

* Up to twist, there are only finitely many potentially p -ordinary abelian varieties over \mathbb{Q} of $GL(2)$ -type with fixed prime-to- p conductor

Haruzo Hida
Department of Mathematics, UCLA,
Los Angeles, CA 90095-1555, U.S.A.

October 15 2011

*A one hour lecture at Iwasawa workshop at University of Arizona.
The author is partially supported by the NSF grant: DMS 0753991 and DMS 0854949 and by Clay Mathematics institute as a senior scholar.

Pick a strictly compatible system $\{\rho_\lambda \circ V(\rho_\lambda) \cong F_\lambda^2\}_\lambda$ of λ -adic odd Galois representations with

$$\det(\rho_\lambda) = \psi \mathcal{N}^{k-1}$$

Here \mathcal{N} : the λ -adic cyclotomic character,
 ρ_λ has Hodge-Tate weight $(k-1, 0)$,
 λ runs over places of a number field F .

Then

$$\prod_p \det(1 - \rho_\lambda(\text{Frob}_p)|_{V(\rho_\lambda)^{I_p}} p^{-s})^{-1} = \sum_{n=1}^{\infty} a_n(\rho) n^{-s}$$

gives rise to a modular form of weight k and of Neben type ψ :

$$f_\rho = \sum_{n=1}^{\infty} a_n(\rho) \exp(2\pi i n z)$$

by the solution of Serre's mod p modularity conjecture by Khare–Wintenberger.

For a number field $K \subset \overline{\mathbb{Q}}$, the field

$$K(a_\rho(n) | n = 1, 2, \dots)$$

is called the Hecke field, which is one of the most **mysterious** series of number fields. Fixing one prime p , and consider a simple extension $K(a_\rho(p))$ or for a family of systems of λ -adic Galois representations $\mathcal{F} = \{\rho\}$, we could think of $K(a_\rho(p))_{\rho \in \mathcal{F}}$, and ask

how big this Hecke field is?

After answering this question to certain extent, as an application, we study rational abelian varieties and its twist classes in the title.

§1. Notation

We study families of modular forms and Hecke fields. To define the family \mathcal{F} , we introduce some notation. Fix

- An odd prime $p > 2$;
- a positive integer N ($p \nmid N$);
- two field embeddings $\mathbb{C} \leftarrow \overline{\mathbb{Q}} \hookrightarrow \overline{\mathbb{Q}}_p$.

Consider the space $S_{k+1,\psi} = S_{k+1}(\Gamma_0(Np^{r+1}), \psi)$ ($r \geq 0$) of cusp forms of weight “ $k+1$ ” with Nebentypus ψ .

Let the rings $\mathbb{Z}[\psi] \subset \mathbb{C}$ and $\mathbb{Z}_p[\psi] \subset \overline{\mathbb{Q}}_p$ be generated by $\psi(n)$ ($n = 1, 2, \dots$) over \mathbb{Z} and \mathbb{Z}_p .

The Hecke algebra over \mathbb{Z} is $h = \mathbb{Z}[\psi][T(n) | n = 1, 2, \dots] \subset \text{End}(S_{k+1,\psi})$. Put $h_{k+1,\psi} = h \otimes_{\mathbb{Z}[\psi]} \mathbb{Z}_p[\psi]$.

Sometimes our $T(p)$ is written as $U(p)$ as the level is divisible by p .

§2. Big Hecke algebra

The ordinary part $h_{k+1,\psi}^{ord} \subset h_{k+1,\psi}$ is the **maximal ring direct summand** on which $U(p)$ is invertible. Let

$$\psi_1 = \psi_N \times \text{the tame } p\text{-part of } \psi.$$

We have a unique ‘big’ Hecke algebra $\mathfrak{h} = \mathfrak{h}_{\psi_1}$ such that

- \mathfrak{h} is free of finite rank over $\mathbb{Z}_p[[T]]$ with $T(n) \in \mathfrak{h}$ ($n = 1, 2, \dots$)
- Let $\gamma = 1 + p$. If $k \geq 1$ and $\varepsilon : \mathbb{Z}_p^\times \rightarrow \mu_{p^\infty}$ is a character,

$$\mathfrak{h}/(1 + T - \psi(\gamma)\varepsilon(\gamma)\gamma^k)\mathfrak{h} \cong h_{k+1,\varepsilon\psi_k}^{ord}$$

for $\psi_k := \psi_1\omega^{1-k}$, sending $T(n)$ to $T(n)$, where ω is the Teichmüller character. Thus

the number of ordinary Hecke eigenforms for any k and ε is bounded by $B = \text{rank}_\wedge \mathfrak{h}$.

