Pacific Journal of Mathematics

EXPLICIT BOUNDS ON TORSION OF CM ABELIAN VARIETIES OVER p-ADIC FIELDS WITH VALUES IN LUBIN–TATE EXTENSIONS

YOSHIYASU OZEKI

Volume 330 No. 1 May 2024

PACIFIC JOURNAL OF MATHEMATICS
Vol. 330, No. 1, 2024
https://doi.org/10.2140/pjm.2024.330.171

EXPLICIT BOUNDS ON TORSION OF CM ABELIAN VARIETIES OVER p-ADIC FIELDS WITH VALUES IN LUBIN–TATE EXTENSIONS

YOSHIYASU OZEKI

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 $L = K(\mu_{p^\infty})$). 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-primary 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 (that is, a finite extension of $\mathbb{Q}_p$). It is a theorem of Mattuck [1955] 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. We study some properties of the torsion subgroup $A(L)_{\mathrm{tor}}$ of $A(L)$. Clark and Xarles [2008] gave an explicit upper bound of the order of $A(L)_{\mathrm{tor}}$ of $A(L)$ in terms of p, g and some numerical invariants of L if A has anisotropic reduction (here, we say that A has anisotropic reduction if its Néron special fiber does not contain a copy of $\mathbb{G}_m$). This includes the case where A has potential good reduction. We consider the case where L/K is *of infinite degree*. There are some situations in which the torsion part $A(L)_{\mathrm{tor}}$ is finite. Suppose that A has potential good reduction. It is a theorem of Imai [1975] that $A(K(\mu_{p^\infty}))_{\mathrm{tor}}$ 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 [2013] showed that $A(K(\sqrt[p^\infty]{K}))_{\mathrm{tor}}$ 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 [Ozeki 2024] that there exists a "uniform" bound of the order of $A(K(\sqrt[p^\infty]{K}))_{\mathrm{tor}}$ under the assumption that A has complex multiplication. (Here we say that A has complex multiplication

MSC2020: 11G10.
Keywords: abelian varieties, Lubin–Tate extensions.

if there exists a ring homomorphism $F \to \mathbb{Q} \otimes_{\mathbb{Z}} \mathrm{End}_{\overline{K}}(A)$ 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 $A(K(\mu_{p^\infty}))_{\mathrm{tor}}$ and $A(K(\sqrt[p^\infty]{K}))_{\mathrm{tor}}$ 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 $A(K(\mu_{p^\infty}))_{\mathrm{tor}}$ 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 $A(K(\mu_{p^\infty}))_{\mathrm{tor}}$.

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 by adjoining all π-power torsion points of the Lubin–Tate formal group associated with π; see [Yoshida 2008] for more details). 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

$$\Phi(n) := \mathrm{Max}\{m \in \mathbb{Z}_{>0} \mid \varphi(m) \text{ divides } 2n\},$$
$$H(n) := \gcd\{\#\mathrm{GSp}_{2n}(\mathbb{Z}/N\mathbb{Z}) \mid N \geq 3\}.$$

Here, φ is 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 [1992, Corollary 3.3] 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 [1962] 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] *and*

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

Denote by $0 < \mu < p$ the minimum integer such that $(q_k^{-1}\mathrm{Nr}_{k/\mathbb{Q}_p}(\pi))^\mu = 1$. For any g-dimensional abelian variety A over a p-adic field K with complex multiplication,

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

where

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

In particular,

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

[1] This condition is equivalent to saying that some finite extension of k_π contains $\mathbb{Q}_p(\mu_{p^\infty})$ (see [Ozeki 2020, Lemma 2.7(2)]).

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 field $K(\sqrt[p^\infty]{K})$ discussed in Kubo and Taguchi, which gives a refinement of the main theorem of [Ozeki 2024].

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*,

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

We can consider some further topics. For example, we do not know what will happen if we remove the CM assumption from the 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 cannot remove the CM assumption from our arguments. To overcome this obstruction, it seems to be helpful for us to study the case of (not necessarily CM) elliptic curves. We will study this case in future work. We are also interested in giving the list of the groups that appear 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 given in [Katz and Lang 1981], 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 $\mathbb{Q}$.)

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*

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

where

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

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 [2019] gave the complete list of the groups that appear 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 [Chou et al. 2021].

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 $\mathcal{O}_F$ the ring of integers of F. 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 a finite 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

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 $\mathrm{Gal}(K^{\mathrm{ab}}/K)$. Denote by Art_K the local Artin map $K^\times \to \mathrm{Gal}(K^{\mathrm{ab}}/K)$. We set $\psi_K := \psi \circ \mathrm{Art}_K$. Denote by $\hat{K}^\times$ the profinite completion of $K^\times$. Note that the local Artin map induces a topological isomorphism $\mathrm{Art}_K : \hat{K}^\times \xrightarrow{\sim} \mathrm{Gal}(K^{\mathrm{ab}}/K)$. For a uniformizer π_K of K, denote by $\chi_{\pi_K} : G_K \to \mathcal{O}_K^\times$ the Lubin–Tate character associated with π_K (see [Serre 1989, Chapter III, A4]). 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 $\chi_\pi : G_k \to \mathcal{O}_k^\times$ is k_π, and k_π is a totally ramified abelian extension of k.

