Complex multiplication : the Shimura - Taniyama formula.

SV defined over number field E $\leftrightsquigarrow$ action of $\mathrm{Aut}(\mathbb{C}/E)$ on $SV(\mathbb{C})$

Hodge type : $\sigma \in \mathrm{Aut}(\mathbb{C}/E)$, $\sigma[A, \cdots] = [\sigma A, \cdots]$

Goal : $\exists$ action of $\mathrm{Aut}(\mathbb{C}/E)$ and it arises from models over E.

Ex. $\{$elliptic curves $/\mathbb{C}\} \twoheadrightarrow \Gamma(1)\backslash\mathcal{H}$

$\sigma \in \mathrm{Aut}(\mathbb{C}/\mathbb{Q})$, $[A] = p \in \Gamma(1)\backslash\mathcal{H}$, $\sigma \cdot p = [\sigma A]$ and $j(\sigma \cdot p) = \sigma j(p)$.

$\sigma \in \mathrm{Aut}(\mathbb{C}/E)$ preserves $\bar{E}$ in $\mathbb{C}$ $\Rightarrow$ $\sigma|_{\bar{E}} \in \mathrm{Gal}(\bar{E}/E)$ $x \in E^{ab}$, $\sigma|_{\bar{E}} \cdot x = \sigma|_{\bar{E}}^{ab} \cdot x$.

Although the action of $\mathrm{Aut}(\mathbb{C}/E)$ is not explicit, for special points whose coordinates are in E^{ab}, the action factors through $\mathrm{Gal}(E^{ab}/E)$ and could be described using class field theory.

Goal : the explicit action on special points determines the "canonical" model.

Review of AV.

A/k AV, a endomorphism of A, $\exists!$ monic polynomial $P_a(T)$ with integer coefficients s.t. $|P_a(n)| = \deg(n-a)$, $n \in \mathbb{Z}$.

P_a is the char. poly. of a acting on $V_\ell A$, $\ell \neq \mathrm{char}\, k$.

A, B AV/K, $\mathrm{Hom}_{AV}(A, B)$ is torsion free $\mathbb{Z}$-mod of finite rank.

$AV^\circ(K)$ the category of AV/K, $\mathrm{Hom}_{AV^\circ}(A, B) = \mathrm{Hom}_{AV}(A, B) \otimes_{\mathbb{Z}} \mathbb{Q}$

Isogenies become Isom. in $AV^\circ(K)$.

A/K simple AV if A nonzero and contains no nonzero proper abelian subvariety. Every AV is isogenous to a product of simple AV.

A, B simple AV, $\forall$ $f: A \to B$ nonzero homomorphism is an isogeny.

$\mathrm{End}^\circ(A)$ division algebra if A simple AV

semisimple algebra if A AV.

CM fields.

E number field is called CM if it is a quadratic totally imaginary extension of a totally real field F. $a \mapsto a^*$ the nontrivial involution of E fixing F, $\rho(a^*) = \overline{\rho(a)}$ for any $\rho: E \hookrightarrow \mathbb{C}$.

noncanonical

$$\begin{array}{ccc} E \otimes_{\mathbb{Q}} \mathbb{R} & \xrightarrow{\sim} & \prod_{\sigma: F \hookrightarrow \mathbb{R}} \mathbb{C}_\sigma \\ \uparrow & & \uparrow \\ F \otimes_{\mathbb{Q}} \mathbb{R} & \xrightarrow{\sim} & \prod_{\sigma: F \hookrightarrow \mathbb{R}} \mathbb{R}_\sigma \end{array}, \quad \mathbb{C}_\sigma = E \otimes_{F, \sigma} \mathbb{R} \simeq \mathbb{C}$$

$$(a \otimes r) \longmapsto (\sigma a \cdot r)_\sigma$$

The involution $*$ is positive as $tr_{E\otimes_{\mathbb{Q}}\mathbb{R}/F\otimes_{\mathbb{Q}}\mathbb{R}}(b^* b) = tr_{\mathbb{C}/\mathbb{R}}(\bar{z} z) > 0$

$\sigma : F \hookrightarrow \mathbb{R}$ extends to two conjugate embeddings of E into $\mathbb{C}$

A CM type Φ for E is $\Phi \subset Hom(E, \mathbb{C})$ s.t. $Hom(E, \mathbb{C}) = \Phi \amalg \bar{\Phi}$.

