\mathbb{Q}_p}$ which is of the form $\hat{\omega} = \prod_{r=1}^{n}(\omega^{\tau_r}_{\ell_r})^{s_r}$, where s_r is defined inductively by the following.

$$(s_1, s_2) = \begin{cases} (0,1) & \text{if } v_p(y^{\tau_1}_{1,\ell_1}) = v_p(y^{\tau_2}_{1,\ell_2}), \\ (1,0) & \text{if } v_p(y^{\tau_1}_{1,\ell_1}) \neq v_p(y^{\tau_2}_{1,\ell_2}) \text{ and } v_p(y^{\tau_1}_{2,\ell_1}) = v_p(y^{\tau_2}_{2,\ell_2}), \\ (1,1) & \text{if } v_p(y^{\tau_1}_{1,\ell_1}) \neq v_p(y^{\tau_2}_{1,\ell_2}) \text{ and } v_p(y^{\tau_1}_{2,\ell_1}) \neq v_p(y^{\tau_2}_{2,\ell_2}). \end{cases}$$

$$s_3 = \begin{cases} p & \text{if } v_p(s_1 y^{\tau_1}_{3,\ell_1} + s_2 y^{\tau_2}_{3,\ell_2}) \neq v_p(p y^{\tau_3}_{3,\ell_3}), \\ p^2 & \text{if } v_p(s_1 y^{\tau_1}_{3,\ell_1} + s_2 y^{\tau_2}_{3,\ell_2}) = v_p(p y^{\tau_3}_{3,\ell_3}). \end{cases}$$

For $r \ge 4$,

$$s_r = \begin{cases} p s_{r-1} & \text{if } v_p(\sum_{j=1}^{r-1} s_j y^{\tau_j}_{r,\ell_j}) \neq v_p(p s_{r-1} y^{\tau_r}_{r,\ell_r}), \\ p^2 s_{r-1} & \text{if } v_p(\sum_{j=1}^{r-1} s_j y^{\tau_j}_{r,\ell_j}) = v_p(p s_{r-1} y^{\tau_r}_{r,\ell_r}). \end{cases}$$

We calim that we have

$$1+v_p(2)\le v_p\left(\sum_{r=1}^{n} s_r y_{i,\ell_r}^{\tau_r}\right)\le \delta_{(i)}+C(d_K,M,h)$$

for any i, where $\delta_{(i)}$ is as in the statement (1). The inequality $1+v_p(2)\le v_p\left(\sum_{r=1}^{n} s_r y_{i,\ell_r}^{\tau_r}\right)$ is clear since we always have $1+v_p(2)\le v_p(y_{i,\ell}^{\tau})$ by definition of $y_{i,\ell}^{\tau}$. We show $v_p\left(\sum_{r=1}^{n} s_r y_{i,\ell_r}^{\tau_r}\right)\le \delta_{(i)}+C(d_K,M,h)$ by induction on i.

- Suppose either $i=1$ or $i=2$. By (2.6) and the inequality $0<v_p(s_r)$ for $r\ge 3$, it is not difficult to check $v_p\left(\sum_{r=1}^{n} s_r y_{i,\ell_r}^{\tau_r}\right)=v_p(y_{i,\ell_i}^{\tau_i})$. Furthermore, we have $v_p(y_{i,\ell_i}^{\tau_i})\le C(d_K,M,h)=\delta_{(i)}+C(d_K,M,h)$ by Lemma 2.5.
- Suppose $i\ge 3$. By definition of s_i we have $v_p\left(\sum_{r=1}^{i-1} s_r y_{i,\ell_r}^{\tau_r}\right)\ne v_p(s_i y_{i,\ell_i}^{\tau_i})$. We also have $v_p\left(\sum_{r=i}^{n} s_r y_{i,\ell_r}^{\tau_r}\right)=v_p(s_i y_{i,\ell_i}^{\tau_i})$ since $v_p(s_i y_{i,\ell_i}^{\tau_i})<v_p(s_r y_{i,\ell_r}^{\tau_r})$ for $i<r$. Hence, it follows from Lemma 2.5 that we have

$$\begin{aligned} v_p\left(\sum_{r=1}^{n} s_r y_{i,\ell_r}^{\tau_r}\right) &= \mathrm{Min}\left\{v_p\left(\sum_{r=1}^{i-1} s_r y_{i,\ell_r}^{\tau_r}\right), v_p(s_i y_{i,\ell_i}^{\tau_i})\right\}\\ &\le v_p(ps_{i-1}y_{i,\ell_i}^{\tau_i})\le 1+v_p(s_{i-1})+C(d_K,M,h)\end{aligned}$$

  if $i\ge 4$. Since we have $v_p(s_{i-1})\le 2(i-3)$ if $i\ge 4$, the claim for $i\ge 4$ follows. The claim for $i=3$ follows by a similar manner; we have $v_p\left(\sum_{r=1}^{n} s_r y_{3,\ell_r}^{\tau_r}\right)\le v_p(py_{3,\ell_3}^{\tau_3})\le 1+C(d_K,M,h)=\delta_{(3)}+C(d_K,M,h)$.

By construction of $\hat{\omega}$ and Lemma 2.4, we see

$$\psi_{i,K}(\hat{\omega})^{-1}=\prod_{r=1}^{n}\psi_{i,K}(\omega_{\ell_r}^{\tau_r})^{-s_r}=\prod_{r=1}^{n}\exp\left(s_r y_{i,\ell_r}^{\tau_r}\right)=\exp\left(\sum_{r=1}^{n} s_r y_{i,\ell_r}^{\tau_r}\right).$$

Thus we find $v_p(\psi_{i,K}(\hat{\omega})^{-1}-1)=v_p\left(\sum_{r=1}^{n} s_r y_{i,\ell_r}^{\tau_r}\right)$. Therefore, the claim above gives the statement (1) of Theorem (2.3).

We show (2). We set $m_i:=\psi_{i,K}(x)^{-1}-1$ and $\theta_i^{(s)}=\psi_{i,K}(\hat{\omega}^{p^s})^{-1}-1$ for any $s\ge 0$. It follows from the condition $v_p(\psi_{i,K}(\hat{\omega})^{-1}-1)\ge 1+v_p(2)$ that the equality $v_p(\theta_i^{(s)})=s+v_p(\theta_i^{(0)})$ holds. For each $1\le i\le n$, there exists at most only one integer $s\ge 0$ so that $v_p(m_i)=v_p(\theta_i^{(s)})$ since $\{v_p(\theta_i^{(s)})\}_s$ is strictly increasing. Hence, there exists an integer $0\le s(x)\le n$ with the property that $v_p(m_i)\ne v_p(\theta_i^{(s(x))})$ for every $1\le i\le n$ (by "Pigeonhole principle"). With this choice of $s(x)$, we obtain $v_p(\psi_{i,K}(x\hat{\omega}^{p^{s(x)}})^{-1}-1)=v_p(m_i+\theta_i^{(s(x))}+m_i\theta_i^{(s(x))})\le v_p(\theta_i^{(n)})=n+v_p(\theta_i^{(0)})$. This finishes the proof of (2). □

3 Proof of main theorems

The main purpose of this section is to show Theorems 1.1 and 1.2 in Introduction. As for Theorem 1.1, we show a slightly refined statement as follows.

Theorem 3.1. *Let $g>0$ be a positive integer. Let k be a p-adic field with residue cardinality q_k and π a uniformizer of k. Put $p'=p$ or $p'=4$ if $p\ne 2$ or $p=2$, respectively. Let $\mu\ge 1$ be the smallest integer*[2] *so that*

$$(q_k^{-1}\mathrm{Nr}_{k/\mathbb{Q}_p}(\pi))^{\mu}\equiv 1 \bmod p'.$$

[2] If $q_k^{-1}\mathrm{Nr}_{k/\mathbb{Q}_p}(\pi)$ is a root of unity, the constant μ here coincides with μ appeared in Theorem 1.1.

Assume the following conditions[3].

(i) $v_p((q_k^{-1}\mathrm{Nr}_{k/\mathbb{Q}_p}(\pi))^\mu - 1) > g \cdot (2g)! \cdot \Phi(g)H(g) \cdot \mu \cdot d_{Kk/k}f_k$ *and*

(ii) d_k *is prime to* $(2g)!$.

Then, for any g-dimensional abelian variety A over a p-adic field K with complex multiplication, we have

$$A(Kk_\pi)[p^\infty] \subset A[p^C]$$

where

$$C := 2g^2 \cdot (2g)! \cdot \Phi(g)H(g) \cdot \mu \cdot d_{Kk} + 12g^2 - 18g + 10.$$

In particular, we have

$$\sharp A(Kk_\pi)[p^\infty] \leq p^{2gC}.$$

Our proofs of Theorems 3.1 and 1.2 proceed by similar methods. As in the previous section, we fix an algebraic closure $\overline{\mathbb{Q}}_p$ of $\mathbb{Q}_p$ and suppose that K is a subfield of $\overline{\mathbb{Q}}_p$. In this section, we often use the following technical constants:

$$L_g(m) := \left[\log_p(1 + p^{\frac{m}{2}})^{2g}\right],$$
$$C(m, M, h) := v_p\left(\frac{m}{d_M}\right) + h + \frac{d_M}{2}\left(d_M + v_p(e_M) - \frac{1}{e_M} + v_p(2)(d_M - 1)\right).$$

Here, $m \geq 1$ and $h \geq 0$ are integers and M is a p-adic field.