Proposition 2.1. *Let $\psi_1, \dots, \psi_n : G_K \to \overline{\mathbb{Q}}_p^\times$ be continuous characters. Then*

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

Proof. This is [Ozeki 2024, Proposition 2.1] but we include a proof here for 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 $\hat{k}^\times = \pi^{\hat{\mathbb{Z}}} \times \mathcal{O}_k^\times$ of index $[M : k] = f_{Kk/k}$. Thus it holds that $\mathrm{Art}_k^{-1}(\mathrm{Gal}(k^{\mathrm{ab}}/M)) = \pi^{f_{Kk/k}\hat{\mathbb{Z}}} \times \mathcal{O}_k^\times$. Since $\mathrm{Art}_k^{-1}(\mathrm{Gal}(k^{\mathrm{ab}}/k_\pi)) = \pi^{\hat{\mathbb{Z}}}$, we obtain that $\mathrm{Art}_k^{-1}(\mathrm{Gal}(k^{\mathrm{ab}}/Mk_\pi)) = \pi^{f_{Kk/k}\hat{\mathbb{Z}}}$. 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 that $\mathrm{Res}_{Kk/k}^{-1}(\mathrm{Gal}(k^{\mathrm{ab}}/Mk_\pi)) = \mathrm{Gal}((Kk)^{\mathrm{ab}}/Kk_\pi)$, and therefore we find that $\mathrm{Art}_{Kk}^{-1}\big(\mathrm{Gal}((Kk)^{\mathrm{ab}}/Kk_\pi)\big) = \mathrm{Nr}_{Kk/k}^{-1}(\pi^{f_{Kk/k}\hat{\mathbb{Z}}})$. Now the lemma follows from

$$\mathrm{Min}\left\{ \sum_{i=1}^{n} v_p(\psi_i(\sigma)-1) \,\middle|\, \sigma \in G_{Kk_\pi} \right\} = \mathrm{Min}\left\{ \sum_{i=1}^{n} v_p(\psi_{i,Kk}\circ \mathrm{Art}_{Kk}^{-1}(\sigma)-1) \,\middle|\, \sigma \in \mathrm{Gal}((Kk)^{\mathrm{ab}}/Kk_\pi) \right\}. \quad \square$$

We often use p-adic Hodge theory, which plays an important role in this paper. For the basic notion of p-adic Hodge theory, it is helpful for the reader to refer to [Fontaine 1994a; 1994b]. Let B_{cris} be the Fontaine's p-adic period ring and set $D_{\mathrm{cris}}^K(V) := (B_{\mathrm{cris}} \otimes_{\mathbb{Q}_p} V)^{G_K}$ for any $\mathbb{Q}_p$-representation V of G_K. Let us denote by K_0 the maximal unramified subextension of $K/\mathbb{Q}_p$ and denote by φ_{K_0} the arithmetic Frobenius map of K_0, that is, the (unique) lift of the p-th power map on the residue field of K_0. Since $B_{\mathrm{cris}}^{G_K} = K_0$, $D_{\mathrm{cris}}^K(V)$ is a K_0-vector space. Moreover, $D_{\mathrm{cris}}^K(V)$ is a filtered φ-module over K; it is of finite dimension over K_0, it is equipped with a bijective φ_{K_0}-semilinear Frobenius operator φ and it is equipped with a decreasing exhaustive and separated filtration on $D_{\mathrm{cris}}^K(V)\otimes_{K_0} K$. We say that V is crystalline if the equality $\dim_{\mathbb{Q}_p} V = \dim_{K_0} D_{\mathrm{cris}}^K(V)$ holds. Let M be a finite extension of $\mathbb{Q}_p$ and $\psi : G_K \to M^\times$ a continuous character. We denote by $M(\psi)$ the $\mathbb{Q}_p$-representation of G_K underlying a 1-dimensional M-vector space endowed with an M-linear action by G_K via ψ. We say that ψ is crystalline if $M(\psi)$ is crystalline. On the other hand, we denote by $\underline{K}^\times$ the Weil restriction $\mathrm{Res}_{K/\mathbb{Q}_p}(\mathbb{G}_m)$. This is an algebraic torus such that, for a $\mathbb{Q}_p$-algebra R, the R-valued points $\underline{K}^\times(R)$ of $\underline{K}^\times$ is $\mathbb{G}_m(R\otimes_{\mathbb{Q}_p} K)$.

Proposition 2.2. *Let $\psi : G_K \to M^\times$ be a continuous character.*

(1) *$M(\psi)$ is crystalline if and only if there exists a* (*necessarily unique*) *$\mathbb{Q}_p$-homomorphism $\psi_{\mathrm{alg}} : \underline{K}^\times \to \underline{M}^\times$ such that ψ_K and ψ_{alg}* (*on $\mathbb{Q}_p$-points*) *coincide on $\mathcal{O}_K^\times$* ($\subset \underline{K}^\times(\mathbb{Q}_p)$).