We can find $\alpha \in E$, $E = F[\alpha]$, $\alpha^2 \in F^\times$, $\alpha^* = -\alpha$.

AV of CM type.

Let E be a CM field, $[E : \mathbb{Q}] = 2g$.

$A/\mathbb{C}$ AV of dim g, $i : E \to End^\circ A$.

We say (A, i) is of CM type (E, Φ) if Φ is a CM type for E s.t. $T_0 A \simeq \mathbb{C}^\Phi$ as $E \otimes_{\mathbb{Q}} \mathbb{C}$ - mods.

RMK. (A, i) is always of CM type for some Φ.

$A(\mathbb{C}) \simeq T_0 A / \Lambda$, $\Lambda = H_1(A, \mathbb{Z})$

$\Lambda \otimes \mathbb{R} \simeq T_0 A$, $\Lambda \otimes \mathbb{Q} \simeq H_1(A, \mathbb{Q})$

$\Lambda \otimes \mathbb{C} \simeq H_1(A, \mathbb{C}) \simeq H^{-1,0} \oplus H^{0,-1} \simeq T_0 A \oplus \overline{T_0 A}$

$\dim_E H_1(A, \mathbb{Q}) = 1 \Rightarrow H_1(A, \mathbb{C}) \simeq \bigoplus_{\varphi : E \hookrightarrow \mathbb{C}} \mathbb{C}_\varphi$

φ occurs in $T_0 A \Leftrightarrow \bar{\varphi}$ occurs in $\overline{T_0 A}$

$T_0 A \simeq \bigoplus_{\varphi \in \Phi} \mathbb{C}_\varphi$ for some CM type Φ.

In particular, (A, i) is of CM type (E, Φ) $\Leftrightarrow$ $tr(i(a) | T_0 A) = \sum_{\varphi \in \Phi} \varphi(a)$.

Let Φ be a CM type for E, Φ gives a map

$$O_E \longrightarrow \mathbb{C}^{\Phi}, \quad \Phi(a) = (\varphi(a)).$$

Prop. $\Phi(O_E)$ is a lattice in $\mathbb{C}^{\Phi}$ and $A_{\Phi} = \mathbb{C}^{\Phi}/\Phi(O_E)$ is AV of CM type (E, Φ) for the natural map $i_{\Phi}: E \longrightarrow \mathrm{End}^{\circ}(A_{\Phi})$. Moreover any other (A, i) of CM type (E, Φ) is E-isogenous to (A_{Φ}, i_{Φ}).

Pf.

$$O_E \otimes_{\mathbb{Z}} \mathbb{R} \simeq E \otimes_{\mathbb{Q}} \mathbb{R} \xrightarrow[\sim]{\Phi} \mathbb{C}^{\Phi} \quad \Rightarrow \quad \Phi(O_E) \subset \mathbb{C}^{\Phi} \text{ is a lattice.}$$

Let $E = F[\alpha]$, $\alpha^2 \in F$. By weak approximation, we may find $f \in F$ s.t. $\alpha' = f\alpha$, $E = F[\alpha']$, $(\alpha')^2 \in F$, $\forall \varphi \in \Phi$, $\mathrm{Im}\, \varphi(\alpha') > 0$. Moreover we can assume α' is an algebraic integer.

Define $\psi(u, v) = \mathrm{tr}_{E/\mathbb{Q}}(\alpha' u v^*)$, $u, v \in O_E$.

Then $\psi(u, v) \in \mathbb{Z}$.

$\psi_{\mathbb{R}} = \sum_{\varphi \in \Phi} \psi_{\varphi}$ where $\psi_{\varphi}(u, v) = \mathrm{tr}_{\mathbb{C}/\mathbb{R}}(\alpha'_{\varphi} \cdot u \cdot \bar{v})$, $\alpha'_{\varphi} = \varphi(\alpha')$, $u, v \in \mathbb{C}$.

$$= \alpha'_{\varphi} u \bar{v} + \overline{\alpha'_{\varphi} u \bar{v}}$$

$$= \alpha'_{\varphi}(u\bar{v} - \bar{u} v) \in \mathbb{R}$$

and $\psi_{\varphi}(u, u) = 0$, $\psi_{\varphi}(iu, iv) = \psi_{\varphi}(u, v)$, $\psi_{\varphi}(u, iu) > 0$ if $u \neq 0$.