§3. Galois representation

Each **irreducible component**

$$\mathrm{Spec}(\mathbb{I}) \subset \mathrm{Spec}(\mathfrak{h})$$

has a **Galois representation**

$$\rho_{\mathbb{I}} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \rightarrow \mathrm{GL}(2)$$

with **coefficients** in \mathbb{I} (or its quotient field) such that

$$\mathrm{Tr}(\rho_{\mathbb{I}}(\mathrm{Frob}_l)) = a(l)$$

(for the image $a(l)$ in \mathbb{I} of $T(l)$) for almost all primes l . Usually $\rho_{\mathbb{I}}$ has values in $\mathrm{GL}_2(\mathbb{I})$, and we suppose this for simplicity.

We regard $P \in \mathrm{Spec}(\mathbb{I})(\overline{\mathbb{Q}}_p)$ as an algebra homomorphism $P : \mathbb{I} \rightarrow \overline{\mathbb{Q}}_p$, and we put $\rho_P = P \circ \rho_{\mathbb{I}} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \rightarrow \mathrm{GL}_2(\overline{\mathbb{Q}}_p)$.

§4. Analytic family

A point P of $\text{Spec}(\mathbb{I})(\overline{\mathbb{Q}}_p)$ is called **arithmetic** if $P(1 + T - \varepsilon\psi_k(\gamma)\gamma^k) = 0$ for $k \geq 1$ and $\varepsilon : \mathbb{Z}_p^\times \rightarrow \mu_{p^\infty}$.

If P is arithmetic, we have a Hecke eigenform $f_P \in S_{k+1}(\Gamma_0(Np^{r(P)}), \varepsilon\psi_k)$ such that

$$f_P|T(n) = a_P(n)f_P \quad (n = 1, 2, \dots)$$

for $a_P(n) := P(a(n)) = (a(n) \bmod P) \in \overline{\mathbb{Q}}_p$.

We write $\varepsilon_P = \varepsilon$ and $k(P) = k$ for such a P .

Thus \mathbb{I} gives rise to an **analytic family**

$$\mathcal{F}_{\mathbb{I}} = \{f_P | \text{arithmetic } P \in \text{Spec}(\mathbb{I})\}.$$

§5. CM component and CM family

We call a Galois representation ρ **CM** if there exists an open subgroup $G \subset \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ such that the semi-simplification $(\rho|_G)^{ss}$ has abelian image over G .

We call \mathbb{I} a *CM component* if $\rho_{\mathbb{I}}$ is CM.

If \mathbb{I} is a CM component, it is known that for an imaginary quadratic field M in which p splits, there exists a Galois character $\varphi : \text{Gal}(\overline{\mathbb{Q}}/M) \rightarrow \mathbb{I}^\times$ such that $\rho_{\mathbb{I}} \cong \text{Ind}_M^{\mathbb{Q}} \varphi$.

If $\rho_P \cong \text{Ind}_M^{\mathbb{Q}} \varphi_P$ for some arithmetic point P , \mathbb{I} is a CM component.

§6. A theorem on Hecke fields

Pick an infinite set \mathcal{A} of arithmetic points P with fixed weight $k(P) = k \geq 1$. Write $H_{\mathcal{A}}(\mathbb{I}) \subset \overline{\mathbb{Q}}$ for the field generated over $\mathbb{Q}(\mu_{p^\infty})$ by $\{a_P(p)\}_{P \in \mathcal{A}}$. Here is what we can prove:

Theorem 1 (H-theorem). *The field $H_{\mathcal{A}}(\mathbb{I})$ is a finite extension of $\mathbb{Q}(\mu_{p^\infty})$ if and only if \mathbb{I} is CM. Moreover if \mathbb{I} is **non CM**,*

$$\limsup_{P \in \mathcal{A}} [\mathbb{Q}(\mu_{p^\infty})(a_P(p)) : \mathbb{Q}(\mu_{p^\infty})] = \infty.$$

Assume that $[H_{\mathcal{A}}(\mathbb{I}) : \mathbb{Q}(\mu_{p^\infty})] < \infty$. We try to prove that \mathbb{I} has CM. The converse is an application of **Galois deformation theory**.