(2) *Assume $M(\psi)$ is crystalline, and let ψ_{alg} be as in* (1). (*Note $M(\psi^{-1})$ is also crystalline.*) *The filtered φ-module $D_{\mathrm{cris}}^K(M(\psi^{-1})) = (B_{\mathrm{cris}}\otimes_{\mathbb{Q}_p} M(\psi^{-1}))^{G_K}$ 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 $\psi_K(\pi_K)\cdot\psi_{\mathrm{alg}}^{-1}(\pi_K) \in M^\times$. Here, π_K is any uniformizer of K.*

Proof. This is Proposition B.4 of [Conrad 2011]. $\square$

Let $\psi : G_K \to M^\times$ be a crystalline character. For any $\sigma \in \Gamma_M$, let $\chi_{\sigma M} : I_{\sigma M} \to \sigma M^\times$ 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

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

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

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

Theorem 2.3. *Let $\psi_1, \dots, \psi_n : G_K \to M^\times$ 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 set of 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) *$\mathrm{Min}\{v_p(h_{i,\sigma} - h_{i,\tau}) \mid \sigma, \tau \in \Gamma_M\} \leq h$ for each i.*

Then:

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

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

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 $0 \leq s(x) \leq n$ such that for every $1 \leq i \leq n$,*

$$v_p(\psi_{i,K}(x \hat{\omega}^{p^{s(x)}})^{-1} - 1) \leq n + \delta_{(i)} + C(d_K, M, h). \tag{2-3}$$

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 $1 \le r \le n$ 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 $1 \le \ell \le d_M$. (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 $1 \le \ell \le d_M$ and $\tau \in \Gamma_M$. Here, exp denotes the p-adic exponential map (see [Neukirch 1999, Chapter II, Proposition 5.5]). By construction, $\omega_\ell^{\tau} \in \ker \mathrm{Nr}_{M/\mathbb{Q}_p}$.

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

Proof. We see

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

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

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

On the other hand, we have

$$\begin{aligned}\exp(y_{r,\ell}^{\tau}) = \exp\biggl(\sum_{\sigma\in\Gamma_M} m_{r,\sigma}^{\tau}(\sigma^{-1}x')^{\ell-1}\biggr) &= \prod_{\sigma\in\Gamma_M} \exp((\sigma^{-1}x')^{\ell-1})^{m_{r,\sigma}^{\tau}} \\ &= \prod_{\sigma\in\Gamma_M} \sigma^{-1}\omega_\ell^{m_{r,\sigma}^{\tau}}.\end{aligned}$$ □

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*

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

Proof. Fix r. By assumption (i), there exist $\tau_1, \tau_2 \in \Gamma_M$ such that $h_{r,\tau_1} \neq h_{r,\tau_2}$. Choose τ_1 and τ_2 so that $v_p(h_{r,\tau_1} - h_{r,\tau_2}) = \mathrm{Min}\{v_p(h_{r,\sigma} - h_{r,\tau}) \mid \sigma, \tau \in \Gamma_M\}$, and set $\tau := \tau_2\tau_1^{-1} \in \Gamma_M$. We write $\Gamma_M = \{\tau_1, \tau_2, \dots, \tau_{d_M}\}$. Note that $m_{r,\tau_1}^{\tau} = d_{K/M}(h_{r,\tau_2} - h_{r,\tau_1})$ 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

$$(y_{r,1}^{\tau} \cdots y_{r,d_M}^{\tau}) = (m_{r,\tau_1}^{\tau} \cdots m_{r,\tau_{d_M}}^{\tau})X \tag{2-4}$$

and

$$\det X = \prod_{1\le i<j\le d_M} (\tau_j^{-1}x' - \tau_i^{-1}x') = (p')^{\frac{1}{2}d_M(d_M-1)} \prod_{1\le i<j\le d_M} (\tau_j^{-1}x - \tau_i^{-1}x).$$

We also have

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

(see [Serre 1979, Chapter 3, Section 6, Proposition 13]), where $\mathcal{D}_{M/\mathbb{Q}_p}$ is the different ideal of $M/\mathbb{Q}_p$. We find

$$v_p(\det X) \le \frac{1}{2}d_M\Big(d_M + v_p(e_M) - \frac{1}{e_M} + v_p(2)(d_M-1)\Big). \tag{2-5}$$

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:

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

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

For $r \ge 4$,

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

We claim 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
$$\begin{aligned} v_p\left(\sum_{r=1}^{n} s_r y_{i,\ell_r}^{\tau_r}\right) &= \operatorname{Min}\left\{ v_p\left(\sum_{r=1}^{i-1} s_r y_{i,\ell_r}^{\tau_r}\right), v_p(s_i y_{i,\ell_i}^{\tau_i})\right\} \\ &\le v_p(p s_{i-1} y_{i,\ell_i}^{\tau_i}) \le 1 + v_p(s_{i-1}) + C(d_K, M, h) \end{aligned}$$
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 $v_p(\sum_{r=1}^{n} s_r y_{3,\ell_r}^{\tau_r}) \le v_p(p y_{3,\ell_3}^{\tau_3}) \le 1 + C(d_K, M, h) = \delta_{(3)} + C(d_K, M, h)$.