Hence ψ is a Riemann form and A_{Φ} is AV.

$\alpha \in O_E$ acts on $\mathbb{C}^\Phi$ by multiplying $\Phi(\alpha)$, this preserves $\Phi(O_E)$ and induce $i_\Phi : E \simeq O_E \otimes_{\mathbb{Z}} \mathbb{Q} \longrightarrow \mathrm{End}^\circ A_\Phi$.

Clearly $\mathbb{C}^\Phi \simeq T_0 A_\Phi$ compatible with the action of E. Hence (A_Φ, i_Φ) is of CM type (E, Φ).

Let (A, i) be of CM type (E, Φ). Then $\exists$ $\mathbb{C}^\Phi \xrightarrow{\sim} T_0 A$ as $E \otimes_{\mathbb{Q}} \mathbb{C}$ modules $\Rightarrow$ $A(\mathbb{C}) \simeq \mathbb{C}^\Phi / \Lambda$, $\mathbb{Q}\Lambda$ stable under the action of E via Φ

$\Rightarrow$ $\mathbb{Q}\Lambda = \Phi(E) \cdot \lambda$, $\lambda \in (E \otimes_{\mathbb{Q}} \mathbb{R})^\times$

$\Rightarrow$ $\mathbb{C}^\Phi \xrightarrow{\lambda} \mathbb{C}^\Phi \xrightarrow{\sim} T_0 A$, $\mathbb{Q}\Lambda = \Phi(E)$, $\Lambda = \Phi(\Lambda')$ for some lattice $\Lambda' \subset E$.

$\Rightarrow$ $N\Lambda' \subset O_E$ for some N and

$\mathbb{C}^\Phi / \Lambda \xrightarrow{N} \mathbb{C}^\Phi / N\Lambda \leftarrow \mathbb{C}^\Phi / \Phi(O_E)$ are all O_E-isogenies. ///

$k \subset \mathbb{C}$ subfield, A/k AV of dim g, $i : E \longrightarrow \mathrm{End}^\circ A$, E CM of deg $2g / \mathbb{Q}$. $T_0 A$ is g-dim k-v.s. on which E acts k-linearly. If k contains all conjugates of E, $\mathrm{Hom}(E, k) \simeq \mathrm{Hom}(E, \mathbb{C})$ and $T_0 A$ will again decompose into 1-dim k-v.s. indexed by $\Phi \subset \mathrm{Hom}(E, k)$, Φ is CM type for E and (A, i) is also called of CM type (E, Φ).

Prop. (A, i) AV/$\mathbb{C}$ of CM type (E, Φ), then (A, i) has a model over $\overline{\mathbb{Q}}$ unique up to Isom.

Pf. Let $k \subset \Omega$ be alg. closed fields of char 0. For A AV/k, $A(k)_{tor}$ is Zariski dense in $A(k)$ and the map $A(k)_{tor} \to A(\Omega)_{tor}$ is bijective. Thus for AV $A, B/k$, any regular map $A_\Omega \to B_\Omega$, the action of $\mathrm{Aut}(\Omega/k)$ on $A(\Omega) \longrightarrow B(\Omega)$ is trivial, hence the map descends to a map over k. In particular $AV/k \to AV/\Omega$ is fully faithful. This proves the uniqueness.

$$A \longmapsto A_\Omega$$

The polynomials defining A and i have coefficients in some subring R of $\mathbb{C}$ finitely generated over $\overline{\mathbb{Q}}$. For any maximal ideal m in R, $R/m = \overline{\mathbb{Q}}$. The reduction (A', i') of (A, i) mod m with A' nonsingular is still of CM type (E, Φ) as the CM type is determined by the set of eigenvalues of a generator e of E over $\mathbb{Q}$ acting on the tangent space and the set is unchanged whether the ground ring is $\mathbb{C}$, R or $\overline{\mathbb{Q}}$. Thus $\exists$ isogeny $(A', i')_{\mathbb{C}} \longrightarrow (A, i)$ whose kernel is a subgroup of $A'(\mathbb{C})_{tor} = A'(\overline{\mathbb{Q}})_{tor}$ and $(A'/\ker, i')$ is a model of (A, i) over $\overline{\mathbb{Q}}$. ///

RMK. Any elliptic curve over $\mathbb{C}$ of CM type must have algebraic j-inv.