Remark 3.2. (1) We have $mg \leq L_g(m) < g(m + 1 + v_p(2))$ for any prime p and $m \geq 1$, and we also have $L_g(m) < g(m + 1)$ if $(p, m) \neq (2, 1), (2, 2)$.
(2) Moreover, we have[4]

$$L_g(m) = mg \quad \text{for } m \geq 8g.$$

This can be checked as follows: It suffices to show $(1 + p^{\frac{m}{2}})^{2g} < p^{mg+1}$ for $m \geq 8g$. This inequality is equivalent to $(1 + p^{-\frac{m}{2}})^{2g} < p$. Thus it is enough to show $(1 + 2^{-\frac{m_0}{2}})^{2g} < 2$ where $m_0 := 8g$. By inequalities $2g < 2^{2g}$ and $\binom{2g}{r} < 2^{2g}$ for $0 \leq r \leq 2g$, we find

$$\left(1 + 2^{-\frac{m_0}{2}}\right)^{2g} = 1 + \sum_{r=1}^{2g} \binom{2g}{r} \left(\frac{1}{2}\right)^{\frac{rm_0}{2}} < 1 + 2g \cdot 2^{2g} \left(\frac{1}{2}\right)^{\frac{m_0}{2}} < 1 + \left(\frac{1}{2}\right)^{\frac{m_0}{2} - 4g} = 2$$

as desired.

3.1 Special cases

We consider Theorem 3.1 under some additional hypothesis. In this section, we show

Proposition 3.3. *Let the situation be as in Theorem 3.1 except assuming not* (i) *but*

(i)' $v_p((q_k^{-1}\mathrm{Nr}_{k/\mathbb{Q}_p}(\pi))^\mu - 1) > L_g((2g)! \cdot \mu \cdot d_{Kk/k}f_k)$.

Moreover, we assume that A has good reduction over K and all the endomorphisms of A are defined over K. Put

$$C_g(K, k) = v_p(d_{Kk}) + \frac{(2g)!}{2}\left((2g)! + v_p((2g)!) + v_p(2)((2g)! - 1)\right),$$
$$\Delta_g(K, k) = \mathrm{Max}\left\{C_g(K, k), L_g((2g)! \cdot \mu \cdot d_{Kk/k}f_k)\right\}.$$

[3]The condition (i) here depends on the choice of K. However, the author hopes that this condition would be replaced with certain one which does not depend on K as (i) in Theorem 1.1.

[4]The evaluation $8g$ here is "rough" but it is enough for our proofs.

Then, we have

$$A(Kk_\pi)[p^\infty] \subset A[p^C]$$

where

$$C := 2g\Delta_g(K,k) + 12g^2 - 18g + 10.$$

Proof. Put $T = T_p(A)$ and $V = V_p(A)$ to simplify notation. Let $\rho\colon G_K \to GL_{\mathbb{Z}_p}(T)$ be the continuous homomorphism obtained by the G_K-action on T. 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 $\bar{P} \in (T/p^nT)^{G_{Kk_\pi}}$. This implies $\sigma P - P \in p^nT$ for any $\sigma \in G_{Kk_\pi}$. 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 $\sigma \in G_{G_{Kk_\pi}}$. Hence we find $\det(\rho(\sigma) - E)P \in p^nT$ for any $\sigma \in G_{Kk_\pi}$. Put

$$c = \mathrm{Min}\{v_p(\det(\rho(\sigma) - E))) \mid \sigma \in G_{Kk_\pi}\}.$$

Then we see $P \in p^{n-c}T$ (if c is finite and $n > c$) and this shows $(T/p^nT)^{G_{Kk_\pi}} \subset p^{n-c}T/p^nT$. This implies an inequality

$$A(Kk_\pi)[p^\infty] \subset A[p^c] \tag{3.1}$$

if c is finite.

On the other hand, let us denote by F the field of complex multiplication of A. We know that V is a free $F \otimes_{\mathbb{Q}} \mathbb{Q}_p$-module of rank one and the G_K-action on V commutes with $F \otimes_{\mathbb{Q}} \mathbb{Q}_p$-action. Let $\prod_{i=1}^n F_i$ denote the decomposition of $F \otimes_{\mathbb{Q}} \mathbb{Q}_p$ into a finite product of p-adic fields. This induces a decomposition $V \simeq \oplus_{i=1}^n V_i$ of $\mathbb{Q}_p[G_K]$-modules. Each V_i is equipped with a structure of one dimensional F_i-modules and the G_K-action on V_i commutes with F_i-action. Let $\rho_i\colon G_K \to GL_{\mathbb{Q}_p}(V_i)$ be the homomorphism obtained by the G_K-action on V_i. Since ρ_i is abelian, it follows from the Shur's lemma that we have $(V_i \otimes_{\mathbb{Q}_p} \overline{\mathbb{Q}}_p)^{\mathrm{ss}} \simeq \oplus_{j=1}^{d_{F_i}} \overline{\mathbb{Q}}_p(\psi_{i,j})$ for some continuous characters $\psi_{i,j}\colon G_K \to \overline{\mathbb{Q}}_p^\times$. Here, the subscript "ss" stands for the semi-simplification. As is well-known, $\psi_{i,j}$ satisfies the following properties (since the G_K-action on V_i is given by a character $G_K \to F_i^\times$):

(a) $\psi_{i,1}, \dots, \psi_{i,d_{F_i}}$ are $\mathbb{Q}_p$-conjugate with each other, that is, $\psi_{i,k} = \tau_{k\ell} \circ \psi_{i,\ell}$ for some $\tau_{k\ell} \in G_{\mathbb{Q}_p}$, and

(b) $\psi_{i,1}, \dots, \psi_{i,d_{F_i}}$ have values in a p-adic field M_i (in the fixed algebraic closure $\overline{\mathbb{Q}}_p$ of $\mathbb{Q}_p$) which is $\mathbb{Q}_p$-isomorphic[5] to the Galois closure of $F_i/\mathbb{Q}_p$ (in an algebraic closure of F_i). We remark that d_{M_i} divides $d_{F_i}!$.

In particular, we have

$$v_p(\det \rho_i(\sigma) - E) = d_{F_i} v_p(\psi_i(\sigma) - 1),$$

where $\psi_i := \psi_{i,1}$. Let M be the composite field of $M_1, \dots, M_n$, and we regard $\psi_1, \dots, \psi_n$ as characters of G_K with values in $M^\times$; $\psi_i\colon G_K \to M^\times$. The field M is a Galois extension of $\mathbb{Q}_p$ in $\overline{\mathbb{Q}}_p$ and d_M divides $d_{F_1}!d_{F_2}!\cdots d_{F_n}!$. Since $\sum_{i=1}^n d_{F_i} = 2g$, we find

$$d_M \mid (2g)!. \tag{3.2}$$

(Here, we recall that the product of consecutive n natural numbers is divided by $n!$ for any natural number n.) In particular, we have $M \cap k = \mathbb{Q}_p$ since d_k is prime to $(2g)!$, and then we obtain

$$\ker \mathrm{Nr}_{M/\mathbb{Q}_p} \subset \ker \mathrm{Nr}_{Mk/k} \subset \ker \mathrm{Nr}_{K_M k/k}.$$

[5]Note that K lives in our fixed algebraic closure $\overline{\mathbb{Q}}_p$ of $\mathbb{Q}_p$ but F_i does not lives in $\overline{\mathbb{Q}}_p$.

Here, K_M is the composite KM of K and M. It follows from Proposition 2.1 that we obtain

$$\begin{aligned} c &\leq \operatorname{Min}\{v_p(\det(\rho(\sigma)-E))) \mid \sigma \in G_{K_M k_\pi}\} = \operatorname{Min}\left\{\sum_{i=1}^{n} d_{F_i} v_p(\psi_i(\sigma)-1) \mid \sigma \in G_{K_M k_\pi}\right\} \\ &\leq \operatorname{Min}\left\{\sum_{i=1}^{n} d_{F_i} v_p(\psi_{i,K_M k}(\pi\omega)^{-1}-1) \mid \omega \in \ker \operatorname{Nr}_{K_M k/k}\right\} \\ &\leq \operatorname{Min}\left\{\sum_{i=1}^{n} d_{F_i} v_p(\psi_{i,K_M k}(\pi\omega)^{-1}-1) \mid \omega \in \ker \operatorname{Nr}_{M/\mathbb{Q}_p}\right\} \\ &\leq \operatorname{Min}\left\{\sum_{i=1}^{n} d_{F_i} v_p(\psi^{\mu}_{i,K_M k}(\pi\omega)^{-1}-1) \mid \omega \in \ker \operatorname{Nr}_{M/\mathbb{Q}_p}\right\}. \end{aligned} \tag{3.3}$$

Here, μ is the integer appeared in the statement of Theorem 3.1. Note that ψ_i is a crystalline character since A has good reduction over K. By rearranging the numbering of subscripts, we may suppose the following situation for some $0 \leq r \leq n$.

(I) For $1 \leq i \leq r$, the set of the Hodge-Tate weights of $M(\psi_i)$ is $\{0, 1\}$.

(II) For $r < i \leq n$, the set of the Hodge-Tate weights of $M(\psi_i)$ is either $\{1\}$ or $\{0\}$.