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

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

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

To show Theorem 2.3(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 the 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. 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 $p \neq 2$ or $p = 2$, respectively. Let $\mu \geq 1$ be the smallest integer*[2] *so that*

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

Assume the following conditions:[3]

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

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

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:

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

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

Remark 3.2. (1) $mg \leq L_g(m) < g(m + 1 + v_p(2))$ for any prime p and $m \geq 1$, and $L_g(m) < g(m+1)$ if $(p, m) \neq (2, 1), (2, 2)$.

(2) Moreover,[4]

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

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

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

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

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

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

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

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

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

Then

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

where

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

Proof. Put $T=T_p(A)$ and $V=V_p(A)$ for brevity. Let $\rho: G_K\to \mathrm{GL}_{\mathbb{Z}_p}(T)$ be the continuous homomorphism obtained by the G_K-action on T. Fix an isomorphism $\iota: T\xrightarrow{\sim}\mathbb{Z}_p^{\oplus 2g}$ of $\mathbb{Z}_p$-modules. We have an isomorphism $\hat{\iota}:\mathrm{GL}_{\mathbb{Z}_p}(T)\simeq \mathrm{GL}_{2g}(\mathbb{Z}_p)$ relative to ι. We abuse notation by writing ρ for the composite map $G_K\to \mathrm{GL}_{\mathbb{Z}_p}(T)\simeq \mathrm{GL}_{2g}(\mathbb{Z}_p)$ 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 saying 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 $\sigma\in G_{G_{Kk_{\pi}}}$. Thus $\det(\rho(\sigma)-E)P\in p^nT$ 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, we recall that A has complex multiplication and all the endomorphisms of A are defined over K. Thus there exists an injective ring homomorphism from a number field F of degree $2g$ into $\mathbb{Q}\otimes_{\mathbb{Z}}\mathrm{End}_K(A)$. By [Serre and Tate 1968, Theorem 5(i)], 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 $V\simeq\bigoplus_{i=1}^n V_i$ 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 the F_i-action. Let $\rho_i : G_K \to \mathrm{GL}_{\mathbb{Q}_p}(V_i)$ be the homomorphism obtained by the G_K-action on V_i. Since ρ_i is abelian, it follows that $(V_i \otimes_{\mathbb{Q}_p} \overline{\mathbb{Q}}_p)^{\mathrm{ss}} \simeq \bigoplus_{j=1}^{d_{F_i}} \overline{\mathbb{Q}}_p(\psi_{i,j})$ for some continuous characters $\psi_{i,j} : G_K \to \overline{\mathbb{Q}}_p^{\times}$. Here, the superscript "ss" stands for the semisimplification. 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 $\tau_{k\ell} \in G_{\mathbb{Q}_p}$.

(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 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,

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

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 $M^{\times}$, that is, $\psi_i : G_K \to M^{\times}$. 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 n natural numbers is divisible 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

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

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

$$\begin{aligned} c &\le \mathrm{Min}\{v_p(\det(\rho(\sigma) - E)) \mid \sigma \in G_{K_M k_\pi}\} \\ &= \mathrm{Min}\left\{ \sum_{i=1}^{n} d_{F_i} v_p(\psi_i(\sigma) - 1) \;\middle|\; \sigma \in G_{K_M k_\pi} \right\} \\ &\le \mathrm{Min}\left\{ \sum_{i=1}^{n} d_{F_i} v_p(\psi_{i,K_M k}(\pi\omega)^{-1} - 1) \;\middle|\; \omega \in \ker \mathrm{Nr}_{K_M k/k} \right\} \\ &\le \mathrm{Min}\left\{ \sum_{i=1}^{n} d_{F_i} v_p(\psi_{i,K_M k}(\pi\omega)^{-1} - 1) \;\middle|\; \omega \in \ker \mathrm{Nr}_{M/\mathbb{Q}_p} \right\} \\ &\le \mathrm{Min}\left\{ \sum_{i=1}^{n} d_{F_i} v_p(\psi^{\mu}_{i,K_M k}(\pi\omega)^{-1} - 1) \;\middle|\; \omega \in \ker \mathrm{Nr}_{M/\mathbb{Q}_p} \right\}. \end{aligned} \tag{3-3}$$

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 (see [Fontaine 1982, Section 6]; see also [Coleman and Iovita 1999, Theorem 1]). By rearranging the numbering of subscripts, we may suppose the following situation for some $0 \le r \le n$.