$\mathcal{O}_{K,\mathfrak{p}}$ DVR, AV over $\mathcal{O}_K/\mathfrak{p}$ can always be lifted to $\mathcal{O}_{K,\mathfrak{p}}$.

K number field, A/K AV, $\mathfrak{p}$ prime ideal of $\mathcal{O}_K$.

(abelian) smooth proper group scheme

A has good reduction at $\mathfrak{p}$ if it has a model over $\mathcal{O}_{K,\mathfrak{p}}$.

Embed A as a closed subvariety of $\mathbb{P}^n_K$, for each $P(x_0, \dots, x_n)$ in the homogeneous ideal defining A, multiply P by element in K so that $P \in \mathcal{O}_{K,\mathfrak{p}}[x_0, \dots, x_n]$. Let $k = \mathcal{O}_K/\mathfrak{p}$. $\bar{P}$ reduction of P in $k[x_0, \dots, x_n]$ and $\bar{A}$ the zero locus of these $\bar{P}$ inside $\mathbb{P}^n_k$. Then A has good reduction at $\mathfrak{p}$ if we can choose the embedding s.t. $\bar{A}$ is AV/k. In this case, up to canonical isom. $\bar{A}$ is independent of choices and for $\ell \neq \operatorname{char} k$, $V_\ell A \xrightarrow{\sim} V_\ell \bar{A}$, $\operatorname{End} A \hookrightarrow \operatorname{End} \bar{A}$.

Prop. (A, i) AV of CM type (E, Φ) over number field $K \subset \mathbb{C}$, $\mathfrak{p}$ prime in $\mathcal{O}_K$. Then $\exists\ L/K$ finite extension s.t. A_L has good reduction at $\mathfrak{p}$.

Pf. Recall Neron-Ogg-Shafarevich criterion:

A AV/K number field has good reduction at $\mathfrak{p}$ iff for some $\ell \neq \operatorname{char}(\mathcal{O}_K/\mathfrak{p})$, the inertia group I at $\mathfrak{p}$ acts trivially on $T_\ell A$.

///

AV over a finite field.

$V/\mathbb{F}_q$ variety, $\pi_V : V \to V$ the absolute Frobenius. If $V = \operatorname{Spec} A$, the map is just $a \mapsto a^q$. For any $V \xrightarrow{\alpha} W$, $\alpha \circ \pi_V = \pi_W \circ \alpha$.

Thm. (Weil) $A/\mathbb{F}_q$ AV, $\operatorname{End}^\circ A$ is finite dimensional semisimple $\mathbb{Q}$-algebra with π_A in the center and for every embedding $\rho : \mathbb{Q}[\pi_A] \to \mathbb{C}$, $|\rho(\pi_A)| = q^{\frac{1}{2}}$.

In case A simple, $\operatorname{End}^\circ A$ simple, $\mathbb{Q}[\pi_A]$ field, π_A algebraic integer.

An algebraic integer π is a Weil q-integer if for all embeddings $\rho : \mathbb{Q}[\pi] \to \mathbb{C}$ $|\rho(\pi)| = q^{\frac{1}{2}}$. Then $\rho(\pi) \cdot \overline{\rho(\pi)} = q = \rho(q) = \rho(\pi) \cdot \rho(\frac{q}{\pi})$, $\rho(\frac{q}{\pi}) = \overline{\rho(\pi)}$ hence $\rho(\mathbb{Q}[\pi])$ is stable under complex conjugation and the automorphism sending π to $\frac{q}{\pi}$ induced by complex conjugation is independent of ρ.

$\Rightarrow \mathbb{Q}[\pi]$ is a CM field or $\mathbb{Q}[\pi] = \mathbb{Q}(\sqrt{q})$

Lemma. Let $\pi, \pi' \in E$ be Weil q-integers. If $\operatorname{ord}_v \pi = \operatorname{ord}_v \pi'$ for all $v | p$ then $\pi' = \zeta \pi$ for some root of unit ζ in E.

Pf. $\frac{q}{\pi}$ is also an alg. integer as it is $\bar{\pi}$ $\Rightarrow \operatorname{ord}_v \pi = 0$, $\forall$ finite $v \nmid p$.