§7. Number of eigenforms bounded

We start preparing to give a proof of the theorem. Put $K(f_P) = K[a_P(n); n = 1, 2, \dots]$ inside $\overline{\mathbb{Q}}$.

Lemma 1 (Bounded degree). *The degree*

$$[\mathbb{Q}(\mu_{p^\infty})(f_P) : \mathbb{Q}(\mu_{p^\infty})(a_P(p))]$$

for arithmetic P with fixed $k(P) \geq 1$ is **bounded** (basically by $B = \text{rank}_{\mathbb{Z}_p[[T]]} \mathfrak{h}$) independently of P .

Let $A(l) =$ a root of $\det(X - \rho_{\mathbb{I}}(\text{Frob}_l)) = 0$ for $l \nmid Np$. Then $\alpha_{l,P} := P(A(l)) \in \overline{\mathbb{Q}}_p$ is a **root** of

$$X^2 - a_P(l)X + \psi_k(l)l^{k(P)} = 0.$$

If $l = p$, we put $A(l) = a(l)$. Fix l . Extending \mathbb{I} , we assume that $A(l) \in \mathbb{I}$. By the lemma, if $[\mathbb{Q}(\mu_{p^\infty})(a_P(p)) : \mathbb{Q}(\mu_{p^\infty})] < B$ for B independent of $P \in \mathcal{A}$, $\mathcal{L}_P = \mathbb{Q}(\mu_{p^\infty})(\alpha_{l,P})$ has **bounded degree** over $\mathbb{Q}(\mu_{p^\infty})$ independent of l and P for all $P \in \mathcal{A}$.

§8. Weil numbers

For a prime l , a Weil l -number $\alpha \in \mathbb{C}$ of integer weight $k \geq 0$ satisfies for all $\sigma \in \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$,

$$(1) |\alpha^\sigma| = l^{k/2}, \quad (2) \alpha \text{ is an algebraic integer.}$$

Two nonzero numbers a and b **equivalent** if a/b is a root of unity. Let \mathcal{K}_d be the set of all extensions of $\mathbb{Q}[\mu_{p^\infty}]$ of **degree** $d < \infty$ inside $\overline{\mathbb{Q}}$ whose ramification at l is **tame**. Here is an elementary fact:

Proposition 1 (Finiteness Proposition). *We have only **finitely many** Weil l -numbers of a given weight in the set-theoretic union $\bigcup_{K \in \mathcal{K}_d} K$ up to equivalence.*

By tameness, there are only **finitely many** isomorphism classes of $K \otimes_{\mathbb{Q}} \mathbb{Q}_l$ for $K \in \mathcal{K}_d$, and one can consider the prime factorization in a fixed algebra $K \otimes_{\mathbb{Q}} \mathbb{Q}_l$.

§9. A rigidity lemma

Let W be a p -adic valuation ring finite flat over \mathbb{Z}_p and $\Phi(T) \in W[[T]]$. Regard Φ as a function of $t = 1 + T$; so, $\Phi(1) = \Phi|_{T=0}$. We start with a lemma whose characteristic p version was studied by Chai:

Lemma 2 (Rigidity). *Suppose that there is an infinite subset $\Omega \subset \mu_{p^\infty}(\overline{K})$ such that $\Phi(\Omega) \subset \mu_{p^\infty}$. Then there exist $\zeta_0 \in \mu_{p^\infty}$ and $s \in \mathbb{Z}_p$ such that $\zeta_0^{-1}\Phi(t) = t^s = \sum_{n=0}^{\infty} \binom{s}{n} T^n$.*

One day at Tata institute, I asked Kiran Kedlaya if this is true. He came up with a proof next day. I also invented a proof before his showing up to my office, though his proof is more elementary. I leave this to you as an exercise.

§10. Frobenius eigenvalue formula

Suppose $[H_{\mathcal{A}}(\mathbb{I}) : \mathbb{Q}(\mu_{p^\infty})] < \infty$. This implies $\mathcal{L}_P = \mathbb{Q}(\mu_{p^\infty})(\alpha_{l,P})$ has bounded degree over $\mathbb{Q}(\mu_{p^\infty})$; so, for primes $l \gg 0$, l is **tamely** ramified in \mathcal{L}_P (the tameness assumption in Finiteness Proposition).