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

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

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

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

Proof. In this proof we set $L := K_M k$. We know that the morphism $\psi_{i,\mathrm{alg}} : \underline{L}^{\times} \to \underline{M}^{\times}$ corresponding to $\psi_i|_{G_L}$ is trivial or $\mathrm{Nr}^{-1}_{L/\mathbb{Q}_p}$ 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

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

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 [Ozeki 2024] that $\psi^{\mu}_{i,L}(\pi\omega)^{-1}$ is a unit root of the characteristic polynomial $f(T)$ of the geometric Frobenius endomorphism of $\bar{A}_{/\mathbb{F}_{L'}}$. Since $f(1) = \#\bar{A}(\mathbb{F}_{q_{L'}})$, we see $v_p(\psi^{\mu}_{i,L}(\pi\omega)^{-1} - 1) \le v_p(\#\bar{A}(\mathbb{F}_{q_{L'}})) \le [\log_p \#\bar{A}(\mathbb{F}_{q_{L'}})]$. It follows from the Weil bound that $v_p(\psi^{\mu}_{i,L}(\pi\omega)^{-1} - 1) \le L_g(f_{L'})$. Since we have $f_{L'} = \mu e_{L/k} f_L = d_{L/Kk} \cdot \mu \cdot d_{Kk/k} f_k \le (2g)! \cdot \mu \cdot d_{Kk/k} f_k$. 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 $\mathrm{Nr}^{-1}_{L/\mathbb{Q}_p}$ on $\mathbb{Q}_p$-points. If we set $\beta := q_k^{-1}\mathrm{Nr}_{k/\mathbb{Q}_p}(\pi)$, we find

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

It again follows from Lemma 9 of [Ozeki 2024] 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 $f^{\vee}(1) = \#\overline{A^{\vee}}(\mathbb{F}_{q_{L'}})$, the same argument as in (I) shows that $v_p((\alpha_i^{-1}q_L)^{\mu e_{L/k}} - 1) \le L_g(f_{L'}) \le L_g((2g)! \cdot \mu \cdot d_{Kk/k} f_k)$. 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 $v_p(\psi^{\mu}_{i,L}(\pi\omega)^{-1} - 1) = v_p((\alpha_i^{-1}q_L)^{\mu e_{L/k}} - 1) \le L_g((2g)! \cdot \mu \cdot d_{Kk/k} f_k)$, as desired. □

By (3-3) and the lemma, in the case where $r = 0$, we have

$$c \le \sum_{i=1}^{n} d_{F_i} L_g((2g)! \cdot \mu \cdot d_{Kk/k} f_k) = 2g L_g((2g)! \cdot \mu \cdot d_{Kk/k} f_k). \tag{3-4}$$

In the rest of the proof, we assume $r > 0$. By (3-3) and the lemma again, we have

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

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

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

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

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

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

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

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

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

Note that this inequality holds also for the case $r = 0$ by (3-4). Now the proposition follows from (3-1). □

General cases. We show Theorems 3.1 and 1.2. For this, we need the following observations given by Serre and Tate [1968] and Silverberg [1992].

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 semistable 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* A *has potential good reduction. Let* $\rho_{A,\ell} : G_K \to \mathrm{GL}_{\mathbb{Z}_p}(T_\ell(A))$ *be the continuous homomorphism defined by the* G_K*-action on the Tate module* $T_\ell(A)$ *for any prime* ℓ.

- (i) *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.
- (ii) *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* A *has complex multiplication. 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. Item (1) follows from [Silverberg 1992, Theorem 4.1] and Raynaud's criterion of semistable reduction [SGA 7_{I} 1972, Proposition 4.7]. Item (2) is [Silverberg 1992, 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 assertions in (3) are consequences of results given in Sections 2 and 4 of [Serre and Tate 1968] but some of them are not directly mentioned in loc. cit. Thus we give a proof here, just in case. The first statement related to H_ℓ in (3)(i) is [Serre and Tate 1968, Section 2, Theorem 2, p. 496]. 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 semidirect 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)(i). Next we show (3)(ii). By assumptions on A, there exists a number field F of degree $2g$ which is a subalgebra of $\mathbb{Q} \otimes_{\mathbb{Z}} \mathrm{End}_K(A)$. It follows from [Serre and Tate 1968, Theorem 5(i)] that $V_\ell(A)$ 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 [Serre and Tate 1968, Section 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 $c \le m \le \Phi(g)$, 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 $d_{L/K} \le \Phi(g)H(g)$, A has good reduction over L, and all the endomorphisms of A are defined over L. In addition, we have

$$\begin{aligned} v_p\big((q_k^{-1}\mathrm{Nr}_{k/\mathbb{Q}_p}(\pi))^{\mu} - 1\big) &> g \cdot (2g)! \cdot \Phi(g)H(g) \cdot \mu \cdot d_{Kk/k} f_k \\ &= L_g\big((2g)! \cdot \Phi(g)H(g) \cdot \mu \cdot d_{Kk/k} f_k\big) \\ &\ge L_g((2g)! \cdot \mu \cdot d_{Lk/k} f_k) \end{aligned}$$

by assumption (i) and Remark 3.2(2). So 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,

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

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

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

for the proof but this is clear. □

Remark 3.6. In the proof of Theorem 3.1, we referred to 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 to the field $K(A[m])$ instead of the above L. Since we have a natural embedding from $\mathrm{Gal}(K(A[m])/K)$ into $\mathrm{GL}(A[m]) \simeq \mathrm{GL}_{2g}(\mathbb{Z}/m\mathbb{Z})$, we obtain a bound for the extension degree of $K(A[m])/K$; we have $[K(A[m]):K] \le G(g)$, where

$$G(n) := \begin{cases} \#\mathrm{GL}_{2n}(\mathbb{Z}/3\mathbb{Z}) = \prod_{i=0}^{2n-1}(3^{2n} - 3^i) & \text{if } p \ne 3, \\ \#\mathrm{GL}_{2n}(\mathbb{Z}/4\mathbb{Z}) = 2^{4n^2}\prod_{i=0}^{2n-1}(2^{2n} - 2^i) & \text{if } p = 3 \end{cases}$$

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). 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,

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

Next we show Theorem 1.2.