Lemma 3.4. *For $r < i \leq n$ and any $\omega \in \ker \operatorname{Nr}_{M/\mathbb{Q}_p}$, we have*

$$v_p(\psi^{\mu}_{i,K_M k}(\pi\omega)^{-1}-1) \leq L_g((2g)! \cdot d_{Kk/k} f_k \cdot \mu).$$

Proof. In this proof we set $L := K_M k$. We know that the morphism $\psi_{i,\mathrm{alg}}\colon \underline{L}^\times \to \underline{M}^\times$ corresponding to $\psi_i|_{G_L}$ is trivial or $\operatorname{Nr}^{-1}_{L/\mathbb{Q}_p}$ on $\mathbb{Q}_p$-points. This in particular gives $\psi_{i,L}(\omega) = 1$. Since $\pi_L^{e_{L/k}}\pi^{-1}$ is a p-adic unit for any uniformizer π_L of L, we find

$$\begin{aligned} \psi_{i,L}(\pi\omega)^{-1} &= \psi_{i,L}(\pi)^{-1} = \psi_{i,L}(\pi_L^{-e_{L/k}} \cdot \pi_L^{e_{L/k}}\pi^{-1}) \\ &= \alpha_i^{-e_{L/k}} \cdot \psi_{i,\mathrm{alg}}(\pi)^{-1} \end{aligned}$$

where $\alpha_i := \psi_{i,L}(\pi_L)\psi_{i,\mathrm{alg}}(\pi_L)^{-1}$. Denote by L' the unramified extension of L of degree $\mu e_{L/k}$.

(I) Suppose that the set of the Hodge-Tate weights of $M(\psi_i)$ is $\{0\}$. In this case $\psi_{i,\mathrm{alg}}$ is trivial and thus we have $\psi^{\mu}_{i,L}(\pi\omega)^{-1} = \alpha_i^{-\mu e_{L/k}}$. It follows from Lemma 9 of [Oz2] that $\psi^{\mu}_{i,L}(\pi\omega)^{-1}$ is a unit root of the characteristic polynomial $f(T)$ of the geometric Frobenius endomorphism of $\overline{A}_{/\mathbb{F}_{L'}}$. Since $f(1) = \sharp\overline{A}(\mathbb{F}_{q_{L'}})$, we see $v_p(\psi^{\mu}_{i,L}(\pi\omega)^{-1}-1) \leq v_p(\sharp\overline{A}(\mathbb{F}_{q_{L'}})) \leq \left[\log_p \sharp\overline{A}(\mathbb{F}_{q_{L'}})\right]$. It follows from the Weil bound that $v_p(\psi^{\mu}_{i,L}(\pi\omega)^{-1}-1) \leq L_g(f_{L'})$. Since we have $f_{L'} = \mu e_{L/k} f_L = d_{L/Kk} \cdot \mu \cdot d_{Kk/k} f_k \leq (2g)! \cdot \mu \cdot d_{Kk/k} f_k$. we obtain the desired inequality.

(II) Suppose that the set of the Hodge-Tate weights of $M(\psi_i)$ is $\{1\}$. In this case $\psi_{i,\mathrm{alg}}$ is $\operatorname{Nr}^{-1}_{L/\mathbb{Q}_p}$ on $\mathbb{Q}_p$-points. If we set $\beta := q_k^{-1}\operatorname{Nr}_{k/\mathbb{Q}_p}(\pi)$, we find

$$\begin{aligned} \psi^{\mu}_{i,L}(\pi\omega)^{-1} - 1 &= (\alpha_i^{-1}\operatorname{Nr}_{k/\mathbb{Q}_p}(\pi)^{f_{L/k}})^{\mu e_{L/k}} - 1 \\ &= ((\alpha_i^{-1}q_L)^{\mu e_{L/k}} - 1)\beta^{\mu d_{L/k}} + (\beta^{\mu d_{L/k}} - 1). \end{aligned}$$

It again follows from Lemma 9 of [Oz2] that $(\alpha_i^{-1}q_L)^{\mu e_{L/k}}$ is a unit root of the characteristic polynomial $f^{\vee}(T)$ of the geometric Frobenius endomorphism of $\overline{A^{\vee}}_{/\mathbb{F}_{L'}}$. Since $f^{\vee}(1) = \sharp\overline{A^{\vee}}(\mathbb{F}_{q_{L'}})$, the same argument as in (I) shows that $v_p((\alpha_i^{-1}q_L)^{\mu e_{L/k}} - 1) \leq L_g(f_{L'}) \leq L_g((2g)! \cdot \mu \cdot d_{Kk/k} f_k)$. In particular, we have $v_p(\beta^{\mu d_{L/k}} - 1) > v_p((\alpha_i^{-1}q_L)^{\mu e_{L/k}} - 1)$ by the assumption (i)'. Since β is a p-adic unit, we obtain $v_p(\psi^{\mu}_{i,L}(\pi\omega)^{-1}-1) = v_p((\alpha_i^{-1}q_L)^{\mu e_{L/k}} - 1) \leq L_g((2g)! \cdot \mu \cdot d_{Kk/k} f_k)$ as desired. □

By (3.3) and the lemma, in the case where $r = 0$, we have

$$c \leq \sum_{i=1}^{n} d_{F_i} L_g((2g)! \cdot \mu \cdot d_{Kk/k} f_k) = 2g L_g((2g)! \cdot \mu \cdot d_{Kk/k} f_k). \tag{3.4}$$

In the rest of the proof, we assume that $r > 0$. By (3.3) and the lemma again, we have

$$\begin{aligned} c \leq \mathrm{Min} &\left\{ \sum_{i=1}^{r} d_{F_i} v_p(\psi^{\mu}_{i,K_M k}(\pi\omega)^{-1} - 1) \mid \omega \in \ker \mathrm{Nr}_{M/\mathbb{Q}_p} \right\} \\ &+ L_g((2g)! \cdot \mu \cdot d_{Kk/k} f_k) \sum_{i=r+1}^{n} d_{F_i}. \end{aligned}$$

Here we remark that $v_p(\mu) = 0$ and the Hodge-Tate weights of ψ^{μ}_i for each $1 \leq i \leq r$ consist of 0 and μ. Hence, applying Theorem 2.3 to the set of characters $\psi^{\mu}_1, \dots, \psi^{\mu}_r \colon G_{K_M k} \to M^{\times}$, an element $x = \pi$ and $h = 0$, there exists an element $\hat{\omega} \in \ker \mathrm{Nr}_{M/\mathbb{Q}_p}$ and an integer $0 \leq s = s(\pi) \leq r$ as in the theorem. Then we obtain

$$\begin{aligned} c &\leq \sum_{i=1}^{r} d_{F_i} v_p(\psi^{\mu}_{i,K_M k}(\pi\hat{\omega}^{p^s})^{-1} - 1) + L_g((2g)! \cdot \mu \cdot d_{Kk/k} f_k) \sum_{i=r+1}^{n} d_{F_i} \\ &\leq \sum_{i=1}^{r} d_{F_i}(r + \delta_{(i)} + C(d_{K_M k}, M, 0)) + L_g((2g)! \cdot \mu \cdot d_{Kk/k} f_k) \sum_{i=r+1}^{n} d_{F_i} \\ &\leq 2g\Delta_0 + \sum_{i=1}^{r} d_{F_i}(r + \delta_{(i)}) \end{aligned}$$

where $\Delta_0 := \mathrm{Max}\left\{C(d_{K_M k}, M, 0), L_g((2g)! \cdot \mu \cdot d_{Kk/k} f_k)\right\}$. Since d_M divides $(2g)!$, we also have

$$C(d_{K_M k}, M, 0) < v_p(d_{Kk}) + \frac{(2g)!}{2}\left((2g)! + v_p((2g)!) + v_p(2)((2g)! - 1)\right).$$

Thus, for the constant $\Delta_g(K, k)$ defined in the statement of the proposition, we obtain $\Delta_0 \leq \Delta_g(K, k)$ and $c \leq 2g\Delta_g(K, k) + \sum_{i=1}^{r} d_{F_i}(r + \delta_{(i)})$.

- If $r \leq 2$, we have $\sum_{i=1}^{r} d_{F_i}(r + \delta_{(i)}) = \sum_{i=1}^{r} d_{F_i} r \leq r \cdot 2g \leq 4g$.
- If $r > 2$, we have $\sum_{i=1}^{r} d_{F_i}(r+\delta_{(i)}) = r\sum_{i=1}^{r} d_{F_i} + \sum_{i=3}^{r} d_{F_i}\delta_{(i)} \leq n\sum_{i=1}^{n} d_{F_i} + \sum_{i=3}^{n} d_{F_i}(2n - 5) \leq n \cdot 2g + (2n-5)(\sum_{i=1}^{n} d_{F_i} - 2) \leq 2g \cdot 2g + (4g-5) \cdot (2g-2) = 12g^2 - 18g + 10$.

Therefore, for any $r > 0$, we find

$$c \leq 2g\Delta_g(K, k) + 12g^2 - 18g + 10.$$

Note that this inequality holds also for the case $r = 0$ by (3.4). Now the proposition follows from (3.1). □

3.2 General cases

We show Theorems 3.1 and 1.2. For this, we need the following observations given by Serre-Tate [ST] and Silverberg [Si1].