Hence $\operatorname{ord}_v \pi = \operatorname{ord}_v \pi'$, $\forall v$ $\Rightarrow \frac{\pi}{\pi'}$ is a root of unity. ///

The Shimura - Taniyama formula.

Lemma. (A, i) AV / K number field of CM type (E, Φ) with good reduction at $\mathfrak{p}$ to $(\bar{A}, \bar{i}) / \kappa$, $\kappa = \mathcal{O}_K/\mathfrak{p} = \mathbb{F}_q$. Then $\pi_{\bar{A}} \in \bar{i}(E)$.

Pf. Write $\pi = \pi_{\bar{A}}$. As $V_\ell A$ is free $E \otimes_{\mathbb{Q}} \mathbb{Q}_\ell$ - mod of rank 1, so is $V_\ell \bar{A}$. Hence the action of π on $V_\ell \bar{A}$ commutes with the action of $E \otimes \mathbb{Q}_\ell$, π itself lies in $E \otimes \mathbb{Q}_\ell$ hence $\bar{i}(E) \otimes_{\mathbb{Q}} \mathbb{Q}_\ell \cap \mathrm{End}^\circ \bar{A} = \bar{i}(E)$. ///

Thm. Assume further that $K/\mathbb{Q}$ Galois and $E \subset K$. Then for $\forall\, v | p$ of E

$$\frac{\mathrm{ord}_v \pi_{\bar{A}}}{\mathrm{ord}_v q} = \frac{|\Phi \cap H_v|}{|H_v|}$$

where $H_v = \{ \rho : E \to K \mid \rho^{-1}\mathfrak{p} = \mathfrak{p}_v \}$.

① $E/\mathbb{Q}$ Galois, $K = E$, $\mathfrak{p} = v_0$, $H_{v_0} = D_{v_0}$
$H_v = \sigma D_{v_0}$, $\sigma^{-1} v_0 = v$, all H_v have same size.

② v comes from a nonsplit place of F
$\Rightarrow v = \bar{v}$, $|\Phi \cap H_v| = \frac{1}{2}|H_v|$.

RMK.

(a) The theorem determines π up to a root of unity and depends only on the CM type (E, Φ). Thus different pairs over K of CM type (E, Φ) could give different π, but they differ only by a root of unity.

(b) $*$ complex conjugation on $\mathbb{Q}[\pi]$. As $\pi\pi^* = q$, $\mathrm{ord}_v \pi + \mathrm{ord}_v \pi^* = \mathrm{ord}_v q$.
Also $\mathrm{ord}_v \pi^* = \mathrm{ord}_{v^*} \pi$ and $\overline{\Phi \cap H_{v^*}} = \bar{\Phi} \cap H_v$. Thus

$$\frac{\mathrm{ord}_v \pi}{\mathrm{ord}_v q} + \frac{\mathrm{ord}_v \pi^*}{\mathrm{ord}_v q} = \frac{|\Phi \cap H_v| + |\bar{\Phi} \cap H_v|}{|H_v|} = 1.$$

Pf. Assume p unramified in E.

$K_\mathfrak{P} / \mathbb{Q}_p$ finite extension, base change A to $K_\mathfrak{P}$, E still acts on A.

Let $T = T_0 A$, it is an $E \otimes_\mathbb{Q} K_\mathfrak{P}$ space, as $K_\mathfrak{P}$ contains all conjugates of E, $T \simeq \bigoplus_{\varphi \in \Phi} K_{\mathfrak{P}, \varphi}$.

A has good reduction at $\mathfrak{P}$, $\exists$ model $\mathcal{A}$ over $O_{K_\mathfrak{P}}$.

$\mathcal{T} = T_0 \mathcal{A}$, $\mathcal{T} \otimes_{O_{K_\mathfrak{P}}} K_\mathfrak{P} \simeq T$, $\mathcal{T} / \mathfrak{P} \mathcal{T} \simeq T_0 \bar{\mathcal{A}} = T_0$

(p) unramified in $O_E \Rightarrow O_E \otimes_\mathbb{Z} \mathbb{Z}_p$ etale over $\mathbb{Z}_p \Rightarrow O_E \otimes_\mathbb{Z} O_{K_\mathfrak{P}}$ etale over $O_{K_\mathfrak{P}} \Rightarrow O_E \otimes_\mathbb{Z} O_{K_\mathfrak{P}} \simeq \prod_{\sigma: E \to K_\mathfrak{P}} O_\sigma$, where $O_\sigma \simeq O_{K_\mathfrak{P}}$ with O_E act by σ.