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

<u>Step 1</u>: 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

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

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 $\rho : G_K \to \mathrm{GL}_{\mathbb{Z}_p}(T_p(A)) \simeq \mathrm{GL}_{2g}(\mathbb{Z}_p)$, $M/\mathbb{Q}_p$ and $\psi_1, \dots, \psi_n : G_K \to M^\times$ 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 $\chi_p : G_K \to \mathbb{Z}_p^\times$ 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. $\chi_p(\sigma_0) - 1 = p^\nu$ *for some* $\sigma_0 \in G$.

Proof. We set

$$K' := \begin{cases} K(\mu_p) & \text{if } p \neq 2, \\ K(\mu_4) & \text{if } p = 2. \end{cases}$$

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 $c \le \mathrm{Min}\{v_p(\det(\rho(\sigma)^{p^\nu} - E)) \mid \sigma \in G_{K(\mu_{p^\infty})}\}$. Mimicking the arguments for inequalities (3-3), we find

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

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 $d_{L/K} \le \Phi(g)H(g)$, 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

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

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

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 semisimplification 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 such 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,

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

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 $(V \otimes_{\mathbb{Q}_p} M)^{\mathrm{ss}} \simeq \bigoplus_{i=1}^{2g} M(\psi_i)$ for some continuous crystalline characters $\psi_i : G_K \to M^\times$. 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 $c \leq \sum_{i=1}^{2g} v_p(\psi_{i,Kk}^{\mu}(\pi)^{-1} - 1)$. 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 $\psi_{i,Kk}^{\mu}(\pi)^{-1}$ is a unit root of the characteristic polynomial $f(T)$ of the geometric Frobenius endomorphism of $\bar{A}_{/\mathbb{F}_{K'}}$; otherwise, $\psi_{i,Kk}^{\mu}(\pi)^{-1}$ 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 $f(1) = \#\bar{A}(\mathbb{F}_{q_{K'}})$ and $f^\vee(1) = \#\overline{A^\vee}(\mathbb{F}_{q_{K'}})$, 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 $c \leq \sum_{i=1}^{2g} v_p(\psi_{i,Kk}^{\mu}(\pi)^{-1} - 1) \leq 2g L_g(\mu d_{Kk/k} f_k)$. 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. 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 semistable 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 semistable 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 [Katz and Lang 1981, Appendix, Lemma] that $L_p = K'(\mu_{p^\infty})$.

(1) Here we mainly follow Ribet's arguments in [Katz and Lang 1981]. 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 the assumption $A[p]^H \neq O$. Let W be a simple G-submodule of $A[p]^H$. Ribet showed in the proof of Theorem 2 of [Katz and Lang 1981] that, since A has semistable 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 $\bar{\chi}_p^n$ for some $0 \leq n \leq p-1$, where $\bar{\chi}_p$ is the mod p cyclotomic character. Moreover, since A has good reduction at some finite place of K' above p ($\neq 2$) and p is unramified in K', it follows from the classification of Tate and Oort [1970, pp. 15–16] 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 [Serre and Tate 1968, Section 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 $p < (1+\sqrt{p_0}^{dh})^{2g}$. This finishes the proof.

(2) Let A be an abelian variety as in the statement. Since A has good reduction everywhere over K, it follows from the Néron–Ogg–Shafarevich criterion 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

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

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 $H(n)$:

$$\Phi(n) := \mathrm{Max}\{m \in \mathbb{Z}_{>0} \mid \varphi(m) \text{ divides } 2n\},$$
$$H(n) := \gcd\{\#\mathrm{GSp}_{2n}(\mathbb{Z}/N\mathbb{Z}) \mid N \geq 3\}.$$

Here, φ is the Euler's totient function. The values of $\Phi(n)$, $H(n)$ (and $G(n)$ for $p \neq 3$; see Remark 3.6) for small n are given in Tables 1–3. In this section, we study some upper bounds of Φ and H.

The function H. For the function H, we refer to results of [Silverberg 1992, Sections 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 $q \leq 2n+1$,

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

Moreover, we have:

Theorem 5.1 [Silverberg 1992, Corollary 3.3]. *We have*

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

for any $n > 0$.

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

$$\Phi(n) = \mathrm{Max}\big\{m \in \mathbb{Z}_{>0} \mid \varphi(m) \text{ divides } 2n, \text{ and } m = 2^r x, \text{ where } r \geq 1 \text{ and } x \geq 3 \text{ is odd}\big\}. \tag{5-1}$$

We show some elementary formulas.