Proposition 2 (Eigenvalue formula). *For sufficiently large prime l , there exists a Weil l -number α_1 of weight 1 and a root of unity ζ_0 such that*

$$A(P) = \alpha_{l,P} = \zeta_0 \langle \alpha_1 \rangle^{k(P)-1}$$

for all arithmetic P ; in other words, for $s = \frac{\log_p(\alpha_1)}{\log_p(\gamma)}$

$$A(T) = \zeta_0 (1 + T)^s.$$

§11. Proof of eigenvalue formula

We give a proof assuming $\mathbb{I} = W[[T]]$. By Finiteness proposition, we have only a **finite** number of Weil l -numbers of weight k in $\cup_{P \in \mathcal{A}} \mathcal{L}_P$ up to multiplication by roots of unity, and hence

$A(P)$ for $P \in \mathcal{A}$ hits one of such Weil l -number α of weight k infinitely many times, up to roots of unity.

After a suitable variable change $T \mapsto Y = \gamma^{-k}(1 + T) - 1$ and division by a Weil number, $A(Y)$ satisfies the assumption of the **rigidity lemma**. We have for $s_1 \in \mathbb{Z}_p$

$$A(Y) = \zeta_\alpha (1 + Y)^{s_1},$$

and $A(T) = \zeta_0 (1 + T)^s$. From this, it is not difficult to determine s as stated in the proposition. \square

§12. Abelian image lemma

Consider the endomorphism $\sigma_s : (1+T) \mapsto (1+T)^s = \sum_{n=0}^{\infty} \binom{s}{n} T^n$ of a power series ring $W[[T]]$ for $s \in \mathbb{Z}_p$. Let A be an integral domain over $W[[T]]$ of characteristic different from 2. Assume that the endomorphism σ_2 on $W[[T]]$ extends to an endomorphism σ of A .

Lemma 3 (Abelian image). *Take a continuous representation $\rho : \text{Gal}(\overline{\mathbb{Q}}/F) \rightarrow GL_2(A)$ for a field $F \subset \overline{\mathbb{Q}}$, and put $\rho^\sigma := \sigma \circ \rho$. If $\text{Tr}(\rho^\sigma) = \text{Tr}(\rho^2)$. Then ρ is absolutely reducible over the quotient field Q of A .*

Heuristically, the assumption implies that the **square map**: $\sigma \mapsto \rho^2(\sigma)$ is still a representation ρ^σ ; so, it has to have an abelian image. Since any automorphism of the quotient field Q of $\mathbb{Z}_p[[T]]$ extends to its algebraic closure $\overline{Q} \supset \mathbb{I}$, we can apply the above lemma to $\rho_{\mathbb{I}}$.

§13. **Proof of the theorem.** Suppose $[H_{\mathcal{A}}(\mathbb{I}) : \mathbb{Q}(\mu_{p^\infty})] < \infty$.

Step 1: We have $[\mathcal{L}_P : \mathbb{Q}(\mu_{p^\infty})]$ bounded independent of l ; so, if $l \gg 0$, \mathcal{L}_P is at most tamely ramified.

Step 2: By Eigenvalue formula, we have $\text{Tr}(\rho(\text{Frob}_l)) = \zeta(1 + T)^a + \zeta'(1 + T)^{a'}$ for two roots of unity ζ, ζ' and $a, a' \in \mathbb{Q}_p$.

Step 3: Not too difficult to show that the order of ζ, ζ' is bounded independent of l .

Step 4: Let $\mathfrak{m}_N = \mathfrak{m}_{\mathbb{I}}^N + (T)$ and $\bar{\rho} = \rho_{\mathbb{I}} \bmod \mathfrak{m}_N$ for $N \gg 0$ and F be the splitting field of $\bar{\rho}$; so, taking $N \gg 0$, we may assume

$$\text{Tr}(\rho(\text{Frob}_l^f)) = (1 + T)^{fa} + (1 + T)^{fa'}$$

for all $l \gg 0$ as long as $\text{Frob}_l^f \in \text{Gal}(\overline{\mathbb{Q}}/F)$.