Theorem 3.5. *Let A be a g-dimensional abelian variety over K.*
(1) Put $m = 3$ or $m = 4$ if $p \neq 3$ or $p = 3$, respectively. Then A has semi-stable reduction over $K(A[m])$ and all the endomorphisms of A are defined over $K(A[m])$.
(2) Let L be the intersection of the fields $K(A[N])$ for all integers $N > 2$. Then, all the endomorphisms of A are defined over L and $[L : K]$ divides $H(g)$.
(3) Assume that A has potential good reduction. Let $\rho_{A,\ell} \colon G_K \to GL_{\mathbb{Z}_p}(T_\ell(A))$ be the continuous homomorphism defined by the G_K-action on the Tate module $T_\ell(A)$ for any prime ℓ.

(3-1) *For any prime ℓ not equal to p, let H_ℓ be the kernel of the restriction of $\rho_{A,\ell}$ to I_K. Then H_ℓ is an open subgroup of I_K, which is independent of the choice of ℓ. Moreover, if we set $c := [I_K : H_\ell]$, then there exists a finite totally ramified extension L/K of degree c such that A has good reduction over L.*

(3-2) *If A has complex multiplication and all the endomorphisms of A are defined over K, then the constant c above satisfies $c \leq \Phi(g)$.*

(4) *Assume that A has complex multiplication (over $\overline{K}$). Then, there exists a finite extension L/K of degree at most $\Phi(g)H(g)$ such that A has good reduction over L and all the endomorphisms of A are defined over L.*

Proof. (1) follows from [Si1, Theorem 4.1] and the Raynaud's criterion of semi-stable reduction [Gr, Proposition 4.7]. (2) is [Si1, Theorem 4.1], and (4) is an immediate consequence of (2) and (3) since A must have potential good reduction under the condition that A has complex multiplication. The first statement related to H_ℓ in (3-1) is [ST, §2, Theorem 2, p.496]. The rest assertions of (3) are also essentially consequences of results given in §2 and §4 of [ST] but it is not directly mentioned in *loc., cit.* Thus we give a proof here, just in case. The group H is a closed normal subgroup of G_K, which is also open in I_K. Let Γ be the closure of the subgroup of G_K generated by any choice of a lift of the q_K-th Frobenius element in $G_{\mathbb{F}_{q_K}}$. The projection $G_K \to G_{\mathbb{F}_{q_K}}$ gives an isomorphism of Γ onto $G_{\mathbb{F}_{q_K}}$; in particular, G_K is the semi-direct product of Γ and I_K. Let K_Γ/K be the field extension (of infinite degree) corresponding to $\Gamma \subset G_K$, and let M/K^{ur} be the finite extension corresponding to $H := H_\ell \subset I_K$. Note that A has good reduction over M. Now we set $L := K_\Gamma \cap M$. Then L/K is totally ramified since so is K_Γ/K. Furthermore, it is immediate to check $H\Gamma \cap I_K = H$; this shows $LK^{\mathrm{ur}} = M$. Hence we obtain that A has good reduction over L and $[L : K] = [M : K^{\mathrm{ur}}] = c$. This shows (3-1). Next we show (3-2). Let F be the number field of degree $2g$ of complex multiplication of A. Then $V_\ell(A)$ has a structure of free $F \otimes_{\mathbb{Q}} \mathbb{Q}_\ell$ module of rank one and the G_K-action on $V_\ell(A)$ commutes with $F \otimes_{\mathbb{Q}} \mathbb{Q}_\ell$. Thus we may consider $\rho_{A,\ell}$ as a character $G_K \to (F \otimes_{\mathbb{Q}} \mathbb{Q}_\ell)^\times$. Moreover, the image of this character restricted to I_K has values in the group $\mu(F)$ of roots of unity contained in F by [ST, §4, Theorem 6, p.503]. Thus we obtain the fact that c divides the order m of $\mu(F)$. On the other hand, since μ_m is a subset of F, we have $\varphi(m) \mid 2g$. Therefore, we obtain $c \leq m \leq \Phi(g)$ as desired. □

Now we are ready to show our main theorems. First we show Theorem 3.1.

Proof of Theorem 3.1. Let A be as in the theorem. Since A has complex multiplication, it follows from Theorem 3.5 (4) that there exists a finite extension L/K such that $d_{L/K} \leq \Phi(g)H(g)$, A has good reduction over L and all the endomorphisms of A are defined over L. In addition, we have $v_p((q_k^{-1}\mathrm{Nr}_{k/\mathbb{Q}_p}(\pi))^\mu - 1) > g \cdot (2g)! \cdot \Phi(g)H(g) \cdot \mu \cdot d_{Kk/k}f_k = L_g((2g)! \cdot \Phi(g)H(g) \cdot \mu \cdot d_{Kk/k}f_k) \geq L_g((2g)! \cdot \mu \cdot d_{Lk/k}f_k)$ by the assumption (i) and Remark 3.2 (2). Thus we can apply Proposition 3.3 to A/L; we have

$$A(Lk_\pi)[p^\infty]) \subset A[p^{C'}]$$

where $C' = 2g\Delta_g(L,k) + 12g^2 - 18g + 10$. Here,

$$\begin{aligned} C_g(L,k) &= v_p(d_{Lk}) + \frac{(2g)!}{2}\left((2g)! + v_p((2g)!) + v_p(2)((2g)! - 1)\right), \\ \Delta_g(L,k) &= \mathrm{Max}\left\{C_g(L,k), L_g((2g)! \cdot \mu \cdot d_{Lk/k}f_k)\right\}. \end{aligned}$$

Note that we have $v_p(d_{Lk}) < d_{Lk} \leq \Phi(g)H(g) \cdot d_{Kk}$ and $L_g((2g)! \cdot \mu \cdot d_{Lk/k}f_k) \leq g \cdot (2g)! \cdot \Phi(g)H(g) \cdot \mu \cdot d_{Kk}$. Therefore, it suffices to show

$$\Phi(g)H(g) \cdot d_{Kk} + \frac{(2g)!}{2}\left((2g)! + v_p((2g)!) + v_p(2)((2g)! - 1)\right) < g \cdot (2g)! \cdot \Phi(g)H(g) \cdot \mu \cdot d_{Kk}$$

for the proof but this is clear. □

Remark 3.6. In the above proof of Theorem 3.1, we referred the field extension L/K of Theorem 3.5 (4) and the upper bound $\Phi(g)H(g)$ of $[L : K]$. By Theorem 3.5 (1), we may refer the field $K(A[m])$ instead of the above L. Since we have a natural embedding from $\mathrm{Gal}(K(A[m])/K)$ into $GL(A[m]) \simeq GL_{2g}(\mathbb{Z}/m\mathbb{Z})$, we obtain a bound for the extension degree of $K(A[m])/K$; we have $[K(A[m])/K] \leq G(g)$, where

$$G(n) := \sharp GL_{2n}(\mathbb{Z}/m\mathbb{Z}) = \begin{cases} \prod_{i=0}^{2n-1}(3^{2n} - 3^i) & \text{if } p \neq 3, \\ 2^{4n^2}\prod_{i=0}^{2n-1}(2^{2n} - 2^i) & \text{if } p = 3. \end{cases}$$

for $n > 0$. Note that we have $G(n) < m^{4n^2}$. It is not difficult to check the inequalities $\Phi(1)H(1) > G(1)$ and $\Phi(g)H(g) < G(g)$ for $g > 1$ (see Section 5 below). Hence, only in the case $g = 1$ of elliptic curves, we can obtain smaller bound than that given in Theorem 3.1 by replacing $\Phi(g)H(g)$ with $G(1)$.

Applying Theorem 1.1 with $k = \mathbb{Q}_p$ and $\pi = p$, we immediately obtain the following.

Corollary 3.7. *Let A be a g-dimensional abelian variety over a p-adic field K with complex multiplication. Then we have*

$$A(K(\mu_{p^\infty}))[p^\infty] \subset A[p^C]$$

where

$$C := 2g^2 \cdot (2g)! \cdot \Phi(g)H(g) \cdot d_K + 12g^2 - 18g + 10$$

In particular, we have

$$\sharp A(K(\mu_{p^\infty}))[p^\infty] \leq p^{2gC}.$$

Next we show Theorem 1.2.

Proof of Theorem 1.2. We follow essentially the same argument as that of Theorem 3.1. Put $\hat{K} = K(\sqrt[p^\infty]{K})$.