The finitely generated projective $O_E \otimes_\mathbb{Z} O_{K_\mathfrak{P}}$ module $\mathcal{T}$ is direct sum of O_σ, and from $T \simeq \bigoplus_{\varphi \in \Phi} K_{\mathfrak{P}, \varphi}$ we see $\mathcal{T} \simeq \bigoplus_{\varphi \in \Phi} O_\varphi$.

As $\pi \bar{\pi} = q$, $(\pi) = \prod_{v | p} P_v^{m_v}$.

For h class number of E, $P_v^{m_v h} = (\gamma_v)$, $\gamma_v \in O_E$.

$\Phi_v = \Phi \cap H_v = \{ \varphi \in \Phi \mid \varphi^{-1} \mathfrak{P} = P_v \}$, $d_v = |\Phi_v|$.

The kernel of $\gamma_v : T_0 \to T_0$ is the span of e_φ for which $\varphi(\gamma_v) \in \mathfrak{P}$, i.e. $\varphi^{-1} \mathfrak{P} = P_v$.

As $\pi^h : A_0 \to A_0$ factors through γ_v, $k_0(A_0)^{q^h} = (\pi^h)^* k_0(A_0) \subset (\gamma_v)^* k_0(A_0)$

$\Rightarrow \deg(A_0 \xrightarrow{\gamma_v} A_0) \le q^{h d_v}$

$\deg(A_0 \xrightarrow{\gamma_v} A_0) = Nm_{E/\mathbb{Q}}(\gamma_v) = Nm_{E/\mathbb{Q}}(P_v^{h m_v})$

$Nm_{E/\mathbb{Q}}(\pi) \le q^g$ $\qquad \Rightarrow \quad Nm_{E/\mathbb{Q}}(P_v^{m_v}) = q^{d_v} = (Nm_{K/\mathbb{Q}} \mathfrak{P})^{d_v}$

$\overset{\triangle}{|\Phi| = g}$

$\parallel$

$\deg(A_0 \xrightarrow{\pi} A_0) = q^g$

$$(Nm_{K/\mathbb{Q}}\,\mathfrak{P})^{d_w} = \prod_{\varphi\in\Phi_v}(Nm_{K/\mathbb{Q}}\,\mathfrak{P}) = \prod_{\varphi\in\Phi_v} Nm_{E/\mathbb{Q}}(\varphi^{-1} Nm_{K/\varphi E}\,\mathfrak{P})$$

$$= Nm_{E/\mathbb{Q}}\Big(\prod_{\varphi\in\Phi_v}\varphi^{-1} Nm_{K/\varphi E}\,\mathfrak{P}\Big)$$

$$\Rightarrow \mathfrak{p}_v^{m_v} = \prod_{\varphi\in\Phi_v}\varphi^{-1} Nm_{K/\varphi E}\,\mathfrak{P}$$

$$\Rightarrow (\pi) = \prod_{\varphi\in\Phi}\varphi^{-1} Nm_{K/\varphi E}\,\mathfrak{P}$$

$$\mathrm{ord}_v\,\pi = \sum_{\varphi\in\Phi}\mathrm{ord}_v\,\varphi^{-1} Nm_{K/\varphi E}\,\mathfrak{P} = \sum_{\varphi\in\Phi}\mathrm{ord}_{\varphi v}\,Nm_{K/\varphi E}\,\mathfrak{P} = \sum_{\varphi\in\Phi_v} f(\mathfrak{P}/\varphi_v)$$

p unramified in E, $\mathrm{ord}_v p = 1$, $\mathrm{ord}_v q = f(\mathfrak{P}/p)$

$$\frac{\mathrm{ord}_v\,\pi}{\mathrm{ord}_v\,q} = \frac{\sum_{\varphi\in\Phi_v} f(\mathfrak{P}/\varphi_v)}{f(\mathfrak{P}/p)} = \sum_{\varphi\in\Phi_v}\frac{1}{f(\mathfrak{P}_v/p)} = \frac{|\Phi\cap H_v|}{|H_v|}.$$

Alternative proof.

Let A model over O_{K_w}, w place of K corresponding to $\mathfrak{P}$.