Proposition 5.2. (1) $\Phi(1) = 6$ *and* $6 \le \Phi(n) < 6n\sqrt[3]{n}$ *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*

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

In particular, $\Phi(n) \le 6n$ *if* n *is odd.*

(3) *If* $n > 3$ *is an odd prime*, *we have*[5]

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

Proof. To check $\Phi(1) = 6$ is an easy exercise. Since $\varphi(6) = 2 \mid 2n$, we have $\Phi(n) \ge 6$ for any n. Suppose that $n > 1$. We take an even integer $m > 0$ of the form $2^r x$, where $r \ge 1$ and $x \ge 3$ 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 $r, s, e_1, \ldots, e_s \ge 1$. 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 $v_2(2n) \ge r - 1 + s$ and thus

$$r + s \le v_2(n) + 2. \tag{5-2}$$

Then we find

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

This shows (2). Furthermore, we have

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

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

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

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

Table 1. $\Phi(n)$.

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 Euler's constant,[6] it is shown in [Rosser and Schoenfeld 1962, Theorem 15] that[7]

$$\varphi(m) > \frac{m}{e^{\gamma}\log\log m + \frac{3}{\log\log m}} \tag{5-3}$$

for $m \geq 3$. We set

$$\Psi(n) := \mathrm{Max}\{m \in \mathbb{Z}_{>0} \mid \varphi(m) \leq 2n\}.$$

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

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

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

for any n large enough.

Proof. The result should be well known as a consequence of Mertens' theorem:

$$\liminf_n \frac{\varphi(n)\log\log n}{n} = e^{-\gamma}.$$

Using (5-3) instead of Mertens' theorem, we can obtain a slightly refined statement (see Remark 5.4). So, for later use, we write down a proof with using (5-3). Put $f(x) = C\log\log x$. Take any integer $N > 0$ satisfying the following: for all $x > N$,

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

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

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

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

by (5-3). Also, $nf(n)/(\log\log(nf(n)) + 1) \leq m/(\log\log m + 1)$ since the function $x/(\log\log x + 1)$ is strictly increasing for $x > e$ and $m \geq nf(n)\ (> e^{e^2}) > e$. Hence

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

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

[6] $\gamma = \int_1^{\infty}\big(\frac{1}{[x]} - \frac{1}{x}\big)\,dx = 0.57721\ldots$. Note also $e^{\gamma} = 1.78107\ldots$.

[7] More precisely, that theorem states $\varphi(m) > m/(e^{\gamma}\log\log m + 5/(2\log\log m))$ for $m \geq 3$ except when m is the product of the first nine primes, $m = 223092870 = 2\cdot 3\cdot 5\cdot\cdot 7\cdot 11\cdot 13\cdot 17\cdot 19\cdot 23$.

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 2. $H(n)$.

Remark 5.4. For a given C, we can modify the phrase "for any n large enough" in the statement of Proposition 5.3. For example, let us consider the case $C = 4$. By studying (i) and (ii) in the above proof more carefully, we can show

$$\Psi(n) < 4n \log\log n \quad \text{for any } n > e^{(1.001e)^9}.$$

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	$2^{32} \cdot 3^{91} \cdot 5^3 \cdot 7^2 \cdot 11^4 \cdot 13^4 \cdot 23^1 \cdot 41^1 \cdot 61^1 \cdot 73^1 \cdot 547^1 \cdot 757^1 \cdot 1093^2 \cdot 3851^1 \cdot 797161^1$

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

Here we check the above inequality. Condition (ii) is equivalent to

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

We assume $x > e^{e^9}$. Since $C/(2e^\gamma) - 1 > \frac{4}{3.6} - 1 = \frac{1}{9}$ and $\log(C \log\log x)/\log x < 0.001$, 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.

Acknowledgements

The author would like to thank Yuichiro Taguchi for useful discussions about the proof of our main results and Manabu Yoshida for advice on an earlier draft. Thanks also are due to Takaichi Fujiwara for helpful advice on the functions discussed in Section 5. This work is supported by JSPS KAKENHI grant number JP19K03433.

References

[Chou 2019] M. Chou, "Torsion of rational elliptic curves over the maximal abelian extension of $\mathbb{Q}$", *Pacific J. Math.* **302**:2 (2019), 481–509. MR Zbl

[Chou et al. 2021] M. Chou, P. L. Clark, and M. Milosevic, "Acyclotomy of torsion in the CM case", *Ramanujan J.* **55**:3 (2021), 1015–1037. MR Zbl

[Clark and Xarles 2008] P. L. Clark and X. Xarles, "Local bounds for torsion points on abelian varieties", *Canad. J. Math.* **60**:3 (2008), 532–555. MR Zbl

[Coleman and Iovita 1999] R. Coleman and A. Iovita, "The Frobenius and monodromy operators for curves and abelian varieties", *Duke Math. J.* **97**:1 (1999), 171–215. MR Zbl