Step 1. First we consider the case where A has good reduction over K and all the endomorphisms of A are defined over K. Put $\nu = v_p(d_K) + 1 + v_p(2)$ and

$$C_g(K) = v_p(d_K) + \nu + \frac{(2g)!}{2}\left((2g)! + v_p((2g)!) + v_p(2)((2g)! - 1)\right),$$
$$\Delta_g(K) = \mathrm{Max}\left\{C_g(K), L_g((2g)! \cdot p^\nu \cdot d_K)\right\}.$$

Following the proof of Proposition 3.3, we show

$$A(\hat{K})[p^\infty] \subset A[p^{C'}] \tag{3.5}$$

where $C' := 2g\Delta_g(K) + 12g^2 - 18g + 10$. Let $\rho\colon G_K \to GL_{\mathbb{Z}_p}(T_p(A)) \simeq GL_{2g}(\mathbb{Z}_p)$, $M/\mathbb{Q}_p$ and $\psi_1, \ldots, \psi_n\colon G_K \to M^\times$ be as in the proof of Proposition 3.3. If we denote by $\hat{K}_{\mathrm{ab}}$ the maximal abelian extension of K contained in $\hat{K}$, all the points of $A(\hat{K})[p^\infty]$ are in fact defined over $\hat{K}_{\mathrm{ab}}$ since ρ is abelian. Thus, setting $c := \mathrm{Min}\{v_p(\det(\rho(\sigma) - E))) \mid \sigma \in G_{\hat{K}_{\mathrm{ab}}}\}$, we find

$$A(\hat{K})[p^\infty] = A(\hat{K}_{\mathrm{ab}})[p^\infty] \subset A[p^c] \tag{3.6}$$

if c is finite (see arguments just above (3.1)). On the other hand, we set $G := \mathrm{Gal}(\hat{K}/K)$ and $H := \mathrm{Gal}(\hat{K}/K(\mu_{p^\infty}))$. 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

$$H/H^{\chi_p(\sigma)-1} \twoheadrightarrow H/\overline{(G, G)} = \mathrm{Gal}(\hat{K}_{\mathrm{ab}}/K(\mu_{p^\infty})) \quad \text{for any } \sigma \in G. \tag{3.7}$$

Lemma 3.8. *We have $\chi_p(\sigma_0) - 1 = p^\nu$ for some $\sigma_0 \in G$.*

Proof. We denote by K' the field $K(\mu_p)$ or $K(\mu_4)$ if $p \neq 2$ or $p = 2$, respectively. If we denote by p^ℓ the order of the set of p-power roots of unity in K', we see $K' \cap \mathbb{Q}_p(\mu_{p^\infty}) = \mathbb{Q}_p(\mu_{p^\ell})$ and thus $\chi_p(G_{K'}) = 1 + p^\ell\mathbb{Z}_p$. Furthermore, since $[\mathbb{Q}_p(\mu_{p^\ell}) : \mathbb{Q}_p]$ divides $[K' : K][K : \mathbb{Q}_p]$, we see $p^{\ell-1-v_p(2)} \mid d_K$. Hence we obtain $\chi_p(G_{K'}) \supset 1 + p^\nu\mathbb{Z}_p$ and the lemma follows. □

By the lemma above and (3.7), we see that $\mathrm{Gal}(\hat{K}_{\mathrm{ab}}/K(\mu_{p^\infty}))$ is of exponent p^ν, that is, $\sigma \in G_{K(\mu_{p^\infty})}$ implies $\sigma^{p^\nu} \in G_{\hat{K}_{\mathrm{ab}}}$. This shows $c \leq \mathrm{Min}\{v_p(\det(\rho(\sigma)^{p^\nu} - E))) \mid \sigma \in G_{K(\mu_{p^\infty})}\}$. Mimicking the arguments for inequalities (3.3), we find

$$c \leq \mathrm{Min}\left\{ \sum_{i=1}^{n} d_{F_i} v_p(\psi_{i,K_M}^{p^\nu}(\pi\omega)^{-1} - 1) \mid \omega \in \ker \mathrm{Nr}_{M/\mathbb{Q}_p} \right\}.$$

Now the inequality (3.6) follows by completely the same method as the proof of Proposition 3.3 (with replacing the pair (k,μ) there with $(\mathbb{Q}_p, p^\nu)$).

Step 2. Next we consider the general case. Since A has complex multiplication, it follows from Theorem 3.5 (4) that there exists a finite extension L/K such that $d_{L/K} \leq \Phi(g)H(g)$, A has good reduction over L and all the endomorphisms of A are defined over L. Thus we can apply the result of Step 1 to A/L; we have

$$A(\hat{K})[p^\infty] \subset A(\hat{L})[p^\infty] \subset A[p^{C''}]$$

where $C'' := 2g\Delta_g(L) + 12g^2 - 18g + 10$. We find

$$\begin{aligned} L_g((2g)! \cdot p^{v_p(d_L)+1+v_p(2)} \cdot d_L) &= L_g((2g)! \cdot p^{1+v_p(2)} \cdot p^{v_p(d_{L/K})} d_{L/K} \cdot p^{v_p(d_K)} d_K) \\ &\leq L_g((2g)! \cdot p^{1+v_p(2)} \cdot (d_{L/K})^2 \cdot p^{v_p(d_K)} d_K) \\ &\leq g \cdot (2g)! \cdot p^{1+v_p(2)} \cdot (\Phi(g)H(g))^2 \cdot p^{v_p(d_K)} d_K. \end{aligned}$$

(For the last equality, see Remark 3.2 (2).) Now Theorem 1.2 immediately follows by $\Delta_g(L) \leq g \cdot (2g)! \cdot p^{1+v_p(2)} \cdot (\Phi(g)H(g))^2 \cdot p^{v_p(d_K)} d_K$. □

One of the keys for our arguments above is a theory of locally algebraic representations. Thus our method essentially works also for abelian varieties A with the property that the G_K-action on the semi-simplification of $V_p(A) \otimes_{\mathbb{Q}_p} \overline{\mathbb{Q}}_p$ is abelian. For example, this is the case where A has good ordinary reduction.

Proposition 3.9. *Let $g > 0$ be a positive integer. Let K and k be p-adic fields. Let π be a uniformizer of k. Assume that $q_k^{-1}\mathrm{Nr}_{k/\mathbb{Q}_p}(\pi)$ is a root of unity; we denote by $0 < \mu < p$ the minimum integer so that $(q_k^{-1}\mathrm{Nr}_{k/\mathbb{Q}_p}(\pi))^\mu = 1$. Then, for any g-dimensional abelian variety A over K with good ordinary reduction, we have*

$$A(Kk_\pi)[p^\infty] \subset A[p^{2gL_g(\mu d_{Kk/k} f_k)}].$$

In particular, we have

$$\sharp A(Kk_\pi)[p^\infty] \leq p^{4g^2 L_g(\mu d_{Kk/k} f_k)} < p^{4g^3(\mu d_{Kk/k} f_k + 1 + v_p(2))}.$$

Proof. Put $V = V_p(A)$, $T = T_p(A)$ and $c = \mathrm{Min}\{v_p(\det(\rho(\sigma) - E))) \mid \sigma \in G_{Kk_\pi}\}$. By the same argument as the beginning of the proof of Proposition 3.3, we obtain

$$A(Kk_\pi)[p^\infty] \subset A[p^c] \tag{3.8}$$

if c is finite. Since A has good ordinary reduction, we have an exact sequence $0 \to V_1 \to V \to V_2 \to 0$ of $\mathbb{Q}_p[G_K]$-modules with the following properties.

(i) $V_1 \simeq W \otimes_{\mathbb{Q}_p} \mathbb{Q}_p(1)$ for some unramified representation W of G_K, and

(ii) V_2 is unramified.

Hence, taking a p-adic field M large enough, we have $(V \otimes_{\mathbb{Q}_p} M)^{\mathrm{ss}} \simeq \oplus_{i=1}^{2g} M(\psi_i)$ for some continuous crystalline characters $\psi_i \colon G_K \to M^\times$. Furthermore, for every i, the set of the Hodge-Tate weights of $M(\psi_i)$ is either $\{1\}$ or $\{0\}$. By Proposition 2.1, we have $c \le \sum_{i=1}^{2g} v_p(\psi^{\mu}_{i,Kk}(\pi)^{-1}-1)$. Let K' be the unramified extension of Kk of degree $\mu e_{Kk/k}$. By a similar method of the proof of Lemma 3.4, we find that $\psi^{\mu}_{i,Kk}(\pi)^{-1}$ is a unit root of the characteristic polynomial $f(T)$ of the geometric Frobenius endomorphism of $\overline{A}_{/\mathbb{F}_{K'}}$, otherwise $\psi^{\mu}_{i,Kk}(\pi)^{-1}$ is a unit root of the characteristic polynomial $f^{\vee}(T)$ of the geometric Frobenius endomorphism of $\overline{A^{\vee}}_{/\mathbb{F}_{K'}}$. We know $f(1) = \sharp\overline{A}(\mathbb{F}_{q_{K'}})$ and $f^{\vee}(1) = \sharp\overline{A^{\vee}}(\mathbb{F}_{q_{K'}})$, and their p-adic valuations are bounded by $L_g(f_{K'})$ by the Weil bound. Since we have $f_{K'} = f_{K'/Kk} f_{Kk} = \mu d_{Kk/k} f_k$, we obtain $c \le \sum_{i=1}^{2g} v_p(\psi^{\mu}_{i,Kk}(\pi)^{-1}-1) \le 2g L_g(\mu d_{Kk/k} f_k)$. Now the result follows from (3.8). □

4 Abelian varieties over number fields

In this section, we suppose that K is a number field. The goal of this section is to give a proof of Theorem 1.3 in Introduction. The theorem is an immediate consequence of the following proposition.

Proposition 4.1. *Let g, K, d and h be as in Theorem 1.3.*
(1) *Let A be a g-dimensional abelian variety over K with semi-stable reduction everywhere. Let p_0 be the smallest prime number such that A has good reduction at some finite place of K above p_0. Then $A(K(\mu_\infty))[p]$ is zero if $p > (1+\sqrt{p_0}^{dh})^{2g}$, p is unramified in K and A has good reduction at some finite place of K above p.*
(2) *Let A be a g-dimensional abelian variety over K with complex multiplication which has good reduction everywhere. Then, for any prime p, we have*

$$A(K(\mu_\infty))[p^\infty] \subset A[p^C]$$

where $C := 2g^2 \cdot (2g)! \cdot \Phi(g)H(g) \cdot dh + 12g^2 - 18g + 10$.