Step 5: This shows $\text{Tr}(\sigma_s \circ \rho) = \text{Tr}(\rho^s)$ over $G = \text{Gal}(\overline{\mathbb{Q}}/F)$. Then by the above lemma, $\rho^{ss}|_G$ is abelian, and hence \mathbb{I} is CM. □

§14. The number of twist classes of abelian variety of $GL(2)$ -type.

An abelian variety A over \mathbb{Q} is of $GL(2)$ -**type** if $\text{End}^0(A/\mathbb{Q}) := \text{End}(A/\mathbb{Q}) \otimes_{\mathbb{Z}} \mathbb{Q}$ contains a totally real or a CM number field F of degree equal to $\dim A$. Such an abelian variety is **CM** if $\text{End}^0(A/\overline{\mathbb{Q}})$ contains a semi-simple quadratic extension of F .

The Galois representation on λ -adic Tate module $T_{\lambda}A = \varprojlim_n A[\lambda^n]$ for a prime λ of F produces a compatible system of λ -adic representations $\rho_A = \{\rho_{\lambda} \circ T_{\lambda}A\}$. Thus we have its L -function $L(s, A) = L(s, \rho_A)$.

We call two \mathbb{Q} -simple abelian varieties A and B are **twist** equivalent if $L(s, \rho_A) = L(s, \rho_B \otimes \chi)$ for a finite order Galois character χ .

§15. Finiteness of twist classes.

Our next goal is:

Theorem 2. *There are only finitely many twist classes of \mathbb{Q} -simple **non-CM** abelian varieties of potentially good ordinary reduction at p and good reduction everywhere else.*

Our strategy of the proof is as follows:

- By a theorem of Khare–Wintenberger, a \mathbb{Q} -simple abelian variety A of $GL(2)$ -type is associated to an elliptic cusp form f_A such that $L(s, A) = L(s, f_A)$ (f_A up to Galois conjugation).
- Since A has potentially **ordinary good reduction** at p , either f_A generates an automorphic representation super-cuspidal at p or we may assume that $|a(p, f_A)|_p = 1$ after twisting by a character.
- Show the super-cuspidal case never occur.
- Count ordinary f_A of p -power level to show the number of such f_A is finite.

§16. Non super-cuspidality

Let A be as in the theorem and the mod p abelian variety \tilde{A} be the reduction modulo p of A over some extension of \mathbb{Z}_p . Suppose that f_A is super-cuspidal at p .

As is well known, for $\lambda \nmid p$, there exists a quadratic extension M/\mathbb{Q}_p such that $\rho_\lambda|_{\text{Gal}(\overline{\mathbb{Q}_p}/\mathbb{Q}_p)} \cong \text{Ind}_M^{\mathbb{Q}_p} \varphi$ for a character $\varphi : \text{Gal}(\overline{\mathbb{Q}_p}/M) \rightarrow F_\lambda^\times$.

By super-cuspidality, $\rho_\lambda|_{\text{Gal}(\overline{\mathbb{Q}_p}/\mathbb{Q}_p)}$ is irreducible, and $\rho_\lambda|_{\text{Gal}(\overline{\mathbb{Q}_p}/M)} = \varphi \oplus \varphi_\sigma$, where $\varphi_\sigma(g) = \varphi(\sigma g \sigma^{-1})$ for $\sigma \in \text{Gal}(\overline{\mathbb{Q}_p}/\mathbb{Q}_p)$ inducing non-trivial automorphism on M .

A power $\varphi([p, M])^m$ is the Frobenius eigenvalue of \tilde{A} . Since $\varphi^2([p, M]) = \varphi\varphi_\sigma([p, M]) = p^e$ with $e > 0$, \tilde{A} cannot be ordinary. This fact was pointed out by A. Yamagami sometimes ago.

§17. Ordinary good reduction

Let V be a valuation ring finite flat over \mathbb{Z}_p over which $\tilde{A} = A \otimes_V \kappa$ for $\kappa := V/\mathfrak{m}_V$ is an ordinary abelian variety:

$$\tilde{A}[p](\overline{\mathbb{F}}_p) \cong (\mathbb{Z}/p\mathbb{Z})^{\dim A}.$$

We regard $\mathbb{Z}[f_A] = \mathbb{Z}[a(n, f_A)]_n \subset \text{End}(A/\mathbb{Q}) \subset \text{End}(\tilde{A}/\mathbb{F})$.