After a possible isogeny, assume $\pi\in O_E$.

The p-divisible group $\{A[p^n]\}$ over O_{K_w}, O_E acts on $A[p^n]$ factoring through $O_E/p^n \simeq \prod_{v|p} O_{E_v}/p^n$. Correspondingly $A[p^n] = \prod_{v|p} G_{v,n}$ and each $G_v = \{G_{v,n}\}$ is again p-divisible group over O_{K_w} of $\underline{\text{height } [E_v:\mathbb{Q}_p]}$.

$= |H_v|$.

Recall Serre - Tate thm:

(R, m) complete local Noetherian ring with residue char p

G connected p-divisible group over R of height h, then $\mathcal{O}_G = \varprojlim \mathcal{O}_{G_n}$

is topologically isom. to $R[\![X_1, \dots, X_d]\!]$ with (m, X)-adic topology, hence a commutative formal Lie group for which $[p]$ is finite flat of deg p^h.

$\{A[p^n]^\circ\} \rightsquigarrow \hat{A}_0$

$\{G^\circ_{v,n}\} \rightsquigarrow \hat{G}_v$

$$\prod_{v|p} \hat{G}_v = \hat{A}_0$$

$\dim \hat{A}_0 = \dim A = |\Phi| \Rightarrow \sum_{v|p} \dim \hat{G}_v = |\Phi|.$

Claim $\dim \hat{G}_v = |\Phi_v|$.

$\prod_{v|p} T(\hat{G}_v) = T(\hat{A}_0)$, $T(\hat{G}_v)$ is $\mathcal{O}_{E_v} \otimes_{\mathbb{Z}_p} \mathcal{O}_{K_w}$ component of $T(\hat{A}_0)$ as $\mathcal{O}_E \otimes_{\mathbb{Z}} \mathcal{O}_{K_w} \simeq \mathcal{O}_{E,p} \otimes_{\mathbb{Z}_p} \mathcal{O}_{K_w}$ - module. Compute the dimension at generic fibre of $\operatorname{Spec} \mathcal{O}_{K_w}$ and base change to $\overline{\mathbb{Q}}_p$, $T_0(A_{\overline{\mathbb{Q}}_p}) \simeq \prod_{\varphi \in \Phi} (\overline{\mathbb{Q}}_p)_\varphi$ hence the dimension correspond to v component is exactly $|\Phi_v|$.

Write $[E_v : \mathbb{Q}_p] = h$, $|\Phi_v| = d$, $\dfrac{\operatorname{ord}_v \pi}{\operatorname{ord}_v q} = \dfrac{d}{h} \Leftrightarrow \dfrac{\pi^h}{q^d}$ is a unit.

Consider the connected - etale sequence

$$0 \to G_v^\circ \to G_v \to G_v^{et} \to 0$$

Pass to generic fibre then take Tate module

$$0 \to T_p(G_v^\circ)_{K_w} \to T_p(G_v)_{K_w} \to T_p(G_v^{et})_{K_w} \to 0$$

and the middle term is free O_{E_v}-module of rank 1. As each term is finite free O_{E_v}-module, either $G_v^\circ = 0$ or $G_v^{et} = 0$.

Suppose $G_v^\circ = 0$ so G_v is etale. Then $d = 0$, Frob acts as an aut $\Rightarrow \pi$ is a unit in O_{E_v}, π^n / q^d is a unit.

Suppose $G_v^{et} = 0$ so G_v is connected. Note that the map $[p]$ on G_v is finite flat of order $p^n = |p|_{E_v}$ thus the map

$$O_{E_v} - \{0\} \to p^{\mathbb{Z}}$$

$$x \mapsto \deg([x]_{G_v})$$

agrees with $|\cdot|_{E_v}$.

ETS π^n and q^d have the same degree.

$\deg [q^d]_{G_v} = q^{dn}$.

To show $\deg [\pi]_{G_v} = q^d$, look at the closed fibre where π acts via Frob. Note that the q-power map on $k[[x_1, \dots, x_d]]$ has degree q^d and as G_v connected, $\deg [\pi]_{G_v} = \deg [\pi]_{G_v^\circ}$

$$\overset{\text{Serre-Tate}}{=} \deg (\cdot)^q_{k[[x_1, \dots, x_d]]}$$

$$= q^d.$$

///