Proof. Let A be a g-dimensional abelian variety over K with semi-stable reduction everywhere. Let K' be the maximal extension of K contained in $K(\mu_\infty)$ which is unramified at all finite places of K. Note that K' is a finite abelian extension of K. In particular, it follows from class field theory that $[K' : K]$ is a divisor of the narrow class number h of K. If we denote by L_p the maximal extension of K contained in $K(\mu_\infty)$ which is unramified at all places except for places dividing p and the infinite places, then it is shown in [KL, Appendix, Lemma] that $L_p = K'(\mu_{p^\infty})$.

(1) We give a proof of the assertion (1). Here we mainly follow Ribet's arguments in [KL]. We suppose that p is prime to $2p_0$ and also suppose that p is unramified in K. Assume that $A(K(\mu_\infty))[p] \neq O$. We claim that there exists a g-dimensional abelian variety A' over K' which is K'-isogenous to A such that $A'(K')[p] \neq O$. We denote by G and H the absolute Galois groups of K' and $K(\mu_\infty)$, respectively. The assumption $A(K(\mu_\infty))[p] \neq O$ is equivalent to say that $A[p]^H \neq O$. Let W be a simple G-submodule of $A[p]^H$. Ribet showed in the proof of Theorem 2 of [KL] that, since A has semi-stable reduction everywhere over K', W is one-dimensional over $\mathbb{F}_p$ and the action of G on W factors through $\mathrm{Gal}(K'(\mu_p)/K')$. Since p is unramified at K', we find that the G-action on W is given by $\overline{\chi}_p^n$ for some $0 \le n \le p-1$, where $\overline{\chi}_p$ is the mod p cyclotomic character. Moreover, since A has good reduction at some finite place of K' above p ($\neq 2$), it follows from the classification of Tate and Oort that n is equal to 0 or 1. Thus W is isomorphic to $\mathbb{F}_p$ or $\mathbb{F}_p(1)$. If we are in the former case, we have $A'(K')[p] \neq O$ for $A' := A$. Suppose that we are in the latter case. Then there exists a surjection $A^{\vee}[p] \to \mathbb{F}_p$ of G-modules. If we denote by C the kernel of this surjection, then the G-action on $A^{\vee}[p]$ preserves C. This implies that $A' := A^{\vee}/C$ is an abelian variety defined over K' and we find that there exists a trivial G-submodule of $A'[p]$ of order p. Thus we have $A'(K')[p] \neq O$. This finishes the proof of the claim.

Now we take a prime $\mathfrak{p}'_0$ of K' above p_0 such that A has good reduction at $\mathfrak{p}'_0$. Since A' above is K'-isogenous to A, we know that A' has good reduction at $\mathfrak{p}'_0$ by [ST, §1, Corollary 2]. If we denote by $K'_{\mathfrak{p}'_0}$ the completion of K' at $\mathfrak{p}'_0$ and also denote by $\mathbb{F}_{\mathfrak{p}'_0}$ the residue field of $K'_{\mathfrak{p}'_0}$, then reduction modulo $\mathfrak{p}'_0$ gives an injective homomorphism

$$A'(K')[p] \subset A'(K'_{\mathfrak{p}'_0})[p] \hookrightarrow \bar{A}'(\mathbb{F}_{\mathfrak{p}'_0}).$$

We recall that $A'(K')[p] \neq O$. Since the order of $\mathbb{F}_{\mathfrak{p}'_0}$ is bounded by p_0^{dh}, it follows from the Weil bound that we have $p < (1 + \sqrt{p_0}^{dh})^{2g}$. This finishes the proof.

(2) We give a proof of the assertion (2). Let A be an abelian variety as in the statement. Since A has good reduction everywhere over K, it follows from the criterion of Néron-Ogg-Shafarevich that the G_K-action on $A[p^\infty]$ is unramified outside p. This gives the fact that the G_K-action on $A(K(\mu_{p^\infty}))[p^\infty]$ factors through $\mathrm{Gal}(L_p/K) = \mathrm{Gal}(K'(\mu_{p^\infty})/K)$. Thus we have

$$A(K(\mu_\infty))[p^\infty] = A(K'(\mu_{p^\infty}))[p^\infty].$$

Since we have $[K' : \mathbb{Q}] \leq dh$, the result follows from Corollary 3.7. □

5 Bounds on $\Phi(n)$ and $H(n)$

We recall the definitions of $\Phi(n)$ and $H(n)$:

$$\Phi(n) := \mathrm{Max}\{m \in \mathbb{Z} \mid \varphi(m) \text{ divides } 2n\},$$
$$H(n) := \gcd\{\sharp \mathrm{GSp}_{2n}(\mathbb{Z}/N\mathbb{Z}) \mid N \geq 3\}.$$

Here, φ is the Euler's totient function. The lists of $\Phi(n)$, $H(n)$ (and $G(n)$ with $p \neq 3$ appeared in Remark 3.6) for small n are given at the end of this paper. In this section, we study some upper bounds of Φ and H.

5.1 The function H

For the function H, we refer results of [Si1, §3 and §4]. The exact formula for $H(n)$ is as follows:

$$H(n) = \frac{1}{2^{n-1}} \prod_q q^{r(q)}$$

where the product is over primes $q \leq 2n+1$,

$$r(2) = [n] + \sum_{j=0}^{\infty} \left[\frac{2n}{2^j}\right], \text{ and } r(q) = \sum_{j=0}^{\infty} \left[\frac{2n}{q^j(q-1)}\right] \text{ if } q \text{ is odd.}$$

Moreover, we have

Theorem 5.1 ([Si1, Corollary 3.3]). *We have*

$$H(n) < 2(9n)^{2n}$$

for any $n > 0$.

5.2 The function Φ

Next we consider the function Φ. At first, we remark that $\Phi(n)$ must be even since $\varphi(x) = \varphi(2x)$ if x is odd. Furthermore, $\Phi(n)$ is not a power of 2. (In fact, we have $\varphi(2^r) = \varphi(2^{r-1} \cdot 3)$ if $r \geq 2$.) Thus it holds that

$$\Phi(n) = \mathrm{Max}\left\{ m \in \mathbb{Z} \,\middle|\, \begin{array}{c} \varphi(m) \text{ divides } 2n, \text{ and } m = 2^r x \\ \text{where } r \geq 1 \text{ and } x \geq 3 \text{ is odd} \end{array} \right\}. \tag{5.1}$$

We show some elementary formulas.

Proposition 5.2. (1) *We have* $\Phi(1) = 6$ *and* $6 \leq \Phi(n) < 6n\sqrt[3]{n}$ *for* $n > 1$.
(2) *Put* $t = v_2(n) + 2$ *and let* $p_1 = 2 < p_2 < \cdots < p_t$ *be the first* t *prime numbers. Then we have*

$$\Phi(n) \leq 2n \prod_{i=1}^{t} \frac{p_i}{p_i - 1}.$$

In particular, we have $\Phi(n) \leq 6n$ *if* n *is odd.*
(3) *If* $n > 3$ *is an odd prime, we have*[6]

$$\Phi(n) = \begin{cases} 6 & \text{if } 2n+1 \text{ is not prime,} \\ 4n+2 & \text{if } 2n+1 \text{ is prime.} \end{cases}$$

Proof. To check $\Phi(1) = 6$ is an easy exercise. Since $\varphi(6) = 2 \mid 2n$, we have $\Phi(n) \geq 6$ for any n. Suppose $n > 1$. We take an even integer $m > 0$, which is of the form $2^r x$ where $r \geq 1$ and $x \geq 3$ is odd, such that $\varphi(m) \mid 2n$. Let $m = 2^r \prod_{i=1}^s q_i^{e_i}$ be the prime factorization of m with $r, s, e_1, \ldots, e_s \geq 1$. Since $\varphi(m) = 2^{r-1} \prod_{i=1}^s q_i^{e_i - 1}(q_i - 1)$ and $\varphi(m) \mid 2n$, we have $v_2(2n) \geq r - 1 + s$ and thus

$$r + s \leq v_2(n) + 2. \tag{5.2}$$

Then we find

$$2n \geq \varphi(m) = m\left(1 - \frac{1}{2}\right) \prod_{i=1}^{s}\left(1 - \frac{1}{q_i}\right) \geq m \prod_{i=1}^{s+1}\left(1 - \frac{1}{p_i}\right) \geq m \prod_{i=1}^{t}\left(1 - \frac{1}{p_i}\right).$$

This shows (2). Furthermore, we have

$$\begin{aligned} \Phi(n) &\leq 2n \prod_{i=1}^{t} \frac{p_i}{p_i - 1} = 6n \prod_{i=3}^{t} \frac{p_i}{p_i - 1} \leq 6n \left(\frac{5}{5-1}\right)^{v_2(n)} \\ &\leq 6n \cdot \left(\frac{5}{4}\right)^{\log_2(n)} < 6n \cdot 2^{\frac{1}{3}\log_2(n)}. \end{aligned}$$

Thus we obtain (1). Let us show (3). From now on we assume that $n > 3$ is an odd prime. Assume that $m \neq 6$. Since n is odd, it follows from (5.2) that the prime factorization of m is of the form $m = 2q^e$ for some odd prime q. Then $\frac{1}{2}\varphi(m) = q^{e-1}\frac{q-1}{2}$ divides n. Since $n > 3$ is a prime and $m \neq 6$, we find $e = 1$ and $\frac{q-1}{2} = n$. This implies $2n + 1$ must be prime and $m = 4n + 2$. Now the result follows. ☐

Let us consider an upper bound of Φ by using an "analytic" lower bound function of φ given by Rosser and Schoenfeld. If we denote by γ the Euler's constant[7], it is shown in [RS, Theorem 15] that we have[8]

$$\varphi(m) > \frac{m}{e^\gamma \log\log m + \frac{3}{\log\log m}}$$

for $m \geq 3$. We set

$$\Psi(n) := \mathrm{Max}\{m \in \mathbb{Z} \mid \varphi(m) \leq 2n\}.$$

We clearly have $\Phi(n) \leq \Psi(n)$ for all $n > 0$.