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

[Fontaine 1982] J.-M. Fontaine, "Sur certains types de représentations p-adiques du groupe de Galois d'un corps local: construction d'un anneau de Barsotti–Tate", *Ann. of Math.* (2) **115**:3 (1982), 529–577. MR Zbl

[Fontaine 1994a] J.-M. Fontaine, "Le corps des périodes p-adiques", pp. 59–111 in *Périodes p-adiques* (Bures-sur-Yvette, France, 1988), edited by J.-M. Fontaine, Astérisque **223**, Soc. Math. France, Paris, 1994. MR Zbl

[Fontaine 1994b] J.-M. Fontaine, "Représentations p-adiques semi-stables", pp. 113–184 in *Périodes p-adiques* (Bures-sur-Yvette, France, 1988), edited by J.-M. Fontaine, Astérisque **223**, Soc. Math. France, Paris, 1994. MR Zbl

[Imai 1975] H. Imai, "A remark on the rational points of abelian varieties with values in cyclotomic Z_p-extensions", *Proc. Japan Acad.* **51** (1975), 12–16. MR Zbl

[Katz and Lang 1981] N. M. Katz and S. Lang, "Finiteness theorems in geometric classfield theory", *Enseign. Math.* (2) **27**:3-4 (1981), 285–319. MR Zbl

[Kubo and Taguchi 2013] Y. Kubo and Y. Taguchi, "A generalization of a theorem of Imai and its applications to Iwasawa theory", *Math. Z.* **275**:3-4 (2013), 1181–1195. MR Zbl

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

[Neukirch 1999] J. Neukirch, *Algebraic number theory*, Grundl. Math. Wissen. **322**, Springer, 1999. MR Zbl

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

[Ozeki 2024] Y. Ozeki, "Bounds on torsion of CM abelian varieties over a p-adic field with values in a field of p-power roots", *New York J. Math.* **30** (2024), 422–435. MR Zbl

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

[Serre 1979] J.-P. Serre, *Local fields*, Grad. Texts in Math. **67**, Springer, 1979. MR Zbl

[Serre 1989] J.-P. Serre, *Abelian l-adic representations and elliptic curves*, 2nd ed., Addison-Wesley, Redwood City, CA, 1989. MR Zbl

[Serre and Tate 1968] J.-P. Serre and J. Tate, "Good reduction of abelian varieties", *Ann. of Math.* (2) **88** (1968), 492–517. MR Zbl

[SGA 7_{I} 1972] A. Grothendieck, "Modèles de Néron et monodromie", pp. 313–523 in *Groupes de monodromie en géométrie algébrique*, *I* (Séminaire de Géométrie Algébrique du Bois Marie 1967–1969), edited by A. Grothendieck, Lecture Notes in Math. **288**, Springer, 1972. MR Zbl

[Silverberg 1992] A. Silverberg, "Fields of definition for homomorphisms of abelian varieties", *J. Pure Appl. Algebra* **77**:3 (1992), 253–262. MR Zbl

[Tate and Oort 1970] J. Tate and F. Oort, "Group schemes of prime order", *Ann. Sci. École Norm. Sup.* (4) **3** (1970), 1–21. MR Zbl

[Yoshida 2008] T. Yoshida, "Local class field theory via Lubin–Tate theory", *Ann. Fac. Sci. Toulouse Math.* (6) **17**:2 (2008), 411–438. MR Zbl

Received October 23, 2023. Revised May 16, 2024.

YOSHIYASU OZEKI
FACULTY OF SCIENCE
KANAGAWA UNIVERSITY
KANAGAWA-KU, YOKOHAMA
JAPAN
ozeki@kanagawa-u.ac.jp

PACIFIC JOURNAL OF MATHEMATICS

Founded in 1951 by E. F. Beckenbach (1906–1982) and F. Wolf (1904–1989)

msp.org/pjm

See inside back cover or msp.org/pjm for submission instructions.

The subscription price for 2024 is US $645/year for the electronic version, and $875/year for print and electronic.
Subscriptions, requests for back issues and changes of subscriber address should be sent to Pacific Journal of Mathematics, P.O. Box 4163, Berkeley, CA 94704-0163, U.S.A. The Pacific Journal of Mathematics is indexed by Mathematical Reviews, Zentralblatt MATH, PASCAL CNRS Index, Referativnyi Zhurnal, Current Mathematical Publications and Web of Knowledge (Science Citation Index).

The Pacific Journal of Mathematics (ISSN 1945-5844 electronic, 0030-8730 printed) at the University of California, c/o Department of Mathematics, 798 Evans Hall #3840, Berkeley, CA 94720-3840, is published twelve times a year. Periodical rate postage paid at Berkeley, CA 94704, and additional mailing offices. POSTMASTER: send address changes to Pacific Journal of Mathematics, P.O. Box 4163, Berkeley, CA 94704-0163.

PJM peer review and production are managed by EditFlow® from Mathematical Sciences Publishers.

PUBLISHED BY

mathematical sciences publishers

nonprofit scientific publishing

http://msp.org/

PACIFIC JOURNAL OF MATHEMATICS

Volume 330 No. 1 May 2024