Again some power α^m for $\alpha = a(p, f_A)$ is the Frobenius eigenvalue of \tilde{A} . The action of α on $\tilde{A}[p](\overline{\mathbb{F}}_p) \cong (\mathbb{Z}/p\mathbb{Z})^{\dim A}$ is invertible.

$$\Sigma_A = \left\{ \sigma : \mathbb{Q}[\alpha] \hookrightarrow \overline{\mathbb{Q}} \mid |\alpha^\sigma|_p = 1 \right\}$$

is a **CM-type** of $\mathbb{Q}[\alpha]$. Thus we need to show:

Theorem 3. *In a non-CM family of prime-to- p level 1, there are only finitely many arithmetic P such that*

$$\Sigma_P = \left\{ \sigma : \mathbb{Q}[a_P(p)] \hookrightarrow \overline{\mathbb{Q}} \mid |a_P(p)^\sigma|_p = 1 \right\}$$

is a CM type of $\mathbb{Q}[a_P(p)]$.

§18. **Proof of Theorem 4, Step. 1.** Supposing to have an infinite set \mathcal{A} of arithmetic points such that Σ_P is a CM type of $\mathbb{Q}[a_P(p)]$ for all $P \in \mathcal{A}$, we bound $[\mathbb{Q}(\mu_{p^\infty})[a_P(p)] : \mathbb{Q}(\mu_{p^\infty})]$. So, \mathbb{I} is a CM component by H-theorem.

Let $F_P = \mathbb{Q}(a(p, f_P))$, $K_P = \mathbb{Q}(\varepsilon_P)$ and $L_P = F_P(\varepsilon_P)$. Then

$$\text{Inf}_{L_P} \Sigma_P = \left\{ \sigma : L_P \hookrightarrow \overline{\mathbb{Q}} \mid \sigma|_{F_P} \in \Sigma_P \right\}$$

is a CM type of L_P . Thus

$$2|\text{Inf}_{L_P} \Sigma_P| = [L_P : \mathbb{Q}].$$

Since $\mathbb{Q}(\mu_{p^\infty})$ has only one p -adic place and $[K_P : \mathbb{Q}] = p^{r(P)-1}(p-1)$, for a fixed embedding $\sigma_0 : \mathbb{Q}(\mu_{p^\infty}) \hookrightarrow \overline{\mathbb{Q}}$, we have

$$\begin{aligned} (*) \quad & \left| \text{Inf}_{L_P} \Sigma_P \right| \\ & = \left| \left\{ \sigma \in \text{Inf}_{L_P} \Sigma_P \mid \sigma|_{K_P} = \sigma_0|_{K_P} \right\} \right| \cdot [K_P : \mathbb{Q}] = Cp^{r(P)} [L_P : K_P] \end{aligned}$$

for the constant C independent of P .

§19. **Proof of Theorem 4, Step. 2.** Write $H = \bigoplus_{j=0}^{p-2} \mathfrak{h}_{\omega^j}$. Since $|\text{Inf}_{L_P} \Sigma_P|$ is the number of conjugate slope 0 forms f_P^σ which is **bounded** by the rank of the Hecke algebra $H/(1+T)^{p^r} - \gamma)H$ acting on them, we have, for $r = r(P)$,

$$|\text{Inf}_{L_P} \Sigma_P| \leq \text{rank}_W \frac{H}{((1+T)^{p^r} - \gamma)H} = p^{r(P)} \text{rank}_{W[[x]]} H. \quad (**)$$

Since

$$\begin{aligned} [\mathbb{Q}(\mu_{p^\infty})(a_P(p)) : \mathbb{Q}(\mu_{p^\infty})] \\ = [L_P : L_P \cap \mathbb{Q}(\mu_{p^\infty})] \leq [L_P : K_P] \end{aligned}$$

as $L_P \cap \mathbb{Q}(\mu_{p^\infty}) \supset K_P$, (*) and (**) combined tells us

$$[\mathbb{Q}(\mu_{p^\infty})(a_P(p)) : \mathbb{Q}(\mu_{p^\infty})] \leq C^{-1} \text{rank}_{W[[x]]} H.$$

This is impossible if \mathbb{I} does not have CM, since $\sup_{P \in \mathcal{A}} [K(a(p, f_P)) : K] = \infty$ by the H-theorem.