[6] A prime number p is called a *Sophie German prime* if $2p + 1$ is also prime. It is not known whether there exist infinitely many Sophie German prime or not. On the other hand, there exist infinitely many prime which is not Sophie German prime. In fact, every prime number p with $p \equiv 1 \bmod 3$ is not Sophie German prime.

[7] $\gamma = \displaystyle\int_1^\infty \left(\frac{1}{[x]} - \frac{1}{x}\right) dx = 0.57721\cdots$. Note also $e^\gamma = 1.78107\cdots$.

[8] More precisely, Theorem 15 of [RS] states that

$$\varphi(m) > \frac{m}{e^\gamma \log\log m + \frac{5}{2\log\log m}} \tag{5.3}$$

for $m \geq 3$ except when m is the product of the first nine primes $m = 223092870 = 2 \cdot 3 \cdot 5 \cdot \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 19 \cdot 23$.

Proposition 5.3. *For any real number $C > 2e^\gamma$, we have*

$$\Psi(n) < Cn \log\log n$$

for any n large enough.

Proof. Put $f(x) = C \log\log x$. Take any integer $N > 0$ which satisfies the following properties: For all $x > N$, it holds

(i) $f(x) > \frac{1}{x} e^{e^2}$ and

(ii) $f(x) > 2e^\gamma(\log\log(xf(x)) + 1)$.

(The assumption $C > 2e^\gamma$ asserts the existence of such N.) Take any integer $n > N$. It suffices to show that n satisfies the desired inequality. Assume that there exists an integer m such that both $\varphi(m) \leq 2n$ and $m \geq nf(n)$ hold. Since we have $e^\gamma > \frac{3}{\log\log x}$ for $x > e^{e^2}$ and $m(\geq nf(n)) > e^{e^2}$, we find

$$\frac{1}{e^\gamma} \cdot \frac{m}{\log\log m + 1} < \frac{m}{e^\gamma \log\log m + \frac{3}{\log\log m}} < \varphi(m) \leq 2n.$$

We also have $\frac{nf(n)}{\log\log(nf(n))+1} \leq \frac{m}{\log\log m+1}$ since the function $\frac{x}{\log\log x+1}$ is strictly increasing for $x > e$ and $m \geq nf(n)(> e^{e^2}) > e$. Hence we obtain

$$\frac{1}{e^\gamma} \cdot \frac{nf(n)}{\log\log(nf(n)) + 1} < 2n,$$

which gives $f(n) < 2e^\gamma(\log\log(nf(n)) + 1)$. This contradicts the condition (ii). Therefore, we conclude that, if $\varphi(m) \leq 2n$, then it holds $m < nf(n)$. This implies $\Psi(n) < nf(n) = Cn \log\log n$. □

Remark 5.4. Consider the case $C = 4$. By studying (i) and (ii) in the above proof more carefully, we can show

$$\Psi(n) < 4n \log\log n$$

for any $n > e^{(1.001e)^9}$.

Here we check the above inequality. The condition (ii) is equivalent to say that

$$(\log x)^{\frac{C}{2e^\gamma}-1} > e\left(1 + \frac{\log(C\log\log x)}{\log x}\right).$$

We assume $x > e^{e^9}$. Since $\frac{C}{2e^\gamma} - 1 > \frac{4}{3.6} - 1 = \frac{1}{9}$ and $\frac{\log(C\log\log x)}{\log x} < 0.001$, the inequality (ii) holds if $(\log x)^{\frac{1}{9}} > 1.001e$, that is, $x > e^{(1.001e)^9}$. Note that (i) clearly holds for such x.

Table 1: $\Phi(n)$

n	$\Phi(n)$	n	$\Phi(n)$	n	$\Phi(n)$
1	$2^1 \cdot 3^1$	41	$2^1 \cdot 83^1$	81	$2^1 \cdot 3^5$
2	$2^2 \cdot 3^1$	42	$2^1 \cdot 3^1 \cdot 7^2$	82	$2^1 \cdot 3^1 \cdot 83^1$
3	$2^1 \cdot 3^2$	43	$2^1 \cdot 3^1$	83	$2^1 \cdot 167^1$
4	$2^1 \cdot 3^1 \cdot 5^1$	44	$2^2 \cdot 3^1 \cdot 23^1$	84	$2^2 \cdot 3^1 \cdot 7^2$
5	$2^1 \cdot 11^1$	45	$2^1 \cdot 31^1$	85	$2^1 \cdot 11^1$
6	$2^1 \cdot 3^1 \cdot 7^1$	46	$2^1 \cdot 3^1 \cdot 47^1$	86	$2^1 \cdot 173^1$
7	$2^1 \cdot 3^1$	47	$2^1 \cdot 3^1$	87	$2^1 \cdot 59^1$
8	$2^2 \cdot 3^1 \cdot 5^1$	48	$2^2 \cdot 3^1 \cdot 5^1 \cdot 7^1$	88	$2^1 \cdot 3^1 \cdot 5^1 \cdot 23^1$
9	$2^1 \cdot 3^3$	49	$2^1 \cdot 3^1$	89	$2^1 \cdot 179^1$
10	$2^1 \cdot 3^1 \cdot 11^1$	50	$2^1 \cdot 5^3$	90	$2^1 \cdot 3^3 \cdot 11^1$
11	$2^1 \cdot 23^1$	51	$2^1 \cdot 103^1$	91	$2^1 \cdot 3^1$
12	$2^1 \cdot 3^2 \cdot 5^1$	52	$2^1 \cdot 3^1 \cdot 53^1$	92	$2^2 \cdot 3^1 \cdot 47^1$
13	$2^1 \cdot 3^1$	53	$2^1 \cdot 107^1$	93	$2^1 \cdot 3^2$
14	$2^1 \cdot 29^1$	54	$2^1 \cdot 3^3 \cdot 7^1$	94	$2^2 \cdot 3^1$
15	$2^1 \cdot 31^1$	55	$2^1 \cdot 11^2$	95	$2^1 \cdot 191^1$
16	$2^3 \cdot 3^1 \cdot 5^1$	56	$2^2 \cdot 3^1 \cdot 29^1$	96	$2^3 \cdot 3^1 \cdot 5^1 \cdot 7^1$
17	$2^1 \cdot 3^1$	57	$2^1 \cdot 3^2$	97	$2^1 \cdot 3^1$
18	$2^1 \cdot 3^2 \cdot 7^1$	58	$2^1 \cdot 3^1 \cdot 59^1$	98	$2^1 \cdot 197^1$
19	$2^1 \cdot 3^1$	59	$2^1 \cdot 3^1$	99	$2^1 \cdot 199^1$
20	$2^1 \cdot 3^1 \cdot 5^2$	60	$2^1 \cdot 3^1 \cdot 7^1 \cdot 11^1$	100	$2^1 \cdot 3^1 \cdot 5^3$
21	$2^1 \cdot 7^2$	61	$2^1 \cdot 3^1$	101	$2^1 \cdot 3^1$
22	$2^1 \cdot 3^1 \cdot 23^1$	62	$2^2 \cdot 3^1$	102	$2^1 \cdot 3^1 \cdot 103^1$
23	$2^1 \cdot 47^1$	63	$2^1 \cdot 127^1$	103	$2^1 \cdot 3^1$
24	$2^1 \cdot 3^1 \cdot 5^1 \cdot 7^1$	64	$2^1 \cdot 3^1 \cdot 5^1 \cdot 17^1$	104	$2^2 \cdot 3^1 \cdot 53^1$
25	$2^1 \cdot 11^1$	65	$2^1 \cdot 131^1$	105	$2^1 \cdot 211^1$
26	$2^1 \cdot 53^1$	66	$2^1 \cdot 3^2 \cdot 23^1$	106	$2^1 \cdot 3^1 \cdot 107^1$
27	$2^1 \cdot 3^4$	67	$2^1 \cdot 3^1$	107	$2^1 \cdot 3^1$
28	$2^1 \cdot 3^1 \cdot 29^1$	68	$2^1 \cdot 137^1$	108	$2^1 \cdot 3^4 \cdot 5^1$
29	$2^1 \cdot 59^1$	69	$2^1 \cdot 139^1$	109	$2^1 \cdot 3^1$
30	$2^1 \cdot 3^2 \cdot 11^1$	70	$2^1 \cdot 3^1 \cdot 71^1$	110	$2^1 \cdot 3^1 \cdot 11^2$
31	$2^1 \cdot 3^1$	71	$2^1 \cdot 3^1$	111	$2^1 \cdot 223^1$
32	$2^4 \cdot 3^1 \cdot 5^1$	72	$2^1 \cdot 3^2 \cdot 5^1 \cdot 7^1$	112	$2^1 \cdot 3^1 \cdot 5^1 \cdot 29^1$
33	$2^1 \cdot 67^1$	73	$2^1 \cdot 3^1$	113	$2^1 \cdot 227^1$
34	$2^2 \cdot 3^1$	74	$2^1 \cdot 149^1$	114	$2^1 \cdot 229^1$
35	$2^1 \cdot 71^1$	75	$2^1 \cdot 151^1$	115	$2^1 \cdot 47^1$
36	$2^1 \cdot 3^3 \cdot 5^1$	76	$2^1 \cdot 3^1 \cdot 5^1$	116	$2^2 \cdot 3^1 \cdot 59^1$
37	$2^1 \cdot 3^1$	77	$2^1 \cdot 23^1$	117	$2^1 \cdot 79^1$
38	$2^2 \cdot 3^1$	78	$2^1 \cdot 3^1 \cdot 79^1$	118	$2^2 \cdot 3^1$
39	$2^1 \cdot 79^1$	79	$2^1 \cdot 3^1$	119	$2^1 \cdot 239^1$
40	$2^1 \cdot 3^1 \cdot 5^1 \cdot 11^1$	80	$2^2 \cdot 3^1 \cdot 5^1 \cdot 11^1$	120	$2^1 \cdot 3^1 \cdot 5^2 \cdot 7^1$

Table 2: $H(n)$

n	$H(n)$
1	$2^4 \cdot 3^1$
2	$2^8 \cdot 3^2 \cdot 5^1$
3	$2^{11} \cdot 3^4 \cdot 5^1 \cdot 7^1$
4	$2^{16} \cdot 3^5 \cdot 5^2 \cdot 7^1$
5	$2^{19} \cdot 3^6 \cdot 5^2 \cdot 7^1 \cdot 11^1$
6	$2^{23} \cdot 3^8 \cdot 5^3 \cdot 7^2 \cdot 11^1 \cdot 13^1$
7	$2^{26} \cdot 3^9 \cdot 5^3 \cdot 7^2 \cdot 11^1 \cdot 13^1$
8	$2^{32} \cdot 3^{10} \cdot 5^4 \cdot 7^2 \cdot 11^1 \cdot 13^1 \cdot 17^1$
9	$2^{35} \cdot 3^{13} \cdot 5^4 \cdot 7^3 \cdot 11^1 \cdot 13^1 \cdot 17^1 \cdot 19^1$
10	$2^{39} \cdot 3^{14} \cdot 5^6 \cdot 7^3 \cdot 11^2 \cdot 13^1 \cdot 17^1 \cdot 19^1$
11	$2^{42} \cdot 3^{15} \cdot 5^6 \cdot 7^3 \cdot 11^2 \cdot 13^1 \cdot 17^1 \cdot 19^1 \cdot 23^1$
12	$2^{47} \cdot 3^{17} \cdot 5^7 \cdot 7^4 \cdot 11^2 \cdot 13^2 \cdot 17^1 \cdot 19^1 \cdot 23^1$
13	$2^{50} \cdot 3^{18} \cdot 5^7 \cdot 7^4 \cdot 11^2 \cdot 13^2 \cdot 17^1 \cdot 19^1 \cdot 23^1$
14	$2^{54} \cdot 3^{19} \cdot 5^8 \cdot 7^4 \cdot 11^2 \cdot 13^2 \cdot 17^1 \cdot 19^1 \cdot 23^1 \cdot 29^1$
15	$2^{57} \cdot 3^{21} \cdot 5^8 \cdot 7^5 \cdot 11^3 \cdot 13^2 \cdot 17^1 \cdot 19^1 \cdot 23^1 \cdot 29^1 \cdot 31^1$
16	$2^{64} \cdot 3^{22} \cdot 5^9 \cdot 7^5 \cdot 11^3 \cdot 13^2 \cdot 17^2 \cdot 19^1 \cdot 23^1 \cdot 29^1 \cdot 31^1$
17	$2^{67} \cdot 3^{23} \cdot 5^9 \cdot 7^5 \cdot 11^3 \cdot 13^2 \cdot 17^2 \cdot 19^1 \cdot 23^1 \cdot 29^1 \cdot 31^1$
18	$2^{71} \cdot 3^{26} \cdot 5^{10} \cdot 7^6 \cdot 11^3 \cdot 13^3 \cdot 17^2 \cdot 19^2 \cdot 23^1 \cdot 29^1 \cdot 31^1 \cdot 37^1$
19	$2^{74} \cdot 3^{27} \cdot 5^{10} \cdot 7^6 \cdot 11^3 \cdot 13^3 \cdot 17^2 \cdot 19^2 \cdot 23^1 \cdot 29^1 \cdot 31^1 \cdot 37^1$
20	$2^{79} \cdot 3^{28} \cdot 5^{12} \cdot 7^6 \cdot 11^4 \cdot 13^3 \cdot 17^2 \cdot 19^2 \cdot 23^1 \cdot 29^1 \cdot 31^1 \cdot 37^1 \cdot 41^1$
21	$2^{82} \cdot 3^{30} \cdot 5^{12} \cdot 7^8 \cdot 11^4 \cdot 13^3 \cdot 17^2 \cdot 19^2 \cdot 23^1 \cdot 29^1 \cdot 31^1 \cdot 37^1 \cdot 41^1 \cdot 43^1$
22	$2^{86} \cdot 3^{31} \cdot 5^{13} \cdot 7^8 \cdot 11^4 \cdot 13^3 \cdot 17^2 \cdot 19^2 \cdot 23^2 \cdot 29^1 \cdot 31^1 \cdot 37^1 \cdot 41^1 \cdot 43^1$
23	$2^{89} \cdot 3^{32} \cdot 5^{13} \cdot 7^8 \cdot 11^4 \cdot 13^3 \cdot 17^2 \cdot 19^2 \cdot 23^2 \cdot 29^1 \cdot 31^1 \cdot 37^1 \cdot 41^1 \cdot 43^1 \cdot 47^1$
24	$2^{95} \cdot 3^{34} \cdot 5^{14} \cdot 7^9 \cdot 11^4 \cdot 13^4 \cdot 17^3 \cdot 19^2 \cdot 23^2 \cdot 29^1 \cdot 31^1 \cdot 37^1 \cdot 41^1 \cdot 43^1 \cdot 47^1$
25	$2^{98} \cdot 3^{35} \cdot 5^{14} \cdot 7^9 \cdot 11^5 \cdot 13^4 \cdot 17^3 \cdot 19^2 \cdot 23^2 \cdot 29^1 \cdot 31^1 \cdot 37^1 \cdot 41^1 \cdot 43^1 \cdot 47^1$

Table 3: $G(n)$ (for $p \neq 3$)

n	$G(n)$
1	$2^4 \cdot 3^1$
2	$2^9 \cdot 3^6 \cdot 5^1 \cdot 13^1$
3	$2^{13} \cdot 3^{15} \cdot 5^1 \cdot 7^1 \cdot 11^2 \cdot 13^2$
4	$2^{19} \cdot 3^{28} \cdot 5^2 \cdot 7^1 \cdot 11^2 \cdot 13^2 \cdot 41^1 \cdot 1093^1$
5	$2^{23} \cdot 3^{45} \cdot 5^2 \cdot 7^1 \cdot 11^4 \cdot 13^3 \cdot 41^1 \cdot 61^1 \cdot 757^1 \cdot 1093^1$
6	$2^{28} \cdot 3^{66} \cdot 5^3 \cdot 7^2 \cdot 11^4 \cdot 13^4 \cdot 23^1 \cdot 41^1 \cdot 61^1 \cdot 73^1 \cdot 757^1 \cdot 1093^1 \cdot 3851^1$
7	$2^{32} \cdot 3^{91} \cdot 5^3 \cdot 7^2 \cdot 11^4 \cdot 13^4 \cdot 23^1 \cdot 41^1 \cdot 61^1 \cdot 73^1 \cdot 547^1 \cdot 757^1 \cdot 1093^2 \cdot 3851^1 \cdot 797161^1$

References

[CCM] M, Chou, P.-L. Clark and M. Milosevic, *Acyclotomy of torsion in the CM case*, Ramanujan J. 55, **3** (2021), 1015–1037.

[Ch] M. Chou, *Torsion of rational elliptic curves over the maximal abelian extension of* $\mathbb{Q}$, Pacific J. Math. 302, no. 2 (2019), 481–509.

[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.

[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.

[KL] N.-M. Katz and S. Lang, *Finiteness theorems in geometric classfield theory*, with an appendix by Kenneth A. Ribet, Enseign. Math. (2) 27 (1981), no. 3-4, 285–319.

[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.

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

[Ne] J. Neukirch, *Algebraic Number Theory*, Translated from the 1992 German original and with a note by Norbert Schappacher. With a foreword by G. Harder. Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], 322. Springer-Verlag, Berlin, 1999.

[Oz1] Y. Ozeki, *Torsion of abelian varieties and Lubin-Tate extensions*, J. Number Theory **207** (2020), 282–293.

[Oz2] Y. Ozeki, *Bounds on torsion of CM abelian varieties over a p-adic field with values in a field of p-power roots*, arXiv:2209.01811

[RS] J.-B. Rosser and L. Schoenfeld, *Approximate formulas for some functions of prime numbers*, Illinois J. Math. **6** (1962), 64–94.

[Se] J.-P. Serre, *Local fields*, Translated from the French by Marvin Jay Greenberg. Graduate Texts in Mathematics, 67. Springer-Verlag, New York-Berlin, 1979.

[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.